

---

# Implementation and Performance Evaluation of IEEE 802.15.4 LECIM DSSS PHY at 2.4 GHz

---

Felix Wunsch, Kristian Maier, Holger Jäkel, Friedrich K. Jondral

FELIX.WUNSCH@KIT.EDU

Communications Engineering Lab (CEL), Karlsruhe Institute of Technology (KIT), Germany

## Abstract

Low Power Wide Area Networks (LPWANs) are thought to provide low-cost coverage for massive numbers of devices. Due to the many business opportunities ahead, the market is currently highly fragmented with many competing waveforms. In order to establish a basis for the comparison of LPWAN waveforms, we present the first open-source, standards-compliant implementation of the IEEE 802.15.4 Low Energy Critical Infrastructure Monitoring (LECIM) Direct Sequence Spread Spectrum (DSSS) physical layer including the fragmentation sublayer in the GNU Radio framework. This Software Defined Radio-based testbed enabled us to conduct the first field trials evaluating the performance in the highly-congested 2.4 GHz band with different configurations at various receiver locations. Our results indicate that there is a considerable potential for LPWANs in the 2.4 GHz range, even in the presence of many uncontrolled Wi-Fi access points.

## 1. Introduction

For the coming years, a massive growth in the market for the Internet of Things (IoT) is expected. Among others, popular application examples comprise smart home, smart cities, industrial and agricultural monitoring, waste management, and many more. The necessary sensor networks, however, can not be served efficiently by existing traditional cellular or short-range services, which eventually gave rise to the Low Power Wide Area Network (LPWAN) paradigm. Typical LPWANs are star-topology networks with cell radii often beyond 10 km, serving thousands of low-complexity sensors that are strictly constrained in size and power consumption (Raza et al., 2017).

With so many potential business opportunities, the relatively young market for LPWAN applications is highly

competitive and being pushed by proprietary solutions (e.g., LoRa, SigFox, and Random Phase Multiple Access (RPMA)). Standards organizations such as the 3GPP and the IEEE, however, also have introduced their own waveforms. While the 3GPP defines enhanced Machine-Type Communication (eMTC), Narrowband IoT (NB-IoT), and Extended coverage GSM IoT (EC-GSM-IoT) for the usage in the licensed bands, the IEEE 802.15.4 standard (802, 2016) specifies Low Energy Critical Infrastructure Monitoring (LECIM) waveforms based on Direct Sequence Spread Spectrum (DSSS) or Frequency Shift Keying (FSK) modulation that are designed to work in the license-exempt spectrum.

Among the proposed solutions for the unlicensed bands, the IEEE 802.15.4 LECIM DSSS Physical Layer (PHY), which is also compliant to RPMA, is an interesting option because it allows the usage of the 2.4 GHz Industrial, Scientific and Medical (ISM) band. While the sub-GHz ISM or Short Range Devices (SRD) bands offer better propagation conditions, the 2.4 GHz band does not suffer from duty cycle restrictions and is globally available, possibly offering better economical scalability for the production of low-cost sensor modules.

Related works comprise simulative evaluations of the IEEE 802.15.4 LECIM PHY, dealing with the impact of self-interference and cross-technology interference robustness (Jin et al., 2012; Tada & Kato, 2013) or the MAC layer performance (Gebremedhin et al., 2015). Practical testbed implementations and measurements for sub-GHz frequencies were presented in (Xiong et al., 2014; Xu et al., 2016). Neither of them, however, seem to be publicly accessible. It also has to be noted that (Xu et al., 2016) changes the PHY layer modulation scheme to GFSK and therefore differs from the standard.

