Meshtastic Under the Microscope

From Chirps to Chat

Allan Boll

RF Village at DEF CON 33

What's Meshtastic?

- Off-grid, multi-mile, low-power mesh network
- Text messages: DMs and group chats
- Open source firmware + phone app
- Censorship resistant
- Community momentum

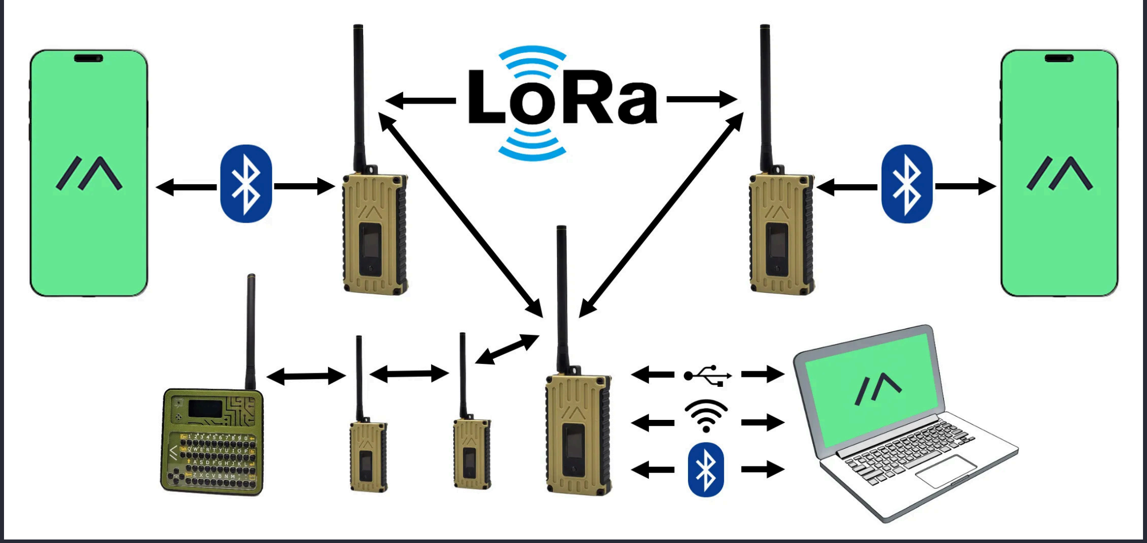
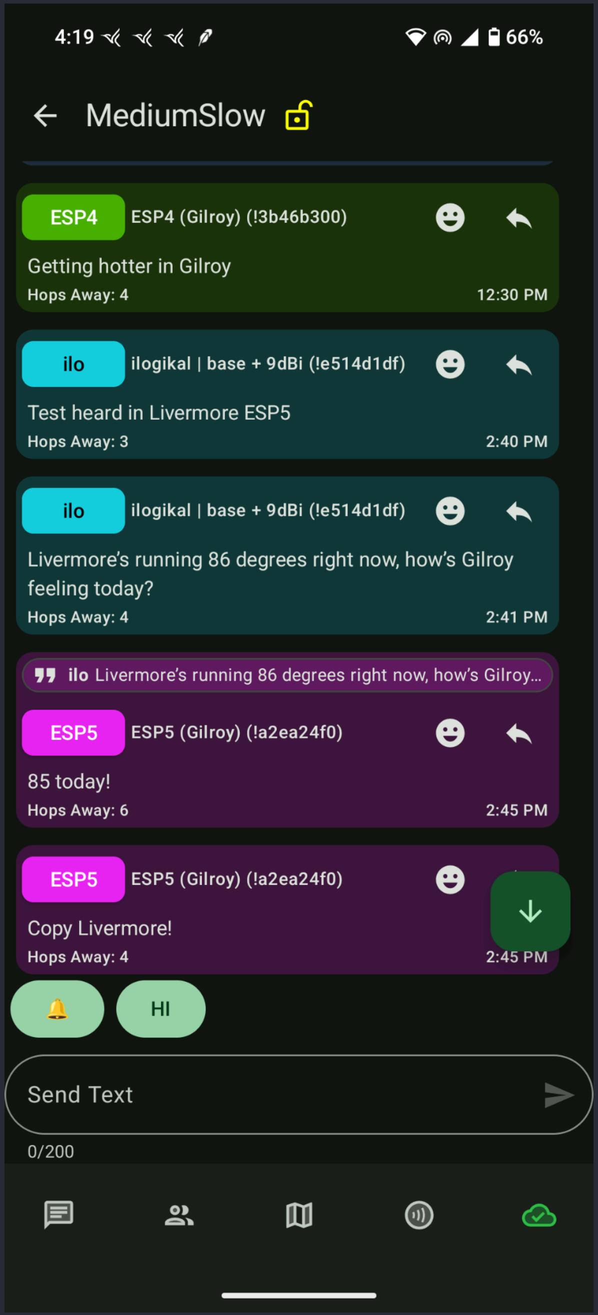


