



University of  
Zurich<sup>UZH</sup>

# Cloud Radio Access Network in LoRa

*Silas Weber*  
*Zurich, Switzerland*  
*Student ID: 14-704-845*

Supervisor: Eryk Schiller  
Date of Submission: February 3, 2019



# Abstract

Das ist die Kurzfassung...



# Acknowledgments

Optional



# Contents

<b>Abstract</b>	<b>i</b>
<b>Acknowledgments</b>	<b>iii</b>
<b>1 Introduction and Motivation</b>	<b>1</b>
1.1 Description of Work . . . . .	2
1.2 Thesis Outline . . . . .	3
<b>2 LoRa and LoRaWAN</b>	<b>5</b>
2.1 LoRaWAN architecture . . . . .	6
2.2 End-node Classes . . . . .	7
2.3 LoRa signal (uplink) . . . . .	8
2.3.1 Chirps . . . . .	8
2.3.2 Symbol and Spreading Factor . . . . .	9
2.3.3 Coding Rate . . . . .	9
2.3.4 Spreading Factor & Time on Air . . . . .	10
2.3.5 Packet structure . . . . .	11
<b>3 LoRa in SDRs</b>	<b>13</b>
3.1 Existing implementations . . . . .	13
3.2 LoRa decoding . . . . .	15

<b>4</b>	<b>C-RAN in cellular networks</b>	<b>17</b>
4.1	D-RAN . . . . .	17
4.2	Moving to C-RAN . . . . .	17
4.3	Virtual RAN . . . . .	18
<b>5</b>	<b>C-RAN for LoRa</b>	<b>21</b>
5.1	Goal . . . . .	21
5.2	Hardware . . . . .	21
5.3	Sending Uplink Signals . . . . .	22
5.4	RRH and BBU . . . . .	22
5.5	Study Subjects . . . . .	22
5.5.1	Network Utilization . . . . .	22
5.5.2	Impact of Delay . . . . .	22
5.5.3	Network Delay . . . . .	23
5.5.4	Processing Delay . . . . .	23
5.6	Architecture . . . . .	23
5.6.1	Overview . . . . .	23
5.6.2	Containerization and Orchestration . . . . .	24
5.6.3	RRH and BBU . . . . .	24
5.7	Implementation . . . . .	24
5.7.1	RRH . . . . .	25
5.7.2	BBU . . . . .	26
5.7.3	Communication Protocol Arduino . . . . .	27
5.8	Results . . . . .	29
5.8.1	Network Utilization . . . . .	29
5.8.2	Cost . . . . .	31
5.8.3	Delays . . . . .	33
<b>6</b>	<b>LoRa Tools</b>	<b>35</b>



<i>CONTENTS</i>	vii
<b>7 Future work</b>	<b>37</b>
7.1 Limitations . . . . .	37
7.2 Improvements . . . . .	37
<b>8 Summary and Conclusions</b>	<b>39</b>
<b>Abbreviations</b>	<b>45</b>
<b>Glossary</b>	<b>47</b>
<b>List of Figures</b>	<b>47</b>
<b>List of Tables</b>	<b>49</b>
<b>A Installation Guidelines</b>	<b>53</b>
<b>B Contents of the CD</b>	<b>55</b>
<b>C README.md</b>	<b>57</b>
C.1 C-RAN for LoRa . . . . .	57
C.1.1 Run with Docker . . . . .	57
C.1.2 RRH . . . . .	58
C.1.3 BBU . . . . .	61
C.1.4 LimeSDR . . . . .	66
C.1.5 Help . . . . .	66
C.2 Arduino . . . . .	66
C.2.1 Manual installation Ubuntu . . . . .	66
C.3 Tools . . . . .	67



# Chapter 1

## Introduction and Motivation

Scalability and improvement of Internet of Things (IoT) devices and protocols are important research questions. Low Power Wide Area Networks (LPWANs) technology offers long-range communication with low power requirements. Battery powered LPWAN devices can run for years. For instance, a node sending 100B once a day lasts for 17 years [1]. LoRa (short for Long Range) is a spread spectrum modulation technique, a wireless radio frequency technology for long range and low power platforms and has become the de facto technology for IoT networks worldwide [2]. LoRaWAN is the open standard backed by the LoRa Alliance. It is a communication protocol and Medium Access Control (MAC) protocol built on the physical LoRa layer. LoRaWAN is designed from the bottom up to optimize LPWANs for battery lifetime, capacity, range, and cost [3]. There are 142 countries with LoRaWAN deployments, 121 network operators, and 76 LoRa Alliance member operators. Swisscom, Amazon, IBM, CISCO are merely a few of the notables LoRa Alliance members [4]. TTN (The Things Network), also a LoRa Alliance member, provides a worldwide LoRaWAN network for and from the community. Anyone with a LoRa gateway can register their gateway on TTN, thereby extending the networks reach. At the time of writing, TTN has 95'208 members, 9'786 gateways, and is present in 147 countries [5]. As LoRaWAN operates in the unlicensed ISM (Industrial, Scientific and Medical) radio bands. Therefore no government license is required to operate LoRa devices and gateways. This allows hobbyist, enthusiasts, and developers to quickly get started and open networks such as TTN to grow rapidly.

In a typical LoRaWAN use case, an IoT device such as a sensor sends data out over the air. Then a LoRa gateway picks the signal up, decodes it, and forwards it over the Internet to the network server which then can send the packet to the application server. If needed, a response message can be scheduled on the network server who then chooses the best gateway to send the response back to the IoT device. LoRa gateways carry the full implementation of the LoRa PHY (the physical layer), the LoRaWAN protocol, as well as the packet forwarder. This architecture of the LoRa gateway can be separated and technological stack on the gateway can be reduced by running the signal processing functions not on the gateway itself but in a cloud environment. Such a Cloud Radio Access Network (CRAN) has been previously shown to be beneficial in the 3rd Generation Partnership Project (3GPP) Long Term Evolution (LTE) [6]. The gateway then is left with only minimal functionality it has to support. As the decoding does not take place on the gateway

itself, it does not need to have any LoRa specific hardware e.g the SX1276 transceiver chip found on LoRa devices and gateways. Rather, the gateway is equipped with an antenna, an amplifier as well as digital to analog (DAC) and analog to digital (ADC) converters. On the upstream, the gateway receives LoRa radio signals which it converts into Inphase and Quadrature (I/Q) sample stream with the ADC and simply forwards them to the cloud signal processing unit via the internet. On the downstream the cloud unit streams a LoRa signal as I/Q samples to the gateway which converts it with the DAC to an analog signal and propagates it out over the air. Signals are encoded and decoded on the cloud unit, the Radio Cloud Center (RCC). There are many advantages in such a setup but they come at a cost. First advantage is that the gateway can be kept at a much simpler design resulting in significant manufacturing cost reduction. Also, modifications to the LoRa PHY or LoRaWAN are easier to introduce as the physical layer is implemented in software. Gateways that are once deployed do not need to be physically replaced in case of an upgrade as they are agnostic to the underlying protocol and just convert and transceive (transmit and receive) I/Q samples. Updates to the protocol can be realized with just updating the software implementation. A Low Power Network (LPN) provider saves cost by not having to drive out to the deployed gateways throughout the country to upgrade their versions. The disadvantage is the high throughput of the I/Q samples stream between the gateway and the RCC. Streaming the I/Q samples between gateway and RCC has significantly higher bandwidth requirements than just demodulating the signal on the gateway and forwarding the decoded LoRa packet as it is done in the non cloudified setup. Cloudifying the LoRa gateways also brings the advantages of setting the base for Software Defined Networking (SDN) and Network Function Virtualization (NFV) by centralizing the resources in the RCC that were before distributed on the individual gateways. Goal of this work is setting up a CRAN architecture for LoRa by simplifying the gateways as described above and moving the signal processing out of the gateway into a cloud ready environment i.e., Docker.

## 1.1 Description of Work

This work first gives a general introduction to LoRa, LoRaWAN and its applications, then dives into more details regarding the LoRa physical layer. Then it gives an overview over existing software implementations of the LoRa PHY. There are two main contributions. First, this work implements a CRAN for LoRa, gives an architectural overview as well as the implementation details. It evaluates the architectural and network related requirements. We developed a simple protocol in raw LoRa, meaning not compliant with the LoRaWAN standard, where a hardware IoT device has a queue of packets to transmit then, depending on whether it requires an acknowledgment, waits for a few seconds for a response or just transmit the next packet in the queue in an interval. If the packet required to be acknowledged but no acknowledgment is received, the same packet will put as first item in the queue. We use this protocol to analyze our CRAN for LoRa architecture. Second, as the LoRa PHY is closed source, there is no official documentation on how the LoRa PHY is implemented. The existing implementations are all reverse engineering attempts with various degree of success. They all focused first on decoding LoRa signals transmitted by a real LoRa hardware. For the CRAN to work, not only is it necessary

to decode signals but also the encoding of downstream LoRa gateway signals is required. To achieve this we developed a tool that allows the generation of downstream signals in software.

## **1.2 Thesis Outline**



## Chapter 2

# LoRa and LoRaWAN

LoRa is a modulation technique derived from chirp spread spectrum technology[2]. Originally developed by Cycleo, a french company, LoRa has been acquired by Semtech [7]. LoRa signals spread over multiple frequencies using the whole available bandwidth. This makes the signal more resilient against noise on a disrupting frequency. As LoRa signal are sent over the unlicensed ISM bands, this resilience is an important factor. While LoRa is the modulation technique on the physical layer, LoRaWAN on the other hand is an open communication protocol backed by the Lora Alliance. LoRaWAN specifies packet format, duty cycles, key exchanges and many more things needed for an efficient and cooperative LoRa network. A LoRa network is and LPWAN where battery powered devices can stay operating up to 17 years, making LoRa a popular choice for IoT devices as shown in the example given in the introduction in chapter 1. The TTN network for example is used for cattle tracking, smart irrigation as well as smart parking applications [5].



Figure 2.1: LoRa vs other wireless technology[8]

Figure 2.1 shows LoRa compared two other wireless technologies, Wi-Fi and cellular. Both Wi-Fi and cellular are high in bandwidth with cellular having a longer range than Wi-Fi.

They both have a much higher power consumption compared to LoRa. LoRa has lower bandwidth but a high range. In a experiment during a TTN conference LoRa signals from a low orbit satellite were received [9]. On the other hand, as LoRa is designed for long range and low power, only few bytes are transmitted per day while Wi-Fi and cellular are capable of video streaming. In urban areas LoRa has a range of 2-5 km and 15 km in suburban areas [7].

LoRaWAN is not the same all around the world. There are regional parameters that come into play, one is for example the frequency band. In Europe LoRaWAN operates on the 863-870MHz and 433MHz ISM band and in North America the 902-928MHz ISM band. Also channel bandwidth and maximum transmission settings are regulated by the government and thus are not the same for all regions [10].

## 2.1 LoRaWAN architecture

A LoRaWAN network architecture is a star-of-stars topology. The gateways relay the messages between the end-devices and a central network server. Gateways are connected to the network server via IP connections, converting the RF packets to IP packets and vice versa [11]. Network nodes are not associated with a specific gateway, rather messages sent by a node can be received by multiple gateways. Each gateway will then forward the the message to the network server who does the complex things such as filtering redundant packages, security checks, forwarding the messages to the right application server etc. [3]. As network communication is bidirectional, the network server is also responsible for scheduling responses to the end-nodes. There are different classes of end-nodes which will be described in the next section.



Figure 2.2: LoRaWAN network architecture [3]

As depicted in Figure 2.2, the packets sent by end-devices (on the far left) such as alarms,



tracking devices and monitoring devices, can be received by multiple gateways. As the end-nodes are not linked to a particular gateway, they can be moved freely which is an important requirement for assets tracking.

The Figure also shows how security is built into LoRaWAN. The payload is end-to-end encrypted from the end-nodes to the applications server. A unique 128-bit network session key is shared between the end-device and the network server and another 128-bit application session key is shared end-to-end at the application level [11]. With those measures LoRaWAN prevents eavesdropping. Spoofing is prevented by a MIC (Message Integrity Code) in the MAC payload, and replay attacks are prevented by utilizing frame counters [12].