Against this background, our contributions comprise the following: To the best of the authors' knowledge, the first open-source implementation of a IEEE 802.15.4 LECIM DSSS PHY transceiver including the fragmentation sublayer that is real-time capable and standards-compliant is presented. The software utilizes the GNU Radio framework (gnu), Universal Software Radio Peripherals (USRPs) (ett), is licensed under the GNU General Pub-

Bytes: 0/2/4	0/1	16/24/32
Preamble	SFD	PHY payload

Figure 1. Frame format of the IEEE 802.15.4 LECIM DSSS PHY. Preamble and SFD together form the SHR.

lic License version 3 (GPLv3), and freely available online (grl). Furthermore, we are the first to report results from field trials in the 2.4 GHz ISM band. These were conducted in the urban area of Karlsruhe (Germany), where the performance with different configurations in exemplary receive scenarios was investigated. This comprises links of up to 3.8 km under Line-of-Sight (LOS) and Non-Line-of-Sight (NLOS) conditions. We also provide some insight on the impact of co-located IEEE 802.11 (Wi-Fi) networks.

The remainder of this paper is structured as follows: Section 2 gives a brief introduction to the IEEE 802.15.4 LECIM DSSS PHY and fragmentation layer. In Section 3, the transceiver implementation is described. Section 4 presents and discusses the results of our measurement campaign. Finally, we conclude the paper in Section 5.

## 2. IEEE 802.15.4 LECIM DSSS PHY

### 2.1. Frame Structure and Modulation

Every transmission frame consists of a Synchronization Header (SHR) that is divided into a preamble and a Start-of-Frame Delimiter (SFD) followed by the PHY payload as depicted in Fig. 1. To enable an efficient and low-complexity Forward Error Correction (FEC), a convolutional code with rate  $\frac{1}{2}$  and subsequent interleaving is applied to the payload. Differential encoding provides robustness against changes in the channel impulse response and allows the receiver to dispense with carrier phase estimation. The high processing gains required to close long-range links are achieved by spreading the binary-valued symbols ( $\pm 1$ ) by the spreading factor  $SF = 2^x, x \in [4, 15]$  using Gold codes. For additional protection between co-located networks, Orthogonal Variable Spreading Factor (OVSF) codes can be applied. The modulation schemes supported in the LECIM DSSS PHY are BPSK and OQPSK. Finally, pulse shaping is performed by a Root-Raised Cosine (RRC) filter with a roll-off factor of 1. A reference modulator block diagram is given in Fig. 2.

### 2.2. Fragmentation Sublayer

To support the transmission of data exceeding the maximum payload length of 32 bytes, a fragmentation sublayer is defined that controls the process of fragmentation and re-assembly of Medium Access Control (MAC) layer frames with a size of up to  $2^{10} - 1$  bytes. According to the stan-

dard, this sublayer shall be supported by all devices using the LECIM DSSS PHY.

During fragmentation, the MAC frames are split into fragments with a size that fits into a single PHY frame. The structure of a fragment frame differs from a "regular" frame in that it has an additional Fragment Header and a Fragment Integrity Check Sequence (FICS). The Fragment Header contains information marking it as a fragment frame, the Transaction Identifier (TID) assigned to the specific transmission, and the sequence number of the fragment, while the FICS represents a variable-length Cyclic Redundancy Check (CRC) to enable the receiver to discard corrupted frames.

The transmission of the fragments is initiated by sending a Fragment Sequence Context Description (FSCD) frame that provides information on the encryption (if enabled), the TID, the Frak policy, the FICS length, the overall payload length, and the addressing. The Frak (fragment acknowledgment) policy determines, how the transmitting side is notified of the successfully received fragments. From the different policies, we implemented the one indicated by the value "1" in the appropriate field that sends out Frak frames as soon as a certain time has elapsed since the successful reception of the last fragment. This basically corresponds to a "Selective Repeat" Automatic Repeat Request (ARQ) scheme.

