DOI 10.5162/sensor2013/C4.1

Low-Cost Spectrum Analyzer for Cognitive Radio Applications and Coexistence Management in the 2.4 GHz ISM-Band

Rainer Hornung, Ralf Heynicke, Gerd Scholl
Electrical Measurement Engineering
Helmut Schmidt University / University of the Federal Armed Forces, Hamburg, Germany
rainer.hornung@hsu-hh.de

Abstract

Interferences between wireless systems have to be avoided, if multiple wireless systems shall operate simultaneously and in a reliable way in the 2.4 GHz ISM-band. This can be achieved, e.g. by intelligent cognitive radio systems or frequency planning strategies. A cognitive radio or an efficient coexistence management scheme requires a spectrum analyzer. In this article, a fast and low-cost spectrum analyzer will be introduced, which is based on a wireless gateway for sensor/actor communication with standard narrowband RF-transceivers. The spectrum analyzer scans the complete ISM-band in 1 MHz steps within only 1.2 ms. An FPGA is employed for parallel preprocessing of the RF-transceivers. A microcontroller is used for a detailed RSSI-signal analysis and classification. Different radio standards such as IEEE 802.11b/g/n (Wi-Fi) and narrowband systems like IEEE 802.15.4, ZigBee or IEEE 802.15.1 (Bluetooth) can be recognized. Additionally Bluetooth in paging procedure with a packet duration of only 68 µs can be detected. The spectrum analyzer can be used as standalone system, e.g. for spectrum monitoring in industrial environments, or can be easily integrated into cognitive radio systems.

Key words: Low-cost spectrum analyzer, cognitive radio, coexistence management, industrial wireless systems, wireless interferences.

Introduction

The number of wireless systems installed in industrial environments is increasing steadily [1]. If these systems are installed correctly, e.g. their antennas well distributed and aligned, their performance measures, like latency and reliability, generally fulfill consumer's requirements. With an increased number of radio systems operating in the same frequency band the probability of mutual interference rises [2] and thus appropriate coexistence strategies have to be employed, especially while unexpected occurrence of interfering wireless systems. In such situations intelligent diagnostic tools identifying such a potentially dangerous situation are vital. We developed a wireless gateway with standard narrowband RF-transceivers for sensor/actuator communication in factory automation environments. RSSI measurements of the RF-transceivers are used to realize a fast and low-cost spectrum analyzer. As both, communication and spectrum sensing can be done with the same hardware, our gateway is a simple form of a cognitive radio.

Low-cost Spectrum analyzers available on the market today typically scan the 2.4 GHz ISM-band within a few hundred milliseconds [3][4][5], with a typical accuracy of ±2 dbm. But for secure detection of unexpected interfering wireless systems, especially Bluetooth or Wi-Fi systems, transmitting short beacon frames, shorter sweep durations are of higher priority than amplitude accuracy.

In the following, we present a spectrum analyzer operating in the 2.4 GHz ISM-band. In Section 2 the hardware architecture is described briefly. The performance of the spectrum analyzer is discussed comprehensively with a typical application example in Section 3. Concluding remarks are given in the final Section.

Spectrum Analyzer Hardware Architecture

We focused on a modular hard- and software design to be able to react quickly and flexibly to future developments of components. E.g. the RF-transceivers can be chosen, if other RF-standards has to be required, one or several RF-transceivers can be replaced without influencing spectrum analyzer functionality

because all RF-transceivers offer the possibility for narrowband RSSI-measurements.

The block diagram of the spectrum analyzer is shown in figure 1.

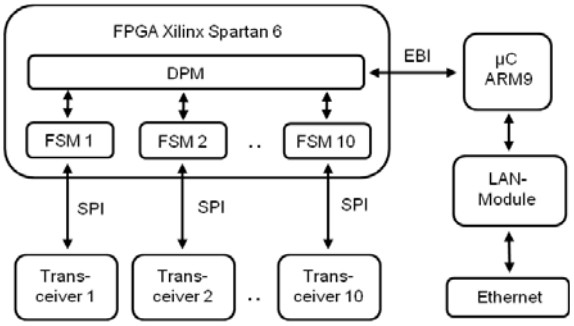

Fig. 1: Block diagram of the spectrum analyzer.

