QMesh: A long-range, low-cost wireless mesh network for digital voice communications

Dan Fay, KG5VBY

TAPR DCC 2020

Who am I?

- Licensed radio amateur since September 2017, callsign KG5VBY
  - Special event communication
  - Packet radio/digital communications
- Presented at TAPR DCC 2018 the paper "Beyond Line-of-Sight UHF Digital Communications with the LoRa Spread Spectrum Waveform"

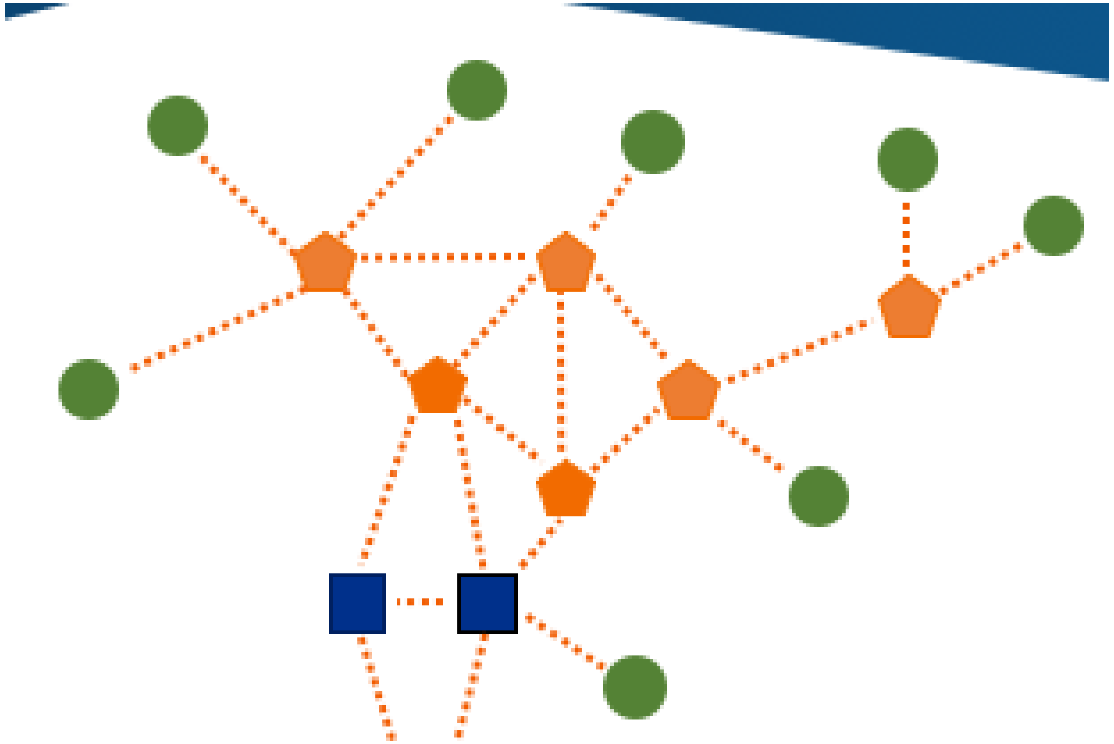
La Luz Trail Run 2018

What is QMesh?

- It’s another MANET/wireless mesh network protocol
- What makes it unique
  - Isochronous -- can handle streaming data like voice
  - Self-healing/self organizing
- Relatively low datarate (at most 10’s of Kb/s)
  - Enough to support vocoded voice (700bps-1600bps)
  - Can also carry small amounts of data (location, telemetry, etc.)
- Uses the LoRa Chirp Spread Spectrum (CSS) waveform
  - Provides better Eb/N0 than “standard” modulations (FSK, PSK, etc.)
  - Unique properties of the LoRa waveform (spread spectrum, low symbol rate) enable QMesh to work

MANETS/Wireless Mesh Networking

- MANET = Mobile Ad-Hoc NETwork
  - Self-assembling
  - Self-healing
- Mesh networking
  - Nodes relay packets until they reach their destination
  - Two major types: routed and flooded

