ZigBee®

Control your world™

June 2007

ZigBee and Wireless Radio Frequency Coexistence

Foreword

Since its inception, the ZigBee Alliance has worked with a singular focus: create a much needed global wireless language capable of giving "voices" to the myriad of everyday devices which surround us as we go about our daily lives. This focus has been aimed at the little devices, often overlooked in an IT centric world, such as light switches, thermostats, electricity meters and more complex sensor devices found abundantly in the commercial building and industrial automation worlds. As a result, ZigBee Alliance members have created a wireless standard offering extraordinary control, expandability, security, ease-of-use and the ability to use ZigBee technology in any country around the world. Today, companies use ZigBee to effectively deliver solutions for a variety of areas including energy management and efficiency, home and commercial building automation as well as industrial plant management. With this comprehensive set of attributes, the non-profit, open membership and volunteer driven Alliance has become a thriving ecosystem of more than 400 members. As an ecosystem, the Alliance offers everything prospective product and service companies need to develop ZigBee products and services and benefit from the Alliance's competitive and stable supply chain.

Executive Summary

ZIGBEE AND WLAN: HARMONIOUS COEXISTENCE FOR RELIABLE OPERATION

ZigBee is built using the Institute of Electrical and Electronics Engineers (IEEE) 802.15.4 standard and follows strict IEEE guidelines to ensure long-term sustainability and reliable operation. The IEEE, a non-profit organization, is the world's leading professional association for the advancement of technology. IEEE is a globally respected standards development group whose members are volunteers working in an open and collaborative manner. Other well known technologies like Bluetooth® (802.15.1) and Wi-Fi® (802.11) are part of the IEEE 802 standards family. The IEEE 802 group continually evaluates its standards to identify areas of ambiguity or concern and works to improve its standards to ensure robustness and long-term success. To be approved as an IEEE 802 standard, IEEE 802 wireless standards must develop a Coexistence Assurance Document and implement a plan as part of the standard that ensures that all 802 wireless standards can operate and coexist in the same space.

Thousands of IEEE members, some of the world's leading scientists and technologist, collaborate and spend thousands of man hours to define standards. Also, since many of the same scientists and technologists work together in several groups at the IEEE, standards such as 802.15.4 and 802.11 are designed to ensure reliable co-existence. In fact, products using both ZigBee and Wi-Fi have been designed and shipped by Alliance members, including Control4 and Digi International, and these products work as promised.

In addition to real-world use by customers, ZigBee members regularly show and demonstrate products around the world at some of largest tradeshows: Consumer Electronics Show, Electronica, Hannover Messe and Wireless Japan, to name a few. These shows often present the harshest locations for radio frequencies (RF) technologies to operate, with dozens of wireless networks including Wi-Fi, Bluetooth and other RF traffic. At times, it can be difficult to get wireless devices to operate properly at these shows, yet users and demonstrators of ZigBee networks report reliable performance.

ZIGBEE ALLIANCE: QUALITY INDEPENDENTLY ASSURED

The ZigBee Alliance's more than 400 members are spending billions of dollars around ZigBee. These companies range from well known global brands to independent start-ups. Most have thoroughly and independently investigated ZigBee prior to investing funds to develop new ZigBee products and services.

Two independent and global test labs National Technical Systems and TUV Rheinland test and verify ZigBee platforms and products. These labs have global reputations to protect and are not ZigBee Alliance funded, rubber stamping organizations. The Alliance sets stringent standards for all products or platforms to ensure everything operates as promised, allowing customers to buy products wearing the ZigBee logo with confidence.

ZigBee Technology Facts

Attribute	ZigBee
Number of Channels	27
Radio Frequency Band[s]	• 2.4 GHz with 16 channels for global use • 915 MHz with 10 channels for N. America, Australia and a few additional countries • 868 MHz with 1 channel for EU countries
Network Capabilities	Self-organizing and self-healing dynamic mesh network based on ZigBee public standard
Network Size	Thousands of devices per network

ZIGBEE: CONTROL YOUR WORLD

Hundreds of companies have selected ZigBee as their wireless technology because ZigBee works. The following pages also provide evidence from both laboratory and real world environments proving reliability. Companies

are selling products with both Wi-Fi and ZigBee installed in the same device. Paul Williams, vice president of Support Services at Control4, says the following about coexistence with Wi-Fi:

> "In the two years we have been shipping products, we have not encountered an issue where ZigBee or Wi-Fi has interfered with, or caused problems with, the operation of products using either communications protocol. We ship products that contain both ZigBee and Wi-Fi technologies in the same physical product. Additionally, we have thousands of systems in operation today around the world with the majority of the installations containing both large ZigBee and Wi-Fi network implementations, all working without interference or problems."

The Alliance has deliberately maintained a commitment to quality by delivering a solid, robust and secure technology, rather than rushing to market. Independent industry analysts, members of the news media and other experts regularly praise ZigBee's technical merits, market approach and durability. As a result, ZigBee is seeing broad adoption by industries which demand products based on standards that deliver long-term stability and feature a solid and competitive supply chain.

Table of Contents

List of Figures

List of Tables

INTRODUCTION

The license-free industrial scientific and medical (ISM) bands have been crucial to the burgeoning market for wireless embedded technology but, as with any resource that is held in common, it is equally crucial that all users of the band act as good citizens. In particular, the designers and implementers of platforms and products must assume that, in the normal case, they will be sharing the RF medium with a variety of other radiators, both intentional and unintentional.

