868 MHz Traffic Detective: A Software-Based Tool for Radio Traffic Monitoring

Jens Saalmüller, Matthias Kuba, Andreas Oeder
Networked Systems and Applications Department, Fraunhofer Institute for Integrated Circuits IIS, Nuremberg
{jens.saalmueller, matthias.kuba, andreas.oeder}@iis.fraunhofer.de

Abstract

Radio traffic monitoring is a crucial task whenever different and incompatible radio frequency (RF) communication standards simultaneously exist within a given environment. In this paper, we present a software-based tool for RF traffic monitoring and diagnosis within the European 868 MHz Short Range Device (SRD) band that is composed of commercially available low-cost receiver hardware and an app-based algorithm for Android OS systems.

I. Introduction

Numerous applications like smart metering, home automation, demand side management, and many more require reliable and cost effective technologies for wireless data transmission. For this purpose, the license-free European 868 MHz SRD frequency band is prevalently used. However, with the increasing presence of wireless applications more and more different and mutually incompatible communication standards and RF-protocols may simultaneously occupy this part of the frequency spectrum. Therefore, special attention has to be paid whenever wireless networks are planned or operated within the 868 MHz SRD band. It is necessary for network specialists to be equipped with powerful and dynamic tools that provide insights into the wireless data traffic present within a certain communication environment.

In this paper, we present a software-based tool in form of an app for Android OS based platforms for RF traffic monitoring and diagnosis within the 868 MHz SRD band, where low-cost DVB-T hardware is used as an analog front-end. The software algorithm comprises state of the art pattern matching techniques for received signal classification. Several statistical key features are extracted from the received signal. The classification of the received communication standard is based on a decision tree that is able to distinguish between different signal footprints in the time and frequency domain, even in noisy and multipath scenarios. Furthermore, occupancy statistics of the different communication standards and frequency channels within the 868 MHz band can be generated and visualized. The complexity of the algorithm allows implementation on mobile handheld devices, as demonstrated on a Samsung Galaxy Tab. The analog front-end used for radio signal reception is a commercially available DVB-T USB stick, based on the Realtek RTL2832U receiver-chip and an Elonics E4000 tuner. The broad availability of these USB sticks and the ample variety of handheld devices renders the tool to be an economic and highly versatile solution for radio traffic monitoring.

The rest of this paper is organized as follows: In the next section, the most relevant communication standards within the 868 MHz SRD band are introduces and the theory behind the communication standard classification algorithm is described briefly. Subsequently, the hardware components used are described and several implementation aspects are discussed. Finally, different potential fields of applications are summarized and the paper is concluded.

II. The Theory Behind

This section first introduces the communications standards considered within this work. Afterwards, an algorithm for the automatic classification of those signals is presented.

A. Communication Standards in the 868 MHz SRD Band

Some of the most relevant and widespread PHY-layer standards within the 868 MHz SRD band are the IEEE 802.15.4 [1], the DIN EN 13757-4 [2] and the ISO/IEC 14543-3-10 [3].
It is noteworthy, that higher-layer protocols like ZigBee, 6LoWPAN, WirelessHART or MiWi are based on the IEEE 802.15.4. Furthermore, higher-layer standards like Wireless M-Bus or KNX RF make use of the DIN EN 13757-4 standard. In addition to that, it is worth noting that the standard ISO/IEC 14543-3-10 is also known as the EnOcean Radio Protocol, which is often used for energy harvesting based RF communication systems.
The IEEE 802.15.4 standard defines three different PHY-layer protocols for the 868 MHz band. Two of them are used in practical applications. One uses binary phase shift keying modulation (BPSK) on a 868.3 MHz carrier wave with a data rate of 20 kbit/s and a direct sequence spread spectrum (DSSS) technique with a spreading gain of 15 (from now on abbreviated as IEEE BPSK). The other wide-spread PHY-layer protocol of IEEE 802.15.4 modulates a data rate of 100 kbit/s with a DSSS gain of 4 onto a carrier wave of 868.3 MHz, using orthogonal quadrature phase shift keying modulation (OQPSK), which is also known as minimum shift keying (MSK). This PHY-layer standard will from now on be referred to as IEEE OQPSK. The DIN EN 13757-4 standard specifies three different PHY-layer substandards, from now on being referred to as wM-Bus A, wM-Bus B and wM-Bus R2, respectively. All of those substandards use a binary frequency shift keying modulation (BFSK). wM-Bus A transmits at a data rate of 16.384 kbit/s on an 868.3 MHz carrier, using Manchester coding. wM-Bus B defines a data rate of 66 kbit/s and a ‘3 out of 6’ coding scheme, as well as a carrier at 868.95 MHz. wM-Bus R2 modulates a Manchester coded bit-stream of 2.4 kbit/s onto a carrier with frequency (868.03+k*0.06) MHz, where k is an integer between 0 and 9. Finally, the ISO/IEC 14543-3-10 standard, which will from now on be referred to as OOK STD, defines a bit rate of 125 kbit/s that is modulated onto an 868.3 MHz carrier using on off keying modulation (OOK).

