2.4 GHz WiFi Spectrum

What's happening in your area?

Jason Hecker

This project takes advantage of certain parts of the circuitry in a 2.4GHz digital radio chip to make a simple spectrum analyser. This can give you a picture of which parts of the 2.4 GHz WiFi spectrum are being used in your immediate vicinity and even be used as an aid in optimising channel use and detection of interfering devices.

The 2.4-GHz Industrial, Science and Medical (ISM) band has been a boon for the short-range personal communications market in recent years. Due to its unlicensed nature and universal allocation, all sorts of communications devices for the home and office have become available. These include the ubiquitous 'WiFi' wireless LAN technology, digital cordless phones, video and audio transmitters, wireless keyboards and mice and Bluetooth among others. 'Unlicensed' does not mean anyone can just build his/her own transmitter and start using it — compliance rules exist in respect of maximum transmitter output power, bandwidth, fixed antenna construction and other aspects, and must be met before commercial 2.4 GHz units are allowed on to the market. Type approval for any 2.4 GHz transmitter equipment has to be obtained from relevant national institutions like FCC.

Heart of the project

The chip we're going to use is the CYWUSB6935 from Cypress Semiconductors, a complete two-way digital radio modem requiring few external components to operate. A similar device, the CYWUSB6934, was discussed in some detail in Ref. [1].

The datasheets of the '6935 device and the module may be found at [2] and [3] respectively. As you can see from the simplified block diagram in **Figure 1**, the '6935 contains a modulator, programmable frequency reference, demodulator, and most importantly for this project a Received Signal Strength Indicator (RSSI). It is through the combination of the programmable frequency generator and RSSI that a basic spectrum analyser can be constructed. By incrementing the frequency of the signal generator and reading the RSSI register shortly after, a useful picture of the 2.4-GHz band can be built up showing the relative levels of activity in this ISM band.

The chip itself is constructed in a QFN package. This is a surface-mount package that doesn't lend itself to soldering with a regular soldering iron. Fortunately Cypress has made available a module which can be utilised by mere soldering iron wielding mortals for useful projects. This module contains the chip, small antennas and the handful of components needed to support it. All the experimenter has to provide is

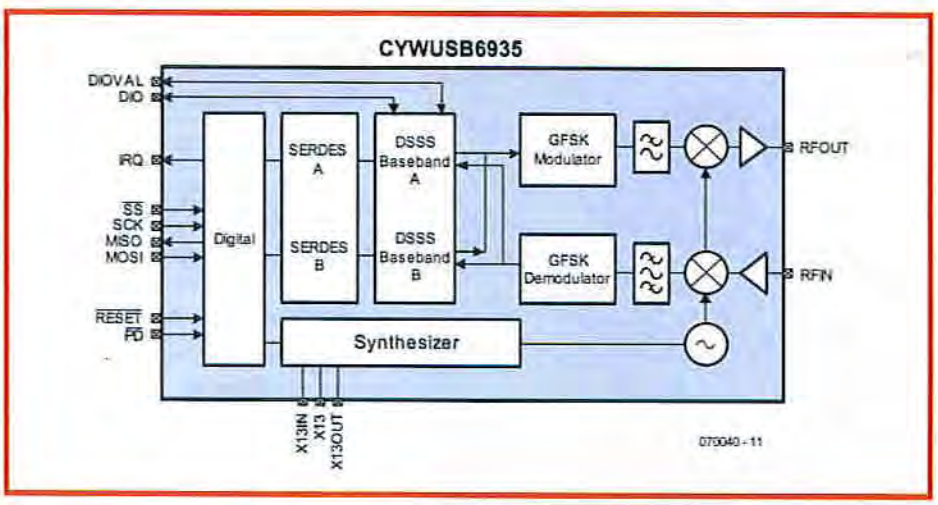


Figure 1. Block diagram of the CYWUSBB6935 WiFi data transceiver from Cypress.

Analyser

some power and a few digital signals to communicate with the chip.
"Lest we forget", samples of the CYWUSB6935 may be obtained from Cypress.

