SEMTECH

WIRELESS & SENSING PRODUCTS

SX1280
Long Range, Low Power
2.4 GHz Transceiver

Application Note:

Wi-Fi Immunity of LoRa® at 2.4 GHz

AN1200.30
Rev 1
June 2017

Table of Contents

List of Figures

1 The Importance of Wi-Fi Immunity

Perhaps the most ubiquitous use of the license free ISM bands is wireless internet connectivity over Wi-Fi. At the time of writing, it is estimated that there is a Wi-Fi hotspot for every 150 people on earth [1].

Although Wi-Fi has seen expansion to neighboring ISM bands due to overcrowding, notably the 5.8 GHz ISM band, the bulk of Wi-Fi traffic remains in the 2.4 GHz ISM band, which typically spans from 2.4 GHz to 2.4835 GHz (at least in the USA and Europe).

Needless to say, any new technology deployed into this band must be robust against interference from incumbent Wi-Fi deployments. Given the recent expansion of LoRa® to the 2.4 GHz band, its coexistence with the most commonly found incarnations of Wi-Fi signal found in the 2.4 GHz band are of significant importance.

The following image shows the occupancy of the license free 2.4 GHz ISM band by wideband data communication using Wi-Fi.

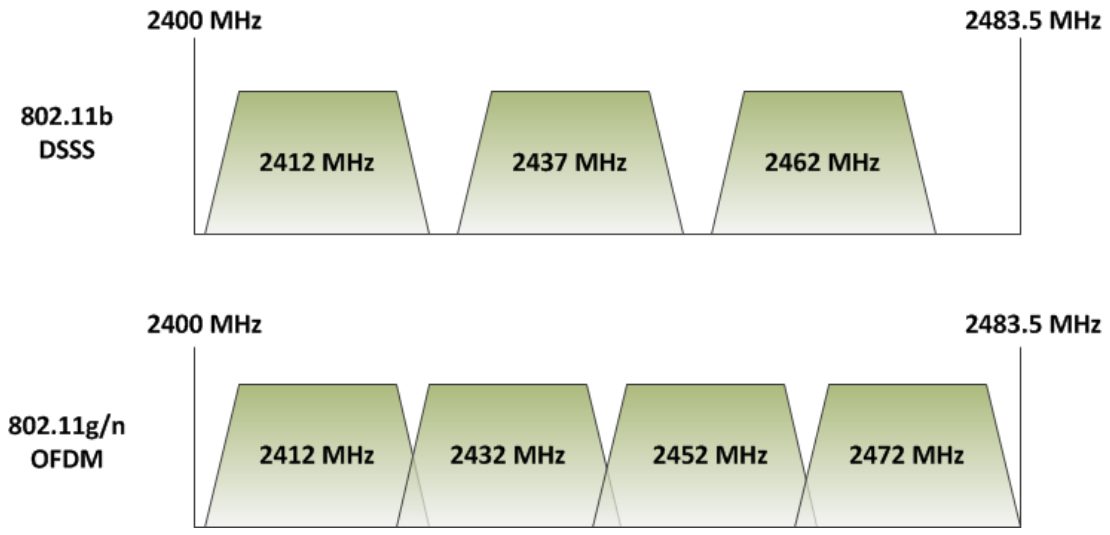

Figure 1: Example Non-Overlapping 2.4 GHz Wi-Fi Channels, Inspired by [2]

2 Generic Strategies for Avoiding Wi-Fi

Immunity to Wi-Fi can come from one, or a combination, of three strategies:

1) **Frequency Separation:** From the channel plan shown above, it is apparent that there is the possibility of avoiding certain portions of the spectrum based upon *a priori* or measured knowledge of the channel. This is an important strategy but is dependent upon some management at the MAC (Media Access Control) layer to achieve it, by sensing what is in the band and intelligently avoiding it. This means that either listening on a certain channel to ascertain the power level or having that information about clear channels sent to the radio implies management at a layer above the physical layer.

2) **Temporal Separation:** Avoiding communication in the 2.4 GHz band at the same time as communication by any Wi-Fi devices in the same vicinity is a challenging proposition. The Wi-Fi signal is characterized by typically high channel occupancy due to the nature of the usage [3] for example cites 50% to 80% occupancy in realistic scenarios.

3) **Spatial Separation:** Where the application use case permits, simply avoiding being in the same location as a Wi-Fi terminal is one of the simplest and most effective means of avoiding or reducing potential interference between radio systems. In this Note, however, we assume that we do not have full control over the location of the either terminal.

3 LoRa® Specific Strategies for Avoiding Wi-Fi

The use of the LoRa® physical layer affords us several potential additional performance benefits compared with legacy modulation techniques for coexistence and additional immunity to in-band and in-channel interference.

1) **Spread Spectrum:** LoRa® is a spread spectrum modulation technique, from which a coding gain is derived as the signal can be received with a negative SNR. Whilst, in the absence of interference, this equates to reception below the noise floor, in the presence of co-channel interference this instead equates to the ability to receive wanted signal powers that are weaker than the interfering signal.