B. Classification Algorithm

In order to automatically distinguish between different communication standards, a pattern-recognition based approach is chosen, where several statistical key features are calculated from the received signal. Then, conclusions can be drawn from the feature values concerning the communication standard of the received signal. However, since the signals may be significantly noisy, the features have to be chosen with care in order to achieve a reliable classification algorithm.
For the classification of the six PHY-layer substandards discussed in the previous section, five of the features that have already been presented in [5] have been implemented in software, however with several hardware-specific adjustments. Then, whenever an RF signal is received, those five key feature values are calculated and compared to predefined threshold values, leading to a certain point in the feature space that is exclusively assigned to one of the six communication substandards.
It was proven in previous publications, that the features chosen facilitate a high probability of correct classification, even in noisy communication scenarios [4], [5].

III. The System

The base of this project is inspired by the RTL software defined radio (RTL-SDR) system [6]. It is a multi-purpose wide band radio scanner consisting of a low-cost hardware part for signal

reception and a software part for signal processing. The hardware part, readily available in the form of DVB-T USB sticks, consists of an antenna connected to a tuner chip (e.g. the Elonics E4000), which in turn is connected to the Realtek RTL2832U chip via I2C. The tuner is used to receive the signal and filter out the required frequency. It then converts this frequency down to baseband (Zero-IF), generates in-phase and quadrature components (I/Q signals) and feeds them into the RTL2832U. This chip then samples the signal with a maximum sampling rate of 3.2 MS/s and outputs 8 bit I/Q samples. These samples are then sent out via USB to the connected host. Although the hardware is intended for reception of DVB-T and radio broadcasting signals, it can be configured to output raw I/Q samples. The software, in form of an Android app, finally processes the raw samples and executes the classification algorithm.

A. The Tuner Elonics E4000

The Elonics E4000 [7] is a multi-standard CMOS terrestrial RF tuner which is ideal for TV and radio broadcast receiver solutions but is not limited to them. Its RF front-end is capable to receive any frequency in the range from 64 MHz to 1700 MHz. The chip is highly configurable and can be controlled via an I2C interface.

The received RF signal is first passed into a low-noise amplifier (LNA) and amplified either automatically or by a manually configurable gain. Then, a certain frequency range is filtered out depending on the selected frequency band (VHF II, VHF III, UHF or L-band). The mixer transforms the signal afterwards into the baseband and passes it along to the intermediate frequency filter and gain section. Here the frequency range is narrowed down even further to extract the desired frequency and bandwidth. Figure 1 gives an overview of the signal processing inside the tuner.

An additional feature is the calculation of the received signal strength indicator (RSSI) which can be used for automatic gain control.

