WiFi Beacon Analysis Report

Timo Niemann

> The code also contains the complete implementation and detailed explanations to the tasks.

Goal

The goal of this lab was to analyze recorded WiFi signals in the 2.4 GHz band. For this, four SDR traces on channels 1, 5, 9, and 13 were evaluated. The first part focused on the visible activity in the spectrum. After that, beacon frames were decoded, the address fields were examined, and possible signs of virtualized access points were checked. Finally, a custom beacon frame was generated and viewed again as a spectrogram.

SDR Trace Analysis

The traces contain complex IQ samples with a sample rate of 20 MS/s. For the spectrograms, the parameters from the task description were used:

Parameter	Value
FFT length	`2048`
Window length	`512`
Overlap	`64`
Sample Rate	`20 MS/s`
Trace duration	`0.25 s`

The color scale was calibrated equally for all four spectrograms so that the channels can be compared fairly. The noise floor was estimated using the 10th percentile of the summed channel power. The occupancy was then calculated as the share of time windows whose power was more than 10 dB above this noise floor. Since the traces are not calibrated to an absolute receive power in dBm, the reported noise floor values are relative dB values derived from the summed spectrogram power. Therefore, they are useful for comparing the traces internally, but they should not be interpreted as absolute RF power levels.

Channel	Center Frequency	Noise Floor	Occupancy
1	2412 MHz	-11.75 dB	2.4 %
5	2432 MHz	-13.25 dB	11.23 %
9	2452 MHz	-13.1 dB	3.36 %
13	2472 MHz	-11.1 dB	2.23 %

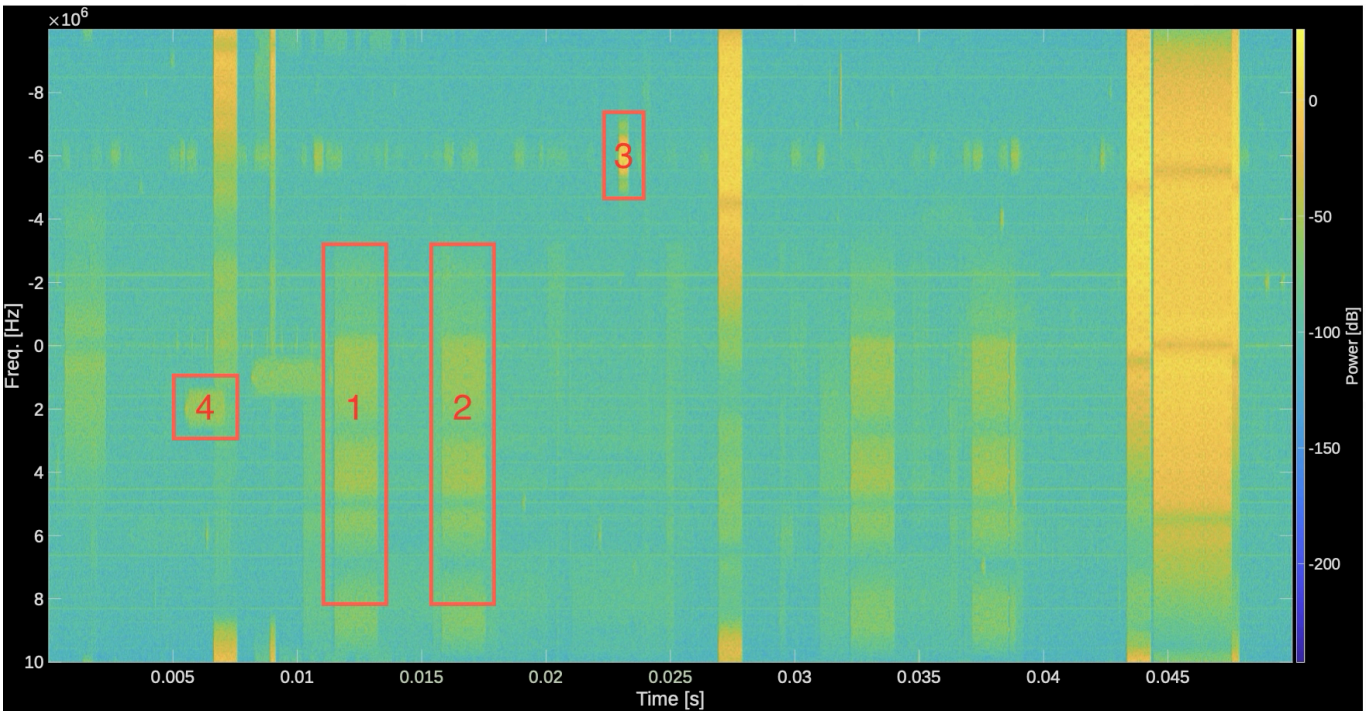
The busiest channel was channel 5.