This white paper describes the efforts that the ZigBee Alliance and the IEEE 802.15.4 working groups have undertaken to ensure that ZigBee devices act as good citizens, and describes some experimental results demonstrating that these efforts have been successful.

USERS OF THE 2.4GHZ ISM BAND

The 2.4GHz ISM band has become particularly popular in the last few years such that households, and virtually all commercial buildings, are likely to have equipment that operates in this band. A short list of possible users and possible interferers includes:

- 802.11b networks
- 802.11g networks
- 802.11n networks
- Bluetooth Pico-Nets
- 802.15.4-based Personal Area Network (PAN)
- Cordless Phones
- Home Monitoring Cameras
- Microwave ovens
- Wireless headsets
- Motorola Canopy systems
- WiMax networks

With so many users, one might reasonably be concerned that crowding in the 2.4GHz band would be a problem. Furthermore, certain promoters of competing technologies that use a different but nonetheless crowded pair of ISM bands have attempted to exploit this concern to commercial advantage with a recent white paper.

Fear, uncertainty and doubt (FUD) aside, however, the sensible approach to the possibility of interference is to expect it and to design the system from the ground up with coexistence in mind. This is what the ZigBee Alliance has done.

COEXISTENCE IN ZIGBEE

The ZigBee stack, as shown in Figure 1, has four layers of which the top two are described in the ZigBee specification and the bottom two – the MAC sub-layer and PHY layer – are described in the IEEE 802.15.4 – 2003 standard.

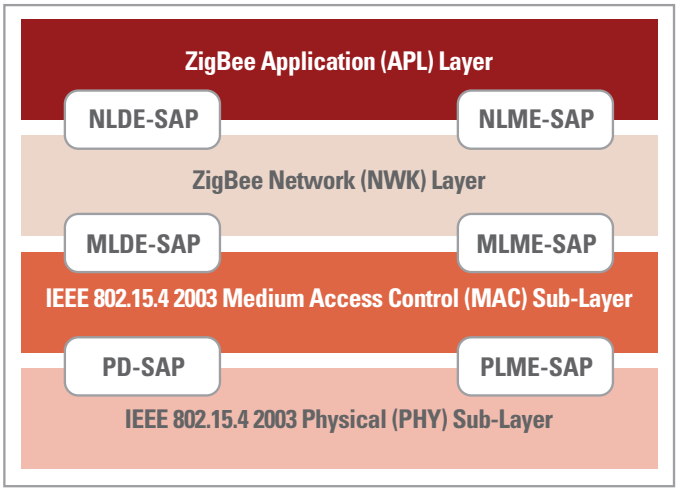


Figure 1 - The ZigBee Stack

Both specifications contain a great deal of functionality that is specifically designed to promote coexistence and mitigation of interference, and this functionality is distributed across all four layers.

IEEE 802.15.4

The policies of the IEEE require that each standards committee under its aegis publish a coexistence statement along with the text of the standard itself. A standard, regardless of its other merits, will not be approved until this coexistence statement has been deemed satisfactory. As a result, the IEEE 802.15.4 – 2003 specification provides support for coexistence at both the PHY layer and the MAC sub-layer, beginning with the physical layer and the adoption of direct sequence spread spectrum (DSSS) technology.

DSSS

The term "spread spectrum" refers to a class of technologies, which are designed to promote coexistence and robustness in the face of interference. There is a broadening consensus

in the standards community that proper use of spread spectrum is crucial for the fair and equitable sharing of ISM spectrum. To illustrate this point, Figure 2 shows a collision between two narrow-band signals, i.e. signals that use only a small band of frequencies around their designated center frequency or channel to encode and transmit information.

Note that even if the center frequencies of these signals are not exactly the same, the overlap can be substantial and is likely to cause data loss. It has been the function of regulatory bodies like the U.S. Federal Communications Commission (FCC) to prevent exactly these sorts of collisions between narrow-band signals by strictly regulating which radiators can operate on which channels of a particular band, and in which geographical regions. This protection is not available in the ISM bands and so users of narrow-band technology run the risk of encountering exactly these kinds of collisions.

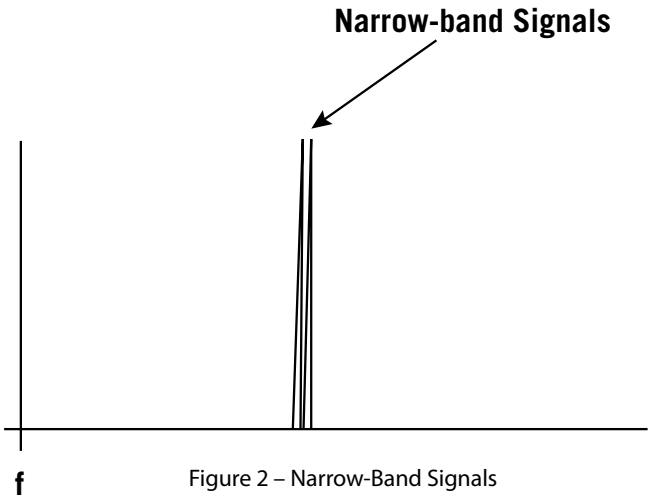


Figure 2 – Narrow-Band Signals

Contrast Figure 2 with Figure 3, which shows a spread signal in collision with a narrow-band signal. There are various spreading methods in common use, but the essential idea behind all of them is to use a bandwidth that may be several orders of magnitude greater than strictly required by the information that is being sent. Because the signal is spread over a large bandwidth, it can coexist with narrow-band signals, which generally appear to the spread-spectrum receiver as a slight reduction in the signal-to-noise ratio over the spectrum being used.