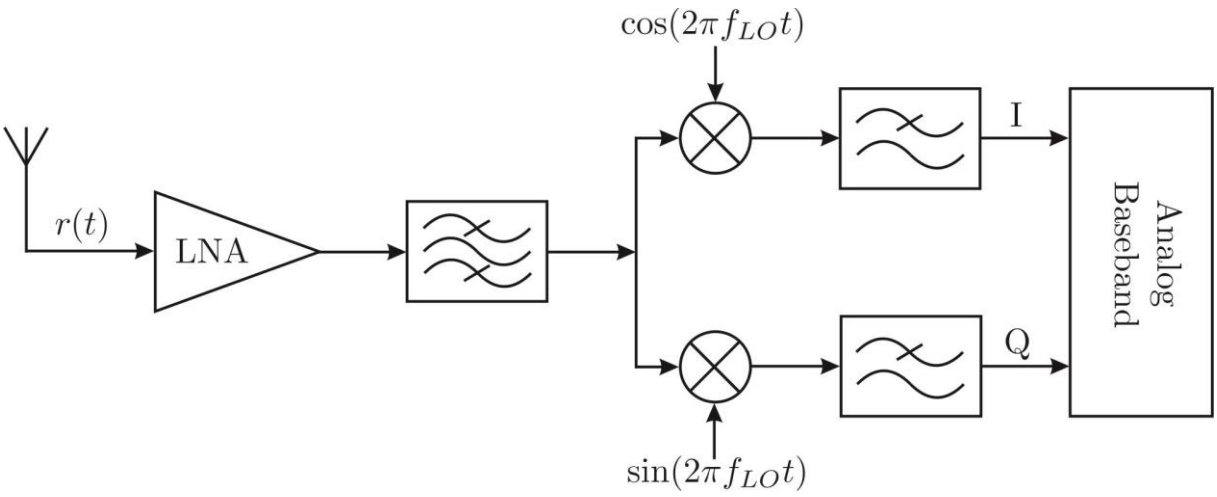

Figure 1 – Signal processing inside the Elonics E4000

B. The Realtek RTL2832U Demodulator

The Realtek RTL2832U is a baseband demodulator designed specifically for DVB-T and radio broadcasting reception but is not limited to these applications. It supports Zero-IF baseband and has a maximum sample rate of 3.2 MS/s. The RTL2832U receives the baseband I/Q signals directly from the E4000 and samples them with a resolution of 8 bit.

The RTL2832U contains an USB 2.0 interface supporting full and high speed modes. This interface is used to transfer the samples via bulk transfer to a connected host and to configure the chip via control transfer messages. An additional feature of this interface is that it can act as a repeater for the I2C bus. If the repeater is enabled, control messages received over USB are forwarded to the I2C bus as well as messages received on the I2C bus are forwarded to the

USB port. This mode allows configuration of the E4000 tuner via the USB interface, as the tuner is connected to the RTL2832U via the I2C interface.

C. Connection to the Tablet

The DVB-T USB stick is connected to the Android tablet via USB On-The-Go. This means that the tablet is acting as the USB host so it is able to communicate with the DVB-T stick. Figure 2 shows the prototype of the Traffic Detective.

