A User-Friendly Android-Based Tool for 868 MHz RF Traffic- and Spectrum-Analysis

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*—In this paper, a software-based implementation of a Traffic Detective for radio traffic monitoring in the 868 MHz band is presented. Besides the user-friendly graphical user interface of the Android app, this paper reports about the algorithms used for traffic monitoring and automatic communication standard recognition, implementation aspects as well as the receiver hardware used. Finally, use-cases and potential application-scenarios for the system are presented.**

***Keywords*—RF analyzer, wireless standard classification, Android app, tablet, 868 MHz SRD, spectrum analyzer**

I. Introduction

Many modern applications that are based on wireless short range communication make use of the European 868 MHz Short Range Device (SRD) frequency band since it offers several advantages compared to the 2.4 GHz ISM band, for instance. However, with an increasing amount of devices occupying the same frequency range the probability of packet collision and data loss rises. Detection of communication problems that come with the over-occupation of frequency channels is usually a quite difficult task that requires special training, experience and high-priced tools for radio traffic analysis. Therefore, in this paper we present a prototype of a user-friendly and portable Android OS based tool for radio traffic monitoring in the 868 MHz band. The solution is inspired by the RTL SDR project [6] that uses off-the shelf and low-cost DVB-T dongles based on the Realtek RTL2832U receiver as inexpensive software defined radio frontends. The traffic monitoring algorithms are implemented in the form of an Android app that runs on handheld end-user devices, connected to the DVB-T dongle via USB. The software is, amongst other things, capable of detecting RF packets and signal spectrum shapes in different channels within the 868 MHz band, automatic recognition of the most common RF standards in this frequency range, signal strength based localization of transmitters, generation of occupancy statistics and visualization of the results in the time and frequency domain.

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 introduced 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. Pattern Recognition for Standards in the 868 MHz Band

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

A. *Communication Standards in the 868 MHz SRD Band*

One of the most prominent standards in the frequency range of interest is certainly the DIN EN 13757-4 [1], which is used by the higher-layer protocols Wireless M-Bus and KNX RF. Another very important standard is the IEEE standard 802.15.4 [2] which serves as PHY- and MAC-layer for various protocols like ZigBee, WirelessHART, MiWi, ISA100.11a and 6LoWPAN. Furthermore, the standard ISO/IEC 14543-3-10 [3], also known as the EnOcean Radio Protocol, is often used for RF communication applications based on energy harvesting.

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), however with different carrier frequencies, coding schemes and data rates.

IEEE 802.15.4 compliant devices essentially make use of two different PHY-layer protocols when used in the 868 MHz band, out of which one utilizes binary phase shift keying (BPSK) while the other one uses orthogonal quadrature phase shift keying (OQPSK) as a modulation format. Hence, those substandards will from now on be referred to as IEEE BPSK and IEEE OQPSK, respectively. Finally, the ISO/IEC 14543-3-10 standard, which will be referred to as OOK STD within the scope of this paper, uses on-off keying modulation.

B. Classification Algorithm

In order to automatically distinguish between different communication standards, an algorithm has been developed that is based on pattern recognition in the digital domain of an RF-receiver. Within this approach, several statistical key features are extracted from the received and digitized signal in order to draw conclusions with respect to the standard the received signal is based on. Once the feature values are calculated, they are compared to static threshold values until an end node of a binary classification tree is reached, that, in turn, is exclusively associated to one of the considered substandards.

It was proven in previous publications, that the chosen features 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 analog signal and filter out the required frequency. It then converts this frequency down to an intermediate frequency (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 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 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 and low frequency IF and has a maximum sample rate of 3.2 MS/s. The RTL2832U receives the IF I/Q signals directly from the analog tuner chip and samples them with a resolution of 8 bit. An optional gain control gives the user another possibility to amplify the signal retrieved from the tuner to a usable amplitude.

The RTL2832U contains a 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 tuner via the USB interface, as the tuner is connected to the RTL2832U via the I2C interface.