## 2.2 End-node Classes

There are three classes of end-devices. The following description is adapted from the LoRa Alliance guide [11, 2]:

- Class A, Lowest power, bi-directional end-devices:

This is the default class, supported by all LoRaWAN devices. It is always the end-node that initiates the communication. After an uplink two downlink windows open for the end-device to receive a response, enabling bi-directional communication. Either the first is used, or the second, but not both receive windows. The end-device can rest in low-power sleep mode, wake up when it needs to send a packet, receive a response in the downlink window, then go back to sleep. This is an ALOHA-type of protocol. Class A devices have the lowest power consumption. Downlinks from the server have to wait for an uplink from end-device and cannot be initiated directly.

- Class B, Bi-directional end-devices with deterministic downlink latency:

Additionally to Class A receive windows, a Class B device opens extra receive windows at scheduled times. This is achieved by time-synchronized beacons from the gateway to the end-device to notify the end-device to open a receive window.

- Class C, Lowest latency, bi-directional end-devices:

Devices of this class have always open receive windows, except for when they are themselves transmitting. A downlink transmission can be initiated by the network server at any time (assuming the device is not currently transmitting) resulting in no latency. Class C devices however use the most energy. They are more suitable for plugged in devices rather than battery powered devices.

## 2.3 LoRa signal (uplink)

### 2.3.1 Chirps

A LoRa signal is a series of so called chirps as LoRa is derived from the Chirp Spread Spectrum modulation (CSS) technique. There are up-chirps and down-chirps. In CSS chirps are deliberately spread across the available bandwidth. Up-chirps go from low frequency to high frequency and down-chirps go from high frequency to low frequency. In Europe the LoRaWAN bandwidth for is 125 kHz. Assuming a center frequency of 868.5 MHz, which is in the european ISM band, a full up-chirp, so called sweep, would go from 868.4375 MHz to 868.5625 MHz.

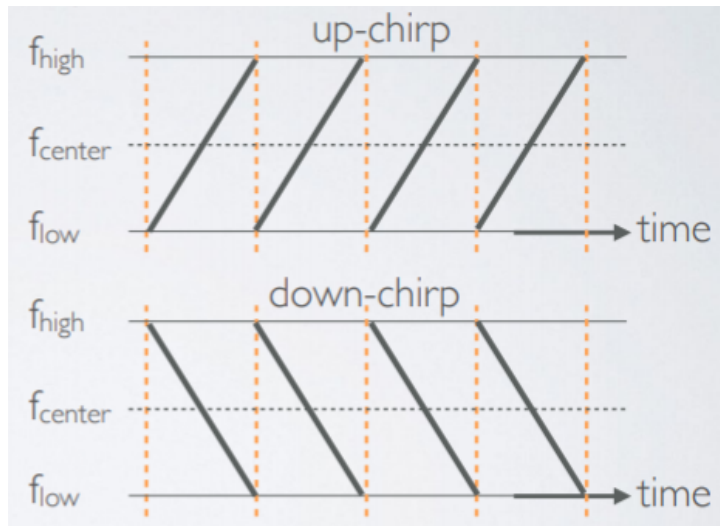


Figure 2.3: Up- and down chirps [13]

Figure 2.3 shows the linear frequency increase resp. decrease over time over the full bandwidth for up-chirps and down-chirps. Data is encoded by frequency jumps in the chirps.

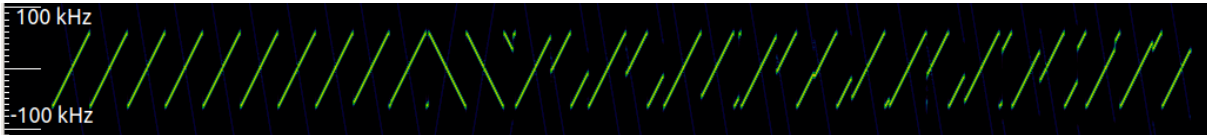


Figure 2.4: Own recording of uplink transmission by arduino equipped with a LoRa shield

The LoRa signal shown in 2.4 carries the message "Goodbye !". This message was sent with a spreading factor (SF) of 9 and coding rate of 4/5. The terms spreading factor and coding rate will be discussed later on.

As one can see, a typical LoRa signal start with a so called preamble, which are the 10 up-chirps at the beginning. Those are followed by two down-chirps, which signify the end of the preamble and the start of the actual payload. In this payload is a header, the actual encoded message followed by a Cyclic Redundancy Check (CRC). The CRC is used for error correction.

### 2.3.2 Symbol and Spreading Factor

A LoRa signal holds various symbols. A symbol encodes one or more bits of data. The spreading factor determines the number of encoded bits in a symbol. In the shown recording one symbol holds 9 bits of data as the spreading factor of that signal was set to 9. It follows that a symbol has  $2^{SF}$  values. Those values range from 0 to 511 in case of SF 9. A sweep signal of SF 9 thus has 512 chips (no to be confused with chirps) [14]. The chips go linearly from low to high and then wrap around once the maximum frequency is reached.

In Figure 2.5 a fictional symbol with SF 7 is shown. This particular arrangement of chips highlighted in orange would denote the symbol "1011111". Those 7 bits correspond to the decimal value 95.

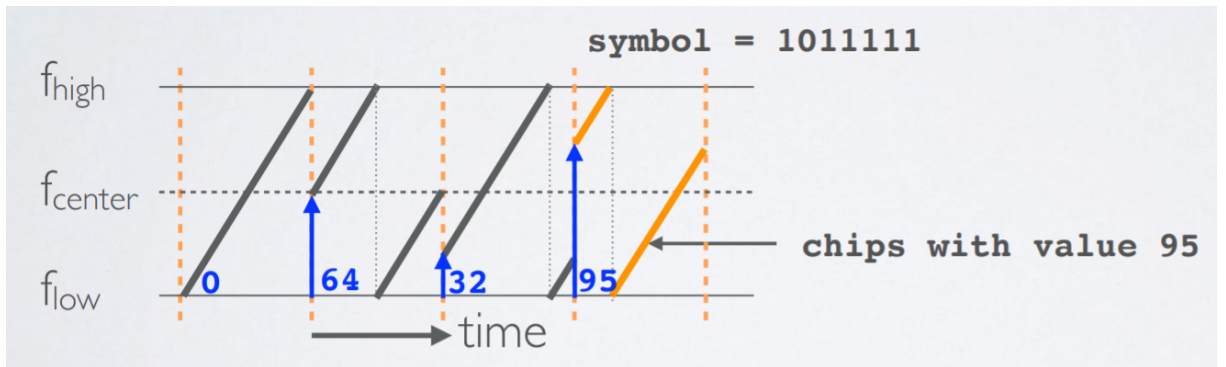


Figure 2.5: Chips and symbols value [14]

In Figure 2.6, a real world example is shown. The same LoRa signal as in Figure 2.4 with SF 9 with the message "Goodbye !" run through modified version of the LoRa decoder by Robyns et al. [15] and then through a python script where we match the samples to the symbols and their values. The last symbols encodes the hex value 142 which corresponds to these 9 bits "101000010". In a SF 9 signal each symbol encodes 9 bits.

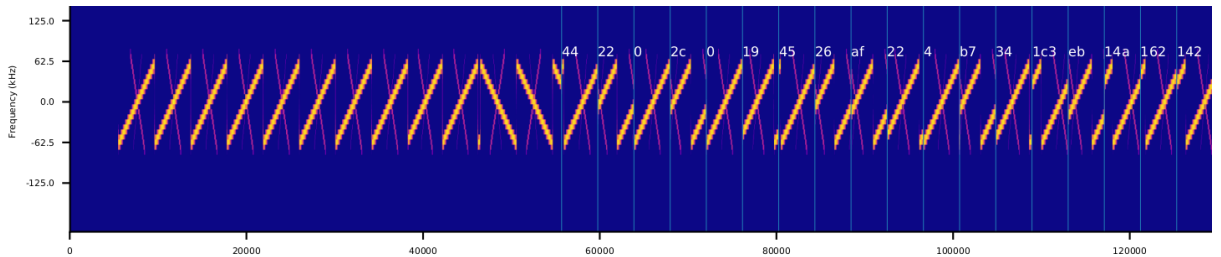


Figure 2.6: Running the signal through our toolchain, matching symbols with samples

### 2.3.3 Coding Rate

LoRa signals are encoded with a coding rate (CR). The CR denotes the proportion of how many bits carry actual information. The bits that do not carry information are used

for Forward Error Correction. The formula for coding rate is  $CR = 4/(4 + CR)$  where  $CR \in \{1, 2, 3, 4\}$ . A CR of 1 is thus the proportion of 4/5 of actual information over bits used for error correction [16, 17]. With FEC, corrupted bits e.g. due to interference can be corrected. With CR of 4, corresponds to  $4/8 = 1/2$ , half the transmitted bits carry information, the other half is for FEC. The higher the CR (from 1-4) the more bits can get corrupted and corrected by FEC. On the other hand, the higher the CR the more bits need to be transmitted which drains the battery more.

### 2.3.4 Spreading Factor & Time on Air

The longer the packet, the longer the transmission time. LoRa packets can be shortened by sending packets with implicit header mode where the no header is sent and the settings that would have been specified in the header have to be predefined manually on the end device.

Assuming constant packet size and same bandwidth, varying the spreading factor increases resp. decreases the time on air. The higher the SF, the longer the time on air. Higher SF means longer range. The spreading factor goes from 7 to 12. SF 7 has the shortest range, SF 12 the longest. The spreading factor essentially sets the duration of a chirp, a full sweep [18].

The symbol time is defined in the LoRa Design guide by  $T_{sym} = \frac{2^{SF}}{BW}$  [16]. It follows as stated above, that the higher the SF the longer the symbol duration. Also, the higher the bandwidth (BW) the shorter the symbol duration. In Europe the BW is 125 kHz, while in North America a BW of 500 kHz is allowed. It also follows that with an increase in SF by 1 the symbol duration is doubled. The bit rate  $R_b$  is then defined by  $R_b = SF * \frac{4*CR}{2^{SF}}$

with CR being the coding rate for the error correction scheme [19]. It follows from the formula that the higher the coding rate the lower the bit rate as with a higher CR more redundancy is added for the error correction scheme. Highest data rate for  $BW = 125 \text{ kHz}$  and  $CR = 1$  is achieved with SF 7 resulting in a data rate of 5.5 kbits/s and the lowest data rate is achieved with SF 12 resulting in a data rate 0.29 kbits/s.

The spreading factors are orthogonal to each other, meaning signals on different spreading factors do not interfere with each other. This is Code Division Multiple Access (CDMA) where a shared medium i.e. the bandwidth is optimized for multiple access.

To optimize network capacity LoRaWAN employs a method called Adaptive Data Rate (ADR). With ADR the network server signals the end-device which spreading factor to use according to some measurements including the signal to noise ratio. Assuming there are multiple devices near a gateway that transmit with SF 12. This occupies the bandwidth for device that are farther away and actually need SF 12. The network server detects that the nearby devices do not need a spreading factor of 12 and signal them to use a lower SF such as SF 7 or SF 8. The ADR setting has to be enabled on the end-devices and can be disabled.