Spread spectrum technologies, such as the well-known code division multiple access technology employed in some mobile phones, can also be used to provide multiple access to a single channel.

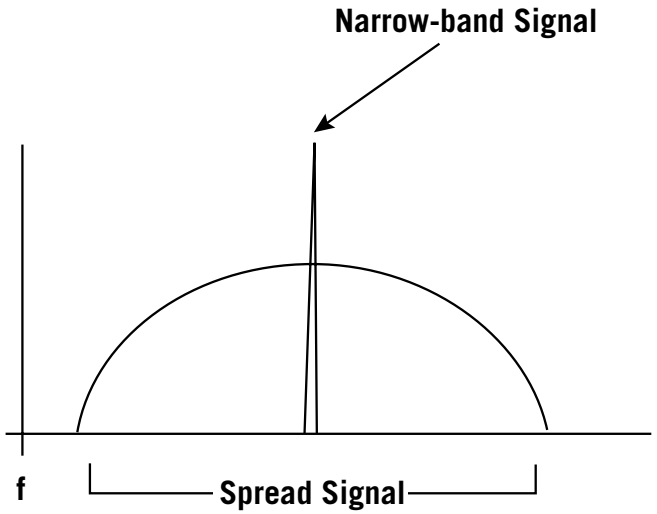


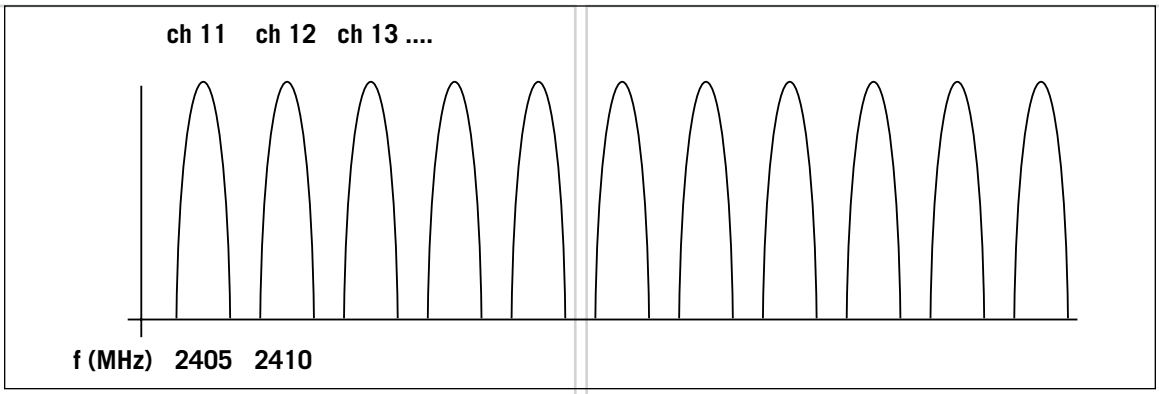
Figure 3 - Spread-Spectrum Signal

Thus, in the ISM bands, a kind of "more is less" approach, exactly opposite to the approach adopted by regulators like the FCC, turns out to be effective.

DSSS, the spreading technique employed by 802.15.4, makes use of a pseudo-random code sequence, often called a "chipping sequence," which is transmitted at a maximum rate called thechip rate. The chipping sequence is used to directly modulate the basic carrier signal – hence the name "direct sequence" – and to encode the data being transmitted. This method is employed, as pointed out above, in some cell-phone platforms, as well and in the widely deployed 802.11b and 802.11g WLAN technologies.

MULTIPLE CHANNELS

In addition to DSSS, 802.15.4 increases the opportunities for coexistence by employing a technique, generally known as frequency division multiple access (FDMA). This simply means that the standard divides the 2.4GHz ISM band into 16 non-overlapping channels, which are 5 MHz apart as shown in Figure 4. At least two of these channels, specifically 15 and 20, fall between the often-used and non-overlapping 802.11 channels 1, 6 and 11.



The minimum required resistance to signals from 802.15.4 devices operating other channels, called the jamming resistance, for a compliant radio is shown in Table 1.

Table 1 - Minimum Jamming Resistance

Adjacent Channel Rejection	Alternate Channel Rejection
0dB	30dB

As a result of these jamming resistance requirements, compliant devices operating in adjacent channels can coexist comfortably and that devices operating in more widely spaced channels will basically not hear each other.

DATA RATE

Many of the intended applications for ZigBee devices require a very low data rate. The obvious example is lighting where it should not take much more than a single bit, or a byte if the protocol designer is feeling profligate, to communicate the intention that a lighting device be turned on or off.

Many designers of RF systems intended to address these same applications have exploited this fact by building transmitters with data rates as low as 9.6Kbps. The designers of the IEEE 802.15.4 PHY; however, have chosen the relatively high data rate of 250Kbps. The reasoning here is that one of the best ways to promote coexistence is to reduce channel occupancy. Clearly, a radio with a high data rate will occupy the channel far less and offer fewer opportunities for collision with other users than one with a lower data rate.

BUILT-IN SCANNING AND REPORTING

In order to fully exploit the opportunity afforded by multiple channels under 802.15.4, the interface to the PHY layer provides the ability to sample a channel and report whether the channel is clear to transmit. It also measures the energy, and thus the interference, that is present on a particular channel. The latter capability is carried through to the MAC and higher layers so that users of 802.15.4 radios have the ability to select the best available channel for operation.

