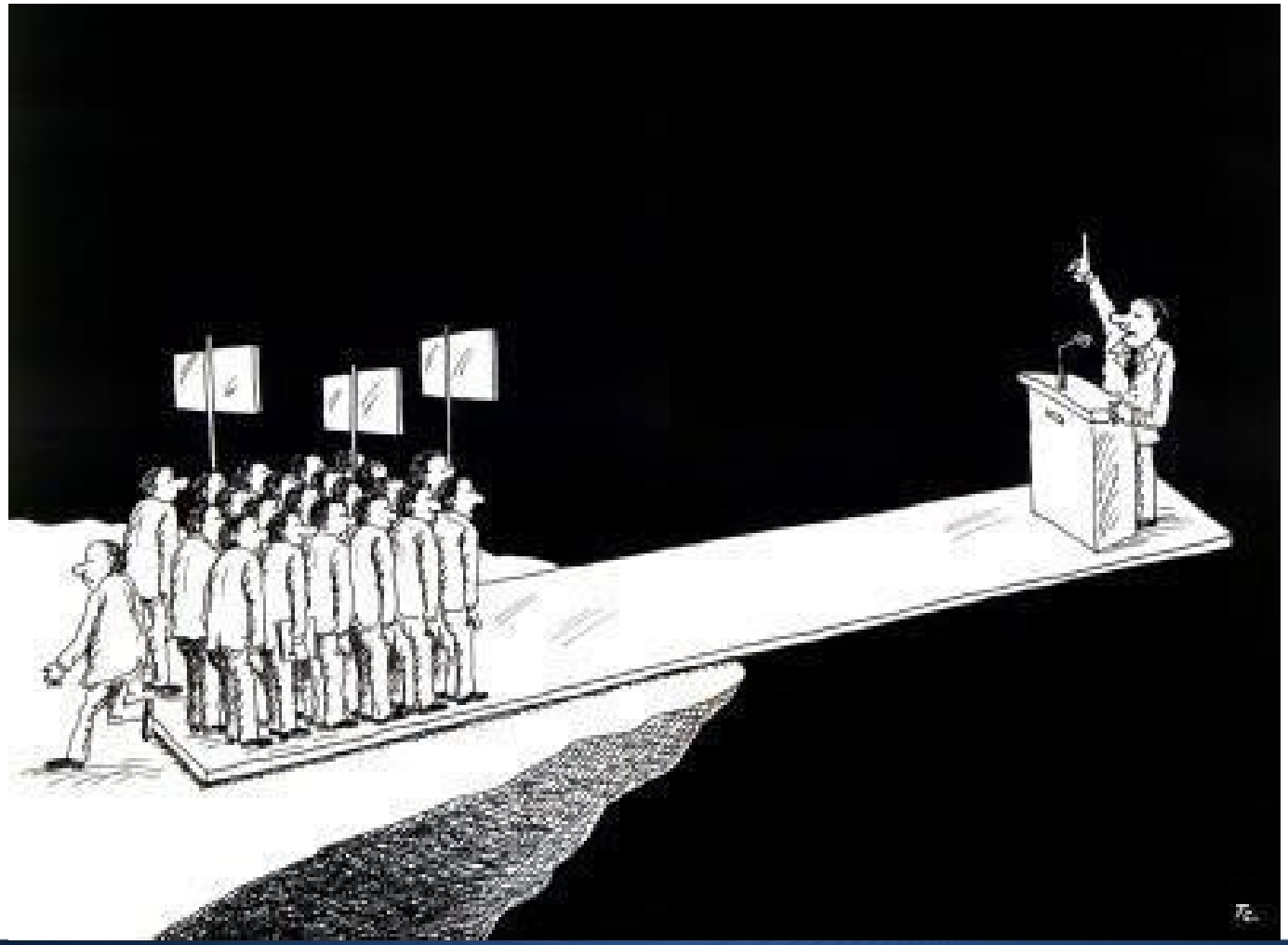
SIGINT and Practical Covert Communication

Resistance is NOT futile



Why Develop Open Covert Communications?

- As an enabler to privacy and liberty
  - Circumvent government restrictions and targeting
  - Political groups, NGOs, demonstrations, war and insurrections
  - Journalists (Marie Colvin)
- Wireless Warrior: a WW II Allied underground radio operator
- Disaster communications
  - Friends and Family
- Affordable/fee-free
- An untapped market: What the intelligence community has today the rich will want tomorrow and attendees here will want too

Why Wireless?

- Infrastructure-less use
- Local, regional and even international links
- Mobility
- No fees

Why NOT wireless?

- Link reliability
- Software immaturity
- Specialized, often non-miniature, antennas
- Only low-speed may be covert
- Equipment cost
- May not be locally legal

Covert Focus

- Low Probability of Detection/Intercept (LPD/LPI)
- Most reliably implemented at the radio/PHY level

Pros

- No more identifiers available as all transmitted bits obfuscated
- No correlations between requests and replies
- Location privacy

Cons

- Development requires deep understanding of radio and signal processing
- Assuring covertness is a multidimensional problem that cannot be solved only by technology
- Covertness failure may be difficult/impossible to detect

What is Covert Communications

- Covert channels
  - Messages hidden within ordinary data (similar to steganography)
  - Which are never intended for information exchange
  - And can be used to hide encrypted communication
- Signals-based
  - Modulation
  - Coding
  - Directivity (e.g., antenna pattern)
- A complement to encryption which is often used in tandem

SDR and Gnu Radio Changed Everything

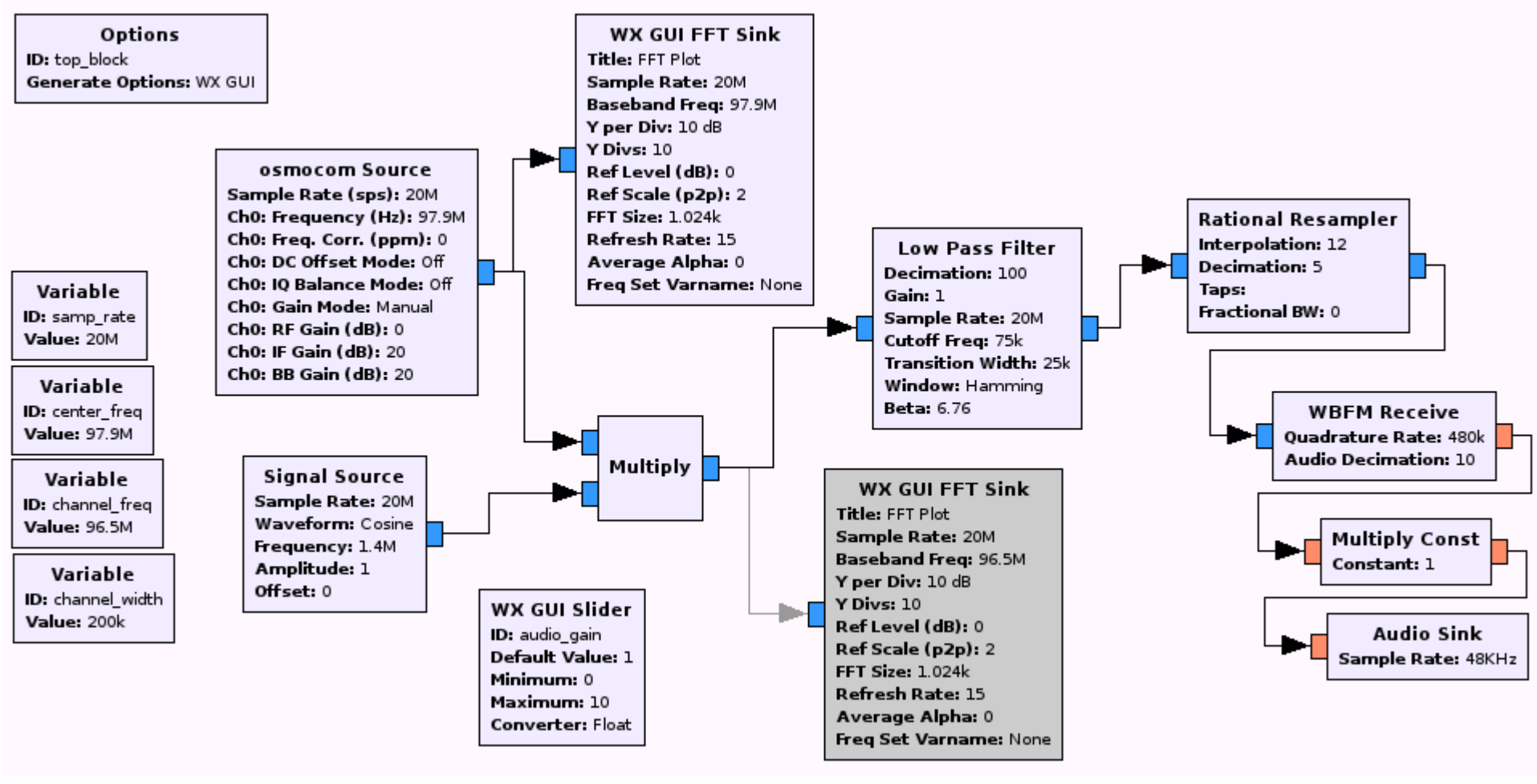
- Before SDR radio design only for large entities and RF engineers
- First SDRs were expensive commercial and proprietary
- Gnu Radio, created to make FOSS radio practical and affordable, is now mature
- Special signal capture and generator devices make SDR practical