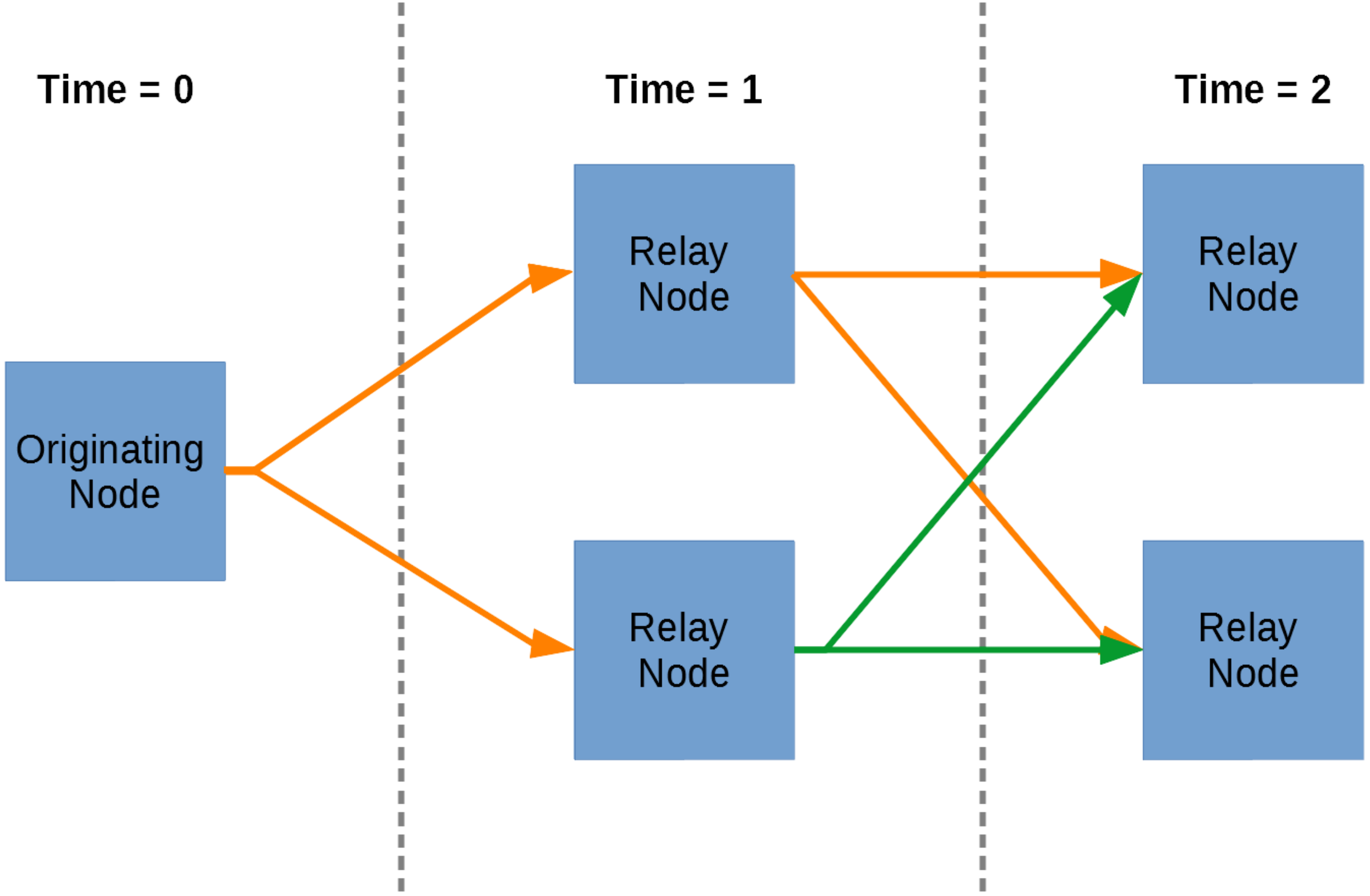


Source: https://blog.particle.io/2018/04/28/how-to-build-a-wireless-mesh-network/

Flooding vs. Routing

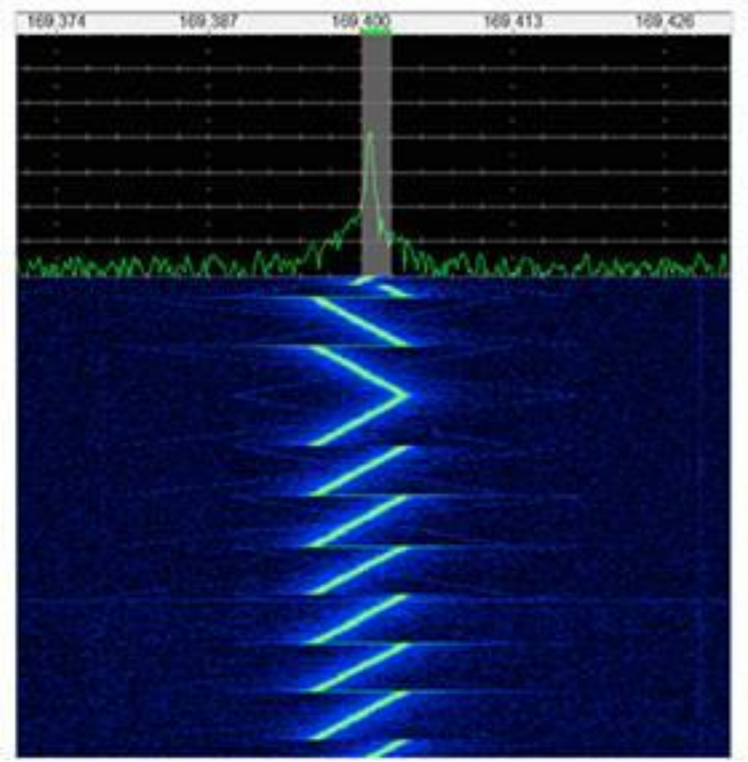
- Routing
  - Nodes repeat packets if they're along a *route* to the packet's destination
  - Doesn't retransmit if it doesn't move the packet closer to its destination
  - Relatively complicated due to need to (re)discover and (re)build routes
- Flooding
  - A node repeats every packet it receives
  - Provides redundancy
  - Self-healing, nodes can freely join and leave without any other communications needed
  - Can be inefficient vs. routing
  - Good for multicast (e.g. PTT voice, tracking telemetry of team members)
  - Susceptible to the *Broadcast storm problem*
- **Synchronized Flooding (what QMesh uses)**
  - Nodes repeat packets at the same time
  - Good for streaming (isochronous) voice
  - Colliding packets could be a problem

