Coexistence of IEEE 802.11b/g WLANs and IEEE 802.15.4 WSNs: Modeling and Protocol Enhancements

Proefschrift

ter verkrijging van de graad van doctor
aan de Technische Universiteit Delft,
op gezag van de Rector Magnificus Prof. ir. K.Ch.A.M. Luyben,
voorzitter van het College voor Promoties,
in het openbaar te verdedigen op dinsdag 6 september 2011 om 15.00 uur

door

Wei YUAN

elektrotechnisch ingenieur
geboren te Baiyin, China.

Dit proefschrift is goedgekeurd door de promotor:
Prof.dr.ir. I.G.M.M. Niemegeers

Samenstelling promotiecommissie:

Rector Magnificus,	Voorzitter
Prof.dr.ir. I.G.M.M. Niemegeers,	Technische Universiteit Delft, promotor
Prof.dr.ir. S.M. Heemstra de Groot,	Technische Universiteit Delft
Prof.dr.ir. N.H.G. Baken,	Technische Universiteit Delft
Dr.ir. J. Weber,	Technische Universiteit Delft
Prof.dr.ir. I. Moerman,	Universiteit Gent
Prof.dr.ir. C.H. Slump,	Universiteit Twente
Dr.ir. M.J. Bentum,	Universiteit Twente

ISBN 978-94-6191017-2

NUR 959

Keywords: Wireless Sensor Network, IEEE 802.15.4, ZigBee, Coexistence, Interference

This research was partially supported by the Dutch Ministry of Economic Affairs through the project PNP2008 under the Freeband Communication Impulse of the technology programme.

Cover design by Di Wang and Wei Yuan

Printed in The Netherlands

Acknowledgements

A voyage exploring uncharted waters would be less daunting and more rewarding if one were kept in company. This thesis is the destination of such a journey that I embarked on five years ago. Thanks to the faithful companionship and all sorts of supports from many people, I have accomplished what I set out to do. Now comes the pleasant moment to express my gratitude.

First of all I am deeply indebted to my promotor Prof. Ignas Niemegeers. It was his guidance, insights, support and encouragement that helped me throughout all the time of research for and writing of this thesis. Ignas has a great sense of humor, which made our every conversation never boring and more importantly, reduced my stress and strengthened me to overcome the next challenge.

Besides, I own great gratitude to Prof. Jean-Paul Linnartz for offering me a research position with a trajectory towards a PhD in Philips Research, and for his insightful comments to my thesis work as well.

Further, I would like to thank Prof. Sonia Heemstra de Groot, Prof. Nico Baken, Dr. Jos Weber, Prof. Ingrid Moerman, Prof. Kees Slump and Dr. Mark Bentum for being in the Doctorate Committee and for providing valuable feedback to this thesis.

I would also like to thank all my colleagues in the Distributed Sensor Systems (DSS) Group of Philips Research. I benefited a lot from the discussions with them. I am thankful to Xiaolei Cui, a student who contributed to this thesis work in his Master project with me.

I own gratitude to Martin Jacobsson for his lots of help in editing this thesis and in the preparation for my PhD defense. Your replies to my emails are always amazingly quick!

I thank to Eric Sloof for translating the summary and propositions into Dutch. Buddy, I wish you much luck and success in the New York marathon!

Moreover, I would like to extend my grateful thanks to Chin Keong, Hongming, Yuki and Ah Hung, Han Jungong and Chunmei, Ashish, and numerous others. Your friendship and companionship brought so much fun into my life in Eindhoven.

Finally, I want to thank my family - my parents, my parent-in-laws, my brother and my wife, for always being there for me. Without your love and support, I would never have been able to get through so many challenges, and to be who I am today and to be where I am standing now.

To my parents, brother and wife.

Contents

Chapter 1

Introduction

In the past decades, information processing technology has been developed greatly. The most common form of information processing has happened on large, general-purpose computational devices, ranging from old-fashioned mainframes to modern laptops. In many applications, like office applications, these computational devices are mostly used to process information that is at its core centered around a human user of a system, but is at best indirectly related to the physical environment. In another class of applications, the physical environment is at the focus of attention. Computation is used to exert control over physical processes, for example, when controlling chemical processes in a factory for correct temperature and pressure. Here, the computation is integrated with the control; it is embedded into a physical system. Unlike the former class of systems, such embedded systems are usually not based on human interaction but are rather required to work without it; they are intimately tied to their control task in the context of a larger system [Kar07].

Technological progress is about to take the spreading of embedded control in our daily lives a step further. Eventually, computation will surround us in our daily lives, realizing a vision of “Ambient Intelligence” [Zel98][Aar01] where many different devices will gather and process information from many different sources to both control physical processes and to interact with human users. To realize this vision, a crucial aspect is needed in addition to computation and control: communication. All these sources of information have to be able to transfer the information to the place where it is needed - an actuator or a user - and they should collaborate in providing as precise a picture of the real world as is required [Kar07]. Recent technological improvements have made the deployment of small, low-cost, low-power, distributed sensors, which are capable of local processing and information transferring, a reality. Each sensor node is capable of only a limited amount of processing. But when coordinated with a large number of other nodes, they have the ability to sense or control physical parameters in a given environment in great detail. Thus, a sensor network can be described as a collection of sensor nodes which co-ordinate to fulfill some specific tasks [Bha04].

Previously, a sensor network consisted of small number of sensor nodes that were wired to a central processing station. However, nowadays, the focus is more on wireless, distributed, sensing nodes. This is because installing wires for sensors are expensive (figures up to US$200 for a single sensor in addition to the cost of the sensor can be found in [Rab00]), in particular, given the large number of devices that are imaginable in our environment; wires constitute a maintenance problem; wires prevent entities from being mobile; and wires can prevent sensors from being close to the phenomenon that they are supposed to control. Hence, wireless communication between such devices is, in many application scenarios, an inevitable requirement. To meet this requirement, a new class of networks has appeared in the last few years: the so-called Wireless Sensor Networks (WSNs) (See e.g., [Pot00][Aky02]).

In addition to the wireless communication capability, a distributed sensing capability is also desirable for WSNs. This is because when the exact location of a particular phenomenon is unknown, distributed sensing allows for closer placement to the phenomenon than a single sensor could be. Also, in many cases, multiple distributed sensor nodes are needed to overcome environmental obstacles. Another requirements for WSNs would be distributed processing capability. This is necessary as communication is a major consumer of energy. While a “Moore’s Law” exists for power consumption of microprocessors with mW/MIPS decreasing by a factor of ten every five year, there is no such similar trend in wireless communications. For example, it is estimated that nearly 80% of the power consumed by wearable computers can be due to communications[Sie01]. A centralized sensor network would mean that some of the sensors would need to communicate over long distances leading to even more energy depletion. Hence, it would be a good idea to process locally as much information as possible in order to minimize the total number of bits transmitted [Bha04]. In addition, communication may not be reliable, particularly in the presence of interference. Therefore, processing information locally can also reduce the unreliable communication and therefore make a WSN more robust against interference. Interference robustness of WSNs is the topic of this thesis.

In the remainder of this chapter, we first introduce IEEE 802.15.4 [IEE06] and ZigBee [Zig07c], the protocols most widely used for WSNs. We then present the problem statement. The research motivation, targets and scope, and contributions of this thesis are then presented, followed by a chapter-based overview of this thesis.

1.1 IEEE 802.15.4 and ZigBee

As IEEE 802.15.4 and ZigBee are the most widely used protocols for WSNs, we focus on IEEE 802.15.4/ZigBee-based WSNs in this thesis.

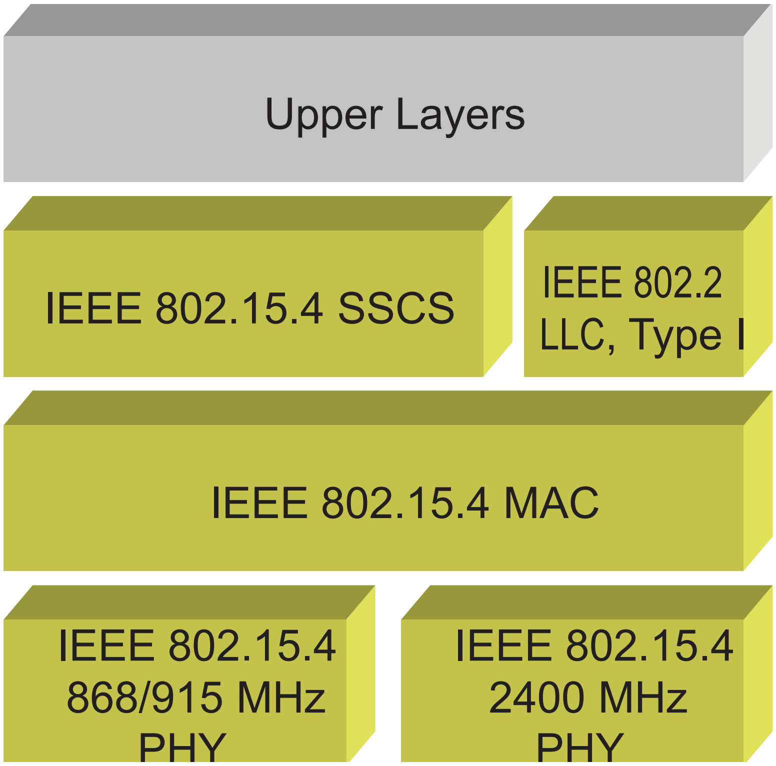


Figure 1.1: IEEE 802.15.4 Architecture

1.1.1 IEEE 802.15.4

The IEEE 802.15.4 protocol [IEE06] specifies the Medium Access Control (MAC) sub-layer and the physical layer (PHY) for Low-Rate Wireless Personal Area Networks (LR-WPANs) (see Figure 1.1).

Note that even though this standard was not specifically developed for WSNs, it is intended to be suitable for them since WSNs can be built up from LR-WPANs. In fact, the IEEE 802.15.4 protocol targets low-data rate, low power consumption, and low cost wireless networking, which typically fits the requirements of WSNs [Kou05]. As shown in Figure 1.2 and Table 1.1, the intent of IEEE 802.15.4 is not to compete with other wireless networking technologies but to complement the range of available wireless technologies in the lower end of the spectrum of data rates, power consumption, and cost. Although possible for certain applications, IEEE 802.15.4 was not designed to overlap its application space with other wireless networking standards.

PHY Layer

The physical layer (PHY) provides the data transmission service, as well as the interface to the physical layer management entity, which offers access to every layer management function and maintains a database of information on related personal area networks. Thus, PHY manages the physical RF

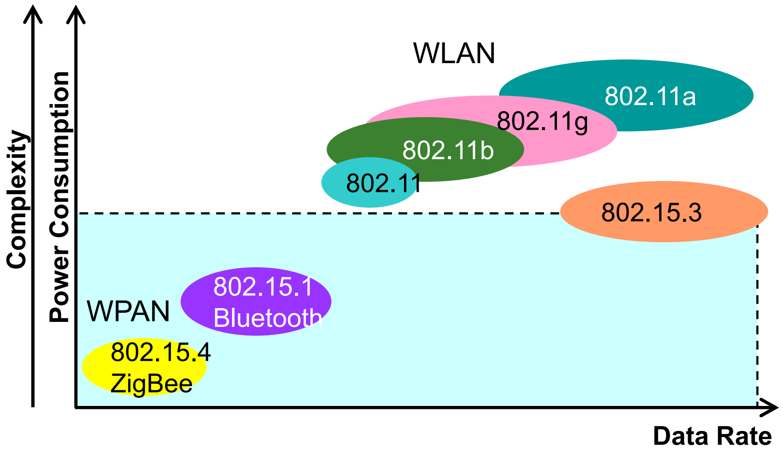


Figure 1.2: Operating space of various WLAN and WPAN standards[Gut03]

Table 1.1: Comparison of IEEE 802.15.4 with other wireless technologies

	IEEE 802.11b	**Bluetooth**	**IEEE 802.15.4**
Range	∼100 m	∼10 - 100 m	10 m
Data Rate	∼2 - 11 Mb/s	1 Mb/s	≤ 0.25 Mb/s
Power Consumption	Medium	Low	Ultra Low
Size	Large	Smaller	Smallest
Cost and Complexity	High	Medium	Very Low

transceiver and performs channel selection and energy and signal management functions. As shown in Figure 1.3, the IEEE 802.15.4 PHY offers three operational frequency bands:

- 868.0-868.6 MHz: Europe, allows one communication channel
- 902-928 MHz: North America, up to ten channels [IEE03c], extended to thirty [IEE06]
- 2400-2483.5 MHz: worldwide use, up to sixteen channels

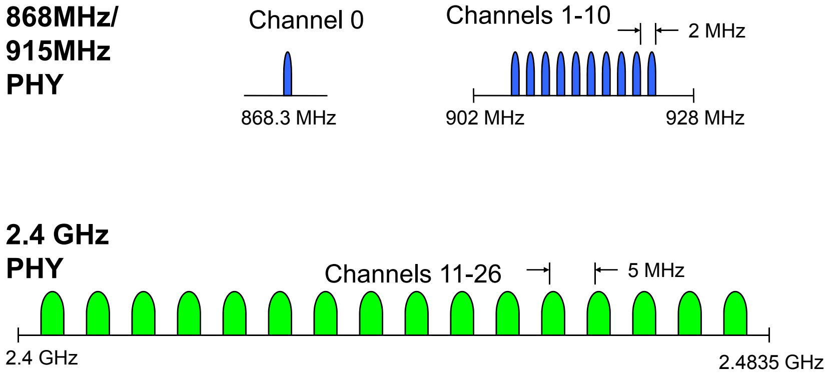


Figure 1.3: IEEE 802.15.4 PHY overview

The original 2003 version of the standard [IEE03c] specifies two physical layers based on Direct Sequence Spread Spectrum (DSSS) techniques: one working on the 868/915 MHz bands with data rates of 20 and 40 kbit/s, and one in the 2450 MHz band with a rate of 250 kbit/s. The 2006 revision [IEE06] improves the maximum data rates of the 868/915 MHz bands, bringing them up to support 100 and 250 kbit/s as well. Moreover, it goes on to define four physical layers depending on the modulation method used. Three of them preserve the DSSS approach: in the 868/915 MHz bands, using either binary or offset quadrature phase shift keying; in the 2450 MHz band, using the latter. Dynamic switching between supported 868/915 MHz PHYs is allowed.

MAC Sub-layer

The MAC sub-layer of the IEEE 802.15.4 protocol provides an interface between the physical layer and the higher layer protocols of LR-WPANs. The MAC sub-layer of the IEEE 802.15.4 protocol has many common features with that of the IEEE 802.11 protocol, such as the use of CSMA/CA (Carrier

Sense Multiple Access / Contention Avoidance) as a channel access mechanism and the support of contention-free and contention-based periods. However, the specification of the IEEE 802.15.4 MAC sub-layer is adapted to the requirements of LR-WPANs by, for instance, eliminating the RTS/CTS (Request to Send / Clear to Send) mechanism used in IEEE 802.11. The MAC protocol supports two operational modes as follows [Kou05]:

- Beacon-enabled mode: beacons are periodically generated by the coordinator to synchronize attached devices. A beacon frame is (the first) part of a superframe, which also embeds all data frames exchanged between the devices and the PAN coordinator. A device has to be synchronized to the coordinator and frame transmissions can only start at the beginning of time slots.
- Non Beacon-enabled mode: in non beacon-enabled mode, the devices can simply send their frames by using unslotted CSMA/CA. There is no use of a superframe structure in this mode.

Figure 1.4 presents a structure of the IEEE 802.15.4 operational modes. In this thesis, we focus on only the popular non beacon-enabled mode and the unslotted CSMA/CA.

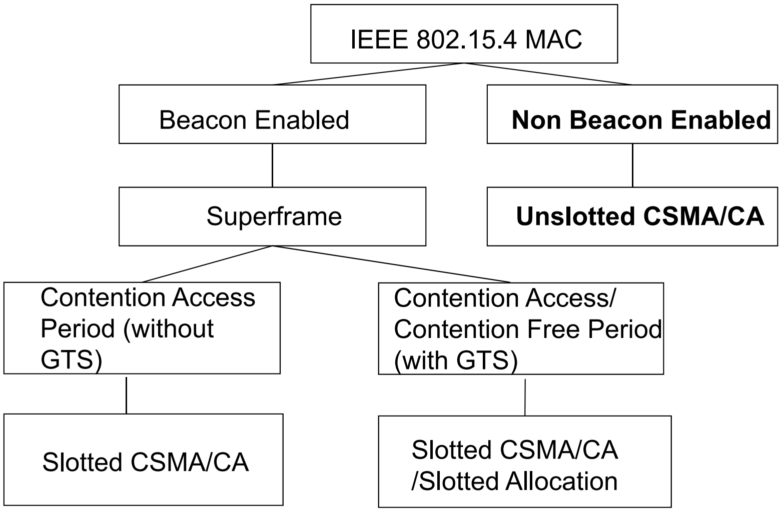

IEEE 802.15.4 MAC
Beacon Enabled
Non Beacon Enabled
Superframe
Unslotted CSMA/CA
Contention Access Period (without GTS)
Contention Access/ Contention Free Period (with GTS)
Slotted CSMA/CA
Slotted CSMA/CA /Slotted Allocation

Figure 1.4: IEEE 802.15.4 operational modes [Kou05]

Device Types

IEEE 802.15.4 networks support two different types of devices: Full Function Devices (FFDs) and Reduced Function Devices (RFDs). An FFD is a device that can support three operation modes, serving as:

- A Personal Area Network (PAN) Coordinator: the principal controller of the PAN. This device identifies its own network, to which other devices may be associated.
- A Coordinator: provides synchronization services through the transmission of beacons. Such a coordinator must be associated to a PAN coordinator and does not create its own network.
- A simple device: a device which does not implement the previous functionalities.

An RFD is a device operating with minimal implementation of the IEEE 802.15.4 protocol. An RFD is intended for applications that are extremely simple, such as a light switch or a passive infrared sensor; they do not have the need to send large amounts of data and may only associate with a single FFD at a time. An IEEE 802.15.4 network must include at least one FFD acting as a PAN coordinator that provides global synchronization services to the network and manages potential FFDs and RFDs.

1.1.2 ZigBee

ZigBee [Zig07c] is the set of specifications built on the top of the IEEE 802.15.4 2003 version standard [IEE03c] and adding network, security and application services as depicted in Figure 1.5. The name “ZigBee” is derived from the erratic zigging patterns many bees make between flowers when collecting pollen. This is evocative of the invisible webs of connections existing in a fully wireless environment [McG10]. The standard itself is regulated by a group known as the ZigBee Alliance, with over 150 members worldwide including Philips. The mission of the ZigBee Alliance is to enable reliable, cost-effective, low-power, wirelessly networked, monitoring and control products based on an open global standard, and the goal is to provide consumers with ultimate flexibility, mobility, and ease of use by building wireless intelligence and capabilities into everyday devices [Zig10].

Device Types

There are three different types of ZigBee devices:

- ZigBee coordinator (ZC): The most capable device, the coordinator forms the root of the network tree and might bridge to other networks. There is exactly one ZigBee coordinator in each network since it is the device that started the network originally. It is able to store information about the network, including acting as the Trust Centre & repository for security keys. A ZC is an FFD.
- ZigBee Router (ZR): As well as running an application function, a router can act as an intermediate router, passing on data from other devices. A ZR is also an FFD.

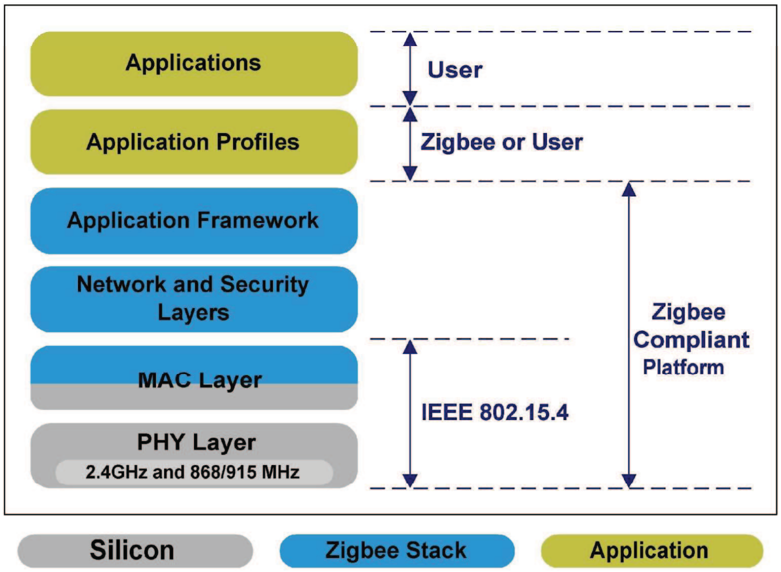


Figure 1.5: ZigBee Protocol Stack

- ZigBee End Device (ZED): Contains just enough functionality to talk to the parent node (either the coordinator or a router); it cannot relay data from other devices. This relationship allows the node to be asleep a significant amount of the time thereby giving long battery life. A ZED requires the least amount of memory, and therefore can be less expensive to manufacture than a ZR or ZC. A ZED is an RFD.

Network Topologies

ZigBee supports three different network topologies: star, mesh, and cluster tree (also called star-mesh hybrid), as illustrated in Figure 1.6. The cluster tree topology is less efficient in a sense of communication among devices than the other two, and is therefore rarely (if ever) implemented.

In a star topology, also called point-to-point, all devices are within direct communication range to the coordinator, through which all messages are routed. A device sends a message to the coordinator, which then passes it on to the destination device. Direct communication between the end devices is not supported. The benefits of the star topology are its simplicity since it does not require a complex network layer or routing protocols, and its high performance since it takes a maximum of two hops for packets to reach their destination. However, the limitations of this topology are its lack of robustness since there are no alternative paths between a device and the coordinator - if a path becomes obstructed, communication is lost between the device and coordinator, and its limited radio range between the coordinator and child devices.

The mesh topology, also called peer-to-peer, consists of a mesh of in-

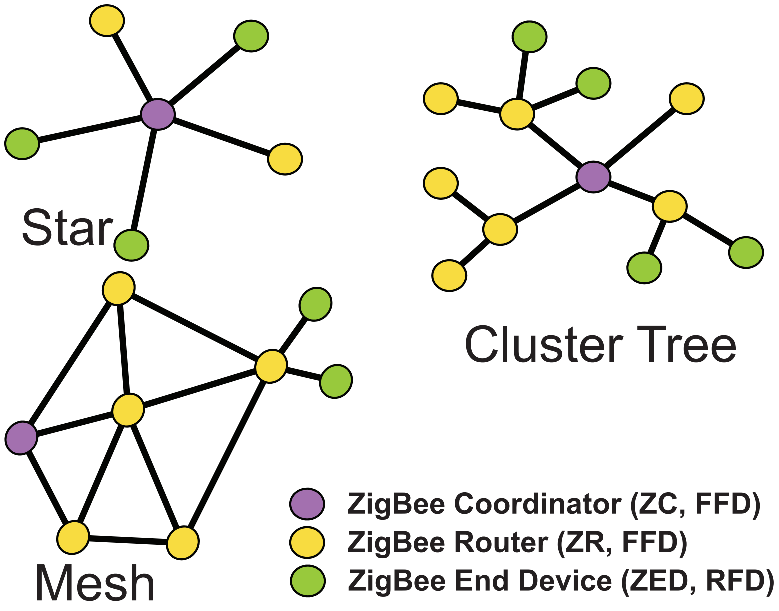


Figure 1.6: ZigBee Network Topologies

terconnected routers and end devices. Each router is typically connected through at least two pathways, and can relay messages for its neighbors. The mesh topology supports "multi-hop" communications, through which data is passed by hopping from device to device using the most reliable communication links and most cost-effective path until its destination is reached. The multi-hop ability also helps to provide fault tolerance, in that if one device fails or experiences interference, the network can reroute itself using the remaining devices. This topology is highly reliable and robust. Should any individual router become inaccessible, alternative routes can be discovered and used. Besides, the use of intermediary devices in relaying data means that the range of the network can be significantly increased, making this topology highly scalable. On the other hand, however, this topology has a higher communications overhead than the star topology, which can result in increased latency and lower end-to-end performance. In addition, the meshed routing requires more complex network protocols. This means routers require more embedded resources, which can result in increased power consumption and costs.

Application Profiles

Application Profiles are an agreement on [Ash09]:

- A set of network and security policies to allow interoperability while providing the appropriate controls
- Definition of specific device types related to that application (using items from a library of functions or creating new if necessary)

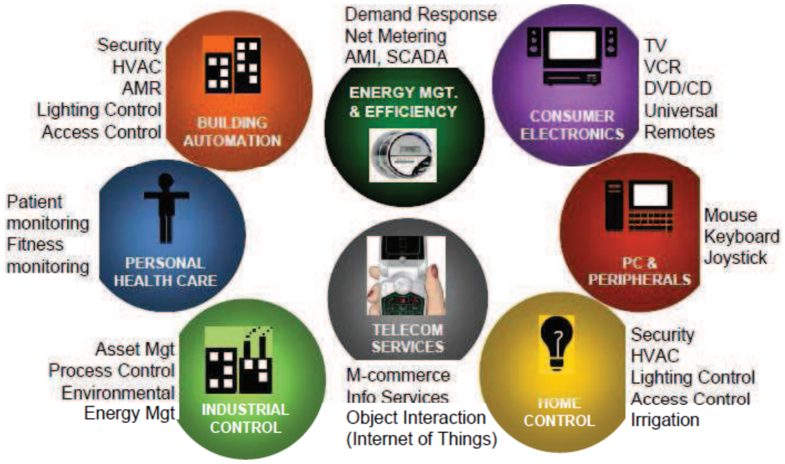


Figure 1.7: ZigBee Application Profiles [Ash09]

- Defining a series of messages and attributes for a device

Designed by end users, equipment providers, service providers with assistance from stack providers, profiles define how to use the underlying stack features. ZigBee targets a wide range of application profiles including home control, industrial control, consumer electronics, PC & peripherals, energy management, building automation, telecom services, personal healthcare, etc., as summarized in Figure 1.7.

1.2 Problem Statement

As mentioned in Section 1.1.1, IEEE 802.15.4/ZigBee mainly operates on the 2.4 GHz ISM band. In addition to IEEE 802.15.4/ZigBee, there are many other systems such as IEEE 802.11b/g Wireless Local Area Networks (WLANs), Bluetooth, cordless phones and even microwave ovens, using the same band, as illustrated in Figure 1.8. This is because the 2.4 GHz ISM band is license-free and deployable almost worldwide. However, as the popularity of these systems, particularly WLANs and WPANs, increases, the 2.4 GHz ISM band becomes more crowded, which leads to the systems' QoS (Quality of Service) degradation. Therefore, it is important to investigate the coexistence among these different systems.

According to IEEE 802.15.2 [IEE03a], "coexistence" is defined as the ability of one system to perform a task in a given shared environment where other systems have an ability to perform their tasks and may or may not be using the same set of rules. What we focus on in this thesis is the coexistence among different systems, i.e., using a different set of rules, and in the 2.4 GHz unlicensed frequency band.

The coexistence of IEEE 802.11b WLANs and Bluetooth networks has been studied extensively.

Figure 1.8: Coexistence in 2.4 GHz ISM Band

The paper by Haartsen and Zürbes [Haa99] examined the impact an 802.11b network would have on Bluetooth performance. The approach used in [Haa99] was based on a combination of analytical and Monte Carlo simulations for a specific network configuration. In [How01a], the impact of Bluetooth on 802.11b was studied and a closed form analytical model was derived for evaluating the impact. The approach was illustrated by examining the coexistence between 802.11b and Bluetooth within typical operational ranges for both network traffic and RF environment. A similar approach was used to evaluate the impact of IEEE 802.11b on Bluetooth as reported in [How02]. Furthermore, Conti *et al.* derived an analytical methodology to evaluate the performance of a Bluetooth link interfered by IEEE802.11b, and *vice versa*, in a Rice/Rayleigh fading channel with Additive White Gaussian Noise (AWGN).

Due to the importance of coexistence of Bluetooth and IEEE 802.11 devices, both the Bluetooth Special Interest Group (SIG) and the IEEE 802 Working Group were actively looking at methods for improved coexistence. The IEEE 802.15.2 Task Group has been formed specifically to consider proposals for mechanisms to improve the level of coexistence between Bluetooth and IEEE 802.11 devices and to come up with recommended practices derived from these. We will discuss this further in Section 1.3.1.

Compared to the extensive work on the coexistence of IEEE 802.11b

WLANs and Bluetooth networks, less research has been done on the coexistence of IEEE 802.11b/g WLANs and IEEE 802.15.4/ZigBee WSNs, which is the focus of this thesis.

IEEE 802.15.4/ZigBee-based WSNs, having very low transmit power, are more vulnerable to the interference generated by other systems which have much higher power. For instance, Kim *et al.* presented in [Kim05] that 802.11 interference can cause serious performance degradation of 802.15.4 networks. The bad coexistence capability of 802.15.4/ZigBee WSNs in the presence of interference can lead to unacceptable user experiences if the interference is not mitigated sufficiently. For example, when a user presses a button of a remote controller using the 802.15.4/ZigBee protocol, a lamp may not respond within an acceptable latency or may not even respond at all if control commands in 802.15.4/ZigBee packets experience serious loss due to heavy WLAN interference. Such a coexistence issue may get more serious for a large scale multi-hop 802.15.4/ZigBee-based lighting control network, which typically covers many floors of a building. This is because:

- A channel free from WLAN interferences might not be consistently available to a whole ZigBee network
- A large number of hops may make the end-to-end packet delivery ratio unacceptably small in the presence of interferences
- The loss of ZigBee control messages, e.g., the message to change the operating channel, could prohibit a ZigBee network from operating resiliently

As a consequence, the lighting control network may not respond in a timely manner to a user's commands. Furthermore, part of the network may not be reachable and the user may lose control over part of the network and its associated lighting devices. Therefore, the coexistence issue between WSNs and other systems, and more generally, the spectrum sharing among different uncoordinated systems in the unlicensed band is a serious problem, which needs to be resolved properly.

In fact, there are three ways to share spectrum: *exclusive access*, *vertical sharing* and *horizontal sharing*. Exclusive access means that only a particular user can access the spectrum. A typical system which uses exclusive access is the cellular system. In spite of its immense success, this model often leads to inefficient spectrum usage in terms of spectral efficiency [Ben09]. A study [Mar02] conducted in the city of New York has shown that only 13% of the spectrum opportunities was utilized on average. This is due to two main reasons: firstly, the spectrum remains non-utilized during the time that the licensed systems are idle. Secondly, the spectrum can be congested in one area while being non-utilized in another due to a low spatial density of radio devices. Likewise, a spectrum occupancy measurement campaign carried out in the city of Chicago [McH06] corroborates the fact that there is a significant amount of non-utilized spectrum bands (i.e., white spectral bands). As a result, over the course of the last decade and motivated by the ever increasing

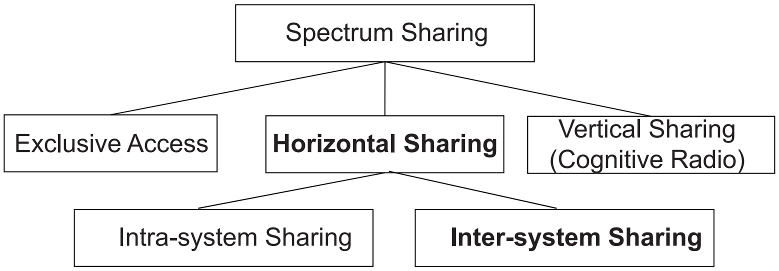


Figure 1.9: Classification/taxonomy of Spectrum Sharing Methods

demands for higher data rates and recent proliferation of networks operating on unlicensed bands such as IEEE 802.11 WLANs a migration from static to flexible and dynamic spectrum allocation has emerged as a new paradigm for more efficient resource allocations.

In [Kru03], Kruys firstly proposed the concepts of vertical sharing and horizontal sharing. The vertical sharing means that systems have different levels of regulatory status (e.g., newcomers that have to live together with incumbents), i.e., the primary user pays money for (primary) access to the spectrum, and the secondary user can borrow the spectrum only if it does not generate “harmful” interference to the primary user. Note that when one talks about *cognitive radio*, one usually means vertical sharing. In contrast, in horizontal sharing, all systems have the same regulatory status and may access spectrum on equal footing. In the horizontal sharing case, it is also useful to distinguish between “intra-system” sharing (between systems that are implemented using the same technology or technology family, e.g., 802.11b devices), and “inter-system” sharing (between technically distinct systems, e.g., 802.11 WLANs and 802.15.4 WSNs). Technical standards and coordination between standard bodies to facilitate efficient shared spectrum use is necessary, but not sufficient. It addresses the intra-system sharing case, but not inter-system sharing [Vri03].

In this thesis, we focus on an inter-system horizontal sharing - IEEE 802.15.4/ZigBee WSNs coexist with other systems in the unlicensed 2.4 GHz ISM frequency band. Figure 1.9 summarizes the classification/taxonomy for the spectrum sharing methods discussed above.

1.3 Coexistence Standardization Activities

The concerns on the coexistence of different wireless systems operating in unlicensed frequency bands has caused some standardization activities. IEEE 802.15.2 [IEE03a] addresses the issue of coexistence of wireless personal area networks (WPAN) with other wireless devices operating in unlicensed frequency bands such as wireless local area networks (WLAN). In the annex of the IEEE 802.15.4 standard [IEE06], several mechanisms that enhance coexistence for IEEE 802.15.4 devices with other wireless devices operating in the industrial, scientific and medical (ISM) bands are described.

We give a brief introduction as follows.

1.3.1 IEEE 802.15.2

IEEE 802.15.1-2002 [IEE02] has derived a Wireless Personal Area Network (WPAN) standard based on the Bluetooth v1.1 specifications. It includes a media access control and physical layer specification. Because both IEEE 802.15.1 and IEEE 802.11b specify operations in the same 2.4 GHz unlicensed frequency band, there is mutual interference between the two wireless systems that may result in severe performance degradation.

To address the coexistence issue between IEEE 802.15.1 devices and IEEE 802.11b devices, several coexistence mechanisms are described in IEEE 802.15.2 standard [IEE03a]. The mechanisms are divided into two classes: collaborative and non-collaborative. A collaborative coexistence mechanism can be used when there is a communication link between the WLAN networks. This is best implemented when both a WLAN and a WPAN device are embedded into the same piece of equipment (e.g., an IEEE 802.11b card and an IEEE 802.15.1 module embedded in the same laptop computer). A non-collaborative coexistence mechanism does not require any communication link between the WLAN and WPAN. These coexistence mechanisms are only applicable after a WLAN or WPAN are established and user data is to be sent. These coexistence mechanisms will not help in the process for establishing a WLAN or WPAN.

Both types of coexistence mechanisms are designed to mitigate interference resulting from the operation of IEEE 802.15.1 devices in the presence of frequency static or slow-hopping WLAN devices. Note that interference due to multiple IEEE 802.15.1 devices is mitigated by frequency-hopping. All collaborative coexistence mechanism described in IEEE 802.15.2 standard are intended to be used when at least one WLAN station and WPAN device are colocated within the same physical unit.

When colocated, there needs to be a communication link between the WLAN and WPAN devices within this physical unit, which could be a wired connection between these devices or an integrated solution.

Non-collaborative coexistence mechanisms are intended to be used when there is no communication link between the WLAN and WPAN.

Collaborative coexistence mechanisms

The three collaborative coexistence mechanisms defined in IEEE 802.15.2 consist of two MAC sublayer techniques and one PHY layer technique. Both MAC sublayer techniques involve coordinated scheduling of packet transmission between the two wireless (WLAN and WPAN) networks. The PHY layer technique is a programmable notch filter in the IEEE 802.11b receiver to notch out the narrow-band IEEE 802.15.1 interferer. These collaborative mechanisms may be used separately or combined with others to provide a better coexistence mechanism.

The collaborative coexistence mechanism provides coexistence of a WLAN (in particular IEEE 802.11b) and a WPAN (in particular IEEE 802.15.1) by sharing information between colocated IEEE 802.11b and IEEE 802.15.1 radios and locally controlling transmissions to avoid interference. These mechanisms are interoperable with legacy devices that do not include these features.

There are two modes of operation and the mode is chosen depending on the network topology and supported traffic. In the first mode, both IEEE 802.15.1 synchronous connection-oriented (SCO) and asynchronous connectionless (ACL) traffic are supported where SCO traffic is given higher priority than the ACL traffic in scheduling. The second mode is based on time-division multiple access and is used when there is ACL traffic in high piconet density areas. In time-division multiple access (TDMA) mode, the IEEE 802.11b beacon-to-beacon interval is subdivided into two subintervals: one subinterval for IEEE 802.11b and other subinterval for IEEE 802.15.1. Since each radio has its own subinterval, both radios will operate properly, due to total orthogonality. This technique does require an additional feature to restrict when the IEEE 802.15.1 master transmits. The mode to be used is chosen under the command of the access point (AP) management software. Frequency nulling may be used in conjunction with these modes to further reduce interference.

Both alternating wireless medium access (AWMA) and packet traffic arbitration (PTA) may be combined to produce a better coexistence mechanism.

It is recommended that when it is possible, or necessary, to colocate a WLAN device and a WPAN device within the same physical unit (e.g., laptop computer), that either the AWMA collaborative coexistence mechanism or the PTA collaborative coexistence mechanism be used. If the PTA mechanism is used it is also recommended that the deterministic interference suppression mechanism be used in concert with the PTA mechanism. While PTA can be used without deterministic interference suppression, the combination of the two mechanisms leads to increased WLAN/WPAN coexistence.

If there is a high density of physical units incorporating both a WLAN and WPAN device in a common area (greater than or equal to three units in a circle of radius 10 meters) and WPAN SCO link (voice link) is not being utilized, then it is recommended that the AWMA mechanism be used. If the density of units incorporating both the WLAN and WPAN devices is low (less than three units in a circle with a radius of 10 meters), or the WPAN SCO link is used, then it is recommended that the PTA mechanism be used in concert with the deterministic interference suppression mechanism.

Non-collaborative coexistence mechanisms

IEEE 802.15.2 describes several methods that enhance the performance of the IEEE 802.15.1 and IEEE 802.11 networks through the use of adaptive interference suppression of IEEE 802.11b devices, adaptive packet selection, and packet scheduling for ACL links. These methods do not require the collaboration between the IEEE 802.11 devices and the IEEE 802.15.1 devices. Therefore, they belong to the general category of non-collaborative coexistence mechanisms.

Two other methods, i.e., packet scheduling for SCO links and adaptive frequency-hopping (AFH) for the IEEE 802.15.1 devices, are provided as information in Annex A and Annex B of the IEEE 802.15.2 standard, respectively.

The key idea for adaptive packet selection and scheduling methods is to adapt the transmission according to channel conditions. For instance, if the channel is dominated by interference from an IEEE 802.11b network, the PER will be mainly due to collisions between IEEE 802.15.1 and IEEE 802.11 systems, instead of bit errors resulting from noise. Packet types that do not include forward error correction (FEC) protection could provide better throughput if combined with intelligent packet scheduling. The foundation for the effectiveness of these types of methods is to be able to figure out the current channel conditions accurately and in a timely manner. Channel estimation may be done in a variety of ways: received signal strength indication (RSSI), header error check (HEC) decoding profile, bit error rate (BER) and PER profile, and an intelligent combination of all of the above.