### 2.3.5 Packet structure

The base form of a LoRa packet starts with the preamble, followed by the optional header with a header CRC, followed by the payload and finally the payload CRC. The number of payload symbols is calculated by the following formula [16]:

$$payloadSymbNb = 8 + \max(\text{ceil}(\frac{8PL-4SF+28+16-20H}{4(SF-2DE)}) * (CR + 4), 0)$$

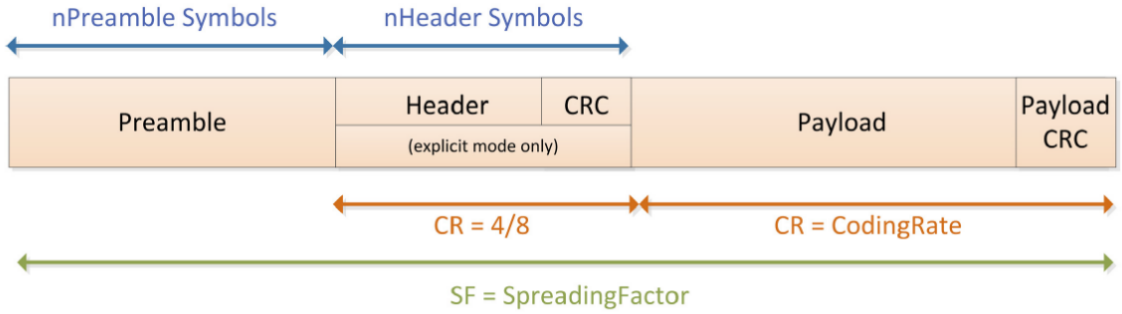


Figure 2.7: LoRa packet structure [16]

With:

1. PL being the number of payload bytes
2. SF being the spreading factor
3.  $H = 0$  if header is enabled and  $H = 1$  if no header
4.  $DE = 0$  if low data rate optimization is enabled and  $DE = 1$  if disabled
5. CR being the coding rate

As Figure 2.7 shows, the header is always encoded with the highest coding rate,  $CR = 4$ . This is because the header contains crucial information such as the packet length.

Figure 2.8 and Figure 2.9 show the structure of an uplink resp. a downlink packet. There is no CRC in downlink packets. PHDR stands for PHY header. Those are "raw" LoRa packets. LoRaWAN packets have additional fields such as MAC header (MHDR) and frame header (FHDR). Those are all in PHY payload of the "raw LoRa" packet as Figure 2.10 shows.

*Uplink PHY:*



Figure 2: Uplink PHY structure

Figure 2.8: LoRa uplink packet structure [20]

*Downlink PHY:*



Figure 3: Downlink PHY structure

Figure 2.9: LoRa downlink packet structure [20]

*Radio PHY layer:*

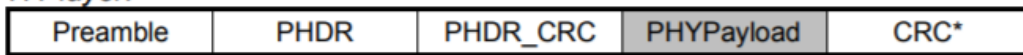
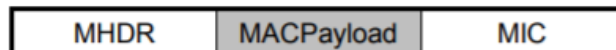
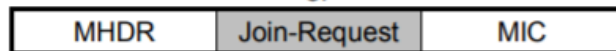


Figure 5: Radio PHY structure (CRC\* is only available on uplink messages)

*PHYPayload:*



or



or

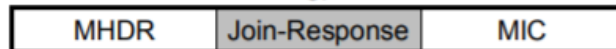


Figure 6: PHY payload structure

*MACPayload:*



Figure 7: MAC payload structure

*FHDR:*

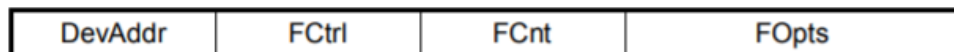


Figure 8: Frame header structure

Figure 2.10: LoRaWAN packet [20]

# Chapter 3

## LoRa in SDRs

Software-defined radios (SDR) implement components that are usually implemented in hardware. The most popular signal processing frameworks is GNU Radio. For LoRa we were looking for an existing implementation that demodulates, and also modulates LoRa signals.

### 3.1 Existing implementations

There are three existing implementations we looked at:

- Josh Blum's LoRa Mod -and Demodulator for LoRa in the Pothos framework <https://myriadrf.org/news/lora-modem-limesdr/>
- Matt Knight's GNU Radio Module <https://github.com/BastilleResearch/gr-lora>
- Robyns et al. LoRa Module for GNU Radio <https://github.com/rpp0/gr-lora>

We tried Blum's implementation in the Pothos first. The Pothos project is an open source data-flow framework supporting SoapySDR, a general framework for supporting SDR devices [21]. Unfortunately the LoRa modem demo application did not work for at all. After spending a few unsuccessful days trying to get to the issue we moved to Knight's application.

Matt Knight held a great talk on reverse engineering LoRa at the GNU Radio conference 2016 <https://www.youtube.com/watch?v=-YNMRZC6v1s>. GNU Radio, as Pothos, is a framework for signal processing.

From the GNU Radio website:

GNU Radio is a free & open-source software development toolkit that provides signal processing blocks to implement software radios. It can be used with

readily-available low-cost external RF hardware to create software-defined radios, or without hardware in a simulation-like environment. It is widely used in research, industry, academia, government, and hobbyist environments to support both wireless communications research and real-world radio systems. [22]

GNU Radio already comes with a wide set of blocks. Extensions are called Out Of Tree modules (OOT) as they are not in the standard tree of blocks. Knight's implementation did not work well for us. If we got an output from the decoder, it was not what was expected. A reason could be that in his examples the signal source block is an USRP SDR while we had a LimeSDR mini at our disposal. Simply switching the source blocks probably is not enough. We did not investigate the compatability between LimeSDR mini and and USRP further but moved on to the final implementation. His blocks are in modular fashion. The demodulator and decoder are separate blocks. Channelization and fine tuning must be done explicitly before passing the stream to the demodulator block.

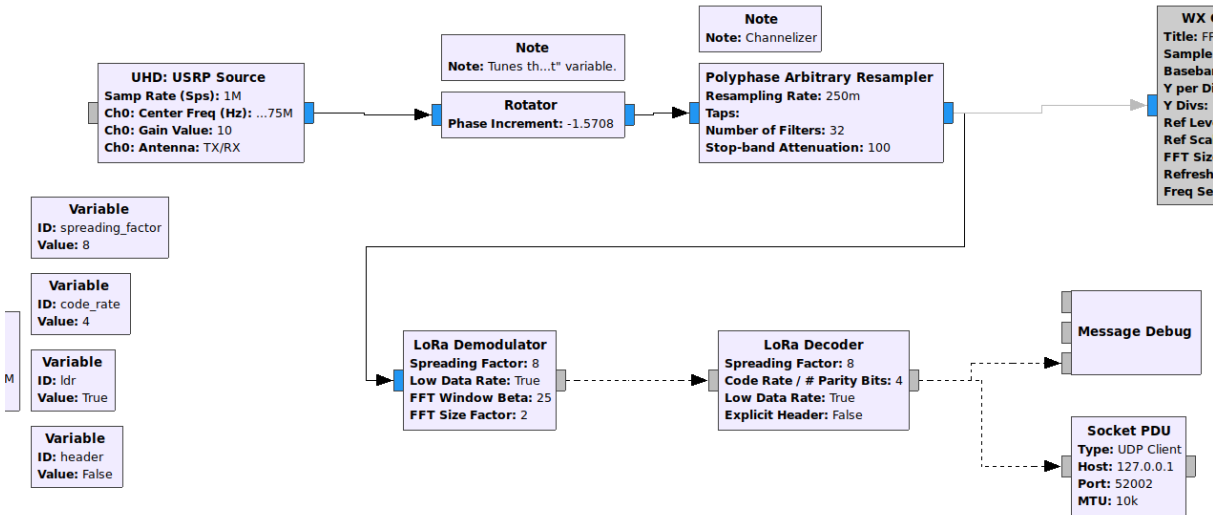


Figure 3.1: Knight's GNU Radio gr-lora OOT RX example [23]

Figure 3.1 shows the typical flow of a GNU Radio flowgraph where data is passed from block to block as a stream (blue connection ports) or as message blocks (grey connection ports).

Robyns' implementation is also an OOT module for GNU Radio. It has a elaborate installation and usage guide. A docker environment is also provided for testing the decoding of a LoRa signal, which is a big plus. Unlike Knight's implementation, this module has demodulation, decoding and channelization all in one single block as shown in Figure 3.2. The module has been tested with various SDR devices but not with the LimeSDR mini. Nevertheless it worked well for us and we based the CRAN implementation for LoRa on this module.



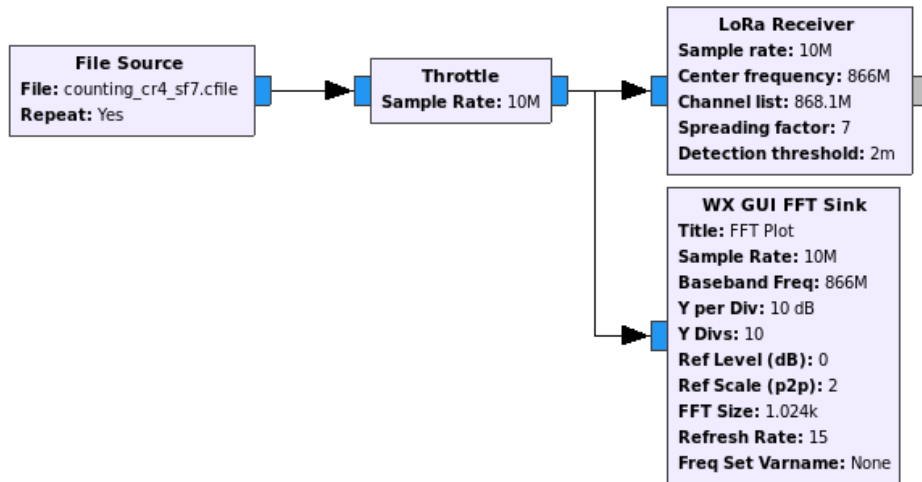


Figure 3.2: Single LoRa Receiver block (top right) [24]

## 3.2 LoRa decoding

The difficulty with reverse engineering LoRa is that its proprietary and there is no official documentation on the PHY. To reverse engineer, information hints on the PHY layer have to be taken from various official LoRaWAN documents, from patents, and the rest is guesswork. To make it more difficult, some of the documentation is a lie as the PHY is not implemented in the way it is described. complete lie, see Knight [25]. The data is encoded before it is sent over the air to make it more resistant against interference. Thus after demodulating the signal with a Fourier Transform, the data has to be decoded to make it usable. Semtech's european patent hints at the following four steps:

1. Symbol gray indexing. This adds error tolerance
2. Data whitening. This induces randomness.
3. Interleaving. This scrambles the bits within a frame
4. Forward Error Correction. This adds correction parity bits.

Those are 4 distinct operations which have to be reverse engineered [25].

Robyns et al. identified and implemented the following seven steps in their receiver to receive and decode a LoRa signal: detection, synchronization, demodulation, deinterleaving, dewatering, decoding, and packet construction [24]. They also provide a detailed description of the packet structure, especially the header. They deduce that because the minimum SF is SF 7, and the header is always transmitted with  $CR = 4$ , it must fit in an interleaving matrix of a certain size which results in the header having a size of 40 bits. The header contains important data as the payload length, thus it makes sense that the header is always sent with the highest coding rate. At the time of Knight's talk, he did not decode the header. Robyns' implementation is quite complete except for CRC checks of the payload and header as well as decoding multiple channels simultaneously.



# Chapter 4

## C-RAN in cellular networks

A Radio Access Network (RAN) provides the connection between an end-device e.g. a mobile phone and the core network e.g. network of the telecom provider. A RAN provides access and manages resources across the radio sites. It is a major component in telecommunications. RAN components include a base station and antennas that cover a specific region. The base stations connect to the core network [26].

### 4.1 D-RAN

Distributed Radio Access Network (D-RAN) is the present mode of operation for many mobile network operators. In a D-RAN, the 4G radio at the site tower consists of a Baseband Unit (BBU) on the ground and a Remote Radio Head (RRH) at the top as Figure 4.1 shows. RRH and BBU are connected via the Common Protocol Radio Interface (CPRI). The BBUs in each tower are connected via ethernet to the Mobile Switching Center (MSC) [27].

### 4.2 Moving to C-RAN

In a Cloud / Centralized RAN (C-RAN) the BBU in each tower site are moved into a centralized place, the BBU hotel, see Figure 4.2. This new architectural setup results in saving cost in capital expenditures as well as operational expenditures. The many small routers in the cell towers can be replaced by one in the BBU hotel. Deployment, maintenance and scaling can be expedited as all the BBU are centralized. Also this enables the BBU for Network Function Virtualization (NFV) and the RAN for Software Defined Networking (SDN) [27].