Synchronized Flooding Example



LoRa

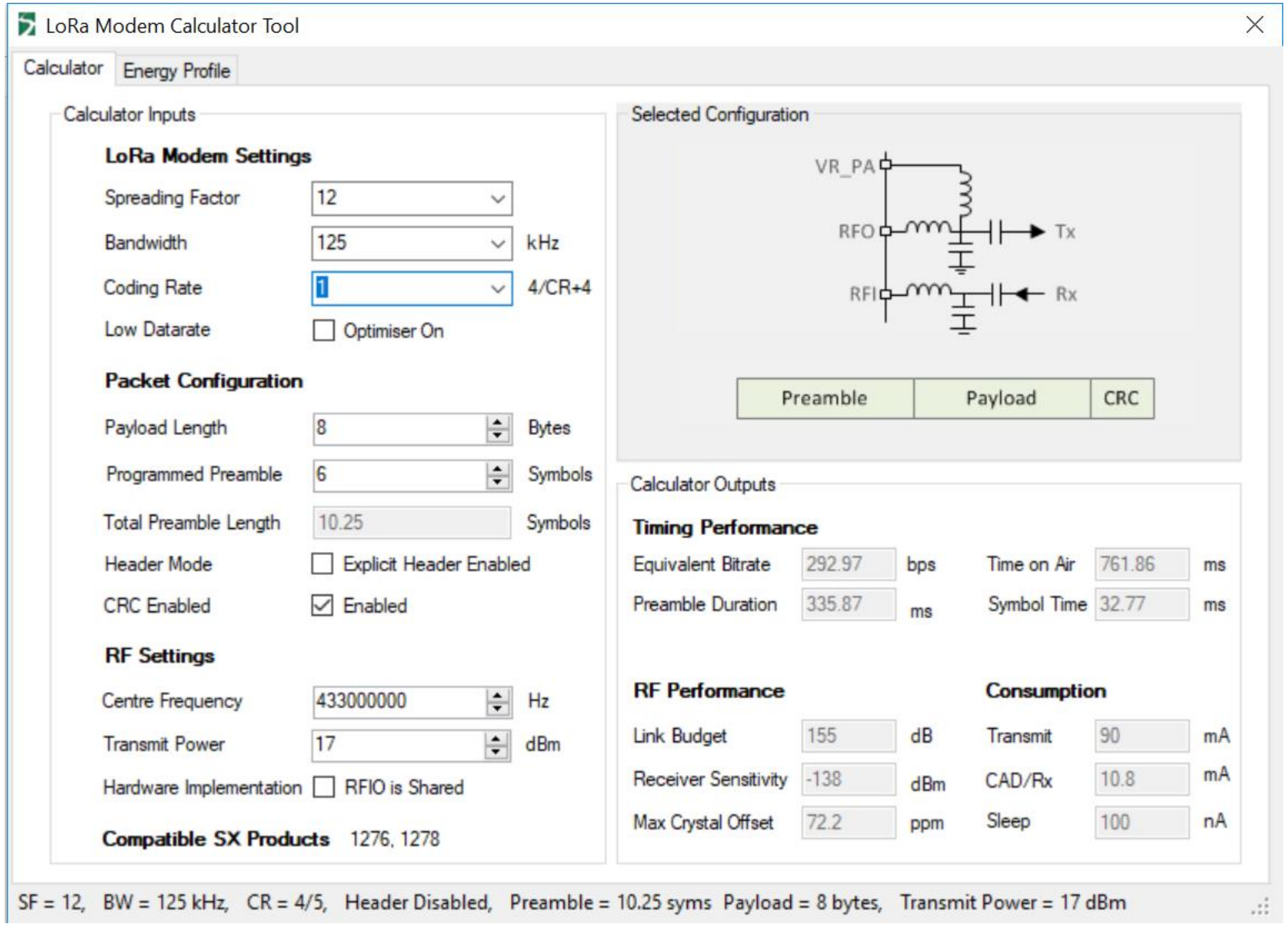
- LoRa is Semtech’s proprietary implementation of Chirp Spread Spectrum (CSS)
  - Targets battery-powered, Internet-of-Things (IoT) devices
  - Used to implement LPWAN protocol LoRaWAN
- Benefit: CSS gives large processing gain vs. FSK/OOK
  - LoRa@1172bps: -132dBm Rx sensitivity on 70cm
  - FSK@1200bps: -123dBm Rx sensitivity on 70cm
  - LoRa supports bitrates up to 37500bps (62500bps on newer chipsets)
- Highest sensitivity rate possible for LoRa is -148dBm
  - Not used much because it requires a TCXO to function
  - Low data rate -- 18bps at this sensitivity level
- LoRa is becoming increasingly popular, so products are easy to find
  - HopeRF is a popular module maker; some integrated w/MCU emerging
  - 33cm and 70cm modules easy to find
  - LoRa chipsets support 137MHz through 1GHz, as well as the 2.4GHz band
- **LoRa provides large sensitivity improvement (9dB or more) vs. FSK**



