Weak-Signal Radio Communications for Bitcoin Network Resilience

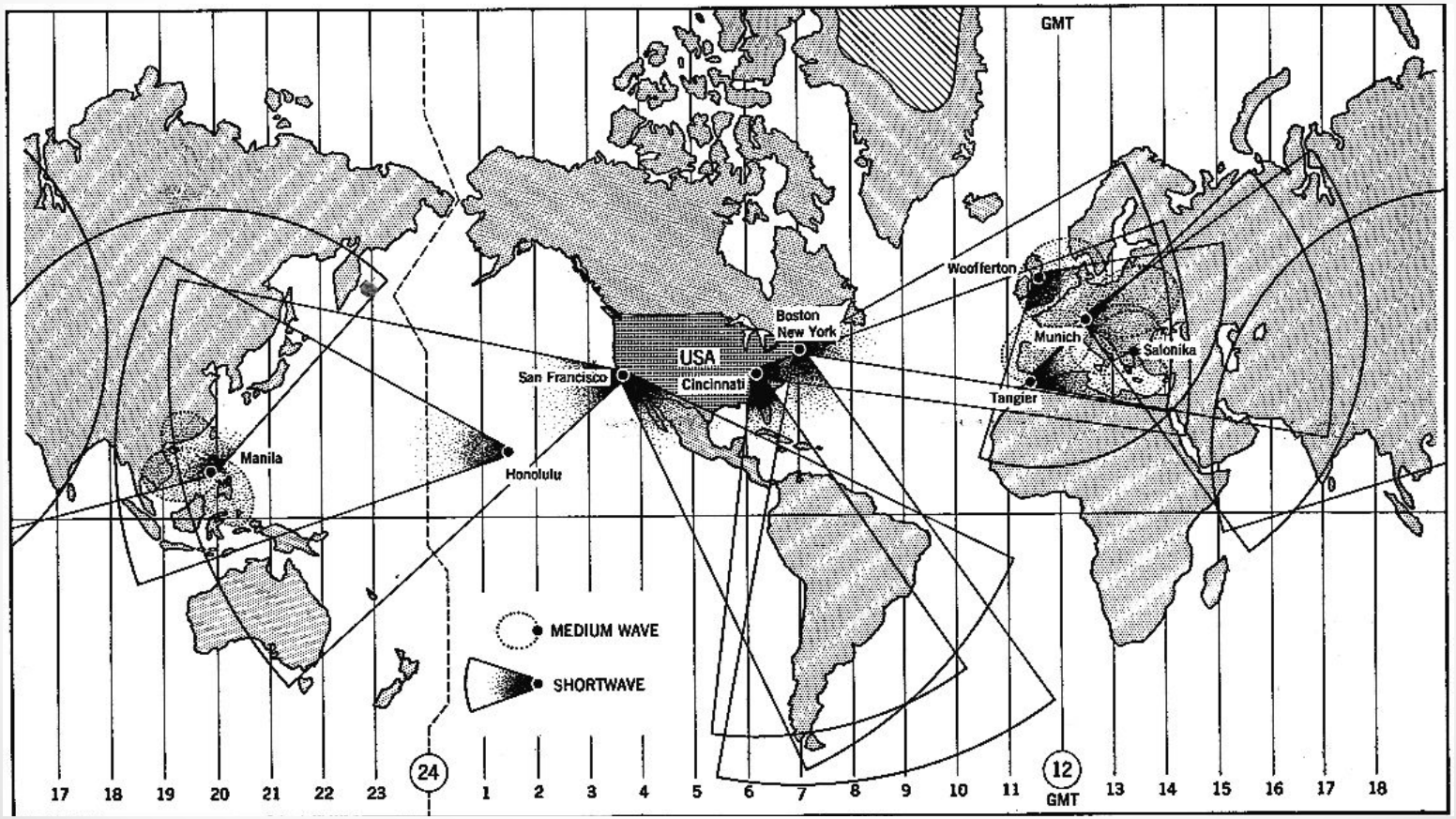
Nick Szabo, Elaine Ou
globalfinancialaccess.com
Scaling Bitcoin 2017

What is Weak-Signal HF Radio?

- Radio transmission using shortwave frequencies (1.6-30 MHz)
- Radio waves in this band can refract off the ionosphere
- Popular for international broadcasting of government propaganda

Cold War Shortwave Radio Broadcasts

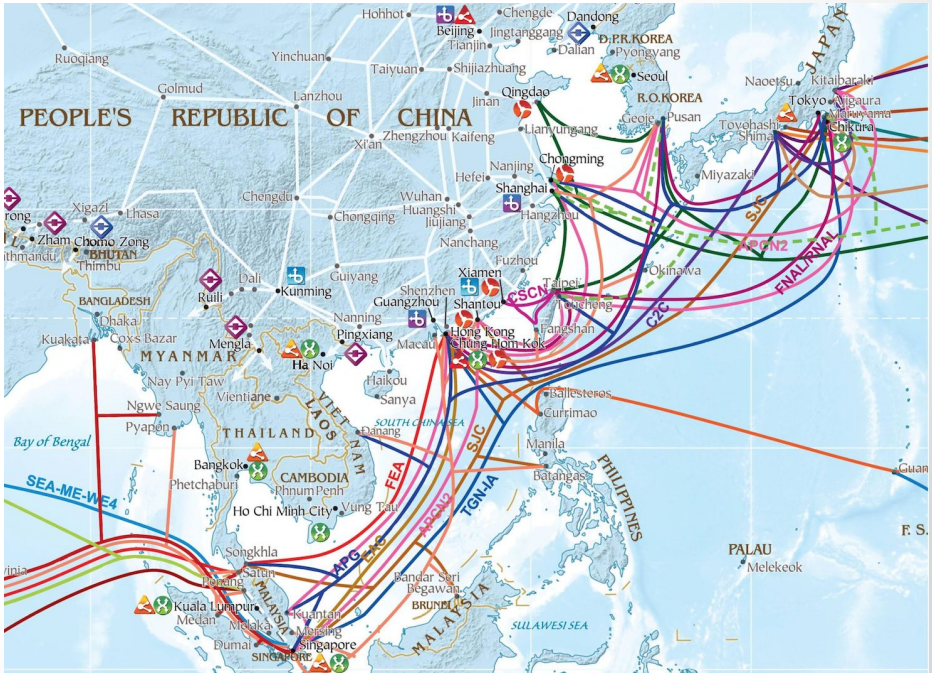
- Office of War Information broadcast anti-communist propaganda during "Campaign of Truth"



Secure Consensus and Broadcast

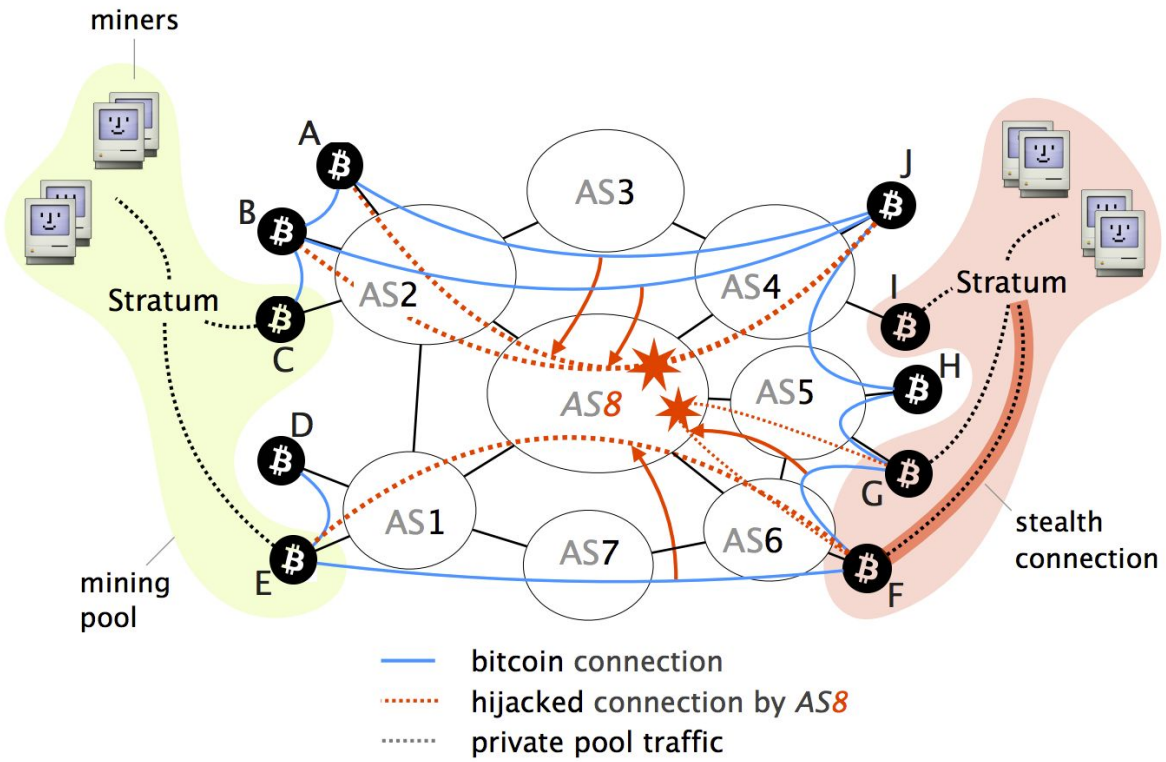
- Most proofs of secure consensus (in general) and of Bitcoin-like formal protocols (in particular) assume trust-minimized fair broadcast
  - Every full node broadcasting directly to every other full node – no intermediaries

- Real-world consensus implementations fall short of provable security



Eclipse and Routing Attacks

- Eclipse attacks (Heilman et al. 2015)
  - Attacker directly connected to the victim



Internet topology & routing attacks (Apostolaki et al. 2017)

- "For 67.9% of nodes, there is at least one AS *other than their provider* that intercepts more than 50% of their connections."
- "Delay attackers intercepting 50% of a node's connection[s] can waste 63% of its mining power."
- "Even a small amount of multi-homing is enough to protect Bitcoin [as a whole] from powerful attackers"

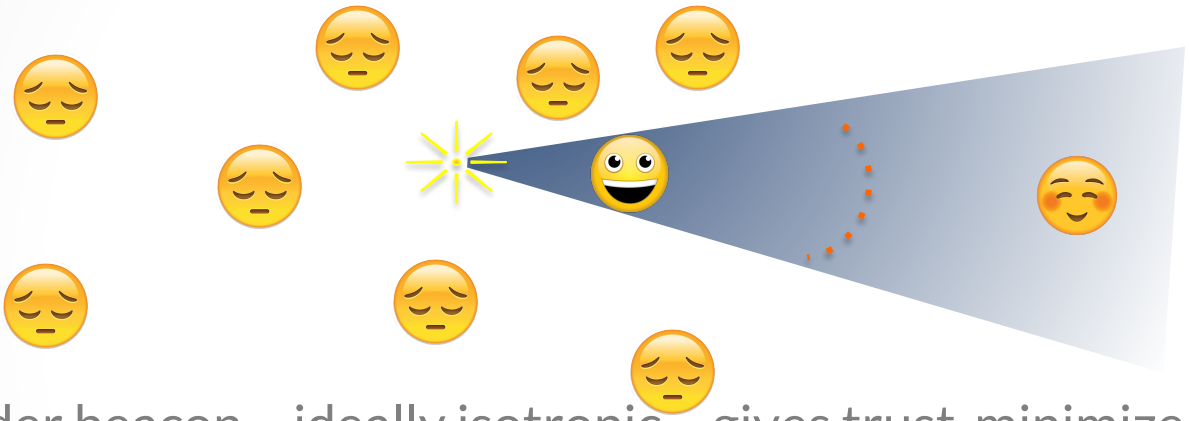
Broadcast and Trust

- Pulsar
  - Inaccessible natural phenomenon => trustless broadcaster
    - Attack structure is nobody
  - Beam covers everybody on earth
    - Access structure is everybody on earth with a big radio dish
- Blockstream Satellite?

