ZigBee – WiFi Coexistence

White Paper and Test Report

Gilles Thonet
Patrick Allard-Jacquin
Pierre Colle

Schneider Electric
Innovation Department
37 Quai Paul Louis Merlin
38000 Grenoble, France

Table of Contents

Executive Summary

ZigBee is a very attractive technology for implementing low-cost, low-power wireless control networks requiring high flexibility in node placement. Supported by an underlying IEEE specification, ZigBee can benefit from an increasingly large ecosystem that is being built around the standard. Although using the license-free 2.4 GHz band is a strong catalyst for fast and worldwide market deployments, the presence of other wireless technologies across the same spectrum has risen concerns about potential coexistence issues.

Most of the worries have concentrated on IEEE 802.11 transmitters (commonly designated as WiFi transmitters in their commercial off-the-shelf versions) since they are now largely spread in both residential and office environments. The present report aims at assessing this potential risk in an unbiased way through both laboratory and real-environment experiments. It also attempts to summarize test results collected by other research groups so as to derive an overall and consensual conclusion on this issue.

Although previous test results seem to have delivered somewhat inconsistent conclusions, a closer look reveals that most of them are on the same line at equivalent experimental conditions (IEEE 802.11b/g mode, power level, traffic type, …). Based on measurements carried out in Schneider Electric's wireless laboratory and real houses, the following conclusions can be formulated:

- ZigBee operating in a real residential environment is not affected by today's most typical WiFi usage patterns, even in the most severe interference conditions (overlapping frequency channels, real-time video traffic). ZigBee packets may experience an increased latency under WiFi interference but delivery is not impacted.
- Laboratory experiments show that WiFi could have a significant impact on ZigBee when increasing WiFi's power level or duty cycle above what is used or reachable in today's applications (file transfer, audio and video streaming). This is especially true when operating in IEEE 802.11b mode. Better coexistence properties in IEEE 802.11g mode can be explained by less time spent by interfering packets on air.

Schneider Electric's investigations suggest that WiFi today does not constitute a threat to satisfactory ZigBee communications in real residential environments.

However, technical evolutions of WiFi technology and possible new application patterns in the future could in theory have more impact on ZigBee. This leads Schneider Electric to recommend, as an additional safety net, having the possibility of changing ZigBee's frequency channel while in operation. This functionality, called Frequency Agility, is provided by the ZigBee PRO stack specification. We believe that, equipped with that feature, ZigBee-based devices will be able to operate in a reliable and future-proof way.

1 Introduction

1.1 Background

Well-accepted wireless communication technologies generally operate in frequency bands that are shared among several users, often using different RF schemes. This is true in particular for WiFi, Bluetooth, and more recently ZigBee. They all three operate in the unlicensed 2.4 GHz band, also known as ISM band, which has been key to the development of a competitive and innovative market for wireless embedded devices. But, as with any resource held in common, it is crucial that those technologies coexist peacefully to allow each user of the band to fulfill its communication goals.

Despite efforts made by standardization bodies to ensure smooth coexistence it may occur that communication technologies transmitting for instance at very different power levels interfere with each other. In particular, it has been pointed out that ZigBee could potentially experience interference from WiFi traffic given that while both protocols can transmit on the same channel, WiFi transmissions usually occur at much higher power level.

1.2 Purpose of the Document

This report aims at providing a comprehensive and objective evaluation of ZigBee/WiFi coexistence. Building on previous studies led by other research groups, it reviews the main techniques implemented in ZigBee to ensure adequate RF coexistence. Both theoretical and practical tests are then carried out in laboratory and residential environments. Contrary to investigations led by other companies, the present study seeks to assess the coexistence limits of both technologies in order to formulate ZigBee development recommendations.

1.3 References

[1] Schneider Electric Internal Report. *ZigBee Coexistence with WiFi*. February 2006.

[2] G. Thonet and M. Bruel. *ZigBee: The Journey Toward Deployment in Industrial Applications*. ST Journal of Research. Vol. 4. No. 1. May 2007.

[3] ZigBee Alliance. *ZigBee and Wireless Radio Frequency Coexistence*. Document 075026r02. May 2007.

[4] Z-Wave Alliance. *WLAN Interference to IEEE 802.15.4*. White Paper. March 2007.

[5] Ember Presentation to the 2006 ZigBee Developers Conference. *ZigBee / 802.11 Coexistence – Testing and Recommendations*. June 2006.

[6] Freescale Semiconductor Application Note. *MC1319x Coexistence*. AN2935. July 2005.

[7] A. Sikora. *Compatibility of IEEE 802.15.4 (ZigBee) with IEEE 802.11 (WLAN), Bluetooth, and Microwave Ovens in 2.4 GHz ISM-Band – Test Report*. Steinbeis-Transfer Center, University of Cooperative Education Lörrach. September 2004.

1.4 Acronyms

ADSK	Asymmetric Digital Subscriber Line
APS	Application Sublayer
CFI	Call For Interest
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DSP	Digital Signal Processor
DSSS	Direct Sequence Spread Spectrum
FHSS	Frequency Hopping Spread Spectrum
FTP	File Transfer Protocol
HDTV	High Definition Television
HDV	High Definition Video
IC	Integrated Circuit
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISM	Industrial, Scientific and Medical
ITU	International Telecommunications Union
JPEG	Joint Picture Expert Group
MAC	Medium Access Control
MPEG	Motion Picture Expert Group
MTU	Maximum Transmission Unit
PCM	Pulse Code Modulation
PCR	Program Clock Reference
PDA	Personal Digital Assistant
PER	Packet Error Rate
PLC	Programmable Logic Controller
PHY	Physical
RF	Radio Frequency
RTP	Real-Time Transport Protocol
UDP	User Datagram Protocol
VAD	Voice Activity Detection
VoIP	Voice over Internet Protocol
WLAN	Wireless Local Area Network

2 Coexistence in ZigBee

This section reviews the main techniques implemented in ZigBee to ensure smooth coexistence with other wireless technologies (and WiFi in particular). Coexistence in ZigBee can be assessed at different levels, roughly matching the various layers constituting the ZigBee protocol stack.

2.1 IEEE 802.15.4 Layers

The IEEE policies require that, along with the specification itself, each standards committee publish a coexistence statement. As a consequence, the IEEE 802.15.4 specification provides support for coexistence at both PHY and MAC layers.

2.1.1 DSSS

The IEEE 802.15.4 standard belongs to the class of spread-spectrum technologies. In contrast to a narrow-band signal, a spread-spectrum signal consists in using a bandwidth that is much larger than strictly required by the information that is being sent (Figure 1). Because the signal is spread over a large bandwidth, it can coexist with other narrow-band signals, which generally incur a slight decrease in the signal-to-noise ratio over the spectrum being used.

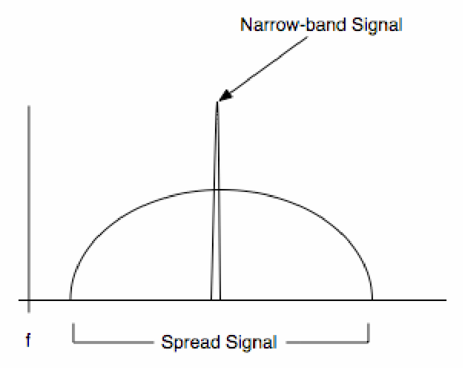


Figure 1 – Spread-spectrum signal (source: [3])

The spreading technique employed by IEEE 802.15.4 is direct sequence, which consists in using a pseudo-random code sequence to directly modulate the basic carrier signal and encode the data being transmitted. The resulting technology is called DSSS and is also found in the IEEE 802.11b/g standards.

2.1.2 Multiple Channels

The IEEE 802.15.4 specification augments the opportunities for smooth coexistence by dividing the 2.4 GHz band into 16 non-overlapping channels, which are 2-MHz wide and 5-MHz apart (Figure 2).

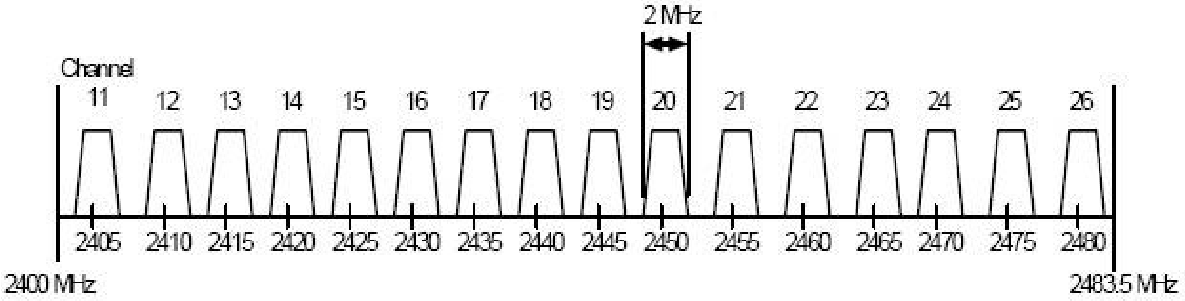


Figure 2 – IEEE 802.15.4 2.4 GHz spectrum

As shown in Figure 3, four of these channels (15, 16, 21, 22) fall between the often-used and non-overlapping 802.11b/g channels (1, 7, 13).

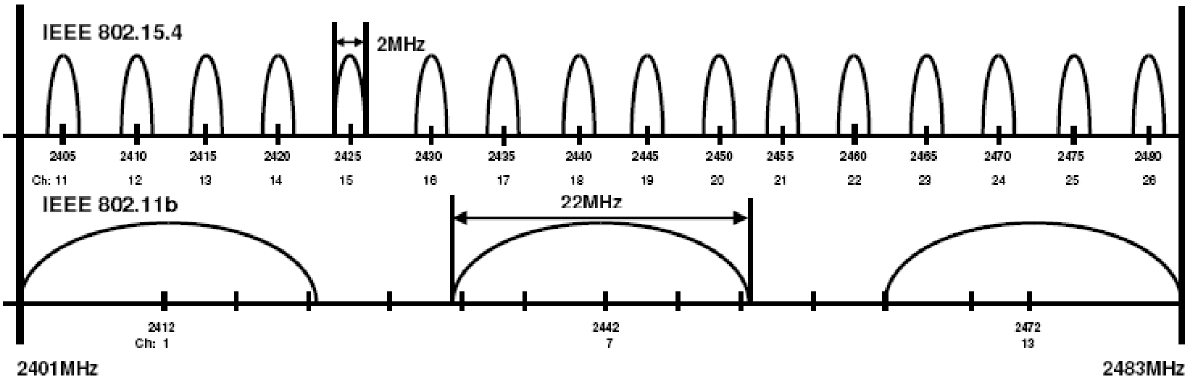


Figure 3 – IEEE 802.15.4 and IEEE 802.11b/g 2.4 GHz interference

Table 1 provides frequency offsets between combinations of IEEE 802.15.4 and IEEE 802.11b/g carrier frequencies leading to minimum interference.

Frequency Offsets		**IEEE 802.11b/g**		
		Channel 1 2412 MHz	**Channel 7** 2442 MHz	**Channel 13** 2472 MHz
IEEE 802.15.4	**Channel 15** 2425 MHz	13 MHz	17 MHz	47 MHz
	Channel 16 2430 MHz	18 MHz	12 MHz	42 MHz
	Channel 21 2455 MHz	43 MHz	13 MHz	17 MHz
	Channel 22 2460 MHz	48 MHz	18 MHz	12 MHz

Table 1 – Frequency offsets between IEEE 802.15.4 and IEEE 802.11b/g

2.1.3 Data Rate

Another way to minimize the risk of interference is to reduce channel occupancy. This approach is followed by the IEEE 802.15.4 standard. While many intended applications for ZigBee devices require a very low data rate (e.g. switching a light on and off, transmitting a temperature value), the underlying PHY layer communicates at 250 kbps. Compared to other RF systems targeting the same application range, this is a high data rate that allows to minimize time spent on air and reduce opportunities for collisions.

2.1.4 Built-in Scanning and Reporting

The IEEE 802.15.4 PHY layer provides the ability to sample a channel, measure the energy, and report whether the channel is free from interference and thus clear to transmit. This information is then made available to higher layers so that devices using IEEE 802.15.4 radios have the possibility to select the best available channel for operation.

2.1.5 CSMA

Even with the techniques described above, a ZigBee device may find itself sharing a channel with interferers, for instance other ZigBee devices that are part of the same network. The IEEE 802.15.4 standard makes use of a simple "listen before talk" strategy also known as CSMA and implemented in other wireless technologies such as WiFi. In this approach, a device that discovers that the channel is busy will wait a while before checking the channel again and transmitting its data.

2.1.6 Acknowledgements and Retransmissions

The IEEE 802.15.4 specification includes by default the acknowledgment of received frames. On receipt of a message, each device has a brief time window in which it is required to send back a short message acknowledging receipt. This technique allows messages that are transmitted but not successfully received to be detected. If the transmitting device does not receive the acknowledgment, it will assume that the message has not been delivered and will try again. Retransmissions are carried out until the message and its acknowledgment are both received or until, usually after a few tries, the transmitter gives up and reports a failure.

2.2 ZigBee Layers

The ZigBee standard adds network and application support on top the of IEEE 802.15.4 specification. In addition to coexistence techniques provided by IEEE 802.15.4 layers, ZigBee offers additional features to mitigate interference.

2.2.1 Network Formation

To form a new network, the first ZigBee node to be powered up, also known as ZigBee Coordinator, is required to scan through the list of available channels using built-in IEEE 802.15.4 mechanisms described in section 2.1.4. This step ensures that the new network will operate on the channel with least interference.

2.2.2 Mesh Networking

ZigBee is a mesh networking technology, which means that devices can automatically route messages on each other's behalf (often called multi-hopping). This allows to deploy larger networks without immoderately increasing the transmission power since direct communications occur only in a geographically-restricted area. Coexistence can clearly benefit from mesh networking. As shown in Figure 4, a ZigBee network will choose a different routing path in case the initial path fails due to interference.

