Aalto University

School of Science

Degree Programme of Computer Science and Engineering

Shichao Dong

Inter- and Cross-protocol Interference in IEEE 802.15.4 Wireless Sensor Network Data Communications

Master's Thesis

Espoo, June 28, 2013

Supervisor: Professor Antti Ylä-Jääski, Aalto University

Instructor: Vilen Looga M.Sc. (Tech.), Aalto University

Zhonghong Ou Post-doc researcher, Aalto University

Aalto University
School of Science

Aalto University
School of Science
Degree Programme of Computer Science and Engineering

ABSTRACT OF
MASTER'S THESIS

Author:	Shichao Dong		
Title:	Inter- and Cross-protocol Interference in IEEE 802.15.4 Wireless Sensor Network Data Communications		
Date:	June 28, 2013	**Pages:**	61
Professorship:	Data Communications Software	**Code:**	T-110
Supervisor:	Professor Antti Ylä-Jääski, Aalto University		
Instructor:	Vilen Looga M.Sc. (Tech.), Aalto University Zhonghong Ou Post-doc researcher, Aalto University		

Interference on wireless sensor networks is a persistent challenge, especially when IEEE 802.15.4 operates in the 2.4 GHz frequency band which has already been crowded by various other wireless technologies, such as IEEE 802.11b/g (WLAN), IEEE 802.15.1 (Bluetooth), ZigBee and proprietary equipments. To maintain or even improve the wireless network performance, the estimation of wireless link quality is necessary. Our work in this thesis is prior to this estimation. We quantified both inter- and cross-protocol interferences by conducting various environments under different conditions. Our results not only offer valuable statistics about how IEEE 802.15.4 data communication can be impacted, but also provide fundamentals for implementing a WiFi interference model in simulators, for instance Cooja.

Keywords:	IEEE 802.15.4, Internet of things, WiFi, Bluetooth, Interference
Language:	English

Acknowledgements

I am particularly grateful to my supervisor Prof. Antti Ylä-Jääski for supervising my thesis. Also I feel lucky to have Vilen Looga and Zhonghong Ou as my instructors. They are duteous and knowledgeable. I benefit a lot from the discussions with them. Without their patient assistance and valuable advice, my thesis would not be this smooth and completed in time.

I would also like to thank Yang Deng, Jiang Dong for their kind and generous help. They gave me a lot of great suggestions during my experiments and thesis presentation.

Finally I would like to thank my parents who supported me to go abroad to enrich my vision and explore new things.

Espoo, June 28, 2013

Shichao Dong

Abbreviations and Acronyms

AFH	Adaptive Frequency Hopping
CANC	cooperative analog network coding
CRC	Cyclic Redundancy Check
DSSS	Direct Sequence Spread Spectrum
FHSS	Frequency Hopping Spread Spectrum
IoT	Internet of Things
ISM	Industrial, Scientific and Medical
LQI	Link Quality Indicator
LR_WPAN	Low-rate Wireless Personal Area Network
MAC	Media Access Control sub-layer
O-QPSK	Orthogonal Quadrature Phase Shift
OS	Operating System
PAN	Personal Area Network
PDR	Packet Drop Ratio
PHR	PHY header
PHY	Physical layer
POS	Personal Operating Space
PRR	Packet Reception Ratio

RF	Radio Frequency
RSSI	Received Signal Strength Indicator
SFD	Start of Frame Delimiter
SHR	Synchronization Header
WBAN	Wireless Body Area Network
WBSN	Wireless Body Sensor Network
WLAN	Wireless Local Area Network
WSN	Wireless Sensor Network

Contents

Chapter 1

Introduction

1.1 Motivation

Due to the unregulated nature and world wide access of the 2.4 GHz Industrial, Scientific and Medical (ISM) frequency band, it has gotten more preferable and popular among many wireless technologies, e.g., IEEE 802.11 Wireless Lan (WLAN), IEEE 802.15.1 (Bluetooth), ZigBee and other devices, for instance, microwave oven, proprietary equipments,etc. We are living in an environment which is flooded by radio signals. There are many wireless networks around to serve us the Internet access. It is very hard to find a free frequency band where we can deploy new wireless technologies without any interference. 2.4 GHz frequency band has already been very crowded, each wireless technology in this free 2.4 GHz frequency band can get easily interfered by another. Even though each wireless technology has been designed and improved in such a way to enhance their resistance to the interference from inter- and cross- protocols and co-existence with those wireless tech-

nologies in a small area, interference still occurs. Problems arise when there are more than one wireless technologies running in the 2.4 GHz frequency band in an area.

In this thesis, we concentrate our research focus on the Wireless Sensor Network (WSN) – network of wirelessly connected sensors. IEEE 802.15.4 is a wireless protocol which is designed for such WSNs. It features low data rate, low power consumption and low cost, and serves as the Media Access Control sub-layer (MAC) and Physical (PHY) layer of protocol stack in small sensors, which are also known as motes. These small motes compose WSNs are usually used in the Internet of Things (IoT). When such WSNs are deployed in working environment or campus buildings which are typical places where Wireless Local Area Network (WLAN), Bluetooth data traffic and Microwave ovens usually operate, IEEE 802.15.4 data communication from these small motes faces a possiblity to get interfered. To maintain or even improve the wireless network performance, wireless link quality estimation is necessary. This potential interference has drawn our attention and makes us want to see the interference imposed on the IEEE 802.15.4 data communication in a statistical way rather than just conceptually knowing that WLAN, Bluetooth and Microwave ovens might damage packet delivery in WSNs.

1.2 Problem statement

In this thesis, we strive to provide the answers to the following questions such that we can understand how the inter- and cross-protocols impose interference on IEEE 802.15.4 peer to peer network when they co-exist in an area.

- How the IEEE 802.15.4 data communication would be impacted when Microwave ovens are operating nearby ?
- How the packet delivery in the IEEE 802.15.4 network is impacted by Bluetooth data traffic ?
- How the IEEE 802.15.4 network is impacted by WLAN network ?

  IEEE 802.15.4 support two network topologies, peer to peer and star networks. Throughout our experiments in this thesis, we focus on the peer to peer topology.

1.3 Contributions

Main contribution of this thesis work is that we conducted various experiments under different conditions to quantify the interference on IEEE 802.15.4 data communications from both inter- and cross-protocols, e.g., interference from IEEE 802.15.4 data networks and from WLAN, Bluetooth and possible equipments, for instance, microwave ovens. Our experimental results offer valuable data for not only statistically giving an introduction of how WLAN, Bluetooth and microwave impact on the packet delivery of the IEEE 802.15.4 data communications, also providing the fundamental data for implementing interference model, e.g., WLAN interference mode, in some simulators, such as the Cooja simulator shipped with the Contiki Operating System (OS).

1.4 Structure of the thesis

The thesis is structured as follows. In Chapter 2, we give the related background knowledge, e.g., IEEE 802.15.4 protocol introduction, potential wireless interference on IEEE 802.15.4 network. Chapter 3 states the current research status of interference on wireless sensor networks. We detail our experimental designs which includes both inter- and cross-protocol interference experimental designs in Chapter 4. Chapter 5 introduces two different application implementations for two scenarios. In Chapter 6, we discussed the experimental results for inter- and cross-protocol interferences. We concluded this thesis in Chapter 7.

Chapter 2

Background

2.1 IEEE 802.15.4

IEEE 802.15.4 [16] is targeted for Low-Rate Wireless Personal Area Networks (LR-WPAN). It attempts to offer a low data rate, low power and low cost solution in terms of wireless networking on the device level communication. At the same time, it eases the deployment by embracing the scalability and reliability thinking when defining the specifications.

IEEE 802.15.4 defines the PHY layer and MAC sub-layer specifications for low data and low power wireless communication among relatively small and simple devices called motes, which typically function in the Personal Operating Space (POS) of around 10 meters or less. As the ubiquitous computing concept gets more and more popular, personal and business domains have been densely populated with sensors. One class of applications which directly results from IEEE 802.15.4 protocol is the wireless sensor networks for monitoring and controlling applications. Examples include interest in

the technical adaptation to operate in and around human body, potential applications like medical sensing control, wearable computing and location identification based on Wireless Body Area Networks (WBANs). All of these applications apply the protocol of IEEE 802.15.4 into the real world [12].

IEEE 802.15.4 standard operates at three bands, 2.4 GHz, 868 and 912 MHz with the data rate from 250kbps, 20kbps and 40kbps respectively. There are 16 channels in the 2.4 GHz ISM band, 10 channels in the 915 MHz band and only one channel in the 868 MHz band. In the 2.4 GHz ISM band, 16 channels are configured with 2 MHz width with 3 MHz inter channel gap. According to the standard, outgoing bytes are split into two 4-bit symbols. Each symbol is mapped to one of 16 pseudo-random, 32-chip sequences. The radio encodes these chip sequences using orthogonal quadrature phase shift keying (O-QPSK) and transmits them at 2 Mchips/s (i.e. 250kbps). The center frequency of each channel is determined by the following formula:

$$Fc = 2405 + 5(k - 11)(MHz), k = 11, 12..26 \tag{2.1}$$

Figure 2.1 indicates the packet format of IEEE 802.15.4 standard. The Synchronization Header (SHR) and the PHY Header (PHR) are included in this packet format. The SHR consists of 4 byte preamble, which is set to 0x00 and 1 byte Start of Frame Delimiter (SFD), which is set to 0x7A. The PHR includes a 1 byte Length field which indicates the number of bytes in the packet's payload, including 2 byte cyclic redundancy check (CRC). The maximum packet size is 133 bytes, including all the headers.

