black hat®

USA 2015

UBM Tech

Spread Spectrum Satcom Hacking

Attacking the Globalstar Simplex Data Service

Colby Moore
@colbymoore - colby@synack.com

Who am I?

Colby Moore
Synack R&D

Synack

Motivation

- Rehashes of same talks
- Satellite hacking talks never deliver
- RF world not heavily explored
- So many of these systems are broken
- I want to inspire and collaborate on research in this department

What are we going to learn?

- Basics of RF signals and modulation
- What is spread spectrum
- Selecting a target and reverse engineering
- Exploiting that target

Prerequisites

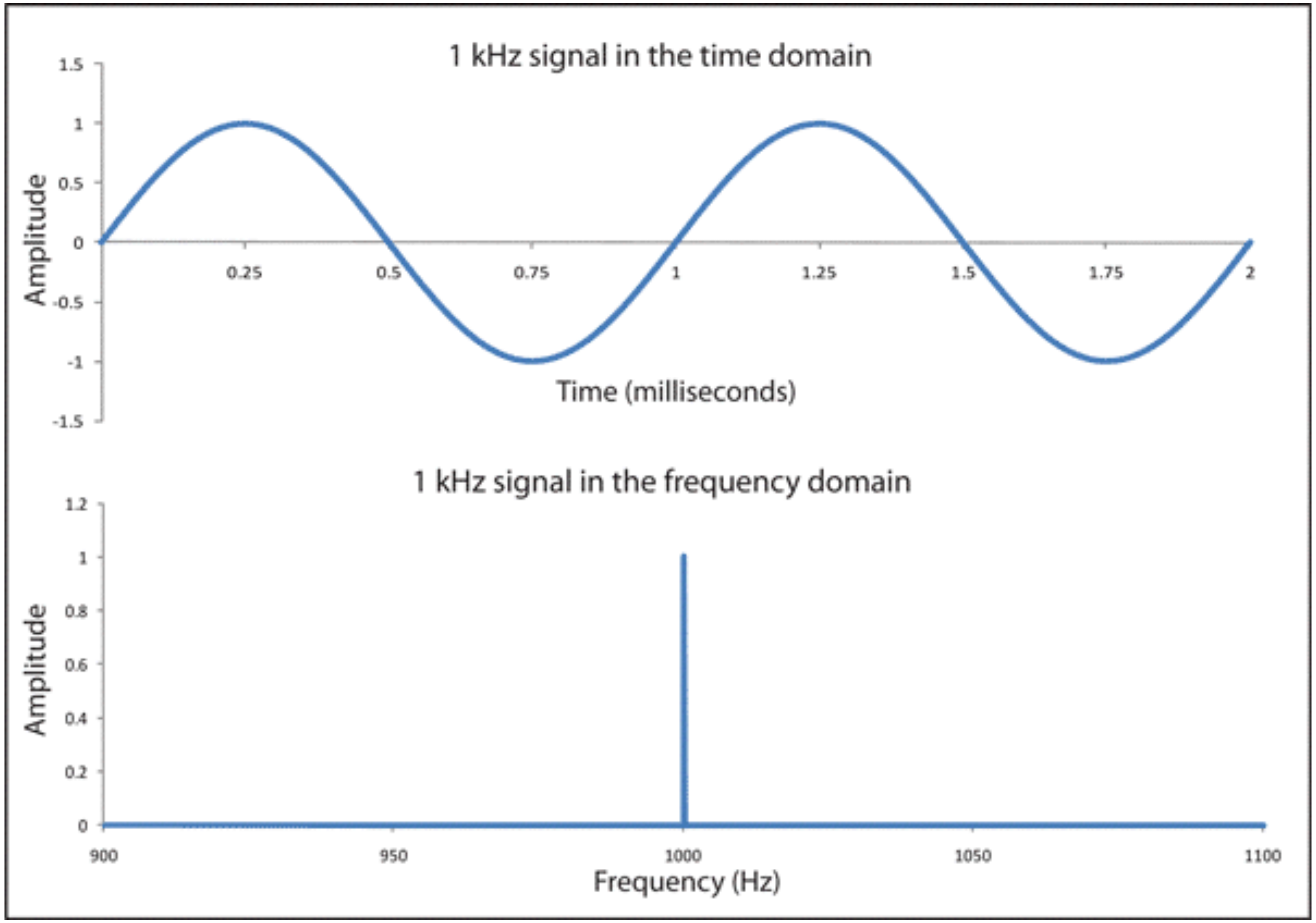
- Keeping things “understandable”
- High school mathematical knowledge
- Will provide resources

Waves

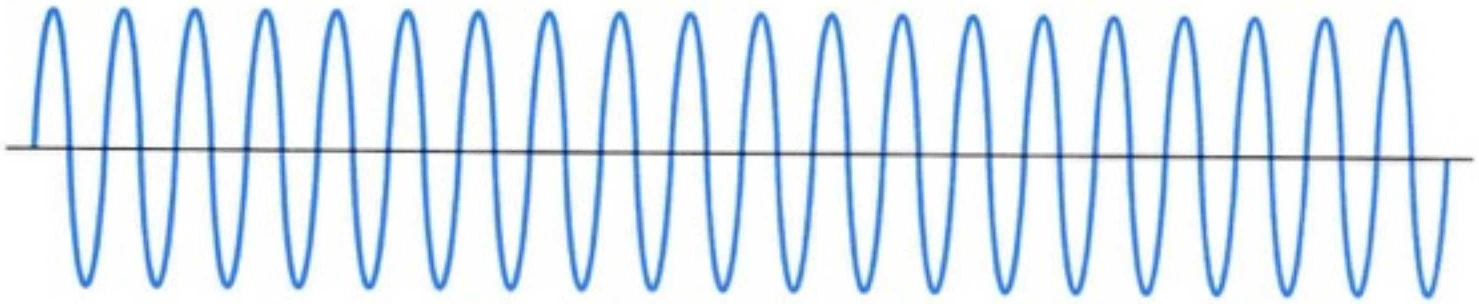
$$y(t) = A * \sin(2\pi ft + \phi)$$

- A - Amplitude
- *f* - Frequency (radians/second)
- ϕ - Phase (radians)