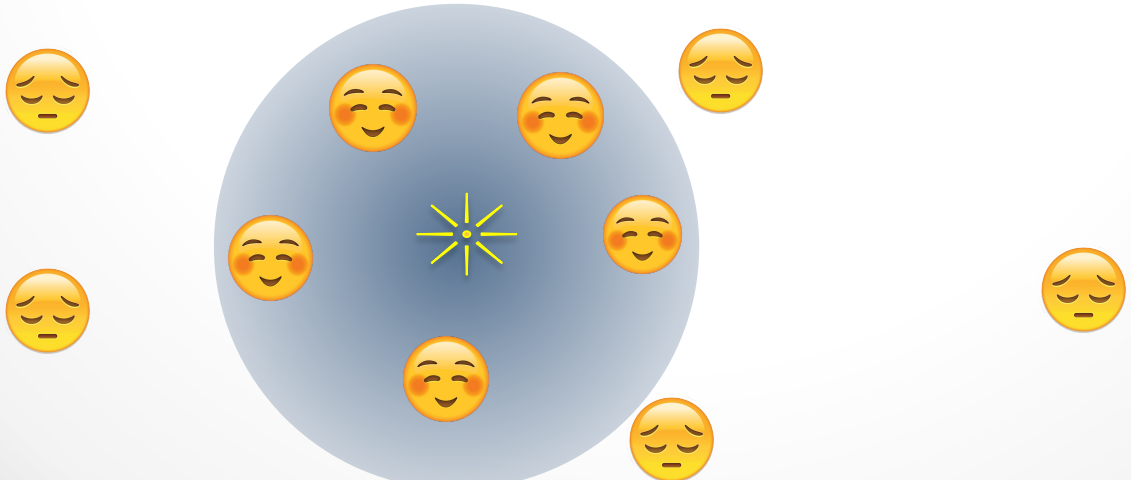
- Clock tower
  - Bell in tower rings at the top of each hour, can hear for miles around
  - Systemically trusted
    - Attack structure is the bell-ringer
  - Isotropic broadcast
    - Access structure is everybody within hearing range of the bell
  - Abstract vs. particular nature of information is important

Beam Width and Gain

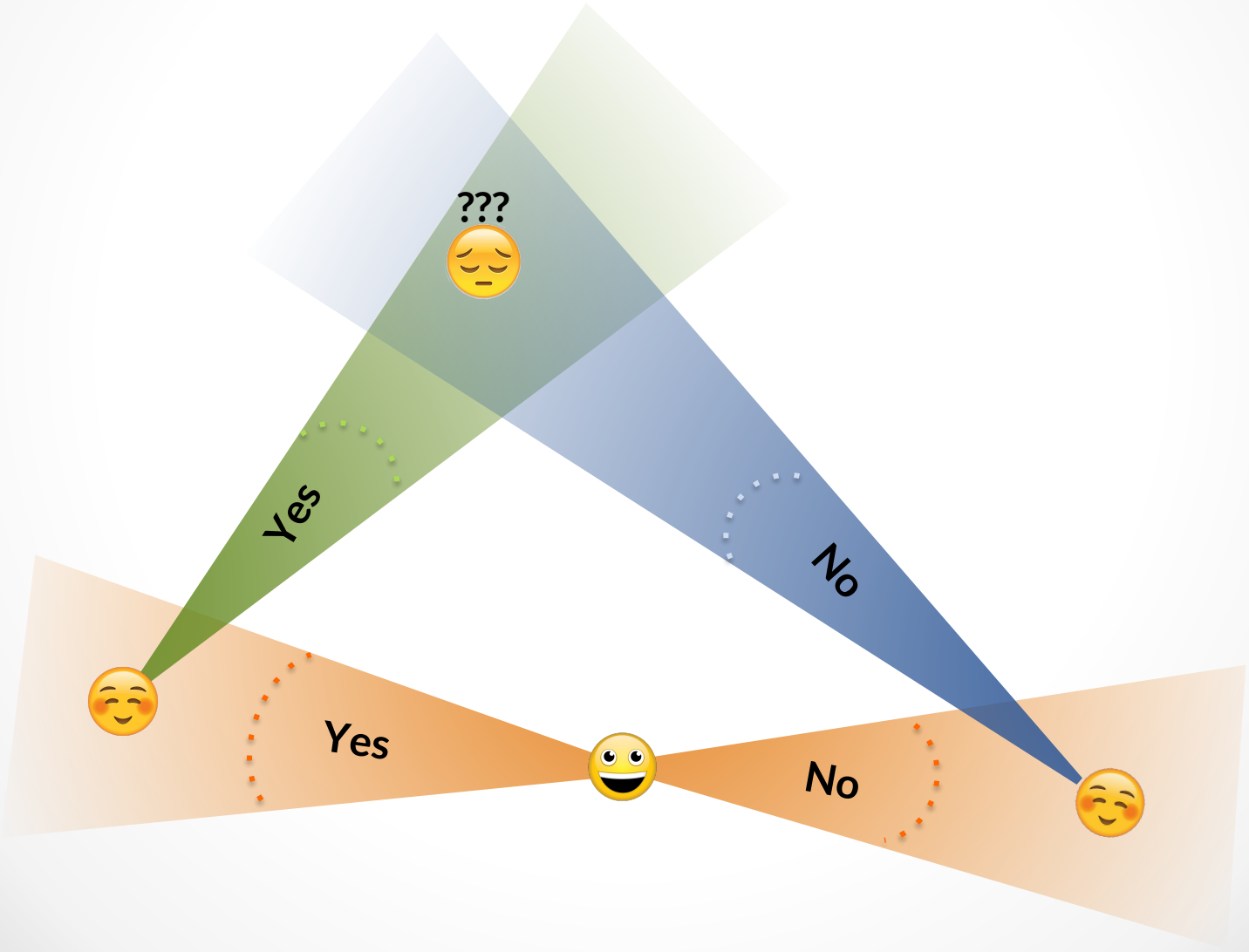
- Narrow beacon provides increases range and bitrate at the expense of trust-minimized fairness and need for prior knowledge
  - Broadcaster can choose direction of beacon but not who is where
  - Allows broadcaster to more choices over the access structure



- A wider beacon – ideally isotropic – gives trust-minimized fairness at the expense of range and bitrate



Byzantine Narrow-Beamer



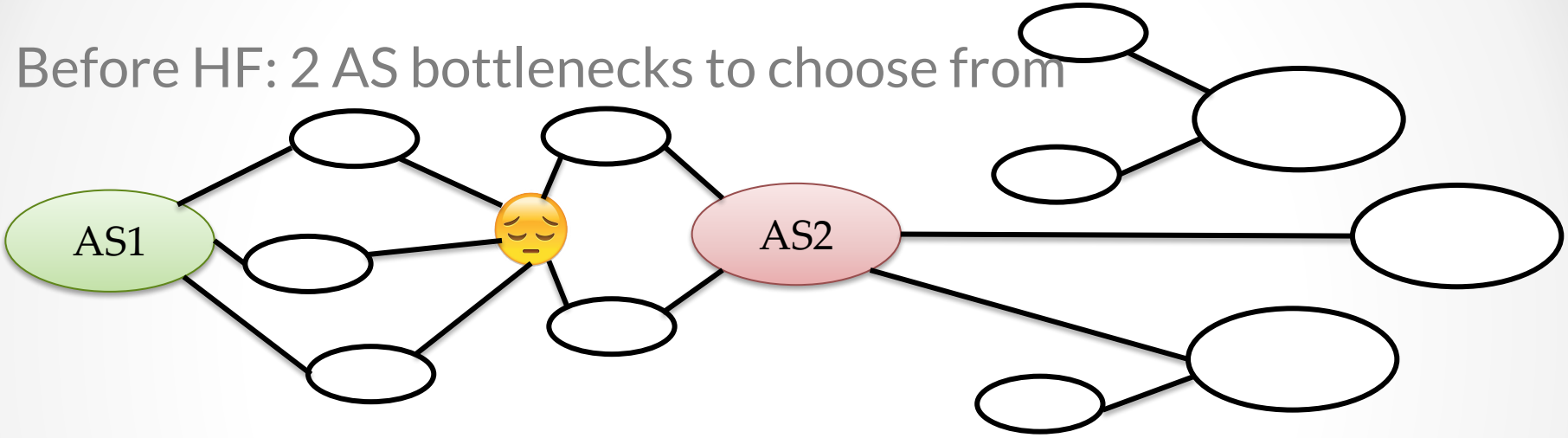
Internet Routing Attacks

Some recommendations from Apostolaki et. al. 2017:

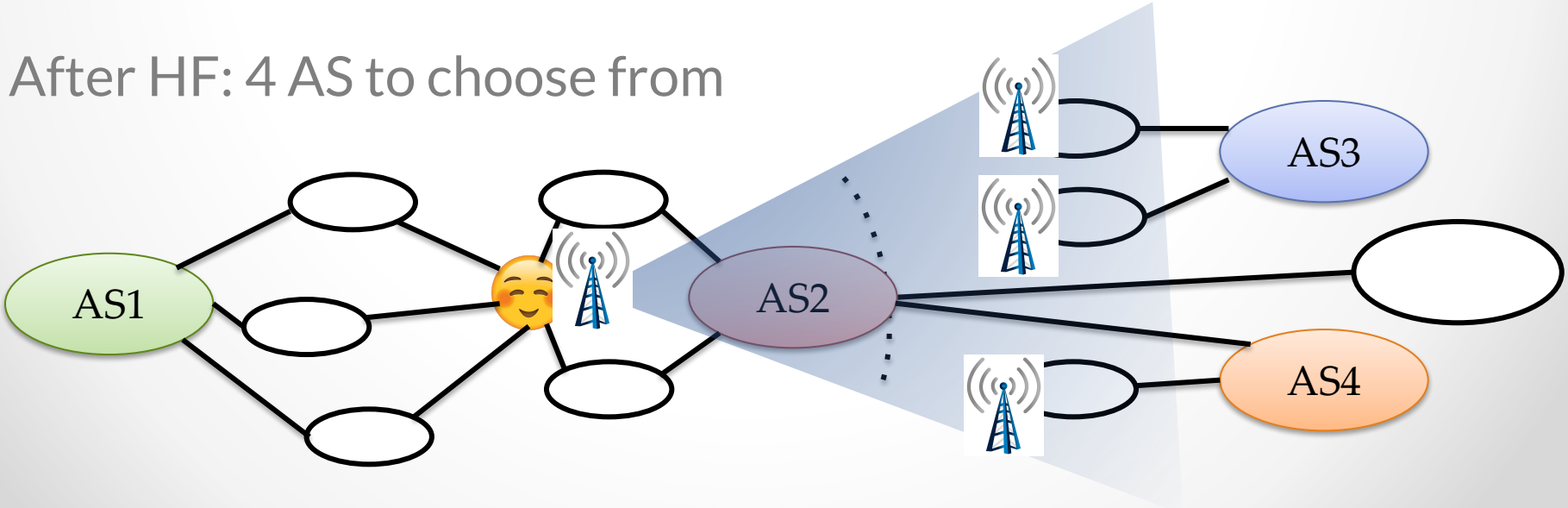
- Increase the diversity of node connections
  - Eg. Ensure that all Bitcoin nodes are multi-homed.
- Select Bitcoin peers in a route-aware way, adding extra random connections if the same AS appears in all paths.

