LoRa wireless standard

Intro and PHY

Matan Leilien

agenda

LPWAN

LoRaWAN

LORA - waveform

Design parameters

Receiver design and impairments mitigation

(Advanced) ranging

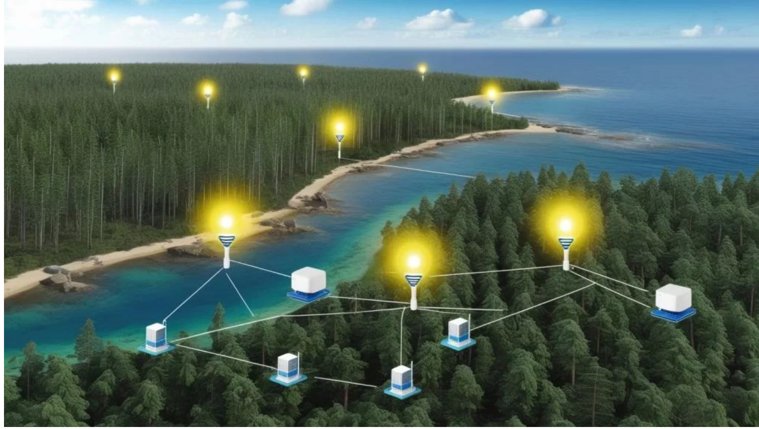
LPWAN/LoRaWAN

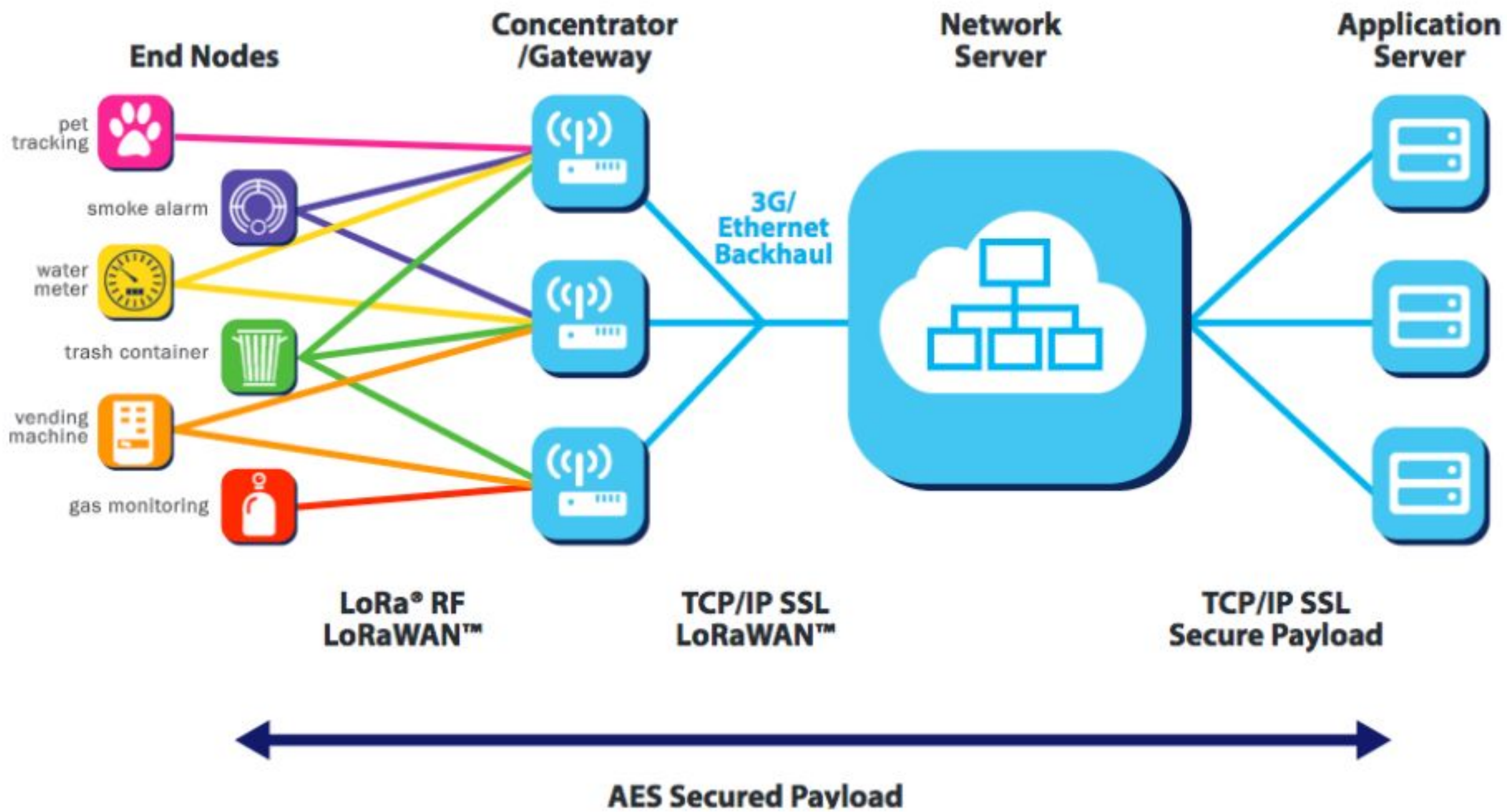
LPWAN

LPWAN (Low-Power Wide-Area Network) enables **battery-powered** IoT devices to transmit **small data** packets over **long distances** with **minimal energy** consumption.

LPWAN technologies, like LoRaWAN, are being used across industries, including agriculture, smart cities, utilities, manufacturing, and environmental monitoring, for real-time insights and automation.

LPWAN use cases





End Nodes
Concentrator /Gateway
Network Server
Application Server
pet tracking
smoke alarm
water meter
trash container
vending machine
gas monitoring
3G/ Ethernet Backhaul
LoRa® RF LoRaWAN™
TCP/IP SSL LoRaWAN™
TCP/IP SSL Secure Payload
AES Secured Payload

ISM deployment

LoRa operates in the unlicensed ISM (Industrial, Scientific and Medical) radio band tha
are available worldwide.

Region	Frequency (MHz)
Asia	433
Europe, Russia, India, Africa (parts)	863-870
US	902-928

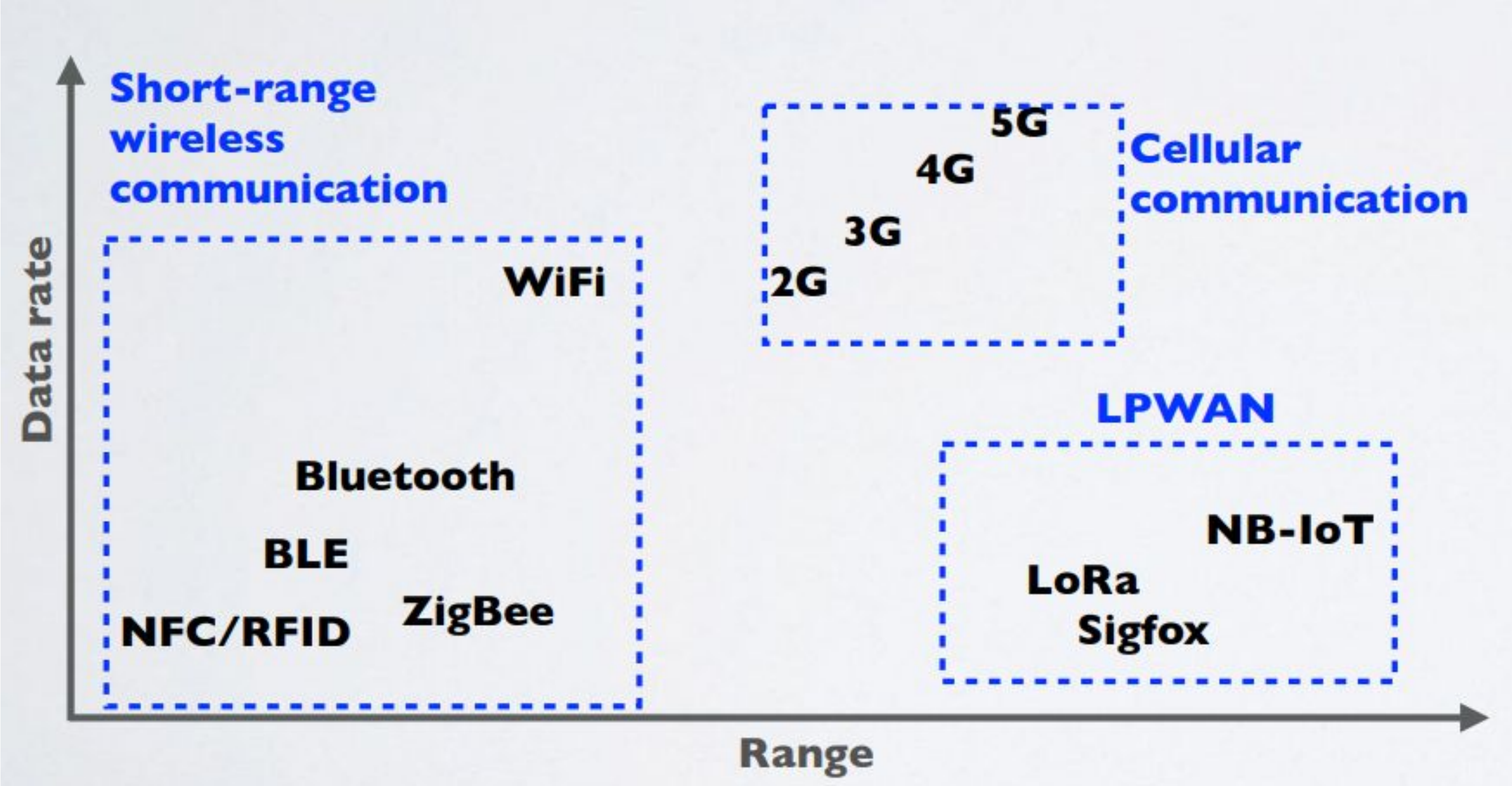
Region	Frequency (MHz)
Australia	915-928
Canada	779-787
China	779-787, 470-510

- also 2.4GHz band worldwide

ISM deployment

Region	Frequency Band (MHz)	Total Bandwidth	Channel Widths	Channels (Min Width)	Channels (Max Width)
North America (US915)	902–928	26 MHz	125 kHz, 500 kHz	208 (125 kHz)	52 (500 kHz)
Europe (EU868)	863–870	7 MHz	125 kHz, 250 kHz, 500 kHz	56 (125 kHz)	14 (500 kHz)
China (CN470)	470–510	40 MHz	125 kHz, 250 kHz	320 (125 kHz)	80 (500 kHz)

LPWAN - Low Power Wide area network



Traditional Cellular

Long Range
High Data Rates
Low Battery Life
High Cost

LPWAN (3-5B in 2022)

LoRa®

Long Range
Low Data Rates
Long Battery Life
Low Cost
High Capacity Potential

Cat-M1

Long Range
High Data Rates
Low Battery Life
Medium Cost

Local Area Network
(Wi-Fi)

Short Range
High Data Rates
Low Battery Life
Medium Cost

Narrow-Band IoT
(NB-IoT)

Stationary Devices
Short Range (indoor coverage)
Low Data Rates
Good Battery Life
Low Cost

Personal Area Network
(Bluetooth®)

Very Short Range
Low data rates
Good Battery Life
Low Cost

Feature	LoRaWAN	NB-IoT (Narrowband-IoT)	LTE-M (LTE for Machines)	Sigfox
Range urban 🏙️	2-5 km	~1 km Excellent building penetration.	~1 km Supports cell handover for mobility.	Up to 10 km
Range rural 🌳	Up to 20 km	Up to 10 km	Up to 10 km	Up to 40 km
Throughput	⬇️ Low0.3 - 50 mbps Best for small, infrequent data packets	↔ Medium Up to 250 kbps Supports larger data packets than LoRaWAN or Sigfox	⬆️ High (for LPWAN)Up to 1 Mbps Suitable for firmware updates and some voice data	⬇️ Very Low~100 bps Limited to very small messages (e.g., 12 bytes per message, max 140 messages/day)
Power Consumption	🔋 Very Low Battery life can exceed 10 years	🔋 Low Optimized for long battery life, often cited as up to 10 years	🔋 Moderate Higher than LoRaWAN and NB-IoT, but significantly lower than standard cellular. Battery life can be several years	🔋 Extremely Low The most power-efficient, enabling very long battery life from small batteries
Cost	💲 Low Module Cost ~$8 - $12	💲 Low Module Cost ~$10-$12	💲 Moderate Module Cost > NB-IoT	💲 Very Low Module Cost <$5

Long Range

- Deep indoor coverage (including multi-floor buildings)
- Star topology network design

Long Battery Life

- Low-power optimized
- Up to 10-year lifetime
- Up to 10x versus Cellular M2M

High Capacity

- High capacity – millions of messages per base station / gateway
- Multi-tenant interoperability
- Public or private network deployments

Low Cost

- Minimal infrastructure
- Low cost end-node
- Open source software

Geolocation

- Indoor/outdoor
- Accurate without the need for GPS
- No battery life impact

FUOTA

- Firmware Updates Over-the-Air for applications and the LoRaWAN stack

Roaming

- Roaming: Seamless handovers from one network to another

Security

- Embedded end-to-end AES-128 encryption
- Unique ID
- Application
- Network

Feature	LoRa	LoRaWAN
Definition	A physical layer (modulation technique)	A communication protocol and system architecture
Function	Enables long-range, low-power wireless transmission	Manages how devices communicate over LoRa networks
Layer	PHY (Physical Layer)	MAC (Media Access Control) Layer
Scope	Only handles radio signal transmission	Includes network management, security, and routing
Standardization	Proprietary (Semtech)	Open standard (LoRa Alliance)
Security	Not included	AES-128 encryption for data integrity and privacy

High network capacity?

Strict timing and fairness regulations:
A single eight-channel gateway can support a few hundred thousand messages over the course of a 24-hour period. **If each end device sends 10 messages a day**, such a gateway can support about 10,000 devices

history

🔹 **Early 2010s: Genesis:** French startup **Cycleo** develops a unique long-range, low-power modulation technology derived from Chirp Spread Spectrum (CSS).

🔹 **2012: Acquisition & Commercialization: Semtech**, a US semiconductor company, acquires Cycleo and its technology, beginning the process of embedding it into silicon chips for broad use.

🔹 **January 2015: The First Specification:** The foundational **LoRaWAN™ 1.0 specification** is released, defining the network architecture and communication protocol.

🔹 **March 2015: The Alliance Forms:** The **LoRa Alliance®** is established as a non-profit organization to standardize the protocol and foster a global ecosystem.

🔹 **2017 - Present: Evolution & Maturity:** Significant updates, including version **1.1 (2017)**, enhance security, roaming, and functionality, with continuous improvements in subsequent releases.

🔹 **December 2021: Global Recognition:** The **International Telecommunication Union (ITU)** officially recognizes LoRaWAN as an international standard for Low-Power Wide-Area Networks (LPWANs).

Wireless Technology	Wireless Communication	Range (m)	Tx power (mW)
Bluetooth	Short range	~10	~2.5
WIFI	Short range	~50	~80
3G / 4G	Cellular	~5000	~500
LoRa*	LPWAN	2000-5000 (urban area) 5000-15000 (rural area) > 15000 (direct line of sight)	~20

System requirements

Simple/cheap implementation

Long range

Low power (lasts decades!)

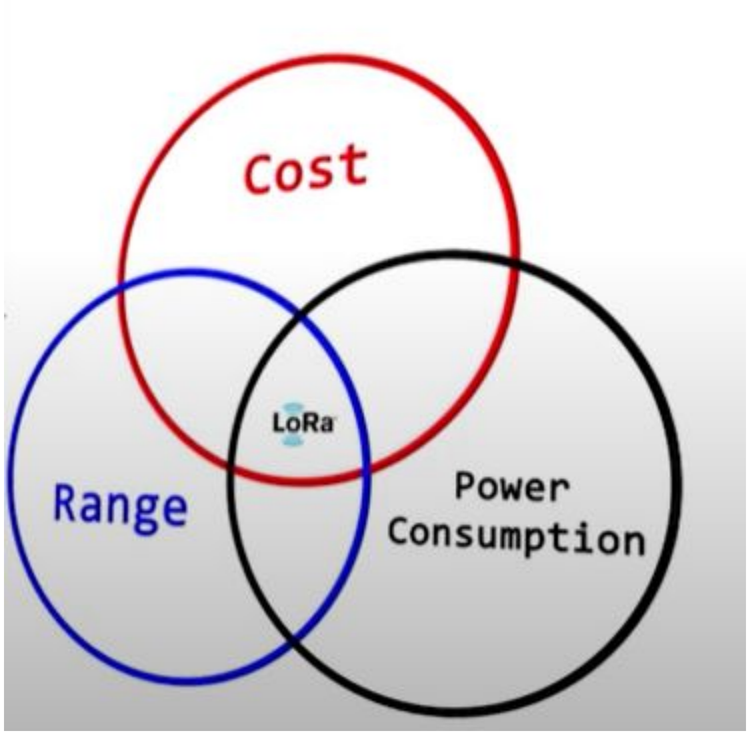
Unlicensed band - expect collisions!

Interference resilience

Scalable data rate

Multi user

Resilience to multipath/Doppler



LoRa range

Environment	Range (km)
Urban areas (towns & cities)	2-5
Rural areas (countrysides)	5-15
Direct Line Of Sight	>15

- Some notable records:
  Andreas Spiess, ground to ground connection: 212 km (= 131.73 miles)
  Weather balloon to ground connection: 702.67 km (= 436.61 miles)

LongRange, Is it even possible?