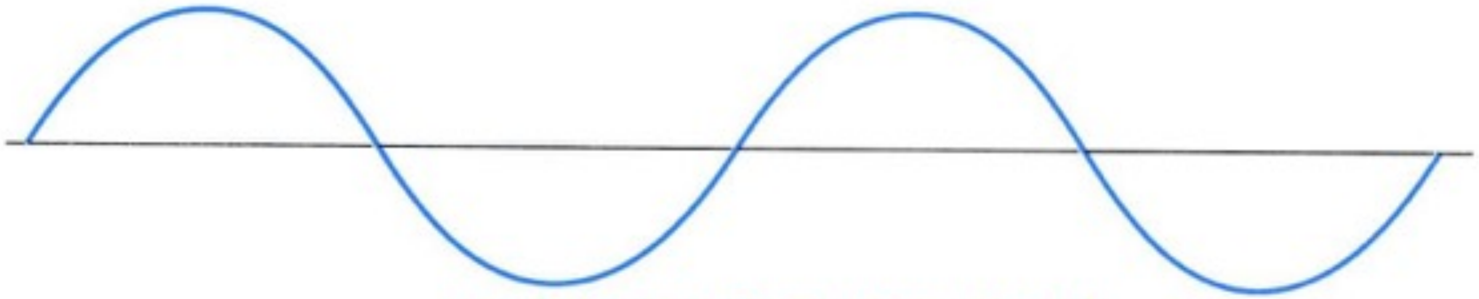
Time Domain vs. Frequency Domain



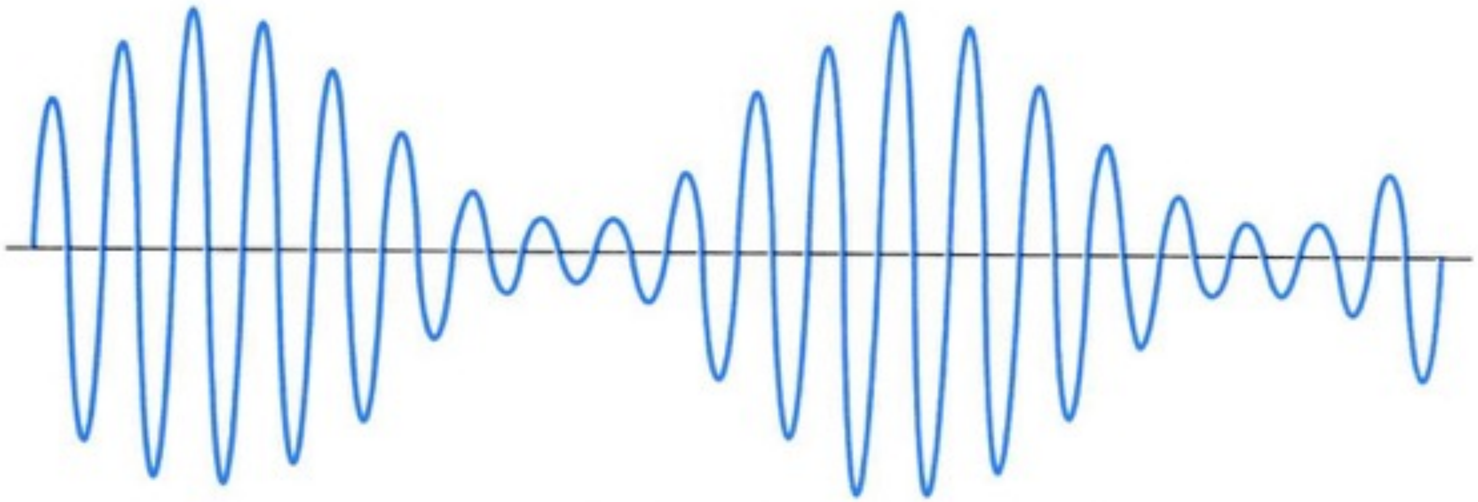
Analog RF Modulation



Carrier Signal

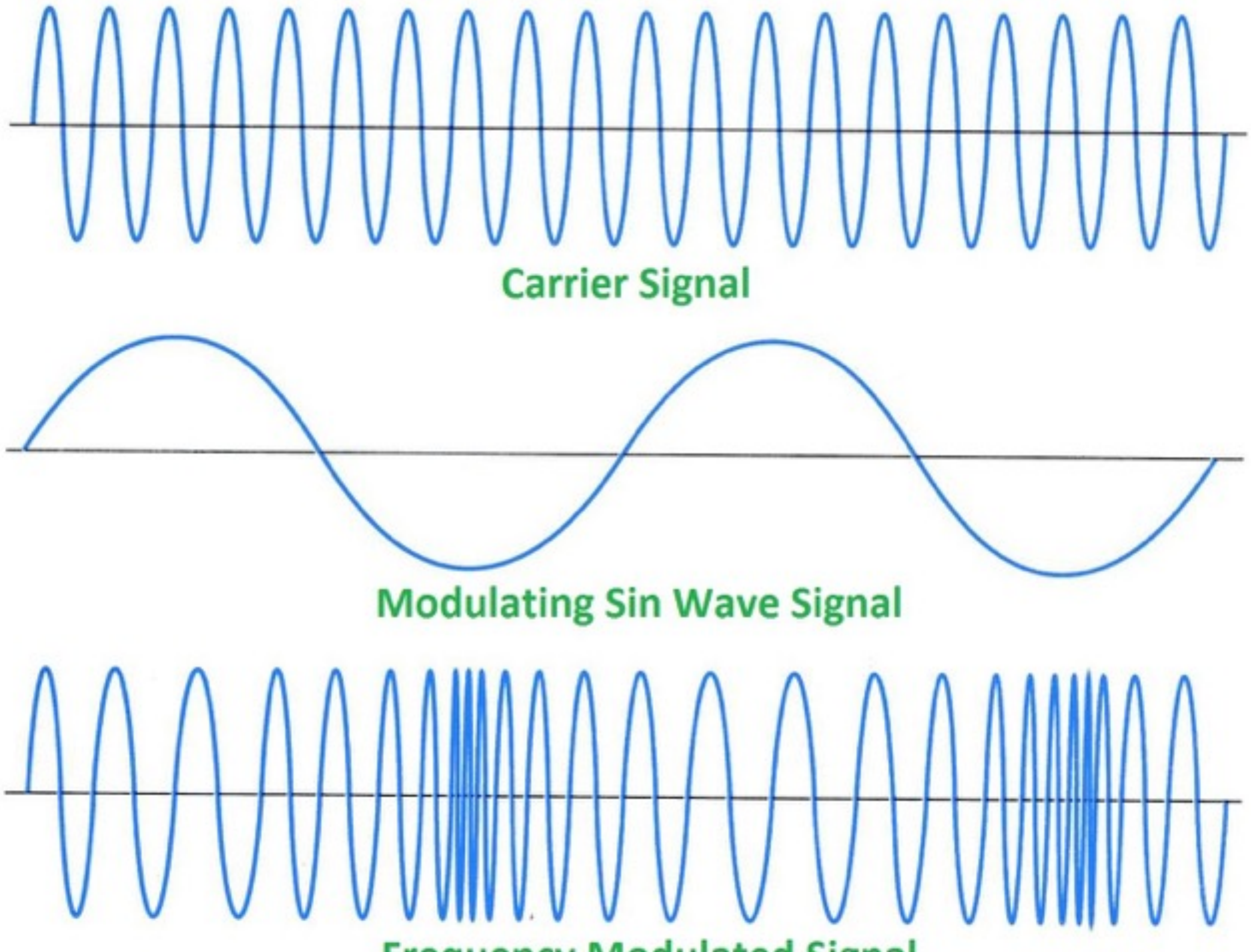


Modulating Sine Wave Signal



Amplitude Modulated Signal

Analog RF Modulation



Carrier Signal

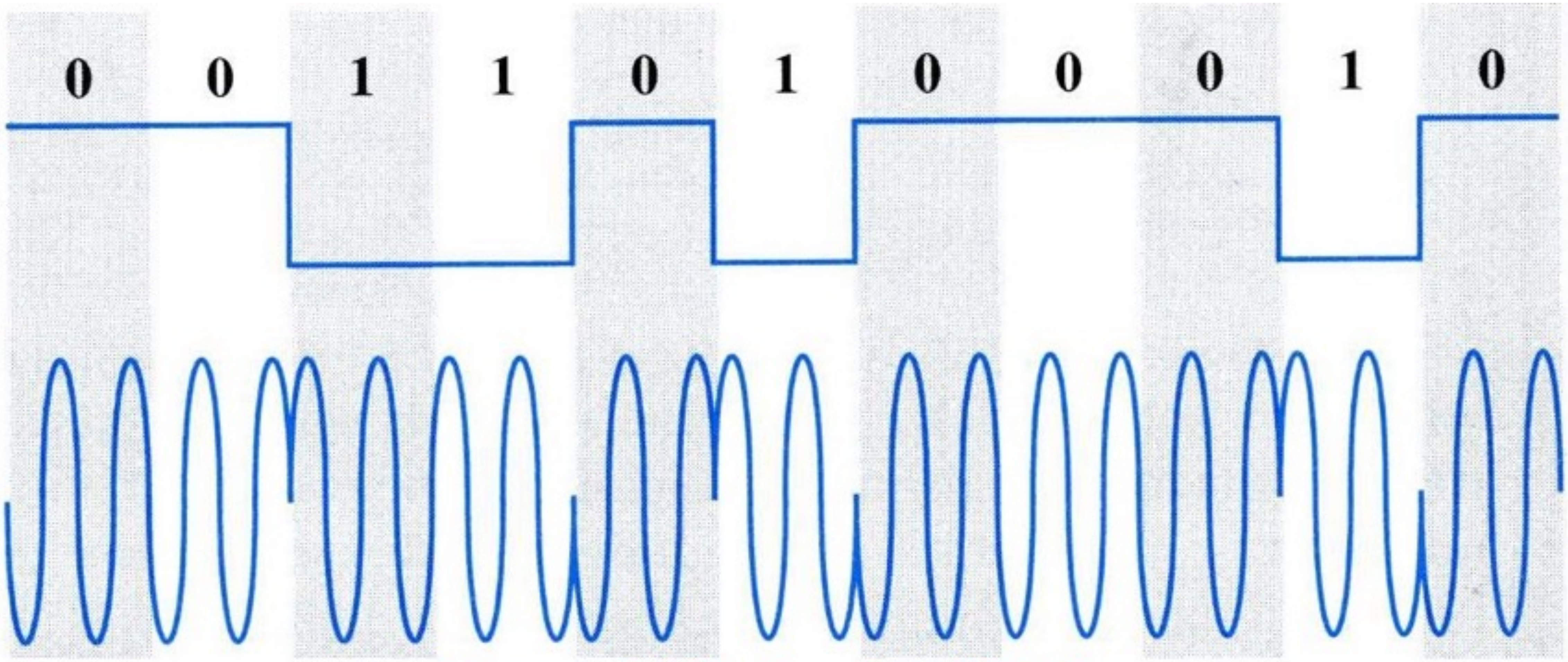
Modulating Sin Wave Signal

Frequency Modulated Signal

Digital RF Modulation

- Amplitude Shift Keying (ASK / OOK)
- Frequency Shift Keying (FSK)
- **Phase Shift Keying (PSK)**

Phase Shift Keying (PSK)

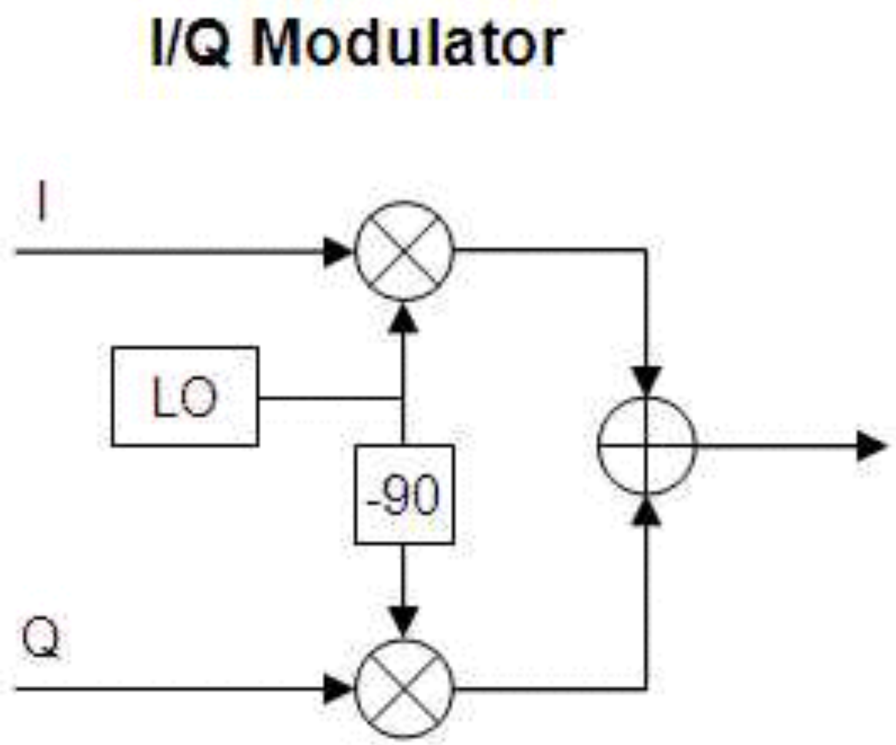


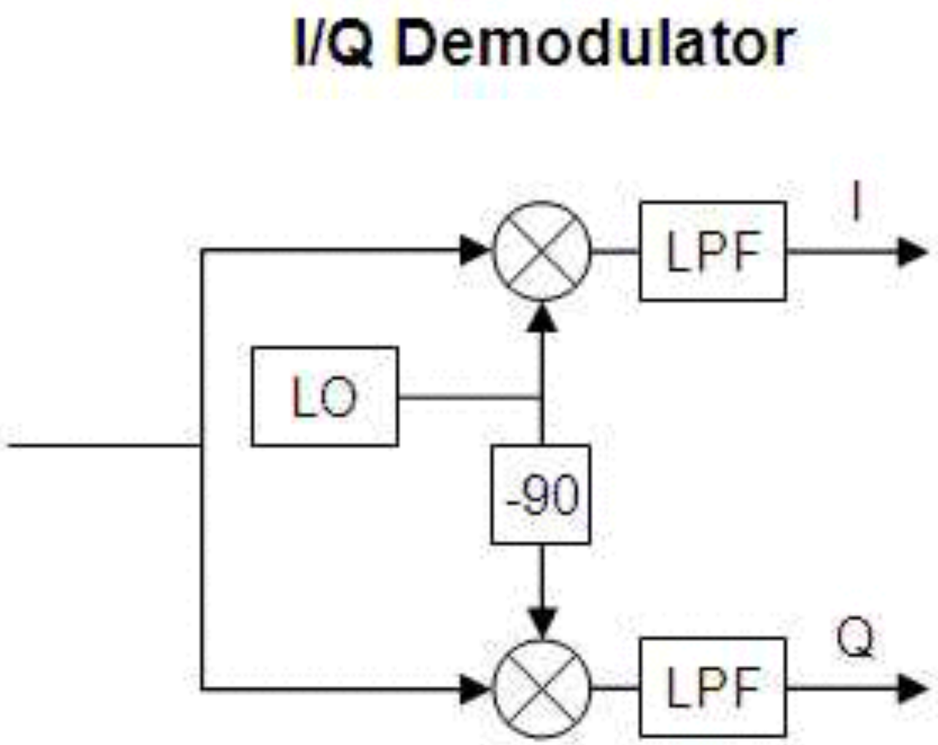
Phase Shift Keying (PSK)

Or called BPSK, uses two phases to represent 0 & 1

IQ Modulation

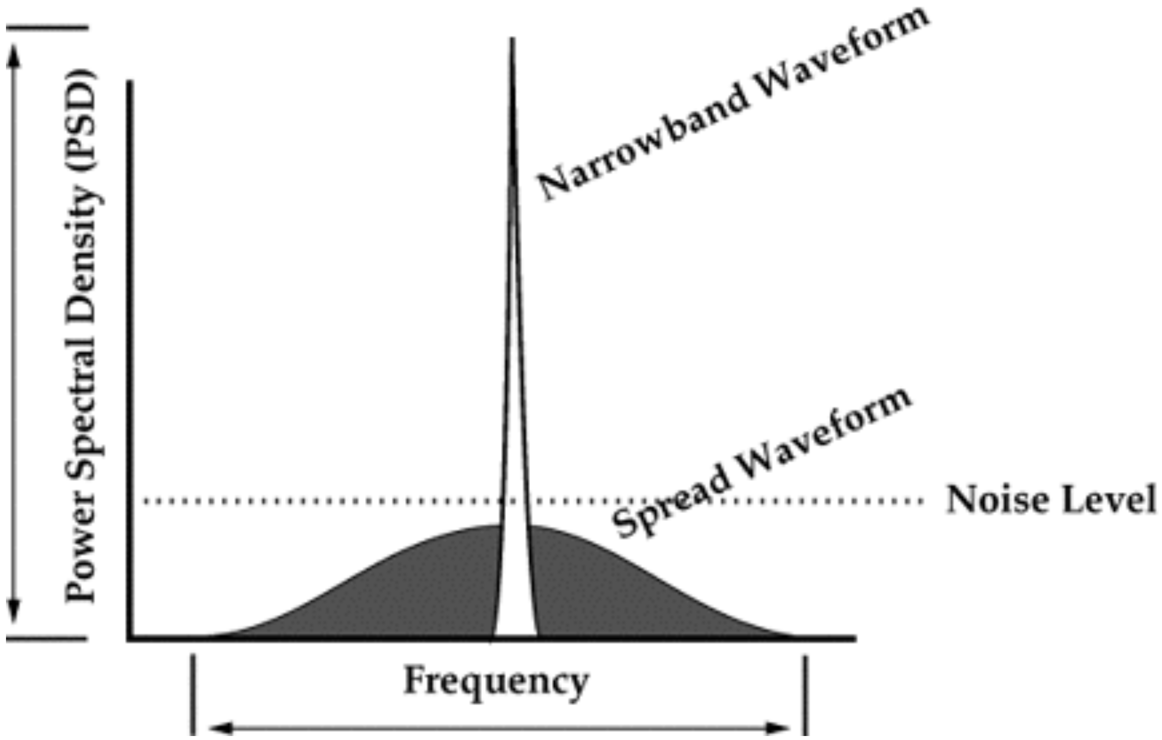
- Makes modulation easy in software!