Decoded Beacon Frames

With the adapted MATLAB example, beacon frames were detected in the traces and decoded with `wlanMPDUDecode`. Trace 1 was especially noticeable because several networks with very similar BSSIDs were found, for example:

SSID	BSSID	Vendor	Time in Record
TUB-IoT	5C:E1:76:66:02:E2	Cisco	40.1149ms
eduroam	5C:E1:76:66:02:E3	Cisco	40.3019ms
TUB-Guest	5C:E1:76:66:02:E4	Cisco	40.4586ms
_Free_Wifi_Berlin	5C:E1:76:66:02:E7	Cisco	40.6286ms

The first five bytes of the BSSIDs are identical, and only the last byte is different. This strongly suggests the use of multiple virtual BSSIDs on the same physical access point. Similar SNR values would further support this assumption, but they are not enough as proof on their own, because several real APs can also be placed very close to each other. The packets are close in time to each other, this suites an internal in code iteration over the to-be-announced-beacons for one AP also highly suggesting these beacons came from one physical device.



Rectangle 1 and 2 are likely WiFi data frames, in the analysis of 2513mhz.mat I've came across an equal looking pattern at 18.4303ms in frame which was decoded as data frame, also they occupy a similar frequency range and show a similar time-frequency pattern, so I assume these as WiFi packets. Rectangle 3 is likely not a WiFi frame because it is firstly not in the frequency range of the other 2 likely data frames and also is much shorter. Short Packages in WiFi would be beacons or ACKs but a beacon is transmitted over the whole frequency band and an ACK is not sent out of the blue, meaning it follows forgoing data, which this marked capture does not seem to have. I classify rectangle 4 also as a non-WiFi frame, it has a relative similar frametime as the likely data frames beside, but the frequency band is much smaler than the repeating data frames.

The address usage in beacon frames is as follows:

- Address 1: used to announce the destination station, in a beacon frame its FF:FF:FF:FF:FF:FF (meaning broadcast to all stations)
- Address 2: used to remark the source device address of the frame, the ap mac who sent the beacon is inserted
- Address 3: used for the bssid of the device sending the beacon, means usually address 2 equals address 3, when no virtual ap is used
- Address 4: this field does not exists, after the seq ctrl the frame body follows containing beacon data instead of an address, like timestamp, beacon interval, capability info, ssid, potentially the channel number, see the extracts from 2.1

For normal data frames, the meaning of the addresses depends on the direction:

- Downlink: AP -> Station
    - Address 1: MAC of the destination station
    - Address 2: MAC of the AP which transmits the frame
    - Address 3: MAC of the initial sender which has started the frame
    - Address 4: not used
- Uplink: Station -> AP
    - Address 1: MAC of the AP that receives and potentially forwards the frame
    - Address 2: MAC of the sending station
    - Address 3: MAC of the final destination station
    - Address 4: not used

The fourth address is only used in special cases, for example:

- 4 Address case: wireless bridge:
    - Address 1: MAC of the AP that should receive / transmit through the frame, for example AP, bridge node, repeater or mesh node
    - Address 2: MAC of the transmitter (into the other network)
    - Address 3: MAC of the final destination
    - Address 4: MAC of the initial sender

Generated Beacon

In the last part, a custom beacon frame with the SSID `wlan fahren wir noch` was generated. The beacon was configured for channel 1 in the 2.4 GHz band and uses a beacon interval of `100 TU`. For the spectrogram view, five beacon frames were generated. For visualization, the idle time was reduced to `1 ms`, so that multiple beacon frames are visible within the short spectrogram window.

In the spectrogram, only short and repeated signal regions are visible. Between them, there is almost no power because the signal was generated synthetically and does not contain real receiver noise, interference, or other WLAN frames. The beacon bursts look very similar because they were generated under ideal conditions.

Conclusion

The analysis shows that the four recorded channels were used with different intensity. Channel 5 was the most active one in this recording, while the other channels only contained short activity phases. By decoding the beacon frames, several SSIDs and their BSSIDs could be identified. The very similar BSSIDs in Trace 1 strongly suggest the presence of a virtualized access point configuration. The generated beacon also confirms how beacon frames appear in a spectrogram as short, repeated transmissions.