APPLICATION NOTE

Conquer IoT Test Challenges

for ZigBee® IoT Products

What is ZigBee?

ZigBee is a widely used protocol for low power, low data rate, short range wireless networking. It is a good candidate for Industrial IoT (Internet of Things) devices requiring wireless communications. Industrial applications use ZigBee for energy management, traffic control, utilities metering and lighting control. Home and building automation networks based on ZigBee are ubiquitous. One reason for this popularity is that ZigBee networks can relay messages through nodes beyond single hop radio range, extending the coverage of low power networks. This paper examines the characteristics of ZigBee and how they are used in new test solutions that help manufacturing engineers build affordable test systems.

Keysight Technologies provides a wide range of electronic test and measurement equipment, software and complete test solutions. The low cost ZA0060A family of wireless test solutions provide just enough test for Wireless IoT devices at manageable expense.

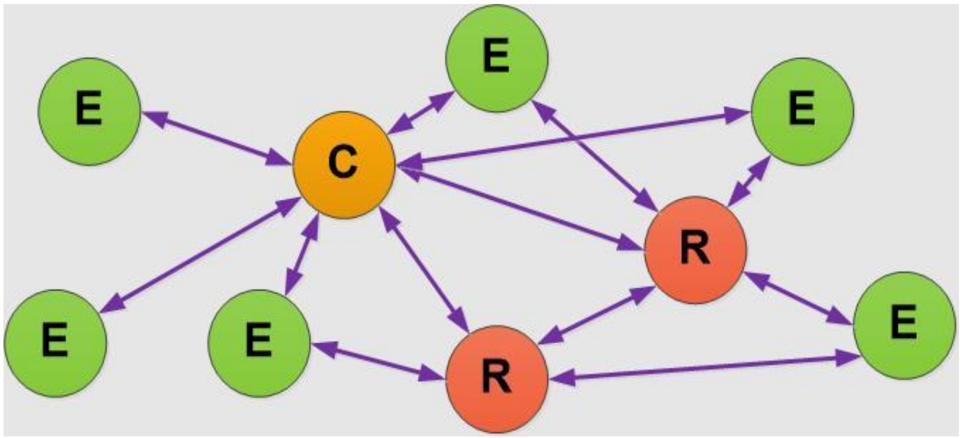

Figure 1: ZigBee can form a mesh network of mixed node types to forward messages

ZigBee Basics

The ZigBee specification builds upon the IEEE 802.15.4 Standard for Low Rate Wireless Networks. IEEE 802.15.4 defines the lower PHY and MAC layers of a network, and the ZigBee specification (sponsored by the ZigBee Alliance) defines the higher Network and Application layers. ZigBee has been enhanced over time, and the recently released Dotdot library adds Internet Protocol IPV6 to address the standard.

The Radio Side of ZigBee

While ZigBee protocols use several frequency bands in various parts of the world, the most common radio frequencies for ZigBee networks are in the 2.4-GHz ISM band. This band is available worldwide, and *Bluetooth*®, WLAN, and other short-range radio systems use this band. A ZigBee network operates on a single channel at a time, but can move the network to a new channel in case of interference. So, it has frequency flexibility, but not true frequency hopping like *Bluetooth*. This has implications for interference in this crowded band.

ZigBee defines several PHY formats used on different bands and in different parts of the world. This paper addresses the most common formats used on the 2.4-GHz band. The low-level ZigBee transmissions are Direct Sequence Spread Spectrum (DSSS), so ZigBee uses low power transmissions with received signal levels below the normal radio noise floor. DSSS is used all over the radio spectrum because the processing gains of DSSS modulation extracts the signal out of the noise. Low power operation extends battery life, which is a primary requirement of most small IoT devices.

The ZigBee transmission is about 3 MHz wide (see Figure 2), which is about 1/10 the bandwidth of the WLAN networks sharing the band. The narrow bandwidth yields lower data rates than WLAN, but these speeds are adequate for many applications. While WLAN can pass 20 to 50 megabits per second, ZigBee networks operate at 250 Kbits per second.