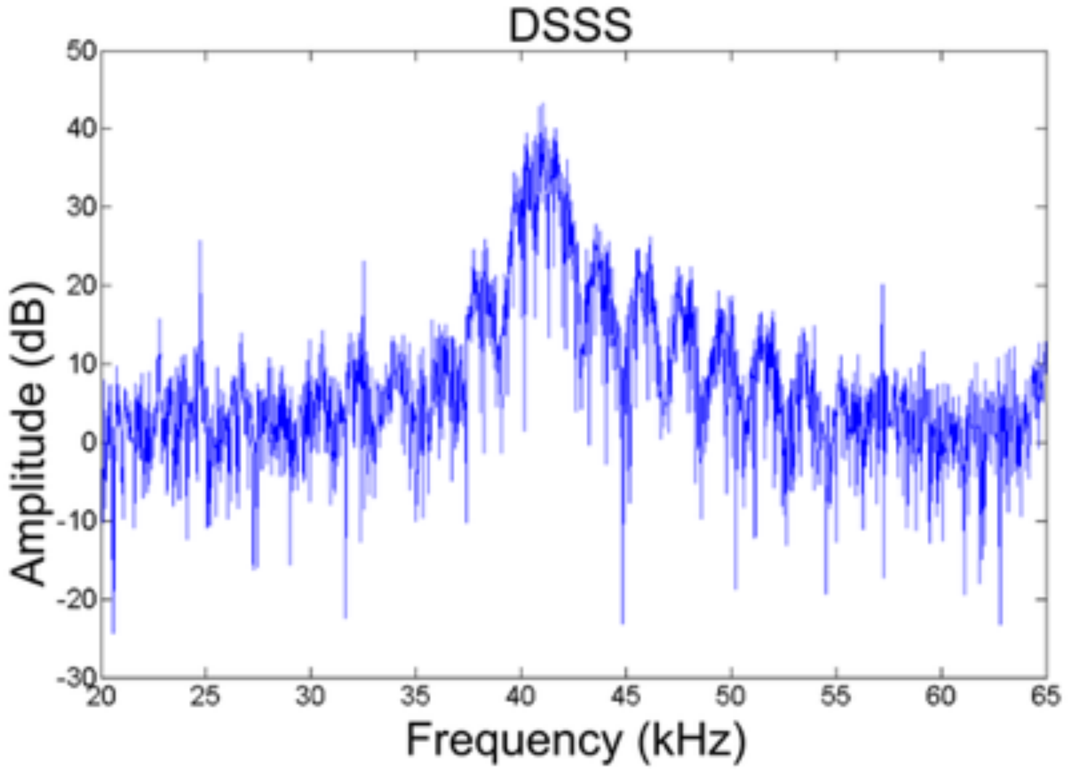
Spread Spectrum Modulation

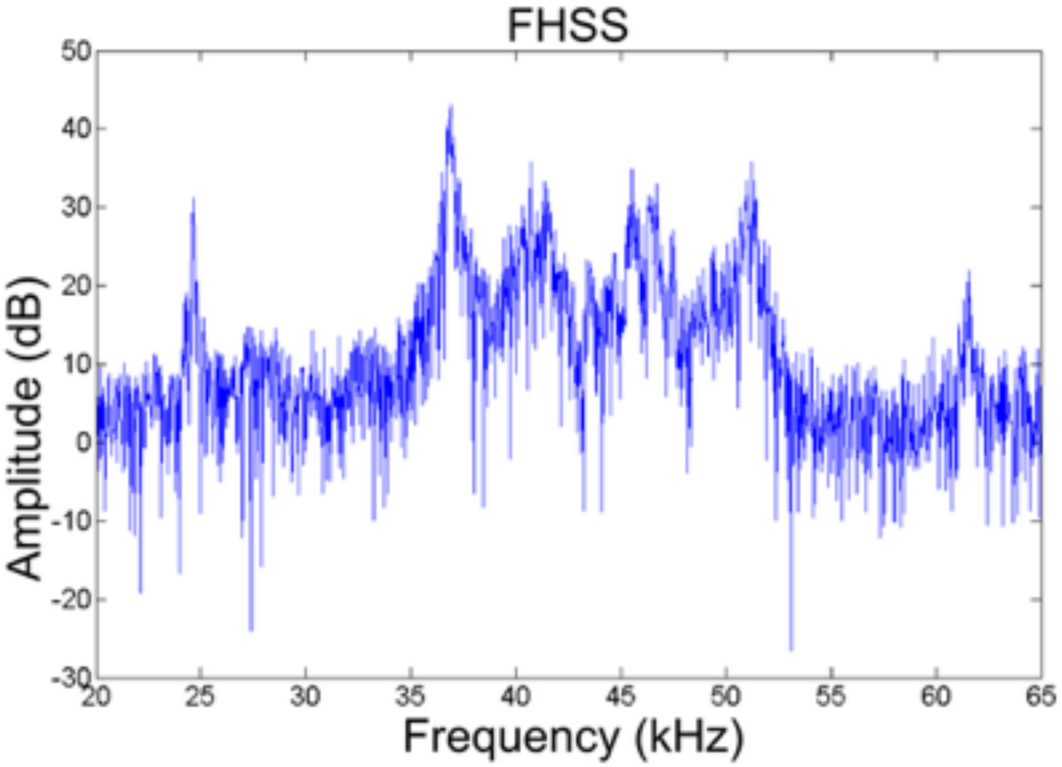
- Why is Spread Spectrum Special?
- WiFi, Bluetooth, Basically all modern RF Communications
- Processing Gain
- Jam Resistant
- CDMA



Spread Spectrum

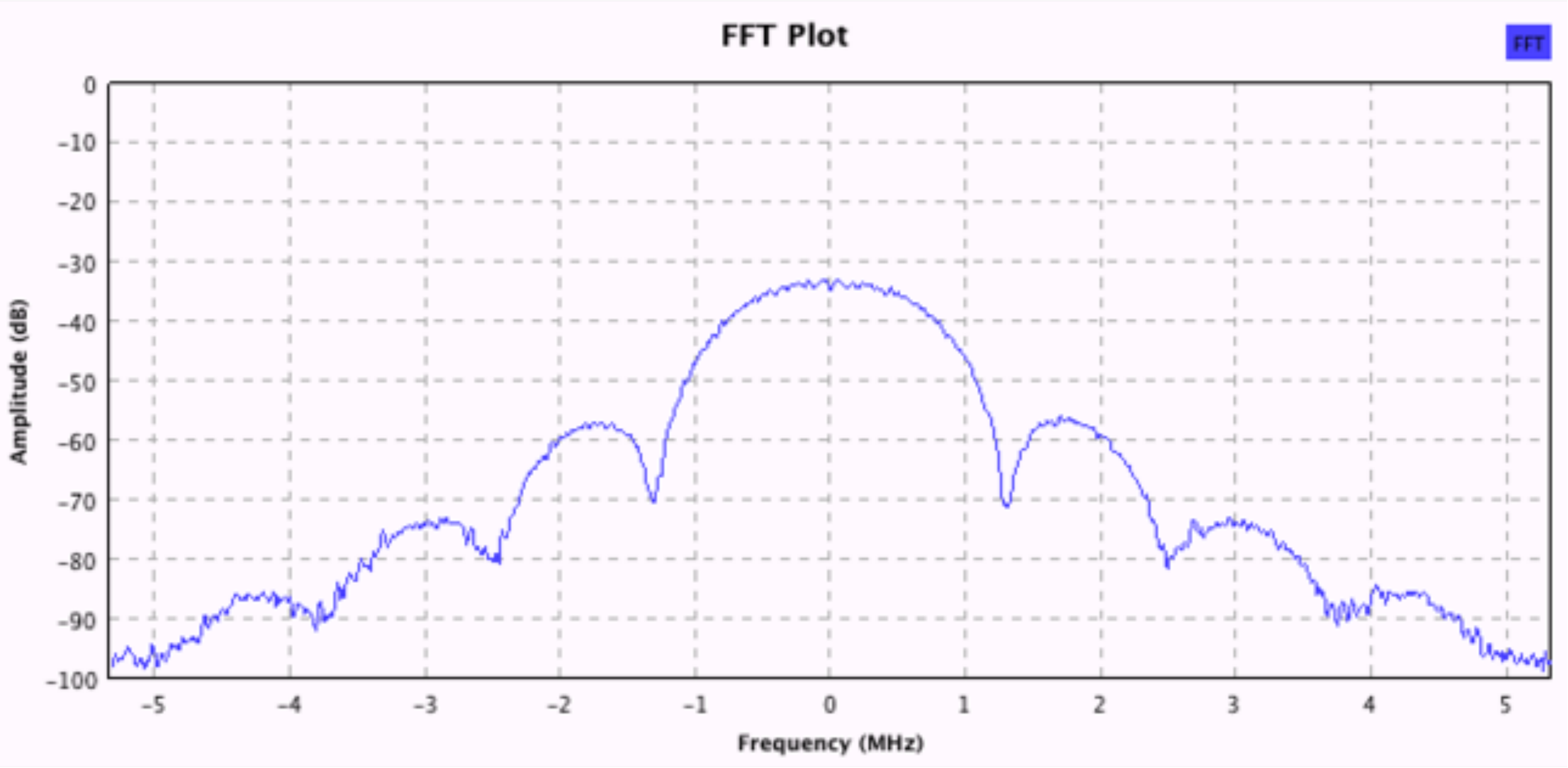
- Frequency Hopping Spread Spectrum (FHSS)
- Direct Sequence Spread Spectrum (DSSS)



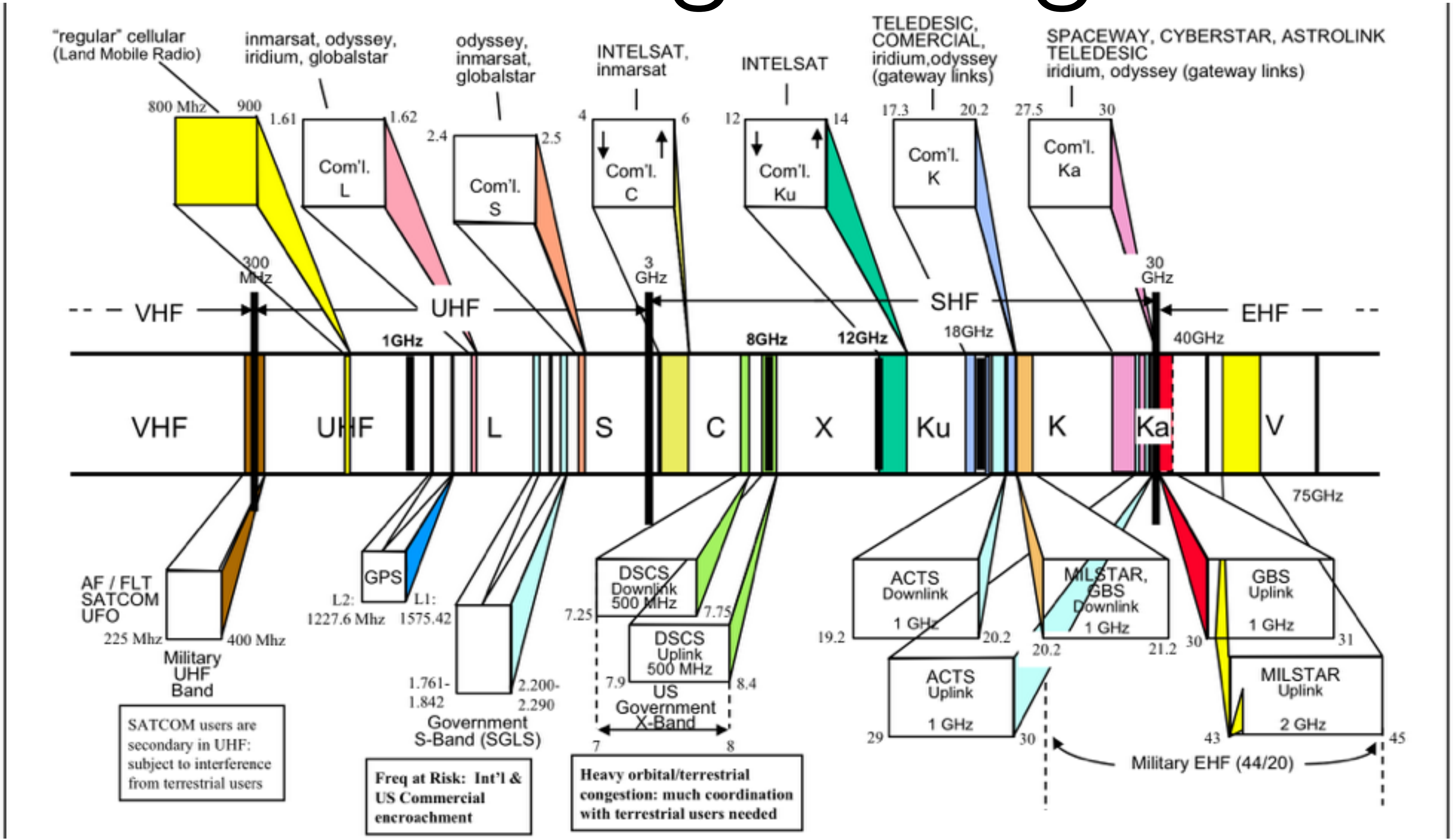


DSSS

- Direct Sequence Spread Spectrum (DSSS)



Selecting a Target

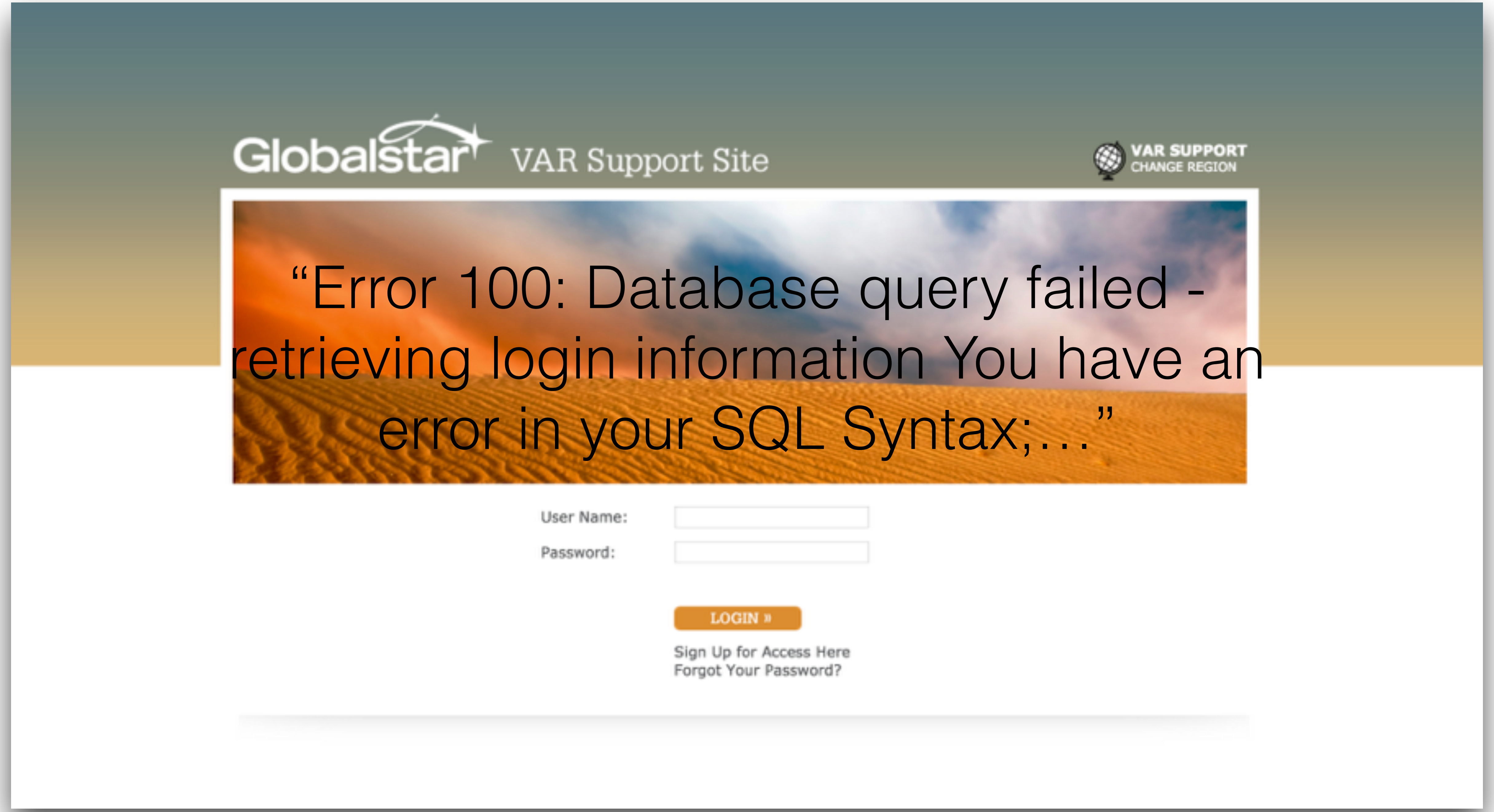


Globalstar

- SPOT - Consumer grade satellite tracking
- But wait… this tech is used everywhere. Goldmine.
- Voice, data, messaging, etc.