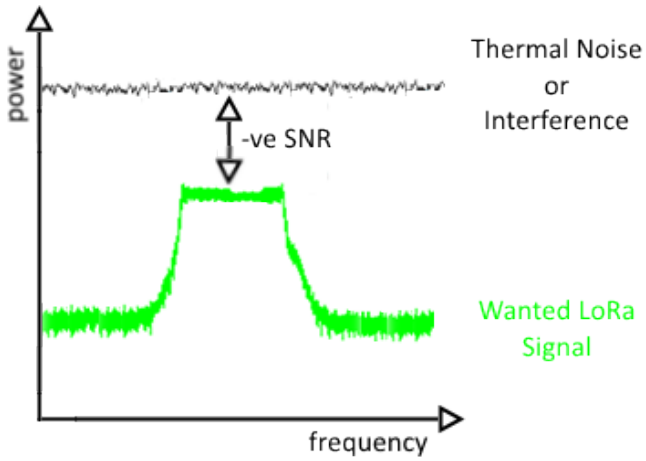

Figure 2: Principle of Reception below Thermal Noise Floor (equivalently Wideband Interferer)

2) **Low Bandwidth:** reduction in bandwidth has two benefits. Firstly, a lower bandwidth signal reduces the impact of adjacent signals so reduces the likelihood of being the victim of interference. If we compare the bandwidth of the LoRa® signal with the wider band Wi-Fi signal, we see that even a wide LoRa® signal only occupies a fraction of a single Wi-Fi channel. This brings us to the second benefit. The power of the Wi-Fi signal is spread across the whole Wi-Fi channel. The power seen in a narrower slice of this channel will therefore be a fraction of this power. Simply put, even in the case of co-channel interference, only exposing ourselves to a narrow portion of the signal power means we receive a proportionately smaller fraction of the Wi-Fi signal power.

3) **Forward Error Correction and Interleaving:** another benefit of the LoRa® modem is the availability of FEC (Forward Error Correction) and interleaving. Forward error correction allows the introduction of redundant information into the message that allows a limited number of bits that are corrupted to be corrected and recovered.

   Even with FEC sequential bit errors (i.e. neighboring corrupted bits) are the hardest to correct. For this reason interleaving is employed. This is a technique that redistributes the information in the packet so that, upon reconstruction, errors are less likely to be from adjacent bits.

4) **Partial Symbol Loss Immunity:** in addition to all of the aforementioned benefits of the LoRa® physical layer, it is also noteworthy that we can lose up to half of a LoRa® symbol (see below) before the data within that symbol is lost. In the case of burst of interference this affords us great interference immunity (over 100 dB in some cases).

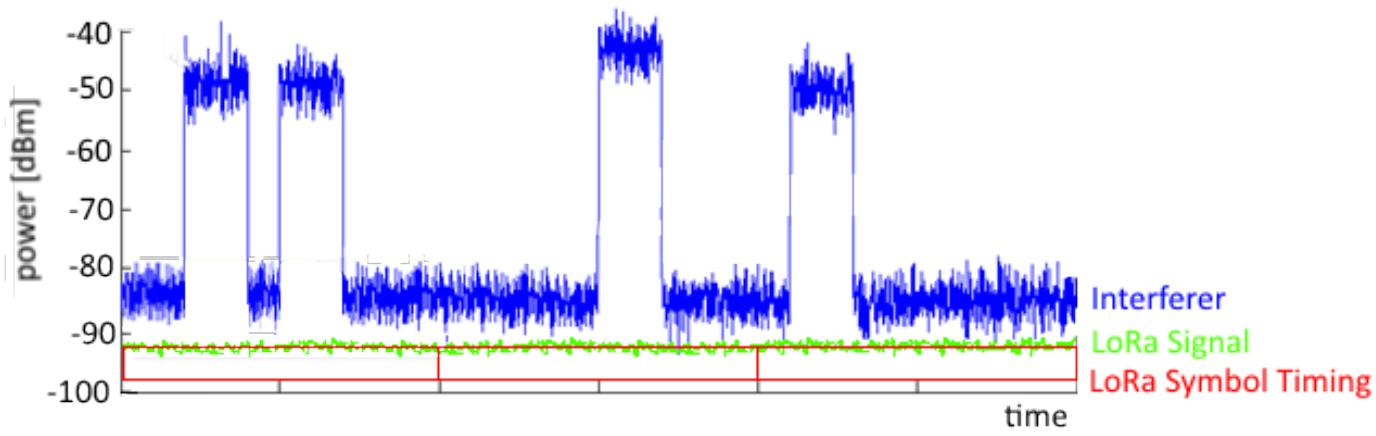

Figure 3: Power vs Time for an Interferer, LoRa® Signal and LoRa® Symbol Timing

A high power burst interferer can be tolerated provided it occupies less than 50% of the duration of a LoRa® symbol.

4 Scope of the Investigation

Any link employing LoRa® will benefit from the LoRa® specific interference immunity benefits detailed above. What is interesting is to determine which of the effects have the most influence and can be combined with the 'generic' avoidance techniques of the previous section to the greatest effect. In this Application Note we focus on this topic in the context of the most common forms of Wi-Fi interference.

