SaFIC: A Spectrum Analysis Framework for Interferer Classification in the 2.4 GHz Band

Bastian Bloessl, Stefan Joerer, Noorsalwati Nordin, Christoph Sommer, Falko Dressler
Institute of Computer Science, University of Innsbruck, Austria
{bloessl,joerer,nordin,sommer,dressler}@ccs-labs.org

***Abstract*—We introduce the Spectrum Analysis Framework for Interferer Classification (SaFIC), a prototyping framework for interferer detection in wireless networks. Robustness has become the major challenge in many application scenarios such as health care and industrial automation. Besides the assessment of the available channel capacity and node mobility, interference among different networks and even network technologies is one of the most critical and challenging problems. SaFIC provides an interface that allows for the implementation of protocol specific detector modules for different sources of interference. Based on a generic interface, the detection modules can schedule individual scan jobs that are served by the framework. Currently, we support TelosB motes running Contiki OS for the scanning of the frequency band. We developed detection models for WiFi and IEEE 802.15.4 to demonstrate the capabilities of the framework.**

I. Introduction

Wireless communication is gaining importance for many applications in our daily life including WiFi access to the Internet. However, the shared use of the unlicensed 2.4 GHz ISM band is also a source of increasing interference among the different protocols. Besides WiFi, sensor networks, and Bluetooth devices, dedicated application specific protocols have been developed. Studies have shown that insufficient knowledge of interfering signals may lead to substantial performance degradation [1], [2]. However, current protocol designs, e.g., IEEE 802.11[abgn] or IEEE 802.15.4 do not take inter-protocol interference into account, thus reducing the robustness of the protocols. This even holds for critical network infrastructures in health care or industrial automation environments, where real-time communication is as important as robust and reliable information exchange [3].

Assuming better knowledge about the source of interference, it would be possible to design protocols using adaptive channel switching strategies as a possible and effective countermeasure [4]. Nonetheless, the aforementioned strategy requires spectral information and would greatly benefit from information about the source of interference. This can be achieved by scanning the spectrum and subsequently analyzing the spectral data for the identification of the interferer.

Among others, Chowdhury and Akyildiz studied the problem of interferer detection and formulated a general methodology [5]. In particular, the authors used sensor nodes to collect spectral data which was used for offline interferer identification. Most of the commercial spectrum analyzers, e.g., AirMagnet Spectrum XT, Agilent Spectrum Analyzer or Bandspeed AirMaestro employ specialized hardware. They are expensive and cannot be easily integrated into an interference-aware protocol design. However, tools such as Wi-Spy and Ubertooth are more affordable, but provide limited capabilities. Based on commodity hardware, Airshark [6] uses WiFi cards to identify different interference sources.

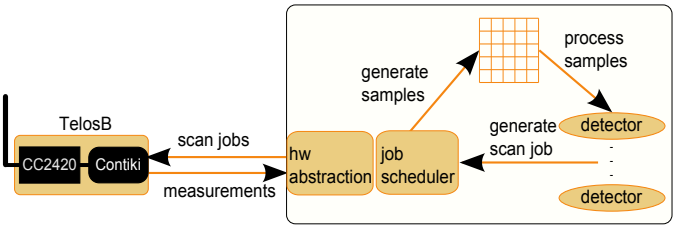


Figure 1. SaFIC Interferer Detection Architecture

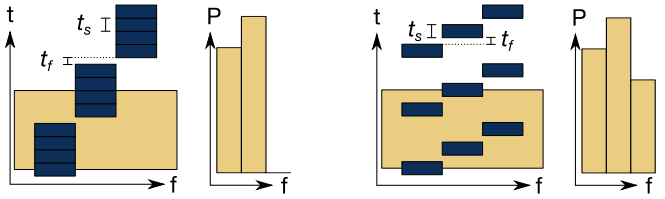
In this paper, we propose the Spectrum Analysis Framework for Interferer Classification (SaFIC), a sensor node-based spectrum analysis framework for the 2.4 GHz ISM band. Our framework uses a sensor node to measure the Received Signal Strength Indicator (RSSI) in a predefined spectrum and visually displays the signal strengths and their corresponding frequencies in real-time. It is implemented on typical sensor node hardware using a Chipcon CC2420 transceiver chip that is widely used in many application domains including health care, building automation, and industry automation.

We employ configurable scans of the entire spectrum or parts of the frequency range either stepping through all available frequencies or scanning each selected frequency for a predefined time, i.e., getting multiple measures per frequency before switching to the next one. One of the key challenges for interferer identification is the timing of the separate sweeps, because each protocol has a completely different fingerprint in time and space (spectrum).

II. Architecture

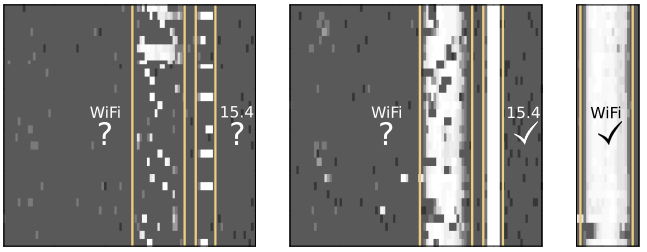
A. Spectrum Analysis Framework for Interferer Classification

The SaFIC framework provides a prototyping environment for a set of interference detection modules as shown in Figure 1. The framework abstracts from the underlying scan device and thus allows hardware independent detector implementations. The detector modules create scan jobs that are served by the SaFIC framework. Each scan job defines how a certain part of the spectrum is sampled. The sampling can be adjusted using *sweep* and *dwell* parameters. While the *dwell* parameter defines



