EUROPEAN UNION

Interreg
EUROPEAN UNION
Austria-Czech Republic
European Regional Development Fund

ATCZ175 InterOP

Analysis of Interfences in LoRa communication

SIX Research Centre
Brno University of Technology

18.12.2020

SIX
RESEARCH CENTRE
SENSOR, INFORMATION AND COMMUNICATION SYSTEMS

Table of content

1 Scope of the document

The extensive development of LoRa networks in recent times has led to the research task of creating a traffic sniffer for long term LoRa/LoRaWAN network monitoring. This report deals with the description of its concept and especially the analysis of data obtained from two localities. Long-term monitoring took place in Brno, additional data from a low-traffic locality were obtained in Trebic. A complete archive of data in SQL database format is attached to this document[1] to allow further investigation and validation by independent researchers.

[1] http://www.radio.feec.vutbr.cz/interop/lora/

2 Measurement setup

The basic concept of result analysis is based on the work from Master's thesis involved in the InterOP project[2]. However, instead of using a custom 1-channel receiver with parameter switching as described in the thesis, we have developed a new setup consisting of two fully equipped LoRa gateways (IMST iC880A[3] + RPi3), placed in a roof box, running poly packet forwarder:

- GW #919: public LoRa prefix, forwarding packets to TheThingsNetwork[4] and our server
- GW #920: private LoRa prefix, forwarding only to our server

The custom server is based on RPi4 with external SSD drive for database storage. It is running a custom version of util_ack script (UDP server) to receive all packets from gateway packet forwarders and store them into MariaDB SQL database backend.

Public LoRaWAN gateway can be optionally connected to TheThingsNetwork. This setup is occasionally used for students working on their bachelor or master theses.

The following sections evaluate the parameters of received packets (frequency, spreading factor, bandwidth, coding rate, RSSI, SNR etc.), as well as LoRaWAN unencrypted MAC layer statistics.

Fig. 1: Components inside the LoRa sniffer box

[2] Jerabek, O.: Signalova analyza LoRa s vyuzitim SDR, Master's thesis, Brno Univ. of Technology, 2019. Available at: https://www.vutbr.cz/studenti/zav-prace/detail/118447

[3] https://shop.imst.de/wireless-modules/lora-products/8/ic880a-spi-lorawan-concentrator-868-mhz

[4] https://www.thethingsnetwork.org/

3 LoRa traffic analysis: Brno

The sniffer box has been placed on the roof of Dept. of Radio Electronics, Technicka 12, Brno. Short period of measurements was also taken from a lab inside the building, close to the window.

Fig. 2: Sniffer placement at DREL

Total packets processed: 1019606

Unique packets processed: 992738

Number of duplicate packets: 26868 = 2.7%

Private (LoRa) packets with valid CRC: 7807 = 0.8%

Public (LoRaWAN) packets with valid CRC: 313828 = 31.6%

Both private (LoRa) and public (LoRaWAN) packets with valid CRC: 348413 = 35.1%

Sniffer running period: 327 days

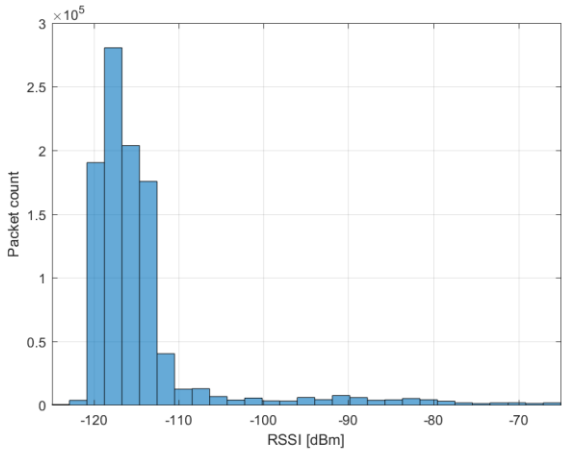
The following sections provide detailed statistics of the received packets.

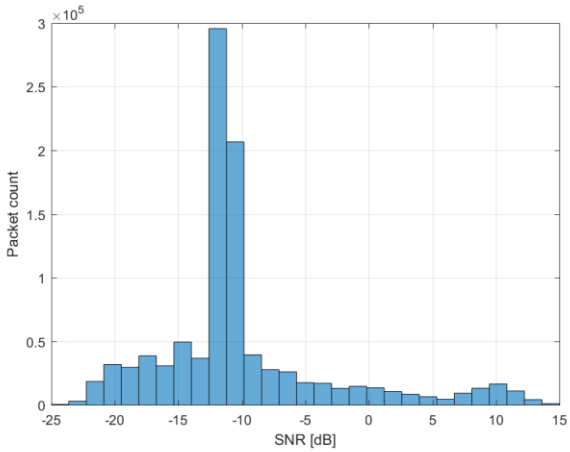
3.1 Analysis overview

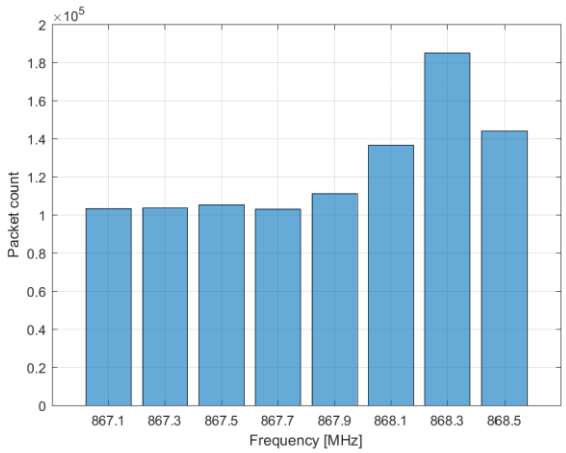
This overview summarises all received packets on both gateways. Only one packet is counted if received by both gateways as duplicate. CRC filtering is not applied, i.e. all received data are shown, both valid and invalid.

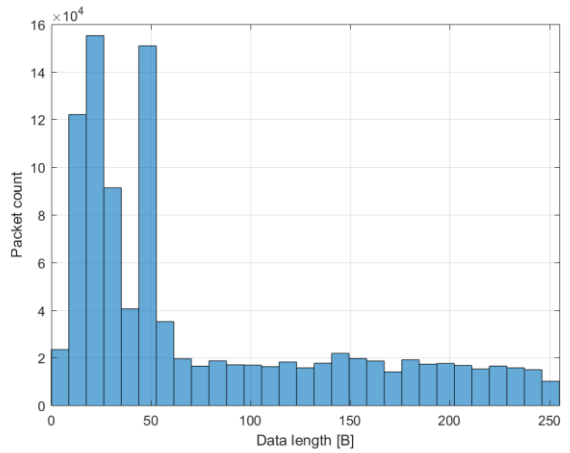
Data from rx41.csv file, SQL query:

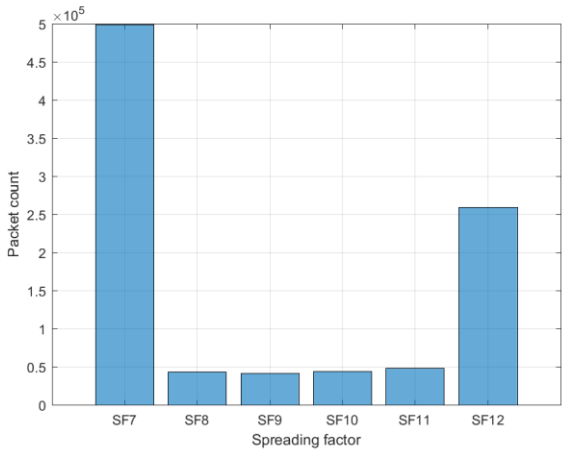
```
select id, freq, sf(datr), cr(codr), lsnr, rssi, size from rxpk4 where
(flag=919 or flag=920 or flag=119)
```

