Mais qui se cache ici ?

Gwendoline Hochet Derévianckine, Alexandre Guitton, Oana Iova, Baozhu Ning, Fabrice Valois

Mais qui se cache ici ?

Gwendoline Hochet Derévianckine[1,2],
Alexandre Guitton[3], Oana Iova[1], Baozhu Ning, Fabrice Valois[1]

[1] *INSA Lyon, Inria, CITI, 69621 Villeurbanne, France*
[2] *Semtech, Meylan, France*
[3] *Université Clermont-Auvergne, CNRS, Mines de Saint-Étienne, Clermont-Auvergne-INP, LIMOS, 63000 Clermont-Fd.*

La bande de fréquences Industrielle, Scientifique et Médicale (ISM) 2.4 GHz est connue pour être très encombrée par une multitude de technologies sans fil telles que Wi-Fi, Bluetooth ou encore IEEE 802.15.4. Le déploiement récent de LoRa®, une modulation radio très utilisée pour l'Internet des Objets (IoT), dans cette bande de fréquences nécessite l'étude préalable des signaux radios déjà présents. Dans ce papier, nous présentons une méthodologie pour la caractérisation d'un environnement radio se basant sur une analyse du canal obtenue avec une radio logicielle (USRP). L'objectif est de connaître les technologies utilisant la bande de fréquences ISM 2.4 GHz, sur quelle largeur de bande elles opèrent, à un instant donné.

1 Introduction

The 2.4 GHz ISM band is a frequency band in the unlicensed spectrum used by many wireless technologies such as Wi-Fi, Bluetooth, and IEEE 802.15.4. Lately, the Internet of Things (IoT) community is showing interest to the features of the 2.4 GHz ISM band, in particular its worldwide availability and lack of duty cycle. In this context, Semtech proposed a version of LoRa [1] to operate in this band.

The main challenge of the use of ISM frequency bands for wireless communication is their coexistence, i.e., how to provide efficient and reliable wireless communication when all radio technologies share the same medium. As the 2.4 GHz ISM band is already crowded, it is of the utmost importance to be able to analyze the use of this frequency band when a new radio technology, such as LoRa, is proposed.

Our contribution here is a methodology to characterize the use of a frequency band. Characterizing the use of a frequency band means being able to analyze a signal and associate it to a known technology using this frequency band. We also apply the proposed methodology to two recorded signals and verify that we are able to associate the signals to the right technology (Wi-Fi and Bluetooth in this case).

2 Background on the users of the 2.4 GHz ISM band

The regulations of the ISM frequency bands differ for each country or region. Depending on national limitations, parameters such as channel bandwidth, duty cycle, or transmission power can vary. The biggest advantages of the 2.4 GHz ISM band are the common and worldwide available set of frequencies, and the common regional parameters. As ISM frequency bands are part of the unlicensed spectrum, the users of these frequency bands have to be resilient to interference. Thus it raises coexistence challenges that need to be addressed, especially as the 2.4 GHz ISM band is known to be an overcrowded frequency band. Figure 1 illustrates the characteristics (channels and bandwidth) and the coexistence challenges of the main wireless technologies using the 2.4 GHz ISM band : IEEE 802.11g (the latest IEEE 802.11 standard designed for the 2.4 GHz ISM band only), Bluetooth, BLE, and IEEE 802.15.4. As we can notice, these four wireless technologies overlap and thus are exposed to interference. In this context, Semtech proposed three channels for LoRa, located 1 MHz away from the Bluetooth advertising channels, and at the edge of the independent Wi-Fi channels. Analyzing the 2.4 GHz ISM band occupancy is of uttermost importance in order to validate this choice of channels, as well as to allow a fair deployment for the original users of this frequency band.