5 The Wi-Fi Signal

Three common configurations of Wi-Fi signal were evaluated:

- 802.11b compatible CCK (DQPSK) 11 Mbps
- 802.11b compatible PBCC (QPSK) 11 Mbps
- 802.11g compatible OFDM (64-QAM) 54 Mbps

All are evaluated using the standard generator settings, which uses a 100 µs inter PPDU delay. The PPDU format is that of a data packet. The modulation bandwidths of the packets are shown below:

5.1 CCK

CCK (Complimentary Code Keying) is the form of modulation typically used when 802.11b operates at 11 Mbit/s. Measured bandwidth in CCK is shown below, as well as the measured time domain envelope of the modulation.

5.1.1 CCK Bandwidth

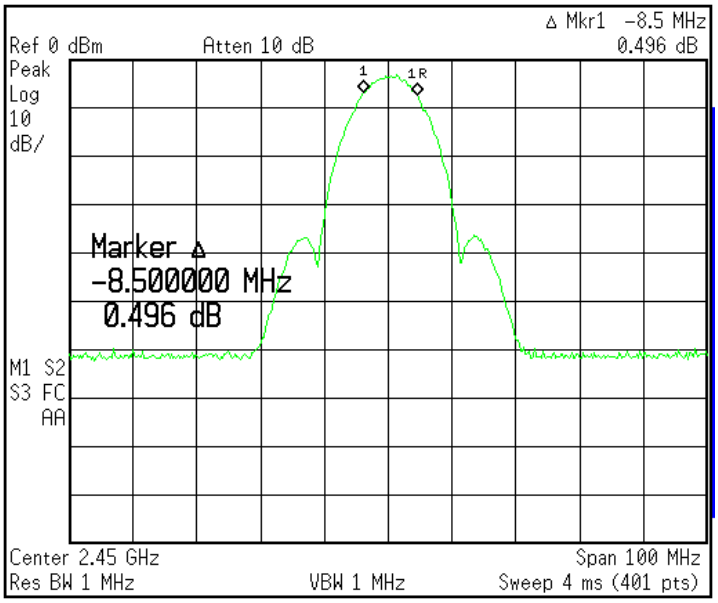

Figure 4: CCK Measured Bandwidth of 8.5 MHz

5.1.2 CCK Duty Cycle

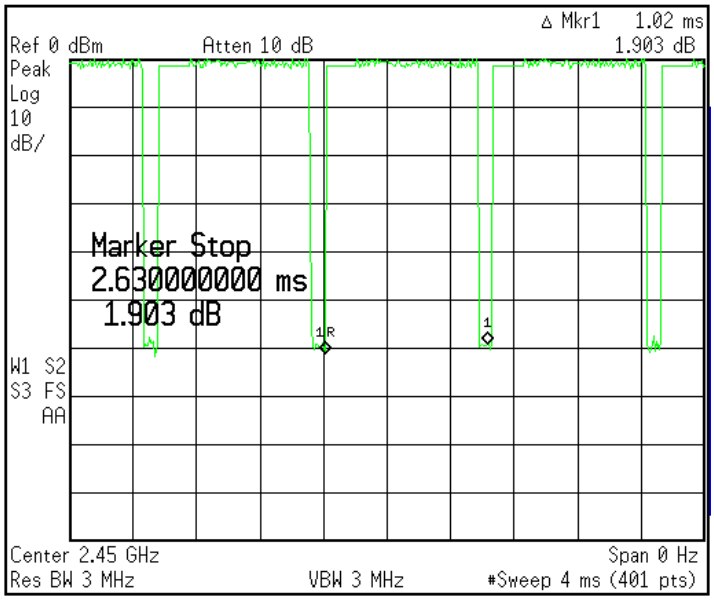

Figure 5: CCK Measured Duty Cycle of approximately 90%

5.2 PBCC

PBCC symbol can carry more data than a CCK symbol and can be used for communication at similar rates to CCK. The same modulation bandwidth and duty cycle information is presented below.