Image credit: https://meshtastic.org/docs/introduction/



ESP4 ESP4 (Gilroy) (!3b46b300)

Getting hotter in Gilroy

Hops Away: 4 12:30 PM

ilo ilogikal | base + 9dBi (!e514d1df)

Test heard in Livermore ESP5

Hops Away: 3 2:40 PM

ilo ilogikal | base + 9dBi (!e514d1df)

Livermore's running 86 degrees right now, how's Gilroy feeling today?

Hops Away: 4 2:41 PM

❞ ilo Livermore's running 86 degrees right now, how's Gilroy...

ESP5 ESP5 (Gilroy) (!a2ea24f0)

85 today!

Hops Away: 6 2:45 PM

ESP5 ESP5 (Gilroy) (!a2ea24f0)

Copy Livermore!

Hops Away: 4 2:45 PM

Agenda

- Audience prerequisites
- How LoRa is modulated and encoded
- How Meshtastic is encoded
- Software:
  - Gqrx
  - Inspectrum
  - GNU Radio
  - Wireshark
  - Bunch of Python

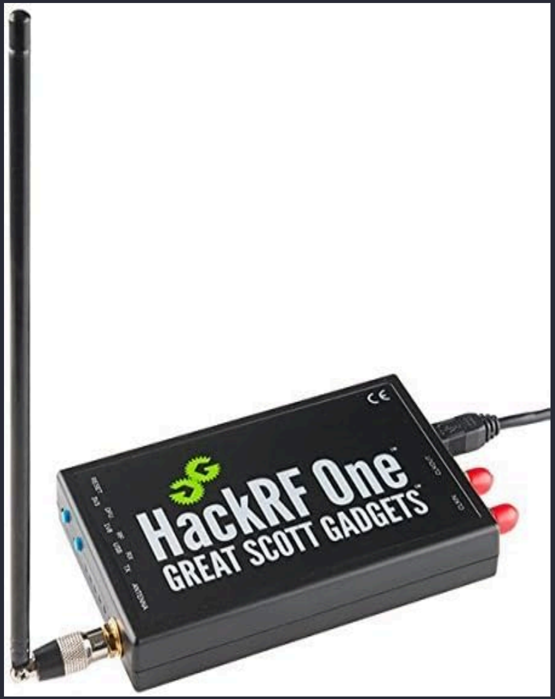
Audience prerequisites

- You probably need some prior knowledge of
  - RF and SDR
    - GNU Radio
  - Packet formats and Protobuf
    - Wireshark