spot™

Stuck in the 90s



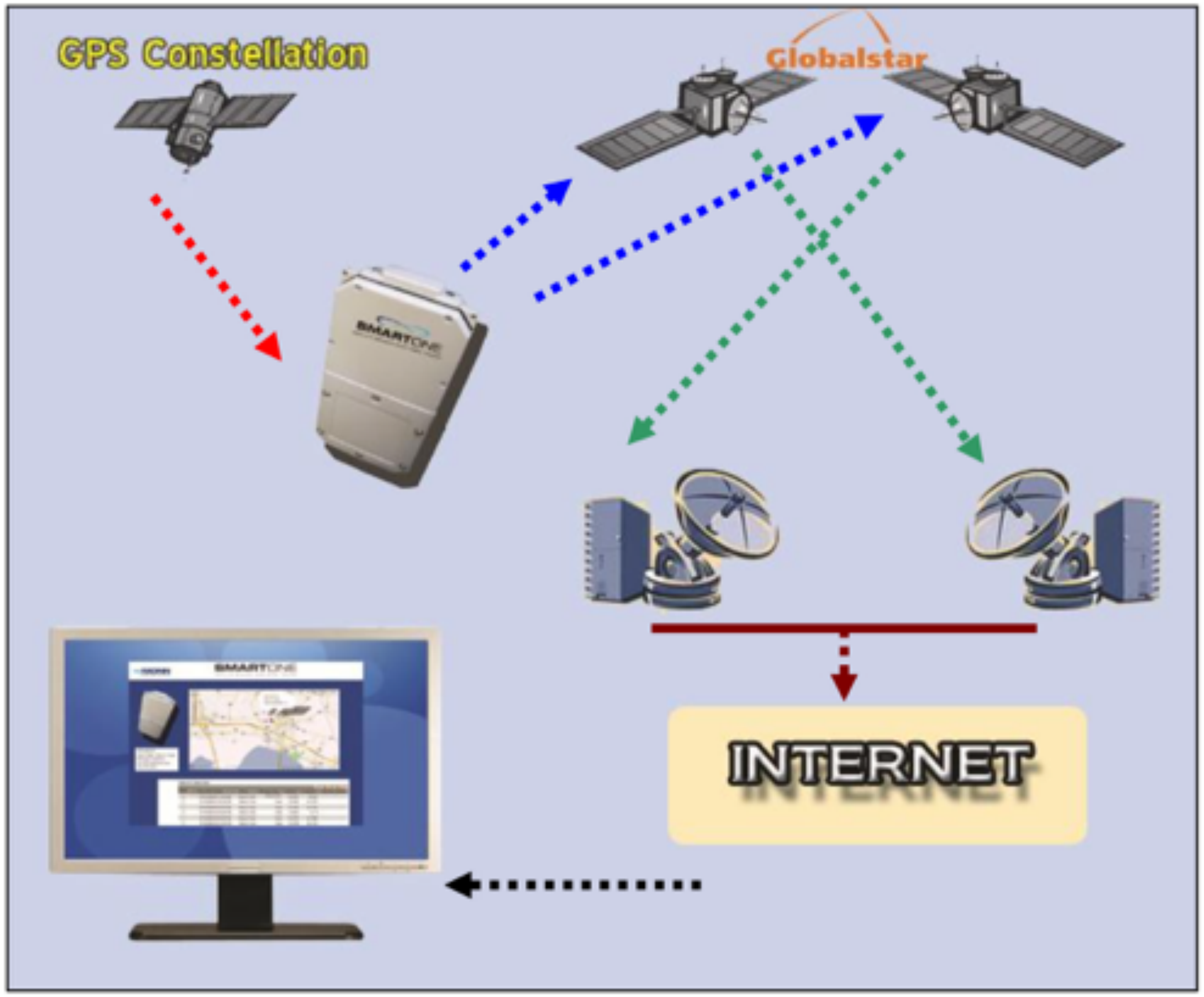
“Error 100: Database query failed - retrieving login information You have an error in your SQL Syntax;…”

User Name:

Password:

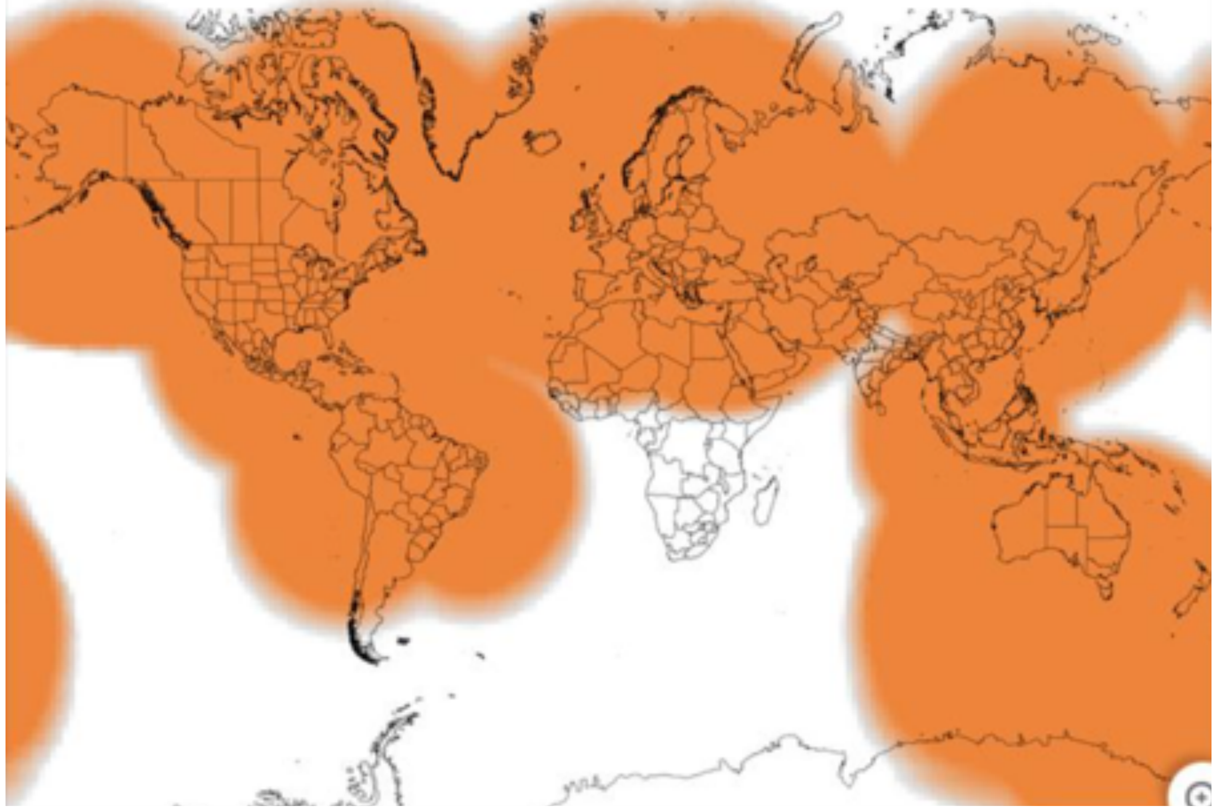
> *“The received data is then forwarded to a user defined network interface that may be in the form of an FTP host or HTTP host where the user will interpret the data for further processing.”*
>
> –Globalstar

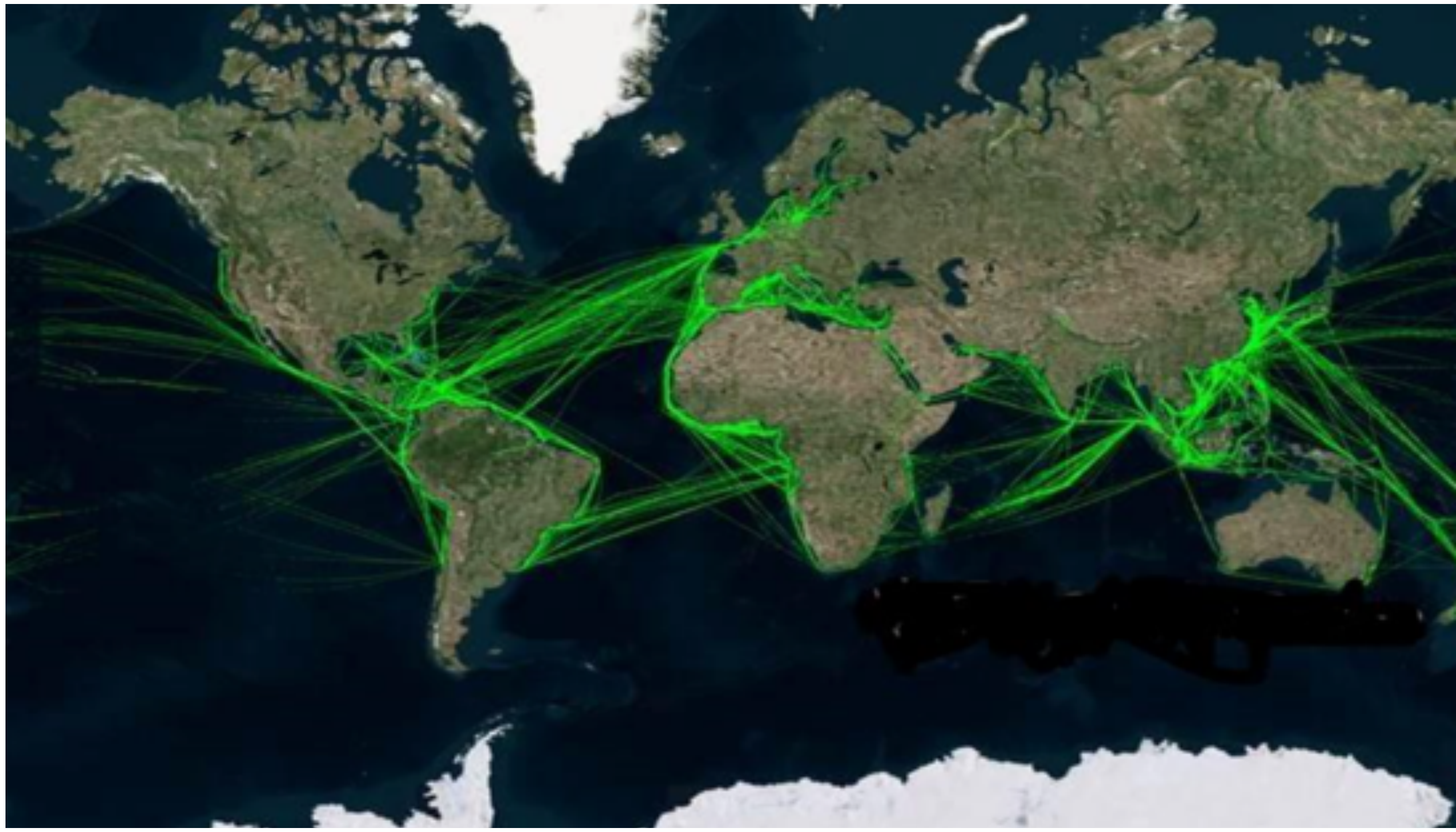
Simplex data network



“Simplex Works where infrequent, small packets of data are to be collected”

Coverage





[redacted]

48 satellites
5850 km diameter footprint
1410 km orbit
In service since 2000

Ground Stations

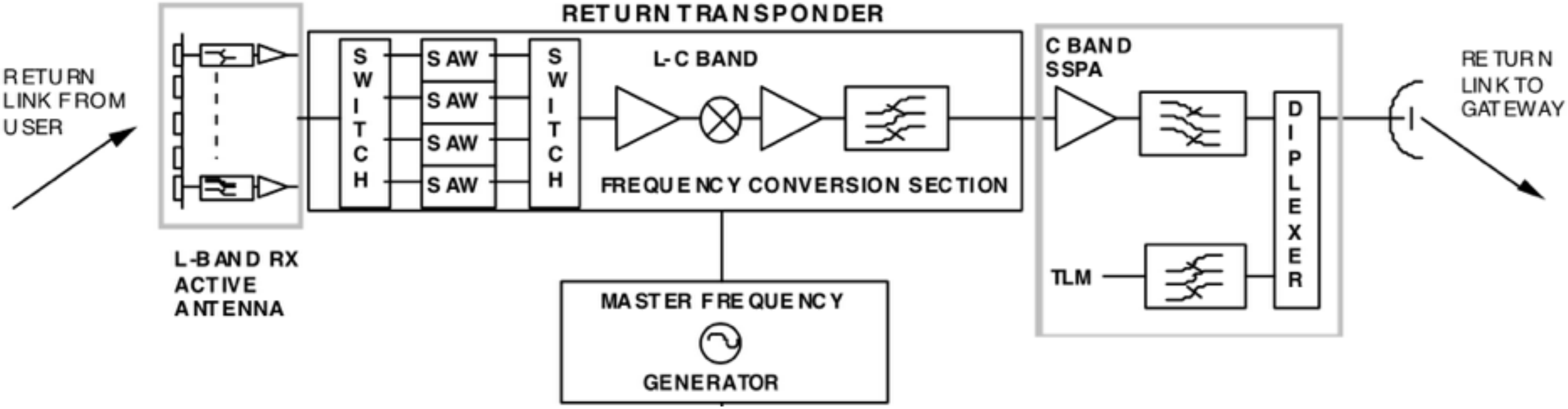
Hundreds of ground stations

Command Centers

Where is it used?