Interfacing

The chip's internal registers can be read from and written to using the simple SPI protocol. Being a 3-volt CMOS part, this means that with suitable level conversion it can be connected to a microcontroller or a TTL parallel port. This project takes advantage of the parallel port (due to its simplicity and ubiquity) found on most PCs and laptops but the ideas demonstrated here can just as easily be applied to a microcontroller connected directly to the part.
Due to the 3 V (or more precisely, 2.7 V to 3.6 V) power, digital interfacing requirements of the chip are straightforward, hence a surprisingly simple circuit diagram can be drawn for the spectrum analyser— see **Figure 2**.
There are a couple of options for powering the chip itself. The parallel port cannot supply enough current to run the chip whereas the USB port has ample current sourcing ability. Two silicon diodes in series can drop the USB power from 5 V to about 3.6 V. Three diodes will drop it down to 2.9 V – both choices are fine for the operation of the chip. Bear in mind that PC power supplies can operate the 5 V power bus as low as 4.7 V (lower for the cheap or overloaded PSUs) so two diodes may be sufficient. The more expensive alternative is to use a 5 V to 3.3 V linear voltage regulator. A bench power supply may also be used if a USB port isn't available.

The TTL interface on a PC's parallel port can be easily used to connect to the 3 V CMOS-based SPI port. The digital output voltage from the parallel port can be reduced to compatible levels by simple voltage division. The signal input to the parallel port is a direct connection, as TTL will acknowledge V_H (logic High level) down to 2.4 V. The output from the TTL port can be as high as 5 V and as low as 2.4 V. In the author's experience, the High level output from the parallel port has been above 4 V so a di-

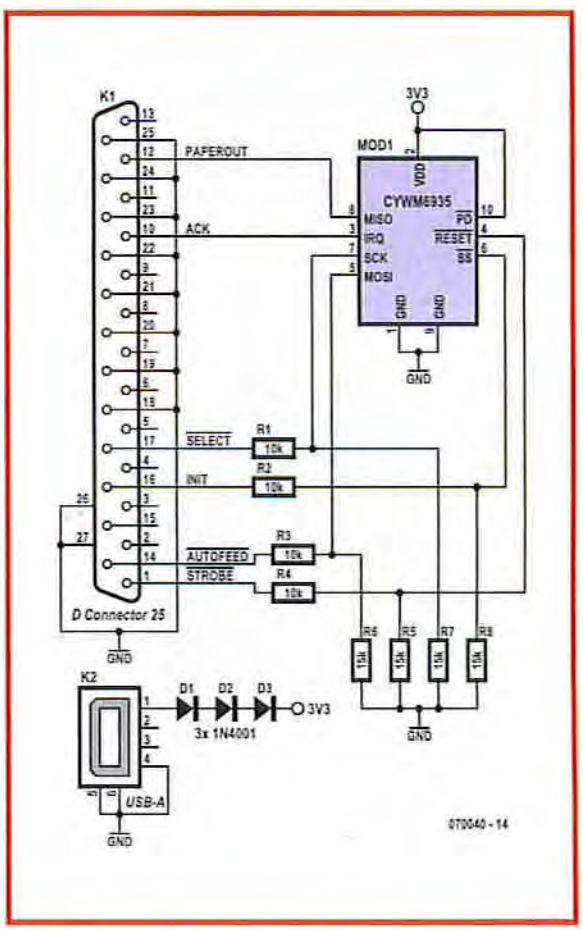


Figure 2. Circuit diagram of the spectrum analyser for the 2.4 GHz WiFi band based on the Cypress CYWUSB6935. USB connectivity is for supply purposes only!

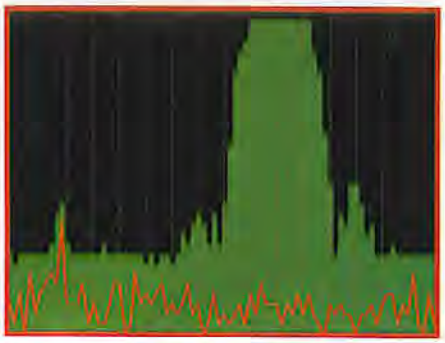


Figure 3a. 802.11b WLAN activity on channel 9.

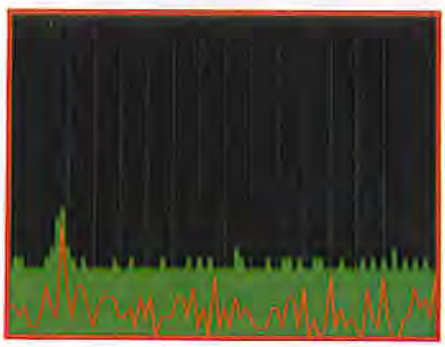


Figure 3b. Local source, probably a CPU clock.