Shannon answers $C = B * log_2\left(1 + \frac{S}{N}\right)$

“For any BW and SNR, comm is possible with capacity C”

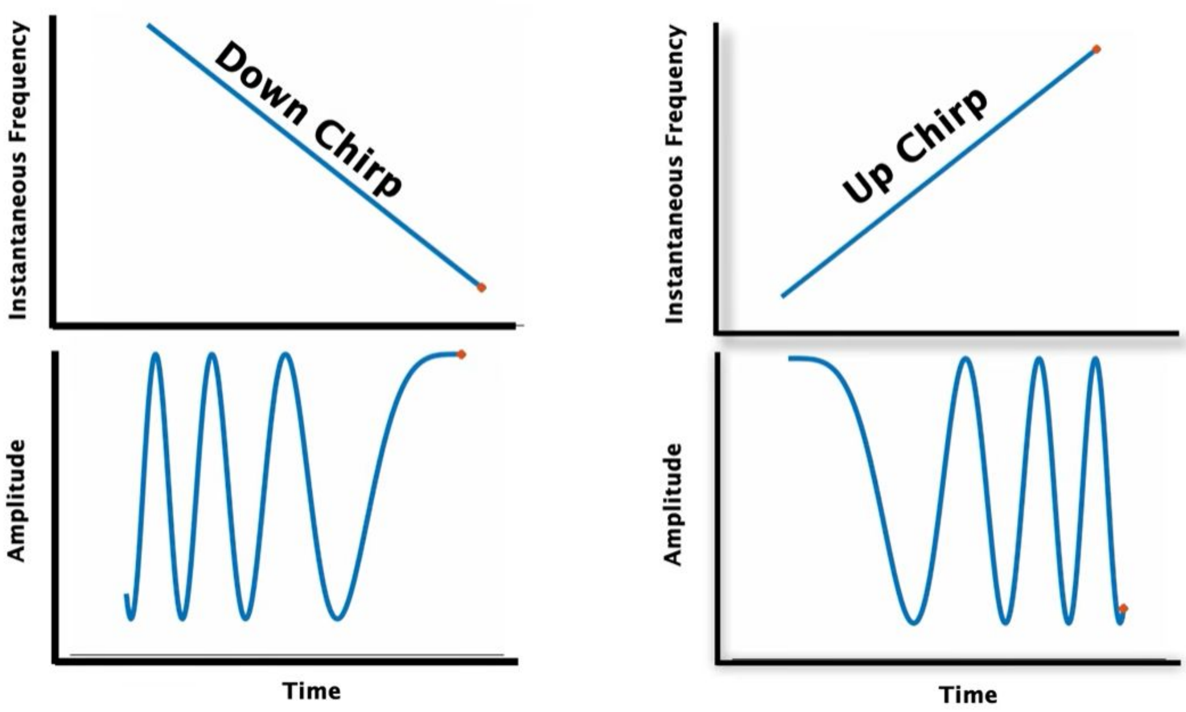
For 125KHz SNR = −20dB C=1.8Kbps

Table 1. Data Rates and Required Signal-to-Noise Ratios

Data Rate	SF5	SF6	SF7	SF8	SF9	SF10	SF11	SF12
Required SINR	-2.5dB	-5dB	-7.5dB	-10dB	-12.5dB	-15dB	-17.5dB	-20dB

LoRa PHY
CSS waveform

CHIRP signal (Compressed High Resolution Pulse)



Chirp waveform

A chirp signal is defined as a frequency modulated exponential, such that the inst. Freq is a linear function of t. The symbol begins from freq f0, goes through B Hz bandwidth during the symbol time T:

$$s(t) = \exp\left(j2\pi\left(f_0 t + \frac{B}{2T}t^2\right)\right)$$

$$f_{\text{inst}}(t) = \frac{d\phi(t)}{dt} = f_0 + \frac{B}{T}t$$

$$f_{\text{inst}}(0) = f_0 + \frac{B}{T}\cdot 0 = f_0 \qquad f_{\text{inst}}(T) = f_0 + \frac{B}{T}\cdot T = f_0 + B$$

LoRa chirp waveform

In LoRa modulation we encode the information on the **initial freq (fi)** from which the chirp | $f_i \in \left[-\frac{BW}{2}, \frac{BW}{2}\right]$

design choice #1:

- **There are M possible such initial freqs.** The symbols are numbered 0 through M−1.
- **M is a power of of two.**
- **M=2^SF**, Each symbol holds SF=log2(M)bits

$m \in \{0, 1, 2, \ldots, M-1\}$, where $M = 2^{SF}$

Each freq offset (called chip) is then B/M [Hz] apart (equally spaced).

The 0 number symbol is called the “base chirp”

LoRa chirp waveform

Design choice #2: symbol duration

The “spreading factor” determines the symbol duration.

$$T_s(\mathrm{CSS}) = \frac{2^{SF}}{BW}$$

Recall that in pulse-based (linear) modulation (for reference), a rectangular TD pulse of duration T will occupy around 1/T of bandwidth.

$$T_s(\text{linear modulation}) \approx \frac{1}{BW}$$

For every increment of SF, we double the duration of the signal, while keeping the same BW.

Design choice #3: f0 = -BW/2

So the initial freq of the m’th symbol:

$$f_m = -\frac{B}{2} + \frac{m \cdot B}{M}$$

LoRa chirp waveform

- $M = 2^{SF}$: number of symbols
- B: bandwidth
- $T = \frac{M}{B}$: symbol duration
- $m \in \{0, 1, \ldots, M-1\}$: symbol index
- $f_0 = -\frac{B}{2}$: base frequency (centered chirp)

Initial freq: $f_m = -\frac{B}{2} + \frac{m \cdot B}{M}$

Inst. freq (across entire symbol): $f_{\text{inst}}^{(m)}(t) = f_m + \frac{B}{T}t = -\frac{B}{2} + \frac{m \cdot B}{M} + \frac{B}{T}t$

Note that B/T is the **chirp rate**

Before (only base chirp): $s(t) = \exp\left(j2\pi\left(f_0 t + \frac{B}{2T}t^2\right)\right)$

Updated LoRa signal (WIP):

$$s_m(t) = \exp\left(j2\pi\left[\left(-\frac{B}{2} + \frac{mB}{M}\right)t + \frac{B}{2T}t^2\right]\right), \quad 0 \le t < T$$

LoRa chirp waveform

$$s_m(t) = \exp\left(j2\pi\left[\left(-\frac{B}{2} + \frac{mB}{M}\right)t + \frac{B}{2T}t^2\right]\right), \quad 0 \leq t < T$$

For any m>0 the symbol inst freq will go out of bounds of [-BW/2,BW/2] at some point during the symbol.

Design choice #4: In the LoRa waveform we stay centered around baseband by wrapping the freq back to -BW/2.

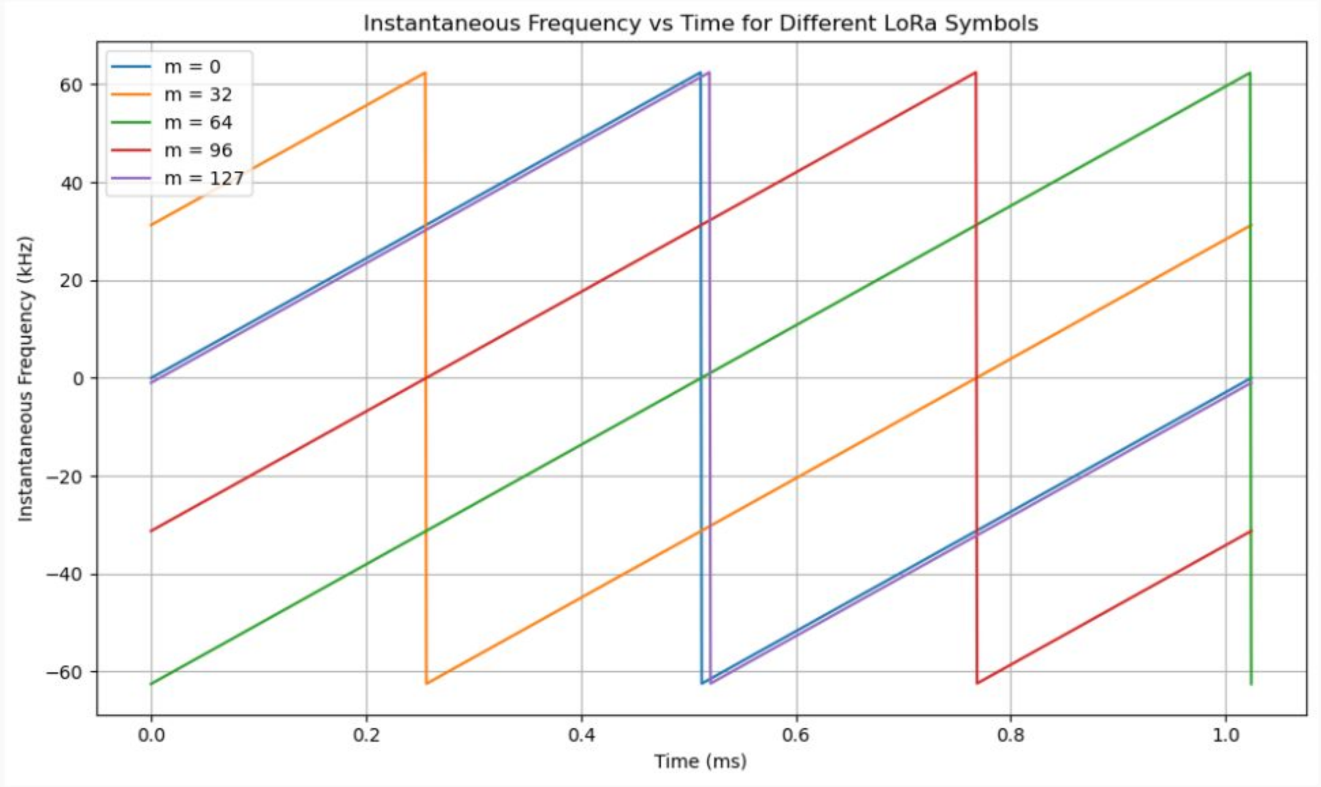
Note that if we set FS = B (“bandwidth-rate system”) we don’t need to explicitly introduce a mod term, the aliasing will do it for us :)

LoRa chirp waveform

Assuming SF = 7

BW = 125KHz

(FFT shifted)



LoRa chip (!= chirp)

Now if Fs = BW and $$T_s(\mathrm{CSS}) = \frac{2^{SF}}{BW}$$

Then Ts is made of 2^SF samples in TD.

At every sample, the inst. Freq circularly increases by BW/M.

Each freq “step” is referred to as a **chip**.

Note that we have M chips in FD and M samples in TD.

LoRa VS QAM of same BitsPerSymbol

Metric	LoRa (SF=8)	256QAM	Key Difference
Bits per Symbol	8	8	Same by definition of the problem
Bandwidth (BW)	500 kHz	500 kHz	Same by definition of the problem
Symbol Duration	512 µs	2 µs	LoRa has a much longer symbol duration.
Symbol Rate	~1.95 ksymbols/s	~500 ksymbols/s	256QAM's symbol rate is vastly higher.
Bit Rate	15.625 kbps	4 Mbps	256QAM achieves a significantly higher bit rate.
Min. SNR (for BER 10^{-6})	~ -10 dB	~ 28.4 dB	LoRa excels in noisy environments; 256QAM needs a very clean signal.

LoRa PAPR

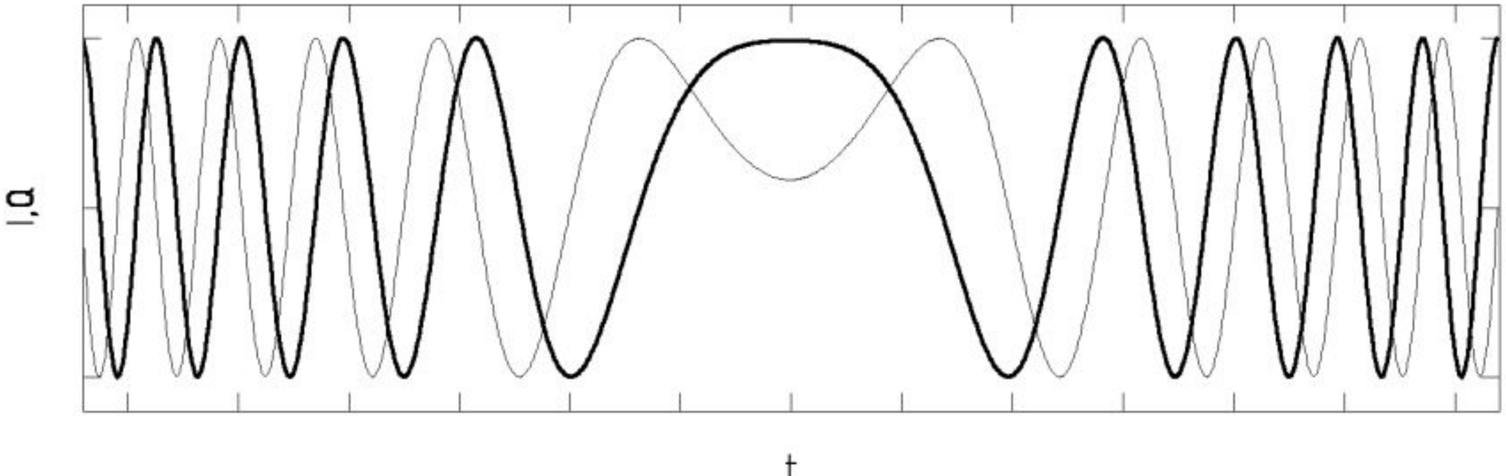
Since LoRa is a freq modulation, it’s amplitude is constant with peak power equal avg power yielding **PAPR = 0**.

This is a very desirable trait enabling operating at a “compressed” region of a cheap PA.

Base chirp BB representation

---

when viewing a complex exponential in TD, the determining factor for the sign of the base freq is weather Q is leading (negative freq) or lagging (positive freq) in relation to I.



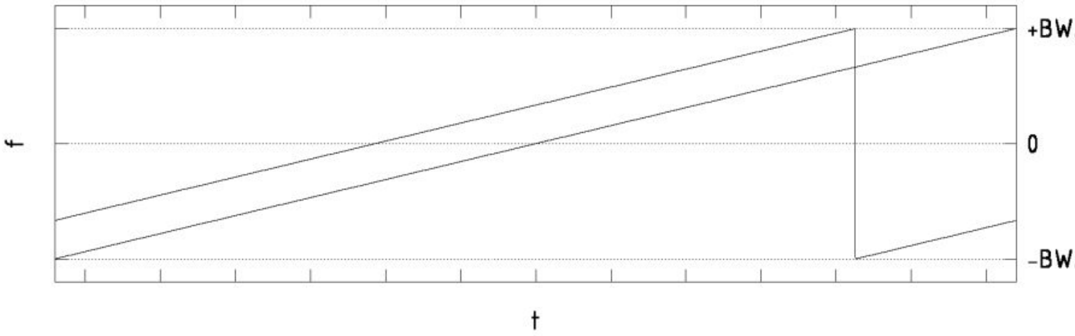
$\phi(t_0)=\phi(t_1)$

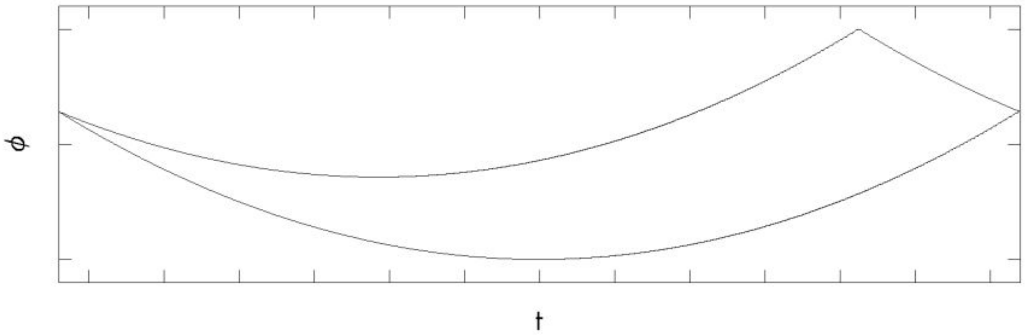
Chirp phase

Another feature of the modulation is continuous phase, so this is a type of cpm.

The total phase accumulation during one symbol is 0 so:

$$\phi(t_0)=\phi(t_1)$$





Orthogonality claim

$$\left\langle c(nT_s + kT)|_{s(nT_s)=i}\,, c(nT_s + kT)|_{s(nT_s)=q} \right\rangle = 0$$

$$i \neq q,\ i, q \in \{0 \ldots 2^{\text{SF}} - 1\}.$$

It can be shown that there is no correlation (complete separability) between two different CSS symbols of the same SF.

Impling optimal receiver.

Frequency shift chirp modulation

Insight: ZC sequences

CSS = ZC

The FSCM modulation employed in the LoRa signalling scheme is an orthogonal modulation with symbols encoded using a set of N cyclically shifted versions of a base Zadoff-Chu (ZC) sequence. The general expression for ZC sequences is defined as follows [15]:

$$u_M[k] = \begin{cases} e^{\frac{j\pi.M.k(k+1)}{N}}, & k = 0, 1 \ldots N-1 \quad \text{if N is odd} \\ e^{\frac{j\pi.M.k^2}{N}}, & k = 0, 1 \ldots N-1 \quad \text{if N is even.} \end{cases}$$

If M and N are relatively prime, i.e. $gcd(M, N) = 1$, the auto correlation of a ZC sequence with all $N-1$ cyclically shifted versions of itself is zero for all values of n different from zero:

$$R_{MM}[n] = \frac{1}{N} \sum_{k=0}^{N-1} u_M[k] u_M[(k+n) \bmod N]^*$$
$$= \begin{cases} 1 & \text{for} \quad n = 0 \\ 0 & \text{for} \quad n \neq 0 \end{cases}$$

ZC sequences

ZC sequences are popular in various wireless communication applications, often used for synchronization, random access, signal quality measurements and parameter estimaiton.

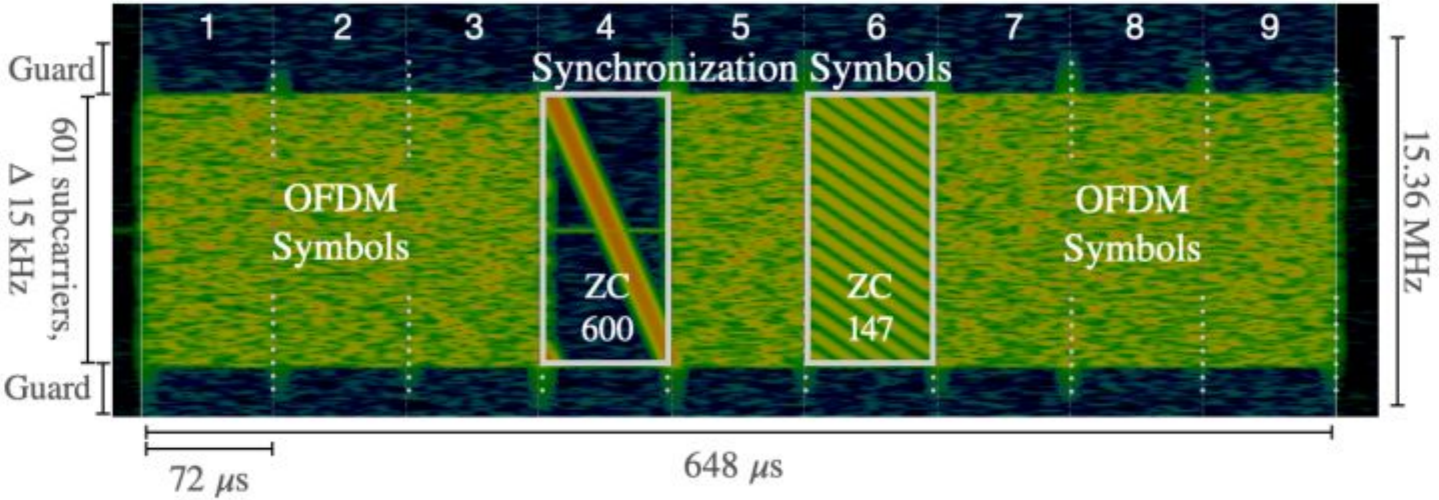
Desired property - CAZAC

Constant Amplitude Zero Auto Correlation

ZC sequence

In the wild:

(from drone ID packet)