The MAC protocol in IEEE 802.15.4 standard defines both beacon-enabled and non-beacon modes. Since we use the Contiki OS [4] throughout our re-

search and Contiki OS only implements the non-beacon mode, we exclude the description of beacon-enabled mode mechanism of IEEE 802.15.4. In the non-beacon mode, the standard utilizes a CSMA/CA protocol. The CSMA/CA protocol uses binary exponential back-off. In fact, Contiki MAC layer capitalizes on a linear back-off where there is a time base calculated based on the channel check interval of the underlying radio duty cycling layer. The maximum number of backoffs in Contiki MAC layer is set to 3 by default. The receiving 802.15.4 radio first synchronizes to the incoming zero symbols and searches for the SFD sequence to the incoming packets. Interference and noise from inter-network and cross-network might corrupt the incoming chip stream, which can result in 32 chip sequences that do not match one of the 16 valid sequences. After successful synchronization and location of the SFD, receiving radio maps the input sequence to the valid sequence with the smallest Hamming distance.

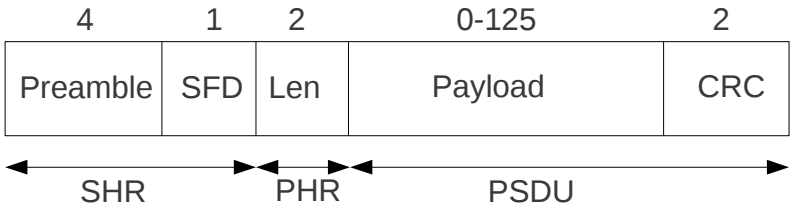

Figure 2.1: Format of a 802.15.4 packet with field size in bytes

2.2 Wireless interference classification

The industrial, scientific and medical(ISM) radio bands, also known as 2.4 GHz frequency, are purposely reserved radio frequencies for industrial, scientific and medical researches. These radio bands can be used without any licence. As a result, many wireless technologies such as Bluetooth, IEEE 802.11 devices all operate in the 2.4 GHz ISM band. Since IEEE 802.15.4 also has 16 channels in the 2.4 GHz ISM band, it is necessary to measure the impact on the communication of IEEE 802.15.4-enabled devices from other wireless technologies. In our experiments, we mainly focus on three possible interference sources, which are Microwave Oven, Bluetooth and WiFi respectively.

2.2.1 Microwave Oven

Microwave ovens , a common kitchen appliance, run at about 2.4 GHz frequency band to cook food by dielectric heating. Most microwave ovens have a central frequency of 2.45 GHz [24]. Ideally, it should be put into a Faraday cage. But as the door gets loose, it is possible for some radios to leak out of the Oven. This makes the Microwave Oven a potential interference source for Low-Rate Wireless Personal Area Network(LR-WPANs).

2.2.2 Bluetooth

The IEEE 802.15.1 Bluetooth standard [15] divides the 2.4 GHz ISM band into 79 channels with channel numbers from 0 to 78. Each channel has a bandwidth of 1 MHz with a channel separation of 1 MHz. Center frequency

of each channel is determined by the following formula:

$$f = 2420 + k(MHz), k = 0..78 \tag{2.2}$$

Bluetooth output power is usually lower than 4 dBm for commonly class 2 devices such as wireless headsets and keyboards. Transmission range in this case is normaly 10 meters. Less common class 1 devices can consume up to 20 dBm power and transmission range increases up to 100 meters.

The transmission scheme utilized in Bluetooth is Frequency Hopping Spread Spectrum (FHSS). FHSS spreads the signal power throughout the entire band by frequently changing the transmit channel frequency in a predefined channel hopping sequence. Both transmitter and receiver must sit on the same channel frequency such that the receiver can receive the data from the transmitter. Bluetooth hopping rate is 1600 hops/s (625 us between two consecutive hops).

2.2.3 WLAN

The IEEE 802.11b/g Wireless LAN (WLAN) [17] also operates in the 2.4 GHz with a total number of 14 channels. Channels are numbered from 1 to 14 with 22 MHz channel width and 5 MHz channel separation. Usually the output power of WLAN is around 20 dBm with a 100 meter transmit range. The transmit scheme utilized by IEEE 802.11b is Direct Sequence Spread Spectrum (DSSS). DSSS is a modulation technique. It utilizes a pseudo-random sequence of 1 and -1 values to multiply with the transmitted data such that resulting signals occupy a much higher frequency than that of the original signal. This modulation technique can help reduce the interference of

the data being transmitted by other noise. 802.11b can provide a data rate up to 11 Mbit/s. The IEEE 802.11g is backwards compatible with IEEE 802.11 b. 802.11 g achieves a maximum physical layer bit rate of 54 Mbit/s by implementing an additional OFDM transmission scheme. Figure 2.2 [20] illustrates the channel allocation of IEEE 802.11 and IEEE 802.15.4 in the 2.4 GHz frequency band. Usually in the WLAN environment, channel 1, 6 and 11 are recommended channels to be used when routers are set up to provide Internet access service because there three channels do not overlap with each other. If only channel 1, 6 and 11 are configured as the WiFi data communication channels, free IEEE 802.15.4 channels in the 2.4 GHz frequency band are 15, 20, 25 and 26. All the rest IEEE 802.15.4 channels are partly overlapped with the WiFi channels. But as Internet coverage through WLAN get bigger and bigger, during a small area, e.g. school building, shopping mall, there are multiple hot spots which are configured to offer Internet access services. In this case, often all channels might be used and IEEE 802.15.4 can only utilize the channel 25 or 26 to conduct the data communication between motes such that there is no interference coming from the WiFi environment.

Since IEEE 802.11 sender output power can be as much as 100 times than that of IEEE 802.15.4 sender, WiFi network can be a very serious potential interferer of the IEEE 802.15.4 wireless network consisting of small motes powered by small batteries.

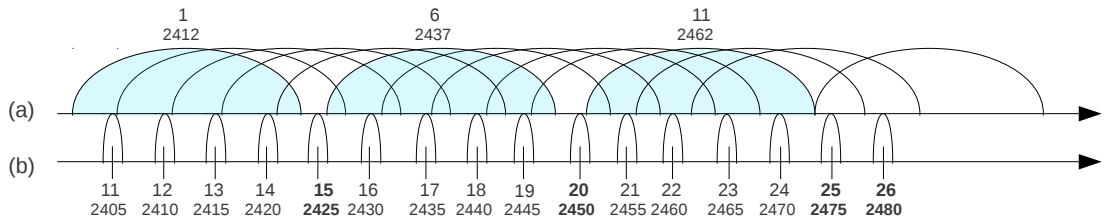

Figure 2.2: Usage of the 2.4 GHz ISM frequency band: (a) IEEE 802.11 (b) IEEE 802.15.4 [20]

Chapter 3

Related work

3.1 Wireless link quality estimation

Wireless link quality estimation plays a significant role in wireless sensor network design and functioning. It not only can affect the the network performance, but also the design of the up-layer protocols. An extensive amount of research has been done to estimate the wireless link quality such that better network performance, e.g. higher successful ratio of packet sending and receiving, could be achieved.

In wireless sensor networks, there are three well-known factors which account for most of the wireless link quality degradation [8]. The first one is the environment. Different environment can cause multipath propagation effects to different extent, which will decrease and weaken the transferring signal power. Also this multipath phenomena contribute to the background noise. The second factor is the interference. The interference can come from the transmission of multiple data connections at the same time in the

same IEEE 802.15.4 network. Also interference can be resulted from other wireless technologies residing in the same area, e.g. WiFi, Bluetooth, microwave oven and cordless phones. The third factor is hardware transceivers. Hardware transceivers after a long time usage might get old and distort the internal sending and receiving signals. In wireless sensor networks, the radio transceivers send out low-power radiated signals, which are very prone to the surrounding noise, interference and multipath distortions. Thus, estimating the link quality has been a very necessary function.

Common used metrics [8] for estimating wireless link qualities are as follows:

– PRR (Packet Reception Ratio). PRR is computed as the number of successfully received packets to the number of transmitted packets. Another similar metric is called PDR, which is short for Packet Drop Ratio. PDR is computed as the 1 - PRR.

– RSSI (Received Signal Strength Indicator). Most of current radios e.g., the CC2420 are shipped with a RSSI register. This register gives the signal strength of the received packet. When there is no transmission going on, this register provides the background noise level.

– LQI (Link Quality Indicator). This metric for wireless link quality is proposed in the IEEE 802.15.4 standard (IEEE 802.15.4 standard 2003). But how this value would be evaluated is dependent on the vendor of radios. For the most widely used CC2420 radio transceiver, LQI is measured based on the first eight symbols of the received packet with the value ranging from 50 to 110. The higher value this LQI is, the better quality the link has.