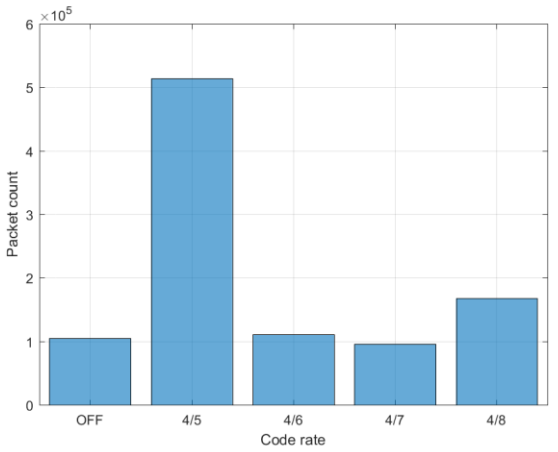




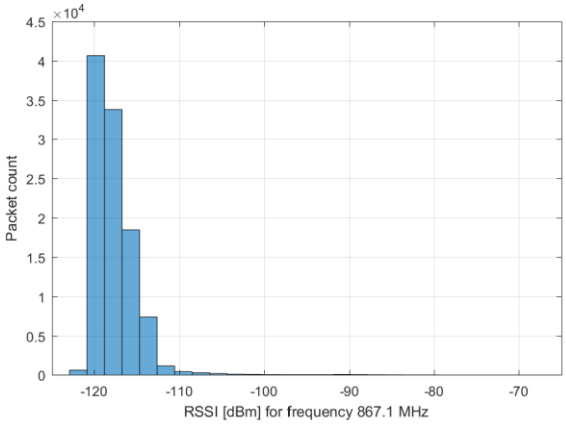


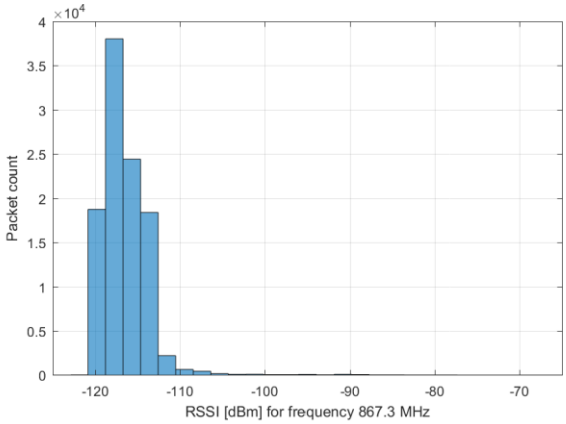


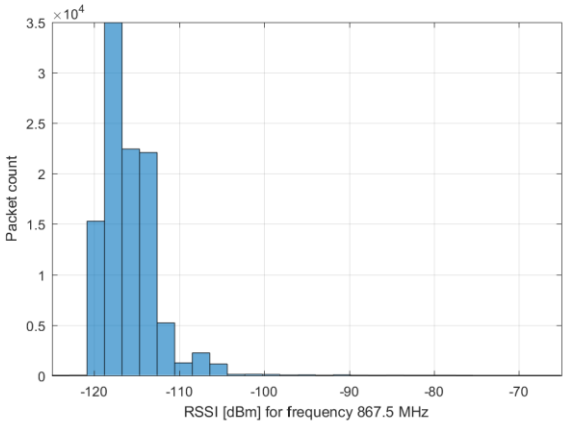


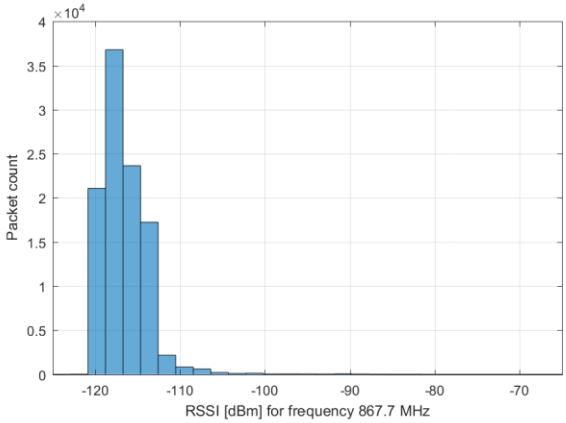


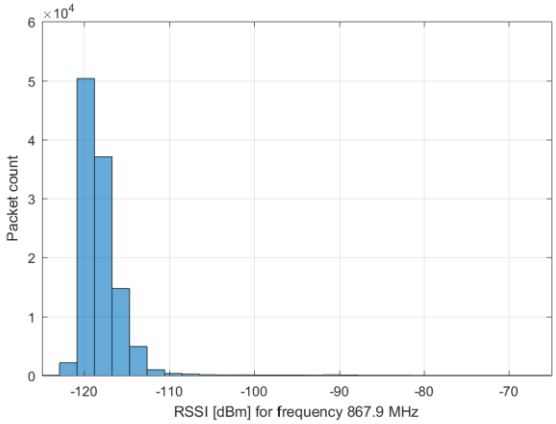
3.1.1 RSSI per channel

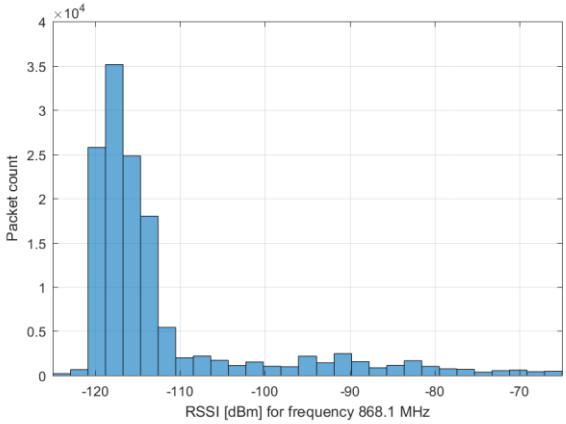


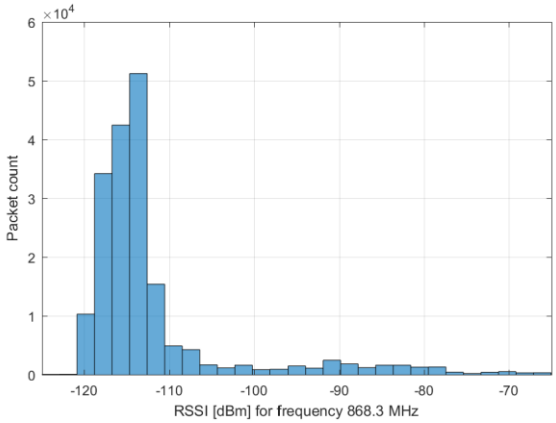


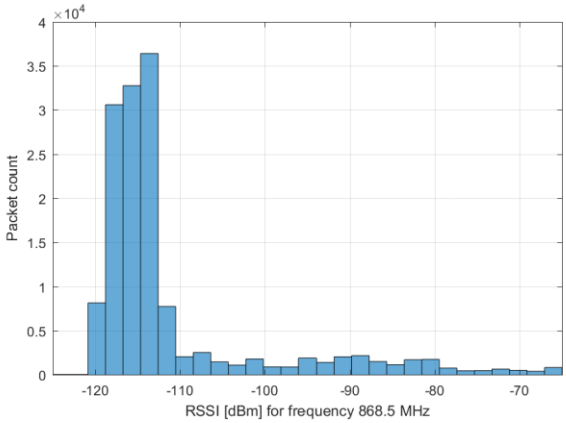




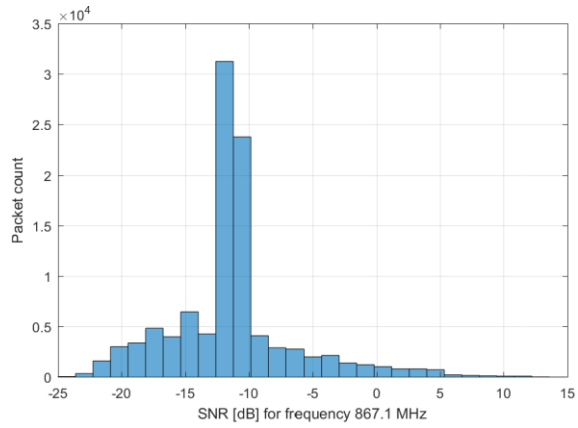


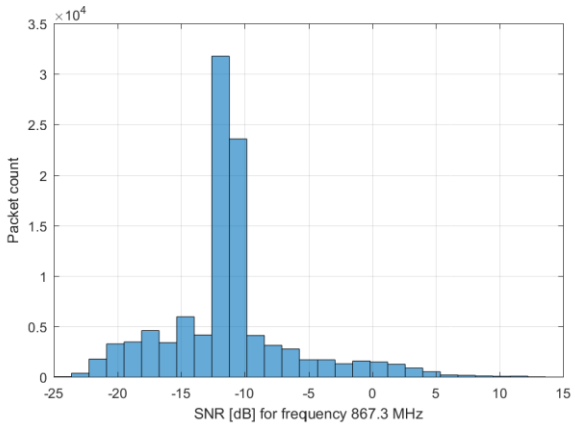


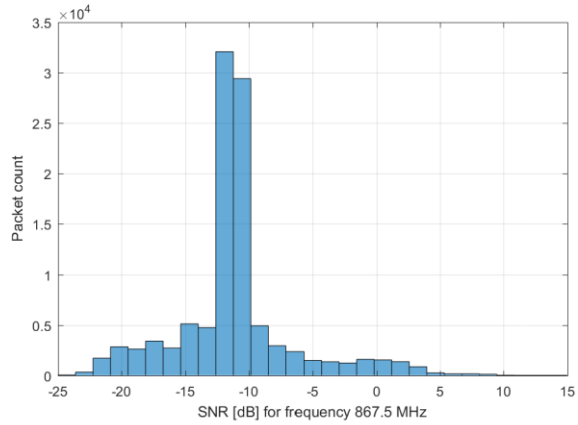


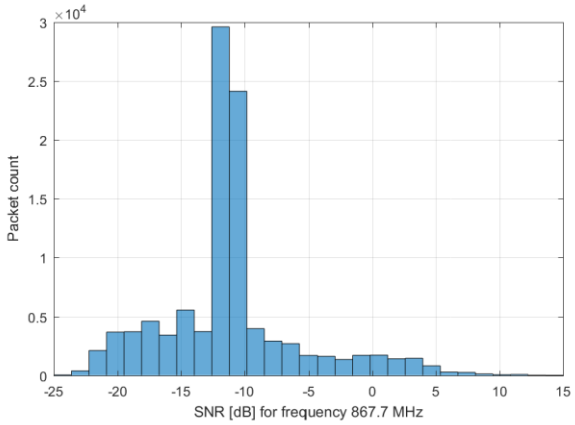


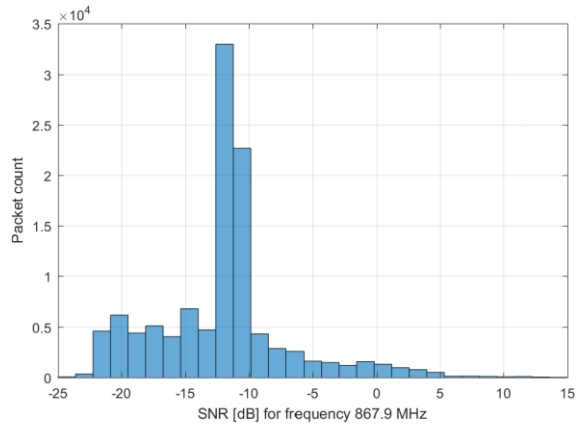
3.1.2 SNR per channel

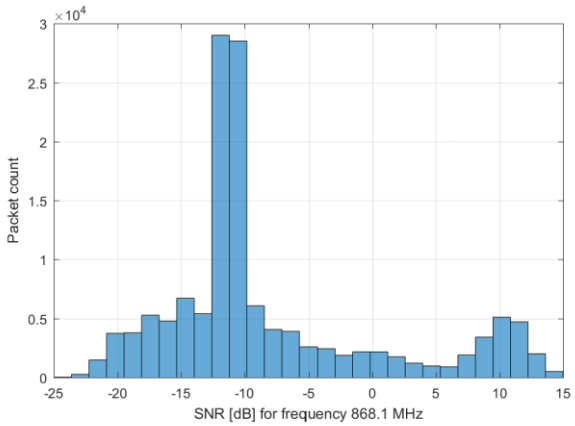


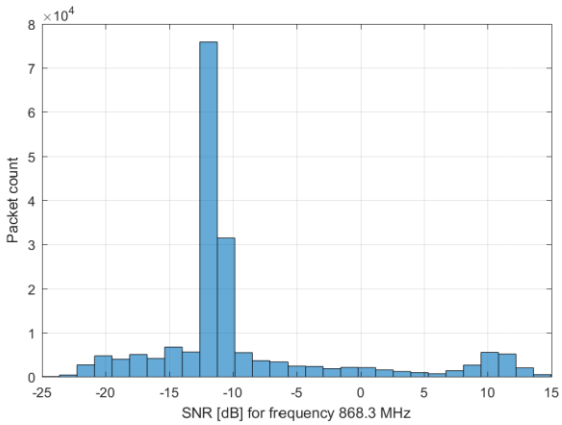


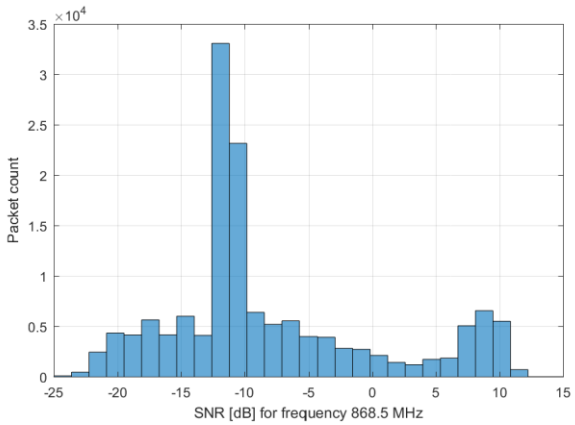










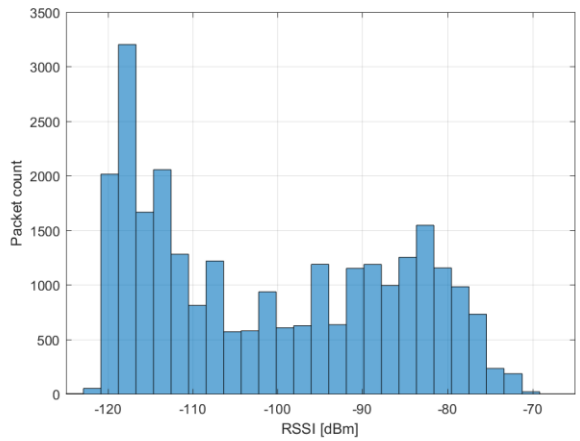


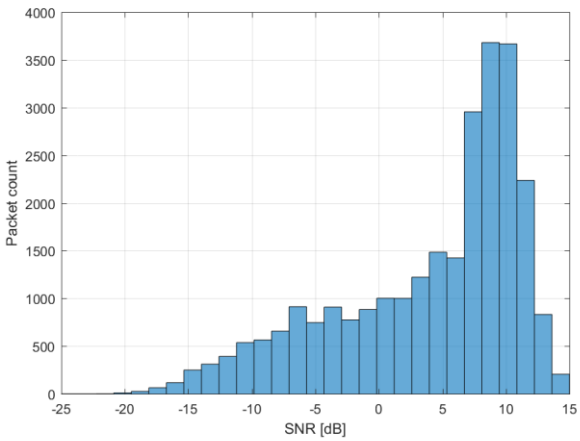
3.2 Duplicate packets

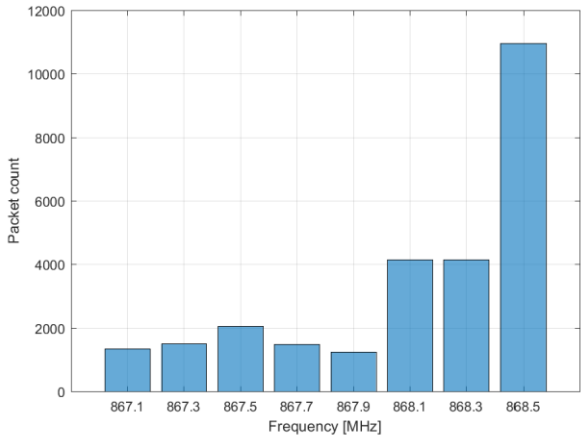
These packets have been received by both gateways. The sync word filtering as implemented in receiving chipset is not 100% reliable and some packets are accepted even with wrong sync word. This is the case especially for packets with high SNR.

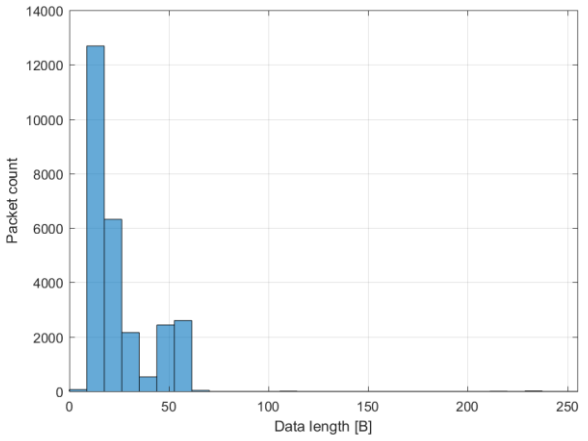
Data from rx42.csv file, SQL query:

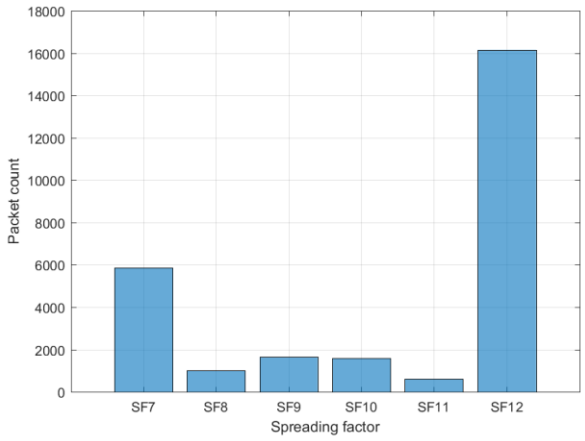
```
select id, freq, sf(datr), cr(codr), lsnr, rssi, size from rxpk4 where (flag=120)
```

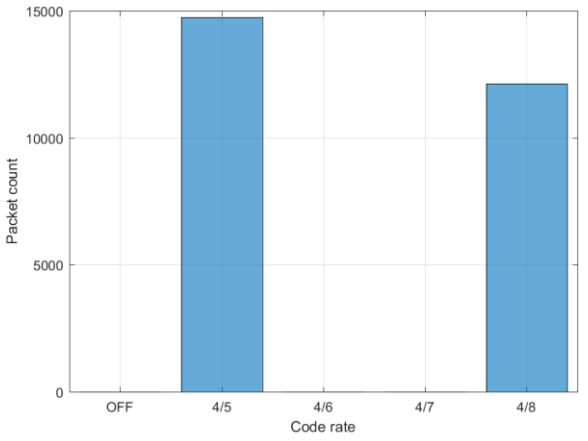




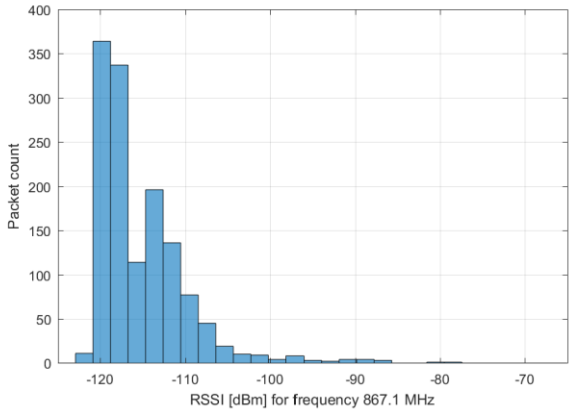


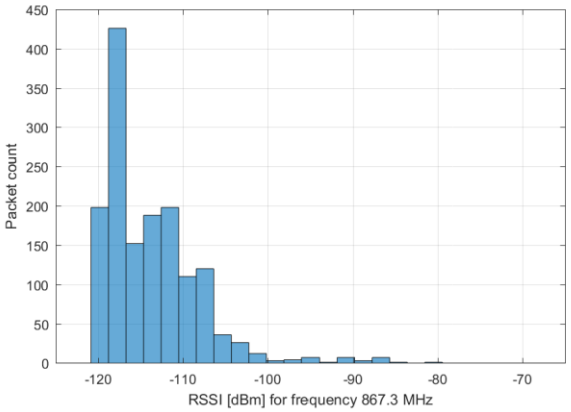


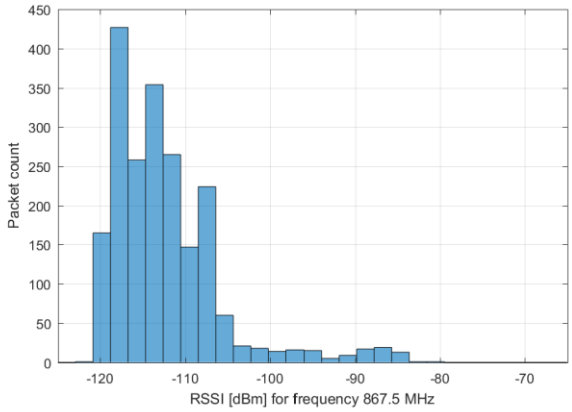


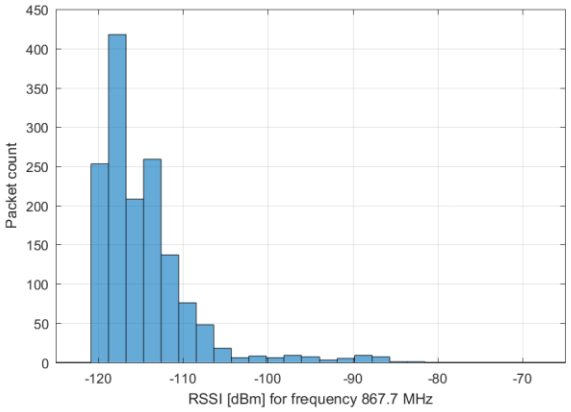


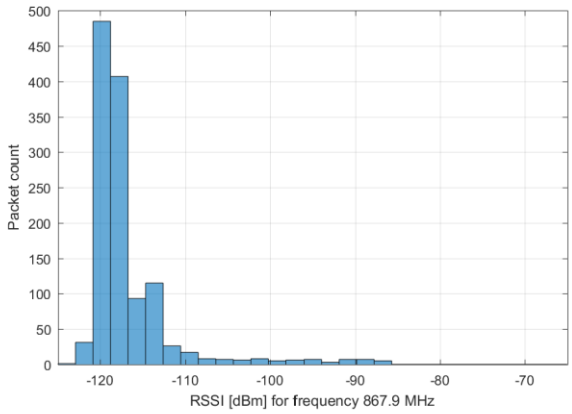
3.2.1 RSSI per channel

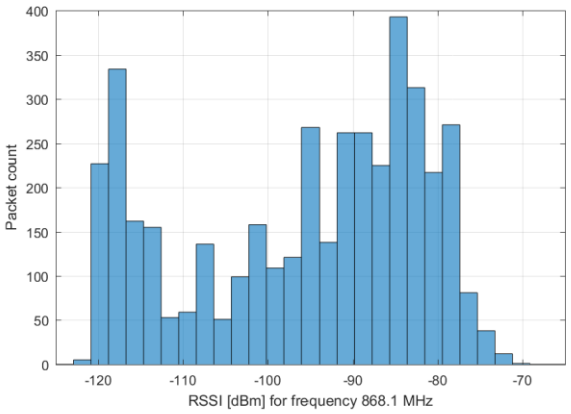


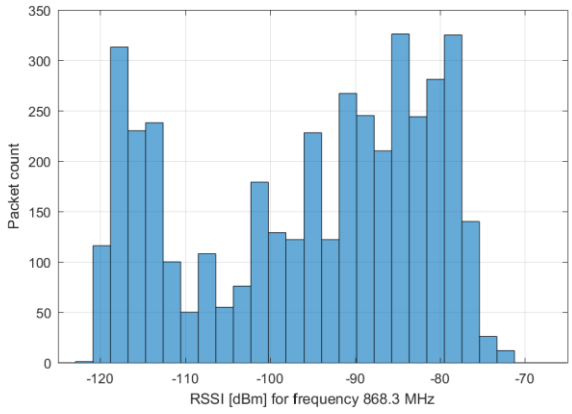


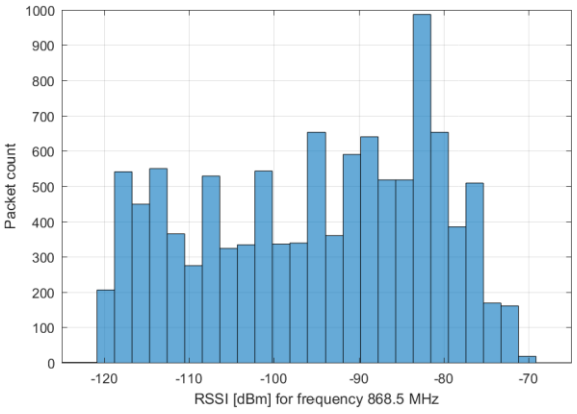




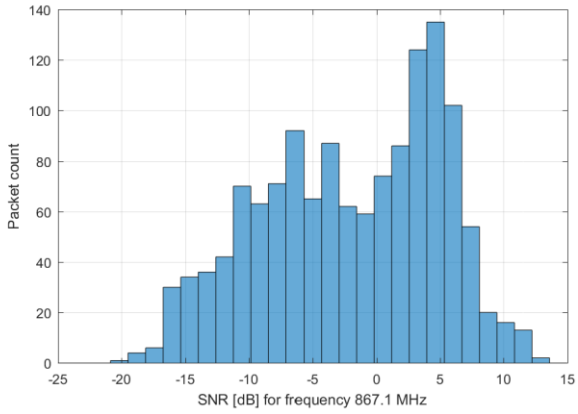


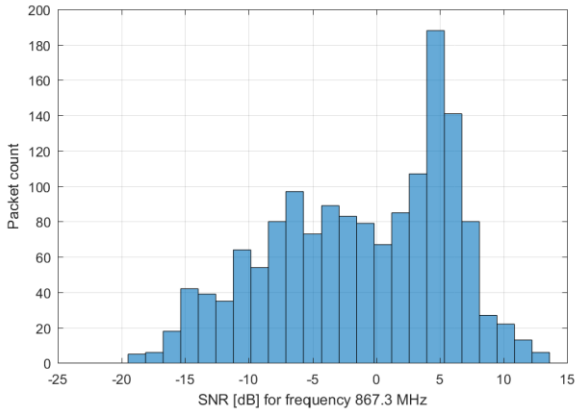


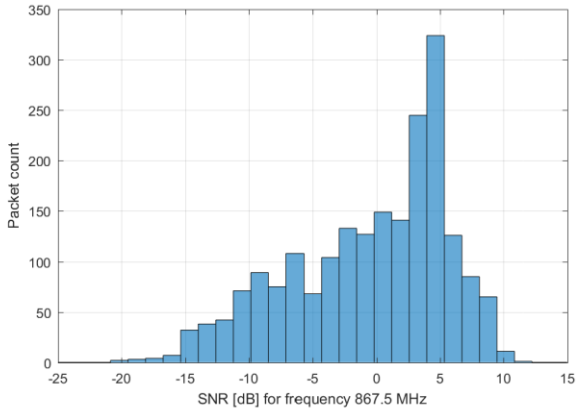


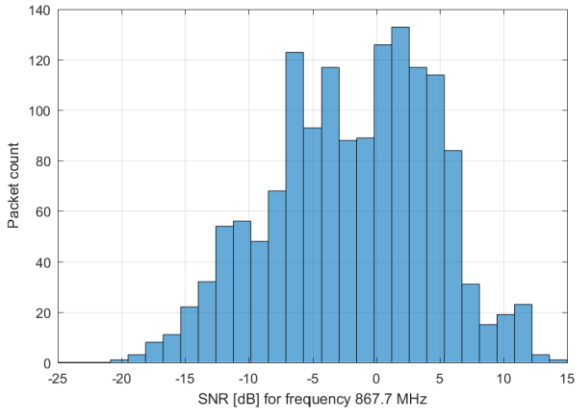


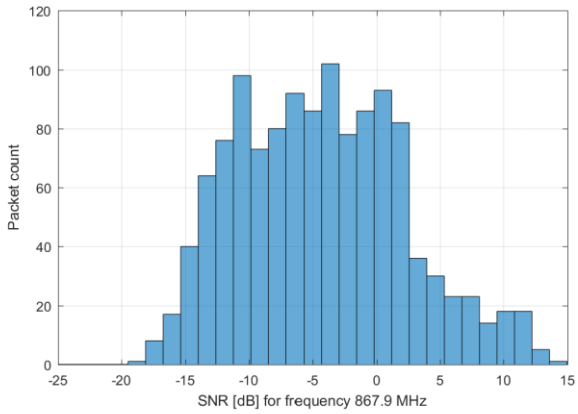
3.2.2 SNR per channel

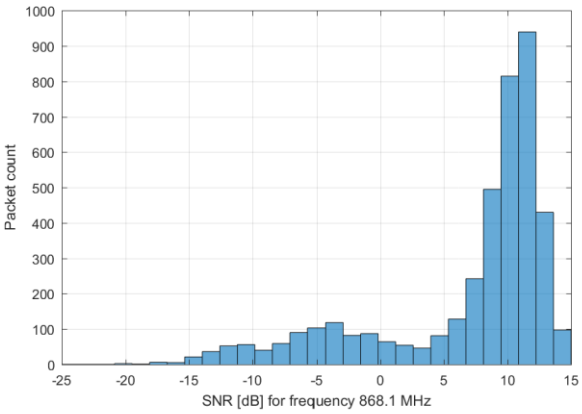


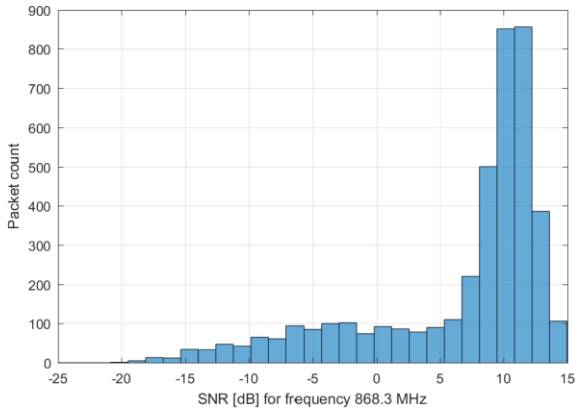


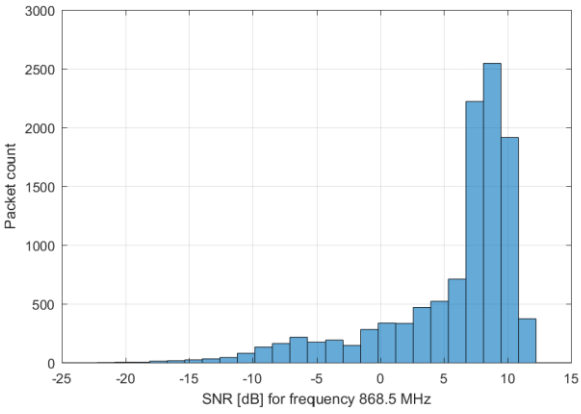










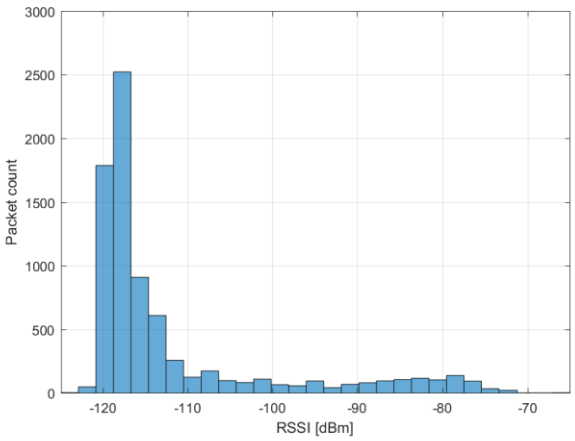


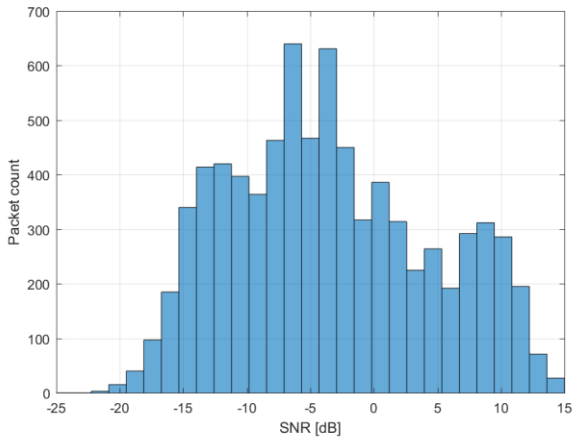
3.3 Private (LoRa) packets with valid CRC