5.2.1 PBCC Duty Cycle

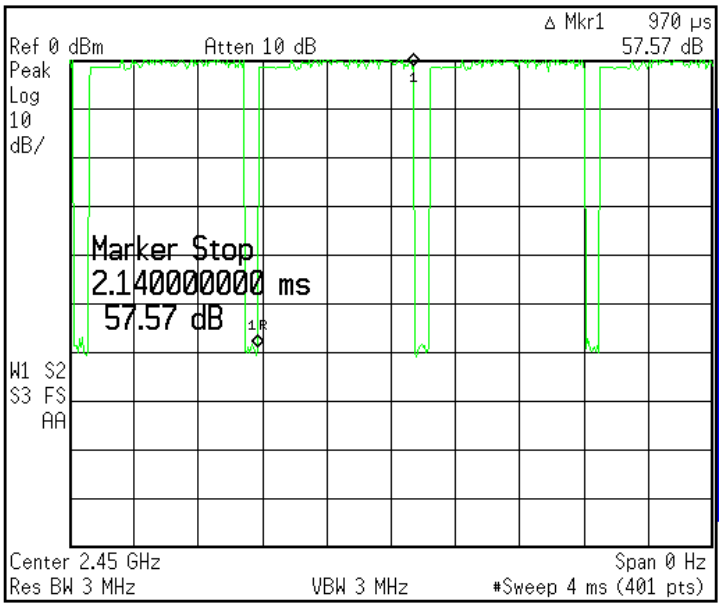

Figure 6: PBCC Measured Duty Cycle of approximately 90%

5.2.2 PBCC Bandwidth

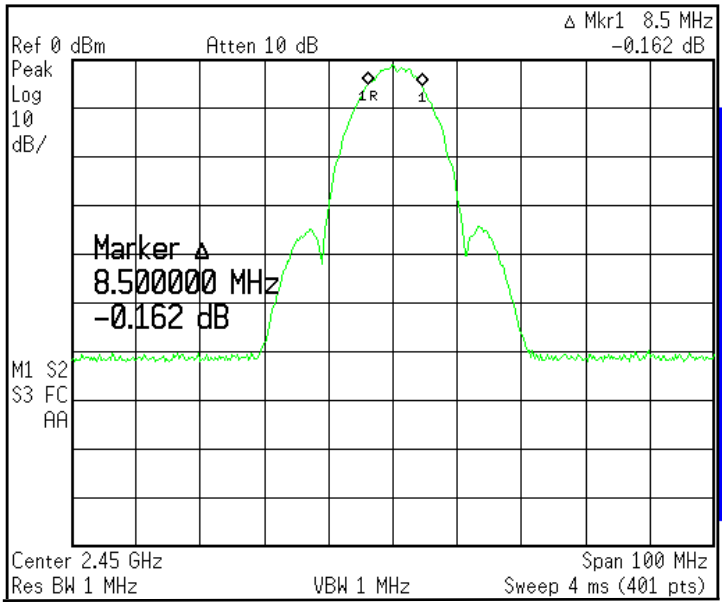

Figure 7: PBCC Measured Bandwidth of 8.5 MHz

5.3 OFDM

The higher spectral efficiency of OFDM allows the communication of much higher data rates in a narrower modulation bandwidth.

5.3.1 OFDM Duty Cycle

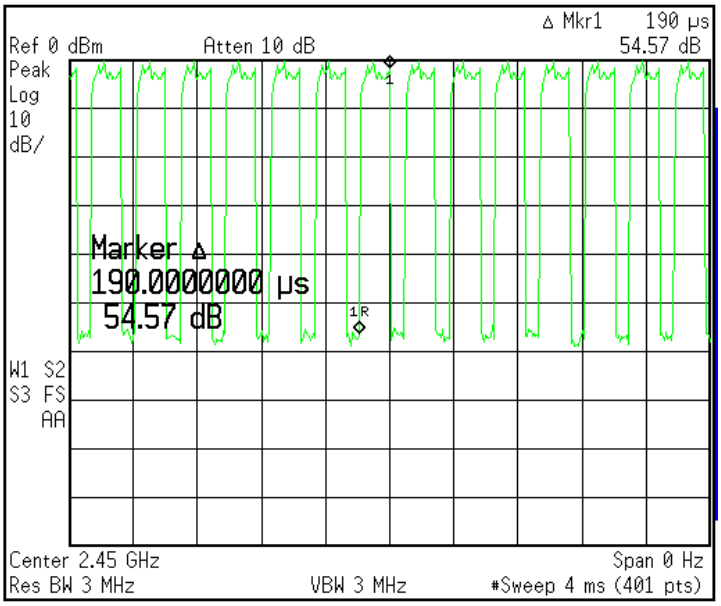

Figure 8: OFDM Measured Duty Cycle of approximately 60%

5.3.2 OFDM Bandwidth

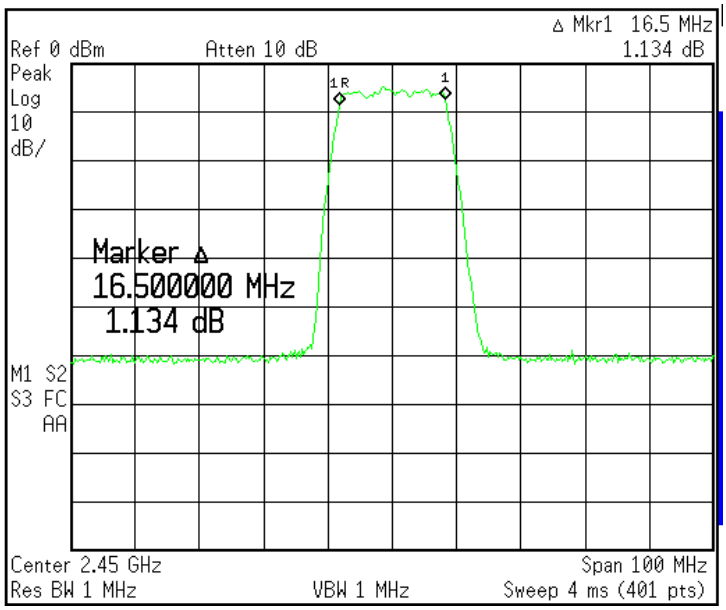

Figure 9: OFDM Measured Bandwidth of 16.5 MHz

6 Equivalence of CCK and PBCC

The CCK and PBCC spectrum are similar enough so that testing both of them independently is deemed not necessary.