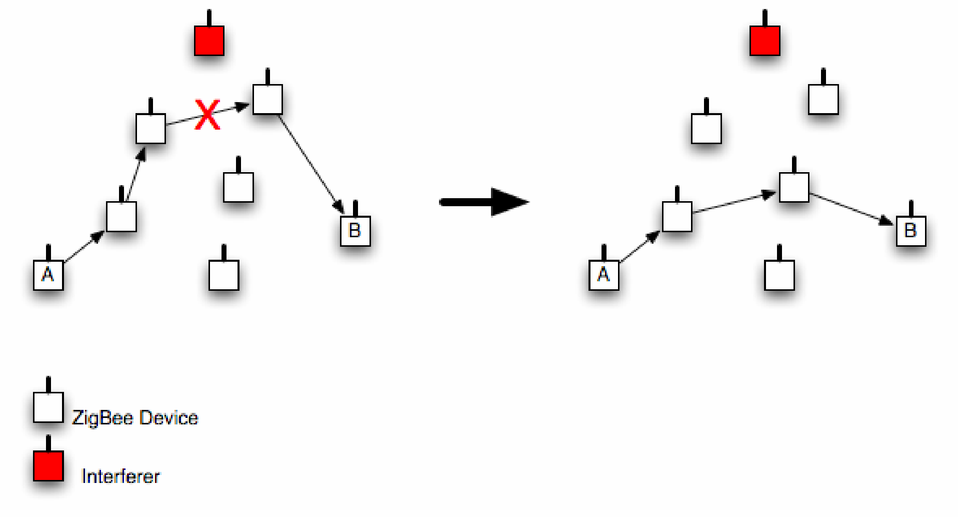


Figure 4 – Mesh networking and interference (source: [3])

2.2.3 End-to-End Acknowledgments and Retransmissions

In the same way single-hop transmissions in IEEE 802.15.4 are acknowledged and retransmitted in case of failure, multi-hop transmissions in ZigBee through the mesh network may also be acknowledged and retransmitted. This ensures end-to-end message delivery.

2.2.4 Frequency Agility

The ultimate feature to mitigate interference is the ability to move a ZigBee network to another channel while in operation. This is called frequency agility and included in the ZigBee PRO stack specification. It is worth noting that frequency agility is fundamentally different from frequency hopping. In cases where the interference detected by the ZigBee Coordinator at network formation (as described in section 2.2.1) changes or fails to reflect the interference profile of the network as a whole, ZigBee devices have the ability to use the built-in scanning mechanism to report interference to a network manager. Upon some criteria provided by the application, the network manager may direct the network to leave the current operating channel and move to another, clearer one.

3 Summary of Previous Studies

3.1 Schneider Electric

The first ZigBee coexistence tests performed at Schneider Electric's Innovation Department took place in 2005 and 2006 and have been documented in both an internal report [1] and an external publication [2]. Three types of measurements have been carried out: PHY-level characterization, Modbus serial line application, and lighting scenario. All tests were carried out using the first generation of ZigBee chipsets, which obviously presented inferior RF performance characteristics than more recent ones. Since at the time full ZigBee stacks were still under development, results were reported for IEEE 802.15.4 devices only, without using subsequent improvements such as end-to-end retransmissions.

3.1.1 Physical Characterization

The goal of the first test was to evaluate the behavior of the IEEE 802.15.4 PHY layer in presence of IEEE 802.11b interference. This experiment aimed at characterizing the interference level supported by IEEE 802.15.4 transceivers, without any CSMA mechanism. A complete description of the test setup and corresponding results can be found in [1].

3.1.2 Modbus Serial Line Application

The second test aimed at evaluating in a real application the full IEEE 802.15.4 transceiver (including MAC layer) in presence of IEEE 802.11b interference. Figure 5 shows the corresponding test block diagram. Two PCs acted respectively as FTP server and FTP client to send and receive pseudo-continuous WiFi frames. The serial line application consisted of a PLC generating Modbus frames that were sent through a ZigBee transmitter to a remote ZigBee receiver.

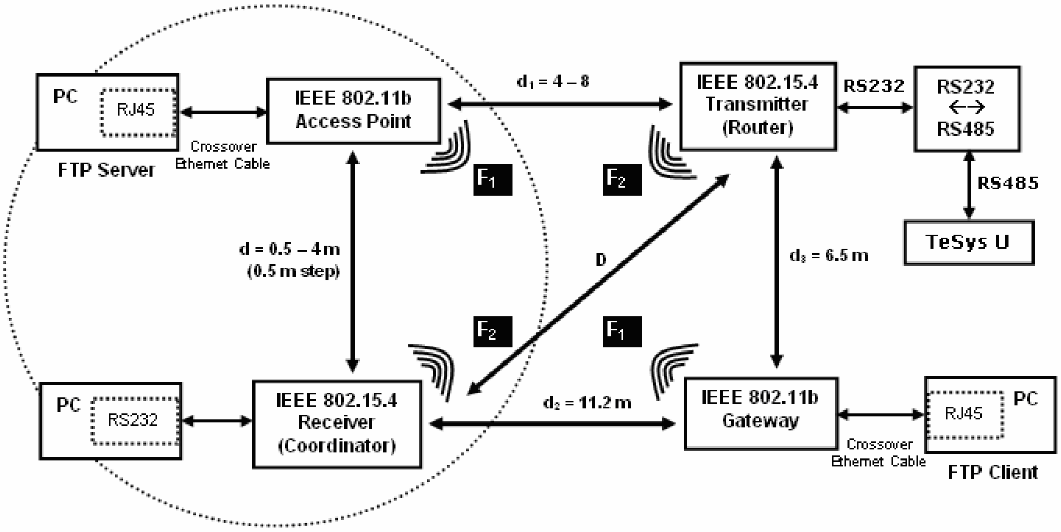


Figure 5 – Schneider Electric Modbus serial line interference test

Based on this experimental setup, physical distances and frequency offset parameters leading to smooth coexistence between WiFi and ZigBee have been determined. Slightly safer values have been selected so as to provide practical recommendations for real environments. Several parameter combinations have been assessed. For instance, to guarantee timely delivery of 80% of the packets, two ZigBee nodes can be 30 m apart in free space if the WiFi interferer is at least 2 m apart and the frequency offset is greater or equal to 25 MHz.

3.1.3 Lighting Application

The third test addressed a real-world ZigBee lighting application in a very functional way. The setup consisted of an IEEE 802.15.4 transceiver acting as a switch, an IEEE 802.15.4 transceiver acting as a lamp, and a WiFi interferer comprising an IEEE 802.11b gateway connected to an FTP client and an IEEE 802.11b access point connected to an FTP server. A simple on/off message was sent a number of times, and the final assessment consisted in both objective (successful/failed command) and subjective (acceptable/non-acceptable response time) criteria.

Results are provided in Table 2. It must be acknowledged that response time had not been assessed in a rigorous way. These observations suggested the following recommendations to ensure smooth coexistence:

- Distance between ZigBee nodes should ideally be less than 9 m. More may give acceptable results depending on local environment and application.
- Distance between a ZigBee node and a WiFi interferer should be more than 2 m.
- Frequency offset between ZigBee and WiFi networks should be at least 30 MHz.

D [m]	d [m]	ΔF [MHz]	Observations	Comments
0 – 9	2	32	Good response time	Acceptable
9 – 11	2	32	Variable response time Lamp responds often with latency Some frames are lost	Depends on application
0 – 6	0.5	3	Bad response time Lamp responds generally with latency Some frames are lost	Not acceptable

Table 2 – Schneider Electric lighting interference test results

3.1.4 Conclusions

Based on these initial results, Schneider Electric's Innovation Department formulated two installation recommendations:

- Distance of WiFi interferers to ZigBee nodes should be at least 2 m.
- Frequency offset between both networks should be at least 30 MHz.

These thresholds were formulated as "safe-side" values, i.e. many situations and environments could accommodate more relaxed recommendations. They should be considered as upper bounds ensuring smooth coexistence of both networks.

Since then, ZigBee chipsets have evolved and ZigBee stacks now include additional possibilities to mitigate interference at application level. Consequently, there was a need to revisit these results in light of up-to-date hardware and protocol stacks.

3.2 Daintree Networks (ZigBee Alliance)

As part of a report released by the ZigBee Alliance [3], Daintree Networks has carried out a series of interference tests aiming at providing deeper insights into the RF coexistence issue.

3.2.1 Hannover Fair Setup

A capture of ZigBee traffic has been made during the 2007 Hannover Fair, where many WiFi networks were running on several channels. A ZigBee network was operating on channel 17 and overlapping with adjacent WiFi activity (see [3] for a detailed list of all WiFi networks). ZigBee performance was measured using Daintree's Sensor Network Analyzer on a single-hop basis and without application-level retransmissions. Results are shown in Table 3.

Total Transmitted Packets	Total Lost Packets	Average Latency [ms]	Maximum Latency [ms]
25676	555	4.42	874.83

Table 3 – ZigBee performance during Hannover Fair 2007

At network layer level, Daintree Networks found a 2% packet loss rate. The same experiment has then been rerun using application-level retransmissions and resulted in a 0% packet loss rate. This underlines the importance of mitigating interference at several protocol stack levels.

3.2.2 Laboratory Setup

The previous experiment being rather functional, Daintree Networks set up a in-house experiment aiming at better characterizing ZigBee performance in presence of heavy WiFi traffic. As shown in Figure 6, ZigBee devices were placed at fixed distances from each other and a single interferer was located within 5 cm of one of them. ZigBee devices were configured to transmit on channel 18. Communications were line-of-sight and single-hop.

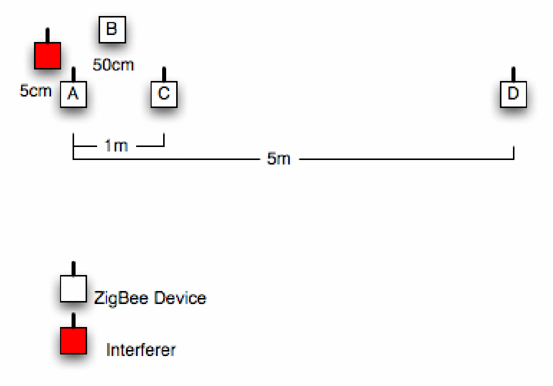


Figure 6 – Daintree Networks interference test setup (source: [3])

For each test run, 1 000 application messages were sent over the air every 50 ms. Message content was 4-byte long and compliant with the ZigBee Home Automation Profile to switch lights on and off.

Several interference sources were used in the experiment, among which an IEEE 802.11b network for FTP, two IEEE 802.11g networks for FTP and audio streaming, a Bluetooth network for computer-to-PDA file transfer, and an FHSS cordless phone (see [3] for a detailed list). WiFi networks were operating on channel 6, overlapping with ZigBee's channel 18.

Test results are depicted in Figure 7 and can be summarized as follows:

- During the entire test exercise, no ZigBee message was lost.
- Interference was nonetheless seen to have an impact on latency.
- IEEE 802.11g networks have less impact on ZigBee than IEEE 802.11b networks due to less time spent on air.

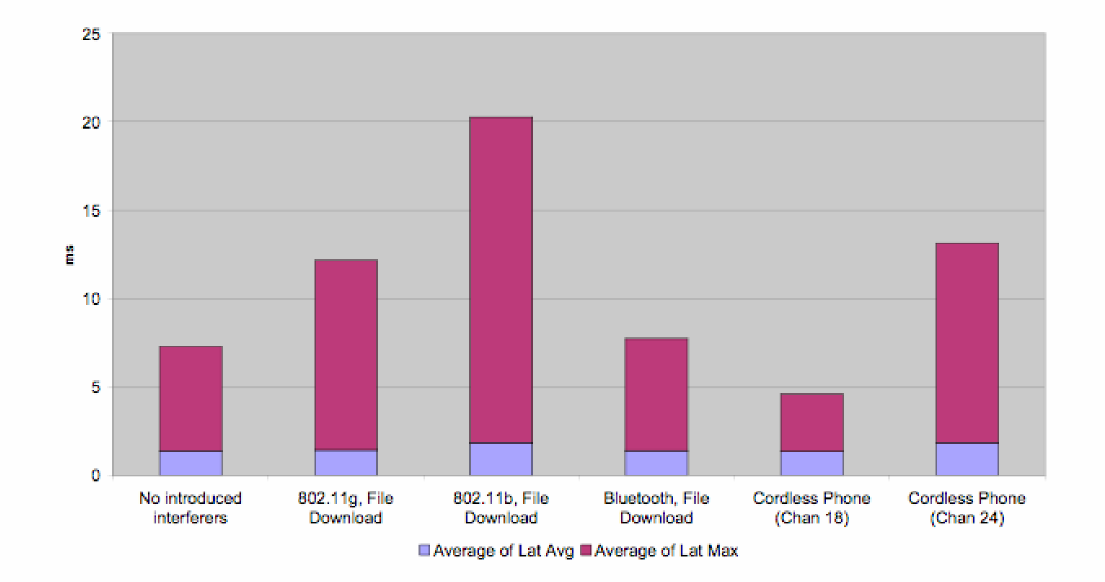


Figure 7 – Daintree Networks interference test latency results (source: [3])

3.3 Danfoss (Z-Wave Alliance)

In an attempt to assess the coexistence properties of ZigBee, researchers from Danfoss have run a series of interference tests that were subsequently incorporated into a report released by the Z-Wave Alliance [4].

Measurement results are shown in Figure 8. Experiments have been carried out using four types of commercial IEEE 802.15.4 devices coming from different manufacturers (labeled A, B, C and D) and an IEEE 802.11b interference source. Three different channel offsets between WiFi and ZigBee have been used: 2 MHz, 13 MHz and 33 MHz. Several interferer distances and duty cycles have also been employed to get a more insightful picture. Additional investigation conditions are described in [4].

