LoRa Radio Networks

Tomáš Rosa
Head of Cryptology and Biometrics Competence Centre of Raiffeisen Bank International
Department of Algebra, Faculty of Mathematics and Physics, Charles University in Prague

Cautionary Note

- **LoRa** ~ Long Range (radio)
  - physical layer based on Chirp Spread Spectrum radio
  - many different networks can be based on LoRa PHY
  - including star as well as mesh and ad-hoc mesh topologies
- **LoRaWAN** ~ Long Range Wide-Area Network
  - particular wireless network architecture with a star topology based on LoRa PHY
- We shall not mix these two terms

Two Faces of LoRa in Security

- Defensive usage
  - critical infrastructure telemetry service
- Offensive usage
  - covert data transfer from/to perimeter of interest
  - autonomous devices supervision and control
  - data exfiltration using physical layer collisions (TEMPEST)

TEMPEST-LoRa: Cross-Technology Covert Communication

Xieyang Sun
Xi'an Jiaotong University
Xi'an, China
xieyangsun@stu.xjtu.edu.cn

Yuanqing Zheng
The Hong Kong Polytechnic University
Hong Kong, China
csyqzheng@comp.polyu.edu.hk

Wei Xi*
Xi'an Jiaotong University
Xi'an, China
xiwei@xjtu.edu.cn

Zuhao Chen
Xi'an Jiaotong University
Xi'an, China
czh869452912@gmail.com

Zhizhen Chen
Xi'an Jiaotong University
Xi'an, China
zhizhenc@stu.xjtu.edu.cn

Han Hao
Xi'an Jiaotong University
Xi'an, China
haohan9717@stu.xjtu.edu.cn

Zhiping Jiang
Xidian University
Xi'an, China
zpj@xidian.edu.cn

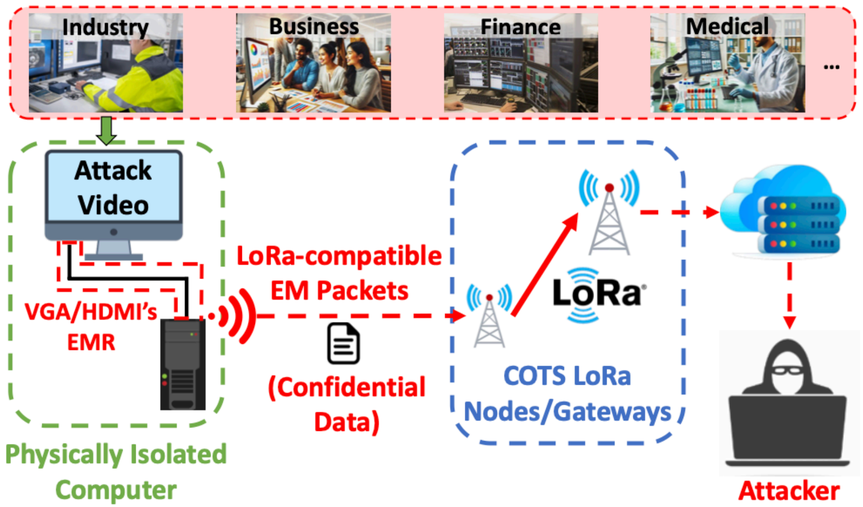
Sheng Zhong
Nanjing University
Nanjing, China
zhongsheng@nju.edu.cn

69v1 [cs.CR] 26 Jun 2025

-- https://arxiv.org/abs/2506.21069v1

Abstract

Electromagnetic (EM) covert channels pose significant threats to computer and communications security in air-gapped networks. Previous works exploit EM radiation from various components (*e.g.*, video cables, memory buses, CPUs) to secretly send sensitive information. These approaches typically require the attacker to deploy highly specialized receivers near the victim, which limits their real-world impact. This paper reports a new EM covert channel, TEMPEST-LoRa, that builds on Cross-Technology Covert Communication (CTCC), which could allow attackers to covertly transmit EM-modulated secret data from air-gapped networks to widely deployed operational LoRa receivers from afar. We reveal the potential risk and demonstrate the feasibility of CTCC by tack-



LoRa (Long Range) PHY Origin

"...The story of LoRa began in 2009, when two friends in France ... Despite encountering resistance, ... Nicolas Sornin and Olivier Seller continued dedicating their time to turn the idea into a reality. In 2010, Nicolas and Olivier met their third partner, François Sforza, and together they started the company Cycleo. ... [Grenoble, FR]"

"... Semtech acquired Cycleo in May 2012. ... [Camarillo, California, USA]"

-- https://blog.semtech.com/a-brief-history-of-lora-three-inventors-share-their-personal-story-at-the-things-conference

(12) **United States Patent**
Sforza

(10) **Patent No.: US 8,406,275 B2**
(45) **Date of Patent: Mar. 26, 2013**

(54) **COMMUNICATIONS SYSTEM**

(75) Inventor: **Francois Sforza**, Nice (FR)

(73) Assignee: **Nanoscale Labs**, La Tronche (FR)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 410 days.

(21) Appl. No.: **12/720,139**

(22) Filed: **Mar. 9, 2010**

(65) **Prior Publication Data**

US 2011/0064119 A1 Mar. 17, 2011

(30) **Foreign Application Priority Data**

Jul. 2, 2009 (EP) 09305641

(51) **Int. Cl.**
H04B 1/00 (2006.01)

(52) **U.S. Cl.** **375/139**

(58) **Field of Classification Search** 375/139, 375/371, 298; 370/441, 307, 516
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,550,549	A *	8/1996	Procter et al.	342/47
6,252,882	B1 *	6/2001	Matsui	370/441
6,549,562	B1 *	4/2003	Olaker et al.	375/139
6,614,864	B1 *	9/2003	Raphaeli et al.	375/371
6,940,893	B1 *	9/2005	Pinkney et al.	375/139
2007/0126622	A1 *	6/2007	Nallapureddy et al.	342/92
2008/0194215	A1 *	8/2008	Bolanos	455/115.1
2008/0309543	A1 *	12/2008	Schaffner	342/21

FOREIGN PATENT DOCUMENTS

EP	0 952 713	10/1999

OTHER PUBLICATIONS

European Search Report dated Nov. 25, 2009, from corresponding European application.

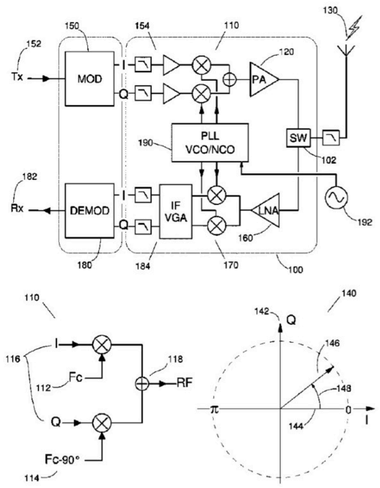
* cited by examiner

Primary Examiner — David C. Payne
Assistant Examiner — Wednel Cadeau
(74) *Attorney, Agent, or Firm* — Young & Thompson

(57) **ABSTRACT**

A communications system includes a modulator for generating a chirp signal aimed at spreading the frequency spectrum of an information signal over a specified spectral bandwidth of a communications channel. The chirp signal has initial and final instantaneous frequency. The chirp signal is controlled from an in-phase control signal and a quadrature-phase control signal to have, in a complex plane, constant amplitude and instantaneous phase. The instantaneous frequency is defined by the speed the instantaneous phase is changed in the complex plane by the in-phase and quadrature-phase control signals; the instantaneous frequency is linearly changed between initial and instantaneous frequencies over the whole duration of the chirp signal; the initial and final instantaneous phases of the chirp signal are identical. The communications system also described an adapted demodulator capable of working even in presence of a significant frequency and/or timing offset between the transmitting and receiving clocking systems.

20 Claims, 11 Drawing Sheets



(12) **United States Patent**
Seller et al.

(10) **Patent No.: US 9,252,834 B2**
(45) **Date of Patent: Feb. 2, 2016**

(54) **LOW POWER LONG RANGE TRANSMITTER**

(71) Applicants: **Olivier B. A. Seller**, Saint Soulle (FR); **Nicolas Sornin**, La Tronche (FR)

(72) Inventors: **Olivier B. A. Seller**, Saint Soulle (FR); **Nicolas Sornin**, La Tronche (FR)

(73) Assignee: **Semtech Corporation**, Camarillo, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **14/170,170**

(22) Filed: **Jan. 31, 2014**

(65) **Prior Publication Data**

US 2014/0219329 A1 Aug. 7, 2014

(30) **Foreign Application Priority Data**

Feb. 5, 2013 (EP) 20130154071

(51) **Int. Cl.**
H04B 1/66 (2006.01)
H03M 13/27 (2006.01)
H04B 1/69 (2011.01)
H03M 5/14 (2006.01)

(52) **U.S. Cl.**
CPC . ***H04B 1/66*** (2013.01); ***H03M 5/14*** (2013.01); ***H03M 13/276*** (2013.01); ***H03M 13/2721*** (2013.01); ***H04B 1/69*** (2013.01); *H04B 2001/6912* (2013.01)

(58) **Field of Classification Search**
CPC H04B 1/66; H04B 1/69; H04B 2001/6912; H03M 13/2721; H03M 13/276; H03M 5/14
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,852,418	A *	12/1998	Ferrell et al.	342/202
6,549,562	B1 *	4/2003	Olaker et al.	375/139
6,614,853	B1 *	9/2003	Koslar et al.	375/271
6,940,893	B1	9/2005	Pinkney et al.	
8,718,117	B2 *	5/2014	Hiscock	375/139
2002/0003846	A1 *	1/2002	Khayrallah et al.	375/341
2007/0002969	A1 *	1/2007	Jeong et al.	375/298
2007/0274338	A1 *	11/2007	Sebire et al.	370/466
2009/0180518	A1 *	7/2009	Ishii et al.	375/130
2011/0064119	A1 *	3/2011	Sforza	375/139

FOREIGN PATENT DOCUMENTS

EP	0952713	A2	10/1999
EP	2278724	A1	1/2011
EP	2449690	A1	5/2012
WO	WO-0158024	A1	8/2001
WO	WO-2011000936	A1	1/2011

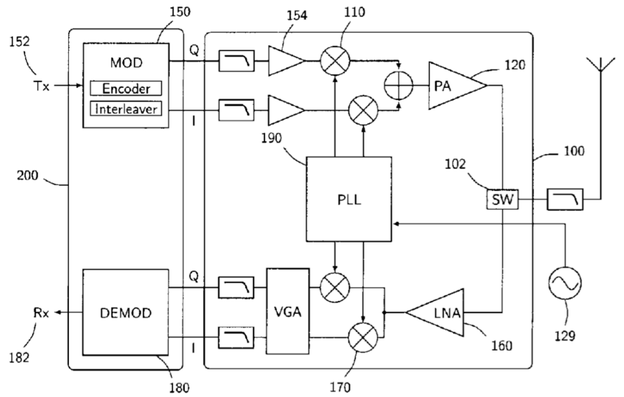
* cited by examiner

Primary Examiner — Kenneth Lam
(74) *Attorney, Agent, or Firm* — Blank Rome LLP

(57) **ABSTRACT**

A transmitter device arranged to encode a set of digital input data into a succession of modulated chirps, whereby said digital input data are encoded according to a Gray code into codewords (**320**, **321**, **322**) having a plurality of bits, and having an interleaver that distributes the bits ($C_{00}, \ldots C_{nn}$) of each codeword into a series of digital modulation values ($S_0, \ldots S_7$), at different bit positions, and to synthesize a series of modulated chirps whose cyclical shifts are determined by the modulation values. A special frame structure is defined in order to ensure high robustness, and variable bit-rate flexibility.

15 Claims, 3 Drawing Sheets



So, the EU independence and sovereignty has its limits here

"... Semtech acquired Cycleo in May 2012. ... [Camarillo, California, USA]"

-- https://blog.semtech.com/a-brief-history-of-lora-three-inventors-share-their-personal-story-at-the-things-conference