Military / Classified
Trailers / Containers
Air Quality Monitoring
Personnel Tracking
Fire Detection and Prevention
Water Quality Monitoring
Tank Level Gauging
Perimeter / Border monitoring
Asset / Vehicle Tracking
Remote Meters
Buoys
Ship Movement
Fishing vessel monitoring
Power line monitoring
Dispersed sensors

Bent Pipe



"A bent pipe satellite does not demodulate and decode the signal. A gateway station on the ground is necessary to control the satellite and route traffic to and from the satellite and to the internet."

Beam Pattern

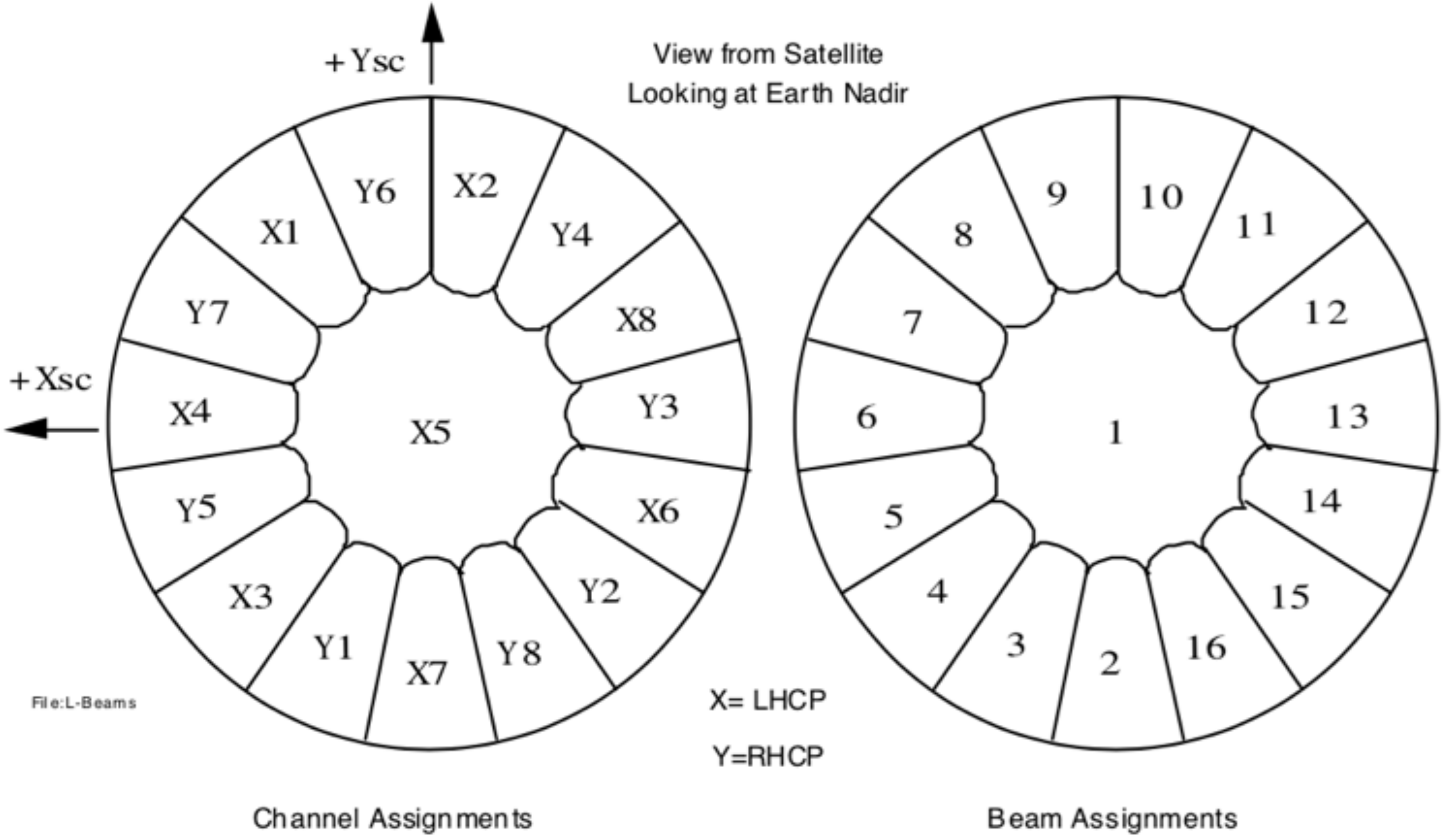
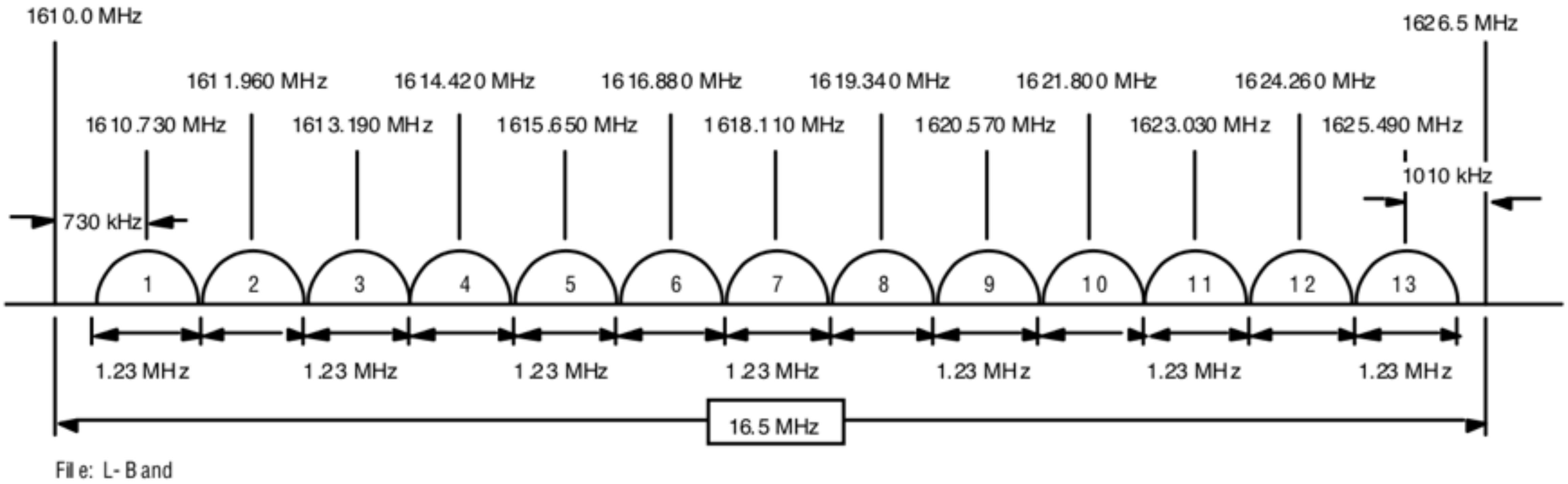
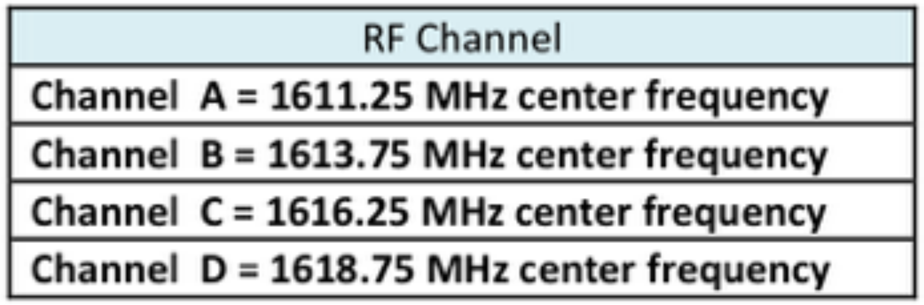


Figure 3-3 L- Band Beams

Frequency Range

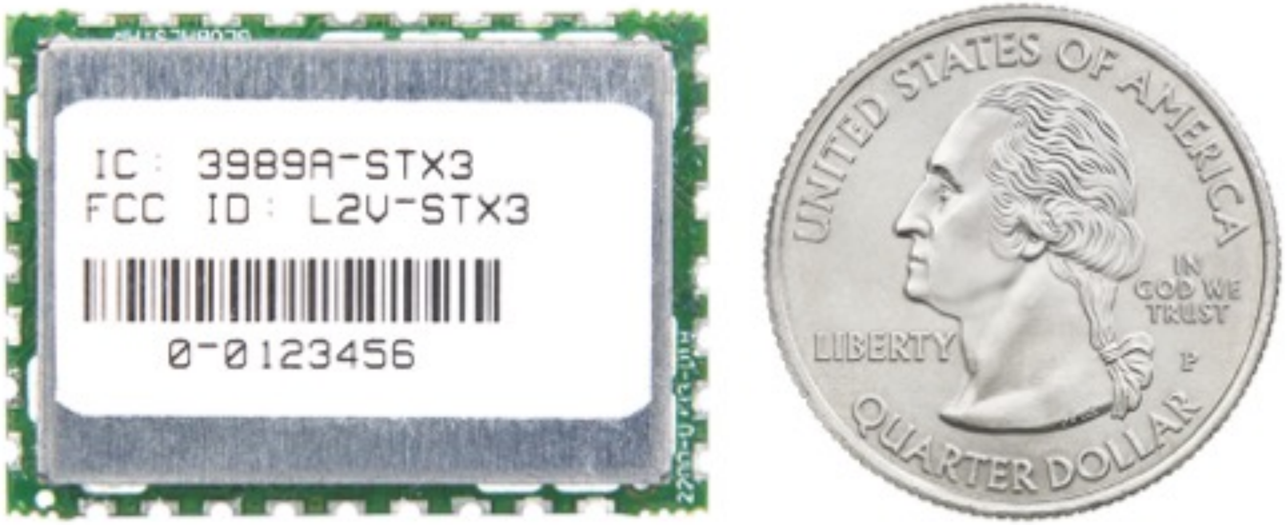


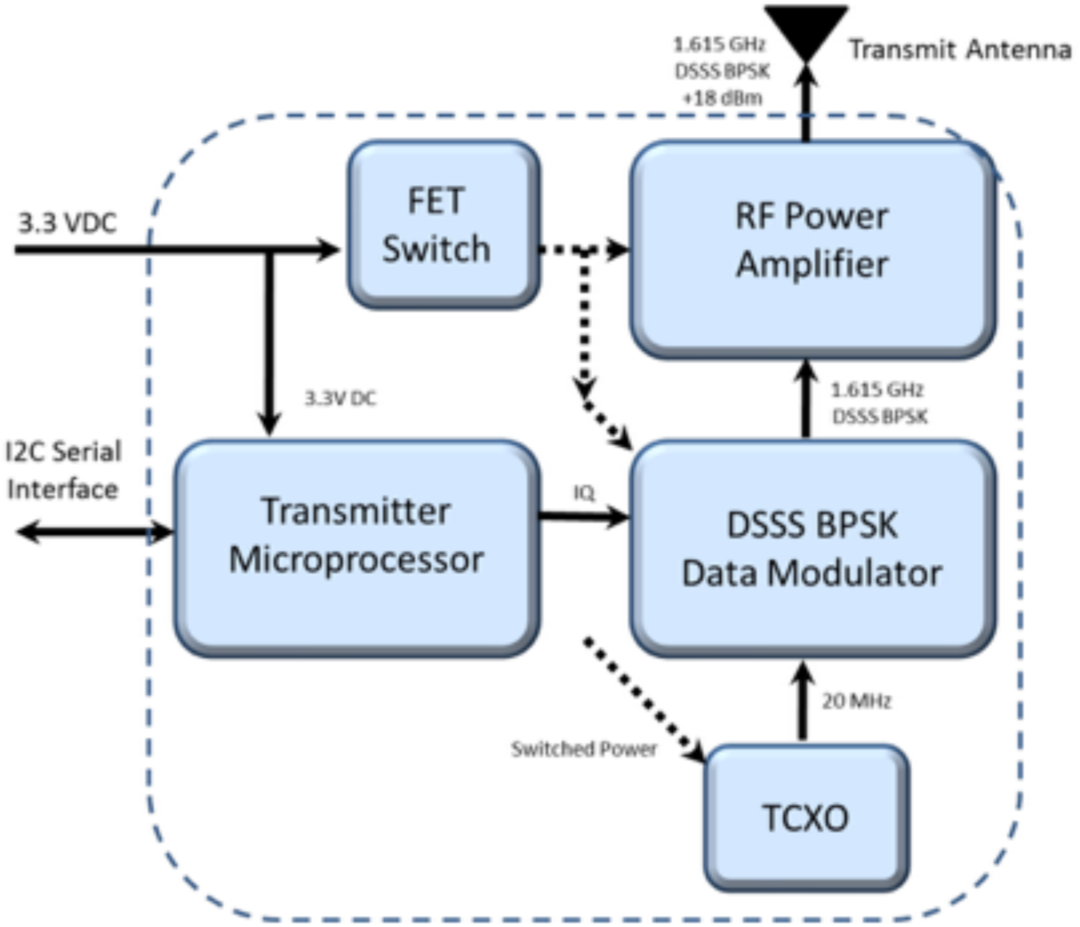


RF Channel
Channel A = 1611.25 MHz center frequency
Channel B = 1613.75 MHz center frequency
Channel C = 1616.25 MHz center frequency
Channel D = 1618.75 MHz center frequency