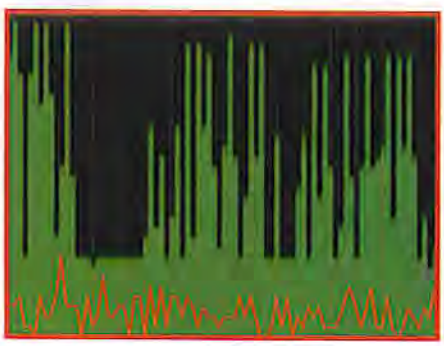


Figure 3c. Bluetooth USB dongle faithfully scanning for other Bluetooth devices.

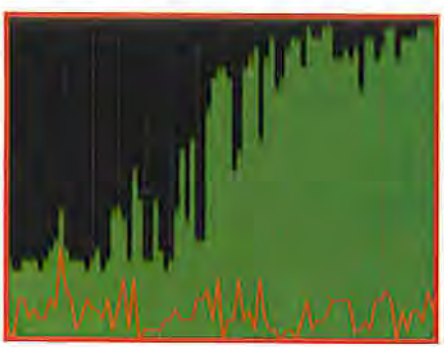


Figure 3d. Microwave oven calling CQ on 2.4 GHz.

vider with a ratio of 0.6 is sufficient to drive 3-V logic.
The SPI signal itself requires RESET, MOSI (data out), MISO (data in), SCK (data clock) and SS (slave select). The latter indicates the start and end of the data transaction. The SPI protocol is a host-driven synchronous signalling interface with the data being sent in MSB (most significant bit) order. The first byte written on the MOSI line contains two control bits and six address bits. A write transaction is followed by another eight bits of data. If a read transaction is being asserted then the slave sends back a byte from the selected address after the initial control byte is written.

Scanning and RSSI

In order to get a picture of the activity in the 2.4 GHz spectrum, the signal generator inside the '6935 must be repetitively swept up in frequency and the signal level at each frequency measured. The frequency generator in the CY-WUSB6935 can be programmed to operate at one of 128 frequencies starting at 2.4 GHz, using intervals of 1 MHz. The ISM band only extends to 2.483 GHz so there is no point scanning beyond this frequency (indeed the device may not actually operate above the 83rd step).
The RSSI circuit in the chip is designed to take a 50 µs snapshot of the incoming signal and make an estimate of the power received at that time. The process of scanning is simple – set the frequency, trigger the RSSI circuit, read the RSSI value after 50 µs.
The RSSI register puts out a value between 0 and 31. According to the datasheet, the range between 0-10 means the received signal level is below –95dBm. The range from 28-31 means the received signal level is above –40dBm. This means each count is approximately –3dBm (i.e.,)

$$(-40) - (-95) / (28-10) = -3.056 \text{ dBm}$$

per count.

The purpose of the register is to give an indication of whether or not something else is transmitting in the band rather than an accurate estimate of the absolute signal power. If there is no signal above a certain threshold, then it should be safe to transmit without fear of being drowned out by other signals at the receiver.
Without some sort of calibration it's not possible to determine the precise power level each register count corresponds to, and may vary from device to device. The datasheet mentions that when scanning for an empty channel, up to 10 reads should be made in order to determine whether or not the channel is indeed clear.

Software

The QTScan software for this program was written to run in Linux and uses QT4 for the GUI. Inside are the parallel port and SPI driver routines. Users of Linux can compile and run the code so long as they have the QT4 runtime and development libraries and headers (for the GUI) and the kernel development libraries and headers (for the parallel port) installed. The binary supplied runs on Ubuntu 6.10 'Edgy Eft' but may work on other recent Linux systems as well. To build QTScan, simply run the executable `make`.

The parallel port should be configured in the BIOS as 'SPP' but depending on your computer hardware it may also work in EPP and ECP mode.
Because SPI is a serial protocol, every byte is serialised and deserialised in software. This serialisation combined with the parallel port running at very slow ISA bus speeds (for historical and backwards compatibility purposes) the scanning software actually runs at a fraction of the speed the chip is capable of scanning at. The scanning speed could be much improved by using a microcontroller with a dedicated SPI port or a general-purpose digital I/O port that is capable of running at much higher speeds. Now there's a challenge — anyone with a successful application running on his/her ARM, PIC24F, R8C or AVR platform should report to Elektor.