HF Radio vs. Routing Attacks

Before HF: 2 AS bottlenecks to choose from



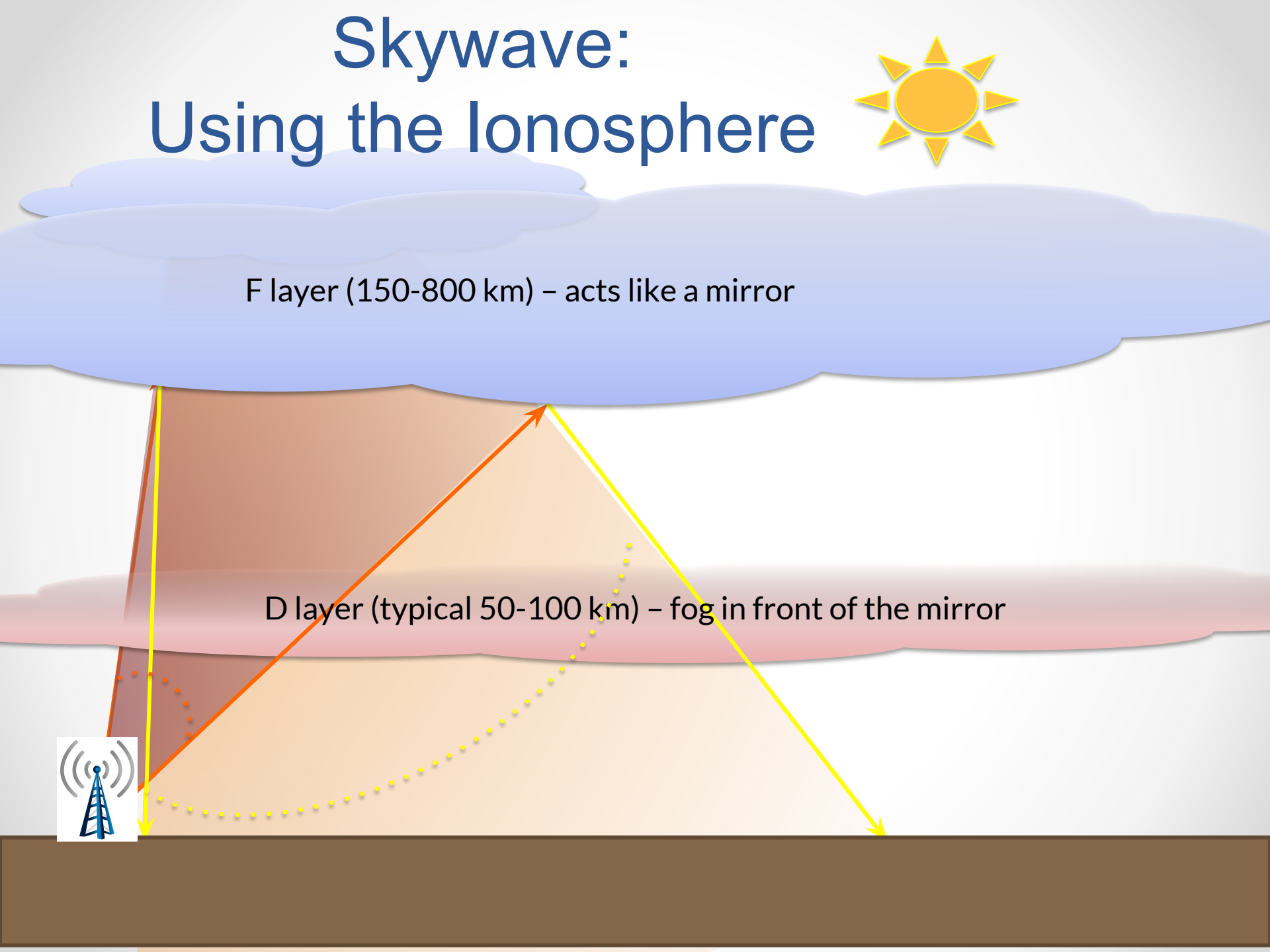
After HF: 4 AS to choose from



Goals of Weak-Signal HF Radio Communication

- Longer range broadcast
  - Avoid injection/modification problems of mesh relay
- Allow censorship-resistant participation in the network
  - Chinese firewalls cannot stop radio
  - Soviet Union needed over 1000 broadcasting stations to jam American radio
- Internet-free participation for SPV nodes
- More diverse multi-homing
  - Ability to choose a more diverse AS set

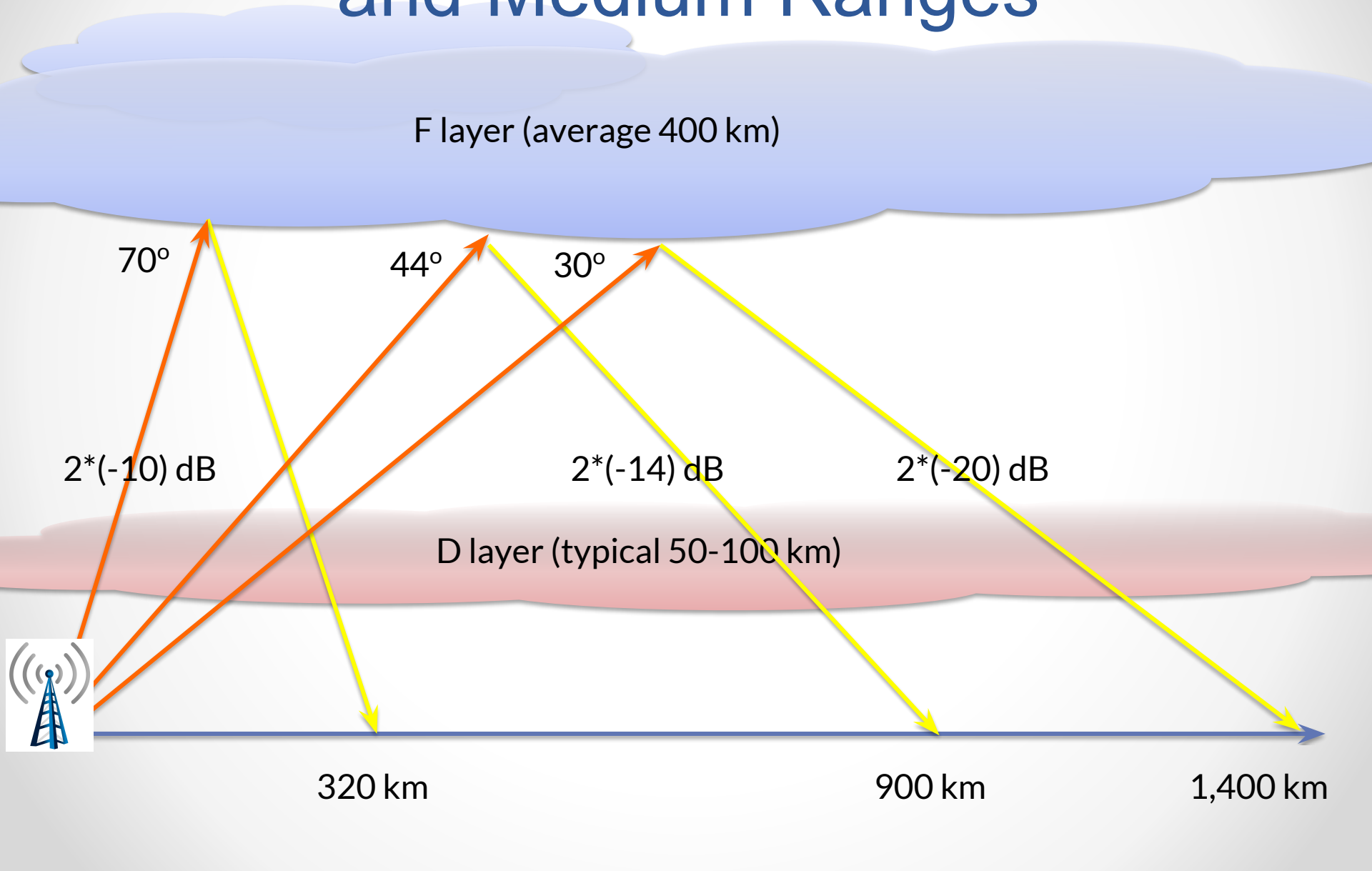
Skywave:
Using the Ionosphere



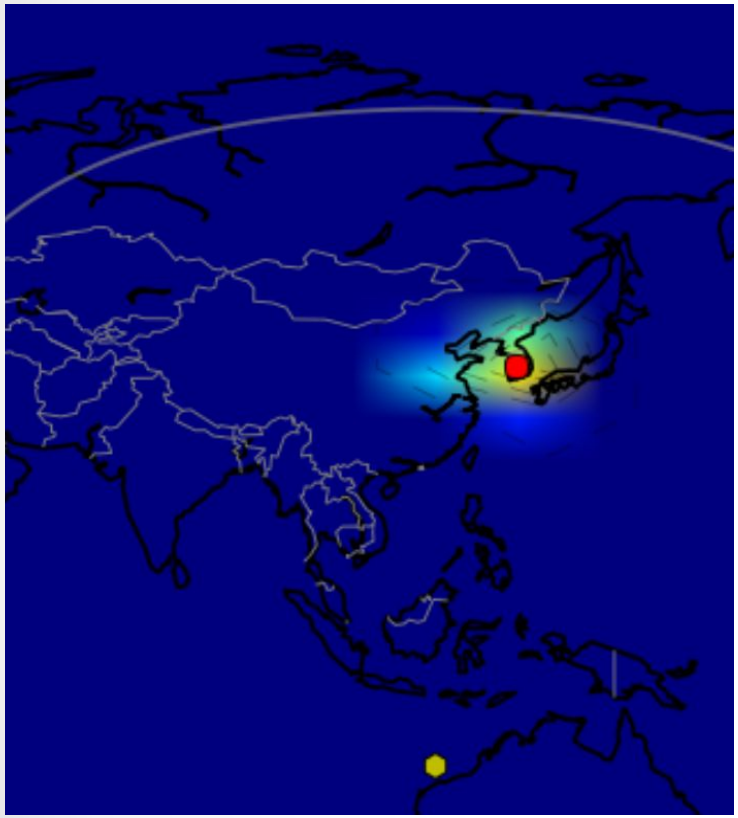
Near-Vertical and Medium-Range Radio

- Near-vertical incidence skywave (NVIS)
  - 50-650 km (30-400 miles)
  - Most reliable frequencies are between wavelengths of 40 and 80 meters
  - Antenna near-horizontal
    - 1/20th to ¼ wavelength off the ground
- Medium-range
  - 500-2500 km (300-1500 miles)
  - Less reliable than NVIS