Source: https://www.digikey.com/en/articles/techzone/2016/nov/lorawan-part-1-15-km-wireless-10-year-battery-life-iot

LoRa Parameters

- **Spreading Factor (SF)**
  - 2^{SF} = number of chips/symbol
  - Higher SF gives higher Rx sensitivity in exchange for lower data rates
  - Different SF's are somewhat orthogonal, as well as different IQ polarities
- **Bandwidth** – how "wide" the chirp is
  - Wider bandwidth gives higher data rates at expense of Rx sensitivity
  - 500KHz, 250KHz, and 125KHz are typically used
- **Coding Rate** specifies the FEC (Hamming code)



The (FM) Capture Effect

- Many types of receivers receive exclusively the strongest signal when that signal is stronger (by 3dB or more) than other signals
  - Necessary for e.g. Wi-Fi, Bluetooth, etc. for coexistence with other transmitters in the area
  - Constant-envelope modulation schemes (FM, FSK, some PSK, etc.) are most well-known for the capture effect
  - AM and SSB receivers do not experience capture
- Effect observed when two people try to transmit into same FM repeater
  - Almost always, one person is heard
  - Other person(s) comes off as some sort of distortion/noise
- LoRa is a constant-envelope modulation that *does* experience the capture effect

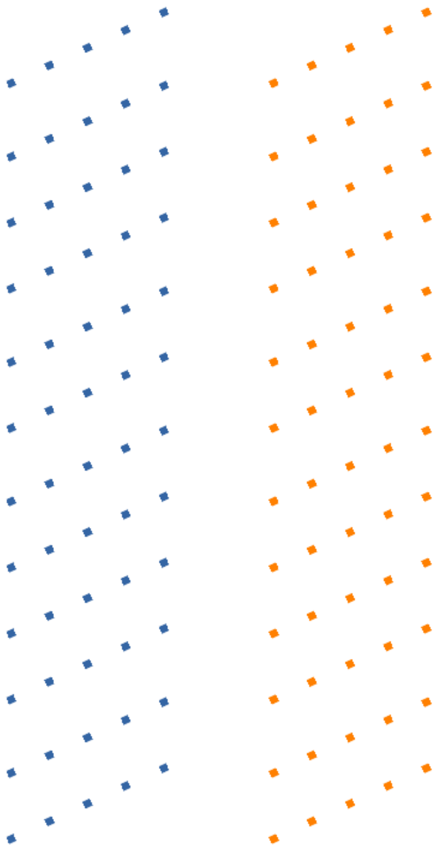
Using the Capture Effect

- Capture effect means that we can successfully receive collisions if the colliding packets are far enough apart in received power
- Can leverage capture effect to make synchronized flooded protocols work without everyone interfering with each other
- Tricky to do with FSK, need some sort of phase dithering with good forward error correction (need SDR or custom radio)
- Easier to do with spread spectrum
  - Glossy Project (academic) used DSSS in 802.15.4
  - Later work has looked at doing the same with LoRa