## 3. Receiver Design

### 3.1. Channel Model

The receiver design assumes a single-tap multipath channel with Rician or Rayleigh fading, depending on if it is a LOS or NLOS environment, respectively. Regarding the channel coherence time, it is assumed that the channel is quasi-static over the duration of at least two symbols, which allows us to use the slow fading approximation due to the differential signaling. Additionally, we take the frequency offset  $f_o$  into account, because especially low-cost oscillators can exhibit considerable deviation from their nominal frequency. The received signal  $r(t)$ , matched-filtered and sampled at the sampling frequency  $f_s$ , can therefore be written as

$$r[k] = h \cdot \tilde{s}[k] e^{j2\pi k f_o / f_s} + \tilde{n}[k] \quad (1)$$

with the Rayleigh or Rice distributed channel coefficient  $h$  with unity variance  $\sigma_h^2 = 1$ , the matched-filtered transmit signal  $\tilde{s}[k]$  and the (correlated) Gaussian noise  $\tilde{n}[k] \sim \mathcal{CN}(0, \sigma^2)$ . As  $f_o$  can be expected to be small compared to the total bandwidth, the exponential term is not affected by the filter. Hence, the average Signal-to-Noise Ratio (SNR) of the sequence  $r[k]$  can be written as  $\text{SNR}_r = 1/\sigma^2$ .

We justify the choice of a flat fading model by considering

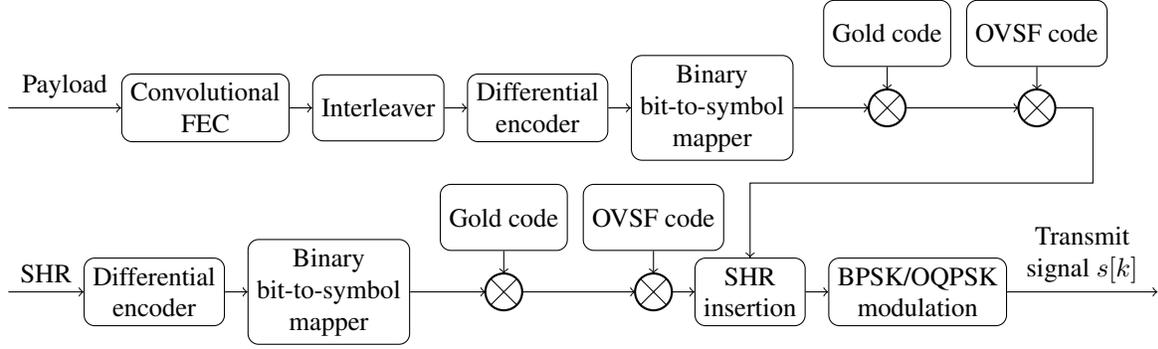


Figure 2. Block diagram of the IEEE 802.15.4 LECIM DSSS PHY modulator (according to (802, 2016))

the good auto-correlation properties of the spreading sequences, which lead to a strong attenuation of the delayed paths. Therefore, the performance is only degraded due to the lost energy in the multipath components.

If desired and feasible considering the often strict complexity constraints of the devices, a RAKE receiver design (Proakis, 2001) may be used to account for significant multipath components and improve the system performance.

### 3.2. Synchronization and Demodulation

In this section, we describe the basic idea of the demodulator. More detailed considerations on specific implementation aspects are presented in Section 3.3.

After matched filtering, the cross-correlation sequence  $\varphi[l]$  between the input signal and the spreading sequence, both oversampled by factor  $M$ , is calculated. To reduce the computational load imposed by the possibly high spreading factor SF, the well-known FFT-based fast correlation approach is adopted. In the next step, the differential symbol encoding is reversed. This yields

$$\varphi_{\text{dec}}[l] = \varphi[l] \cdot \varphi^*[l - M \cdot \text{SF}] \quad (2)$$

where  $M \cdot \text{SF}$  corresponds to the number of samples per (spread) symbol.

Based on the differentially-decoded correlator output, the binary-valued SHR sequence  $p[l]$  is searched for by considering every sample as the possible start of a frame. This second correlation can be written as

$$\psi[l] = \sum_{n=0}^{L_{\text{SHR}}-1} \varphi_{\text{dec}}[l + n \cdot M \cdot \text{SF}] \cdot p^*[n] \quad (3)$$