3.2 Coexistence of 802.15.4 with other wireless technologies

3.2.1 Identification of interference

Emanuele Toscano et al [27] observed that cross channel interference exists in IEEE 802.15.4 network. Based on the IEEE 802.15.4 standard, each channel in IEEE 802.15.4 has a 2 MHz width with 3 MHz inter channel gap. When there is transmission going on one channel, there should not be interference coming from the adjacent channels from the theoretical perspective. With Fc as the center frequency of one channel, the resulting signal should not contribute on frequencies outside the [Fc - 1, Fc + 1] interval. As a matter of fact, such a signal is hard to be obtained due to the lack of an ideal filter. How much further the practical signal is away from the ideal one is heavily dependent on the quality of the hardware components utilized by the producer of the transceiver. Toscano conducted experiments on the relationship between RSSI and distance, PDR and distance to the interferer, RSSI and distance to the interferer. The results from [27] showed that RSSI stays quite stable when such a cross channel interference occurs. The increase in the PDR depends on the power and frequency of transmissions that can result in cross channel interference. As long as interfering node's output power is comparable with that of source node, transmission gets affected slightly (4.5% worst case PDR with equidistant nodes). But when interfering signal is much stronger than the valid signal from source node or the source node is too far away from the destination node compared with the interferer

node, packet loss increases considerably if unacknowledged communication is utilized together with the high duty-cycle transmissions.

Sven et al [31] utilized IEEE 802.15.4 compatible radio chip - CC2420 to obtain a series of Received Signal Strength Indication (RSSI) and used this RSSI values to classify sources of interference e.g., Bluetooth, WLAN and Microwave ovens. In their work, RSSI sampling occurs only on one channel instead of all channels recommended by the ZigBee standard. This enables the WSN nodes to stay connected to the network. The process of classifying external sources of interference consists of three steps: a) sampling, which happens every one second. b) feature extraction based on the classification conditions. c) classification decision. The algorithm proposed by [31] returns the only one main source of interference.

Hermans et al [13] conducted extensive experiments and characterize how different types of interferers can affect the individual IEEE 802.15.4 packets. They based on their observations from the experimental results and defined a set of features to describe various sources of interference. They utilized this set of features to train a neural network to classify the source of interference of a corrupted packet. They claimed their solution is sufficiently lightweight for online use in resource limited sensor motes. Their approach offers a mean classification accuracy of 79.8%, with per interferer accuracies of 64.9% for WiFi, 82.6% for Bluetooth, 72.1% for Microwave oven, and 99.6% for packets corrupted due to insufficient signal strength.

Rahul et al [25] proposed an approach to detecting the interference on IEEE 802.15.4 networks from other co-existing IEEE 802.15.4 networks. They experimented on networks consist of a coordinator node and several

sensor nodes. Their solution is based on two assumptions: a) the coordinator in a network is less resource constrained than sensors. Thus, more work is carried out on the coordinator node. b) each network has a unique Personal Area Network (PAN) ID as stated in the IEEE 802.15.4 standard. Their approach constitutes two steps: interference detection and interference mitigation. Both steps take place on coordinators only. Two interfering networks negotiate via coordinators of each which network should switch to another free channel. Interference happens when one coordinator of a PAN receives packets from other PANs. As to mitigation, the interference mitigation protocol defines a set of rules to assign priorities among interfering netowrks: a) The PAN with a lower rate of interference gets higher priority and stays in the same channel, b) if two PANs have the same priorities, the one with lower PAN ID remains in the same channel.

Bloessl et al [9] presented an extended Spectrum Analysis Framework for Interferer Classification (SaFIC), which is a sensor mote based spectrum analysis framework for the 2.4 GHz ISM band. This framework measures the RSSI in a predefined spectrum and visually displays the signal strengths and their corresponding frequencies in real time. The authors defined a job description language which allows arbitrary combinations of loops, delays and multiple scans within one measurement job.

Noda et al [23] proposed a new channel quality metric based on the fine-grained availability of the channel over time. The metric ranks channels with larger inactive periods or vacancies in a more favourable way. They collected real world interference traces in the 2.4 GHz ISM band. The analysis of the interference data had shown a strong correlation between their new channel

quality metric and the PRR. They discussed that their channel quality metric can be useful in the dynamic resource allocation techniques for interference aware protocols.

3.2.2 Avoidance of interference

Chieh-Jan et al [20] proposed a framework called Buzzbuzz which utilized multi-headers to provide header redundancy such that IEEE 802.15.4 node can have multiple opportunities to detect incoming packets in an area where WiFi co-exists. They claimed that in a medium-sized test-bed, Buzzbuzz can improve the network delivery rate by 70% and reduce the packet retransmission by a factor of three, which increases the WiFi throughput by 10%. Yeonsik et al [18] proposed a interference mitigation solution which relies on adaptive aggregation of packets and adaptive transmission scheduling. De Francesco et al [11] introduced a receiver-oriented scheduling algorithm for cluster-tree WSNs which offers a bounded latency for convergecast data collection. They claimed their algorithm can effectively reduce the interference among clusters when clusters send data to root. Tiancheng et al [21] utilized the topology control to minimize the interference in the WSNs. They proposed a fast polynomial exact algorithm for one-dimensional networks and proved that the maximum interference can be bounded while minimizing the average interference. The bound is only related to the distance between nodes rather than the network size. Yanli et al [29] studied the cooperative analog network coding (CANC) technique and proposed an optimal algorithm called S-CANC which combines the source node selection and CANC to minimize the interference caused by WSNs. Through simulation results, their proposed

algorithm behaved better than the cooperation. Huang et al [14] presented an energy-aware interference -sensitive geographic routing (EIGR) protocol which emphasizes on minimizing the total network energy consumption and reducing interference. This EIGR selects the minimum-interference link from energy-optimal relay region by adaptively using an anchor list to navigate data delivery. Zijian et al [28] proposed a novel interference aware multipath routing (IAMR) protocol for WSNs. Without any hardware support, this IAMR can establish minimum-interference paths in a simple and efficient way. Cao et al [10] investigated and analysed the impact of inter-user interference on PDR and throughput. They proposed a light-weight hopping approach based on practical Wireless Body Sensor Network (WBSN) systems. Their experimental results showed effectiveness of their hopping idea for inter-user interference mitigation, which is based on CSMA/CA mode and with low complexity. Kumar et al [19] proposed an algorithm named Energy Efficient Scheduling (EES) to reduce state transitions of radio in sensor node thereby reducing the energy consumption. Also their EES protocol focuses on reducing co-channel interference and efficiently bandwidth usage. Lu et al [22] adopted probability theory and extended the existed interference model. They provided an interference analysis model and implementation of this model in cross-layer method. They proposed a probabilistic routing algorithm and their simulation results showed with new algorithm better packet delivery ratio was achieved. Dingwen et al [30] introduced an adaptive and distributed channel hopping scheme. This new hopping scheme was built on lightweight yet accurate metric which describes the interference. Their experimentation indicated accurate modelling of real-world conditions by their

hopping scheme, which also offered a very fast response time to adapt the network to interference. Grassl et al [12] introduced a BAN-BAN interference Reduction System (B2IRS). Instead of switching channels, this system rescheduled beacon packets in order to avoid active period overlap whereby interferences between distinct BANs were reduced.

Chapter 4

Experimental environment

4.1 Experimental configuration

4.1.1 Hardware

Zolertia motes Z1 as shown in Figure 4.1 low-power wireless module are utilized through our experiments. The Z1 module is a general purpose development platform for WSNs [7]. The core architecture of Z1 wireless module is based on the MSP430 + CC2420 [3] family of micro-controllers and radio transceivers by Texas Instruments. Core features of Z1 mote used in experiments are as follows:

- industrial-grade temperature range (-40 °C - 85 °C)
- 52-pin expansion connector
- 2nd generation MSP430 ultra-low power 16-bit MCU 16MHz
- 2.4 GHz IEEE 802.15.4, 6LowPAN compliant and ZigBee ready

- 3-Axis, ±2/4/8/16 g digital accelerometer
- Low-power digital temperature sensor with ± 0.5 °C accuracy (in -25 °C - 85 °C range)
- Micro-USB connector for power and debugging
- 5dBi RP-SMA antenna (frequency: 2.4 GHz, antenna type: right angle, termination: RP-SMA)

Figure 4.1: Zolertia Z1 mote

Air Station TURBO G (module: WHR-G54S) [2] is the router used. Major specifications are as follows:

- Standard Compliance : IEEE 802.11b/IEEE 802.11g
- Frequency Range(MHz) : 2.412 - 2.462

- Access Mode : Infrastructure mode
- Power Supply : External, AC 100-240V 50/60 Hz
- Antenna : 1(external)

4.1.2 Contiki OS

Contiki OS [4] is the operating systems running on the Z1 motes in our experiments. Contiki is an open source operating system specifically designed for small, battery powered devices to communicate with the Internet. It supports fully standard IPv4, IPv6, 6LoWPAN, RPL [6], CoAP. In our experiments, we made use of two Z1 motes to consist of a peer to peer network using UDP on the transportation layer and IPv6 on the IP layer. 6LoWPAN [1] is used to compress the packet headers of IEEE 802.15.4, IPv6 and UDP. The protocol stack of Contiki OS in our experiments is depicted in table 4.1:

Table 4.1: Protocol stack in Contiki OS

Application Layer	Application
Transport Layer	UDP
Network Layer	IPv6 with LoWPAN
Data Link Layer	IEEE 802.15.4 MAC
Physical Layer	IEEE 802.15.4 PHY

The network configuration of Contiki operating system in our experiments is shown in table 4.2.