- Popular SDR capturers
  - RTL DVB dongles ~$20 USD
  - FunCube Ham LF-UHF
- Popular SDR captuerers and signal generators, (e.g., HackRF One, BladeRF and USRP)
- Needed: flexible COTS transceiver configurations outside of Ham frequencies and bandwidths

Gnu Radio

- Free & open-source toolkit
  - (GPL) version 3
- Signal processing blocks to implement software radios
  - With low-cost external RF hardware or in a simulation environment
- Mature: widely used in hobbyist, academic and commercial environments
- C++ and Python APIs
- For computation intensive parts C++/VOLK = (vector-optimized library of kernels)
- GR Companion: GUI IDE for prototyping applications

Gnu Radio Companion Example: FM Receiver



HackRF One

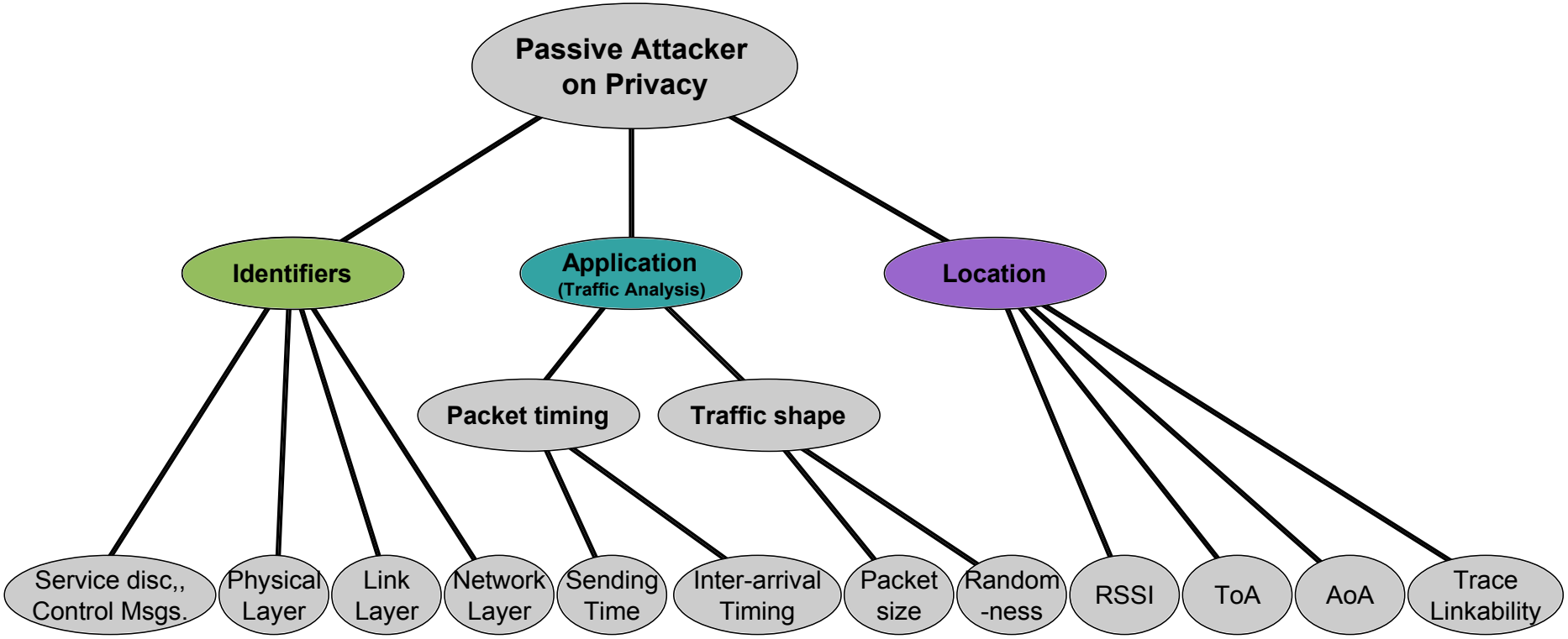
- ~1 MHz to 6 GHz coverage
- Half-duplex transceiver
- Up to 20 MSPs
- Nominal 10 mW transmitter
- **8-bit quadrature samples I/Q**
- Compatible with GNU Radio, SDR#, and more
- Software-configurable RX and TX gain and baseband filter
- Powered antenna port
- USB peripheral or stand-alone
- Clock input and output for synchronization
- Programmable buttons
- Internal pin headers for expansion (e.g.,up to 16-bit A/D or FPGA)
- Hi-Speed USB 2.0 powered
- Open source firmware and hardware

SIGINT/Electronic Warfare Threats

- Passive
  - Signal analysis
    - Type, frequency, bandwidth, etc.
    - Where - Location Privacy?
  - Traffic Analysis
    - Who's communicating with whom?
    - When is someone communicating?
  - Eavesdropping
    - What is the content of their communication?
- Active
  - Probably means you are targeted!
  - Jammers
    - Block Communications
    - Force Insecure Reversion
  - Man-in-the-Middle
  - Black-bag intrusion

Passive Threats

- Many potential privacy leaks of wireless communication protocols for a passive attacker

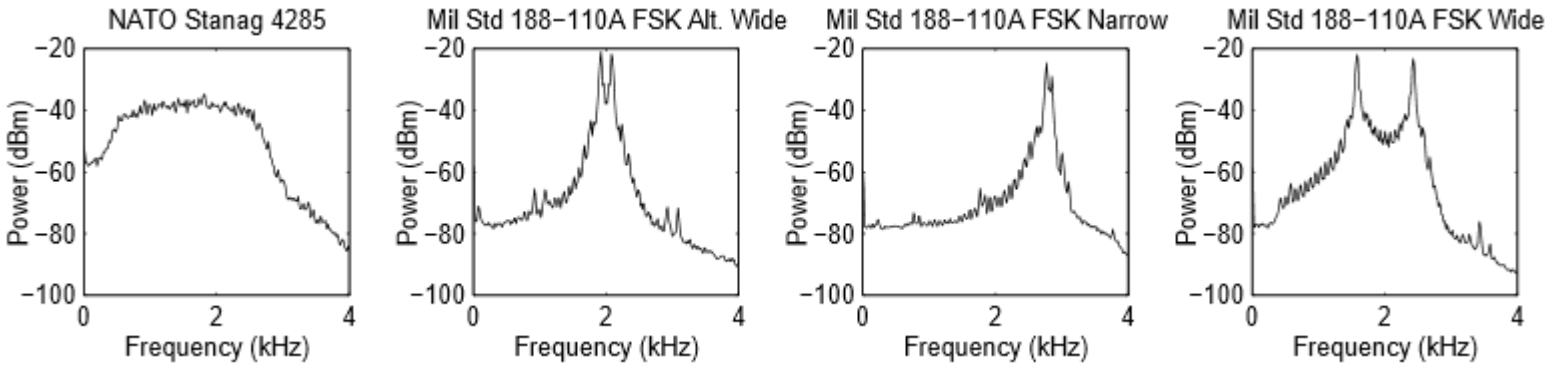


Signal Features Targeted

- Common emission sources and types
  - Frequency, location, time and (if possible) content
- Red October Crawler/Seismic scenario
  - Unusual modulation/coding
  - Transmitter physical layer fingerprinting
  - Code/symbol rate signatures