There are five non-collaborative mechanisms described in IEEE 802.15.2. At least two of these share a common function called channel classification. Three mechanisms are covered under the second item in the following list:

1. adaptive interference suppression. A mechanism based solely on signal processing in the physical layer of the WLAN.
2. adaptive packet selection and scheduling. IEEE 802.15.1 systems utilize various packet types with varying configurations such as packet length and degree of error protection used. By selecting the best packet type according to the channel condition of the upcoming frequency hop, better data throughput and network performance may be obtained. In addition, by carefully scheduling packet transmission so that the IEEE 802.15.1 devices transmit during hops that are outside the WLAN frequencies and refrain from transmitting while in-band, interference to WLAN systems could be avoided/minimized and at the same time increase the throughput of the IEEE 802.15.1 systems.
3. adaptive frequency-hopping (AFH). IEEE 802.15.1 systems frequency hop over 79 channels (in the U.S.) at a nominal rate of 1600 hops/second in connection state, and 3200 hops/second in inquiry and page states. By identifying the channels with interference, it is possible to change

> the sequence of hops such that those channels with interference ("bad" channels) are avoided. From traffic type and channel condition, a partition sequence is generated as input to the frequency re-mapper, which modifies hopping frequencies to avoid or minimize interference effects.

When it is not possible, or necessary, to colocate a WLAN and WPAN device within the same physical unit, then a non-collaborative coexistence mechanism may be the only practical method. There are possible range limitations under which a non-collaborative mechanism may not be sufficient, however. For example, when an IEEE 802.11b system and an IEEE 802.15.1 system are operated 30 centimeters apart, the IEEE 802.15.1 signal will be considerably above the detection threshold of the WLAN system, even when out of band; thus, non-collaboration schemes relying on channel estimation and interference detection will be unable to prevent interference in these short range situations.

The non-collaborative mechanisms considered range from adaptive frequency hopping to packet scheduling and traffic control. They all use similar techniques for detecting the presence of other devices in the band such as measuring the packet or frame error rate, the signal strength or the signal to interference ratio (often implemented as the RSSI).

For example, each device can maintain a frame error rate measurement per frequency used. FH devices can then infer which frequencies are occupied by other users of the band and thus modify their frequency hopping pattern. They can even choose not to transmit on a certain frequency if that frequency is inferred to be occupied.

MAC sublayer packet selection mechanisms consider encapsulation rules and use the variety of IEEE 802.15.1 packet lengths to avoid overlap in frequency between IEEE 802.11 and IEEE 802.15.1. In other words, the IEEE 802.15.1 scheduler knows how to use the packet length of proper duration (1, 3, or 5 slots) in order to skip the so-called "bad" frequency.

It is recommended that AFH be used when appropriate changes to the IEEE 802.15.1 hopping sequence have been implemented.

Furthermore, it is recommended that interference aware packet scheduling and traffic control mechanisms be implemented. These mechanisms can be implemented either separately or in combination with other coexistence schemes such as AWMA, PTA, or AFH for additional performance improvements.

It is recommended that adaptive interference suppression be used with all of the above-mentioned mechanisms because it operates at the physical layer; it can also be used by itself. It is recommended that the adaptive interference suppression filter be used when there is sufficient IEEE 802.15.1 interference to noticeably degrade performance and delaying the IEEE 802.11 traffic is not sufficient. Specifically, delay sensitive traffic such as streaming media will benefit from the use of this mechanism.

1.3.2 Coexistence in IEEE 802.15.4

While not required by IEEE 802.15.4 standard [IEE06], IEEE 802.15.4 devices coexistence with other wireless devices has been taken into account to some extent. In the annex part of the IEEE 802.15.4 standard, several mechanisms that enhance coexistence with other wireless devices operating in the 2.4 GHz band are described. These mechanisms include

- CCA
- Dynamic channel selection
- Modulation
- ED and LQI
- Low duty cycle
- Low transmit power
- Channel alignment

We now briefly describe these mechanisms.

Clear channel assessment (CCA)

IEEE 802.15.4 PHYs provide the capability to perform CCA in its CSMA-CA (Carrier Sense Multiple Access With Collision Avoidance) mechanism. The PHYs require at least one of the following three CCA methods: ED (Energy Detection) over a certain threshold, detection of a signal with IEEE 802.15.4 characteristics, or a combination of these methods. Use of the ED option improves coexistence by allowing transmission backoff if the channel is occupied by any device, regardless of the communication protocol it may use.

However, as we will see in Chapter 2, the timing used in the 802.15.4 CCA mechanism is much longer than that of 802.11b/g, which puts 802.15.4 devices in a disadvantageous position in the channel access competition with 802.11b/g devices.

Dynamic channel selection

When performing dynamic channel selection, either at network initialization or in response to an outage, an IEEE 802.15.4 device will scan a set of channels specified by the ChannelList parameter. For 2.4 GHz band IEEE 802.15.4 networks that are installed in areas known to have high IEEE 802.11b activity, the ChannelList parameter can be defined as the above sets in order to enhance the coexistence of the networks.

However, it is not uncommon that some new (unknown) high IEEE 802.11b activity appears near the area of an established IEEE 802.15.4 network. And when the IEEE 802.11b activity occurs on a channel which is not defined in the ChannelList, it may cause the coexistence problem, which the dynamic channel selection mechanism is not able to solve.

Modulation

In IEEE 802.15.4, the 2.4 GHz PHY uses a quasi-orthogonal modulation scheme, where each symbol is represented by one of 16 nearly orthogonal pseudo-random noise (PN) sequences. This is a power-efficient modulation method that achieves low signal-to-noise ratio (SNR) and signal-to-interference ratio (SIR) requirements at the expense of a signal bandwidth that is significantly larger than the symbol rate. A typical low-cost detector implementation is expected to meet the 1% packet error rate (PER) requirement at SNR values of 5 dB to 6 dB.

Relatively wideband interference, such as IEEE 802.11b, would appear like white noise to an IEEE 802.15.4 receiver. The detector performance in this case is similar to noise performance, but the overall SIR requirement is 9 dB to 10 dB lower because only a fraction of the IEEE 802.11b signal power falls within the IEEE 802.15.4 receiver bandwidth.

The use of PN sequences to represent each symbol in this standard offers DSSS-like (Direct-sequence spread spectrum) processing gains to interferers whose bandwidth is smaller than the bandwidth of the IEEE 802.15.4 standard. For example, this processing gain helps to reduce the impact of an IEEE 802.15.1 [IEE02] interferer, whose 20 dB bandwidth is roughly 50% smaller than the bandwidth of the IEEE 802.15.4 standard. Whereas the SNR requirement is 5 dB to 6 dB for 1% PER in noise, the equivalent SIR requirement for an IEEE 802.15.1 signal centered within the pass band of the IEEE 802.15.4 receiver is only 2 dB.

In terms of interference to others, the IEEE 802.15.4 standard appears as wideband interference to IEEE 802.15.1, and only a fraction ($\sim$ 50%) of the IEEE 802.15.4 signal power falls within the IEEE 802.15.1 receiver bandwidth. Furthermore, due to the bandwidth ratios and to the frequency hopping used in IEEE 802.15.1, IEEE 802.15.4 transmissions will interfere with approximately 3 out of the 79 hops, or approximately 4%. To an IEEE 802.11b receiver, the IEEE 802.15.4 standard looks like a narrowband interferer, and the processing gain resulting from the spread-spectrum techniques in IEEE 802.11b will help reduce the impact of the IEEE 802.15.4 interferer.

Although the modulation scheme of IEEE 802.15.4 can enhance its interference robustness by reducing the collision loss caused by the packet collision, it may not get rid of the collision loss completely in case of a very strong interference as we will show in Chapter 3. Furthermore, the modulation scheme cannot help to reduce any inhibition loss, which occurs when a pending IEEE 802.15.4 packet is discarded if the channel access attempts exceed the maximum number of backoffs the CSMA-CA algorithm will attempt before declaring a channel access failure. We will discuss this in detail in Chapter 3.

ED and LQI

The IEEE 802.15.4 PHYs include two measurement functions that indicate the level of interference within an IEEE 802.15.4 channel. The receiver ED (Energy Detection) measurement is an estimate of the received signal power within an IEEE 802.15.4 channel and is intended for use as part of a channel selection algorithm at the network layer. The LQI (Link Quality Indicator) measures the received energy level and/or SNR for each received packet. When energy level and SNR data are combined, they can indicate whether a corrupt packet resulted from low signal strength or from high signal strength plus interference.

Low duty cycle

The specifications of the IEEE 802.15.4 standard are tailored for applications with low power and low data rates (a maximum of 250 kb/s and down to 20 kb/s). Typical applications for IEEE 802.15.4 devices are anticipated to run with low duty cycles (under 1%). This will make IEEE 802.15.4 devices less likely to cause interference to other standards.

Low transmit power

Although operation in the 2.4 GHz band under Section 15.247 of Federal Communications Commission (FCC) Code of Federal Register (CFR) 47 [FCC] rules allow transmission powers up to 1 W, IEEE 802.15.4 devices will likely operate with much lower transmit power. A key metric of IEEE 802.15.4 is cost, and achieving greater than 10 dBm transmit power in a low-cost system on chip, while feasible, will be economically disadvantageous. Furthermore, European regulations (European Telecommunications Standards Institute (ETSI) EN 300 328 [ETSa] and [ETSb]) for out-of-band emissions make it difficult to transmit above 10 dBm without additional, expensive filtering. These factors limit the distribution of devices with greater than 10 dBm transmit power to a few specialized applications.

At the low end, the IEEE 802.15.4 PHY specifies that devices must be capable of at least −3 dBm transmit power. At this level, actual transmit power represents a small fraction of the overall power consumed by the transmitter, so there is little benefit in terms of energy savings to operate below this level. However, the IEEE 802.15.4 standard does encourage operating with lower transmit power, when possible, to minimize interference.

Thus the majority of IEEE 802.15.4 devices are expected to operate with transmit powers between −3 dBm and 10 dBm, with 0 dBm being typical. IEEE 802.11b devices also operate under Section 15.247 of FCC CFR47 [FCC], where up to 1 W of transmit power is allowed; however, most devices in the market today operate at transmit powers between 12 dBm and 18 dBm. IEEE 802.15.3 devices operate under Section 15.249 of FCC CFR47,

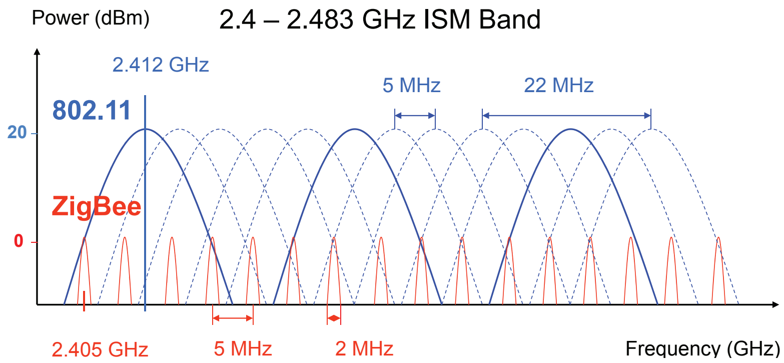


Figure 1.10: IEEE 802.11b/g and IEEE 802.15.4 channels in the 2.4 GHz ISM band [Pol06]

which limits transmit power to 8 dBm equivalent isotropically radiated power (EIRP). The EIRP measurement for the IEEE 802.15.3 PHY includes the antenna gain; therefore, a 1 dB increase antenna gain requires a 1 dB decrease in transmit power. In contrast, devices operating under Section 15.247 of FCC CFR47 are allowed up to 6 dB of antenna gain without modifications to the transmit power.

Assuming moderate antenna gain (∼0 dBi) for typical implementations, the discussion in this subclause implies that a nominal IEEE 802.15.4 transmitter would operate about 8 dB less than the IEEE 802.15.3 transmitter and about 12 dB to 18 dB less than a typical IEEE 802.11b implementation.

Channel alignment

The alignment between IEEE 802.11b (nonoverlapping sets) and IEEE 802.15.4 2.4 GHz band channels is shown in Figure 1.10. There are four IEEE 802.15.4 channels that fall in the guard bands between (or above) the three IEEE 802.11b channels (n = 15, 20, 25, 26 for North America; n = 15, 16, 21, 22 in Europe). While the energy in this guard space will not be zero, it will be lower than the energy within the channels; and operating an IEEE 802.15.4 network on one of these channels will minimize interference between systems.

In practice, however, there is no guarantee that an IEEE 802.11b network and an IEEE 802.15.4 network always operate on the nonoverlapping channels. Thus, the coexistence problem arises.

To sum up, from the descriptions above, we can learn that the coexistence issue has been taken into account in the IEEE 802.15.4 standard. However, as shown in Chapter 2 and Chapter 3, due to its low transmit power and longer timing used in its CCA mechanism, IEEE 802.15.4 devices are often in a weak position when they coexist with devices using other standards like IEEE 802.11b/g. Besides, as IEEE 802.15.4 WSNs and IEEE 802.11b/g WLANs are more and more popular, the coexistence issue is becoming more critical. Therefore, a coexistence standard like IEEE 802.15.2 should be made as soon as possible.

1.4 Research Motivation, Targets and Scope

As addressed in Section 1.2, the coexistence issue between IEEE 802.15.4/ZigBee WSNs and other systems sharing the same unlicensed frequency band is getting increasing attention and interest as well from academia and industrial research communities, which includes Philips Research, where this thesis has been done. Philips intends to use ZigBee technology for a new generation of lighting control [Zig07b]. The Philips vision is to "unleash the full potential" of lighting environments by enabling new applications for personal comfort, safety, security and efficiency. Philips believes the role of lighting has become increasingly significant to enable smarter building systems and enhance environments. The company selected ZigBee technology for its ability to create interoperability between lighting control systems and other building subsystems, and its mesh network capabilities which enable redundancy and eliminate single points of failure in a lighting control system. By using ZigBee in the lighting control system of the future, Philips expects building owners to realize valuable return on investment through conservation, energy efficiency and reduction of harmful greenhouse gas emissions. ZigBee technology will help Philips lighting control systems realize other benefits by creating centralized, integrated systems that can be both centrally and locally controlled and managed. For example, occupants can control individual lighting and thermostats or facilities can internally or externally change these systems and make adjustments. A monitored system can also capture data for the facility manager to see, for example, that a lamp has burned out and needs replacement. As ZigBee technology plays such an important role for Philips and the coexistence capability of ZigBee WSNs is relevant to a satisfactory user experience, the research work on exploring the coexistence capability of ZigBee WSNs in the unlicensed frequency band in this thesis was thus motivated and performed.

The targets of this thesis work are to achieve a clear understanding on the coexistence issue between IEEE 802.15.4/ZigBee WSNs and other systems sharing the same unlicensed 2.4 GHz ISM frequency band, and then to propose cost-effective methods to enhance the coexistence capability of IEEE 802.15.4/ZigBee WSNs. Among various systems sharing the 2.4 GHz ISM frequency band with IEEE 802.15.4/ZigBee WSNs, IEEE 802.11b/g WLANs are the most widely deployed. We therefore focus on the coexistence between IEEE 802.15.4/ZigBee WSNs and IEEE 802.11b/g WLANs in this thesis.

1.5 Contributions and Thesis Outline

Based on the research targets defined in Section 1.4, our work has generated the following contributions.

Our first contribution is the introduction of a coexistence model of IEEE 802.15.4 and IEEE 802.11b/g networks. The model precisely exposes the interplay between these two standards and therefore clearly explains their coexistence performance. The coexistence behavior between 802.15.4 and 802.11b/g has been investigated by many previous research such as [How03] [Pet06][Shi05][Sik05]. However, the conclusions of these are incomplete and some are even in conflict, causing the coexistence issue between 802.15.4 and 802.11b/g confusing. For example, [How03] and [Pet06] conclude that 802.15.4 has little impact on the 802.11 performance, and this result should hold unless the device is located near an IEEE 802.15.4 cluster with a high aggregate activity level. However, our model shows that 802.15.4 can have a serious impact on the 802.11 performance even when they are not located near to each other. Actually, in case that they are so close that they can hear each other, the 802.11 performance will get less impacted. This is because the 802.11's Media Access Control (MAC) mechanism uses shorter timing than does that of 802.15.4, and the shorter timing gives 802.11 an advantage over 802.15.4 in terms of the media access. Moreover, in [Shi05], the Packet Error Rate (PER) of IEEE 802.15.4 under the IEEE 802.11b interference is analyzed from an assumption of blind transmissions, i.e., both IEEE 802.11b and IEEE 802.15.4 transmit packets regardless of whether the channel state is busy or not. However, our model shows that this assumption is realistic in only one of the three coexistence regions and therefore the analysis in [Shi05] should be refined.

Chapter 2 describes our coexistence model of 802.15.4 and 802.11b/g. The model considers two aspects, namely power and timing. These two aspects jointly have different impacts on the performance of 802.15.4 networks, depending on the coexistence situations. To classify the coexistence situations, we introduce a concept of "coexistence region". We characterize the coexistence behavior in each coexistence region and identify for each region the underlying coexistence mechanism and protocol interactions. The supporting publication is [Yua07].

To evaluate the analytical model proposed in Chapter 2 in a real-life environment, we conducted experiments, which are described in Chapter 3. Through the experiments, some implementation-related factors such as the Rx-to-Tx turnaround time are identified. These factors can significantly affect the 802.15.4/ZigBee WSNs coexistence performance in the presence of 802.11b/g interference. By taking these factors into account, we improved our analytical model so that it can more precisely explain and predict the 802.15.4/ZigBee WSNs coexistence performance in real-life environments. The supporting publications include [Yua09], [Yua10c], and [Yua11].

By creating a clear picture of the coexistence issue between 802.11 and 802.15.4, the model inspired us to propose two coexistence capability enhancement approaches for 802.15.4/ZigBee WSNs, i.e., our second and third contributions as follows.

Our second contribution is that we propose a robust, responsive and easy to be implemented approach to help 802.15.4/ZigBee devices mitigate interference including but not limited to 802.11b/g. As described in Chapter 4, in the presence of heavy interference, 802.15.4/ZigBee devices can mitigate the interference by adaptively and distributively adjusting their Clear Channel Assessment (CCA) thresholds. As the communication, which is quite vulnerable under the heavy interference, among 802.15.4/ZigBee devices is not needed, the approach is interference-robust. Besides, as adjusting the CCA thresholds can be done very quickly and easily, the approach is also responsive and easy to be implemented. The OPNET simulation shows that in the presence of heavy interference, the approach can substantially reduce the amount of discarded packets due to channel access failures, and therefore significantly enhance the performance of 802.15.4/ZigBee WSNs. This contribution is published in [Yua10b].

Our third contribution is that we propose a distributed adaptive multi-channel interference-avoidance protocol, which is described in Chapter 5. Different from the approach mentioned above, which enhances the 802.15.4/ZigBee devices' performance in the presence of heavy interference by increasing their interference tolerance at the single channel they use, our multi-channel interference-avoidance approach focuses on making good use of multiple channels that 802.15.4/ZigBee devices can use. Although the ZigBee specification [Zig07c] proposes a feature called *frequency agility*, which refers to the ability of ZigBee networks to change the operational channel in the presence of interference, for a large-scale ZigBee network, changing the whole network operational channel to an idle one, may be neither appropriate if there is only local interference nor possible if there is not any single idle channel available globally. Our multi-channel interference-avoidance approach enables a single-channel large-scale ZigBee network to distributively, adaptively and partially change the operational channel in the presence of local interference. As a result, the ZigBee network performance under interference can be effectively and efficiently improved. This contribution is published in [Yua10a].

In Chapter 6, we conclude the thesis and point out the future research directions.

The structure of this thesis is schematically depicted in Figure 1.11. As it shows, besides the introduction and the conclusion chapters, the thesis consists of two parts: coexistence modeling and coexistence enhancement. Chapter 2 and 3 present our contributions to the part of coexistence modeling. Chapter 4 and 5 show our contributions to the part of coexistence enhancement.

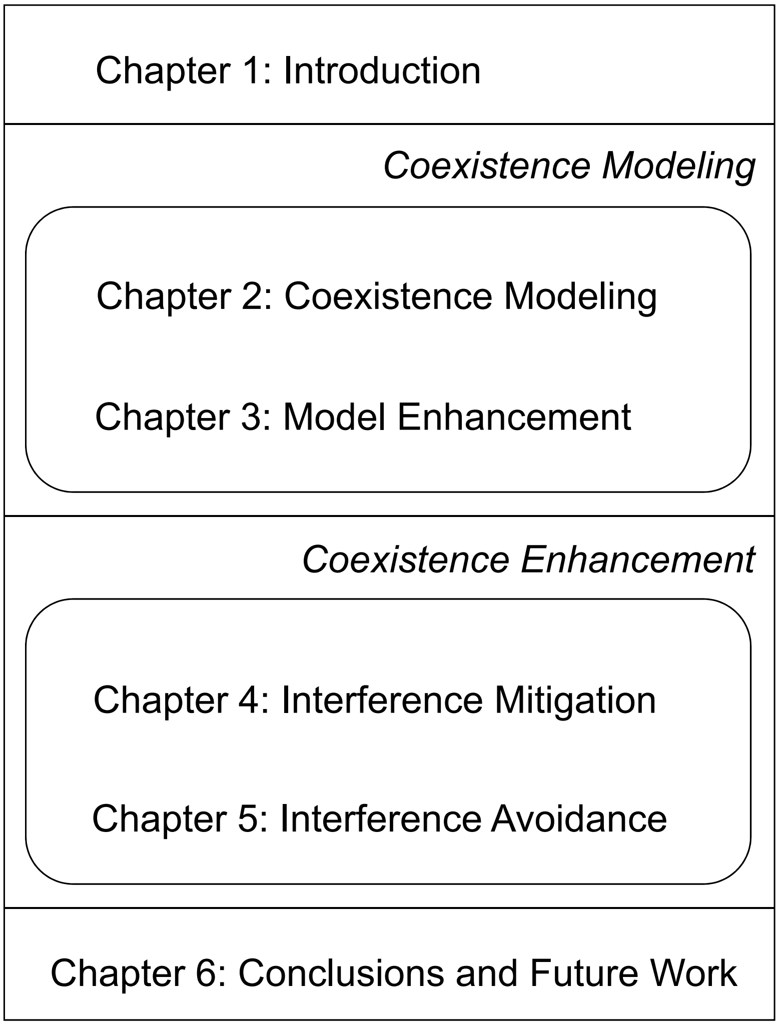

Chapter 1: Introduction
Coexistence Modeling
Chapter 2: Coexistence Modeling
Chapter 3: Model Enhancement
Coexistence Enhancement
Chapter 4: Interference Mitigation
Chapter 5: Interference Avoidance
Chapter 6: Conclusions and Future Work

Figure 1.11: Thesis structure

Chapter 2

Coexistence Modeling

Essentially, all models are wrong, but some are useful.

- George E. P. Box

As stated in Section 1.4, the targets of this thesis work are to achieve a clear understanding of the coexistence issue between IEEE 802.15.4/ZigBee WSNs and other systems sharing the same unlicensed 2.4 GHz ISM frequency band, and then to propose cost-effective methods to enhance the coexistence capability of IEEE 802.15.4/ZigBee WSNs. Among various systems sharing the 2.4 GHz ISM frequency band with IEEE 802.15.4/ZigBee WSNs, IEEE 802.11b/g WLANs are the most widely deployed. We therefore focus on the coexistence issue between IEEE 802.15.4/ZigBee WSNs and IEEE 802.11b/g WLANs in this thesis as well as in this chapter.

Although many studies on the coexistence between IEEE 802.15.4/ZigBee WSNs and IEEE 802.11b/g WLANs have been done, the conclusions they drew are incomplete and/or conflicting, and therefore confusing. In this chapter, we propose a coexistence model of IEEE 802.15.4/ZigBee WSNs and IEEE 802.11b/g WLANs. The model is to expose the interplay between these two wireless systems and therefore explain their interesting coexistence performance as well as the incompatible conclusions of many previous studies.

This chapter is organized as follows. First, Section 2.1 defines some main concepts and terminology used in this thesis. Then, Section 2.2 gives an overview of the coexistence issue between IEEE 802.15.4/ZigBee WSNs and IEEE 802.11b/g WLANs. Related work is addressed in Section 2.3. The standards IEEE 802.11b, IEEE 802.11g and IEEE 802.15.4 are introduced with an emphasis on their MAC sublayers in Section 2.4. Next, Section 2.5 presents a coexistence model to characterize the coexistence issue in various scenarios. Further, Section 2.6 gives an analysis of the coexistence model, and simulation results are shown in Section 2.7. Finally, our conclusions are drawn in Section 2.8.

2.1 Main Concepts and Terminology

In this section, we define the concepts and terminology used in the remainder of the thesis.

Coexistence

IEEE 802.15.2 [IEE03b] defines coexistence as: “The ability of one system to perform a task in a given shared environment where other systems have an ability to perform their tasks and may or may not be using the same set of rules.” In the thesis, however, we mainly consider coexistence among systems using *different* sets of rules. This is because, on the one hand, as stated in Section 1.2 we focus on the coexistence between IEEE 802.15.4 WSNs and other systems sharing the same unlicensed 2.4 GHz ISM frequency band, i.e., “inter-system” spectrum sharing (see Figure 1.9), and on the other hand, the coexistence among systems based on a same set of rules usually has been taken into account, e.g., the IEEE 802.11’s collision avoidance algorithm (i.e., listen before talk).

Coexistence Performance

A system’s performance in terms of throughput, packet loss ratio, transmission delay, etc., in the presence of interference caused by other systems sharing the same frequency band.

Coexistence Capability

The ability of one system to perform a task in the presence of interference caused by other systems sharing the same frequency band.

Coexistence Region

An area where one system which coexists with other systems sharing the same frequency band exhibits a characteristic coexistence state. The system can be in one of three coexistence states, i.e., the system and the other systems have a mutual influence, an one-way influence or no influence between each other.

2.2 802.11b/g and 802.15.4 Coexistence Issue Overview

IEEE 802.11b and IEEE 802.11g WLANs are probably the most widely deployed wireless systems. As a low-power and low-cost technology, IEEE 802.15.4 [1]is establishing its place in the market as an enabler for the emerging wireless sensor networks (WSNs) [Pet06]. Due to supporting complimentary applications, they are often colocated with each other.

Like IEEE 802.11b and IEEE 802.11g WLANs, IEEE 802.15.4 WSNs also use the 2.4 GHz ISM band as shown in Figure 1.10. As we see, there is not any single IEEE 802.15.4 channel which is guaranteed not to be covered by IEEE 802.11b/g channels if they are not coordinated properly as it is actually. Besides, Figure 1.10 also illustrates that transmit powers of IEEE 802.11b/g and IEEE 802.15.4 are significantly different. Indeed, the transmit power of IEEE 802.15.4 is typically as low as 1 mW [IEE06], while that of IEEE 802.11b/g is typically 100 mW [IEE99b].

As they share the same frequency band and are often colocated with each other, their coexistence has been investigated in many research activities, as described in the following section.

2.3 Related Work

There have been lots of studies about coexistence between the IEEE 802.11b/g and IEEE 802.15.4. Some studies conclude that IEEE 802.15.4 has little impact on the IEEE 802.11b performance. For example, in [How03], Howitt and Gutierrez propose a method for analyzing the coexistence impact of an IEEE 802.15.4 network on an IEEE 802.11b device. Analysis based on an analytical model suggests the following general conclusion: assuming either automated or manual frequency management is employed, it is reasonable to conclude that the IEEE 802.15.4 network will typically have little to no impact on the IEEE 802.11b' s performance. This result should hold unless the device is located near an IEEE 802.15.4 cluster with a high aggregate activity level. In [Pet06], Petrova *et al.* also conclude that the IEEE 802.15.4 operation has practically no negative influence on the concurrent IEEE 802.11b communication.

On the other hand, some studies conclude that IEEE 802.11b can have a serious impact on the IEEE 802.15.4 performance if the channel allocation is not carefully taken into account. For instance, in [Sik05], the impact of IEEE 802.11b on IEEE 802.15.4 is measured. The measurements show that the impact of IEEE 802.11b stations with high duty cycle on IEEE802.15.4 stations may be extremely critical, if the same carrier frequencies are selected. Also, the results in [Pet06] show that if no care is taken of the operational channels of the two technologies, the IEEE 802.11b itself will have a negative effect on the performance of the IEEE 802.15.4 transmission. While these conclusions are true in general, we believe the studies so far have dealt with only limited coexistence scenarios.

[1] For convenience, in this chapter, we interchangeably use the terms, IEEE 802.15.4 and ZigBee.

Besides, in [Shi05], the Packet Error Rate (PER) of IEEE 802.15.4 under the IEEE 802.11b interference is analyzed from an assumption of blind transmissions, i.e., both IEEE 802.11b and IEEE 802.15.4 transmit packets regardless of whether the channel state is busy or not. However, in this chapter, we will show that this assumption is realistic in only one of the three coexistence regions and therefore the analysis in [Shi05] should be refined.

Moreover, in [Sik05], measurements are performed to quantify coexistence issues. The author concluded that even in the worst case conditions such as frequency overlapping, small physical separation and high traffic load for interference, the packet error rate never reaches 100 % and there is still a chance for IEEE 802.15.4 to transmit some packets successfully, as the IEEE802.11 interframe spaces still may give room, though the PER is above 95%. In this chapter, we also quantify the coexistence issues and show that in some cases, the PER can reach 100% in fact.

Despite the conclusion, drawn from many studies such as those mentioned above, that the performance of IEEE 802.15.4 transmission can be seriously negatively affected by intense IEEE 802.11b traffic if their channels are not allocated properly, the ZigBee Alliance claimed in [Zig07a] that even in the presence of a surprising amount of interference, ZigBee devices continue to communicate effectively.

These conflicting conclusions make the coexistence between IEEE 802.15.4 and IEEE 802.11b/g confusing. In the following sections we shall create a clear picture of the coexistence issue. We start with a brief introduction about IEEE 802.11b/g and IEEE 802.15.4 with an emphasis on their MAC sublayers.

2.4 IEEE 802.11b/g and IEEE 802.15.4

2.4.1 IEEE 802.11b/g

As mentioned earlier, IEEE 802.11b and IEEE 802.11g are standards defining the Medium Access Control (MAC) and Physical layer (PHY) specifications for WLANs. Both standards operate in 13 overlapping channels in the 2.4 GHz ISM band and the bandwidth of each channel is 22 MHz. Different modulation techniques are used to provide different data rates, e.g., Complementary Code Keying (CCK) is used to deliver 5.5 and up to 11 Mbps for IEEE 802.11b, and Orthogonal Frequency Division Multiplexing (OFDM) is used to deliver up to 54 Mbps for IEEE 802.11g.

IEEE 802.11b/g MAC employs the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism for medium access control, which is illustrated in Figure 2.1.

Before initiating a transmission, an IEEE 802.11b/g node senses the channel to determine whether another node is transmitting. If the medium is sensed idle for a Distributed coordination function Inter-Frame Space (DIFS)

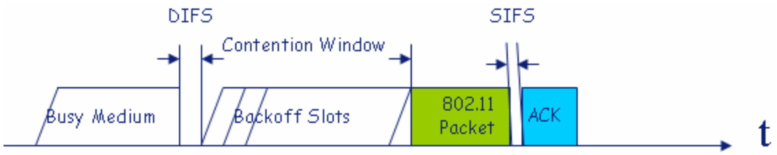


Figure 2.1: IEEE 802.11b/g medium access control mechanism

time interval the transmission will proceed. If the medium is busy the node defers its transmission until the end of the ongoing transmission. When the medium becomes idle for a DIFS interval, the node will generate a random backoff delay based on an integer uniformly chosen in an interval. This interval $[0, W]$ is called Contention Window (CW), where W is the size of the contention window. The initial W is set to CW_{min}. The backoff timer is decreased by one as long as the medium is sensed idle for a backoff time slot. The backoff counter will become frozen when a transmission is detected on the medium, and resumed when the channel is sensed idle again for a DIFS interval. When the backoff timer reaches zero, the node transmits a DATA packet. Immediately after receiving a packet correctly, the destination node waits for a Short Inter Frame Spacing (SIFS) interval and then transmits an ACK back to the source node. If two or more nodes decrease their backoff timers to zero at the same time, a collision occurs. Upon not receiving an ACK, the CW is doubled and a retransmission is scheduled. The CW is doubled at each retransmission until it reaches a maximum value. If an ACK is still not received, the MAC sublayer will report a packet transmission error to its upper layer.

2.4.2 IEEE 802.15.4

The IEEE 802.15.4 MAC sublayer supports two types of channel access mechanisms, unslotted CSMA/CA mechanism in non-beacon-enabled network and slotted CSMA/CA mechanism in beacon-enabled network. In non-beacon-enabled mode, which is the more popular one so far, a node simply transmits its data packet, using unslotted CSMA/CA, when it wants to send data to a coordinator. In beacon-enabled mode, however, a node has to be synchronized to a coordinator and packet transmissions can only start at the beginning of time slots.

Like IEEE 802.11b/g, IEEE 802.15.4 also employs CSMA/CA for medium access control. However there is a key difference between their CSMA/CA mechanisms. Unlike in IEEE 802.11b/g, as shown in Figure 2.2, a channel in IEEE 802.15.4 is not sensed during backoff periods but only during Clear Channel Assessment (CCA) periods. Furthermore, the contention window in IEEE 802.15.4 is doubled correspondingly whenever the channel is determined to be busy during a CCA period. In IEEE 802.11b/g, however, the contention window remains the same when the channel is determined to be

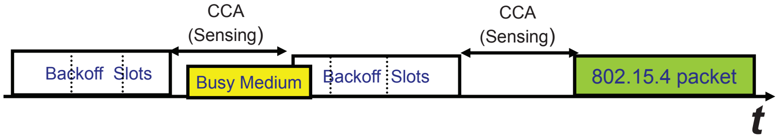


Figure 2.2: IEEE 802.15.4 medium access control mechanism

busy and is doubled only when an ACK is not received. This difference has a significant impact on their behavior of sharing a channel, which we shall show in detail in the following sections.

2.5 A Coexistence Model of 802.11b/g and 802.15.4

As mentioned in Section 2.3, there were many studies on the coexistence of IEEE 802.11b/g WLANs and IEEE 802.15.4 WSNs, but the conclusions they drew are often conflicting. To gain a clear understanding, we need to develop a model, which, by reasonably simplifying the complex reality and exposing essential aspects, can give people insights into the coexistence behavior of IEEE 802.11b/g WLANs and IEEE 802.15.4 WSNs. Not only can one use the model to understand the interplay between an IEEE 802.11b/g WLAN and an IEEE 802.15.4 WSN when they coexist, but also to predict their coexistence performance, which can help people set up a colocated IEEE 802.11b/g WLAN and IEEE 802.15.4 WSN with less mutual interference.

We now develop the model. First, as mentioned in Section 1.2, due to very low transmit power, IEEE 802.15.4 devices are more vulnerable to the interference generated by IEEE 802.11b/g devices which have much higher power. We therefore focus on the interference that IEEE 802.11b/g devices bring to IEEE 802.15.4 devices when they coexist. Second, we assume that IEEE 802.11b/g interference is always saturated, which means there is always an IEEE 802.11b/g packet available for transmission. This corresponds a worst-case interference scenario, which in reality would occur for instance when people watch videos via IEEE 802.11b/g devices. This is becoming increasingly prevalent as the online video applications like YouTube and IEEE 802.11b/g-supported smart electronic devices like iPhones are more and more popular. Besides, this assumption eases our analysis and therefore allows us to focus on the most critical aspects of the coexistence issue. To investigate the worst case, we also assume that their operational frequency bands overlap each other to the most extent, i.e., there is only 2 MHz offset between the center frequency of IEEE 802.15.4 and that of IEEE 802.11b/g as listed in Table 2.1. The coexistence effects caused by the different operational frequency offsets have been studied. As shown in Figure 2.3, the measurement in [Pet06] suggests that a 2 MHz offset between the center frequencies can

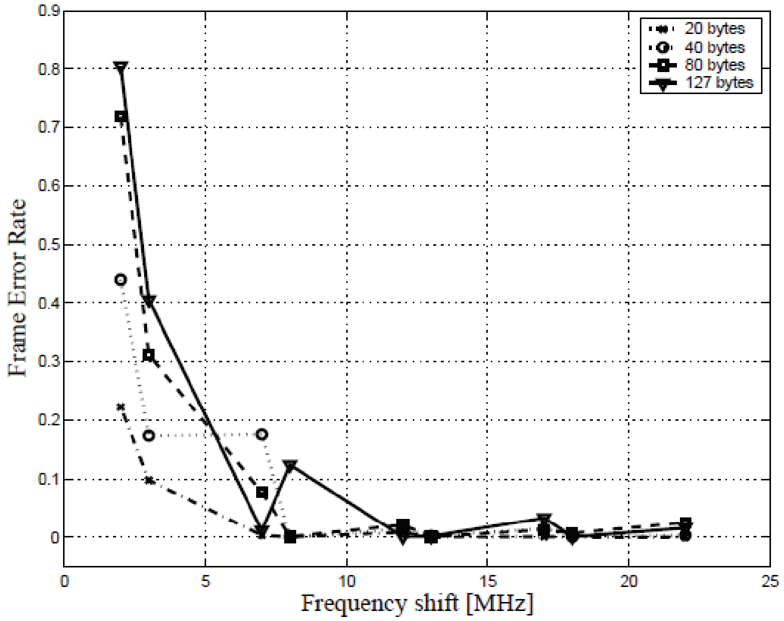


Figure 2.3: IEEE 802.15.4 Frame Error Rate when interfered by a 802.11b transmission[Pet06]

cause an IEEE 802.15.4 frame error rate to be 0.22 to 0.81, depending on the size of the IEEE 802.15.4 packets. As expected, the larger the IEEE 802.15.4 packet size is, the higher the frame error rate caused by IEEE 802.11b interference. As the offset increases, the IEEE 802.15.4 frame error rate caused by the IEEE 802.11b interference declines. When the offset is larger than 7 MHz, the frame error rate gets close to zero. This means that to achieve a a nearly "interference-free" IEEE 802.15.4 performance, the offset between the operational frequencies of IEEE 802.11b and IEEE 802.15.4 needs to be at least 7 MHz. Finally, we consider only the unslotted IEEE 802.15.4 MAC. This is because the case of slotted IEEE 802.15.4 has been studied extensively [Pet06][Shi05][Tam10], and also because the case of unslotted IEEE 802.15.4 has been less studied while being more popular in practice.

Under IEEE 802.11b/g interference, an IEEE 802.15.4 packet can be successfully received if either of the following two conditions is satisfied.

(1)*Power Condition*: When an IEEE 802.15.4 packet overlaps an IEEE 802.11 packet, the in-band interference power from the IEEE 802.11 packet is significantly lower than the useful signal power from the IEEE 802.15.4 packet at an IEEE 802.15.4 receiver. According to the specification [IEE99b], if IEEE 802.11b/g interference is weak enough so that the in-band signal-to-interference ratio (SIR) is larger than 5 - 6 dB, an IEEE 802.15.4 packet could be successfully received with a probability of 99%. Note that IEEE 802.15.4 has no error correction capability and just one bit error can make the complete packet erroneous.