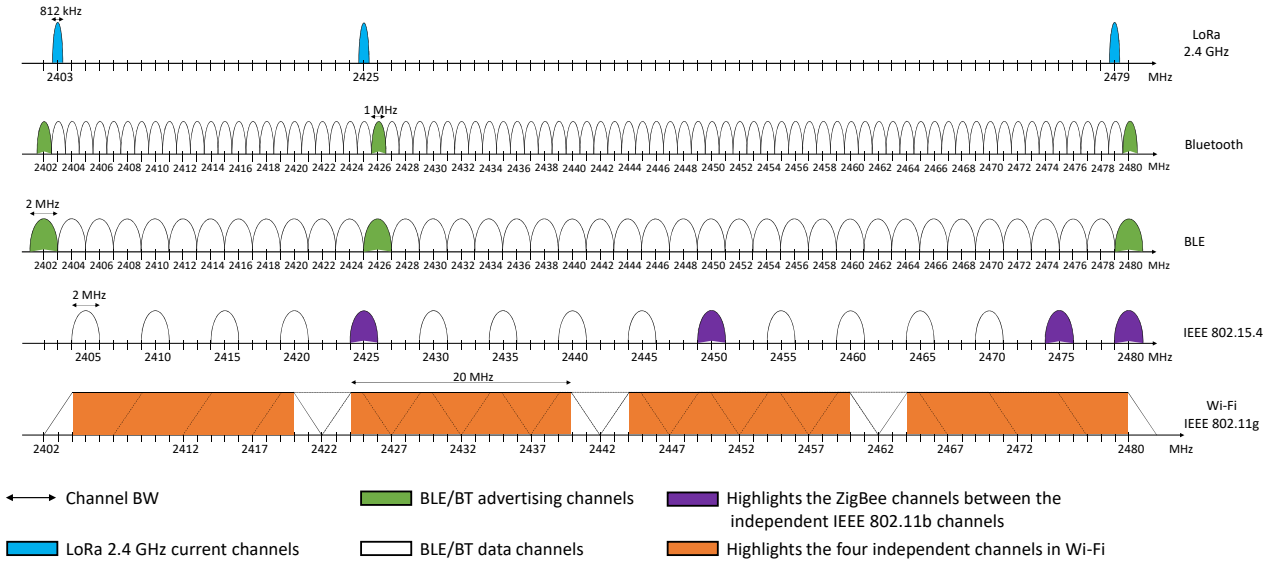

FIGURE 1 : Spectrum occupancy of LoRa and the main wireless technologies using the 2.4 GHz ISM band.

The existing literature encompasses several works around measurements and analysis of spectrum occupancy. For example, Höyhtyä et al. make measurements in the 2.4 GHz ISM band to estimate the idle time of the channels to potentially use those inactivity periods for cognitive radios, especially LTE [2] [3]. In both papers, the authors highlight the difficulty of differentiating a radio signal from a noise. Thus, they introduce a threshold to evaluate if the data collected is noise or signal. The authors obtain an amount of time when the spectrum is occupied, and they make assumptions of what applications it could correspond to, e.g., cameras and amateur radio services. However, to the best of our knowledge, no research paper focuses on mapping the measured signals to one particular technology.

3 Methodology for wireless technology detection

The goal of this work is to identify which (well-known) radio technologies are using the 2.4 GHz ISM band considering only the analysis of the signal. Our methodology for wireless technology detection following the characterization of the radio environment of the 2.4 GHz ISM band consists of the following steps :

1. We sense the radio environment and we capture the wireless signals that are present using a software defined radio (the USRP B200 mini in our case) connected to a laptop. We used the GNURadio software [4], which allows the visualization of the I/Q signals, and save them into binary files.
2. We perform a Fast Fourier Transform (FFT) on the obtained signal, to convert it into individual spectral components. We apply Parseval's theorem hence we can output a heatmap of energy distribution.
3. We compute a threshold to define if the recorded signal is either a noise or a radio transmission from a wireless technology.
4. We compare each energy sample to this threshold, and we store the result in a gradient matrix : 0 if the energy sample is below the threshold, otherwise 1, 2, or 3 depending on how many times the energy sample is above the threshold value.
5. We convert the matrix into a figure to visualize the energy levels allowing us to associate the result to a wireless technology.

For all the post-processing of data (steps 2 to 5), we used Python programming combined with the JupyterLab software [5].

One question that arises is how much of the recorded bandwidth should we analyze. From Figure 1, we note that LoRa uses a narrow bandwidth in comparison with the other technologies in this frequency

band. To be able to identify a LoRa signal (bandwidths from 203 kHz to 1625 kHz), a Bluetooth signal (bandwidth equal to 1 MHz), a Bluetooth Low Energy signal (bandwidth equal to 2 MHz), and a Wi-Fi signal (bandwidth equal to 20 MHz for the IEEE 802.11g standard), we claim that for a 4 MHz recorded bandwidth, we are able to detect and to map a signal to the right wireless technologies if we split the record bandwidth into sub-channels of 200 kHz.