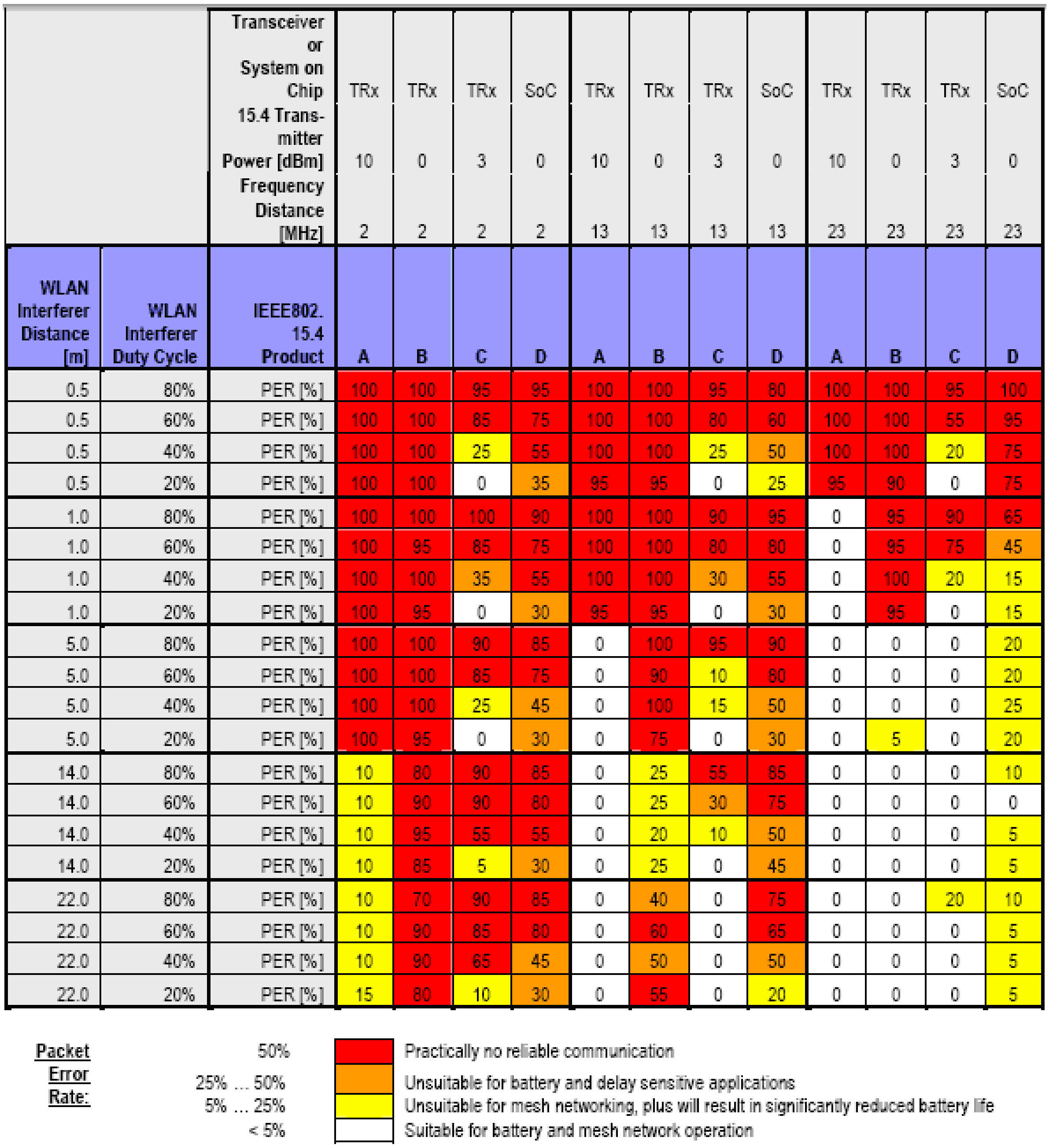
The authors of this report concluded that reliable operation of IEEE 802.15.4 devices under WiFi interference can be obtained only when the distance to the interferer is greater than 1 m and when the frequency offset to the interferer is larger than the width of a WiFi channel.

Although these results contradict those obtained by similar experiments conducted by the ZigBee Alliance (described in section 3.2), they could be explained by the following differences:

- Danfoss made use of a programmed traffic generator, which does not behave in the same way as an actual WiFi base station.
- Daintree Networks' tests referred to a real (and constrained) environment, whereas Danfoss' tests arbitrarily set up WiFi duty cycles.
- It is not fully clear how Danfoss chose the IEEE 802.15.4 chipsets under study. It is likely that they belonged to the first generation of RF boards, in line with what Schneider Electric used in its first coexistence study (described in section 3.1).

Also, the unverified claim that IEEE 802.11g networks would have a greater impact on coexistence is not supported by experimental results and contradicts results obtained by Daintree Networks (described in section 3.2). Findings reported in the present document will demonstrate that this assertion is not correct.

In spite of obviously biased results, this study is however interesting in suggesting that usage patterns outside "normal conditions" could lead to worse coexistence and call for specific recommendations or mitigation means.



		Transceiver or System on Chip	TRx	TRx	TRx	SoC	TRx	TRx	TRx	SoC	TRx	TRx	TRx	SoC
		15.4 Transmitter Power [dBm]	10	0	3	0	10	0	3	0	10	0	3	0
		Frequency Distance [MHz]	2	2	2	2	13	13	13	13	23	23	23	23
WLAN Interferer Distance [m]	WLAN Interferer Duty Cycle	IEEE802.15.4 Product	A	B	C	D	A	B	C	D	A	B	C	D
0.5	80%	PER [%]	100	100	95	95	100	100	95	80	100	100	95	100
0.5	60%	PER [%]	100	100	85	75	100	100	80	60	100	100	55	95
0.5	40%	PER [%]	100	100	25	55	100	100	25	50	100	100	20	75
0.5	20%	PER [%]	100	100	0	35	95	95	0	25	95	90	0	75
1.0	80%	PER [%]	100	100	100	90	100	100	90	95	0	95	90	65
1.0	60%	PER [%]	100	95	85	75	100	100	80	80	0	95	75	45
1.0	40%	PER [%]	100	100	35	55	100	100	30	55	0	100	20	15
1.0	20%	PER [%]	100	95	0	30	95	95	0	30	0	95	0	15
5.0	80%	PER [%]	100	100	90	85	0	100	95	90	0	0	0	20
5.0	60%	PER [%]	100	100	85	75	0	90	10	80	0	0	0	20
5.0	40%	PER [%]	100	100	25	45	0	100	15	50	0	0	0	25
5.0	20%	PER [%]	100	95	0	30	0	75	0	30	0	5	0	20
14.0	80%	PER [%]	10	80	90	85	0	25	55	85	0	0	0	10
14.0	60%	PER [%]	10	90	90	80	0	25	30	75	0	0	0	0
14.0	40%	PER [%]	10	95	55	55	0	20	10	50	0	0	0	5
14.0	20%	PER [%]	10	85	5	30	0	25	0	45	0	0	0	5
22.0	80%	PER [%]	10	70	90	85	0	40	0	75	0	0	20	10
22.0	60%	PER [%]	10	90	85	80	0	60	0	65	0	0	0	5
22.0	40%	PER [%]	10	90	65	45	0	50	0	50	0	0	0	5
22.0	20%	PER [%]	15	80	10	30	0	55	0	20	0	0	0	5

Packet Error Rate:			
	50%	🟥	Practically no reliable communication
	25% ... 50%	🟧	Unsuitable for battery and delay sensitive applications
	5% ... 25%	🟨	Unsuitable for mesh networking, plus will result in significantly reduced battery life
	< 5%	⬜	Suitable for battery and mesh network operation

Figure 8 – Danfoss interference test results (source: [4])

3.4 Ember

Based on the test network installed in their premise, Ember performed several experimental characterizations of ZigBee/WiFi coexistence. The main results are summarized in [5].

3.4.1 Physical Characterization

As illustrated in Figure 9, Ember performed a PHY-level IC characterization of their EM250 chip. Reference IEEE 802.15.4 and IEEE 802.11b/g sources were used to achieve a PER test for ZigBee devices. IEEE 802.11b/g references were filtered and shaped to match commercially available chipsets (Atheros and Broadcom). The power level of interfering source was constant, while useful signal was swept to find the level that the IEEE 802.15.4 receiver can receive packets at PER < 1%.

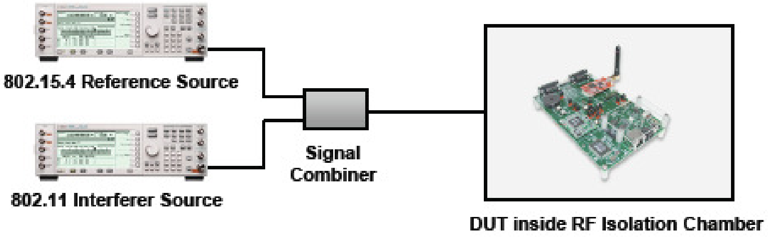


Figure 9 – Ember PHY performance test setup (source: [5])

Conclusions presented in [5] suggest that IEEE 802.11b/g interference can have a significant effect on the reception ability of IEEE 802.15.4. Such interference is primarily an in-channel radio issue, with some effects seen on the channel adjacent to the interference. As expected, increasing the distance from the WiFi source to the ZigBee receiver increases the useful communication range.

3.4.2 Network-level Characterization

Additional testing made on Ember’s in-house test network (Figure 10) allowed to show real-world effects of WiFi on operating ZigBee networks. Various interference scenarios were implemented (beacons only, maximum traffic using FTP, audio streaming) without any application-level retransmissions. The deployment area included both line-of-sight and non-line-of-sight ZigBee transmissions. Several channels were compared, with IEEE 802.15.4 channel 17 exhibiting the most interference.

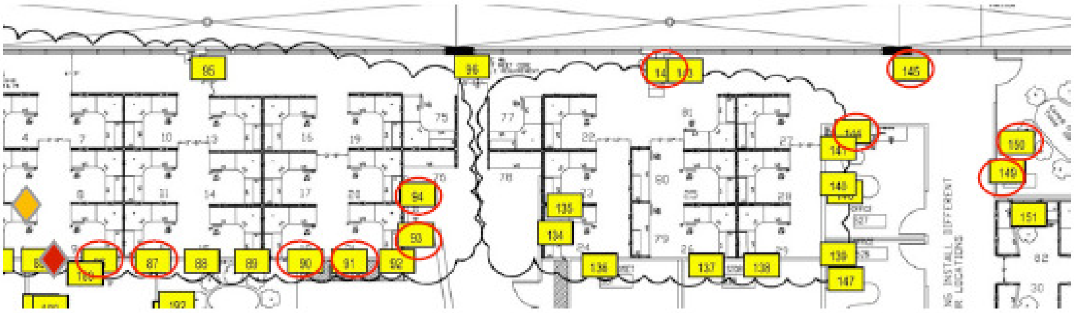


Figure 10 – Ember in-house ZigBee test network (source: [5])

Results showed that delivery ratio was 100% at network level, but some latencies exceeded MAC retry capability. Using network-level or application-level retransmission capabilities was shown to greatly contribute to mitigating WiFi interference. Figure 11 also shows that IEEE 802.11g networks have less impact on coexistence than IEEE 802.11b networks. All these results are consistent with the ones published by Daintree Networks for the ZigBee Alliance [3].

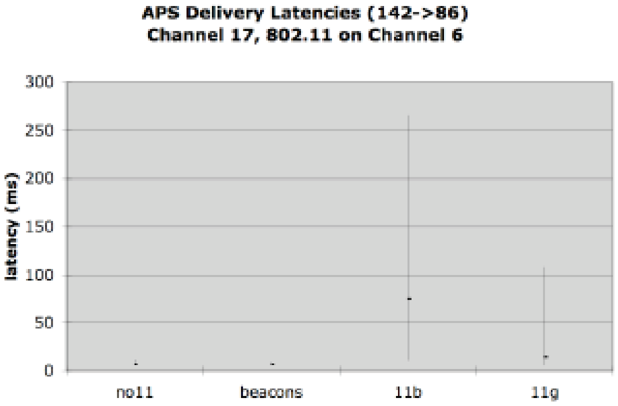


Figure 11 – Ember network-level interference test results (source: [5])

3.5 Freescale

Freescale released with one of its ZigBee chipsets an application note on RF coexistence [6]. Measurements were performed with Bluetooth and WiFi interferers in a hallway of a commercial building according to the setup shown in Figure 12. All tests were radiated and retransmissions were implemented at MAC level only.

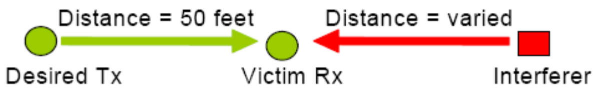


Figure 12 – Freescale interference test setup (source: [6])

In Figure 13, results show that when the transmitter was placed 50 feet (15 m) from the receiver and the interferer one foot (30 cm) away from the receiver, all IEEE 802.15.4 packets were delivered for frequency offsets greater than 25 MHz. The interference rejection degraded when frequency offsets were below 25 MHz. Based on these measurements, application note [6] recommends to place the desired carrier more than 25 MHz away from the interferer (in line with initial recommendations made by Schneider Electric in section 3.1.4).

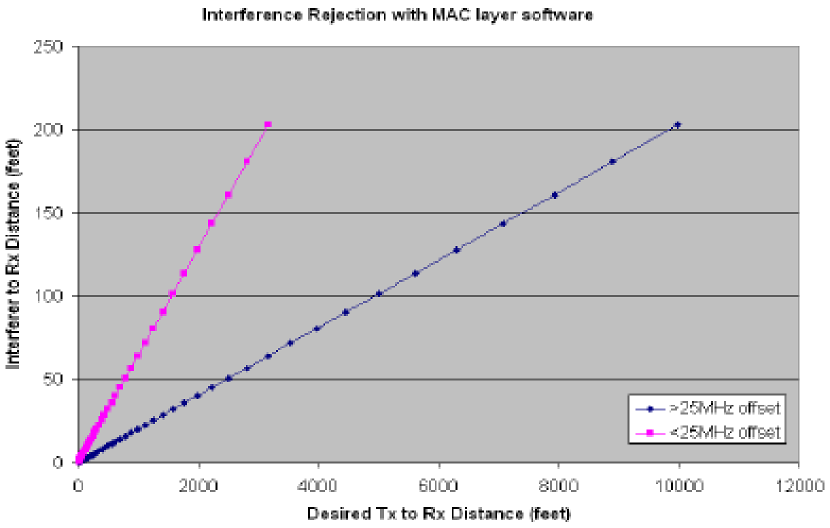


Figure 13 – Freescale interference test results (source: [6])

3.6 University of Cooperative Education Lörrach

One of the first test reports involving ZigBee RF coexistence has been released by a research team working at the University of Cooperative Education in Lörrach, Germany [7]. This paper presents experiments aiming at assessing the 2.4 GHz compatibility of IEEE 802.15.4 devices with IEEE 802.11 devices, Bluetooth devices and microwave ovens. Here also, tests are performed at MAC level and do not take into account higher-layer ZigBee mitigation mechanisms.