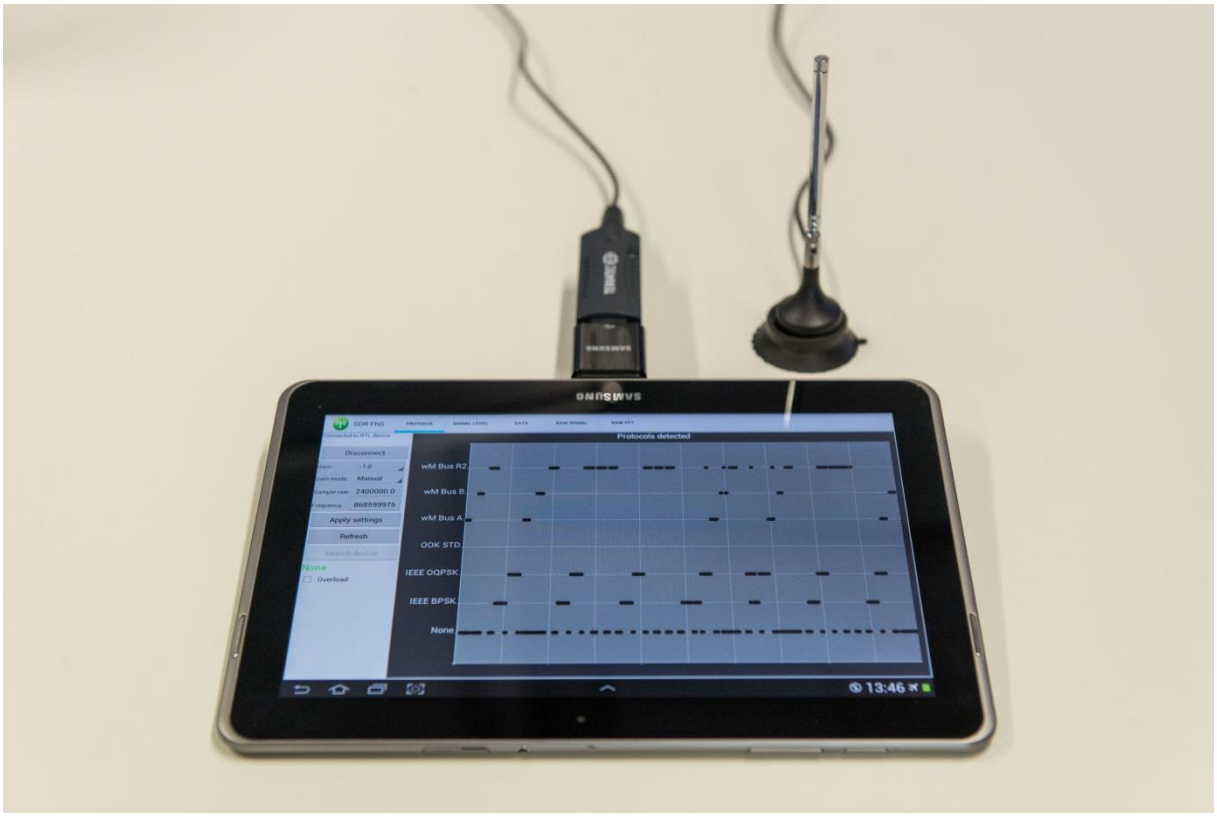

Figure 2 – Prototype of the Traffic Detective

IV. Implementation Aspects

The Android OS app Traffic Detective is the main front-end for the user. It controls the settings of the DVB-T USB stick and processes the raw I/Q samples. It is intended for use with a tablet device as a bigger screen improves the visibility of the displayed graphs and information. The DVB-T USB stick is attached to the tablet via a USB On-The-Go adapter. For this project, the Samsung Galaxy Tab 10.1N with an Android version 4.0.4 is used. The DVB-T USB stick used is the Terratec ran-T Stick+.

A. The Android App

The app is automatically started after the USB stick has been plugged in. In order to receive the desired signals, the app offers several configuration options. The center frequency in combination with the sample rate defines the frequency range which the tuner extracts from the received signals. Furthermore, the gain can be adjusted either automatically or manually. The former lets the tuner determine the optimal gain depending on the measured RSSI. The latter can be used to make user specific settings and fine adjustments.

The classification algorithm is run continuously once the DVB-T stick has been connected to the app. The received samples are analyzed about four times per second and, in case one of the supported wireless standards has been detected, it is displayed to the user. All calculations

based on the raw I/Q samples are executed in software without the need for specialized hardware. The classification is based on the last 512 I and Q samples.
One important aspect to note about the classification is that the center frequency is set to 868.6 MHz although most supported wireless standards use a frequency of either 868.3 MHz or 868.95 MHz. As a result, the signals do not necessarily have to be mixed down to baseband in order to be analyzed successfully. This makes the classification algorithm very adaptive and allows simultaneous classification of wireless standards in different frequency ranges.