7 PSD Measurement

The power spectral density seen in the 100 kHz and 3 MHz bandwidths are also explored below. Here we see that there is 10 to 15 dB of difference in the received power level. The spread, noise-like power spectral density of the Wi-Fi signal, is of significant interest as we expect to see an improvement in Wi-Fi immunity proportional to any reduction in receiver (modulation) bandwidth.

7.1 PBCC PSD

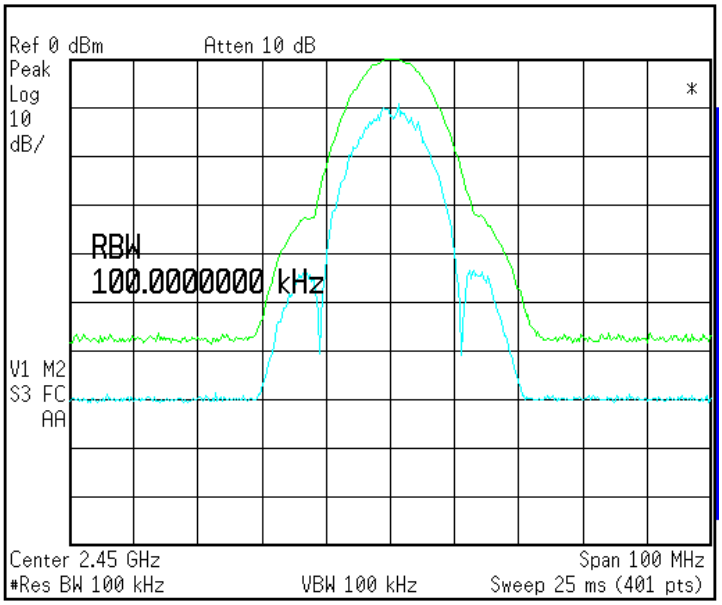

Figure 10: PBCC Measured Power Spectral Density at 3 MHz (green) and 100 kHz (cyan)

7.2 OFDM PSD

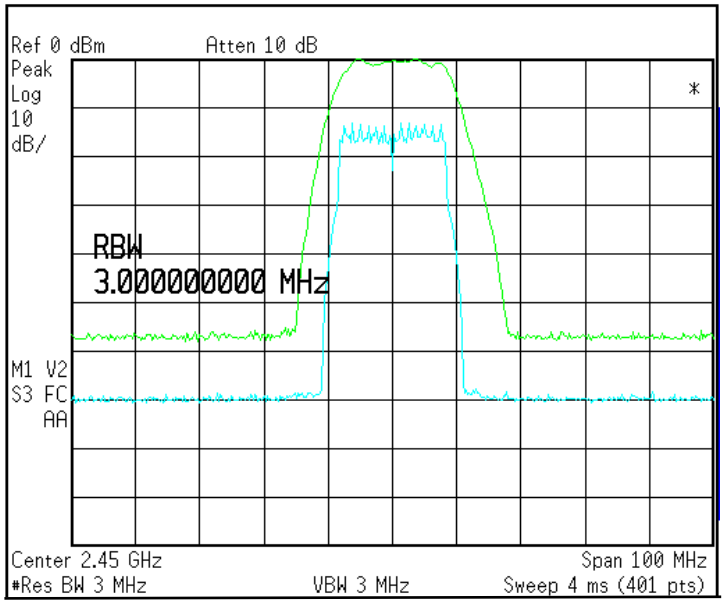

Figure 11: OFDM Measured Power Spectral Density

8 Aside: LoRa® Symbol Period

The time domain envelopes of the previous sections showed very little 'off' time compared with the high occupancy 'on' time. This high duty cycle unfortunately reduces the efficacy of the interference avoidance performance gains in the face of partial symbol loss.

However, lower duty-cycle interfering signal types, although now beyond the scope of our broadband Wi-Fi immunity study (such as Bluetooth) could still benefit from this mechanism.

So although not possible for broadband Wi-Fi signals which are characterized by high duty cycles, for completeness, the efficacy of any interference avoidance that relies on recovery of partially lost LoRa® symbols will rely on a favorably low ratio of symbol duration to the measured duty cycle of the interfering signal.

The LoRa® symbol period is given by:

$$T_S = \frac{2^{SF}}{BW}$$

where *SF* is the spreading factor and *BW* the programmed modulation bandwidth in Hz.
The figure below details the **ratio** of a single LoRa® symbol period to the corresponding OFDM transmit 'on' time (see *Section 5.3.1*). This is displayed as a function of SF and bandwidth below. This approach could be used as the starting point of evaluating the likelihood of benefiting from partial symbol recovery effects; however such effects will only be possible in the presence of other, lower duty cycle, interfering signals due to the limited 'off' time of the Wi-Fi signal.