Signal Tech They Are Using

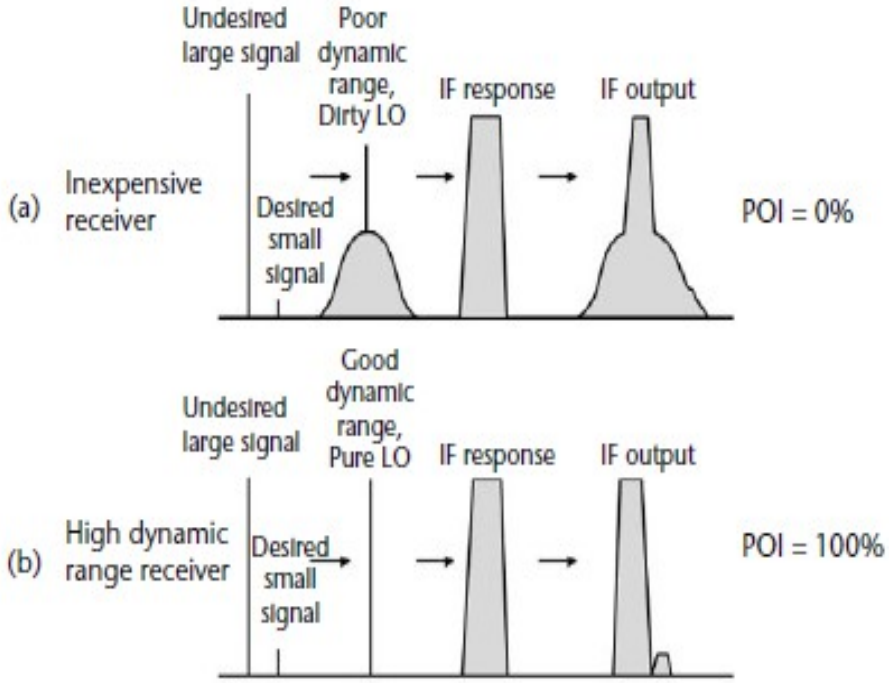
- Feature Extraction
  - Instantaneous amplitude
  - Phase variance
  - Spectral symmetry
  - Transmission models
  - Higher order statistics
- Classification association
  - Threshold detection
  - Artificial neural networks
  - Pattern recognition algorithms



High Probability Of Intercept (HPOI) Receivers

- Purpose: Capture as much RF spectrum as quickly as possible with the highest frequency resolution and dynamic range.
- Probability of Intercept (POI) % = probability to detect, process, and identify an emitter within a specified time

- Example
  - A weak CW signal hidden in the side-bands of a strong signal and close frequency

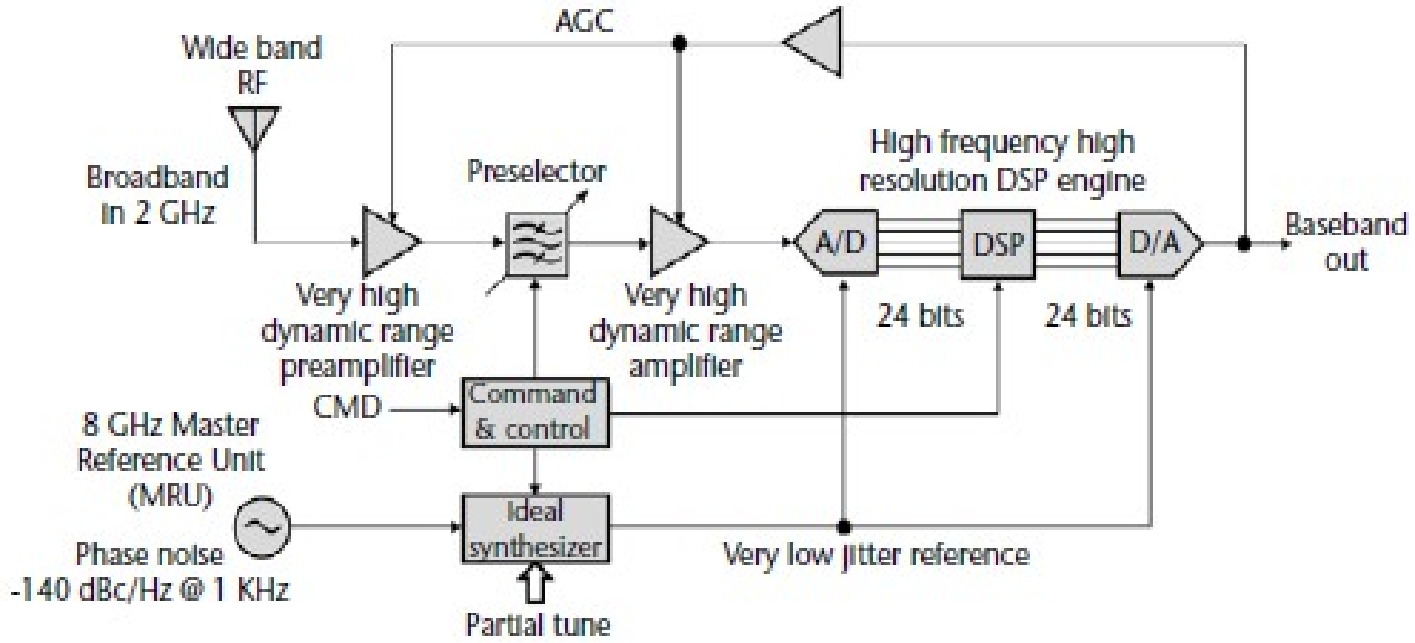


POI Factors

- A priori signal knowledge
  - **Prevention is key to covert**
  - Frequency and modulation
  - Probable location
  - Bandwidth and coding
  - Transmission time(s)
  - Repetition rate
  - Antenna (e.g., pattern)
- HPOI design elements
  - Dynamic range
  - LO and synthesizer quality
  - Noise figure & Compression points
- Capture likelihood
  - Emitter's vs. receiver's beam width
  - Emitter pulse width
  - Instantaneous bandwidth
  - Receiver sensitivity, resolution, dwell time, scan time
  - SIGINT system throughput
  - Reaction time constraints
  - Emitter parameter validation
  - Channel conditions (e.g., number of emitters/Hz &QRM)

HPOI Designs

- Ideal HPOI Receiver
  - SDR on steroids
  - Cognitive radio: recognize & adapts to received information
  - **Wanted a FOSS HPOI**
- Limitations
  - A/D speed – dynamic range
  - Synthesizers/oscillators
  - Band/channel conditions