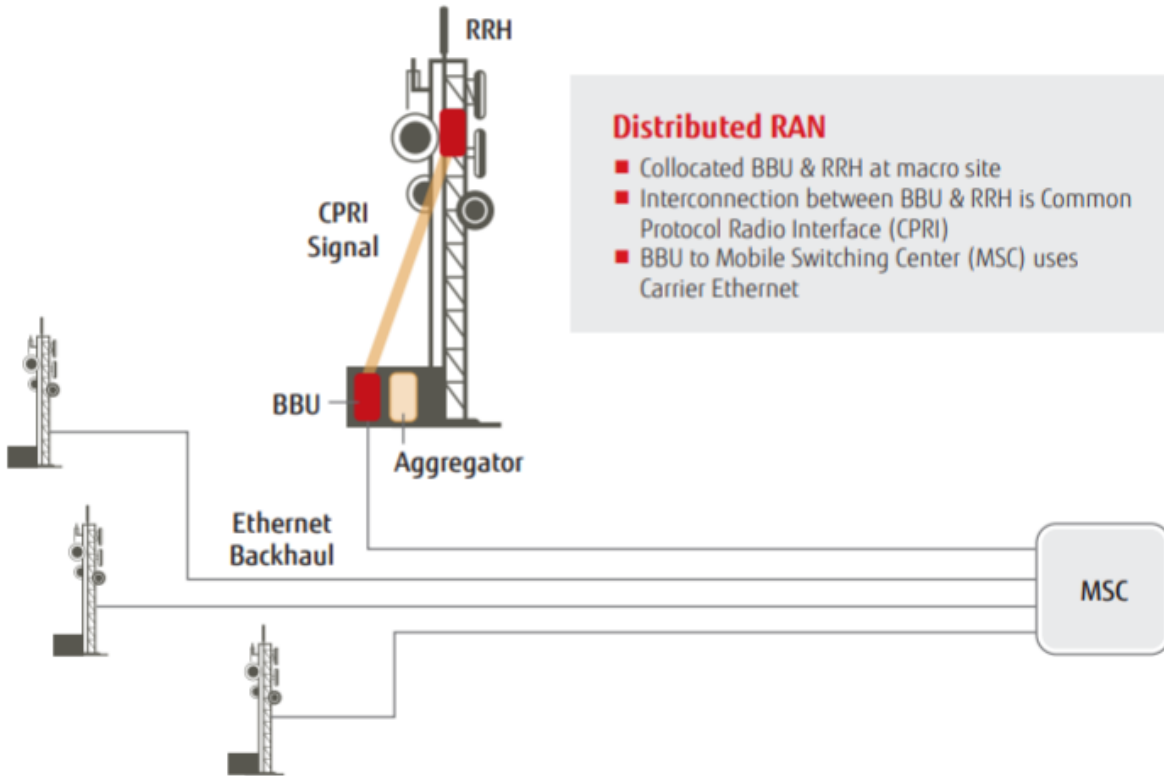


Figure 4.1: Distributed cell towers with each with a RRH and BBU [27]

### 4.3 Virtual RAN

In virtual RAN the execution environment is abstracted i.e. virtualized. Radio functions applications operate on a virtualized environment and interact with physical resources directly or through hardware emulation. Such a cloud environment enables RAN as a service [28]. For C-RAN this means instead of having a separate standalone physical device for each BBU in the BBU hotel the BBUs now can run on a single physical server with each BBU in a virtualized environment.

Nikaein et al. describe two main steps for realizing a C-RAN namely:

- **Commoditization and Softwarization** which essentially is the implementation of network and RF function in software.
- **Virtualization and Cloudification** which is the execution of network functions and management of physical resources by a cloud OS [28].

Nikaein et al. found that containers e.g. docker proved to be more adequate in their RAN as a service experiment as they offer near bare metal performance and provide direct access to the RF hardware. Virtual machines in, particular KVM, also gave them good performance, but require low latency mechanism to access I/O resources.

For the C-RAN for LoRa, described in chapter 5, docker is used for the virtualization layer.

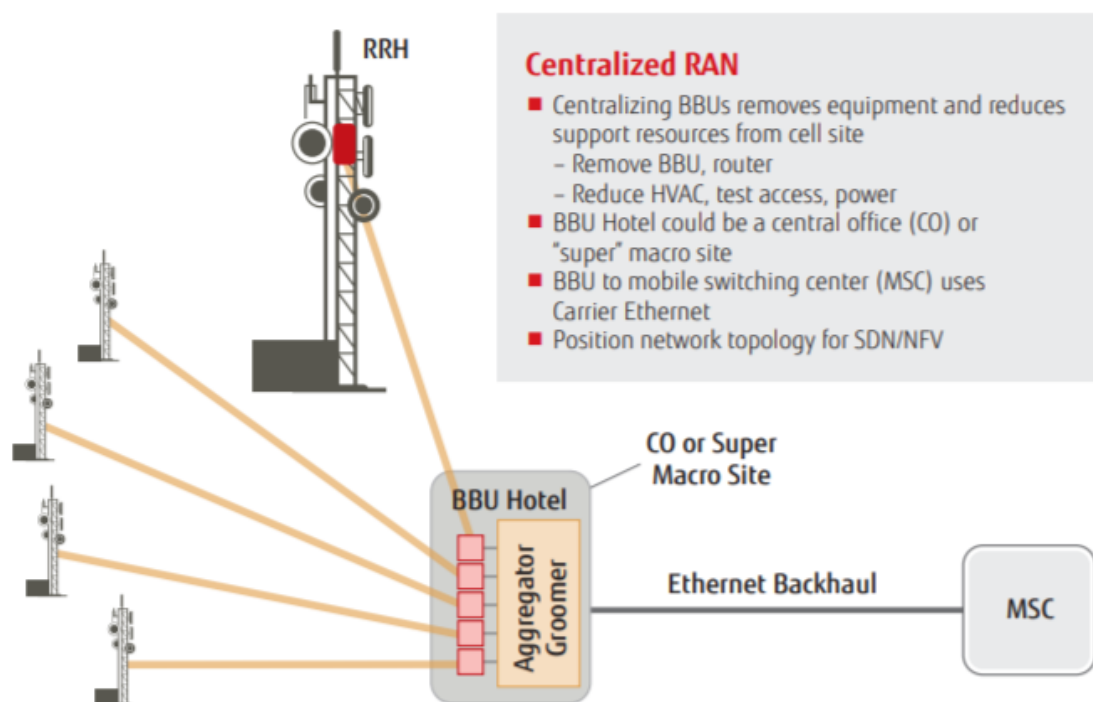


Figure 4.2: BBUs are centralized in the BBU hotel [27]



# Chapter 5

## C-RAN for LoRa

### 5.1 Goal

The goal is to set up a minimal working environment for a LoRa C-RAN. The gateway's functionality should be separated into an RRH and BBU component and the BBU component should be virtualized and run on general purpose hardware. A simple network server should process the uplink message and schedule a response if required. From this setup basic network requirements can be derived and measured as well as costs estimated.

### 5.2 Hardware

An Arduino Mega 2560 with the Dragion LoRa Shield v1.4 is the end device, see Figure 5.1a. A LimeSDR mini, Figure 5.1b, serves as the receiver for the RRH. The Raspberry Pi, Figure 5.1c with a LoRa hat was used for testing up -and downlink signals, but not for the experiment itself. Its hat is the iC880A LoRaWAN concentrator for the 868MHz frequency.

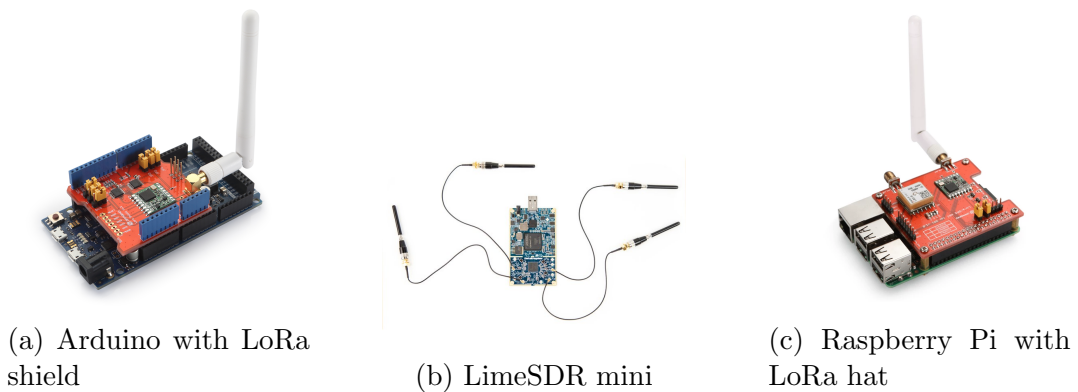


Figure 5.1: Hardware devices

## 5.3 Sending Uplink Signals

Uplink signals are sent with an arduino device equipped with a LoRa shield. The arduino is controlled with an adapted form of the IBM LoraMAC-in-C (LMIC) library, modified to run on arduino devices. Using this library we implemented a simple communication protocol where a queue of packets is sent out in an interval. See section 5.7.3 for detailed information.

## 5.4 RRH and BBU

For splitting up the LoRa gateway's functionality we use two laptops. One laptop has the LimeSDR mini plugged in and serves as the RRH. The other decodes the LoRa signal in software, processes the signal and also generates LoRa signals in software and sends those downlink I/Q samples back to the RRH. The processes on the second laptop run in virtualized environment with docker, more specifically docker compose, dockers orchestration tool.

The LoRa OOT module by Robyns et al. has a branch called "encoder" where they began the implementation of modulating an uplink LoRa signal in software. It is able to generate a specific test packet but the modulated signal has errors as we saw when we inspected the data payload on the LoRa gateway. Having an uplink signal generator was a nice starting point, but we needed something to generate downlink signal. In the end we extended the existing implementation by adding a downlink signal generation ability, see section ??.

Though, as a first workaround we set up a private LoRaWAN network, scheduled a downlink, and recorded it to a file. Now we can stream that file as a response by streaming its content, which are I/Q samples, to the RRH.

## 5.5 Study Subjects

### 5.5.1 Network Utilization

For measuring network traffic, the tool "bmon" is used which stands for bandwidth monitor. It estimates the bits per second on all available network interfaces, ingoing as well as outgoing.

### 5.5.2 Impact of Delay

Speed is essential for most communication systems. LoRaWAN specifies two receive windows for class A devices. One 1 second after transmission, and if not received in this window, another one 2 seconds after transmission. The protocol for this experiment is more lenient. After transmission, the device starts listening for at least 4 seconds before retransmitting the unacknowledged packet.



### 5.5.3 Network Delay

Using the command line tool *netem*, which stands for network emulator, we introduce some delay between the RRH and the BBU. The command is: `tc qdisc add dev interface_name root netem delay 200ms`. In which *interface\_name* is something like `eth0`.

This instructs `tc` (traffic control) to modify the `qdisc` (queuing discipline) by adding (add) a new rule to the device (dev) e.g. `eth0` to modify the outbound traffic scheduler (root) using the network emulator (*netem*) with a delay of 200ms [29].

This setup can be easily seen and tested in action:

- On the RRH add a delay of 8000ms
- On the BBU, in a terminal, type `nc -l 4040`
- On the RRH, in a terminal, type `nc <IP-ADDRESS-OF-THE-BBU> 4040`

On the RRH on the same terminal on, type a message and send with enter. It should arrive on the BBU's terminal after 8 seconds, which was the case.

### 5.5.4 Processing Delay

Not only are network delays of importance, but also the processing time it takes for decoding incoming messages and scheduling downlink messages. In the python script that sends the downlink, a call to `time.sleep()` can simulate longer processing times.