(a) Slow sweep (b) Fast sweep

Figure 2. Sweep strategies



(a) Cfg 1 (b) Cfg 2 (c) Cfg 3

Figure 3. Spectrum visualization for different sampling strategies

how many RSSI values are collected on a certain frequency, the *sweep* parameter specifies how often to cycle through the spectrum. The conceptual characteristics and impact of these parameters are depicted in Figure 2a, which shows a job with 1 *sweep* and 4 *dwells*, while Figure 2b shows a scan job with 3 *sweeps* and 1 *dwell*. Assuming a frequency spectrum over time indicated by the large colored box, the spectral analysis using the two sampling strategies results in the observed power distributions depicted in the corresponding histograms. When using multiple detector modules, their synchronization, however, is a critical challenge.

B. Hardware Description

The currently supported hardware for measuring the RSSI values is a TelosB mote running Contiki OS. The system is based on a Chipcon CC2420 transceiver chip and a MSP430 microcontroller [7]. According to the data sheet, the transceiver can measure RSSI values at a frequency resolution of 1 MHz. The achieved sample rate of the framework is around 5 kHz. The mote transmits raw sampling data back to the SaFIC framework via an emulated serial port over USB.

We measured the sampling frequency using the Contiki `rtimer` library. The time resolution of `rtimer` is $1/425984 = 2.348\,\mu s$. The measured time between two samples on the same frequency is 3 cycles, resulting in a sampling time of $t_s = 7.043\,\mu s$. In contrast, the measured time to switch between two samples on different frequencies ranges from 12 to 13 cycles, i.e., 28.17 µs to 30.518 µs. Hence, the time t_f for changing the frequency is 21.128 µs to 23.475 µs.

C. Visualization and Detection Modules

We implemented a visualization module that displays the aggregated spectrum use. The visualization helps in the algorithm development by getting a feeling for the limitations of the hardware and the impact of different sampling strategies. Figure 3 depicts the influence of the *sweep* and *dwell* parameters when sampling concurrent WiFi and IEEE 802.15.4 transmissions. Each line of the heatmaps represents a single scan job. As can be seen, the detection quality strongly depends on the selected sampling technique and frequency. For the first configuration, neither WiFi nor IEEE 802.15.4 can be positively identified. Changing the sampling parameters to the second configuration allows to identify IEEE 802.15.4. The third configuration, however, perfectly samples WiFi transmissions.

We currently evaluate the detection modules based on a threshold-based algorithm that compares the measurements to the shape of WiFI and IEEE 802.15.4 spectral masks, respectively. As indicated in Figure 3, the modules are already able to detect individual interfering transmissions. However, differentiating multiple interferers that operate in the same frequency range remains a challenge. Our current work focuses on overcoming these limitations.

III. Conclusion and Future Work

We introduced the interference detection framework SaFIC, which allows us to analyze the used spectrum in the 2.4 GHz ISM band for interferer detection. Furthermore, we implemented basic detector modules for IEEE 802.11 and IEEE 802.15.4. Although these modules leave much room for further optimization, it turns out that these simple implementations already provide very good results. Moreover, the development and testing of interference detection algorithms is aided by modules for visualization of the measured RSSI values and the results of the detectors. The visualization of the spectrum also emphasizes the influence and importance of different sampling strategies. For future versions, we plan to add detector modules for additional interference sources such as Bluetooth or microwave ovens. Especially for Bluetooth the timing of the measurements might be the key challenge as its channel hopping frequency is 1.6 kHz. Based on the identification process, adaptive and interferer-aware protocol versions can then be investigated.

References

[1] S. Shin, H. Park, and W. Kwon, "Mutual Interference Analysis of IEEE 802.15.4 and IEEE 802.11b," *Elsevier Computer Networks*, vol. 51, no. 12, pp. 3338–3353, 2007.

[2] A. Sikora and V. Groza, "Coexistence of IEEE 802.15.4 with Other Systems in the 2.4 GHz-ISM-Band," in *IEEE IMTC 2005*, vol. 3, Ottawa, Canada, May 2005, pp. 1786–1791.

[3] F. Chen, R. German, and F. Dressler, "Towards IEEE 802.15.4e: A Study of Performance Aspects," in *IEEE PERCOM 2010, IQ2S Workshop*, Mannheim, Germany, March 2010, pp. 68–73.

[4] R. Gummadi, D. Wetherall, B. Greenstein, and S. Seshan, "Understanding and Mitigating the Impact of RF Interference on 802.11 Networks," in *ACM SIGCOMM 2007*, Kyoto, Japan, August 2007, pp. 385–396.

[5] K. R. Chowdhury and I. F. Akyildiz, "Interferer Classification, Channel Selection and Transmission Adaptation for Wireless Sensor Networks," in *IEEE ICC 2009*, Dresden, Germany, June 2009, pp. 1–5.

[6] R. Shravan, P. Ashish, and B. Suman, "Airshark: Detecting Non-WiFi RF Devices Using Commodity WiFi Hardware," in *ACM SIGCOMM 2011*, Berlin, Germany, November 2011, pp. 2–4.

[7] J. Polastre, R. Szewczyk, and D. Culler, "Telos: Enabling Ultra-Low Power Wireless Research," in *ACM/IEEE IPSN 2005*, Los Angeles, CA, April 2005, pp. 364–369.