

Embedded Systems: Sniff ZigBee Packets

Jon Titus, Senior Technical Editor

Embedded Systems

Sniff ZigBee Packets

A variety of software and hardware lets you monitor and analyze IEEE 802.15.4 radio traffic.

by Jon Titus, Senior Technical Editor



When engineers tackle a project that uses ZigBee communications they may get a surprise. Unlike point-to-point communications, ZigBee involves a network that can establish nodes, repeaters and complex mesh topologies. The proper test tools--often called "sniffers"--help engineers diagnose ZigBee-network problems that could otherwise turn into nightmares.

Microchip Technology includes the ZENA Wireless Network Analyzer with its PICDEM Z demonstration kit so engineers can see what goes on among ZigBee devices. The ZENA tool also can sniff and decode Microchip's MiWi protocol that, like ZigBee, uses IEEE 802.15.4 radios. According to Steve Bible, an applications engineering manager at Microchip, ZENA time stamps packets and displays them in a graphical format.

"The screen shows the destination and source addresses, the payload and the data," explained Bible. "We add some color coding and provide data as hexadecimal values. Users also see a received signal strength indication, or RSSI--an uncalibrated relative value."

Not only will ZENA display the packets, but it also shows how a network forms. "When you power a ZigBee node, it first looks for an available ZigBee network," said Bible. "If none exists, it sets itself up as the network coordinator and waits for other stations to query it as they power up. The coordinator lets the newly powered nodes know a network exists, it lets them join and it assigns them an ID number. Some

Embedded Systems: Sniff ZigBee Packets

Published on Electronic Component News (<http://www.ecnmag.com>)

customers find that a difficult concept to grasp."

The ZENA analyzer also logs data into a file so users can later examine in detail the association and disassociation of nodes. "When customers email us a log file, we can help analyze it," said Bible. "ZENA goes beyond analysis and lets you specify radio channels, whether a radio will serve as a coordinator, and so on. Then it creates .h files that go into our MPLAB IDE to produce code for Microchip MCUs."

Engineers who need detailed analyses of ZigBee and 802.15.4 communications can purchase more sophisticated products from companies such as Frontline Test Equipment and Perytons.

"ZigBee and IEEE 802.15.4 technologies require a shift in how we analyze and manage ad-hoc wireless networks," said Matt Perkins, VP of technology development at Awarepoint, a supplier of wireless asset-tracking systems. "An analyzer should take time-sliced snapshots of network traffic, 'mine' the traffic for metrics such as throughput, bottlenecks and end-to-end delays, and presents information in a concise graphical form."

Perkins has used the Frontline MeshDecoder packet sniffer and protocol analyzer and he looks for two features in such a product. "First, you must be able to view an entire network and view details that convey how each node connects to its neighbors. Second, designers want to quickly relate custom packet information to their top-level application." Frontline's DecoderScript language lets designers create such decoders.

Eric Kaplan, Frontline's founder, describes protocol analysis in three areas, debug, interoperability test and verification. Debugging helps engineers figure out why their program or network doesn't work. "You can see messages and responses to determine if they are correct and then give that information to programmers," said Kaplan.

"If devices from two vendors don't interoperate properly, watch the packets as they attempt to communicate and then analyze where the problems lie," said Kaplan. "Often specs are ambiguous, companies misinterpret them or don't stay current with changes."

Kaplan also noted, "You must verify that in addition to interoperating, your devices exchange the proper information. So you watch the communications and verify that messages conform to the spec."

"The 802.15.4 communications use only 16 channels in the 2.4 GHz band, so you can use inexpensive dongles and monitor all channels simultaneously," explained Yaron Soffer, founder and CEO at Perytons. "You also want time-domain information that shows related events such as beacon transmissions, queries, replies, and so on."

A Perytons analyzer monitors multiple channels, so it can overcome problems with multi-path communications. "A typical network uses retransmissions to try to

Embedded Systems: Sniff ZigBee Packets

Published on Electronic Component News (<http://www.ecnmag.com>)

overcome multipath problems," noted Soffer. "But a passive analyzer cannot do that. We put two dongles on the same 802.15.4 channel and use antenna diversity to mitigate multipath and interference effects. In some cases we can reduce the number of lost packets from 10 percent down to 0.1 percent."

Perytons' analyzer provides many analysis tools as well as a pointer tool that displays definitions of packets and signal characteristics in a given signal. Thus, technicians need not master the 802.15.4 or ZigBee specs before they can interpret information.

"We discovered many engineers use 802.15.4 radios in proprietary ways because they couldn't wait for the ZigBee protocol to become a standard," said Soffer. "They can use our APIs and examples to put their own protocol into the analysis software. They don't need one instrument to analyze lower protocol layers and another to analyze their data." "This permits people to use the same tool during development, production, testing, quality assurance and other functions."

A protocol analyzer's software should be flexible enough to adapt to revised standards, too. "The approval of the ZigBee Pro protocol in 2007 required some software changes, but engineers didn't have to buy new hardware because the basic 802.15.4 radios stayed the same," noted Soffer. "You don't want to ask your boss for a new instrument when standards change."

Source URL (retrieved on 04/26/2015 - 3:19am):

<http://www.ecnmag.com/articles/2008/08/embedded-systems-sniff-zigbee-packets>