(2)*Timing Condition*: The transmission time of an IEEE 802.15.4 packet

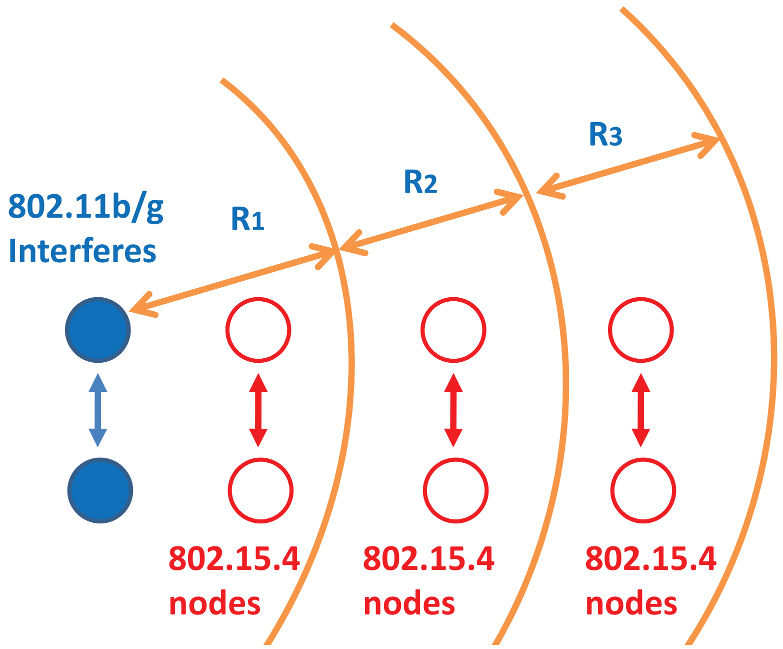


Figure 2.4: Coexistence regions of IEEE 802.15.4 and IEEE 802.11b/g

is smaller than the inter-frame idle time, denoted by T_{idle}, between two consecutive IEEE 802.11b/g packets so that the IEEE 802.15.4 packet does not overlap an IEEE 802.11 packet.

Correspondingly, our coexistence model includes the power and timing aspects, which are discussed as follows.

2.5.1 Power Aspect

As shown in Table 2.1, the transmit powers of IEEE 802.11b/g nodes and IEEE 802.15.4 nodes are typically 100 mW [IEE99b] and 1 mW [IEE06], respectively, while the clear channel assessment (CCA) thresholds of IEEE 802.11b/g nodes and IEEE 802.15.4 nodes are typically -84 dBm and -85 dBm, respectively. Since omnidirectional antennas are most commonly used by both IEEE 802.11b/g nodes and IEEE 802.15.4 nodes in practice, we consider only omnidirectional antennas in this work. Thus, given such comparable CCA thresholds, the significant differences in the transmit power can result in the following three distinct regions, R_1, R_2 and R_3 as illustrated in Figure 2.4:

R_1: a region in which IEEE 802.15.4 nodes and IEEE 802.11b/g nodes can sense each other. This happens when IEEE 802.15.4 nodes and IEEE 802.11b/g nodes are close to each other.

R_2: a region in which IEEE 802.15.4 nodes can sense IEEE 802.11b/g nodes, but not *vice versa*. This is because IEEE 802.11b/g nodes have much more power than IEEE 802.15.4 nodes.

Table 2.1: IEEE 802.15.4 and IEEE 802.11b/g System Parameters and additional parameters used to obtain simulation results

	IEEE 802.15.4	**IEEE 802.11b**	**IEEE 802.11g**
Transmit power	0 dBm	20 dBm	20 dBm
Receiver Sensitivity	-85 dBm	-76 dBm	-82 dBm
CCA threshold	-85 dBm	-84 dBm	-84 dBm
Bandwidth	2 MHz	22 MHz	22 MHz
Inter-arrival time	640 μs	744 μs	1365 μs
Transmit rate	250 kbps	11 Mbps	6 Mbps
Payload size	1 byte	1024 bytes	1024 bytes
Backoff unit T_{bs}	320 μs	20 μs	9 μs
SIFS	192 μs	10 μs	10 μs
DIFS	N/A	50 μs	28 μs
CCA	128 μs	N/A	N/A
DIFS	N/A	50 μs	28 μs
CW_{min}	7	31	15
Center frequency	2410 MHz	2412 MHz	2412 MHz

R_3: a region in which neither can sense the other, but IEEE 802.15.4 nodes may still suffer IEEE 802.11b/g interference. This happens especially when links among IEEE 802.15.4 nodes are very weak.

We define these areas as *coexistence regions*. Since omnidirectional antennas are considered, R_1, R_2 and R_3 are an area of circle, annulus, and annulus, respectively. Note that for saving space, we show only parts of these areas in Figure 2.4. In case of non-omnidirectional antennas, the shapes of the three regions will change or even these regions may not exist.

To quantify these regions, we use a path loss model which is described in [IEE99a] and recommended in the IEEE 802.15.2 specification [IEE03b]. The path loss follows free-space propagation up to 8 meters and then attenuates more rapidly with a coefficient of 3.3, which is adjusted to 4 in this thesis to correspond to the 32 meters indoor reliable transmission distance of IEEE 802.15.4 nodes reported in [Pet06]. The path loss is expressed as:

$$PL(d) = \begin{cases} 20\log_{10}(\frac{4\pi d}{\lambda}) & \text{if } d \leq d_0 \\ 20\log_{10}(\frac{4\pi d_0}{\lambda}) + 40\log_{10}(\frac{d}{d_0}) & \text{if } d > d_0 \end{cases} \tag{2.1}$$

where d is the distance between a transmitter and a receiver, and d_0, i.e., 8 m, is the length of *line-of-sight* (LOS); $\lambda = c/f_c$, where c is the velocity of light and f_c is the carrier center frequency. By taking the receiver sensitivities, which are shown in Table 2.1, as the received powers, and taking the SIR of 6 dB at the receivers, we obtain R_1, R_2 and R_3 as illustrated in Table 2.2.

Note that for simplicity, when computing the radius of R_3, we have not

Table 2.2: Coexistence Regions of IEEE 802.15.4 and IEEE 802.11b/g

Range	**IEEE 802.11b**	**IEEE 802.11g**
R_1	22 m	32 m
R_2	67 m	67 m
R_3	95 m	95 m

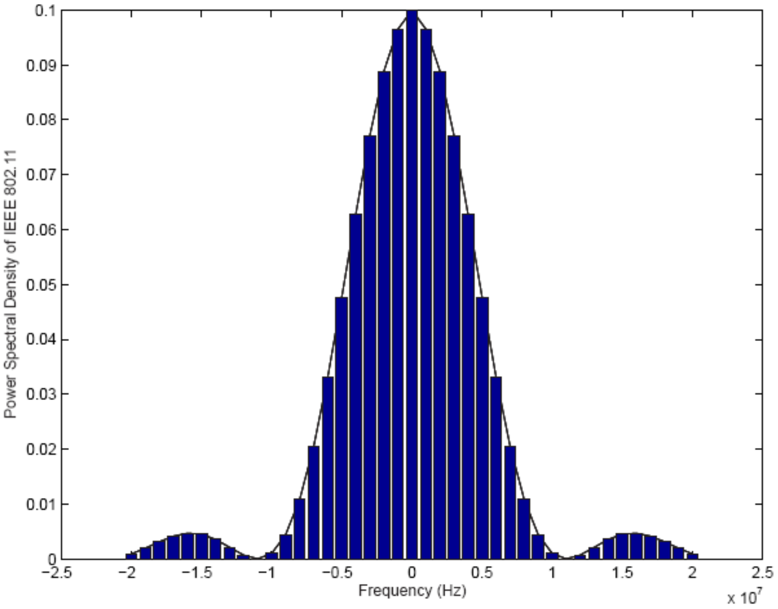


Figure 2.5: Power Spectral Density of the IEEE 802.11b [IEE99a]

taken the environment noise into account. However, it could not be ignored in case of very weak useful signal. Besides, although the transmit power of an IEEE 802.11b/g node is distributed across the 22 MHz frequency band, only a part of the total IEEE 802.11b/g transmit power can fall into the 2 MHz band of an IEEE 802.15.4 node. For convenience, in the computation, we simply took 2/22 of the total IEEE 802.11b/g transmit power as the power which an IEEE 802.15.4 node could receive. In fact, as it is shown in Figure 2.5, the power spectral density of 802.11b is not uniformly distributed across the 22 MHz band. There are more power distributed closely around the center frequency. Thus, as the offset between the center frequencies of IEEE 802.11b/g nodes and IEEE 802.15.4 nodes is small, IEEE 802.15.4 nodes can receive more power from IEEE 802.11b/g nodes, resulting in a larger radius of R_2. Instead, a bigger frequency offset will lead to less power falling into the band of IEEE 802.15.4 nodes and therefore a smaller radius of R_2. We will have a further discussion on this in Section 2.8.

Let us present the timing aspect of our coexistence model.

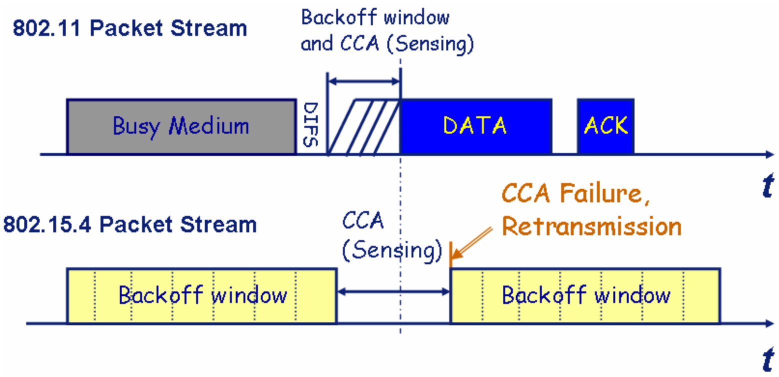


Figure 2.6: In R_1: An IEEE 802.15.4 node has few chances to access the channel due to the longer time interval used in its MAC mechanism

2.5.2 Timing Aspect

In Region R_1

In R_1, an IEEE 802.11b/g node and an IEEE 802.15.4 node can sense each other and therefore both of their CSMA/CA mechanisms work, i.e., as one is transmitting; the other has to wait.

The CSMA/CA mechanism ensures that no overlapping of transmissions can happen if one node seizes the medium first. According to the conditions we discussed for successful transmissions, we know that the IEEE 802.15.4 throughput performance depends on how many chances it can get to transmit packets between two consecutive IEEE 802.11b/g packets. IEEE 802.15.4 nodes typically use a 10 to 30 times longer time interval than IEEE 802.11b/g nodes, e.g., the backoff slot unit is 320 μs, 50 μs and 9 μs for IEEE 802.15.4, IEEE 802.11b and IEEE 802.11g, respectively. The shorter time interval gives IEEE 802.11b/g nodes priority over IEEE 802.15.4 nodes to access the channel and therefore cause unfairness to the IEEE 802.15.4 nodes. This is illustrated in Figure 2.6.

However, once IEEE 802.15.4 nodes seize the channel, they can transmit packets free from interference because the IEEE 802.11b/g nodes will defer for the packet transmission of IEEE 802.15.4 nodes in this region. Therefore, the sufficient coexistence condition for this scenario is that a CCA of IEEE 802.15.4 happens during the period of the idle time, t_{idle}, between two consecutive IEEE 802.11b/g packets.

Now we see whether this sufficient coexistence condition could be satisfied. According to the specification [IEE99b],

$$t_{idle} \triangleq DIFS + t_{bo} \triangleq DIFS + m \cdot T_{bs} \tag{2.2}$$

where t_{bo} is a random period of time for an additional deferral time before transmitting and $t_{bo} \triangleq m \cdot T_{bs}$, where T_{bs} is a backoff unit and m is a random

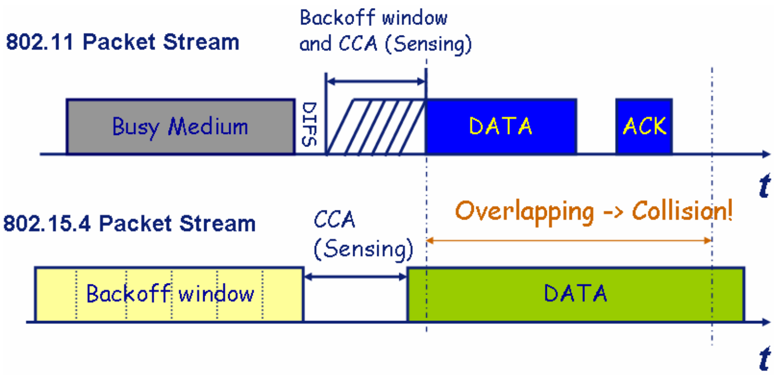


Figure 2.7: In R_2: IEEE 802.11b/g nodes fail to sense IEEE 802.15.4 nodes

integer drawn from a uniform distribution over the interval $[0, CW_{min}]$. The values of these parameters are shown in Table 2.1.

When $m \geq 4$ and 12 for IEEE 802.11b and IEEE 802.11g respectively, $t_{idle} \geq CCA$. Thus, when m is chosen to be a value in the range [4, 31] and [12, 15] for IEEE 802.11b and IEEE 802.11g respectively, t_{idle} is long enough for performing a CCA. The performance of an IEEE 802.15.4 network under IEEE 802.11b/g interference will be quantified in Section 2.6.

In Region R_2

In R_2, IEEE 802.15.4 nodes can sense IEEE 802.11b/g nodes but not vice versa, because the transmit power of IEEE 802.11b/g nodes is much higher than that of IEEE 802.15.4 nodes. Consequently, when IEEE 802.11b/g nodes are transmitting, IEEE 802.15.4 nodes have to be waiting, whereas when IEEE 802.15.4 nodes are transmitting, IEEE 802.11b/g nodes are not aware of this and thus they simply proceed to transmit, probably causing an overlapping in packet transmissions. This is shown in Figure 2.7.

To check whether IEEE 802.15.4 nodes can have successful transmissions here, we will first see whether non-overlapping transmissions can happen in the region R_2.

Similar to the region R_1, an IEEE 802.15.4 node has to seize the channel so that its transmission can start. Hence, t_{idle} also needs to be longer than a CCA period in the region R_2. Furthermore, as IEEE 802.11b/g nodes do not defer anymore for the transmissions of IEEE 802.15.4 packets, to ensure non-overlapping transmissions, the following condition needs to be satisfied:

$$t_{idle} \triangleq DIFS + m \cdot T_{bs} \geq CCA + t_p + SIFS + ACK \tag{2.3}$$

where t_p is the transmission time of an IEEE 802.15.4 packet.

We now show that the inequality (2.3) cannot hold. We take the maximum value of the LHS, LHS_{max}, and the minimum value of the RHS,

RHS_{min}, of (2.3) as follows:

$$\begin{aligned} LHS_{max} &= DIFS + CW_{min} \cdot T_{st} \\ &= \begin{cases} 50 + 31 \cdot 20 = 670\mu s & \text{for 802.11b} \\ 28 + 15 \cdot 9 = 163\mu s & \text{for 802.11g} \end{cases} \end{aligned}$$

$$\begin{aligned} RHS_{min} &= CCA + t_{pmin} + SIFS + ACK \\ &= 128 + 640 + 192 + 160 = 1120\mu s \end{aligned}$$

where $t_{idlemax}$ is the maximum t_{idle} and t_{pmin} is the minimum packet transmission time, which is 640 μs, given by a minimum packet size of 160 bits transmitted at the rate of 250 kbps. The values of the relevant parameters are given in Table 2.1.

We see that since LHS_{max} is less than RHS_{min}, the inequality (2.3) cannot hold in any case. Even for the case that an ACK is not employed, where the RHS of (2.3) has only two items, CCA and t_p, (2.3) still cannot hold because LHS_{max} remains less than RHS_{min}, which is 768 μs. As such, in R_2, no IEEE 802.15.4 packet can be received during an interval of two consecutive IEEE 802.11b/g packets.

In Section 2.5, we addressed that under IEEE 802.11b/g interference, an IEEE 802.15.4 packet cannot be received successfully unless at least one of the two conditions, i.e., the power conditions and the timing condition, can be satisfied. The power condition says that an IEEE 802.15.4 packet and its following ACK if any can be received successfully in spite of overlapped IEEE 802.11b/g interference as long as the Signal-to-Interference-Ratio (SIR) is good enough. And the timing condition actually says that no matter how severe IEEE 802.11b/g interference is, an IEEE 802.15.4 packet and its following ACK if any can be transmitted and received successfully in an interval between two consecutive IEEE 802.11b/g packets.

According to the analysis above, we learn that in R_2, since no IEEE 802.15.4 packet (regardless of using an ACK or not) can be received during an interval of two consecutive IEEE 802.11b/g packets, an IEEE 802.15.4 packet cannot be received successfully unless the Signal-to-Interference-Ratio (SIR) is good enough.

In Region R_3

In this region, neither IEEE 802.15.4 nodes nor IEEE 802.11b/g nodes can sense the other. IEEE 802.15.4 nodes, however, may still suffer from the IEEE 802.11b/g interference in case of weak IEEE 802.15.4 links, because a region in which a wireless device can cause interference to others is usually larger than that where it can be sensed by the others. This means both IEEE 802.15.4 nodes and IEEE 802.11b/g can freely transmit packets without deferring for the other, which is described as the assumption, called blind transmissions in [Shi05].

It can be shown that like in R_2, in case of using ACKs, the timing condition described as inequality (2.3), i.e., the condition for non-overlapping transmissions, can never hold in R_3, too. Therefore, for a successful IEEE 802.15.4 transmission, a good SIR at the receivers is necessary. By contrast, unlike in R_2, in case of not using ACKs, the condition for non-overlapping transmissions could be satisfied in R_3.

From the discussion above, we see that IEEE 802.11b/g nodes and IEEE 802.15.4 nodes have a mutual impact only in R_1, which makes the coexistence in R_1 the most interesting as well as the most complicated. Therefore, in the following section, we will focus on analyzing the coexistence performance in R_1.

2.6 Throughput Analysis of 802.15.4 networks in R_1

In this section, we analyze the IEEE 802.15.4 coexistence performance in terms of throughput in R_1. For ease of analysis, we assume that there are only one pair of IEEE 802.15.4 nodes and one pair of IEEE 802.11b/g nodes. We will discuss this assumption at the end of this section. Furthermore, in each pair, one node is a transmitter and the other is a receiver. In addition, we assume the physical channel conditions are ideal, i.e., no transmission error would occur if there is no interference. Thus, the IEEE 802.11b/g transmitter can always receive ACKs after transmitting data packets, causing its contention window to keep the initial value, i.e., CW_{min}. According to [How03] [Pet06] [Sik05] and our own simulation, IEEE 802.15.4 has little impact on IEEE 802.11 performance, which justifies our assumption that the IEEE 802.11b/g traffic is not affected by the IEEE 802.15.4 traffic. Finally, we assume that both IEEE 802.11b/g traffic and IEEE 802.15.4 traffic are in the saturation mode, which implies that there is always at least one packet awaiting transmission at the transmitters.

As shown in Figure 2.8, for each transmission attempt, an IEEE 802.15.4 node performs a backoff first for an interval sampled from a uniform distribution over the range $[0, 2^{BE_i - 1}](i = 0, 1, 2, 3, 4)$, where BE_i is the backoff exponent for the i^{th} retransmission attempt and 0^{th} retransmission attempt means the first transmission attempt. A successful CCA will be followed by a successful IEEE 802.15.4 packet transmission. Otherwise, in the case of a busy channel, the IEEE 802.15.4 node will defer for a backoff period defined by BE_{i+1} and then perform a CCA again until the default maximum retry limit, i.e., 4, is reached [IEE06]. Subsequently, an error of channel access failure will be reported to the upper layer. In either case, a new transmission cycle will start with a backoff period defined by BE_0 for the next packet to

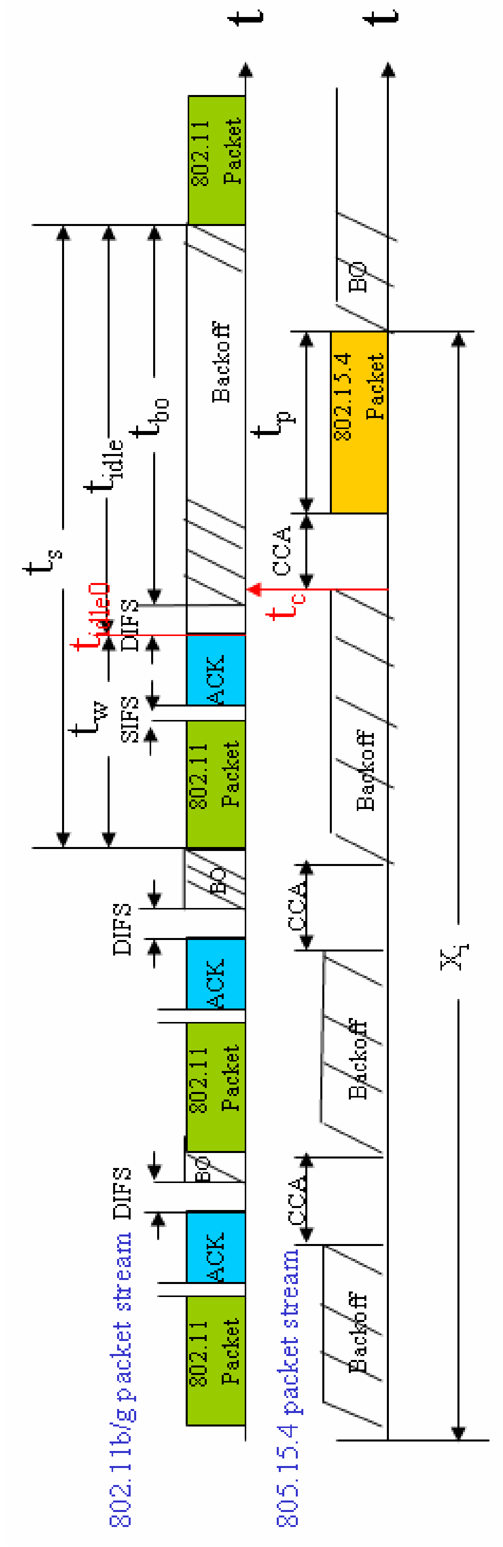


Figure 2.8: Coexistence Model: Timing Aspect in R_1

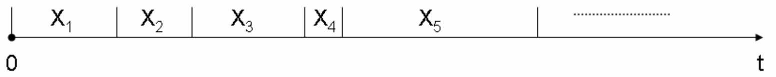


Figure 2.9: Packet Transmission Renewal Process (X_j: the transmission cycle time of the j^{th} packet)

be transmitted.

Owing to the assumption that the IEEE 802.11b/g traffic is not affected by the IEEE 802.15.4 traffic and the fact that the timing of IEEE 802.11b/g and IEEE 802.15.4 is significantly different, the transmission cycle times of IEEE 802.15.4 packets are considered independent of each other. Therefore, the transmission of IEEE 802.15.4 packets is essentially a renewal process. Let X denote the transmission cycle time of a packet, which either is transmitted successfully at i^{th} retransmission or fails to be transmitted eventually after the default five unsuccessful channel access attempts [IEE06]. Thus, X is actually the inter-renewal time of the renewal process. Furthermore, let X_j denote the transmission cycle time of the j^{th} packet, shown in Figure 2.9 and let $\{W(t); t > 0\}$ be a renewal reward function for the renewal process with expected value of the inter-renewal time $\mathbb{E}$(X). Thus according to [Gal96], the throughput S is given by

$$S = \lim_{t \to 0} \frac{1}{t} \int_{t}^{\tau} W(\tau) d\tau = \frac{\mathbb{E}[W_n]}{\mathbb{E}[X]} \quad \text{with probability 1} \tag{2.4}$$

where $\mathbb{E}[W_n]$ is the expected value of the reward, i.e., the transmission time of one IEEE 802.15.4 packet, denoted by t_p, in the n^{th} renewal interval.

We now compute $\mathbb{E}[W_n]$. Since during the n^{th} renewal interval, either only one packet or no packet is transmitted, W_n correspondingly equals either t_p or zero. Thus,

$$\mathbb{E}[W_n] = p \cdot \mathbb{E}[t_p] \cdot \sum_{i=0}^{4} (1-p)^i + 0 \cdot (1-p)^5 = p \cdot \mathbb{E}[t_p] \cdot \sum_{i=0}^{4} (1-p)^i \tag{2.5}$$

where $\mathbb{E}[t_p]$ is the expected value of t_p and p is the probability that the channel is sensed idle during a CCA period. According to the assumption that the IEEE 802.11b/g traffic is not affected by the IEEE 802.15.4 traffic, the IEEE 802.11b/g interference is actually an on-off autonomous process, independent of the IEEE 802.15.4 traffic. It is on for a period t_p and off for a period $DIFS + t_{bo}$, where t_{bo} is a uniform RV on $[0, CW_{min}] \cdot T_{bs}$. Therefore, between two successive transmission attempts of an IEEE 802.15.4 node, the state, on or off, of the interference is independent. To make the transmission attempts of an IEEE 802.15.4 node successful, two conditions need to be satisfied:

1. The idle time t_{idle} between two consecutive IEEE 802.11b/g packets needs to be longer than the CCA period of an IEEE 802.15.4 packet,

i.e., $t_{idle} \geq CCA$, so that the IEEE 802.15.4 packet could seize the channel;

2. Given 1), the CCA starts and ends within the period t_{idle}. This event is denoted by E.

Thus, p is given by

$$\begin{aligned} p &= P\{t_{idle} \geq CCA \cup \mathsf{E}\} \\ &= P\{t_{idle} \geq CCA\} \cdot P\{\mathsf{E} \mid t_{idle} \geq CCA\} \end{aligned} \quad (2.6)$$

Given the parameter values in Table 2.1, the condition $t_{idle} \geq CCA$ holds if $t_{bo} \in [a, CW_{min}] \cdot T_{bs}$, where a equals 4 and 12 for IEEE 802.11b nodes and IEEE 802.11g nodes respectively. Thus, p is further given by

$$\begin{aligned} p = &\sum_{i=a}^{CW_{min}} P\{t_{idle} = DIFS + iT_{bs}\} \\ &\cdot P\{t_{idle0} \leq t_c \leq t_{idle0} + DIFS + iT_{bs} - CCA\} \\ = &\frac{1}{CW_{min}+1} \cdot \sum_{i=a}^{CW_{min}} \frac{DIFS + iT_{bs} - CCA}{\mathbb{E}[t_w] + DIFS + iT_{bs}} \end{aligned} \quad (2.7)$$

where t_{idle0} is the start time of the period t_{idle}, t_c is the CCA start time, uniformly distributed over $[0, t_s]$, where t_s is the transmission cycle time of an IEEE 802.11b/g packet, i.e., $t_s = t_w + DIFS + iT_{bs}$, $i = a, \ldots, CW_{min}$, and t_w is the sum of an IEEE 802.11b/g packet transmission time, a following SIFS time and an ACK time. These parameters are shown in Figure 2.8.

By substituting (2.7) in (2.5), $\mathbb{E}[W_n]$ is given. We now compute $\mathbb{E}[X]$ as follows.

$$\begin{aligned} \mathbb{E}(X) = &\sum_{i=0}^{4} \left[p(1-p)^i \Big(\sum_{j=0}^{i} \mathbb{E}[B_i] + (i+1)CCA + \mathbb{E}[t_p] \Big) \right] \\ &+ (1-p)^5 \Big(\sum_{i=0}^{4} \mathbb{E}[B_i] + 5CCA \Big) \end{aligned} \quad (2.8)$$

where $\mathbb{E}[B_i]$, is the expected value of the backoff time, B_i, for the i^{th} retransmission, and B^i is uniformly distributed in $[0, 2^{BE_i}]$, owing to the assumption that the IEEE 802.11b/g traffic is not affected by the IEEE 802.15.4 traffic.

By substituting (2.5) and (2.8) into (2.4), the throughput S is obtained. When using the parameter values in Table 2.1, we get that when saturate IEEE 802.11b interference occurs in R_1, the throughput of the IEEE 802.15.4 nodes declines to 5.75% of the original value, which clearly shows that IEEE 802.11b interference can affect the performance of an IEEE 802.15.4 WSN significantly.

2.7 Coexistence Model Evaluation

In this work, we use a simulation tool, OPNET, to evaluate the coexistence model we proposed[1]. We first give a brief introduction about OPNET.

2.7.1 OPNET

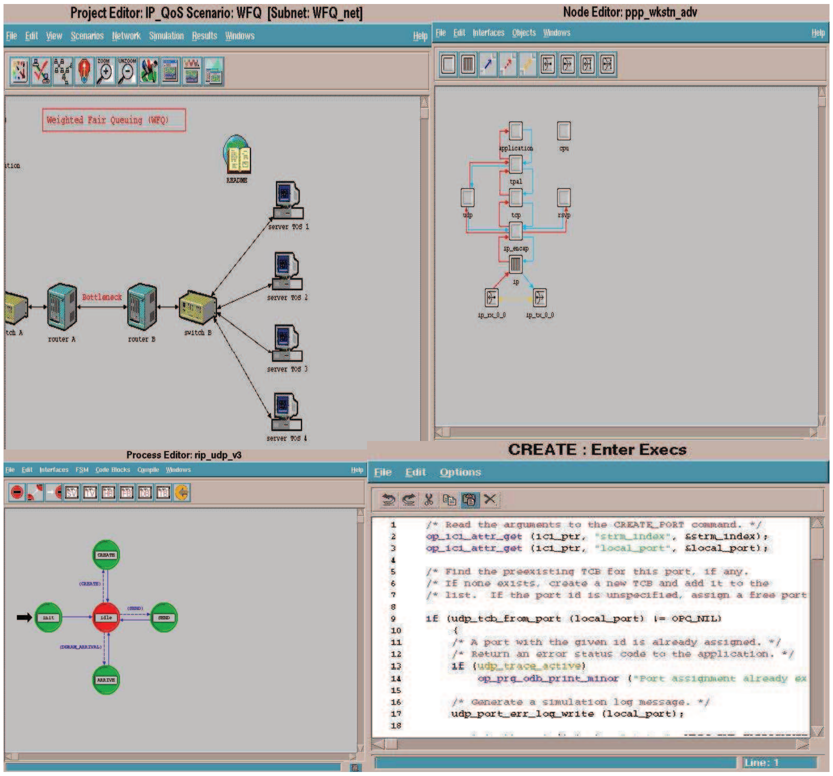
OPNET is one of the most popular simulator tools specialized for network research and development [OPN]. It is developed by OPNET Technologies, Inc. OPNET stands for Optimized Network Engineering Tools. It provides a graphical editor interface to build models for various network entities from physical layer modulator to application processes. Built on the top of a discrete event system, OPNET simulates the system behavior by modeling each event happening in the system and processes it by user-defined processes. All components are modeled using an object-oriented approach which gives an intuitive mapping to real systems. As shown in Figure 2.10, OPNET uses a three-tiered hierarchical structure to organize all the components in three domains, which are network, node, and process models. A network model is a high-level description of the objects contained in the system. It specifies the objects in the system as well as their physical locations, interconnections and configurations. A node model specifies the internal structure of a network node. Typical nodes include workstations, packet witches, satellite terminals and remote sensors. A process model is used to specify the behavior of a processor and queue modules, which exists in a node domain.

The design methodology for OPNET simulation is usually bottom-up in that a user first creates process models, then constructs node models which incorporate the processes, and finally constructs network models that are populated with the node models. OPNET also provides programming tools for users to define any type of packet format they want to use in their own protocols. Programming in OPNET includes the following major tasks: define the protocol packet format, define the state transition machine for processes running the protocol, define process modules and transceiver modules we need in each device node, finally define the network model by connecting the device nodes together using user-defined link models [Pan10]. As such, OPNET enables users to design and study communication networks, devices, protocols, and applications.

2.7.2 Simulation configuration and parameters

The values of relevant parameters are listed in Table 2.1. Note that the bandwidth of IEEE 802.11b is 22 MHz, which is much larger than that of

[1] The source code of OPNET simulation in this thesis is the property of Koninklijke Philips Electronics N.V. For information about the source code, please contact Philips Research in Eindhoven, The Netherlands.


Project Editor: IP_QoS Scenario: WFQ [Subnet: WFQ_net]
File Edit View Scenarios Network Simulation Results Windows Help
Weighted Fair Queuing (WFQ)
README
server ToS 1
server ToS 2
server ToS 3
server ToS 4
Bottleneck
router A
router B
switch B
Node Editor: ppp_wkstn_adv
File Edit Interfaces Objects Windows Help
application
cpu
tpal
udp
tcp
rsvp
ip_encap
ip
ip_rx_0_0
ip_tx_0_0
Process Editor: rip_udp_v3
File Edit Interfaces FSM Code Blocks Compile Windows Help
CREATE
init
idle
SEND
ARRIVE
CREATE : Enter Execs
File Edit Options
Line: 1

```
/* Read the arguments to the CREATE_PORT command. */
op_ici_attr_get (ici_ptr, "strm_index", &strm_index);
op_ici_attr_get (ici_ptr, "local_port", &local_port);

/* Find the preexisting TCB for this port, if any.
/* If none exists, create a new TCB and add it to the
/* list.  If the port id is unspecified, assign a free port

if (udp_tcb_from_port (local_port) != OPC_NIL)
    {
    /* A port with the given id is already assigned. */
    /* Return an error status code to the application. */
    if (udp_trace_active)
        op_prg_odb_print_minor ("Port assignment already ex

    /* Generate a simulation log message. */
    udp_port_err_log_write (local_port);

```

Figure 2.10: Three-tiered OPNET Hierarchy

IEEE 802.15.4, i.e., 2 MHz. So the signal of IEEE 802.11b/g interference can be modeled as bandlimited Additive White Gaussian Noise (AWGN) to IEEE 802.15.4 signals [Shi05]. Since the bandwidth of 802.11b/g is 11 times that of 802.15.4, in-band interference power of 802.11b/g to 802.15.4 is usually calculated as $P_r/11$, where P_r is the received power. However, the power spectral density of 802.11b/g is not uniformly distributed across the 22 MHz band. Figure 2.5 from [IEE99a] illustrates the power spectral density of 802.11b.

In our simulations, to show the worst case of sharing spectrum, we employ the channels for IEEE 802.11b/g and IEEE 802.15.4 in the 2.4 GHz ISM band in such a way that the center frequencies f_c of the channels are closest to each other. Thus, we employ 2412 MHz and 2410 MHz as the center frequencies for IEEE 802.11b/g and IEEE 802.15.4 respectively, shown in Figure 1.10. The closer their center frequencies become; the stronger IEEE 802.11b/g interference to IEEE 802.15.4 is, because more power is distributed around the center frequency as shown in Figure 2.5[IEE99a].

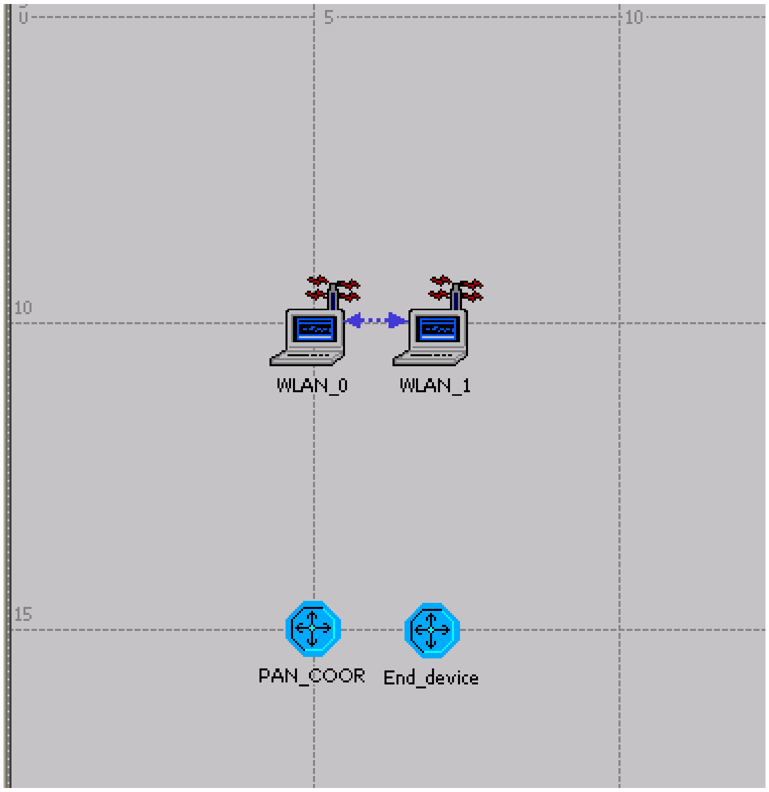


Figure 2.11: In R_1: 802.15.4 and 802.11b/g are in a region where they can sense each other

2.7.3 Simulation of the IEEE 802.15.4 Coexistence Performance in R_1

Given the parameter values in Table 2.2, R_1 is a circle area, of which the radius is less than 22 m and 32 m for IEEE 802.11b and IEEE 802.11g, respectively. Hence as shown in Figure 2.11, we set the distance between two IEEE 802.11 nodes and that of IEEE 802.15.4 nodes as 2 m, and the distance between IEEE 802.11 nodes and IEEE 802.15.4 nodes as 5 m, to ensure both can sense each other, i.e., in R_1. A saturated UDP packet traffic, which, in our simulation, is 532 packets per second at a rate of 11 Mbps, is transmitted between IEEE 802.11b WLAN_0 and WLAN_1. Only the IEEE 802.15.4 coordinator, PAN_COOR, transmits data packets, while the destination node, End_device, sends only ACKs.

Figure 2.12 shows that when the 802.11b interference occurs, the throughput of the IEEE 802.15.4 node goes from 18000 bps on average down to 1000 bps on average, i.e., only 5.56% throughput remains. This result matches the analytical result, i.e., 5.75%, in Section 2.6 and thus verifies our analysis.

From both analytical and simulation results above, we conclude that even in the worst case in the region R_1, the throughput of an IEEE 802.15.4 WSN,

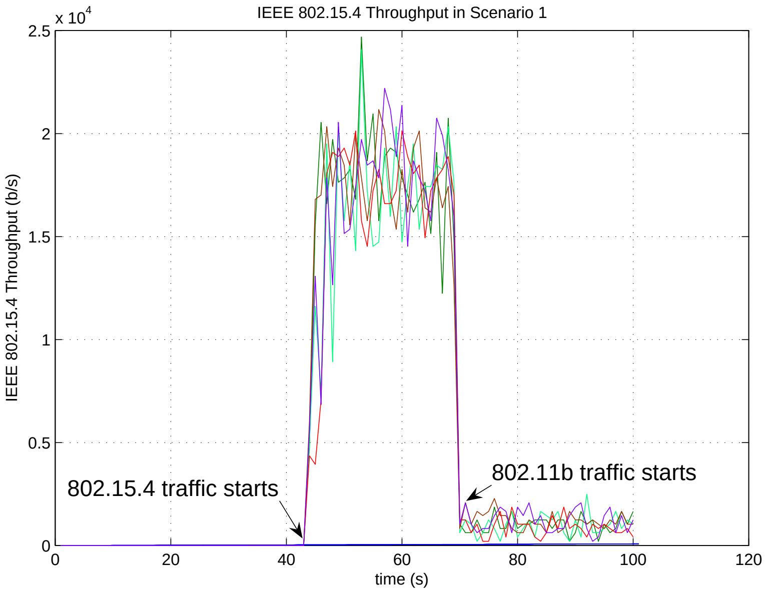


Figure 2.12: Throughput of IEEE 802.15.4 nodes before and after IEEE 802.11b interference occurs in R_1

though it declines significantly, never reach zero. This is because in R_1, IEEE 802.11b/g nodes can sense IEEE 802.15.4 traffic, and therefore may pause, which allows a small part of IEEE 802.15.4 traffic to pass. The conclusion is also validated by the experiments in [Sik05].