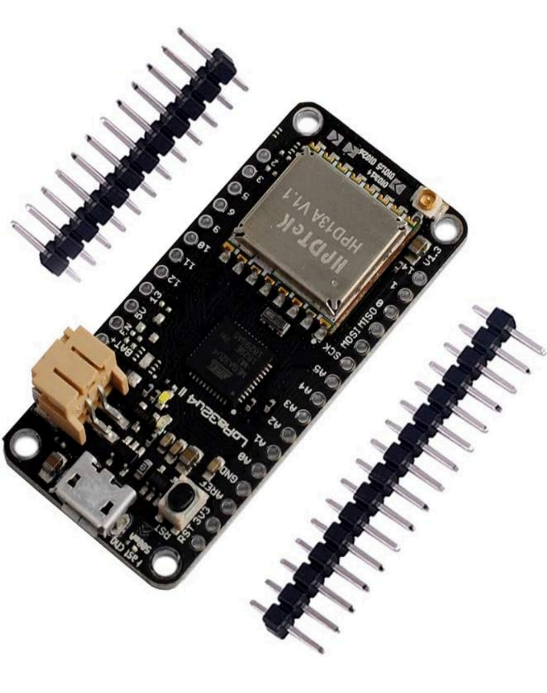
Hardware

SenseCAP T1000-E

HackRF SDR



Arduino with LoRa

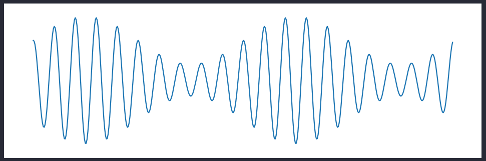


What is LoRa?

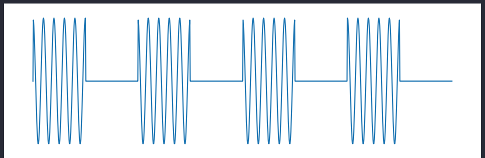
- A radio modulation and encoding
- Closed source chips by Semtech
- Primary use: LoRaWAN
- Also, the physical layer Meshtastic uses

Recap of common modulations

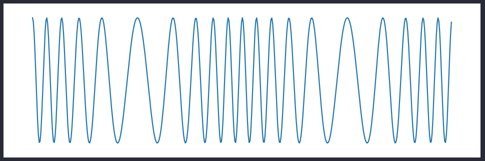
- **AM** - Amplitude Modulation



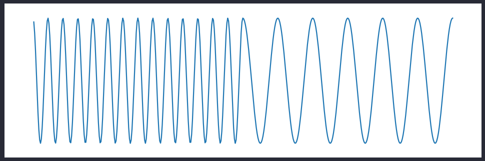
- **ASK** - Amplitude-shift keying



- **FM** - Frequency Modulation

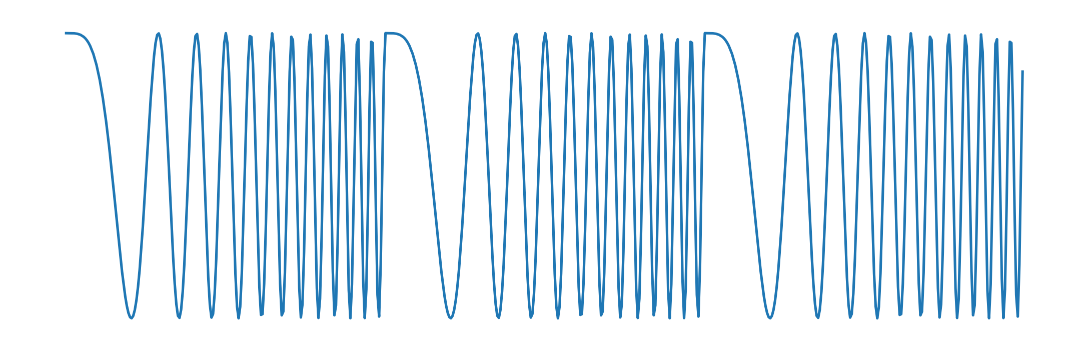


- **FSK** - Frequency-Shift Keying



LoRa's (Meshtastic's) modulation

- **CSS** - Chirp Spread Spectrum
- Aka. **FSCM** - Frequency shift chirp modulation
- More resilient to noise even at very low power
- LoRa can work below the noise floor



Let's capture a chirp!