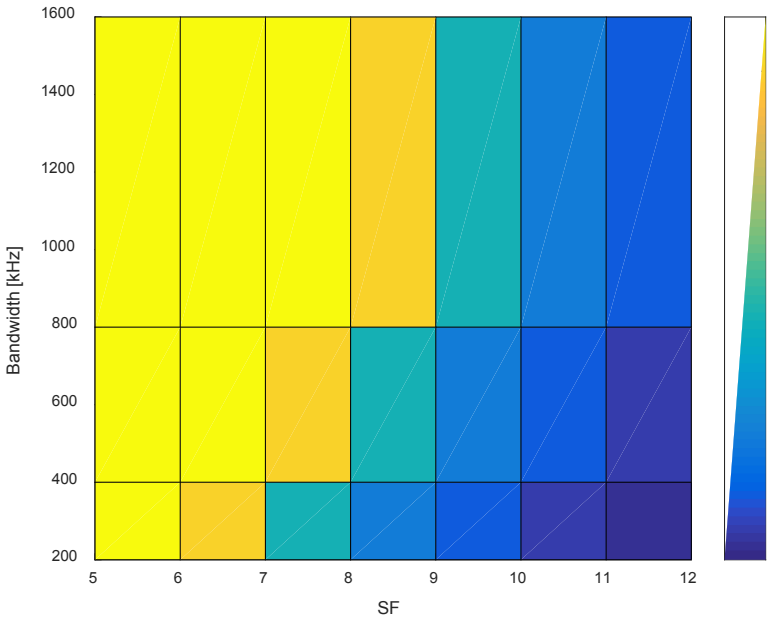

Figure 12: Fraction of a LoRa® Symbol Occupied by the OFDM Modulation 'on' Time

9 Measurement Setup

Returning to the question of broadband Wi-Fi interference immunity, the test setup used for our co-channel and in-band testing is shown below. Here RF signal generators are used to produce both the wanted signal and the interfering signal. Three interfering signal types were produced and tested against several format of LoRa® modulation at an RF center frequency of 2.45 GHz for both wanted and unwanted signal, together with the SX1280 receiver frequency. The signals were combined through a -6 dB passive splitter and a shielded box was employed to reduce the influence of local Wi-Fi traffic on the results.

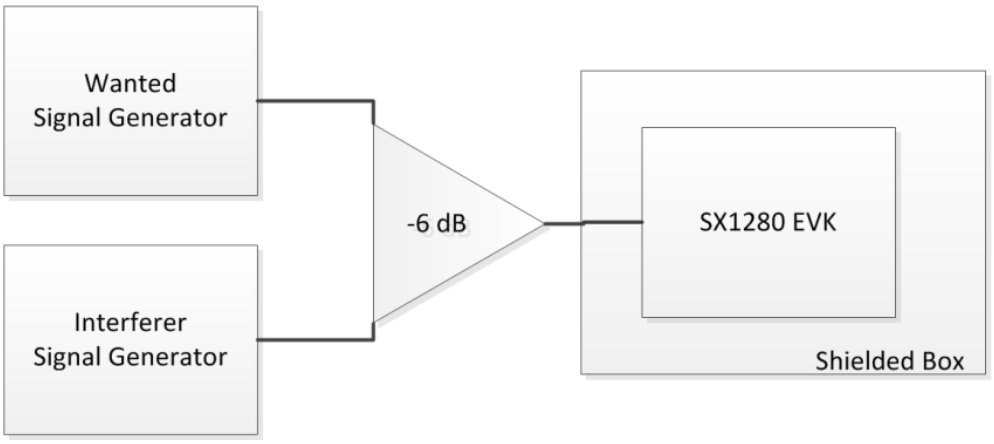

Figure 13: Simplified Block Diagram of the Experimental Setup

10 Co-Channel Interferer Test Results

Concentrating first on the co-channel testing results, here five modem configurations all using 20 byte payload, long interleaving and the wanted signal power is +3 dB above sensitivity unless otherwise stated. Immunity was tested to 10% Packet Error Rate (PER).

1) SF12 200 kHz
2) SF6 200 kHz
3) SF12 1.6 MHz
4) SF6 200 kHz (no long interleaving, 10 byte payload)
5) GFSK 1 Mbps

The results of the immunity testing in response to a continuous Wave (CW), Wi-Fi PBCC and Wi-Fi OFDM interferers is shown below. Figures are reported as the relative power difference between the wanted signal and the co-channel interferer power.