2.7.4 Simulation of the IEEE 802.15.4 Coexistence Performance in R_2

In Section 2.5, the sensing range is 22 m for IEEE 802.11b. In the current simulation scenario, we set the distance between two IEEE 802.11b nodes still as 2 m and that of IEEE 802.15.4 nodes as 15 m to show a case where the power condition is not satisfied. The distance between IEEE 802.11b nodes and IEEE 802.15.4 nodes is 30 m, which is 8m further away from the IEEE 802.11b nodes' sensing range.

Figure 2.13 shows that the throughput of IEEE 802.15.4 goes down to zero as the IEEE 802.11b interference occurs, which verifies that the coexistence is impossible if the power condition is not satisfied in the region R_2.

The results given in Section 2.7.3 and 2.7.4 show that IEEE 802.11b/g interference can affect an IEEE 802.15.4 WSN's performance very badly. Thus, the ZigBee Alliance's claim in [Zig07a], i.e., "even in the presence of a surprising amount of interference, ZigBee devices continue to communicate effectively", is not universally true.

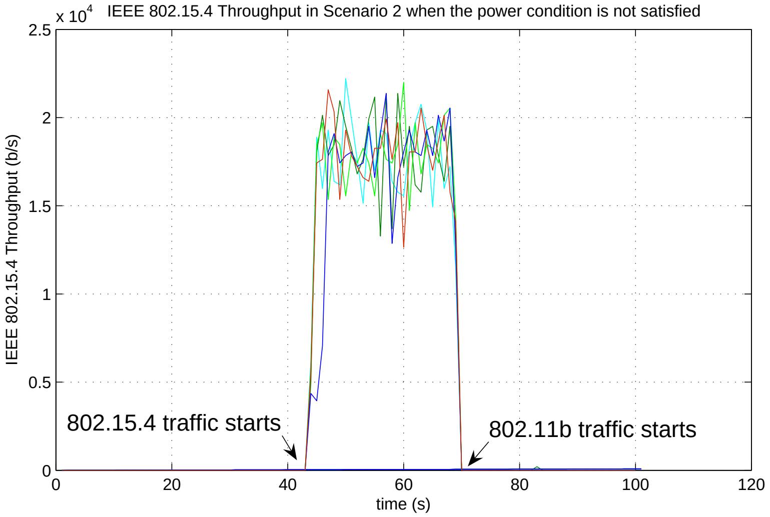


Figure 2.13: Throughput of IEEE 802.15.4 nodes before and after IEEE 802.11b/g interference occurs in R_2

2.8 Conclusions and Further Discussion

In this chapter, we proposed a coexistence model of IEEE 802.15.4 nodes and IEEE 802.11b/g nodes based on two aspects, i.e., power and timing. Due to the significant difference in transmit powers of IEEE 802.15.4 and IEEE 802.11b/g, the sensing ranges of them are quite asymmetric. As a result, three distinct coexistence regions can be identified. In each of these coexistence regions, IEEE 802.11 nodes and IEEE 802.15.4 nodes exhibit different interplay and hence different coexistence performances, which may not be the same as we expected. For example, instinctively, we may feel that the closer an IEEE 802.15.4 node gets to an IEEE 802.11b/g interferer, the worse performance the IEEE 802.15.4 node would have. Our coexistence model, however, reveals that this perception is not true. In fact, as the IEEE 802.15.4 node and the IEEE 802.11b/g interferer get so close that they are in the coexistence region R_1, where they can sense each other, the coexistence performance of the IEEE 802.15.4 node is not necessary the worst. Instead, in the coexistence region R_2, where the IEEE 802.11b/g interferer cannot sense the IEEE 802.15.4 and therefore does not respect the IEEE 802.15.4 transmission, the coexistence performance of the IEEE 802.15.4 node could get even worse than in R_1.

While developing the coexistence model, we made several assumptions. Those assumptions simplified the complex reality so that we were able to develop an analytical model, which reflects only the most essential aspects of the coexistence. Meanwhile, those assumptions must have brought about some effects on our work. The effects are therefore worthy of further discussion.

First of all, we assumed the IEEE 802.11b/g interference is always saturated. In fact, despite the increasing popularity of IEEE 802.11b/g-based applications, IEEE 802.11b/g interference cannot be always saturated. Non-saturated IEEE 802.11b/g interference will change the timing aspect of our coexistence model, i.e., give a longer space of time for IEEE 802.15.4 packet transmission. Thus, a better coexistence performance of an IEEE 802.15.4 WSN can be expected under non-saturated IEEE 802.11b/g interference. It would make sense to examine the coexistence performance of an IEEE 802.15.4 WSN under some real and typical IEEE 802.11b/g traffic in the future. Besides, although non-saturated IEEE 802.11b/g traffic has nothing to do with the transmit power of either IEEE 802.11b/g or IEEE 802.15.4, i.e., does not change the power aspect of our coexistence model, the three coexistence regions will therefore still somehow exist but become less recognizable as IEEE 802.11b/g traffic gets lighter.

Second, also for investigating the worst case, we assumed that the operational frequency bands of IEEE 802.11b devices and IEEE 802.15.4 devices overlap each other to the most extent, i.e., only 2 MHz offset between the center frequency of IEEE 802.15.4 and that of IEEE 802.11b. The power spectral density of IEEE 802.11b in Figure 2.5 shows that most of its power is concentrated in a narrow band around the center frequency. Thus, as the frequency offset increases, the portion of IEEE 802.11b device power which can impact on IEEE 802.15.4 devices declines. This means that the coexistence region R_1 shrinks until it totally disappears. Meanwhile, the part of IEEE 802.15.4 device power which is received by IEEE 802.11b devices declines, too. This means that the coexistence region R_2 also shrinks until it totally disappears. Moreover, when there is no overlap in their operational frequency bands, the coexistence R_3 disappears too.

Third, for ease of analysis, we assumed that there are only one pair of IEEE 802.15.4 devices and one pair of IEEE 802.11b/g devices. In fact, it is not uncommon that there are more than just one pair of IEEE 802.11b/g devices and one pair of IEEE 802.15.4 devices in a certain environment. In such a case, one IEEE 802.11b/g device may have a mutual influence with one IEEE 802.15.4 device but an one-way influence with another IEEE 802.15.4 device at the same time, which would make a theoretical analysis very complicated. If one of the influences is dominant, a theoretical analysis may be done by ignoring the other influence. Otherwise, if there are many different influences and the influences are comparably strong, a theoretical analysis may be too complicated to be done. In this case, one can use simulation tools. These are not part of this thesis, but would be worthwhile to be investigated in the future.

The assumptions above simplified the complexity of the real world and therefore made it possible for us to make an analytical coexistence model, which was further validated by the OPNET simulation. Each assumption, on the other hand, inevitably made its own impact on the analytical and simulation results. Thus, it would be interesting and valuable to examine the model further by performing experiments. We hope that not only can the experiments validate our analytical model, but, more importantly, bring to us more insights into the coexistence issue. If it is the case, then we could be able to improve the model so that it describes the real world better.

Let us more explore the coexistence of IEEE 802.15.4 and IEEE 802.11b/g in the next chapter.

Chapter 3

Model Enhancement

It can enhance our vision, so that we become aware of a new and deeper meaning in what we see around us.

- Walter T. Monnington

In the previous chapter, we built a coexistence model of IEEE 802.15.4 WSNs and IEEE 802.11b/g WLANs. By identifying three distinct coexistence regions, the model explained the coexistence behavior of IEEE 802.15.4 WSNs and IEEE 802.11b/g WLANs. In this chapter, we will improve the model by introducing two important implementation factors: the transceiver's Rx-to-Tx turnaround time and the CCA partial detection effect. We expect the enhanced model can provide more insights about the coexistence of IEEE 802.15.4 WSNs and IEEE 802.11b/g WLANs in the real-life environment, and therefore more accurately explain and predict the IEEE 802.15.4 coexistence performance in reality. Thus, we will validate the enhanced model by not only OPNET simulation but experiments as well. Besides, in the previous chapter, the coexistence performance of IEEE 802.15.4 WSNs and IEEE 802.11b/g interference was investigated in only one of three coexistence regions defined in the model. In this chapter, however, we will extend the investigation to all the three coexistence regions and various scenarios.

The remainder of the paper is organized as follows: Section 3.1 presents the enhanced coexistence model to characterize the coexistence issue. Then the model is validated by experiments and simulation in Section 3.3. Section 3.2 provides a performance analysis of IEEE 802.15.4 WSNs under IEEE 802.11b/g interference in all the three coexistence regions, and Section 3.3.3 shows the simulation results in various scenarios. Finally, conclusions are drawn in Section 3.4.

3.1 An Enhanced Coexistence Model

In Section 2.5, we proposed a coexistence model of IEEE 802.11b/g and IEEE 802.15.4 networks. By incorporating some implementation factors, in this section, we will enhance the model. First, we give a short recap about the model.

For the following discussion on the new model, the assumptions in the Section 2.5 still hold, e.g., saturated IEEE 802.11b/g interference is always assumed. This corresponds to the presence of the worst-case of interference, which in practice would occur, e.g., as IEEE 802.11b/g nodes transfer video streams or large files.

As discussed in Section 2.5, under IEEE 802.11b/g interference, an IEEE 802.15.4 packet can be successfully received if either of the following two conditions is satisfied [Yua07].

Condition A: When the IEEE 802.15.4 packet overlaps an IEEE 802.11b/g packet, the in-band interference power from the IEEE 802.11b/g packet is significantly lower than the useful signal power from the IEEE 802.15.4 packet at an IEEE 802.15.4 receiver. According to the IEEE 802.15.4 specification [IEE06], if interference is so weak that the in-band signal-to-interference ratio (SIR) is larger than 5-6 dB, an IEEE 802.15.4 packet can be successfully received with a probability of 99%.

Condition B: The transmission time of an IEEE 802.15.4 packet is shorter than the inter-frame idle time between two consecutive IEEE 802.11b/g packets so that the IEEE 802.15.4 packet does not overlap an IEEE 802.11b/g packet.

Correspondingly, the new model still includes the power and timing aspects as follows:

Power Aspect

The transmit powers of IEEE 802.11b/g nodes and IEEE 802.15.4 nodes are typically 100 mW [IEE99b] and 1 mW [IEE06], respectively. In case of comparable CCA thresholds as they are in fact (see Table 3.1), the significant difference in the transmit power can result in three distinct regions as illustrated in Figure 2.4:

R1: a region in which IEEE 802.15.4 nodes and IEEE 802.11b/g nodes can sense each other;

R2: a region in which IEEE 802.15.4 nodes can sense IEEE 802.11b/g nodes, but not *vice versa*;

R3: a region in which neither can sense the other, but IEEE 802.15.4 nodes could still suffer IEEE 802.11b/g interference.

Timing Aspect

- **In R1**

In R1, an IEEE 802.11b/g node and an IEEE 802.15.4 node can sense each other by ED and therefore both of their CSMA/CA mechanisms work, i.e., as one is transmitting, the other has to be waiting. IEEE 802.15.4 nodes,

Table 3.1: IEEE 802.15.4 and IEEE 802.11b/g System Parameters and additional parameters used in simulation and experiments

	IEEE 802.15.4	**IEEE 802.11b**	**IEEE 802.11g**
Transmit power	0 dBm	17 dBm	17 dBm
Receiver sensitivity	-85 dBm	-76 dBm	-82 dBm
Bandwidth	2 MHz	22 MHz	22 MHz
Data rate	250 kbps	11 Mbps	54 Mbps
Backoff unit T_{bs}	320 μs	20 μs	9 μs
SIFS	192 μs	10 μs	10 μs
DIFS	N/A	50 μs	28 μs
CCA duration	128 μs	$\leq$ 15 μs	$\leq$ 4 μs
CCA threshold	-85 dBm	-84 dBm	-84 dBm
CW_{min}	7	31	15
Center frequency	2410 MHz	2412 MHz	2412 MHz
Payload size	30 bytes	1500 bytes	1500 bytes
ACK	No	Yes	Yes
Transmit intensity	Every 20 ms	Saturated	Saturated
Tx-to-Rx turnaround	$<$ 192 μs	$<$ 10 μs	$<$ 10 μs
Rx-to-Tx turnaround	$<$ 192 μs	$<$ 5 μs	$<$ 5 μs

however, typically have a 10 - 30 times longer timing than IEEE 802.11b/g nodes, e.g., the backoff slot unit is 320 μs, 20 μs and 9 μs for IEEE 802.15.4, IEEE 802.11b and IEEE 802.11g, respectively, shown in Table 3.1. The shorter timing gives IEEE 802.11b/g nodes priority over IEEE 802.15.4 nodes to access the channel and therefore causes unfairness to the IEEE 802.15.4 nodes in R1, as illustrated in Figure 3.1.

Once the IEEE 802.15.4 nodes sense the channel idle for a CCA duration and therefore seize the channel, they can transmit packets, theoretically, free from interference because the IEEE 802.11b/g nodes will defer for the IEEE 802.15.4 packet transmission in this region, i.e., R1. In practice, however, the IEEE 802.15.4 nodes have to spend 12 symbol periods, i.e., 192 μs, at most on turning around their states from receiving to transmitting, i.e., an ***Rx-to-Tx turnaround time*** [IEE06], T_{ta}, *during which, however, the channel state may change from idle to busy.*

Besides, in many research papers and widely used simulation tools like OPNET, it is often ignored and therefore implicitly assumed that a CCA always reports a busy channel once the CCA window has an overlap to any extent with a transmitting packet. In practice, however, this is not true. A typical digital ED receiver samples the channel N times during the CCA, sums up the sampled energy and compares the sum, $E_{samples}$, to a preset ED threshold Γ. If $E_{samples} > \Gamma$, ED reports the channel busy; otherwise, it

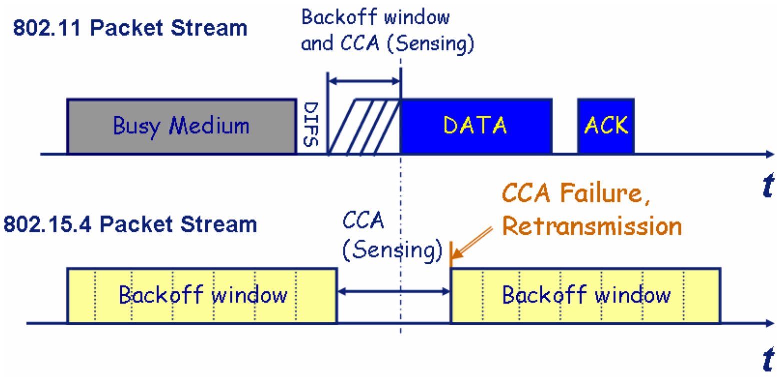


Figure 3.1: In R1: the shorter timing gives IEEE 802.11b/g nodes priority over IEEE 802.15.4 nodes to access the channel and therefore causes unfairness to the IEEE 802.15.4 nodes

reports the channel idle. It is not uncommon that ED samples only a part of a packet, i.e., the overlapping part, denoted as d, shown in Figure 3.2. We call this effect ***CCA partial detection***. We define a specific overlapping duration, d_m, such that given a Γ, d_m equals the maximum d over which $E_{samples} \leq \Gamma$.

Thus, under the saturated IEEE 802.11b/g interference in R1, IEEE 802.15.4 nodes could seize the channel and transmit packets if

$$CCA - d_m \leq t_{idle} \tag{3.1}$$

where t_{idle} is the idle time between two consecutive IEEE 802.11b/g packets. According to the specification [IEE99b],

$$t_{idle} \triangleq DIFS + t_{bo} = DIFS + m \cdot T_{bs} \tag{3.2}$$

where t_{bo} is a random period of time for an additional deferral time before transmitting and $t_{bo} \triangleq m \cdot T_{bs}$, where T_{bs} is a backoff unit and m is a random integer drawn from a uniform distribution over the interval $[0, CW_{min}]$. Note that Equation (3.2) does not include the turnaround time of Rx-to-Tx and Tx-to-Rx for IEEE 802.11b/g nodes since it is very short (<15 μs in total [IEE99b]). By contrast, the turnaround time, T_{ta}, of Rx-to-Tx and Tx-to-Rx for IEEE 802.15.4 nodes should be taken into account because it could be even longer than an IEEE 802.15.4 CCA duration. The values of these parameters are shown in Table 3.1.

In practice, satisfying Inequation (3.1) can only ensure IEEE 802.15.4 nodes seize the channel and transmit packets but not guarantee the transmitted packets free from IEEE 802.11b/g interference, which additionally requires either

$$CCA + T_{ta} - d_m \leq t_{idle} \tag{3.3}$$

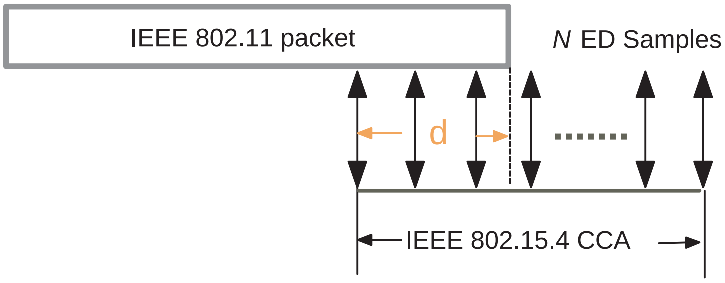


Figure 3.2: IEEE 802.15.4 ED detects only a partial IEEE 802.11b packet over a CCA duration

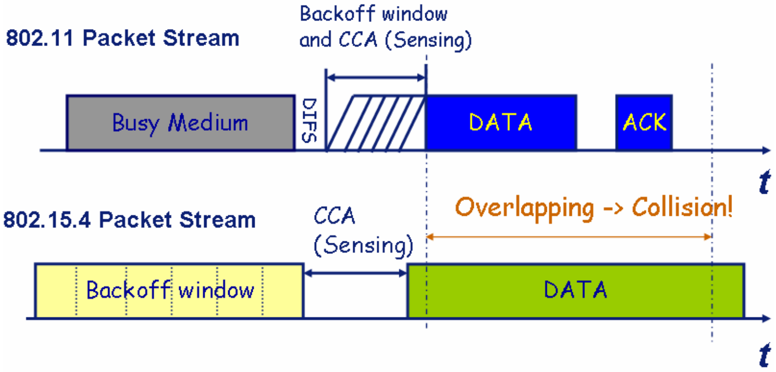


Figure 3.3: In R2, IEEE 802.11b/g nodes fails to sense IEEE 802.15.4 nodes

or a constantly sufficient SINR at the IEEE 802.15.4 receivers.

From the discussion above, we learn that the practical CCA implementation has a significant impact on the performance of CCA, causing the IEEE 802.15.4 CCA performance in practice not as "perfect" as described in theory. In Section 3.3, we will further investigate the real IEEE 802.15.4 CCA performance in more detail.

- **In R2**

In R2, IEEE 802.15.4 nodes can sense IEEE 802.11b/g nodes but not *vice versa* in case of comparable CCA thresholds as they actually are (see Table 3.1), because the transmit power of IEEE 802.11b/g nodes is much higher than that of IEEE 802.15.4 nodes. Consequently, when IEEE 802.11b/g nodes are transmitting, IEEE 802.15.4 nodes have to be waiting, whereas when IEEE 802.15.4 nodes are transmitting, IEEE 802.11b/g nodes are not aware and thus simply proceed to transmit, probably causing an overlapping in packet transmissions, as shown in Figure 3.3.

Therefore, to check whether IEEE 802.15.4 nodes can have successful transmissions in R2, we first see whether non-overlapping transmissions are possible. Like in R1, Inequation (3.1) needs to be satisfied. In addition, since IEEE 802.11b/g nodes do not defer anymore for IEEE 802.15.4 packets in R2, to ensure non-overlapping transmissions, the following condition also needs to be satisfied:

$$CCA + T_{ta} - d_m + t_p + SIFS + ACK \leq t_{idle} \tag{3.4}$$

where t_p is the transmission time of an IEEE 802.15.4 packet, and SIFS and ACK are those of IEEE 802.15.4. According to the parameter values given in Table 3.1, however, this condition cannot be satisfied. Thus, in case of using ACK, for successful transmissions of IEEE 802.15.4 packets in R2, the power condition A in Section 3.1 has to be satisfied. In case of not using ACK, the condition (3.4) becomes

$$CCA + T_{ta} - d_m + t_p \leq t_{idle} \tag{3.5}$$

This condition could be satisfied if IEEE 802.15.4 packets are very short, e.g., $t_p = 512\ \mu s$ (corresponding to 16-byte packets transmitted at the rate of 250 kbps), given that $t_{idle} = 670\ \mu s$ (i.e., m = CW_{min}= 31, $T_{bs} = 20\ \mu s$ in Equation (3.2)) and CCA = 128 μs.

- **In R3**

In R3, neither IEEE 802.15.4 nodes nor IEEE 802.11b/g nodes can sense the other. IEEE 802.15.4 nodes, however, may still suffer from the IEEE 802.11b/g interference in case of weak IEEE 802.15.4 links, because a range in which a wireless device can cause interference to others is usually larger than that where it can be sensed by the others. This means both IEEE 802.15.4 nodes and IEEE 802.11b/g nodes can freely transmit packets without deferring for the other, which is described as an assumption called blind transmissions in [Shi05].

Like in R2, it can be shown that in case of using ACK, the condition for non-overlapping transmission can never hold in R3, whereas it could hold in case of not using ACK and very short transmitted packets. In both cases, the successful transmissions of IEEE 802.15.4 packets could happen if the power condition A in Section 3.1 is satisfied.

3.2 Coexistence Performance Analysis

We have done a performance analysis of IEEE 802.15.4 WSNs under IEEE 802.11b/g interference in Section 2.6. However, the analysis there does not take into account the Rx-to-Tx turnaround time and CCA partial detection as addressed above, which may have a significant effect. Besides, the analysis was limited only to the coexistence region R1. Also, only one performance metric, i.e., throughput, is derived there. In this section, we will consider those factors, extend the analysis to all the three coexistence regions, and derive the other two important performance metrics, i.e., *packet loss ratio* and *packet delay*, in addition to *throughput*. Moreover, we will propose two important concepts: ***inhibition loss*** and ***collision loss***.

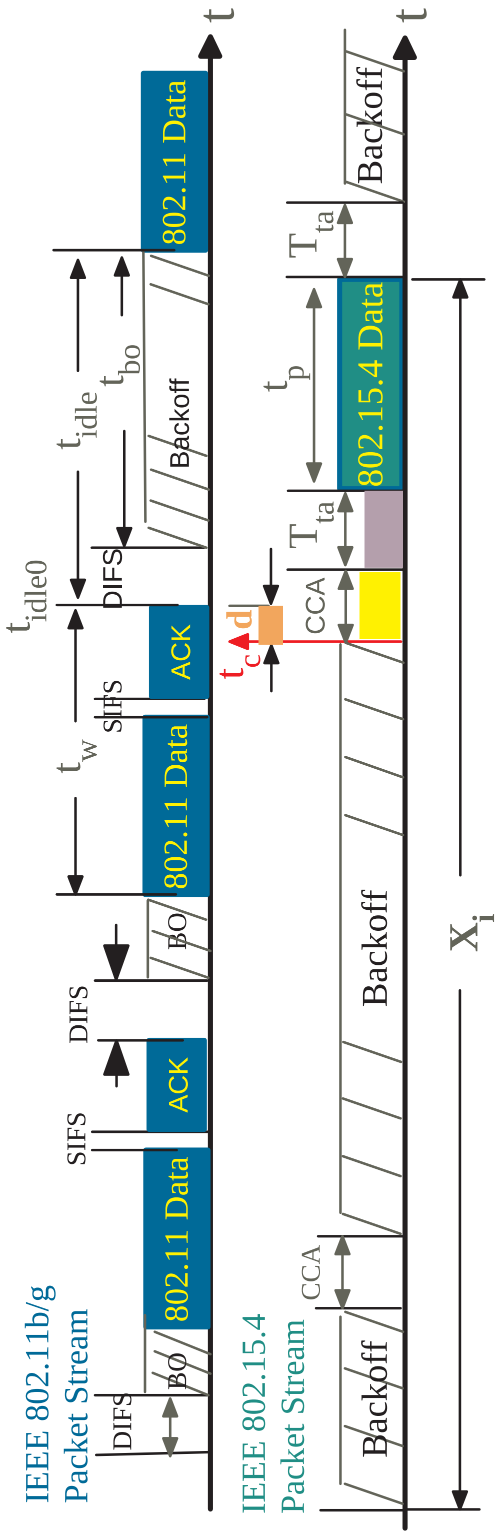


Figure 3.4: Coexistence Model in Timing Aspect

Like in Section 2.6, we assume that there is only one pair of IEEE 802.15.4 nodes and one pair of IEEE 802.11b/g nodes. In each pair, one node is a transmitter and the other is a receiver. Moreover, the physical channel condition is ideal. According to [Pet06] [How03] [Sik05] and our own simulation, IEEE 802.15.4 has little impact on the IEEE 802.11 performance, which suggests us to assume that the IEEE 802.11b/g traffic is not affected by the IEEE 802.15.4 traffic. Thus, the IEEE 802.11b/g transmitter can always receive ACKs after transmitting data packets, keeping its contention window equal to the initial value, i.e., CW_{min}. Finally, we assume that IEEE 802.11b/g traffic is in the saturation mode, which means that there is always at least one packet awaiting transmission at the transmitter.

As shown in Figure 3.4, for each transmission attempt, an IEEE 802.15.4 node performs a backoff first for an interval sampled from a uniform distribution over $[0, 2^{BE_i} - 1](i = 0, 1, 2, 3, 4)$, where BE_i is the backoff exponent for the i^{th} retransmission attempt, where the 0^{th} retransmission attempt means the first transmission attempt. A successful CCA will be followed by an IEEE 802.15.4 packet transmission. Otherwise, in the case of a busy channel, the IEEE 802.15.4 node will defer for a backoff period defined by BE_{i+1} and then perform a CCA again until the default maximum retry limit, i.e., 4, is reached [IEE06], where an error of channel access failure will be reported to the upper layer. In either case, a new transmission cycle will start with a backoff period defined by BE_0 for the next packet to be transmitted.

To obtain the IEEE 802.15.4 network performance metrics such as packet loss ratio, throughput and packet delay, we need to get **two key probabilities**, p_i and p_c, where p_i is the probability that the channel is idle over an IEEE 802.15.4 CCA duration and p_c is the probability that the transmitted IEEE 802.15.4 packets are hit by IEEE 802.11b/g interference. Let us first derive p_i and p_c, and then the performance metrics in R1, R2 and R3 respectively.

3.2.1 Coexistence Performance in R1

Owing to the assumption that the IEEE 802.11b/g traffic is not affected by the IEEE 802.15.4 traffic, p_i is constant. In fact, p_i is the equivalent of the probability that $E_{samples} \leq \Gamma$ as addressed in Section 3.1.

Although an IEEE 802.15.4 CCA may start at any point of the IEEE 802.11b/g packet stream, for a successful IEEE 802.15.4 packet transmission, denoted as E, the CCA should start within the interval $[t_{idle0} - d_m, t_{idle0} + t_{idle} - CCA + d_m]$, where t_{idle0} is the start time of the idle period t_{idle}. Thus, p_i is given by

$$p_i = P\{\mathsf{E}\} = \sum_{m=a-k}^{CW_{min}} P\{\mathsf{E_m}\} \tag{3.6}$$

where $\mathsf{E_m}$ represents E, i.e., a successful IEEE 802.15.4 packet transmission, conditioned on the chosen retransmission moment m, with $t_{bo} = mT_{bs}$, a equals 4 and 12 for IEEE 802.11b and IEEE 802.11g nodes, respectively, and $k = \lfloor d_m/T_{bs} \rfloor$.

Furthermore,

$$\begin{aligned} P\{\mathsf{E_m}\} &= P\{t_{bo} = mT_{bs}\} \\ &\quad \cdot P\{t_{idle0} - d_m \leq t_c \leq t_{idle0} + DIFS + mT_{bs} - CCA + d_m\} \end{aligned} \tag{3.7}$$

where t_c is the CCA start time, uniformly distributed over $[0, t_s]$, t_s is the transmission cycle time of an IEEE 802.11b/g packet, i.e., $t_s = t_w + DIFS + mT_{bs}$ and t_w is the sum of an IEEE 802.11b/g packet transmission time, a following SIFS period and ACK period, shown in Figure 3.4.

Since the backoff time is uniformly distributed, we get

$$P\{t_{bo} = mT_{bs}\} = \frac{1}{CW_{min} + 1} \tag{3.8}$$

Besides, as $k = \lfloor d_m/T_{bs} \rfloor$,

$$\begin{aligned} P\{t_{idle0} - d_m \leq t_c \leq t_{idle0} + DIFS + mT_{bs} - CCA\} \\ \approx \frac{DIFS + mT_{bs} - CCA + 2kT_{bs}}{\mathbb{E}[t_w] + DIFS + mT_{bs}} \end{aligned} \tag{3.9}$$

Thus, according to (3.6)(3.7)(3.8)(3.9), p_i is given by

$$p_i = \frac{1}{CW_{min} + 1} \sum_{m=a-k}^{CW_{min}} \frac{DIFS + mT_{bs} + 2kT_{bs} - CCA}{\mathbb{E}[t_w] + DIFS + mT_{bs}} \tag{3.10}$$

According to the IEEE 802.15.4 specification [IEE06], a pending IEEE 802.15.4 packet shall be discarded if the channel access attempts exceeds $macMaxCSMABackoffs$, the maximum number of backoffs the CSMA-CA algorithm will attempt before declaring a channel access failure. We let M denote $macMaxCSMABackoffs$. We call this kind of loss ***inhibition loss***. Thus the inhibition loss probability, denoted as α, is given by

$$\alpha = (1 - p_i)^{M+1} \tag{3.11}$$

Then β, the probability of IEEE 802.15.4 packets which can be sent out, is given by

$$\beta = 1 - \alpha \tag{3.12}$$

Now we deal with p_c, the probability that an IEEE 802.15.4 packet, though sent out by a transmitter, collides with an IEEE 802.11b/g packet. We call this kind of loss ***collision loss***. As the collision is due to an overlapping of the IEEE 802.15.4 packet and an IEEE 802.11b/g packet, let us get the probability, p_{no}, that a transmitted IEEE 802.15.4 packet does not overlap (hence not collide) with an IEEE 802.11b/g packet. Actually, p_{no} is the equivalent of the probability that a CCA together with a following Rx-to-Tx turnaround time T_{ta} fall into the period $[t_{idle0} - d_m, t_{idle0} + t_{idle}]$ as shown in Figure 3.4. This is because in such a case, IEEE 802.11 nodes will be able to sense the coming IEEE 802.15.4 packet and therefore suspend the transmission of their own packets. Thus, similar to the derivation of p_i, p_{no} is given by

$$p_{no} = \frac{1}{CW_{min} + 1} \sum_{n=b-k}^{CW_{min}} \frac{DIFS + nT_{bs} + 2kT_{bs} - CCA - T_{ta}}{\mathbb{E}[t_w] + DIFS + nT_{bs}} \tag{3.13}$$

where $b = \lceil (CCA + T_{ta})/T_{bs} \rceil$, which equals 14 and 33 for IEEE 802.11b and IEEE 802.11g, respectively, given the default 192 μs of T_{ta}. Since the IEEE 802.11g CW_{min} is only 15, less than 33, Equation (3.13) cannot hold in case of IEEE 802.11g given our assumption that the size of the contention window stays at CW_{min}. Thus, $p_{no} = 0$ for IEEE 802.11g in our case.

Then p_c can be given by

$$p_c = \beta \cdot (1 - \frac{p_{no}}{p_i}) \cdot p_e \tag{3.14}$$

where p_e is the IEEE 802.15.4 packet error rate. Assuming that bit errors are independent, p_e is given by

$$p_e = 1 - (1 - p_b)^N \tag{3.15}$$

where p_b is the IEEE 802.15.4 Bit Error Rate (BER) and N is the number of bits of an IEEE 802.15.4 packet. According to [IEE06], p_b is given by

$$p_b = \frac{8}{15} \times \frac{1}{16} \times \sum_{r=2}^{16} (-1)^r \binom{16}{r} e^{\left(20 \times SINR \times (\frac{1}{r} - 1)\right)} \tag{3.16}$$

Thus, p_c can be computed by Equation (3.14) (3.13) (3.15) (3.16).

With p_i and p_c, we now derive *throughput* S, *packet loss ratio* η and *expected packet delay* $\mathbb{E}(t_d)$, respectively. Owing to the assumption that the IEEE 802.11b/g traffic is not affected by the IEEE 802.15.4 traffic and the fact that the timing of IEEE 802.11b/g and IEEE 802.15.4 is significantly different, the transmission cycle times of IEEE 802.15.4 packets are considered independent of each other. Therefore, the transmission of IEEE 802.15.4 packets is essentially a renewal process. Let X denote the transmission cycle time of a packet, which either is transmitted successfully at the i^{th} retransmission or fails to be transmitted eventually after the $M+1$ unsuccessful channel access attempts, where M is the maximum number of backoffs the CSMA-CA algorithm will attempt before declaring a channel access failure. The default M is 4 [IEE06]. Therefore, X is actually the inter-renewal time of the renewal process. Furthermore, let $\{W(t); t > 0\}$ be a renewal reward function for the renewal process with expected value of the inter-renewal time $\mathbb{E}$(X).

Thus according to [Gal96], the normalized IEEE 802.15.4 throughput S is given by

$$S = \lim_{t\to\infty} \frac{1}{t} \int_{\tau=0}^{t} W(\tau) d\tau = \frac{\mathbb{E}[W_m]}{\mathbb{E}[X]} \quad \text{with probability 1} \tag{3.17}$$

where $\mathbb{E}[W_m]$ is the expected value of the reward, which is either t_p or zero, depending on whether a packet is sent out during the m^{th} renewal interval and whether the packet is received successfully. Therefore,

$$\begin{aligned}\mathbb{E}[W_m] &= (1-p_c)\Big[\mathbb{E}[t_p] \cdot p_i \cdot \sum_{m=0}^{M} (1-p_i)^m + 0 \cdot (1-p_i)^{M+1}\Big] \\ &= (1-p_c) \cdot \mathbb{E}[t_p] \cdot p_i \cdot \sum_{m=0}^{M} (1-p_i)^m \end{aligned} \tag{3.18}$$

where $\mathbb{E}[t_p]$ is the expected t_p. We now compute $\mathbb{E}[X]$. In case of the saturated IEEE 802.15.4 traffic,

$$\begin{aligned}\mathbb{E}(X) = \sum_{m=0}^{M} \Big[p_i(1-p_i)^m \Big[\sum_{n=0}^{m} \mathbb{E}[B_n] + (m+1)CCA + 2T_{ta} + \mathbb{E}[t_p] \Big] \Big] \\ +(1-p_i)^{M+1} \Big[\sum_{n=0}^{M} \mathbb{E}[B_n] + (M+1)CCA \Big] \end{aligned} \tag{3.19}$$

where $\mathbb{E}[B_n]$ is the expected backoff time B_n for the n^{th} retransmission. By substituting Equation (3.18)(3.19) into Equation (3.17), the IEEE 802.15.4

throughput S is obtained. Note that in case of non-saturated IEEE 802.15.4 traffic, the expected inter-renewal time is different from the one computed in Equation (3.19). For example, for a traffic with a constant packet interval time $T > \mathbb{E}(X)$ in Equation (3.19), the throughput $S = \mathbb{E}[W_n]/T$.

The IEEE 802.15.4 packet loss consists of two kinds of losses: inhibition loss and collision loss. Therefore, the IEEE 802.15.4 packet loss ratio η is given by

$$\eta = \alpha + p_c \tag{3.20}$$

The expected packet delay $\mathbb{E}(t_d)$ includes only the delay between packet arrival and the start of its first transmission attempt. For those packets that fail to seize a transmission opportunity, the contribution to $\mathbb{E}(t_d)$ is set to zero, even though a retry at upper protocol layers may cause a larger delay. Thus, $\mathbb{E}(t_d)$ is computed by

$$\mathbb{E}(t_d)=\sum_{m=0}^{M} p_i \cdot (1-p_i)^m \cdot \left[\sum_{n=0}^{m} \mathbb{E}[B_n] + (m+1) \cdot CCA + T_{ta}\right] \tag{3.21}$$

3.2.2 Coexistence Performance in R2

In R2, IEEE 802.15.4 nodes can still sense IEEE 802.11b/g traffic. Therefore, p_i stays the same as in R1 and so does the inhibition loss probability α. Since IEEE 802.11b/g nodes cannot sense an IEEE 802.15.4 packet any more in R2, for avoiding an overlapping transmission, the Inequation (3.4) or (3.5) needs to be satisfied, which is almost impossible as addressed in Section 3.1. Thus, $p_c = \beta \cdot p_e$. The throughput S can also be given by Equation (3.17)(3.18)(3.19). The packet loss ratio η and the expected packet delay $\mathbb{E}(t_d)$ are give by Equation (3.20) and (3.21), respectively.

3.2.3 Coexistence Performance in R3

In R3, $p_i = 1$ and therefore the inhibition loss probability $\alpha = 0$. Thus, $p_c = p_e$. The throughput S is given by Equation (3.17) , where $\mathbb{E}(W_m) = (1-p_e) \cdot \mathbb{E}(t_p)$ and $\mathbb{E}(X) = \mathbb{E}(B_0) + CCA + 2T_{ta} + \mathbb{E}(t_p)$. The packet loss ratio $\eta = \alpha + p_c$ and the expected packet delay $\mathbb{E}(t_d) = 0$.

3.3 Coexistence Model Validation

In order to validate our enhanced analytical model in a nearly real-world environment, we carried out a number of experiments using off-the-shelf hardware. In some cases, OPNET simulation results are also provided as a reference.