The CC2420 radio transceiver provides programmable RF output power. Table 4.3 shows the eight different output power level offered by CC2420.

Table 4.2: Configuration of Contiki OS

Network driver	Sicslowpan
MAC driver	CSMA unslotted
RDC driver	nullrdc
Radio driver	CC2420
Frame format	IEEE 802.15.4 frame format
Channel selection	by default 26
DLL buffer size	4
# of frame retransmission	3
Mote power level	by default 31

4.2 Experimental framework

4.2.1 Influential factors of wireless link quality

All the experiments conducted are in the corridor along the office side in the school building at midnight such that no extra interference, e.g., people movements, extra usage of Aalto open WiFi in the daytime, interferes with our experiments. The traffic which serves as background noise in the corridor at midnight when no one uses Aalto Open free WiFi is 526 bytes per second.

Throughout all the experiments, we utilized a pair of Z1 motes as the testing pair. One laptop was used for each Z1 mote such that packet sending and receiving information can be logged into files on the laptop and seen via the terminal. We implement two versions of applications denoted as V1 and

Table 4.3: Output power settings of CC2420 at 2.4 GHz

PA_LEVEL	Output Power (dBm)
31	0
27	-1
23	-3
19	-5
15	-7
11	-10
7	-15
3	-25

V2 which run on the Contiki operating system. In V1, IP packets are sent to the data link layer frame buffer each 0.2 seconds no matter if previous frame has been ACKed or not. In V2, each IP packet is sent to the data link layer, added with frame header and then sent to the receiver. If one frame is ACKed by the receiver side, then one ACK event would be sent from data link layer to the IP layer and notifies the application to send the next packet to the data link layer.

4.2.1.1 RSSI v.s distance

This experiment is to find out the impact of the distance of two Z1 motes on RSSI of received packets on receiver side. RSSI values are usually provided by current radios, e.g., CC2420. Measuring the RSSI values can be a straight-forward and energy efficient way to estimate the wireless link quality.

Experimental setup is demonstrated in figure 6.1 During these experiments, all the sent packets are successfully received by the Z1 receiver. The possible values for distance are 0, 10, 20, 30 and 40 in meters.

Besides different distance values, we also changed the output power settings of Z1 sender mote if there is any correlation between output power levels and distances. All eight output power settings as shown in table 4.3 had been utilized in our experiments.

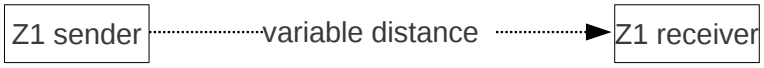

Figure 4.2: Experimental setup of RSSI v.s. distance

4.2.1.2 LQI v.s. distance

LQI is another metric to access the wireless link quality even though it is vendor dependent. In our experiments, CC2420 transceiver acts as the wireless radio. For CC2420 radio transceiver, LQI is estimated based on the first eight symbols of the received packet. The value of LQI varies from 50 to 110. The closer the value gets to 110, the better the wireless link quality is.

The experimental setup is the same as that in RSSI v.s. distance experiment. We utilized the same pair of Z1 motes. Also, eight output power levels of CC2420 had been used in our experiments.

4.2.1.3 Tx-power v.s. PDR

For this experiment, we fixed the distance between two Z1 motes as 40 meters. Then we changed the Radio Frequency (RF) output power settings of the Z1 sender mote. From this experiment, we want to see if there is any correlation between the PDR and transmit power. The experiment is carried out with using the V1 version application since with V2 version application, PDR would be zero if there is no obvious interference existing around.

4.2.2 Inter-protocol inference

4.2.2.1 IEEE 802.15.4 same channel

In this experiment, we chose two pairs of Z1 motes. One pair acted as the interfering pair, which generated interference. The other pair acted as the testing pair. In this experiment, we wanted to observe the relationship between the Packet Drop Ratio (PDR) of testing pair and the UDP packet sending interval of the interfering pair. Figure 4.3 shows the layout of this experiment. The distance between Z1 sender mote and Z1 receiver mote is 40 meters for both testing pair and interfering pair.

4.2.3 Cross-protocol inference

4.2.3.1 Microwave Oven v.s. IEEE 802.15.4

Microwave ovens operate in the 2.4 GHz frequency band. When it runs, it covers a big portion of this frequency band. We put the one pair of Z1 testing motes 1.5 meters away from the microwave oven. The Z1 sender mote is 2 meters away from the Z1 receiver mote. We started the microwave

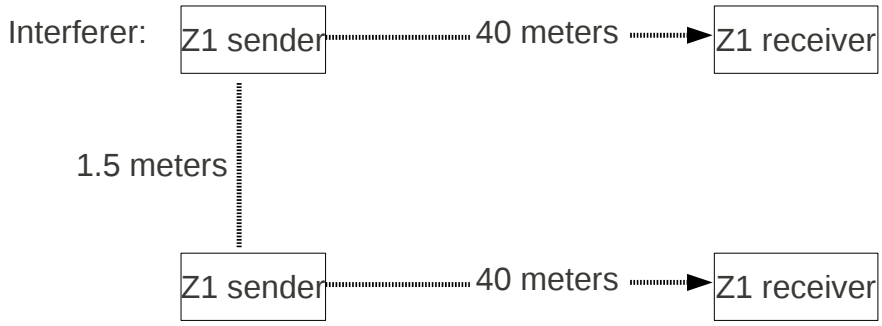

Figure 4.3: Experimental setup of Bluetooth v.s. IEEE 802.15.4

oven first, then activated the UDP packet sending process from Z1 sender mote to receiver mote. This experiment aims to see how much impact of the microwave oven can have on the IEEE 802.15.4 data communication.

4.2.3.2 Bluetooth v.s. IEEE 802.15.4

As another wireless technology which operates in the 2.4 GHz frequency band, we set up this experiment to see if Bluetooth traffic has any impact on the PDR of IEEE 802.15.4 communication.

The experimental setup is shown in the figure 4.4. Figure 4.4 only shows the experimental setup of Bluetooth devices put near Z1 sender mote. This is to see if Bluetooth traffic interferes with the packet sending process. We also conducted the experiments where Bluetooth devices were put near the Z1 receiver side to see if Bluetooth traffic have any impact on the packet receiving.

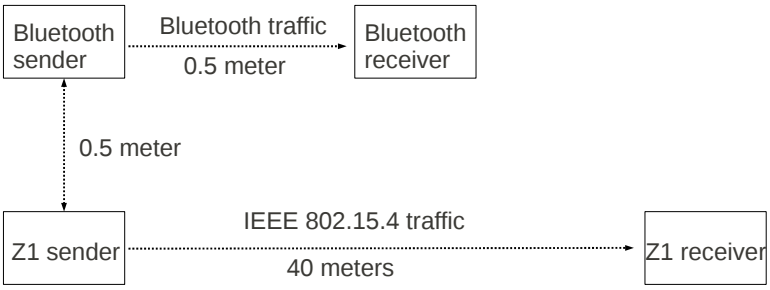

Figure 4.4: Experimental setup of Bluetooth v.s. IEEE 802.15.4

4.2.3.3 WiFi v.s. IEEE 802.15.4

WiFi output power can be 100 times that of the IEEE 802.15.4 output power. It can definitely have a large impact on the IEEE 802.15.4 traffic. In these experiments, we conducted with both UDP and TCP traffic. In both experiments, we use the same experimental setup which is demonstrated in firgure 4.5 except we used different transport layer protocols – TCP and UDP. The router we used is the Air Station TURBO G (module: WHR-G54S).

We used the Iperf [5] tool to generate both TCP and UDP traffic. Iperf is a network performance measurement tool. It can generate UDP traffic with certain bandwidth. One example of generating UDP traffic using Iperf is as follows:

Iperf -c ip_of_server -i 1 -f k -t time -b 1000k -u

In the above example, Iperf connects to the server with the ip address

of *ip_of_server* and default port 5001 (-c ip_of_server). Every second Iperf prints out packet sending information on the terminal (-i 1). The bandwidth unit is in kbps (-f k). The bandwidth is throttled to 1000 kbps (-b 1000k). Option "-u" indicates that Iperf is generating UDP traffic. On the server side, command "Iperf -su" runs to start the server daemon of Iperf which listens on port 5001 by default.

An example of generating TCP traffic would be:

Iperf -c ip_of_server -i 1 -f k -t time

Still, by default, port 5001 is used on both server and client. Without u option, TCP packets are sent from client to server. To control the TCP packet sending rate, Traffic Control (TC) command is utilized on the client side.

For both TCP and UDP traffic, we experimented with the data rate of 100, 500, 900, 1000, 1300, 1700, 2000, 3000, 4000, 5000, 6000, 7000, 8000, 9000, 10000, 11000, 12000, 13000, 14000 and 15000 Kbps.

For this WiFi v.s. IEEE 802.15.4 experiments, since this radio coverage of the WiFi signal has a 100 diameter range, we just put the WiFi environment near the Z1 sender mote.