Increasing Capture Success with LoRa

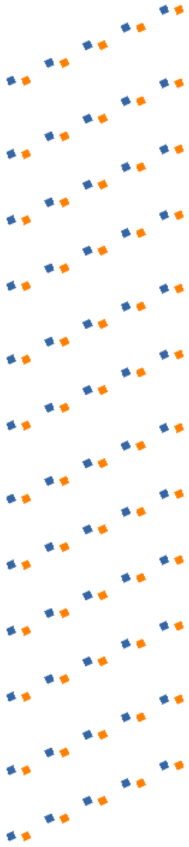
- Basically, “spread out” the overlapping LoRa signals so they interfere less with each other
- LoRa has some features we can use to increase the likelihood of successful capture
  - Frequency separation between chips
  - Low chirp (symbol) rate
  - Tolerance of frequency error (up to +/- 25% of the LoRa bandwidth)
- Randomly “wobble” the frequency
  - Can put chips “between” each other
  - Shift chirps around so that they don’t overlap in time/frequency
- Can also shift things around by adding a timing offset
  - Need to encode timing offset within the packet so that the next node can compensate
  - Can’t shift timing more than half a symbol -- receiver locks onto weaker packet first, then gets drowned out by stronger packet coming in later

Chip-Level LoRa Overlap Reduction



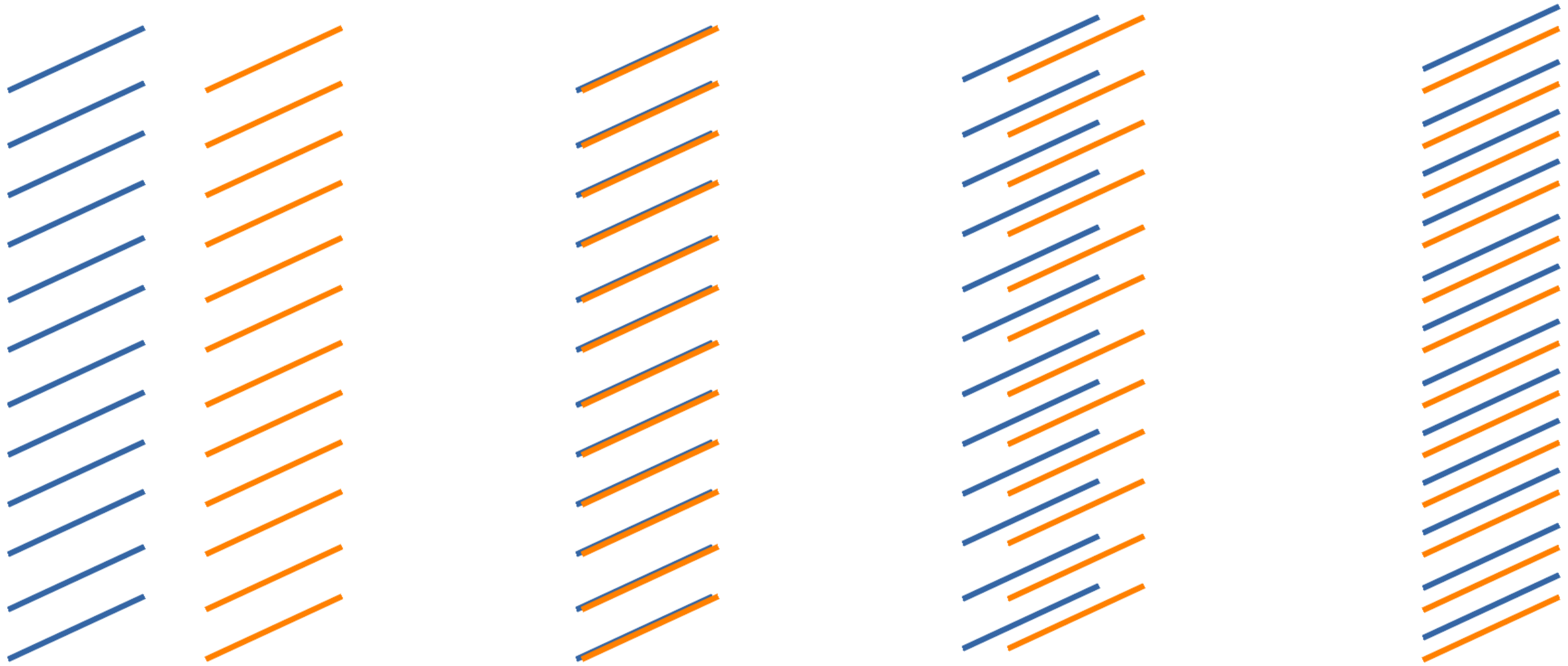
Two LoRa signals on completely Different channels