B. The GUI

The app offers several different views to display the classified standards. The *Protocol* view is the main view and gives an overview of the history of standards recently detected. An example is shown in Figure 3. In case a protocol has been detected, it is shown by a dot on the respective line. For every classification attempt where no known standard has been detected, a dot is printed on the "None" line. This is also the case if the tuner detects an overload, e.g. if the antenna is too close to the sender or the gain is too high.

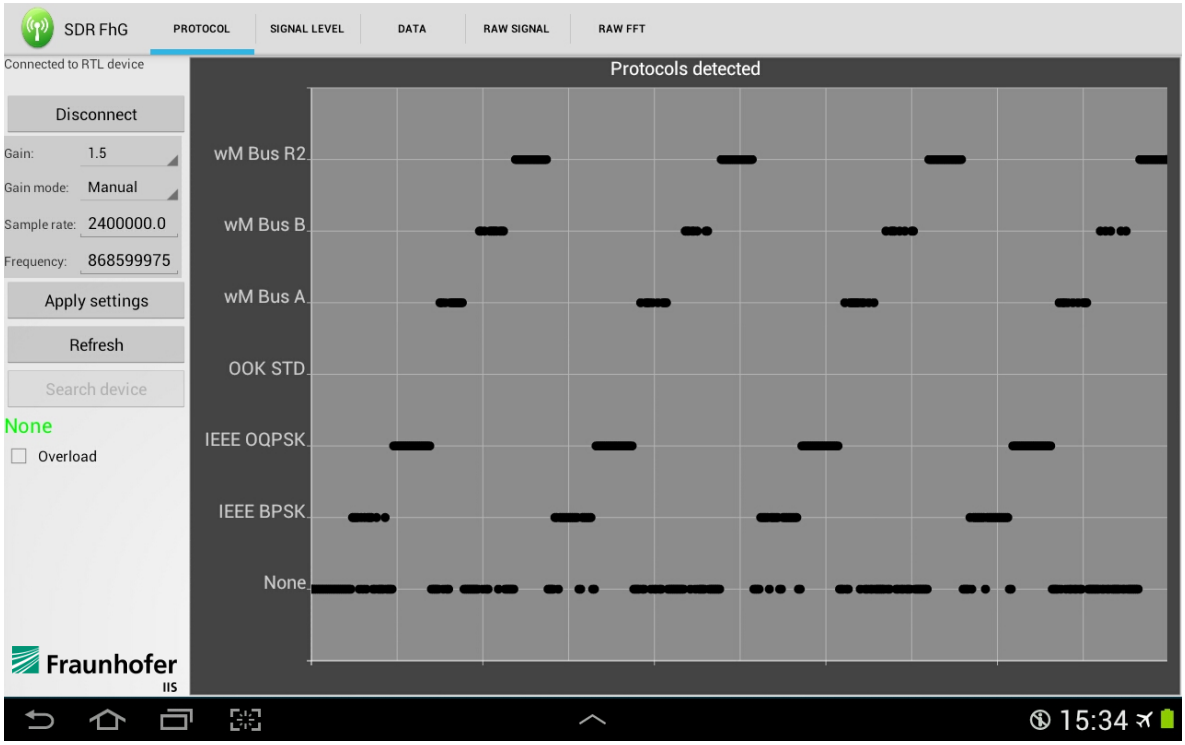

Figure 3 – Traffic Detective – History of classified standards

[Note that dots which are shown on both the *None* and a certain protocol's line at the same time are due to the resolution of the classifier. The classifier executes its algorithm faster than the transmitters send out the packets which results in a *None*-classification between two packets. Furthermore, the dots are scaled in a way that it seems to be a solid line where in reality there is a gap inbetween them. The reason for the large size of the dots is better readability for the user on a tablet screen.]