$$e^{i\varphi(t)} = \cos\varphi(t) + i\sin\varphi(t)$$

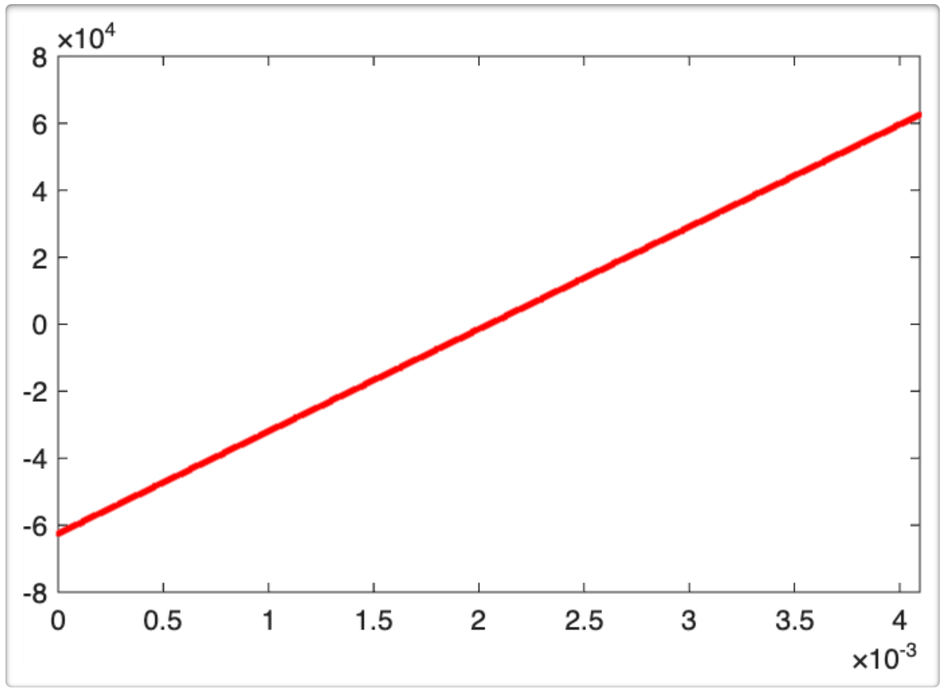
in-phase component

quadrature ($\frac{\pi}{2}$ shift) component

radio terminology

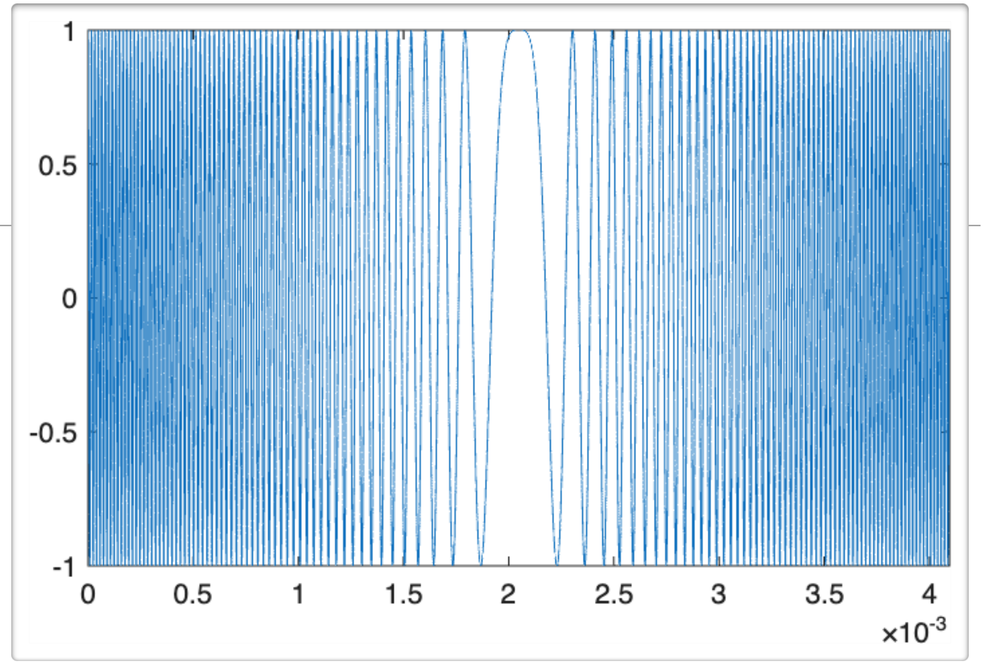
LoRa Radio: Basal UpChirp

instant frequency plane

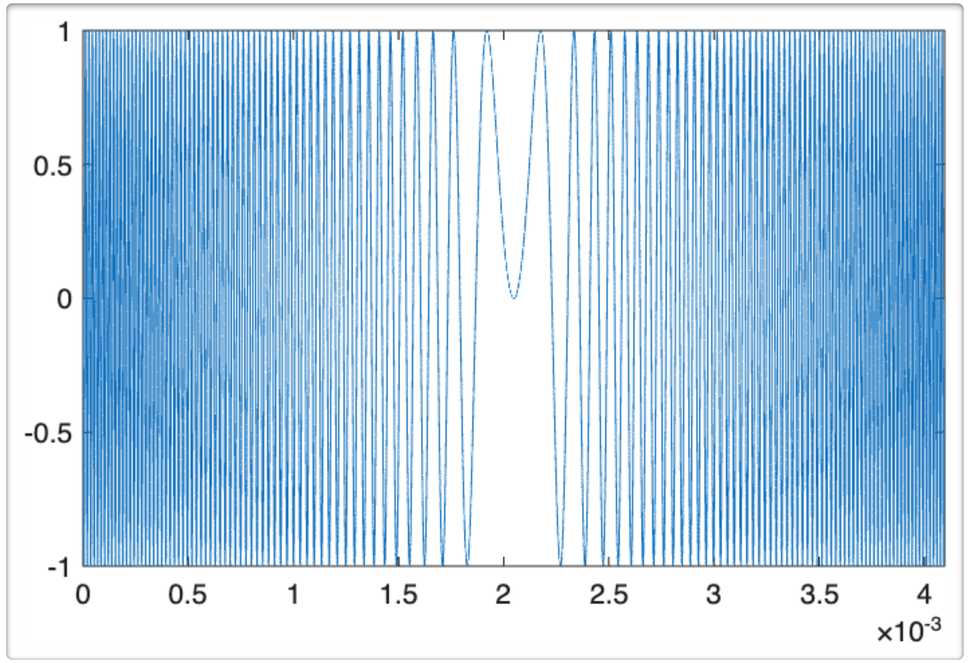


signal plane

in-phase



quadrature



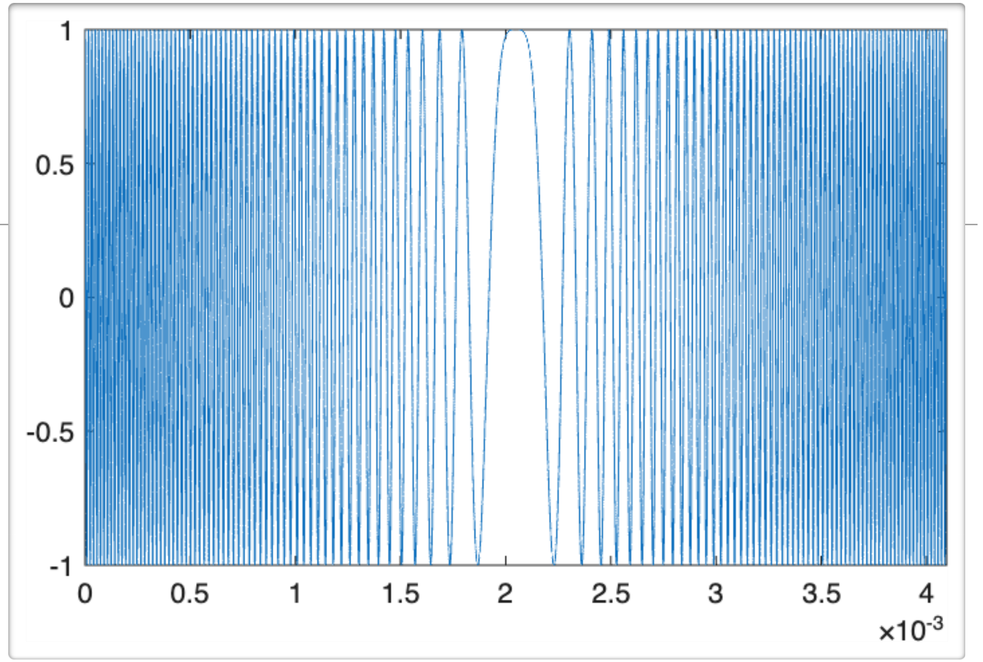
SF = 9, BW = 125 kHz

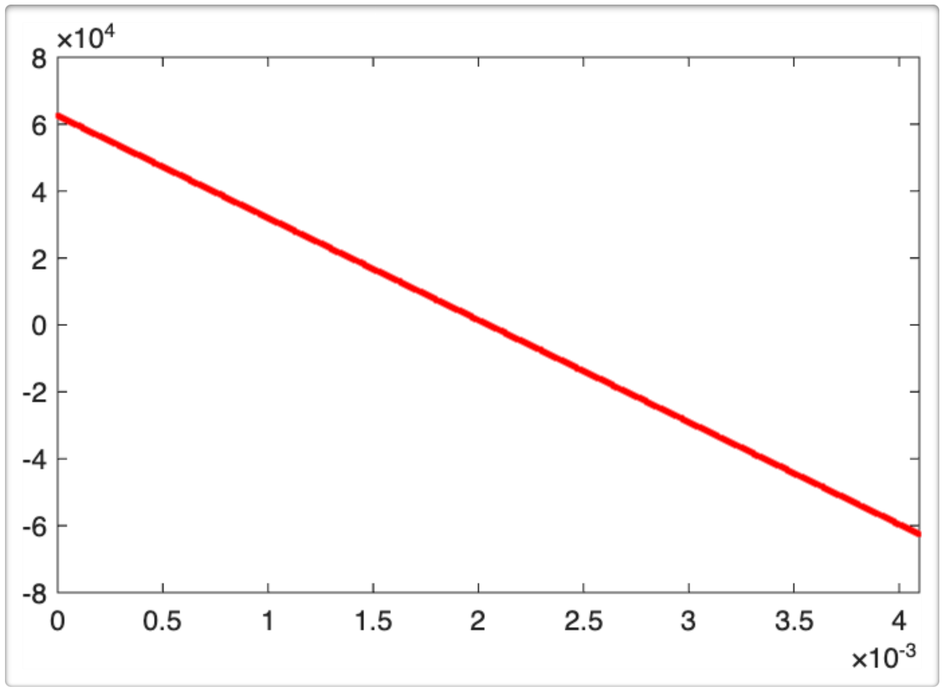
LoRa Radio: Basal DownChirp

instant frequency plane

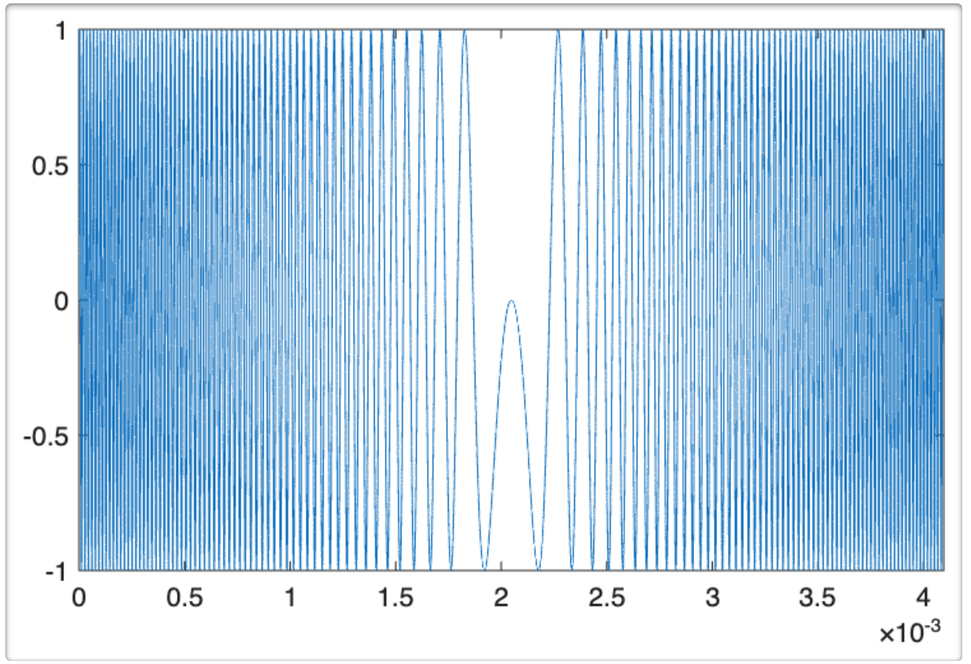
signal plane

in-phase





quadrature



SF = 9, BW = 125 kHz

LoRa Core Modulator Parameters

- **Spreading Factor (SF)**
  - governs the spreading ratio of the modulated chirp signal
  - technically, it is the number of raw data bits per modulation symbol
  - possible values: 5, 6, 7, 8, 9, 10, 11, 12
- **Bandwidth (BW)**
  - sets the symmetric bandwidth predominantly occupied by the chirp
  - possible values (kHz): 7.81, 10.42, 15.63, 20.83, 31.25, 41.67, 62.5, 125, 250, 500

Defining equation for the modulated symbol (chirp) period: $T_s = \frac{2^{SF}}{BW}$

-- SX1261/2 Data Sheet, Rev 2.2, DS.SX1261-2.W.APP, Semtech Corporation, December 2024

LoRa Complex Modulated Signal in Baseband (UpChirp based)

$$f_S(t) = \frac{BW}{T_s}t - \frac{BW}{2} + \frac{S}{T_s} - BW \cdot u\left(t - t_{fold}\right),\ S \in \left\{0, 1, \ldots, 2^{SF} - 1\right\},\ 0 \le t < T_s$$

$$\varphi_S(t) = 2\pi \int_0^t f_S(\tau)\, d\tau = 2\pi \left(\frac{BW}{2T_s}t^2 - \frac{BW}{2}t + \frac{S}{T_s}t - BW \cdot \left(t - t_{fold}\right) u\left(t - t_{fold}\right) \right)$$

$$x_s(t) = e^{i\varphi_S(t)} = e^{i2\pi\left(\frac{BW}{2T_s}t^2 - \frac{BW}{2}t + \frac{S}{T_s}t - BW \cdot t \cdot u\left(t - t_{fold}\right) \right)}$$

$$T_s = \frac{2^{SF}}{BW},\ t_{fold} = T_s - \frac{S}{BW}$$

$$BW \cdot t_{fold} = \left(2^{SF} - S\right) \in \mathbb{Z}$$

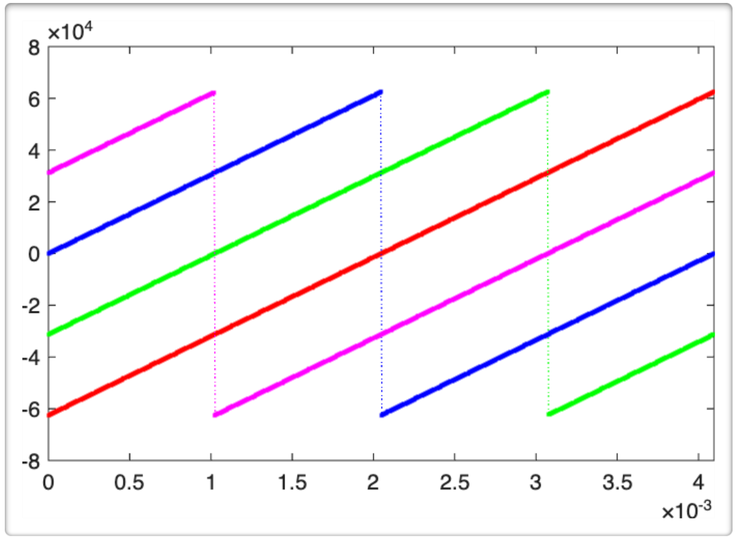
-- Chiani, M. and Elzanaty, A.: *On the LoRa Modulation for IoT: Waveform Properties and Spectral Analysis*, IEEE, 2019

Real Passband Quadrature Modulated Signal Form

$$y_s(t) = \Re\left\{x_s(t) \cdot e^{i2\pi f_c t}\right\} = \Re\left\{ e^{i2\pi\left(\frac{BW}{2T_s}t^2 - \frac{BW}{2}t + \frac{S}{T_s}t - BW \cdot t \cdot u\left(t - t_{fold}\right) + f_c \cdot t\right)} \right\}$$

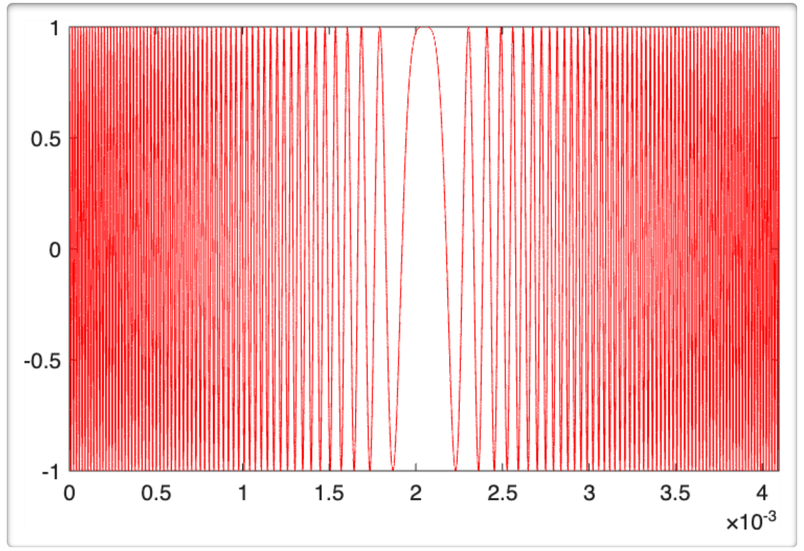
unless stated otherwise, however, we work with complex baseband signals in the following slides

-- Chiani, M. and Elzanaty, A.: *On the LoRa Modulation for IoT: Waveform Properties and Spectral Analysis*, IEEE, 2019