Two LoRa signals on the same frequency



Two LoRa signals with a very small frequency offset

Symbol-Level LoRa Overlap Reduction



Two LoRa signals on completely Different channels

Two LoRa signals on the same frequency

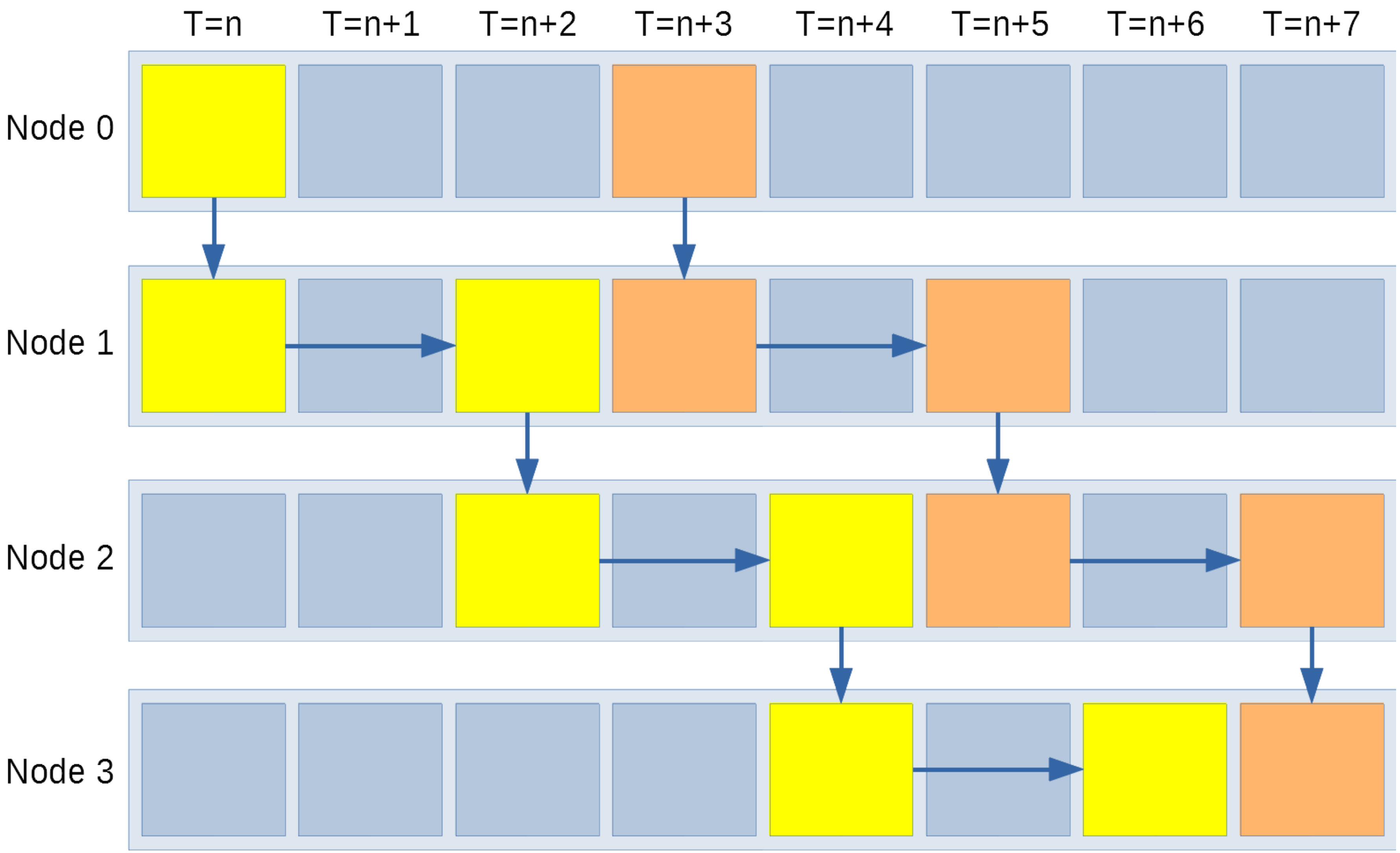
Two LoRa signals with a small frequency offset

Two LoRa signals with a timing offset

The QMesh Protocol Overview

- Is based on TDMA (Time Division Multiple Access), with same-size time slots.
- A transmitter operates at a 33% duty cycle
  - Transmits a packet every third time slot (waits two timeslots before transmitting again)
- A receiving node
  - Decodes the packet and retransmits if appropriate
  - If retransmitting, waits one timeslot before retransmitting
- Time gap between receipt and retransmission
  - Allows time to decode packets, including complicated forward error correction
  - Gives a “second chance” to receive a packet by a node one hop downstream