Due to the slow nature of the ISA bus parallel port, we measured about 600,000 `ioctl()` functional calls per second that could be executed when reading and writing the parallel port registers. The `inb` and `outb` instructions called by `ioctl()` are stalled by the parallel port hardware for what is an eternity for a modern CPU. This puts a very high system load on the computer, effectively slowing it down while it twiddles its thumbs waiting for the parallel port to complete the `inb` and `outb` transactions.

The software simply sweeps all 83 channels in a repetitive fashion. As you can see from the examples in Figures 3a-2d, QTScan shows the results of the current scan as a red line. In the background, a green histogram captures the peak level detected in each frequency bin. With this device the peak histogram can take tens of seconds to develop a useful picture of ac-

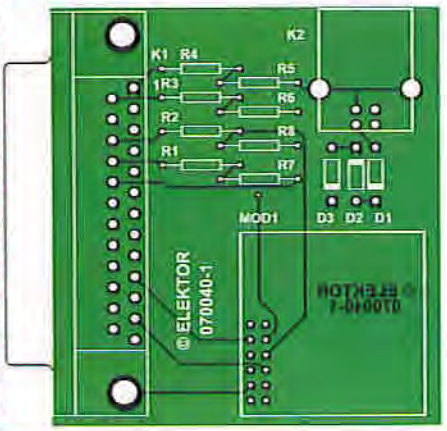
tivity in the 2.4 GHz band, so be patient. Most sweeps however will only produce about one peak per scan.
The vertical yellow lines mark the centre frequency of the 802.11 WiFi channels. The x-axis starts at 2.4 GHz and ends at 2.483 GHz. Each x-axis tick is 1 MHz. The y-axis spans the 32 count levels available in the RSSI register. Assuming the dBm per count levels discussed above, the y-axis starts at –125.6 dBm and ends at –30.8 dBm.
MS Windows software is being developed at the time of writing this article.

All software for this project is available free of charge from the project page on the Elektor website. Simply follow Magazine → June 2007 → 2.4 GHz WiFi Spectrum Analyser, or search for archive file **070040-11.zip**.

Results

The author's household contains various sources of 2.4 GHz radiation, including the computer, microwave oven, Bluetooth devices and an IEEE 802.11b (WiFi) access point. If this sounds familiar to you, read on.

IEEE 802.11b



COMPONENTS LIST

Resistors
R1-R4 = 10kΩ
R5-R8 = 15kΩ

Semiconductors
D1,D2,D3 = 1N4001

Miscellaneous
MOD1 = Cypress module type CYWM6935
K1 = 25-way sub-D plug (male), angled pins, PCB mount
K2 = USB-B connector
PCB, ref. 070040-1 from www.thePCBshop.com

Figure 4. Component mounting plan of the PCB designed for the spectrum analyser.

proc/cpuinfo information said the CPU is running at 2.310 GHz but the peak is shown to be at 2.410GHz in QTScan. It could also be a harmonic from one of the many clocks operating in a modern PC. The signal is present in all the scans.

Bluetooth
Bluetooth devices utilise the entire 2.4 GHz ISM spectrum. **Figure 3c** is a scan of a USB Bluetooth dongle scanning for other Bluetooth devices. It is apparent that it is hopping among many of its own channels in the search for a Bluetooth client device it's eager to talk to. This scan lasted for 10 seconds.

Microwave Oven
It's no accident that the unlicensed 2.4 GHz spectrum falls within the same band allocated to microwave ovens. Such ovens can put out over a kilowatt of (pulsed) broad spectrum microwave power and it's inevitable that some of it will leak out. **Figure 3d** shows the signal levels leaked by the author's microwave oven operating in the kitchen about 5 metres away through two walls. You can see how it swamps the spectrum. WiFi can overcome such interference to a point due to the spread-spectrum process it uses along with packet retransmission techniques. This scan lasted about 50 seconds.

Antenna modifications

The antennas on the PCB are only designed for short-range operation – according to Cypress, up to 50 m or so for the original purposes of data transmission and reception. The on-board antenna could be disconnected (with a knife or scalpel) and an SMA or MCX connector attached to allow for the connection of a larger antenna, either directly or via a length of low-loss coax cable. This would extend the detection range of the device as well as accommodate directionality with the use of an antenna such as a Conifer [4], Pringles cantenna or the Elektor 'precision' Cantenna [5].