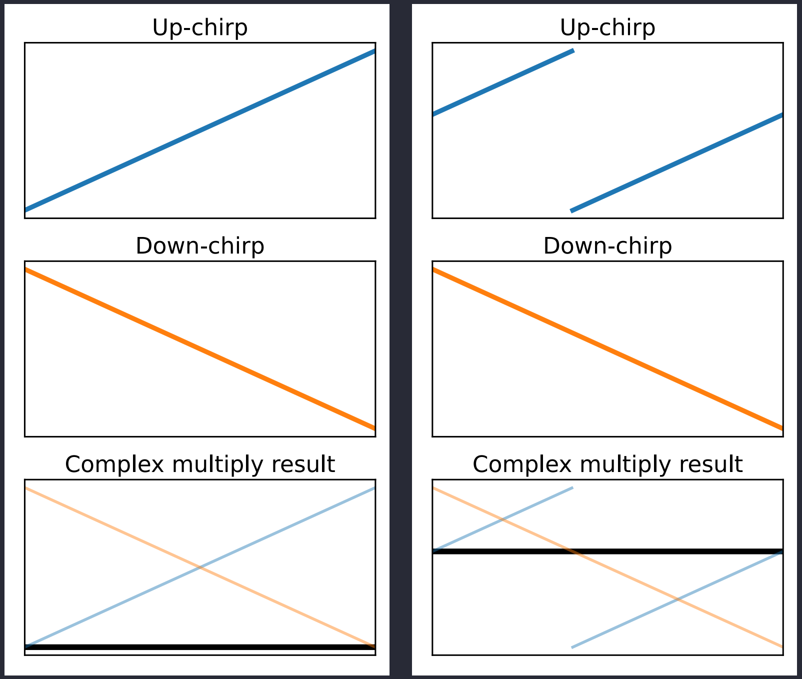
- We will first use:
  - **A HackRF** as my SDR device
  - **Gqrx** to find and capture
  - **Inspectrum** to zoom really close