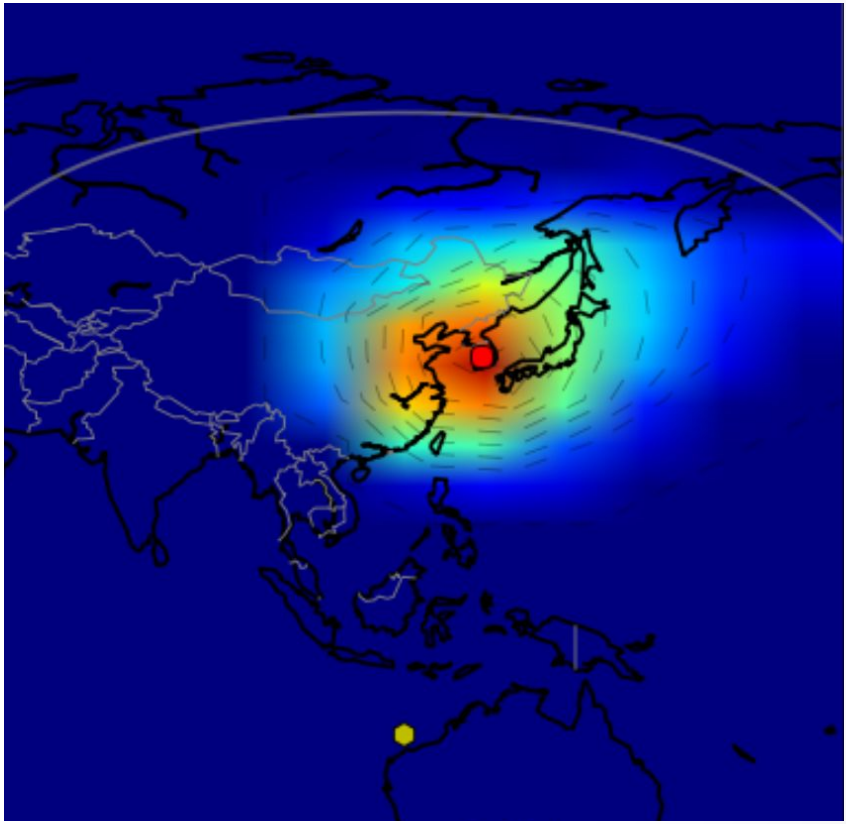
Daytime D-layer Attenuation at NVIS and Medium Ranges



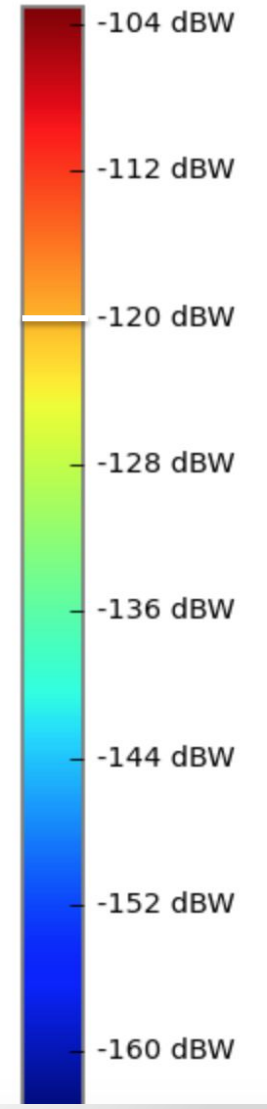
VOA Propagation Map
South Korea



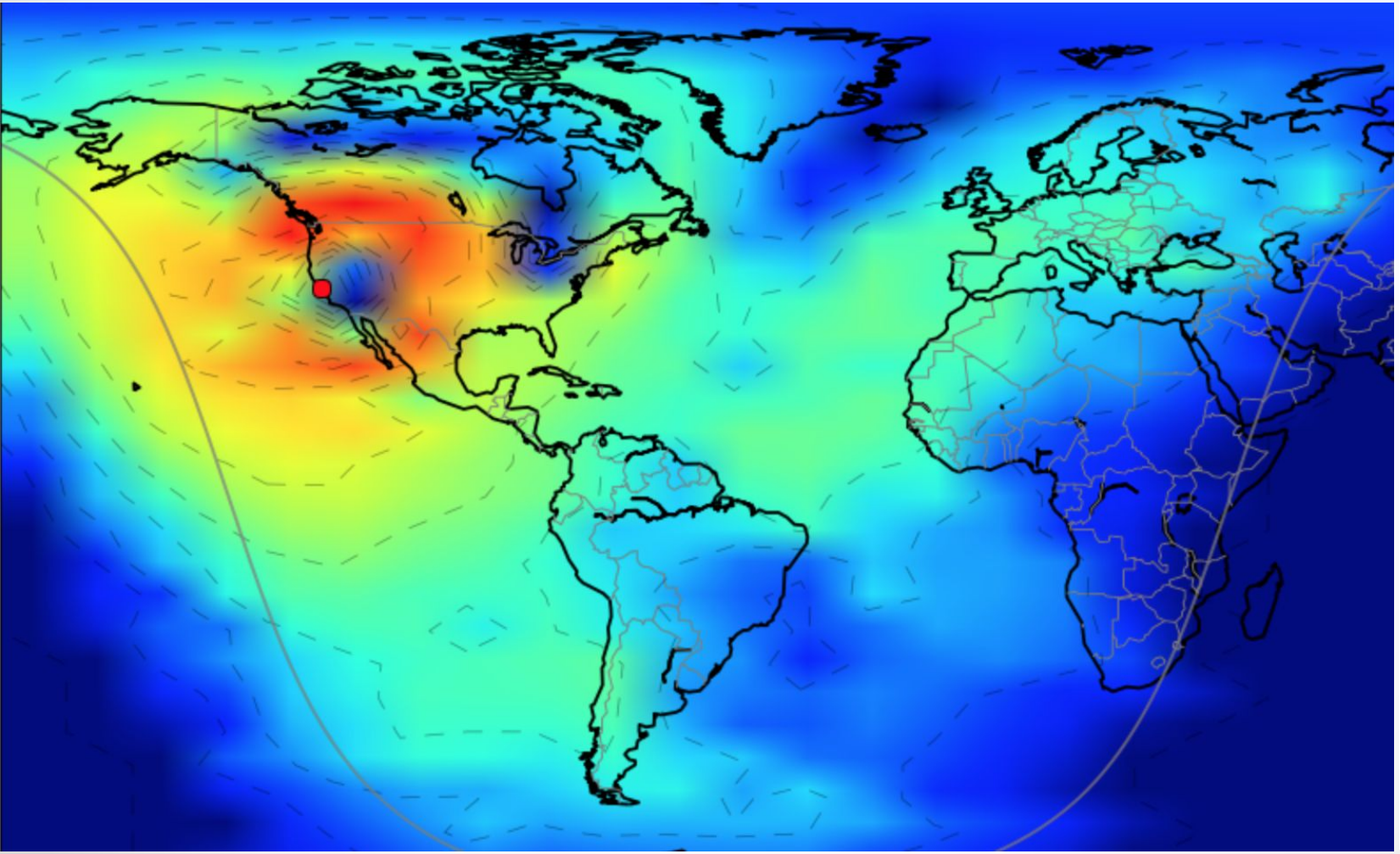
80M, 3.7 MHz,
4W

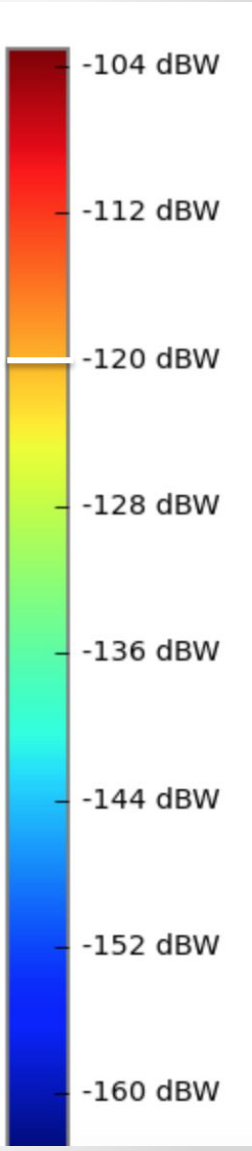


40M, 7.1 MHz,
4W



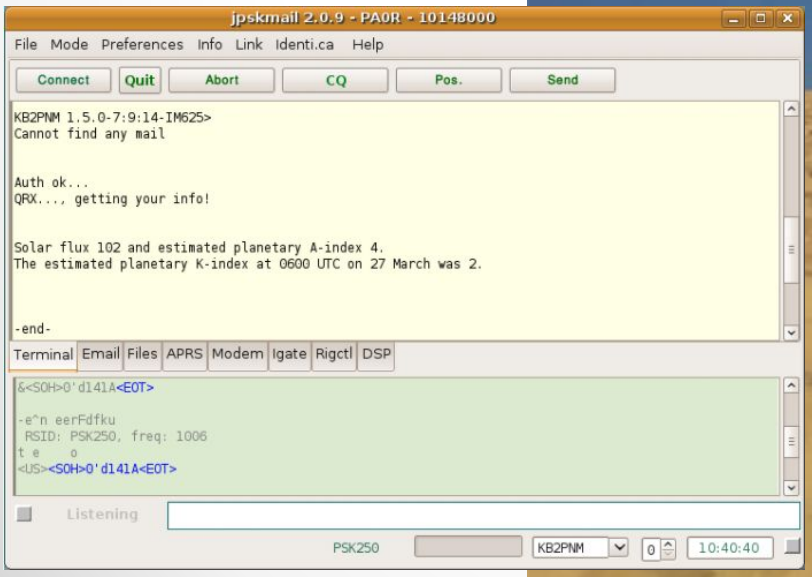
VOA Propagation Map
40M, 7MHz 5W TX





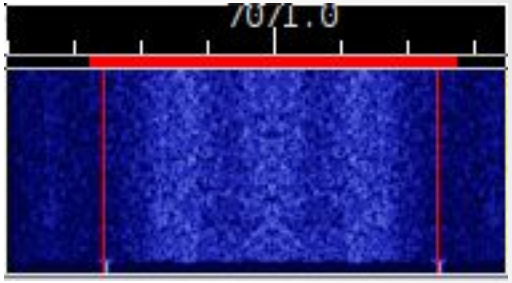
Digital Mode Over Radio

- Any radio can be a modem
  - Modulator/Demodulator
- Airchat radio mesh network by Anonymous
- PSKmail

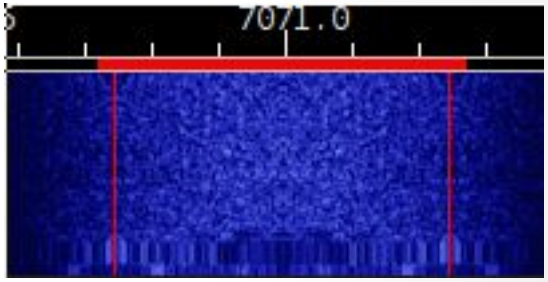


Modulation

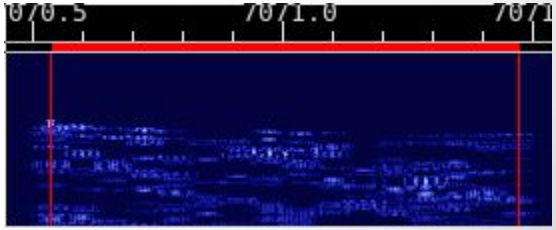
- Ideal conditions: BPSK500
  - 500 bps, 1000 Hz bandwidth