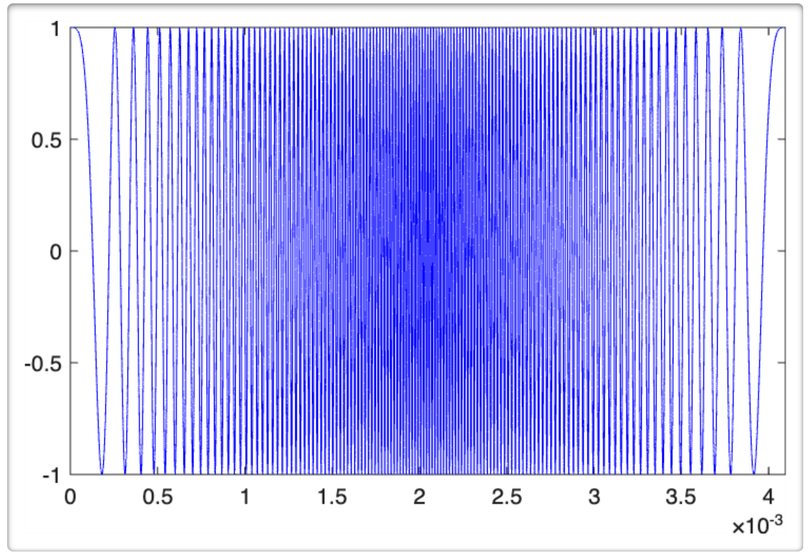


frequency plane modulated symbols

SF = 9, BW = 125 kHz
Ts = 4.096 ms



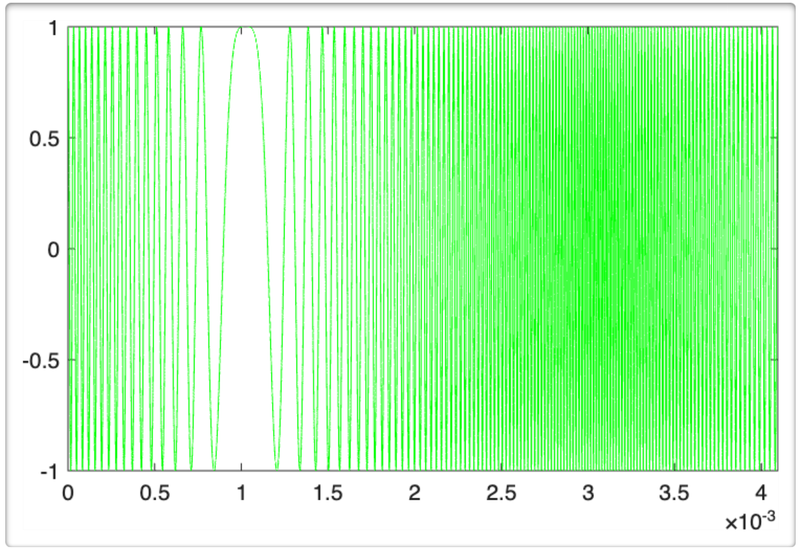
symbol #0



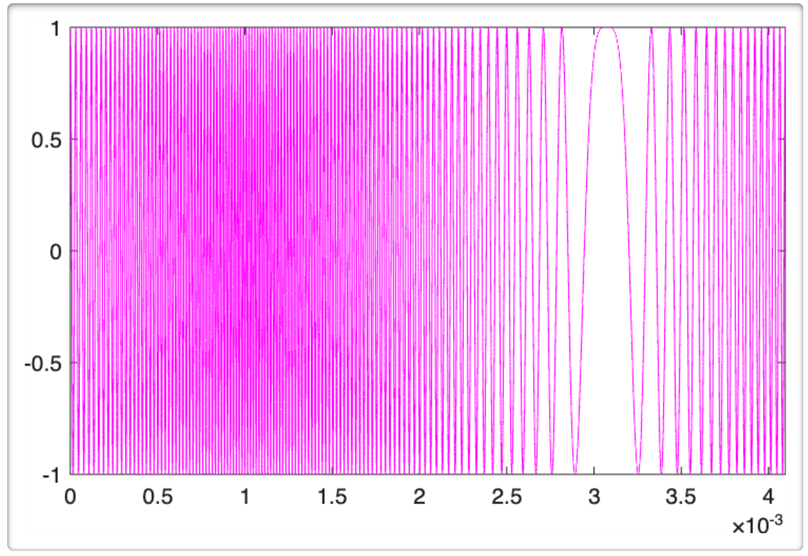
symbol #256

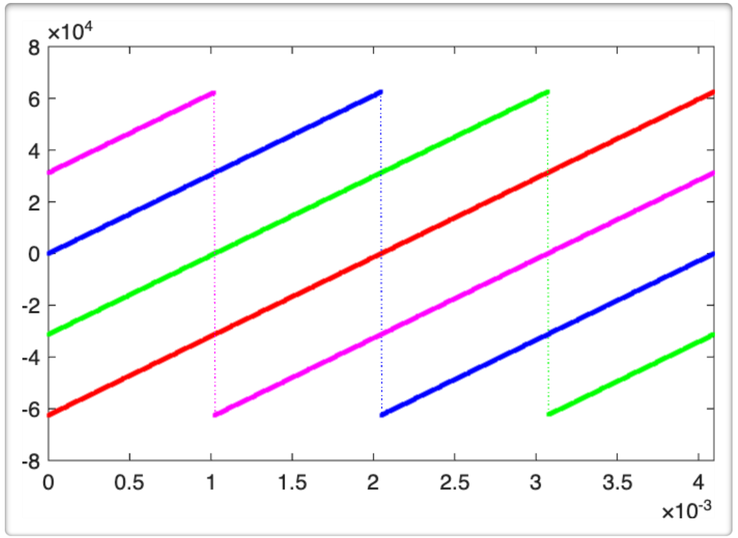
in-phase signal plane

symbol #128



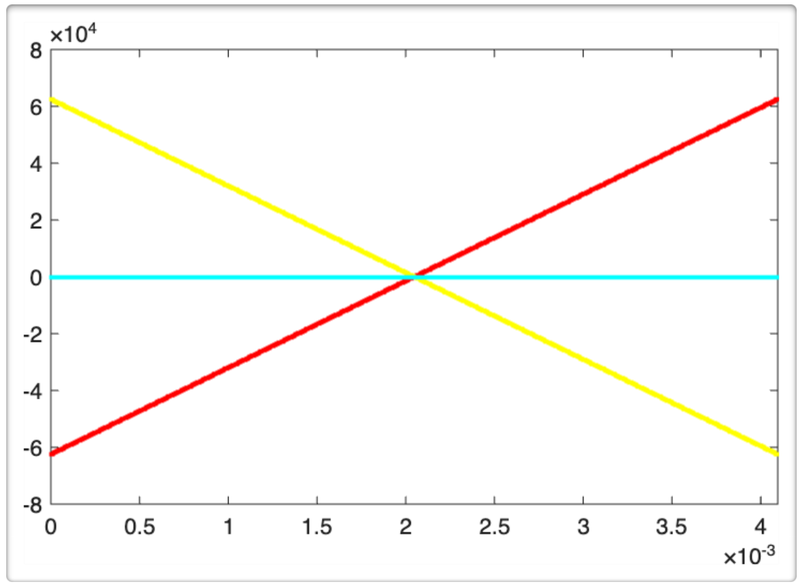
symbol #384





frequency plane modulated symbols

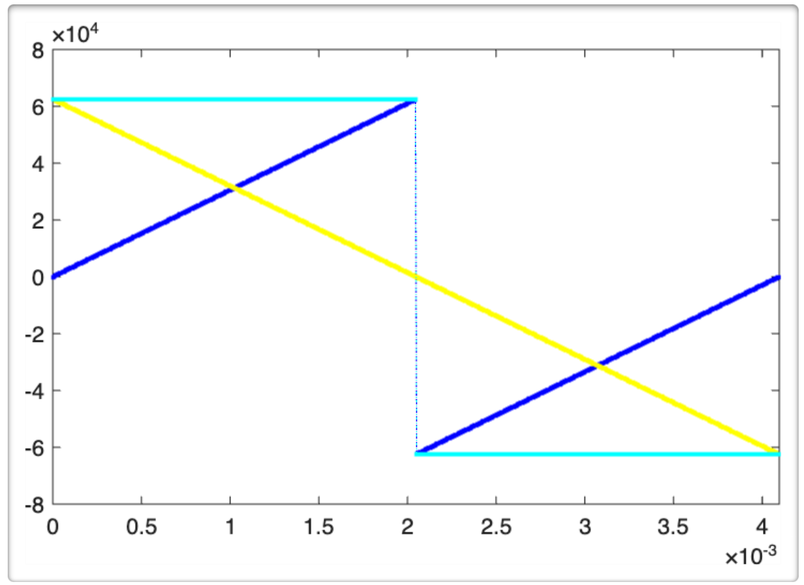
SF = 9, BW = 125 kHz
Ts = 4.096 ms



symbol #0

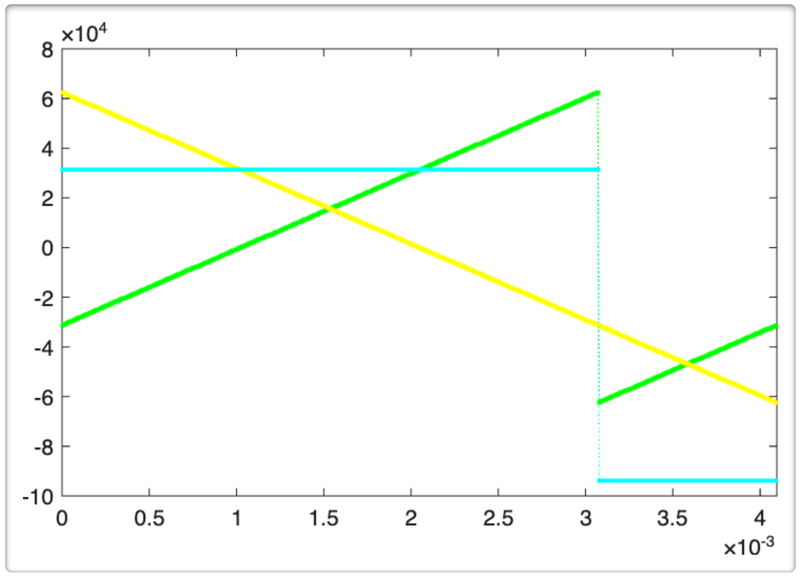
symbol #128

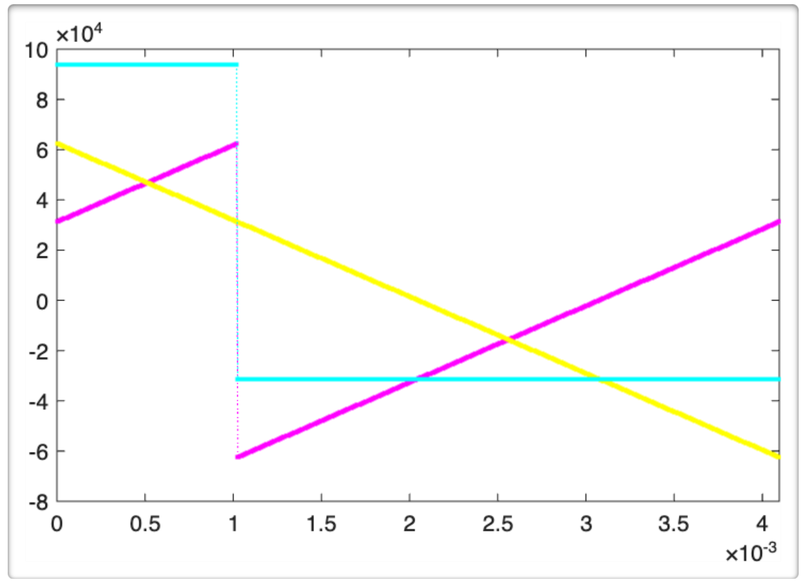
frequency plane dechirping



symbol #256

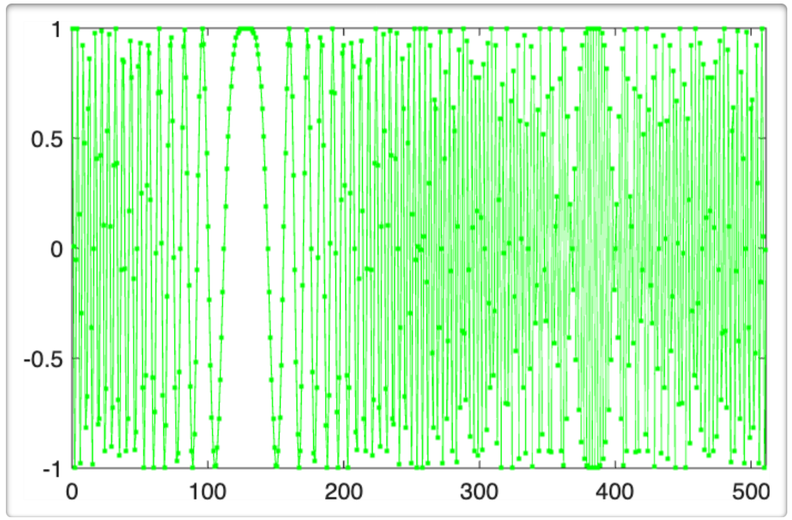
symbol #384

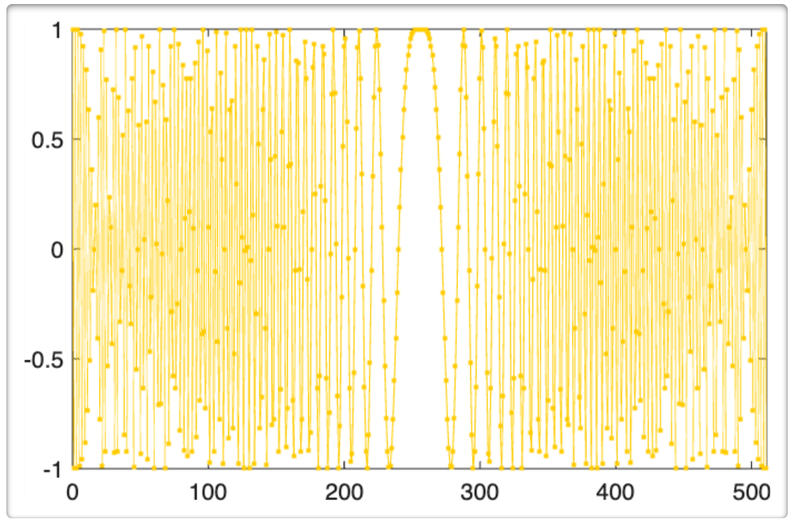


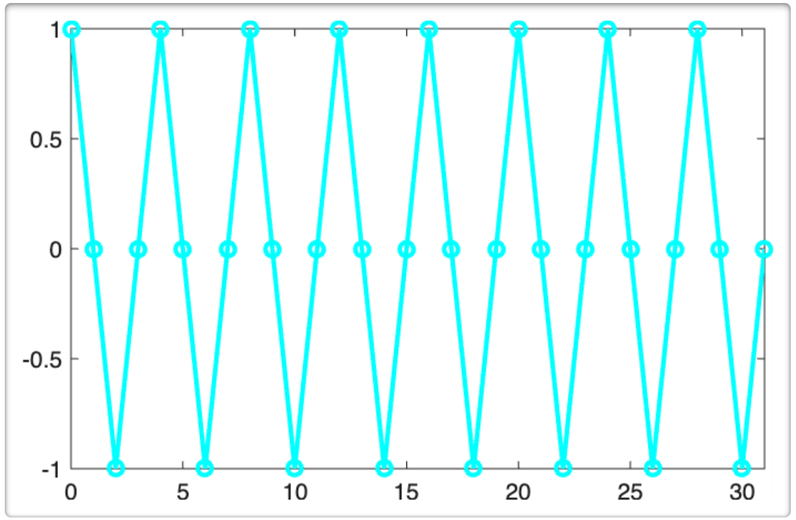


discrete time signal plane dechirping (BW sample rate gives 2^SF samples)

in-phase

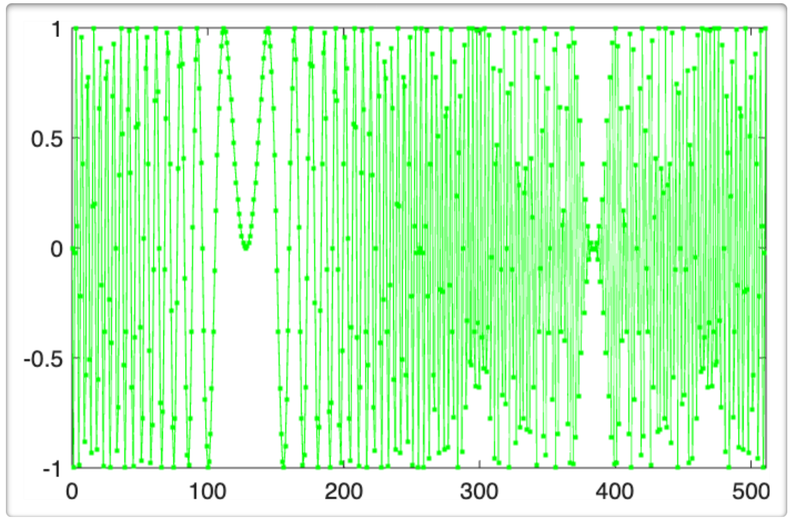


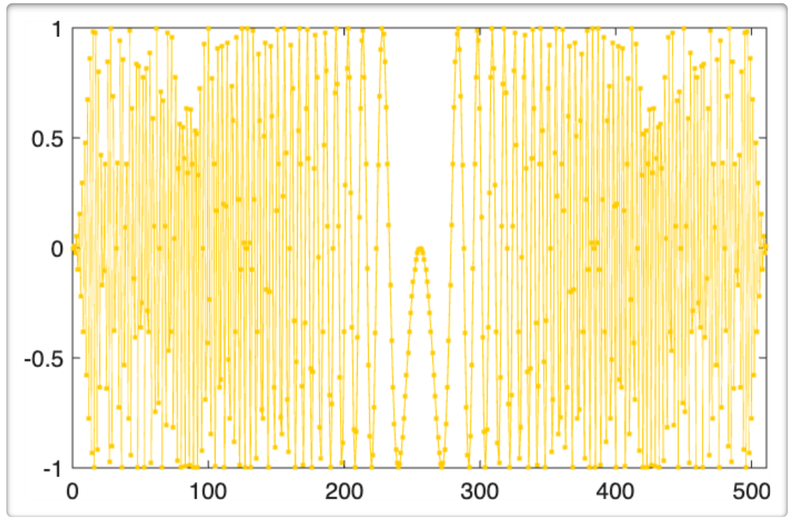


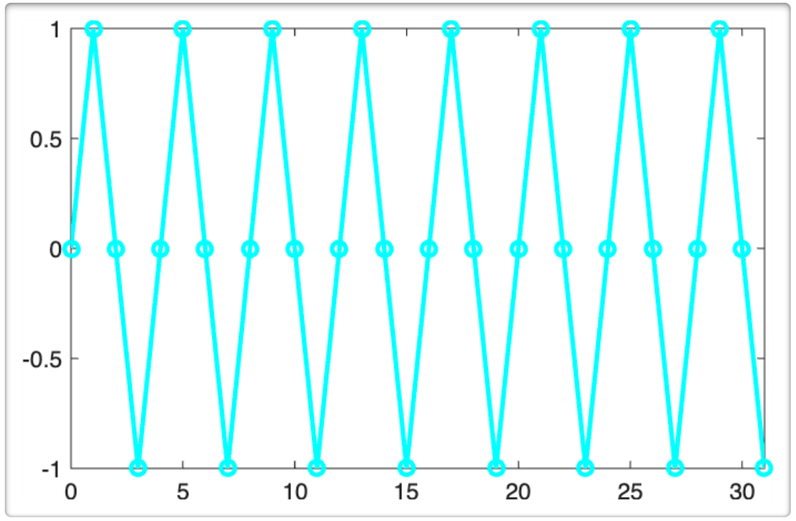


upchirp symbol #128 x basal downchirp = dechirped #128 (zoom)