The history of signal strength (RSSI) is plotted on the view *Signal Level*. It is measured by the tuner chip in automatic gain mode and expresses the current RSSI value in dBm. This indication helps to analyze the signal strength on different locations. Figure 4 shows an example of this view. The rightmost end of the blue line indicates the current signal strength while the other values to the left are the measurements before.

Figure 4 – Traffic Detective – History of signal strength

For a more in-depth analysis, the *Data* view shows two graphs of the samples of the last detected standard. One shows the Fast-Fourier-Transformation (FFT) and the other one the I-value of the samples. Figure 5 shows an example analysis of the samples of the IEEE BPSK standard. On the top figure, the FFT is plotted. The center frequency of the IEEE BPSK is at 868.3 MHz, which can also be assumed by looking at the peak of the plot. The associated I-values of the waveform of the input signal are shown in the plot at the bottom. It consists of the 512 last received samples with their amplitude expressed in 8-bit values as retrieved by the Analog-Digital-Converter (ADC).

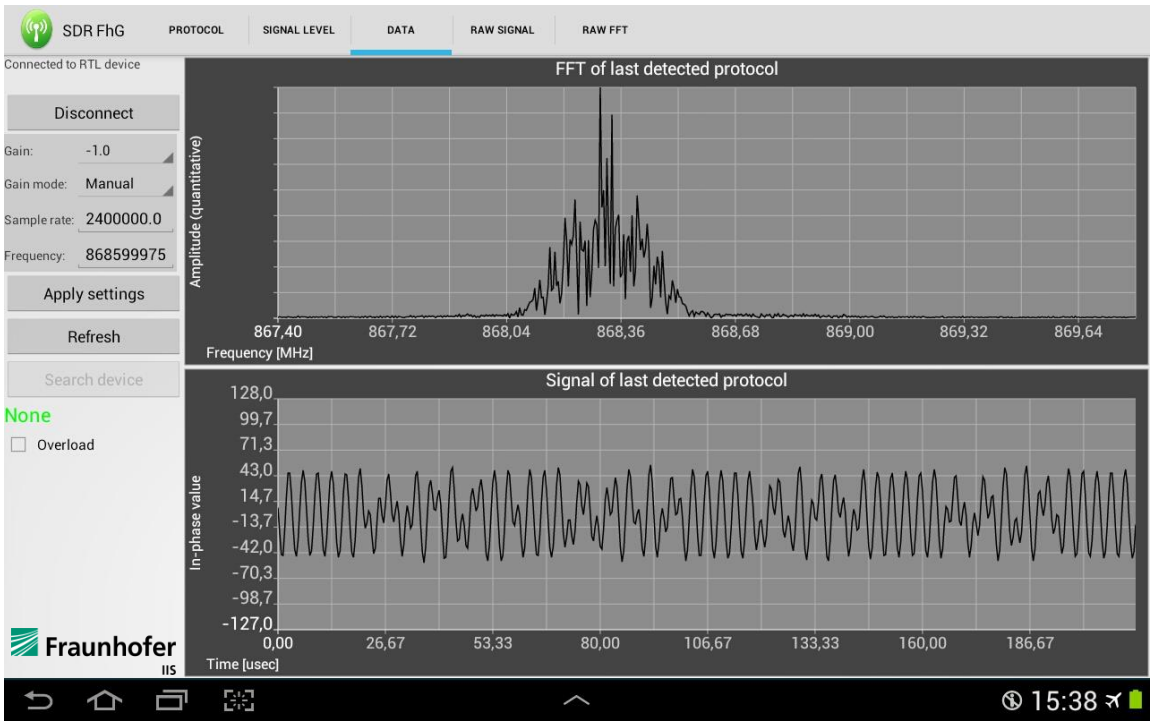

Figure 5 – Traffic Detective – Analysis of the last detected standard

Two additional views, *Raw Signal* and *Raw FFT*, allow a real-time insight into the surrounding wireless signals. The former view, Raw Signal, shows an accumulated statistic of the history of the minimum, mean, and maximum of the signal. The latter view, Raw FFT, is a real-time spectrum analyzer, enabling the user to determine whether there is wireless traffic on a certain frequency.