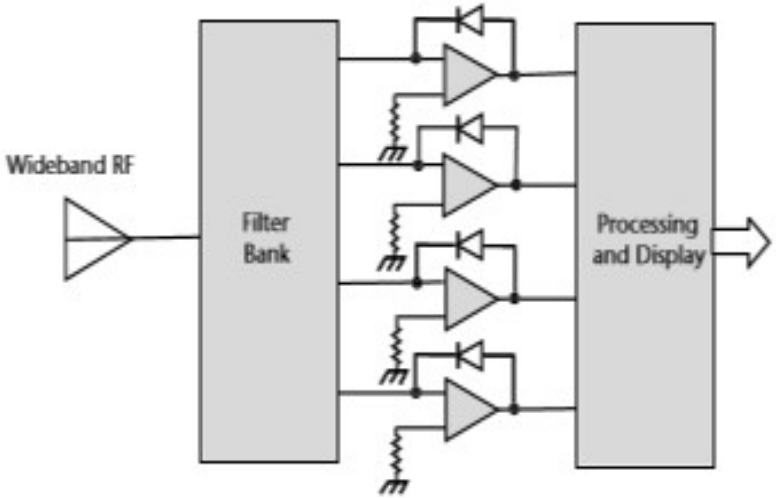
Common SIGINT/Electronic Warfare Receivers

- Crystal video—warning receiver
- Instantaneous frequency measurement (IFM)
- Phase detection—used for direction of arrival
- Ultra-wideband scanning superheterodyne
- Channelized receiver—activity monitor
- Bragg cell—activity monitor
- Combinations of the above

Crystal Video Receiver

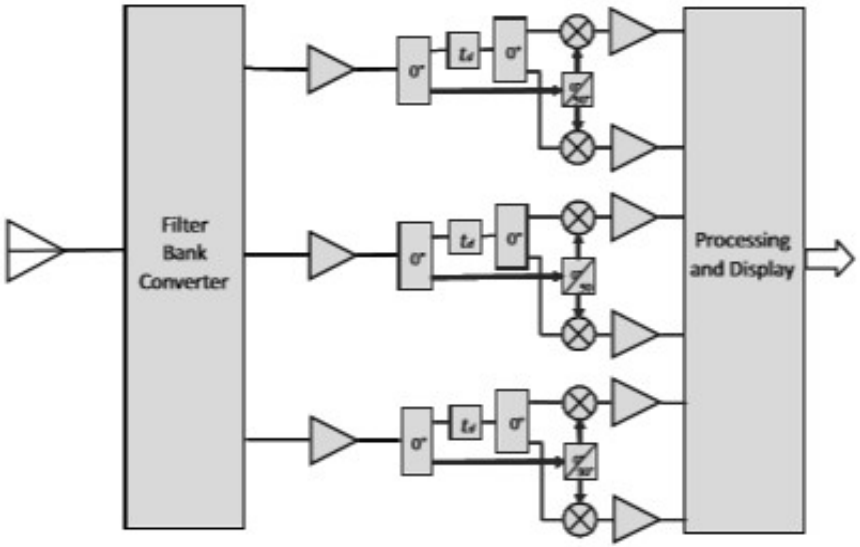
- A form of a tuned radio frequency (TRF) receiver
  - Splits a wide input frequency range into several broad contiguous bands, which are
  - Filtered and logarithmically amplified before detection
- Simplest electronic counter measures (ECM) receiver
- Usually used as warning (police) radar receivers

- Low cost and small but
  - Low sensitivity due to a large noise bandwidth, and
  - Subject to blocking from strong in-band signals.



Instantaneous Frequency Measurement (IFM)

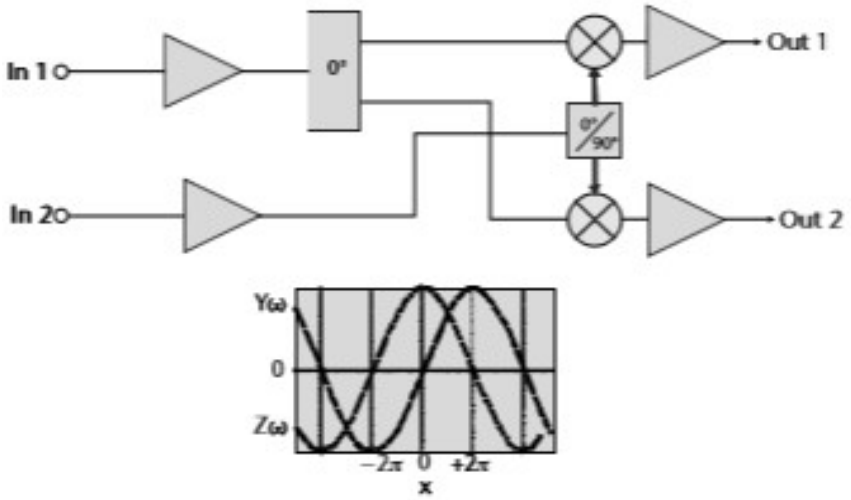
- A more complex form of the TRF receiver, using
  - Bandpass/band reject front-end filters +
  - Delay lines and phase detectors
- Near instantaneous frequency measurement of single pulse signatures
- For jammer quick set-on or
- Acquisition receiver to set up a slower, narrowband, high-resolution receiver



Phase Detection in Interferometer Receivers

- Not strictly considered a type of receiver but
- Important discriminator type used in interferometer receivers
- Used for direction finding

- Typical phase detector arrangement used in an interferometer receiver



Swept Superheterodyne Receivers (SSR)

- Wideband
  - Fast sweeping/hopping wide IF bandwidth receiver
  - FFT directly at the IF and
  - >1 GHz, center frequency, bandpass A/D-DSP
  - Complex auto-switched half-octave front-end filters
- Typical Performance

Total bandwidth	2 to 18 GHz
IF center frequency	1 GHz typical
Front end composite	8 half-octave filter bank
Instantaneous bandwidth	1 GHz typical
Ultimate resolution	Limited by A/D
Linear dynamic range	>100 dB typical
MDS	−110 dBm typical
POI	<100% near instantaneous

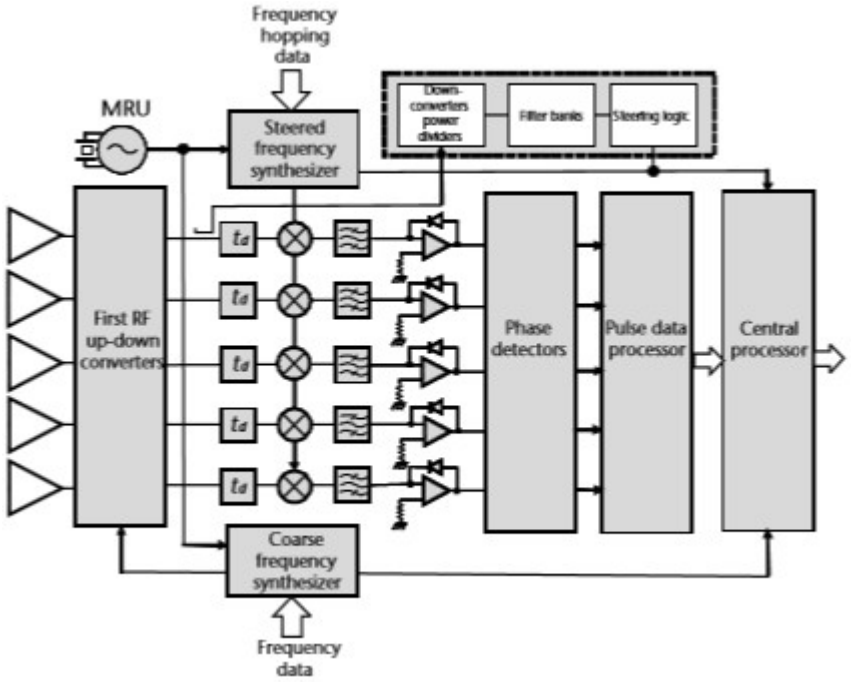
- Narrowband
  - Wideband SSR + narrowband second or third IF sweeping through the first very wide bandwidth IF for increased resolution

Total bandwidth	2 to 20 GHz
Double conversion superheterodyne	First IF: 1.5 GHz typical, second IF: 0.5 GHz typical
Front end composite	7 half-octave filter bank
Instantaneous bandwidth	>0.5 GHz typical
Ultimate resolution	10/100 Hz typical
Linear dynamic range	>130 dB
MDS	−138 dBm typical
POI	<100% not instantaneous

Channelized Receiver (Bulk or Channelizer)