STX-3

Worlds’ smallest and lowest power consuming industrial-use satellite transmitter





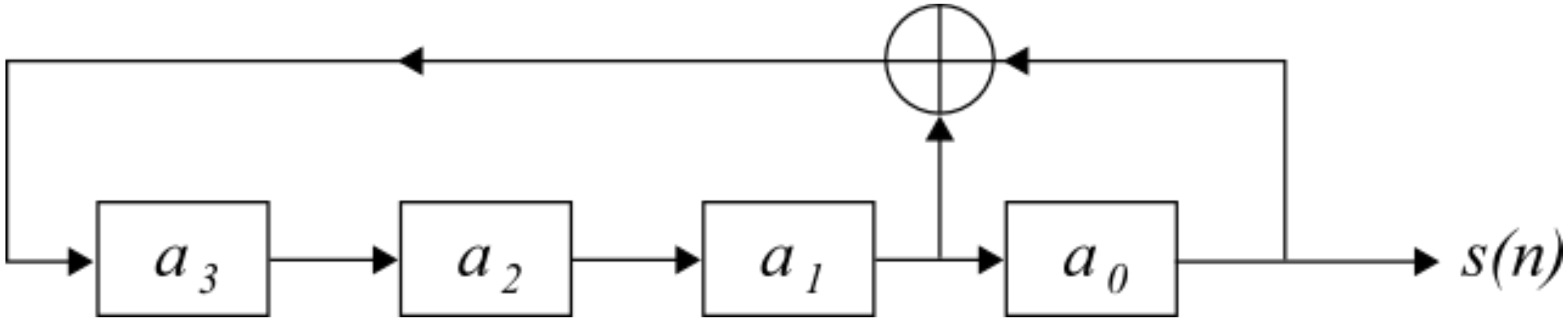
Intelligence Gathering

- Google
- FCC Database
- Academic Papers
- Integrator Spec Sheets

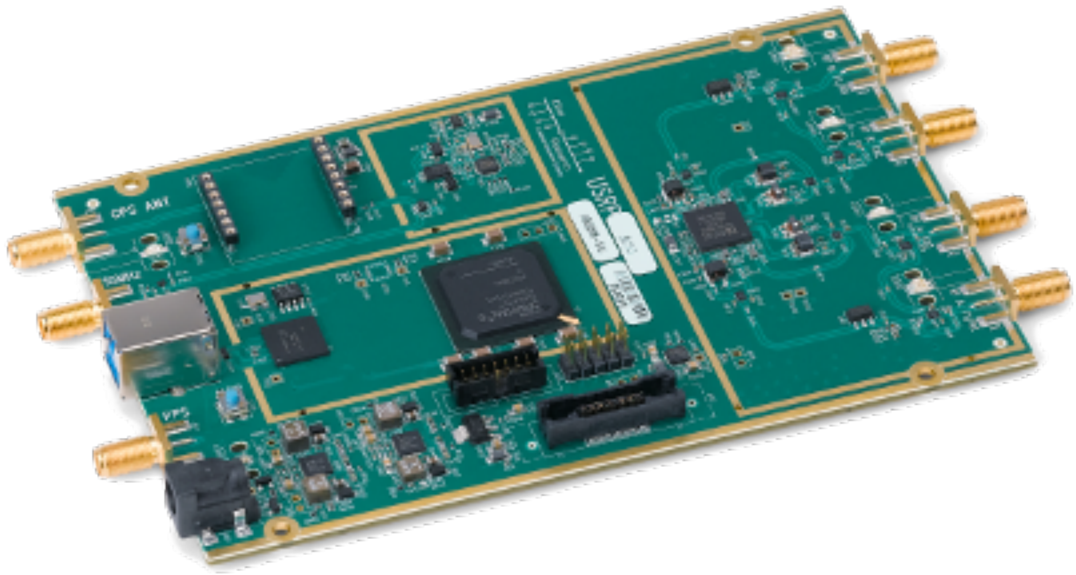
Intelligence Gathering Continue

- 1.61125 ghz
- 100 bit/second BPSK signal
- Spread using 255 Chip M-Sequence
- 144 bit message

M-Sequences and PN Codes



Hardware and Validation



- USRP B200
- GQRX and GNURADIO

GNURadio

THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

Antennas

- Left Hand Circular Polarized

Decoding Theory

- Simple in practice. More difficult in theory
- Re-Mix signal with PN sequence and the BPSK signal will drop out.
- Signal needs to be aligned with PN code
- Compensate for frequency differential between local and remote oscillators

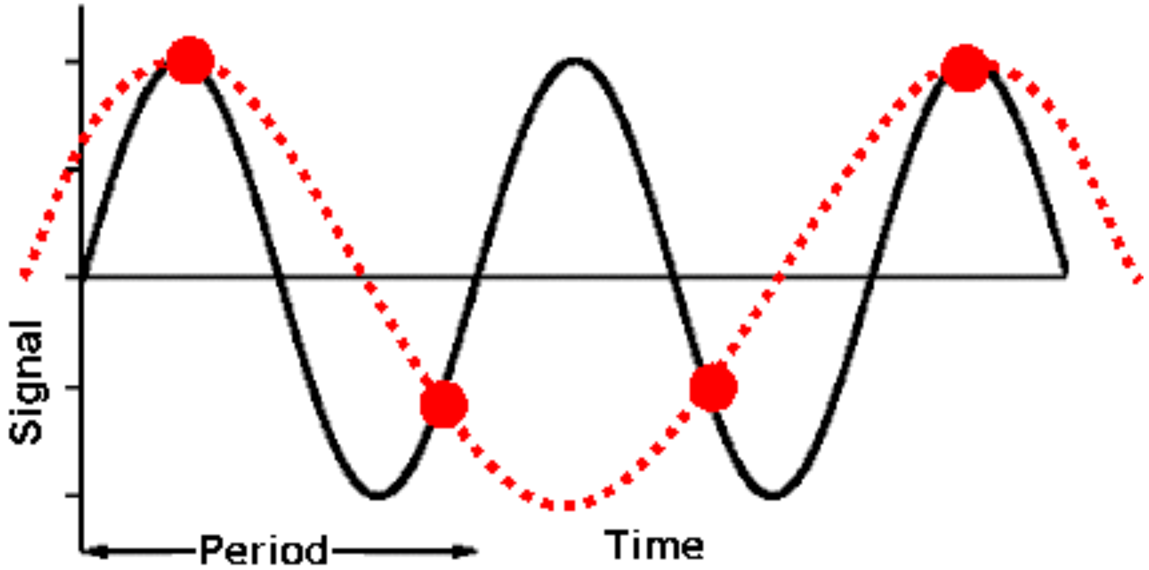
Decoding / PN Recovery

- Remember that BPSK spread with DSSS == faster BPSK
- PN Sequence is much shorter than bit length (49x)
- Since PN is repeats for each bit
- PN xor Data == PN

Decoding Continued

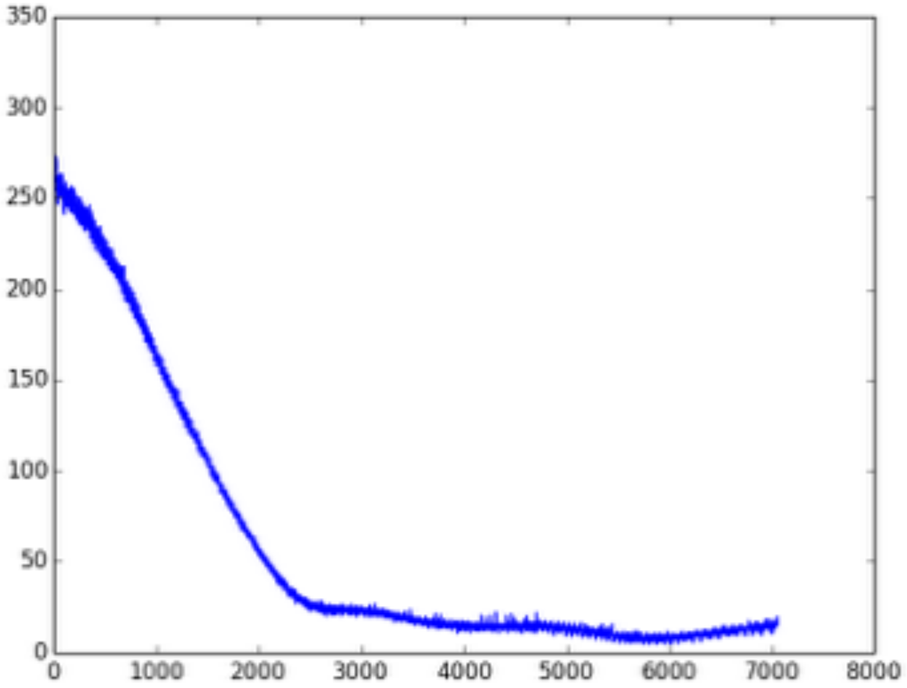
- Shortcut: Decode DSSS as BPSK
- We receive none of the processing gain, but its perfectly legitimate.

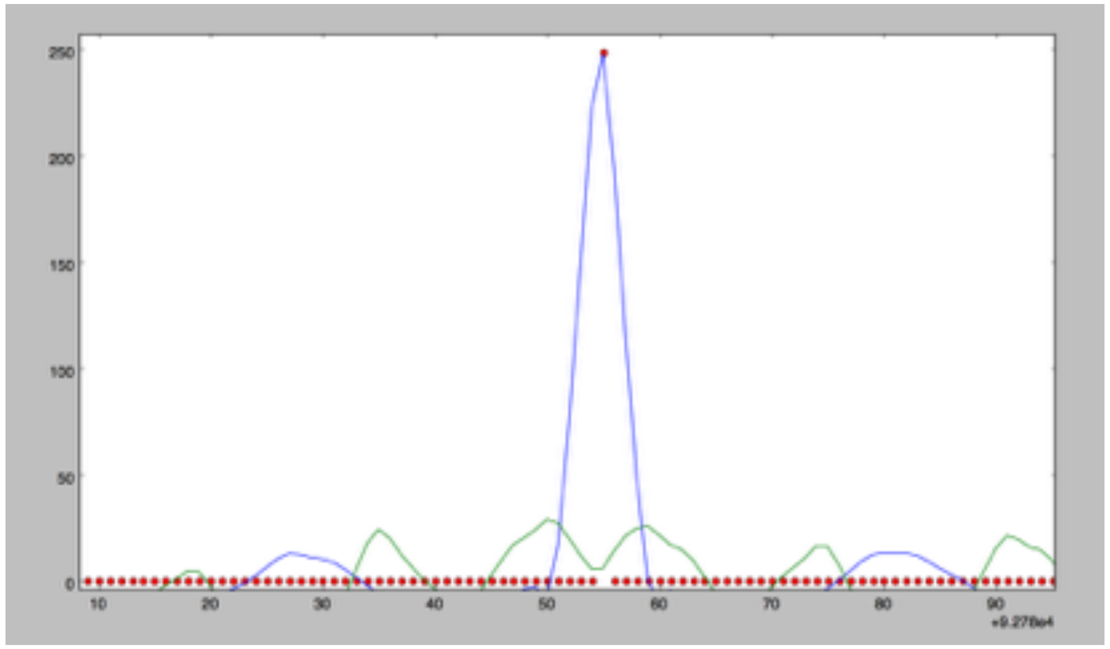
Sampling

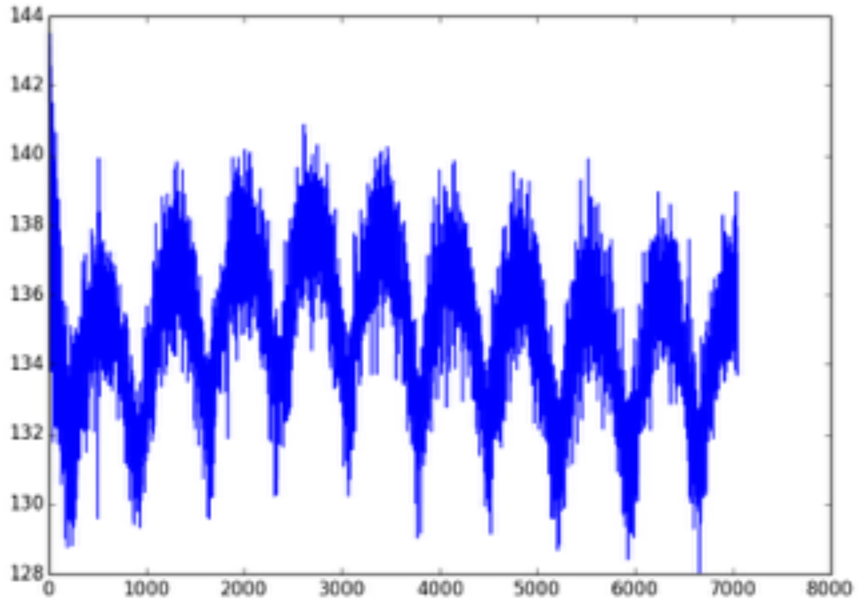


- Nyquist Theorem
- Sampling Requirements:
  - > 2x faster than 1.25 mhz
  - Even multiple of 32mhz
  - Even samples / symbol