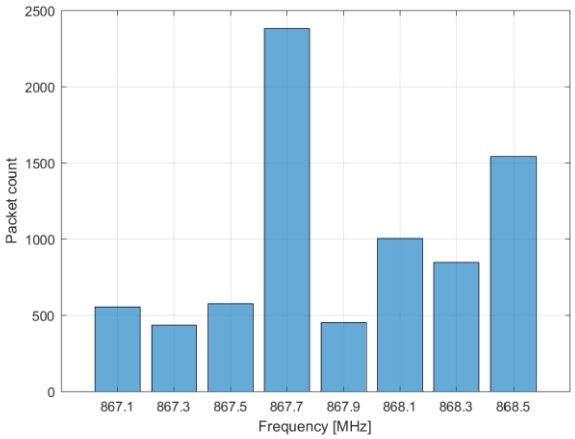
Following packets have been exclusively received by gateway with private sync-word. Only packets with valid CRC are shown.

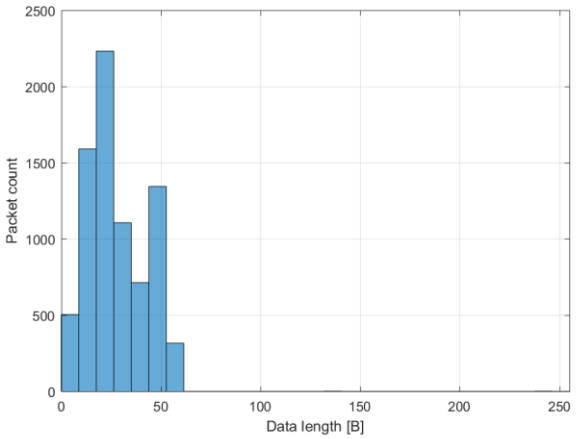
Data from rx43.csv file, SQL query:

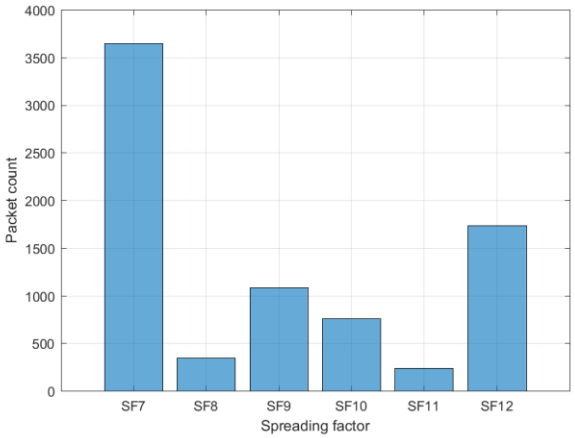
```
select id, freq, sf(datr), cr(codr), lsnr, rssi, size from rxpk4 where
(flag=920) and stat=1
```