Next, we apply the proposed methodology on two different captured files of one minute each.

4 Signal association

We present in this section two results: the detection of a Bluetooth signal (Fig. 2) and the detection of a Wi-Fi signal (Fig. 3). These figures represent the output of our methodology (the gradient matrix with energy levels), where each line represents 250 μs and each rectangle represents 200 kHz.

In Figure 2, we observe that lines **50888** and **50889** have a sample energy at least three times above the threshold value. Six consecutive rectangles are detected as a signal. This means a signal of 1200 kHz bandwidth was detected. Since Bluetooth uses 1 MHz of bandwidth, we can associate this signal to the Bluetooth technology.

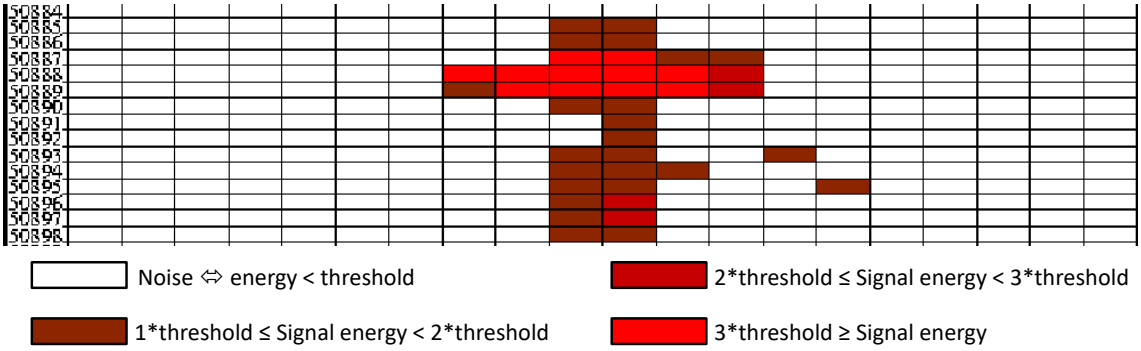

FIGURE 2 : Gradient matrix of a Bluetooth signal.

In this particular case, we recorded a Bluetooth advertisement on channel 37 centered at 2402 MHz. Bluetooth periodically advertises on three channels (37, 38 and 39). The interval between two consecutive advertisements varies from 20 ms to 10 s. After each advertisement, a random delay (between 0 and 10 ms) is added to avoid collision on the medium. Thus, using the post-processing, presented in Section 3, we are able to detect a Bluetooth signal and its periodicity.

In our second example, we apply our characterization methodology to the record of a Wi-Fi signal using channel 1 centered at 2412 MHz. Usually, a Wi-Fi access point sends a beacon every 100 ms. The duration of a beacon depends on the IEEE 802.11 standard used to transmit.

In Figure 3, we observe that lines **54297**, **54303**, **54321** and **54324** have all the rectangles colored. This means that there is a signal using at least 4 MHz of bandwidth. As the other main wireless technologies using the 2.4 GHz ISM band have narrower bandwidth, we can associate the signals to Wi-Fi. We make the assumption that lines where only few rectangles are not filled with color are also Wi-Fi signals, e.g., line **54318**. The observed empty rectangles are probably a result of how we compute the threshold value, combined with the fact that a Wi-Fi spectrum is not uniform on a given bandwidth.

5 Conclusions

In this paper, we propose a methodology to identify a wireless technology only based on its signal footprint. We validate our characterization method by applying it to Bluetooth and Wi-Fi recorded signals in the 2.4 GHz ISM band. The main challenge in this type of work (mapping a signal to a given technology) is to distinguish between the noise and the signal. We considered a threshold to distinguish between them, but it impacts the resulting energy heatmap after applying the FFT on each recorded sample. Plus, the energy of