Figure 14 depicts the test setup used for assessing coexistence with WiFi in IEEE 802.11b mode. Interfering traffic was chosen to represent the maximum available load on a ZigBee overlapping channel to characterize worst-case conditions.

Figure 15 shows an extract of experimental results obtained when placing WiFi devices on channel 6 and ZigBee devices on channel 18. The horizontal axis refers to the number of frames, while the vertical axis indicates the transmission status (0 for success, 1 for frame loss). More than 92% of the IEEE 802.15.4 frames were destroyed by interfering IEEE 802.11b traffic, exhibiting a bursty character for interference. Carried out on neighboring channels, these measurements also suggested that a frequency offset of two WiFi channels allows for negligible interference.

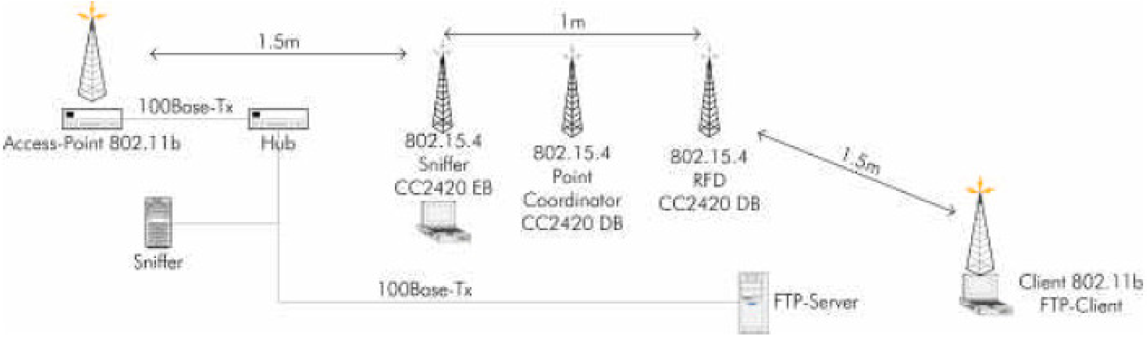


Figure 14 – UCE Lörrach interference test setup (source: [7])

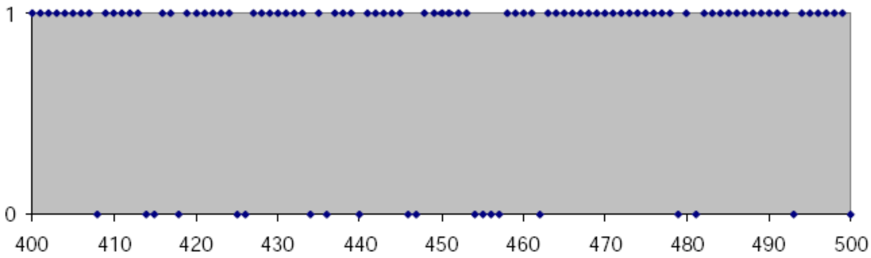


Figure 15 – UCE Lörrach interference test results (extract) (source: [7])

The authors conclude that although 90% of ZigBee traffic can be affected by WiFi interferers, these are worst-case conditions. Since some time slots remain for successful transmissions, they advocate for the use of higher-layer retransmissions to improve RF coexistence.

3.7 Summary

The review of previous ZigBee/WiFi coexistence studies is summarized in Table 4. Different test methodologies and environments have been used, leading obviously to distinct interference results and recommendations. However, some common trends can be singled out, based on the test parameters listed in the table:

- Tests making use of IEEE 802.15.4 (PHY and MAC) layers only generally report packet losses depending on frequency offset between ZigBee and WiFi carriers and physical distance between ZigBee and WiFi devices. In these cases, there was an overall consensus that interference becomes negligible whenever the frequency offset is at least the size of a WiFi lobe (around 20 MHz) and the minimal distance between ZigBee and WiFi devices is 1 to 2 m.
- Tests making use of a full ZigBee stack, including network-level or application-level retransmissions report an impact on latency but no packet loss. This underlines the strategic importance of higher-layer retransmissions compared to MAC-level retries only.
- WiFi power levels of 20 dBm (theoretical maximal limit) incur a greater impact on coexistence than commercial-grade power levels (around 15 dBm).
- Real-life WiFi traffic patterns (such as FTP and audio streaming) generally exhibit a lower impact on coexistence than arbitrarily loaded UDP transmissions simulated by a local traffic generator. This observation suggests that coexistence might present some limitations if the channel is loaded to a very high level.
- There seems to be a consensus that IEEE 802.11g traffic has less impact on ZigBee than IEEE 802.11b traffic. This assertion is easily understood when considering than spending less time on air reduces the risk of collisions.

These results will be revisited in the present study through further laboratory and real-environment experiments.

	Schneider	Daintree	Danfoss	Ember	Freescale	UCE Lörrach
ZigBee Chipset	TI CC2420	?	Multiple vendors	Ember EM2420 Ember EM250	Freescale MC1319x	TI CC2420
ZigBee Stack	PHY PHY+MAC	PHY+MAC APS Retry	PHY+MAC	PHY+MAC NWK Retry	PHY+MAC	PHY+MAC
ZigBee Power Level	0 dBm	?	0 dBm, 3 dBm, 10 dBm	0-4 dBm	0 dBm	0 dBm
WiFi Hardware	Acksys	?	?	Atheros Broadcom	?	DrayTek Agere
WiFi Mode	IEEE 802.11b	IEEE 802.11b IEEE 802.11g	IEEE 802.11b	IEEE 802.11b IEEE 802.11g	IEEE 802.11b	IEEE 802.11b
WiFi Power Level	20 dBm	?	20 dBm	14-18 dBm	15 dBm	20 dBm
WiFi Traffic	FTP	FTP Audio streaming	UDP with 20-80% duty cycle	FTP Audio streaming	UDP with 10-90% duty cycle	FTP
Communication Modes	Line-of-sight Single-hop	Line-of-sight Single-hop	Non-line-of-sight Single-hop	Line-of-sight Non-line-of-sight Single-hop Multi-hop	Line-of-sight Single-hop	Line-of-sight Single-hop
ZigBee Channels	All	18	17, 20, 24	17	11, 16, 21, 26	18
WiFi Channels	7	6	6	6	All	6
Frequency Offset WiFi/ZigBee	2 MHz, then all offsets	3 MHz	2 MHz, 13 MHz, 33 MHz	2 MHz	12 MHz, then all offsets	3 MHz
Distance WiFi/ZigBee	0.5 – 4 m (0.5 m step)	5 cm	0.5 m, 1 m, 5 m, 14 m, 22 m	Multiples	30 cm	1.5 m
Distance ZigBee/ZigBee	8.5 m, 20 m, 30 m, 90 m	50 cm, 1 m, 5 m	8 m	Multiples	15 m	1 m
Conclusions	Impact on packet delivery depending on distance and frequency offset	Impact on latency but not on packet loss 802.11g better	Impact on packet delivery depending on distance and frequency offset	Impact on latency but not on packet loss 802.11g better	Impact on packet delivery depending on distance and frequency offset	Impact on packet delivery depending on distance and frequency offset
Recommendations	Distance WiFi – ZigBee ≥ 2 m Frequency offset ≥ 30 MHz	No – works well in all cases Use 802.11g rather than b	Distance WiFi – ZigBee ≥ 1 m Frequency offset ≥ 22 MHz	Maximize frequency offset Use 802.11g rather than b	Frequency offset ≥ 25 MHz	Frequency offset ≥ 10 MHz

Table 4 – Summary of previous coexistence test results

4 Residential Tests

4.1 House 1

4.1.1 Deployment Environment

This set of tests has been carried out in a real house to assess the coexistence behavior of ZigBee in a residential environment. The deployment area consisted in an individual house located in Meylan, France, and spanning three floors over approximately 180 m^2. An ADSL connection provided Internet access to the house. The ADSL box was equipped with WiFi, whose technical characteristics are listed in Table 5. A laptop comprising a WiFi connection was used as second interfering transmitter.

Characteristics of ADSL Interface	
Manufacturer/Type	Freebox
Effective Bandwidth	3-6 Mbps (depending on traffic conditions)
WiFi Mode	IEEE 802.11g
WiFi Channel in Use	11

Table 5 – Characteristics of ADSL/WiFi interface

Two test configurations have been considered across the deployment area:

- ZigBee devices on the same floor (depicted in Figure 16).
- ZigBee devices on different floors (depicted in Figure 17).

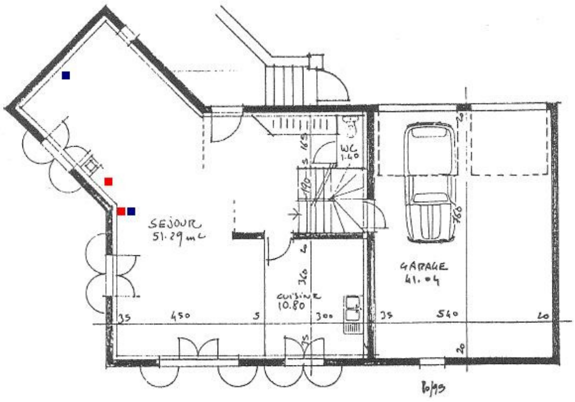


Figure 16 – Configuration <1> (ZigBee devices in blue, WiFi devices in red)

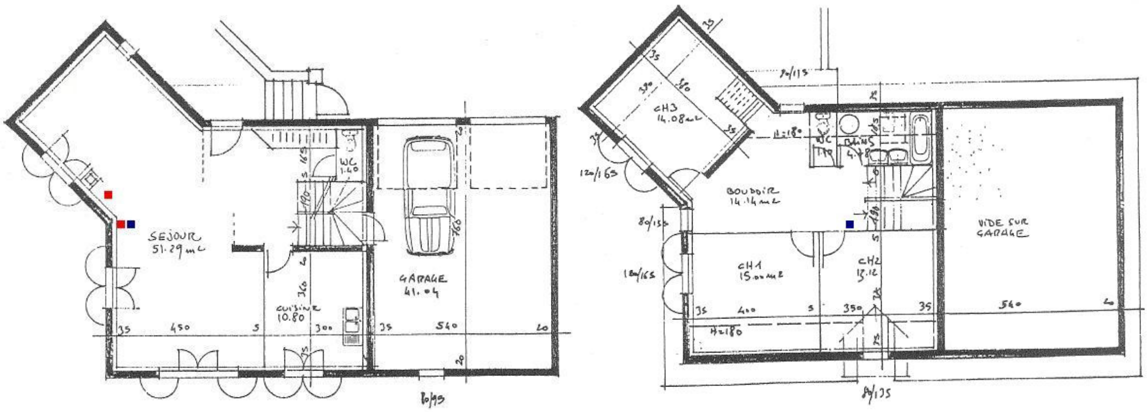


Figure 17 – Configuration <2> (ZigBee devices in blue, WiFi devices in red)

Placement configurations are described in Table 6 and are assumed to represent possible localizations for switch/lamp pairs. It must be noted that, for easiness of installation, both ZigBee and WiFi devices were located at an approximate elevation of 1 m. This might provide slightly worse test results given that several objects (sofas, table including metallic parts) are in the way of line-of-sight transmissions.

Test Configurations	<1>	<2>
Distance between WiFi transmitters	1 m	1 m
Distance between ZigBee transmitters	4 m (on ground floor)	8 m (on ground and 1st floor)
Minimal distance between ZigBee and WiFi transmitters	20 cm	20 cm

Table 6 – Description of test configurations

4.1.2 Methodology

Interference tests have been performed with two ZigBee evaluation boards described in Table 7. One board represented a lighting switch while the other one represented a lamp. Both devices had been uploaded with a sample code performing the transmission of a simple "switch light on/off" ZigBee frame.

These commands were sent to the "switch" device from a PC using a hyper-terminal application and through the serial port. Commands were sent continuously every 3 s, until stopped by the user. Frames received by the "lamp" device and acknowledgements received by the "switch" devices were counted and stored by the hyper-terminal application. The stack was configured for both network-level (automatically operated by Ember's stack) and application-level (APS Retry) retransmissions.

Characteristics of ZigBee Devices	
Hardware	Ember EM250 evaluation board
Software	EmberZNet 3.0.2 (pre-ZigBee PRO) stack
ZigBee Power Level	1 mW
ZigBee Channel in Use	22 (overlap with WiFi channel 11)

Table 7 – Characteristics of ZigBee devices

Interference tests have been run over a one-week period using several WiFi traffic profiles:

- Web surf
- File download
- Audio streaming
- Real-time television

4.1.3 Results

4.1.3.1 Web Surf

Daily web surf (reading news, checking weather forecasts, …) and emailing have been running over a week at random intervals (generally evening time). This test sequence has been run using Test Configuration <1>.

Results: No ZigBee packets lost.

4.1.3.2 File Download

A punctual download of the ZigBee standard specification document (4.2 Mb) has been performed to assess the resilience of ZigBee transmissions under this WiFi profile. This test sequence has been run using Test Configuration <1>.

Results: No ZigBee packets lost.