Table 1: Co-Channel Wi-Fi Immunity for Various SX1280 Modem Configurations

Setup	Modem	Data Rate	BW [kHz]	CW [dB]	PBCC [dB]	OFDM [dB]
1	LoRa®	SF12	200	22	47	61
2	LoRa®	SF6	200	6	19	33
3	LoRa®	SF12	1600	20	27	34
4	LoRa®	SF6	200	4	20	33
5	GFSK	1 Mbps	1200	-8	-8	-10

In the case of GFSK we see the anticipated performance. Here we rely on positive signal to noise ratio. The 1.2 MHz receiver bandwidth used for that data rate integrates much of the interfering signal power.

Due to the ability of the LoRa® modem to receive powers below the interferer power, even the continuous wave interferer rejection results in positive figures. i.e. the interferer is stronger than the wanted signal. In concert with the lower bandwidth that further reduces the strength of the interfering signal integrated in the receiver this results in 61 dB of co-channel rejection of interfering OFDM signals.

In summary, we confirm that the main interference mitigation techniques are:

- **Increasing Spreading Factor:** This permits reception below what ever interfering noise power is seen within the modulation bandwidth.
- **Reduction of the Bandwidth:** As mentioned earlier, reduction of the bandwidth reduces the interferer power integrated at the receiver input.

The equivalence of the results of setups 2 and 4 show that the use of long interleaving and the halving of the payload length have no discernible influence on the immunity exhibited in these tests.

11 In-Band Interferer Test Results

The generator configuration was varied slightly in this next test - to avail of a slightly different interfering Wi-Fi signal (here using an R&S SMBV 100 and optional SMBV-K54 to generate the interfering Wi-Fi signal).

Using this new test signal, we use the same setup as indicated in Figure 13. The modem configuration used was configuration 1) of the previous Section, namely SF12 200 kHz with a 20 byte payload. The Wi-Fi signal was then swept in frequency along a range of discrete measurement points illustrated by the points in the following plot (starting at 0 Hz and ending at 64 MHz frequency offset between wanted and interfering signal).

The results of this measurement are shown in the plot below. Here we see that at the center frequency of this new test signal there is an up-tick in the immunity compared with that of the previous test signal.

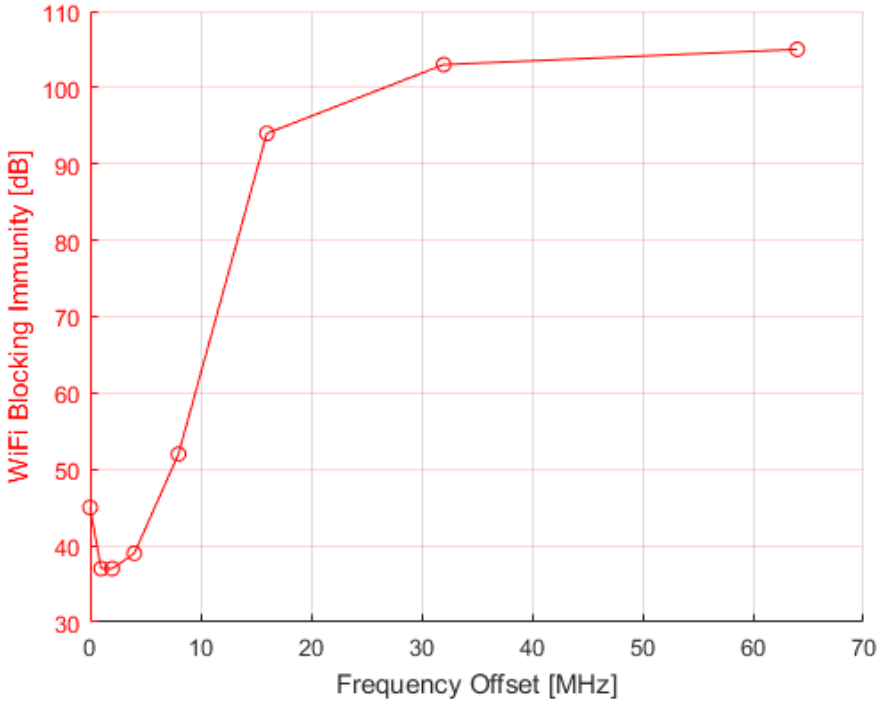

Figure 14: Wi-Fi Immunity of the SX1280 (SF12 200 kHz) as Function of Frequency Offset

This is explained if we compare the new Wi-Fi test signal with the immunity plot (next figure). Here we see that the actual measurement points (squares) overlap at the center with minima in the power spectrum of the interferer. (This is also visible upon close inspection of the 100 kHz PSD of Figure 10).

Were more measurements to be performed at a lower frequency separation, we would expect to see the underlying spectrum of the modulation become apparent.

Otherwise, at our existing measurement resolution, at greater offsets, the immunity rises steadily from 36 dB of in-band rejection i.e. the ability to receive the wanted signal in the presence of a proximate Wi-Fi signal 36 dB stronger. This increases to in excess of 90 dB at 16 MHz, up to over 100 dB at offsets above about 25 MHz.

This shows that adaptive interference avoidance mechanisms, to exploit unused portions of the 80 MHz wide 2.4 GHz ISM band are a suitable strategy for avoiding proximate in-band interference.