quadrature



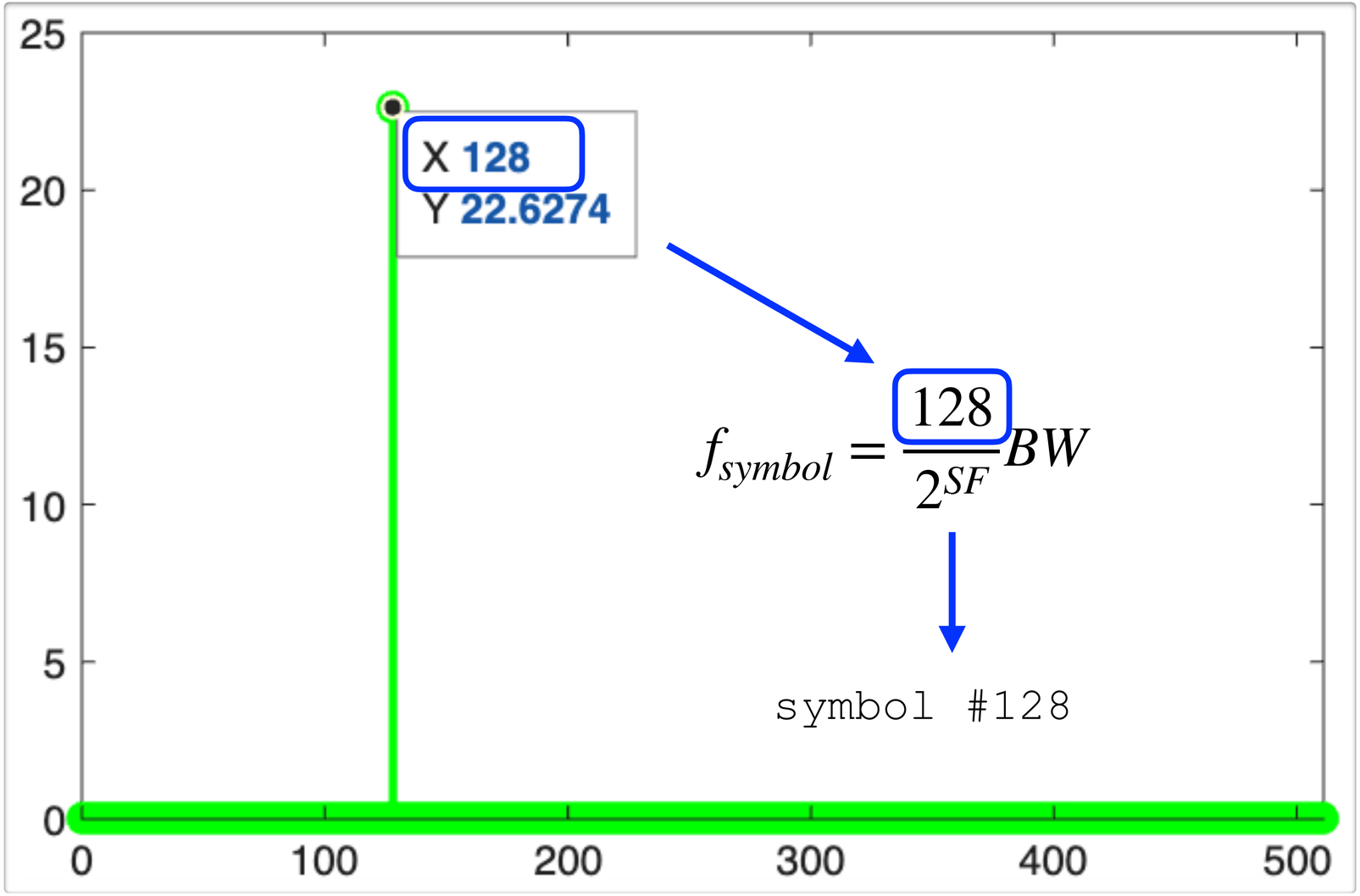




BW = 125 kHz, 1/BW = 8 us, SF = 9, 2^SF = 512

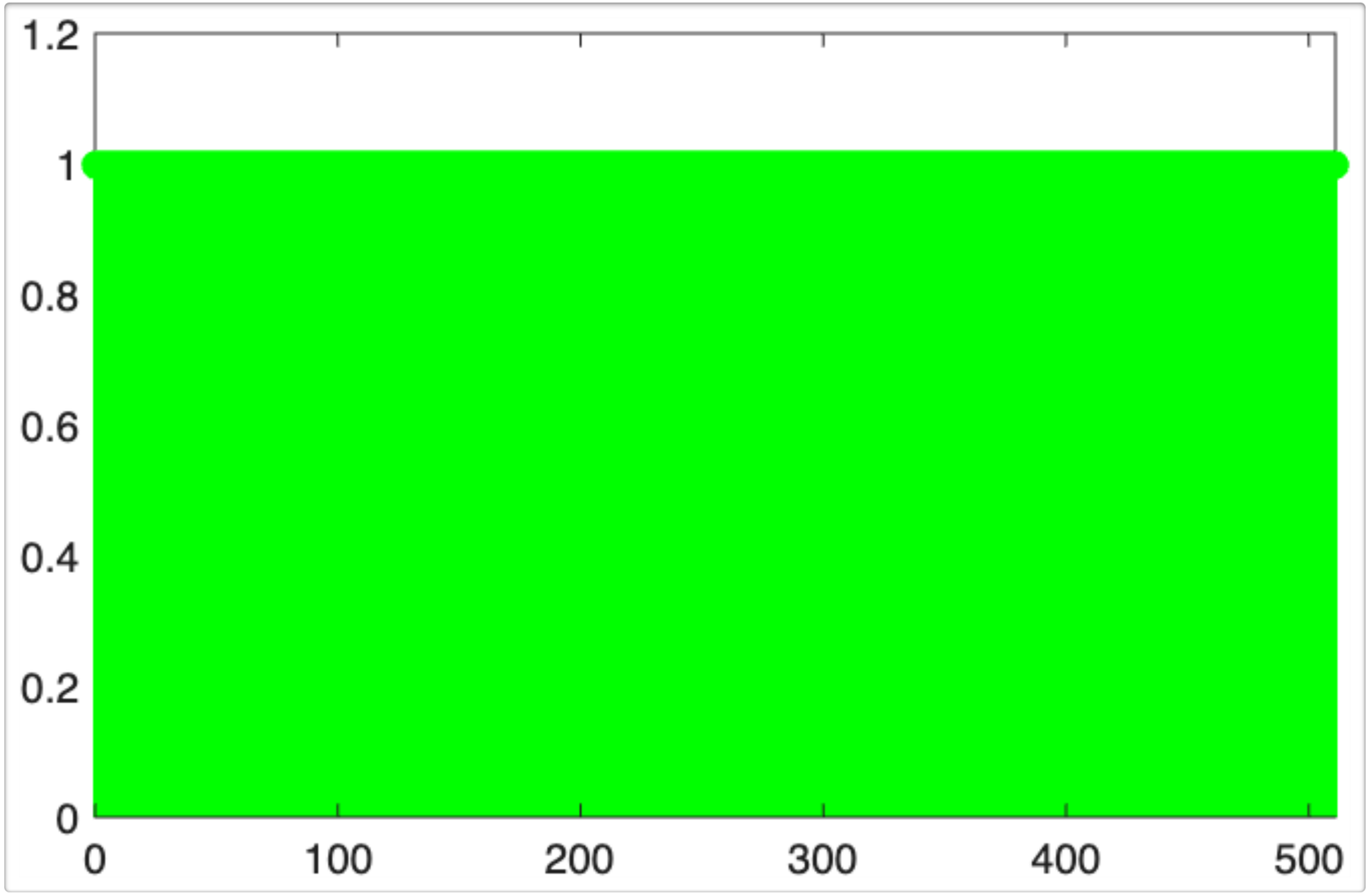
complex multiplication rules shall be applied: $(a+ib)\times(c+id)=(ac-bd)+i(ad+bc)$

final step: DFT-based decoding



SF = 9
2^SF = 512
BW = 125 kHz

What if we did not dechirp? We get white noise spectrum instead...



BW = 125 kHz
SF = 9
2^SF = 512

Chirp period Ts = 2^SF / BW [ms]

SF	5	6	7	8	9	10	11	12
BW [kHz]								
7.81	4.0973	8.1946	16.389	32.778	65.557	131.11	262.23	524.46
10.42	3.071	6.142	12.284	24.568	49.136	98.273	196.55	393.09
15.63	2.0473	4.0947	8.1894	16.379	32.758	65.515	131.03	262.06
20.83	1.5362	3.0725	6.145	12.29	24.58	49.16	98.32	196.64
31.25	1.024	2.048	4.096	8.192	16.384	32.768	65.536	131.07
41.67	0.76794	1.5359	3.0718	6.1435	12.287	24.574	49.148	98.296
62.5	0.512	1.024	2.048	4.096	8.192	16.384	32.768	65.536
125	0.256	0.512	1.024	2.048	4.096	8.192	16.384	32.768
250	0.128	0.256	0.512	1.024	**2.048**	4.096	**8.192**	16.384
500	0.064	0.128	0.256	0.512	1.024	2.048	4.096	8.192

MeshCore CZ //\ medium fast //\ long fast

Raw bit rate Rb = SF/Ts = (SF/2^SF)*BW [kbps]

SF	5	6	7	8	9	10	11	12
BW [kHz]								
7.81	1.2203	0.73219	0.42711	0.24406	0.13729	0.07627	0.041948	0.022881
10.42	1.6281	0.97688	0.56984	0.32562	0.18316	0.10176	0.055967	0.030527
15.63	2.4422	1.4653	0.85477	0.48844	0.27475	0.15264	0.08395	0.045791
20.83	3.2547	1.9528	1.1391	0.65094	0.36615	0.20342	0.11188	0.061025
31.25	4.8828	2.9297	1.709	0.97656	0.54932	0.30518	0.16785	0.091553
41.67	6.5109	3.9066	2.2788	1.3022	0.73248	0.40693	0.22381	0.12208
62.5	9.7656	5.8594	3.418	1.9531	1.0986	0.61035	0.33569	0.18311
125	19.531	11.719	6.8359	3.9062	2.1973	1.2207	0.67139	0.36621
250	39.062	23.438	13.672	7.8125	**4.3945**	2.4414	**1.3428**	0.73242
500	78.125	46.875	27.344	15.625	8.7891	4.8828	2.6855	1.4648

-- code rate omitted MeshCore CZ //\ medium fast //\ long fast

BW [kHz]
7.81
10.42
15.63
20.83
31.25
41.67
62.5
125
250
500

$$\text{Chip rate } R_c = \frac{2^{SF}}{T_s} = BW$$

- rather a pseudo quantity, since this was possibly a design axiom to allow for DSSS-like processing gain estimation (rule of thumb)
- there is no chipping sequence per se with CSS (Chirp Spread Spectrum)
- perhaps, we could consider baseband discrete-time samples as "chips"
- this axiom then gives T_s definition as used before

Processing gain PG = 10*Log[Rc / Rb] = 10*Log[(2^SF)/SF]

SF	5	6	7	8	9	10	11	12
PG [dB]	8.0618	10.28	12.621	15.051	**17.55**	20.103	**22.699**	25.332
SX126x typical min LoRa demodulator SNR [dB]	-2.5	-5	-7.5	-10	**-12.5**	-15	**-17.5**	-20

MeshCore CZ //\ medium fast //\ long fast

$$SNR = 10 \cdot \log_{10} \frac{signal_{pwr}}{noise_{pwr}} \text{ [dB]}$$

SEMTECH

SX1261/2

SX1261/2 Datasheet

Long Range, Low Power, sub-GHz RF Transceiver

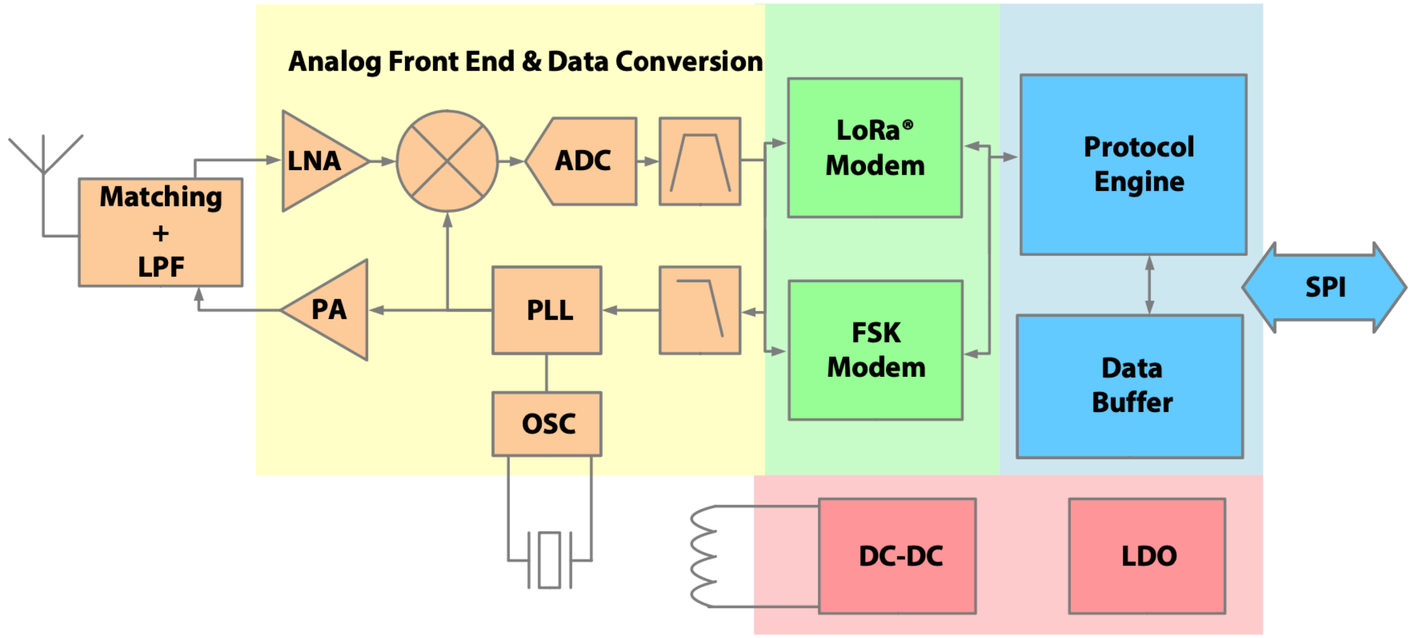


Figure A: SX1261/2 Block Diagram

LoRa IP generation: 2
Freq: 150 - 960 MHz
Link budget: 170 dB
Rx current max: 4.6 mA
Sensitivity max: -148 dBm
Tx power max: 22 dBm
SF: 5 - 12
BW: 7.8 - 500 kHz

-- SX1261/2 Data Sheet, Rev 2.2, DS.SX1261-2.W.APP, Semtech Corporation, December 2024

LoRa Packet Structure

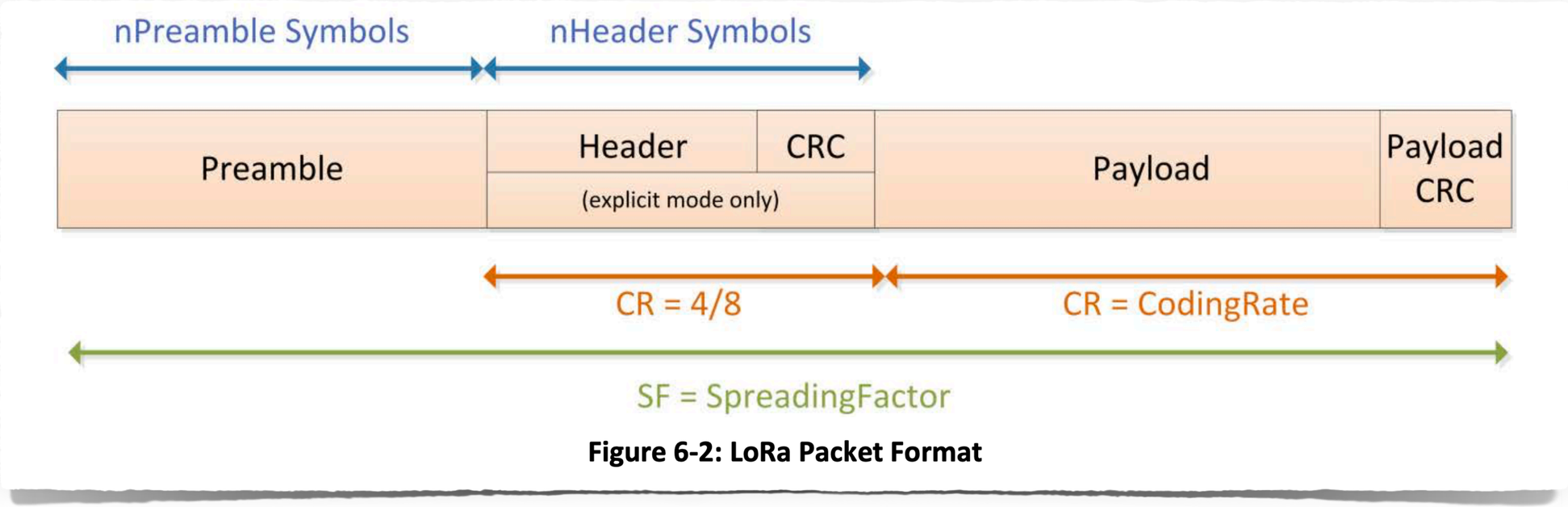


Figure 6-2: LoRa Packet Format

-- SX1261/2 Data Sheet, Rev 2.2, DS.SX1261-2.W.APP, Semtech Corporation, December 2024