Orthogonality claim

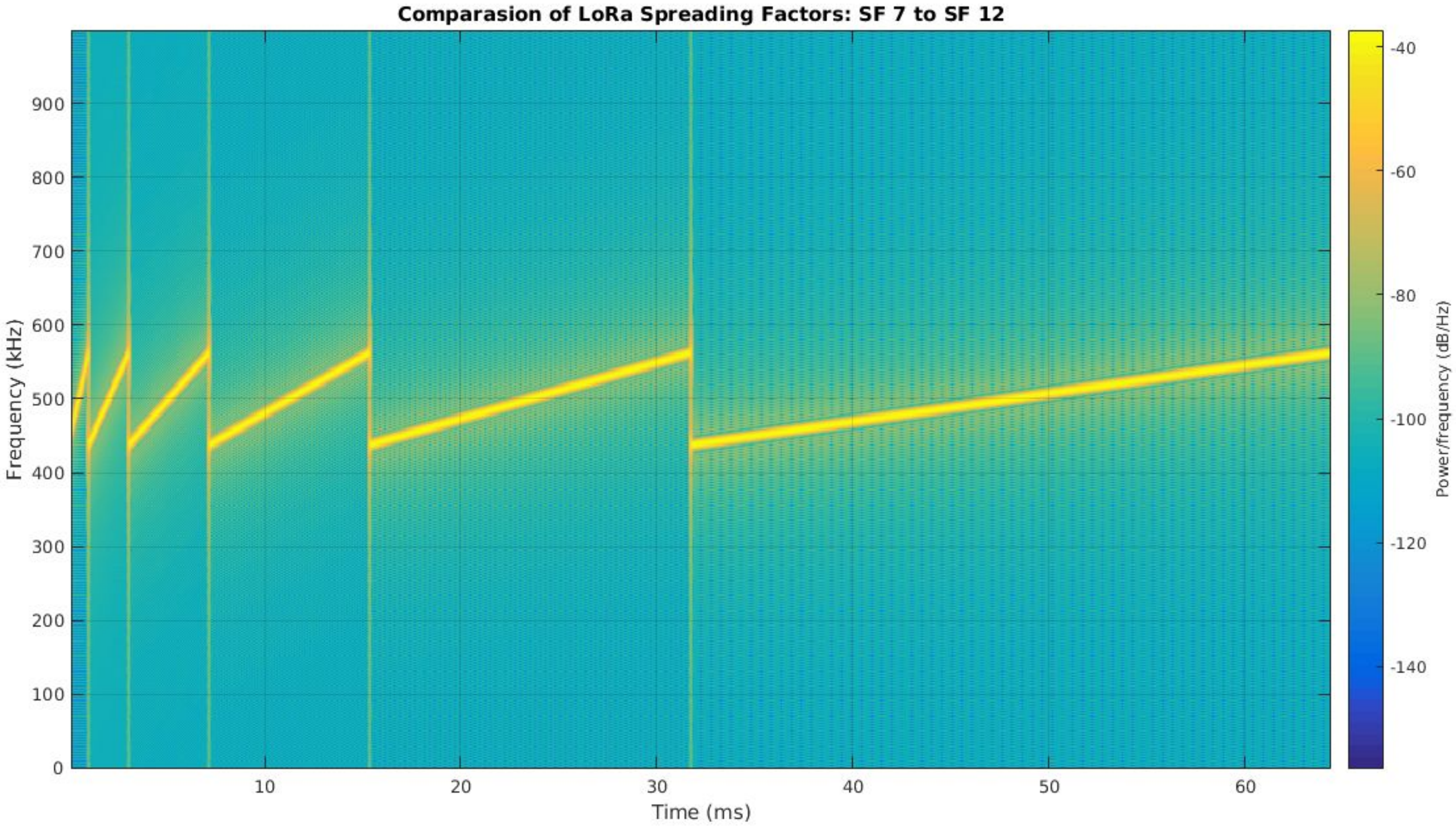
There is also “quasi orthogonality” between chirps of different SFs

Table shows effect of interfering LoRa signal on Packet error

Table 2. Orthogonality Matrix

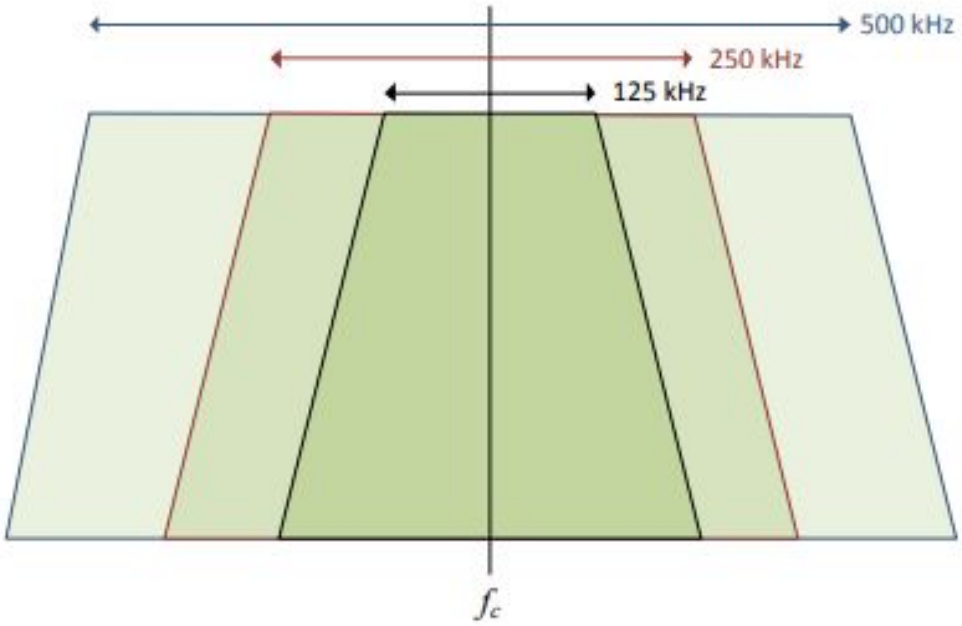
Data Rate	SF7	SF8	SF9	SF10
SF7 as victim	86%	10%	3%	8%
SF8 as victim	8%	84%	2%	6%
SF9 as victim	11%	9%	85%	8%
SF10 as victim	6%	5%	2%	78%

LoRa Design parameters


Comparasion of LoRa Spreading Factors: SF 7 to SF 12
Frequency (kHz)
900
800
700
600
500
400
300
200
100
0
10
20
30
40
50
60
Time (ms)
-40
-60
-80
-100
-120
-140
Power/frequency (dB/Hz)

Scalable BW

LoRa WAN channel BW is also a parameter:



LoRa bit rate

$$R_b = SF \cdot R_{\text{symbol}} \cdot \text{CR}$$

$$R_b = SF \cdot \left(\frac{B}{2^{SF}}\right) \cdot \text{CR}$$

- SF: Spreading Factor (typically 7–12)
- $R_{\text{symbol}} = \frac{B}{2^{SF}}$: Symbol rate
- CR: Code rate (e.g., $\frac{4}{5}, \frac{4}{6}, \frac{4}{7}, \frac{4}{8}$)

- Both BW and SF affect **throughput**

LoRa min SNR vs SF

SF (Spreading Factor)	Chips/Symbol	SNR limit	Time on Air for 10 byte packet (ms)	Bit Rate (bps)
7	128	-7.5	56	5470
8	256	-10	103	3125
9	512	-12.5	205	1758
10	1024	-15	371	977
11	2048	-17.5	741	537
12	4096	-20	1483	293

x2

<x2

LoRa sensitivity

$$\text{Sensitivity} = -174 + 10\log_{10}(BW_{[Hz]}) + NF + SNR_{min}$$

Minimal SNR is dependant on SF

- Both BW and SF affect **sensitivity / range**

SF effect

–

Table 2. Influence of SF on Time on Air and Sensitivity (CR=2, BW=250)

SF	Time on air [ms]	Sensitivity [dBm]
12	528.4	-134
10	132.1	-129
8	39.2	-124

Table 3. Influence of BW on Time on Air and Sensitivity (CR=2, SF=10)

BW	Time on air [ms]	Sensitivity [dBm]
125	264.2	-132
250	132.1	-129
500	66	-126

SF effect

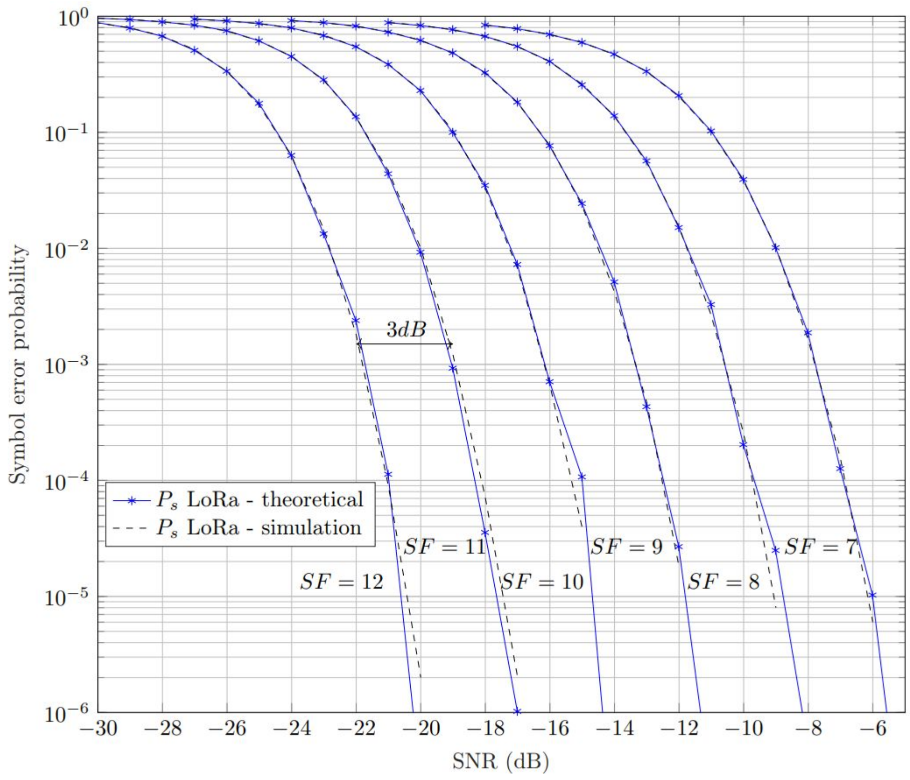
Spreading Factor (For UL at 125 KHz)	Bit Rate	Range (Depends on Terrain)	Time on Air for an 11-byte payload
SF10	980 bps	8 km	371 ms
SF9	1760 bps	6 km	185 ms
SF8	3125 bps	4 km	103 ms
SF7	5470 bps	2 km	61 ms

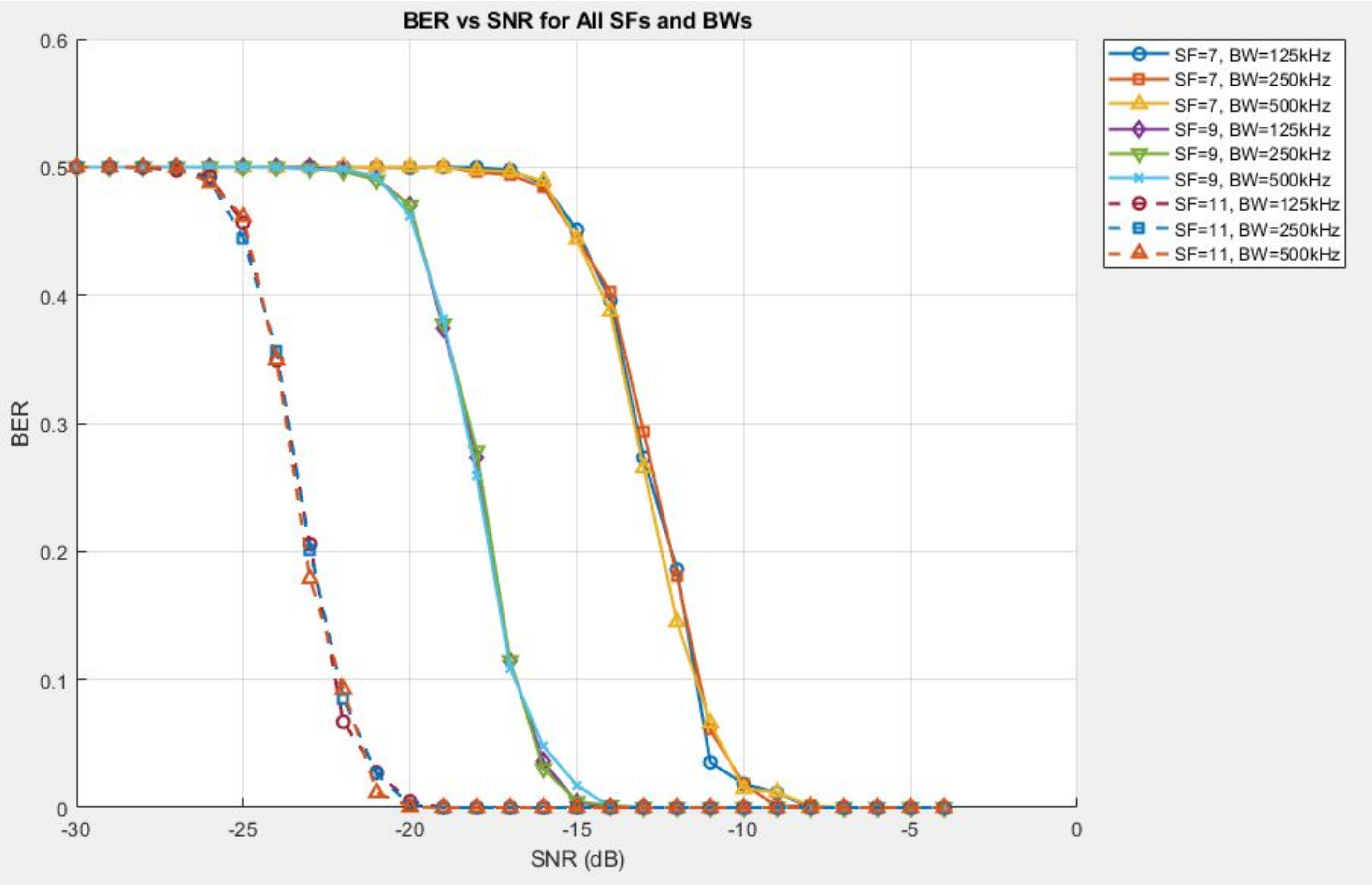
Each increment increase in SF encodes +1 bit / symbol

But takes *2 time to transmit, halving the rate.

SER VS SF

Each increase in SF yields effective 3dB processing gain





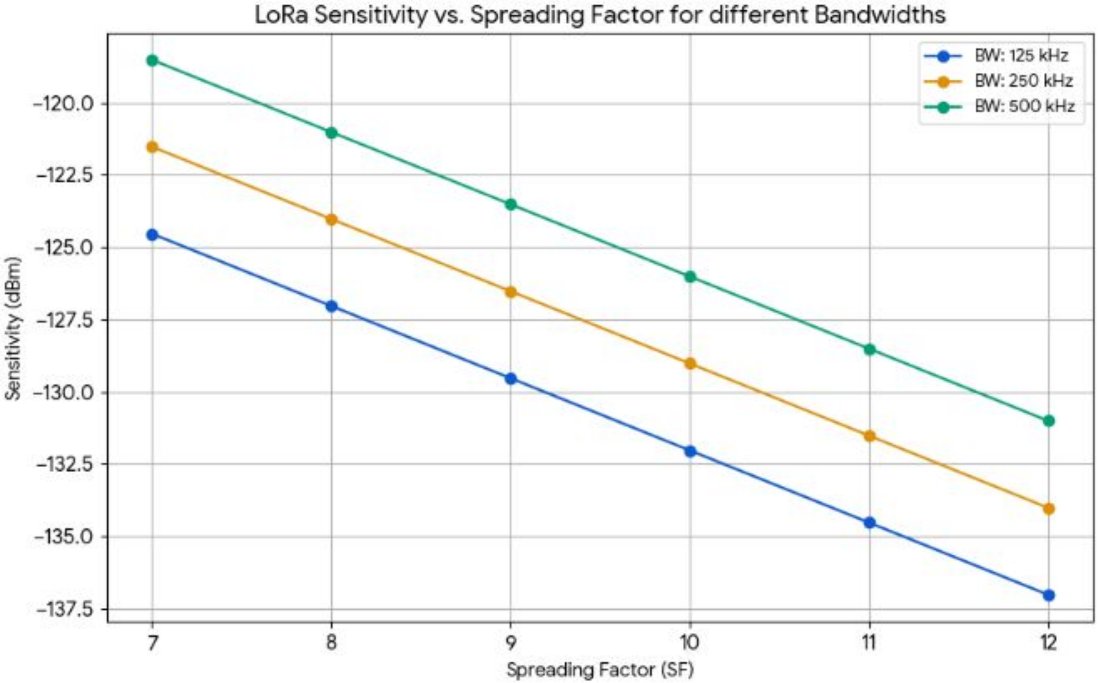
BER vs SNR for All SFs and BWs
0.6
0.5
0.4
0.3
0.2
0.1
0
BER
-30
-25
-20
-15
-10
-5
0
SNR (dB)
SF=7, BW=125kHz
SF=7, BW=250kHz
SF=7, BW=500kHz
SF=9, BW=125kHz
SF=9, BW=250kHz
SF=9, BW=500kHz
SF=11, BW=125kHz
SF=11, BW=250kHz
SF=11, BW=500kHz

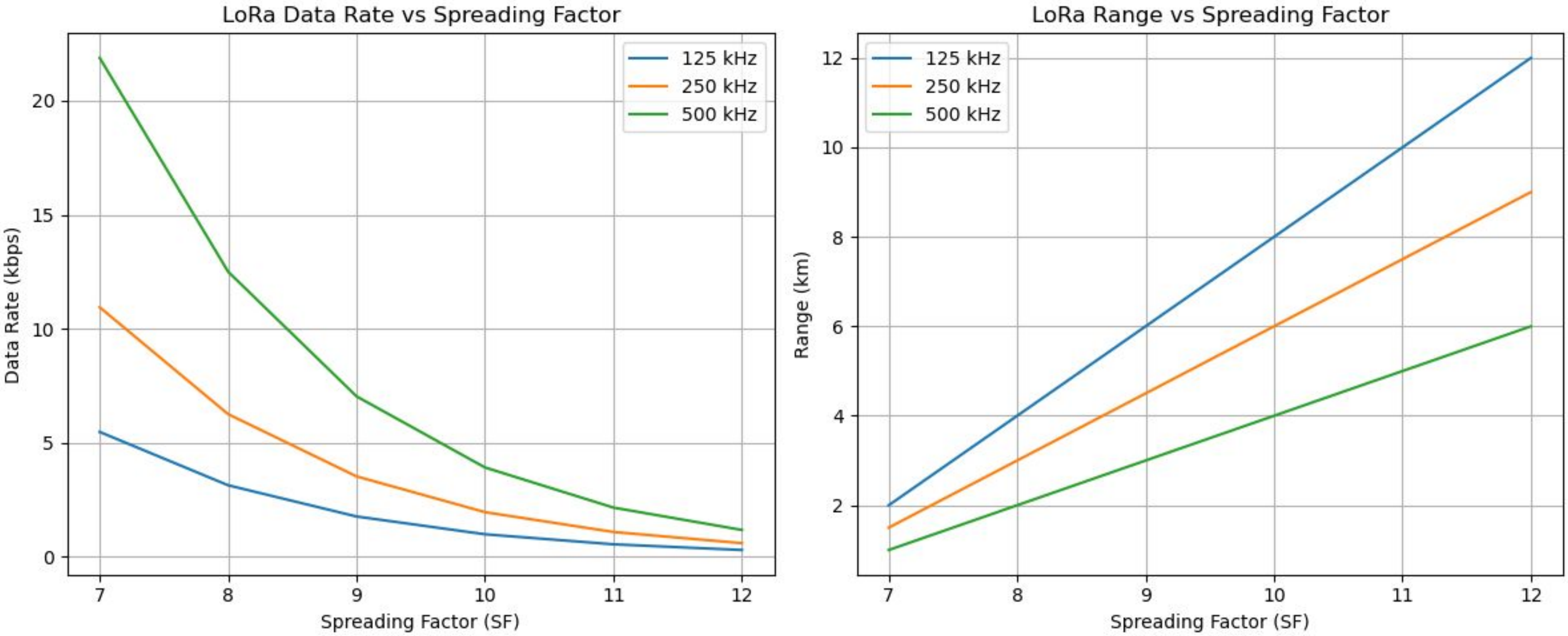
BW effect

For CR = 2 ,SF =10

BW	Time on air [ms]	Sensitivity [dBm]
125	264.2	-132
250	132.1	-129
500	66	-126

$$T_s(\mathrm{CSS}) \approx \frac{2^{SF}}{BW}$$




LoRa Data Rate vs Spreading Factor
Data Rate (kbps)
Spreading Factor (SF)
125 kHz
250 kHz
500 kHz
0
5
10
15
20
7
8
9
10
11
12
LoRa Range vs Spreading Factor
Range (km)
Spreading Factor (SF)
125 kHz
250 kHz
500 kHz
2
4
6
8
10
12
7
8
9
10
11
12

LoRa alternatives

(from the top of my head)

Relevant references

NB-SC

FHSS

DSSS

Where does processing gain come from?