A frame start is detected whenever  $|\psi[l]| > \lambda$ . The threshold  $\lambda$  is defined as

$$\lambda = \underbrace{\sigma^2 \cdot \text{SF} \cdot \sqrt{L_{\text{SHR}}}}_{\text{noise floor of } |\psi[l]|} \cdot \gamma \quad (4)$$

with  $L_{\text{SHR}}$  denoting the length of the SHR in binary symbols or bits and  $\gamma$  controlling the minimum correlation magnitude required for a packet detection. While a high  $\gamma$  reduces the false alarm rate and therefore also the computational load in the following demodulation chain, such a choice might also lead to many missed packets and vice versa. The threshold is also adaptive because the noise power  $\sigma^2$  is continuously estimated by averaging the input power, which is a simplifying yet practical assumption, considering that the SNR before despreading is usually well below 0 dB. Furthermore, a frequency offset estimate is given by

$$\hat{f}_o = \frac{\angle \psi[l] \cdot f_s}{2\pi \cdot M \cdot \text{SF}}. \quad (5)$$

Once the position of the beginning of the frame is known, the payload data is demodulated in a similar fashion by first correcting the frequency offset, calculation of  $\varphi[l]$ ,  $\varphi_{\text{dec}}[l]$ , and downsampling to the symbol rate. The binary symbols are then de-interleaved and sent to the Viterbi convolutional decoder. The final CRC check is used to either discard the frame or pass it to the MAC layer or the fragmentation sub-layer, respectively.

### 3.3. Implementation Aspects

With an increasing spreading factor, even a relatively small  $f_o$  can lead to a severe degradation of the correlation sequence  $\varphi[l]$ . Considering the signal model in (1), the SNR of the correlation with perfect timing can be shown to be

$$\text{SNR}_{f_o} = \frac{1}{\text{SF} \cdot \sigma^2} \frac{\sin^2(\pi f_o / f_s \cdot \text{SF})}{\sin^2(\pi f_o / f_s)} \Big|_{f_o=0} \frac{\text{SF}}{\sigma^2}, \quad (6)$$

which is why we employ not only a single correlator, but a bank of correlators that processes frequency-shifted versions of  $r$  to be able to deal with higher values of  $f_o$ . This is also the approach taken by the inventors of RPMA (rpm).

At the output of the structure, the highest correlation value is selected, i.e., selection combining is performed. Consid-

ering that the maximum frequency offset that is unambiguously resolvable when using BPSK is  $|f_{\max}| = \frac{f_s}{2M \cdot \text{SF}}$ , the correlators should have a maximum spacing of  $2f_{\max}$ . It is important to note that  $|f_{\max}|$  reduces to about 15 Hz for the maximum spreading factor of 32768, therefore requiring a rather large number of correlators in order to be able to account for even small frequency offsets. The unambiguous frequency range and therefore also the correlator spacing doubles for OQPSK, which leads to a considerably reduced computational load at high spreading factors.

Evaluation of the intersection of the  $\text{SNR}_{f_o}$  curves of correlators spaced by  $2f_{\max}$  shows that the SNR loss factor  $\text{SNR}_{\text{loss}} = \frac{\text{SNR}_{f_o}}{\text{SNR}_{f_o=0}} \geq \frac{4}{\pi^2} \approx 0.41$  for any spreading factor. As exploiting the entire unambiguous region might degrade the performance unnecessarily, we use a slightly closer spacing that is given by the 3 dB "bandwidth" of the  $\text{SNR}_{\text{loss}}$  curve. This SNR loss, however, is only relevant for the frame detection. As soon as a frame start is detected,  $f_o$  can be estimated according to (5) and corrected for the following payload demodulation, which also mitigates the associated performance loss.

Another issue that is connected to high spreading factors and therefore long frame durations is the rate mismatch between transmitter and receiver, which leads to symbols being sampled farther from the maximum eye opening over time after the initial timing synchronization, and, in consequence, high frame error rates. To alleviate this, we implement a symbol-level Delay Locked Loop (DLL) that utilizes the early-late gate synchronization principle (Proakis, 2001) to adjust the sampling time during payload demodulation.