CSMA

Even with the techniques described above in place, a ZigBee device may find itself sharing a channel with interferers. Undoubtedly, a ZigBee device will find itself sharing the channel with other ZigBee devices. One might then assume that if every device just transmits whenever it wants to, collisions would arise; however, this scenario has been accounted for. There are a number of ways to approach this problem but the approach taken by the IEEE in the 802.15.4 standard is one known as carrier sense multiple access (CSMA). This technique, which has been used successfully for years in Ethernet, has the virtue that it requires no synchronization between devices. Instead, it employs a simple "listen before you talk" strategy. The device, on listens to see if the channel is busy, and if it is, it waits before checking again. The concept is like the strategy of people trying to talk on a busy conference call – simply wait and then speak when no one else is talking.

In a simplified form, the algorithm is as shown in Figure 5. Note that, if the channel is busy and the device keeps failing to find a clear channel, the wait intervals increase exponentially. Also note that the wait intervals are random, which makes subsequent collisions less likely.

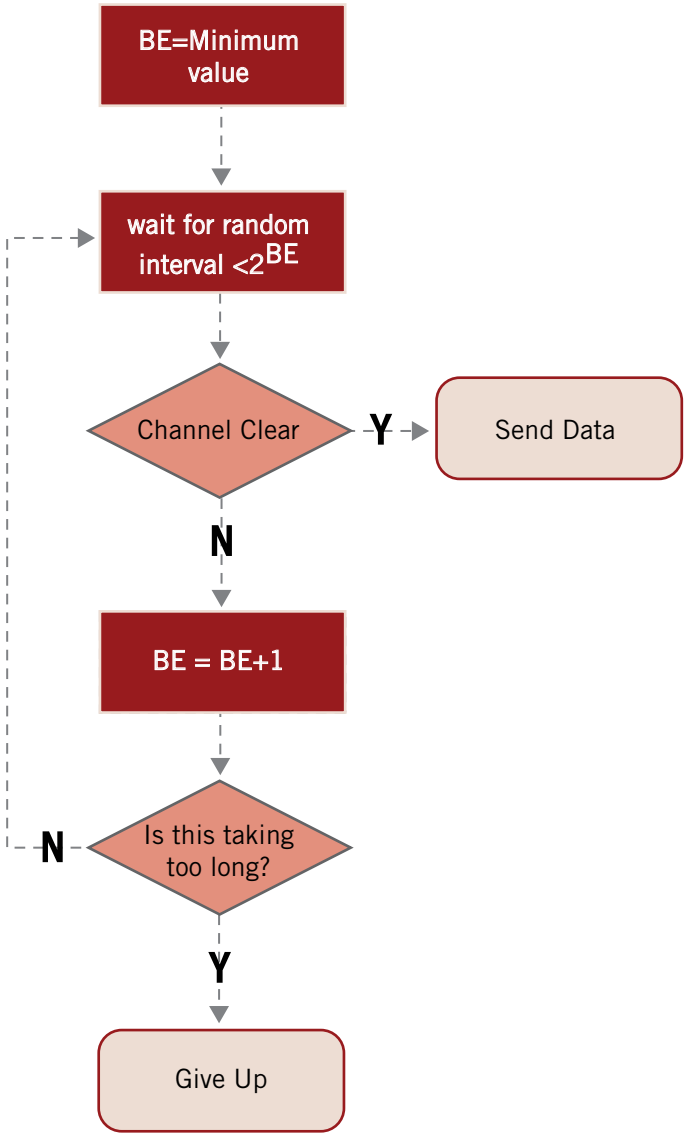


Figure 5 - CSMA

ACKNOWLEDGED TRANSMISSION AND RETRY

Often, devices transmit messages, but sometimes, the message is not successfully received. All communications are normally acknowledged in 802.15.4. Each device, on receipt of a message, has a brief time window in which it is required to send back a short message acknowledging receipt. The transmitting device will wait to hear this response, commonly known as an ACK. If it does not hear the ACK, it will assume that the message was not received, and will retry its message again. This process repeats until the message and ACK are both received or until, usually after a few tries, the transmitter gives up and reports a failure.

ADDITIONAL FEATURES OF ZIGBEE

The ZigBee standard builds on the IEEE 802.1.5.4 standard and adds networking and application support functionality. Among the many additional features are several that are intended to promote coexistence and mitigate interference.

NETWORK FORMATION PROCEDURES

When a ZigBee network is formed, the device that initiates formation, the ZigBee Coordinator (ZC), is required to scan through the list of available channels using the features provided by 802.15.4, and automatically select the best channel with the least interference.

MESH NETWORKING AND PATH DIVERSITY

ZigBee uses mesh networking technology. Mesh networking is motivated by the following two observations:

1. In many environments, the devices of interest are sufficiently close together that a robust network can be formed by simply allowing some of them to route messages on each other's behalf.

2. In this kind of environment, better use of the channel can be made if devices limit their transmit power and communicate only with their near neighbors.

Once a mesh network is in place, a number of possible paths exist between devices in the network as shown

in Figure 6. ZigBee exploits this path diversity by using a form of dynamic routing.

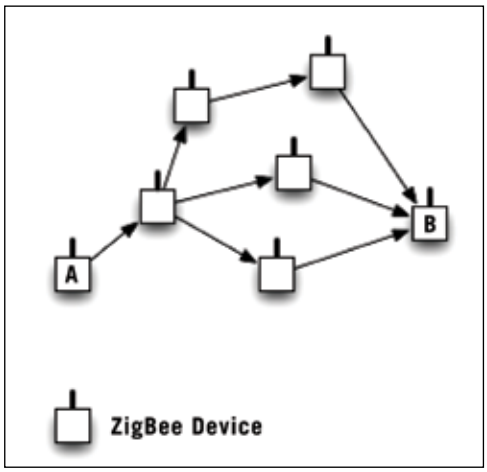


Figure 6 - Mesh Network

Should a chosen path fail, as a result of interference or some other change in the environment, the network will pick a different path as shown in Figure 7.