From “lora modulation basics”:

“The principle of increasing the wanted signal **bandwidth** to transmit error free data over longer distance”

“it can be seen that to transmit error free information in a channel of fixed noise-to-signal ratio, only the transmitted signal **bandwidth** need be increased. “

Where does processing gain come from?

Semtech’s claims are **misleading**

DSSS and CSS spread the signal over time and freq

Time spreading - increases signal total energy (higher Eb)

Freq spreading - allows for multiple access employing orthogonality!

LoRa VS unspread FSK - unfair comparison

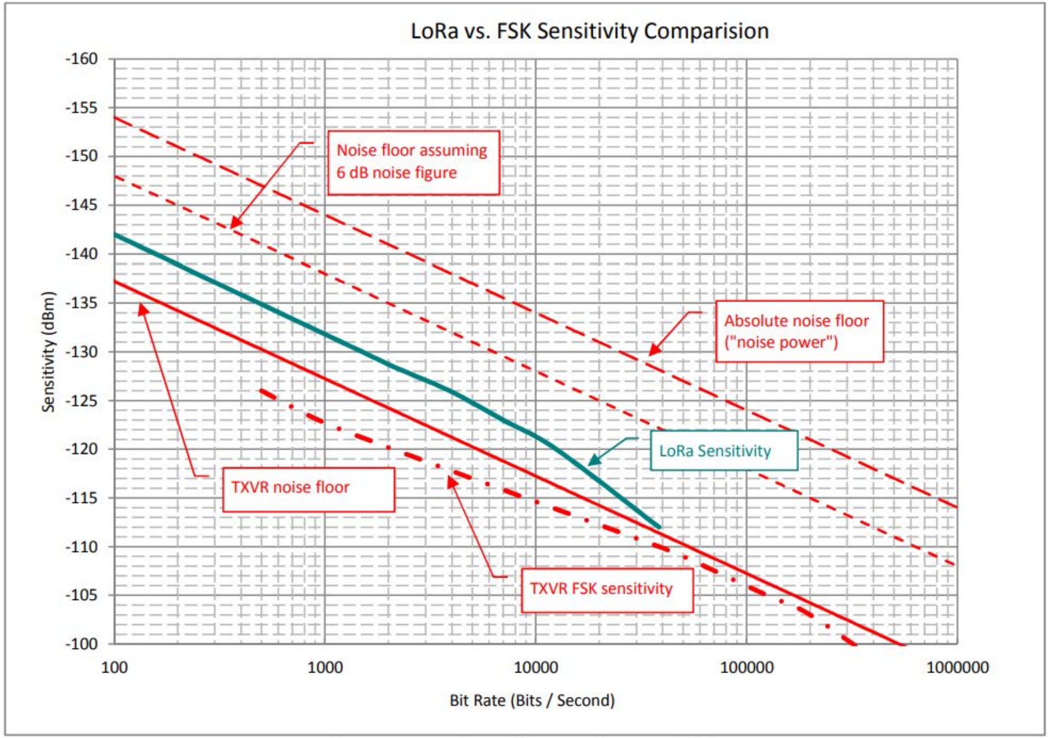


Figure 3: Comparison of LoRa and FSK Sensitivity

Spreading factor

Gain over what?

$$\text{Processing Gain (dB)} = 10 \cdot \log_{10}(2^{\text{SF}})$$

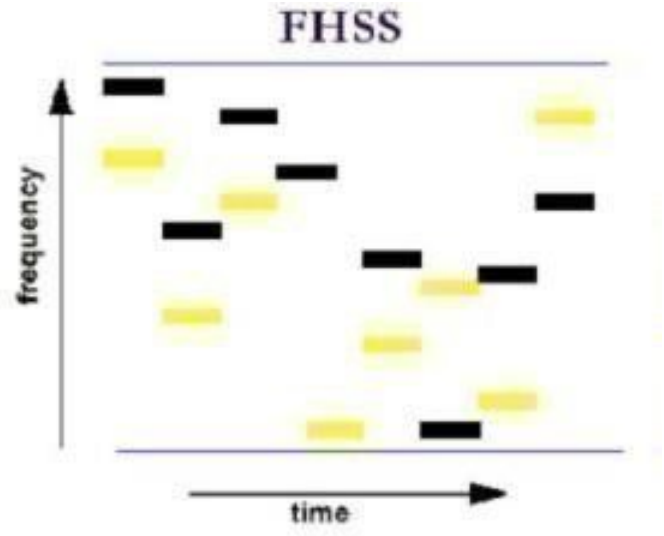
For example, with SF = 12:

$$PG = 10 \cdot \log_{10}(2^{12}) \approx 36 \text{ dB}$$

So the “unspread” signal is 2^SF times shorter in time!

FHSS

In Frequency Hopping Spread Spectrum (FHSS) systems, the spreading factor is the number of carrier frequencies over which a modulation symbol hops.



FHSS

Resilience to multipath and interference using multiple transmissions

Every “hop” needs to be distinguishable at the receiver

No processing gain element from spreading

NOT viable alternative

DSSS transmitter

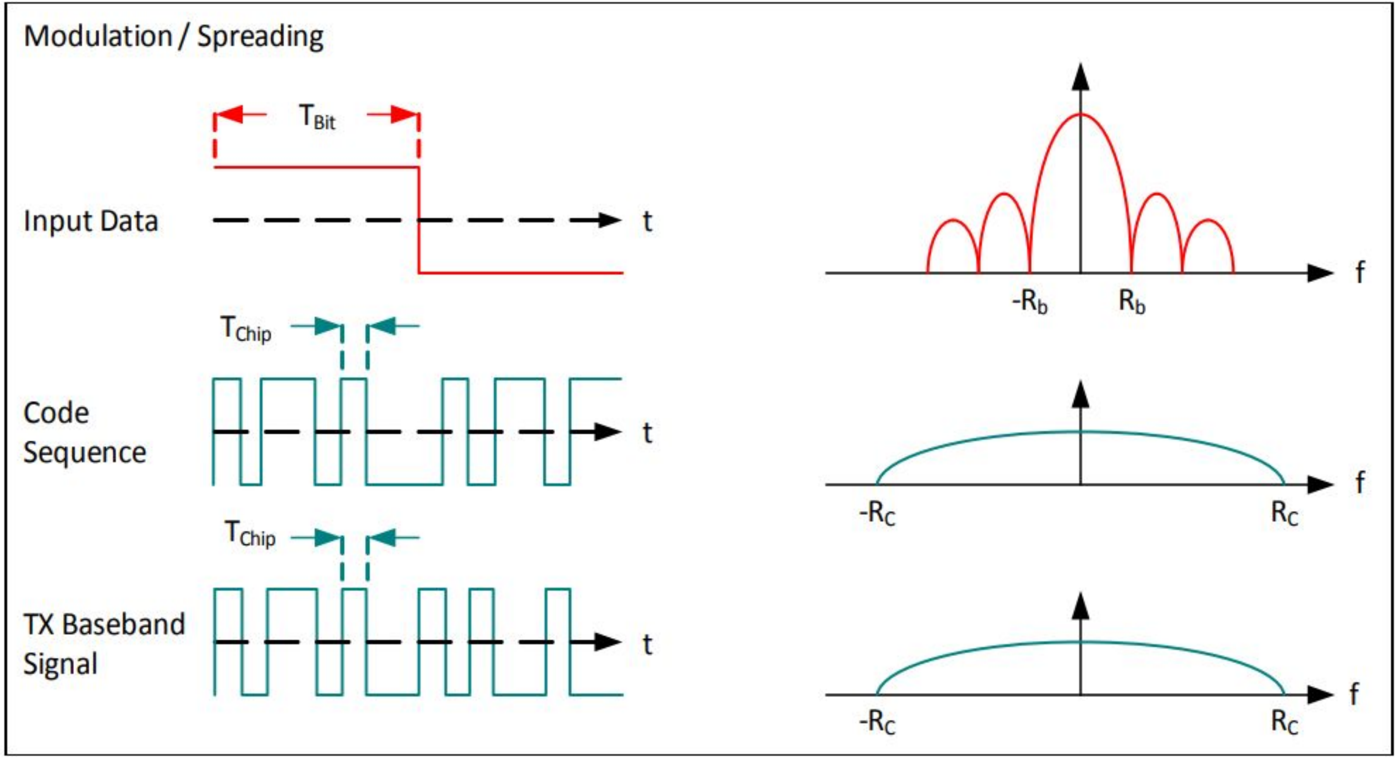


Figure 1: Modulation / Spreading Process

DSSS receiver

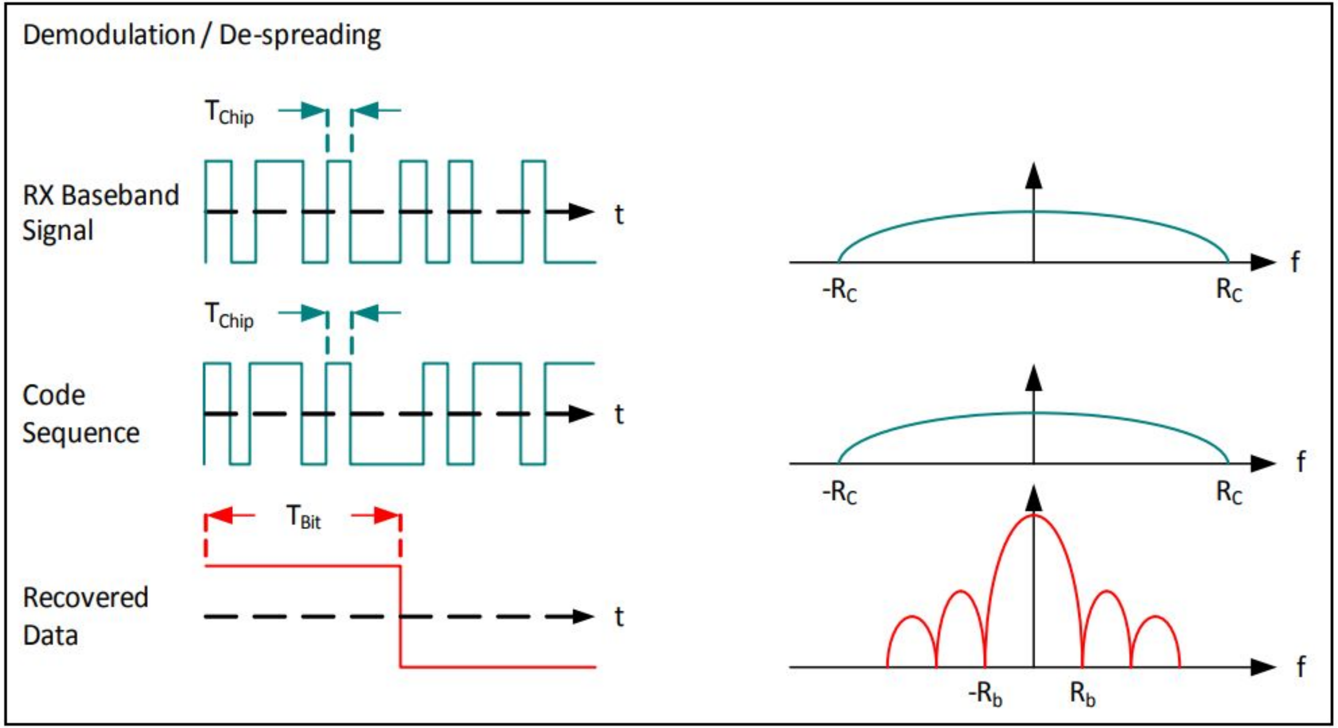


Figure 2: Demodulation / De-spreading Process

DSSS VS LoRa

In Direct Sequence Spread Spectrum (DSSS) systems, the spreading factor is the length of the spreading sequence that reflects in the number of chips for each modulation symbol.

$$G_P = 10 * log_{10}\left(\frac{R_C}{R_b}\right)(dB)$$

relevant comparison: comparable Processing/spreading gain

(-) Requires precise clock

(-) Relatively costly acquisition phase (correlate over all possible codes, freq offsets and timing offsets)

Alternative #1 reduce code rate

---

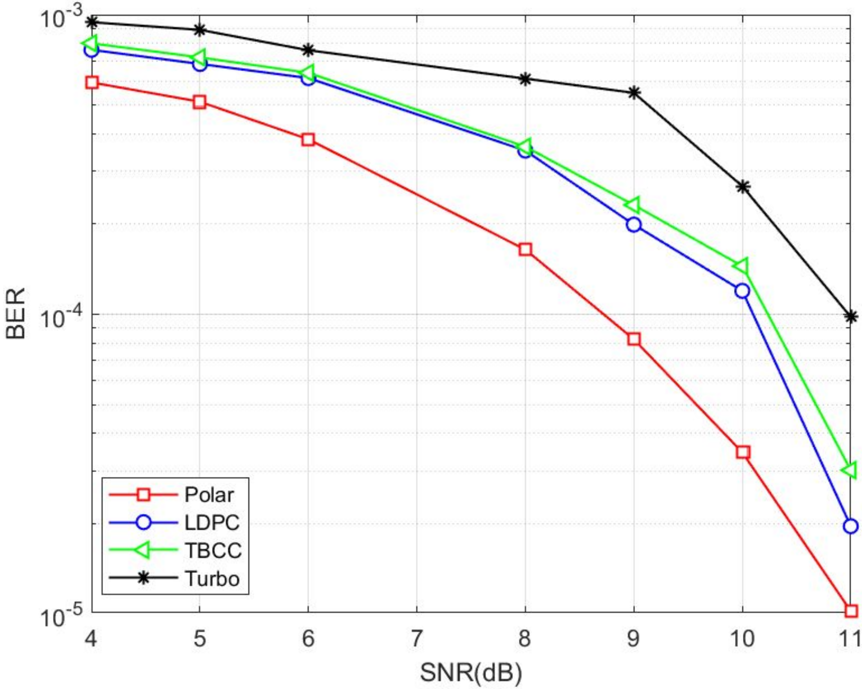
correct errors using FEC/ECC

ECCs offer tradeoff between throughput and BER

problems:

Cliff effect

Limited gain



Alternative #1 reduce code rate

EC Type	Typical Use Case	Max Theoretical Coding Gain (dB)	Notes
Reed-Solomon (RS)	Optical networks, legacy systems	~6–8 dB	Hard-decision; good for burst errors; e.g., RS(255,239) used in G.709
LDPC (Low-Density Parity-Check)	DVB-S2, 5G, Wi-Fi, deep space	~9–11 dB	Soft-decision; excellent near Shannon limit; widely adopted
Turbo Codes	3G/4G, satellite, deep space	~8–10 dB	Soft-decision; good at low SNR; used in CCSDS and 3GPP
Polar Codes	5G NR (control channels)	~9–10 dB	Capacity-achieving; efficient for short block lengths
Product/Trellis Codes	Legacy modems, magnetic storage	~6–8 dB	Moderate complexity; used in older systems

Acceptable BER (post FEC)

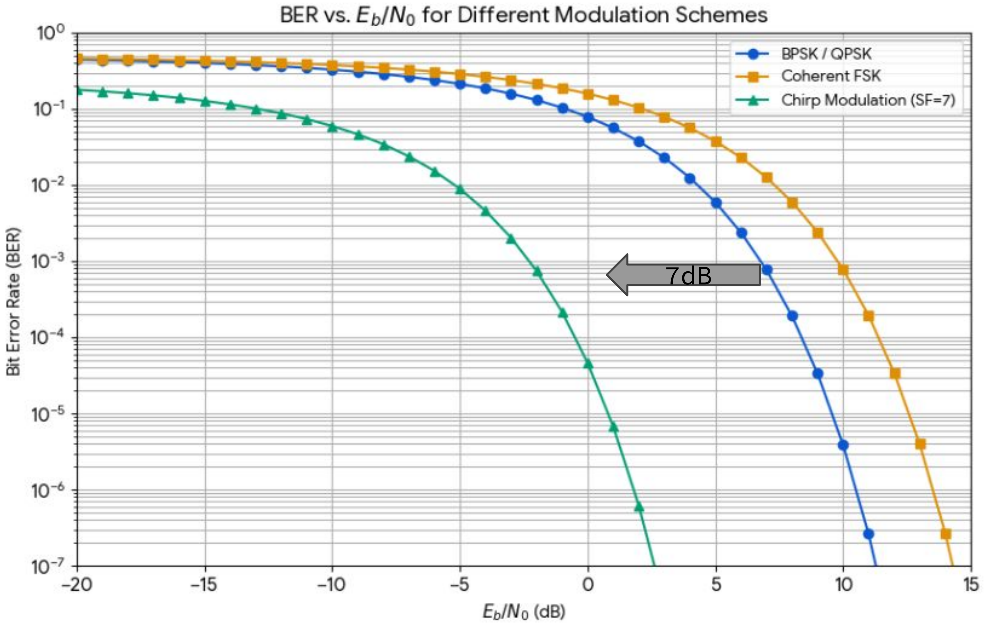
Application	Typical Acceptable Post-FEC BER	Why?
Telemetry and Sensor Data	10^{-5} to 10^{-6}	Occasional errors may be tolerable, and data can often be re-requested or interpolated.
Voice Communication	10^{-3} to 10^{-4}	The human ear can tolerate some level of digital artifacts before the quality becomes unacceptable.
Standard Data Transfer (e.g., file transfers)	10^{-7} to 10^{-9}	Higher-level protocols like TCP/IP can handle retransmissions, but a high error rate will significantly slow down the transfer.
Critical Control Systems	10^{-9} or lower	Errors could have serious consequences, requiring a very high degree of reliability.
High-Quality Video Streaming	10^{-9} to 10^{-12}	To avoid visible artifacts and ensure a smooth viewing experience.

Compare to LoRa

For CR = 4/7 (Hamming(7,4)): The maximum tolerable pre-FEC BER is approximately **1.8×10-3** (about 18 raw errors per 10,000 bits).

Spreading Factor (SF)	Required SNR for Post-FEC BER ≈ 10^{-5}	Semtech Demodulation Floor (SNR Limit)	Cliff Proximity
SF7	-5.5 dB	-7.5 dB	Operating ~2.0 dB above the absolute limit.
SF8	-8.0 dB	-10.0 dB	Operating ~2.0 dB above the absolute limit.
SF9	-10.5 dB	-12.5 dB	Operating ~2.0 dB above the absolute limit.
SF10	-13.0 dB	-15.0 dB	Operating ~2.0 dB above the absolute limit.
SF11	-15.5 dB	-17.5 dB	Operating ~2.0 dB above the absolute limit.
SF12	-18.0 dB	-20.0 dB	Operating ~2.0 dB above the absolute limit.