## 5.6 Architecture

### 5.6.1 Overview

This section aims to first give a high level overview of the architecture and then give a more detailed architectural overview of each component. Figure 5.2 shows the high level architecture with all the hardware components involved. There are two laptops in the same network connected by an ethernet cable. One laptop serves as an RRH. It has the LimeSDR mini plugged into its USB port so it can send and receive signals. Incoming signals come from the arduino device. The arduino transmits packets over the air as radio waves. Those get picked up by the RRH which converts the analog signal and send them as digital 32bit floats as I/Q samples over ethernet to the second laptop. This second laptop is the host for the virtual BBU that runs in a docker container. There the signals get demodulated and decoded. Then the decoded signal gets processed. In case a response is requested, a response signal is generated and sent as I/Q samples back to the RRH. From there it gets transmitted back to the arduino.

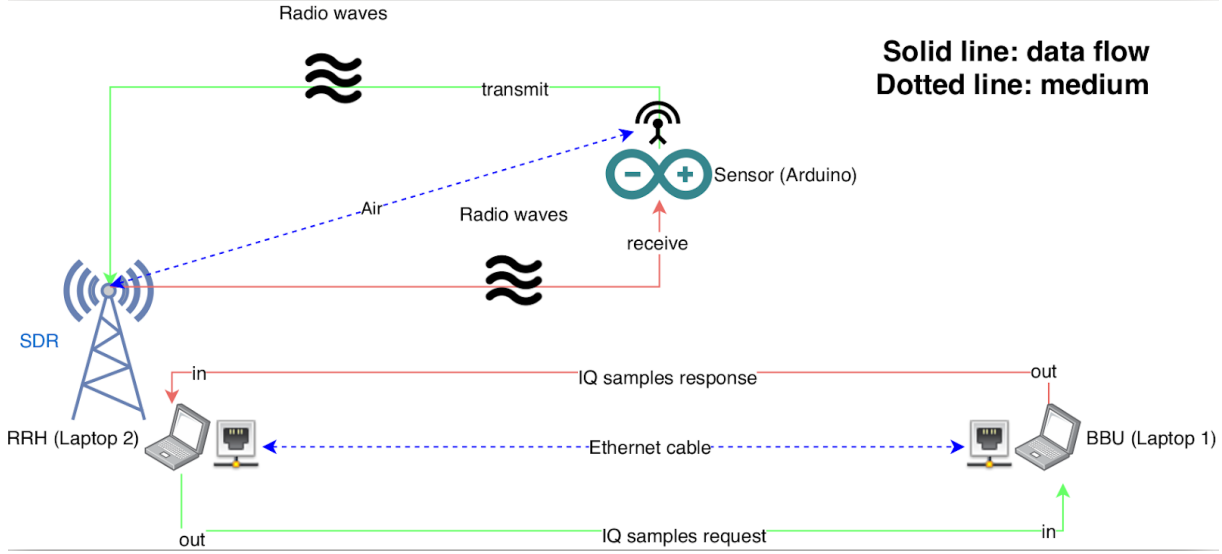


Figure 5.2: High level architecture

### 5.6.2 Containerization and Orchestration

docker docker compose, ready for cran as service openstack

### 5.6.3 RRH and BBU

The RRH is the simplest component. It has an antenna for input and one for output. In Figure 5.3 the RRH is composed by the two components "SDR RX" and "SDR TX". They correspond to the physical RX and TX slots on the SDR device. The BBU is the "Lora Decoder" component. It runs in a virtualized environment. Decoded messages get passed to the "Python Script" component. This acts as a network server that schedules an acknowledgement message back to the arduino. It could run on a third laptop connected via ethernet to the BBU laptop, but for our purposes it runs on the same laptop as the BBU but in a separate docker container.

## 5.7 Implementation

All communication between the components happens over sockets. We use the ZeroMQ (ZMQ) networking library. It is a good messaging library that offers N-to-N patterns as possible ways to connect the sockets, such as a request-reply pattern or pub-sub pattern and many more [30]. GNU Radio offers ZMQ blocks out of the box, The TCP sink and source blocks for socket communication are still available but deprecated. For communication between the RRH and the BBU the pub-sub (publish-subscribe) pattern is used. Figure 5.3 shows the "PUB" and "SUB" blocks and the data flow. The RRH has a PUB socket that takes as input the I/Q sample stream generated by the RX of the SDR. The SUB socket in the BBU subscribes to this publishing socket. As this socket connection

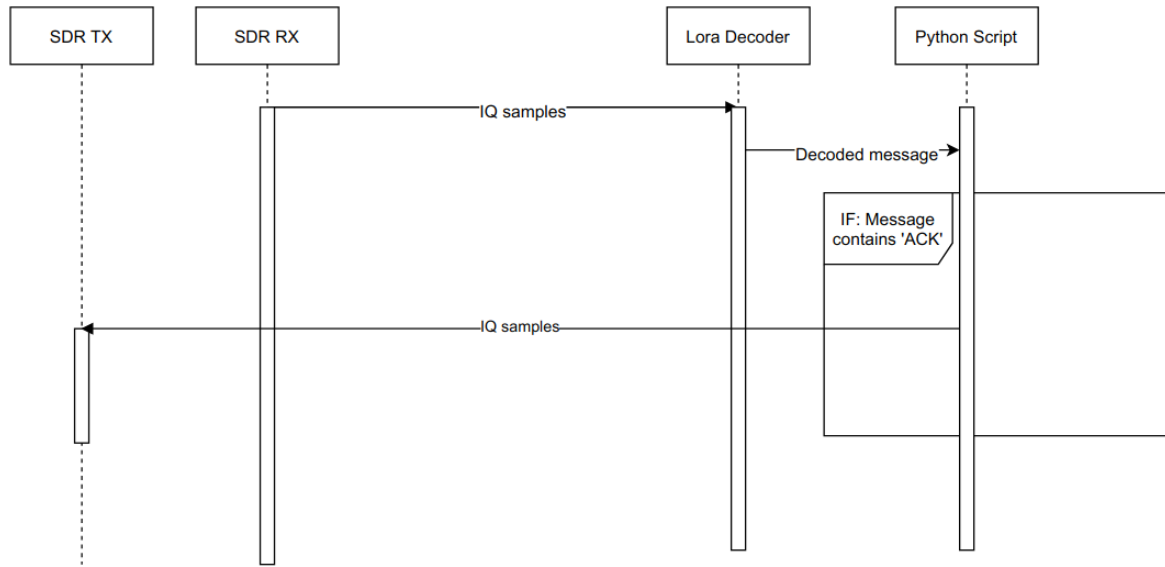


Figure 5.3: Sequence diagram

happens with TCP, the I/Q samples arrive in the order they are sent and can be directly passed to the LoRa Decoder. Robyns' et al. implementation of LoRa Decoder sends the decoded message out on a UDP socket. The "Python Script" block which is our LoRa network server takes the decoded messages over on this UDP socket and then, streams out I/Q samples of the response message over a ZMQ publishing socket to which the RRH's TX slot subscribes to. This closes the cycle. One of the advantages of using ZMQ is that the sockets can be given the option to not time out or close. This means a subscribing socket can be started before a publishing socket without issues. The subscribing socket can wait for the publishing socket to get instantiated. For our architecture this means the docker containers for the RRH and BBU can be started in any order and more instances of the BBU can be added at runtime. The sub-pub pattern allows new subscribers and publisher to join.

### 5.7.1 RRH

The RRH implementation is straightforward. Figure 5.5 shows the necessary GNU Radio blocks. On the left is the RX block of the LimeSDR that streams the incoming signals to the PUB socket. The response message from the network server to send out comes through a SUB socket which streams directly to the TX block of the LimeSDR on the far right of the Figure. The parameter blocks allow the passing of command line arguments to the resulting application to configure the socket addresses if necessary. As there is a OOT module needed for GNU Radio to work with the LimeSDR, the RRH comes also in a docker container to quickly get started as the necessary dependencies have all been installed in that container.

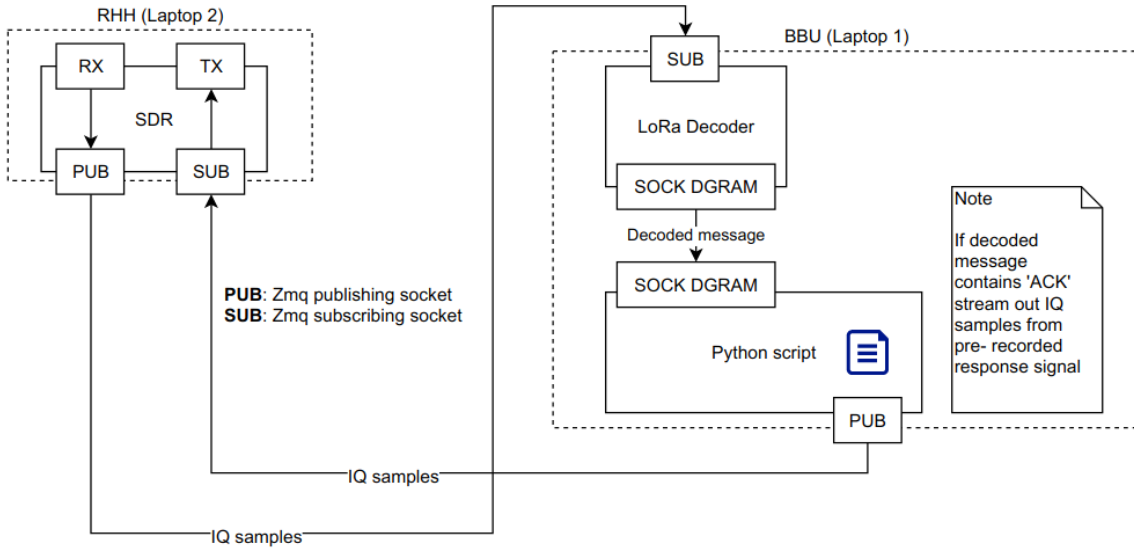


Figure 5.4: Socket communication between components

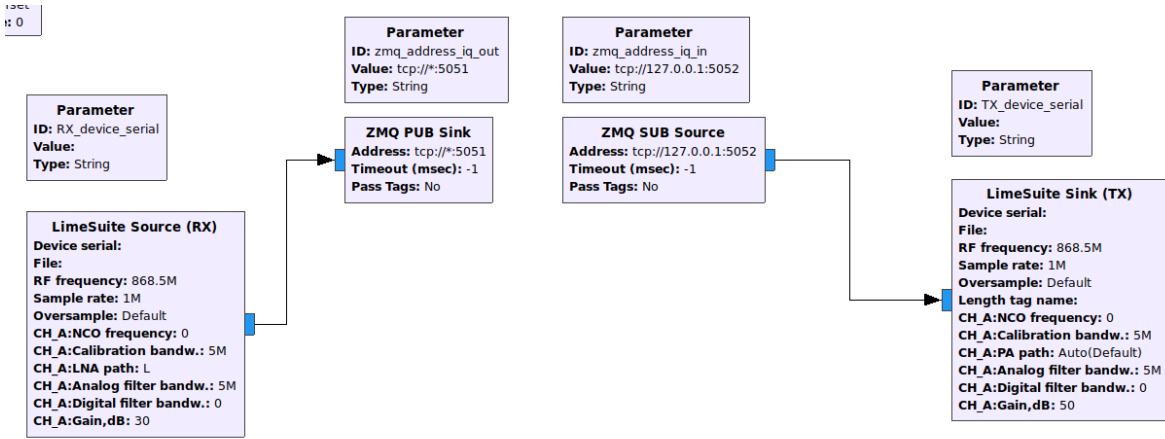


Figure 5.5: GNU Radio blocks for the RHH

### 5.7.2 BBU

The BBU as shown in Figure 5.6 takes in the RX stream of the RHH on a SUB socket, passes the I/Q samples to the LoRa decoder. The decoder decodes LoRa signal and outputs them as a message on the message socket sink, far right in the Figure.