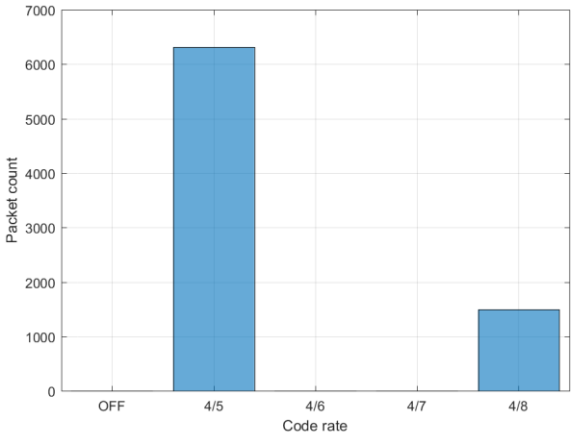




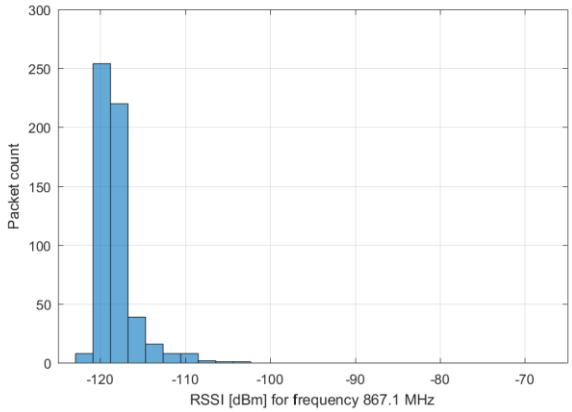


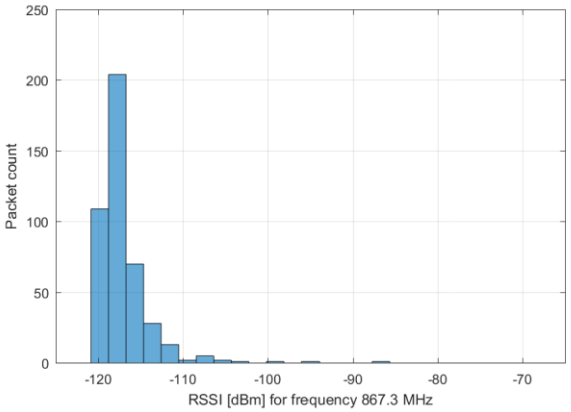


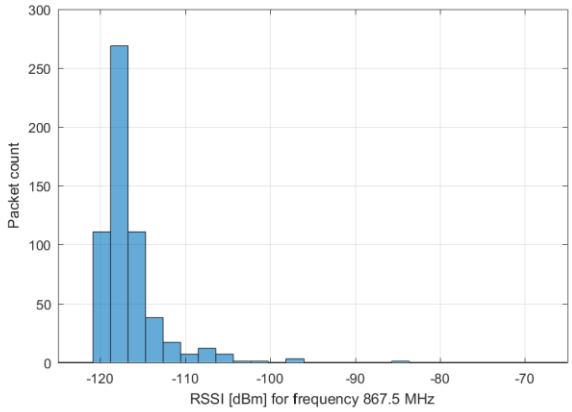


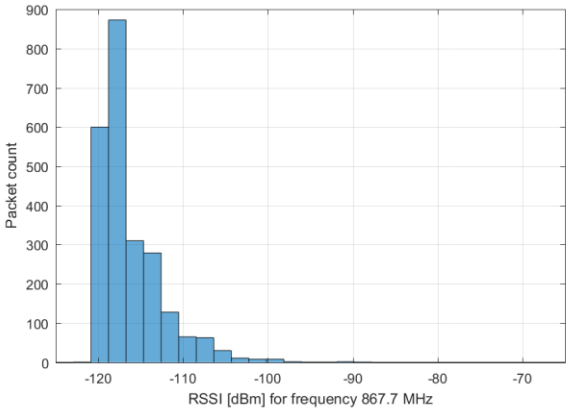


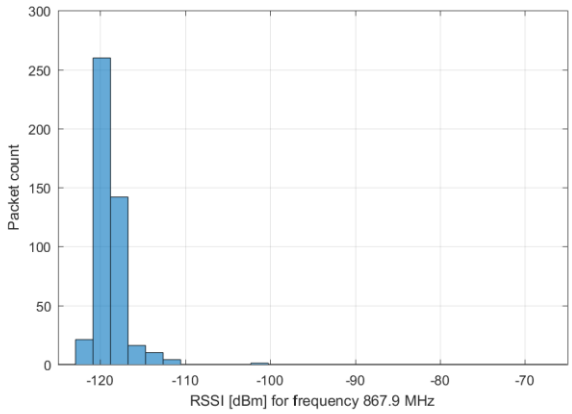
3.3.1 RSSI per channel

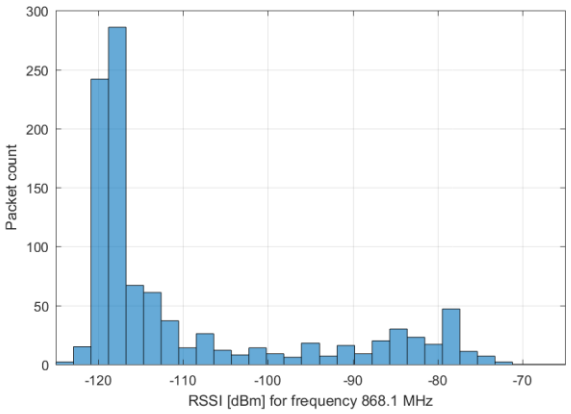


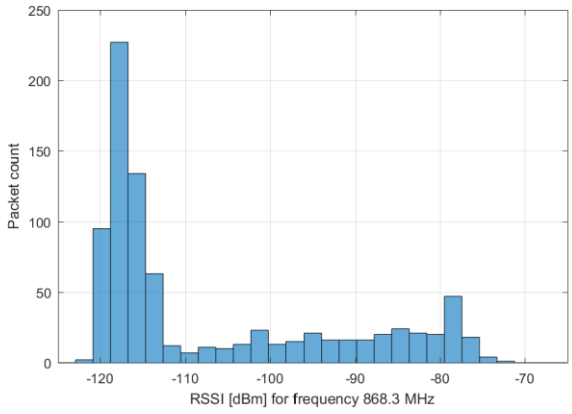


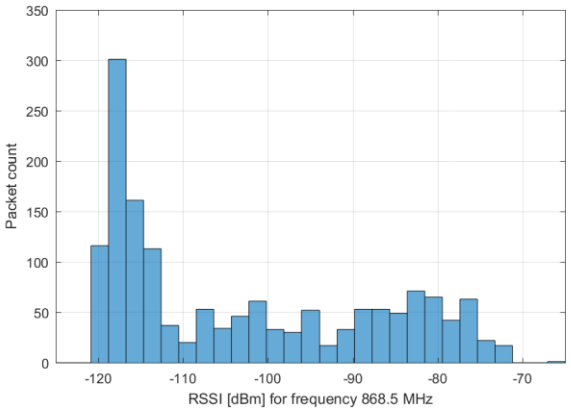




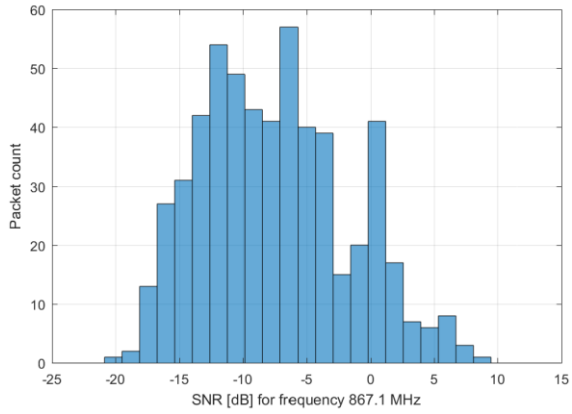


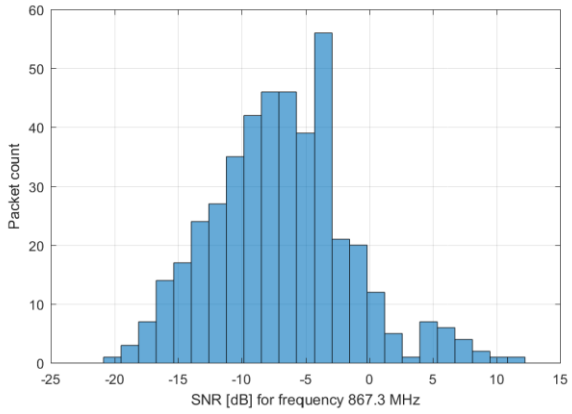


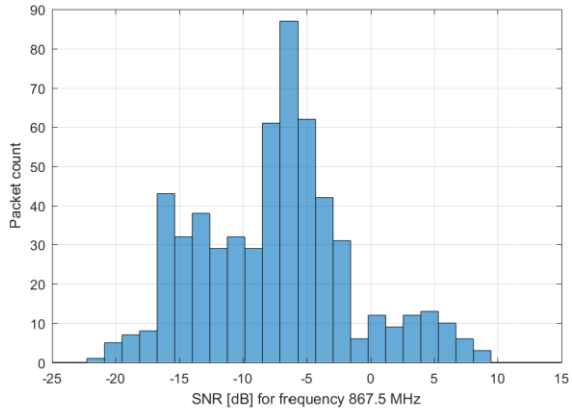


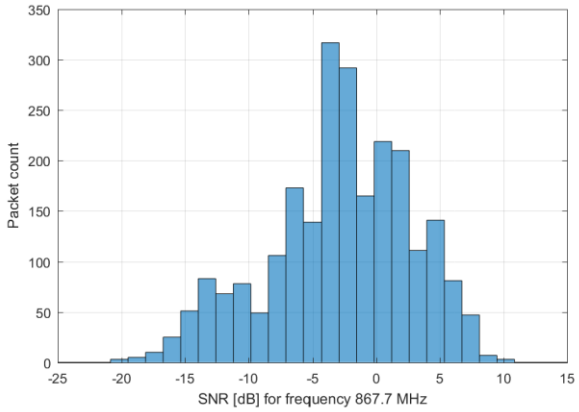


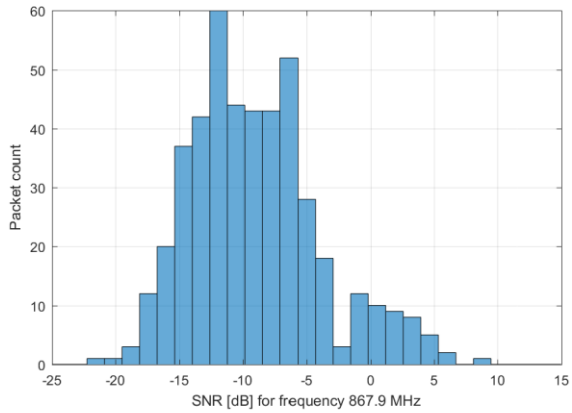
3.3.2 SNR per channel

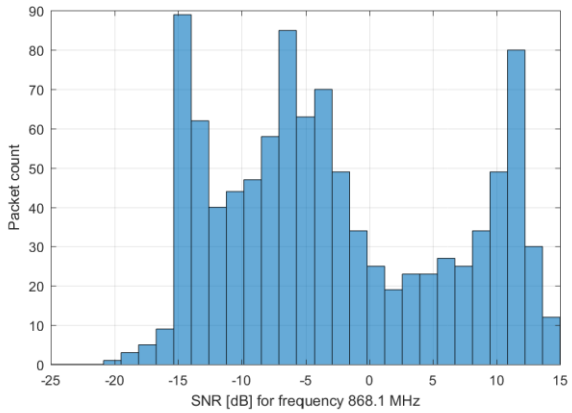


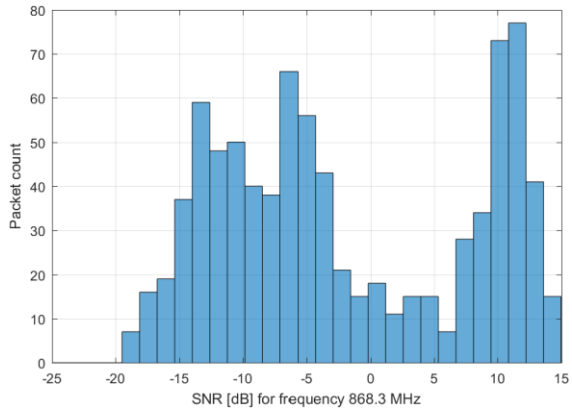


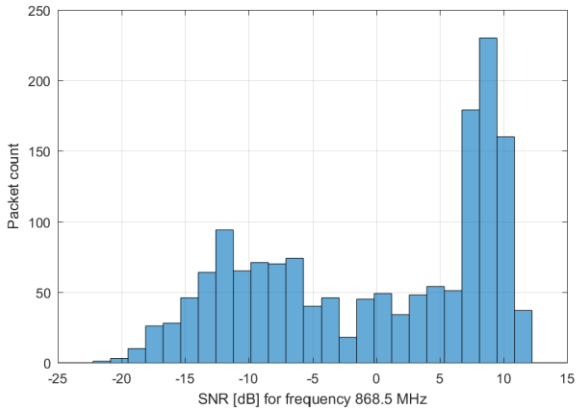










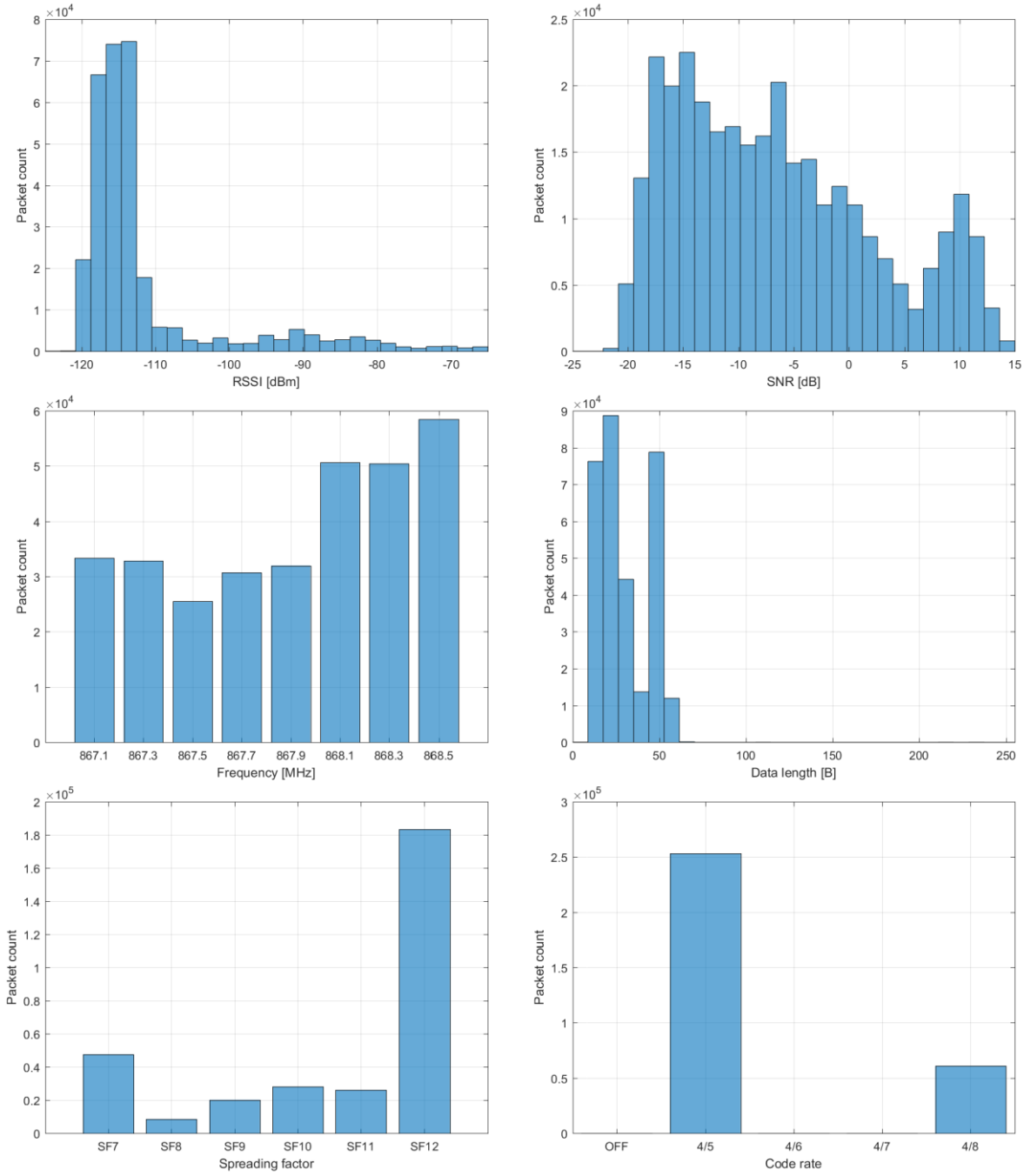


3.4 Public (LoRaWAN) packets with valid CRC

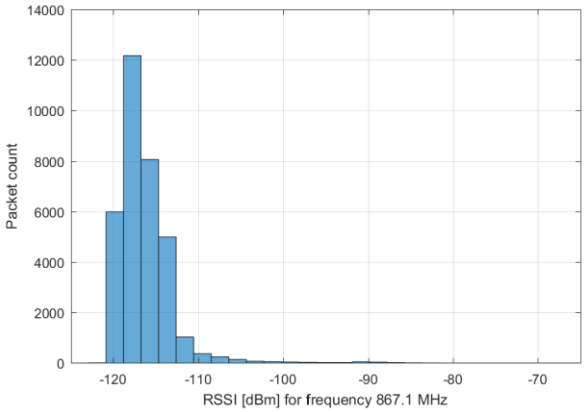
Following packets have been exclusively received by gateway with public sync-word. Only packets with valid CRC are shown.

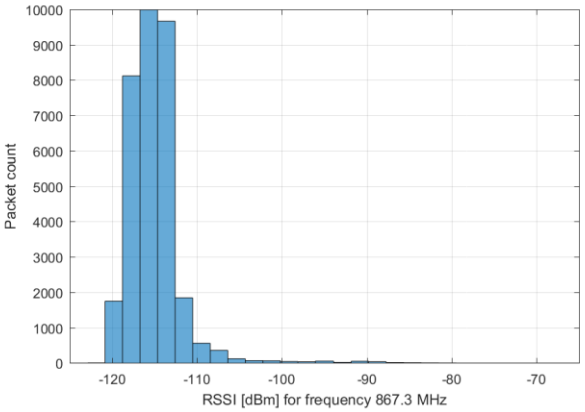
Data from rx44.csv file, SQL query:

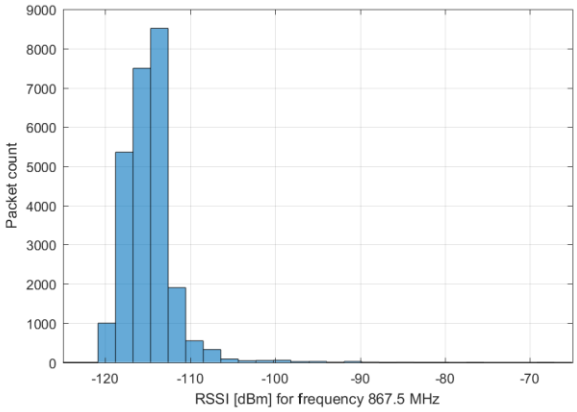
```
select id, freq, sf(datr), cr(codr), lsnr, rssi, size from rxpk4 where (flag=919) and stat=1
```

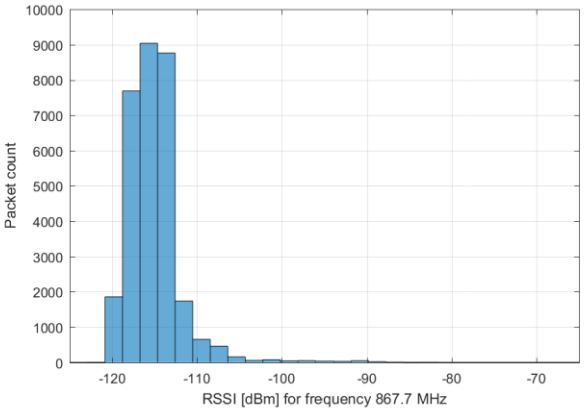


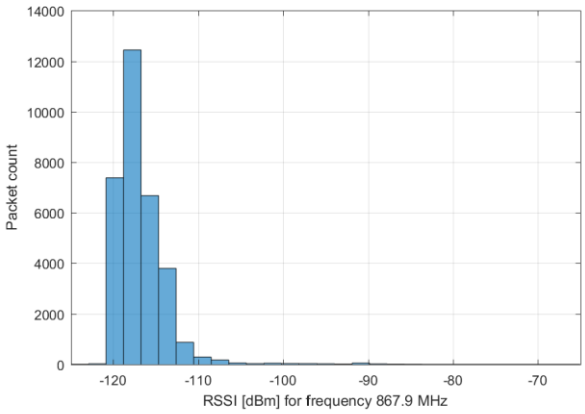
3.4.1 RSSI per channel

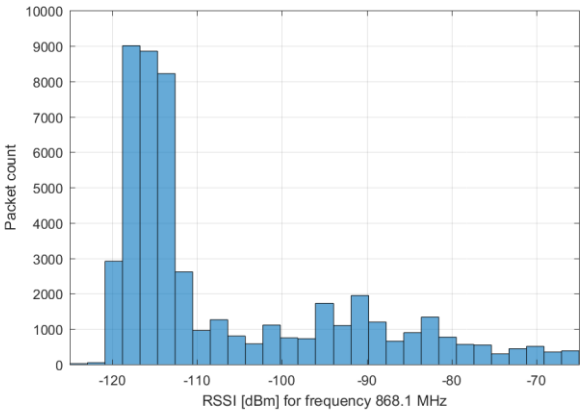


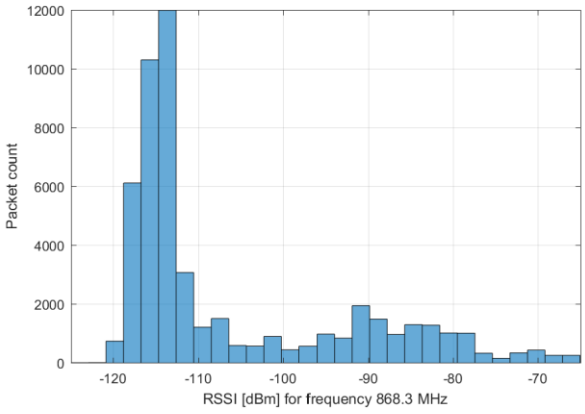


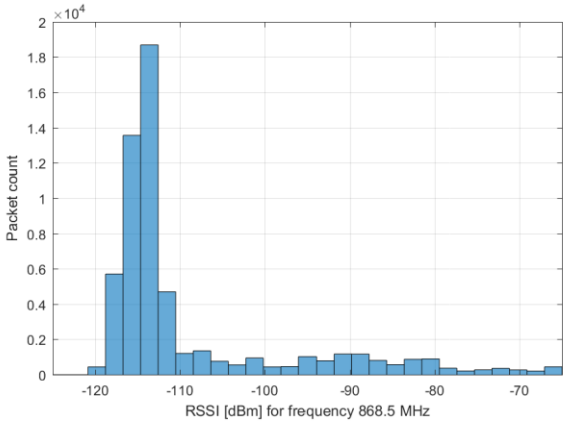




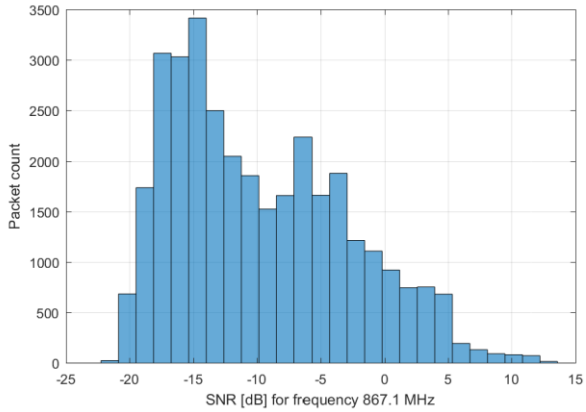


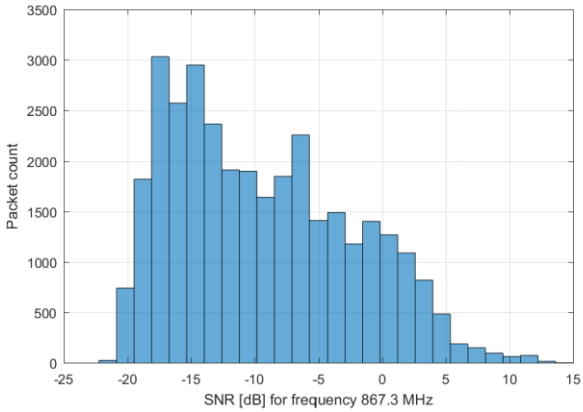


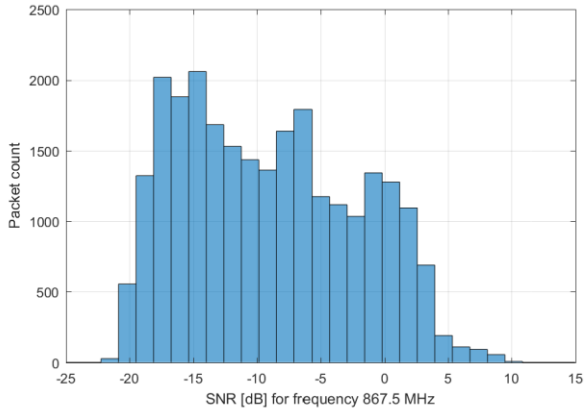


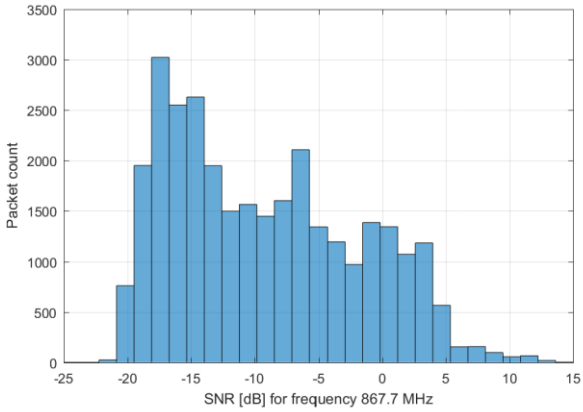


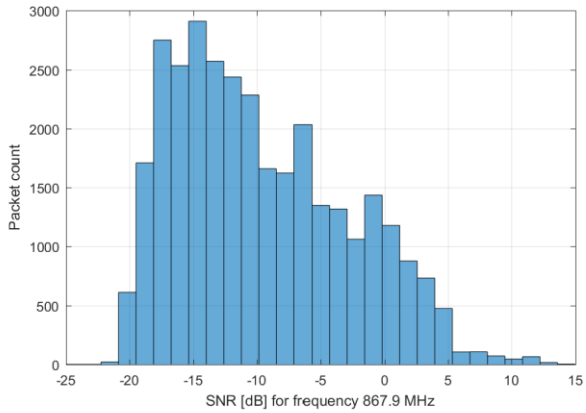
3.4.2 SNR per channel

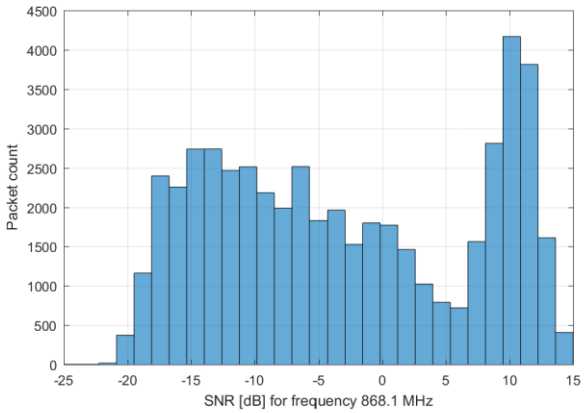


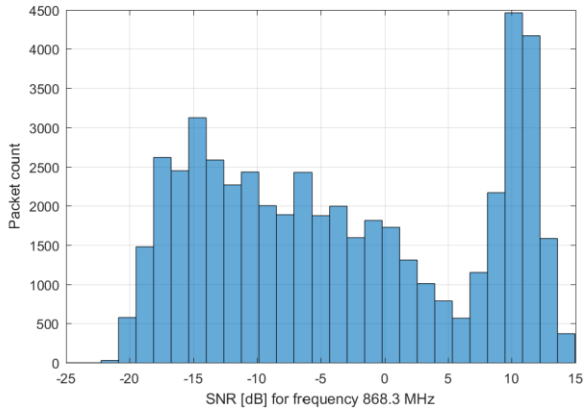


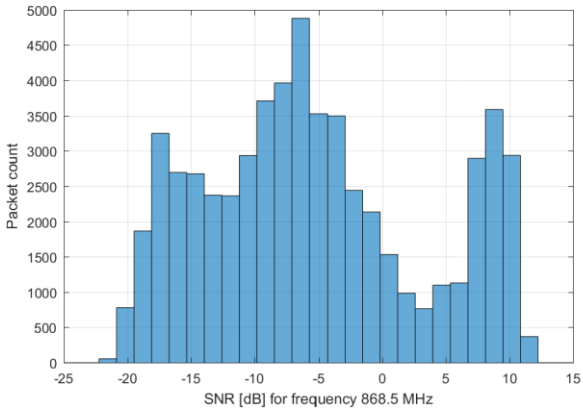










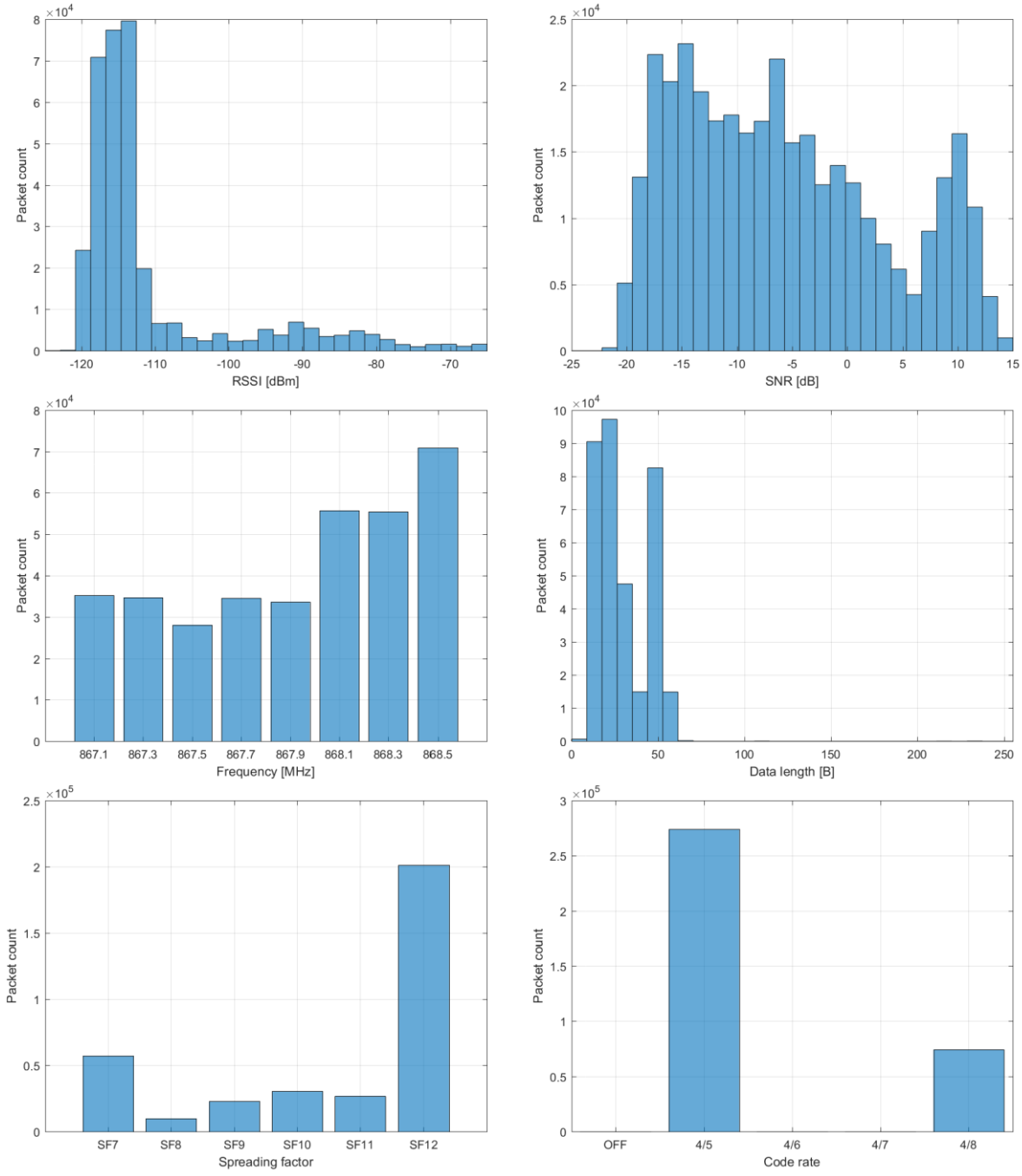


3.5 Both private (LoRa) and public (LoRaWAN) packets with valid CRC

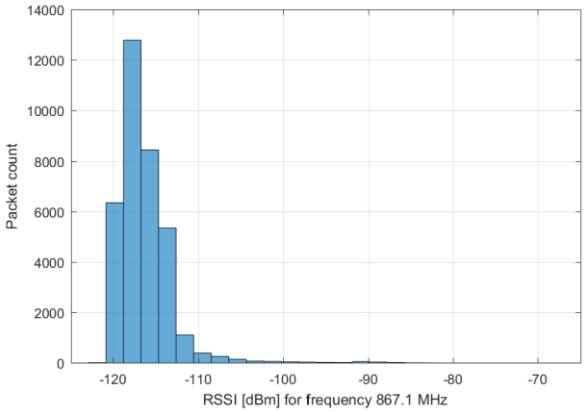
Following valid packets have been received by one of the gateways. Duplicates received by both gateways are counted only once. Only packets with valid CRC are shown.