To enable a reliable demodulation without a DLL, we constrain the accumulated clock drift at the end of the frame to  $t_{\Delta} = \frac{M}{4f_s}$ , which corresponds to one quarter of the opening in the eye diagram. We can use this to derive a condition on the spreading factor for a given configuration, yielding

$$\text{SF} \leq \frac{k}{4\epsilon \cdot N_b} \quad (7)$$

with  $\epsilon$ ,  $N_b$ , and  $k$  representing the relative clock drift, the number of (channel-coded) bits per frame, and the bits per symbol, respectively. Considering our testbed devices and the configuration given in Table 2 ( $k = 2$ ,  $N_b = 288$ ,  $\epsilon = 2 \cdot 10^{-6}$ ), this condition is already violated for a spreading factor of 1024, which shows the importance of the DLL.

## 4. Measurement Campaign

In order to evaluate the performance of the IEEE 802.15.4 LECIM DSSS PHY in the 2.4 GHz ISM band, we conducted over-the-air frame error rate measurements in the urban area of Karlsruhe, Germany. The transmitter was set

up on a high building on the campus of KIT in the city centre, while the receivers were mostly on ground level. For each measurement 1000 frames filled with random payload data were sent periodically and without any overlap to avoid issues with Multiple Access Interference (MAI). The ratio of the number of successfully received frames to the total transmitted frames is referred to as the Frame Success Ratio (FSR). A frame is considered to be successfully received if the payload CRC check passes. The device configuration and receiver positioning are given in Table 1 and 2, respectively.

All measurements were carried out on two different frequencies, 2.45 GHz and 2.48 GHz, both of them being considered to be favorable choices, as they do not lie in the typically used Wi-Fi channels 1, 6, and 11. While 2.45 GHz is still quite close to the band edges of channels 6 and 11, transmissions on 2.48 GHz are expected to receive considerably less interference from transmissions on channel 11 due to the larger distance from its band edge.

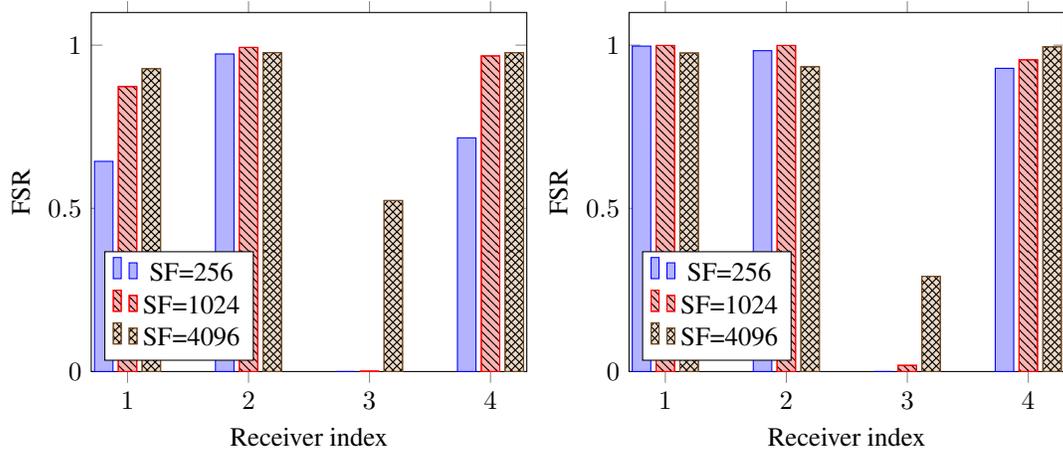
This assumption is confirmed in Fig. 3, where the FSR at receiver location 1 shows considerable frame loss for 2.45 GHz, while practically all frames could be received on 2.48 GHz. The interference of course also depends on the distance and the current activity of the IEEE 802.11 access points, which can be seen in the results for receiver location 2. Despite the severe shadowing and a similar Wi-Fi density, only negligible frame loss occurred.