QMesh Protocol In Action

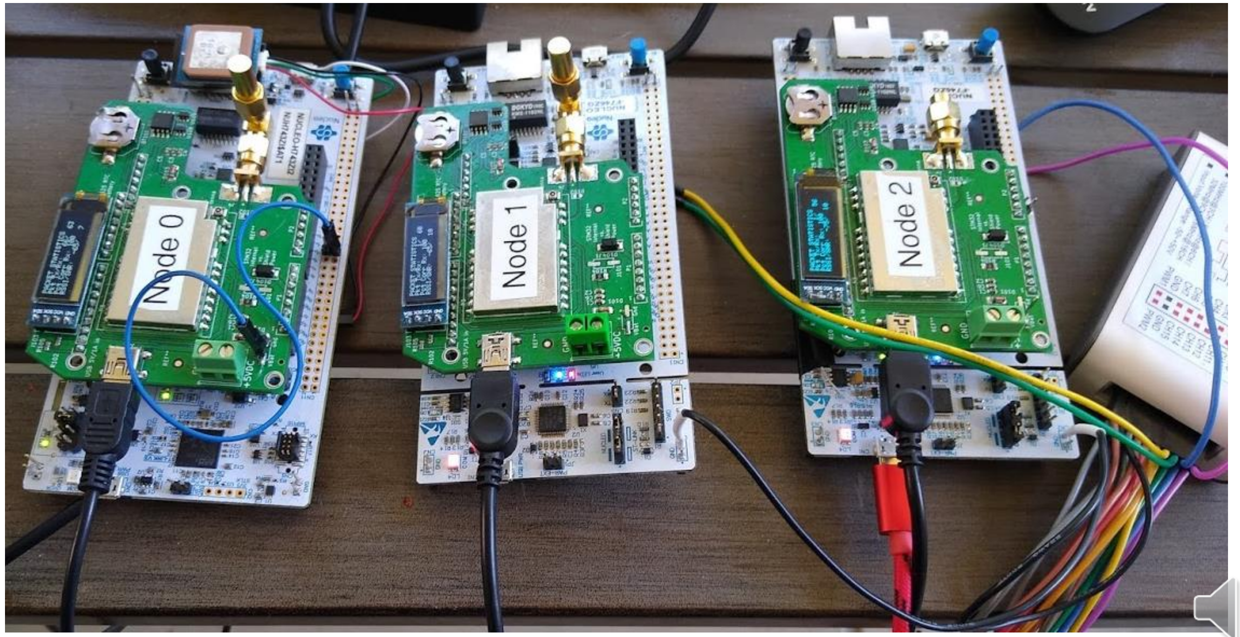


Forward Error Correction (FEC)

- LoRa has a very simple, Hamming Code-based FEC built into it
- Can likely gain at least a few dB of performance with a decent FEC
  - Theoretical gain may be 2-10dB of coding gain in an AWGN channel (Additive White Gaussian Noise – free space line-of-sight)
  - Possibly even better in multipath-heavy situations
  - **Substantial benefits in a collision-heavy environment**
- Currently using Reed-Solomon-Viterbi (RSV) coding
  - Using `libcorrect`, which is a simplified port of Phil Karn KA9Q's `libfec`
  - ½ rate (encoded with twice as many bits as the original data)
  - Constraint length = 7 used
  - 8 additional bytes for Reed-Solomon outer code
- Hard decoding – may be possible to extract soft decoding information from radio in the future

QMesh Test Node

- LoRa Shield + STM32 NUCLEO-144 Board
- USB on the shield (black cable) supplies power to both boards
- Red USB cable connects to computer, provides debug and serial port
- OLED display provides live information without needing a connected PC



QMesh LoRa Shield Overview

- Built a custom shield for the “Zio” connector on the STM32 NUCLEO-144 board
  - 1W LoRa module
  - 128Mbit QSPI NOR flash for configuration and logging
  - OLED display
  - Capable of powering itself and STM32 board via USB
- Uses EByte 400M30S module
  - Supports 410MHz-493MHz (entire 70cm amateur band)
  - Based on SX1268 LoRa radio
  - 30 dBm (1W) PA
  - External LNA (roughly 2dB improvement in Rx sensitivity)
  - TCXO
- EByte also makes a pin-compatible version that supports the 915MHz/33cm band
- EByte module’s output tested as clean by Sean Turner KI5CBG
  - ~29-30dBm power output measured
  - Spurious harmonics at least 60dB below fundamental

QMesh LoRa Shield Design

- Designed in KiCAD
  - Free, Open Source (FOSS) PCB design tool
  - Reasonably competitive with commercial tools (Eagle, Altium Designer)
- Two-layer board
  - Chinese board houses will produce two-layer boards that are <10cm on a side for cheap ($5-$10 for a run of 5-10)
  - Some will also populate some SMT parts for cheap
  - Power/ground planes and trace routing can be tricky vs. 4+ layer boards
  - Coplanar waveguide best way to do transmission lines on the board
- Lots of power decoupling capacitors
- Ample ESD protection on data lines, power, and RF

Node Configuration

- 24 bytes packet size, header+payload
- 51 bytes total coded data
- BW=250KHz, SF=9, CR=0*
- Originator node at minimum Tx power (0dBm into PA) transmitting through a dummy load
- Other nodes transmitting at maximum power
  - 20dBm into PA, ~1W output
  - 2m/70cm HT whip antennas
- Testing collisions
  - Worst case scenario for interference
  - Antennas are ¼ wavelength apart