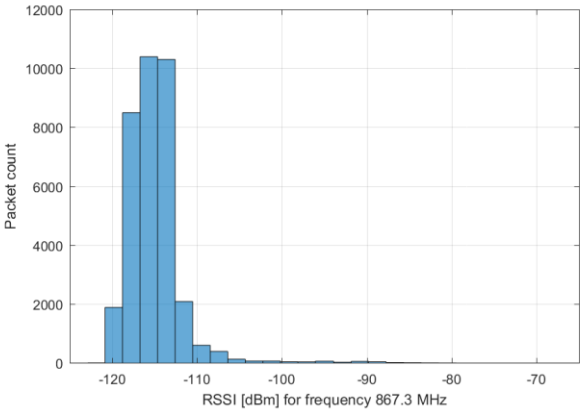
Data from rx45.csv file, SQL query:

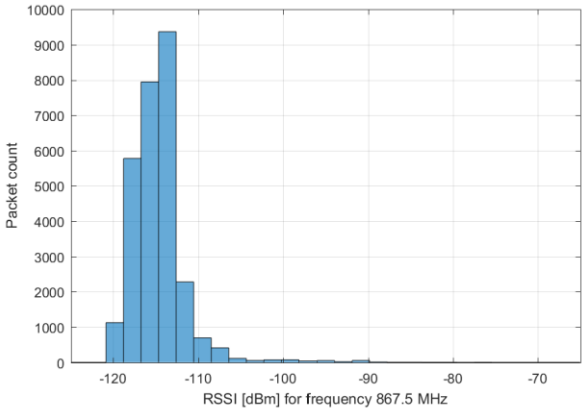
```
select id, freq, sf(datr), cr(codr), lsnr, rssi, size from rxpk4 where
(flag=919 or flag=920 or flag=119) and stat=1
```

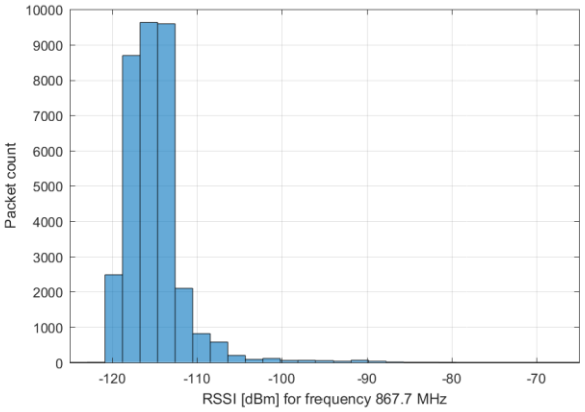


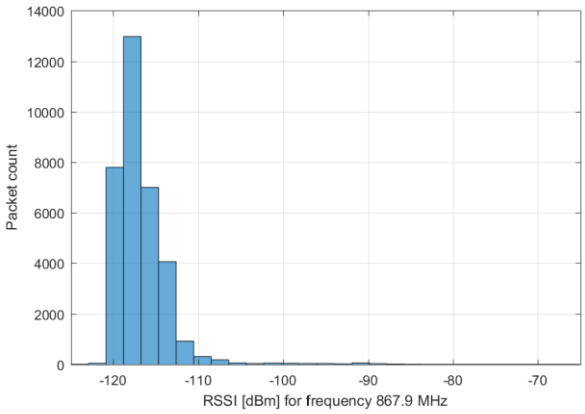
3.5.1 RSSI per channel

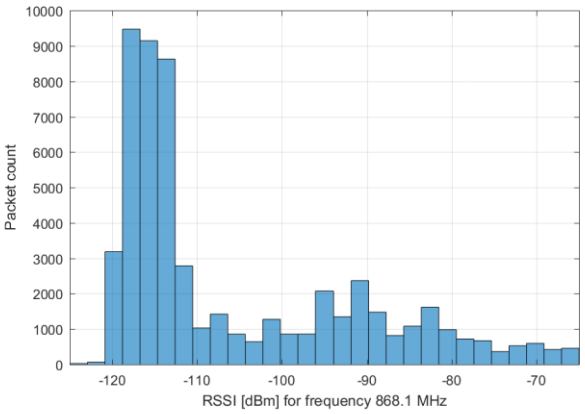


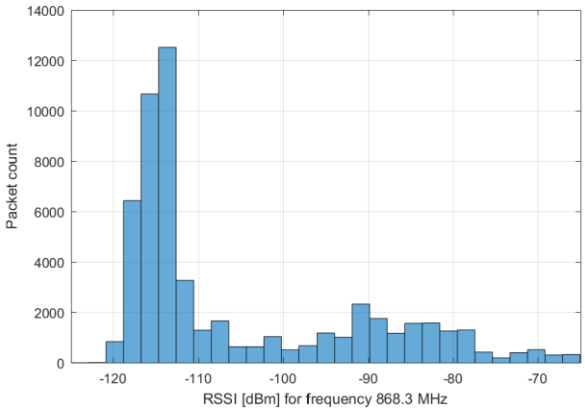


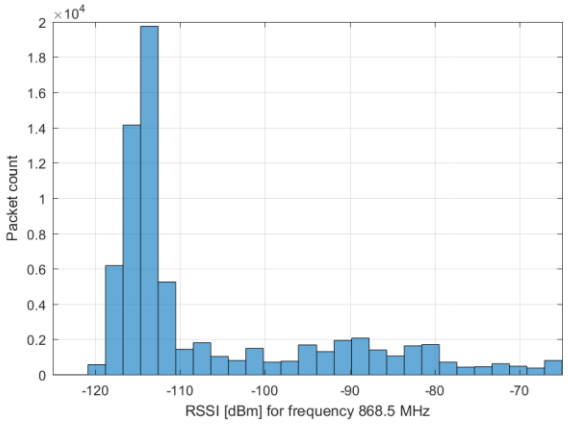




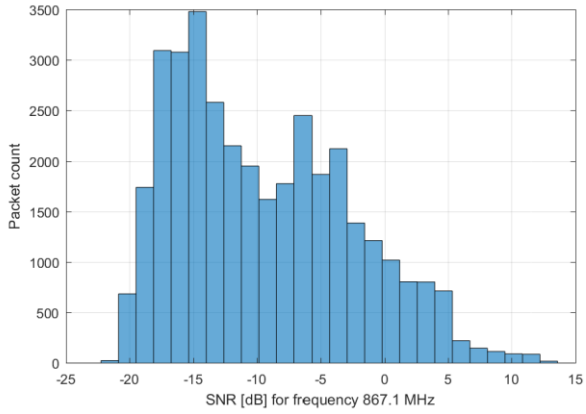


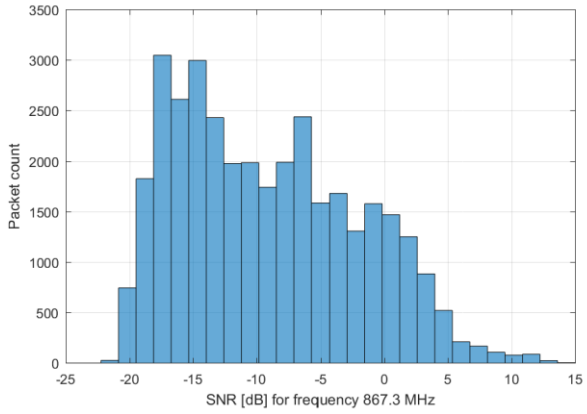


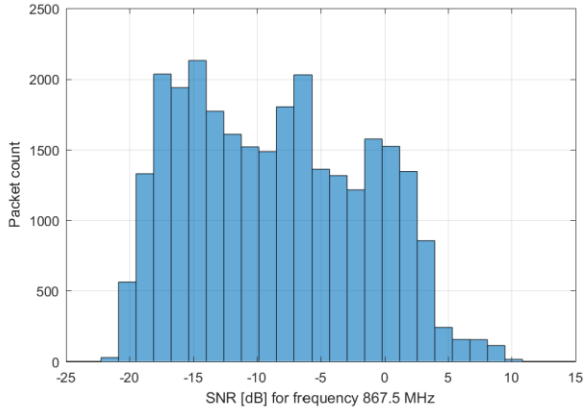


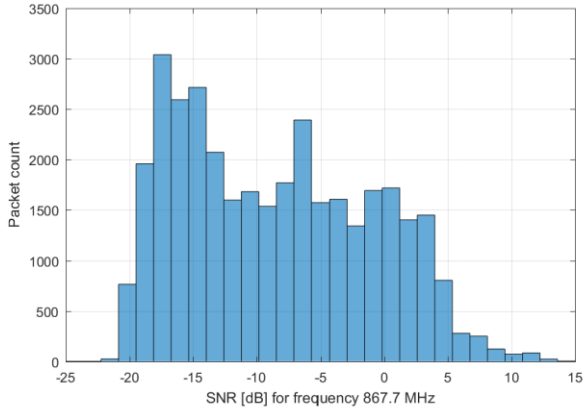


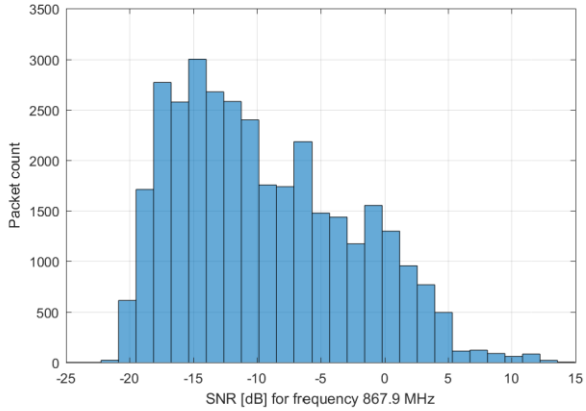
3.5.2 SNR per channel

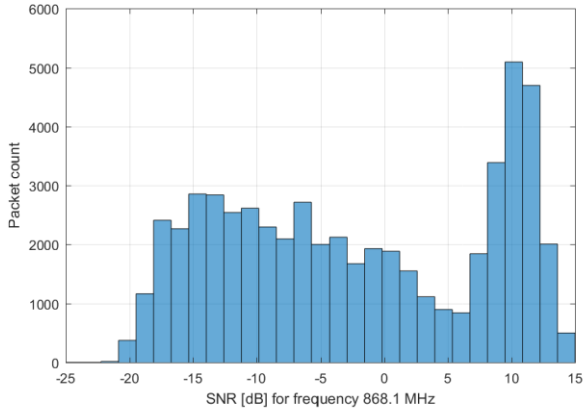


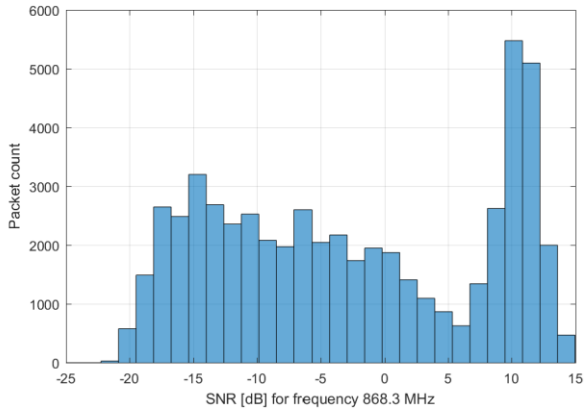


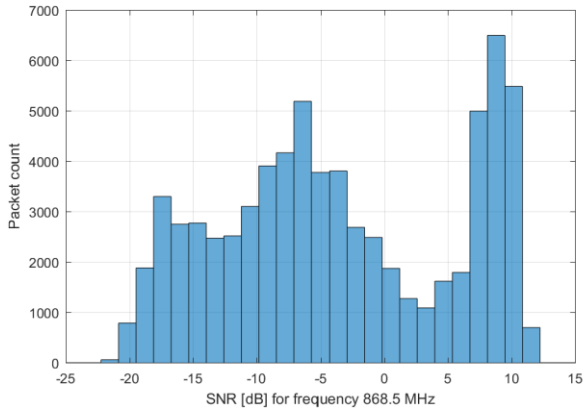










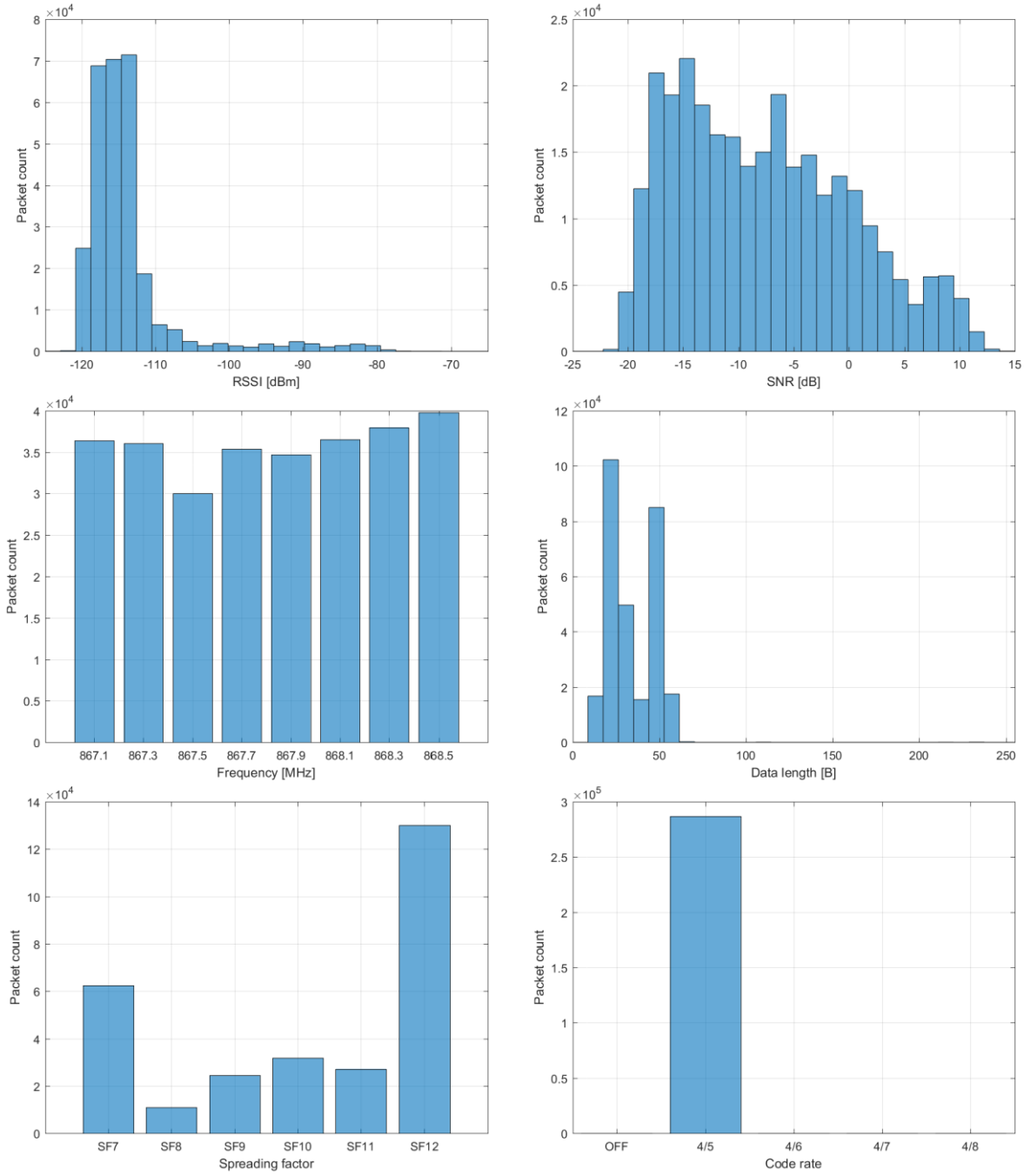


3.6 Valid LoRaWAN packets only

The following packets has been correctly decoded by LoRaWAN packet decoder. Together with verified CRC, there packet are considered as valid independently on receiving gateway.

Data from rx46.csv file, SQL query:

```
select id, freq, sf(datr), cr(codr), lsnr, rssi, size from rxpk4 where
(flag2<40) and stat=1
```



3.6.1 LoRaWAN MAC layer analysis

An extended analysis was performed on the LoRaWAN data. The individual types of messages were identified and their frequency determined:

Valid LoRaWAN packets only: 286867

Join Requests: 4484 = 1.6%

Join Accepts: 1

Data Up Unconfirmed: 239510 = 83.5%

Data Up Confirmed: 37480 = 13.1%

Data Down Unconfirmed: 739 = 0.3%

Data Down Confirmed: 4653 = 1.6%

Large number of stations reported Adaptive Data Rate support (ADR) during uplink data transmission:

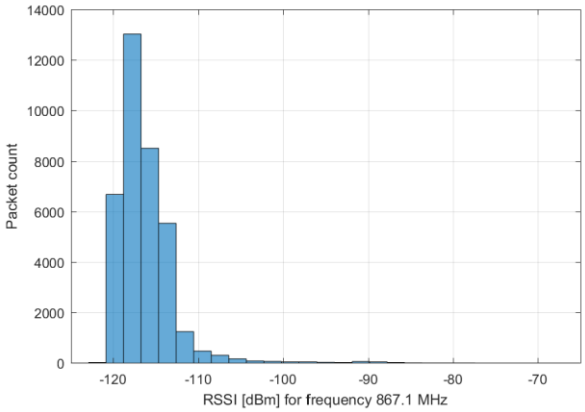
Uplink ADR Support: 208055/276990 = 75.1%

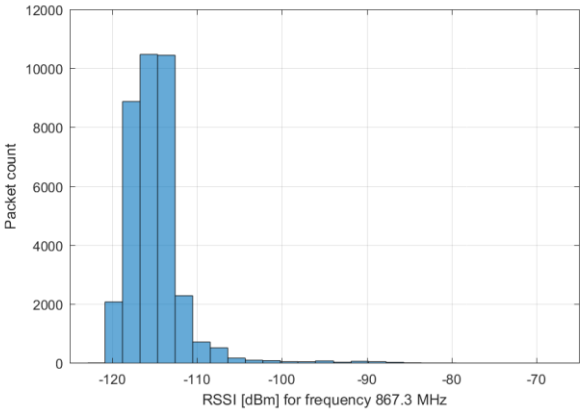
Analysis of deveui field inside Join Request messages provides an overview of the most common vendors of client devices in the LoRaWAN network on monitored location:

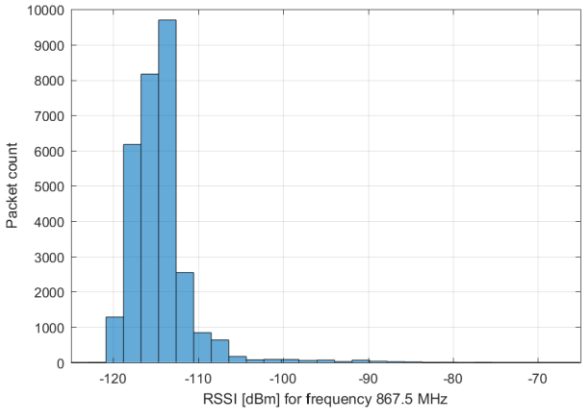
OUI	count	vendor
000000	931	unknown
0004A3	771	Microchip Technology Inc.
000425	491	Atmel Corporation
70B3D50072	374	Sensoneo
D8A01D	287	Espressif Inc.
C00000	210	Western Digital ???
C0FFFF	194	unknown
47DB55	165	unknown
0017E7	96	Texas Instruments
A81758	83	Elektronik System i Umeå AB
70B3D57ED0	76	The Things Network Foundation
3FFCFF	60	unknown
C10000	51	unknown
303838	50	unknown
000797	46	Netpower Co., Ltd.