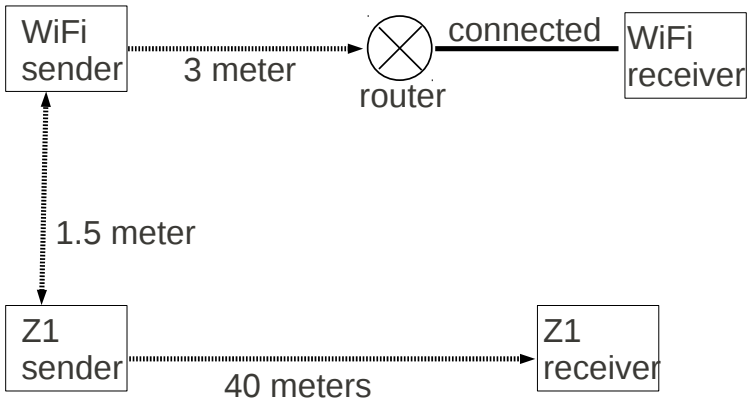

Figure 4.5: Experimental setup of WiFi v.s. IEEE 802.15.4

Chapter 5

Implementation

In our experiments, we implemented two different versions of applications. The version 1 application is indicated in figure 5.1. In version 1 application, packets are sent to the IEEE 802.15.4 MAC layer in a fixed time interval (we set this time interval to 0.2 seconds on testing pairs of Z1 motes) from the upper layer. On the IEEE 802.15.4 MAC layer, each frame is sent to the receiver side as long as the previous frame has been ACKed. In our experimental environment, usually it takes at least 3 to 4 milliseconds for the frame to be sent from the Z1 sender mote and the corresponding ACK frame arrives at the Z1 sender mote from the Z1 receiver mote. This version of application can increase the network throughput when the wireless link quality is good by speeding up the packet sending rate from the upper layer to the IEEE 802.15.4 MAC layer (less than 3 milliseconds). When the wireless link gets jammed or interfered by other interference, it takes more time for the ACK frame to travel from the Z1 receiver mote to the Z1 sender mote. In this case, on the IEEE 802.15.4 MAC layer, frame buffer overflow problem

occurs. Packets sent from the upper layer just gets dropped due to the fact that there is no empty slots in the frame buffer.

As the figure 5.1 indicates, after the Frame 0 (F0) is sent to and successfully accepted by receiver mote, an ACK frame corresponding to the Frame 0 is generated by the Z1 receiver mote and sent back to the Z1 sender mote. After the sender receives the ACK frame, Frame 0 is dropped from the Z1 sender frame buffer on the IEEE 802.15.4 MAC layer. Then, an empty frame slot exists to be ready to hold a new frame which contains a new packet just arrives from the upper layer. Frame buffer overflow happens when ACK for F1 comes back to Z1 sender late, which takes more time for the ACK than that of generating a new packet and sending the packet to IEEE 802.15.4 MAC layer of the sender from the upper layer. In the figure 5.1, when ACK for F1 does not come back after the F5 has been generated and sent to the MAC layer, then F5 would be just dropped. This is the MAC layer frame buffer overflow problem. If the ACK for F1 comes back in time (less than 0.2 seconds) from the Z1 receiver to the Z1 sender, F1 frame would be dropped from the frame buffer of the Z1 sender mote. Then another slot in the frame buffer is available, at this time a new frame which holds the newly created packet from the IP layer would come to the MAC layer of the Z1 sender and be put into the frame buffer. Now in this case there would be frames, F5, F4, F3, F2 , in the frame buffer.

In the version 2 of the application shown as in figure 5.2, we added an notification mechanism into the version 1 application. After F1 is sent and accepted by the receiver, an ACK frame would be sent back to the sender. Then F1 would be dropped from the frame buffer and an notification would be

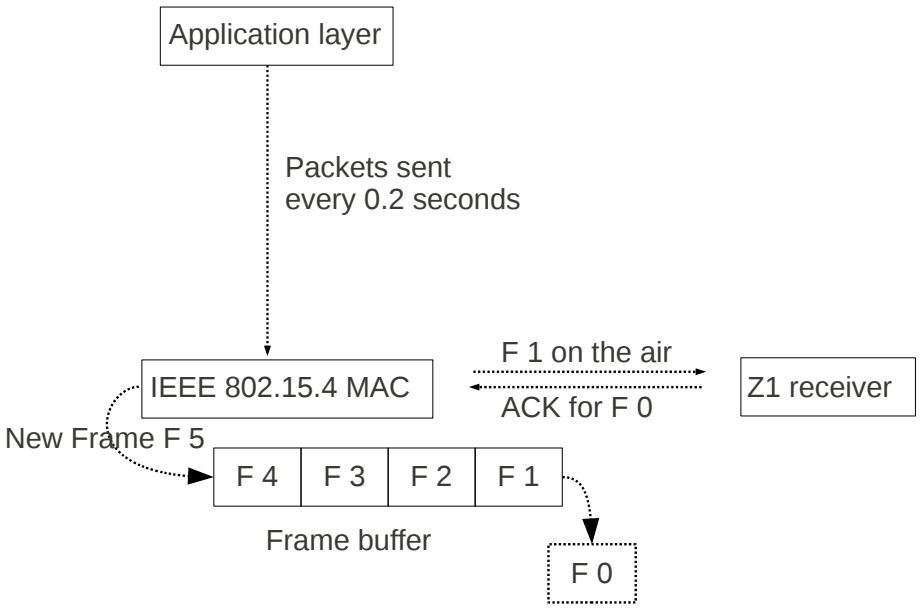

Figure 5.1: Version 1 application

generated by the IEEE 802.15.4 MAC layer on the Z1 sender mote to notify the upper layer that previous frame has been ACKed. Then next packet would be sent to the MAC layer. After the incorporation of this notification mechanism, frame buffer overflow problem is solved. No frames would be dropped before they are sent. In this case, we do not need to specify the time between sending of two consecutive packets because each packet would be generated only after the IP layer has received the notification event saying that previous frame has been successfully received by the Z1 receiver mote. In figure 5.2, ACK for F0 is received by Z1 sender mote, F0 is dropped away from the frame buffer in the Z1 sender mote. A new frame slot is available. An notification even is created by the MAC layer of Z1 sender and set to

the upper IP layer. A new packet is generated and sent to the MAC layer on the sender mote. This new frame is F4 and it is inserted into the frame buffer. There will be no frame buffer overflow problem in this version due to the fact that a new frame slot is already available when a new packet is sent to the MAC layer and put into a new frame. Meanwhile, after the F0 is dropped from the frame buffer, F1 is sent on the fly to the Z1 receiver mote. When ACK for F1 is sent back and received by the Z1 sender mote, a new notification which indicats the successful delivery of F1 would be generated and sent to the upper IP layer. Then a new packet is generated by upper layer and sent to the MAC layer of the Z1 sender mote. A new frame (F5) holding this new packet is created and put into the frame buffer. At this time, F1 is already dropped off frame buffer on the Z1 sender and a new frame slot is already free.

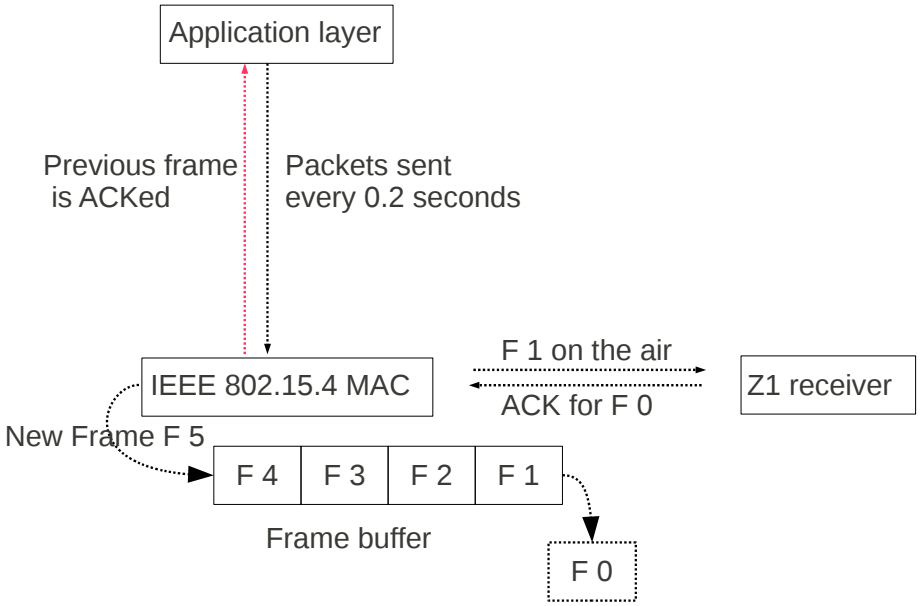

Figure 5.2: Version 2 application

Chapter 6

Evaluation

6.1 Wireless link quality indicators

6.1.1 RSSI v.s. distance

Figure 6.1 shows the relationship between RSSI and distance. As the figure indicates, for different transmit powers of the sender Z1 mote, the RSSI value change follows almost the same pattern, which is RSSI drops gradually when the distance increases. About 30 dBm drop occurs for each transmit power when the distance changes from 0 to 40 meters. The higher the transmit power is, the higher RSSI value is. This means the signal for holding the valid data to be transferred is more resistant to the background noise when the transmit power is set to a higher value. The reason for this RSSI dropping trend is because when the distance gets longer and longer, the signal faces more and more path loss and multi-path effects so that the signal energy gets reduced when it reaches the Z1 receiver mote. The higher the transmit power is, the more multi-path and path loss it can withstand. That is why higher

transmit powers has larger RSSI values at the same distance than that of lower transmit powers.