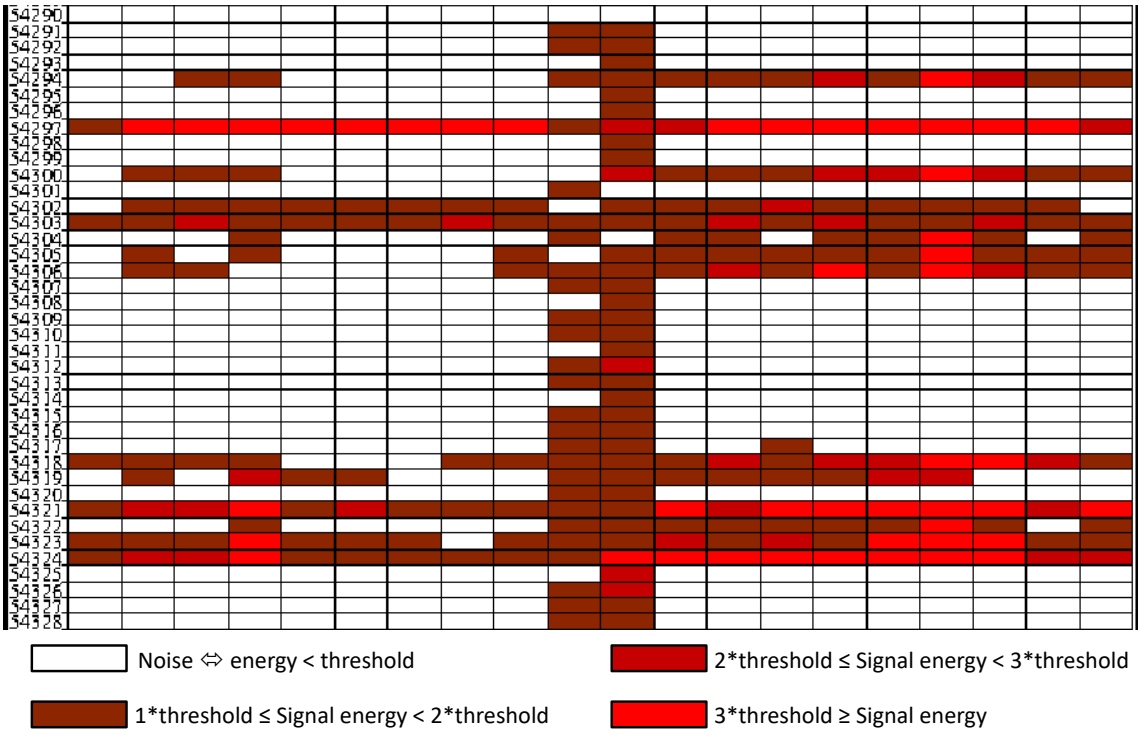

FIGURE 3 : Gradient matrix of a Wi-Fi signal.

a signal is not constant over time, so it might happen that in some cases, we have an energy higher than the threshold on one sub-channel and not on the adjacent sub-channel, making the signal mapping impossible because of insufficient information. Also, since the LoRa signal can be decoded under the noise level, more work is needed to have a good signal association in this case.

Going back to our motivation for this work (the study of the use of the 2.4 GHz ISM band), the proposed methodology gives us the fundamental building block to investigate the coexistence between LoRa and the other wireless technologies. We can now gather important information for studying interference detection and propose mitigation schemes.

Future work will include fine tuning of the threshold value, the automation of the technology identification process, and an improvement to our methodology to allow the detection of concurrent transmissions with signals from different wireless technologies.

Références

[1] Semtech, "LoRa technology," https://www.semtech.com/lora, accessed on: 2024-02-21. LoRa is a registered trademark or service mark of Semtech Corporation or its affiliates.

[2] M. Höyhtyä, J. Lehtomäki, J. Kokkoniemi, M. Matinmikko, and A. Mämmelä, "Measurements and analysis of spectrum occupancy with several bandwidths," in *2013 IEEE International Conference on Communications (ICC)*, Jun. 2013, pp. 4682–4686, iSSN: 1938-1883.

[3] M. Höyhtyä, M. Matinmikko, X. Chen, J. Hallio, J. Auranen, R. Ekman, J. Röning, J. Engelberg, J. Kalliovaara, T. Taher, A. Riaz, and D. Roberson, "Measurements and analysis of spectrum occupancy in the 2.3–2.4 GHz band in Finland and Chicago," in *Int. Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM)*, 2014, pp. 95–101, iSSN: 2166-5419.

[4] GnuRadio, "GnuRadio software radio ecosystem," https://www.gnuradio.org/, accessed on 2024-02-21.

[5] Jupyter, "Jupyter lab," https://jupyter.org/, accessed on 2024-02-21.