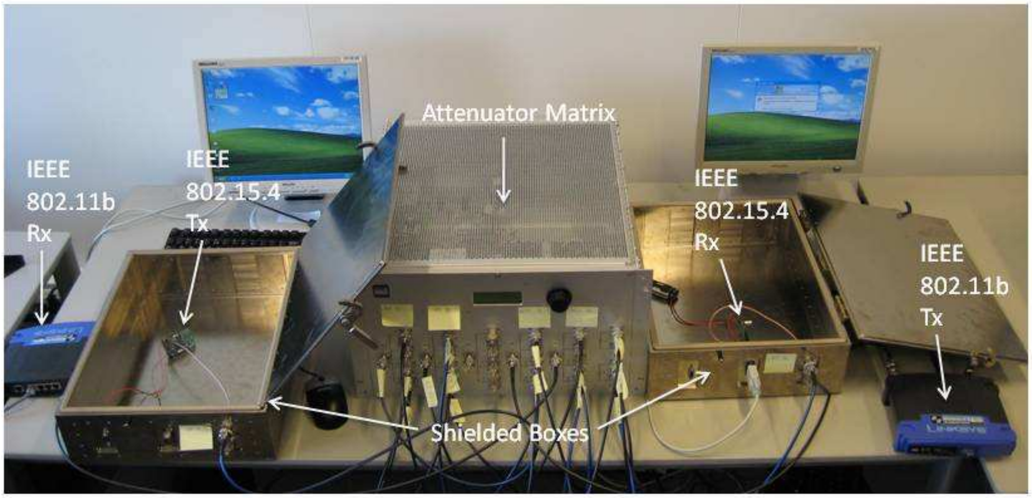


Figure 3.5: Testbed of the coexistence model of IEEE 802.11b and IEEE 802.15.4 networks

3.3.1 Experimental Testbed and Configurations

We designed and set up a compact testbed as shown in Figure 3.5, which includes the following items:

- two IEEE 802.11b nodes (Linksys WRT54G - *we used only the IEEE 802.11b mode in the experiments, but the conclusions would also applicable to the IEEE 802.11g case*): a Tx and an Rx;
- two IEEE 802.15.4 nodes (AquisGrain [Esp07]);
- two RF shielded isolation boxes;
- one attenuator matrix box;
- two PCs with testing software.

The antennas of IEEE 802.11b nodes and IEEE 802.15.4 nodes were connected by cables via the attenuator matrix, the attenuation values of which can be adjusted to emulate various physical distances in a wireless environment. To isolate from other RF interference, IEEE 802.15.4 nodes were put into the RF shielded isolation boxes such that we got a controlled RF environment, allowing the measurements to be repeatable.

A functional diagram of the testbed is depicted in Figure 3.6. The attenuation losses among those nodes are as follows,

- x_1: between IEEE 802.11b Tx and IEEE 802.15.4 Tx;
- x_2: between IEEE 802.11b Rx and IEEE 802.15.4 Tx;
- y_1: between IEEE 802.11b Tx and IEEE 802.15.4 Rx;
- y_2: between IEEE 802.11b Rx and IEEE 802.15.4 Rx.

x_1, x_2, y_1 and y_2 are adjustable, from 32 dB to 212 dB. Moreover, we set both the attenuation losses between IEEE 802.11b Tx and Rx and between IEEE 802.15.4 Tx and Rx at 70 dB, so that the two links have a very good quality, i.e., the packet loss ratio of the IEEE 802.15.4 link is close to zero

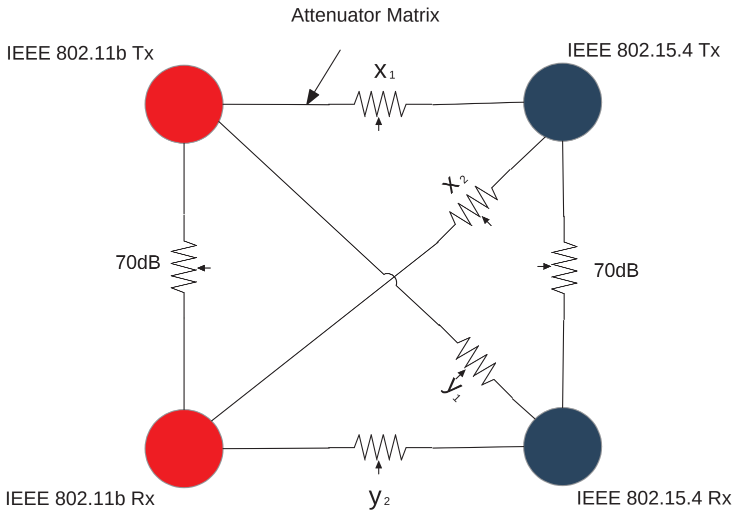


Figure 3.6: Functional diagram of the coexistence testbed

and the throughput of the IEEE 802.11b link is 6.82 Mbps, the maximum value achievable in our case given the parameter values in Table 3.1.

In the experiments, the IEEE 802.15.4 Tx constantly sends only broadcast packets and the IEEE 802.15.4 Rx does not send any packets including ACKs. The IEEE 802.11b Tx generates a saturated packet stream and the IEEE 802.11b Rx sends ACKs only. Moreover, we made the IEEE 802.11b Tx and the Rx have the same impact on the IEEE 802.15.4 Tx and on the IEEE 802.15.4 Rx, respectively. We therefore always set the same values for x_1 and x_2 , and y_1 and y_2, respectively. For the sake of brevity, we let $x = x_1 = x_2$ and $y = y_1 = y_2$. The parameter values used in the experiments are shown in Table 3.1.

Before carrying out the experiments, let us calculate R1, R2 and R3 first.

- R1: Given the IEEE 802.15.4 transmit power of 0 dBm and the IEEE 802.11b CCA threshold of -84 dBm, when $x \geq 84$ dB, the IEEE 802.11b nodes will not be able to sense the IEEE 802.15.4 nodes, i.e., R1 is the region where $x < 84$ dB.

- R3: Although the IEEE 802.11b transmit power is 17 dBm, only 16.9% falls into the 2 MHz band of IEEE 802.15.4 [Shi05], i.e., 9.3 dBm. Given the CCA threshold of -85 dBm, the IEEE 802.15.4 nodes will not be able to sense the IEEE 802.11b nodes when $x \geq 94.3$ dB, i.e., R3 is the region where $x \geq 94.3$ dB.

- R2: By definition, R2 is in between R1 and R3. Therefore, R2 is the region where 84 dB $< x <$ 94.3 dB.

3.3.2 Experimental Validation

We now carry out the experiments to identify these regions. For convenience, we start with identifying R1, followed by R3 and R2.

R1 Identification

To identify R1 and to investigate details of the coexistence behavior of IEEE 802.11b and IEEE 802.15.4 networks, we measure the IEEE 802.11b throughput and the IEEE 802.15.4 packet loss ratio in the following two cases:

- ***y = 212 dB(inhibition loss only)***: Given such a high attenuation loss, the IEEE 802.11b Tx and Rx have actually no impact on the IEEE 802.15.4 Rx but only on the Tx. Therefore, in this case, the IEEE 802.15.4 packet loss is due to not collision but only to inhibition, i.e., $p_e = 0$ and therefore $p_c = 0$ by Equation(3.14). As the IEEE 802.15.4 Rx does not send any packets including ACKs in our experiments, only the IEEE 802.15.4 Tx could affect the throughput of the IEEE 802.11b network. Thus, we can adjust only x to observe the impact of the IEEE 802.15.4 Tx on the IEEE 802.11b Tx and Rx.

As an example, in Figure 3.7, we can see that as $x = 32$ dB, the IEEE 802.11b throughput is approximately 6.54 Mbps, less than its maximum, i.e., 6.82 Mbps, which suggests that the IEEE 802.11b network is suffering, though not very seriously, from the IEEE 802.15.4 traffic.

As x increases, we expected the IEEE 802.11b throughput to increase as well because of the weakening IEEE 802.15.4 Tx impact. However, we surprisingly found in Figure 3.7 that as x increases until about 75 dB, the IEEE 802.11b throughput actually decreases, which suggests that the impact of the IEEE 802.15.4 Tx on the IEEE 802.11b network increases rather than decreases. This is confirmed by Figure 3.8, in which we can see that for 32 dB $< x <$ 80 dB, as x increases, the IEEE 802.15.4 CCA failure rate decreases, which suggests that more IEEE 802.15.4 packets were sent out indeed and the impact of the IEEE 802.15.4 Tx on the IEEE 802.11b network therefore increases. The explanation we have for this is that as x increases, the missed probability of the IEEE 802.15.4 ED increases and consequently, more often the IEEE 802.15.4 Tx senses the channel idle and sends out more packets than it should, which lowers the channel occupancy of the IEEE 802.11b traffic and thus the throughput of the IEEE 802.11b network. As addressed in [Ram07], with a high missed probability, ED is not a reliable CCA method. Especially, as the detected signal weakens, the missed probability of ED goes even higher.

In Figure 3.7, for 75 dB $< x <$ 84 dB, as x increases, which suggests that the influence from the IEEE 802.15.4 Tx is getting less. This is because the IEEE 802.11b Tx/Rx are leaving the region where they are able to sense the IEEE 802.15.4 Tx.

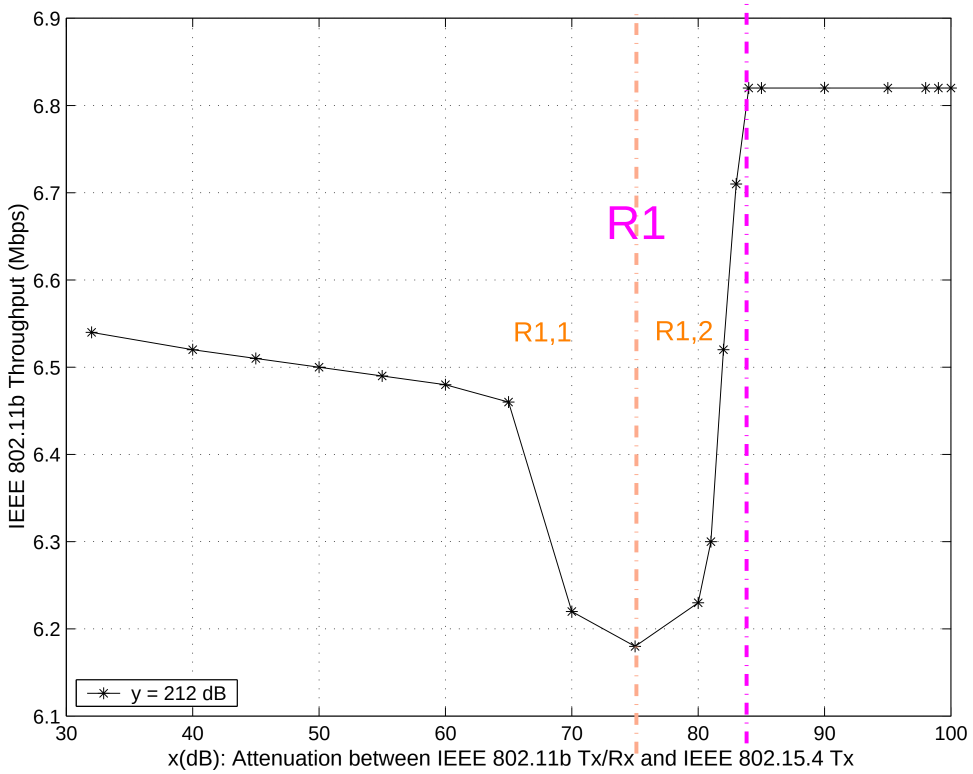


Figure 3.7: In R1: IEEE 802.11b/g nodes can also sense IEEE 802.15.4 traffic

For $x \geq 84$ dB, as x increases, the IEEE 802.11b throughput stays constant at its maximum, i.e., 6.82 Mbps, suggesting that the IEEE 802.11b Tx/Rx are not able to sense the IEEE 802.15.4 Tx and are not affected by the IEEE 802.15.4 Tx anymore. On the other hand, from the Figure 3.9 we see that in the region of $x < 84$ dB, the IEEE 802.15.4 Tx has a high packet loss ratio, which suggests it can sense IEEE 802.11b traffic there. We therefore conclude that the region where $x < 84$ dB is R1.

We may further divide R1 into two subregions as R1,1 (x < 75 dB) and R1,2 (75 dB < x < 84 dB), illustrated in Figure 3.7. R1,2 is the transition region, where the IEEE 802.11b Tx is leaving the region in which it is able to sense the IEEE 802.15.4 nodes.

Note that the curve representing the case of "inhibition loss only ($y =$ 212 dB)" in Figure 3.9 is not monotonic. We see that when $x \geq 80$ dB, there is a "hump", i.e., the IEEE 802.15.4 packet loss ratio goes up first until $x = 83$ dB and then goes down again to zero at $x = 98$ dB. The "hump" is because the IEEE 802.11b Tx and Rx are leaving R1, as shown in Figure 3.7, and therefore getting less influence from the IEEE 802.15.4 traffic, which results in more IEEE 802.11b packets sent out and therefore more IEEE 802.15.4 channel access failures. For $x \geq 83$ dB, as x increases, although more IEEE 802.11b packets are sent out, these packets cause only decreasing

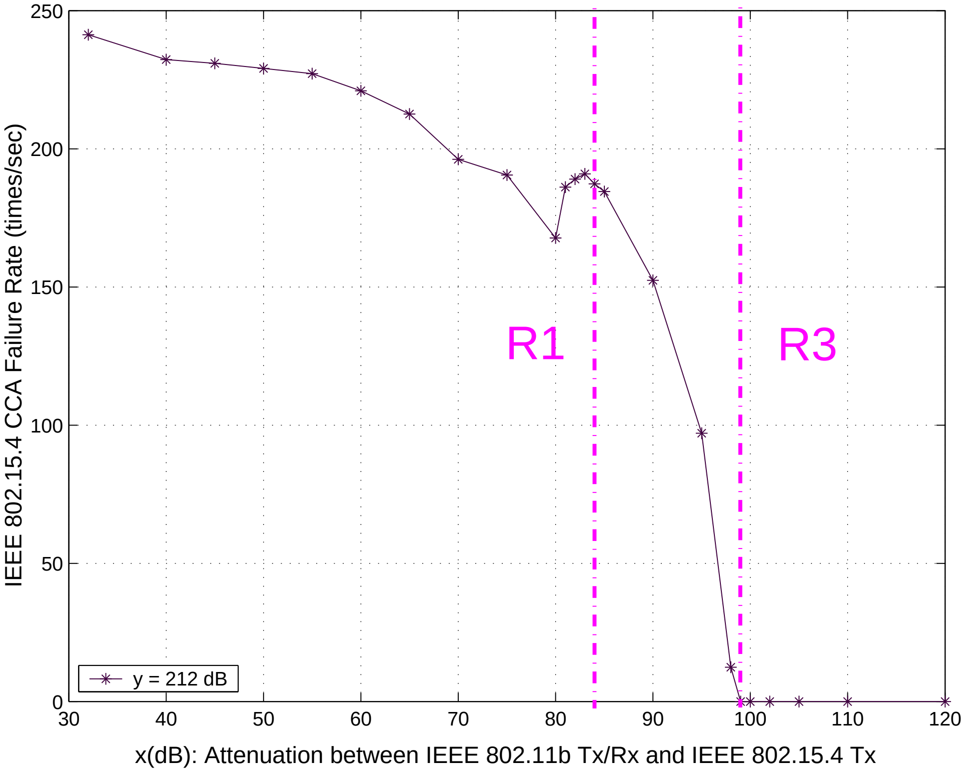


Figure 3.8: IEEE 802.15.4 Tx CCA Failure Rate

IEEE 802.15.4 channel access failures owing to their weakening power. For $x \geq 98$ dB, the IEEE 802.15.4 packet loss ratio equals zero, which means that IEEE 802.15.4 Tx cannot sense IEEE 802.11b traffic anymore and therefore does not suffer from the channel access failures. This is confirmed in Figure 3.8, where we can see that the IEEE 802.15.4 CCA failure stays zero for $x \geq$ 98 dB.

It is worthy noting that according to [Pet06][How03][Sik05], IEEE 802.15.4 WSNs has little impact on the IEEE 802.11 WLANs performance. This conclusion is true in general, but in some cases, IEEE 802.15.4 WSNs may have a non-negligible impact on the performance of IEEE 802.11b/g WLANs. For example, in Figure 3.7, we see that for 70 dB $< x <$ 80 dB, the IEEE 802.11b throughput is about 6.2 Mbps, approximately 10% less than its maximum, i.e., 6.82 Mbps. In case of weaker IEEE 802.11b links and heavier IEEE 802.15.4 traffic, the IEEE 802.11b throughput is supposed to be even lower.

In Section 3.2, we derived the packet loss ratio of IEEE 802.15.4 WSNs under IEEE 802.11b/g interference. To validate our analysis, we put the analytical results and the experimental results together in Figure 3.10, which also includes an OPNET simulation result as a reference. We can see that in case of y = 212 dB (inhibition loss only), the analytical, the OPNET simulation and the experimental results have a good match in general. Some

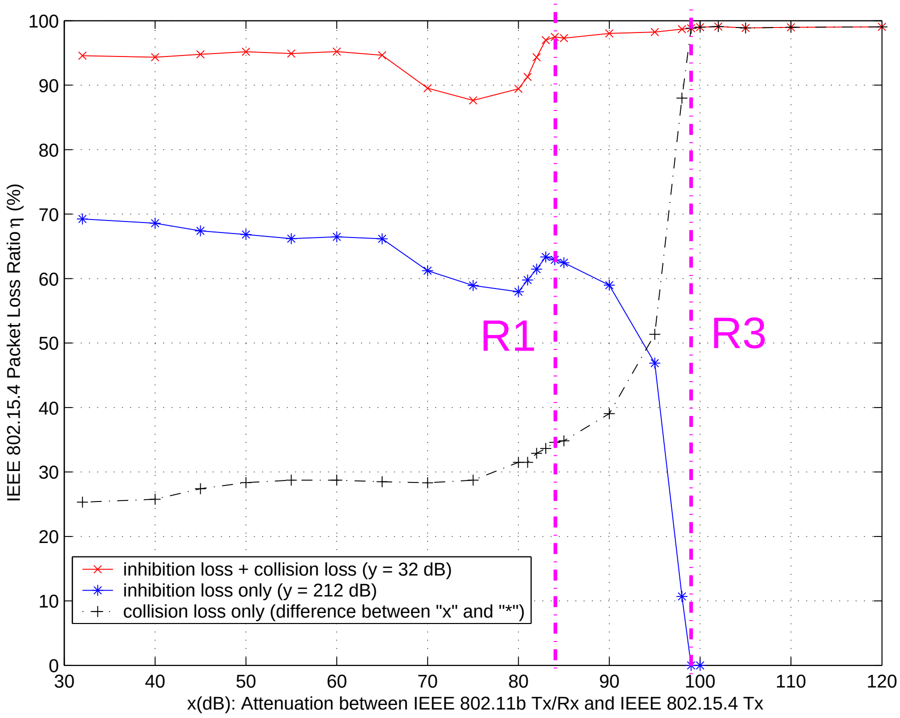


Figure 3.9: In R3: neither can sense the other, but IEEE 802.15.4 nodes could still suffer IEEE 802.11b/g interference

small mismatches in details, e.g., the 3.7 dB difference in the lower-bound of R3 between the analytical value (94.3 dB) and the experimental value (98 dB), may be attributed to the errors in the measurement and/or the hardware implementation.

Although R1 has been identified, to reveal more insights about the impact from the IEEE 802.11b traffic on the IEEE 802.15.4 network, we further measured the IEEE 802.15.4 packet loss ratio in the following case.

- ***y = 32 dB(inhibition loss + collision loss)***: In this case, the IEEE 802.11b Tx and Rx influence not only the IEEE 802.15.4 Tx but also the IEEE 802.15.4 Rx. Consequently, the IEEE 802.15.4 packet loss includes not only the inhibition loss but also the collision loss. Note that given y = 32 dB, the IEEE 802.11b Tx and Rx impact on the IEEE 802.15.4 Rx is so strong that SINR < -45 dB, which suggests $p_e = 1$ and therefore p_c depends only on p_{no} by Equation (3.14). The relationship between x and the packet loss ratio η is based on Equation (3.20), which is shown by the curve of "inhibition loss + collision loss ($y = 32$ dB)" in Figure 3.10.

Given the detailed discussion about the coexistence behavior of IEEE 802.11b and IEEE 802.15.4 networks above in R1, the identification of R3 and R2 is straightforward as follows.

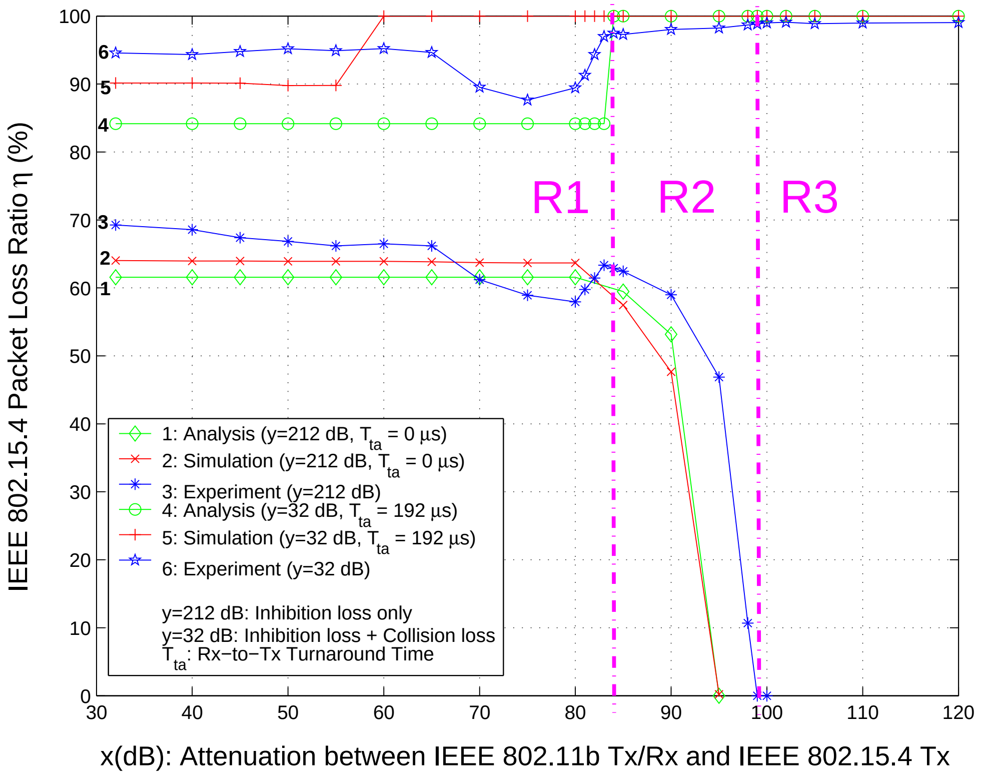


Figure 3.10: Analysis, simulation and experimental results for the performance of an IEEE 802.15.4 WSN under IEEE 802.11b/g interference

R3 Identification

From the curve of “inhibition loss only (y = 212 dB)” in Figure 3.9, we see that as $x \geq 98$ dB, the IEEE 802.15.4 packet loss ratio because of the channel access failures goes down to zero, which means that IEEE 802.15.4 Tx cannot sense IEEE 802.11b traffic and therefore does not suffer from the channel access failures anymore. This is confirmed in Figure 3.8, where we can see that the IEEE 802.15.4 CCA failure rate goes down to zero as $x \geq$ 98 dB. We therefore conclude that in the region where $x \geq 98$ dB, neither IEEE 802.15.4 nodes nor IEEE 802.11b nodes can sense the other, but IEEE 802.15.4 nodes may still suffer from the IEEE 802.11b interference, which is exactly what R3 defines. Note that we have calculated that R3 is the region where $x \geq 94.3$ dB rather than 98 dB as suggested by the experiment. The 3.7 dB difference may be attributed to the errors in the measurement and/or the hardware implementation, which has been mentioned in Section 3.3.2.

R2 Identification

For convenience, Figure 3.7 is superimposed on Figure 3.9, resulting in Figure 3.11. We can see that in the region between R1 and R3, i.e., 84 dB $< x <$ 98 dB, there is still some IEEE 802.15.4 packets loss owing to the channel access failures, which suggests in that region, IEEE 802.15.4 Tx can still sense the IEEE 802.11b Tx/Rx, while not *vice versa*. This is exactly the region which R2 defines.

Upon till now, all R1, R2 and R3 have been clearly identified and our coexistence model has been validated by the experiments.

More Discussions

In case of y = 32 dB (inhibition loss + collision loss), we can see from the experimental result shown as the curve 6 in Figure 3.10 that the IEEE 802.15.4 packet loss ratio is quite high, even in the region R1, where the IEEE 802.15.4 packet loss ratio is supposed to be low instead because in R1, IEEE 802.15.4 nodes and IEEE 802.11b nodes can hear each other and therefore their CSMA/CA mechanism should be working there. We found out that this is because in reality, an IEEE 802.15.4 node cannot send out a packet immediately after a successful CCA. Instead, the node has to take an additional time as long as an Rx-to-Tx turnaround time after the CCA to switch its transceiver state from receiving to transmitting. During this Rx-to-Tx turnaround time, however, the channel may become busy again due to the IEEE 802.11b/g traffic, which can cause a collision with a coming IEEE 802.15.4 packet. As such, the effectiveness of CCA gets impaired. Curve 4 and 5 in Figure 3.10 show the analytical and the simulative results, respectively, given an Rx-to-Tx turnaround time of 192 μs, the default value specified in the standard [IEE06]. These results are close to the experimental

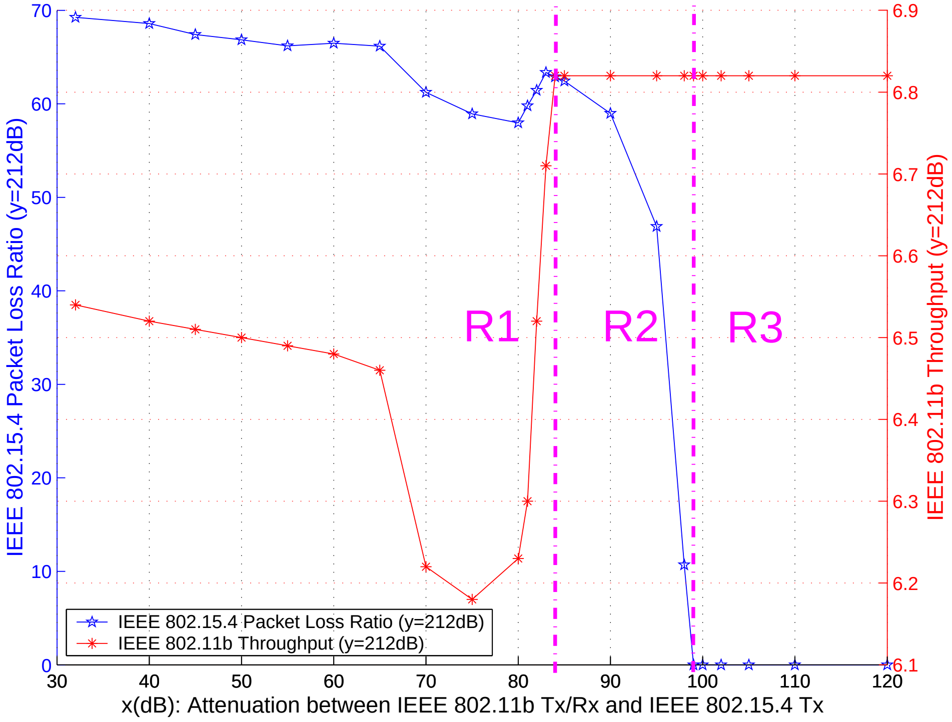


Figure 3.11: In R2: IEEE 802.15.4 nodes can sense IEEE 802.11b/g nodes, but not *vice versa*

one shown as Curve 6, which suggests the Rx-to-Tx turnaround time in the experiment is around 192 μs.

To learn that how much IEEE 802.15.4 coexistence performance could deteriorate due to a none-zero Rx-to-Tx turnaround time in reality, we compare curve 1 and curve 2 with curve 3 and curve 6, respectively, in the region R1 of Figure 3.10. Curve 1 and curve 2 show the analytical and simulative IEEE 802.15.4 packet loss ratios, respectively, in case of a zero Rx-to-Tx turnaround time, while Curve 3 and curve 6 show the experimental IEEE 802.15.4 packet loss ratios in case of around 192 μs Rx-to-Tx turnaround time. We first compare curve 1 and curve 2 to curve 3, all of which happen in case of no collision loss. We take the case of x = 40 dB for instance and see the IEEE 802.15.4 packet loss ratios in curve 1 and curve 2 are approximately 5 - 7 % less than that in curve 3. Furthermore, comparing curve 1 and curve 2 to curve 6, where there is collision loss, we still take the case of x = 40 dB for instance and see the IEEE 802.15.4 packet loss ratios in curve 1 and curve 2 are approximately 30 - 35 % less than that in curve 6. Therefore, in reality, an Rx-to-Tx turnaround time can lead to a significant decline in IEEE 802.15.4 coexistence performance, especially when collision loss exists.

Moreover, the CCA partial detection effect addressed in Section 3.1 can also be observed in Figure 3.10. In case of y = 212 dB, taking curve 3 for example, we see that in R2, curve 3 shows an “arc” rather than a “1-0” type of right-angle, which exactly reflects the CCA partial detection effect.

3.3.3 Simulation Results

In Section 3.3, the coexistence performance metrics of IEEE 802.15.4 WSNs under IEEE 802.11b/g interference are given by Equation (3.17), (3.20) and (3.21), respectively. Among those metrics, the analytical packet loss ratio performance has been evaluated by the simulation and the experiments as shown in Figure 3.10 where our analysis, simulation and experimental results have a good match. To evaluate our analysis of the other two performance metrics, i.e., throughput and the expected packet delay, we are using only the OPNET simulation both because these two metrics are not able to be achieved directly from our experiment implementation and because the simulation results have proved to have a good match with the experimental ones in Section 3.3.2.

Furthermore, we investigate the IEEE 802.15.4 coexistence performance in all the three coexistence regions. We therefore set the attenuation losses between an IEEE 802.11b Tx/Rx and an IEEE 802.15.4 Tx are 50 dB (R1), 70 dB (R1), 90 dB (R2) and 100 dB (R3), respectively. For getting good links as assumed in Section 3.3.1, we put the IEEE 802.11b Tx and Rx 1 meter away from each other, and 0.1 meter in between the IEEE 802.15.4 Tx and Rx. Besides, as always assumed in this work, the IEEE 802.11b traffic intensity is set as saturated. And the IEEE 802.15.4 traffic intensity is set in two modes: saturated and constant transmission with 50 ms packet interval time, respectively. The rest of simulation parameters are shown in Table 3.1. As shown in Figure 3.12 and Figure 3.13, in general, the analytical results have a good match with the simulation ones in all three regions and in both IEEE 802.15.4 transmission modes, which suggests our performance analysis in Section 3.2 is reasonably accurate.

3.4 Conclusions

In this chapter, we studied the coexistence performance of IEEE 802.15.4 WSNs under IEEE 802.11b/g interference. By well-designed experiments, our work confirmed that IEEE 802.15.4 WSNs can suffer from heavy IEEE 802.11b/g interference if the channel is not allocated properly. Moreover, we revealed two important implementation factors, i.e., IEEE 802.15.4 Rx-to-Tx turnaround time and CCA partial detection effect, which can have significant impact on IEEE 802.15.4 WSNs coexistence performance in reality, e.g., a long IEEE 802.15.4 Rx-to-Tx turnaround time can impair the CCA performance and therefore the IEEE 802.15.4 WSNs coexistence performance. Taking these implementation factors into account, we improve the analytical coexistence model that we proposed in the previous chapter. The

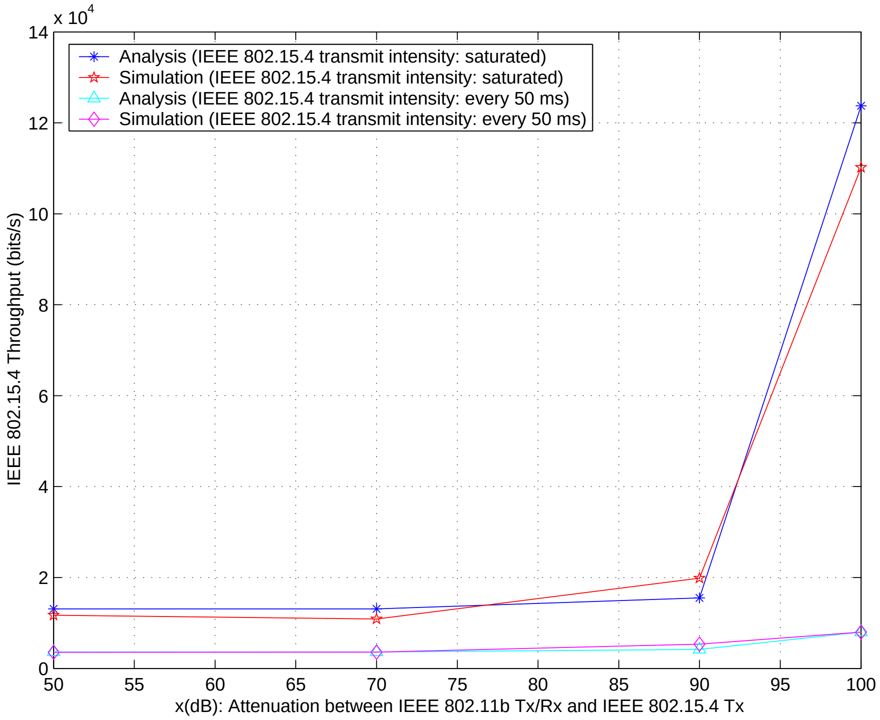


Figure 3.12: IEEE 802.15.4 Throughput in Three Coexistence Regions

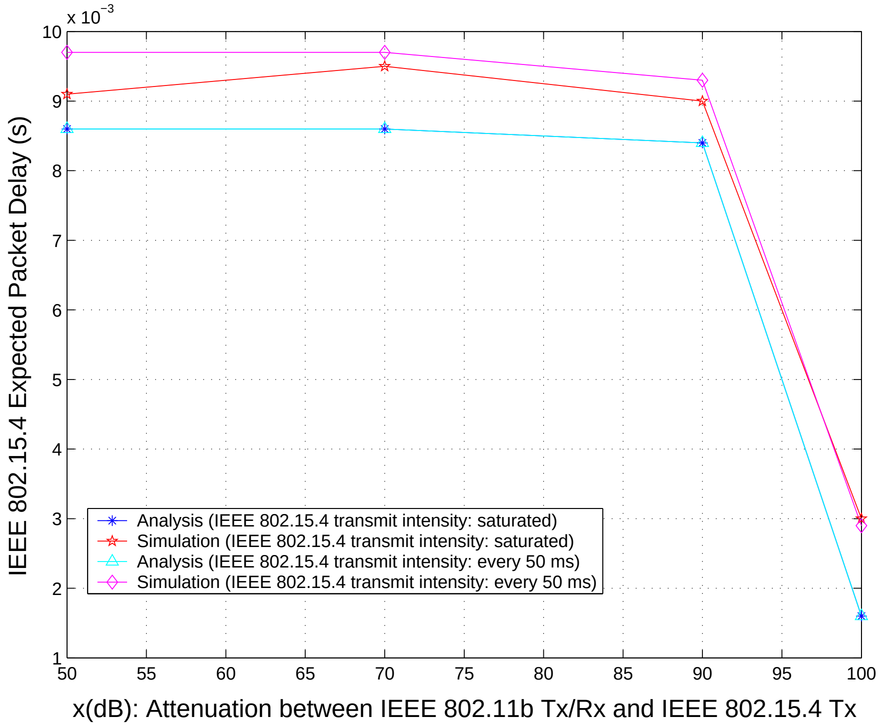


Figure 3.13: IEEE 802.15.4 Expected Packet Delay Three Coexistence Regions

enhanced model can precisely explain and predict the IEEE 802.15.4 WSNs coexistence performance. Furthermore, under the guidance of the model, the IEEE 802.15.4 WSNs coexistence performance are extensively investigated in all of the three coexistence regions in different scenarios by analysis, simulation and experiments. The simulation and experimental results agree with our analysis. Integrating many insights into the coexistence issue, the model can be helpful in resolving the coexistence issue. We then present two solutions to the coexistence issue in the following two chapters.

Chapter 4

Interference Mitigation

It is a terrible phenomenon, whose laws we must study, and to whose conditions we must submit, if we would mitigate it.

- Sheridan Le Fanu

In the previous two chapters, we have fulfilled one of the thesis targets stated in Section 1.4, i.e., to achieve a clear understanding of the coexistence issue between IEEE 802.15.4/ZigBee WSNs and IEEE 802.11b/g WLANs, by analysis, simulation and experiments. Based on this, we explore the means to help IEEE 802.15.4 WSNs deal with interference. Basically, there are two categories for the way to deal with interference: interference control or mitigation and interference avoidance. In the following two chapters, we are addressing solutions in each of these two categories. In this chapter, we propose an approach to interference mitigation. This approach may significantly enhance the robustness of IEEE 802.15.4 WSNs in the presence of heavy interference (in particular IEEE 802.11b/g interference). The approach is robust, responsive and can be implemented easily at a low cost. The remainder of the chapter is organized as follows: Section 4.1 introduces some related work on the coexistence solutions. Section 4.2 presents our adaptive Clear Channel Assessment (CCA) algorithm for IEEE 802.15.4 WSNs to mitigate interference. Simulation results are given in Section 4.3. Section 4.4 concludes the chapter and proposes some future research.

4.1 Related Work

As mentioned above, there are essentially two categories for the way to deal with interference, i.e., interference avoidance and interference control or mitigation. In this section, we give a brief introduction to typical approaches in these two categories.

Table 4.1: Time Agility Algorithm [Jin05]

```
**if** $SINR >> 12dB$ **then** transmit at probability 1
**if** $SINR >\approx 12dB$ **then** transmit probability is proportional to
the inverse of interference power
**if** $SINR < 12dB$ **then** transmit probability is proportional to SINR.
$Prob_{tx} = max\{0, SINR/max\{SINR\}\}$
```

4.1.1 Interference Avoidance

Time Agility

An interference avoidance scheme, called Time Agility (TA), is investigated in [Jin05], where TA enables spectrum coexistence between short-range IEEE 802.11b (Wi-Fi) and long range IEEE 802.16a (Wi-Max) radios. The basic idea is to allow 802.16a and 802.11b devices to adapt to each other's traffic pattern and the time varying channel conditions. To avoid transmissions (and thus potential re-transmissions) during poor channel conditions, the transmit probability is decreased when interference power increases, thus avoiding severe interference scenarios. The algorithm is described in Table 4.1. Note that the SINR threshold of 12 dB is used to decide on interference avoiding action.

In the TA algorithm, an SINR close to the threshold may indicate potential close interferers around, and to avoid interference with the potential interferers, the transmit probability is made inversely proportional to the sensed interference power. When the SINR is less than the threshold, the radio can infer that either the signal strength is too weak, or that the interference power is too strong, or both. Thus it is preferable to control the transmit probability to be proportional to current SINR value to avoid mutual interference.

In the sense of traffic engineering, when the traffic pattern is easy to learn (e.g., Pareto ON/OFF traffic model [Ahl03] with relatively long OFF periods), this algorithm can help radios to adapt to each other's traffic pattern and effectively utilize the available degree of freedom in time. It is accomplished by transmitting when the interferer's traffic load is low (or off), and avoids transmitting when the interferer's traffic load is high. This algorithm is traffic-type-independent, and the difference is in the degree of difficulty in adapting to the specific traffic pattern. For example, Pareto ON/OFF is easier to adapt to than CBR traffic with the same load, due to the extended OFF period. When implementing this algorithm, a piggybacking scheme is also used to embed the transmit probability in the packet header, which is calculated by the receiver and sent to the transmitter. However, in case of severe interference, the piggybacking scheme is not reliable at all.