- Noisy conditions: BPSK500R
  - Convolutional encoding
    - Rate R=1/2, Constraint length K=7
  - Interleaved data
  - 250 bps, 1000Hz bandwidth

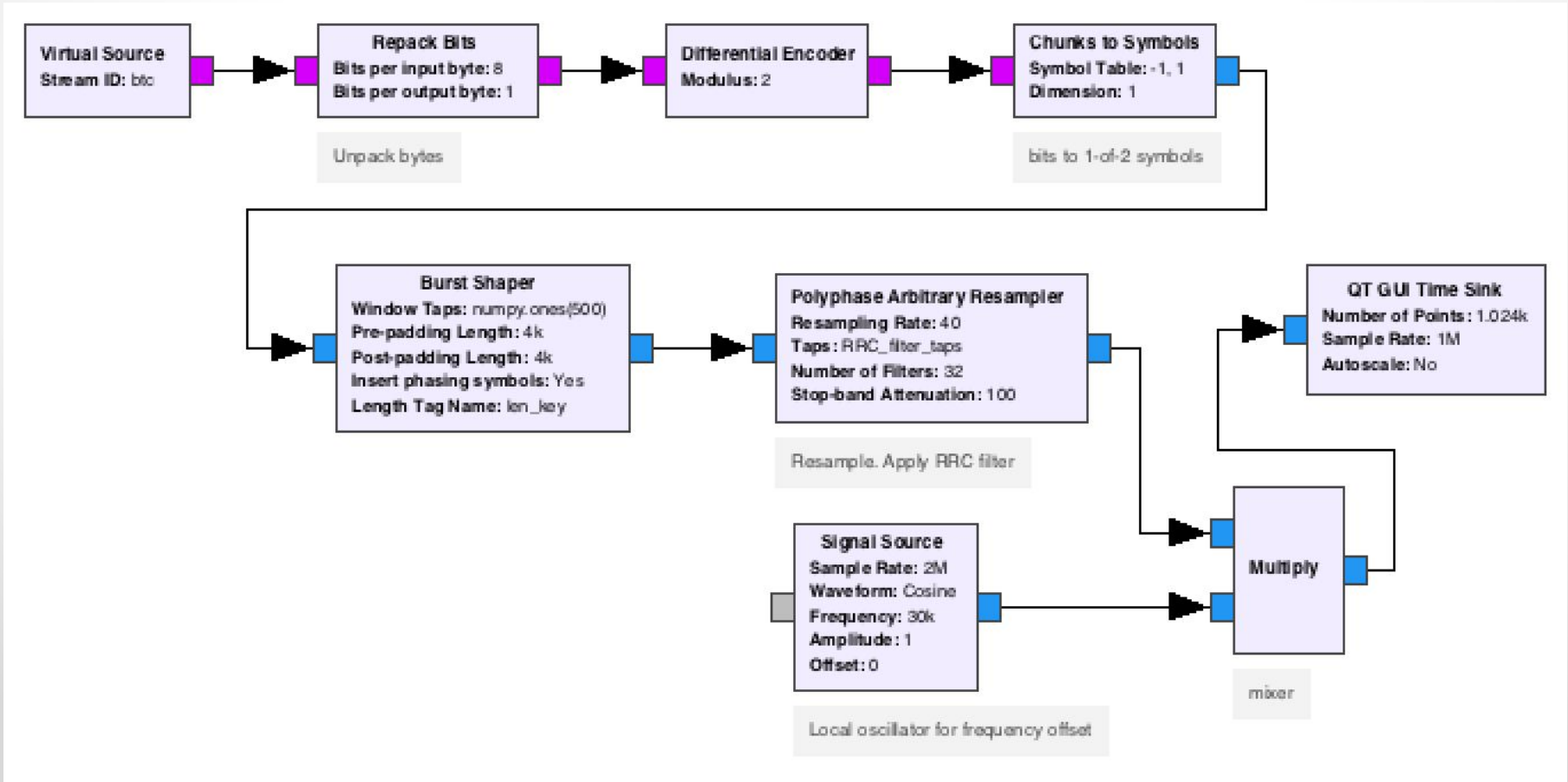


- Awful conditions: MFSK
  - 62.5 bps, 1260 Hz bandwidth

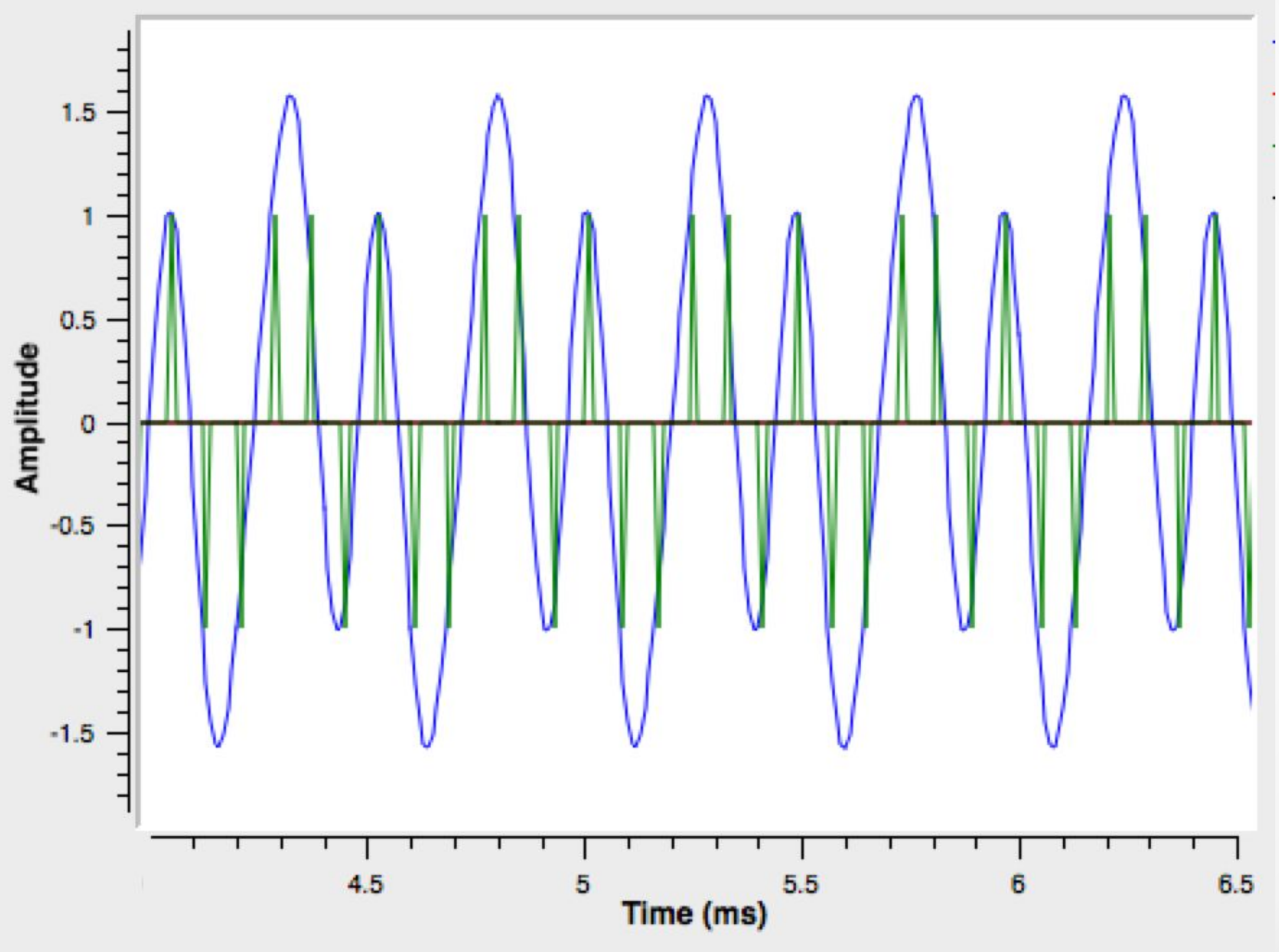


Implementation (TX)

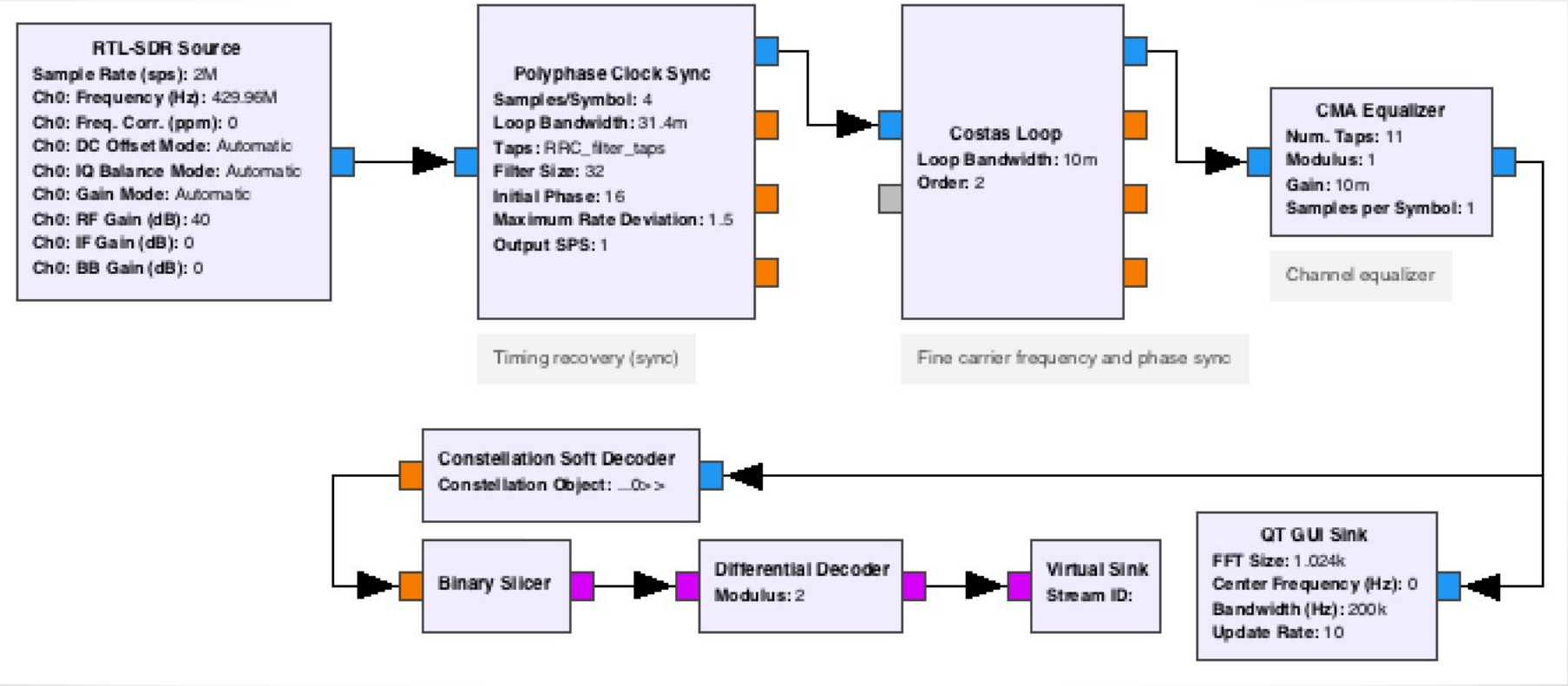
- Binary PSK
  - Low bandwidth, decent bit-error rate