LoRa Preamble with Sync Word (Network Identifier)

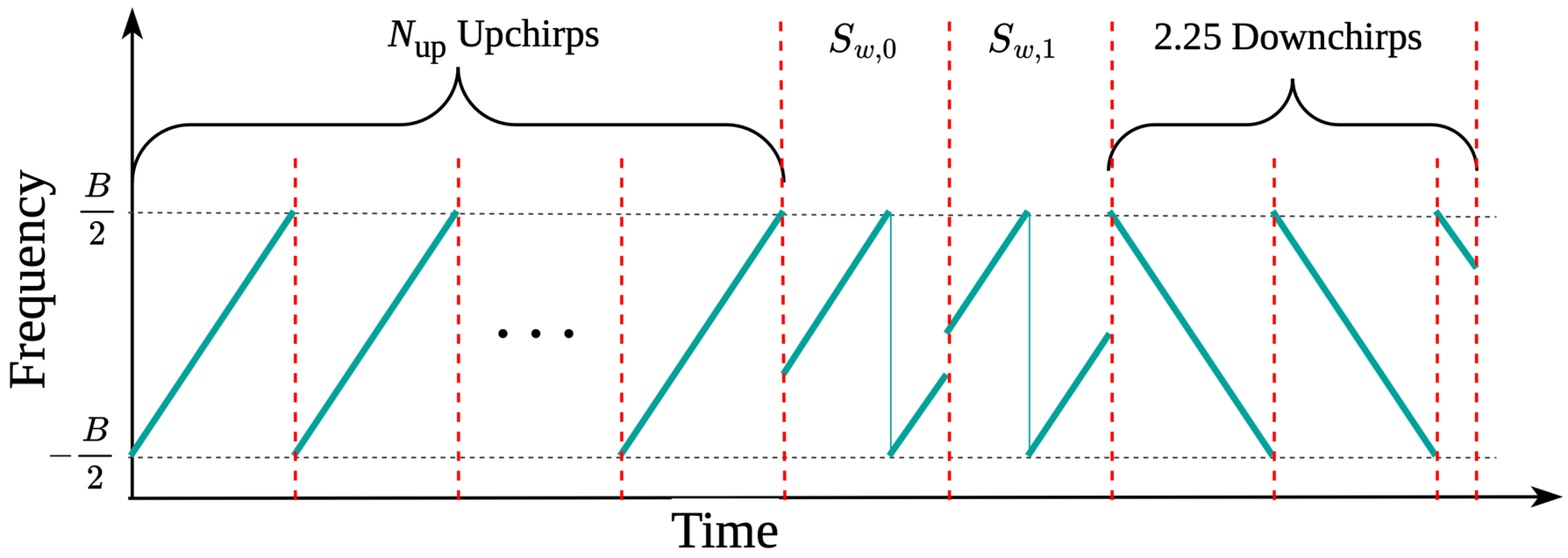


Figure 6. Spectrogram of the preamble of a LoRa frame

Sync word:
0x34 ~ LoRaWAN
0x2B ~ Meshtastic
0x12 ~ private / Meshcore

N_{up}:
16 ~ Meshtastic

-- Tapparel, J. and Burg, A.: *Design and Implementation of LoRa Physical Layer in GNU Radio*, 14th GNU Radio Conference, 2024

-- https://meshtastic.org/docs/overview/mesh-algo/

Example Network Header - Meshtastic

Offset	Length	Type	Usage
0x00	4 bytes	Integer	Packet Header: Destination. The destination's unique NodeID. `0xFFFFFFFF` for broadcast. Little-endian.
0x04	4 bytes	Integer	Packet Header: Sender. The sender's unique NodeID. Little-endian.
0x08	4 bytes	Integer	Packet Header: The sending node's unique packet ID for this packet. Little-endian.
0x0C	1 byte	Bits	Packet Header: Flags. See the header flags for usage.
0x0D	1 byte	Bits	Packet Header: Channel hash. Used as hint for decryption for the receiver.
0x0E	1 byte	Bytes	Packet Header: Next-hop used for relaying.
0x0F	1 byte	Bytes	Packet Header: Relay node of the current transmission.
0x10	Max. 237 bytes (excl. protobuf overhead)	Bytes	Actual packet data. Unused bytes are not transmitted.

Packet Header Flags

Index	# of Bits	Usage
0	3	HopLimit (see note in Layer 3)
3	1	WantAck
4	1	ViaMQTT (packet came via MQTT)
5	3	HopStart (original HopLimit)

-- https://meshtastic.org/docs/overview/mesh-algo/

SRD ~ Short Range Devices (EU)

CEPT ECC
Electronic Communications Committee

ERC Recommendation
70-03

Relating to the use of Short Range Devices (SRD)

approved 1997 (Tromsø)

Subsequent amendments 14 February 2025

Please Note

Implementation Status page 46

Frequency Band		Power / Magnetic Field	Spectrum access and mitigation requirements	Modulation / occupied bandwidth	ECC/ERC Deliverable	ETSI ENs	Notes
f3	169.4875-169.5875 MHz	10 mW e.r.p.	≤ 0.001% duty cycle except for 00:00 h to 06:00 h local time where the duty cycle limit is ≤ 0.1%	Not specified	ECC/DEC/(05)02		The frequency band is also identified in Annex 10
f4	169.5875-169.8125 MHz	10 mW e.r.p.	≤ 0.1% duty cycle	Not specified	ECC/DEC/(05)02		
g1	433.05-434.79 MHz	10 mW e.r.p.	≤ 10% duty cycle	Not specified			
g2	433.05-434.79 MHz	1 mW e.r.p.	No requirement	Not specified			
g3	434.04-434.79 MHz	10 mW e.r.p.	No requirement	≤ 25 kHz			
h0	862-863 MHz	25 mW e.r.p.	≤ 0.1% duty cycle	≤ 350 kHz			
h1.0	863-870 MHz (note 2)	25 mW e.r.p.	≤ 0.1% duty cycle (note 1)	≤ 100 kHz for 47 or more hop channels			For FHSS. Parts of the frequency band are also identified in Annexes 2, 3, 10 and 11
h1.2	863-870 MHz (note 2)	25 mW e.r.p. -4.5 dBm/100 kHz e.r.p.	≤ 0.1% duty cycle or LBT+AFA	Not specified			For Non-FHSS. Parts of the frequency band are also identified in Annexes 2, 3, 10 and 11
h1.3	863-865 MHz	25 mW e.r.p.	≤ 0.1% duty cycle or LBT+AFA	Not specified			The frequency band is also identified in Annexes 3 and 10
h1.4	865-868 MHz	25 mW e.r.p.	≤ 1% duty cycle or LBT+AFA	Not specified			The frequency band is also identified in Annexes 2, 3 and 11
h1.5	868-868.6 MHz	25 mW e.r.p.	≤ 1% duty cycle or LBT+AFA	Not specified			
h1.6	868.7-869.2 MHz	25 mW e.r.p.	≤ 0.1% duty cycle or LBT+AFA	Not specified			
h1.7	869.4-869.65 MHz	500 mW e.r.p.	≤ 10% duty cycle or LBT+AFA	Not specified			
h1.8	869.7-870 MHz	5 mW e.r.p.	No requirement	Not specified			
h1.9	869.7-870 MHz	25 mW e.r.p.	≤ 1% duty cycle or LBT+AFA	Not specified			

Annexes to ERC/REC 70-03	ALB	AND	AUT	AZE	BEL	BIH	BUL	CVA	CYP	CZE	D	DNK	E	EST	F	FIN	G	GEO	GRC	HNG	HOL	HRV	I	IRL	ISL	LIE	LTU	LUX	LVA	MCO	MDA	MKD	MLT	MNE	NOR	POL	POR	ROU	S	SMR	SRB	SUI	SVK	SVN	TUR	UKR
ANNEX 1: NON-SPECIFIC SHORT RANGE DEVICES																																														
Annex a: 13553-13567 kHz	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Annex b: 26957-27283 kHz	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Annex c1: 26990-27000 kHz	Y	Y	Y	?	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Annex c2: 27040-27050 kHz	Y	Y	Y	?	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Annex c3: 27090-27100 kHz	Y	Y	Y	?	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Annex c4: 27140-27150 kHz	Y	Y	Y	?	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Annex c5: 27190-27200 kHz	Y	Y	Y	?	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Annex d: 40.66-40.7 MHz	Y	Y	Y	?	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Annex e: 138.2-138.45 MHz	Y	N	Y	?	N	Y	Y	N	Y	Y	N	Y	N	Y	N	Y	Y	Y	Y	N	N	Y	Y	Y	Y	N	Y	Y	N	N	Y	Y	Y	Y	Y	N	Y	Y	N	N	Y	N	Y	N	Y	N	N
Annex f1: 169.4-169.475 MHz ECC/DEC/(05)02	Y	Y	Y	?	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	L	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	U
Annex f2: 169.4-169.4875 MHz ECC/DEC/(05)02	Y	Y	Y	?	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Annex f3: 169.4875-169.5875 MHz ECC/DEC/(05)02	Y	Y	Y	?	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Annex f4: 169.5875-169.8125 MHz ECC/DEC/(05)02	Y	Y	Y	?	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Annex g1: 433.05-434.79 MHz	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Annex g2: 433.05-434.79 MHz	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	L	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Annex g3: 434.04-434.79 MHz	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	L	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Annex h0: 862-863 MHz	Y	?	Y	?	Y	?	Y	Y	?	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	?	?	Y	Y	Y	Y	Y	Y	P	Y	Y	Y	Y	?	?	Y	?	Y	Y	Y	?	Y	Y	Y	Y	Y	?
Annex h1.0: 863-870 MHz	Y	Y	Y	?	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	L	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	Y	Y	Y	L	?	Y	Y	Y	Y	Y	Y
Annex h1.2: 863-870 MHz	Y	Y	Y	?	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	L	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	Y	Y	Y	L	?	Y	Y	Y	Y	Y	Y
Annex h1.3: 863-865 MHz	?	?	Y	?	Y	?	Y	?	?	Y	Y	Y	Y	Y	Y	Y	Y	?	Y	?	?	Y	Y	Y	Y	Y	Y	P	Y	?	Y	Y	?	?	Y	?	Y	Y	Y	?	Y	Y	Y	?	Y	?
Annex h1.4: 865-868 MHz	?	?	Y	?	Y	N	Y	?	?	Y	Y	Y	Y	Y	Y	Y	Y	?	Y	?	?	L	?	Y	Y	Y	Y	P	Y	?	Y	Y	?	?	Y	?	Y	Y	Y	?	Y	Y	Y	?	Y	?
Annex h1.5: 868-868.6 MHz	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	L	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	?	Y	Y	Y	Y	Y	Y
Annex h1.6: 868.7-869.2 MHz	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	L	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	?	Y	Y	Y	Y	Y	N
Annex h1.7: 869.4-869.65 MHz	Y	Y	Y	?	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	L	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	?	Y	Y	Y	Y	Y	N
Annex h1.8: 869.7-870 MHz	Y	Y	Y	?	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	L	Y	Y	Y	Y	Y	Y	Y	?	Y	Y	Y	Y	Y	Y	Y	Y	Y	?	Y	Y	Y	Y	Y	N
Annex h1.9: 869.7-870 MHz	?	?	Y	?	Y	N	Y	?	?	Y	?	Y	Y	Y	Y	Y	Y	Y	Y	Y	?	Y	Y	Y	Y	Y	Y	P	Y	?	?	Y	?	?	Y	?	Y	Y	Y	?	Y	Y	Y	?	Y	?
Annex h2: 870-874.4 MHz	Y	N	Y	N	L	N	Y	?	?	Y	N	Y	Y	Y	N	L	Y	Y	Y	Y	N	Y	Y	Y	Y	L	L	Y	N	?	Y	Y	?	?	Y	?	Y	N	Y	?	L	L	Y	Y	N	N
Annex h3: 915-919.4 MHz	Y	N	Y	N	L	N	Y	?	?	L	N	Y	Y	Y	N	N	Y	Y	Y	Y	N	Y	?	Y	Y	L	L	Y	N	?	Y	Y	?	?	Y	?	Y	L	Y	?	L	L	Y	Y	N	N

Highlighted yellow: ? = no info / see remarks	Highlighted yellow: N = not implemented / see remarks	Y = implemented	L = limited implementation / see remarks	P = planned	U = under study	NR = not regulated *)

//\ Meshtastic EU in 868 MHz band

869.525 MHz

-- https://meshtastic.org/docs/overview/radio-settings/

MeshCore CZ in 868 MHz band

869.432 MHz

-- https://meshcore.cz/nastaveni_site_meshcore_cz

LoRa Sniffing

- **Offline - harvest now, decode later**
  - SDR is an obvious option, see GitHub (etc.) for GNU Radio low-level blocks
  - for instance: https://github.com/rpp0/gr-lora, https://github.com/tapparelj/gr-lora_sdr
  - we have a plenty of time to get the parameters right - essentially "MATLAB exercise"
- **Online - realtime, as the communication unfolds**
  - tiny time window to estimate the modulator setup
  - still doable if we allow for certain capture lag - assumes the parameters do not vary with time (!)
  - complicates further with possible frequency hopping

Chasing Modulator Parameters

- We need at least **correct SF and BW**
  - **wrong SF** makes the dechirping with Fourier transform decoding fail
  - we would see a noise-like signal
  - **wrong BW** (actually wider) can capture unnecessary noise
  - furthermore, incorrect sampling makes the Nyquist folding frequency tricks fail
- Also a possibly different **base chirp polarity** is then a cherry on the cake
- Seems the **brute force** by parallel running radios is not that bad option
  - *this is probably expensive in realtime, or ... ?*