Besides, from our studies described in the previous chapters, we have learnt that due to the low power and the long timing in its MAC mechanism, IEEE 802.15.4 nodes suffer unfairness in competing with IEEE 802.11b/g nodes in the medium access. In case of the coexistence of IEEE 802.15.4 nodes and IEEE 802.11b/g nodes, since the TA scheme makes the transmit probability decrease when interference power increases, it would cause IEEE 802.15.4 nodes to suffer more severe unfairness.

Dynamic Frequency Selection (DFS)

There is another typical interference avoidance scheme called dynamic frequency selection. Normally, a wireless system operates on a frequency band, which is divided into multiple channels. The wireless system may dynamically select an operational channel so as to dynamically avoid harmful interference from other wireless systems sharing the same frequency band. This scheme for dynamically selecting one of the possible channels within the band is referred to as Dynamic Frequency Selection (DFS).

An adaptive DFS scheme using multiple radios has been proposed in [Won05]. The scheme uses three mechanisms: Interference Detection, Group Formation, and Demolition. Each 802.15.4 node checks for interference on the current channel using the Interference Detection (ID). It can be called periodically or on demand. In case of interference, the node enters into Group Formation (GF). During GF, the nodes in the same interference area form a group and a new channel is selected as the current channel for the group. When the current interference is diminished, the group is torn down and its current channel is switched back to the previous one.

This scheme is centralized, which requires a reliable communication between devices, even in spite of heavy interference happening on the communication channel. This is not robust to the extreme interference which we deal with.

To minimize the impact of the 802.11 interference, some distributed and adaptive frequency channel selection algorithms for IEEE 802.15.4 nodes are proposed in [Pol06]. However, the algorithms are based on either increased spectrum scanning, resulting in much more energy consumption and additional hardware requirements, or increased learning, requiring sophisticated algorithms as function of the environment and its dynamic behavior.

In Chapter 5, we propose a distributed adaptive multi-channel interference-avoidance scheme, which enables a conventional single-channel IEEE 802.15.4 network to distributedly, adaptively and partially change the operational channel in the presence of local interference. As a result, the IEEE 802.15.4 network performance under interference can be significantly improved in an efficient way.

4.1.2 Interference Control/Mitigation

Transmit Power Control (TPC)

Traditional approaches for the coexistence of wireless devices focus on transmit power control (TPC). The idea of TPC is that each device transmits only the minimum power necessary to maintain communications. This would help in minimising interference into other existing services and facilitate frequency reuse between devices. For instance in [Sah04], the allowable transmit power is determined in order to guarantee a protected radius to primary users that should not be interfered with. This is especially useful to enable spectrum sharing between systems with different levels of regulatory status, e.g., primary and secondary users, but does not fit the coexistence situation of systems with equal regulatory status, e.g., IEEE 802.15.4 WSNs and IEEE 802.11b/g WLANs.

In [Zha06], a transmit power control algorithm, i.e., Goodput-oriented Utility-based Transmit Power Control (GUTPC), is proposed for mitigating interference caused by coexistence of heterogeneous Ultra-Wide Band (UWB) systems. The idea is to improve the performance of the coexisting systems fairly by maximizing their net utilities, where the gain is the goodput achieved, while the cost is the power used and the signal-to-interference-and -noise ratio (SINR) observed. This method fits coexisting systems which have comparable adjustable transmit power scopes, rather than the coexisting IEEE 802.15.4 WSNs and IEEE 802.11b/g WLANs, whose adjustable transmit power scopes are substantially different. Hence, it is not a good solution for the scenarios we are considering.

Transmit Interval Control (TIC)

Another category of solutions focus on Transmit Interval Control (TIC). In [Zho09], a hub-assisted WLAN/Zigbee coexistence method is proposed. The hub, i.e., a special ZigBee coordinator which integrates both functions of IEEE 802.11b and ZigBee is designed. It is capable of controlling the transmit interval of 802.11b interferer by generating periodic "fake IEEE 802.11b CTS (Clear To Send)" frames to silence 802.11b traffic and thus reserve the channel for ZigBee transmission. This method is useful in some cases, but it may degrade the IEEE 802.11b performance dramatically even in case of no pending ZigBee transmission. Besides, fake CTS frames sent by the hub need to be able to cover all the potential IEEE 802.11b interferers, which may, on the one hand, not be guaranteed and on the other hand, make the exposed node problem more serious for the coexisting IEEE 802.11b and ZigBee networks. Hence, it is not a good solution for the scenarios we are considering.

In the following section, we will present a decentralized approach to help IEEE 802.15.4 nodes mitigate interference. The approach is robust, responsive and easy to be implemented at a low cost.

4.2 Adaptive CCA Algorithm

In the presence of heavy interference, two types of IEEE 802.15.4 packet loss are identified in [Yua09], i.e., **inhibition loss** and **collision loss**. The inhibition loss is due to channel access failures, i.e., an IEEE 802.15.4 packet shall be discarded after $M+1$ times channel access failures, where M is the maximum number of backoffs the CSMA-CA algorithm will attempt before declaring a channel access failure. The collision loss is due to collisions with interfering frames.

Referring to Figure 2.4, in R1, heavy IEEE 802.11b/g interference can cause a high inhibition loss but little collision loss to IEEE 802.15.4 WSNs if the CSMA/CA works well. In R2, besides causing the inhibition loss, IEEE 802.11b/g interference could cause collision loss to some extent depending on Signal to Interference plus Noise Ratio (SINR). In R3, IEEE 802.11b/g interference could cause only collision loss. As R1 could cover as much as 35m, the inhibition loss accounts for a major part of the total loss, especially for an indoor environment. Even for the further region, R2, the inhibition loss could also account for a major part of the total loss in case of good IEEE 802.15.4 links (e.g., SINR> 5-6 dB, an IEEE 802.15.4 packet could be successfully received with a probability of 99% [IEE06]). In addition, a high inhibition loss suggests that for transmitting a single packet, an IEEE 802.15.4 node needs to perform CCA many times in general, which results in a high power consumption for the IEEE 802.15.4 node. Therefore, reducing the inhibition loss can not only improve the performance but also save energy for IEEE 802.15.4 WSNs in the presence of heavy IEEE 802.11b/g interference.

We now present such an approach to reduce the inhibition loss to an acceptably low level by adaptively and distributively adjusting ED thresholds of IEEE 802.15.4 nodes.

The following notations will be used in our adaptive CCA algorithm, which is described in Algorithm 1:

- γ: instant ED threshold
- γ_0: initial ED threshold
- Γ_{max}: maximum allowable ED threshold
- K: maximum number of channel access attempts before declaring a channel access failure
- M: total number of channel access failures
- N: total number of the channel access attempts
- ζ: channel access failure ratio, defined as $\zeta = M/N$
- ζ_{max}: maximum acceptable channel access failure ratio
- ζ_{min}: minimum allowable channel access failure ratio
- η: packet inhibition loss proportion, defined as $\eta = \zeta^{K+1}$

- η_{max}: maximum acceptable packet inhibition loss proportion
- η_{min}: minimum allowable packet inhibition loss proportion
- δ_i: step-up size to adjust the ED threshold, γ
- δ_d: step-down size to adjust the ED threshold, γ

Given a η_{max} and a η_{min}, we can correspondingly derive a ζ_{max} and a ζ_{min}, respectively, by

$$\eta = \zeta^{K+1} \tag{4.1}$$

Algorithm 1 Pseudo-code for Adaptive CCA Algorithm

```
if $\zeta > \zeta_{max}$ then
    if $(\gamma + \delta_i) < \Gamma_{max}$ then
        $\gamma = \gamma + \delta_i$
    end if
    if $(\gamma + \delta_i) \geqq \Gamma_{max}$ then
        $\gamma = \Gamma_{max}$
    end if
end if
if $\zeta < \zeta_{min}$ then
    if $(\gamma - \delta_d) > \gamma_0$ then
        $\gamma = \gamma - \delta_d$
    end if
    if $(\gamma - \delta_d) \leqq \gamma_0$ then
        $\gamma = \gamma_0$
    end if
end if
```

As such, when an IEEE 802.15.4 WSN encounters heavy interference, the nodes will distributively reduce their inhibition losses by increasing their ED thresholds, and when the interference disappears, the nodes will decrease their ED thresholds back to the initial values so as to avoid having a permanent channel access privilege over their peers.

Since only simple additive and subtractive operations are involved, the algorithm is easy to be implemented at a marginal cost. In the next section, we will validate the algorithm by OPNET simulation.

4.3 Simulation Results

In this section, we will validate the algorithm by OPNET simulation in the region R1 and R2 2.1, respectively. Furthermore, we will check if the algorithm is responsive and robust.

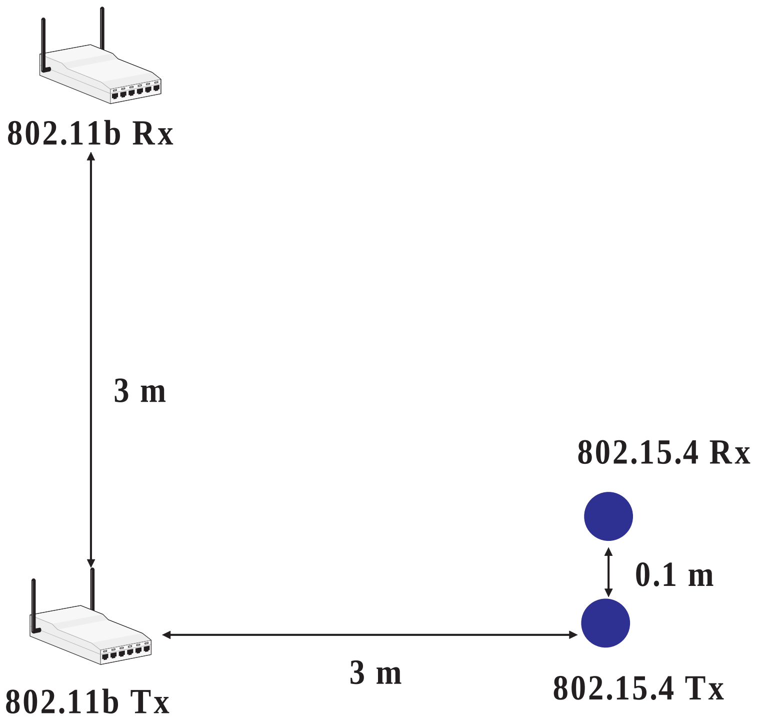


Figure 4.1: 802.11b interferers and 802.15.4 WSN are in R1

4.3.1 Simulation in Region R1

We first consider a simple scenario where there are only one pair of IEEE 802.15.4 nodes and one pair of IEEE 802.11b nodes in the region R1. As shown in Figure 4.1, for each pair, one node is a transmitter, Tx, and the other is a receiver, Rx. The physical channel condition is assumed ideal, i.e., no packet error occurs. Therefore, the IEEE 802.11b Tx can always receive ACKs after transmitting data packets, keeping its contention window at the initial value. There are 3m between the IEEE 802.11b Tx and the Rx, 0.1m between the IEEE 802.15.4 Tx and the Rx, and 3m between the IEEE 802.11b Tx and the IEEE 802.15.4 Tx. Given the parameter values in Table 4.2, these distances can guarantee that the IEEE 802.11b nodes and the IEEE 802.15.4 nodes are in the region R1, i.e., they can hear each other, and therefore the packet loss of IEEE 802.15.4 nodes is due only to the inhibition loss.

According to the frequency agility function described in the ZigBee standard [Zig07c], a node shall report to a network manager when its transmission failure exceeds 25%. In our simulation, we therefore choose $\eta_{max} = 25\%$ for an instance. (Certainly, η_{max} can be chosen as other values based on different situations. We will have a further discussion on this in Section 4.4.) Correspondingly, $\zeta_{max} = 0.758$ by Equation (4.1) given K = 4, the default value. Furthermore, we choose a $\eta = 3\%$ for example and get a corresponding

Table 4.2: IEEE 802.15.4 and IEEE 802.11b Simulation Parameters

Parameters	**IEEE 802.15.4**	**IEEE 802.11b**
Transmit power	0 dBm	17 dBm
Receiver sensitivity	-85 dBm	-76 dBm
Data rate	250 kbps	11 Mbps
ED default threshold	-85 dBm	-84 dBm
Center frequency	2410 MHz	2412 MHz
Payload size	30 bytes	1500 bytes
ACK	No	Yes
Transmit pattern	Every 30 ms	Saturated, UDP

$\zeta_{min} = 0.496$. Finally, we set the step size $\delta_i = \delta_d = 1$ dB. The simulation runs five times in each case of using adaptive CCA and NOT using adaptive CCA, respectively. For each time, the simulation runs 360 seconds, among which the IEEE 802.15.4 Tx starts to send packets at the 15^{th} second to make certain that the IEEE 802.15.4 network has been established before. The IEEE 802.11b Tx starts saturated User Datagram Protocol (UDP) traffic at the 120^{th} second and does not stop until the simulation ends. Other simulation parameters are shown in Table 4.2. The transmit powers of 0 dBm and 17 dBm are typical values for IEEE 802.15.4 devices and IEEE 802.11b devices, respectively. The chosen values of receiver sensitivity and ED threshold are default ones given in the IEEE 802.15.4 [IEE06] and IEEE 802.11b [IEE99b] standards. The date rates of 250 kbps and 11 Mbps are also typical values for IEEE 802.15.4 devices and IEEE 802.11b devices, respectively. To show the worst case of coexistence, we choose operational channels with the closest center frequencies. The payload size of 30 bytes and 1500 bytes are typical values in control applications for IEEE 802.15.4 devices, and in data transfer applications for IEEE 802.11b devices, respectively. To observe the impact from interference on IEEE 802.15.4 data transfer, we choose not to use ACK for IEEE 802.15.4 devices, while using ACK is mandatory as defined in the IEEE 802.11b standard [IEE99b]. In case of using ACK, IEEE 802.15.4 coexistence performance will become worse since when an ACK is not received due to interference, a retransmission has to occur. To show the worst case of interference, we make a saturated UDP IEEE 802.11b data stream, which means there is always an IEEE 802.11b packet ready to transmit. We also introduce an intensive IEEE 802.15.4 traffic, where the transmission interval is fixed as 30 ms. The intensive traffic helps to show a more visible interference effect and an improved result due to our proposed solution.

Simulation results on the IEEE 802.15.4 WSN are shown in Figure 4.2. In case of not using adaptive CCA, as IEEE 802.11b interference does not start, the IEEE 802.15.4 WSN throughput, TP, stays at 8000 b/s, whereas it drops down dramatically to 3700 b/s on average, only 46.25% of 8000 b/s, as the

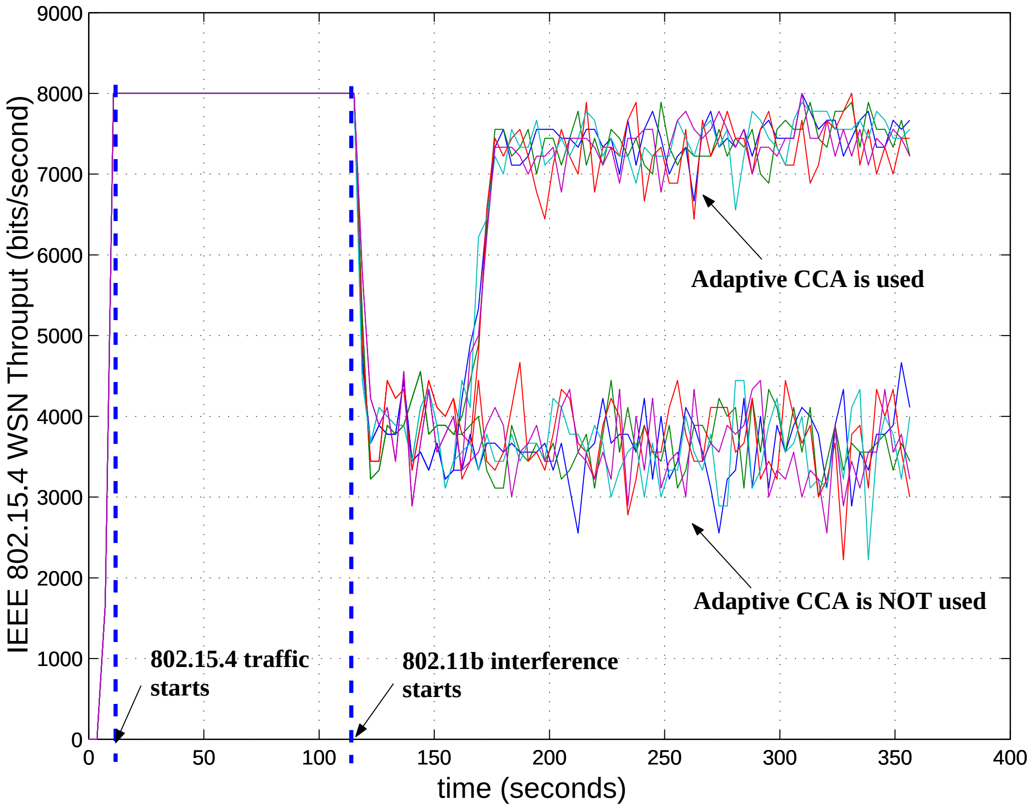


Figure 4.2: Adaptive CCA for 802.15.4 WSN to mitigate 802.11b/g interference in R1

IEEE 802.11b interference appears. In case of using adaptive CCA, however, *TP* drops down to about 3700 b/s first, but after a short time, as the Tx ED threshold is increased from the default -85 dBm to -45 dBm, *TP* goes up to around 7400 b/s on average, i.e., 92.5% of 8000 b/s. This shows that our adaptive CCA approach can significantly improve the IEEE 802.15.4 WSN throughput performance under heavy IEEE 802.11b interference by 46.25%, i.e., 100% performance increment, in this case. Besides, as the approach is purely distributive while not requiring communication among IEEE 802.15.4 devices, it is therefore robust even in the presence of heavy interference which is the case we are addressing here. Moreover, the approach can be responsive, depending on the scale of the adjustment step sizes, i.e., δ_i and δ_d. In the case shown in Figure 4.2, we see that the 802.11b interference starts at the 120th second and the IEEE 802.15.4 TP goes up to around 7400 b/s at around the 170th second. That is, it takes 50 seconds for the approach to get the IEEE 802.15.4 TP performance improved, which can be regarded as responsive if we consider applications such as environment monitoring. Plus the improvement time can be shortened further by choosing bigger step sizes.

Figure 4.3 shows the IEEE 802.15.4 WSN's impacts on the IEEE 802.11b WLAN in the region R1. The throughput values are averaged our five simu-

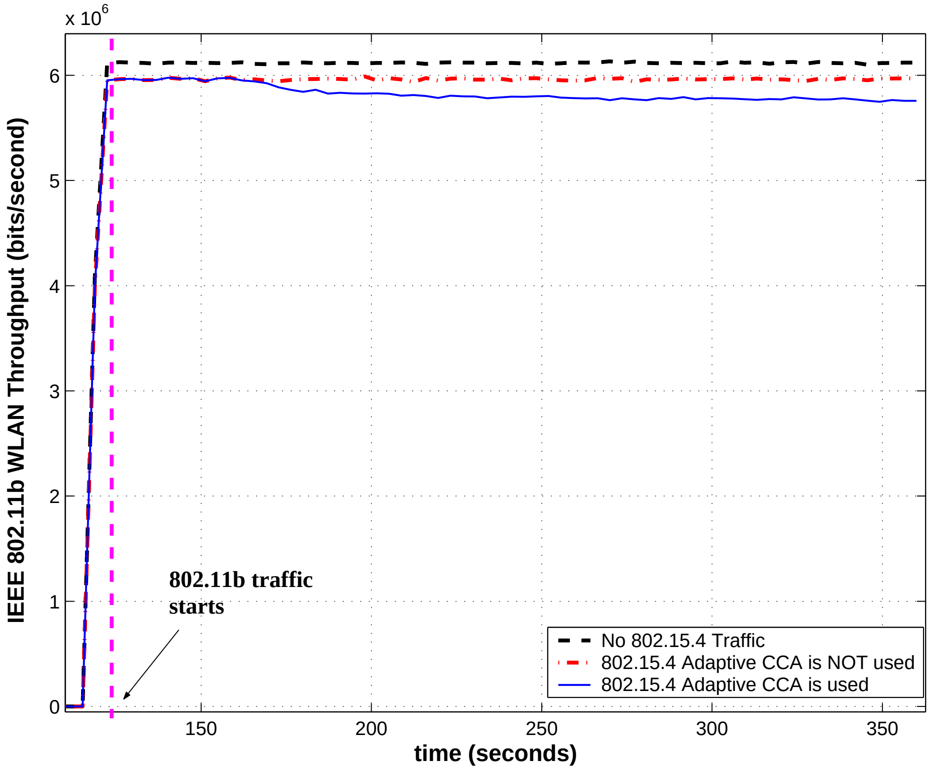


Figure 4.3: 802.11b WLAN throughput in R1

lation runs. The curve for the case of No 802.15.4 Traffic is shown to give a benchmark of the maximum IEEE 802.11b WLAN throughput achievable in this case, i.e., about 6.2 Mb/s, as there is not any IEEE 802.15.4 traffic. The curve for the case of 802.15.4 Adaptive CCA is NOT used shows the IEEE 802.11b WLAN throughput as the IEEE 802.15.4 traffic is ongoing but the adaptive CCA mechanism is not used. The throughput is approximately 5.95 Mb/s, which is 4.03% lower than the maximum value. The curve of “802.15.4 Adaptive CCA is used” shows the IEEE 802.11b WLAN throughput as the IEEE 802.15.4 traffic is ongoing and the adaptive CCA mechanism is used. The throughput is approximately 5.75 Mb/s, 3.36% lower than the one in the case that the adaptive CCA mechanism is not used. This result is reasonable because the adaptive CCA adjustment gives the IEEE 802.15.4 Tx more chances to access the channel and then send packets, which reduces the IEEE 802.11b WLAN's throughput. A further reduction in the IEEE 802.11b throughput can be expected as the IEEE 802.15.4 traffic is more intensive, but in case of the typical $< 1\%$ low duty-cycle operations of IEEE 802.15.4 WSNs [Gut03] such as lighting control, the impact of IEEE 802.15.4 traffic on IEEE 802.11b WLAN performance would be limited.

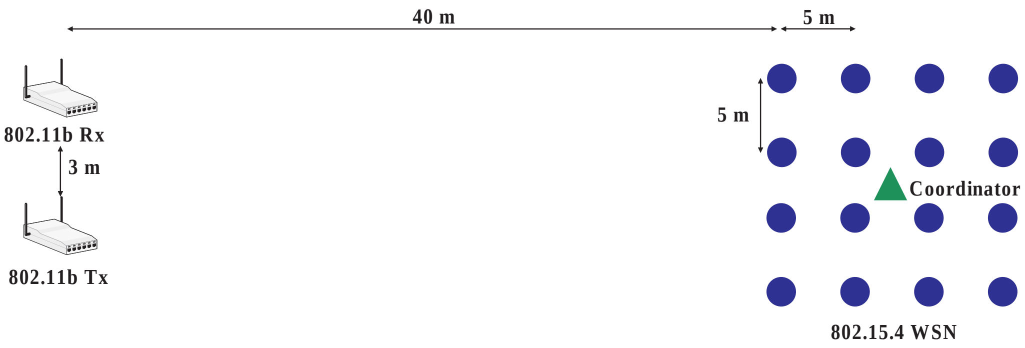


Figure 4.4: 802.11b interferers and 802.15.4 WSN are in R2

4.3.2 Simulation in Region R2

Next, we consider another scenario, where an IEEE 802.15.4 WSN and the same pair of IEEE 802.11b nodes in the last scenario are in the region R2, i.e., the IEEE 802.15.4 nodes can hear the IEEE 802.11b traffic but not *vice versa*. The IEEE 802.15.4 WSN has 16 nodes deployed in a square array with a coordinator in the center, as shown in Figure 4.4. There are 5m between two neighboring nodes. A pair of IEEE 802.11b nodes are 40m away from the WSN. Given the parameter values in Table 4.2, the distances above guarantee that the IEEE 802.11b nodes and the IEEE 802.15.4 nodes are in the region R2 and the packet loss of IEEE 802.15.4 nodes is due to the inhibition loss only. Each IEEE 802.15.4 node sends packets to randomly chosen destination nodes in a poisson packet generation mode every 50 ms on average. Adaptive CCA is used and the adaptive CCA step size $\delta_i = \delta_d = 1$ dB. There is 3m distance between the pair of IEEE 802.11b nodes. The IEEE 802.11b traffic is saturated, starts at 100^{th} second and ends at 400^{th} second. The simulation runs for 1200 seconds.

Simulation results are shown in Figure 4.5. We see that before the IEEE 802.11b traffic starts, the IEEE 802.15.4 WSN throughput TP is around 32 kb/s and the global average ED threshold, $\overline{\gamma}$, of the IEEE 802.15.4 WSN, stays at the default value of -85 dB. When the IEEE 802.11b traffic starts at t = 100 s, TP drops down dramatically to 22 kb/s. At the moment, $\overline{\gamma}$ starts to increase. After a short time, as $\overline{\gamma}$ reaches around 81.7 dB, TP increases to around 27 kb/s, i.e., 22.7% increment. Note that compared to the 100% increment in the last case, the 22.7% increment looks not much. This is because in the region R2, the IEEE 802.11b Tx cannot sense the traffic of the IEEE 802.15.4 WSN, making the situation for the IEEE 802.15.4 WSN even worse than in the region R1 [Yua07].

As the IEEE 802.11b traffic ends at t = 400 s, we see that $\overline{\gamma}$ starts to decline, while TP goes back to the initial level, i.e., around 32 kb/s. As the time goes, $\overline{\gamma}$ would eventually return to the default value of -85 dB so as to avoid having a permanent channel access privilege. However, the return rate

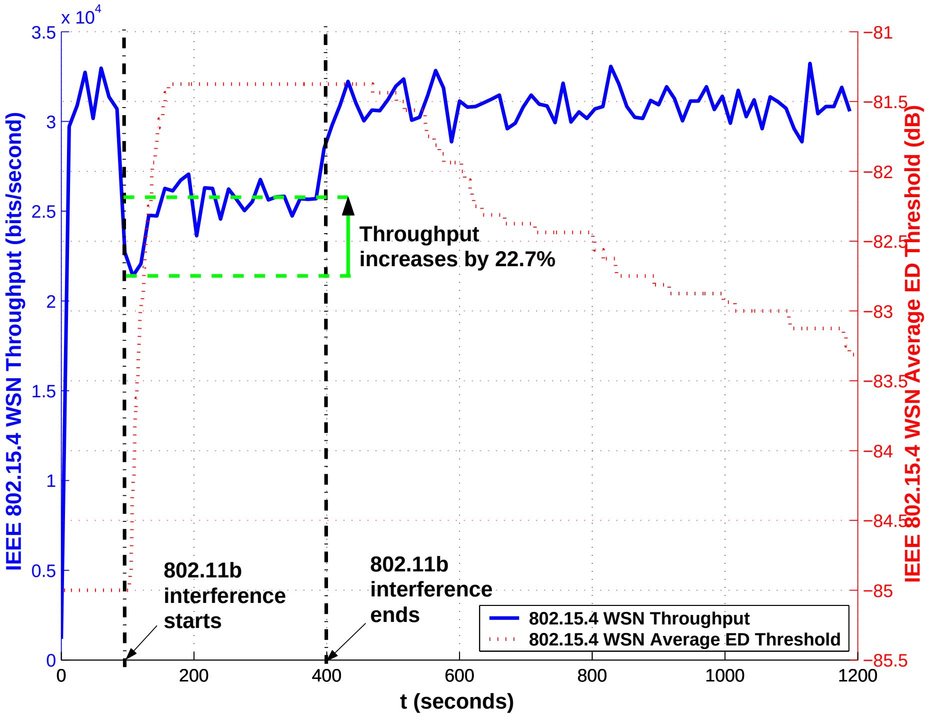


Figure 4.5: Adaptive CCA for 802.15.4 WSN to Mitigate Interference in R2

of $\overline{\gamma}$ is low due to the small step-down size δ_d of 1 dB. We expect a larger δ_d would help. In Figure 4.6, the simulation results are shown in case of $\delta_d =$ 1 dB, 3 dB and 5 dB, respectively. We see that with a larger δ_d, the return rate of $\overline{\gamma}$ is improved indeed. Besides, Figure 4.7 shows the IEEE 802.15.4 WSN's impact on the IEEE 802.11b WLAN in the region R2. As expected, the IEEE 802.11b WLAN throughput is not tangibly affected by the traffic of the IEEE 802.15.4 WSN as the IEEE 802.11b Tx is not able to sense the IEEE 802.15.4 traffic in R2 and therefore can transmit freely.

4.3.3 Simulation Summary

To sum up, the simulation results above validate that our adaptive CCA approach can significantly improve the robustness and therefore the performance of IEEE 802.15.4 WSNs in the presence of heavy interference. Note that although the interference in the simulations are from the IEEE 802.11b nodes, the adaptive CCA approach can actually work under any other type of interference as long as it causes the inhibition packet loss of IEEE 802.15.4 WSNs.

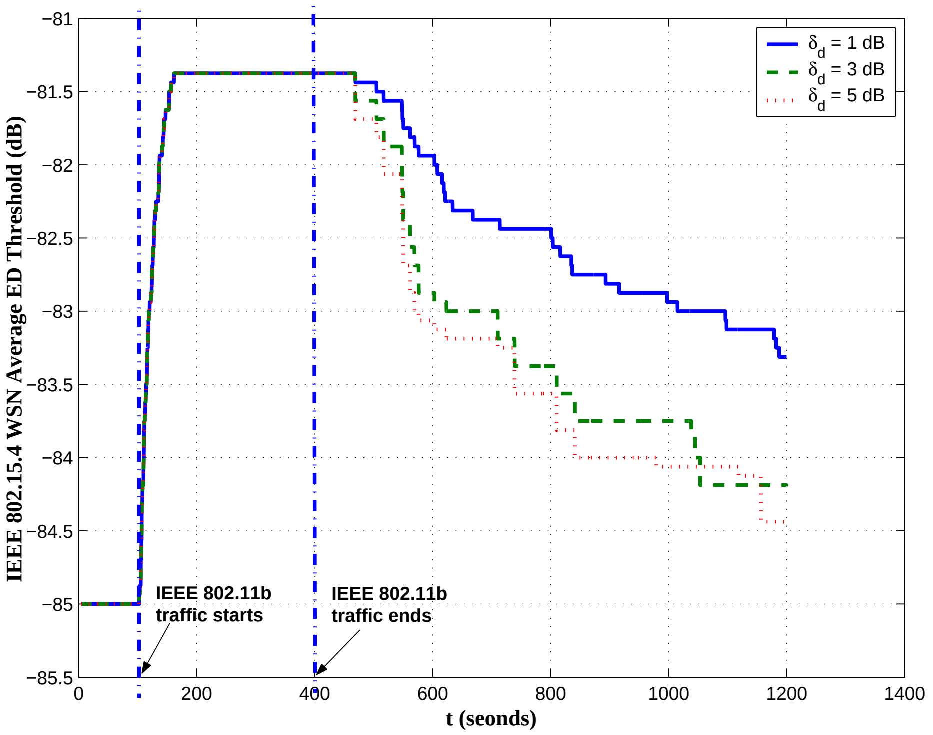


Figure 4.6: Global average ED threshold $\overline{\gamma}$ return rates with different step-down size δ_d

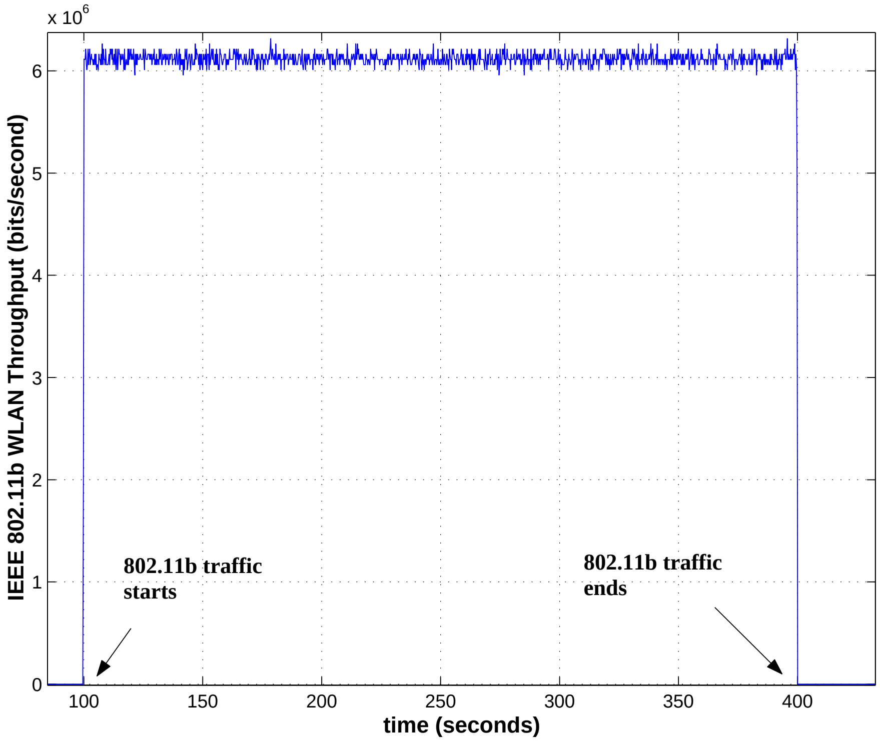


Figure 4.7: 802.11b WLAN throughput in R2

4.4 Conclusions and Future Work

After concluding the present proposed solutions are not adequate for an IEEE 802.15.4 WSN to mitigate heavy interference, in this chapter, we proposed an approach enabling an IEEE 802.15.4 WSN to mitigate heavy interference by adaptively adjusting ED thresholds of its nodes in a distributed manner. As the heavy interference appears, the ED thresholds are increased in order to reduce the inhibition loss, whereas the ED threshold gets decreased so as to avoid having a permanent channel access privilege over peers as the interference disappears. Compared to the centralized interference management approaches, e.g., the frequency agility approach specified in [Zig07c], which inappropriately assumes a reliable two-way communication between nodes even in the presence of heavy interference, our adaptive CCA approach is simpler but more robust, more responsive, and easier to be implemented at a lower cost. Simulation results validate that our adaptive CCA approach can significantly improve IEEE 802.15.4 WSNs performance in the presence of heavy interference.

In addition to effectively reducing the inhibition loss, our approach could also reduce the collision loss. This is because the approach increases IEEE 802.15.4 packet transmission, which could silence a nearby IEEE 802.11b/g packet transmission to some extent. This would happen when IEEE 802.15.4 devices and IEEE 802.11b/g interferers are in R1. On the other hand, however, if IEEE 802.15.4 devices and IEEE 802.11b/g interferers are in R2 or even R3, increased IEEE 802.15.4 packet transmission may incur more collision loss. Therefore, an interesting future research topic can be to introduce more intelligence in IEEE 802.15.4 devices so that they can learn and know their surroundings well, and then adapt to and even influence, if they can, the transmission pattern of interferers. For example, when suffering interference, an IEEE 802.15.4 device can try increasing its transmissions first. If, subsequently, detecting a decreasing interference, the IEEE 802.15.4 device may keep the increased transmissions in order to get some satisfactory packet loss level. Otherwise, if detecting a non-decreasing interference for some period of time, the IEEE 802.15.4 device may decrease its transmissions to avoid the interference and to save energy at the same time.

Besides, the parameters such as η_{max}, η_{min}, δ_i, δ_d, etc. in our adaptive CCA algorithm should be chosen and even optimized based on different situations. For example, in the environment monitoring application with a low duty-cycle of 1 packet per 3 minutes, we might need to choose a small η_{max} and η_{min}, and a large δ_i and δ_d. Thus, in the presence of interference, the application performance can get improved timely rather than too late, otherwise. For another example, in an environment where interference does neither happen too often nor takes too long, we might need to choose some large η_{max} and η_{min} to avoid changing ED threshold too often.

Moreover, although the scenarios in this chapter suggest that the increased IEEE 802.15.4 ED thresholds have just a limited impact on the IEEE 802.11b WLAN performance, this may not be universally true, especially in case of high intensive IEEE 802.15.4 operations and/or as IEEE 802.15.4 devices coexist with other wireless technologies operating on the same frequency band. Hence, it is meaningful to do more extensive investigations.

In the next chapter, we will continue our journey of exploring solutions to help IEEE 802.15.4 devices deal with interference.

Chapter 5

Interference Avoidance

The only alternative to coexistence is codestruction.

- Jawaharlal Nehru

In the previous chapter, we presented an interference mitigation method, which can increase the channel access competence of an IEEE 802.15.4 WSN. As a consequence, however, a channel access competitor, e.g., an IEEE 802.11b/g WLAN, may suffer a performance degradation. This can be avoided if the IEEE 802.15.4 WSN can find and move to an idle channel. Thus, the precious spectrum resource can be used efficiently and both systems, i.e., the IEEE 802.15.4 WSN and the IEEE 802.11b/g WLAN, can be free from mutual interference.

ZigBee[1]specification [Zig07c] proposes a feature called frequency agility, which refers to the ability of ZigBee networks to change the operational channel in the presence of interference. However, for a large-scale ZigBee network, changing the operational channel of the whole network to an idle one, may be neither appropriate, if there is only local interference, nor possible if there is no single idle channel available globally.

In this chapter, we propose a distributed adaptive multi-channel interference avoidance protocol, which enables a conventional single-channel ZigBee network to distributedly, adaptively and partially change the operational channel in the presence of local interference. As a result, the ZigBee network performance under interference can be effectively and efficiently improved.

The remainder of the chapter is organized as follows: Section 5.1 gives an overview of related studies. Section 5.2 presents our distributed adaptive multi-channel interference-avoidance protocol. OPNET simulation results and discussion are provided in Section 5.3. Section 5.4 concludes the paper and proposes some potential future work.

[1] In this chapter, we interchangeably use the terms, IEEE 802.15.4 and ZigBee.

5.1 Related Work

Interference between wireless networks has been extensively addressed in recent literature. In [Yua10b], which is also presented in Chapter 4, Yuan *et al.* proposed an approach to help ZigBee networks mitigate interference. By adaptively and distributively adjusting Clear Channel Assessment (CCA) thresholds of ZigBee devices in the presence of heavy interference, the approach can substantially reduce the inhibition loss, and therefore significantly enhance the performance of ZigBee networks under interference. However, the increased ZigBee transmission could cause performance degradation of other coexisting wireless systems, in particular IEEE 802.11b/g system. This issue may be resolved by enabling a ZigBee network to operate on multiple channels in order to avoid the interference.

There are many studies on multi-channel protocols for wireless networks. Nasipuri *et al.* [Nas99] proposed a multi-channel CSMA protocol with "soft" channel reservation. If there are N channels, the protocol assumes that each host can listen to all N channels concurrently. A host wanting to transmit a packet searches for an idle channel and transmits on that idle channel. Among the idle channels, the one that was used for the last successful transmission is preferred. As this protocol requires N transceivers for each host, it is too expensive to be suitable for a ZigBee host.

In [So04][Luo06][Nam09], only a single transceiver is used to transmit data by exploiting non-overlapping multiple channels. That is, available channels are separated into a dedicated control channel and multiple data channels. As such, however, the network performance is critically affected by the condition of the control channel. If the control channel is seriously interfered, the probability of successful negotiation severely drops and so does the network performance since losing control, the network fails to avoid interference effectively by switching to other non-interfered channels.