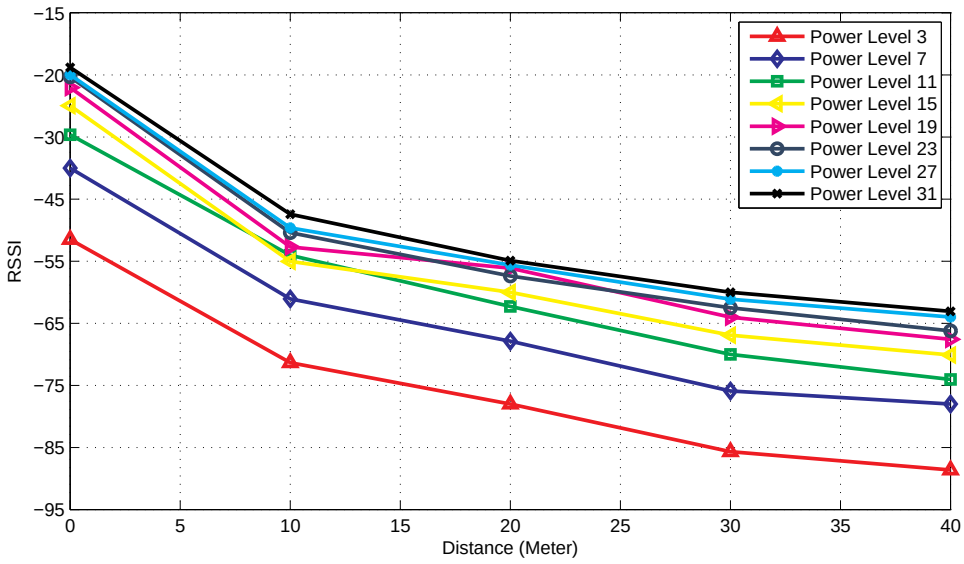

Figure 6.1: Change of RSSI with distance

6.1.2 LQI v.s. distance

Figure 6.2 shows the change of LQI when distance between two testing motes increases. From the figure we observed that for transmit power level 7 to 31, when the distance value increases from 0 to 40 meters, the LQI value remains between the range of 107 and 108 with slight decrease. But for transmit power level 3, when distance value increases from 0 to 20 meters, the LQI value stays in the same range as other transmit power level does. When distance values continue increasing from 20 to 40 meters, the LQI value drops from about 107 to a bit over 100. It should be noted that in both RSSI

and LQI experiments, the PDR of testing Z1 pair is 0, which means there is no packet loss.

According to CC2420 data sheet [3], LQI is calculated based on the average correlation value of the 8 first symbols of the received PHY header. The data sheet does not mention the exact algorithm. But since each packet is received successfully by the Z1 receiver mote, only the symbol energy is reduced due to the multi-path and path loss effects resulted from the increasing distance. This is reason that we observe the decreasing of LQI.

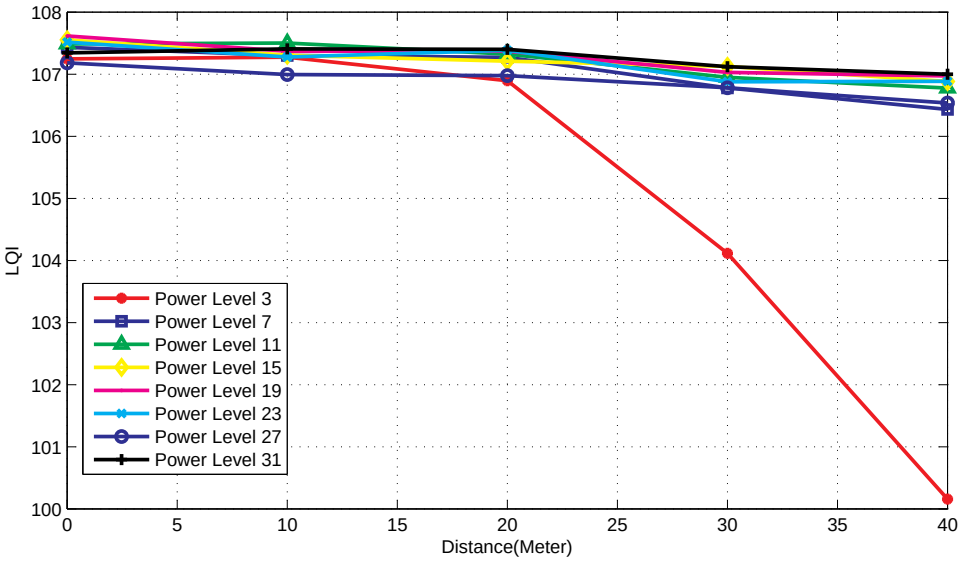

Figure 6.2: Experimental result of v.s. distance

6.2 Inter-protocol interference

6.2.1 IEEE 802.15.4 same channel

In this experiment, we used two pairs of Z1 motes. One pair acted as the interfering pair. The other pair acted as the testing pair. The UDP packet sending interval of the interfering pair got discrete values which can be 0.2, 0.4, 0.6, 0.8 and 1 second. The UDP packet sending interval was fixed to 0.2 seconds.

Figure 6.3 shows the relationship between the PDR of IEEE 802.15.4 data communication and the packet sending interval of the interfering pair. When the packet sending interval of the interfering pair is set to 0.2 seconds, this interfering pair has the strongest impact on the PDR of the testing pair. About 8% of the UDP packets sent by the Z1 mote sender of the testing pair got lost. When the UDP packet sending interval was equal to or greater than 0.6 seconds, the PDR of testing pair remained at around 3%. In this case, both testing pair and interfering pair interferes with each other. Since both pairs use the same transmit power and CSMA/CA is used by the IEEE 802.15.4 MAC sublayer, both Z1 senders of testing and interfering pair can sense the existing of each other. When one sender is occupying the channel with frames, another sender would back off. This is the reason that we see the packet loss in this inter-protocol interference. The result from this inter-protocol interference is very different from that in the cross-protocol interference, e.g., WiFi interference. The PDR in this inter-protocol interference is much smaller than that in the WiFi experiment. The reason for this big difference between PDR is explained in the cross-protocol WiFi

experiment part.

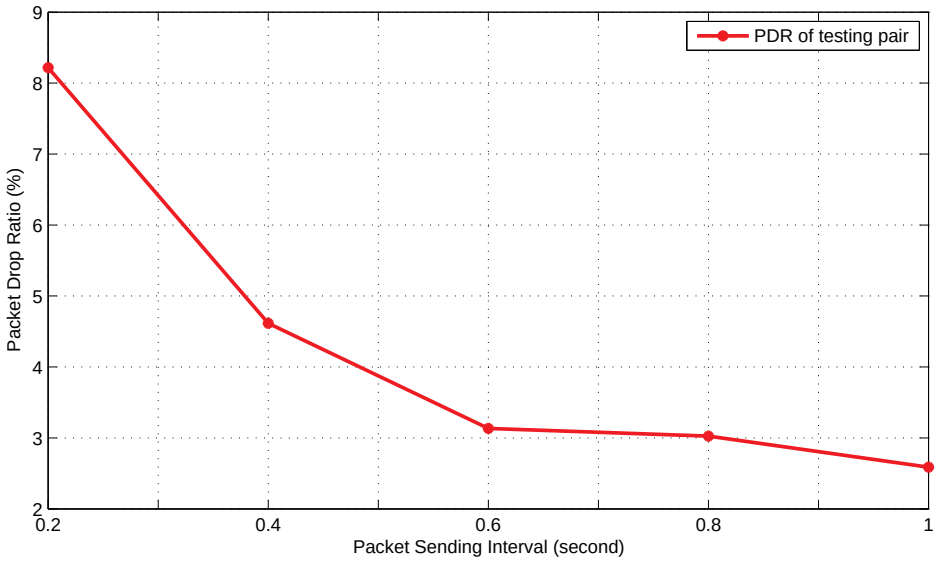

Figure 6.3: PDR change with distance

6.3 Cross-protocol interference

6.3.1 Microwave Oven v.s. IEEE 802.15.4

In this experiment, there was no interference from the Microwave oven on the IEEE 802.15.4 data communication. The reason behind this result is that the microwave oven that we used in our experiment is in a good condition with good seal. There is no radio signals leaked from it. Previous results [26] show that when the microwave oven is put more than 1 meter away from the motes, no interference would be imposed on the motes.

6.3.2 Bluetooth v.s. IEEE 802.15.4

For the Bluetooth experiment, there is also no interference coming from the Bluetooth traffic. The reason behind this result is that the Bluetooth versions that we used were 2.1 and 4.0. Since Bluetooth version 1.2, a technology called Adaptive Frequency Hopping (AFH) was introduced into the Bluetooth specifications. The AFH technique allows the Bluetooth to dynamically identify the channels which have been already occupied by other fixed interfering sources. AFH would exclude such busy channels from the hopping list and let the Bluetooth communication adapt to the environment.