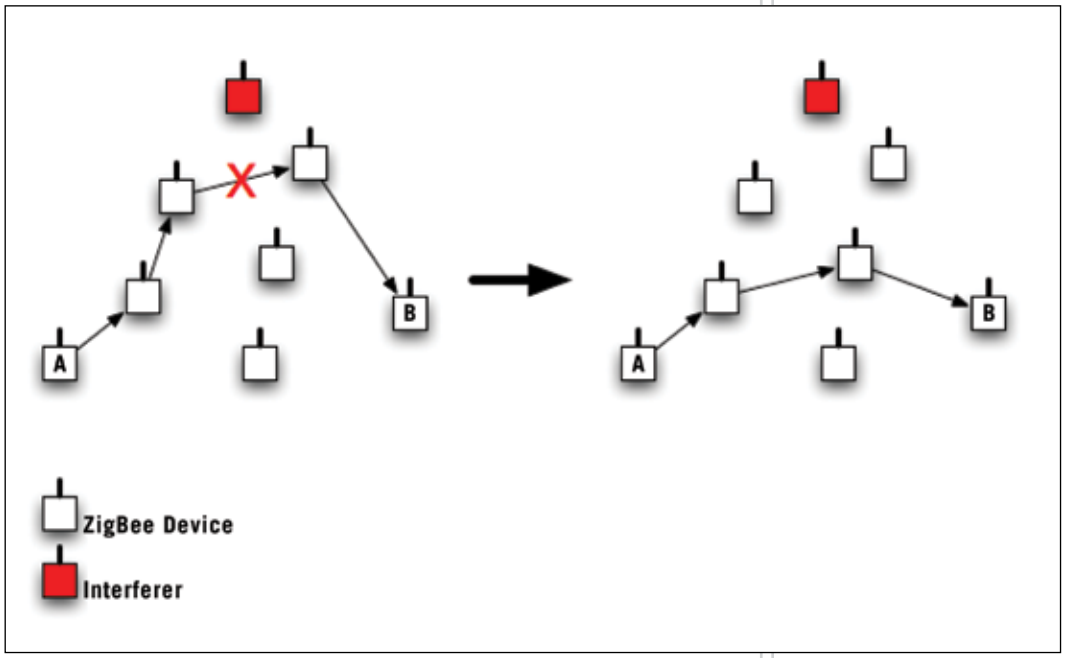


Figure 7 - Mesh Network with Interference

NETWORK-LAYER FREQUENCY AGILITY

In cases where the interference detected by the ZC, as described above in Section 3.2.1, changes or fails to reflect the interference profile for the network as a whole, ZigBee devices use the scanning facilities in 802.15.4 to detect interference and report it to the ZC or a device acting as the network manager. This device may direct the network to leave the channel it is currently using and form on another channel.

END-TO-END ACKNOWLEDGEMENT AND RETRANSMISSION

Just as single-hop transmissions in 802.15.4 are acknowledged and retried if they fail, multi-hop transmissions through the mesh may also be acknowledged and retried in ZigBee.

ZigBee Performs

There has been a great deal of evidence to suggest that ZigBee devices perform efficiently and effectively in a variety of environments. For example, ZigBee Alliance member Control4 (http://www.control4.com/) produces wireless home automation solutions. Paul Williams, their VP of Support Services, says the following about coexistence with Wi-Fi:

"In the two years we have been shipping products, we have not encountered an issue where ZigBee or Wi-Fi has interfered with, or caused problems with, the operation of products using either communications protocol. We ship products that contain both ZigBee and Wi-Fi technologies in the same physical product. Additionally, we have thousands of systems in operation today around the world with the majority of the installations containing both large ZigBee and Wi-Fi network implementations, all working without interference or problems."

Furthermore, ZigBee Alliance members demonstrate products at some of the world's largest trade shows each year. These shows provide a great Petri dish for studying ZigBee coexistence. The show floor at a trade show is a soup of communications technologies including IEEE