Construction

Thanks to the use of a ready-made module there are no gigahertz construction nightmares like tuning PCB striplines, buying PTFE Duroid® board, adjusting oscillators, knowing if the receiver works at all or indeed what GHz stands for.

Design challenge — anyone with a successful application of the CYWUSB6935 running on his/her ARM, PIC24F, R8C or AVR platform should report to Elektor.

Figure 3a shows a WLAN access point operating on channel 9. This scan took two minutes to accumulate all the peaks. The signal displayed comes from the regular beacon signal any access point will continuously transmit. It shows the main lobe centred nicely on the channel 9 indicator line. The lumps either side of the main lobe are the sidelobes typical of a QPSK (quadrature phase shift keying) spectrum. You can also see how the adjacent channels overlap. The best way to ensure that multiple local 802.11b networks aren't interfering is to make sure none of the main lobes overlap.

PC CPU Clock
In the scan in **Figure 3b**, the peak at the left is what's strongly suspected to be emitted from a computer. The /

Figure 5. Prototype of the spectrum analyser Jason kindly sent us by mail (from Australia).

The Cypress module and a ridiculously low number of other components are simply mounted on an Elektor-designed PCB of which the artwork is shown in **Figure 4**. The board is available from our business partner The PCBShop (www.thepcbshop.com). Mounting the parts should not present problems.

Finally, Elektor is sometimes criticised for not showing the 'less organized side of things'. Here we apologise and make amends by printing a photograph of the author's prototype of the WiFi spectrum analyser, see **Figure 5**. As you can see it's perfectly possible to construct the circuit on a piece of perfboard. We're now anxiously waiting for emails from SticklersforPerfection & Co. in response to printing an example of 'not so slick' (but fully functional) electronics hardware!

(070043-I)

References and web links

[1] Radio Control using WLAN ICs, Elektor Electronics December 2006.

[2] www.cypress.com/portal/server.pt?space=CommunityPage&control=SetCommunity&CommunityID=209&PageID=259&fid=65&rpn=CYWUSB6935

[3] http://download.cypress.com/published-content/publish/design_resources/datasheets/contents/cywm6935_8.pdf

[4] www.mrx.com.au/wireless/ConfierModifications.htm

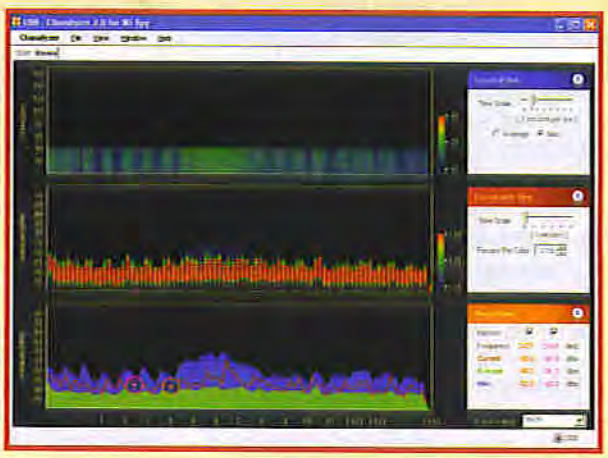
[5] WLAN Antenna Design, Elektor Electronics December 2006.

A commercial unit

The Wi•Spy Spectrum Analyser is proudly announced as "the smallest spectrum analyser in the world, an invaluable tool for making WLAN price quotes, troubleshooting WiFi problems and optimising WiFi implementations".

The hardware actually consists of no more than a carefully sealed USB stick with a length of 4.5 cm. The software supplied on CD is called Chanalyser 2.0 (beta) and hints at metageek.net for its source. Compatibility with Win2000, XP, Linux and MacOS is claimed on the box.

Wi•Spy has some interesting features like data trace, average trace, peak trace, frequency/channel view and record/playback. Remarkably, Wi•Spy is claimed as being able to track down interference from DECT phones, which (we would hope) work between 1.880 and 1.900 GHz i.e., well outside the 2.4 – 2.483 GHz ISM frequency range. But then the receiver inside may be a very wideband type.



The unit costs €119 (approx. £82); we got ours from www.wlan-shop.nl.