Receiver location 3, an open, commercial area with the LOS blocked by some low houses and a small forest, shows the importance of the high spreading factors to overcome the effects of shadowing. Considering the low transmit power of only 5 dBm and the possible eight-fold increase of the spreading factor, we expect that a reliable communication is still possible in this situation. Interestingly, earlier measurements at the same location provided very good results (53% and 99% FSR at 2.48 GHz for a spreading factor of 256 and 1024, respectively), which we put down to the trees growing leaves in the meantime. This is an interesting aspect to consider, especially in the use case of animal tracking.

Similar to receiver location 1, receiver location 4 experienced some Wi-Fi-related degradation on 2.45 GHz for low spreading factors. Due to the direct LOS connection, however, the connection proved to be very stable, even for the lowest measured spreading factor of 256. The multi-story apartment building might also be an interesting scenario for Smart City applications, while the interference situation with many uncoordinated wireless networks is unpredictable and challenging. In this special case, over a dozen of different Wi-Fi networks with different bandwidths were located on practically every channel, even though a clustering on channels 1, 6, 11 was observable. The fact that our

Table 1. Description of the different receive scenarios.

Pos.	Distance	LOS	Environment	Co-located IEEE 802.11 access points
1	350 m	(Yes)	Densely-built campus, LOS blocked (single tree)	Many (exclusively channels 1, 6, 11)
2	450 m	No	Densely-built campus, LOS blocked (tall buildings)	Many (exclusively channels 1, 6, 11)
3	2100 m	No	Commercial area, LOS blocked (low houses, trees)	Few
4	3800 m	Yes	Multi-story apartment building, unobstructed LOS	Many (uncoordinated, mainly 1, 6, 11)



(a) Frame Success Ratios for a center frequency of 2.45 GHz. (b) Frame Success Ratios for a center frequency of 2.48 GHz.

Figure 3. Frame Success Ratios for different receive scenarios, spreading factors, and center frequencies.

Table 2. IEEE 802.15.4 LECIM DSSS PHY configuration for outdoor measurements.

Parameter	Value
Center frequencies	2.4 GHz to 2.48 GHz
Bandwidth	1 MHz (excluding roll-off)
Gold code spreading factors	{256, 1024, 4096}
OVSF code spreading factor	1 (disabled)
Preamble length	4 bytes
SFD	Disabled
Payload length	16 bytes
CRC length	4 bytes
Modulation type	OQPSK
Frame durations	{38.86, 147.5, 589.2}ms
Radio front end	USRP B210
Transmit power	5 dBm
Oscillator accuracy	2 ppm
Antenna type	Omnidirectional
Sampling rate $f_s$	4 MS/s
Oversampling factor $M$	4

experiment was still successful is probably due to the fact that all of these networks are deployed indoors, which is in contrast to receiver locations 1 and 2, where the access points are supposed to provide coverage for the entire campus.

To provide some more insight on the impact of Wi-Fi interference, we also conducted a number of measurements at receiver location 4 where we varied the center frequency in the range of the entire ISM band. The results shown in Fig. 4 clearly show a high number of corrupted frames around the center frequencies of channels 1, 6, and 11, while the link proved to be very reliable for the channels in-between, even though these channels were not entirely free of interference.

## 5. Conclusions

In this paper, we presented the design of our Software Defined Radio-based implementation of the IEEE 802.15.4 LECIM DSSS PHY and discussed solutions to important design challenges that arise due to the very large spreading factors. Our code also includes the fragmentation sub-layer and is fully standards-compliant, while being able to run on off-the-shelf hardware. With publishing our code

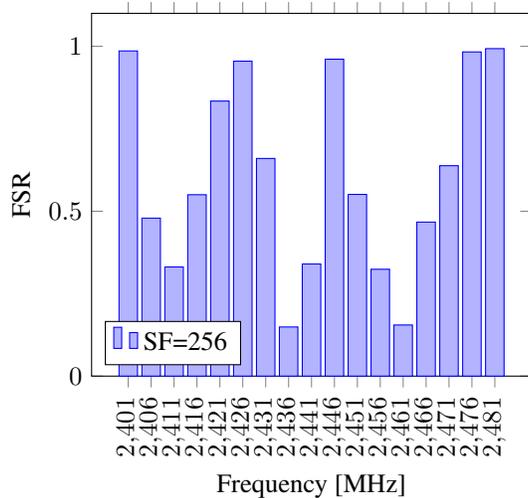


Figure 4. Impact of IEEE 802.11 interference at receiver position 4 (suburban apartment building) with many co-located IEEE 802.11 networks on the FSR. Strong degradation occurred in the vicinity of the typically used Wi-Fi channels 1, 6, and 11.