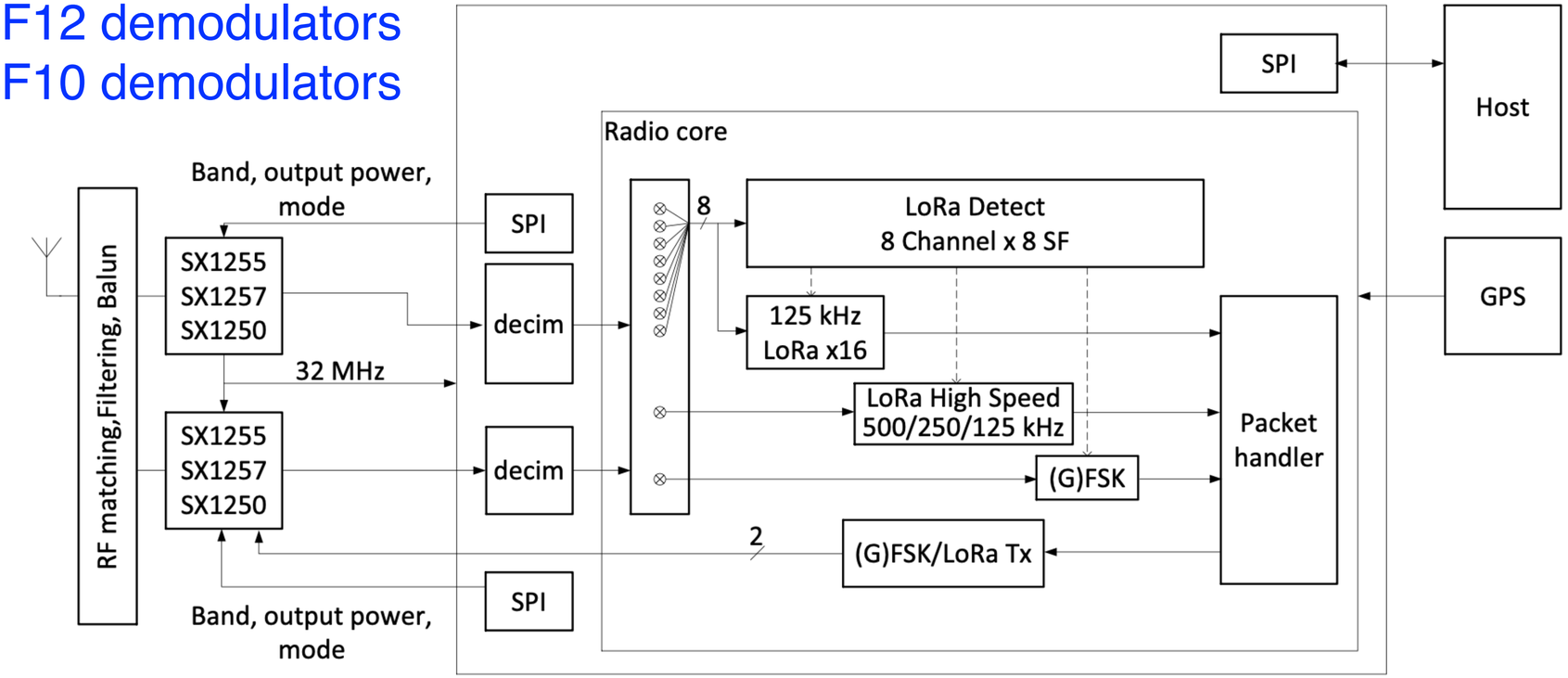
SEMTECH

SX1302

LoRa Gateway Baseband Processor

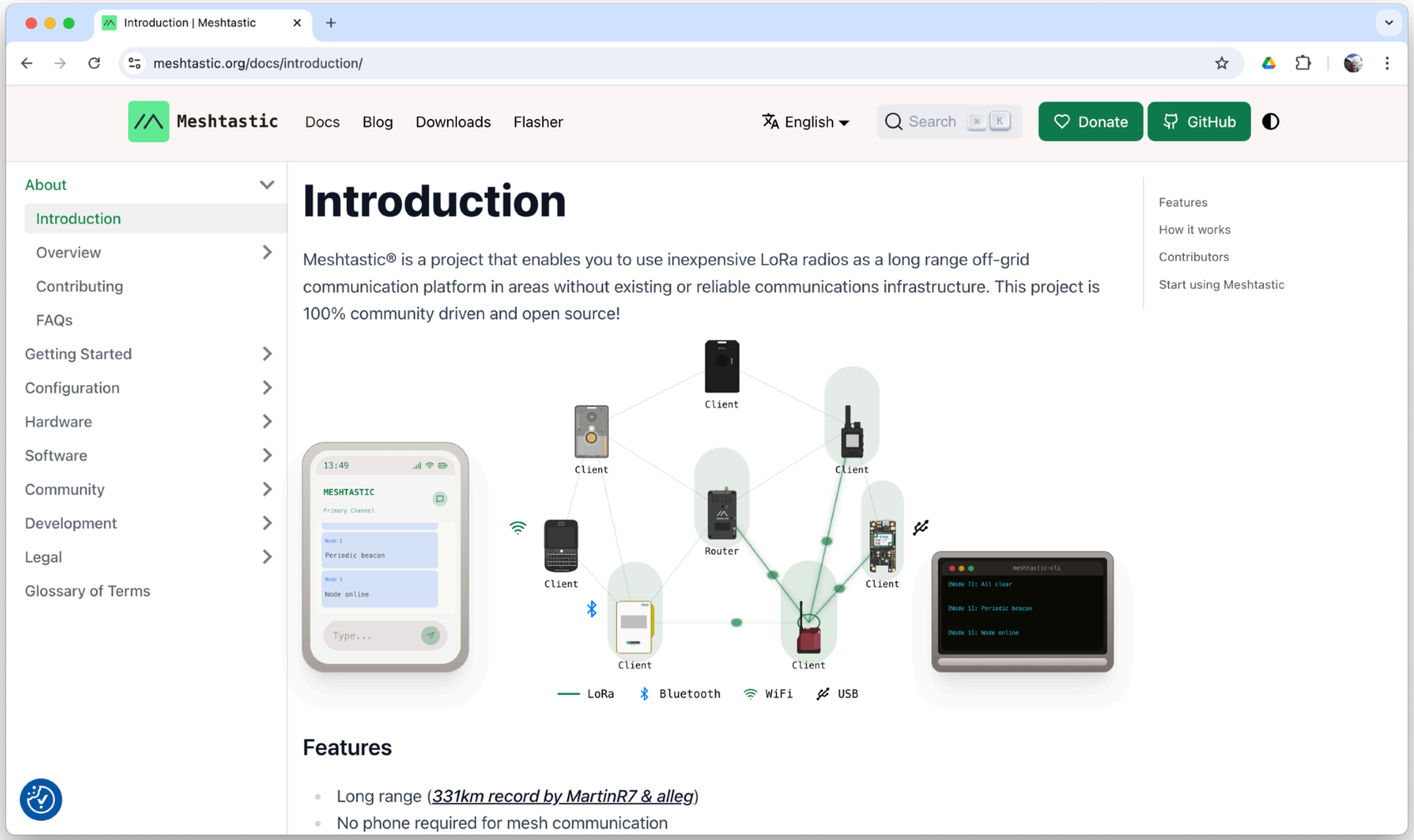
125kHz LoRa reception with:

- 8 x 8 channels packet detectors
- 8 x SF5-SF12 demodulators
- 8 x SF5-SF10 demodulators



-- SX1302 Data Sheet, Rev 1.2, DS.SX1302.W.APP Semtech Corporation, October 2020

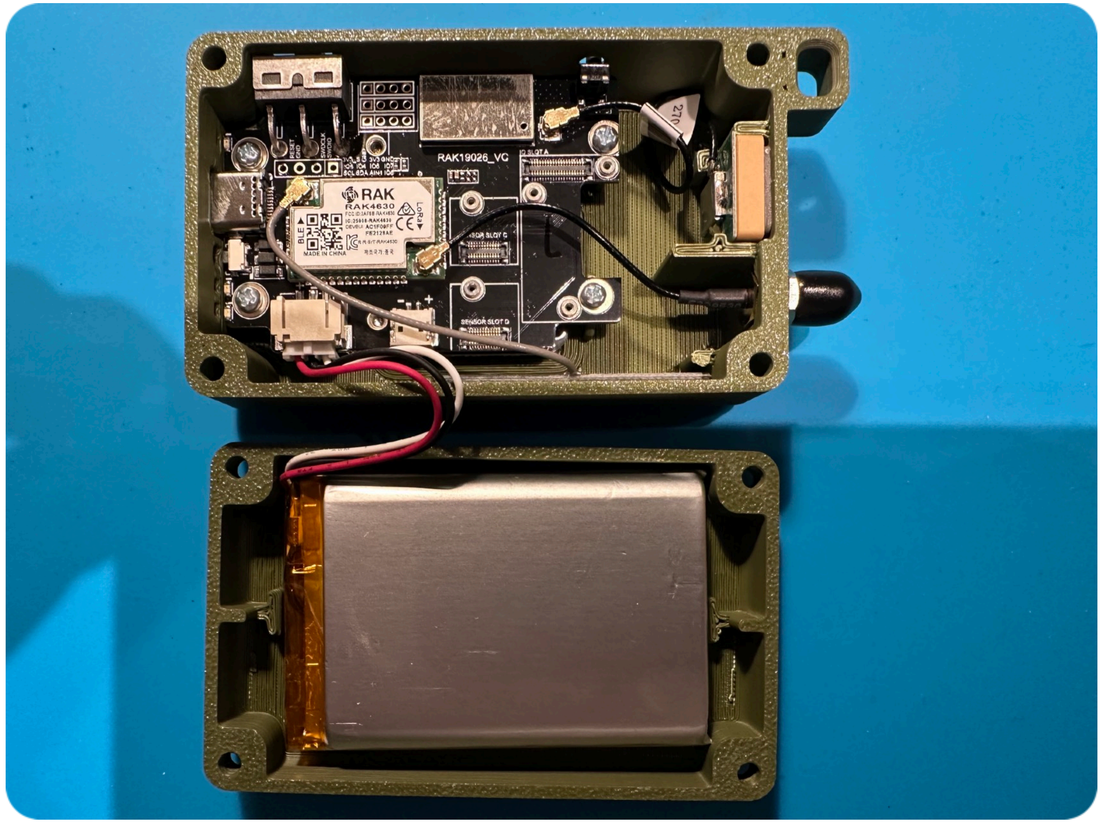
Meshtastic /\ - Easy Way to Practice (with ad hoc mesh topology)



-- https://meshtastic.org/docs/introduction/

RAK WisMesh Pocket V2

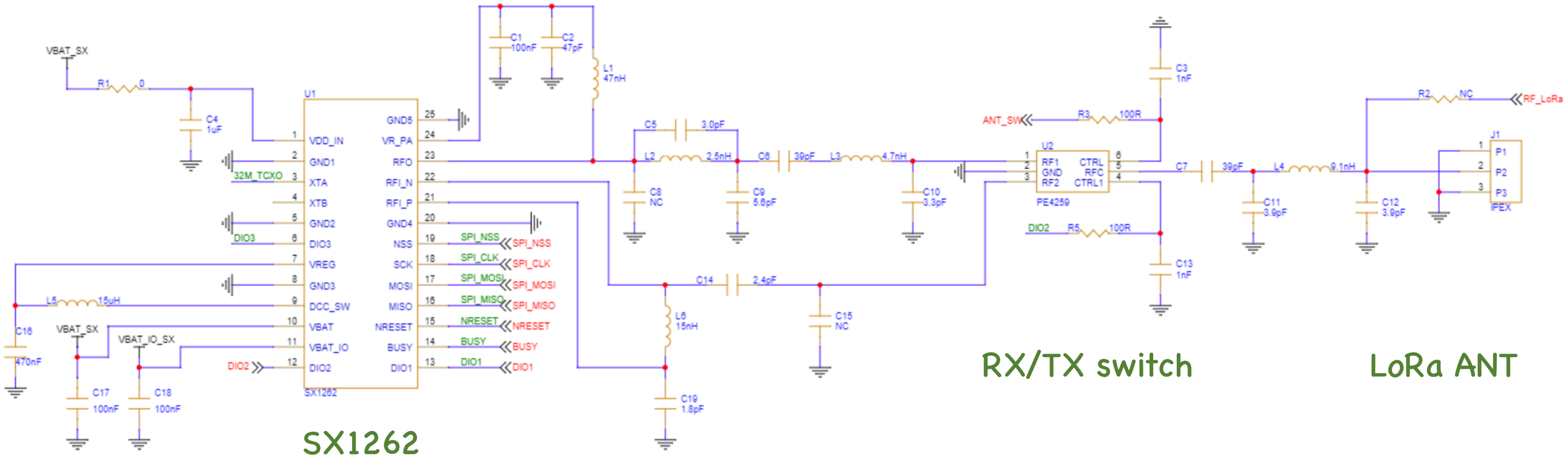
LoRa RF: Semtech SX1262
controller: Nordic nRF52840
display: 1.3" OLED
battery: 3200mAh
supports: LoRa, BLE, GNSS, NFC-A, USB-C*



-- https://store.rakwireless.com/products/wismesh-pocket

-- https://hexaspot.com/products/wismesh-pocket-v2-ready-to-use-meshtastic-devicet

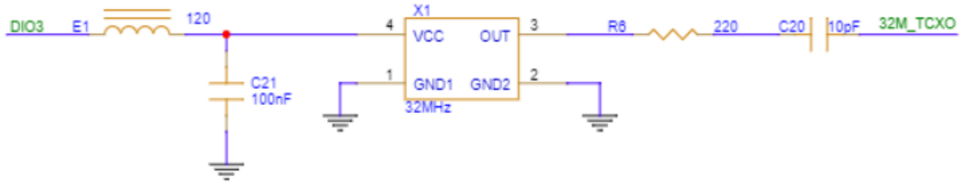
*) rather USB 2.0 via USB-C



SX1262

RX/TX switch

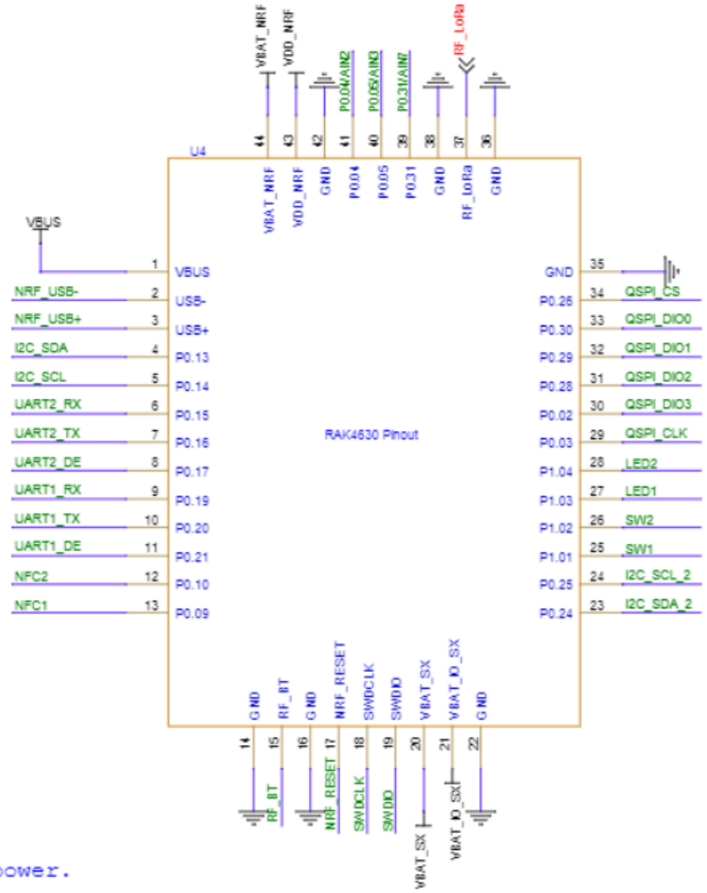
LoRa ANT



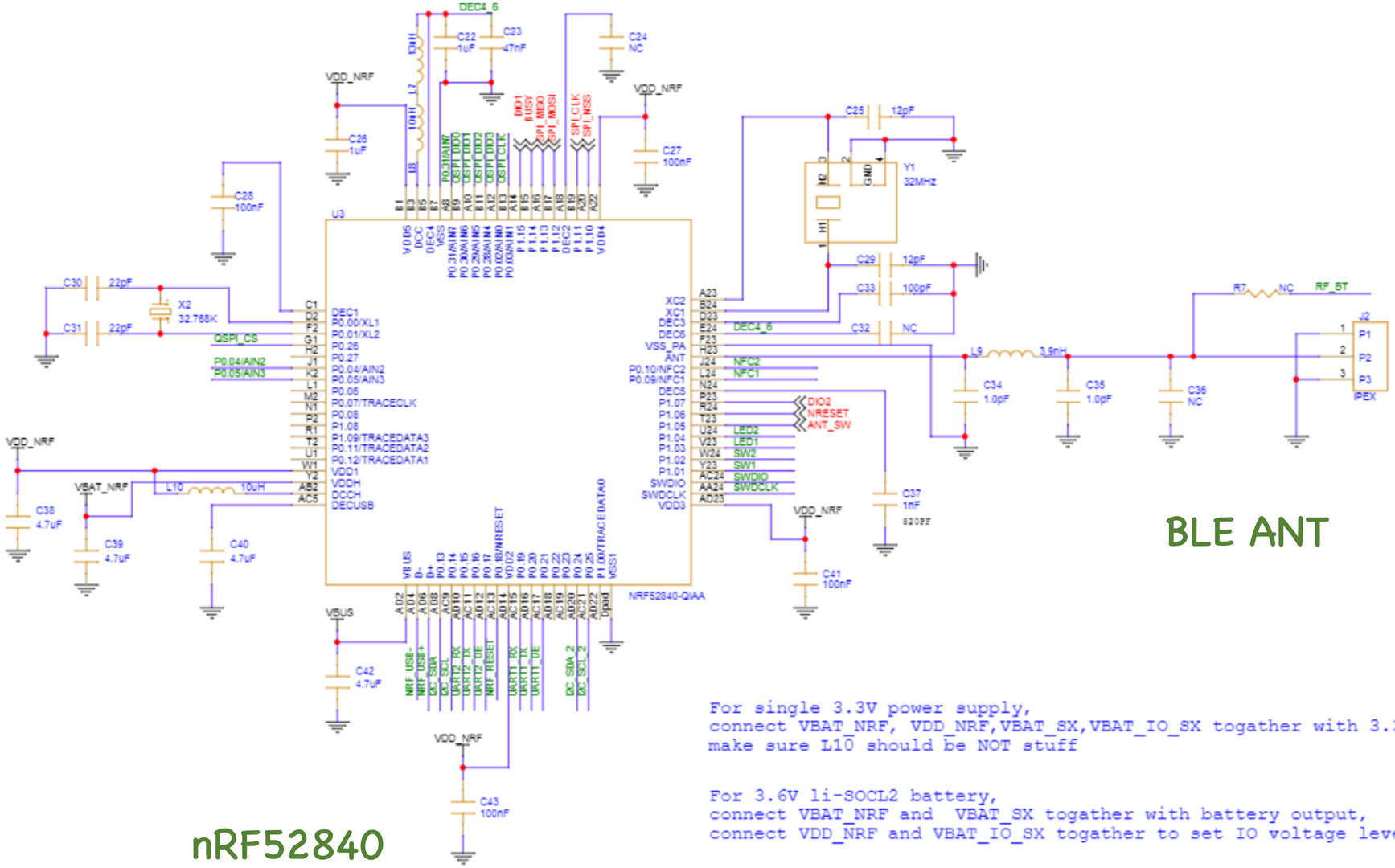
TCXO

-- https://docs.rakwireless.com/product-categories/wisduo/rak4630-module/datasheet/