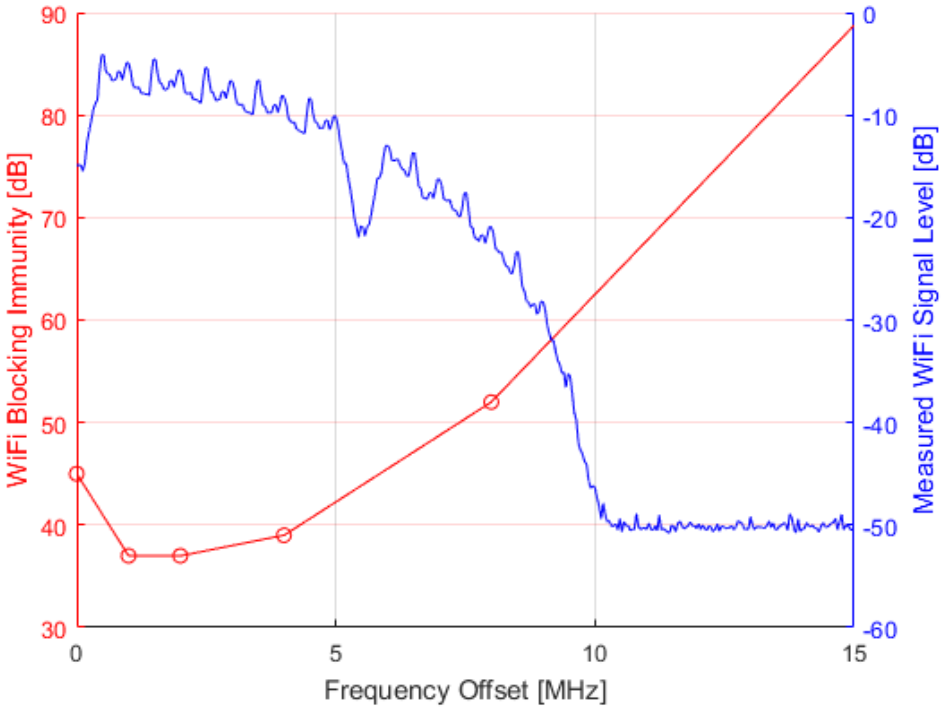

Figure 15: Wi-Fi Blocking Immunity and Measured Wi-Fi Signal Level vs Frequency Offset

The features seen in the shape of the Wi-Fi immunity curve of SX1280 are explained by the location of the measurement points and the corresponding modulated spectrum.

12 Conclusion

Strong in-band Wi-Fi interference immunity, in excess of 100 dB is possible using the LoRa® modulation of SX1280. Although preferable to avoid channels occupied by Wi-Fi, where this is not possible, the co-channel interference rejection has been shown to be a function of SF and bandwidth employed.

Reduction of the bandwidth and increasing the spreading factor (both of which reduce the LoRa® data rate) will improve Wi-Fi interference immunity. In the case of 802.11n OFDM modulation, the modem may be configured to give up to 61 dB of co-channel immunity.

13 References

[1] https://www.ipass.com/press-releases/the-global-public-wi-fi-network-grows-to-50-million-worldwide-wi-fi-hotspots/

[2] By Liebeskind (Own work) GFDL or CC BY via Wikimedia Commons

[3] M. Oularbi, A. Aissa-El-Bey, and S. Houcke, "Physical Layer IEEE 802.11 Channel Occupancy Rate Estimation," in ISIVC 2010: Proceedings of the Fifth International Symposium on I/V Communications over fixed and Mobile Networks, 2010.

Important Notice

Information relating to this product and the application or design described herein is believed to be reliable, however such information is provided as a guide only and Semtech assumes no liability for any errors in this document, or for the application or design described herein. Semtech reserves the right to make changes to the product or this document at any time without notice. Buyers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. Semtech warrants performance of its products to the specifications applicable at the time of sale, and all sales are made in accordance with Semtech's standard terms and conditions of sale.

SEMTECH PRODUCTS ARE NOT DESIGNED, INTENDED, AUTHORIZED OR WARRANTED TO BE SUITABLE FOR USE IN LIFE-SUPPORT APPLICATIONS, DEVICES OR SYSTEMS, OR IN NUCLEAR APPLICATIONS IN WHICH THE FAILURE COULD BE REASONABLY EXPECTED TO RESULT IN PERSONAL INJURY, LOSS OF LIFE OR SEVERE PROPERTY OR ENVIRONMENTAL DAMAGE. INCLUSION OF SEMTECH PRODUCTS IN SUCH APPLICATIONS IS UNDERSTOOD TO BE UNDERTAKEN SOLELY AT THE CUSTOMER'S OWN RISK. Should a customer purchase or use Semtech products for any such unauthorized application, the customer shall indemnify and hold Semtech and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs damages and attorney fees which could arise.

Contact Information

Semtech Corporation
Wireless & Sensing Products
200 Flynn Road, Camarillo, CA 93012
E-mail: sales@semtech.com
Phone: (805) 498-2111, Fax: (805) 498-3804
www.semtech.com