4.1.3.3 Audio Streaming

Punctual accesses to several YouTube audio recordings have been carried out on three different days. This test sequence has been run using Test Configuration <1>.

Results: No ZigBee packets lost.

4.1.3.4 Real-time Television

Test Configurations <1> and <2> have been used in the test sequence consisting in running real-time television (www.bfmtv.fr) on the PC through WiFi connection to the ADSL port. Real-time video streaming has been performed over a 10-hour period for each Test Configuration.

Results: No ZigBee packets lost in both test configurations.

4.1.4 Conclusions

The above-described sequence of tests represents typical use patterns in a real home environment. Different WiFi traffic profiles have been used (simple web surf, file download, audio streaming and video streaming) to assess the coexistence properties of ZigBee in various operating conditions. Results show that, under all interferer traffic patterns, no single ZigBee packet has been lost.

4.2 House 2

4.2.1 Deployment Environment

The deployment environment for the second set of residential tests consisted in an individual house located in St Martin d'Uriage, France, and spanning three floors over approximately 140 m^2 (Figure 18 and Figure 19). The heating system was operating through circulating water on the two upper floors.

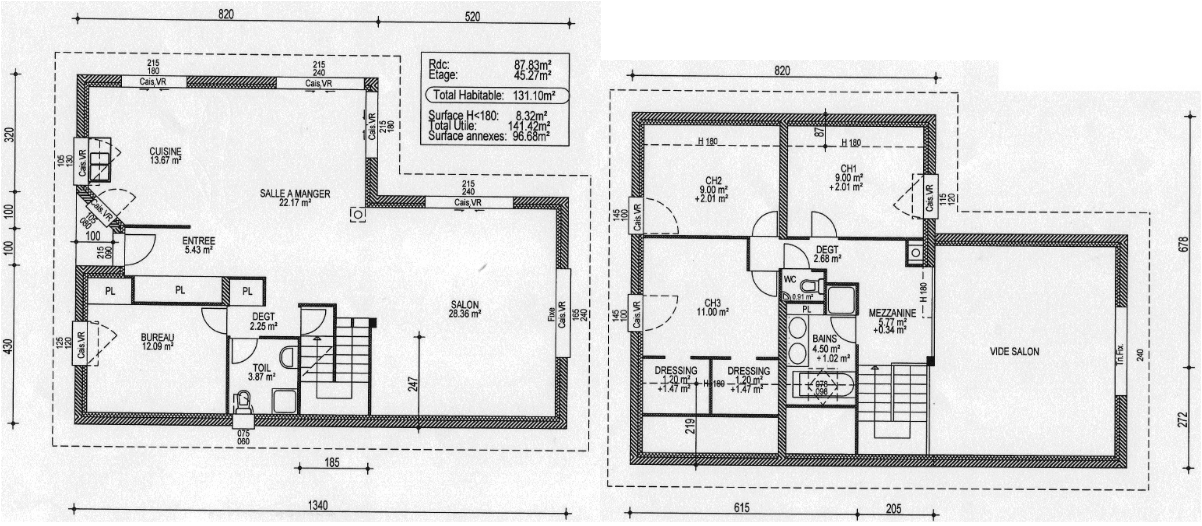


Figure 18 – Deployment area for House 2 (first and second floors)

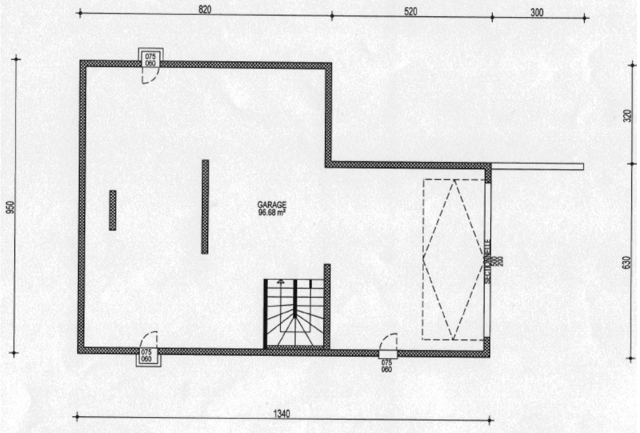


Figure 19 – Deployment area for House 2 (basement)

An ADSL connection provided Internet access to the house. Its mode (IEEE 802.11b/g) was forced to one or the other depending on tests. The ADSL box was equipped with WiFi, whose technical characteristics are listed in Table 5.

Characteristics of ADSL Interface	
Manufacturer/Type	Linksys WAG354G
Effective Bandwidth	512 kbps
WiFi Mode	IEEE 802.11b/g
WiFi Channel in Use	11

Table 8 – Characteristics of ADSL/WiFi interface

Other WiFi equipments listed in Table 9 were switched on or off during the tests.

List of Interfering Equipments	
Mobile Phone Bluetooth 2.0	Nokia 2630
PC WiFi 802.11b/g + Bluetooth	Dell 610
iMac WiFi 802.11b/g (15 dBm) + Bluetooth	Apple iMac 4.1
Radio 802.11b/g	Noxon iRadio Terratec
Radio 802.11b/g	Nabaztag
WiFi 802.11b/g access point	Apple Airport Express 6.3
Microwave	Candy
Neighbor’s WiFi network also detected	

Table 9 – Interfering devices

4.2.2 Methodology

Tests were done with one ZigBee device (“light”) next to the Linksys modem router, while the second ZigBee device (“sensor”) was moved in all the different rooms. The number of ZigBee packets lost was checked far around one minute in each configuration. The Dell PC was put next to second ZigBee device to measure the WiFi signal strength received from the Linksys modem router. Test configurations were as follows:

- Audio streaming from iMac to Airport express: 1 Mb/s, 6 m away from Linksys modem router.
- Audio streaming from Linksys modem router to radio: 128 kb/s, 7 m away from Linksys modem router.

- IEEE 802.11b or g modes forced on all devices, operating on channel 11.
- ZigBee "light" device was 50 cm away from Linksys modem router on the first floor, operating on channel 22 and at 0 dBm transmitting power level. Dell PC indicated a received signal of -30 dBm and a noise level of -87 dBm for that same position.
- ZigBee devices were placed at an elevation of 80 cm.

4.2.3 Results

All WiFi devices worked fine during the tests. There has been no glitch heard on audio streaming or file transfer disruption.

4.2.3.1 Test 1 (Line-of-sight, 802.11b)

Additional setup:

- Audio streaming from Linksys modem router to Nabaztag (6 m distance).
- Web browsing from Dell PC connected to Linksys modem router (6 m distance).
- Mobile phone with Bluetooth on but not used (20 cm away for ZigBee sensor).
- Dell PC with Bluetooth on but not used (20 cm away from ZigBee sensor).
- Microwave on during 2 minutes (8 m away from Linksys modem router and ZigBee sensor).

All equipments were in line-of-sight. Dell PC indicated a received signal of -54 dBm and a noise level of -88 dBm.

Results: No ZigBee packets lost.

4.2.3.2 Test 1bis (Line-of-sight, 802.11g)

Setup identical to Test 1 but using 802.11g mode.

Results: No ZigBee packets lost.

4.2.3.3 Test 2 (ZigBee sensor in office room, first floor)

Dell PC indicated a received signal of -77 dBm and a noise level of -86 dBm.

Estimated distance between ZigBee devices: 11 m.

Obstacles: one door, almost one floor.

Results: No ZigBee packets lost.

4.2.3.4 Test 3 (ZigBee sensor in bathroom, first floor)

Dell PC indicated a received signal of -67 dBm and a noise level of -92 dBm.

Estimated distance between ZigBee devices: 7 m.

Obstacles: one door, almost one floor.

Results: No ZigBee packets lost.

4.2.3.5 Test 4 (ZigBee sensor in kitchen, first floor)

Dell PC indicated a received signal of -63 dBm and a noise level of -85 dBm.

Estimated distance between ZigBee devices: 9 m.

Obstacles: none.

Note: ZigBee sensor is 50 cm away from microwave oven turned on.

Results: No ZigBee packets lost.

4.2.3.6 Test 5 (ZigBee sensor in bathroom, second floor)

Dell PC indicated a received signal of -51 dBm and a noise level of -90 dBm.

Estimated distance between ZigBee devices: 5 m.

Obstacles: one door.

Results: No ZigBee packets lost.

4.2.3.7 Test 6 (ZigBee sensor in parents bedroom, second floor)

Dell PC indicated a received signal of -54 dBm and a noise level of -91 dBm.

Estimated distance between ZigBee devices: 10 m.

Obstacles: one door.

Results: No ZigBee packets lost.

4.2.3.8 Test 7 (ZigBee sensor in child bedroom, second floor)

Dell PC indicated a received signal of -56 dBm and a noise level of -87 dBm.

Estimated distance between ZigBee devices: 10 m.

Obstacles: one door.

Results: No ZigBee packets lost.

4.2.3.9 Test 8 (ZigBee sensor in guest bedroom, second floor)

Dell PC indicated a received signal of -45 dBm and a noise level of -87 dBm.

Obstacles: one plaster wall.

Results: No ZigBee packets lost.

4.2.3.10Test 9 (ZigBee sensor in basement, below modem router)

ZigBee devices bound with some difficulty (device had to be moved slightly).

Dell PC indicated a received signal of -80 dBm and a noise level of -90 dBm.

Estimated distance between ZigBee devices: two floors.

Obstacles: two floors including ground heating.

Results: 58% ZigBee packets lost.

4.2.3.11Test 10 (ZigBee sensor in basement, maximum distance from modem router)

WiFi connection still worked but ZigBee devices were unable to bind with each other.

Dell PC indicated a received signal of -89 dBm and a noise level of -86 dBm.

Estimated distance between ZigBee devices: 15 m.

Obstacles: two floors including ground heating.

Results: 100% ZigBee packets lost.

4.2.3.12Test 11 (concrete wall, ZigBee devices at floor level)

Dell PC indicated a received signal of -69 dBm and a noise level of -91 dBm.

Estimated distance between ZigBee devices: 10 m (ZigBee sensor in parents bedroom and ZigBee light in second floor bathroom).

Obstacles: one concrete wall, one plaster wall.

Results: No ZigBee packets lost.

4.2.4 Conclusions

The above-described sequence of tests represent typical use patterns in a real home environment. Different WiFi traffic profiles have been used (simple web surf, file download, audio streaming) to assess the coexistence properties of ZigBee in various operating conditions. Results show that, under all interferer traffic patterns, no single ZigBee packet has been lost. The only cases that experienced lost packets were due to propagation issues in which ZigBee packets had to cross two floors.

5 Laboratory Tests

5.1 Description of Test Environment

Interference tests have been performed at Schneider Electric Innovation Department's wireless laboratory in order to characterize potential theoretical coexistence limits. The aim was to generate various WiFi traffic patterns and assess the impact on ZigBee of varying parameters such as WiFi power level, WiFi duty cycle, and physical distance between devices.

5.1.1 Test Platform

A test platform based on Spirent's SmartBits 600 performance analysis system (Figure 20) has been designed by Schneider Electric for various research purposes involving Ethernet and WiFi communications. This tool enables to generate and control traffic corresponding to user-defined traffic protocols and bandwidth occupancy.

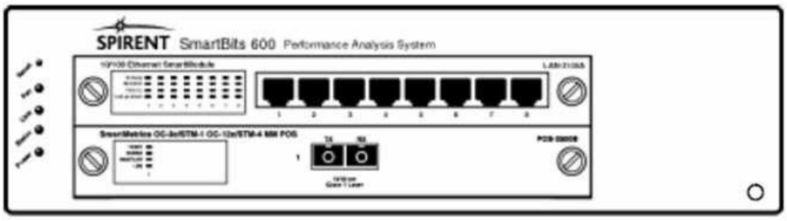
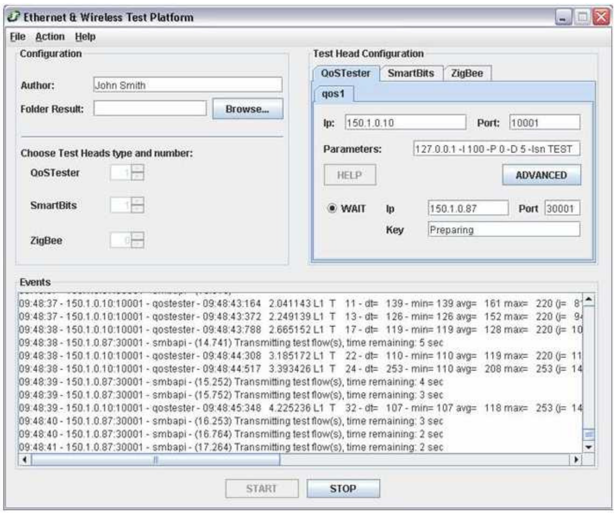


Figure 20 – Spirent SmartBits 600 performance analysis system

On top of this tool, Schneider Electric has built up an Ethernet and wireless test platform allowing to carry out various traffic performance measurements. Figure 21 shows the platform user interface.