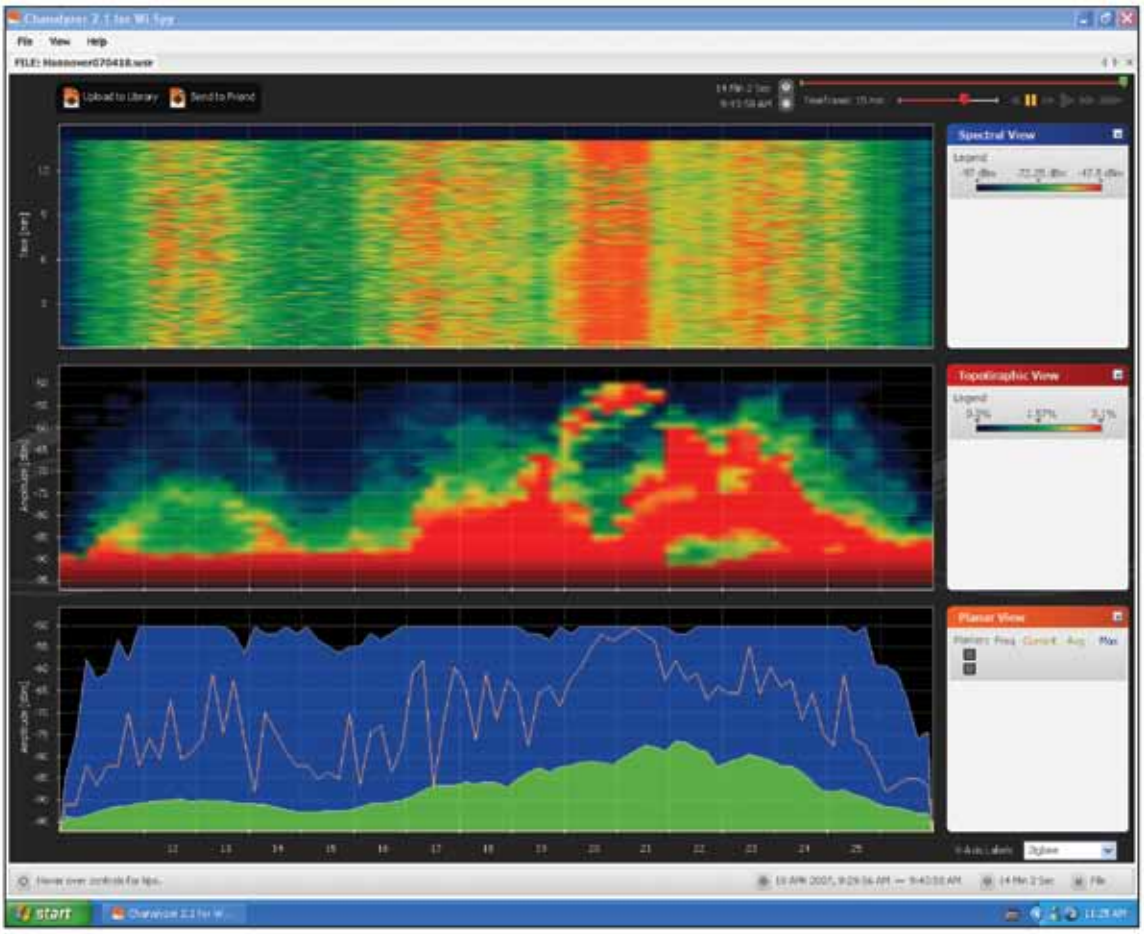


Figure 8 - Hannover Messe Spectrum

802.11b/g, Bluetooth, IEEE 802.15.4, 2.4GHz frequency hopping spread spectrum portable phones and numerous proprietary wireless technologies. Even in this demanding environment, ZigBee networks continue to operate successfully.

As an example, Figure 8 shows spectrum analysis over a 14-minute period, captured at Hannover Messe – Europe's largest electronics show. The capture was done using the excellent and inexpensive Wi-Spy tool and displayed using the Chanalyzer package (http://www.metageek.net/).

The channel numbers along the bottom are ZigBee channels.

The figure shows a very active air environment with a number of Wi-Fi networks in operation, notably around ZigBee channels 12 and 21. There is at least one ZigBee network operating as well, visible as a cluster of activity on ZigBee channel 17 and overlapping with the adjacent Wi-Fi activity. A table of the actual (and considerable) Wi-Fi activity measured on the floor, using NetStumbler (http://www.netstumbler.com/), is shown in. Table 2. Note that the channels in the table are Wi-Fi channels and not ZigBee channels. Service set identifiers (SSIDs) are not shown.

ZigBee performance for the network situated on ZigBee channel 17 was measured with the Daintree Sensor Network Analyzer (http://www.daintree.net/). The results are summarized in Table 3.

It is important to note that all of these figures are measured at the ZigBee network layer and that the modest 2% packet loss rate at the NWK layer results in an effective loss rate of 0% if application retries are also employed.

Finally, Daintree Networks recently carried out a round of formal testing. The results appear below. ZigBee platform suppliers Ember Corporation, Texas Instruments, Freescale Semiconductors and Crossbow all publish application notes covering their own testing, which largely agree with the results published below.

Table 2 - Wi-Fi Activity

Type	[SNR Sig Noise]	Beacon Interval	Data Rate	Channel
BSS	[62 111 49]	100	110	9
ad-hoc	[47 96 49]	100	540	11
BSS	[50 99 49]	100	110	11
BSS	[45 94 49]	100	540	11
BSS	[49 98 49]	100	540	7
BSS	[62 111 49]	100	540	6
BSS	[61 110 49]	100	110	9
BSS	[31 80 49]	100	540	11
BSS	[37 86 49]	100	540	7
BSS	[49 98 49]	100	540	11
BSS	[56 105 49]	100	540	11
BSS	[41 90 49]	100	540	6
BSS	[60 109 49]	100	540	6
BSS	[54 103 49]	100	110	1
BSS	[53 102 49]	100	540	7
BSS	[41 90 49]	100	540	6
ad-hoc	[40 89 49]	100	110	1
ad-hoc	[50 99 49]	100	110	11
BSS	[49 98 49]	100	540	11
BSS	[35 84 49]	100	540	11
ad-hoc	[44 93 49]	200	540	11
ad-hoc	[50 99 49]	100	540	11
BSS	[31 80 49]	100	540	2
BSS	[30 79 49]	100	540	3
ad-hoc	[50 99 49]	100	540	11
ad-hoc	[51 100 49]	100	540	11
BSS	[27 76 49]	100	110	7
ad-hoc	[37 86 49]	100	110	1
ad-hoc	[49 98 49]	100	540	2
ad-hoc	[53 102 49]	100	540	2
ad-hoc	[47 96 49]	100	540	11
BSS	[26 75 49]	100	540	9
ad-hoc	[43 92 49]	100	540	11
ad-hoc	[48 97 49]	100	540	11
ad-hoc	[51 100 49]	100	540	11
ad-hoc	[35 84 49]	100	110	1
ad-hoc	[33 82 49]	100	110	1
ad-hoc	[48 97 49]	100	540	11
ad-hoc	[49 98 49]	100	540	11
ad-hoc	[51 100 49]	100	540	11
ad-hoc	[37 86 49]	100	110	10
BSS	[28 77 49]	100	110	7

Table 3 - ZigBee Performance

Total Tx packets	Total lost packets	Average latency (ms)	Maximum latency (ms)
25676	555	4.42	874.83

METHODOLOGY

The test setup is as shown, in schematic form, in Figure 9.