The ZigBee RF4CE standard [Zig09] defines a simple, robust and low-cost Remote Control (RC) network that allows wireless connectivity in applications in the Consumer Electronics (CE) domain. In an attempt to be robust against interference in the 2.4 GHz ISM frequency band, a ZigBee RF4CE RC network can dynamically operate over three channels, namely channel 15, 20 and 25. However, as shown in Figure 1.10, any of these three operational channels cannot guarantee a ZigBee RF4CE RC network to be free from 802.11 b/g interference, i.e., the interference that RF4CE intends to avoid, since interference can appear in any ZigBee channel including those of RF4C.

To mitigate interference, a function called frequency agility is proposed in the ZigBee standard [Zig07c]. The frequency agility enables a ZigBee network to change its operational channel in the presence of interference basically using the following method. There is a device which has a role of "network channel manager" in a ZigBee network. This device acts as the

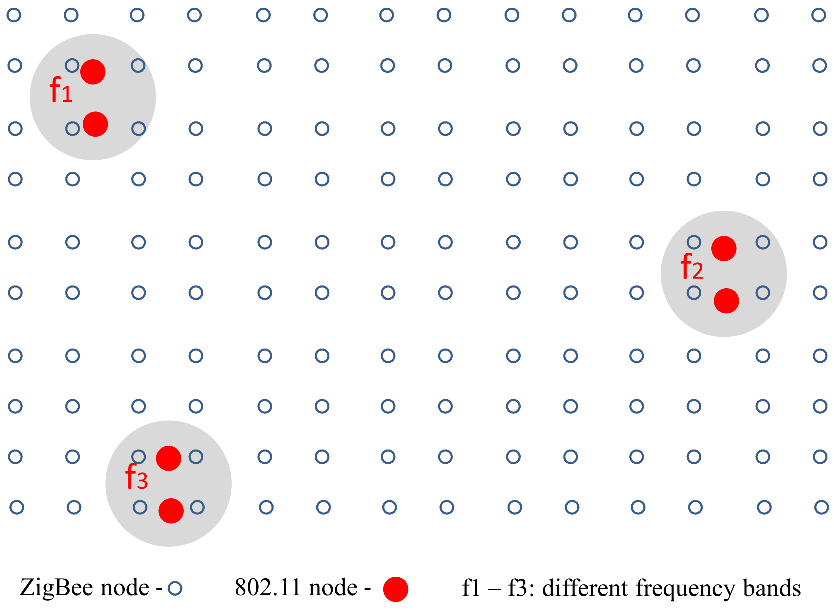


Figure 5.1: A large ZigBee network with local interference

central mechanism for reception of network interference reports and changing the channel of the network if interference is detected. The default network channel manager is the coordinator of a ZigBee network, but can be any other router-capable devices as well. Each router or coordinator is responsible for tracking transmit failures. Once the total transmissions attempted is over 20, if the transmit failures exceed 25% of the messages sent, the device may have detected interference on the channel in use. The device is then responsible for taking the following steps:

1. Conduct an energy scan on all channels. If this energy scan does not indicate higher energy on the current channel then other channels, no action is taken. The device should continue to operate as normal and the message counters are not reset. However, repeated energy scans are not desirable as the device is off the network during these scans and therefore implementations should limit how often a device with failures conducts energy scans.
2. If the energy scan does indicate increased energy on the channel in use, a Mgmt_NWK_Update_notify should be sent to the Network Manager to indicate interference is present. This report is sent with an ACK request and once the ACK is received the total transmit and transmit failure counters are reset to zero.
3. To avoid a device with communication problems from constantly sending reports to the network manager, the device should not send a Mgmt_NWK_Update_notify more than 4 times per hour.

Upon receipt of an unsolicited Mgmt_NWK_Update_notify, the network manager must evaluate if a channel change is required in the network. The specific mechanisms the network manager uses to decide upon a channel change are left to the implementers. It is expected that implementers will apply different methods to best determine when a channel change is required and how to select the most appropriate channel. The following is offered as guidance for implementation. The network manager may do the following:

1. Wait and evaluate if other reports from other devices are received. This may be appropriate if there are no other failures reported. In this case the network manager should add the reporting device to a list of devices that have reported interference. The number of devices on such a list would depend on the size of the network. The network manager can remove the reporting devices out of this list after some time.
2. Request other interference reports using the Mgmt_NWK_Update_req command. This may be done if other failures have been reported or the network manager device itself has failures and a channel change may be desired. The network manager may request data from the list of devices that have reported interference plus other randomly selected routers in the network. The network manager should not request an update from the device that has just reported interference since this data is fresh already.
3. Upon receipt of the Mgmt_NWK_Update_notify, the network manager shall determine if a channel change is required using whatever implementation specific mechanisms are considered appropriate.
4. If the above data indicate that a channel change should be considered, the network manager selects a single channel based on the lowest energy. This is the proposed new channel. If this new channel does not have an energy level below an acceptable threshold, a channel change should not be done.
5. Prior to changing channels, the network manager should store the energy scan value as the last energy scan value and the failure rate from the existing channel as the last failure rate. These values are useful to allow comparison of the failure rate and energy level on the previous channel to evaluate if the network is causing its own interference.
6. The network manager should broadcast a channel change request to all routers and coordinator with the new channel number.

Upon receipt of a channel change request the local network manager shall set a timer and switch channels upon expiration of this timer. Each device shall also reset the total transmit counters and the transmit failure counters, and then switch channels.

From the description above, we know that this solution requires two-way communication between the network manager and the other ZigBee devices on a channel, even after interference has been detected on that channel. This is not robust to the extreme interference patterns which are encountered in the context we are considering. Furthermore, this solution may work for a small-scale ZigBee network, but not be suitable for a large-scale one with local interference as shown in Figure 5.1. This is because changing the operational channel of a large-scale network to an idle one takes quite a long time, during which the network would not function properly. In the worse case, it may not be possible for the large-scale ZigBee network to find a common idle channel globally. An example is a large-scale ZigBee-based lighting control network deployed in a sports stadium where there are several local 802.11b/g interferences introduced by laptops in the audience.

Hence, in this chapter, we focus on solutions for a large-scale ZigBee network in the presence of local interference. We will propose a distributed adaptive interference-avoidance multi-channel protocol to improve the robustness and performance under interference for large-scale ZigBee network in the following section.

5.2 A Distributed Adaptive Multi-channel Protocol

Our protocol consists of two phases, i.e., an interference detection phase and an interference avoidance phase, during which an interfered ZigBee device may select a better channel. The protocol is illustrated in 5.2.

5.2.1 Interference detection

Our interference detection method is inspired by a mechanism proposed by Kim [Kim05]. This mechanism however has some drawbacks which our proposed are not present. Kim [Kim05] proposed an ACK/NACK based interference detection scheme. After a sender transmits a frame, it waits for an ACK from its recipient. When the sender does not receive the ACK within a given period (determined by a timer value), it reports a NACK for this transmission to the network layer of the sender. Whenever a NACK is reported, it increments a counter $\sharp SuccessiveNACK$ by 1. When $\sharp SuccessiveNACK$ becomes greater than the threshold TH_{NACK}, the sender decides that it suffers from interference. However, if the receiver rather than the sender is under interference or the receiver is simply defective, the sender may also not receive an ACK within the time out. Thus, the ACK/NACK based interference detection scheme would draw a wrong conclusion in such cases.

Inspired by the method of Kim [Kim05], we propose a simple but more reliable interference detection approach. Each device detects interference on its own, not requiring information exchange among each other. During every M transmission attempts, a device tracks transmission failures due to the inhibition loss, i.e., the loss due to channel access failures, as addressed in Section 3.2.1. We define transmission failures due to the inhibition loss

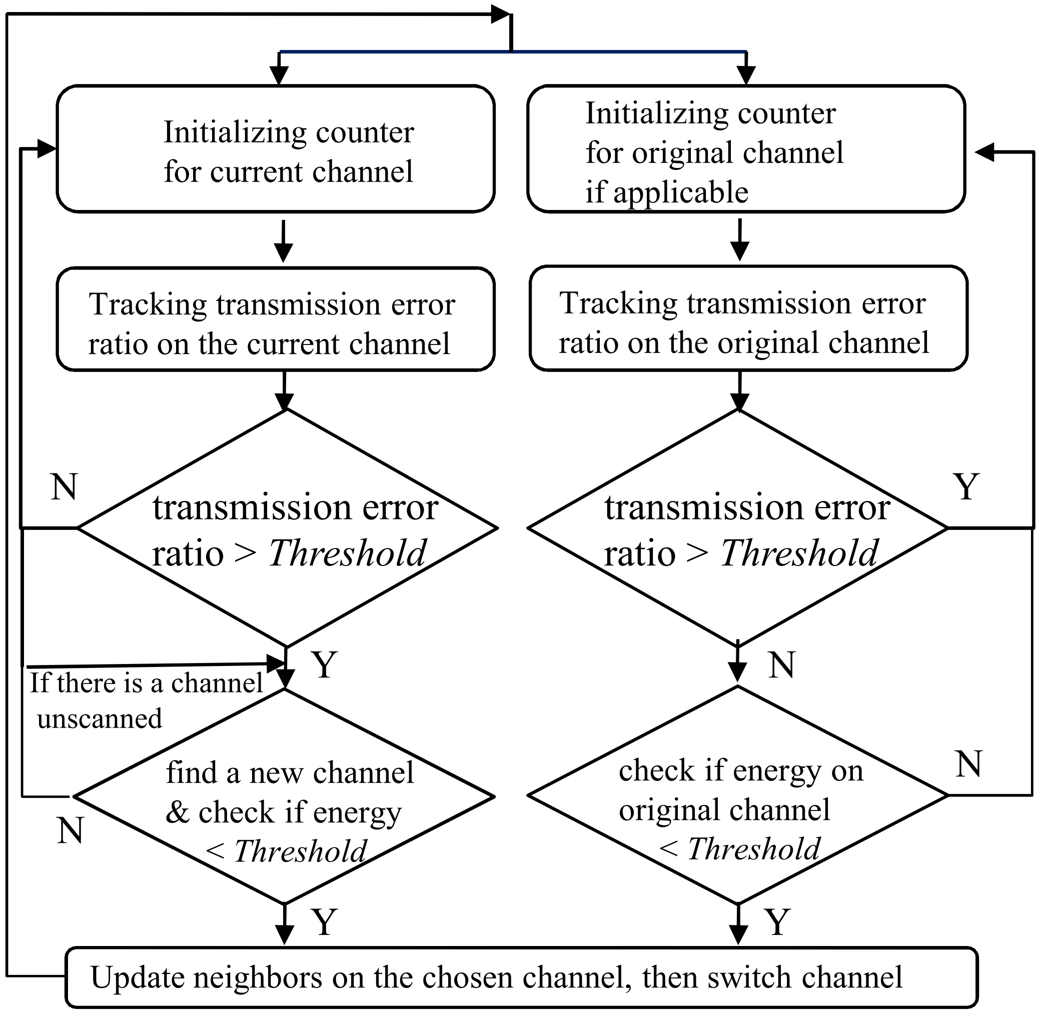

Initializing counter for current channel
Initializing counter for original channel if applicable
Tracking transmission error ratio on the current channel
Tracking transmission error ratio on the original channel
N
transmission error ratio > *Threshold*
Y
transmission error ratio > *Threshold*
Y
If there is a channel unscanned
N
find a new channel & check if energy < *Threshold*
N
check if energy on original channel < *Threshold*
N
Y
Y
Update neighbors on the chosen channel, then switch channel

Figure 5.2: Flowchart of distributed adaptive multi-channel protocol

during M transmission attempts as N. Thus, transmission failure ratio, ζ, is defined as M/N. If ζ is not greater than a threshold, $TH_{transfailure}$, i.e., $\zeta \leqq TH_{transfailure}$, the transmission failure counter resets to zero. Then, a new tracking round starts. Otherwise, if $\zeta > TH_{transfailure}$, the device performs the following interference avoidance method.

5.2.2 Interference avoidance

When a ZigBee device detects interference, according to the method we just described, it conducts energy scans on channels in a sequence specified by the following channel selection algorithm until it finds a channel on which the energy level is less than TH_{energy}. If the device fails to find such a channel after getting through all the other 15 channels, it stays at its current channel. As the most likely interference is from 802.11b/g, each channel of which overlaps four ZigBee channels, the ZigBee device will conduct the energy scan starting from a channel, which is at least four channels away from its current channel, in an attempt to avoid the possible 802.11b/g interference. Each of the 15 channels shall be gone through one by one. For example, assuming the current channel is channel 12, then the next channel would be channel 16, 20, 24, 13, 17, 21, 25, 14, 18, 22, 26, 15, 19, 23, 11, respectively. The channel selection algorithm is formally described in Algorithm 2.

Algorithm 2 Pseudo-code for Channel Selection Algorithm

```
$OriginalChannel = CurrentChannel$
$StartingChannel = CurrentChannel$
while Energy level in the current channel $> TH_{energy}$ do
    $channel = CurrentChannel + 4$
    if $channel > 26$ then
        $channel = channel - 26 + 10$
    end if
    if $channel == StartingChannel$ then
        $channel = channel + 1$
        if $channel > 26$ then
            $channel = channel - 26 + 10$
        end if
    end if
    $CurrentChannel = channel$
    Do energy scan in the current channel
end while
```

As a new channel is selected, the device then broadcasts in one-hop radius to notify its neighbors about its new operational channel number. The broadcasting does not stop until one notification is successfully transmitted, i.e., not discarded due to channel access failures, or the transmission attempt number exceeds the maximum limit, e.g., five times. Next, the device shall switch its current channel to the new one. After moving to the new channel, the device shall broadcast every *nwkLinkStatusPeriod* [Zig07c] seconds in one-hop radius a link status command including its new operational channel number on its neighbors' operational channels, in an attempt to keep its neighbors updated. Upon receiving the broadcast, the neighbors shall update the stored information about the device. If some neighbors of a device still operate on the original channel, whereas the device itself and its other neighbors operate on the other channels, the device is called an "edge" device. For an edge device, it shall also track transmission failures due to the inhibition loss as it sends frames to its neighbors that still operate on the original channel. As the transmission failure ratio gets below a threshold, the device will conduct an energy scan on the original channel. If the energy level is less than TH_{energy}, the device shall change its operational channel back to the original one and update its neighbors. This scheme allows devices which have already changed their operational channels to gradually move back to their original channel as the interference at the original channel disappears. Thus, the whole network could operate on the same channel again as the interference is gone. This procedure is illustrated in Figure 5.2.

In the following Section, we will perform OPNET simulation to examine if the solution described above can work and to what extent if so. To simulate the scenario we focus on in this chapter, i.e., a large-scale ZigBee network suffering local interference, we first need to work out a network topology, where the intensity of 802.11b interference is such that only a part of the ZigBee network can be triggered to move to a new idle channel, while leaving the rest of devices on the original interfered channel. Then we will see if those ZigBee devices which suffer severe interference can actually change their operational channel to the idle one, and switch back to their original operational channel as the interference is gone. Furthermore, we will see if the ZigBee network coexistence performance can be improved significantly by our solution above.

5.3 Simulation Results and Discussion

Simulation parameters are shown in Table 5.1. The transmit powers of 0 dBm and 17 dBm are typical values for ZigBee devices and IEEE 802.11b devices, respectively. The chosen values of CCA threshold are default ones given in the IEEE 802.15.4 [IEE06] and IEEE 802.11b [IEE99b] standards. The date rates of 250 kbps and 11 Mbps are also typical values for ZigBee devices and IEEE 802.11b devices, respectively. To show the worst case of coexistence, we choose operational channels with the closest center frequencies, which are 2410 MHz (channel 12) and 2412 MHz for ZigBee devices and IEEE 802.11b devices, respectively. Besides, we choose a channel with

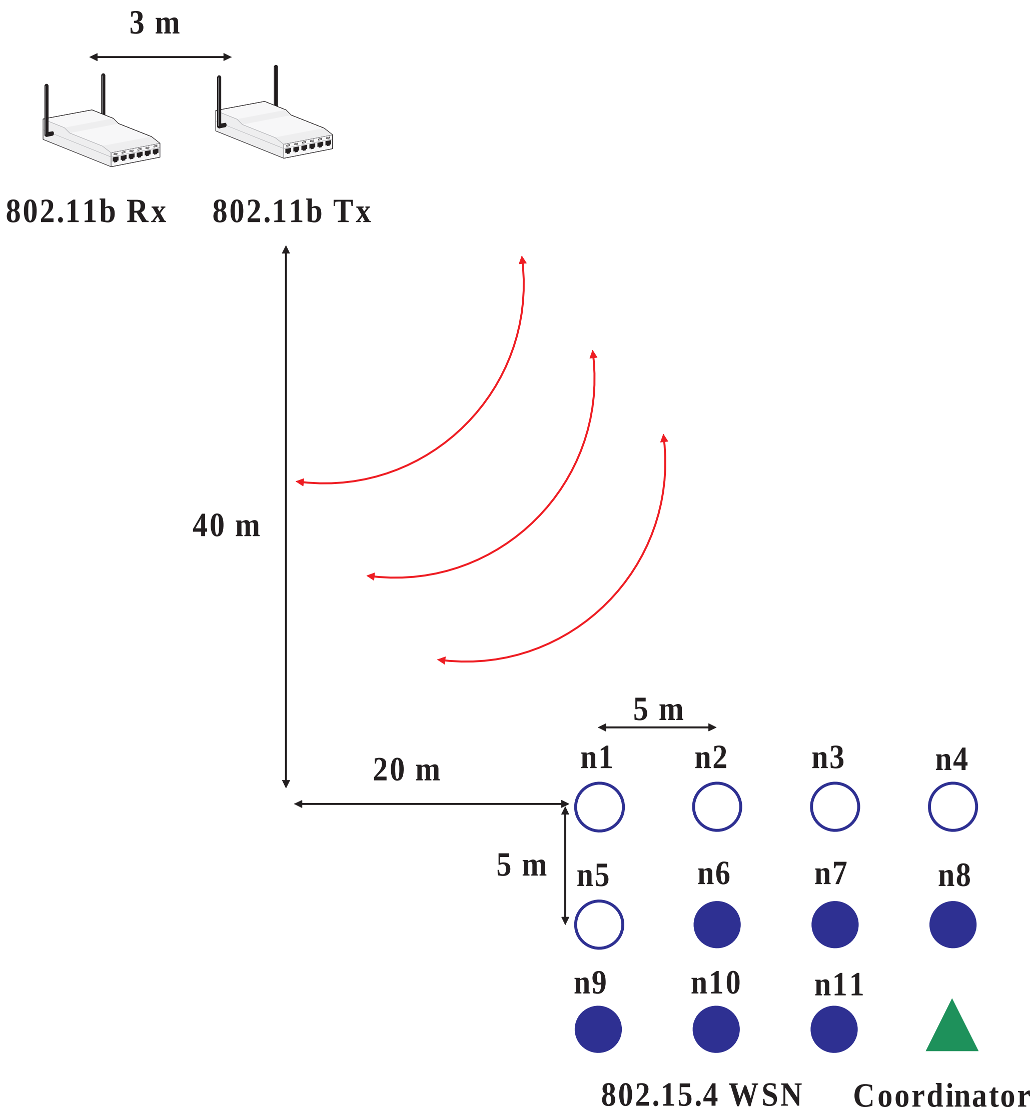


Figure 5.3: Simulation topology

Table 5.1: Simulation Parameters

	ZigBee	**IEEE 802.11b**
Transmit power	0 dBm	17 dBm
Data rate	250 kbps	11 Mbps
CCA threshold	-85 dBm	-84 dBm
Center frequency	2410 MHz, 2430 MHz (new)	2412 MHz
Traffic mode	Constant 5 pkt/s	Saturated
Packet size	30 bytes	1500 bytes
ACK	No	Yes

the center frequency of 2430 MHz (channel 16) for the ZigBee devices to move to in case of using the multiple channel operation when suffering interference. As shown in Figure 1.10, ZigBee channel 16 (2430 MHz) does not overlap the channel (2412 MHz) of IEEE 802.11b, which therefore guarantee ZigBee devices free from IEEE 802.11b interference. The payload size of 30 bytes and 1500 bytes are typical values in control applications for IEEE 802.15.4 devices, and in data transfer applications for IEEE 802.11b devices, respectively. To observe the impact from interference on IEEE 802.15.4 data transfer, we choose not to use ACK for IEEE 802.15.4 devices, while using ACK is mandatory as defined in the IEEE 802.11b standard [IEE99b]. In case of using ACK, IEEE 802.15.4 coexistence performance will become worse since when an ACK is not received due to interference, a retransmission has to occur. To show the worst case of interference, we make a saturated IEEE 802.11b data stream, which means there is always an IEEE 802.11b packet ready to transmit. We also introduce an intensive IEEE 802.15.4 traffic with a constant 5 packets per second. The intensive traffic helps to show a more visible interfered effect and then an improved result due to our proposed solution. We consider transmission failures due to the inhibition loss during every 100 transmission attempts, i.e., $M = 100$, and choose the transmission failure threshold $TH_{transfailure} = 25\%$. Smaller (larger) M and $TH_{transfailure}$ make the network more (less) sensitive to interference and then change the operational channel more (less) frequently. We have a further discussion on this in Section 5.4.

To simulate the scenario we focus on in this chapter, i.e., a large-scale ZigBee network suffers local interference, we work out a network topology as shown in Figure 5.3, where the 802.11b interference can force only a part of the ZigBee network, i.e., device n1, n2, n3, n4 and n5, to move to a new idle channel, i.e., channel 16, according to Algorithm 2, while leaving the rest of devices on the original interfered channel, i.e., channel 12.

In Figure 5.3, where there are a pair of 802.11b Tx/Rx devices and a ZigBee network consisting of 12 devices, which can be regarded as a corner part of a large-scale ZigBee network. Each ZigBee device sends packets to a randomly chosen device at the constant rate of 5 packet/second. The ZigBee devices track transmission failures on channel 12, their original channel. After sending 50 packets on channel 12, a ZigBee device checks the transmission failure ratio, defined in Section 5.2.1. When the transmission failure ratio exceeds 25% (a discussion on this figure is given in Section 5.4), a threshold specified in the ZigBee frequency agility [Zig07c], the device will look for the next idle channel, according to Algorithm 2, and if finding one, it will broadcast a notification and switch its channel to the new one, i.e., following the procedure addressed in Section 5.2. Reversely, as the transmission failure ratio on the original channel, i.e., channel 12, gets less than e.g., 3%, a ZigBee device which has moved to the new channel, will conduct an energy scan on channel 12. If the energy level is less than TH_{energy}, the device shall broadcast a notification and move back to channel 12. The traffic between the IEEE 802.11b devices is saturated, which starts at the $t = 400$ second and stops at the $t = 700$ second. The rest of the simulation parameters are shown in Table 5.1.

The simulation results are averaged over five runs, taking 1000 seconds for each. We investigate the network performance in two cases: “Multi-channel Enabled”and “Multi-channel Disabled”, where the multi-channel operation is “enabled” and “disabled”, respectively. As shown in Figure 5.4, we see that before the IEEE 802.11b traffic starts, the throughput of device n1 is around 1050 bits/s. When the IEEE 802.11b traffic starts at the $t = 400$ second, the throughput drops by 29% to approximately 750 bits/s in case of the multi-channel operation disabled as shown by the curve of “Multi-channel Disabled”, whereas by only 9.5% to around 950 bits/s in case of the multi-channel operation enabled as shown by the curve of “Multi-channel Enabled”. In other words, the multiple channel operation improves the ZigBee device performance under interference by about 20% in this case. We find that in case of “Multi-channel Enabled”, device n1, n2, n3, n4 and n5 actually moved to a new idle channel, which is channel 16, according to Algorithm 2, while the rest of devices, i.e., the less interfered ones, still stay on the original channel, i.e., channel 12.

When the IEEE 802.11b traffic stops at the $t = 700$ second, the throughput gets back to the previous 1050 bits/s in both cases, which shows that our approach really enables ZigBee devices to move back to their original channel as the interference on that original channel is gone.

The global throughput changes for the whole network are shown in Figure 5.5. As expected, the global performance is improved, too. In fact, the global throughput improvement reflects a cumulative effect of those in each individual devices. Thus, for a large-scale ZigBee network in the presence of few local interferences, the performance improvement for the whole network may not be noticeable, but for the individual devices, the performance improvement would be significant as shown in Figure 5.4.

To measure an inhibition loss level, we can use an inhibition loss rate defined as the number of bits lost per second due to inhibition loss. A global inhibition loss rate is a sum of inhibition loss of all devices in a network. We see in Figure 5.6, when our multi-channel operation is used, the inhibition loss rate drops (and therefore the throughput increases) significantly from approximately 3300 bits/s to around 300 bits/s.

The simulation results above show that our distributed adaptive multi-channel protocol can help a large-scale ZigBee network efficiently and effectively mitigate local interference and therefore improve the ZigBee coexistence performance, especially for devices suffering from local interference. In case of small-scale ZigBee networks, our protocol, which allows a conventional single-channel ZigBee network to *partially* change the operational channel, may not be better than the way of changing the network’s channel *entirely*

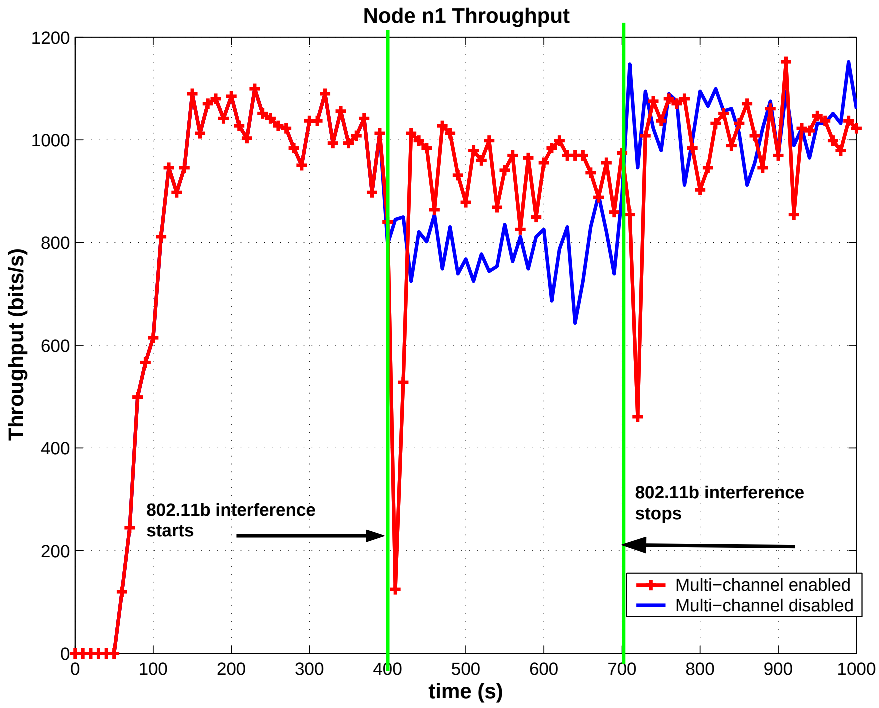


Figure 5.4: Device n1 throughput in cases: “Multi-channel Enabled” and “Multi-channel Disabled”

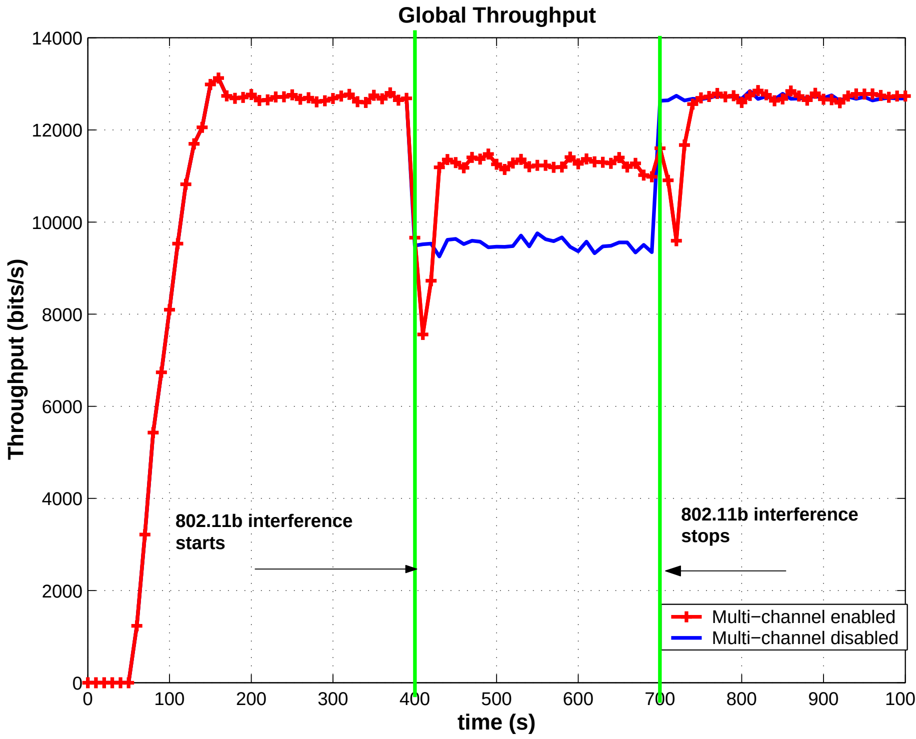


Figure 5.5: Global throughput in cases: “Multi-channel Enabled” and “Multi-channel Disabled”

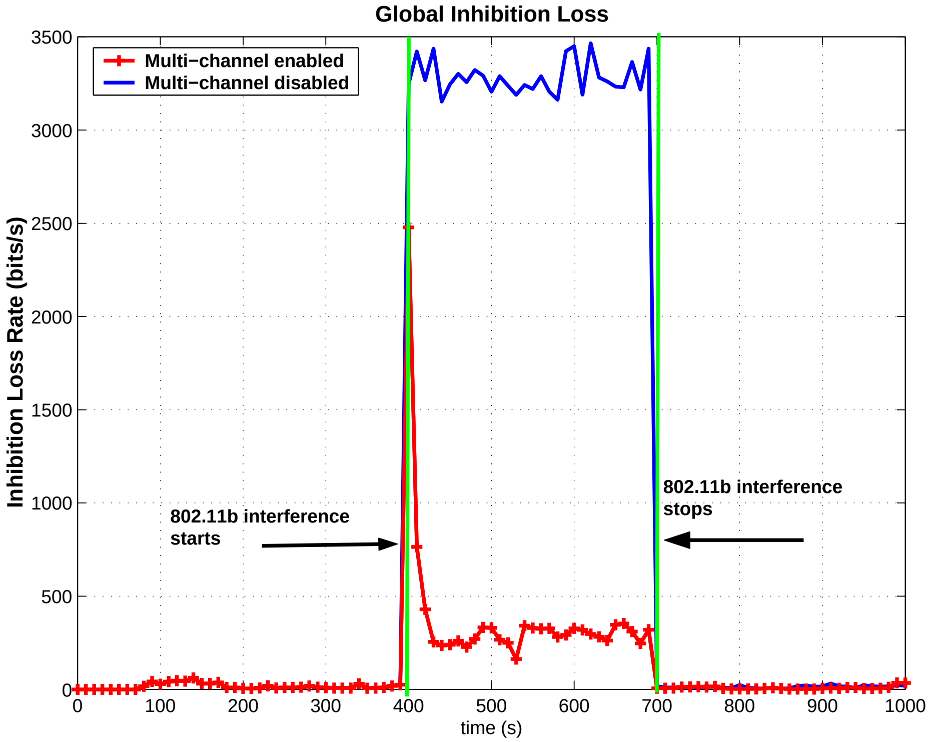


Figure 5.6: Global inhibition loss rate in cases: "Multi-channel Enabled" and "Multi-channel Disabled"

as proposed in the ZigBee frequency agility [Zig07c] in terms of the extent of the global performance improvement. However, unlike the ZigBee frequency agility [Zig07c], our approach does not require information exchange among devices for dealing with interference, and therefore is more robust. Besides, it is worthwhile to note that although in this chapter we take 802.11b as the interference source due to its popularity, our approach can actually work in the presence of any kind of interference as long as it leaves an idle channel for ZigBee networks to move to.

Our approach can be improved further. Many parameters involved in this method could be optimized in the future according to different applications. For example, in our simulation, as specified in the ZigBee frequency agility [Zig07c], we also chose 25% as the transmission failure ratio threshold for a ZigBee device to decide whether changing the operational channel. However, 25% may not be the optimized value, depending on applications. When an application is time-critical and thus needs to be more sensitive to interference, a smaller value than 25% will help. When an application is non-time-critical but energy-critical, and thus needs to be less sensitive to interference, a larger value than 25% is more suitable.

Furthermore, the interference mitigation and the interference avoidance methods could combine to deal with the coexistence issue more effectively and efficiently. For example, when a ZigBee network encounters interference, it may try mitigating the interference on the current operational channel first. If its performance cannot be improved to a satisfactory level, it can further try to avoid the interference by changing the operational channel. In case there is no channel free from interference, it may select and switch to a channel which has the least interference level, and then use interference mitigation methods on that channel.

5.4 Conclusions and future work

In this chapter, we propose a distributed adaptive interference avoidance multi-channel protocol, which enables a conventional single-channel large-scale ZigBee network to distributively, adaptively and partially change the operational channel in the presence of local interference. The protocol is distributed, i.e., each device can individually make decision to change the operational channel based on its local perception while no communication with a network manager gets involved. This makes the protocol robust especially in the presence of severe interference. Furthermore, the protocol is adaptive, i.e., a device can switch the operational channel to an idle one when it suffers interference, and it can also switch the operational channel back to the original one when the interference is gone. As such, each device of a network always works on the original operational channel as long as they are free from interference, which gets rid of unnecessary channel switching overheads after interference disappears and thus makes the whole network work not only robustly but more efficiently. Moreover, the protocol allows a part of a network rather than an entire large-scale network to change the operational channel in the presence of local interference, which reduces channel switching overheads and also makes the network more responsive to react to the interference. OPNET simulation results validate that the protocol can efficiently and effectively improve the robustness of a ZigBee network and therefore its coexistence performance. In addition, note that since no communication mechanism but only simple computation is involved in the protocol, it is easy to be implemented at a low cost. Last but not least, although the protocol is mainly designed to improve the coexistence performance of a large-scale ZigBee network with local interference, it can also help a small-scale ZigBee network, where each device of the network suffers interference at a similar severe level. In such a case, the entire network can move to an idle channel.

Compared with the interference mitigation method presented in Chapter 4, the interference avoidance method in this chapter needs at least one ZigBee channel free from a local interference, which is, though not guaranteed, very likely to be the case. By enabling an interfered system to move to an idle channel, the interference avoidance method enhances the spectrum usage efficiency and makes the competing systems free from mutual interference.

Chapter 6

Conclusions and Future Work

It's more fun to arrive at a conclusion than to justify it.
-Malcolm Forbes

6.1 Conclusions

In this thesis, we have extensively studied the coexistence issue between IEEE 802.15.4/ZigBee WSNs and IEEE 802.11b/g WLANs. Although many studies on the coexistence issue between IEEE 802.15.4/ZigBee WSNs and IEEE 802.11b/g WLANs have been done, the conclusions they drew are incomplete and/or conflicting, and therefore confusing. To get a clear understanding about the coexistence issue between IEEE 802.15.4/ZigBee WSNs and IEEE 802.11b/g WLANs, an extensive study is needed.

In Chapter 2, we propose a coexistence model of IEEE 802.15.4 nodes and IEEE 802.11b/g nodes. The model is based on two aspects, i.e., power and the timing. Due to the significant difference in transmit powers of IEEE 802.15.4 and IEEE 802.11b/g, the sensing ranges of them are quite asymmetric. As a result, three distinct coexistence regions can be identified. In each of these coexistence regions, IEEE 802.11 nodes and IEEE 802.15.4 nodes exhibit different interplay and hence different coexistence performances, which may not be the same as we expected. For example, instinctively, we may feel that the closer an IEEE 802.15.4 node gets to an IEEE 802.11b/g interferer, the worse performance the IEEE 802.15.4 node would have. Our coexistence model, however, reveals that this perception may not be true. In fact, as the IEEE 802.15.4 node and the IEEE 802.11b/g interferer get so close that they are in the coexistence region R_1, where they can sense each other, the coexistence performance of the IEEE 802.15.4 node is not necessary the worst. Instead, in the coexistence region R_2, where the IEEE 802.11b/g interferer cannot sense the IEEE 802.15.4 and therefore does not respect the IEEE 802.15.4 transmission, the coexistence performance of the IEEE 802.15.4 node could get even worse than in R_1. Clearly, the three coexistence regions and the different interplay between IEEE 802.15.4 WSNs and

IEEE 802.11b/g WLANs in each region explain the incomplete/conflicting conclusions drawn by many previous studies from their incomplete analysis and/or observations.

Next, in Chapter 3, we improved the coexistence model proposed in Chapter 2 by taking into account some important implementation factors and studied the coexistence performance of IEEE 802.15.4 WSNs under IEEE 802.11b/g interference in a nearly real-life environment. We revealed that some implementation factors such as the IEEE 802.15.4 Rx-to-Tx turnaround time and the CCA partial detection effect can have significant impact on IEEE 802.15.4 WSNs coexistence performance in reality, e.g., a long IEEE 802.15.4 Rx-to-Tx turnaround time can impair the CCA performance and therefore the IEEE 802.15.4 WSNs coexistence performance. The enhanced model can precisely explain and predict the IEEE 802.15.4 WSNs coexistence performance. Furthermore, under the guidance of the model, the IEEE 802.15.4 WSNs coexistence performance were extensively investigated in all of the three coexistence regions in different scenarios by analysis, simulation and experiments. The simulation and experimental results agree with our analysis.

In sum, from the work in Chapter 2 and Chapter 3, we can draw the following conclusions:

- the performance of an IEEE 802.15.4 WSN can be considerably negatively affected by a heavy IEEE 802.11 interference if their channels are not allocated properly
- Due to low power and long timing in the MAC mechanism, IEEE 802.15.4 nodes suffer unfairness in the channel access when competing with IEEE 802.11b/g nodes
- When IEEE 802.15.4 nodes coexist with IEEE 802.11b/g nodes, three coexistence regions may be identified. They have different coexistence behaviors in each of the regions
- Some implementation factors such as 802.15.4 Rx-to-Tx turnaround time and CCA partial detection effect can impair the CCA performance and therefore IEEE 802.15.4 WSNs coexistence performance in reality
- Although generally IEEE 802.15.4 WSNs has little impact on the IEEE 802.11 WLANs performance, in some cases, IEEE 802.15.4 WSNs may have a non-negligible impact (e.g., 10%) on the performance of IEEE 802.11b/g WLANs.

In the previous two chapters, we have fulfilled one of the thesis targets stated in Section 1.4, i.e., to achieve a clear understanding on the coexistence issue between IEEE 802.15.4/ZigBee WSNs and IEEE 802.11b/g WLANs, by analysis, simulation and experiments. Based on such a clear understanding, we are exploring the solutions to help IEEE 802.15.4 WSNs deal with interference. Basically, there are two categories for the ways of dealing with interference: interference control/mitigation and interference avoidance. In Chapter 4 and Chapter 5, we are addressing solutions in each of these two categories, respectively.