6.3.3 WiFi v.s. IEEE 802.15.4

Figure 6.4 shows the impact of WiFi TCP and UDP traffic on the Packet Drop Ratio (PDR) of the IEEE 802.15.4 data communication. From the graph, we observe that WiFi TCP and UDP data traffic have similar impact on the PDR of IEEE 802.15.4 data communication. When WiFi data rate is set to 100 kbits/s, the PDR of IEEE 802.15.4 data communication is close to 0. When the WiFi data rate continues to increase, the PDR grows also until about 90%. This is because the WiFi data rate has reached the maximum value under our experiment setup. The reason that PDR of testing pair is at worst around 90% instead of 100% is that IEEE 802.15.4 MAC can always sense free status of the channel thereby new IEEE 802.15.4 frames can be sent to and received by the Z1 receiver mote.

In the experiment shown by figure 6.5, we conduct our experiments by using different WiFi UDP payload sizes and also different transmit powers. Since WiFi TCP and UDP data traffic have the similar impact on the PDR

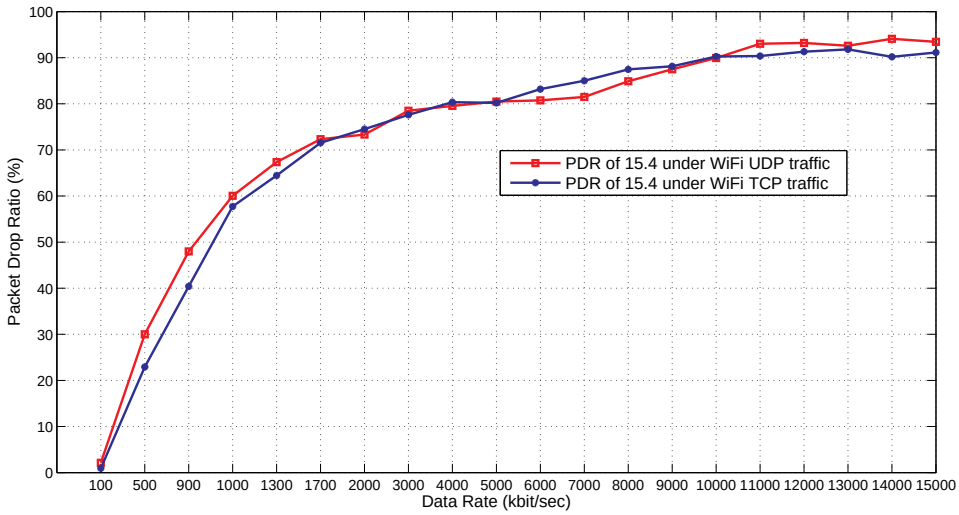

Figure 6.4: Experimental result of PDR of IEEE 802.15.4 v.s. WiFi TCP and UDP traffic

of the IEEE 802.15.4 data communication, we only use the WiFi UDP data traffic in this experiment. From figure 6.5, we can see that different UDP payload sizes have similar impact on the PDR of IEEE 802.15.4 data communication. Experiments are carried out with the configuration of the transmit power of the sender mote from the testing pair to highest level – level 31(0 dBm). Experiments shown by green line is done under the transmit power of the same sender mote set to the lowest level – level 3(-25 dBm). When the transmit power of the sender mote is set to level 31, the PDR of IEEE 802.15.4 data communication is about 30% at 500 kbits/s WiFi data rate. But when the transmit power is set to the lowest level 3 and the WiFi data rate is 500 kbits/s, which is low, the PDR of IEEE 802.15.4 is already as high as 70%. When the WiFi data rate increases to just 2000 kbits/s, the PDR

is already approaching 100%. At the same WiFi data rate (2000 kbits/s), with the highest transmit power, the PDR of IEEE 802.15.4 data communication is a bit over 70%. When transmit power of Z1 sender mote is set to level 3, multi-path and path loss has already negative impact on the radio signals output by the CC2420. The bigger power of WiFi even worsens this impact which has more interference on the CC2420 radio signals and makes the symbols tampered easily. The lower the transmit power of Z1 mote is, the less likely the WiFi transmitting source would sense the existence of radio signals of the CC2420. This would falsely make the WiFi transmitting source think the channel as free even though in fact the channel is occupied by the CC2420 radio signal. This false channel sense of WiFi and radiating of WiFi signals make more CC2420 radio sigals to be damaged so that IEEE 802.15.4 frames are dropped. The higher transmit power of Z1 mote (level 31) can mitigate this WiFi interference to some extent.

Figure 6.6 indicates the impact of WiFi TCP and UDP data traffic on the throughput of the IEEE 802.15.4 data communication. From this graph, we observe that WiFi TCP and UDP data traffic have the similar impact on the throughput of the IEEE 802.15.4 data communication. One thing should be noted that when the WiFi data rate reaches the 11000 kbits/s, it has arrived the maximum data rate. So the lowest throughput that IEEE 802.15.4 data communication can achieve is 60 bytes/s. The throughput of IEEE 802.15.4 is not zero is because IEEE 802.15.4 frames can always be sent to the Z1 receiver mote even though most of the packets are interfered by the WiFi.

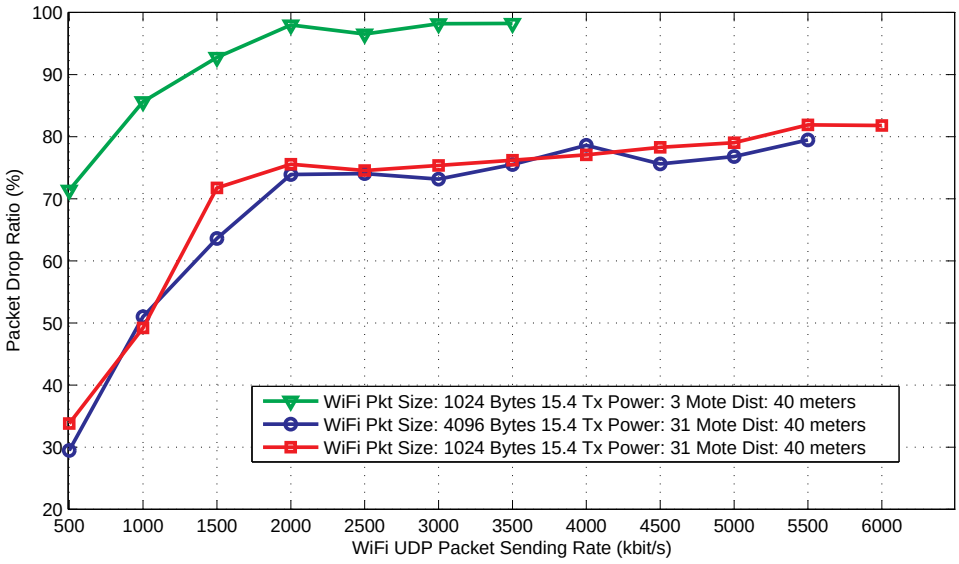

Figure 6.5: Experimental result of v.s. distance

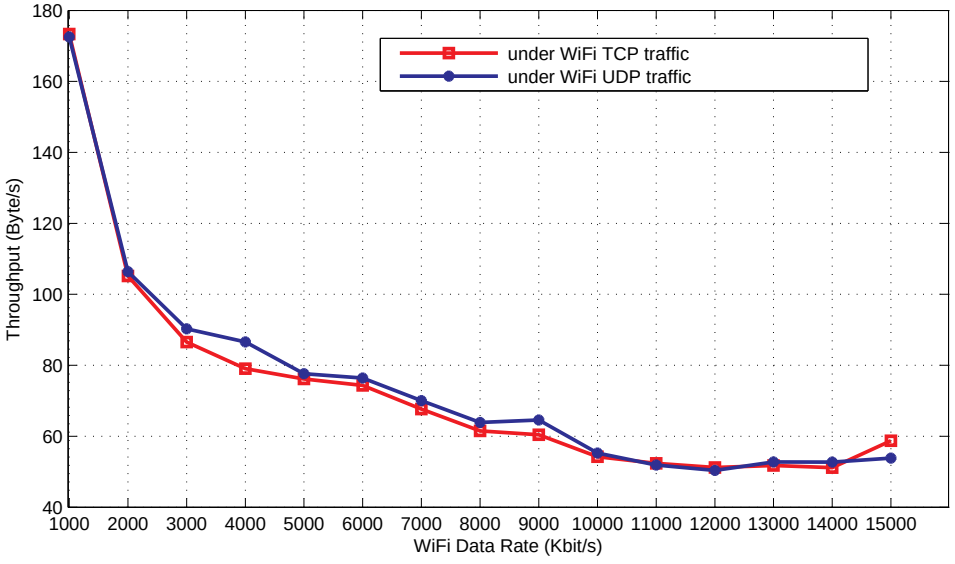

Figure 6.6: Experimental setup of RSSI v.s. distance

Chapter 7

Conclusions

The goal of this thesis is to quantify the interference from inter- and cross-protocols on the IEEE 802.15.4 data communications by conducting extensive experiments under different environment conditions. We first examined the experimental environment by carrying out several sets of experiments without any inte- or cross- protocol interference. We chose two commonly used indicators, LQI and RSSI. We used two Z1 motes. One played the sender role. The other acted as receiver. We varied the distance between these two motes to see the relationship between the LQI, RSSI and distance. We also tested different transmit power for the sender mote. This set of experiments gave us an overview of the environment where we conducted our other experiments to see how the wireless link behaves without any interference.