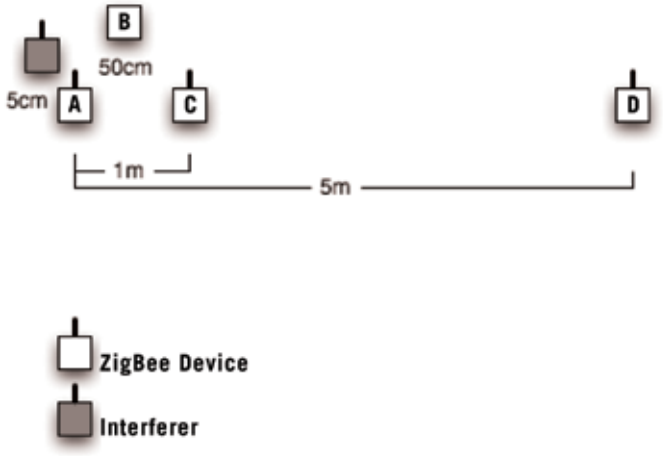


Figure 9 - Test Setup

ZigBee devices were placed at fixed distances from each other and a single interferer was placed within 5 centimeters of one of them – A at the left. The devices were set to use ZigBee channel 18. The ZigBee devices were all standard development boards from a single vendor and were not subject to any kind of amplification, nor was any effort made to select devices based on their performance.

All communications in this test setup were line-of-sight and single-hop.

In each test run, 1,000 application messages were sent over the air separated by intervals of approximately 50 milliseconds. The message used was a 4-byte message that is employed in the ZigBee Home Automation profile to switch lights on and off. Tests were run for all pairs of devices and in both directions for a total of eight tests. Some runs were repeated at the discretion of the testers but no data were discarded.

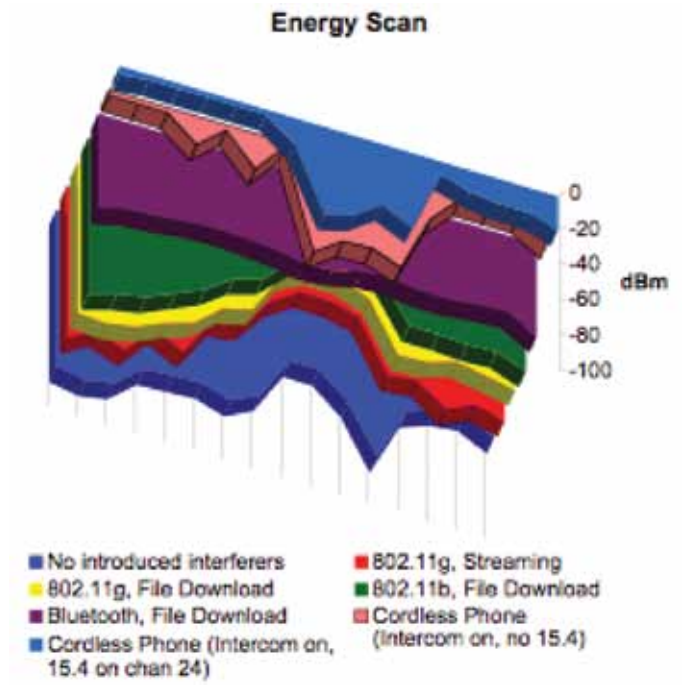


Figure 10 - Interference Sources

RF ACTIVITY

The interference sources used in the test were as shown in Figure 10. All of the devices used for the test were off-the-shelf consumer devices. Measurements were made from the "ZigBee's eye view" using an actual ZigBee device located approximately 1 meter from the device shown as A in Figure 9.

The interferers employed in this test, and shown in Figure 10, are further described in Table 5.

ZIGBEE DELIVERS

The test results can be summarized as follows:

- During the entire test exercise in which tens of thousands of messages were sent, not one was lost.
- Interference was nonetheless seen to have an impact on latency.
- Figure 11 below provides more detail on both the average overall latency (bottom blue measurement) and the average maximum latency over all runs with that interferer. Latencies are in milliseconds.