- A multiple superhet
  - Divides the frequency range into contiguous channels
  - Parallel receiver architecture with a wide input bandwidth and multiple narrowband outputs
- Features
  - Wider bandwidths monitored at each coarse frequency step
  - 2-20-GHz band scanned in 36 steps instead of 1,800 steps for a 10-MHz IF bandwidth
  - Reduces scanning time and greatly increases POI

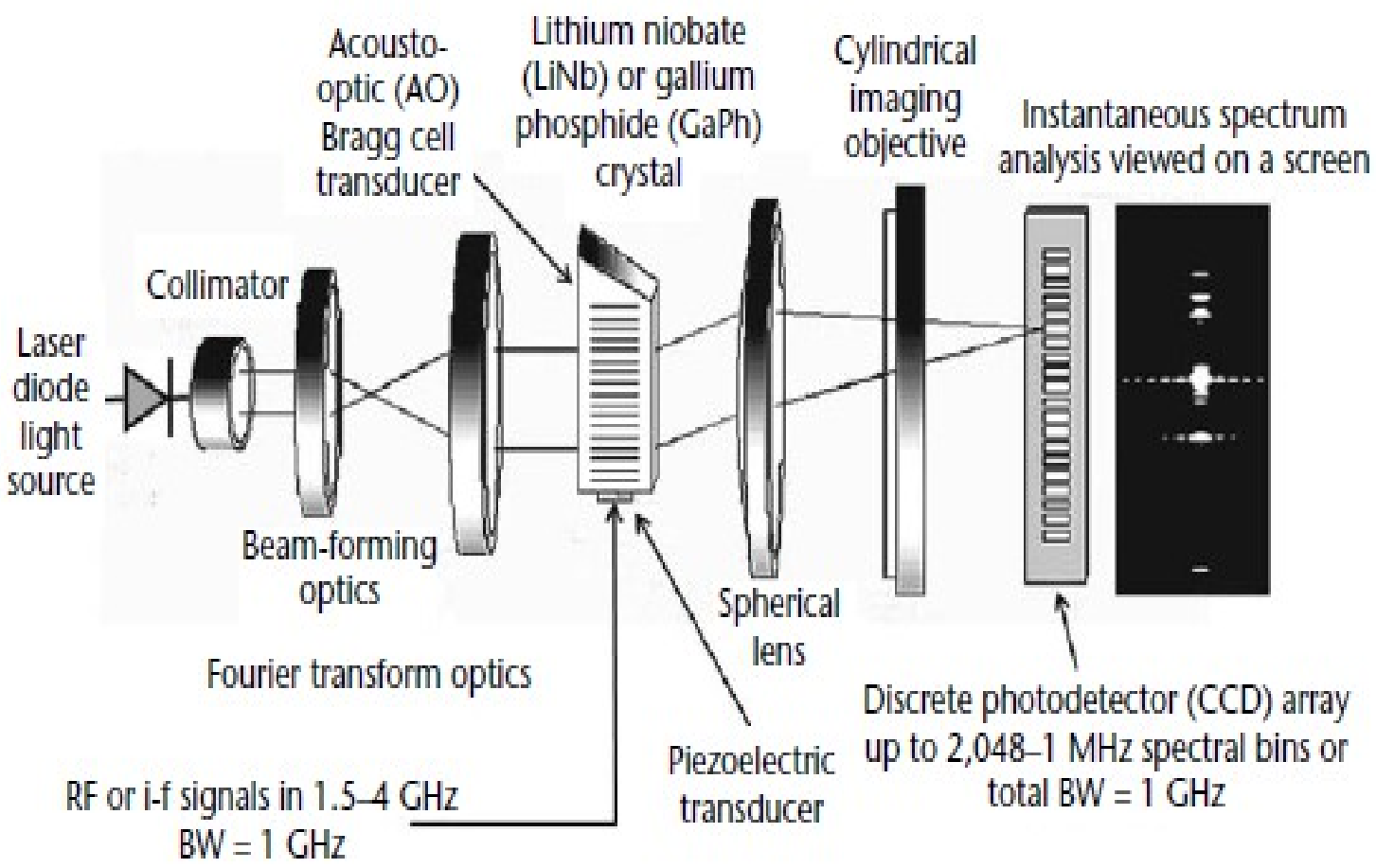
Total bandwidth	2 to 20 GHz
Instantaneous bandwidth	0.5 GHz typical
MDS	−85 dBm typical
Pulse width resolution	100 ns typical
Signal resolution	10 MHz minimum, 30 MHz for a 50-dB signal separation
Frequency accuracy	+/– 2 MHz pulse-to-pulse
Data throughput	1 Mpps
POI	<100%



Bragg Cell Receiver

- Originally from radio astronomy
  - Ultra-wide-band instantaneous receiver
  - Blends RF and photonic technologies (acousto-optic modulator)
  - Can be used to steer much higher resolution receivers, or
  - Replacement for state-of-the art A/D converter technology receivers
- Pros
  - No variable LO required for resolution over the bandwidth of interest
  - Allows high probability of intercept (POI) of many signals at the same time (e.g., crowded band conditions)
- Cons
  - Limited linear spurious-free dynamic range (*may* not very effective against some broadband, very low spectral energy, signals especially under crowded band conditions)