V. Potential Fields of Application

The presented 868 MHz Traffic Detective is suitable for numerous applications and scenarios where deeper insight into a certain communication scenario or network is required.
The device can be deployed for network management and monitoring tasks: For instance, the device can be used for network planning purposes whenever a new communication network is to be installed into a given environment. In order to make sure that the new wireless network will work reliably, a pre-analysis of the channel occupation in the area of interest is crucial, hence enabling the network planner to avoid those channels that are already significantly occupied. Once a network is installed, the Traffic Detective can be used for easy and user-friendly network management and monitoring. Functioning as a low-cost spectrum analyzer, time and frequency characteristics of received signals can easily be observed. Based on this, occupancy- and transmission-statistics of different frequency channels and communication standards can be generated, providing the network manager with detailed insights into the RF-traffic present within the environment and allowing him to identify the sources of potential or existing problems or interferences. This becomes more and more an issue, as the number of communication devices using the 868 MHz band is increasing steadily, and it is not assured that all of those devices are in accord with the mandated duty cycle regulations. Furthermore, jammers or intruders that deliberately try to occupy a certain channel or maliciously block the whole traffic on a frequency band may be detected. For this reason, the Traffic Detective can be permanently installed within a network for traffic observation or brought into an environment for diagnosis purposes whenever problems or malfunctions are recognized.
Even beyond this field of application, the device can be used as a simple and portable tool for RF-spectrum analysis, as time and frequency domain plots of received signals can be displayed and observed in real-time and in a very easy and user-friendly manner. Important transmission characteristics such as packet duration, packet repetition rate, center frequency and duty cycle can be examined as well as the exact time and frequency footprints of the signals.
Finally, it is worth noting that the presented approach is extendable to frequencies and communication standards beyond those mentioned within this paper. Therefore, it constitutes a highly dynamic tool for manifold tasks that frequently arise within typical RF-based areas of applications, like e.g. ambient assisted living (AAL), smart home, home automation, industrial communication networks, smart metering and many more.

VI. Conclusion

In this paper, we have shown that it is possible to use a portable tablet device with minimum external hardware as a low-cost spectrum analyzer. It provides in-depth insights into the surrounding wireless traffic and enables the user to monitor and debug wireless networks. The tool is able to classify several protocols, even at different frequencies, without reconfiguration. It is extendable to support a variety of additional standards and frequency ranges while reducing costs and complexity to a minimum.

References

[1] "IEEE Standard for Information Technology Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)", IEEE Standard 802.15.4-2006, Sep. 2006.

[2] "Communication Systems for Meters and Remote Reading of Meters - Part 4: Wireless Meter Readout (Radio Meter Reading for Operation in the 868 MHz to 870 MHz SRD Band)", DIN EN Standard 13757-4, 2005.

[3] "Information Technology - Home Electronic Systems (HES) - Part 3-10: Wireless Short-Packet (WSP) Protocol Optimized for Energy Harvesting - Architecture and Lower Layer Protocols", ISO/IEC Standard 14543-3-10:2012, 2012.

[4] Kuba, M.; Ronge, K.; Weigel, R., "Development and implementation of a feature-based automatic classification algorithm for communication standards in the 868 MHz band", *Global Communications Conference (GLOBECOM), 2012 IEEE*, vol., no., pp.3104, 3109, 3-7 Dec. 2012.

[5] Kuba, M., "Automatische Klassifikation von Kommunikationsstandards im europäischen 868 MHz Short Range Device-Band", *Ph.D. Thesis, University of Erlangen-Nuremberg*, 2012.

[6] RTL-SDR Website, http://www.rtl-sdr.com/, 10.10.2014.

[7] Elonics Ltd., "Multi-Standard CMOS Terrestrial RF Tuner", *E4000 Datasheet 4v0*, 2010.