B. Supported Tuners

The I2C interface of the RTL2832 demodulator allows any tuner chip which supports configuration over I2C to be used as the analog frontend. Thus, the app includes drivers for three common tuner chips which are:

- E4000 from Elonics
- R820T from Raphael Micro
- FC0013 from Fitipower

After connecting a DVB-T stick to the tablet, the app automatically determines which tuner is available. If a supported tuner is available, the app loads the appropriate driver and configures the app as well as the possible user settings according to the functionality (e.g. available gains) supported by the tuner.

Each tuner offers different frequency ranges, gains, amplifiers and filters. All have in common that they support a frequency range of at least 60 to 1100 MHz. Two of the most important differences between the chips are the power consumption and the gain settings. Depending on the individual situation where the Traffic Detective should be used in, each DVB-T stick offers different properties and is better suited than the others.

Fig. 1 gives an overview of the signal processing inside the tuner. 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 a low frequency IF or Zero-IF 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.

An additional feature of the E4000 tuner is the calculation of the received signal strength indicator (RSSI) which can be used for automatic gain control and can even be read out by the app.

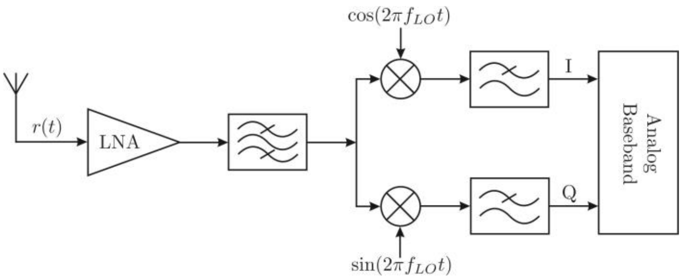


Fig. 1. General signal processing inside a tuner chip

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. Fig. 2 shows the prototype of the Traffic Detective.

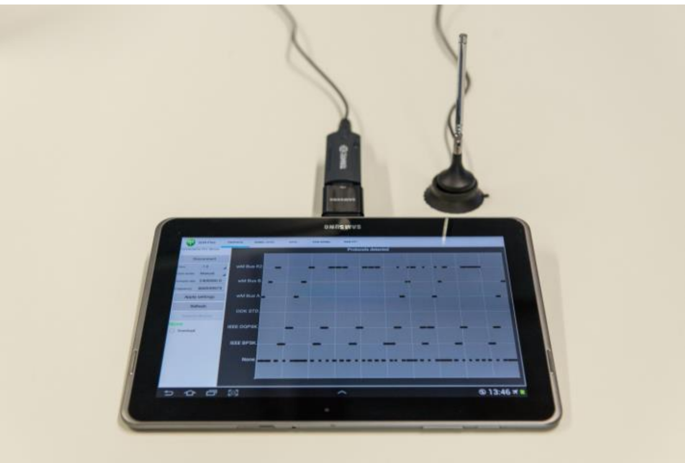


Fig. 2. Prototype of the Traffic Detective

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. The app is intended for use with a tablet device because 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, two tablets were tested which are the Samsung Galaxy Tab 10.1N with an Android version 4.0.4 and the Sony Xperia Z2 tablet with Android version 4.4.2. The DVB-T USB sticks used are the Terratec ran-T Stick+, Salcar TStick+ and the LogiLink VG0002A.

A. The Android App

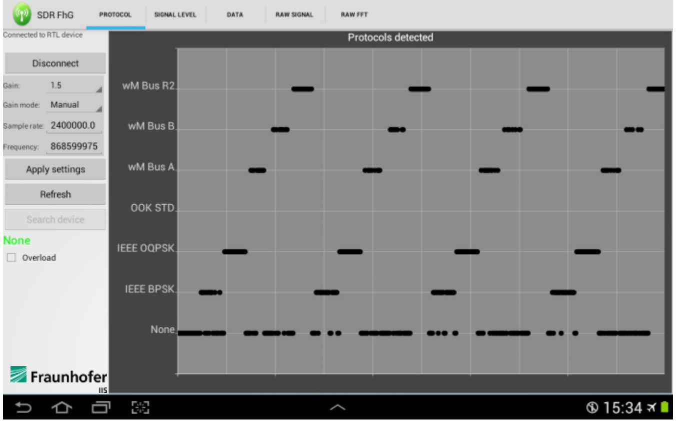
The app is automatically started after the USB stick has been plugged in. In order to receive the desired signals, the app offers several configuration options. The center frequency in combination with the sample rate defines the frequency range which the tuner extracts from the received signals. Furthermore,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

