



ZigBee sniffer for IEEE 802.15.4 protocols

- ◆ Real-time IEEE 802.15.4/ZigBee protocol analyzer
- ◆ Entire ZigBee stack is decoded
- ◆ Built-in support for user-defined decoding of any IEEE 802.15.4- based protocol
- ◆ Finger-sized ZigBee ComProbe air sniffing USB hardware
- ◆ Packets with protocol violations flagged in red
- ◆ Capture files can be exchanged with other FTS4ZB users to quickly pinpoint bugs and interop problems

The well known Frontline Test System for Bluetooth FTS4BT now is available as Frontline Test System for ZigBee, named FTS4ZB. It consists of the FTS software and the ComProbe hardware which sniffs the ZigBee-packets from the air interface. The „FrameDecoder“ can read the protocol IEEE 802.15.4 and decodes down to bit level.

This is very important, because many companies are expected to use 802.15.4 without ZigBee. Also, there will be many applications that use ZigBee and then run a custom protocol on top of ZigBee. The “write-your-own” decode feature enables the user to control his own protocol in the air interface.

ZigBee sniffer FTS4ZB

FTS4ZB system requirements are WIN 2000 or WIN-XP and a free USB port for the sniffer hardware. FTS4ZB consists of the FTS software which needs 50MB disk space and the sniffer hardware to air sniff data at the physical layer and provide visibility into the entire ZigBee stack.

Technical Background

Of key importance is the „high end“ range at 2,4 GHz in the ISM-band (industrial, scientific, medical) due to the high data rate of 250 kbit/s compared to 20 and 40 kbit/s in the „low end“ range of 868,3 MHz.

ZIGBEE applications

Typical applications are :

- Centralised security systems
- Automation of home switching cycles
- Sensoring of critical values in automotive environment
- Super vision in storage areas
- Reporting of medical indicators etc...

The screenshot shows the 'Frame Display' window for a ZigBee frame. The tree view on the left shows the following structure:

- MAC:
 - MHR:
 - Radio Supplied Information:
- NWK:
 - Frame Control:
 - Routing Fields:
 - Destination Address: 0x0000
 - Source Address: 0x030e
- APS:
 - Frame control:
 - Cluster Identifier: 0x02
 - Source Endpoint: Application 0x01
 - Application Framework:
 - Transaction Count: 1
 - Frame Type: Key Value Pair (KVP)
 - Home Controls and Lighting:
 - Transaction Sequence Number: 1
 - Command Type: SET
 - Attribute Data Type: Unsigned Integer 8-bit
 - Attribute ID: Dim Bright
 - Fade Time: 1 Second(s)
 - Brightness State: 88

The table in the middle shows the following data:

...	Frame#	Trans Seq #	Cmd Type	Data Type	Attrib ID
C	268	0	SET	UINT8	On Off
C	273	0	SET	UINT8	On Off
S	281	1	SET	UINT8	Dim Bright

The hex data view shows the following bytes: 61 88 12 ff 29 00 00 0e 03 04 00 00 0e 03 14 02 01 11 01 11 00 01 58 ff 07 58

ZigBee in comparison

ZIGBEE is built with a more simple and consequently more compact protocol compared to Bluetooth and was developed to offer a low cost tool for command and report functionality through the air. Bluetooth however, with its intelligent protocol is more suited for complex tasks and also speech with a data rate up to 3 Mbit/s in the new version 2.1 + EDR (enhanced data rate).

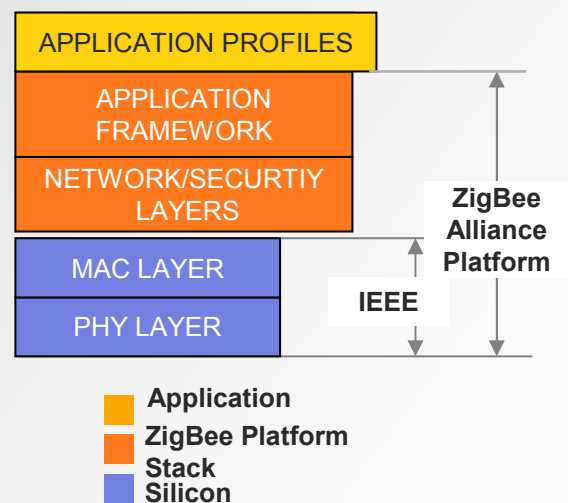
Another aspect for ZigBee was a very low power consumption, resulting in a battery life cycle of at least one year. For the envisioned applications, a maximum number of 65000 nodes per master was realized, with 7 slaves per master compared to Bluetooth.

Protocol	ZigBee	Bluetooth	Wi-Fi
IEEE	802.15.4	802.15.1	802.11a/b/g
Memory	4-32Kb	250 Kb+	1Mb+
Battery Life	years	days	hours
Net members	65.000	7	32
Speed	250 Kb/s	3Mb/s	11-54-108 Mb/s
Range	100m	10 – 100m	300m

Interoperability

Some parameters are not strictly defined by the ZigBee alliance, which explains the interest from chip manufacturers and application engineers for intuitive protocol analysers. Besides the use as development tool, the sniffer is also valid for optimization of the place of installation and the transmission path.

With more and more chip manufacturers and application software coming on the market, the more and more interoperability between different vendors will be an issue. FTS4ZB is sniffing the protocols in the air between two ZigBee products and allows to check in real time the conformity of the interchanged protocols.



Picture 1: The ZigBee protocol stack

Order number :

FTS for ZIGBEE with one year warranty and software care

FTS4ZB

Two years of additional ZB software care

FTS4ZB-PS2



www.rohde-schwarz.com



www.fte.com