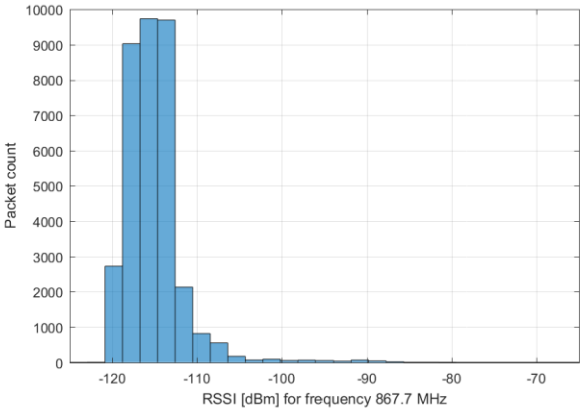
Tab. 1: Most common LoRaWAN device vendors

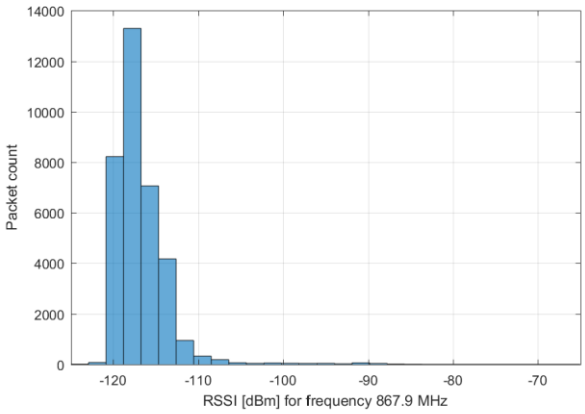
3.6.2 RSSI per channel

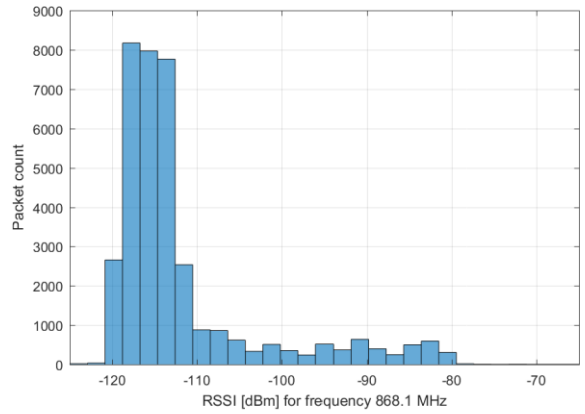


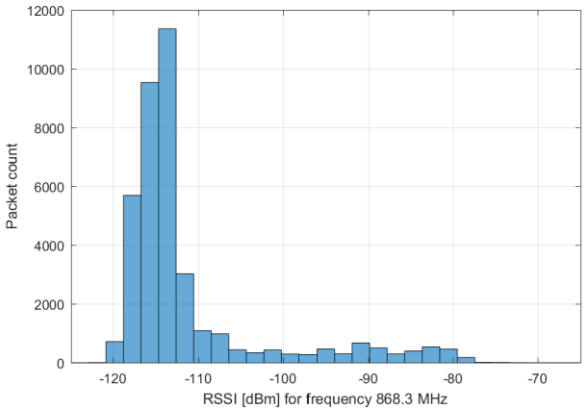


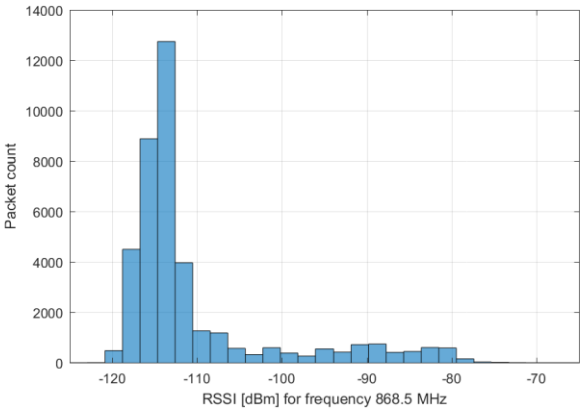




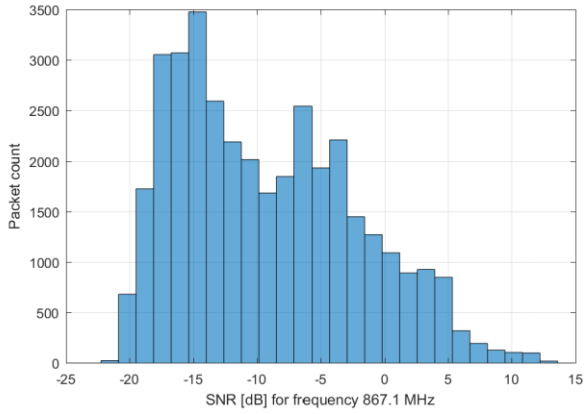


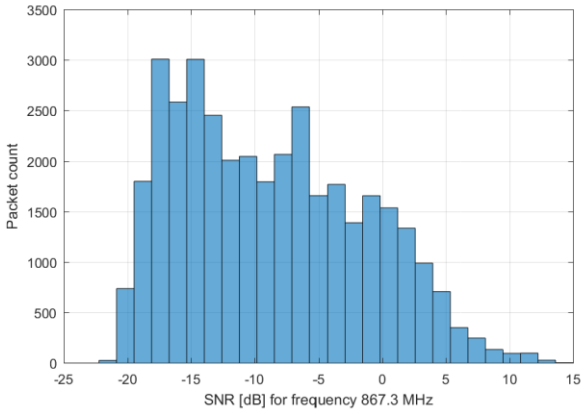


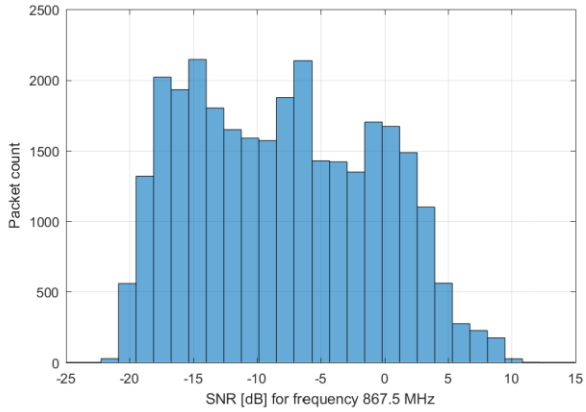


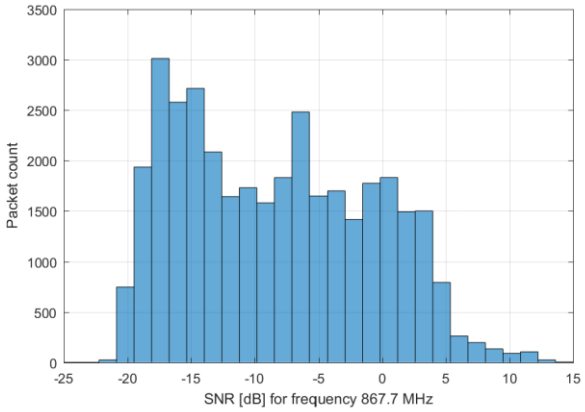


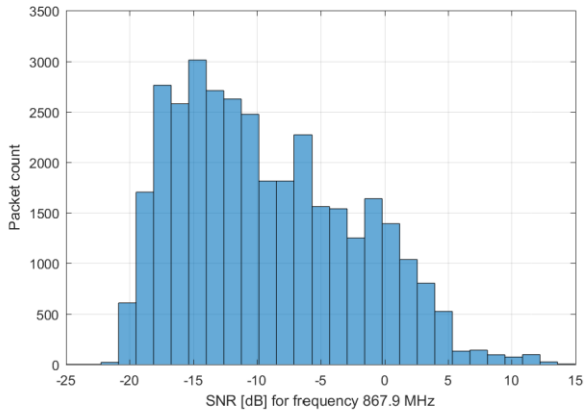
3.6.3 SNR per channel

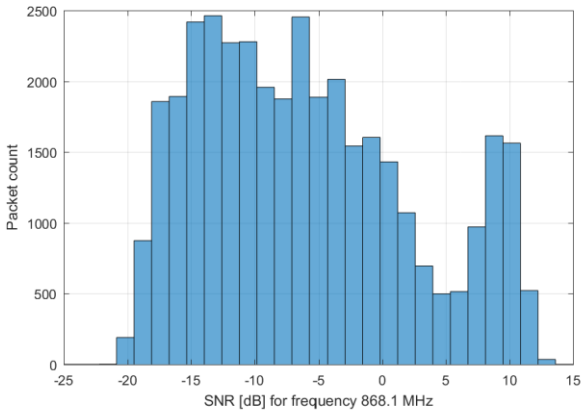


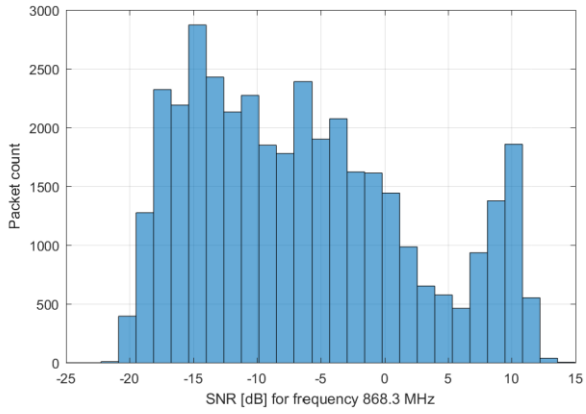


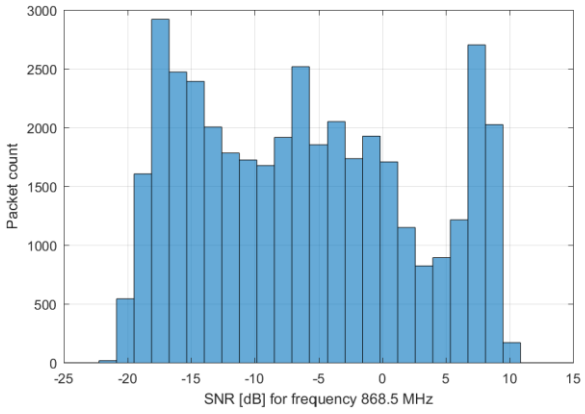












4 LoRa traffic analysis: Trebic

The sniffer box has been placed on the roof of a private company building at Heliadova street, Trebic.

Fig. 3: Sniffer placement in Trebic

Total packets processed: 36209

Unique packets processed: 34952

Number of duplicate packets: 1257 = 3.6%

Private (LoRa) packets with valid CRC: 8437 = 24.1%

Public (LoRaWAN) packets with valid CRC: 2405 = 9.6%

Both private (LoRa) and public (LoRaWAN) packets with valid CRC: 12100 = 34.6%

Sniffer running period: 14 days

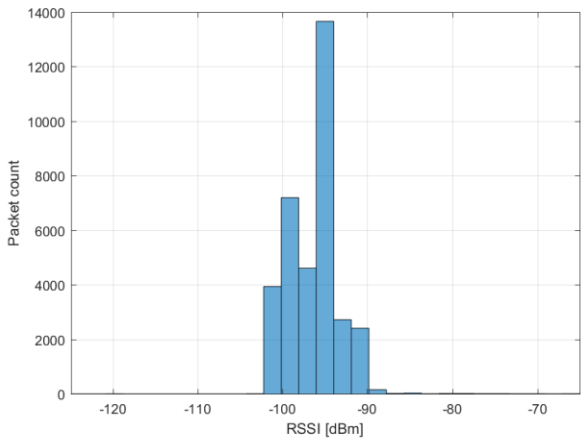
Most of the LoRaWAN packets belong to Join Requests. However, detailed analysis of the data revealed these packets as private traffic with wrong headers. Only 18 packets of Join Request type was found, together with two (2) valid data packets. Such small numbers are probably caused by low LoRaWAN traffic in the area and also by suboptimal placement of the sniffer box.

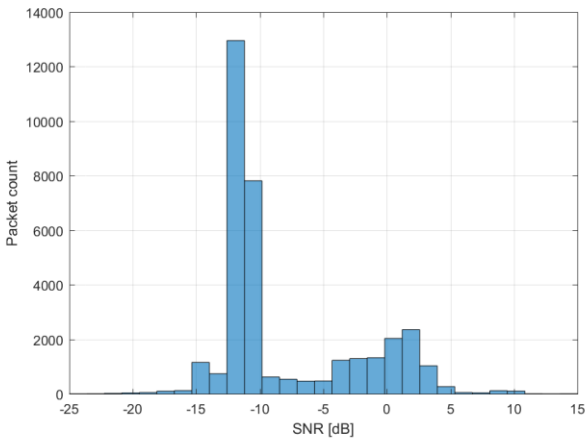
4.1 Analysis overview

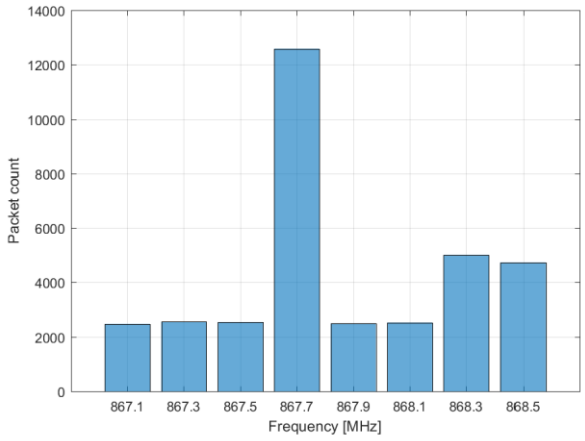
This overview summarises all received packets on both gateways. Only one packet is counted if received by both gateways as duplicate. CRC filtering is not applied, i.e. all received data are shown, both valid and invalid.

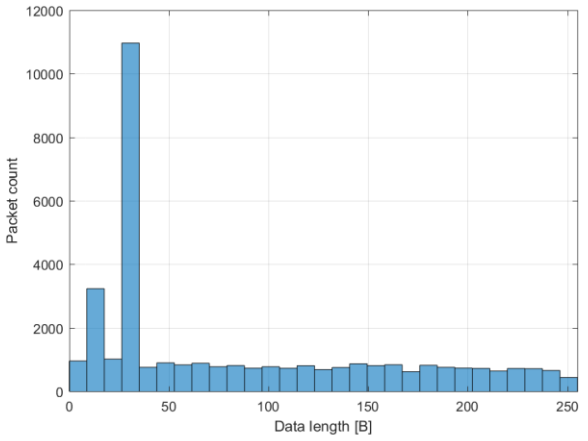
Data from rx51.csv file, SQL query:

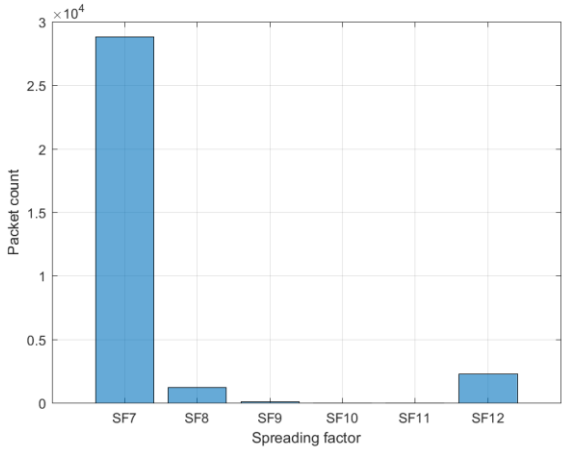
```
select id, freq, sf(datr), cr(codr), lsnr, rssi, size from rxpk4 where
(flag=919 or flag=920 or flag=119)
```