In Chapter 4, we proposed an approach enabling an IEEE 802.15.4 WSN to mitigate heavy interference by adaptively adjusting CCA thresholds of its nodes in a distributed manner. As the heavy interference appears, the CCA thresholds are increased in order to reduce the inhibition loss, whereas the CCA threshold gets decreased so as to avoid having a permanent channel access privilege over peers as the interference disappears. Compared to the centralized interference management approaches, e.g., the frequency agility approach specified in the ZigBee specification[Zig07c], which inappropriately assumes a reliable two-way communication between nodes even in the presence of heavy interference, our adaptive CCA approach is simpler but more robust, more responsive, and easier to be implemented at a lower cost. The simulation results validate that the adaptive CCA approach may significantly improve IEEE 802.15.4 WSNs performance in the presence of heavy interference.

ZigBee specification [Zig07c] proposes a feature called frequency agility, which refers to the ability of ZigBee networks to change the operational channel in the presence of interference. However, for a large-scale ZigBee network, changing the whole network operational channel to an idle one, may be neither appropriate if there is only local interference nor possible if there is no any single idle channel available globally. Therefore, in Chapter 5, we propose a distributed adaptive interference-avoidance multi-channel protocol, which enables a conventional single-channel large-scale ZigBee network to distributively, adaptively and partially change the operational channel in the presence of local interference. As a result, the ZigBee network performance under interference can be effectively and efficiently improved.

6.2 Future Directions

Although being discussed through the whole thesis, the coexistence issue certainly needs to explore further much beyond a single PhD thesis. Besides this thesis, many studies have been done on the coexistence issue between two wireless systems, e.g., the coexistence between 802.11b and Bluetooth have been extensively studied in [How01b][Jo03][Sak03][Fen02], and the coexistence between IEEE 802.15.4 and other systems has been investigated in [Sik05] and [How03], but few work has been done on the coexistence among multiple (>2) wireless systems. In reality, however, it is more often to happen that there are more than two wireless systems work closely to each other. For example, a person may take a ZigBee personalcare monitor, listen music via a bluetooth headset and surf the Internet by a WiFi connection of a laptop at the same time. As such, there is an increasing demand for researchers to study the coexistence of multiple wireless systems.

Essentially, to make a truly wireless "ecosystem" where each system can coexist in harmony, it requires both academia and industry to put serious thought into coexistence when they develop and standardize radio technologies, and some systematic approaches in incorporating coexistence methodology in designing future radio technologies must be employed.

Appendix A

List of Abbreviations

ACL	Asynchronous Connectionless
ACK	Acknowledgment
AFH	Adaptive Frequency-Hopping
AP	Access Point
AWGN	Additive White Gaussian Noise
AWMA	Alternating Wireless Medium Access
BER	Bit Error Rate
CCA	Clear Channel Assessment
CCK	Complementary Code Keying
CFR	Code of Federal Register
CTS	Clear to Send
CSMA-CA	Carrier Sense Multiple Access with Collision Avoidance
CW	Contention Window
DIFS	Distributed coordination function Inter-Frame Space
DFS	Dynamic Frequency Selection
DSSS	Direct-Sequence Spread Spectrum
ED	Energy Detection
EIRP	Equivalent Isotropically Radiated Power
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FEC	Forward Error Correction
FFD	Full Function Device
GF	Group Formation
GTS	Guaranteed Time Slot
GUTPC	Goodput-oriented Utility-based Transmit Power Control
HEC	Header Error Check
ID	Interference Detection

IEEE	Institute of Electrical and Electronics Engineers
ISM	Industrial, Scientific, and Medical
LOS	Line-Of-Sight
LQI	Link Quality Indicator
MAC	Medium Access Control
OFDM	Orthogonal Frequency Division Multiplexing
PAN	Personal Area Network
PER	Packet Error Rate
PHY	PHYsical layer
PN	Personal Network
PNP2008	Personal Network Pilot 2008
PTA	Packet Traffic Arbitration
RSSI	Received Signal Strength Indication
RFD	Reduced Function Device
RTS	Request to Send
SCO	Synchronous Connection-Oriented
SIFS	Short Inter Frame Spacing
SINR	Signal-to-Interference-plus-Noise Ratio
SIR	Signal-to-Interference Ratio
SNR	Signal-to-Noise Ratio
TDMA	Time-Division Multiple Access
TIC	Transmit Interval Control
TPC	Transmit Power Control
UDP	User Datagram Protocol
UWB	Ultra-Wide Band
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Network
ZC	ZigBee Coordinator
ZED	ZigBee End Device
ZR	ZigBee Router
WSN	Wireless Sensor Network

Appendix B

Supporting Projects

In addition to Delft University of Technology and Philips Research, the work in this thesis has been partially funded by the Dutch Ministry of Economic Affairs through the project PNP2008 under the Freeband Communication Impulse of the technology programme. Below, we give an brief introduction to this project.

Freeband PNP2008

The PNP2008 project is part of the Freeband Communication programme, which aims at the generation of public knowledge in advanced telecommunication (technology and applications). Freeband is based on the vision of 4G networks and services. It specifically aims at establishing, maintaining and reinforcing the Dutch knowledge position at the international forefront of scientific and technological developments, addressing the most urgent needs for research and novel applications in the present unfolding of new technology. Freeband comprises more than 25 organizations, including all-important technology providers and many representative end-user organizations. The Dutch Ministry of Economic Affairs is co-funding this programme as part of the BSIK plan.

The goal of the PNP2008 project is to develop and demonstrate the novel concept of the Personal Network (PN), which is a distributed personal environment consisting of clusters of geographically dispersed devices that dynamically changes according to the context and needs of the user. Preparing and running a real-life pilot once a year, starting from the first year of the project, will provide a unique insight and feedback in the technical, business and user-related issues associated with the introduction of PN. A distinctive element of this project is the investigation, development and demonstration of the concept of a Personal Network Gateway, an important enabling factor for the incorporation of the Personal Area Network into a fully functional PN. As important will be a Mobility Provider platform that provides an operational environment to manage user, service and network related issues.

The main results foreseen by the project are in the field of network architectures and protocols, security, biometric authentication, mobility management and user aspects. Developing an automated and context sensitive concept is a challenging research task, but it has a strong industrial potential, since it would bring in the possibility to build a whole new class of applications, services and devices.

This project concludes in 2008.
http://pnp2008.freeband.nl/

Bibliography

[Aar01] E. Aarts, R. Harwig, and M. Schuurmans. *Ambient Intelligence in The Invisible Future: The Seamless Integration Of Technology Into Everyday Life*. McGraw-Hill, 2001.

[Ahl03] H. AhleHagh, W. Michalson, and D. Finkel. Statistical Characteristics of Wireless Network Traffic and Its Impact on Ad Hoc Network Performance. In *the 2003 Applied Telecommunication Symposium*. 2003.

[Aky02] I. F. Akyildiz, W. Su, Y. Sankasubramaniam, and E. Cayirci. Wireless Sensor Networks: A Survey. *Computer Networks*, vol. 38:pp. 392–422, 2002.

[Ash09] S. Ashton. ZigBee Technology Overview. Tech. Rep. 095376r00ZB, Ember Corporation, 2009.

[Ben09] M. Bennis. *Spectrum Sharing for Future Mobile Cellular Systems*. Phd, Universityof Oulu, Finland, 2009.

[Bha04] A. Bharathidasan and V. A. S. Ponduru. Sensor Networks: An Overview. In *the 23rd Conference of the IEEE Communications Society (INFOCOM)*. Hong Kong, 2004.

[Esp07] J. Espina, T. Falck, and O. Mülhens. Network Topologies, Communication Protocols, and Standards. In *Body Sensor Networks*, pp. 145–182. Springer, 2007.

[ETSa] ETSI. *ETSI EN 300 328-1, Electromagnetic Compatibility and Radio Spectrum Matters (ERM); Wideband Transmission Systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Part 1: Technical characteristics and test conditions.*

[ETSb] ETSI. *ETSI EN 300 328-2, Electromagnetic Compatibility and Radio Spectrum Matters (ERM); Wideband Transmission Systems; Data transmission equipment operating in the 2,4 GHz ISM band*

and using spread spectrum modulation techniques; Part 2: Harmonized EN covering essential requirements under article 3.2 of the R and TTE Directive.

[FCC] FCC. *FCC Code of Federal Register (CFR), Part 47, Section 15.35, Section 15.205, Section 15.209, Section 15.231, Section 15.247, and Section 15.249.*

[Fen02] W. Feng, N. Arumugam, and G. H. Krishna. Impact of Interference on a Bluetooth Network in the 2.4 GHz ISM band. In *the International Conference on Computational Science*, vol. 2, pp. 820–823. Amsterdam, The Netherlands, 2002.

[Gal96] R. G. Gallager. *Discrete Stochastic Processes*. Kluwer, 1996.

[Gut03] J. A. Gutierrez, E. H. Callaway, and R. Barrett. *Low-Rate Wireless Personal Area Networks - Enabling Wireless Sensors with IEEE 802.15.4*. IEEE Press, 2003.

[Haa99] J. C. Haartsen and S. Zürbes. *Bluetooth Voice and Data Performance in 802.11 DS WLAN Environment.* Ericsson Sig Publication, 1999.

[How01a] I. Howitt. IEEE 802.11 and Bluetooth Coexistence Analysis Methodology. In *the 53rd IEEE Vehicular Technology Conference*, pp. 1114–1118. Rhodes, Greece, 2001.

[How01b] I. Howitt. WLAN and WPAN Coexistence in UL Band. *IEEE Transactions on Vehicular Technology*, vol. 50(4):pp. 1114–1124, 2001.

[How02] I. Howitt. Bluetooth performance in the presence of 802.11b WLAN. *IEEE Transactions on Vehicular Technology*, vol. 51(6):pp. 1640–1651, 2002.

[How03] I. Howitt and J. A. Gutierrez. IEEE 802.15.4 Low Rate Wireless Personal Area Network Coexistence Issues. In *the IEEE Wireless Communications and Networking Conference (WCNC)*, vol. 3, pp. 1481–1486. New Orleans, U.S.A., 2003.

[IEE99a] IEEE. *Physical Model Sub-Group Discussion and Questions - IEEE 802.15/138R0*, 1999.

[IEE99b] IEEE 802.11. *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 1999.

[IEE02] IEEE 802.15.1. *Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs)*, 2002.

[IEE03a] IEEE 802.15.2. *Part 15.2: Coexistence of Wireless Personal Area Networks with Other Wireless Devices Operating in Unlicensed Frequency Bands*, 2003.

[IEE03b] IEEE 802.15.2. *Part 15.2: Coexistence of Wireless Personal Area Networks with Other Wireless Devices Operating in Unlicensed Frequency Bands*, 2003.

[IEE03c] IEEE 802.15.4. *Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)*, 2003.

[IEE06] IEEE 802.15.4. *Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)*, 2006.

[Jin05] X. Jing, S. Mau, D. Raychaudhuri, and R. Matyas. Reactive cognitive radio algorithms for co-existence between IEEE 802.11b and 802.16a networks. In *the 2005 IEEE Global Telecommunications Conference (GLOBECOM'05)*, pp. 1–5. IEEE, St. Louis, U.S.A., 2005.

[Jo03] J. H. Jo and H. Jayant. Performance Evaluation of Multiple IEEE 802.11b WLAN Stations in the Presence of Bluetooth Radio Interference. In *the IEEE International Conference on Communications (ICC)*, vol. 2, pp. 1163–1168. Anchorage, Alaska, U.S.A., 2003.

[Kar07] H. Karl and A. Willig. *Protocols and Architectures for Wireless Sensor Networks*. John Wiley & Sons, 2007.

[Kim05] S. M. Kim, J. W. Chong, C. Y. Jung, T. H. Jeon, J. H. Park, Y. J. Kang, S. H. Jeong, M. J. Kim, and D. K. Sung. Experiments on Interference and Coexistence between ZigBee and WLAN Devices Operationg in the 2.4 GHz ISM Band. In *the Next Generation Personal Computer Conference*, pp. 15–19. 2005.

[Kou05] A. Koubaa, M. Alves, and E. Tovar. IEEE 802.15.4 for Wireless Sensor Networks: A Technical Overview. Tech. Rep. HURRAY-TR-050702, IPP-HURRAY! GROUP, POLYTECHNIC INSTITUTE OF PORTO (ISEP-IPP), PORTUGAL, July 2005.

[Kru03] J. Kruys. Co-existence of Dissimilar Wireless Systems. Web page, 2003. `http://www.wi-fi.org/opensection/pdf/co-existence_dissimilar_systems.pdf`.

[Luo06] T. Luo, M. Motani, and V. Srinivasan. CAM-MAC: A Cooperative Asynchronous Multi-Channel MAC Protocol for Ad Hoc Networks.

In *the Third International Conference on Broadband Communications, Networks, and Systems (Broadnets 2006)*. San José, U.S.A, 2006.

[Mar02] M. Marcus, J. Burtle, B. Franca, A. Lahjouji, and N. McNeil. Report of the Unlicensed Devices and Experimental Licenses Working Group. Tech. Rep. 02-135, Federal Communications Commission (FCC) Spectrum Policy Task Force, 2002.

[McG10] B. McGuigan. What is ZigBee? Web page, 2010. `http://www.wisegeek.com/what-is-zigbee.htm`.

[McH06] M. A. McHenry, P. A. Tenhula, D. McCloskey, D. A. Roberson, and C. S. Hood. Chicago Spectrum Occupancy Measurements and Analysis and a Long-term Studies Proposal. In *the Workshop on Technology and Policy for Accessing Spectrum (TAPAS)*. Boston, USA, 2006.

[Nam09] P. G. Namboothiri and K. M. Sivalingam. Performance of a Multichannel MAC Protocol Based on IEEE 802.15.4 Radio. In *the IEEE 34th Conference on Local Computer Networks (LCN 2009)*. Zürich, Switzerland, 2009.

[Nas99] A. Nasipuri, J. Zhuang, and S. R. Das. A Multichannel CSMA MAC Protocol for Multihop Wireless Networks. In *the IEEE Wireless Communications and Networking Conference (WCNC)*. New Orleans, U.S.A., 1999.

[OPN] OPNET. `http://www.opnet.com/`. Web Page. The last accessed was in 14th November 2010.

[Pan10] Y. Pan. Introduction to OPNET simulator. Web page, 2010. `http://bolero.ics.uci.edu/~ypan/OPNET/Introduction%20to%20OPNET%20simulator.pdf`.

[Pet06] M. Petrova, J. Riihijärvi, P. Mähönen, and S. Labella. Performance Study of IEEE 802.15.4 Using Measurements and Simulations. In *the IEEE Wireless Communications and Networking Conference (WCNC)*. Las Vegas, U.S.A., 2006.

[Pol06] S. Pollin, M. Ergen, A. Dejonghe, L. V. D. Perre, F. Catthoor, I. Moerman, and A. Bahai. Distributed Cognitive Coexistence of 802.15.4 with 802.11. In *the 1st International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2006)*. Mykonos, Greece, 2006.

[Pot00] G. J. Pottie and W. J. Kaiser. Embedding the Internet: Wireless Integrated Network Sensors. *Communications of the ACM*, vol. 43(5):pp. 51–58, 2000.

[Rab00] J. M. Rabaey, M. J. Ammer, J. L. da Silva, D. Patel, and S. Roundy. PicoRadio Supports Ad Hoc Ultra-Low Power Wireless Networking. *IEEE Computer*, vol. 33(7):pp. 42–48, 2000.

[Ram07] I. Ramachandran and S. Roy. Clear Channel Assessment in Energy-constrained Wideband Wireless Networks. *IEEE Wireless Communications Magazine*, vol. 14(3):pp. 70–78, 2007.

[Sah04] A. Sahai, N. Hoven, and R. Tandra. Some Fundamental Limits on Cognitive Radio. In *the 42nd Annual Allerton Conference on Communication, Control, and Computing*. Monticello, U.S.A, 2004.

[Sak03] I. Sakal and D. Simunic. Simulation of Interference Between Bluetooth and 802.11b System. In *the IEEE International Symposium on Electromagnetic Compatibility*, vol. 2, pp. 1321–1324. Istanbul, Turkey, 2003.

[Shi05] S. Shin, S. Choi, H. Park, and W. Kwon. Packet Error Rate Analysis of IEEE 802.15.4 Under IEEE 802.11b Interference. In *the the Third International Conference on Wired/Wireless Internet Communications (WWIC)*. Xanthi, Greece, 2005.

[Sie01] D. Siewiorek. Energy locality: processing/communication/interface tradeoffs to optimize energy in mobile systems. In *the IEEE Computer Society Annual Workshop on VLSI*. Orlando, USA, 2001.

[Sik05] A. Sikora. Coexistence of IEEE 802.15.4 with Other Systems in the 2.4 GHz-ISM-Band. In *the IEEE Instrumentation and Measurement Technology Conference*, vol. 3, pp. 1786–1791. Ottawa, Canada, 2005.

[So04] J. So and N. H. Vaidya. Multi-channel MAC for Ad Hoc Networks: Handling Multi-channel Hidden Terminals Using A Single Transceiver. In *the 5th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 222–233. Tokyo, Japan, 2004.

[Tam10] G. Tamilsevan and A. Shanmugam. Interference Cancellation and Performance Enhancement in Coexistent Heterogeneous Wireless Packet Networks using Packet Transmission Time Sharing. *IEEE Transactions on Vehicular Technology*, vol. 2(1):pp. 1793–8163, 2010.

[Vri03] P. D. Vries and A. Hassan. Spectrum Sharing Rules for New Unlicensed Bands. Web page, 2003. `http://www.wi-fi.org/files/kc_32_Spectrum%20Sharing%20Rules%20for%20New%20Unlicensed%20Brands.pdf`.

[Won05] C. Won, J. Youn, H. Ali, H. Sharif, and J. Deogun. Adaptive Radio Channel Allocation for Supporting the Coexistence of 802.15.4 and 802.11. In *the 62nd IEEE Vehicular Technology Conference (VTC2005-Fall)*. Dallas, U.S.A, 2005.

[Yua07] W. Yuan, X. Wang, and J. P. M. G. Linnartz. A Coexistence Model of IEEE 802.15.4 and IEEE 802.11b/g. In *the 14th IEEE Symposium on Communications and Vehicular Technology in the Benelux (SCVT'07)*, pp. 1–5. IEEE, Delft, The Netherlands, 2007.

[Yua09] W. Yuan, X. Wang, J. P. M. G. Linnartz, and I. G. M. M. Niemegeers. Experimental Validation of a Coexistence Model of IEEE 802.15.4 and IEEE 802.11b/g Networks. In *the 4th International Symposium on Innovations and Real-time Applications of Distributed Sensor Networks (IRA-DSN)*, pp. 17–22. Hangzhou, China, 2009.

[Yua10a] W. Yuan, X. Cui, and I. G. M. M. Niemegeers. Distributed Adaptive Interference-Avoidance Multi-channel Protocol for ZigBee Networks. In *the 10th IEEE International Conference on Computer and Information Technology (CIT)*. Bradford, UK, 2010.

[Yua10b] W. Yuan, J. P. M. G. Linnartz, and I. G. M. M. Niemegeers. Adaptive CCA for IEEE 802.15.4 Wireless Sensor Networks to Mitigate Interference. In *the IEEE Wireless Communications and Networking Conference (WCNC)*. Sydney, Australia, 2010.

[Yua10c] W. Yuan, X. Wang, J. P. M. G. Linnartz, and I. G. M. M. Niemegeers. Experimental Validation of a Coexistence Model of IEEE 802.15.4 and IEEE 802.11b/g Networks. *International Journal of Distributed Sensor Networks (IJDSN)*, 2010.

[Yua11] W. Yuan, X. Wang, J. P. M. G. Linnartz, and I. G. M. M. Niemegeers. Coexistence Performance of IEEE 802.15.4 Wireless Sensor Networks under IEEE 802.11b/g Interference. *Submitted to Spring Journal Wireless Personal Communication*, 2011.

[Zel98] E. Zelkha and B. Epstein. From Devices to Ambient Intelligence. In *the Digital Living Room Conference*. Laguna Niguel, USA, 1998.

[Zha06] Y. Zhang, H. Wu, Q. Zhang, and P. Zhang. Interference Mitigation for Coexistence of Heterogeneous Ultra-Wideband System.

EURASIP Journal on Wireless Communications and Networking, vol. 2006:pp. 1–13, 2006.

[Zho09] W. Zhou. *Design and Evaluation of a Hub-Assisted WLAN/Zigbee Coexistence Method*. M. sc, Eindhoven University of Technology, The Netherlands, 2009.

[Zig07a] ZigBee Alliance. *ZigBee and Wireless Radio Frequency Coexistence*, 2007.

[Zig07b] ZigBee Alliance. *ZigBee Enables Smart Buildings of the Future Today*, 2007.

[Zig07c] ZigBee Alliance. *ZigBee Specification 053474r17*, 2007.

[Zig09] ZigBee Alliance. *ZigBee RF4CE Specification 094945r00ZB*, 1.0 edn., 2009.

[Zig10] ZigBee Alliance. Mission Statement. Web page, 2010. `http://www.zigbee.org/About/OurMission/tabid/217/Default.aspx`.

Summary

As an emerging short-range wireless technology, IEEE 802.15.4/ZigBee Wireless Sensor Networks (WSNs) are increasingly used in the fields of home control, industrial control, consumer electronics, energy management, building automation, telecom services, personal healthcare, etc. IEEE 802.15.4/ZigBee WSNs share the same 2.4 GHz license-free Industrial, Scientific, and Medical (ISM) band with many other wireless systems such as IEEE 802.11b/g WLANs, Bluetooth, cordless phones, etc. Due to the low power, IEEE 802.15.4/ZigBee WSNs are potentially more vulnerable to interference by those systems. Among those systems, IEEE 802.11b/g WLANs are probably the most widely deployed ones. Because of their complementary applications, IEEE 802.15.4 WSNs and IEEE 802.11b/g WLANs are often colocated, which causes the coexistence issue between them. In this thesis, we focus on the coexistence between IEEE 802.15.4/ZigBee WSNs and IEEE 802.11b/g WLANs. The targets of this thesis work are to achieve a clear understanding on the coexistence issue between IEEE 802.15.4/ZigBee WSNs and IEEE 802.11b/g WLANs, and then to propose cost-effective methods to enhance the coexistence capability of IEEE 802.15.4/ZigBee WSNs.

Although many studies on the coexistence issue between IEEE 802.15.4/ZigBee WSNs and IEEE 802.11b/g WLANs have been done, the conclusions they drew are incomplete and/or conflicting, and therefore confusing. To get a clear understanding about the coexistence issue between them, an extensive study is needed. First, we propose a coexistence model of IEEE 802.15.4 nodes and IEEE 802.11b/g nodes. The model is based on two aspects, i.e., power and the timing. Due to the significant difference in transmit powers of IEEE 802.15.4 and IEEE 802.11b/g, the sensing ranges of them are quite asymmetric. As a result, three distinct coexistence regions can be identified. In each of these coexistence regions, IEEE 802.11 nodes and IEEE 802.15.4 nodes exhibit different interactive behavior and hence different coexistence performances, which may not be the same as we expected. For example, instinctively, we may feel that the closer an IEEE 802.15.4 node gets to an IEEE 802.11b/g interferer, the worse performance the IEEE 802.15.4 node would have. Our coexistence model, however, reveals that this perception is not true. In fact, as the IEEE 802.15.4 node and the IEEE 802.11b/g interferer get so close that they are in the coexistence region R_1, where they can sense each other, the coexistence performance of the IEEE 802.15.4 node

is not necessarily the worst. Instead, in the coexistence region R_2, where the IEEE 802.11b/g interferer cannot sense the IEEE 802.15.4 and therefore does not respect the IEEE 802.15.4 transmission, the coexistence performance of the IEEE 802.15.4 node could get even worse than in R_1. Clearly, the three coexistence regions and the different interactive behavior between IEEE 802.15.4 WSNs and IEEE 802.11b/g WLANs in each region explain the incomplete/conflicting conclusions drawn by many previous studies from their incomplete analysis and/or observations.

Next, by taking into account some important implementation factors, we improved the coexistence model and studied the coexistence performance of IEEE 802.15.4 WSNs under IEEE 802.11b/g interference in a real-life environment. We revealed that some implementation factors such as IEEE 802.15.4 Rx-to-Tx turnaround time and Clear Channel Assessment (CCA) partial detection effect can have significant impact on IEEE 802.15.4 WSNs coexistence performance in reality, e.g., a long IEEE 802.15.4 Rx-to-Tx turnaround time can impair the CCA performance and therefore the IEEE 802.15.4 WSNs coexistence performance. The enhanced model can precisely explain and predict the IEEE 802.15.4 WSNs coexistence performance. Furthermore, under the guidance of the model, the IEEE 802.15.4 WSNs coexistence performance were extensively investigated in all of the three coexistence regions in different scenarios by analysis, simulation and experiments. The simulation and experimental results agree with our analysis.

Based on the clear understanding achieved from the work above, we then explore the solutions to help IEEE 802.15.4 WSNs deal with interference. Basically, there are two categories for the ways of dealing with interference: interference control/mitigation and interference avoidance. We address solutions in each of these two categories, respectively. We first propose an interference mitigation approach, which enables an IEEE 802.15.4 WSN to mitigate heavy interference by adaptively adjusting CCA thresholds of its nodes in a distributed manner. As the heavy interference appears, the CCA thresholds are increased in order to reduce the inhibition loss, whereas the CCA threshold gets decreased so as to avoid having a permanent channel access privilege over peers as the interference disappears. Compared to the centralized interference management approaches, e.g., the frequency agility approach specified in the ZigBee specification, which inappropriately assumes a reliable two-way communication between nodes even in the presence of heavy interference, our adaptive CCA approach is simpler but more robust, more responsive, and easier to be implemented at a lower cost. The simulation results validate that the adaptive CCA approach may significantly improve IEEE 802.15.4 WSNs performance in the presence of heavy interference.

Then, we consider an interference avoidance solution. ZigBee specification proposes a feature called frequency agility, which refers to the ability of ZigBee networks to change the operational channel in the presence of interfer-

ence. However, for a large-scale ZigBee network, changing the whole network operational channel to an idle one, may be neither appropriate if there is only local interference nor possible if there is no single idle channel available globally. Therefore, we propose a distributed adaptive interference-avoidance multi-channel protocol, which enables a conventional single-channel large-scale ZigBee network to distributively, adaptively and partially change the operational channel in the presence of local interference. As a result, the ZigBee network performance under interference can be effectively and efficiently improved.

The main contributions of this thesis are a coexistence model of IEEE 802.15.4/ZigBee WSNs and IEEE 802.11b/g WLANs, and two solutions to the coexistence issue between them. The model not only explains the interesting interactive coexistence behavior of the two systems, but provides many insights on the coexistence issue. Under the guidance of those insights, two solutions are proposed. The solutions can enhance the coexistence capability of IEEE 802.15.4/ZigBee WSNs and therefore their coexistence performance in the presence of interference, which includes but not limited to IEEE 802.11b/g interference.

Samenvatting

Als opkomende korte afstand draadloze technologie wordt IEEE 802.15.4/ZigBee Wireless Sensor Networks (WSN's) in toenemende mate gebruikt in de gebieden van thuis controle, industriële controle, consumenten electronica, energie management, gebouwautomatisering, telecom diensten, persoonlijke gezondheidszorg, etc. Daar IEEE 802.15.4/ZigBee WSN's dezelfde 2.4 GHz licentievrije Industriële, Wetenschappelijke en Medische band deelt met vele andere draadloze systemen, zoals IEEE 802.11b/g WLAN's, Bluetooth, draadloze telefoons, etc. Vanwege het lage vermogen, zijn IEEE 802.15.4/ZigBee WSN's potentieel kwetsbaarder voor de interferentie door deze systemen. Van deze systemen is de IEEE 802.11b/g WLAN's waarschijnlijk de meest wijdverspreidde. Vanwege hun complementaire applicaties, worden IEEE 802.15.4/ZigBee WSN's en IEEE 802.11b/g WLAN's vaak gecoalloceerd, wat leidt tot coexistentie problematiek tussen beide systemen. In deze proefschrift, concentreren wij ons op de coexistentie tussen IEEE 802.15.4/ZigBee WSN's en IEEE 802.11b/g WLAN's. De doelstellingen van deze proefschrift werk zijn het bereiken van een duidelijk begrip van de coexistentie problematiek tussen IEEE 802.15.4/ZigBee WSN's en IEEE 802.11b/g WLAN's, en om vervolgens kost effectieve methoden, die de coexistentie capaciteit van de 802.15.4/ZigBee WSN's verhogen, te kunnen voorstellen.

Alhoewel er al veel onderzoek is verricht naar de coexistentie problematiek tussen de IEEE 802.15.4/ZigBee WSN's en IEEE 802.11b/g WLAN's, zijn de daaruit voortkomende conclusies vaak onvolledig en/of conflicterend, en daardoor verwarrend. Ten einde een duidelijk begrip te krijgen betreffende de coexistentie tussen beide systemen, is een diepgaand onderzoek vereist. Ten eerste stellen wij een coexistentie model voor van IEEE 802.15.4 nodes en IEEE 802.11b/g nodes. Het model is gebaseerd op twee aspecten: vermogen en tijdsverloop. Vanwege het significante verschil in transmissie vermogen tussen de IEEE 802.15.4 nodes en IEEE 802.11b/g nodes, is het sensor bereik van beide systemen behoorlijk assymetrisch. Als resultaat kunnen drie coexistentie gebieden geïndentificeerd worden. In elk van deze coexistentie gebieden IEEE 802.11 nodes en IEEE 802.15.4 nodes huist verschillend interactief gedrag en vandaar ook verschillende coexistentie prestaties, dat anders kan zijn dan we verwachtten. Bijvoorbeeld, zouden we instinctief kunnen denken dat hoe dichter een IEEE 802.15.4 node bij de IEEE 802.11b/g node interferentie komt, hoe slechter het prestatie vermogen van de IEEE 802.15.4

node. Ons coexistentie model laat echter zien dat deze perceptie niet klopt. Het is zelfs zo dat zodra een IEEE 802.15.4 node en de IEEE 802.11b/g interfererend zo dicht bij elkaar komen dat ze in coexistentie gebied R1 komen, daar waar de sensoren elkaars signalen oppikken, de coexistentie prestatie van de IEEE 802.15.4 node niet noodzakelijkerwijs het slechtste is. In plaats daarvan, in het coexistentie gebied R2, daar waar de IEEE 802.11b/g interfererend buiten het bereik van de sensor van de IEEE 802.15.4 blijft en daardoor de IEEE 802.15.4 transmissie niet respecteert, kan de coexistentie prestatie van de IEEE 802.15.4 node zelfs slechter worden dan in gebied R1. Heel duidelijk verklaren alle drie coexistentie gebieden en het zich onderscheidend interactieve gedrag tussen de IEEE 802.15.4 WSN's en de IEEE 802.11b/g WLAN's in ieder gebied, waarom incomplete/conflicterende conclusies zijn getrokken bij vele voorgaande onderzoeken vanuit incomplete analyses en/of observaties.

Vervolgens, door het rekening the houden met een aantal belangrijke implementatie factoren, hebben we het coexistentie model verbeterd en hebben de coexistentie prestaties van de IEEE 802.15.4 WSN's bestudeerd in een alledaagse omgeving. Wij ontdekten dat sommige implementatie factoren zoals de IEEE 802.15.4 Rx naar Tx doorlooptijd en Duidelijk Kanaal Toegankelijkheid (Clear Channel Assessment, (CCA)) gedeeltelijk detectie effect een significante impact kan hebben op de IEEE 802.15.4 WSN's coexistentie prestatie in de werkelijkheid, o.a., een lange IEEE 802.15.4 Rx naar Tx doorlooptijd kan nadelig zijn voor de CCA prestatie en daardoor ook voor de IEEE 802.15.4 WSN's coexistentie prestatie. Het verbeterde model kan de IEEE 802.15.4 WSN's coexistentie prestatie precies verklaren en voorspellen. Verder is, onder de begeleiding van het model, de IEEE 802.15.4 WSN's coexistentie prestatie nog uitgebreid onderzocht in alle drie coexistentie gebieden bij verschillende scenarios door middel van analyse, simulatie and experimenten. De simulatie en experimentele resultaten zijn in lijn met onze analyse.

Gebaseerd op het duidelijk beeld verschaft door dit onderzoek, zijn wij op zoek gegaan naar oplossingen die IEEE 802.15.4 WSN's helpen met interferentie. Feitelijk zijn er twee categorieën om met interferentie om te gaan: interferentie controle/vermindering en interferentie vermijding. Wij zullen oplossingen aandragen voor ieder van deze twee cateogorien, respectievelijk. Allereerst stellen wij een interferentie vermindering benadering voor, die IEEE 802.15.4 WSN in staat stelt zware interferentie te verminderen door adaptief bijstellen van de CCA drempel van de nodes op een gespreide manier. Zodra de zware interferentie zich voordoet, zullen de CCA drempel verhoogd worden ten einde het remmings verlies te reduceren; de CCA drempels worden daarentegen verlaagd om te voorkomen dat een blijvend kanaal toegangs voorkeur, boven collega's zal ontstaan, zodra de interferentie verdwijnt. Vergeleken met de gecentraliseerde interferentie management benaderingen, o.a. de frequentie behendigheids benadering, zoals gespecificeerd in de ZigBee specificatie, dat onterecht aanneemt dat een betrouwbare tweewegs communicatie tussen nodes zelf in de aanwezigheid van zware interferentie plaats kan vinden, is onze aanpasbare CCA benadering eenvoudiger, maar tegelijkertijd meer robuust, meer ontvankelijk, en makkelijker te implementeren tegen lagere kosten. De simulatie resultaten bevestigen dat de adaptief CCA benadering mogelijk de 802.15.4 WSN's prestatie significant verbeterd, bij aanwezigheid van zware interferentie.

Vervolgens nemen we de interfentie vermijdings oplossing in aanschouw. De ZigBee specificatie stelt een toepassing voor genaamd frequentie behendigheid, wat refereert aan de capaciteit van ZigBee netwerken om het operationele kanaal te veranderen bij aanwezigheid van interferentie. Alhoewel voor een grote schaal ZigBee netwerk, het veranderen van het gehele netwerk kanaal naar een inactieve, mogelijk ongewenst kan zijn in het geval van alleen locale interferentie; ook is het mogelijk dat er geen enkelvoudig inactief kanaal beschikbaar is op globaal niveau. Derhalve stellen wij een gespreid aanpasbaar interferentie vermijdend multi kanaal protocol voor, dat een conventioneel enkelvoudig kanaal grote schaal ZigBee netwerk in staat stelt om verdeling, aanpassing en gedeeltelijke verandering van het operationele kanaal, bij aanwezigheid van locale interferentie toe te passen. Als resultaat kan de ZigBee netwerk prestatie gedurende interferentie effectief en efficient worden verbeterd.

De hoofd bijdragen van deze proefschrift zijn een coexistentie model van IEEE 802.15.4/ZigBee WSN's en IEEE 802.11b/g WLAN's, en twee oplossingen voor de het coexistentie probleem tussen beiden. Het model verklaard niet alleen het interesante interactieve coexistentie gedrag van beide systemen, maar verschaft tevens vele inzichten betreffende het coexistentie probleem. Op basis van deze inzichten, worden twee oplossing voorgedragen. De oplossingen kunnen de coexistentie capaciteit verbeteren van IEEE 802.15.4/ZigBee WSN's en daardoor ook de coexistentie prestatie bij aanwezigheid van interferentie, waaronder, maar niet gelimiteerd tot, IEEE 802.11b/g interferentie.

Curriculum Vitae

Personalia

Full Name	Wei Yuan
Date of Birth	16 January, 1975
Place of Birth	Baiyin, China
Gender	Male

Profile

Wei Yuan received an M.Sc. degree in Telecommunication Engineering from Xi'an Jiaotong University, Xi'an, China, and an M.Sc. degree in Electrical Engineering from University of Twente, Enschede, The Netherlands, in 2000 and 2005, respectively.

From 2006 to 2010, he was with Connectivity System and Networks Group (now Distributed Sensor System Group), Philips Research in Eindhoven, as a Research Scientist. Meanwhile, he was also working towards a Ph.D. degree on the subject of wireless sensor networks in Wireless and Mobile Communications group in Delft University of Technology, Delft, The Netherlands.

Since 2010, he is with ZTE The Netherlands B.V., The Hague, The Netherlands.

Journal Publications

[Yua10c] W. Yuan, X. Wang, J. P. M. G. Linnartz and I. G. M. M. Niemegeers *Experimental Validation of a Coexistence Model of IEEE 802.15.4 and IEEE 802.11b/g Networks.* International Journal of Distributed Sensor Networks (IJDSN), vol. 2010, Article ID 581081

[Yua11] W. Yuan, X. Wang, J. P. M. G. Linnartz and I. G. M. M. Niemegeers *Coexistence Performance of IEEE 802.15.4 Wireless Sensor Networks under IEEE 802.11b/g Interference.* Submitted to Spring Journal Wireless Personal Communication, 2011.

Conference Publications[1]

[Yua07] W. Yuan, X. Wang, and J. P. M. G. Linnartz. A Coexistence Model of IEEE 802.15.4 and IEEE 802.11b/g. In *the 14th IEEE Symposium on Communications and Vehicular Technology in the Benelux (SCVT'07)*, pp. 1–5. IEEE, Delft, The Netherlands, 2007.

[Yua09] W. Yuan, X. Wang, J. P. M. G. Linnartz and I. G. M. M. Niemegeers. Experimental Validation of a Coexistence Model of IEEE 802.15.4 and IEEE 802.11b/g Networks. In *the 4th International Symposium on Innovations and Real-time Applications of Distributed Sensor Networks (IRA-DSN)*, pp. 17–22. Hangzhou, China, 2009.

[Yua10b] W. Yuan, J. P. M. G. Linnartz and I. G. M. M. Niemegeers. Adaptive CCA for IEEE 802.15.4 Wireless Sensor Networks to Mitigate Interference. In *the IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–5. Sydney, Australia, 2010.

[Yua10a] W. Yuan, X. Cui and I. G. M. M. Niemegeers. Distributed Adaptive Interference-Avoidance Multi-Channel Protocol for ZigBee Networks. In *the 10th IEEE International Conference on Computer and Information Technology (CIT)*, pp. 1–5. Bradford, UK, 2010.

Patents

- B. Erdmann, A. M. M. Lelkens, L. M. G. M. Tolhuizen and W. Yuan, "Method for Controlling Transmissions from a Resource-restricted Device, and Batteryless Device", WO/2010/128422, 11 November 2010
- W. Yuan, L. M. G. M. Tolhuizen, B. Erdmann and S. Schlumbohm, "Single point of failure (SPOF) prevention for batteryless devices", filing in progress, November 2010
- B. Erdmann, L. M. G. M. Tolhuizen and W. Yuan, "Multicast-based proxy redundancy feature for resource-restricted devices", filing in progress, November 2010

Other Academic Achievements

- Participated in the research projects: Personal Networking Pilot 2008 (PNP2008)
- Participated in ZigBee Green Power Device and Application Standardization and achieved three patents
- Supervised an M.Sc. student, Xiaolei Cui, in his master thesis work: "Improving ZigBee Network Robustness with Multi-channel Capability" (Completed August 2009)

[1] All conference papers were selected for oral presentations.