We chose two categories of interference. The first one is the inter-protocol interference. We constructed the experimental layout which included two pairs of Z1 motes. One pair worked as the interfering source. The other pair acted as the testing pair. We got results data from the testing pair for

analysis. The sender mote of the interfering pair sent packets using different packet sending interval. The sender mote of the testing pair was fixed as 0.2 seconds. From the results we learned that at most 8% packets from the testing sender mote were lost when the packet sending interval of the interfering sender was set to 0.2 seconds. At least around 3% packets went missing from the testing sender when packet sending interval of the interfering sender was set over or equal to 0.6 seconds.

The other category of experiments is the cross-protocol interference. In this case, we chose interference sources which are very likely to be encountered in our working environment or campus buildings. These are Microwave oven, Bluetooth and WLAN. From our experimental results, the microwave oven had no interference on the IEEE 802.15.4 data communication since it is in good condition without radio leakage or put more than 1 meter away from the IEEE 802.15.4 sensor networks. The Bluetooth data traffic also had no interference on the IEEE 802.15.4 data communication. The reason for that is Bluetooth introduced a new technique called Adaptive Frequency Hopping(AFH) into Bluetooth specifications since version 1.2. Now most smart phones have Bluetooth version over 1.2. The Bluetooth versions that we utilized in our experiments were 2.1 and 4.0. This AFH technique can identify occupied channels by other fixed interfering sources and exclude these busy channels out of the hopping list dynamically.

We carried out different WLAN experiments. We first tested the impact of the WiFi TCP and UDP data traffic on the Packet Drop Ratio (PDR) of the IEEE 802.15.4 data communications. The experimental results showed that WiFi data traffic had similar impact on the PDR of the sensor network

communication. Then we examined different UDP packet payload sizes and different transmit powers of the sender mote. We observed that different UDP packet payload sizes have similar impact on the PDR of the IEEE 802.15.4 data communication. When the sender mote was configured to have the lowest level of transmit power, the PDR was as high as 70% when the WiFi data rate was only 500 kbits/s. And this PDR quickly reached nearly 100% when WiFi data rate approached to 2000 kbits/s. When the transmit power was set to the highest level, the PDR was about 30% when WiFi data rate was 500 kbits/s. This indicated that the larger the transmit power is, the more resistance the radio signals have against the background noise. Finally, we conducted experiments to see the impact of WiFi TCP and UDP data traffic on the throughput of the IEEE 802.15.4 data communication. The results was that we got similar impact from both WiFi TCP and UDP traffic on the throughput of the IEEE 802.15.4 network communication.

Our work measured interference on the IEEE 802.15.4 data communication in a relatively complete manner from both inter- and cross- protocols by conducting various experiments under different experimental environment. Our experimental results give valuable indications about the interference on the IEEE 802.15.4 data communication. In addition to that, our results can be used to implement interference model, e.g., WiFi interference model, in some simulators, for instance, Cooja.

Bibliography

[1] 6LoWPAN protocol. http://openwsn.berkeley.edu/wiki/OpenLowPan.

[2] Air Station TURBO G. http://www.buffalotech.com/products/wireless.

[3] Chipcon CC2420 Website. http://www.ti.com/product/cc2420.

[4] Contiki OS. http://www.contiki-os.org/.

[5] Iperf netowrk performance tool. http://iperf.fr/.

[6] RPL. http://tools.ietf.org/html/rfc6553.

[7] Z1 wireless module. http://www.zolertia.com/products/Z1.

[8] Baccour, N., Koubâa, A., Mottola, L., Zúñiga, M. A., Youssef, H., Boano, C. A., and Alves, M. Radio link quality estimation in wireless sensor networks: A survey. *ACM Trans. Sen. Netw. 8*, 4 (Sept. 2012), 34:1–34:33.

[9] Bloessl, B., Joerer, S., Mauroner, F., and Dressler, F. Low-cost interferer detection and classification using telosb sensor motes. In *Proceedings of the 18th annual international conference on Mobile*

computing and networking (New York, NY, USA, 2012), Mobicom '12, ACM, pp. 403–406.

[10] Cao, B., Ge, Y., Tan, H., Feng, G., Kim, C., and Li, Y. An experimental study for inter-user interference mitigation in wireless body sensor networks, 2013.

[11] Di Francesco, M., Pinotti, C. M., and Das, S. K. Interference-free scheduling with bounded delay in cluster-tree wireless sensor networks. In *Proceedings of the 15th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems* (New York, NY, USA, 2012), MSWiM '12, ACM, pp. 99–106.

[12] Grassi, P., Rana, V., Beretta, I., and Sciuto, D. B x0b2;irs: A technique to reduce ban-ban interferences in wireless sensor networks. In *Wearable and Implantable Body Sensor Networks (BSN), 2012 Ninth International Conference on* (2012), pp. 46–51.

[13] Hermans, F., Larzon, L.-A., Rensfelt, O., and Gunningberg, P. A lightweight approach to online detection and classification of interference in 802.15.4-based sensor networks. *SIGBED Rev. 9*, 3 (July 2012), 11–20.

[14] Huang, H., Hu, G., Yu, F., and Zhang, Z. Energy-aware interference-sensitive geographic routing in wireless sensor networks. *Communications, IET 5*, 18 (2011), 2692–2702.

[15] IEEE Standard for Information technology . Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs), 2005.

[16] IEEE Standard for Information technology . Part 15.4:wireless mac and phy specifications for low-rate wireless personal area networks(LR-WPANs), IEEE Computer Society, 2006.

[17] IEEE Standard for Information technology . Part 11:wireless lan medium access control (MAC) and physical layer (PHY) specifications, IEEE Computer Society, 2012.

[18] Jeong, Y., Kim, J., and Han, S.-J. Interference mitigation in wireless sensor networks using dual heterogeneous radios. *Wirel. Netw. 17*, 7 (Oct. 2011), 1699–1713.

[19] Kumar, S., Sharma, A., and Raghuvanshi, S. Energy efficient scheduling algorithm with interference reduction for wireless sensor networks. In *Computational Intelligence and Communication Networks (CICN), 2011 International Conference on* (2011), pp. 328–332.

[20] Liang, C.-J. M., Priyantha, N. B., Liu, J., and Terzis, A. Surviving wi-fi interference in low power zigbee networks. In *Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems* (New York, NY, USA, 2010), SenSys '10, ACM, pp. 309–322.

[21] Lou, T., Tan, H., Wang, Y., and Lau, F. C. M. Minimizing average interference through topology control. In *Proceedings of the 7th international conference on Algorithms for Sensor Systems, Wireless*

Ad Hoc Networks and Autonomous Mobile Entities (Berlin, Heidelberg, 2012), ALGOSENSORS'11, Springer-Verlag, pp. 115–129.

[22] Lu, J., and Wang, X. Interference-aware probabilistic routing for wireless sensor networks. *Tsinghua Science and Technology 17*, 5 (2012), 575–585.

[23] Noda, C., Prabh, S., Alves, M., Boano, C. A., and Voigt, T. Quantifying the channel quality for interference-aware wireless sensor networks. *SIGBED Rev. 8*, 4 (Dec. 2011), 43–48.

[24] P. Gawthrop, F. Sanders, K. Nebbia, J. Sell. Radio spectrum measurements of individual microwave ovens. In *NTIA Report 94-303-1, Tech. Rep.* (Mar. 1994), vol. 2.

[25] Shah, R., and Nachman, L. Interference detection and mitigation in ieee 802.15.4 networks. In *Information Processing in Sensor Networks, 2008. IPSN '08. International Conference on* (2008), pp. 553–554.

[26] Sikora, A., and Groza, V. Coexistence of ieee802.15.4 with other systems in the 2.4 ghz-ism-band. In *Instrumentation and Measurement Technology Conference, 2005. IMTC 2005. Proceedings of the IEEE* (2005), vol. 3, pp. 1786–1791.

[27] Toscano, E., and Lo Bello, L. Cross-channel interference in ieee 802.15.4 networks. In *Factory Communication Systems, 2008. WFCS 2008. IEEE International Workshop on* (2008), pp. 139–148.

[28] Wang, Z., and Zhang, J. Interference aware multipath routing protocol for wireless sensor networks. In *GLOBECOM Workshops (GC Wkshps), 2010 IEEE* (2010), pp. 1696–1700.

[29] Xu, Y., Hu, J., and Shen, L. Analog network coding interference mitigation methods for wireless sensor networks. In *Wireless Communication Systems (ISWCS), 2012 International Symposium on* (2012), pp. 516–520.

[30] Yuan, D., Riecker, M., and Hollick, M. Hopscotch: An adaptive and distributed channel hopping technique for interference avoidance in wireless sensor networks. In *Local Computer Networks (LCN), 2012 IEEE 37th Conference on* (2012), pp. 635–642.

[31] Zacharias, S., Newe, T., O'Keeffe, S., and Lewis, E. 2.4 ghz ieee 802.15.4 channel interference classification algorithm running live on a sensor node. In *Sensors, 2012 IEEE* (2012), pp. 1–4.