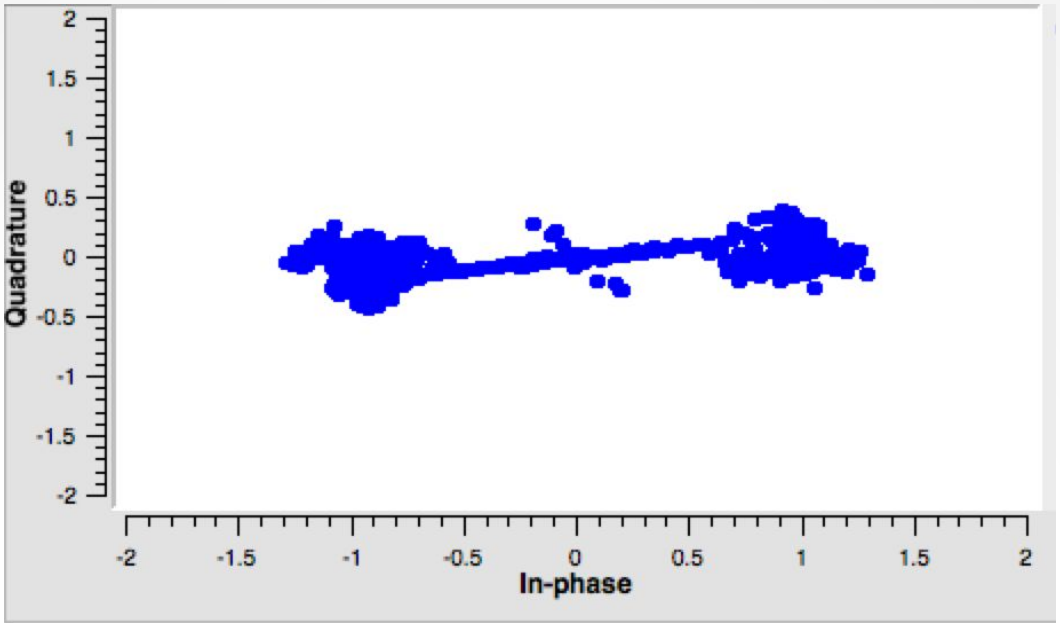


Implementation (TX)

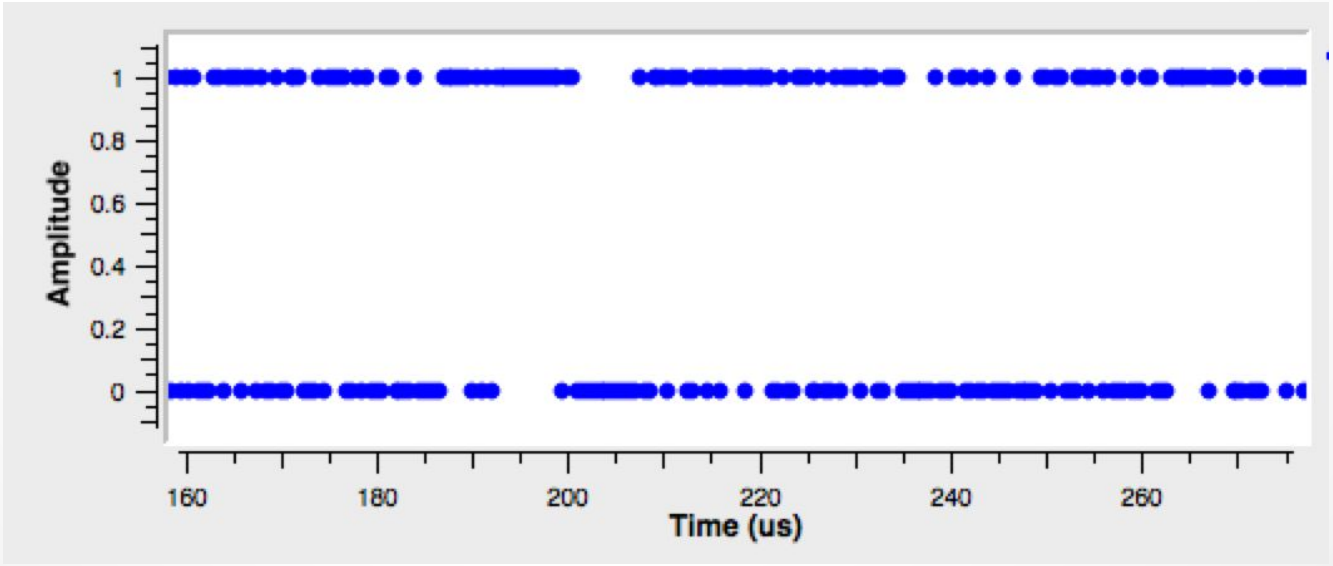


Implementation (RX)