Table 4 - Interference Sources

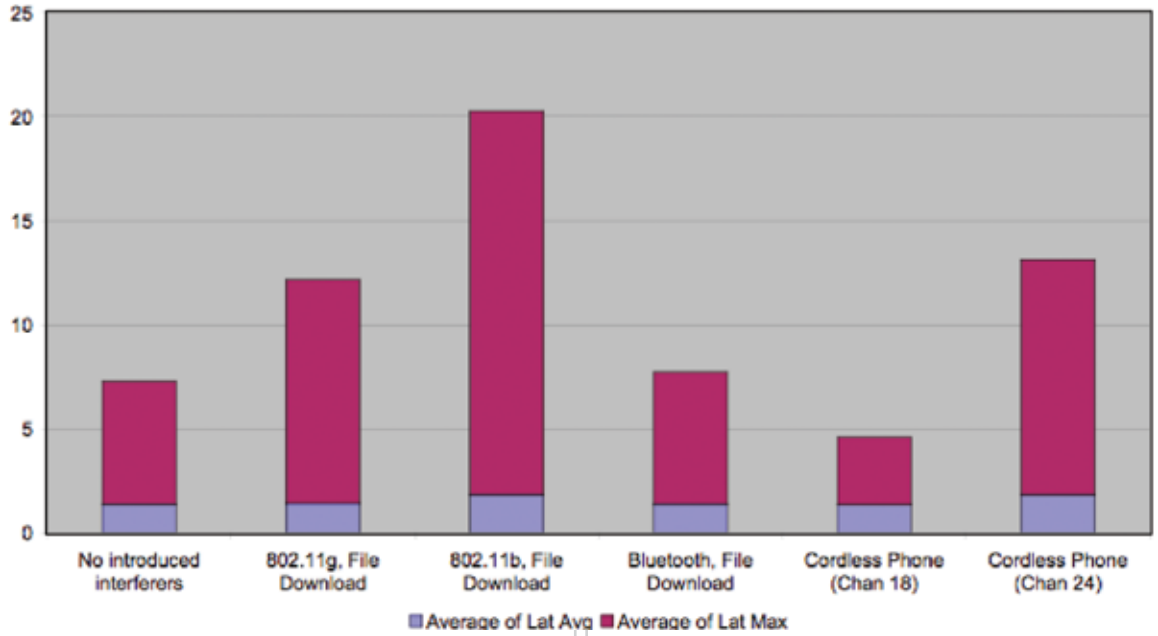
Interferer	Color	Channel	Notes
Ambient	Dark Blue	-	A scan using iStumbler () showed 17 networks of which the strongest were on WiFi channels 1 and 6.
802.11g	Red	6	Streaming audio.
802.11g	Yellow	6	ftp
802.11b	Green	6	ftp
Bluetooth	Purple	-	Computer-to-PDA file transfer.
FHSS Phone	Pink	-	Idle.
FHSS Phone	Light Blue	-	Intercom in use.

FUD: PROPRIETARY TECHNOLOGY ATTACKS ZIGBEE

A small company with proprietary radio and networking technology, recently published a white paper, "WLAN Interference with IEEE 802.15.4", which attempts to paint a much bleaker picture of WLAN and 802.15.4 coexistence than the one shown in the current document. Briefly summarized, the paper claims that, except under the most benign and favorable of conditions, Wireless LAN, where the paper mostly refers to 802.11b/g, will effectively prevent 802.15.4 networks from operating.

The ZigBee Alliance offers the following points:

- This other white paper only reports on the RF performance of 802.15.4 and does not include tests involving ZigBee technology, namely the ZigBee stack. This is done intentionally and makes the performance data look worse. It leaves out the network functionality, such as retries and packet acknowledgement, added by a ZigBee stack which enhances the robustness and performance of an 802.15.4 network.
- The white paper is based on an earlier paper showing results generated by a ZigBee Alliance member company, which is also a promoter of another proprietary 900 MHz technology. One significant difference between the two



result-sets; however, is that the channel-occupancy percentage of the interferer has been restated in the whitepaper at a much lower value without justification. Thus, what was stated, in the earlier paper, as "800 packets per second – approx. full usages of the WLAN channel," is simply restated as "80%," giving a much less favorable picture of 802.15.4's ability to cope.

- The method for selection of chipsets is not discussed in any detail in the whitepaper, although the author does claim to have discarded chipsets from certain vendors. It is not at all clear whether the chipsets in use were the best or the worst available.
- The tests were performed using a programmed traffic generator, which does not behave in the same way as an actual WLAN base station.
- When the test results which form the basis of this other white paper were presented to other ZigBee Alliance members, the results were immediately called into question by chip companies, platform suppliers and other test tool vendors. The test results have never been verified by another company or lab and in fact bear no resemblance to testing performed by dozens of other companies in their development of ZigBee products. In spite of the author's claims, the tests hardly reflect "normal" conditions in the home or small office since WLAN traffic in homes or small offices is variable and intermittent in nature.
- The author draws the conclusion, again without justification, that 802.11g will constitute a greater interference problem for 802.15.4 than 802.11b. Based on results shown here, this seems incorrect.

Given these inadequacies in methodology and the preponderance of evidence to the contrary, the conclusions drawn in a whitepaper supported by a proprietary competitive wireless technology should be considered questionable at best.

There are companies who promote a proprietary, low-data-rate, single-channel, narrowband solution meant to operate in an unlicensed ISM band already crowded with, cordless phones, wireless speaker systems, TETRA systems and other interferers in the home and small office environment. It is interesting to note, the inability of their own radios to change channels in the face of interference and which are based on older radio technology that does not offer the robustness and interference tolerance offered by 802.15.4 solutions. Also, they promote a proprietary networking scheme developed by one small start-up company that does not even begin to offer the benefits of a well developed wireless networking standard such as ZigBee, which is designed, built and supported by hundreds of the world's leading technology companies.

CONCLUSIONS

Based on work to-date, it is safe to draw the following conclusions:

- ZigBee contains a great many features that are designed to promote coexistence and robust operation in the face of interference.
- Even in the presence of a surprising amount of interference, ZigBee devices continue to communicate effectively.
- Both tests and everyday use in realistic environments with real data traffic bear prove ZigBee's robustness.