Author: John Smith

Folder Result:

Choose Test Heads type and number:

QoSTester 1

SmartBits 1

ZigBee 0

Ip: 150.1.0.10 Port: 10001

Parameters: 127.0.0.1 -I 100 -P 0 -D 5 -lsn TEST

● WAIT Ip 150.1.0.87 Port 30001

Key Preparing

```
09:48:37 - 150.1.0.10:10001 - qostester - 09:48:43:164  2.041143 L1  T   11 - dt=  139 - min= 139 avg=  161 max=  220 (j=  8
09:48:37 - 150.1.0.10:10001 - qostester - 09:48:43:372  2.249139 L1  T   13 - dt=  126 - min= 126 avg=  152 max=  220 (j=  9
09:48:38 - 150.1.0.10:10001 - qostester - 09:48:43:788  2.665152 L1  T   17 - dt=  119 - min= 119 avg=  128 max=  220 (j= 10
09:48:38 - 150.1.0.87:30001 - smbapi - (14.741) Transmitting test flow(s), time remaining: 5 sec
09:48:38 - 150.1.0.10:10001 - qostester - 09:48:44:308  3.185172 L1  T   22 - dt=  110 - min= 110 avg=  119 max=  220 (j= 11
09:48:38 - 150.1.0.10:10001 - qostester - 09:48:44:517  3.393426 L1  T   24 - dt=  253 - min= 110 avg=  208 max=  253 (j= 14
09:48:39 - 150.1.0.87:30001 - smbapi - (15.252) Transmitting test flow(s), time remaining: 4 sec
09:48:39 - 150.1.0.87:30001 - smbapi - (15.752) Transmitting test flow(s), time remaining: 3 sec
09:48:39 - 150.1.0.10:10001 - qostester - 09:48:45:348  4.225236 L1  T   32 - dt=  107 - min= 107 avg=  118 max=  253 (j= 14
09:48:40 - 150.1.0.87:30001 - smbapi - (16.253) Transmitting test flow(s), time remaining: 3 sec
09:48:40 - 150.1.0.87:30001 - smbapi - (16.764) Transmitting test flow(s), time remaining: 2 sec
09:48:41 - 150.1.0.87:30001 - smbapi - (17.264) Transmitting test flow(s), time remaining: 2 sec
```

Figure 21 – Ethernet and wireless test platform interface

Using this test platform, a test sequencer (depicted in Figure 22) allows to automate the whole configuration and traffic generation procedure, as well as to collect test results in Excel files and sketch packet delivery histograms in a user-friendly way.

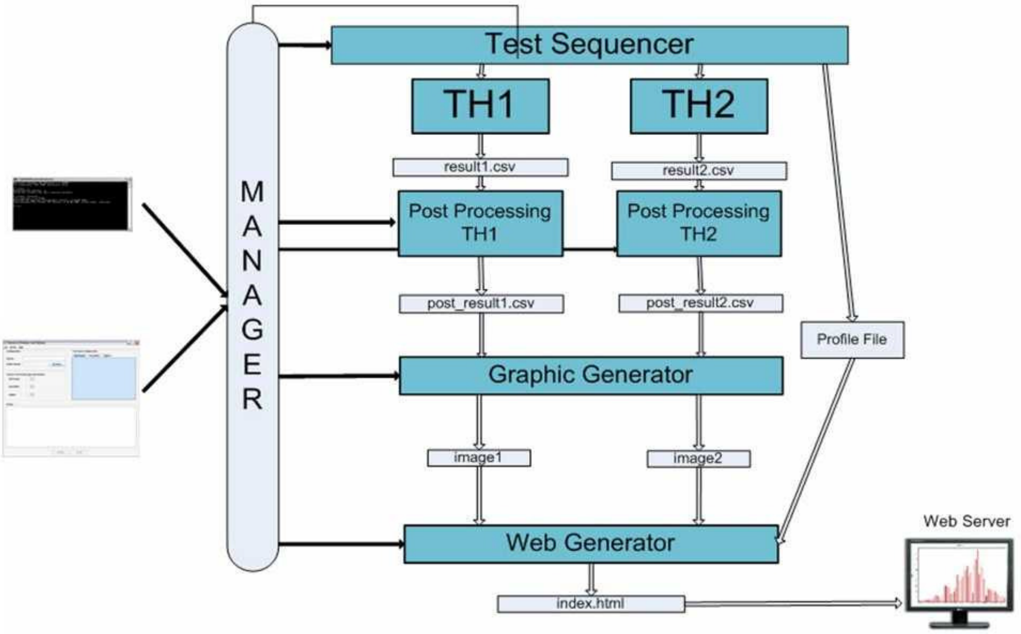


Figure 22 – Test platform sequence diagram

5.1.2 Interference Test Setup

Using the previously described traffic generator and test platform, a test setup has been elaborated to assess the coexistence between WiFi and ZigBee transmissions occurring on overlapping channels. Figure 23 illustrates the laboratory setup, in which one WiFi access point is transmitting to another WiFi access point according to traffic characteristics specified by the traffic generator. Interfering devices are further described in Table 10. Two ZigBee devices, whose characteristics are listed in Table 11, are exchanging simple lighting commands, with one of them logging latency and packet delivery results in a file that can further be utilized by the test platform to display the outcome of the whole testing process. A physical wire was placed between the two ZigBee devices to accurately determine the packet delivery latency.

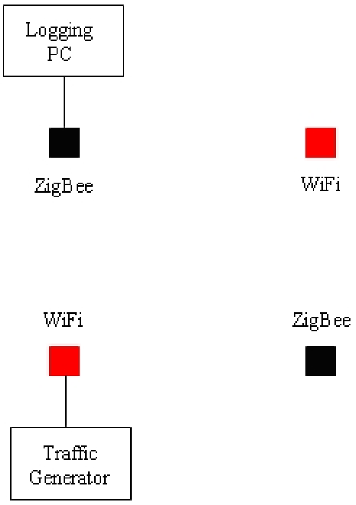


Figure 23 – Laboratory test setup

Characteristics of WiFi devices	
Manufacturer/Type	Linksys WAP54
WiFi Modes	IEEE 802.11b/g
WiFi Power Level	Variable (20 mW nominal)
WiFi Channel in Use	3

Table 10 – Characteristics of WiFi devices

Characteristics of ZigBee Devices	
Hardware	Ember EM250 evaluation board
Software	EmberZNet 3.0.2 (pre-ZigBee PRO) stack
ZigBee Power Level	1 mW
ZigBee Channel in Use	14 (overlap with WiFi channel 3)

Table 11 – Characteristics of ZigBee devices

5.1.3 Interference Test Procedure

Several test batches have been run by changing the following parameters:

- IEEE 802.11b mode and IEEE 802.11g mode.
- Distance between ZigBee devices: 1.5 m and 6 m.
- Distance between WiFi devices: 1.5 m.
- Minimal distances between ZigBee and WiFi devices: 1 m and 0.2 m.
- WiFi power level: variable, from a nominal value of 20 mW.
- Using ZigBee application-level retransmissions (APS retries).

Each test batch included 1 000 ZigBee commands launched every 3 s. ZigBee packets that were not received after 1 s were considered lost.

5.2 WiFi Traffic Patterns

In order to assess coexistence in representative WiFi applications, several traffic profiles have been defined in the test platform. The rationale of these profiles is described below, as well as the corresponding parameters used to configure the SmartBits traffic generator.

5.2.1 Data Traffic

5.2.1.1 Traffic Description

Two types of data flows should be considered:

- Transactional: Bandwidth is expected to be lower than 5 kbps. It corresponds to interactive client/server applications such as Telnet sessions and web surfing. This type of data flow is bursty.
- File transfer: Nowadays a data rate of 10 Mbps should be acceptable. This type of data flow attempts to use all the bandwidth available for a few minutes. It is not sensitive to packet loss or delays. Note that a few file transfers can occur during web browsing (for image or audio download).

With IPv4 the minimum MTU that routers and physical links were required to handle is 576 bytes. With IPv6 all links must handle a datagram size of at least 1 280 bytes. Ethernet maximum data payload is 1 500 bytes.

5.2.1.2 Traffic Requirements

Bandwidth and maximum delay required really depend on application. Still, it is well known that an application should provide feedback in less than 250 ms in order for the user to feel there is no delay.

For Internet Table 12 presents some typical performance figures.

Continent	Average Response Time	Average Packet Loss
Asia	327 ms	3%
Australia	285 ms	0%
Europe	180 ms	1%
North America	67 ms	0%
South America	160 ms	0%
Globally	**127 ms**	**< 1%**

Table 12 – Typical Internet performance according to world regions

On-line gaming requires latency between 30 and 50 ms. Game developers are advised to build application accepting latency between 50 and 120 ms. The majority of online games needs a throughput of at least 256 kbps, preferably 1 to 2 Mb/s (upstream and down-stream).

5.2.1.3 Summary

Following the description above, recommended configuration parameters for data traffic pattern are:

- Data rate: 10 Mbps.
- Packet size: 576 bytes.
- Network delay: < 50 ms.
- Network jitter: Not significant for this type of traffic flow.
- Packet loss: < 1%.

5.2.2 Voice Traffic

5.2.2.1 Traffic Description

Global switched-circuit telephone networks reserve a 64 kbps bandwidth for voice following ITU recommendation G.711. But codecs actually used for VoIP might use a lower data rate (32 kbps for G.726 down to 5.3 kbps for G.723.1). Payload size depends on codec used but is lower than 240 bytes, as shown in Table 13. Note that G.729 is the default VoIP codec.

Codec	Data Rate	Payload Size	Packetization Delay / Payload Size
G.711 (PCM)	64 kbps	160 bytes (default) 240 bytes	20 ms 30 ms
G.729 (CS-ACELP)	8 kbps	20 bytes (default) 30 bytes	20 ms 30 ms
G.723.1 (MP-ACELP)	5.3 kbps	20 bytes (default) 60 bytes	30 ms 60 ms

Table 13 – Payload sizes for various codec specifications

The protocol used to transfer the payload might require some extra bytes for headers:

- Ethernet IEEE 802.3: 21 bytes.
- IP: 20 bytes (IPv4), 40 bytes (IPv6).
- UDP: 8 bytes.
- RTP: 12 bytes header.

In circuit-switched voice networks, all voice calls use 64 kbps fixed-bandwidth links regardless of how much of the conversation is speech and how much is silence. In VoIP networks, all conversation and silence are normally packetized. However, packets of silence can be suppressed using VAD. Over time and as an average on a volume of more than 24 calls, VAD may provide up to 35% bandwidth saving. For a single call, this number is reduced. Features such as music on hold render VAD ineffective.

5.2.2.2 Traffic Requirements

Delay

The ITU addresses network delay for voice applications in recommendation G.114 (Table 14).

One-way Delay Range	Description
Under 150 ms	Acceptable for most user applications
150 – 400 ms	Acceptable provided that administrators are aware of the transmission time and the impact it has on the transmission quality of user applications
Above 400 ms	Unacceptable for general network planning purposes

Table 14 – Classification of ITU network delay ranges

These figures are for a one-way delay. Other sources indicate that callers usually notice roundtrip voice delays of 250 ms or more.

Typical sources of delays are:

- Packetization delay: Around 30 ms, depending on sample size. This is the time to fill a packet with voice payload.
- Coder delay: Around 20 ms, depending on sample size and codec. It includes the DSP processing time to compress a block of PCM sample and the look ahead delay of the compression algorithm.
- Serialization delay: Around 5 ms, depending on frame size and line clock rate. When using a trunk, it corresponds to the delay required to clock a voice frame onto the network interface. So it is directly related to the clock rate of the line.
- Queuing/buffering delay: Variable delay, depending on traffic. When using Ethernet, it corresponds to the encapsulation in an IP packet and access to Ethernet using CSMA/CD.
- Network switching delay: Variable, around 100 µs, depending on the Ethernet switch hardware. It is the time used to transmit data from one port of the switch to the other one. Switching is assumed to use MAC addresses.
- Propagation delay: 0.5 µs for 100 m. The speed of electrons in a copper line is around 200 000 km/s.

Once all codec delays have been subtracted, the recommended network latency can be evaluated between 45 and 65 ms.

Jitter

Network jitter can be measured in several ways. The recommended acceptable value is usually between 0.5 and 2 ms. This requirement can be loosen using buffering as long as delay is still acceptable.

Packet Loss

Intelligibility of the conversation is also decreasing with packet loss. Different levels of quality are defined: Telecom quality (G.711 standard for toll quality), clear, understandable, non understandable. VoIP is not tolerant to packet loss. Even 1% packet loss can significantly degrade a VoIP call using a G.711 codec. Other more compressing codecs can tolerate even less packet loss. If TCP is used, packet loss is even worse as retransmissions create additional delays.

The recommended acceptable packet loss is between 0 and 0.5%.

5.2.3 Video Traffic Pattern

5.2.3.1 Traffic Description

Bandwidths required for different types of video flows are summarized in Table 15.

Video Types	Required Data Rates
MPEG-1 Video	1.5 Mbps (352 x 288 + sound)
Camcorder	1.5 Mbps (352 x 288) 8.5 Mbps (720 x 576)
MPEG-2 DVD	9.8 Mbps (720 x 576, 25 frames/s)
MPEG-2 SD	6 Mbps (720 x 576, 24 frames/s: TNT, DVB-T)
MPEG-2 HDTV	19.4 Mbps (1080i or 720p, 24 frames/s, over the air)
HDV	19 Mbps for 1080i or 25 Mbps for 720p

SD: Standard Definition
HDTV: High Definition Television
HDV: High Definition Video for recording compressed video on Digital Video (DV) tape

Table 15 – Required data rates for various types of video flows

It is important to note that MPEG-2 generates a variable bit rate. This results from the encoding scheme; when MPEG or H.261 methods for compression are used, the bit rate varies depending on the level of motion between frames. A coded video or audio frame is fragmented into MPEG-2 transport packets. These packets have a fixed size of 188 bytes. A 13 bit packet identifier is present in every MPEG-2 packet, which allows multiplexing of different flows over the same transport channel. To carry MPEG-2 over IP, UDP is most commonly used. Typically, 7 MPEG-2 packets are placed in a UDP message. So frame size over Ethernet would be 1 362 bytes.

Other formats could be used:

- H323 or H261 (used often for video surveillance or video conferencing)
- MJPEG (Motion JPEG)

These flows are also encapsulated in UDP/IP packets. They have a high level of compression. Timing constraints are weaker than MPEG-2, but video frames exchanged might be large and as a consequence need to be sent as a fragmented IP stream.

Bandwidths required for different types of audio flows are summarized in Table 16.

Audio Types	Required Data Rates
CD	1.411 Mbps (44.1 kHz / 16 bit)
DVD Audio	9.6 Mbps (Meridian Lossless Packing)
DVD Video	6.4 Mbps (lossy compression systems)
SACD	2.8 Mbps

Table 16 – Required data rates for various types of audio flows

It should be noted that these are standard formats. Available products usually convert an analog input into digital data to distribute the flow. Data formats used are unknown and so are the constraints. Here we will consider MPEG-2 only as it is the common standard.