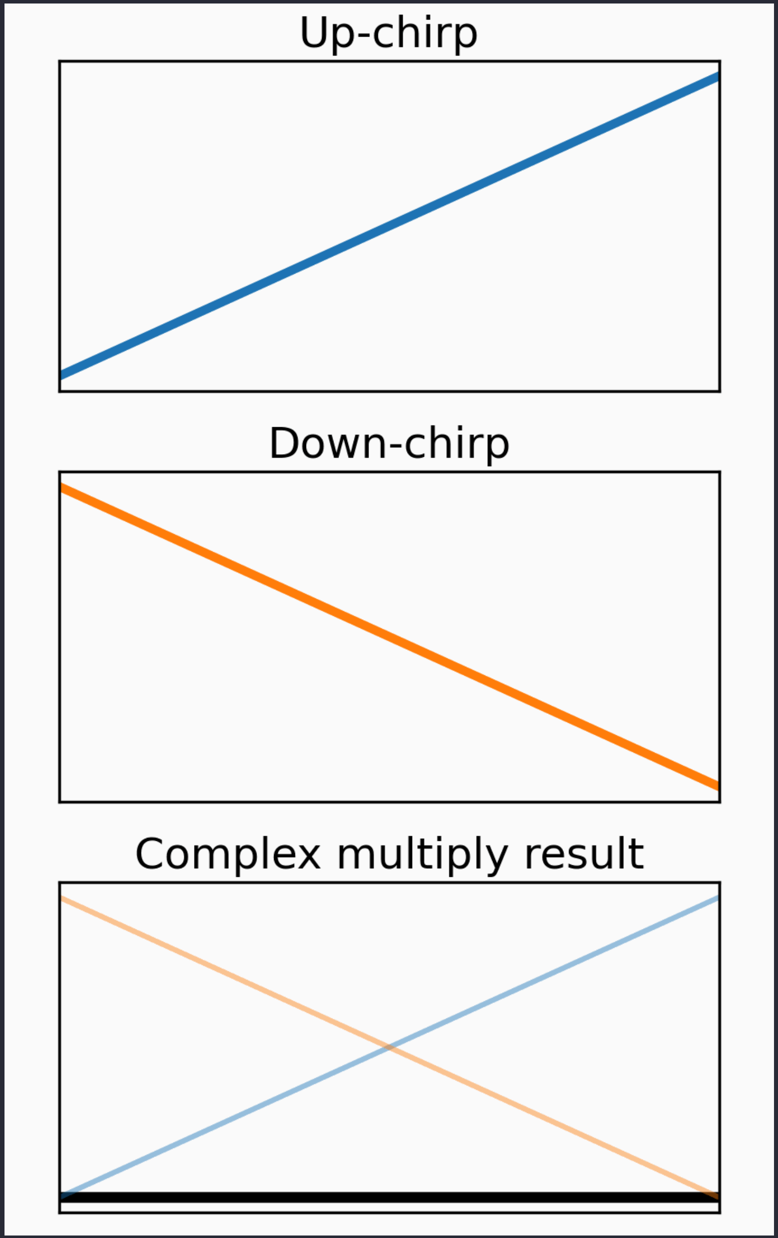
LoRa packet anatomy

- Lora packet
  - **Preamble**: 8-16 up chirps
  - **Sync Word**: Meshtastic uses `0×2B`
  - **Down chirps**: 2.25
  - **Payload**: Meshtastic packet
- Let's look in Inspectrum!

A useful property of chirps

- Dechirp: Complex multiply by downchirp to get a constant freq signal
  - Now it looks like frequency shift keying
    - Run N-point discrete fourier transform




Up-chirp
Down-chirp
Complex multiply result

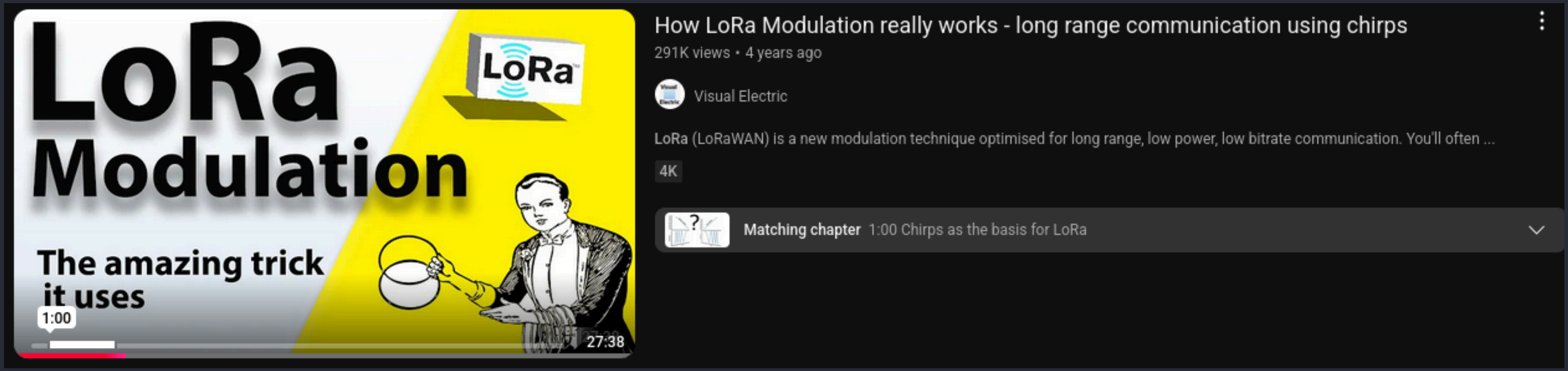
Preamble syncing

- Symbol 0 repeats e.g. 16 times
- Dechirp offset anywhere still gives const freq signal
- Calc sync offset based on symbol we randomly aligned at

Learn more about LoRa demodulation

YouTube video by Visual Electric

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



How LoRa Modulation really works - long range communication using chirps

291K views • 4 years ago

Visual Electric

LoRa (LoRaWAN) is a new modulation technique optimised for long range, low power, low bitrate communication. You'll often ...