PCB pinout



BLE ANT



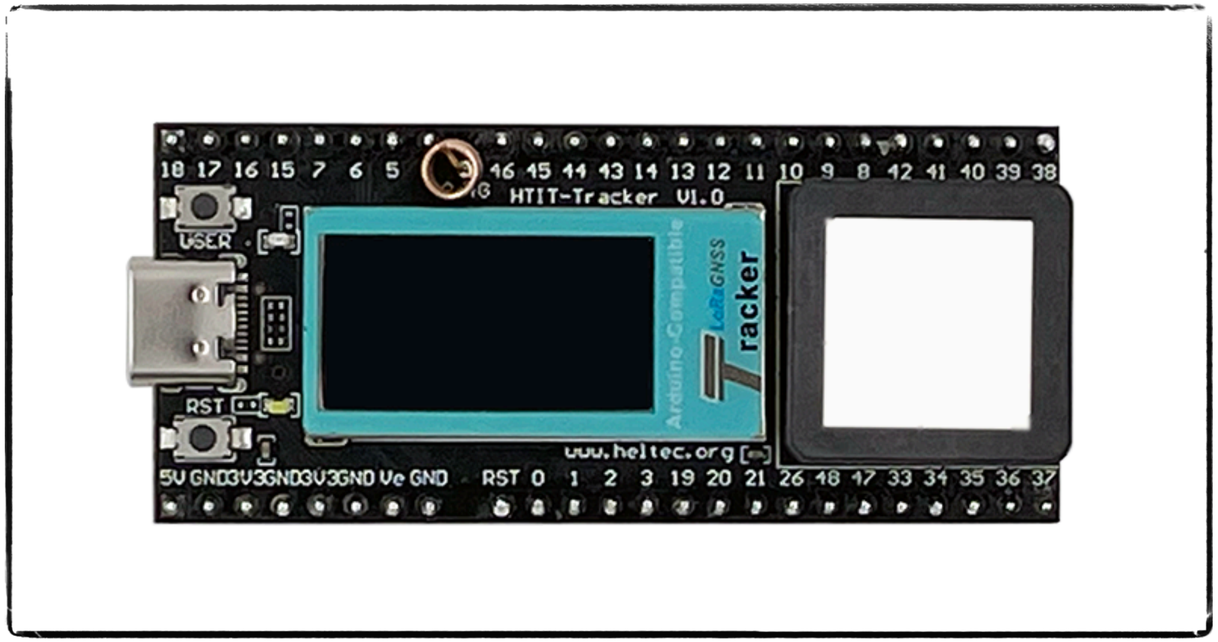
nRF52840

For single 3.3V power supply,
connect VBAT_NRF, VDD_NRF,VBAT_SX,VBAT_IO_SX togather with 3.3V power.
make sure L10 should be NOT stuff

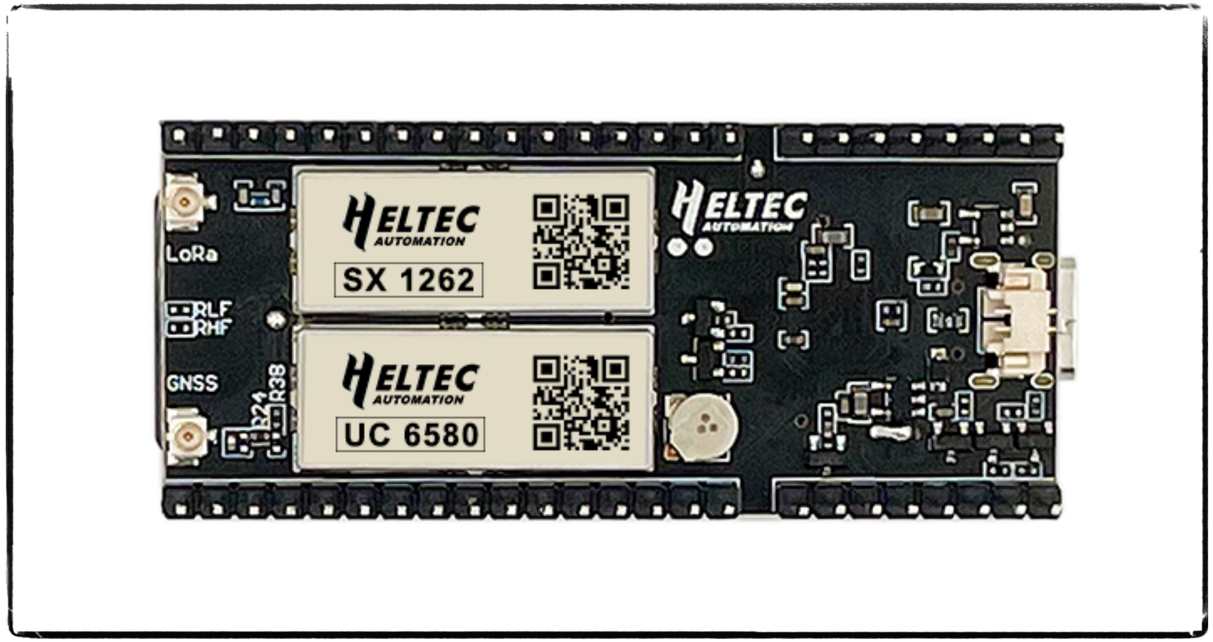
For 3.6V li-SOCL2 battery,
connect VBAT_NRF and VBAT_SX togather with battery output,
connect VDD_NRF and VBAT_IO_SX togather to set IO voltage level.

For 4.2V li-MnO2 battery,
connect VBAT_NRF with battery output,
should add external DC-DC convert or LDO for VBAT_SX(3.3V)
connect VDD_NRF and VBAT_IO_SX togather to set IO voltage level.

-- https://docs.rakwireless.com/product-categories/wisduo/rak4630-module/datasheet/



LoRa RF: Semtech SX1262
controller: Espressif ESP32-S3FN8
display: 0.96" TFT
battery: none, 3.7V LiPo ready
supports: LoRa, BLE, WiFi, GNSS, USB-C*



Heltec Wireless Tracker V1.1

-- https://heltec.org/project/Wireless-Tracker/

-- https://www.laskakit.cz/heltec-wireless-tracker-v1-1-868mhz-sx1262-uc6580-wifi-gps-modul/

*) rather USB 2.0 via USB-C

Pixelure 10 dBi Gain/868MHz

-- https://www.amazon.de/dp/B0F8VHHS1G

Meshtastic Web Flasher

flasher.meshtastic.org

MESHTASTIC WEB FLASHER

Update your Meshtastic device with official firmware, straight from your browser

1

Select Target Device

2

Select Firmware

3

Flash

DEVICE

Plug in your device via USB. Please ensure the cable is not a power-only one.

FIRMWARE

Choose from the release options or upload a release zip downloaded from Github.

FLASH

Flash your device. Choose whether you wish to update your device or wipe the flash and install from scratch.

-- https://flasher.meshtastic.org/

Meshtastic Web Flasher

flasher.meshtastic.org

Select your connected device

All Devices | RAK | B&Q | LilyGo | Seeed | Heltec | Elecrow | M5Stack | NomadStar | muzi WORKS

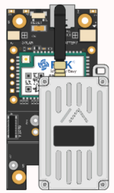
esp32 | nrf52840 | esp32-s3 | rp2040 | esp32-c3 | esp32-c6

If your connected device already has Meshtastic installed, you can automatically detect it: Auto-detect

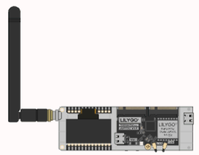
Supported Devices

LILYGO T-Echo
nrf52840 LilyGo

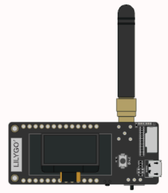
RAK WisBlock 4631
nrf52840 RAK



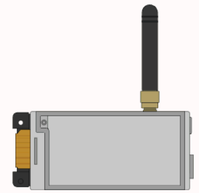
LILYGO T-Beam Supreme
esp32s3 LilyGo



LILYGO T-LoRa T3-S3
esp32s3 LilyGo



LILYGO T-LoRa T3-S3 E-Ink
esp32s3 LilyGo



RAK WisMesh Repeater
nrf52840 RAK

LILYGO T-Echo Plus
nrf52840 LilyGo

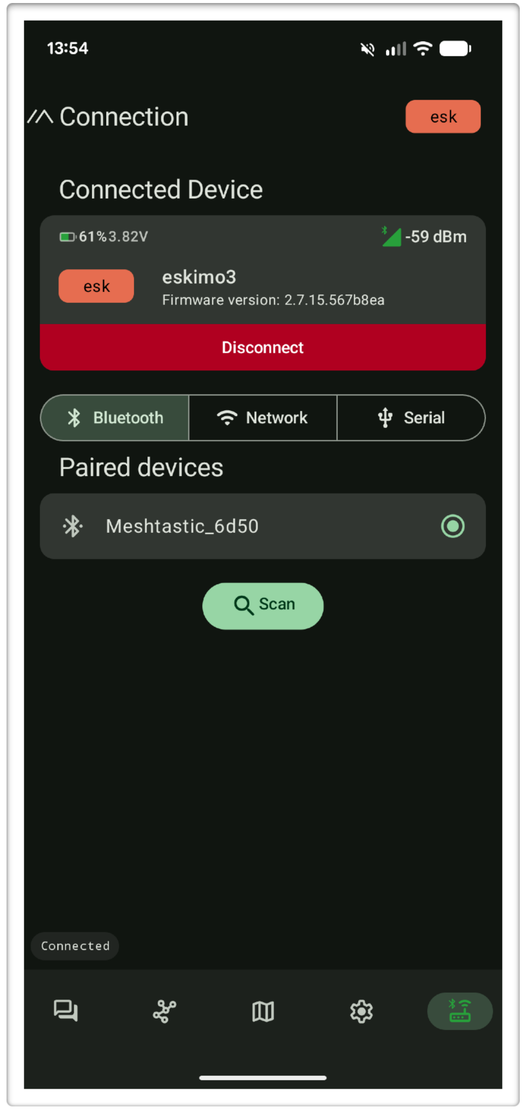
Heltec V3
esp32s3 Heltec

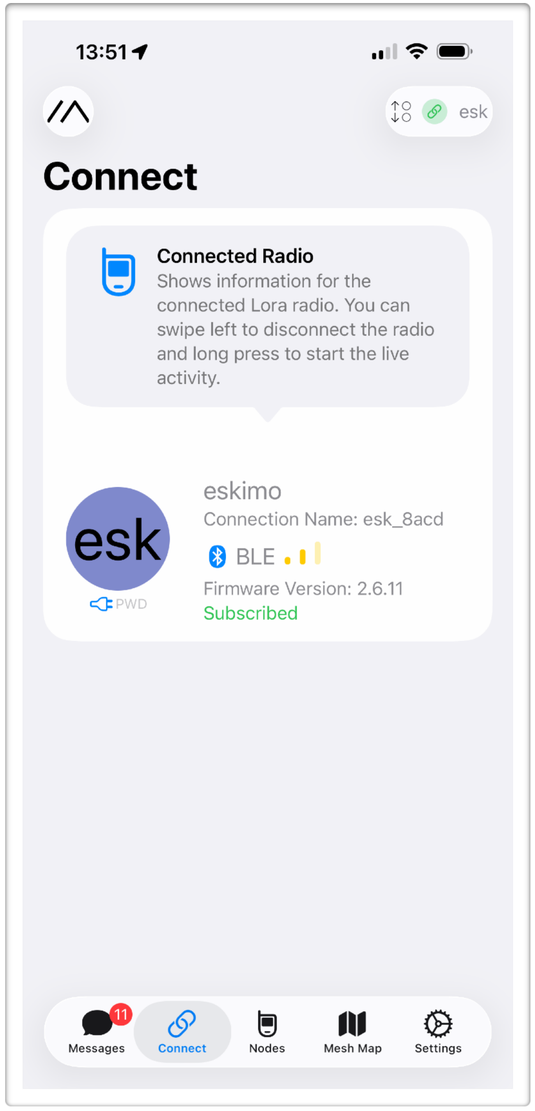
Heltec Wireless Stick Lite V3
esp32s3 Heltec

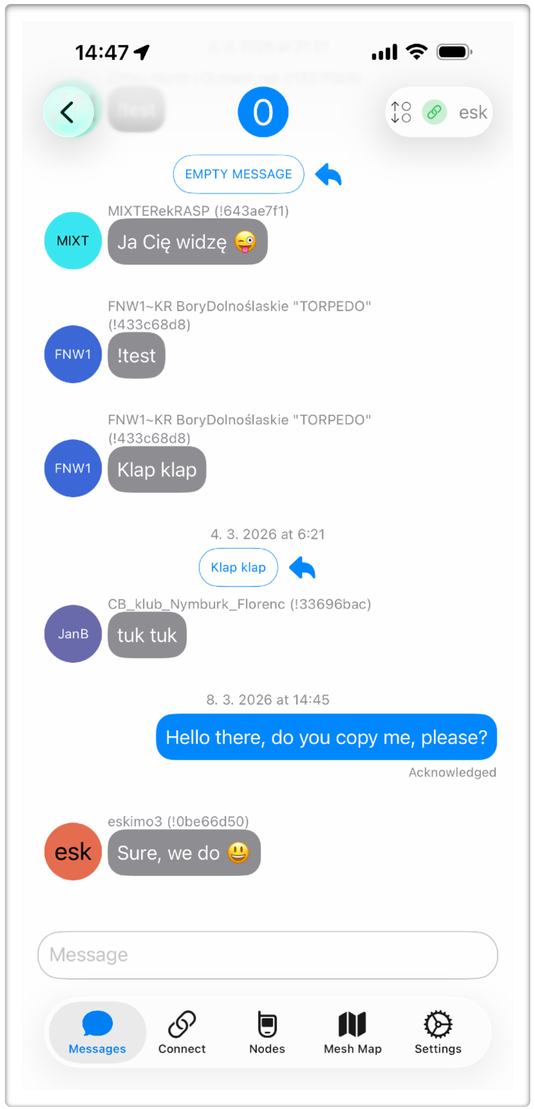
Heltec Wireless Tracker V1.1
esp32s3 Heltec