5.2.3.2 Traffic Requirements

Most video broadcasts use MPEG-2 transport standard. ISO 13818-1 details how MPEG-encoded digital video and audio streams should be multiplexed, packetized and encoded into transport streams. MPEG-2 is sensitive to jitter because the transport stream carries timing information used by the receiver to decode and regenerate the program. If jitter is too important, overflow and underflow might occur at the decoder buffer, which could generate packet loss.

Timing information inserted by the encoder is called PCR and provides a resolution of 1 in 27 000 000. It is inserted into the transport stream at intervals of 100 ms (or 40 ms for DVB compliance). It is a real-time snapshot of the counter in the encoder. The receiver extracts this counter to regenerate a 27 MHz video clock that is locked in phase to the encoder. ISO 13818-1 specifies a maximum PCR jitter of 500 ns but excluding the transport layer. Most common decoders cannot lock on the encoder clock when jitter exceeds 500 ns. So buffering is required to get rid of jitter.

MPEG-2 defines four levels of coding parameter constraints (Table 17). Note that constraints are upper limits and that codecs may be operated below these limits (e.g. a high-1440 decoder will decode a 720 pixels by 576 lines picture).

Level	Max Frame Width [pixels]	Max Frame Height [pixels]	Frame Rate [Hz]	Data Rate [Mbps]	Buffer Size [bytes]
Low	352	288	30	4	475 136
Main	720	576	30	15	1 835 008
High-1440	1 440	1 152	60	60	7 340 032
High	1 920	1 152	60	80	9 781 248

Table 17 – MPEG-2 levels

In broadcasting terms, standard-definition TV requires Main level and HDTV requires High-1440 level. The bit rate required to achieve a particular level of picture quality approximately scales with resolution. Standards for HDTV are given in Table 18.

Standard	Resolution x Definition	Format	Refresh Rate
720p	1 280 x 720	16/9	24p (cinema standard), 30p or 60i
1080i	1 920 x 1 080	16/9	24p (cinema standard), 30p or 60i

Table 18 – HDTV standards [(p) progressive, (i) interlaced]

Recommended network delay and jitter vary depending on references.

Reference 1

IEEE 802.3 Residential Ethernet CFI defines the following applications and requirements:

- Multi-room synchronization
  - Audio playback synchronized across multiple rooms (latency must be small enough to prevent reverberation).
  - Video playback synchronized across multiple rooms.
- Jam session (based on Gibson Guitar experiment)
  - Multiple instruments with live effects and mixing.
  - Turn on instruments and immediately begin playing.

- Network Video Trickplay
  - Multiple HDTVs accessing recorded shows on a DVD player.
  - Each TV attempts slow/fast playback at the same time.

Application	Maximum Latency
Multi-room synchronous audio playback	500 µs
Jam session	500 µs
Audio/video conferencing	100 ms (round trip including application layer)
Network Video Trickplay	100 ms (round trip including application layer)

Table 19 – Maximum latency for Reference 1

This same group recommends also a jitter equal to 0 ms.

Reference 2

Another study performed by Cisco provides different results.

Flow Type	Maximum Latency	Maximum Jitter
MPEG1 1.5 Mbps Video	5 ms	6.5 ms
MPEG2 19.4 Mbps HDTV	800 µs	1 ms

Table 20 – Maximum latency and jitter for Reference 2

5.2.3.3 Summary

Final recommended configuration parameters for video traffic are:

- Data rate: 19.4 Mbps up to 60 Mbps.
- Packet size: 1 362 bytes (over Ethernet).
- Network delay: < 500 µs.
- Network jitter: 0 (without buffering for de-jitterization).
- Packet loss: None.

5.3 Results

5.3.1 Arbitrarily Loaded Traffic

In order to assess the coexistence limitations of ZigBee, WiFi traffic has been loaded with UDP packets at several duty cycles and using different power levels. Although this traffic pattern is theoretical and does not take into account real-life traffic constraints (delay, jitter, …), this experiment allowed to underline the impact of WiFi on ZigBee in extreme conditions.

5.3.1.1 IEEE 802.11b

Tests in IEEE 802.11b mode have been run using Acksys equipment operating at a unique power level of 100 mW. Results provided in Table 21 show that IEEE 802.11b transmissions affect ZigBee traffic for duty cycles above 60%. They also underline the impact of transmitting at the maximum WiFi power level allowed.

Duty Cycles	Packet Loss 100 mW
20%	0%
50%	0.01%
60%	80%
70%	85%

Table 21 – ZigBee packet loss results for IEEE 802.11b arbitrarily loaded traffic

5.3.1.2 IEEE 802.11g

Tests in IEEE 802.11g mode have been run using the Linksys equipment, which allowed to go up to 50 mW power level. Above 40% duty cycle, the SmartBits traffic generator was not able to create reliable traffic. Table 22 provides the corresponding results and clearly shows that increasing both WiFi duty cycle and WiFi power level affects ZigBee packet delivery rate.

Duty Cycles	Packet Loss 20 mW	Packet Loss 30 mW	Packet Loss 50 mW
10%	0%	0%	0%
20%	0%	0%	0%
40%	0%	4%	9%

Table 22 – ZigBee packet loss results for IEEE 802.11g arbitrarily loaded traffic

5.3.2 Data Traffic

5.3.2.1 IEEE 802.11b

Figure 24 shows the resulting latency histogram for 1 000 ZigBee packets sent under the data WiFi traffic. In IEEE 802.11b mode, the Linksys equipment in use commands the power value to be at nominal level, i.e. 20 mW.

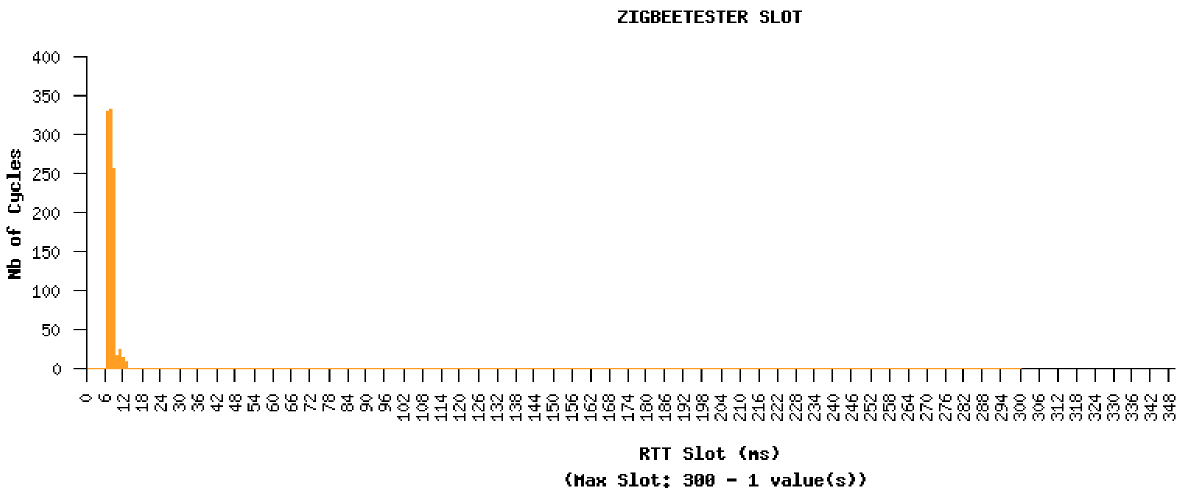


Figure 24 – ZigBee latency histogram for IEEE 802.11b data traffic at nominal power

5.3.2.2 IEEE 802.11g

Figure 25 and Figure 26 show the resulting latency histogram for 1 000 ZigBee packets sent under the data WiFi traffic at, respectively, 20 mW and 50 mW.

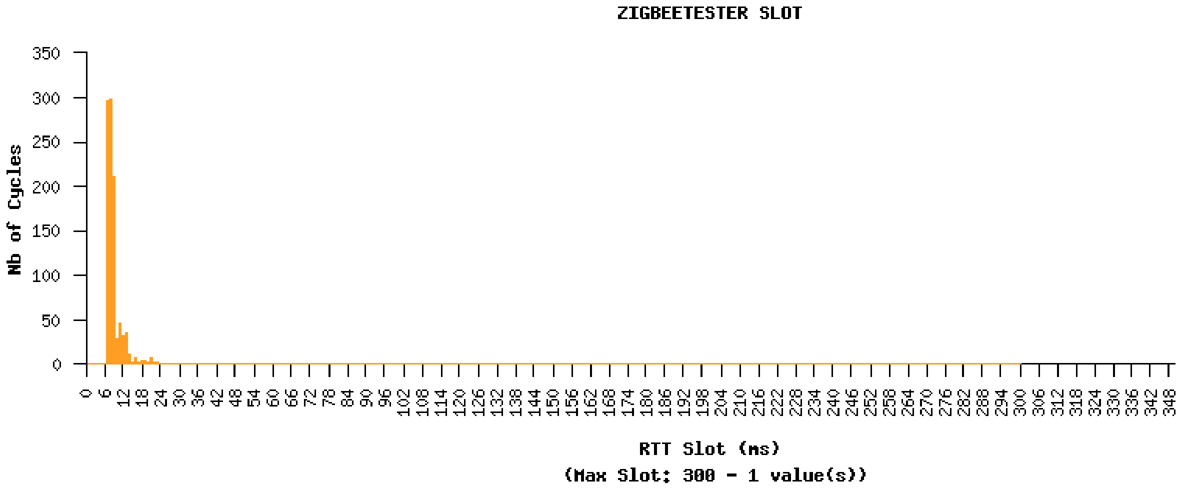


Figure 25 – ZigBee latency histogram for IEEE 802.11g data traffic at 20 mW

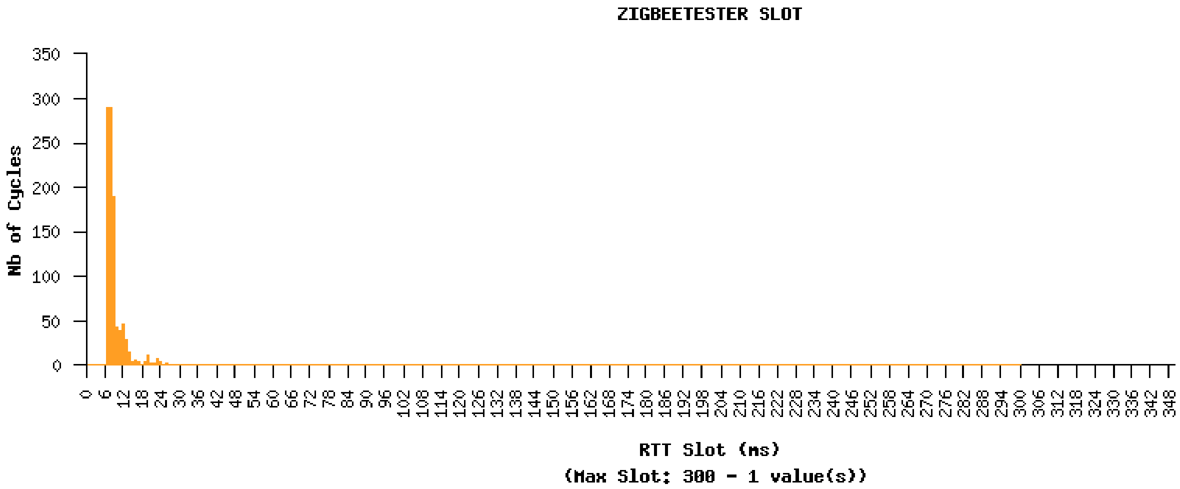


Figure 26 – ZigBee latency histogram for IEEE 802.11g data traffic at 50 mW

5.3.3 Voice Traffic

5.3.3.1 IEEE 802.11b

Figure 27 shows the resulting latency histogram for 1 000 ZigBee packets sent under the voice WiFi traffic. In IEEE 802.11b mode, the Linksys equipment in use commands the power value to be at nominal level, i.e. 20 mW.

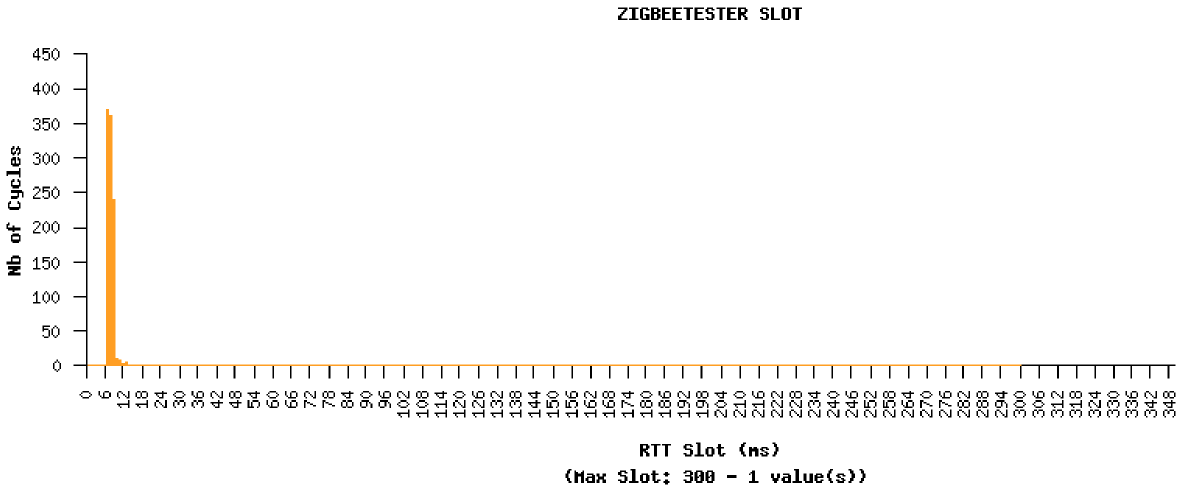


Figure 27 – ZigBee latency histogram for IEEE 802.11b voice traffic at nominal power

5.3.3.2 IEEE 802.11g

Figure 28 and Figure 29 show the resulting latency histogram for 1 000 ZigBee packets sent under the voice WiFi traffic at, respectively, 20 mW and 50 mW.