4K

Matching chapter 1:00 Chirps as the basis for LoRa

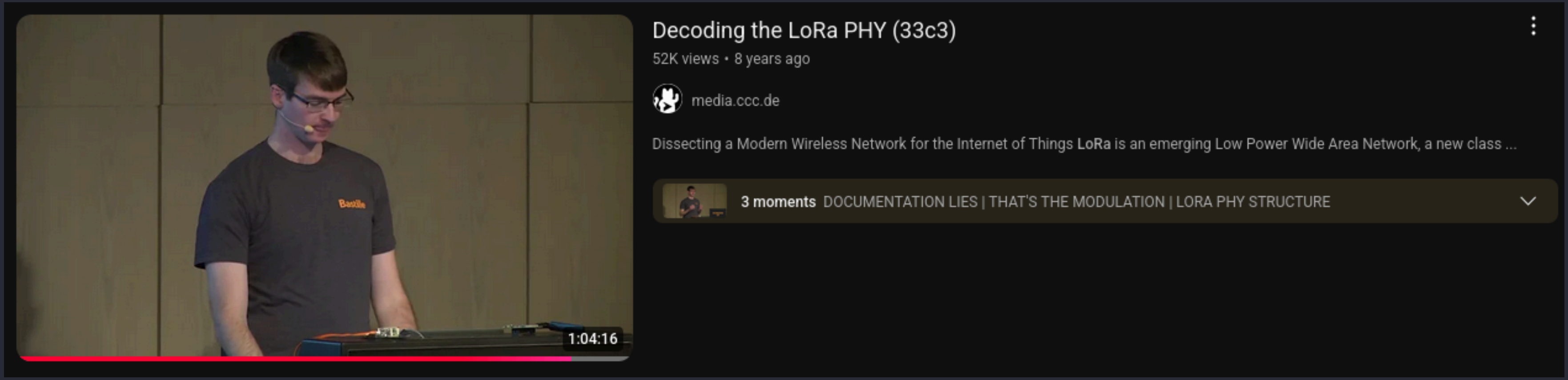
LoRa encoding

- Before modulation, data bits are encoded:
  - CRC: **Error detection**
  - Whitening: Scrambling for **long-run avoidance**
  - Hamming coding: Forward **error correction**
  - Interleaving: **Spread bits** over multiple symbols
  - Gray coding: **Reduce impact of errors**
- Let's look in GNU Radio!

Learn more about LoRa encoding/decoding

Talk on YouTube video by Matt Knight

https://www.youtube.com/watch?v=NoquBA7IMNc



Decoding the LoRa PHY (33c3)

52K views • 8 years ago

media.ccc.de

Dissecting a Modern Wireless Network for the Internet of Things **LoRa** is an emerging Low Power Wide Area Network, a new class ...

3 moments DOCUMENTATION LIES | THAT'S THE MODULATION | LORA PHY STRUCTURE

Meshtastic LoRa modem settings

Param	**Example**
Preset name	MediumSlow
Frequency	914.875 kHz (calc)
Bandwidth	250 kHz
Spread factor	7-12 bits per sym
Hamming coding rate	4/5 - 4/8
Preamble len	8-16
Sync word	`0×2B`

Presets are in src/mesh/RadioInterface.cpp

Meshtastic packet anatomy

- Meshtastic packet (payload of LoRa packet)
  - 16-byte header (docs)
    - Destination (4 bytes)
    - Sender (4 bytes)
    - Channel hash (1 byte):
      - `xor_hash(name) xor xor_hash(key)`
    - ...
  - Payload: AES256-CTR encrypted
    - `Data` protobuf source
    - Encrypted with channel key
- Let's look in Wireshark

Payload Data protobuf

```
message Data {
  PortNum portnum          = 1;
  bytes payload            = 2;
   …
}

message User {
  string id = 1;
  string long_name = 2;
  string short_name = 3;
  HardwareModel hw_model = 5;
  bytes public_key = 8;
   …
}
```

Github links: Data, User

Encryption

- AES-256-CBC
- Default key in firmware/src/mesh/Channels.h
  - Not actually literally "AQ=="
- DMs use public key cryptography
- No perfect-forward-secrecy
  - Nice discussion in the docs

Transmission

- Using an Arduino with a LoRa radio
  - Simple relay program
- Using a Python script to drive the Arduino
- No Multi-Hop Messaging
- And no CSMA/CA though ... woops ...

Questions?