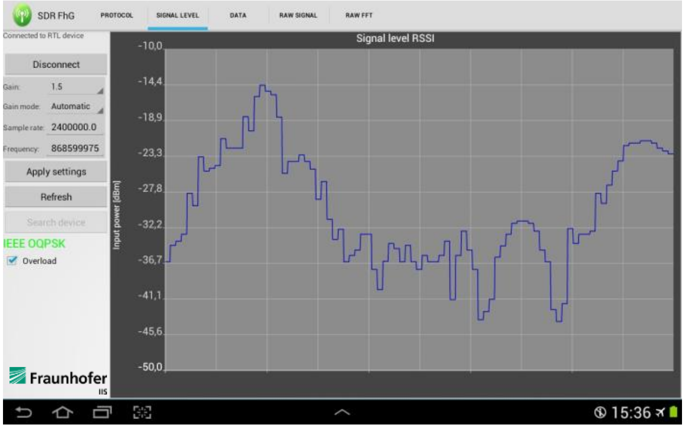


Gain: 1.5
Gain mode: Manual
Sample rate: 2400000.0
Frequency: 868599975

Fig. 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. Fig. 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. Note that this feature is only available when using the E4000 tuner because the others don’t support reading out the current RSSI value.



Connected to RTL device

Gain: 1.5

Gain mode: Automatic

Sample rate: 2400000.0

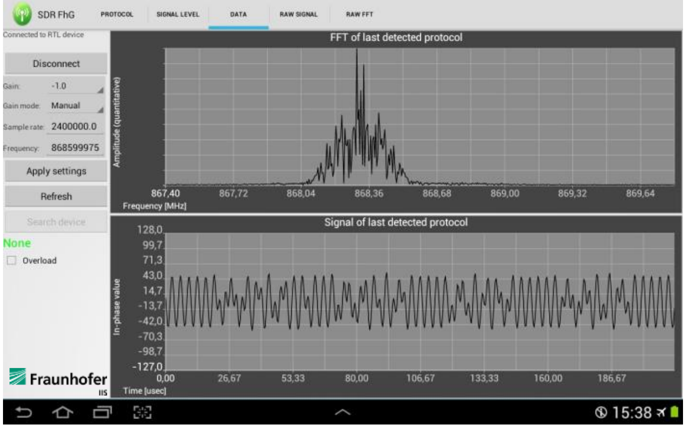
Frequency: 868599975

IEEE OQPSK

☑ Overload

Fig. 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. Fig. 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).



Connected to RTL device

Gain: -1.0

Gain mode: Manual

Sample rate: 2400000.0

Frequency: 868599975

None

☐ Overload

Fig. 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.

C. *Using an Emulated Android Device*

In addition to running the app natively on an Android device it can also be used in an emulated environment on a PC or similar. In this project, VirtualBox [7] was used to emulate Android. The app was installed into it and the DVB-T stick was attached to the Virtual Box. With this method, the user is not necessarily bound to using a native Android device but may also run the app on virtually any device (e.g. PC or laptop) where an emulated Android can be run.

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. Depending on customer needs, the Traffic Detective can be adjusted so it might be installed permanently 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.

The tool can be extended to be used as a frequency scanner over a broader bandwidth than the natively supported 2.4 MHz. This allows the user to receive an impression of the frequency occupation even on wider frequency bands. Further custom additions can include the implementation of important transmission characteristics such as packet duration, packet repetition rate, center frequency, duty cycle 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 ambient assisted living (AAL), smart home, home automation, industrial communication networks, smart metering and many more. The final use cases eventually depend on the customer needs for which the Traffic Detective can be customized in many ways.

VI. Conclusion

In this paper, we have shown that it is possible to use an Android app running on a portable tablet device with minimum external hardware as a low-cost and user-friendly 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] "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.

[2] "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.

[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] Oracle, VirtualBox Version 4.3.12, https://www.virtualbox.org, 2014.