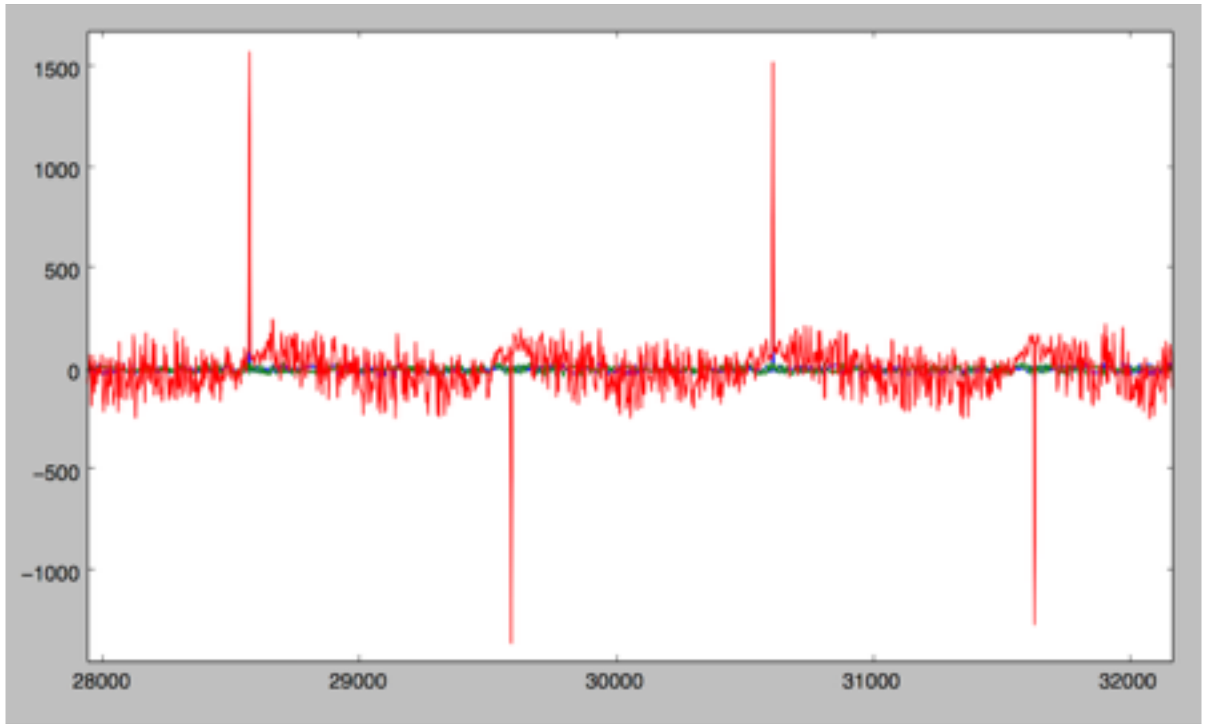
Code Tracking

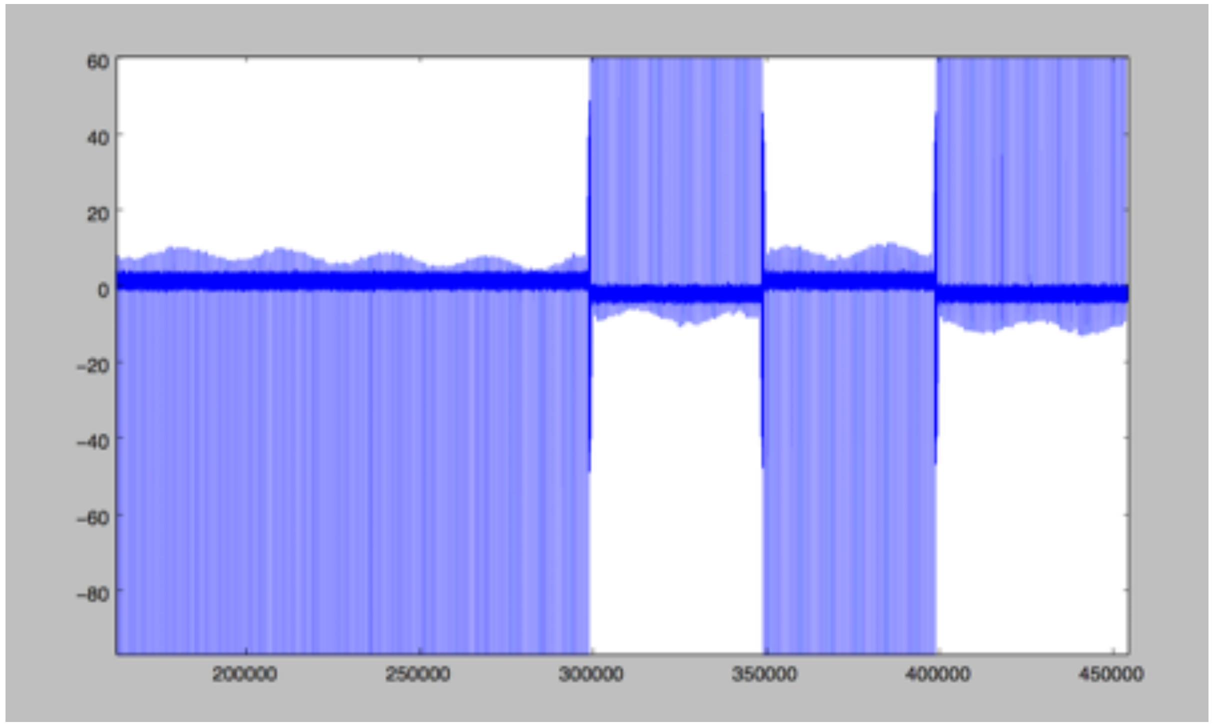


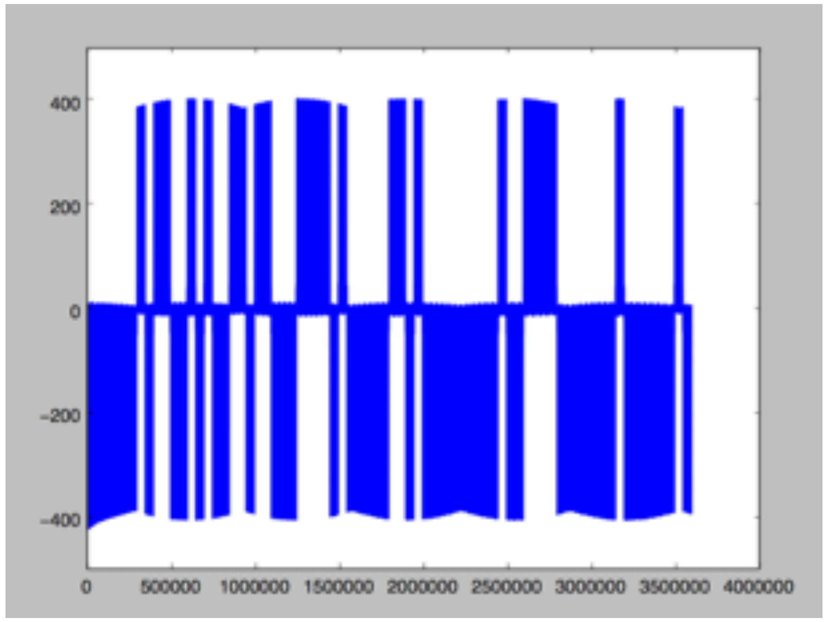




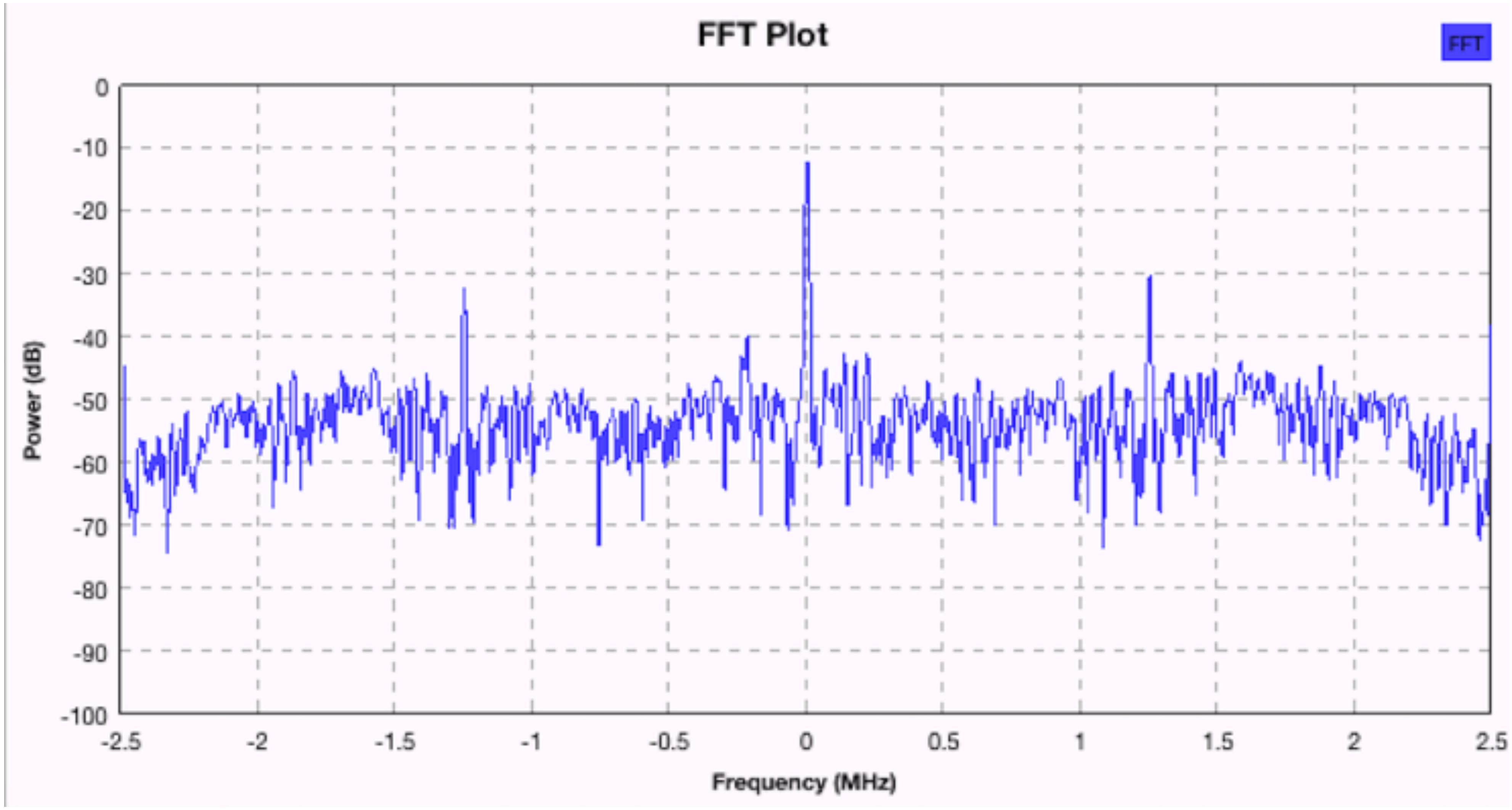
Code Tracking Cont.