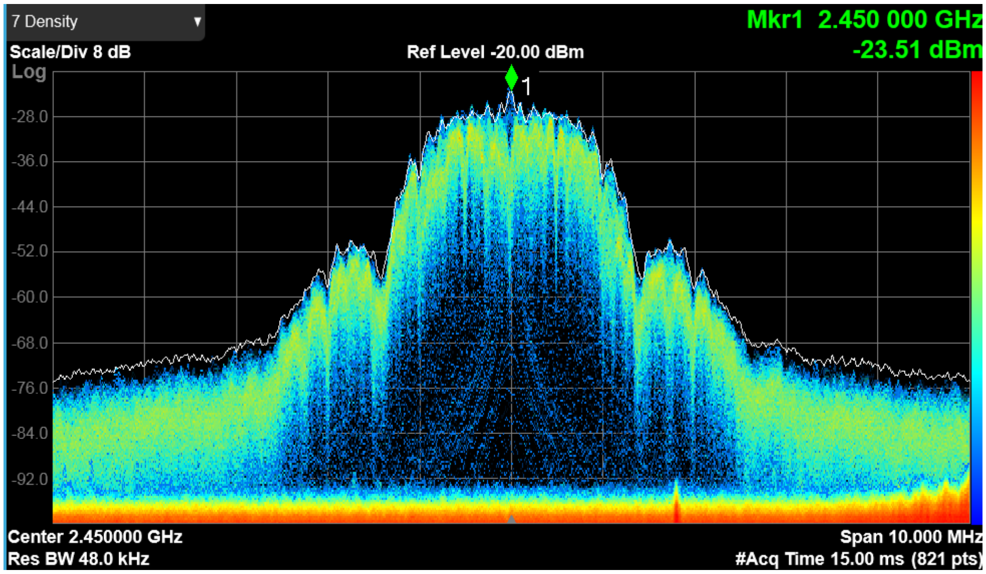

Figure 2: A ZigBee signal is about 3 MHz wide

Because the ZigBee transmission is narrower than WLAN, it can reduce interference by using the spectrum between the three main WLAN channels. These WLAN channels are heavily used in urban and suburban areas, and ZigBee networks have to cope with this radio noise. Using a narrower bandwidth means ZigBee benefits from lower noise in its receiver, so the receiver is more sensitive, and the processing gain from DSSS modulation gives additional improvement in receiver performance. This improvement, on the order of 20 or 25 dB, means a much longer range for a given transmitter power. Other wireless standards like WLAN also use DSSS for this and other reasons. Figure 3 shows this difference in bandwidth.

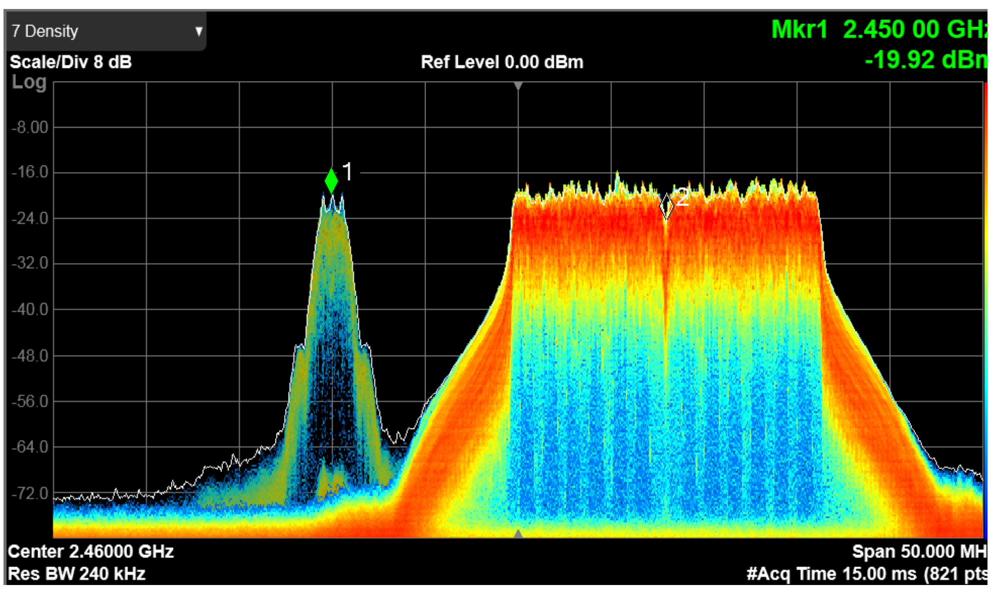

Figure 3: A ZigBee signal (left) is much narrower than a Wi-Fi signal (right)

The Network Side of ZigBee

A typical ZigBee network has three classes of devices: A Coordinator (master of the network), a Router (which can relay messages to other nodes) and an End Device such as a wireless sensor. WLAN and *Bluetooth* are point-to-point systems without routing (recent *Bluetooth* specifications add mesh networks).