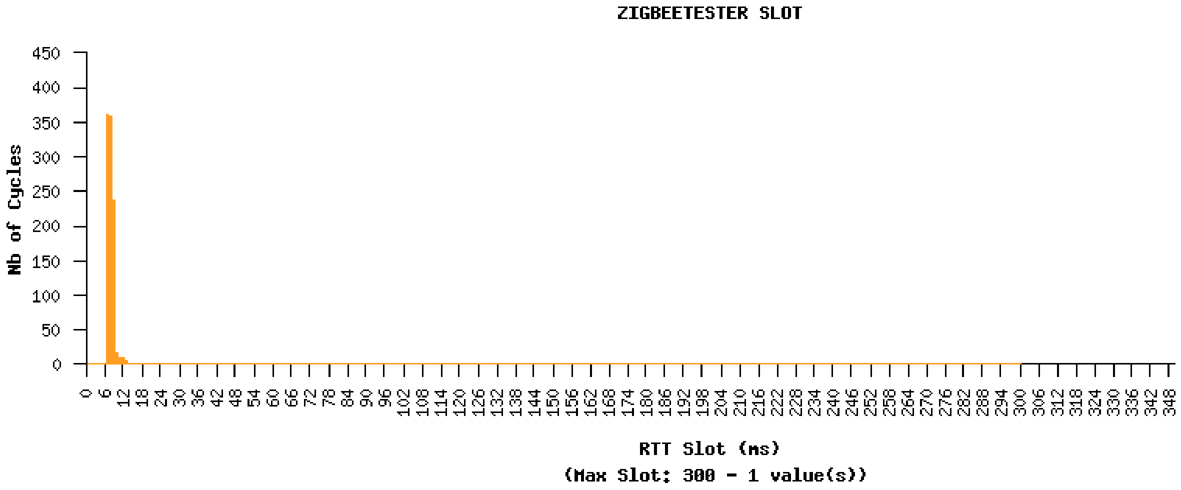


Figure 28 – ZigBee latency histogram for IEEE 802.11g voice traffic at 20 mW

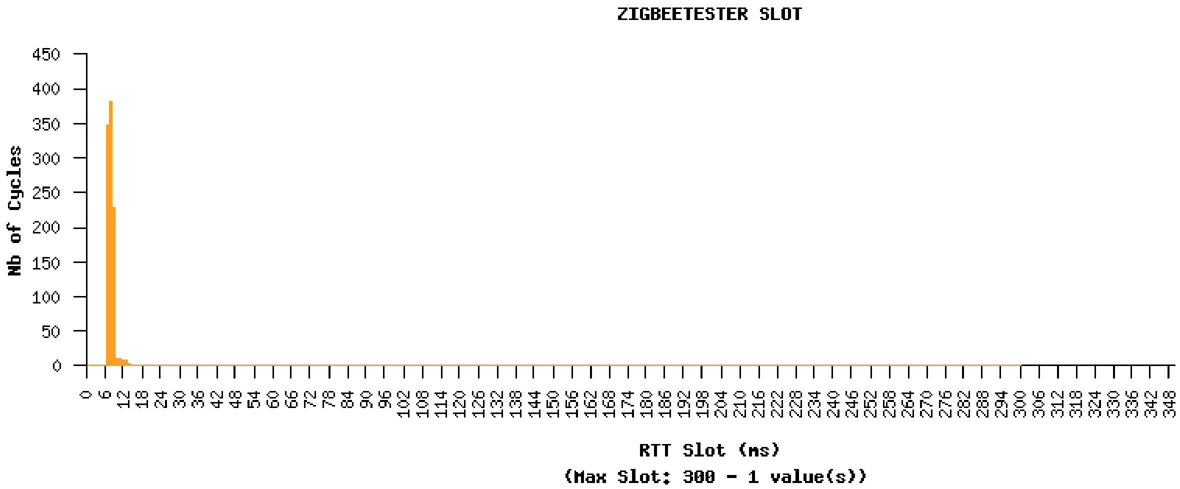


Figure 29 – ZigBee latency histogram for IEEE 802.11g voice traffic at 50 mW

5.3.4 Video Traffic

5.3.4.1 <u>IEEE 802.11b</u>

Figure 30 shows the resulting latency histogram for 1 000 ZigBee packets sent under the video WiFi traffic. In IEEE 802.11b mode, the Linksys equipment in use commands the power value to be at nominal level, i.e. 20 mW.

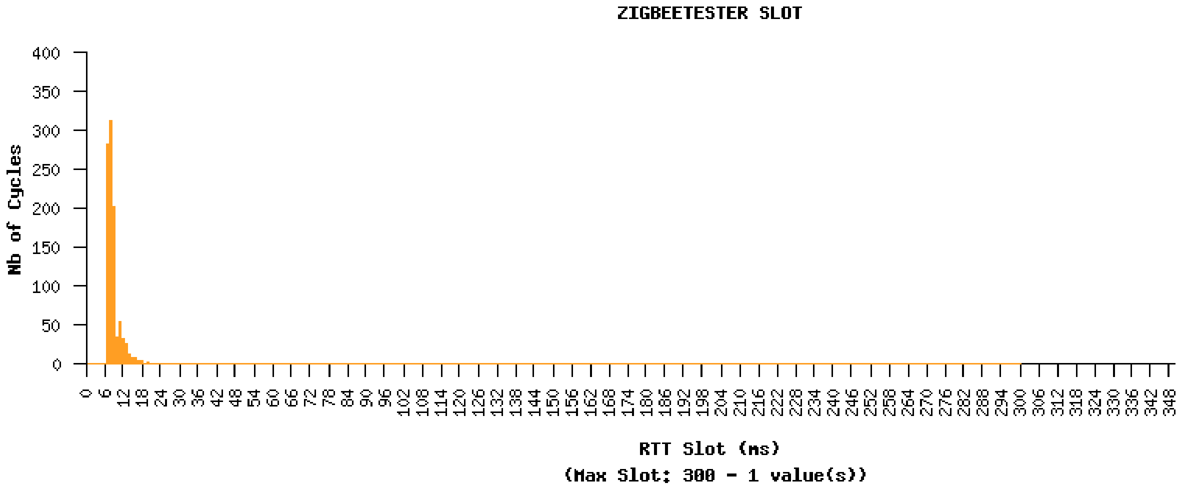


Figure 30 – ZigBee latency histogram for IEEE 802.11b video traffic at nominal power

5.3.4.2 <u>IEEE 802.11g</u>

Figure 31 and Figure 32 show the resulting latency histogram for 1 000 ZigBee packets sent under the video WiFi traffic at, respectively, 20 mW and 50 mW.

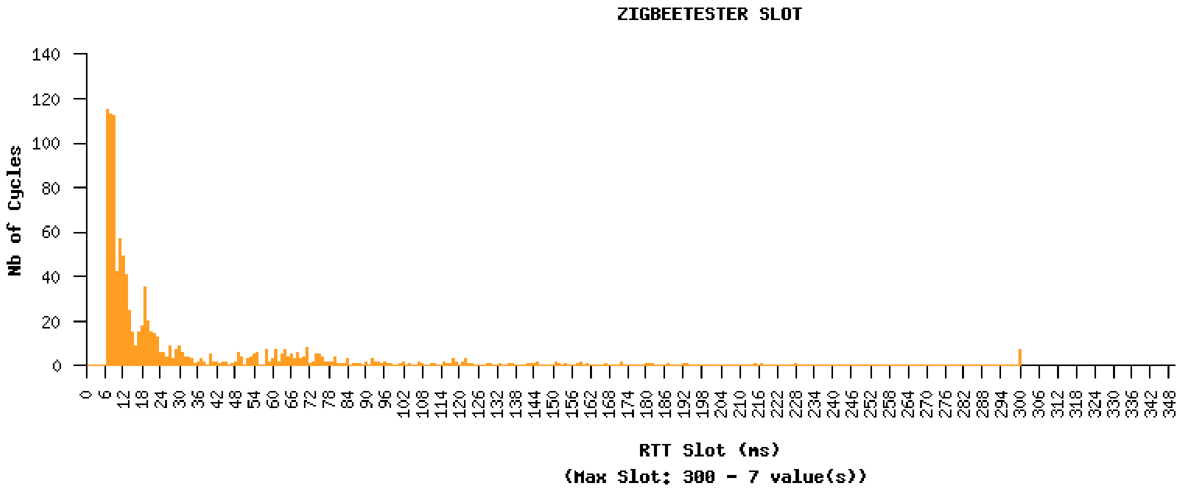


Figure 31 – ZigBee latency histogram for IEEE 802.11g video traffic at 20 mW

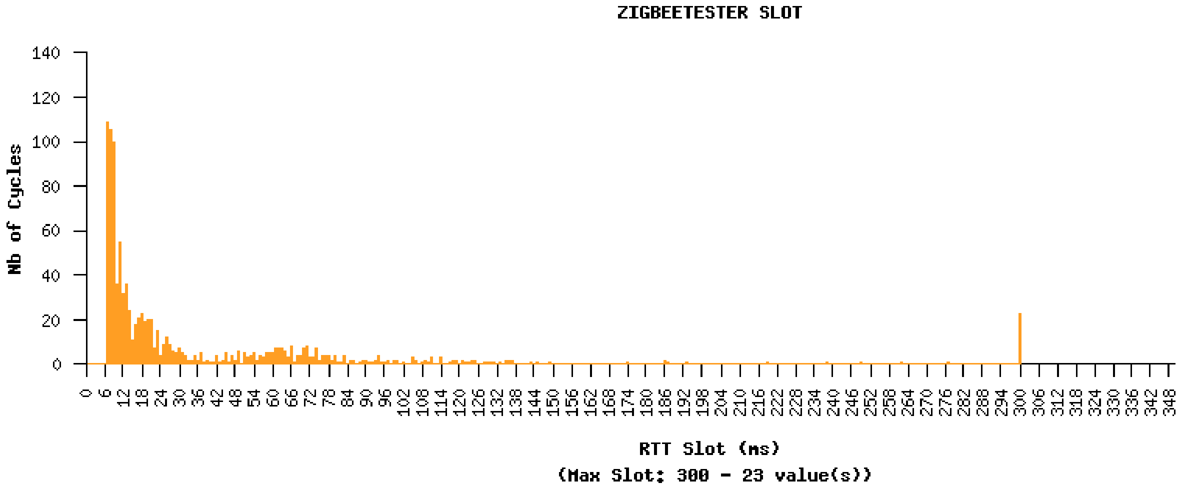


Figure 32 – ZigBee latency histogram for IEEE 802.11g video traffic at 50 mW

5.3.5 Summary of Results

The three following tables sum up the test results in terms of packet delivery and latency statistics for the three WiFi traffic profiles under study. They suggest that real WiFi traffic patterns do not have a significant impact on ZigBee transmissions. Latency is, as expected, increased under heavy WiFi traffic. This is especially true when WiFi power level is raised above its typical value (20 mW today for commercial equipments). Results also show that packet delivery can be slightly affected (1% loss) at higher WiFi power level for the toughest traffic pattern, i.e. video flow.

In the scenarios considered here, IEEE 802.11b and IEEE 802.11g modes provide comparable results. This could be understood by remembering that real traffic conditions are tied to network and hardware constraints that leave enough space on the channel to insert ZigBee transmissions.

Test Results	IEEE 802.11b	IEEE 802.11g	
WiFi Power Level	20 mW	20 mW	50 mW
Packet Loss	0%	0%	0%
Min Latency	6.9 ms	6.7 ms	6.2 ms
Max Latency	21.9 ms	26.9 ms	75.9 ms
Average Latency	8.3 ms	7.8 ms	7.7 ms

Table 23 – Test results for data traffic pattern

Test Results	IEEE 802.11b	IEEE 802.11g	
WiFi Power Level	20 mW	20 mW	50 mW
Packet Loss	0%	0%	0%
Min Latency	6.7 ms	6.8 ms	6.8 ms
Max Latency	20.9 ms	19.0 ms	20.0 ms
Average Latency	8.6 ms	7.4 ms	8.5 ms

Table 24 – Test results for voice traffic pattern

Test Results	IEEE 802.11b	IEEE 802.11g	
WiFi Power Level	20 mW	20 mW	50 mW
Packet Loss	0%	0%	1%
Min Latency	6.6 ms	6.9 ms	6.9 ms
Max Latency	58.3 ms	227.9 ms	276.9 ms
Average Latency	10.3 ms	29.3 ms	15.8 ms

Table 25 – Test results for video traffic pattern

6 Conclusions and Recommendations

The present study aimed at better characterizing the effect of WiFi transmissions on ZigBee traffic. This has been achieved following three investigation directions:

- Review of previous coexistence test results provided by both Schneider Electric and other research groups.
- Experiments carried out in two real houses using today's most typical WiFi applications.
- Laboratory experiments carried out at Schneider Electric using both real and arbitrarily loaded traffic patterns to assess potential coexistence limits.

All these investigations converge to the following conclusions:

- In presence of today's real WiFi applications (web surfing, file transfer, audio and video streaming), ZigBee operates satisfactorily, even in the most adverse interference conditions. Although ZigBee packets are delivered successfully, they can experience an increased latency due to a higher number of retransmissions. In real environments, WiFi interference is not an issue for ZigBee applications.
- When increasing WiFi's duty cycle and power level above what is achievable or available today (by arbitrarily increasing the channel occupancy), coexistence properties of ZigBee can be affected and packets can be lost. This is true in particular in IEEE 802.11b mode since interfering packets spend more time on air.

- These results confirm that although ZigBee/WiFi coexistence has theoretical limits that have been highlighted in our laboratory experiments, those limits are not reached today given real traffic conditions, hardware limitations or nominal power levels of commercial WiFi equipments.
- As a consequence, we do not see WiFi interference as an obstacle to incorporating ZigBee into home and building automation products. In order to cope with possible enhancements of WiFi technology and related equipments in the future, we also recommend to adopt frequency agility.