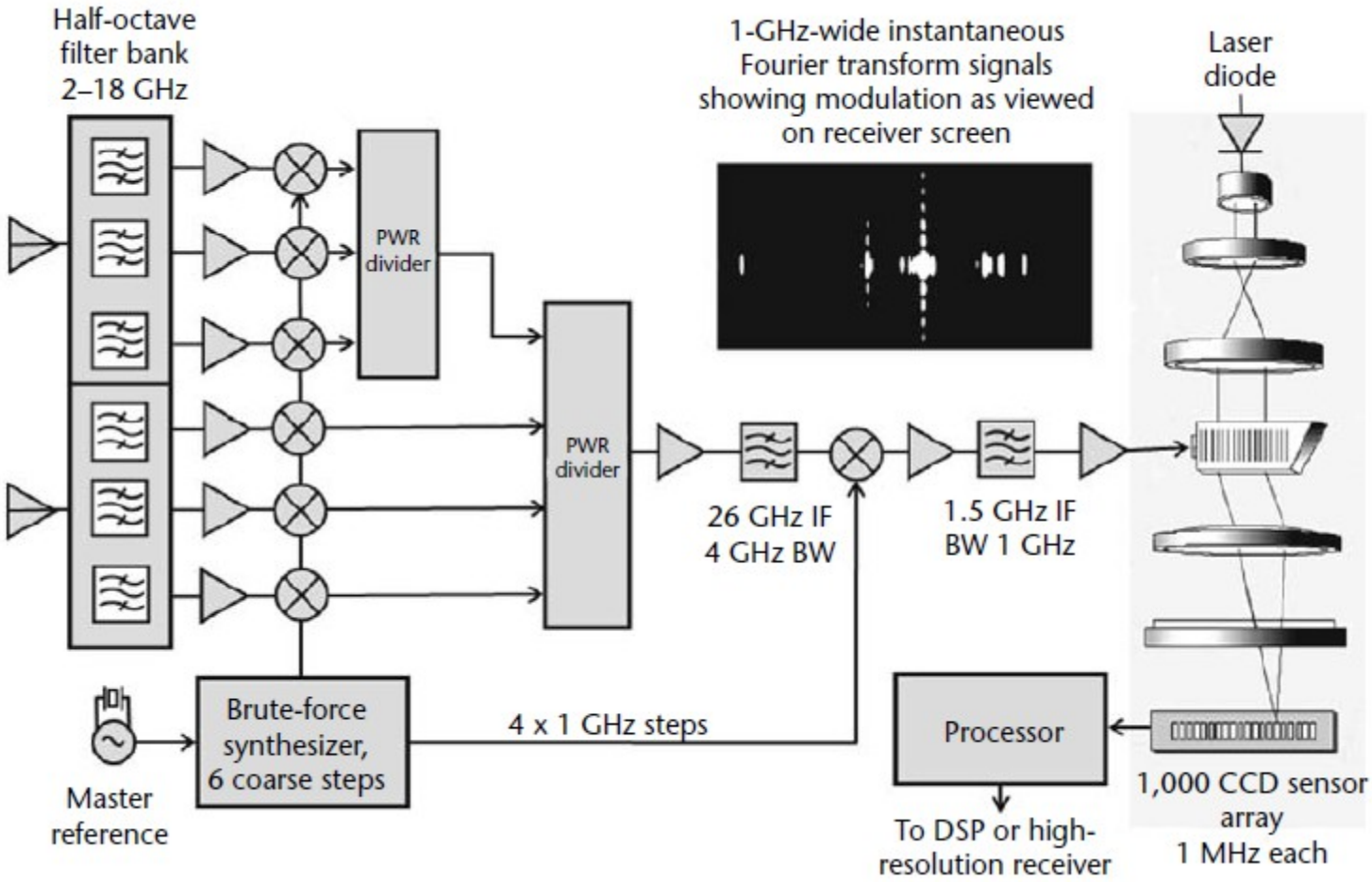
Bragg cell receiver principle



Commercial Bragg Cells

- Single cell (256 frequency spots)
- Bragg cell assembly
  - 16 channels 180 MHz each
  - 1 GHz composite bandwidth
  - 20 spots/channel
  - 2 watts of RF drive/channel
  - Laser wavelength is 355 nm

EW Bragg Cell Receiver



Active Threats

Jammers

- Detecting a jammer is challenging because there exist numerous intelligent jammer strategies
- Either blocks the source from sending packets or the receiver from receiving legitimate packets
- Performance indices/measures
  - JSR (Jammer-to-Signal Ratio)
  - PSR (Packet Send Ratio): creating congestion to cause sender's network interface packet buffer to drop packets
  - PDR (Packet Delivery Ratio)

Jammer Types

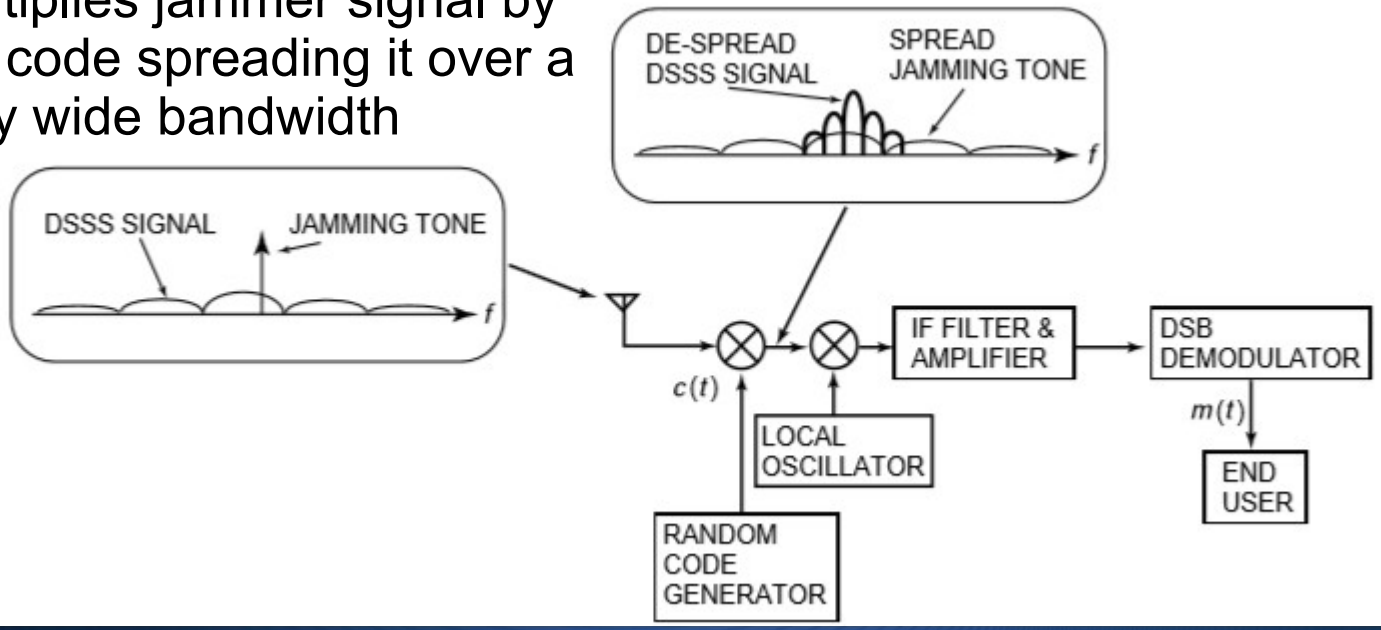
- Repeat-back (Multipath)
  - DSSS largely immune as autocorrelation of spreading code typically very small for time delays greater than one chip time
- Partial-band
- Broadband
  - Additive White Gaussian Noise (AWGN)
- Multitone
- Pulse
- Packet jammer
  - Sends initiation data packets in a loop to capture receiver's state machine

Digital RF Memory (DRFM)

- Digitally capture and re-transmit an RF signal
- Used with channelized HPOI receivers for jamming

CW and Multitone Jammers

- DSSS has relative immunity
  - Despreading mixer collapses the DSSS signal back to a narrowband signal
  - Multiplies jammer signal by PN code spreading it over a very wide bandwidth
- Majority of jammer signal will fall well outside the passband of the IF filters, significantly decreasing the JSR at the demodulator



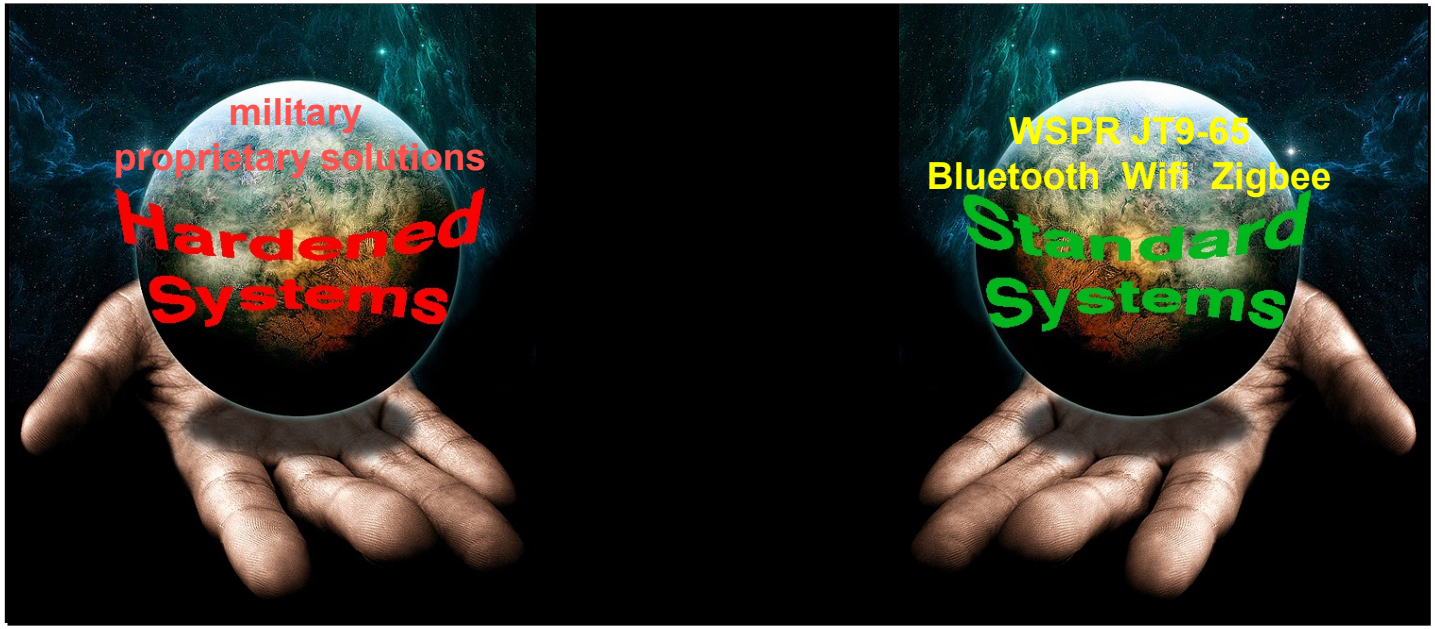
Fortune Favors the Prepared

- Intel agencies have huge resources & experience
- But monitoring all wireless communications is still a Sisyphean task
- Defenders must counter all exploits, attacker must only find one and exploit: works for intel and adversaries
- Physics and HPOI receiver constraints are like Zero-Days that cannot be fixed
- Unless targeted, those using good covert communications and trade-craft, are in minimal danger