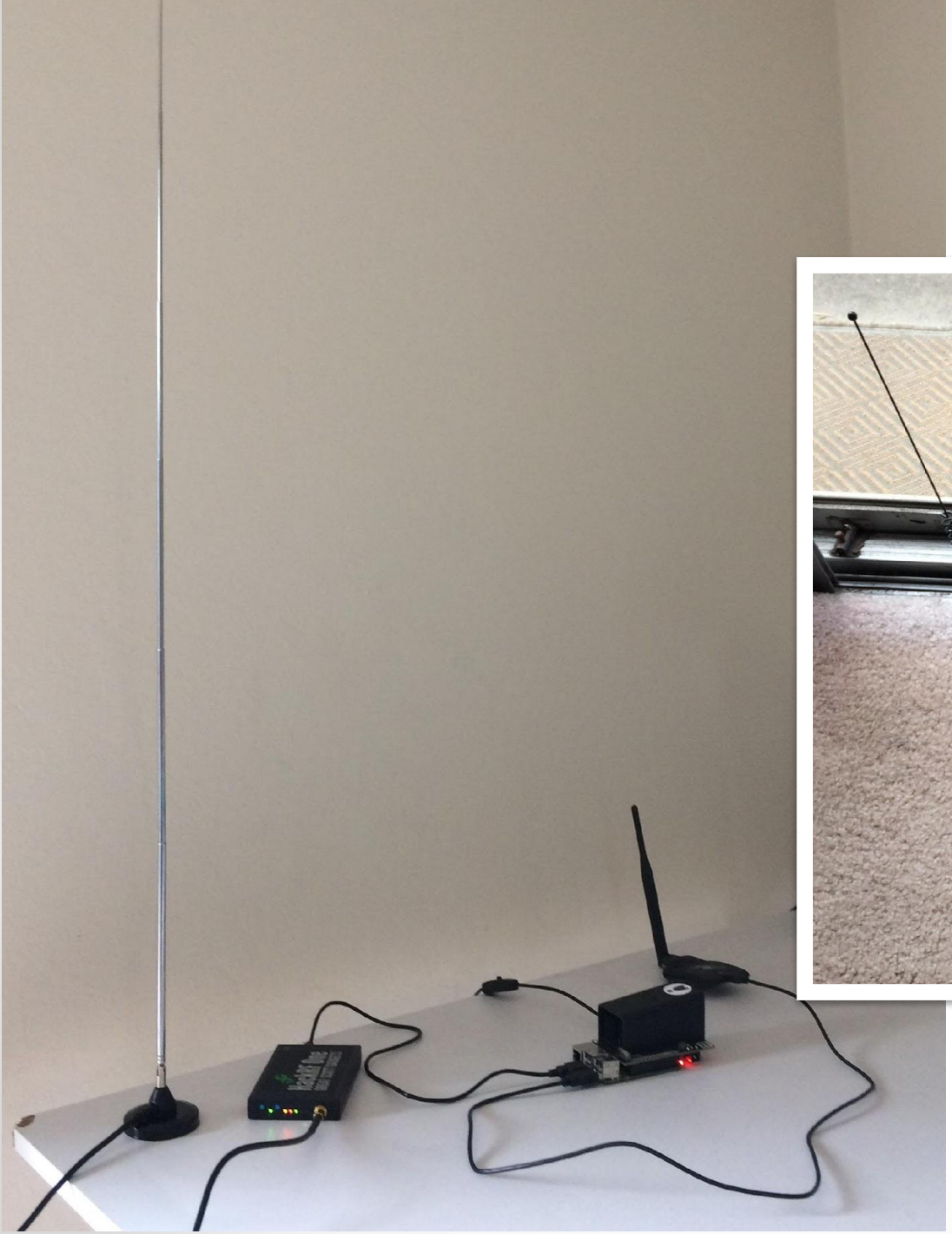


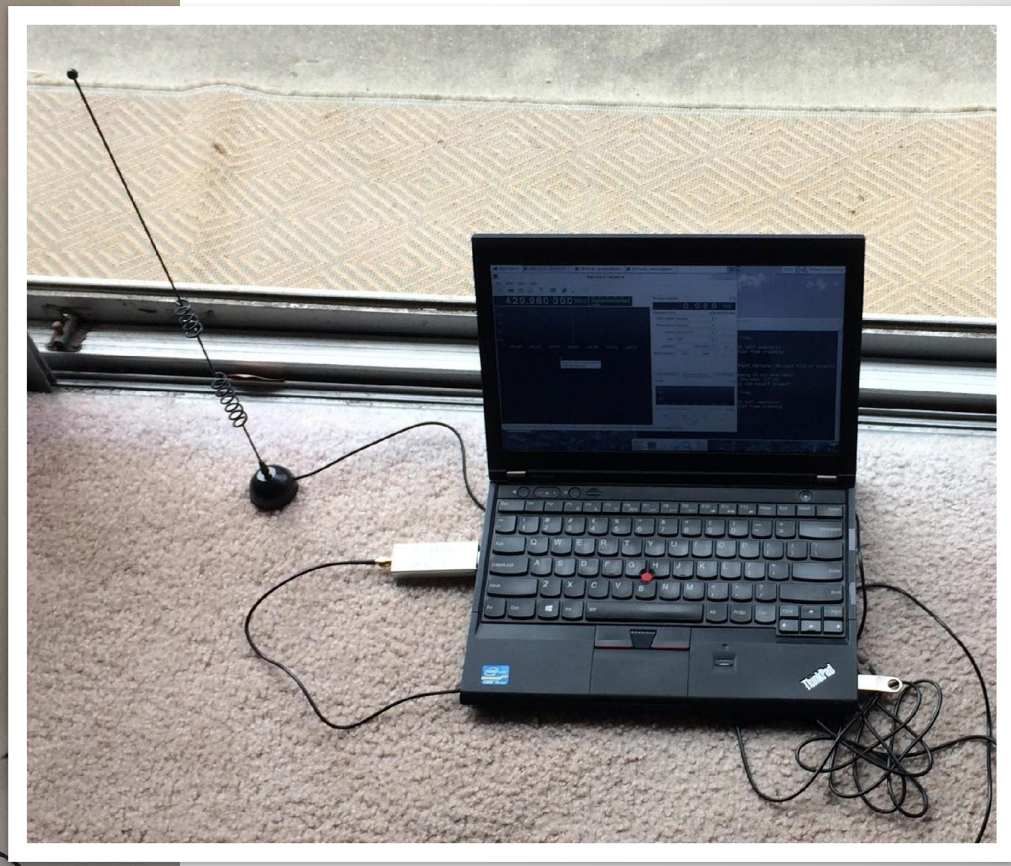


Constellation Diagram – Output of Phase Locked Loop

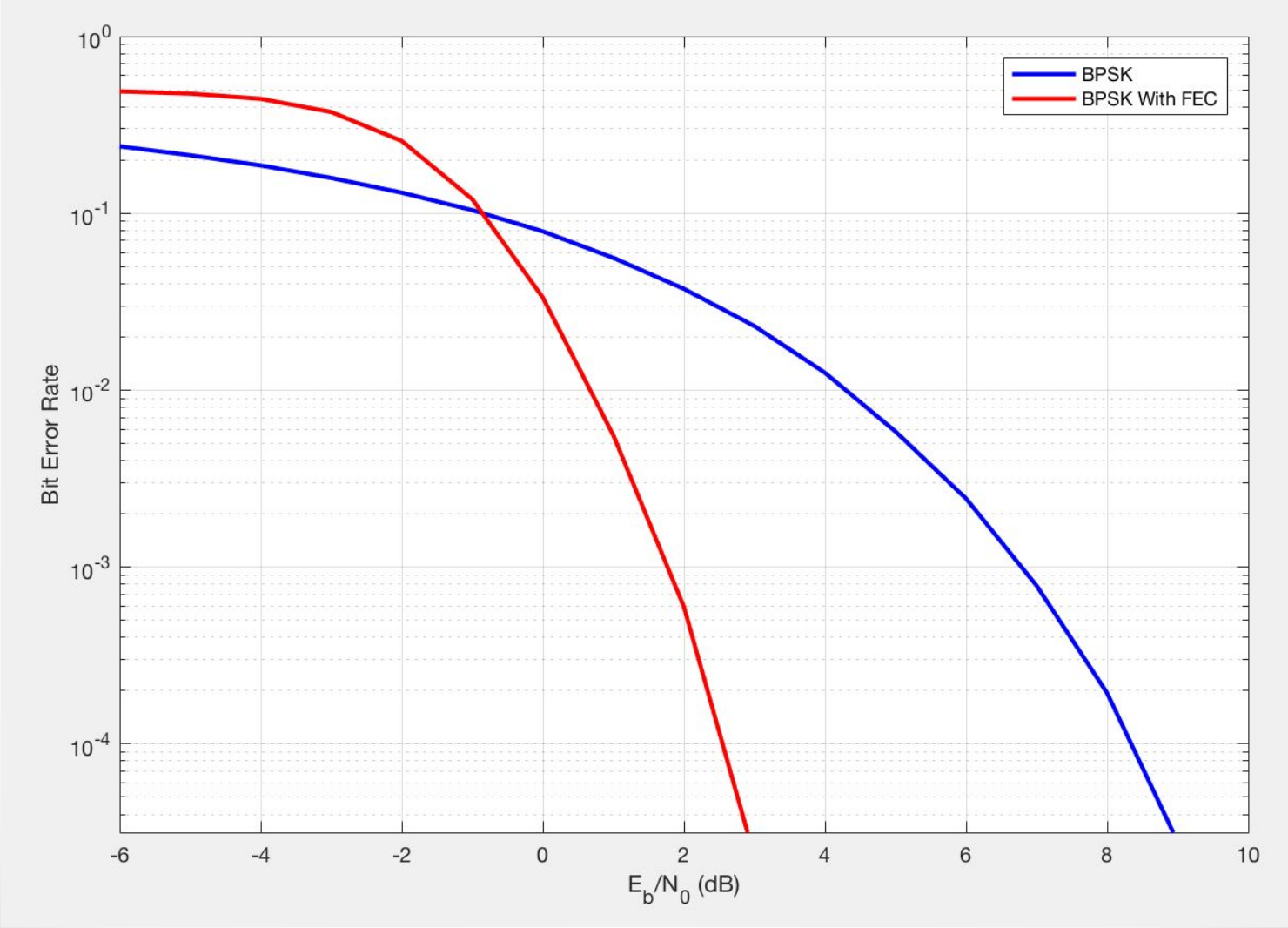


Output of Binary Slicer





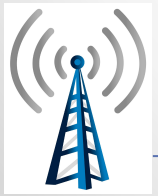
Bit-Error Rate vs E_b/N_0



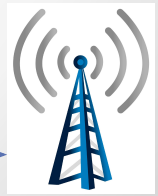
Messaging Protocol: Frames

Frame			Frame	Frame			
Header	Payload	CRC					
<SOH> +3 bytes	0-512 bytes	4 bytes					

- Header
  - <SOH> 0x01
  - Version 0x30
  - Stream ID 0x30
  - Block type
    - Connection Request, acknowledge, data, etc
- Payload
  - Callsign: source socket
  - Destination port (8333)
  - Stream ID
  - Max Payload size
    - 2^n



Connection request



Data Transmission

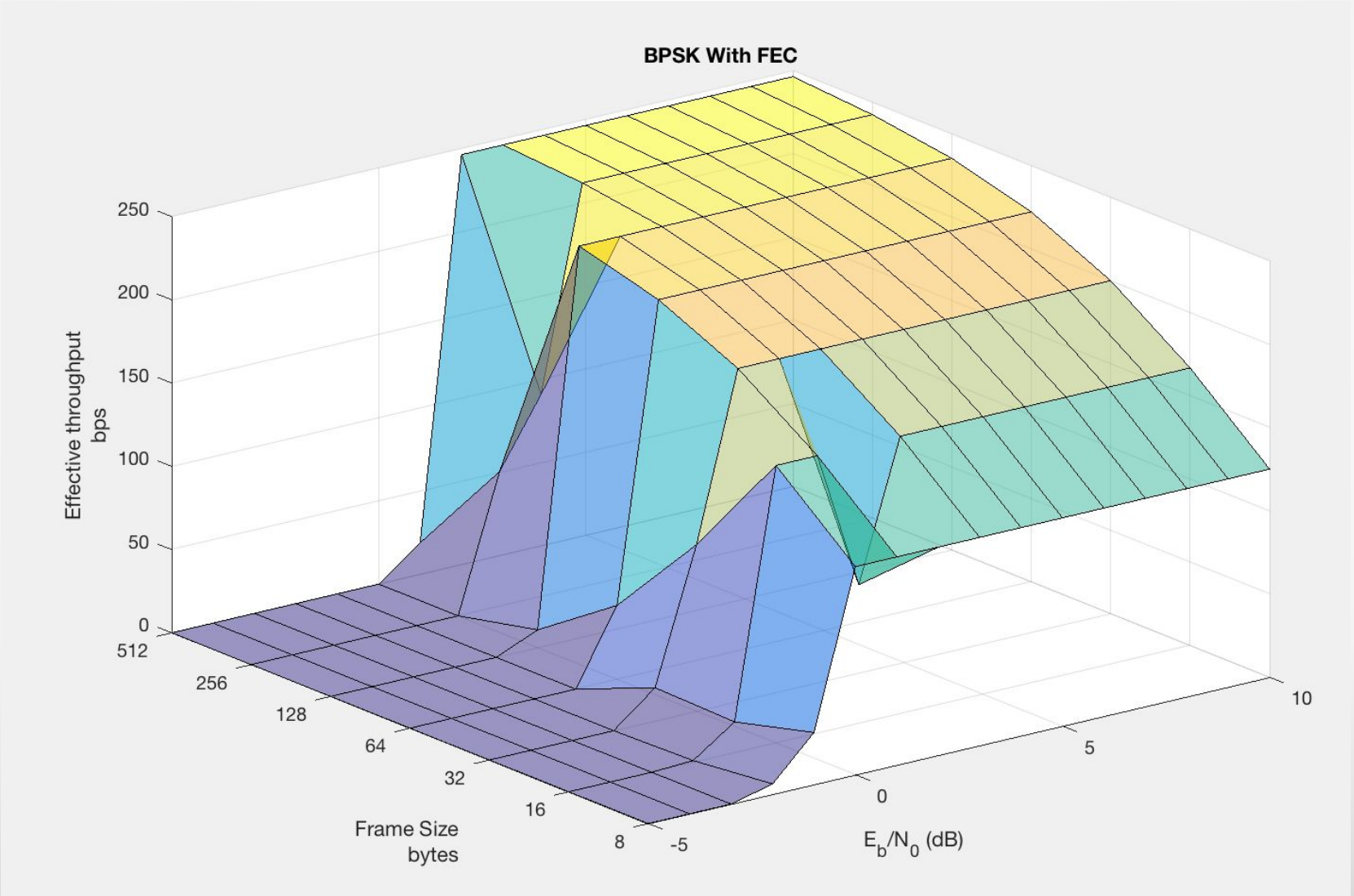
- Header
  - <SOH> 0x01
  - Version 0x30
  - Stream ID
  - Block number
- Data

- Counter (block num)
  - 6 bits: 0-63
  - Counter wraps around to 0
  - Sender will not allow counter to get more than 62 ahead of last acknowledged frame

Data Acknowledge, Retransmission Request

- Ack / Retransmit Payload
  - Last block number transmitted
  - Last block number correctly received, with no gaps
  - Last block number received
- Frame size adjusted dynamically based on number of retransmit requests