So our “limit” for 10^-5 BER post ECC is ~ 0.5% (5 x 10^{-3}) ~+7dB SNR



Alternative #2 time spreading/reduced BW

For 125KHz Ts = ~250mSec SF = 10 → BAUD = 4

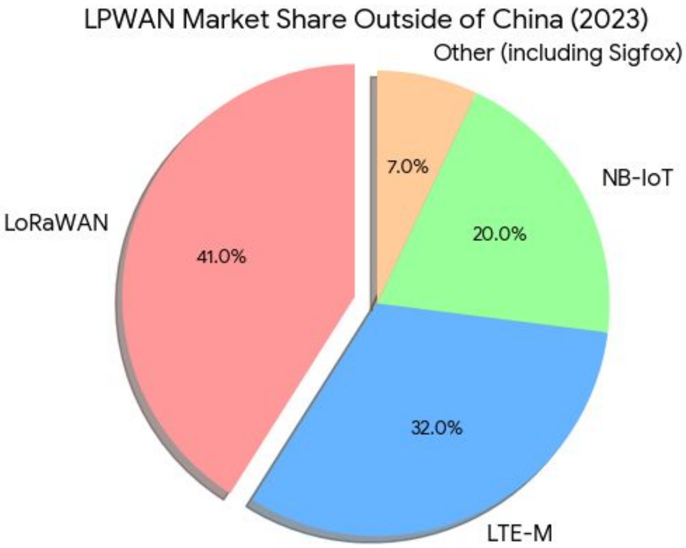
So how many SC symbols fit side by side?

Number of Channels = 125,000 Hz / 4 Hz/channel = **31,250** channels

Problem : ICI, need high two stage receiver (super heterodyne) for channel separation

LoRa alternatives

(real ones)


LPWAN Market Share Outside of China (2023)
Other (including Sigfox)
7.0%
NB-IoT
20.0%
LoRaWAN
41.0%
32.0%
LTE-M

Sigfox: The "Laser Pointer" Approach 🔦

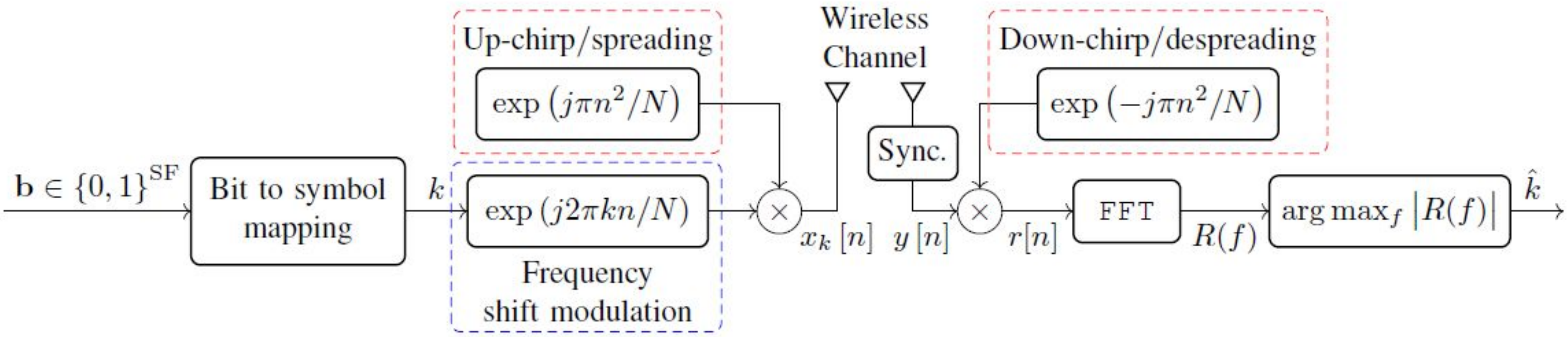
- Sigfox uses Ultra-Narrowband (UNB) modulation for long range.
- It transmits data on a very narrow 100 Hz channel.
- Concentrated power allows signals to stand out from noise.
- Sigfox devices send data packets three times on different frequencies.

NB-IoT & LTE-M: The "Repetition" Approach 🗣️

- NB-IoT and LTE-M achieve range through data packet repetition.
- Devices retransmit the same data multiple times, up to 2,048 for NB-IoT.
- Receivers combine these repetitions to decode weak signals.
- This "Coverage Enhancement" balances range, data rate, and power.

CSS receiver and demodulator

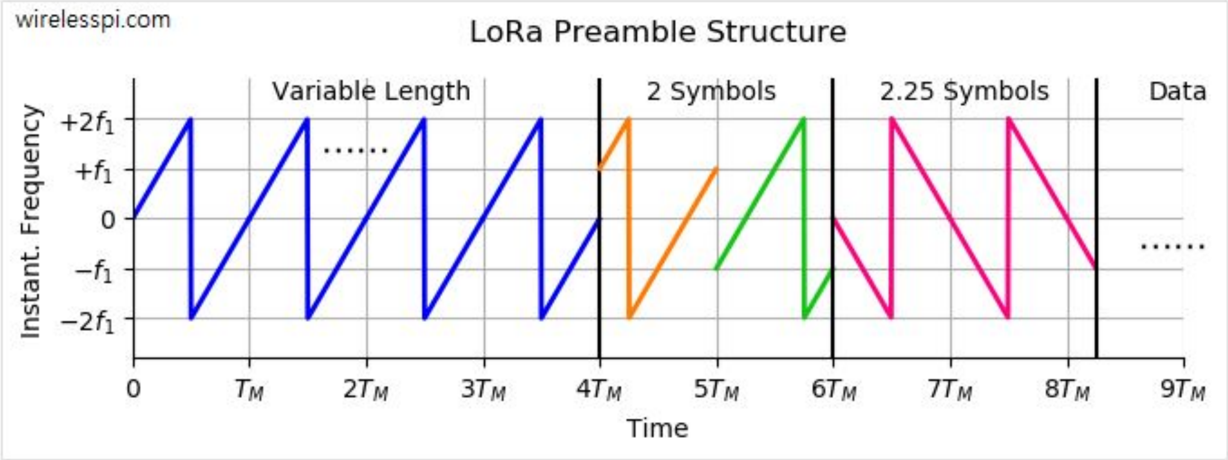
LoRa TRx block diagram



LoRa receiver

1. Preamble detection
2. Time /freq sync
3. Demodulation

LoRa preamble



8x (or more) unmodulated “base” upchirps

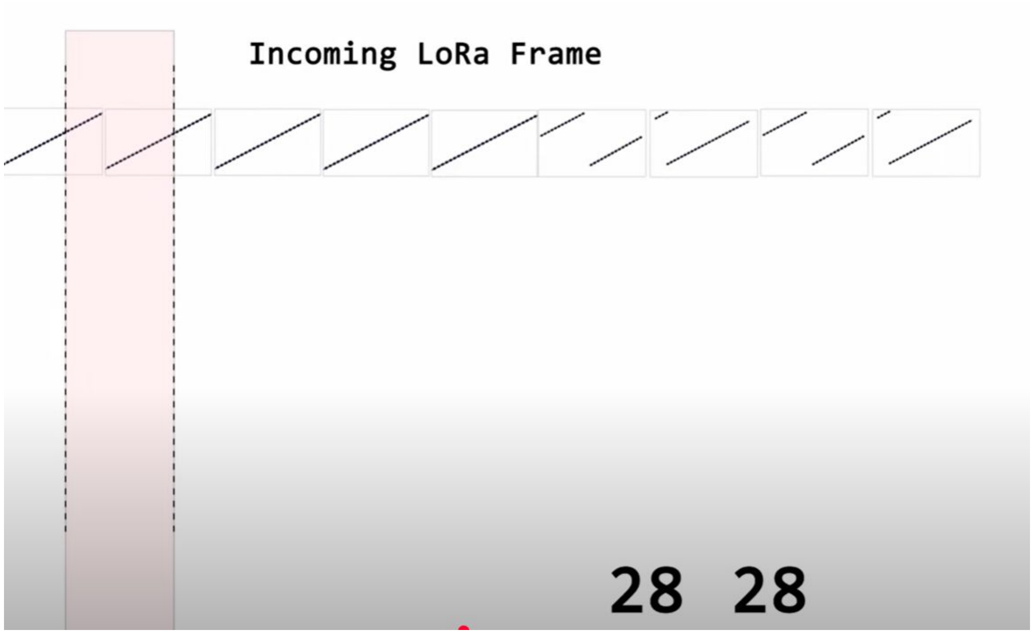
2x modulated upchirps (network ID/sync word)

2.25x down chirps (conjugate/freq flipped version of an up chirp)

detection

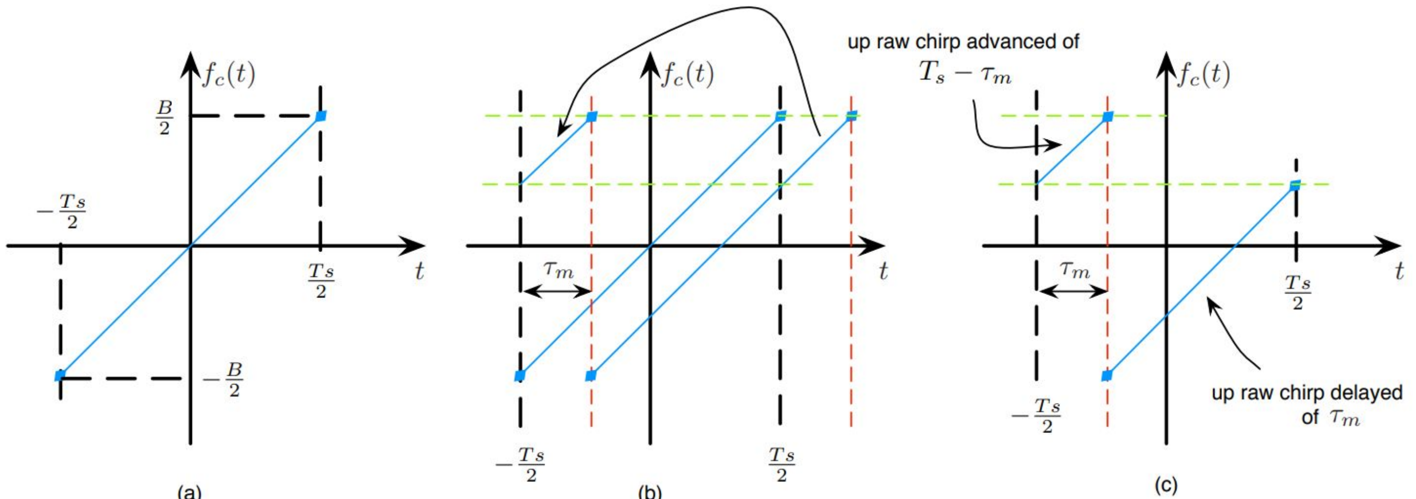
Repetitive symbols indicate activity

Can be configured to have many symbols - suitable for detection in very low SNRs



LoRa under timing offset

Since a LoRa symbol is created by cyclically shifting the base chirp, a time delay (of a repeated signal, say during the preamble results in symbol mismatch



CFO range

---

from loraWAN spec:

An end-device operating in the **EU863-870 MHz** band must have a clock source with a tolerance **better than ±20 ppm**. (17.4KHz)

An end-device operating in the **US902-928 MHz** band must have a clock source with a tolerance **better than ±30 ppm**. (31.25KHZ)

For a standard **125 kHz** LoRa channel, an offset of ±17.4 kHz is a significant error—it's almost 14% of the entire channel bandwidth.

The LoRaWAN specification actually requires that a receiver must be able to tolerate a frequency offset of at least **25% of the channel bandwidth**. For a 125 kHz channel, this means it must work even with an offset of **±31.25 kHz**.

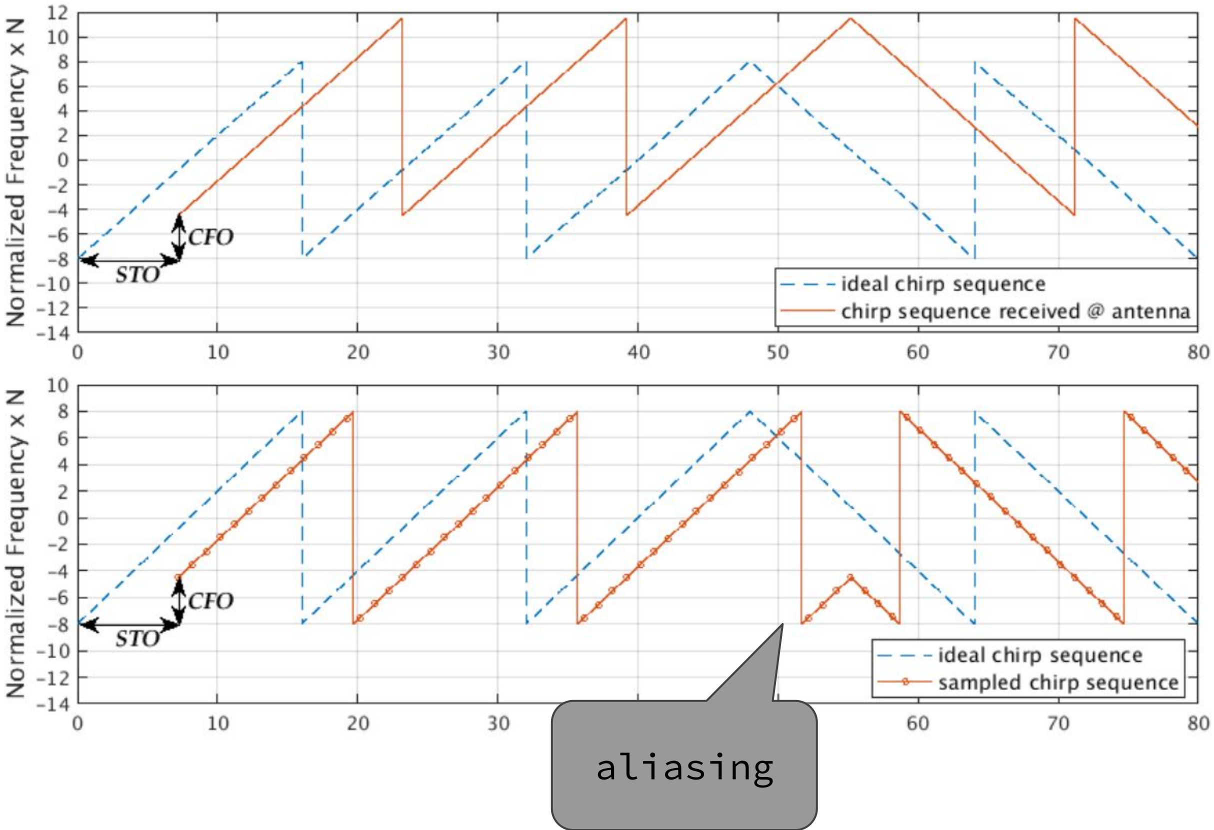
Freq offset insight

For a BW rate receiver (Fs = BW), freq offset appears to be cyclic due to aliasing.

For an OverSampling receiver in inherently more complex and expensive thus more specialized estimation and correction is feasible

Effect of timing and freq offset at receiver

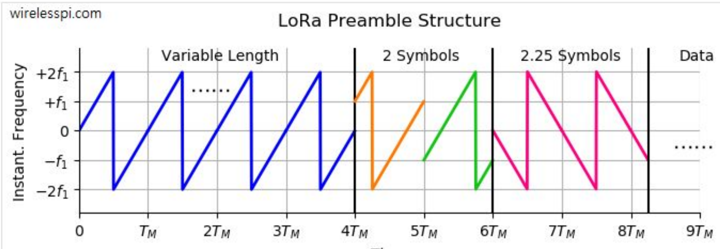
Top: signal received at the antenna suffering from an *STO* of 7.2 samples and a *CFO* of 3.5 frequency bins. Bottom: same signal after sampling at a normalized rate of 1/N (assuming *SF* = 0).



The LoRa Preamble: Purpose & Structure

The preamble is the critical first part of a LoRa packet, designed to achieve three main goals:

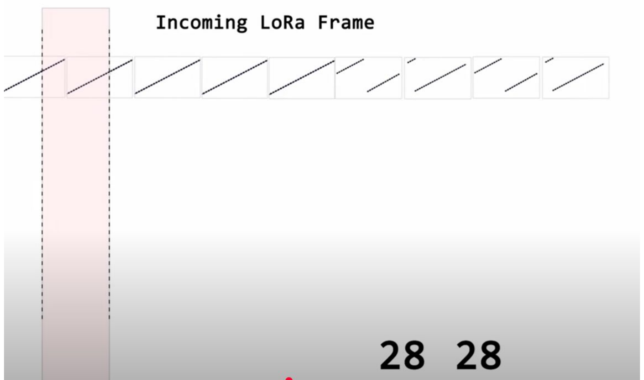
- **Detection**: Wake up the receiver and signal that a packet is arriving.
- **Identification**: Allow the receiver to filter for packets on its specific network.
- **Synchronization**: Precisely align the receiver's timing and frequency for decoding.



Stage 1 - Searching for the Preamble

Method: The receiver continuously scans the spectrum. It uses a correlator to find a match for the basic LoRa "up-chirp" symbol.

Detection: When it finds a sequence of several identical up-chirps in a row, it concludes that it has detected the start of a preamble.



Coarse timing correction

We can use the demodulated signal value as an estimate of timing offset (why?)

Stage 2 - Network ID Filtering

Goal: Verify the packet belongs to the correct network and discard irrelevant traffic.

Method: After the initial up-chirps, the receiver expects to see two specific, different symbols. The value of these two symbols is derived from the pre-configured Network ID (also called a Sync Word).

Filtering: The receiver compares the symbols it just received to the Network ID it is configured to listen for.

Match: If the IDs match, the receiver continues processing the packet.

No Match: If they don't match, the packet is discarded, saving power and processing time. The receiver goes back to searching for a new preamble.

Stage 3: isolating up and down chirps for freq/time synchronization

---

After net ID, we either search for two consecutive value down-chirp (post FFT).

Now we have successfully isolated up and down chirps.

Effect of timing and freq offset at receiver

These effects can be separated into fractional and integer components.

$$y(t) = e^{j2\pi t \Delta f_c} x_s(t + \tau)$$

$$\Delta f_c = B \cdot \frac{L_{\mathrm{CFO}} + \lambda_{\mathrm{CFO}}}{N}, \tau = \frac{L_{\mathrm{STO}} + \lambda_{\mathrm{STO}}}{B}$$

Compare with “classic” correction methods

———

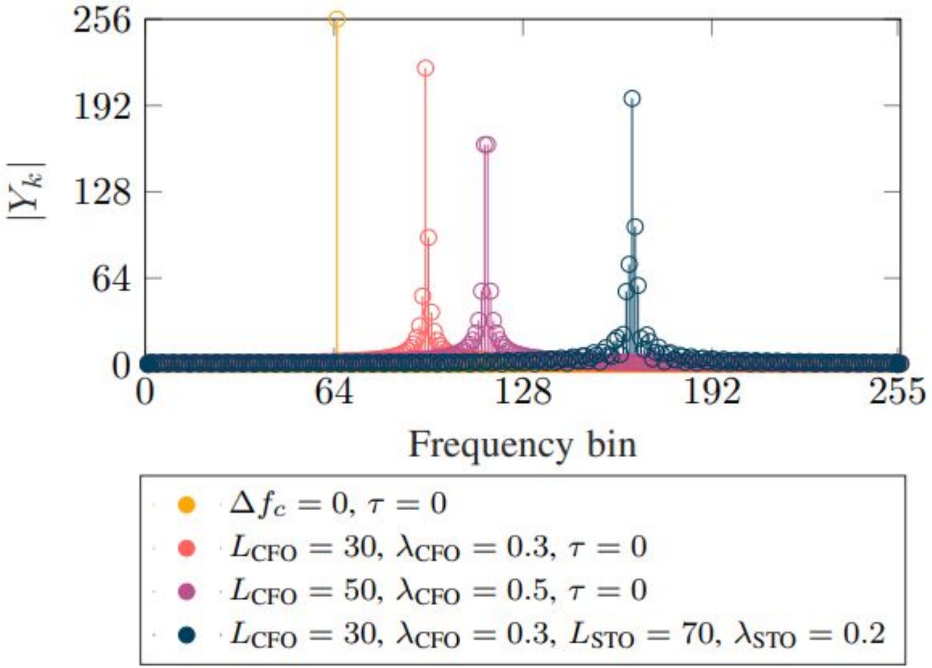
Auto-correlation of repeating signal for coarse timing

Coarse freq estimation and correction…

Cross correlation for fractional timing estimation and correction

fractional timing estimation and correction (early-late, eye diagram)

Effect of timing and freq offset at receiver



Amplitudes |Y_k| obtained when demodulating a repeating symbol s = 64 (SF = 8) without AWGN for different CFO and STO values. Integer offsets displace the Kronecker delta originally located at k = 64, whereas fractional offsets scatter the delta on several frequency bins.