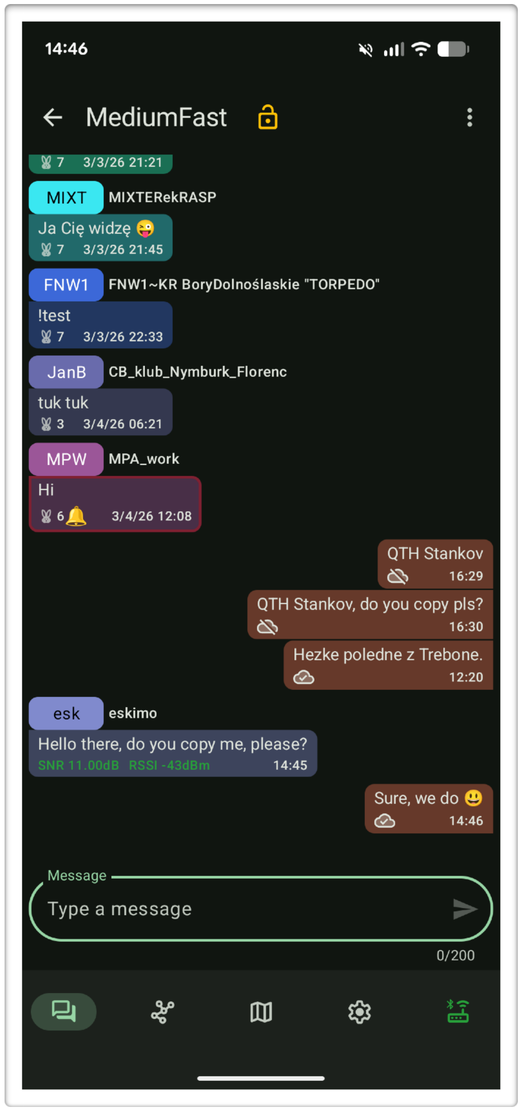
-- https://flasher.meshtastic.org/

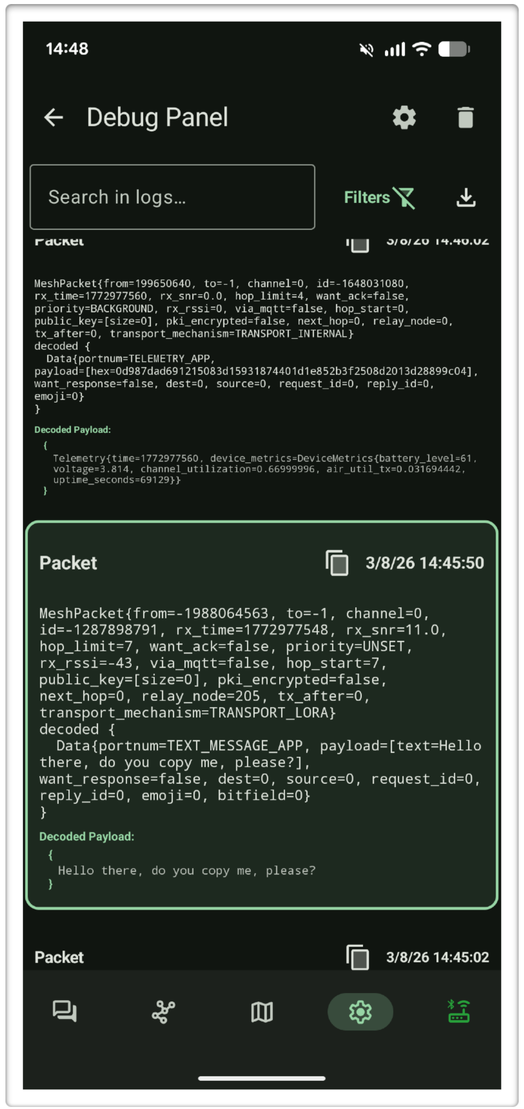
After flashing FW, connect the device to the client application (BLE)

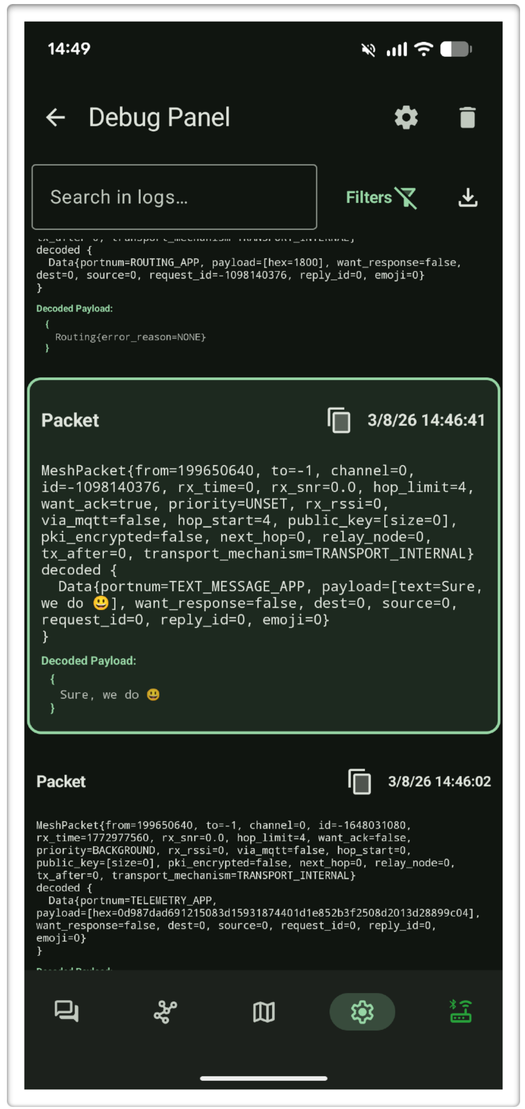


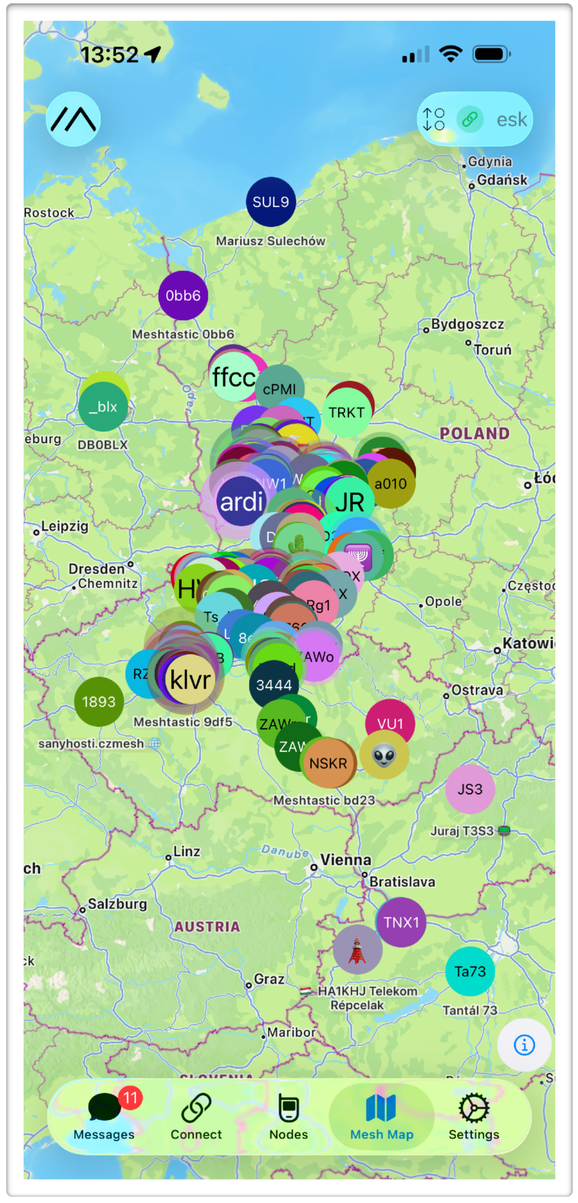



14:47
0
esk
EMPTY MESSAGE
MIXTERekRASP (!643ae7f1)
MIXT
Ja Cię widzę 😜
FNW1~KR BoryDolnośląskie "TORPEDO" (!433c68d8)
FNW1
!test
FNW1~KR BoryDolnośląskie "TORPEDO" (!433c68d8)
FNW1
Klap klap
4. 3. 2026 at 6:21
Klap klap
CB_klub_Nymburk_Florenc (!33696bac)
JanB
tuk tuk
8. 3. 2026 at 14:45
Hello there, do you copy me, please?
Acknowledged
eskimo3 (!0be66d50)
esk
Sure, we do 😃
Message
Messages
Connect
Nodes
Mesh Map
Settings

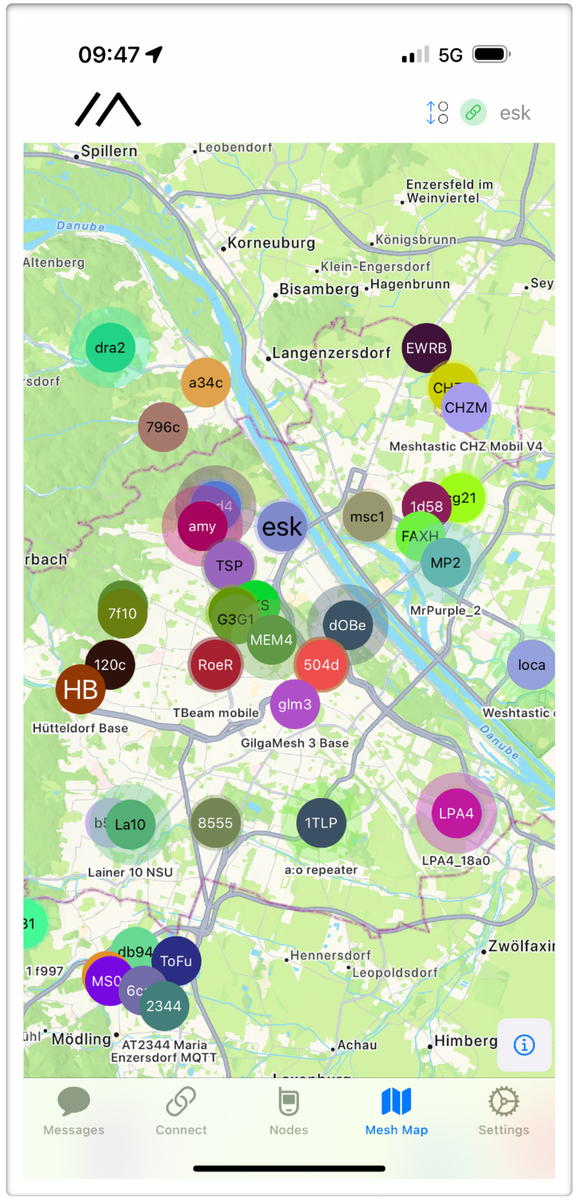

14:46
MediumFast
7 3/3/26 21:21
MIXT
MIXTERekRASP
Ja Cię widzę 😜
7 3/3/26 21:45
FNW1
FNW1~KR BoryDolnośląskie "TORPEDO"
!test
7 3/3/26 22:33
JanB
CB_klub_Nymburk_Florenc
tuk tuk
3 3/4/26 06:21
MPW
MPA_work
Hi
6 3/4/26 12:08
QTH Stankov
16:29
QTH Stankov, do you copy pls?
16:30
Hezke poledne z Trebone.
12:20
esk
eskimo
Hello there, do you copy me, please?
SNR 11.00dB RSSI -43dBm 14:45
Sure, we do 😃
14:46
Message
Type a message
0/200


14:48
Debug Panel
Search in logs...
Filters
MeshPacket{from=199650640, to=-1, channel=0, id=-1648031080, rx_time=1772977560, rx_snr=0.0, hop_limit=4, want_ack=false, priority=BACKGROUND, rx_rssi=0, via_mqtt=false, hop_start=0, public_key=[size=0], pki_encrypted=false, next_hop=0, relay_node=0, tx_after=0, transport_mechanism=TRANSPORT_INTERNAL}
decoded {
Data{portnum=TELEMETRY_APP, payload=[hex=0d987dad691215083d15931874401d1e852b3f2508d2013d28899c04], want_response=false, dest=0, source=0, request_id=0, reply_id=0, emoji=0}
}
Decoded Payload:
{
Telemetry{time=1772977560, device_metrics=DeviceMetrics{battery_level=61, voltage=3.814, channel_utilization=0.66999996, air_util_tx=0.031694442, uptime_seconds=69129}}
}
Packet
3/8/26 14:45:50
MeshPacket{from=-1988064563, to=-1, channel=0, id=-1287898791, rx_time=1772977548, rx_snr=11.0, hop_limit=7, want_ack=false, priority=UNSET, rx_rssi=-43, via_mqtt=false, hop_start=7, public_key=[size=0], pki_encrypted=false, next_hop=0, relay_node=205, tx_after=0, transport_mechanism=TRANSPORT_LORA}
decoded {
Data{portnum=TEXT_MESSAGE_APP, payload=[text=Hello there, do you copy me, please?], want_response=false, dest=0, source=0, request_id=0, reply_id=0, emoji=0, bitfield=0}
}
Decoded Payload:
{
Hello there, do you copy me, please?
}
Packet
3/8/26 14:45:02


14:49
Debug Panel
Search in logs...
Filters
decoded {
Data{portnum=ROUTING_APP, payload=[hex=1800], want_response=false, dest=0, source=0, request_id=-1098140376, reply_id=0, emoji=0}
}
Decoded Payload:
{
Routing{error_reason=NONE}
}
Packet
3/8/26 14:46:41
MeshPacket{from=199650640, to=-1, channel=0, id=-1098140376, rx_time=0, rx_snr=0.0, hop_limit=4, want_ack=true, priority=UNSET, rx_rssi=0, via_mqtt=false, hop_start=4, public_key=[size=0], pki_encrypted=false, next_hop=0, relay_node=0, tx_after=0, transport_mechanism=TRANSPORT_INTERNAL}
decoded {
Data{portnum=TEXT_MESSAGE_APP, payload=[text=Sure, we do 😃], want_response=false, dest=0, source=0, request_id=0, reply_id=0, emoji=0}
}
Decoded Payload:
{
Sure, we do 😃
}
Packet
3/8/26 14:46:02
MeshPacket{from=199650640, to=-1, channel=0, id=-1648031080, rx_time=1772977560, rx_snr=0.0, hop_limit=4, want_ack=false, priority=BACKGROUND, rx_rssi=0, via_mqtt=false, hop_start=0, public_key=[size=0], pki_encrypted=false, next_hop=0, relay_node=0, tx_after=0, transport_mechanism=TRANSPORT_INTERNAL}
decoded {
Data{portnum=TELEMETRY_APP, payload=[hex=0d987dad691215083d15931874401d1e852b3f2508d2013d28899c04], want_response=false, dest=0, source=0, request_id=0, reply_id=0, emoji=0}
}

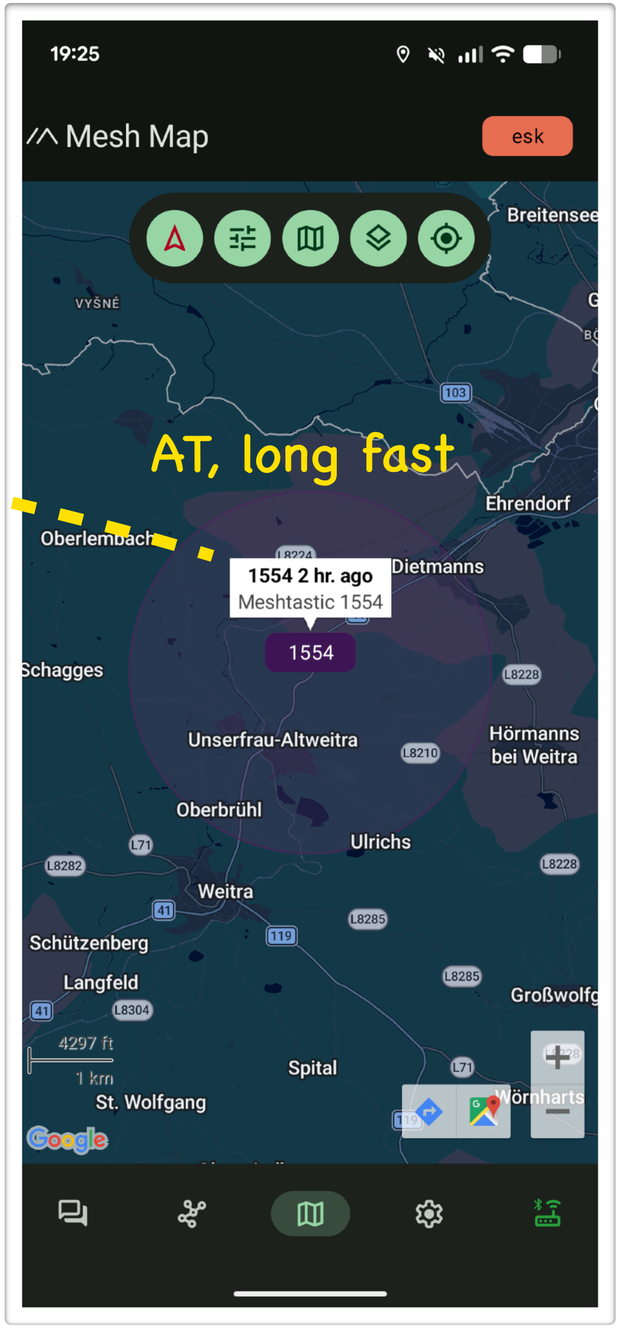


Prague, CZ, medium fast



Vienna, AT, long fast

contact
received
7.3.2026
cca 27 km
RSSI -121 dBm
SNR -13.25 dB



Thank you for your attention ///... //..\\ ...

Co-funded by the European Union
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them

Supported by ECCC
The project funded under Grant Agreement No. 101158662 is supported by the European Cybersecurity Competence Centre

History (year-month-day format)

- 2026-05-18, version 1.2, MFF UK release
- 2026-03-27, version 1.1, symbols annotated
- 2026-03-20, version 1.0 released