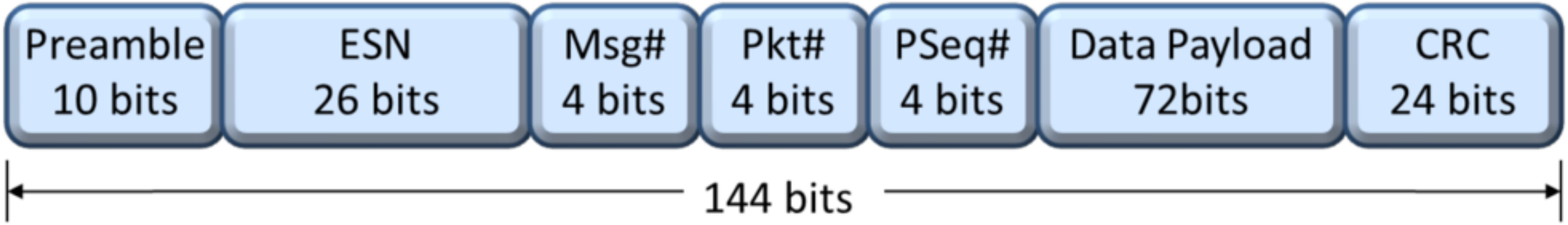




Despread Signal



Packet Format



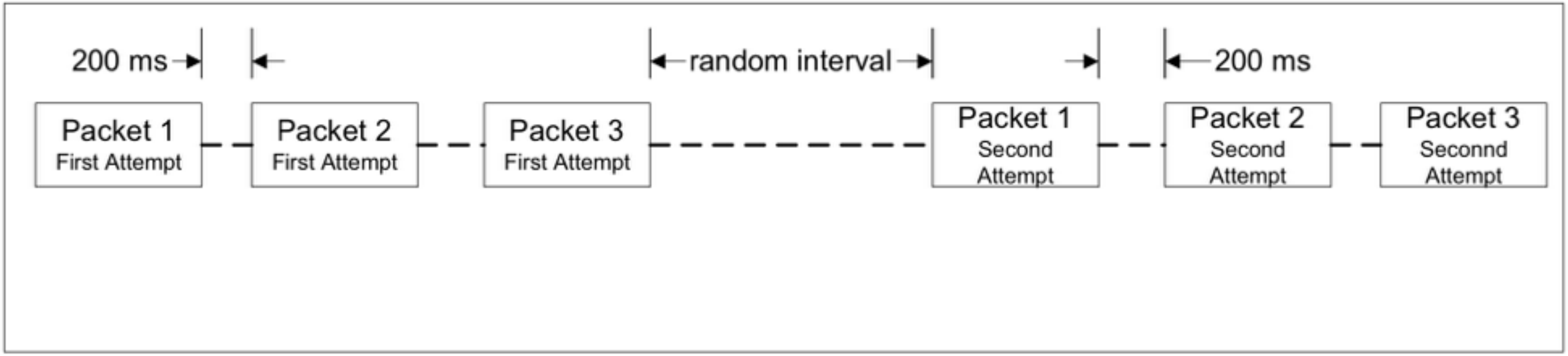
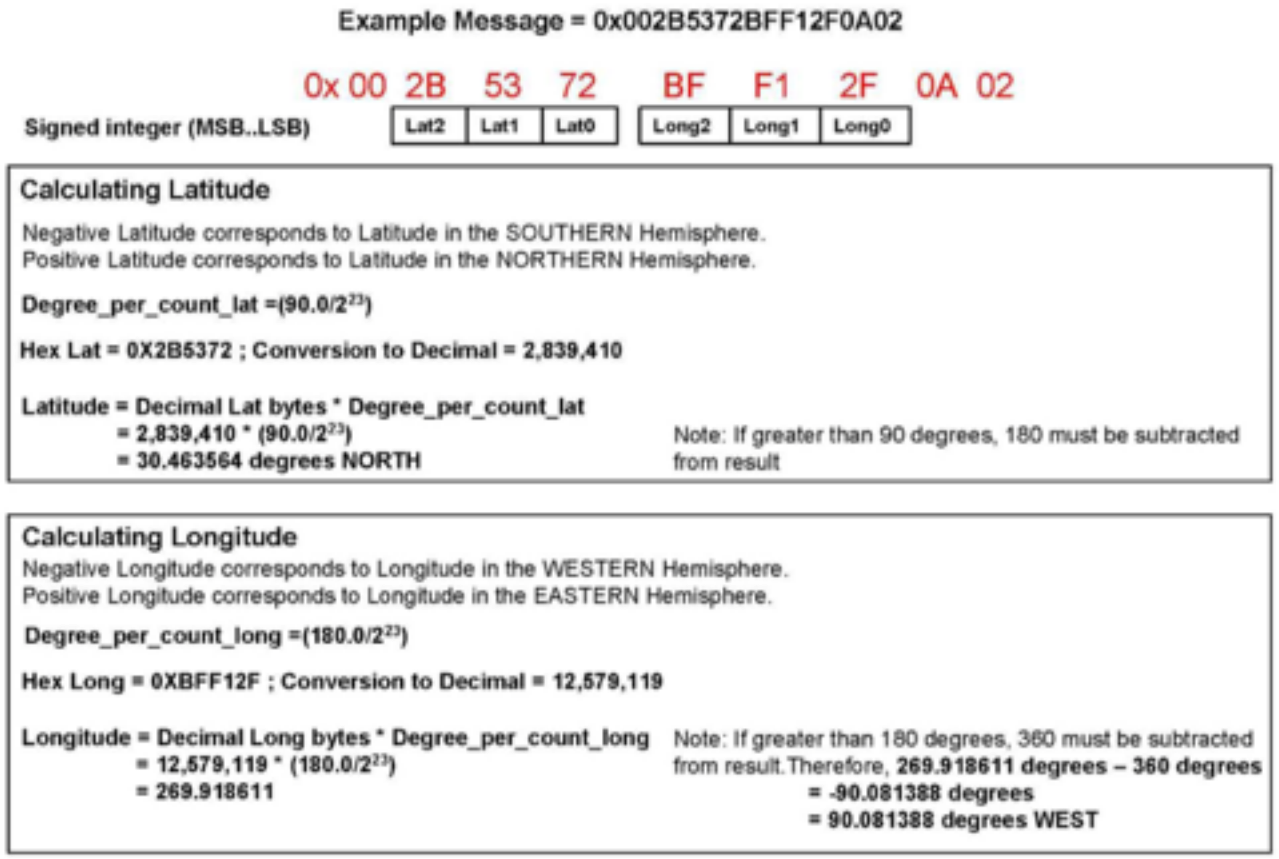


Figure 5, Packet On-Air Redundancy

Packet Format Contd.

- There is no signing, no encryption
- We can create packets if we known how to reproduce the checksum
- Reverse engineering the checksum

Message Decoding



Example Message = 0x002B5372BFF12F0A02

0x 00 2B 53 72 BF F1 2F 0A 02

Signed integer (MSB..LSB) | Lat2 | Lat1 | Lat0 | Long2 | Long1 | Long0

Calculating Latitude

Negative Latitude corresponds to Latitude in the SOUTHERN Hemisphere.
Positive Latitude corresponds to Latitude in the NORTHERN Hemisphere.

Degree_per_count_lat =(90.0/2^{23})

Hex Lat = 0X2B5372 ; Conversion to Decimal = 2,839,410

Latitude = Decimal Lat bytes * Degree_per_count_lat
= 2,839,410 * (90.0/2^{23})
= 30.463564 degrees NORTH

Note: If greater than 90 degrees, 180 must be subtracted from result

Calculating Longitude

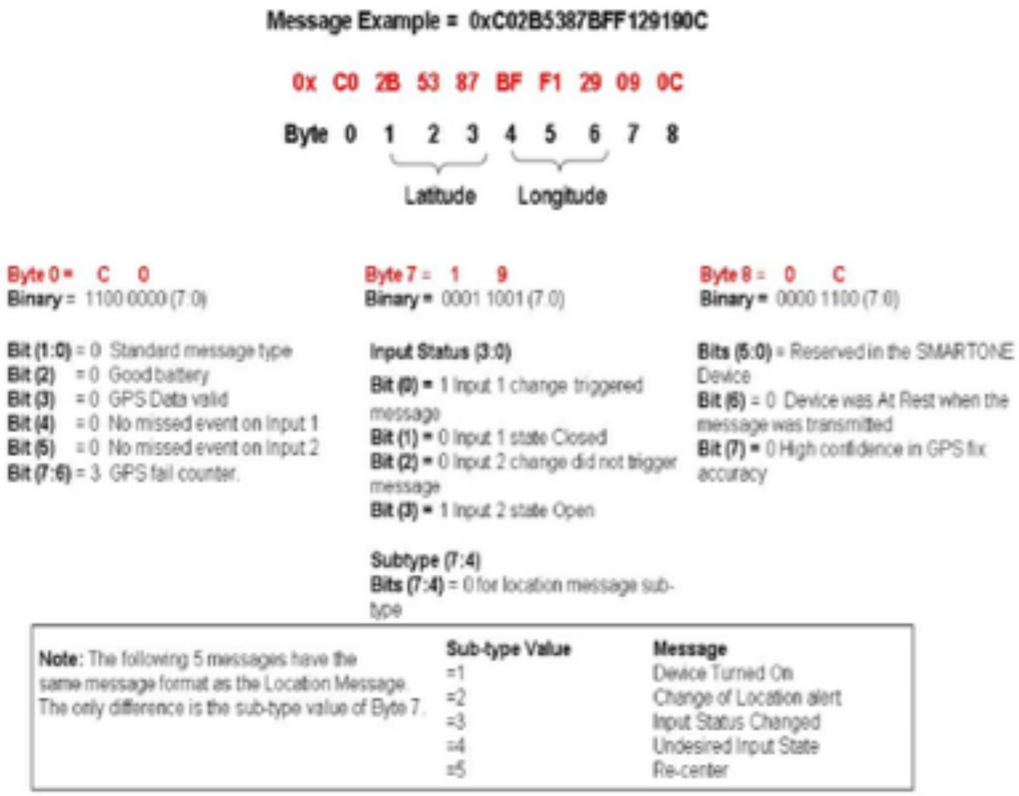
Negative Longitude corresponds to Longitude in the WESTERN Hemisphere.
Positive Longitude corresponds to Longitude in the EASTERN Hemisphere.

Degree_per_count_long =(180.0/2^{23})

Hex Long = 0XBFF12F ; Conversion to Decimal = 12,579,119

Longitude = Decimal Long bytes * Degree_per_count_long
= 12,579,119 * (180.0/2^{23})
= 269.918611

Note: If greater than 180 degrees, 360 must be subtracted from result. Therefore, **269.918611 degrees – 360 degrees**
= -90.081388 degrees
= 90.081388 degrees WEST



Message Example = 0xC02B5387BFF129190C

0x C0 2B 53 87 BF F1 29 09 0C

Byte 0 1 2 3 4 5 6 7 8

Latitude
Longitude

Byte 0 = C 0
Binary = 1100 0000 (7:0)

Bit (1:0) = 0 Standard message type
Bit (2) = 0 Good battery
Bit (3) = 0 GPS Data valid
Bit (4) = 0 No missed event on Input 1
Bit (5) = 0 No missed event on Input 2
Bit (7:6) = 3 GPS fail counter.

Byte 7 = 1 9
Binary = 0001 1001 (7:0)

Input Status (3:0)
Bit (0) = 1 Input 1 change triggered message
Bit (1) = 0 Input 1 state Closed
Bit (2) = 0 Input 2 change did not trigger message
Bit (3) = 1 Input 2 state Open

Subtype (7:4)
Bits (7:4) = 0 for location message sub-type

Byte 8 = 0 C
Binary = 0000 1100 (7:0)

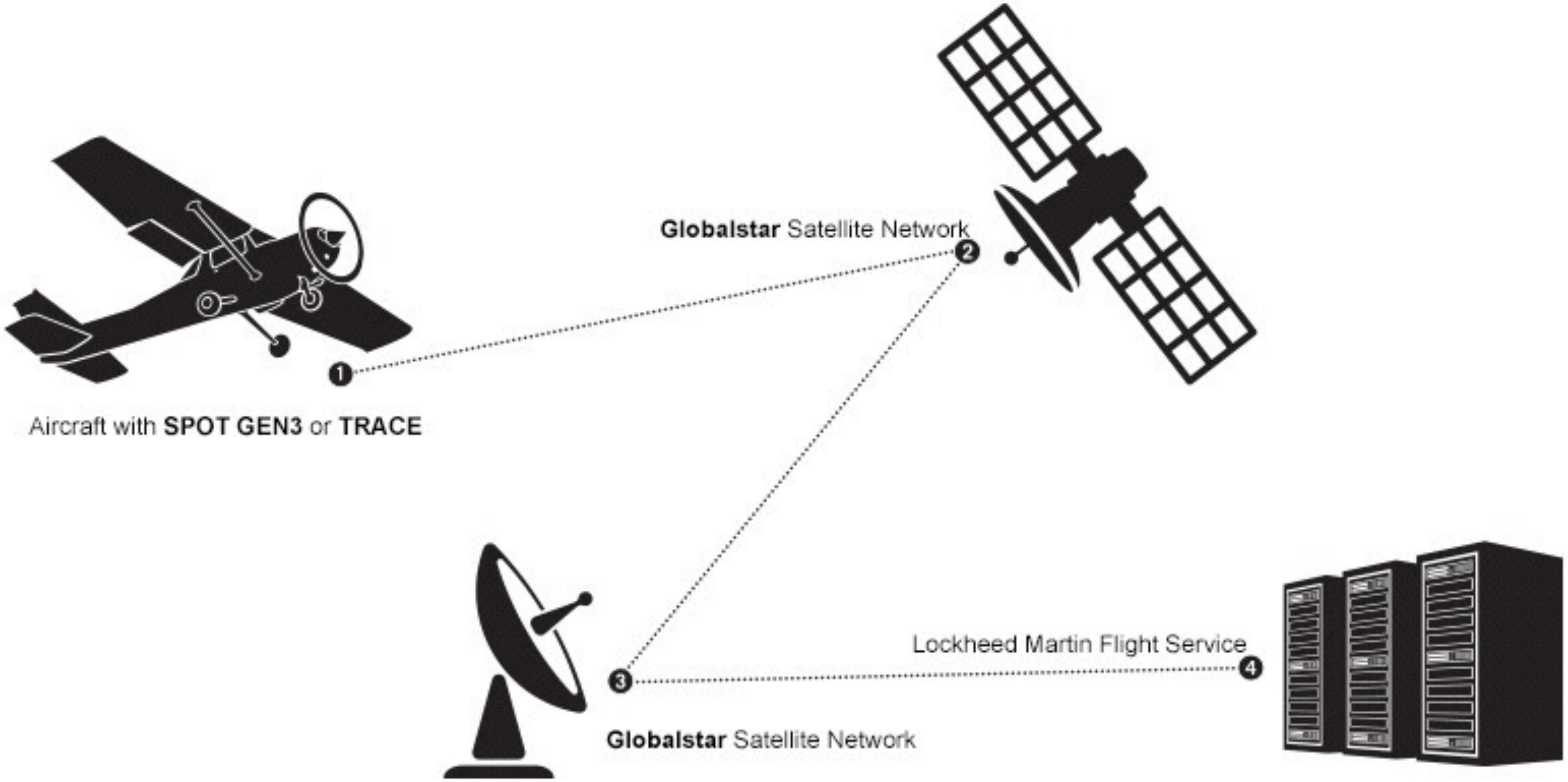
Bits (5:0) = Reserved in the SMARTONE Device
Bit (6) = 0 Device was At Rest when the message was transmitted
Bit (7) = 0 High confidence in GPS fix accuracy

Note: The following 5 messages have the same message format as the Location Message. The only difference is the sub-type value of Byte 7.

Sub-type Value	Message
=1	Device Turned On
=2	Change of Location alert
=3	Input Status Changed
=4	Undesired Input State
=5	Re-center

Video Demo

But Wait, There's More


Aircraft with **SPOT GEN3** or **TRACE**
1
Globalstar Satellite Network
2
Globalstar Satellite Network
3
Lockheed Martin Flight Service
4

Questions?

Images

https://upload.wikimedia.org/wikipedia/commons/9/99/Lfsr.gif

http://www.mccauslandcenter.sc.edu/CRNL/wp-content/upLoads/nyquist.png

https://awrcorp.com/download/faq/english/questions/images/iq_mod_dmod.png

http://ironbark.xtelco.com.au/subjects/DC/lectures/7/

http://www.mdpi.com/sensors/sensors-14-03172/article_deploy/html/images/sensors-14-03172f5-1024.png

https://www.tapr.org/images/ssfig1.gif