Effective Data Rate vs SNR

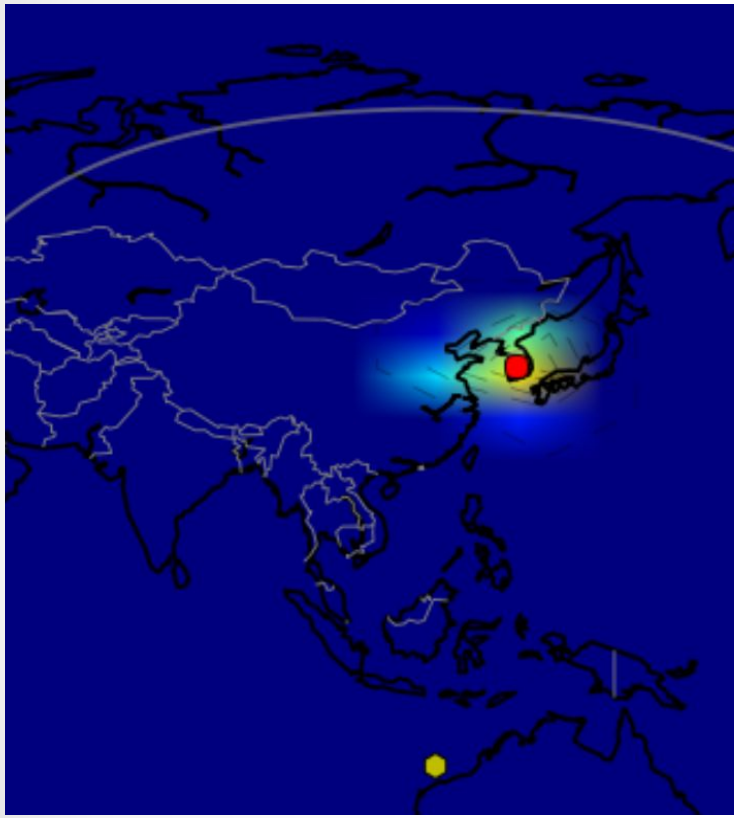


Expected Latency

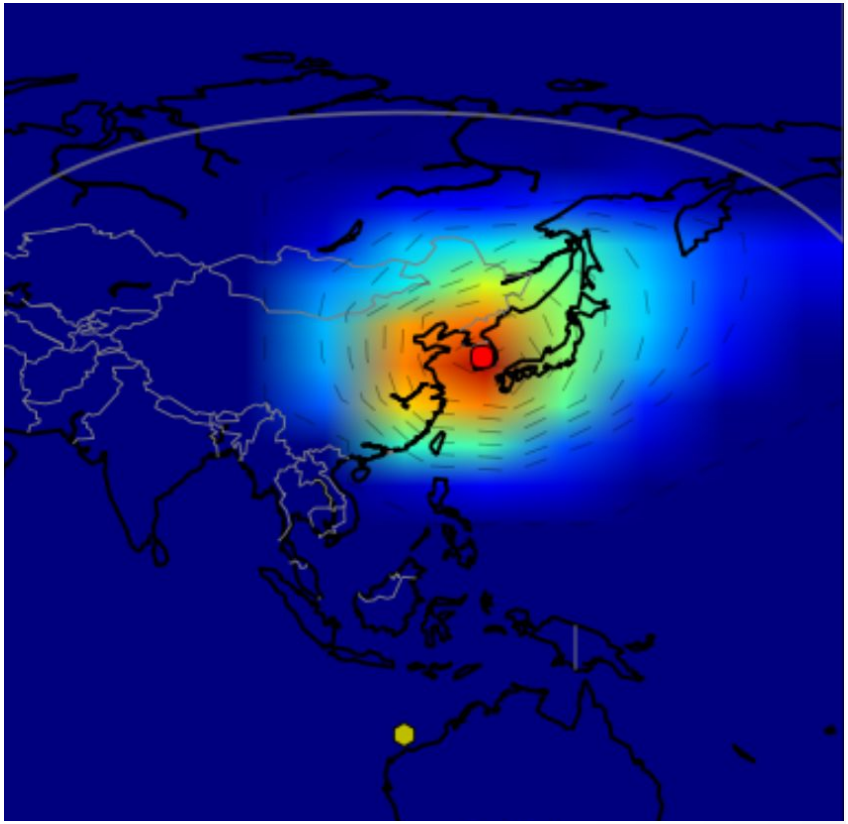
	Bytes	Bytes + overhead	-5 dB	0 dB	10 dB
version	85	113	5.42	1.81	0.46
verack	0	24	1.15	0.38	0.10
getheaders	94	126	6.05	2.02	0.51
headers	69	101	4.85	1.62	0.41
filterload	36000	36592	1756.42	585.47	148.66
filteradd	544	584	28.03	9.34	2.37
merkleblock	604	644	30.91	10.30	2.62
transaction	258	290	13.92	4.64	1.18
block	1024000	1040024	49921.23	16640.38	4225.10

Latency in seconds

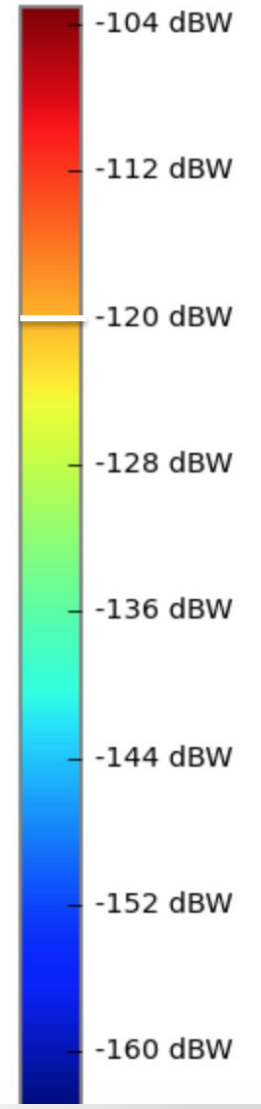
VOA Propagation Map
South Korea

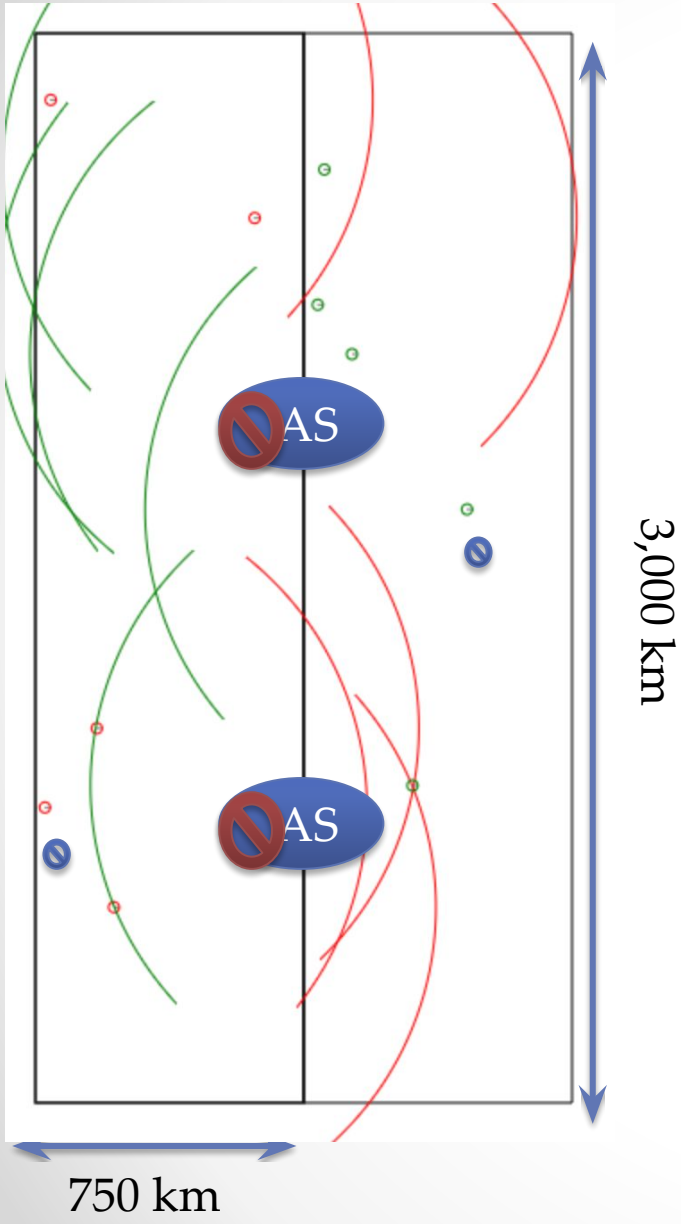


3.7 MHz, 4W



7.1 MHz, 4W

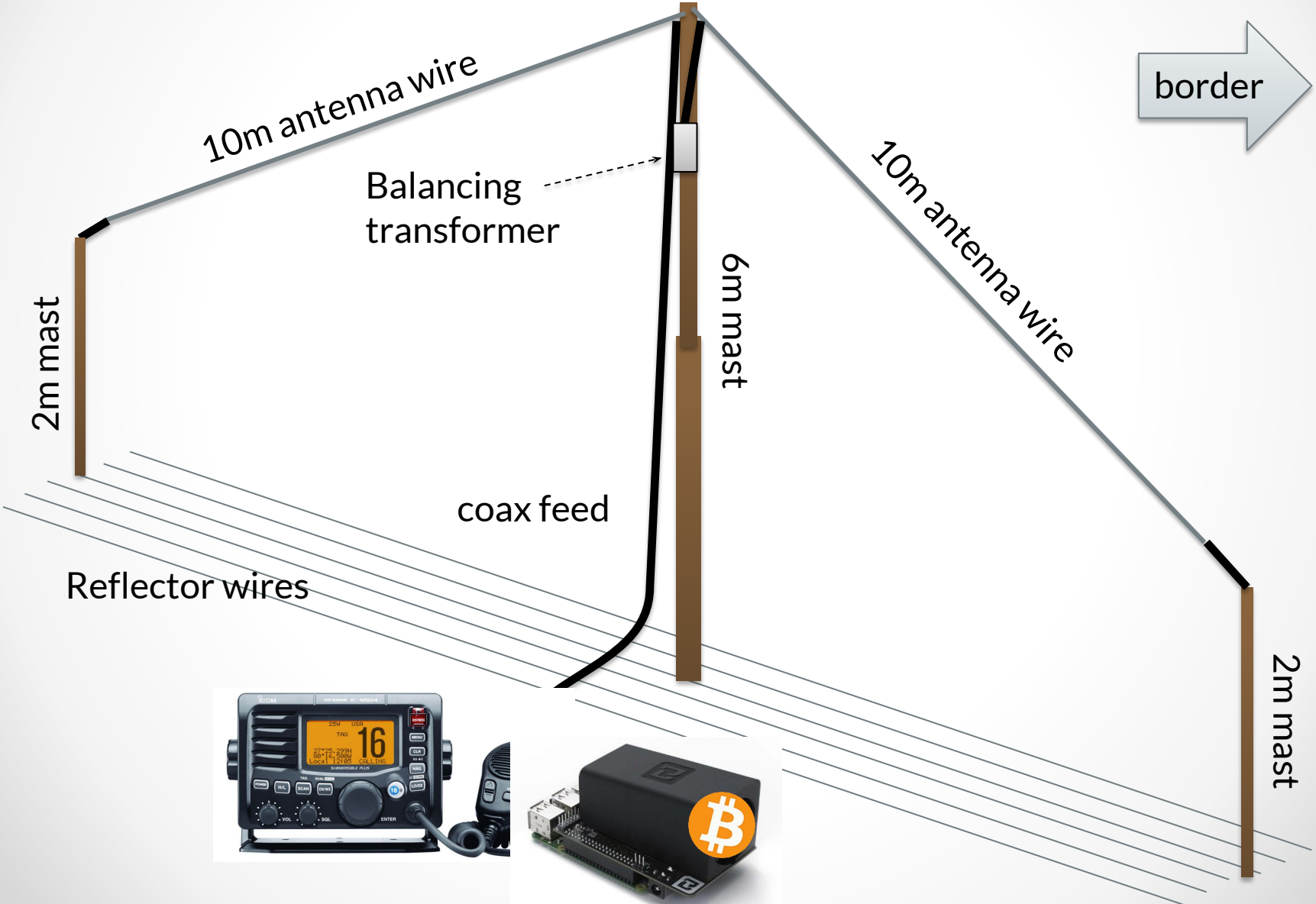




Border Simulation

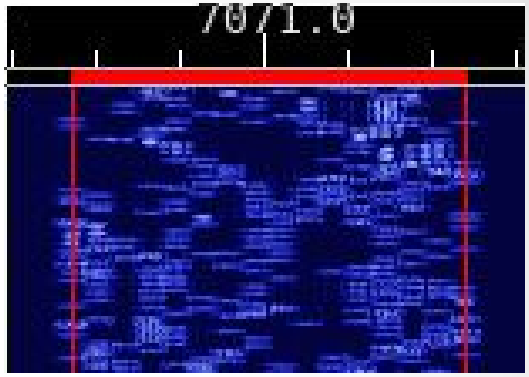
- 5 stations randomly placed on each side of the border; 900 km range
  - 40m or 75m for medium range skywave & near-vertical incidence skywave (NVIS)
  - 10m dipole antenna
- Stations in left country last only long enough to transmit & confirm a transaction
- Stations in right country relatively permanent

Design of Portable Temporary V-Dipole Antenna for NVIS & Medium Range, 40-80m



Future Work

- Improve noise rejection with MFSK
  - Better performance in low power long distance links
  - SNR target: -10 dB
  - Dynamic modulation based on conditions
- Custom Messaging Protocol
  - Reduce overhead



- Electrical shortening for antennas
- Run long-distance tests with antenna rigs
  - Volunteers needed!