The python script which acts as our network server, inspects the message payload and if an acknowledgement is required by the sender it generates the response signal. Listing 1 shows an excerpt of that python script. The acknowledgement message is a recording of a LoRa downlink signal. Its I/Q samples get read into memory. The script connects to the UDP socket. As the BBU component and this python script run on the same host, it connects to 127.0.0.1, the port is passed as argument to the script. As the focus lies on the split between RHH and BBU we decided to hard code the IP address to localhost for the LoRa decoder and the network server as they run on the same machine as depicted in

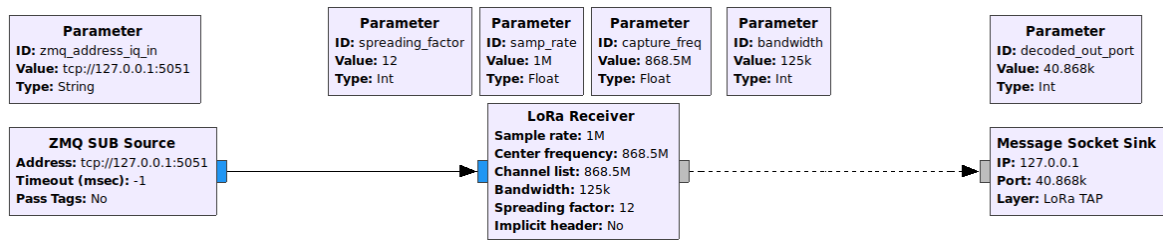


Figure 5.6: GNU Radio blocks for the BBU

Figure 5.4. Then, in an endless loop, data gets received from the socket. The buffer size is 1024 bytes. Whenever "ACK" is in the message payload, the acknowledgement signal get streamed out over a ZMQ publishing socket.

The BBU and the network server run each in a container started with docker compose.

```
import zmq
import socket
...
with open (dir_path + "/ACK_DOWN_SF12_CR4.raw") as f:
    ack = f.read()
...
zmq_socket = context.socket(zmq.PUB)
...
s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
s.bind(("127.0.0.1", udp_port))
print ('listen for decoded lora packages on udp port ' + str(udp_port))
while True:
    data, addr = s.recvfrom(1024)

    if ("ACK" in data):
        zmq_socket.send(ack)
    else:
        print ("received package requests no ACK")
```

Listing 1: Excerpt of the python script that functions as the network server

### 5.7.3 Communication Protocol Arduino

The LMIC library runs a loop that executes jobs scheduled to run at a specified time. In the `setup()` function that runs once when the arduino starts settings such as the spreading factor, frequency and coding rate are set. The frequency is given in Hertz and the the datarate is set with a predefined enum from the LMIC library. Also, the initial job for the LMIC is initialized there, see Listing 2 last line.

```

void setup() {
    Serial.begin(9600);
    ...
    // initialize runtime env
    os_init();
    ...

    LMIC.freq = 868500000;
    LMIC.txpow = 27; // Maximum TX power
    LMIC.datarate = DR_SF9;
    // This sets CR 4/5, BW125 (except for DR_SF7B, which uses BW250)
    LMIC.rps = updr2rps(LMIC.datarate);

    Serial.println("Started");
    Serial.flush();

    // setup initial job
    os_setCallback(&txjob, my_tx_func);
}

```

Listing 2: Arduino setup() function

The last line schedules the initial job *txjob* with the *my\_tx\_func* function that gets run on execution of the job, see Listing 4. It takes the the index of the packet to send, Listing 3, and checks if the packet has "ACK" appended. Then the transmit function *tx(packet, callback)* gets executed. It takes a packet and a callback function that gets executed after the transmission is finished. If an "ACK" is present, the callback function is set to *my\_txdone\_func*, if not it is set to *my\_txdone\_no\_ack\_func*. Finally, in line 16 in Listing 4, schedules itself to be run again after *TX\_INTERVAL* which is 4 seconds.

```

#define TX_INTERVAL 4000

int currentPacketIndex = 0;
const int numOfPackets = 3;
char *myPackets[numOfPackets] = {
    "This is packet 1ACK",
    "This is packet 2ACK",
    "This is packet 3",
};

```

Listing 3: Packets 1 and 2 have "ACK" appended in their payload, while packet 3 does not

The difference between the callback functions passed to the transmission function is that one waits to receive an acknowledgement while the other simply increases the *currentPack-*

```

1  static void my_tx_func(osjob_t *job) {
2  if (currentPacketIndex < numOfPackets) {
3      ...
4      char lastThree[3];
5      memcpy(lastThree, &myPackets[currentPacketIndex][length - 3], 3);
6      const char ack[] = {'A', 'C', 'K'};
7      if (!memcmp(lastThree, ack, 3)) {
8          // send and start rx for receiving ACK
9          Serial.print("transmitting packet with ACK, packet: ");
10         tx(myPackets[currentPacketIndex], my_txdone_func);
11     } else {
12         // send and schedule next packet
13         Serial.print("transmitting packet without ACK, packet: ");
14         tx(myPackets[currentPacketIndex], my_txdone_no_ack_func);
15     }
16     os_setTimedCallback(&txjob, os_getTime() +
17                         ms2osticks(TX_INTERVAL), my_tx_func);
18 } else {
19     Serial.println("No more packets to send, done");
20 }
21 }

```

Listing 4: *my\_tx\_fun* function

*etIndex* so the next packet gets sent the next time *my\_tx\_func* get called. The callback to the RX function gets executed every time a packets is received. Listing 5 shows the implementation. The response signal by sent by the network server has the payload "ACK", which is three bytes. If the *LMIC.dataLen* is three bytes, it is assumed it is the expected acknowledgement signal. The *currentPacketIndex* gets incremented and the next transmission job gets set up. Else, the *currentPacketIndex* does not get incremented so the same packet gets rescheduled for transmission and the RX function gets called again.

## 5.8 Results

### 5.8.1 Network Utilization

Monitoring the network utilization with bmon yields 335 bytes per second on the ethernet network interface when idle. Once the C-RAN gets started the network utilization rises to 8MiB/s (Mebibytes) which are equal to 67'108'864 bits. Bmon only gives an estimation. The theoretical value can be derived the following way:

- The LimeSDR had the sample rate set to 1 million samples per second by default.

```

1 static void my_rx_func(osjob_t *job)
2 {
3     if (LMIC.dataLen == 3)
4     {
5         Serial.println("Got ACK");
6         // if we get our ACK, start with next transmission,
7         // reschedules transmission at half TX_INTERVAL
8         currentPacketIndex++;
9         os_setTimedCallback(&txjob, os_getTime()
10                             + ms2osticks(TX_INTERVAL / 2), my_tx_func);
11     }
12     else
13     {
14         Serial.println("NOT AN ACK");
15         // resend packet if no ACK received within 3*TX_INTERVAL,
16         // reschedules transmission in 3* TX_INTERVAL
17         os_setTimedCallback(&txjob, os_getTime()
18                             + ms2osticks(3 * TX_INTERVAL), my_tx_func);
19         // listen again
20         rx(my_rx_func);
21     }
22 }

```

Listing 5: RX function that checks for the response or reschedules the packet transmission

- The type is of complex type of 32 bit, (I/Q) => 2 x 32 bit, which gives 64 million bits/s
- MTU (Maximum Transmission Unit) on most systems is 1500 bytes.
- Overhead for TCP and IP is 20 bytes each => 40 bytes
- This gives a MSS (Maximum Segment Size) of 1460 bytes
- $64\text{M bits} \div (1460 \text{ bytes} \times 8) = 5479.45$  packets needed
- Total overhead:  $5480 \text{ packets} \times (40 \text{ bytes} \times 8) = 175360$  bits
- $64'000'000 \text{ bits} + 1'753'600 \text{ bits} = 65'753'600 \text{ bit/s} = 7.8 \text{ MiB/s}$

The RRH is constantly sending samples to the BBU. It does not matter if the arduino sends 1 signal every 4 seconds or 40 signals per second, the network utilization stays the same as the sample rate stays the same. The experiment worked without error with the 10 gigabit ethernet connection, but it did not work over Wi-Fi connection. The response signal sent from the BBU to the RRH did not arrive on the RRH.



**Optimization:** The load on the network can be reduced. According to the Nyquist-Shannon sampling theorem [31] a sufficient sampling rate  $f_s$  for a signal with bandwidth  $B$  is given by:

$$f_s > 2 * B$$

The signal bandwidth of the LoRa signal sent with the arduino is set to 125 kHz. Thus the minimum sampling frequency according to the formula above is 250'000 samples per second which is a quarter of the previous sample rate of 1 million. This also quarters the network utilization from 8 MiB to 2 MiB, see Table 5.1. Lowering the sampling rate below the Nyquist-Shannon limit results in the signal not getting successfully decoded.

Sample Rates and Network Utilization			
Samples per second	Max. Signal Bandwidth	Network Utilization	Decode Success in Experiment
1'000'000	500 kHz	8 MiB/s	yes
500'000	250 kHz	4 MiB/s	yes
250'000	125 kHz	2 MiB/s	yes
125'000	62.5 kHz	1 MiB/s	no

Table 5.1: Sampling rates and network utilization

LoRaWAN defines different regional parameters. In the EU SF 8 to SF 12 signals are sent with 125 kHz bandwidth, while SF 7 can be sent with 125 kHz or 250 kHz bandwidth. In the US on the other hand SF 7 to SF 12 can also be sent with a 500 kHz bandwidth [32]. This has to be taken into consideration when designing a LoRaWAN compliant C-RAN architecture. The network load for decoding a 500 kHz bandwidth US signal is for times higher than a EU 125 kHz bandwidth signal.

### 5.8.2 Cost

LoRa gateways come in various prices. The low cost indoor commercial gateway by TTN costs around 70\$ while their higher end gateway sells for 300\$. Cheaper gateways can be built with and Arduino and a LoRa shield such as the Dragino shield (22\$). The issue is that those are often based on the SX1272/SX1276 chips. While cheaper, those gateways are so called single channel gateways. They can only listen on one channel with one spreading factor. They are not LoRaWAN compliant [33]. LoRaWAN compliant gateways can be built with a Raspberry Pi with a iC880A concentrator (130\$) which use the SX1301/SX1257 chips. They can receive packets of sent with different spreading factors on up to 8 channels in parallel.

The LoRa Decoder block of Robyns et al. does not yet support multichannel decoding. Spreading factor and center frequency need to be set explicitly, making it a single channel gateway. The advantage of having a decoder in software is that new instances of the LoRa Decoder block can be added without additional hardware costs. As the BBU is containerized, starting up a new instance is as easy as instructing docker to start a new instance of the decoder and pass it the desired frequency and SF. This saves the costs

of a LoRaWAN concentrator. These savings are offset by the need for general purpose hardware the containers can run on and the higher bandwidth requirements.

Using the amazon aws cost calculator <https://calculator.s3.amazonaws.com/index.html> the following three fields are of importance :

- Compute:
  - Amazon EC2 Instance
- Data Transfer:
  - Data Transfer In
  - Data Transfer Out

For the EC2 instance we select the *a1.medium* which comes with 1 vCPU and 2 GiB of memory at *0.0255\$* per hour.

Data Transfer In has to be 8 MiB/s to accommodate the maximum possible signal bandwidth of 500 kHz in the US or 4 MiB/s for the maximal signal bandwidth of 250 kHz in EU. In this cost estimation example we proceed with 4 MiB/s for Europe. 4 MiB per second are 363 GB per day. Data input is free on AWS giving a daily cost of 0\$.

Data Transfer Out on the other hand does cost. The amount of data that gets sent out depends on how many uplink signals require a downlink signal. In our example a fixed 3 byte payload response is sent. In LoRaWAN, downlink messages can have variable length, multiple bytes long. Sticking with our example, the fixed downlink response signal with a payload of 3 bytes (excluding preamble, header and crc ), SF 7 and coding rate 4/5, yields an I/Q sample stream of 248 kB (including preamble, header and crc) after modulation. How many downlink signals will the required? That depends on whether the end-node requires a confirmed uplink. However, there is an upper limit. The EU specifies a 1% duty cycle for the 868.0 - 868.6 MHz frequency plan [34]. The downlink signal has an airtime of 25.86 ms. With a duty cycle of 1% a downlink signal can be sent every 3 seconds. This means a maximum of 28'800 downlink signals of this type can be sent by one gateway a day. Data Transfer Out is thus limited to 7 GB a day if duty cycles are respected,  $28800 * 248 \text{ kB} = 7 \text{ GB}$ . TTN encourages end-devices to not use confirmed uplinks as most gateways are not designed to send and receive simultaneously. We assume for our experiment that about 30% of total possible downlink signals need to be sent which gives a Data Transfer Out of 2.1 GB/day.