- ZigBee allows construction of networks of varying architecture, such as star and mesh networks, which means the nodes can pass messages across several links in the network. ZigBee networks can serve larger areas than point-to-point links of similar RF technologies can manage.
- ZigBee networks can self-heal (change routes for messages) if a router node fails.
- ZigBee shares a goal of long battery life with *Bluetooth*, but because of networking overhead (processing and passing network control messages) ZigBee devices would consume batteries more quickly when operating as routers and coordinators.
- Coordinators and Routers in a ZigBee network must be always available on the air to handle messages, so they cannot sleep. These nodes consume more power than end nodes and usually are not battery-powered.
- Some end nodes can have long operating lives by using small batteries, long sleep modes, and infrequent wakeups. These sleep modes reduce battery consumption by orders of magnitude. In comparison, constant power must be supplied to WLAN nodes because their protocols require it. WLAN devices also consume more power with fast, spectrally wide and complex modulation. Battery powered WLAN networks are rare.
- ZigBee networks require some processing and radio overhead to maintain and operate on the network. Data packets have additional fields due to network addressing requirements.
- Control of network and application layers also means design investment in configuring the ZigBee devices to form and operate these networks. But the benefit is reliable self-healing networks.
- Since adding IPv6 support, ZigBee has enough addressing capability to enable connection to the Internet and to larger networks such as LAN and WLAN. ZigBee networks can connect to the internet using a router.

ZigBee is used for industrial applications like utility metering, where Routers in a neighborhood can relay messages from end devices in utility closets and basements of buildings to the Coordinators beyond radio range of the sensors. Parking management can use ZigBee end nodes that sleep most of the time, and batteries may never need to be changed during the lifetime of the parking sensor. Applications like water leak sensors have very low data rates, perhaps only waking a few times per hour. These industrial uses do not require wires, and small sensors can be placed once and very rarely serviced in their lifetimes.

Running a complex network layer does come at a cost, however, and ZigBee chipsets tend to consume more battery power than *Bluetooth* chips. This is both because the CPU must do more processing at the Network and Application layers, and because more frequent transmission and reception requires the radio to be turned on more often, or even constantly. The essential nodes must handle the overhead messages which check and maintain the network, so battery management may be a greater challenge for ZigBee than for *Bluetooth* devices.

ZigBee fits somewhere between *Bluetooth* and WLAN application spaces and is designed for slightly larger networks than *Bluetooth* and for lower data rates than WLAN. Later *Bluetooth* revisions have more networking capability than older ones, and as more IoT standards appear the distinctions may overlap. When planning a new device or network function, check the released application profiles for ZigBee to see if the desired network function is already defined.

The ZigBee Test Challenges

ZigBee products have some of the same manufacturing challenges as other wireless devices. But the protocol also enables creative and inexpensive solutions. Testing the wireless functionality is a challenge but certain inexpensive test methods can still perform robustly. Low cost, high volume IoT devices need low cost manufacturing tests.

Challenge 1: Testing RF performance is new and unfamiliar.

For many IoT test engineers, radio frequency (RF) communications is a new area of expertise. Older products have been updated with inexpensive wireless capability, and that brings great convenience to the users. However, test engineers now face a new task of testing the RF section of the updated device. The methods and equipment for RF test need to balance cost and complexity, and RF test gear can be expensive.

The simplest test might be wirelessly connecting the device to a known-good companion device, which is sometimes called a “golden radio” test. A simple golden radio test is insufficient if a device is manufactured with misplaced, badly soldered or incorrect parts in the RF/antenna zone, and may not ensure satisfactory operation. This simple “can I connect?” test might allow defective products to pass even if the radio signal is 20 or 30 dB lower than the target specification, because the ZigBee modulation can operate at very low signal strength.

Later, customers will notice a significant range problem on some devices with the defective RF circuit that passed the simple connect test. Warranty expense can easily exceed the cost of these small wireless devices. This problem can be avoided with the “just enough” test method. Because the RF signal path is commonly identical in both transmit and receive operation, a similar test can be used for both, and the same golden radio errors can occur for both receiver test and transmitter test. Instead of using golden radio methods, the best solution to manufacturing test of small Wireless IoT devices is some form of inexpensive RF parametric test.