To manage control tasks and to perform signal analysis, a Spartan 6 FPGA and an ARM9-microcontroller (µC) were applied. The low-power Spartan 6-family delivers clock rates up to 1 GHz. The ARM9-µC is based on a 32 bit RISC-architecture guaranteeing high computational power.

A synchronized parallel structure of finite state machines (FSM 1 - FSM 10) was programmed into the FPGA, allowing a time-efficient processing of the RSSI-measurements delivered by the RF-transceivers. The FPGA communicates with the RF-transceivers over serial peripheral interfaces (SPI). The ARM9-µC reads the measured data from the FPGA's dual-port-memory (DPM) via an external bus interface (EBI), allowing a maximum transmission rate of 200 MByte/s. The LAN-module is used for data exchange over Ethernet to a diagnostic software application.

In Fig. 2 the hardware of the spectrum analyzer is depicted. In the center of Fig. 2 the FPGA can be seen, in the lower part the ARM9-µC and the LAN-module are located. The RF-transceivers are located on the left side and in the upper part of the PCB, respectively.

Fig. 2: Prototype of the spectrum analyzer.

Spectrum Analyzer Operation

For spectrum sensing ten standard narrowband RF-transceivers are used allowing sensor/actuator communication and RSSI measurements. According to the data sheet of the CC2400 RF-transceivers [6] lock time for RSSI-measurement is equal to 20 µs with an accuracy of ±4 dB.

Wireless systems are using different message lengths, typically and partially they are using frequency hopping, for data transfer. Therfore two different sweep-modes were implemented to detect wireless systems securely.

The first sweep-mode is used for detection of frequency hopping wireless devices with short messages like Bluetooth in paging procedure. The paging procedure represents a key challenge, because this operation mode very often occurs when a Bluetooth device is activated. In this mode Bluetooth uses the whole ISM-band with 68 µs message length [7]. To identify a Bluetooth device within this time interval, the sweep bandwidth can be reduced and the spectral resolution can be increased. E.g., the spectrum analyzer enables a 30 MHz frequency sweep with a spectral resolution of 3 MHz within 32 µs.

The second sweep-mode is for detection of non-hopping wireless systems like IEEE 802.11b/g/n (Wi-Fi) and narrowband systems like IEEE 802.15.4, ZigBee and for detection of hopping systems with large packet lengths like IEEE 802.15.1 (Bluetooth) in 'data transfer mode'. The whole 80 MHz ISM-band can be scanned by ten RF-transceivers. The operating frequency of each transceiver is positioned at the lowest frequency with one of ten 8 MHz non-overlapping frequency sub-bands. After a specified measurement time the frequencies of each transceiver are shifted within the sub-bands in steps of 1 MHz and the process mentioned above is repeated eight times. This procedure guarantees a 1.2 ms sweep duration for the complete 2.4 GHz ISM-band with a spectral resolution of 1 MHz, in which each frequency point is scanned with a 2.66 % duty cycle. The challenge is to capture a Wi-Fi beacon (IEEE 802.11b) with a spectral bandwidth of 22 MHz which corresponds to 22 frequency points in the spectrogram. Thus, if the Wi-Fi beacon frame with a 432 µs duration is captured by our spectrum analyzer with a 1.2 ms sweep duration, at least 8 of 22 frequency points are matched. With this information the implemented algorithms is able to identify a Wi-Fi. If less than ten RF-transceivers used, a secure detection of a Wi-Fi beacon cannot be guaranteed

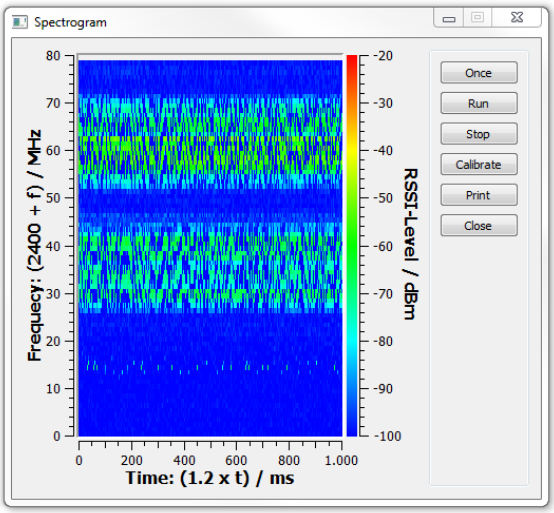

Fig. 3: Spectrogram of 2.4 GHz ISM-band with 1.2 ms sweep duration.