Total monthly cost amounts to 24.07\$:

- Compute:
  - Amazon EC2 Instance: 18.67\$
- Data Transfer:

- Data Transfer In: 0\$
- Data Transfer Out: 5.40\$

As the modulated signals have to be sent out over TCP/IP from the BBU to the RRH, a TCP/IP overhead of 2.7% could theoretically be added, but it is negligible as it is an estimation for comparison and not for absolute numbers.

In the traditional LoRa setup where the gateway is not split into an RRH and BBU component the decoded packet gets sent to the network server and not the I/Q samples. Assuming the same setup as before, instead of calculating  $28800 * 248 \text{ kB} = 7 \text{ GB}$ , the following has to be calculated:

- payload size: 3 bytes
- header size: 4 bytes
- CRC size: 0 bytes, downlink messages do not have a CRC

This yields the following  $28800 * 7 \text{ Bytes} = 0.0002016 \text{ GB}$ , which is an insignificant daily amount for AWS as it gives already 0\$ as cost estimation before we even apply the 30% usage assumptions. Thus, sending the I/Q samples over the internet to the cloud is infinitely more expensive compared to just sending the demodulated signal.

However, in a local cloud setup where RRH and BBU are on the same network or in a network architecture the data does not have to be routed over the internet and the BBU can still be virtualized and centralized in a BBU hotel for much cheaper. In such a setup hardware and operational costs can be saved as outlined in section 4.2. For each gateway at least 130\$ costs for the LoRa concentrator could be saved by doing its job in software. For a hobbyist that operates a single gateway it may not be useful as now he needs to invest in general purpose hardware that is fast enough to do the decoding in software. Though, for an operator with multiple gateways, centralizing and virtualizing the decoding has similar benefits as a C-RAN for LTE.

### 5.8.3 Delays

Various network delays for the outgoing sample stream from the RRH to the BBU were set. Table 5.2 summarizes the results.

The higher the delay the less network utilization was measured with bmon. But only after delay, namely 300ms. Without delay, RX resp. TX on the ethernet ports of the RRH and BBU is 8 MiB/s. With a 800ms delay it is about 2.32 MiB/s. With a 400 ms delay it is 5.5 MiB/s. With a delay of 300ms or less it bmon measured still 8 MiB/s.

Delay (ms)	Network Traffic (MiB/s)	Decode Success	
		Single Signal	Multiple Signal
0	8	yes	yes
0	6.4	yes	yes
0	2.1	yes	yes
0	500	yes	yes

Table 5.2: Effect of delay on network traffic on decode process

Table 5.3: Standard behaviour of the S column type.

Some Values
2.3456
34.2345
−6.7835
90.473
5642.5
$1.2 \times 10^3$
$10^4$

# Chapter 6

## LoRa Tools



# Chapter 7

## Future work

### 7.1 Limitations

### 7.2 Improvements





## Chapter 8

### Summary and Conclusions



# Bibliography

- [1] Elodie Morin, Mickael Maman, Roberto Guizzetti, Andrzej Duda, *Comparison of the Device Life-time in Wireless Networks for the Internet of Things*. IEEE Access, IEEE, 2017, 5, pp.7097 - 7114. 10.1109/ACCESS.2017.2688279. hal-01649135.
- [2] “What is LoRa.” <https://www.semtech.com/lora/what-is-lora>, last visited 27.12.19.
- [3] “What is LoRaWAN.” <https://loro-alliance.org/sites/default/files/2018-04/what-is-lorawan.pdf>, last visited 27.12.19.
- [4] “LoRa Alliance.” <https://loro-alliance.org>, last visited 27.12.19.
- [5] “The Things Network.” <https://www.thethingsnetwork.org>, last visited 27.12.19.
- [6] B. Sousa, L. Cordeiro, P. Simões, A. Edmonds, S. Ruiz, G. A. Carella, M. Corici, N. Nikaein, A. S. Gomes, E. Schiller, T. Braun, and T. M. Bohnert, “Toward a Fully Cloudified Mobile Network Infrastructure,” vol. 13, no. 3, pp. 547–563, 2016.
- [7] F. Adelantado, X. Vilajosana, P. Tuset-peiro, B. Martinez, J. Melià-seguí, and T. Watteyne, “Understanding the Limits of LoRaWAN,” no. September, pp. 34–40, 2017.
- [8] “Lora vs other wireless technology.” [https://www.semtech.com/uploads/images/LoRa\\_Why\\_Range.png](https://www.semtech.com/uploads/images/LoRa_Why_Range.png), last visited 27.12.19.
- [9] “LoRa signals from a low orbit satellite.” <https://twitter.com/telkamp/status/956900631985475586?lang=en>, last visited 27.12.19.
- [10] “LoRaWAN regional parameters.” [https://loro-alliance.org/sites/default/files/2018-04/lorawantm\\_regional\\_parameters\\_v1.1rb\\_-\\_final.pdf](https://loro-alliance.org/sites/default/files/2018-04/lorawantm_regional_parameters_v1.1rb_-_final.pdf), last visited 27.12.19.
- [11] “About LoRaWAN.” <https://loro-alliance.org/about-lorawan>, last visited 27.12.19.
- [12] “LoRaWan security.” [https://loro-alliance.org/sites/default/files/2019-05/lorawan\\_security-faq1.pdf](https://loro-alliance.org/sites/default/files/2019-05/lorawan_security-faq1.pdf), last visited 27.12.19.
- [13] “LoRa / LoRaWAN tutorial 12, Modulation types and Chirp Spread Spectrum.” [https://www.mobilefish.com/download/lora/lora\\_part12.pdf](https://www.mobilefish.com/download/lora/lora_part12.pdf), last visited 27.12.19.

- [14] “LoRa / LoRaWAN tutorial 13, Symbol, Spreading Factor & Chip.” [https://www.mobilefish.com/download/lora/lora\\_part13.pdf](https://www.mobilefish.com/download/lora/lora_part13.pdf), last visited 27.12.19.
- [15] P. Robyns, P. Quax, W. Lamotte, and W. Thenaers, “A Multi-Channel Software Decoder for the LoRa Modulation Scheme,” pp. 41–51, 01 2018.
- [16] “SX1272/3/6/7/8: LoRa Modem, Designer’s Guide.” <https://www.rs-online.com/designspark/rel-assets/ds-assets/uploads/knowledge-items/application-notes-for-the-internet-of-things/LoRa%20Design%20Guide.pdf>, last visited 27.12.19.
- [17] “LoRa / LoRaWAN tutorial 14, Coding Rate and Forward Error Correction.” [https://www.mobilefish.com/download/lora/lora\\_part14.pdf](https://www.mobilefish.com/download/lora/lora_part14.pdf), last visited 27.12.19.
- [18] “Exploratory engineering, data rate and spreading factor.” [https://docs.exploratory.engineering/lora/dr\\_sf/](https://docs.exploratory.engineering/lora/dr_sf/), last visited 27.12.19.
- [19] “AN1200.22 LoRa Modulation Basics.” <http://wiki.lahoud.fr/lib/exe/fetch.php?media=an1200.22.pdf>, last visited 27.12.19.
- [20] “LoRaWAN Specification 1.0.3.” <https://lora-alliance.org/sites/default/files/2018-07/lorawan1.0.3.pdf>, last visited 27.12.19.
- [21] “Pothosware.” <http://www.pothosware.com/#about>, last visited 27.12.19.
- [22] “About GNU Radio.” <https://www.gnuradio.org/about/>, last visited 27.12.19.
- [23] “GNU Radio OOT module implementing the LoRa PHY, based on [https://github.com/matt-knight/research/tree/master/2016\\_05\\_20\\_jailbreak](https://github.com/matt-knight/research/tree/master/2016_05_20_jailbreak).” <https://github.com/BastilleResearch/gr-lora>, last visited 27.12.19.
- [24] “GNU Radio blocks for receiving LoRa modulated radio messages using SDR.” <https://github.com/rpp0/gr-lora>, last visited 27.12.19.
- [25] “GRCon16 - Reversing and Implementing the LoRA PHY with SDR, Matt Knight.” <https://www.youtube.com/watch?v=-YNMRZC6v1s>, last visited 27.12.19.
- [26] “Radio access network (RAN).” <https://searchnetworking.techtarget.com/definition/radio-access-network-RAN>, last visited 27.12.19.
- [27] “Centralized Radio Access Network (C-RAN) Transport.” <https://www.fujitsu.com/us/Images/Centralized-Radio-Access-Network-C-RAN-Transport-Application-Note.pdf>, last visited 27.12.19.
- [28] N. Nikaein, R. Knopp, L. Gauthier, E. Schiller, T. Braun, D. Pichon, C. Bonnet, F. Kaltenberger, and D. Nussbaum, “Demo – Closer to Cloud-RAN : RAN as a Service,” pp. 193–195, 2015.
- [29] “How to Use the Linux Traffic Control.” <https://netbeez.net/blog/how-to-use-the-linux-traffic-control/>, last visited 27.12.19.
- [30] “Radio access network (RAN).” <https://zeromq.org/>, last visited 27.12.19.

- [31] C. Shannon, "Communication in the presence of noise," *Proceedings of the IRE*, vol. 37, pp. 10–21, jan 1949.
- [32] "LoRaWAN Regional Parameters." [https://loro-alliance.org/sites/default/files/2018-05/lorawan\\_regional\\_parameters\\_v1.0.2\\_final\\_1944\\_1.pdf](https://loro-alliance.org/sites/default/files/2018-05/lorawan_regional_parameters_v1.0.2_final_1944_1.pdf), last visited 27.12.19.
- [33] "Single Channel Gateways." <https://www.thethingsnetwork.org/forum/t/the-future-of-single-channel-gateways/6590>, last visited 27.12.19.
- [34] "TTN Duty Cycle." <https://www.thethingsnetwork.org/docs/lorawan/duty-cycle.html>, last visited 27.12.19.
- [35] "Arduino-based Library for Dragino Lora Shield v1.4" <https://github.com/arduino-org/arduinolibary-lora-node-shield>, Last visit."



# Abbreviations

AAA      Authentication, Authorization, and Accounting





# Glossary

## **Authentication**

**Authorization** Authorization is the decision whether an entity is allowed to perform a particular action or not, e.g. whether a user is allowed to attach to a network or not.

## **Accounting**



# List of Figures

2.1	LoRa vs other wireless technology[8]	5
2.2	LoRaWAN network architecture [3]	6
2.3	Up- and down chirps [13]	8
2.4	Own recording of uplink transmission by arduino equipped with a LoRa shield	8
2.5	Chips and symbols value [14]	9
2.6	Running the signal through our toolchain, matching symbols with samples	9
2.7	LoRa packet structure [16]	11
2.8	LoRa uplink packet structure [20]	12
2.9	LoRa downlink packet structure [20]	12
2.10	LoRaWAN packet [20]	12
3.1	Knight's GNU Radio gr-lora OOT RX example [23]	14
3.2	Single LoRa Receiver block (top right) [24]	15
4.1	Distributed cell towers with each with a RRH and BBU [27]	18
4.2	BBUs are centralized in the BBU hotel [27]	19
5.1	Hardware devices	21
5.2	High level architecture	24
5.3	Sequence diagram	25
5.4	Socket communication between components	26
5.5	GNU Radio blocks for the RRH	26
5.6	GNU Radio blocks for the BBU	27



# List of Tables

5.1	Sampling rates and network utilization . . . . .	31
5.2	Effect of delay on network traffic on decode process . . . . .	34
5.3	Standard behaviour of the <b>S</b> column type. . . . .	34



# Appendix A

## Installation Guidelines

For Docker, see C.1.1. For manual installation, see C.2.1





# Appendix B

## Contents of the CD

The CD contains the following:

- a folder with the arduino source code
- a folder for the docker setup
- a folder with the grc (gnuradio companion) files
- a folder with various signal recordings
- a folder with the thesis source code and the final thesis pdf
- a folder with various tools for decoding, encoding and visualization of LoRa signals
- a README.md file

*All contents of the CD are available online on my GitHub <https://github.com/mustard123/master-thesis>*



# Appendix C

## README.md

Below is the README.md file converted to  $\text{\LaTeX}$ . It is recommended to view the file in a markdown viewer e.g. VS Code or on GitHub <https://github.com/mustard123/master-thesis>

### C.1 C-RAN for LoRa

An arduino with a LoRa shield sends out packets over the air in an interval. Some packets require an acknowledgment (ACK). If an ACK is required, the arduino waits for a certain amount of time for the ACK. If the ACK arrives in time, the arduino starts transmitting the next packet. If not, the arduino will resend the packet and again wait for the ACK.