Figure 4: The Keysight ZA0060A brings economy to RF manufacturing test

The Keysight ZA0060A test solution is both robust and inexpensive for the testing of ZigBee devices. The ZA0060A is a tailored solution based on X8711A IoT Device Functional Test Solution. The ZA0060A solution challenges the DUT with ZigBee network probe signals and looks for the proper response from the DUT. If the DUT answers, it indicates that most of the DUT is operating. However, we have not yet measured RF performance in a quantitative way. Next, the test steps down signal strength, evaluating both receiver sensitivity and transmitter power. When the error rates pass a threshold, we then know the performance of the RF section and can make a pass/fail decision. Test limits are adjustable, not binary. Higher level network functions will work if the RF circuit is operating correctly. The ZigBee devices do not require final test because they are controlled by device firmware that was tested in development phases.

Challenge 2: My DUT has no connectors for test use.

Many small wireless devices have cost, size, and ease of use as their primary design goals. Some manufacturing test solutions use a connector to put a device into special test mode, to read out device operating parameters, or to load special test code into the test device. But space and budget constraints may preclude adding a connector that is used only for manufacturing test. Tiny wearable devices have concerns about connector openings that can collect dirt and debris, shortening device lifetime. A wired connection to a device in manufacturing test also requires time to connect, and time is money in high volume manufacturing. So how do I test this device without a connector?

The solution lies in the device's wireless capability. The Keysight ZA0060A test solution tests devices using over-the-air operations, and testing can proceed without a wired connection via the wireless functions already present in the device. The operator positions the DUT in the ZA0060A's shield chamber and the DUT is challenged with a radio signal containing ZigBee standard operating commands. If the DUT answers satisfactorily over a range of signal amplitudes, measuring receive and transmit operation, the device passes and the next DUT can quickly take its place with no time spent on physically connecting and disconnecting the test equipment. Because these ZigBee functions are present in all ZigBee devices, no special functions or software are required, and the DUT needs no special behavior.

Challenge 3: I want to test my DUT with shipping code, not test code.

This challenge is like the one above, but with even greater implications on time and cost of test. If a test requires special test firmware, writing and testing the special test code consumes time and incurs expenses. Loading the test code into the device and later replacing the test code with production code also increases time and expense. This process itself is also vulnerable to error. Even if this were performed over the air without a wired connection, the time, development cost, risk, and reliability issues remain.

The solution is to test the device with the same firmware used by the consumers, which should already be loaded in the device. This saves time and cost, and reduces the risks of the test code. The Keysight ZA0060A uses standard functions of the ZigBee over-the-air protocol, so no additional investment in DUT firmware is required.

Challenge 4: RF test equipment is expensive.

Many test systems are highly leveraged from the electronic test equipment used in the product development lab, which usually is far more capable (and expensive) than needed by manufacturing test. By the time a ZigBee device reaches the manufacturing stage, the design has been verified in prior stages of development using the high-end RF test instruments of the lab. But many performance parameters are guaranteed by the digital nature of most IoT devices. There is no need to check the higher levels of wireless protocol, for example, or many of the detailed signal characteristics that were tested in the development lab. Manufacturing test can benefit from this fact and focus only on the manufacturing defects, not the entire DUT design.

These manufacturing defects may be due to incorrect part loading in the RF filters and connectors, bad soldering, or missing or misplaced parts. These manufacturing defects will result in low transmit power and reduced receiver sensitivity, and tests which target these possible defects can be performed by low cost test instruments that specialize in finding these types of problems.

Challenge 5: I need a scalable test system

When success in the market means higher product volume, it is a time for celebration, but when the test station reaches capacity it can be expensive to build the second or third line. The Keysight ZA0060A is a low-cost solution and adding additional ZA0060A units increases capacity at a manageable price.

Capitalize on the Standard, Focus on the Probable

The ZigBee protocol requires some low-level operations that stimulate DUT behaviors. All ZigBee devices should already have these functions implemented. Inexpensive test equipment can measure these RF signals, so the test engineer can be confident that the RF performance of the DUT meets specifications. Since the engineer’s focus is on finding the most likely defects happening in manufacturing, as opposed to design errors, tests can zero in on the symptoms of these defects. Using this knowledge, a simpler test system can quickly and inexpensively find defects.

Conclusion

The Keysight ZA0060A wireless test solution is an inexpensive alternative to traditional wireless test methods. It replaces the inexpensive but unreliable “golden radio” test method with a parametric RF test appropriate to low-cost, high-volume products. It delivers the parametric measurements of transmitter and receiver performance without the cost of full featured RF measurement equipment. By testing only those parameters most likely to suffer because of manufacturing defects, this solution implements just enough testing without the cost or risk of other methods.

References

The X8711A IoT Device Functional Test Solution:
https://literature.cdn.keysight.com/litweb/pdf/5992-3642EN.pdf

For more information, please visit https://www.keysight.com/find/X8711A