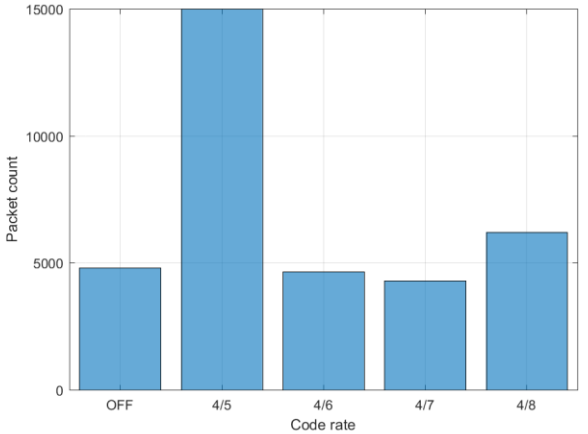




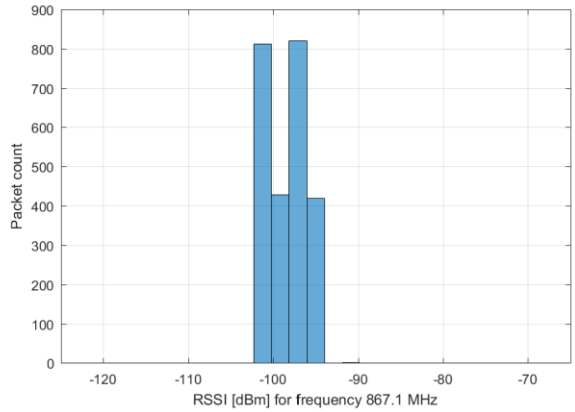


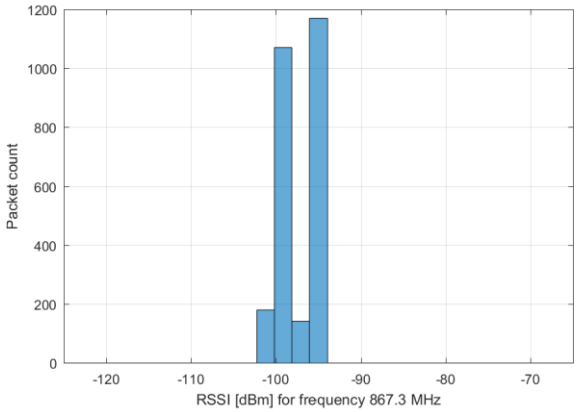


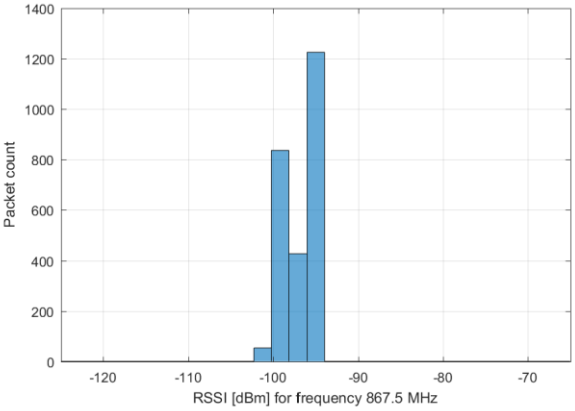


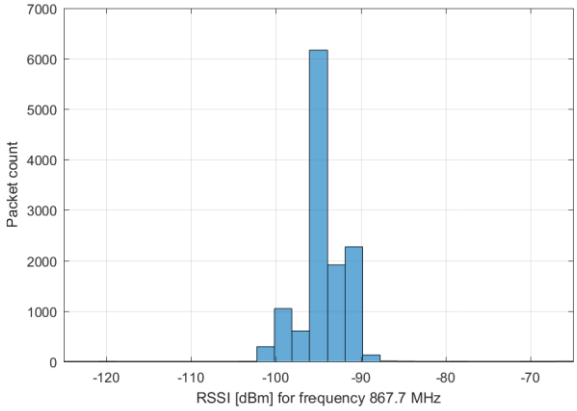


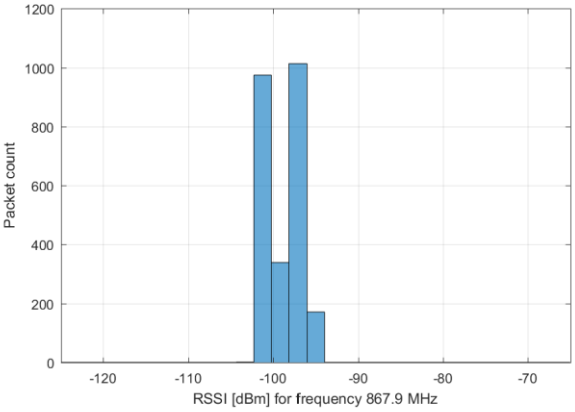
4.1.1 RSSI per channel

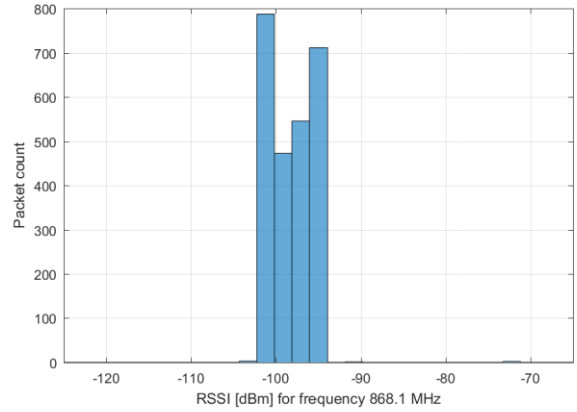


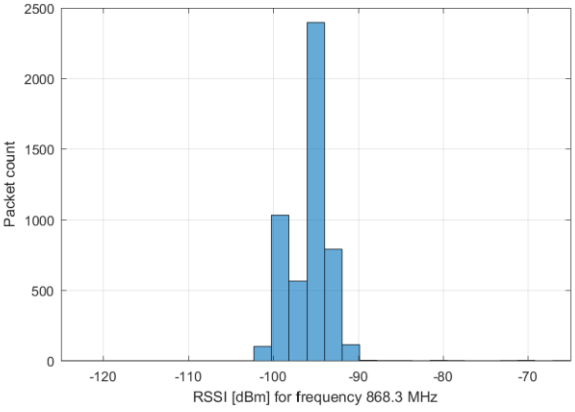


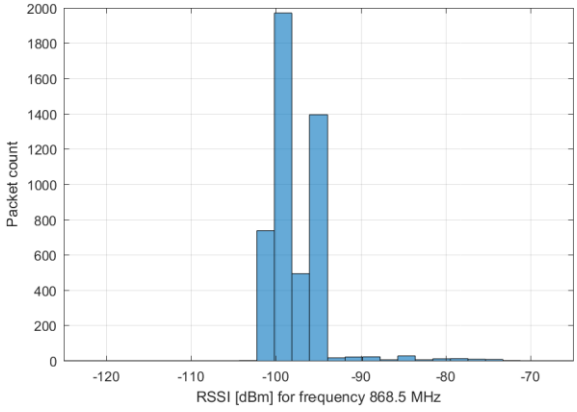




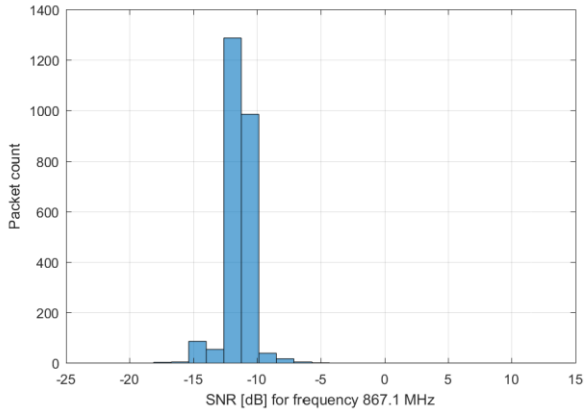


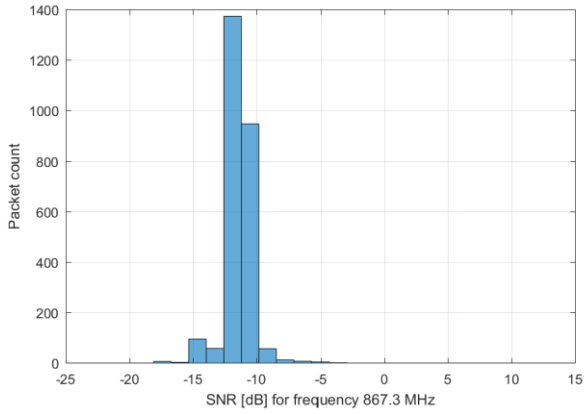


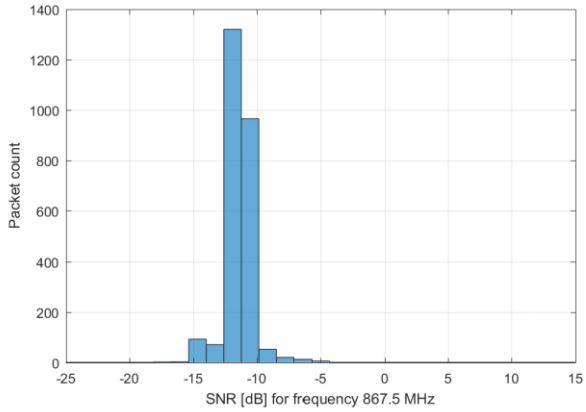


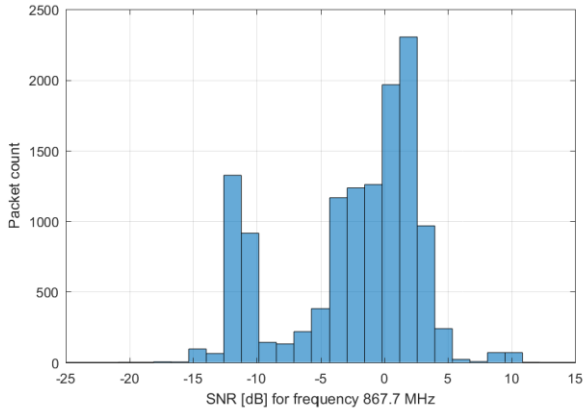


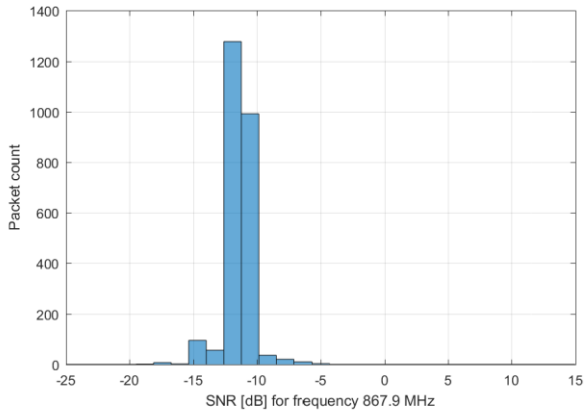
4.1.2 SNR per channel

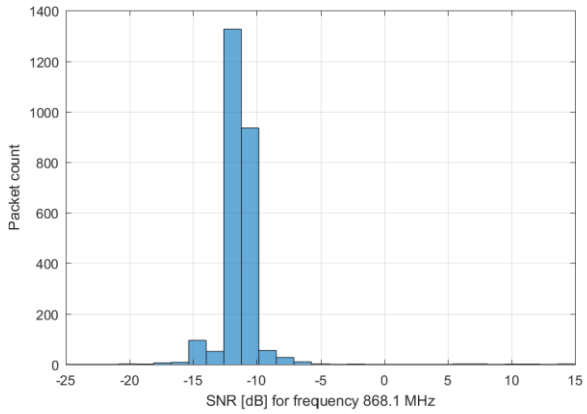


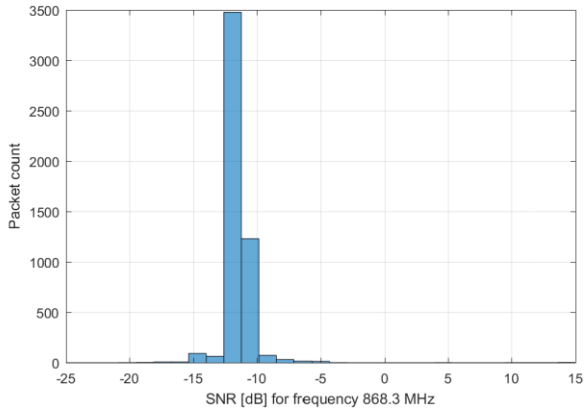


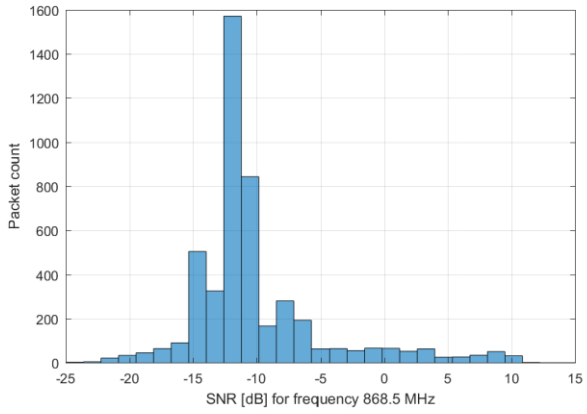










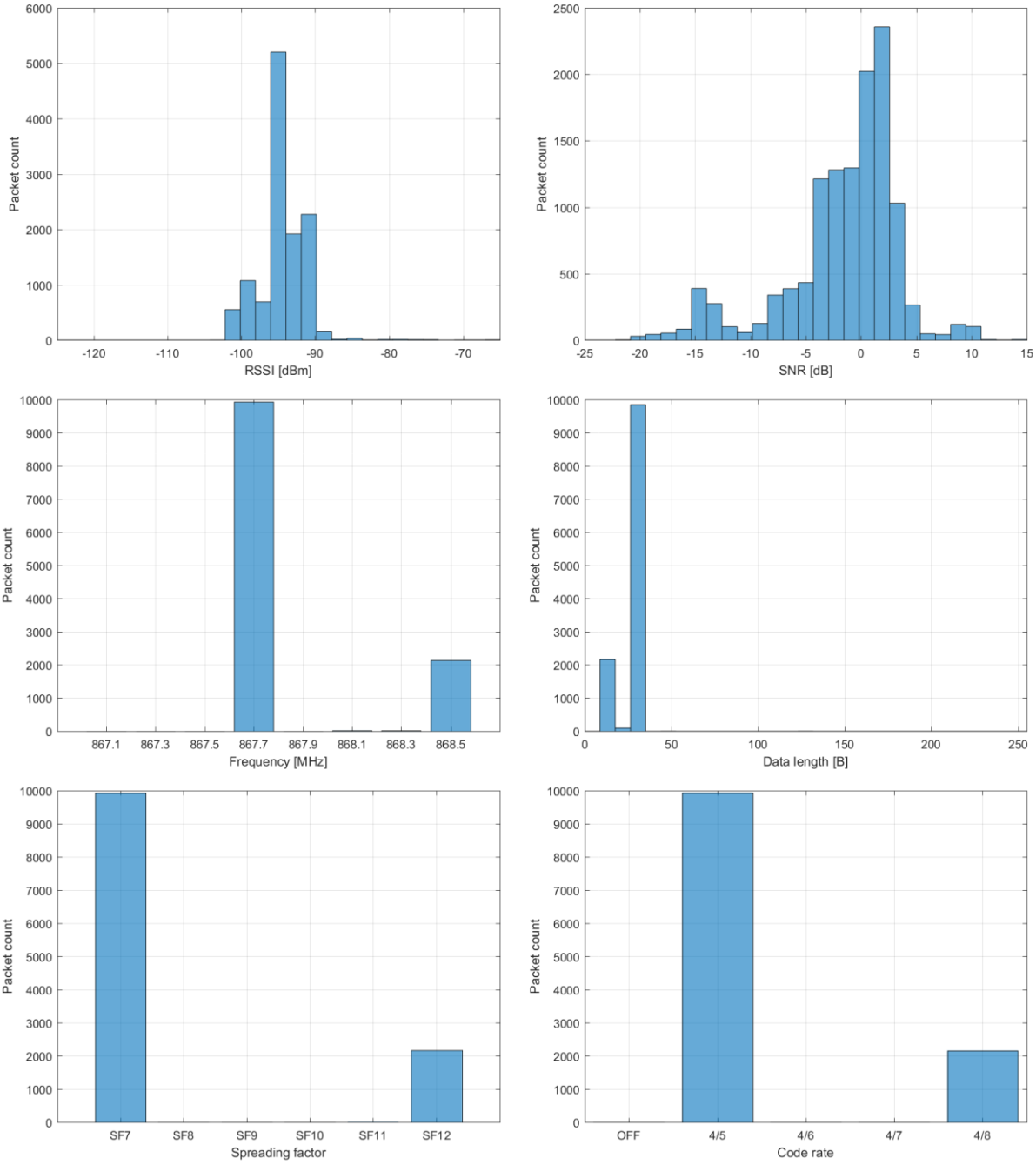


4.2 Both private (LoRa) and public (LoRaWAN) packets with valid CRC

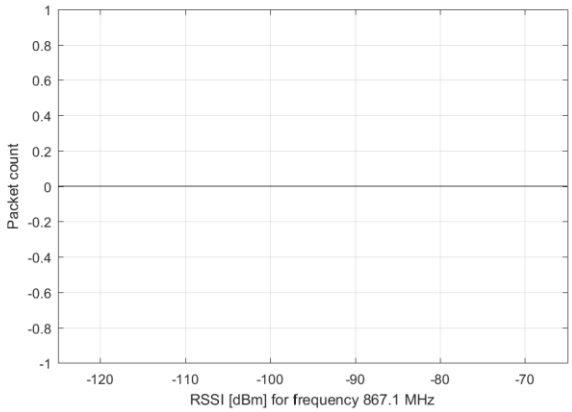
Following valid packets have been received by one of the gateways. Duplicates received by both gateways are counted only once. Only packets with valid CRC are shown.

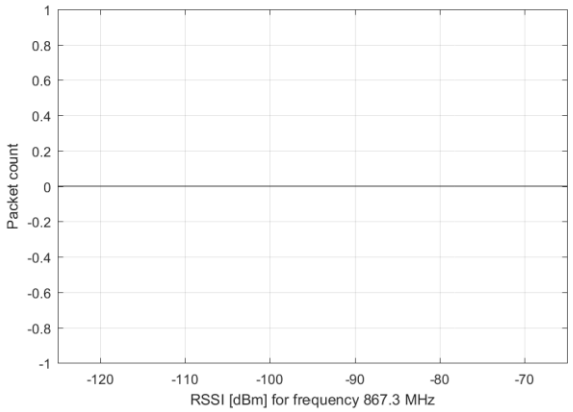
Data from rx55.csv file, SQL query:

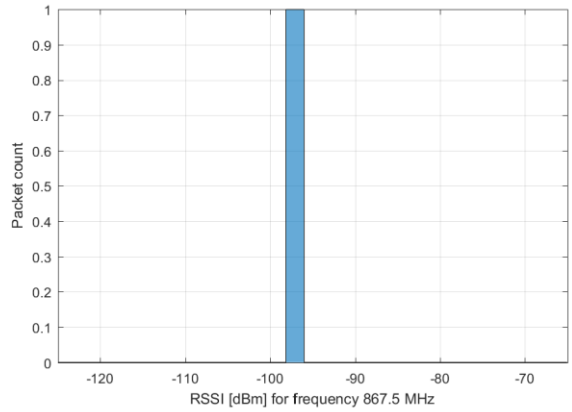
```
select id, freq, sf(datr), cr(codr), lsnr, rssi, size from rxpk4 where
(flag=919 or flag=920 or flag=119) and stat=1
```