Good OPSEC

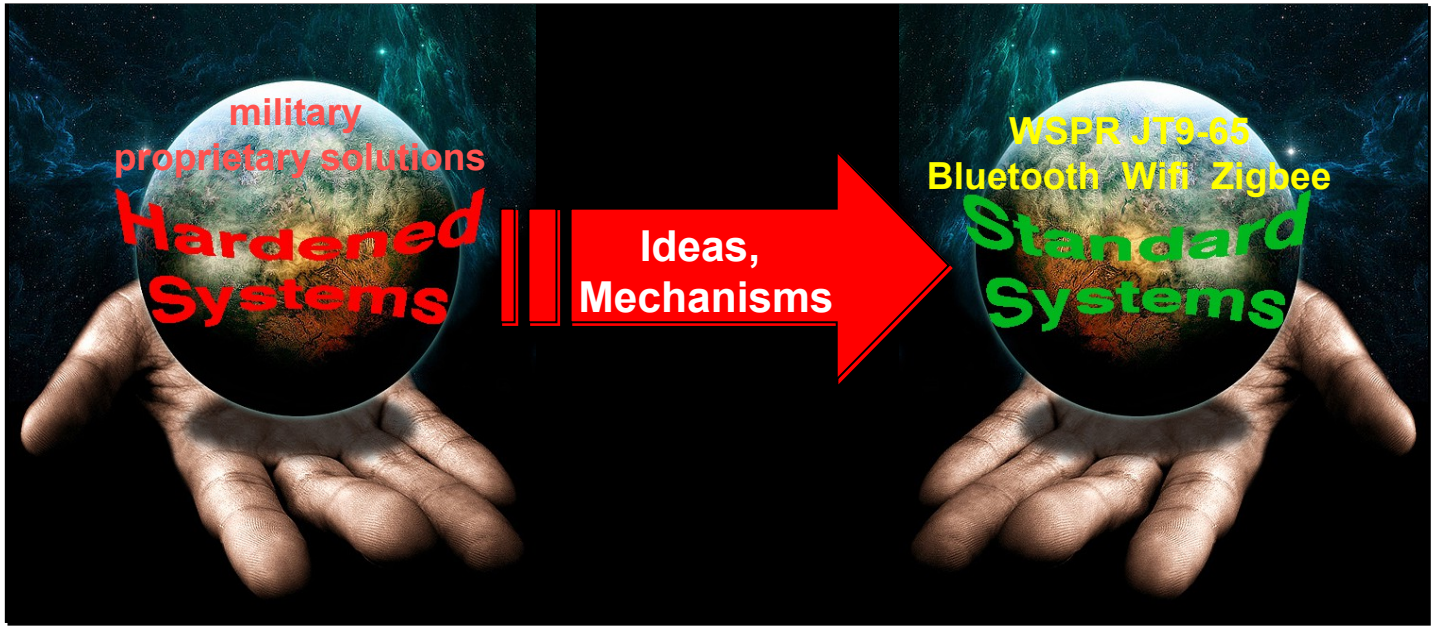
- … means hiding in plain sight
- Invisible to neighbors and average citizens
- “Plausible deniability”
- Not this -->

Where To Look For Solutions

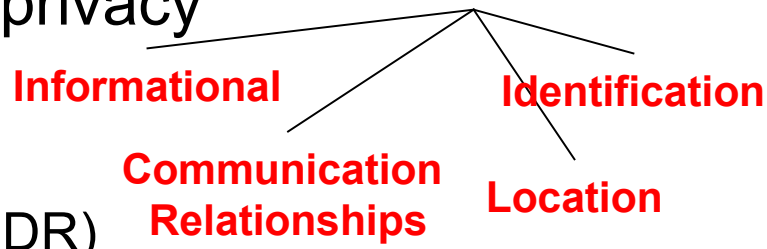


- Hardened Systems:
  - Specialized
  - High security and privacy
  - High costs
  - Proprietary and hard to get
- Open Systems:
  - Standardized/Open source
  - Low security and privacy
  - Low costs
  - High interoperability

Where To Look For Solutions (con't)



- **Goal:** Harden open/standard wireless communication protocol(s) to increase the users "privacy"
- **Conditions:**
  - Based on an open source/standards
  - Using OS Software Defined Radio (SDR)



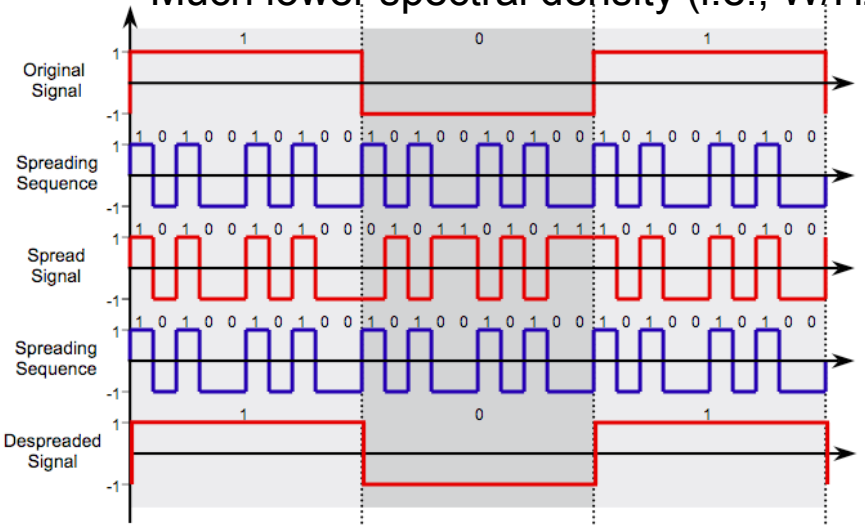
Major LPD/LPI methods

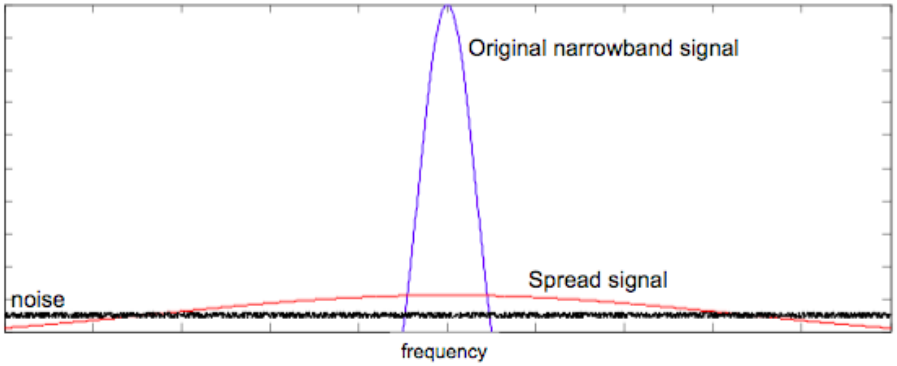
- Hide the Signal below the noise (Spread spectrum/UWB, chaotic and QRP)
- Hide the Signal within or below a cover signal or data (Steganography)
- Alice selectively blocks Bob's Signal to thwart Eve (Controlled jamming)
- Greatly reduce narrow-beam off-axis reception (Side-lobe suppression)
- Re-purpose widespread commercial service