on GitHub (grl), we want to encourage reuse and help to establish a basis for realistic comparisons, e.g. in future field trials, between the many competing LPWAN waveforms. As identified in (Raza et al., 2017), interoperability between different LPWAN technologies is also likely to become a challenge in the future, which represents another aspect that is difficult to tackle without freely available implementations and testbeds.

Using our testbed, we also provide the first results for the practical performance of the IEEE 802.15.4 LECIM DSSS PHY in the 2.4 GHz ISM band in the urban area of Karlsruhe, Germany. Frame Success Ratios were measured for different carrier frequencies, spreading factors and receiver locations. The field trials indicate that, even though Wi-Fi interference can cause considerable degradation and the free space loss in the chosen band is generally higher than for sub-GHz frequencies, reliable communication is possible even for links over multiple kilometers. While careful frequency planning of course helps, this could also be confirmed for challenging scenarios with many uncoordinated Wi-Fi networks in the vicinity.

Interesting topics for future research comprise the further investigation of cross-technology interference, interference mitigation strategies as well as a quantitative comparison with competing LPWAN waveforms.

## References

Ettus Research website. <https://www.ettus.com/>. Accessed: 2017-04-11.

GNU Radio website. <http://www.gnuradio.org>. Accessed: 2017-04-11.

GitHub repository for gr-lpwan. <https://github.com/kitt-ctrl/gr-lpwan>. Accessed: 2017-04-11.

RPMA white paper. <https://www.ingenu.com/portfolio/how-rpma-works-white-paper/>. Accessed: 2017-04-11.

IEEE Standard for Low-Rate Wireless Networks. *IEEE Std 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011)*, pp. 1–709, April 2016. doi: 10.1109/IEEESTD.2016.7460875.

Gebremedhin, B. G., Haapola, J., and Iinatti, J. Performance Evaluation of IEEE 802.15.4k Priority Channel Access with DSSS PHY. In *Proceedings of European Wireless 2015; 21th European Wireless Conference*, pp. 1–6, May 2015.

Jin, Y., Ameen, M. Al, Liu, Hongwu, and Kwak, K. S. Interference mitigation study for low energy critical infrastructure monitoring applications. In *2012 International Symposium on Communications and Information Technologies (ISCIT)*, pp. 962–966, Oct 2012. doi: 10.1109/ISCIT.2012.6381044.

Proakis, J.G. *Digital Communications*. McGraw-Hill, 2001. ISBN 9780072321111.

Raza, U., Kulkarni, P., and Sooriyabandara, M. Low Power Wide Area Networks: An Overview. *IEEE Communications Surveys Tutorials*, PP(99):1–1, 2017. ISSN 1553-877X. doi: 10.1109/COMST.2017.2652320.

Tada, Y. and Kato, S. A star-topology sensor network system for agriculture using 802.15.4k standard. In *2013 IEEE 24th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC Workshops)*, pp. 76–80, Sept 2013. doi: 10.1109/PIMRCW.2013.6707840.

Xiong, X., Wu, T., Long, H., and Zheng, K. Implementation and performance evaluation of LECIM for 5G M2M applications with SDR. In *2014 IEEE Globecom Workshops (GC Wkshps)*, pp. 612–617, Dec 2014. doi: 10.1109/GLOCOMW.2014.7063500.

Xu, R., Lei, L., Xiong, X., Zheng, K., and Shen, H. A Software Defined Radio Based IEEE 802.15.4k Testbed for M2M Applications. In *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*, pp. 1–5, Sept 2016. doi: 10.1109/VTCFall.2016.7880880.