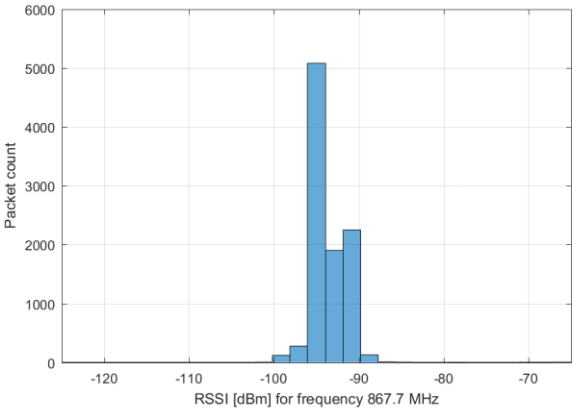


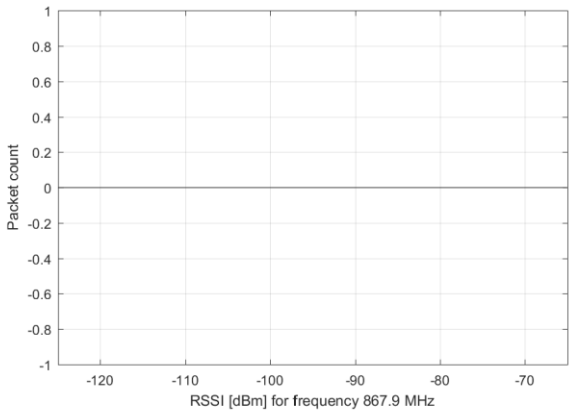
4.2.1 RSSI per channel

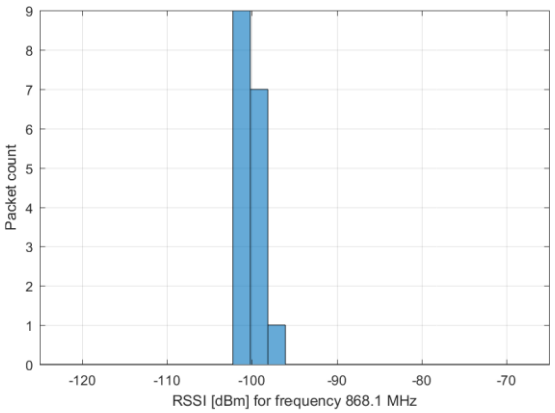


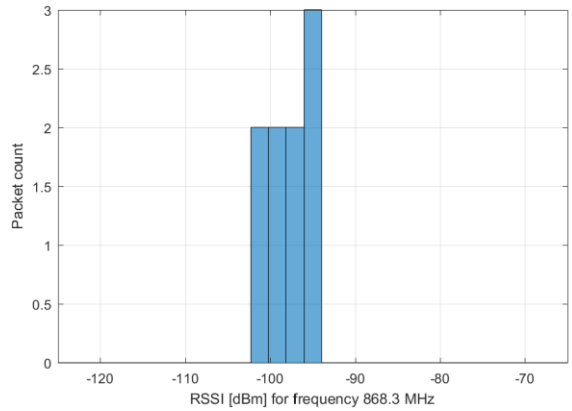


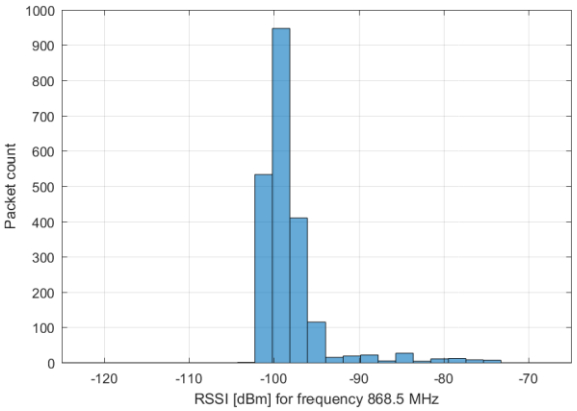




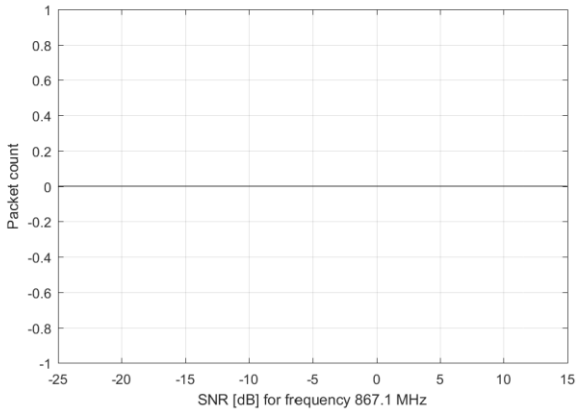


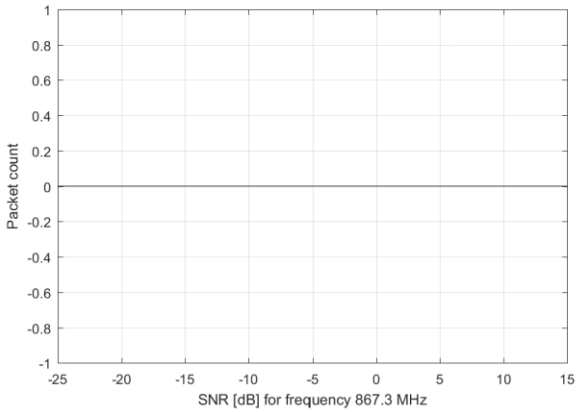


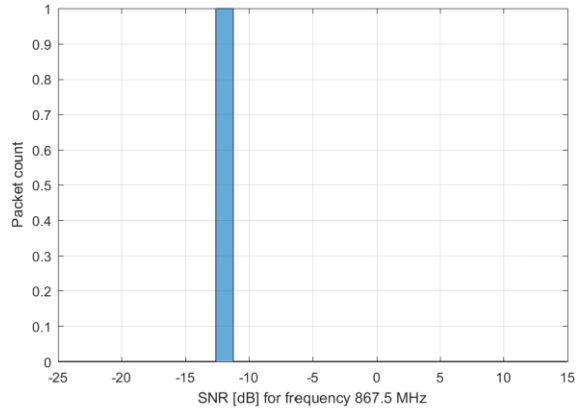


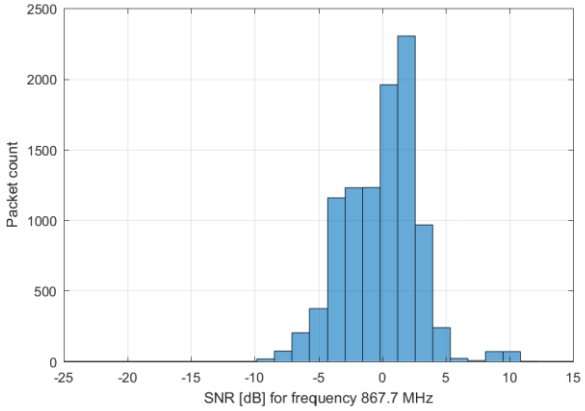


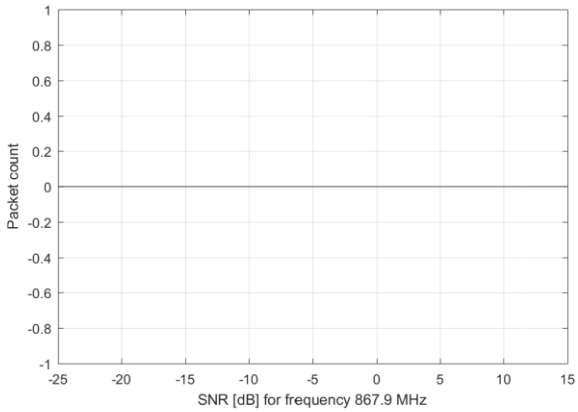
4.2.2 SNR per channel

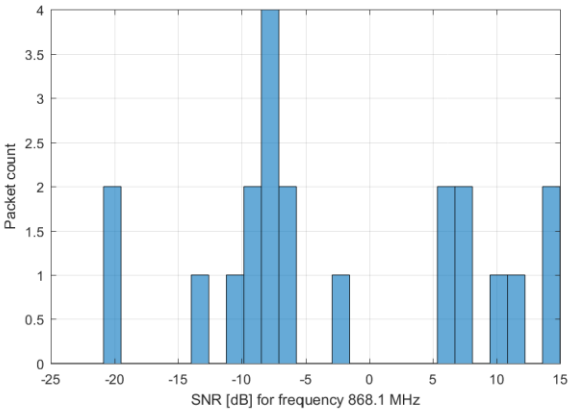


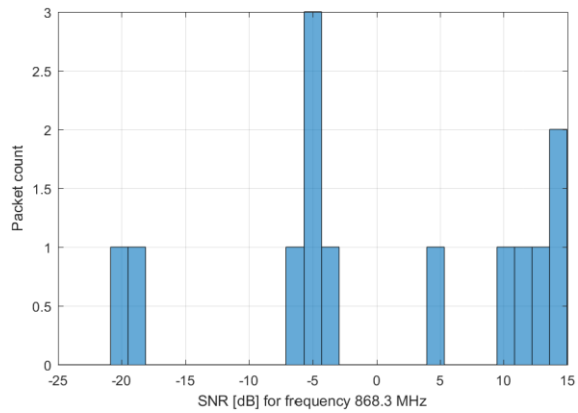


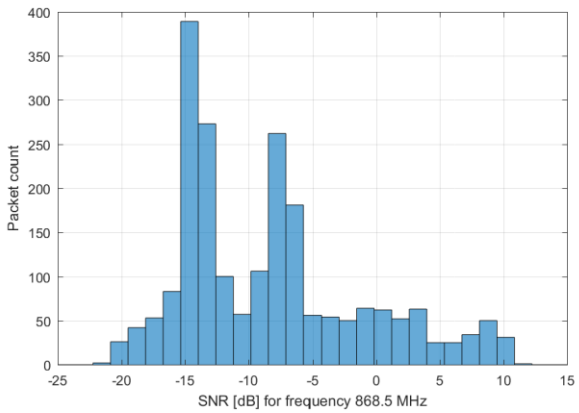












5 Database structure

All received packets obtained during monitoring periods are available as an attachment to this report[5]. The utilities used for data processing (modified version of LoRaWAN packet decoder and util_ack.sh packet receiver) are publicly available[6] under MIT license. Data are stored in SQL format in MariaDB database. Each database contains the following tables:

```
CREATE TABLE IF NOT EXISTS rxpk (
  id int(11) NOT NULL PRIMARY KEY,
  sgwm varchar(40) NOT NULL,
  tmst int(11) NOT NULL,
  `time` varchar(40) NOT NULL,
  chan int(11) NOT NULL,
  rfch int(11) NOT NULL,
  freq decimal(5,2) NOT NULL,
  stat int(11) NOT NULL,
  modu varchar(10) NOT NULL,
  datr varchar(10) NOT NULL,
  codr varchar(10) NOT NULL,
  lsnr decimal(5,2) NOT NULL,
  rssi int(11) NOT NULL,
  size int(11) NOT NULL,
  `data` varchar(4096) NOT NULL
);

CREATE TABLE IF NOT EXISTS stat (
  id int(11) NOT NULL PRIMARY KEY,
  sgwm varchar(40) NOT NULL,
  `time` varchar(40) NOT NULL,
  rxnb int(11) NOT NULL,
  rxok int(11) NOT NULL,
  rxfw int(11) NOT NULL,
  ackr int(11) NOT NULL,
  dwnb int(11) NOT NULL,
  txnb int(11) NOT NULL,
  `desc` varchar(40) NOT NULL
);
```

Tables rxpk and stat are directly stored by util_ack.sh, with data obtained from packet forwarders running on physical LoRa gateways. Table rxpk contains received packets, i.e. source gateway ID, timestamps, RF channel and frequency, CRC state, modulation, data and coding rate, SNR, RSSI, packet size and base64-encoded data. Table stat contains periodic gateway statistics, especially the number of RX packets (all and with valid CRC).

```
CREATE TABLE IF NOT EXISTS rxpk4 (
  id int(11) NOT NULL PRIMARY KEY,
  flag int(11) DEFAULT NULL,
  flag2 int(11) DEFAULT NULL,
  sgwm varchar(40) NOT NULL,
  tmst int(11) NOT NULL,
  `time` varchar(40) NOT NULL,
  chan int(11) NOT NULL,
  rfch int(11) NOT NULL,
```

[5] http://www.radio.feec.vutbr.cz/interop/lora/
[6] https://github.com/alpov/lora-packet/tree/interop

```
  freq decimal(5,2) NOT NULL,
  stat int(11) NOT NULL,
  modu varchar(10) NOT NULL,
  datr varchar(10) NOT NULL,
  codr varchar(10) NOT NULL,
  lsnr decimal(5,2) NOT NULL,
  rssi int(11) NOT NULL,
  size int(11) NOT NULL,
  `data` varchar(4096) NOT NULL
);
```

Table rxpk4 provides processed data. Its structure is similar to rxpk except it adds two more fields – flag and flag2. The flag field denotes source gateway and can contain the following values:

- 919 ... received from GW with public prefix
- 920 ... received from GW with private prefix
- 119 ... received duplicate from both GWs, packet from GW with public prefix
- 120 ... received duplicate from both GWs, packet from GW with private prefix

The flag field has been created by comparison of similar timestamp, data and frequency of received packets, using the following SQL:

```
update rxpk4 set flag=919 where sgwm="b827ebfffeafacff"
update rxpk4 set flag=920 where sgwm="b827ebfffe269969"

create table id3tmp (id int(11) not null unique key);

insert into id3tmp (id) select rxpk4.id from rxpk4 group by
round(unix_timestamp(rxpk4.time)/4),rxpk4.data,rxpk4.freq having count(*)=1

update rxpk4 left join id3tmp on id3tmp.id=rxpk4.id set rxpk4.flag=111
where id3tmp.id is null

update rxpk4 set flag=119 where sgwm="b827ebfffeafacff" and flag=111
update rxpk4 set flag=120 where sgwm="b827ebfffe269969" and flag=111

drop table id3tmp;
```

The flag2 field shows result of LoRaWAN packet decoder processing and can contain the following values:

- 10 ... Join Request
- 20 ... Join Accept
- 30 ... Data Message
- 40, 41 ... unknown, wrong format, decode error

Note that the LoRaWAN decoder has processed all the packet, including private non-LoRaWAN packets and packets with wrong CRC.

The decoder has been run on CSV data exported by phpMyAdmin from rxpk4 table. It produces four CSV output files: log_all.csv (classification of all packets), log_data.csv (processed Data Message packets), log_joinacc.csv (processed Join Accept messages), and log_joinreq.csv (processed Join Request messages).

The flag2 field of rxpk4 table has been filled using the following SQL:

```
create table log_all (
  id int(11) not null primary key,
```

```
  flag2 int(11) default null
);

-- now run the following command on server:
-- mysqlimport --fields-terminated-by=\; --fields-enclosed-by=\" \
-- --local -u root -p lora-urel log_all.csv

update rxpk4 set flag2=(select flag2 from log_all where
log_all.id=rxpk4.id)
drop table log_all;
```

Finally, three tables for classification of each LoRaWAN identified packet has been created. The following tables has been filled with mysqlimport command and their structures are based on LoRaWAN decoder output:

```
CREATE TABLE IF NOT EXISTS log_data (
  id int(11) NOT NULL PRIMARY KEY,
  `data` varchar(200) NOT NULL,
  mhdr varchar(30) NOT NULL,
  mic varchar(30) NOT NULL,
  fhdr varchar(30) NOT NULL,
  fport varchar(30) NOT NULL,
  frmpayload varchar(100) NOT NULL,
  devaddr varchar(30) NOT NULL,
  fctrl varchar(30) NOT NULL,
  fcnt varchar(30) NOT NULL,
  fopts varchar(30) NOT NULL,
  mtype varchar(30) NOT NULL,
  dir varchar(30) NOT NULL,
  cnt varchar(30) NOT NULL,
  fctrlack tinyint(1) NOT NULL,
  fctrladr tinyint(1) NOT NULL,
  flag varchar(5) DEFAULT NULL
);

CREATE TABLE IF NOT EXISTS log_joinacc (
  id int(11) NOT NULL PRIMARY KEY,
  `data` varchar(200) NOT NULL,
  mhdr varchar(10) NOT NULL,
  mic varchar(30) NOT NULL,
  appnonce varchar(30) NOT NULL,
  netid varchar(30) NOT NULL,
  devaddr varchar(30) NOT NULL,
  dlsettings varchar(30) NOT NULL,
  rxdelay varchar(30) NOT NULL,
  cflist varchar(30) NOT NULL,
  rx1 varchar(30) NOT NULL,
  rx2 varchar(30) NOT NULL,
  del varchar(30) NOT NULL,
  flag varchar(5) NOT NULL
);

CREATE TABLE IF NOT EXISTS log_joinreq (
  id int(11) NOT NULL PRIMARY KEY,
  `data` varchar(200) NOT NULL,
  mhdr varchar(10) NOT NULL,
  macpayload varchar(200) NOT NULL,
  mic varchar(30) NOT NULL,
  appeui varchar(30) NOT NULL,
  deveui varchar(30) NOT NULL,
  devnonce varchar(10) NOT NULL,
```

```
  flag varchar(5) NOT NULL
);
```

Data has been visualised using MATLAB. The CSV files should contain only numeric values to allow easy import using csvread(). For this conversion, two SQL functions has been created:

```
create function sf(inp varchar(30))
returns int
begin
  declare result int;
  if inp='SF7BW125' then
    set result=7;
  elseif inp='SF8BW125' then
    set result=8;
  elseif inp='SF9BW125' then
    set result=9;
  elseif inp='SF10BW125' then
    set result=10;
  elseif inp='SF11BW125' then
    set result=11;
  elseif inp='SF12BW125' then
    set result=12;
  else
    set result=0;
  end if;
  return result;
end;

create function cr(inp varchar(30))
returns int
begin
  declare result int;
  if inp='4/5' then
    set result=5;
  elseif inp='4/6' then
    set result=6;
  elseif inp='4/7' then
    set result=7;
  elseif inp='4/8' then
    set result=8;
  else
    set result=0;
  end if;
  return result;
end;
```

6 Conclusion

In this document, we described the setup for capturing LoRa traffic and analyzed in detail the data from the almost annual run of the sniffer in the Brno area. Additional data were obtained in another location. Detailed statistics were processed, especially RSSI and SNR indicators for individual radio channels, which provides information on the use and interoperability of traffic on individual frequencies in the 868 MHz band.

Based on the data evaluation, we identified a problem with crosstalk between LoRa gateways with private and public sync word. This issue was further investigated by project partners from TU Wien[7]. From the obtained data it is clear that this is a problem of LoRa gateway chipset, which manifests itself especially in packets with a very high SNR around +10 dB.

A number of conclusions can be drawn from the examined data. Code rates 4/5 and 4/8 are used, for identified LoRaWAN operation practically exclusively 4/5. All spreading factors are used, most often SF12 and then SF7. Almost all valid packets were up to 64B in length, although LoRa theoretically allows packets of up to 255B to be transmitted.

In terms of frequency band utilization, we observe that the use of channels 1 to 3 (868.1 MHz, 868.3 MHz, 868.5 MHz) dominates for general LoRa traffic, with traffic about 50% higher than other channels. Channel 7 (867.7 MHz) is very popular for private operation. However, decodable LoRaWAN operation is statistically balanced between all channels 1 to 8 (frequencies 867.1 to 868.5 MHz), code rate 4/5 is used.

A number of strong signals with RSSI in the range -100 to -70 dBm were detected as packets with invalid CRC. In addition, most of these packets were received on channels 1 - 3 (868.1 MHz, 868.3 MHz, 868.5 MHz) and were often packets with private to public sync word crosstalk issue. In contrast, most valid packets were relatively weak with RSSI in the range -120 to -110 dBm.

The SNR analysis of received packets shows that the receiving gateway reports SNR in a narrow range of -12.2 dB to -10.5 dB for the dominant majority of packets with an invalid CRC. This deviation is clearly visible from the histograms. This is probably another issue with the LoRa base station chipset.

Given the above results, we can recommend to operate private LoRa communication on less used channels 4, 5, 6 and 8 (867.1 MHz, 867.3 MHz, 867.5 MHz, 867.9 MHz). Operation in LoRaWAN networks is strongly dependent on the gateway settings, but the current use of channels is relatively even. Interference from high-powered RFID devices was not observed on the analyzed data.

[7] http://www.interreg-interop.eu/results/lorawan/privatepublic_syncword_crosstalk/