Solving for integer freq and timing offset

Note that a whole ferq offset of BW/2^SF results in **one bin shift in the output of the FFT**

Note that whole sample offset of T/2^SF results in **one bin shift in the output of the FFT**

Solving for integer freq and timing offset

An incoming signal, $r(t)$, received with a time offset τ and a carrier frequency offset (CFO) Δf, can be modeled as:

$$r(t) = s_u(t-\tau)e^{j2\pi\Delta f t} = e^{j2\pi(f_0(t-\tau)+\frac{1}{2}k(t-\tau)^2)}e^{j2\pi\Delta f t}$$

$k = \frac{B}{T}$ is the chirp rate,

The receiver performs de-chirping by multiplying the received signal $r(t)$ with the complex conjugate of a locally generated, ideal reference up-chirp, $s_u^*(t)$.

$$y(t) = r(t) \cdot s_u^*(t)$$

$$y(t) = \left[e^{j2\pi(f_0(t-\tau)+\frac{1}{2}k(t-\tau)^2)}e^{j2\pi\Delta f t}\right] \cdot \left[e^{-j2\pi(f_0 t+\frac{1}{2}kt^2)}\right]$$

Solving for integer freq and timing offset

$$y(t) = e^{j2\pi\boxed{(\Delta f - k\tau)}t} \cdot e^{j2\pi(\frac{1}{2}k\tau^2 - f_0\tau)}$$

The second term is a constant phase shift so peak power of FFT output is:

For an **up-chirp** (where the chirp rate is $+k$), the measured peak frequency from the FFT is:

$$f_{up} = \Delta f - k\tau \qquad (1)$$

For a **down-chirp** (where the chirp rate is $-k$), the same derivation yields:

$$f_{down} = \Delta f - (-k)\tau = \Delta f + k\tau \qquad (2)$$

The receiver now has a system of two linear equations with two unknowns, Δf and τ.

Solving for integer freq and timing offset

Solving for Frequency Offset (Δf)

Adding equation (1) and equation (2):

$$f_{up} + f_{down} = (\Delta f - k\tau) + (\Delta f + k\tau)$$

$$f_{up} + f_{down} = 2\Delta f$$

$$\Delta f = \frac{f_{up} + f_{down}}{2}$$

Solving for Timing Offset (τ)

Subtracting equation (1) from equation (2):

$$f_{down} - f_{up} = (\Delta f + k\tau) - (\Delta f - k\tau)$$

$$f_{down} - f_{up} = 2k\tau$$

$$\tau = \frac{f_{down} - f_{up}}{2k}$$

Solving for fractional freq offset

---

recall that the phase at the transmitter (upper image) is both continuous and does not accumulate between symbols (always resets at symbol boundary).

The phase contribution from STO wraps around symbol boundary

The phase contribution from CFO wraps around [-pi,pi]

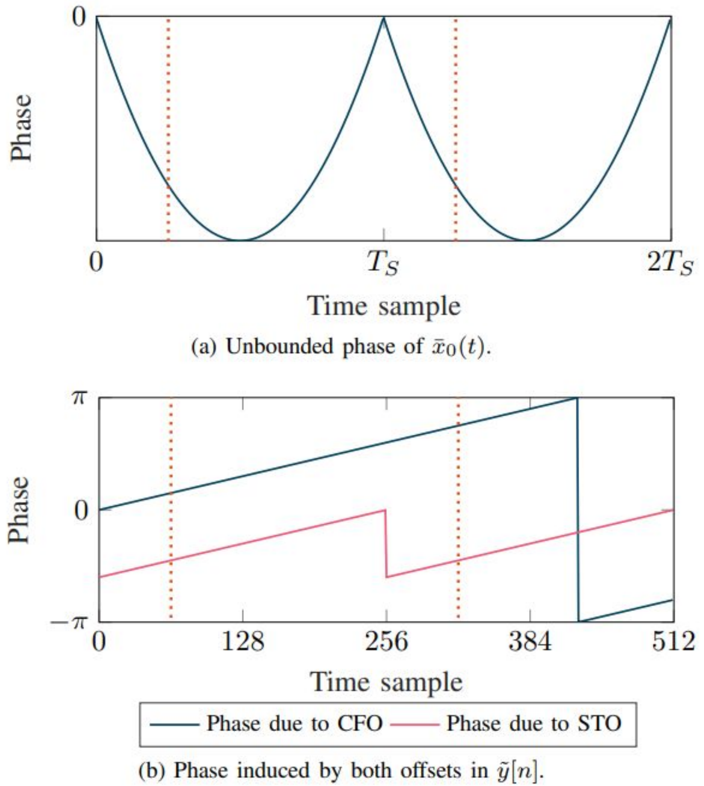


Fig. 5: Phases of two consecutive upchirps from the preamble (a) at the transmitter (b) after dechirping, at a receiver contaminated with a CFO $L_{\text{CFO}} = 10$, $\lambda_{\text{CFO}} = 0.3$ and an STO $L_{\text{STO}} = 64$, $\lambda_{\text{STO}} = 0.3$. The dotted lines indicate the windows of N samples processed by the receiver.

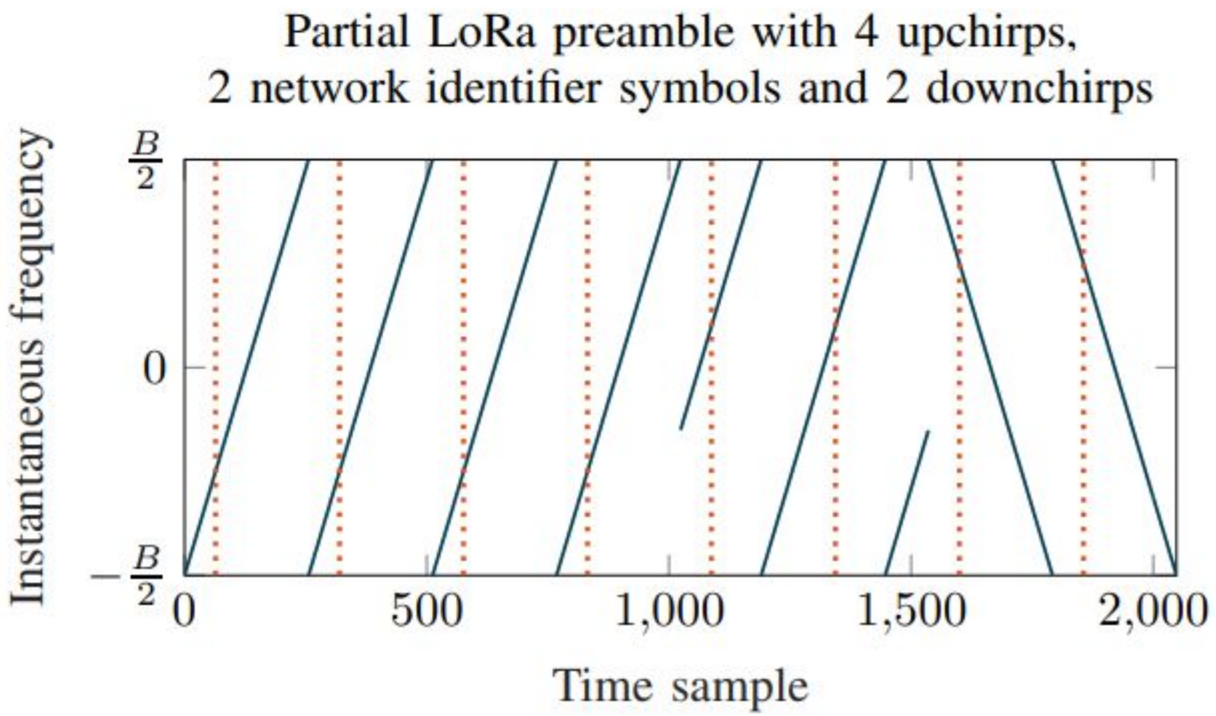


Fig. 4: Structure of a preamble for $\mathrm{SF} = 8$. The dotted lines delimitate the consecutive windows of N samples received under an integer STO $L_{\mathrm{STO}} = 64$. Only 4 upchirps are shown for the sake of clarity.

Solving for fractional freq offset

It can be shown that after FFT:

$$Y_k^l = e^{j2\pi\lambda_{\text{CFO}}} Y_k^{l-1}$$

Thus we can build the fractional CFO estimator:

$$\widehat{\lambda}_{\text{CFO}} = \frac{1}{2\pi} \text{angle} \left(\sum_{l=2}^{N_C} \sum_{p=-2}^{2} Y_{i+p}^l \cdot \overline{Y}_{i+p}^{l-1} \right)$$

with $i = \arg\max_k |Y_k^l|$. To improve the accuracy of the estimate, the five Y_k^l values of each symbol centered around the bin of maximum height are used.

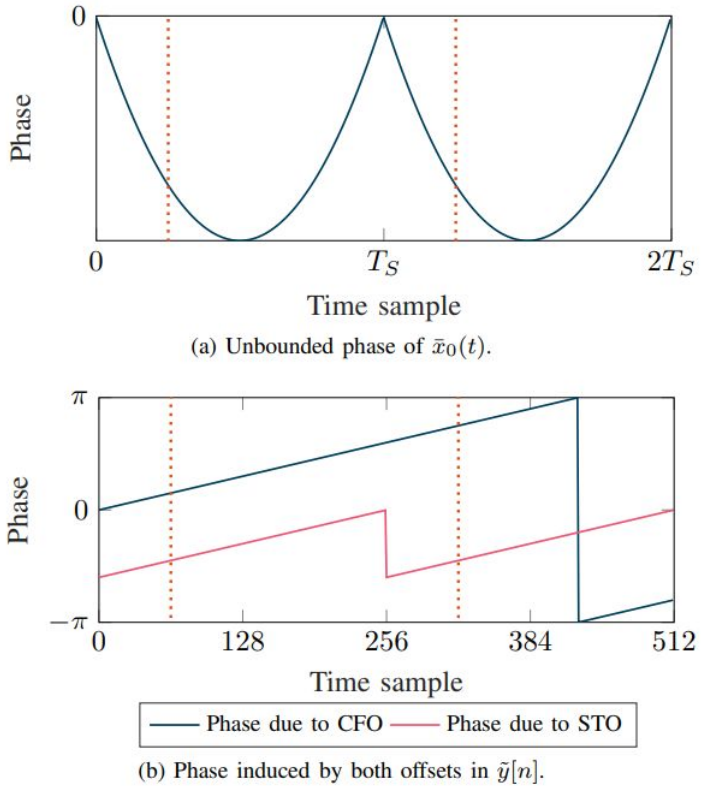


Fig. 5: Phases of two consecutive upchirps from the preamble (a) at the transmitter (b) after dechirping, at a receiver contaminated with a CFO $L_{\text{CFO}} = 10$, $\lambda_{\text{CFO}} = 0.3$ and an STO $L_{\text{STO}} = 64$, $\lambda_{\text{STO}} = 0.3$. The dotted lines indicate the windows of N samples processed by the receiver.

Fractional timing estimation

After integer and fractional freq correction, the receiver can perform cross correlation (match filtering) between a Rx, coarse-corrected and upsampled up chirp and an ideal locally stored up-chirp and search for the time offset that has the most energy.

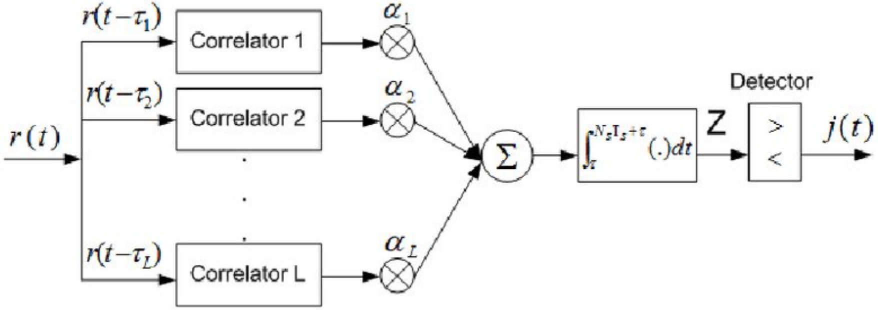
Fractional timing estimation viable due to pulse compression properties of chirp (later)

Handling multipath and doppler

Different paths show up after FFT as different symbols.

The receiver can either select the strongest, or use a rake receiver to combine all paths energy and increase SNR

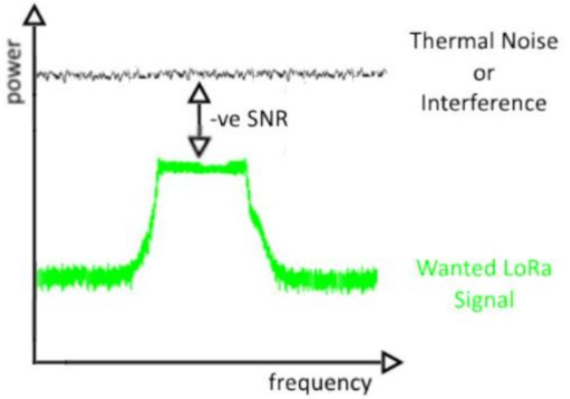
Diversity! Similar to rake receiver? For reference:



ISI

Negligible, due to extremely long symbol duration

Interferer immunity - LoRa specific strategies

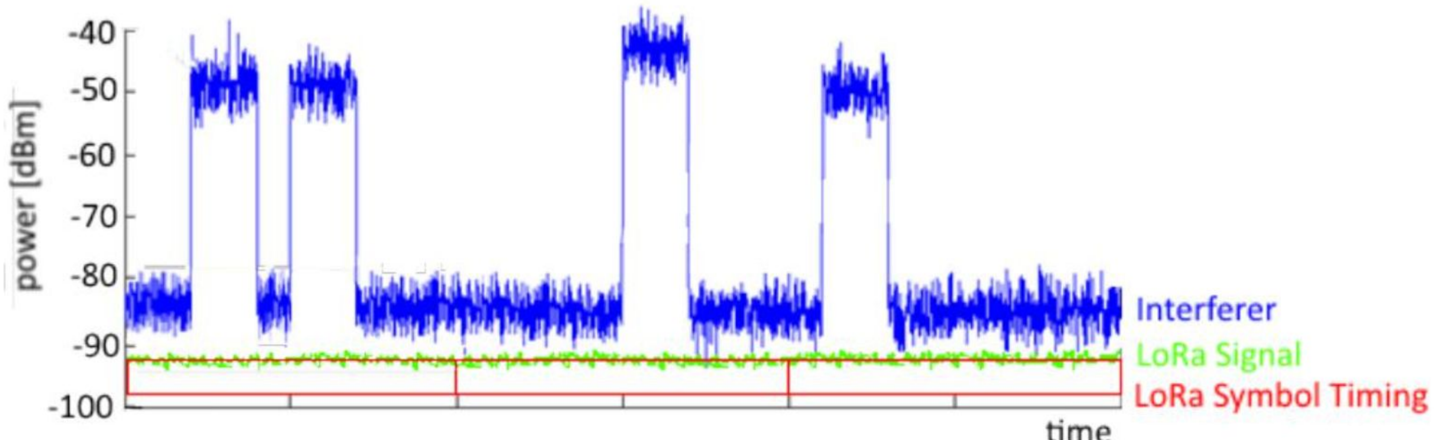


Spread spectrum gain- irrelevant for wideband interferer

Low BW → less power from interferer leaking

Scrambling and ECC

LoRa symbol is recoverable up to 50% loss from burst interferer



Ranging

chirp and time resolution

The chirp signal used in LoRa has a high BTP (BWxTs)

High BTP signals have a very sharp autocorrelation property

Making them ideal for timing synchronization and ranging

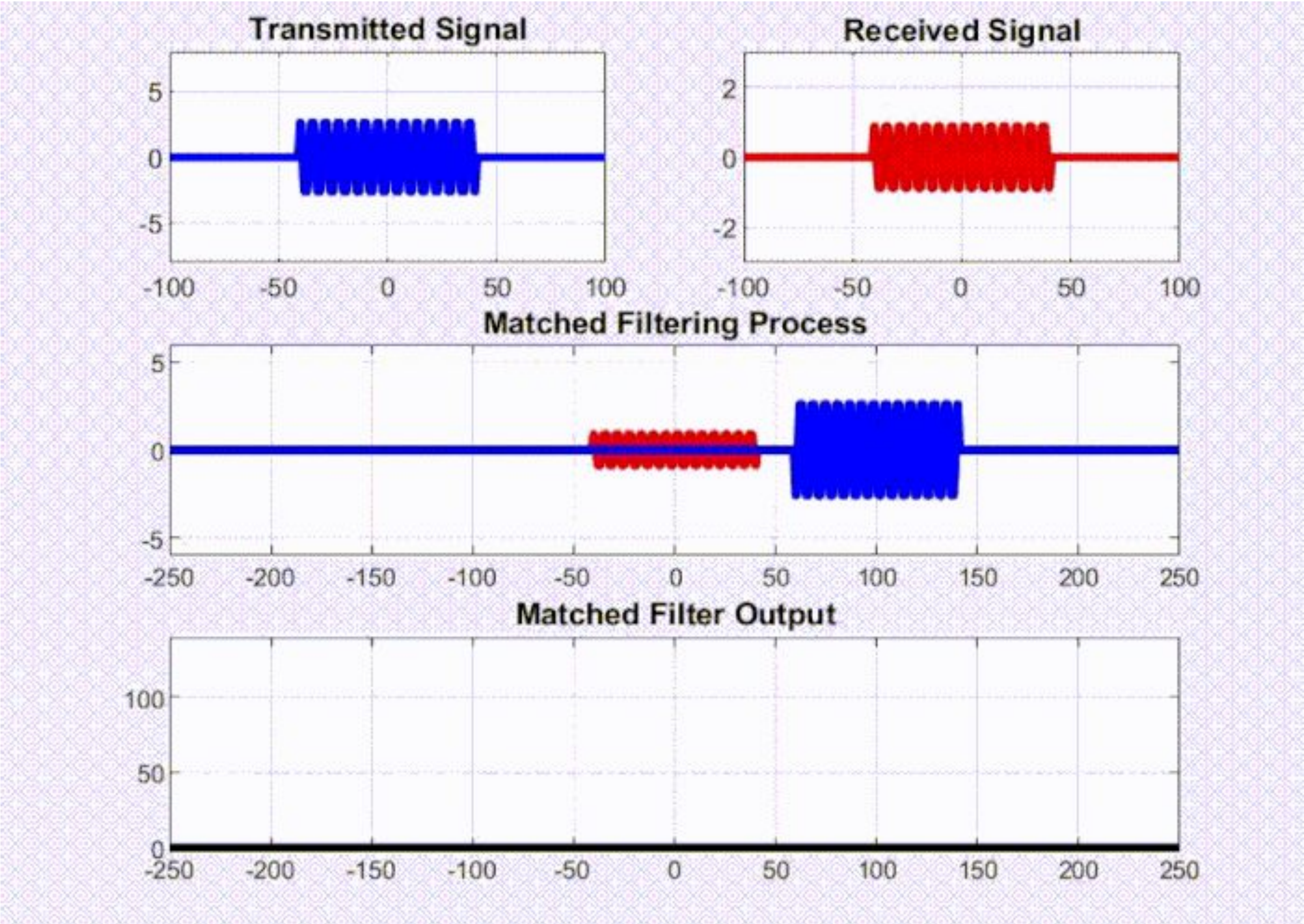
Chirp compression in radar

For chirp signal, after match filtering, the result is a sinc pulse with $\tau \approx 1/B$ TD width, and power proportional to $\sqrt{(T \times B)}$