In Fig. 3 the spectrogram of the 2.4 GHz ISM-band is shown. Two systems are active, one at channel 6 (2.426 GHz - 2.448 GHz) and another at channel 11 (2.451 GHz - 2.473 GHz), each with receive levels of approximately -60 dBm, respectively. Furthermore, a narrowband RF-system is detected at 2.416 GHz.

The classification-algorithms implemented in an ARM9-µC are specially designed for low computational effort to use them in high performance cognitive radios for real-time sensor/actuator communication in factory automation applications. By means of statistical analysis like arithmetic averaging or higher order statistics the center frequencies and the mean duty cycle of radio communication systems can be identified.

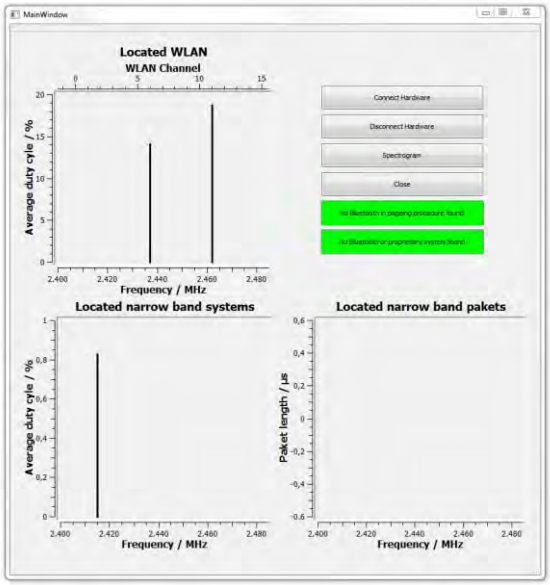

Fig. 4: Duty cycles and packet lengths of Wi-Fi as well as narrowband RF-systems

Duty cycle as well as packet length of classified wireless systems are given in Fig. 4. As shown in the left part of the spectrum analyzer's user interface the Wi-Fi system, operating at channel 6, exhibits a mean duty cycle of 14 %, whereas the Wi-Fi system of channel 11 has a duty cycle of 19 %. The narrowband RF-system with a center frequency of 2.416 GHz achieves a mean duty cycle of nearly 1 %. The lower two buttons indicate that no Bluetooth device is operating in the paging procedure, as well as a 'data transfer mode' was found.

Conclusion

In this article a fast spectrum analyzer with 1.2 ms sweep duration and 1 MHz spectral resolution operating in the 2.4 GHz ISM-band is presented. It was shown that a 30 MHz sweep bandwidths combined with a spectral resolution of 3 MHz, the sweep duration can be reduced to 32 µs. To ensure rapid and efficient data processing the spectrum analyzer uses ten RF-transceiver, controlled by a Spartan 6 FPGA combined with a ARM9-µC, enabling a fast identification of wireless systems. Analyzed data is visualized as spectrogram and histogram of duty cycle and packet length.

The hardware of the spectrum analyzer can be used as gateway for real-time wireless sensor/actuator communication. With minor modifications a cognitive radio system can be realized.

References

[1] Heynicke, R.; Krüger, D.; Scholl, G.: Wireless Automation. *Sensor + Test Conference*, Nürnberg, June 2011

[2] Wattar, H.; Heynicke, R.; Krüger, D.; Scholl, G.: Messtechnische Bestimmung der Bit- und Paketfehlerrate bei Wi-Fi-WPAN Koexistenz. VDI-Berichte 2067, Düsseldorf: VDI-Verlag, 2009, S. 191 - 194

[3] Aaronia AG: SPECTRAN HF-2025E V3, Strickscheid, January 2013

[4] FLUKE networks Corp.: AirMagnet Spectrum XT, Everett, 2012

[5] MetaGeek LLC: Wi-Spy 2.4x, Boise, 2012.

[6] TEXAS INSTRUMENTS INC.: 2.4 GHz Low-Power RF Transceiver CC2400. Oslo, Datasheet, March 2007

[7] Institute of Electrical and Electronics Engineers, Inc.: IEEE Std 802.15.1™ - IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs). NY, USA, 2005