The RRH (Remote Radio Head) receives radio waves with a LimeSDR. The RRH streams the IQ samples over the network to the BBU (Base Band Unit).

The BBU decodes the message. If the message says it requires an ACK, the BBU sends out IQ samples of the ACK message over the network to the RRH which transmits them back over the air to the arduino.

#### C.1.1 Run with Docker

1. Clone the repo
2. Go to the docker directory

#### *Info*

- The container runs in privileged mode to easily access plugged-in USB devices

- The container run in network mode host (No NAT or Bridge has to be considered). This means the containers have the ip address of the host machine. If RRH and BBU run on different machines, find out their respective IP with *ifconfig* and pass the address as arguments in the docker-compose.yml, see below.

---

### C.1.2 RRH

In the RRH directory run:

```
docker-compose up
```

This starts the Remote Radio Head. The RRH looks for a LimeSDR, it prints errors if it cannot find one. You can plug one in after the container has started and it should get detected. By default it uses the first LimeSDR it can find.

#### Parameters

There are various parameters which you can specify in the *docker-compose.yml* file.

Run this to see what the possible params are:

```
./zero_mq_split_a.py -h
```

Output:

Usage: zero\_mq\_split\_a.py: [options]

Options:

```
-h, --help                show this help message and exit
--RX-device-serial=RX_DEVICE_SERIAL
                          Set RX_device_serial [default=]
--TX-device-serial=TX_DEVICE_SERIAL
                          Set TX_device_serial [default=]
--capture-freq=CAPTURE_FREQ
                          Set capture_freq [default=868.5M]
--samp-rate=SAMP_RATE
                          Set samp_rate [default=1.0M]
--zmq-address-iq-in=ZMQ_ADDRESS_IQ_IN
                          Set zmq_address_iq_in [default=tcp://127.0.0.1:5052]
--zmq-address-iq-out=ZMQ_ADDRESS_IQ_OUT
                          Set zmq_address_iq_out [default=tcp://*:5051]
```

Param	Explanation
RX-device-serial	By default, the program will use the first LimeSDR it can find for receiving and transmitting signal. If you have two devices you can specify which should receive by passing the device Serial (See section <b>Help</b> for more info)
TX-device-serial	By default, the program will use the first LimeSDR it can find for receiving and transmitting signal. If you have two devices you can specify which should transmit by passing the device Serial (See section <b>Help</b> for more info)
capture-freq	The frequency in Hz at which the RRH listens for signals. Default value is 86850000

Param	Explanation
samp-rate	How many samples per second. Default value is 1000000. Must be at least double the bandwidth of the expected signal see <i>Nyquist-Shannon principle</i>
zmq-address-iq-in	ZMQ address to which the RRH subscribes to receive an IQ samples stream (from the BBU) to then send out (TX). Default value is tcp://127.0.0.1:5052 meaning the IQ samples are expected to come from localhost on port 5052. Normally RRH and BBU are on different devices but on the same network

---

Param	Explanation
-zmq-address- iq-out	ZMQ address on which the RRH streams out the IQ samples (to the BBU) it receives (RX). Default is tcp://*:5051 meaning it publishes the stream on all interface on port 5051

---



---

To pass the parameters you have to specify them in the docker-compose.yml

Example:

To pass a capture frequency of 915M and a sample rate of 250k enter the params in the following way in the command field:

*docker-compose.yml*

```
version: '3'
services:
  rrh:
    build: .
    privileged: true
    network_mode: host
    volumes:
      - /dev/bus/usb:/dev/bus/usb
    command: ["--capture-freq", "915000000", "--samp_rate", "250000"]
```

---

### C.1.3 BBU

The BBU has two components: \* LoRa\_Decoder: receives a stream of IQ samples from the RRH, decodes the LoRa signal and sends the decoded message out on a UDP socket  
 \* LoRa\_Network\_Server: receives the messages from that UDP socket and, depending on message content, streams response IQ samples to the RRH or does not give a response

In the BBU directory run:

```
docker-compose up
```

This starts both components of the BBU

## Params

The LoRa\_Decoder has the following params:

Usage: zero\_mq\_split\_b.py: [options]

Options:

```
-h, --help          show this help message and exit
--bandwidth=BANDWIDTH
                    Set bandwidth [default=125000]
--capture-freq=CAPTURE_FREQ
                    Set capture_freq [default=868.5M]
--decoded-out-port=DECODED_OUT_PORT
                    Set decoded_out_port [default=40868]
--samp-rate=SAMP_RATE
                    Set samp_rate [default=1.0M]
--spreading-factor=SPREADING_FACTOR
                    Set spreading_factor [default=12]
--zmq-address-iq-in=ZMQ_ADDRESS_IQ_IN
                    Set zmq_address_iq_in [default=tcp://127.0.0.1:5051]
```

Param	Explanation
bandwith	The bandwidth in Hz of the LoRa signal. Default is 125000.
capture-freq	The frequency in Hz of the LoRa signal. The RRH of course must also listen on this frequeny. Default is 868500000.



Param	Explanation
decoded-out-port	On which port the decoded messages will be sent out. Localhost only. The LoRa_Network_Server needs to be configured to listen on this port. Default is 40868.
samp-rate	How many samples per second to expect from the RRH. Default is 1000000
spreading-factor	The spreading factor of the incoming LoRa signal. From [7-12] inclusive. Default is 12

Param	Explanation
<code>-zmq-address-iq-in</code>	ZMQ address to which the BBU subscribes to receive an IQ samples stream (from the RRH) to decode. Default value is <code>tcp://127.0.0.1:5051</code> meaning the IQ samples are expected to come from localhost on port 5051. Normally RRH and BBU are on different devices but on the same network

The `LoRa_Network_Server` has the following params:

```
usage: lora_socket_server.py [-h] [-o OUT_PORT] [-i INPUT_PORT]
```

Connect to udp port for receiving decoded LoRa signals, if an ACK is required publish ACK iq samples via zmq socket for Remote Radio Head to receive and send out (TX).

optional arguments:

```
-h, --help          show this help message and exit
-o OUT_PORT, --out-port OUT_PORT
                    zmq port to publish downstream (i.e ACK) iq samples
                    (default: 5052)
-i INPUT_PORT, --input-port INPUT_PORT
                    UDP port to connect for receiving decoded lora
                    messages (default: 40868)
```

Param	Explanation
out-port	Publish the response IQ samples on all interface on this port. Default is 5052. (The response is 3 bytes long ("ACK") and SF 12. This is hardcoded for now)
input-port	UDP port to receive the decoded messages sent by the LoRa_Decoder. Default is 40868

To pass the parameters you have to specify them in the docker-compose.yml file.

Example:

To have the LoRa\_Decoder send the decoded messages out on port 30300 and the Lora\_Network\_Server to listen on port 30300 accordingly pass the arguments like below to the respective command field:

*docker-compose.yml*

```
version: '3'
services:
  lora_decoder:
    build: ./LoRa_Decoder
    network_mode: host
    tty: true
    command: ["--decoded-out-port", "30300"]
  lora_network_server:
    build: ./LoRa_Network_Server
    network_mode: host
    tty: true
    command: ["--input-port", "30300"]
```

### C.1.4 LimeSDR

- Plug in the antennas on the LimeSDR board on *RX1\_L* and *TX1\_1*

### C.1.5 Help

- LimeSDR calibration/gain error:
  - Download LimeSuite Toolkit to calibrate the LimeSDR
  - LimeSDR find device serial:
  - With LimeSuite installed run *LimeUtil -find*
  - Or run *lsusb -v* and look for the LimeSDR device
- 

## C.2 Arduino

The `arduino-lmic` library is required [Instructions here](#)

1. Go to the arduino directory.
2. Compile and upload the code to the arduino
3. The arduino runs the protocol in the manner described at the beginning.
4. It send packets with SF9 and expects the ACK response to be SF12 as well.
5. After 3 packets the arduino has finished.
6. Look at the Serial output for details. Baud rate 9600

### Info

PlatformIO was used to compile and upload the image to the arduino.

---

### C.2.1 Manual installation Ubuntu

Visit [this guide](#) for installing LimeSDR Plugin for GNU Radio for more detail. This guide only has the short version.

Install dependencies for signal processing:

```
sudo apt-get update && sudo apt-get install -y gnuradio=3.7.11-10 libboost-all-dev s
libcppunit-1.14-0 libfftw3-bin libvolk1-bin liblog4cpp5v5 python libliquid1d libliqu
&& pip install numpy && pip install scipy
```

Install LimeSuite

```
sudo add-apt-repository -y ppa:myriadrfr/drivers && sudo apt-get update \
&& sudo apt-get install -y limesuite liblimesuite-dev limesuite-udev limesuite-image
soapysdr-tools soapysdr-module-lms7
```

Clone and install LimeSDR Plugin for GNU Radio:

```
git clone https://github.com/myriadrfr/gr-limesdr && cd gr-limesdr && mkdir build &&
```

Clone and install rpp0's LoRa decoder for gnuradio

```
git clone https://github.com/rpp0/gr-lora.git && cd gr-lora && git checkout b1d38fab
&& mkdir build && cd build \
&& cmake .. && make && sudo make install \
&& cd .. && rm -rf build \
&& git checkout -b encoder origin/encoder && git checkout 3c9a63f1d148592df2b715496
&& mkdir build && cd build \
&& cmake .. && make && sudo make install && sudo ldconfig
```

With pip for python2 install the zmq package:

```
pip install pyzmq==18.1.0
```

Then open the *zero\_mq\_split\_a.grc* and the *zero\_mq\_split\_b.grc* file in the docker/RRH directory resp. in the docker/BBU/LoRa\_Decoder directory. Or run the *zero\_mq\_split\_a.py* resp. the *zero\_mq\_split\_b.py* script in those directories with your shell. Also run the *lora\_socket\_server.py* script inside docker/BBU/LoRa\_Network\_Server with your shell.

## C.3 Tools

In the tools directory in the Encode and Decode directory are multiple useful scripts for encoding and decoding lora without gnuradio

1. First, after you recorded a signal trim the signal with a tool like audacity. Else if you want to visualize it with *plot\_signal.py* the signal is shrunk too much to make it fit in the plot.

2. After trimming, channelize the signal else the decoder cannot properly decode the signal. Run `channelizer.py -h` to see the options. It takes an signal recording via the `-input-file` option and outputs the channelized file as “channelized.raw”. Don’t forget to specify bandwidth and sample rate if they differ from the set default values.
3. The channelized signal can the be passed to the decoder. The decoder prints out the decoded signal and generates a csv file (`words.csv`) containing the words at each sample. Don’t forget to specify bandwidth and sample rate etc if they differ from the set default values.
4. This csv file can be passed to `plot_signal.py` which draws the signal and the words in the csv file to a pdf (`rawframe.pdf`). Don’t forget to specify bandwidth and sample rate if they differ from the set default values.

Use the encoder to generate samples for the `test_packet[] uint8` array in the code. The samples are written to the fiel “output.bin”

Use the two scripts `decoder_build.sh` and `encoder_build.sh` to compile the `encode.cc` and `decode.cc` files.

Use VsCode to open the directory “Encode and Decode” to have predefiend debug configurations. The folder ‘.vscode’ has been committed in this repo.

All recorded uplink signals have been recorded with sample rate 1Million and transmitted with a bandwidth of 125’000

The decoder only works for signals with an explicit header.