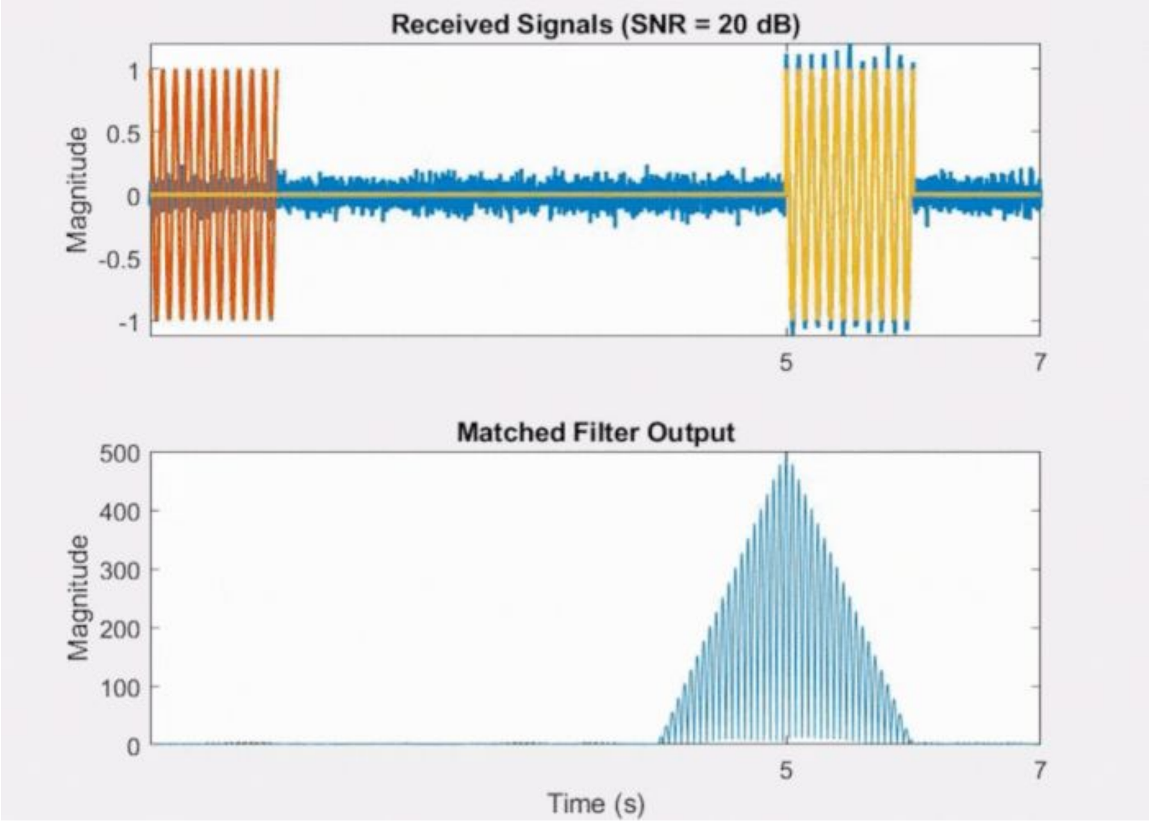
$$|\text{Compressed Output}| \approx \sqrt{T.B} \times \frac{\sin(\pi B t)}{(\pi B t)}$$

A chirp signal is then desirable for RADAR (Radio Detection And Ranging) as it offers high temporal resolution.

Match filter output for sinusoidal signal

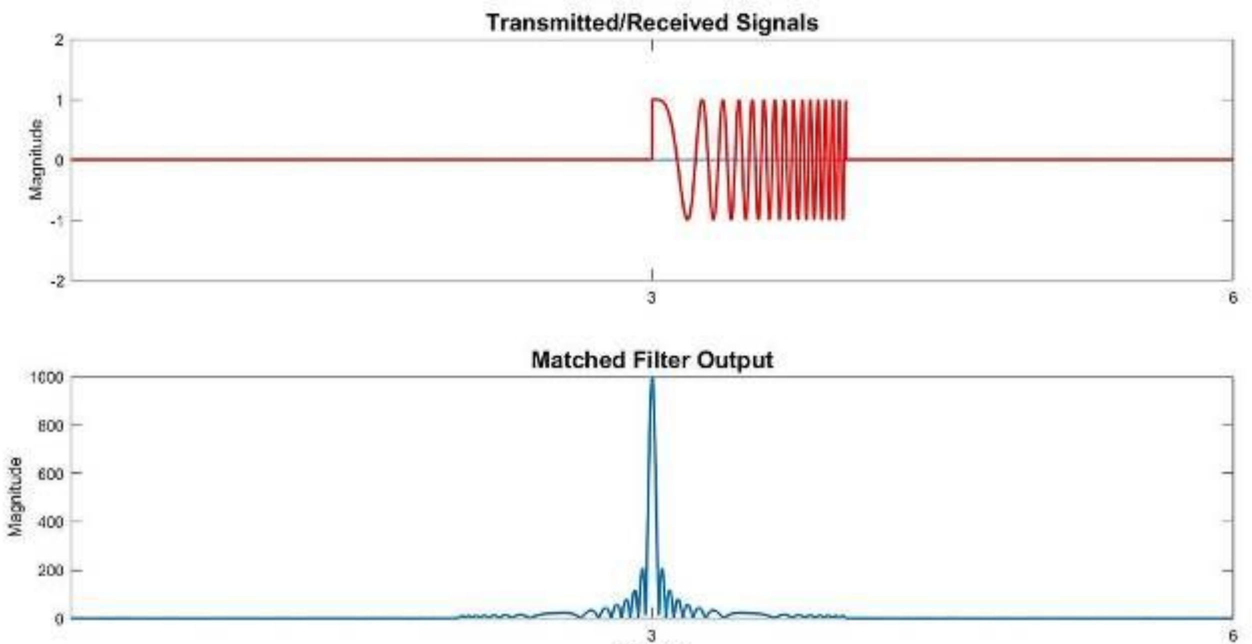


Rectangular pulse under low SNR

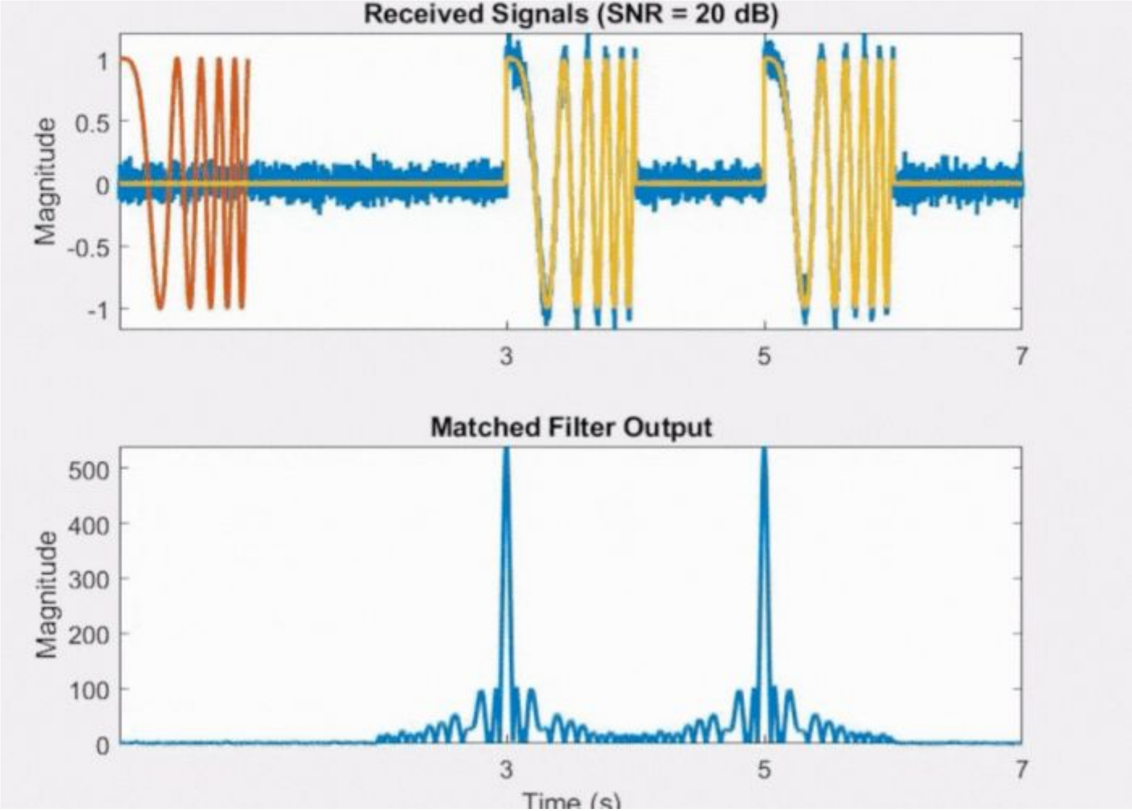


MF output for chirp signal

The output seems “compressed” in time



Chirp pulse under low SNR



simulator

Simulator

https://matanleilien.github.io/teaching_aids/

LO requirements for ranging

Feature	Crystal Oscillator (XO)	Temperature-Compensated Crystal Oscillator (TCXO)
Frequency Stability	Moderate (±10 to ±30 ppm)	High (±1 to ±5 ppm)
Approximate Ranging Error	Potentially >100 meters	As low as a few meters
Approximate Cost (Bulk Qty)	\$0.30 - \$0.90	\$1.50 - \$4.00+ (approx. 3-5x more expensive)
Approximate Power Consumption	Very Low (tens to hundreds of μA)	Low (a few mA) (approx. 5-10x more)
Performance Over Temperature	Significant frequency drift	Minimal frequency drift
Complexity	Simpler	More complex internal circuitry

Ranging procedure

For ranging, the group delay of the RFFE is calibrated before hand such that the LoRa ranging device has in HW/FW fine control of the delay between reception of ranging signal to the transmission of the ranging reply.

So for this discussion we assume that ranging reply is sent instantaneously (delay = 0).

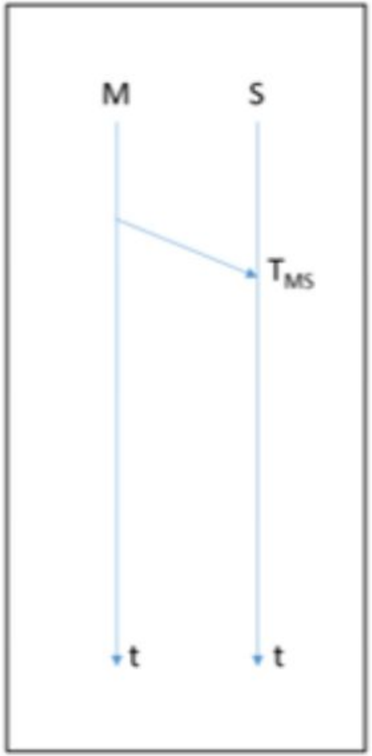
Basic ranging

Relies on Round Trip Time-of-Flight (RTToF) measurements

The basic principle of RTToF distance measurement is illustrated below. In this first diagram, a ranging request is sent from the ranging Master to the ranging Slave. At the same moment that the Master transmits its request, it also starts an internal timer.

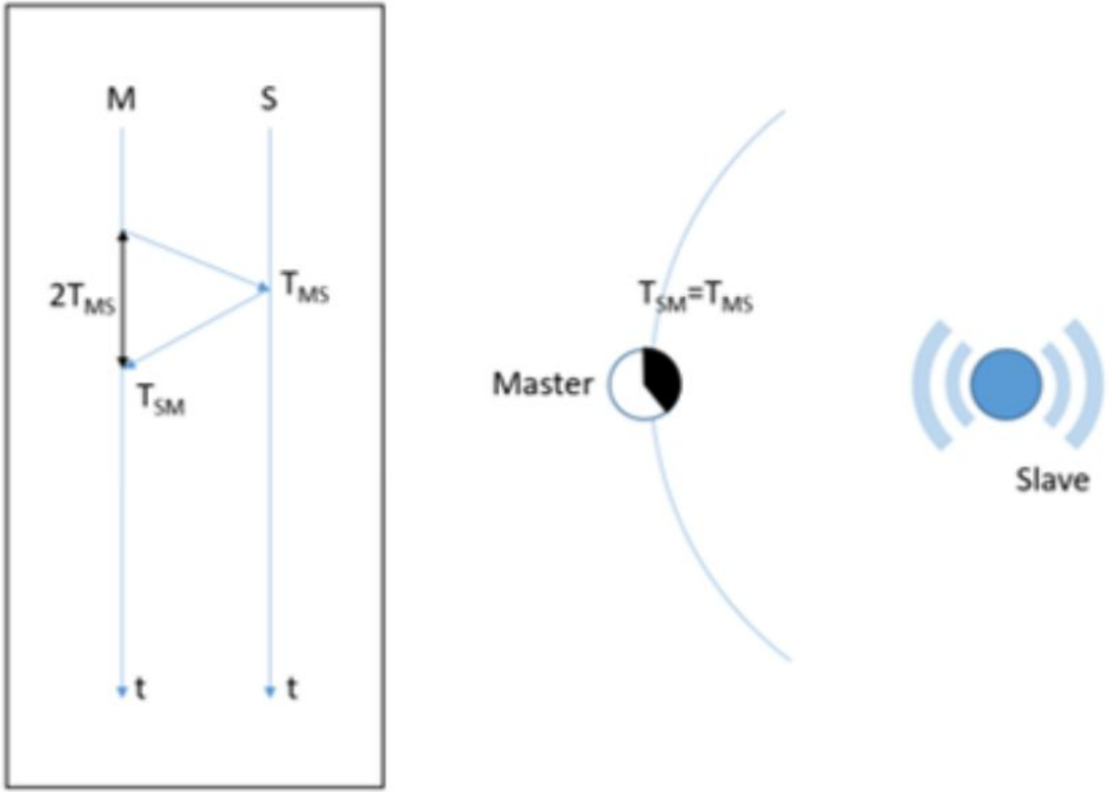
Basic ranging

The line indicates the geometrical position of all locations of equal Tms



Ranging response

The ranging result is a sphere at distance Tms around the master

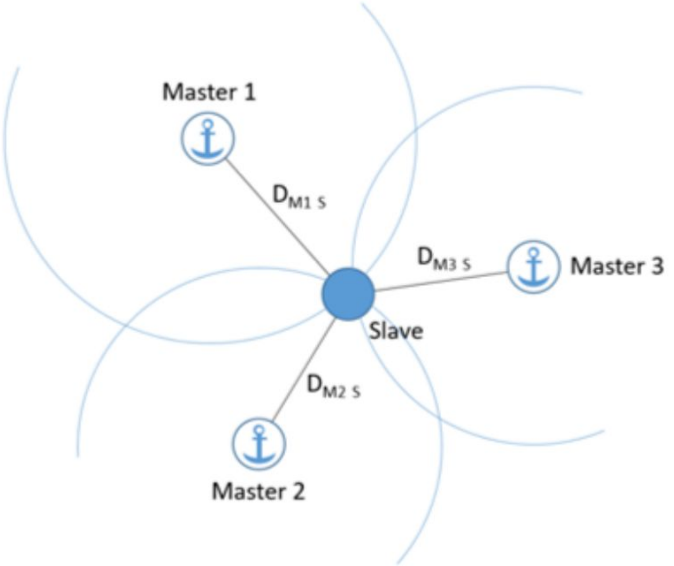


Ranging localization

“Anchors” have a known and fixed location.

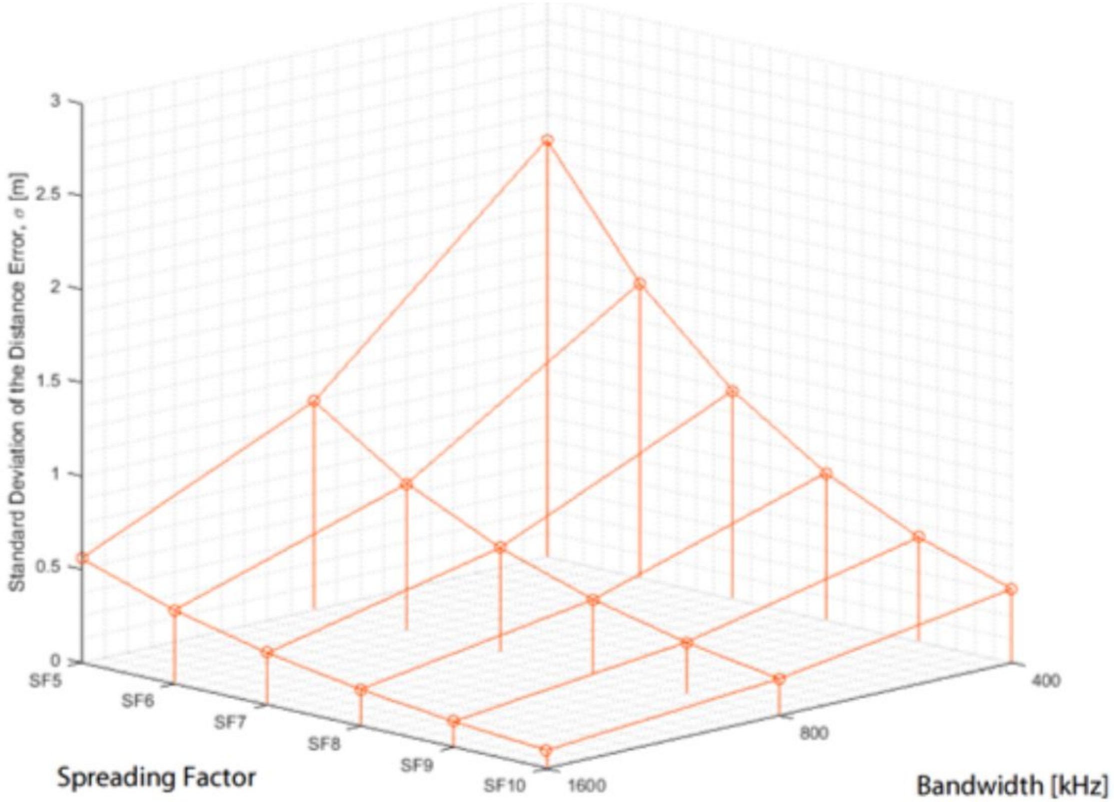
Localization requires the intersection of (at least) 3 spheres:

Master role can also be the mobile tag for the purpose of self localization



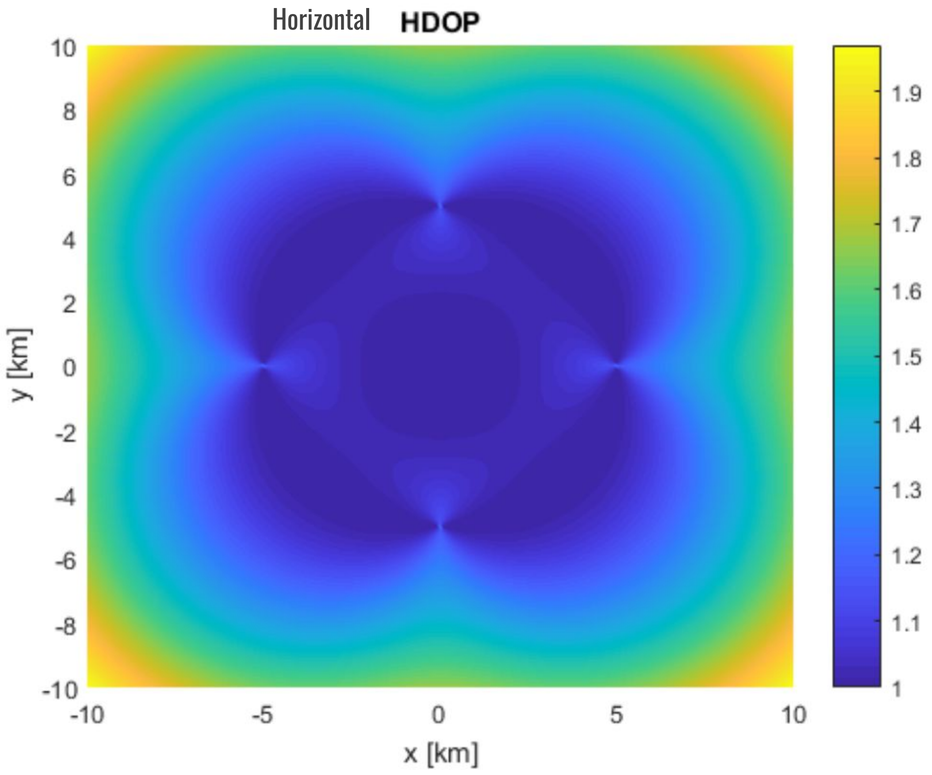
Ranging theoretical performance

Recall that the time resolution of a compressed chirp is proportional to BTP



geometric dilution of precision (GDOP)

The implication of this theoretical result is that a tag will be a located with greater precision within the area delimited by the four anchors and, as we travel outside of this area, so the attainable location precision reduces

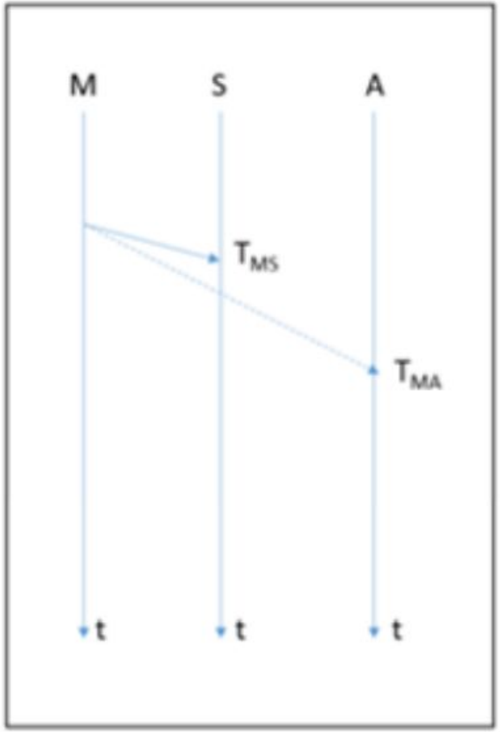


Advanced ranging

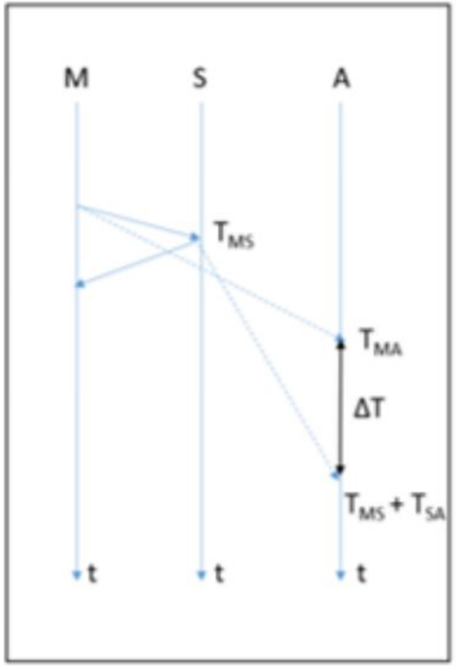
Instead of actively exchanging timing information, Advanced Ranging allows us to **passively** overhear ranging exchanges.

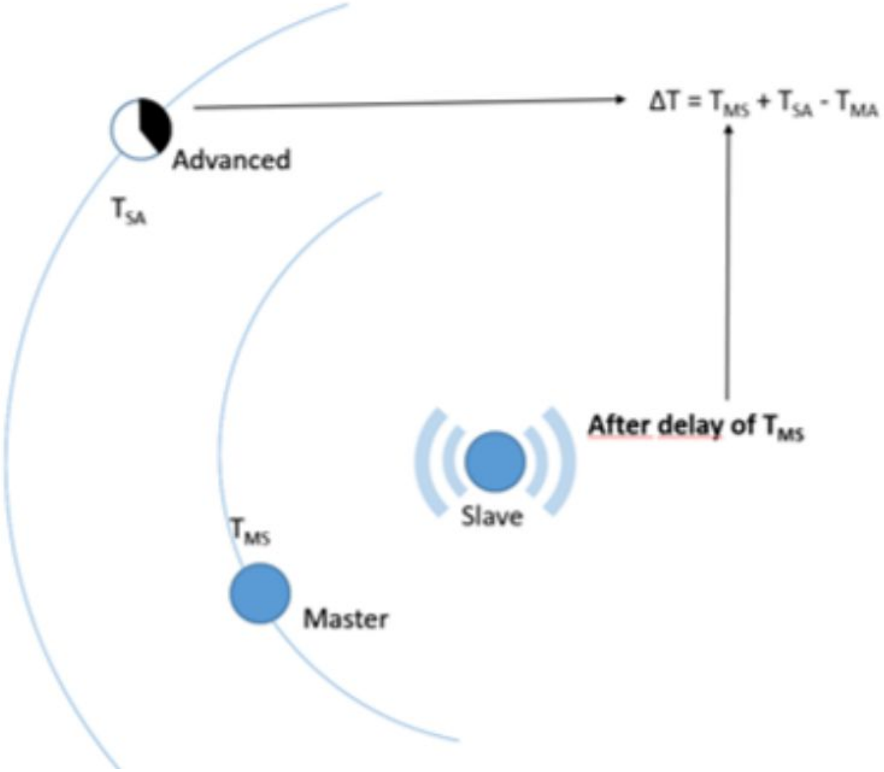
- Better positioning
- Higher network capacity
- Power conservation of listener tags

Advanced ranging



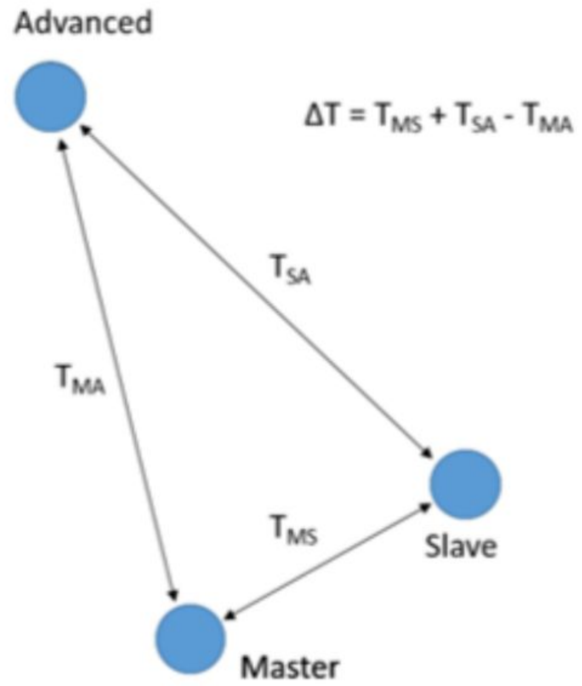
Advanced ranging





Advanced ranging

We now have a relationship between the distances on a triangle.



Advanced ranging tag

$$\Delta T = T_{MS} + T_{SA} - T_{MA}$$

Using this relationship, the geometrical position of the tag as the advanced unit is on a hyperbola (with anchors at foci).

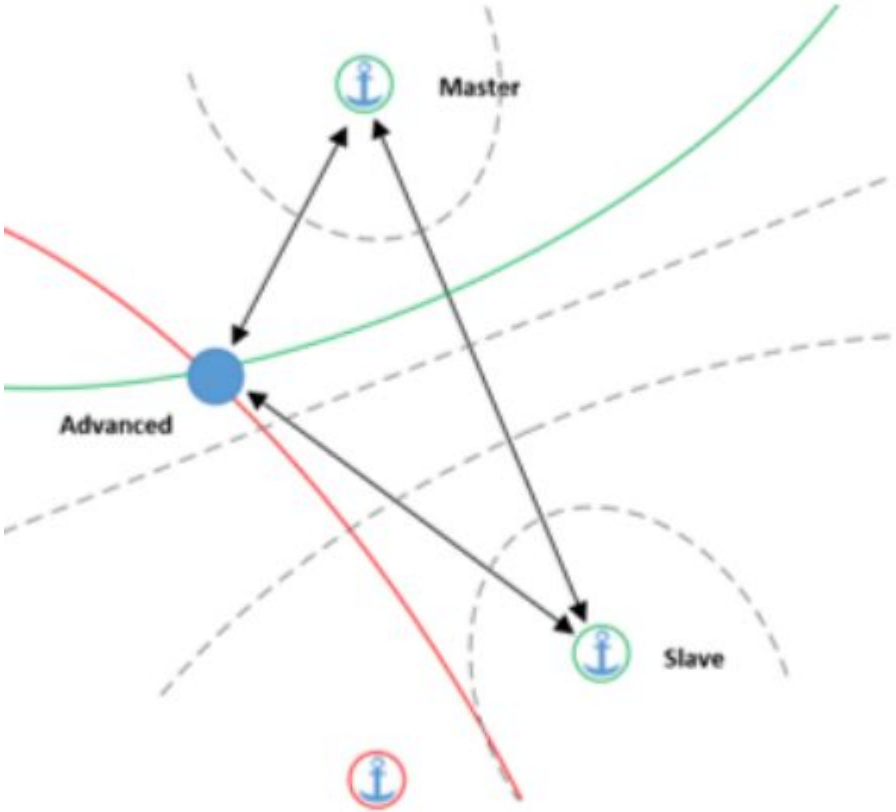
Dotted lines are lines of equal delta_T

Another measurement

We can now properly intersect two hyperbolas to localize in 2D.

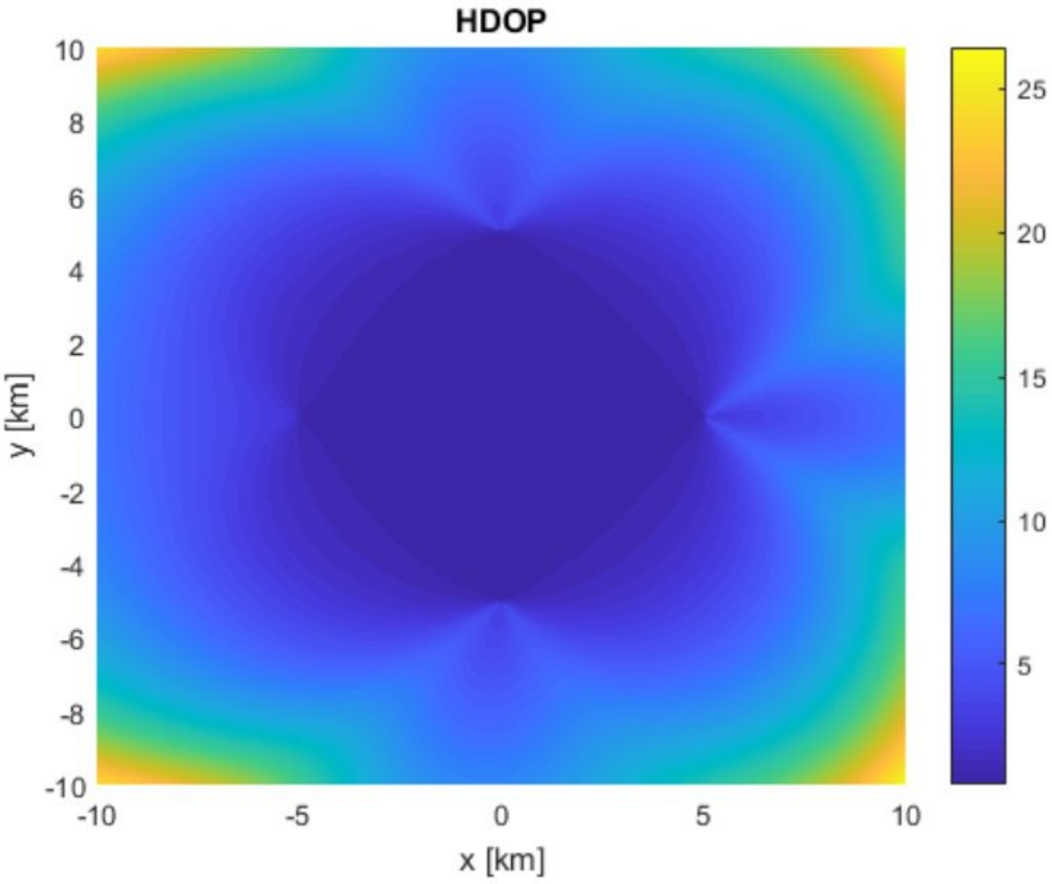
Note that the tag as advanced unit is totally passive.

This also means than infinite tags can benefit from the same measurements from anchors.



Tag as advanced HDOP

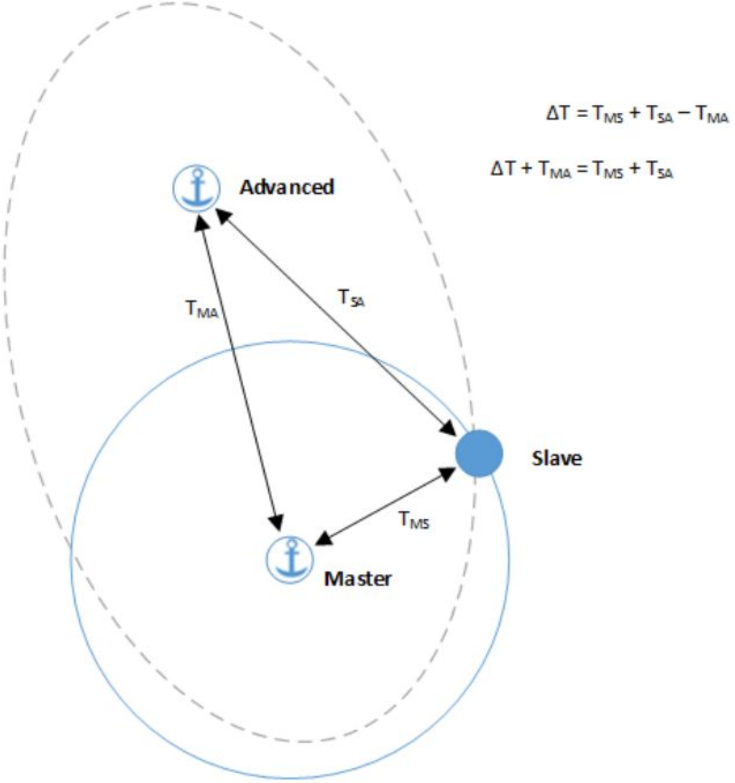
Advanced ranging tag exhibits similar accuracy between the anchors, but rapid degradation outside The anchors.



Advanced ranging with tag as slave

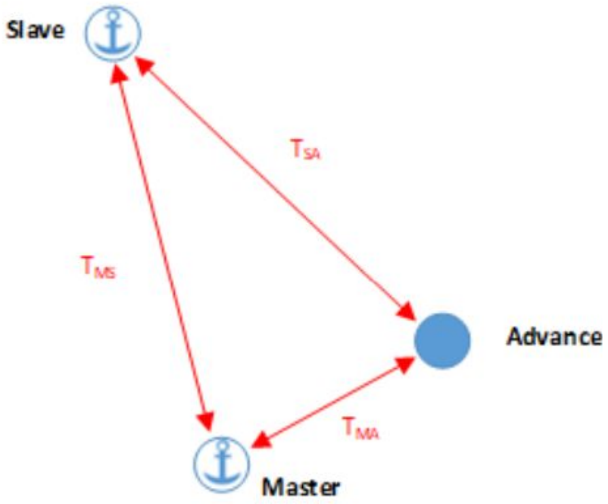
Here we use conventional RTToF measurement between master and slave, with another anchor as the advanced unit.

Note that not Tma is known in advanced.

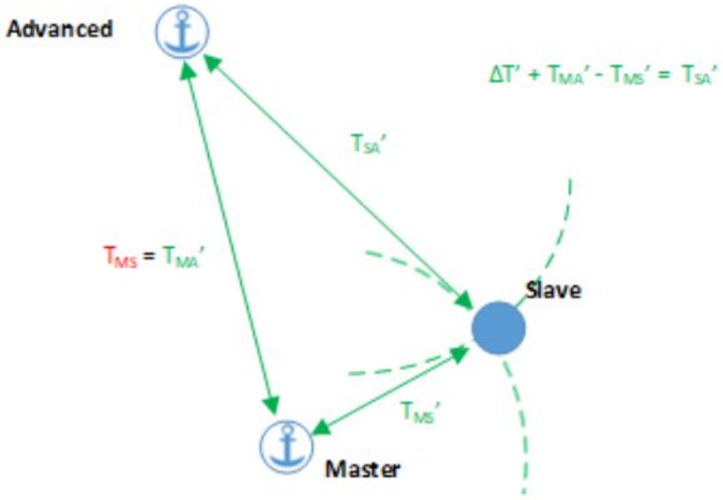


Hybrid approach

Step 1: Anchor Calibration



Step 2: Tag Measurement



This approach improves accuracy while keeping to a single RTToF measurement from the tag

sources

references

[1] L. Vangelista, "Frequency Shift Chirp Modulation: The LoRa Modulation," *IEEE Signal Processing Letters*, vol. 24, no. 12, pp. 1818-1821, Dec. 2017, doi: 10.1109/LSP.2017.2762723.

https://www.youtube.com/watch?v=jHWepP1ZWTk

[1] Semtech Corporation, "LoRa® Modulation Basics," Application Note AN1200.22, Rev. 2, May 2015.

[2] Semtech Corporation, "SX1272/73/76/77/78: LoRa Modem Designer's Guide," Application Note AN1200.13, Rev. 1, Jul. 2013.

https://wirelesspi.com/understanding-lora-phy-long-range-physical-layer/

https://www.semtech.com/uploads/technology/LoRa/theory-and-principle-of-advanced-ranging.pdf

https://www.semtech.com/uploads/technology/LoRa/lora-and-lorawan.pdf

https://dadb.com/in/blog/lpwan-use-cases-how-long-range-iot-connectivity-is-transforming-industries/

https://www.mobilefish.com/developer/lorawan/lorawan_quickguide_tutorial.html

https://www.semtech.com/uploads/technology/LoRa/predicting-lorawan-capacity.pdf

https://hal.science/hal-01977497/document

https://wirelesspi.com/the-power-of-pulse-compression/

https://patentimages.storage.googleapis.com/10/39/89/920d2ef29fb62e/EP3264622B1.pdf

https://www.researchgate.net/publication/344337974_In-phase_and_Quadrature_Chirp_Spread_Spectrum_for_IoT_Communications/link/5fbf9e3a299bf104cf7aa28b/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6Il9kaXJlY3QiLCJwYWdlIjoicHVibGljYXRpb24iLCJwcmV2aW91c1BhZ2UiOiJfZGlyZWN0In19