CR=0 is an undocumented feature in the SX126X that completely disables the built-in error correction

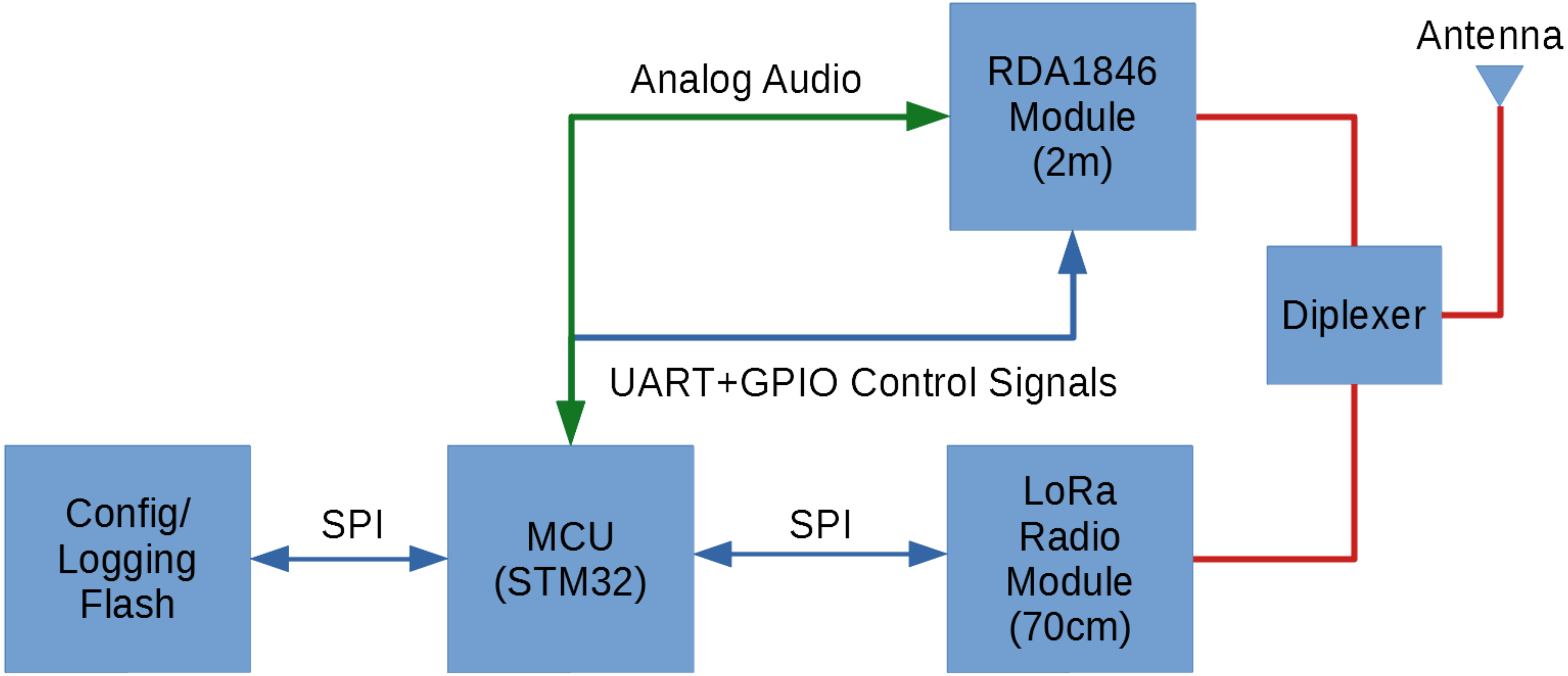
Discussion

- When FEC is used, PRR is 99%+ for one, two and three node setups
- FEC seems to make a big difference here
  - One node has 99%+ PRR w/o FEC
  - Two nodes has ~93% PRR w/o FEC
  - Three nodes has ~90% PRR w/o FEC
- Appears the raise the noise floor
  - Weak signals do not get received

Next Steps – FM Micro-Repeaters

- Develop small FM repeaters that encode/decode voice as `codec2` and use QMesh as a backhaul
  - Compact, can run off solar power
  - Easy to stand up a series of linked repeaters
  - Can also be used to extend coverage of existing repeaters
- Big benefit is accessibility
  - People can use their existing radios, so can benefit from QMesh without having to design special radios
  - Less hardware needed by users to benefit from QMesh

LoRa + Analog FM Architecture



Contact Info

- **QMesh project**
  - **Github:** https://github.com/faydr/QMesh -- source code
  - **Hackaday.io:** https://hackaday.io/project/161491-lora-based-voice-mesh-network – project overview
- **Blog:** https://faydrus.wordpress.com (describes a lot of my radio/maker experiments)
- **E-mail:** Daniel.fay@gmail.com (kg5vby@arrl.net should also work)
- **Twitter:** @faydrus