Hiding the Signal below the Noise

Direct Sequence Spread Spectrum

- Information spread to a bandwidth much greater than required for transmission
- Spreading by modulating each information bit on a spreading sequence (chips)
  - Spreading sequence independent of data
  - **Narrowband signal spread to a broadband signal**
  - Much lower spectral density (i.e., W/Hz)

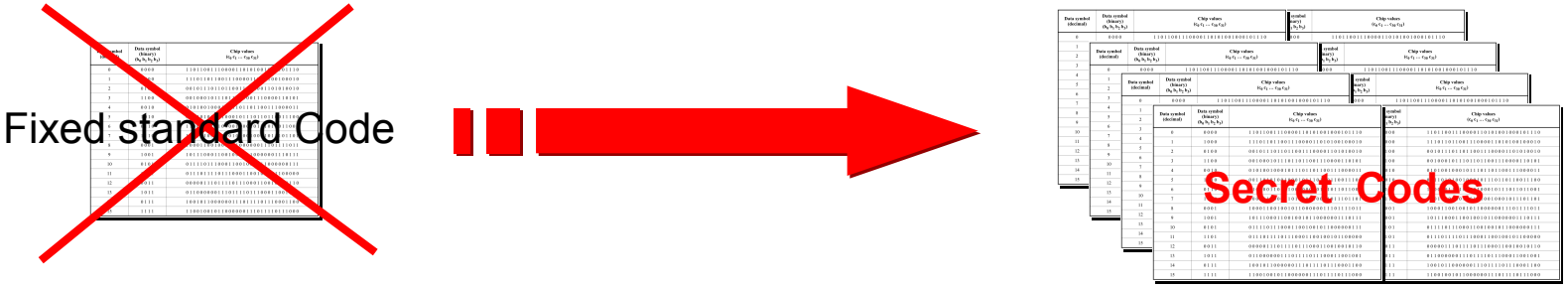




- **Benefits:** anti-jamming, anti-interference, **possible low probability of detection/intercept**, uncoordinated frequency reuse (e.g. CDMA)

Hiding the Signal Below the Noise Approach #1

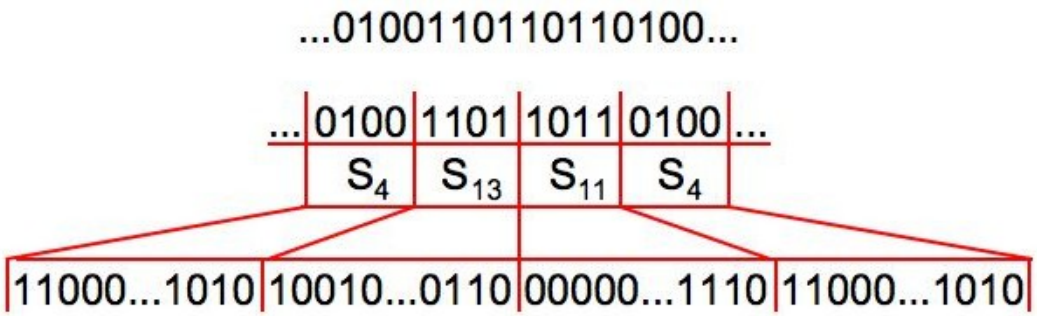
Idea: Secret & random symbol-to-chip table dynamically changing

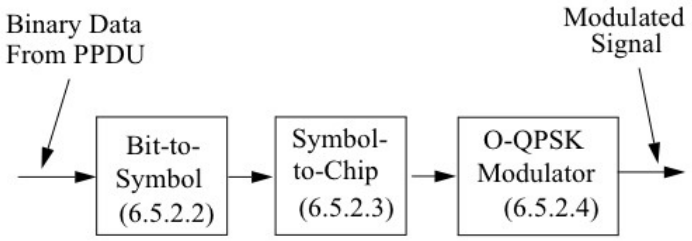


- Obfuscate all transmitted data at the lowest possible layer (PHY)
- Maximize LPD/LPI properties of DSSS

M-ary Spread Codes

- Example: 16-ary Direct Sequence Spread Spectrum technique and O-QPSK modulation (16 spreading sequences, not only one!)

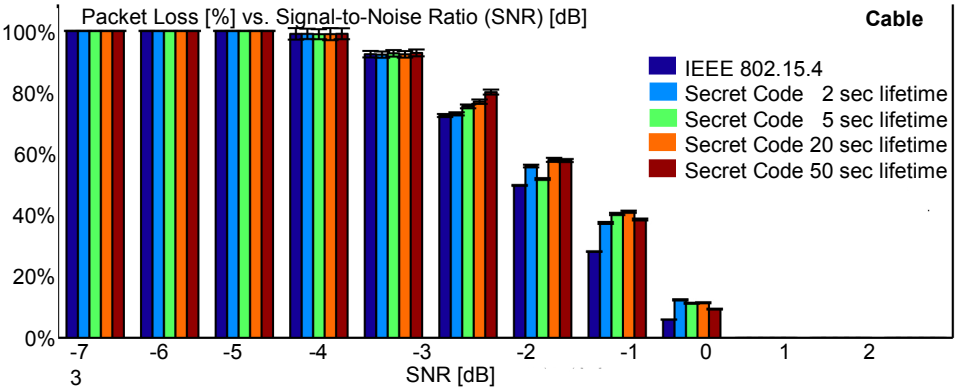


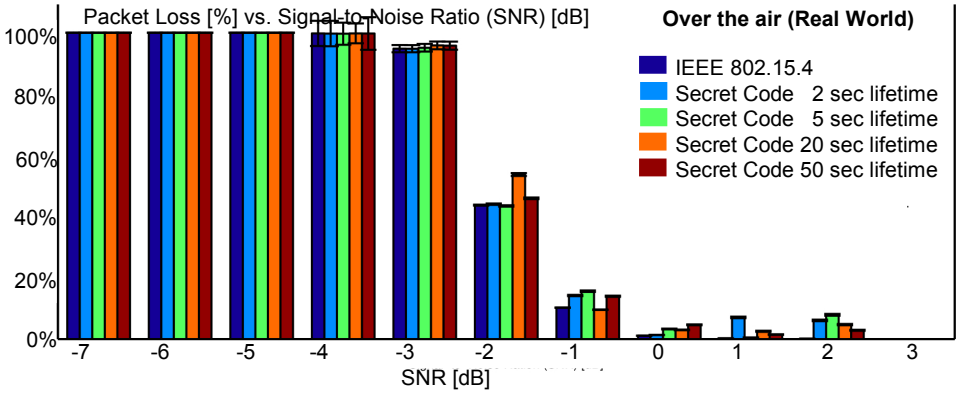


Data symbol (decimal)	Data symbol (binary) (b_0 b_1 b_2 b_3)	Chip values (c_0 c_1 … c_{30} c_{31})
0	0 0 0 0	1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0
1	1 0 0 0	1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 0 1 0
2	0 1 0 0	0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0
3	1 1 0 0	0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1
4	0 0 1 0	0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 0 1 1
5	1 0 1 0	0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0
6	0 1 1 0	1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1
7	1 1 1 0	1 0 0 1 1 1 0 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1
8	0 0 0 1	1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1
9	1 0 0 1	1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1
10	0 1 0 1	0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1
11	1 1 0 1	0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0
12	0 0 1 1	0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0
13	1 0 1 1	0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1
14	0 1 1 1	1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0
15	1 1 1 1	1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0

- **Normally publicly known** symbol-to-chip table used by all

Evaluation: Packet Loss





- Left: Cable

Right: Over the air (real world scenario)

- Random Codes compared to nearly orthogonal Code from IEEE 802.15.4 standard:
  - No minimum distance between chip-sequences of a Code
- PER increase below 13 %

Attacking the Secrecy of the Codes

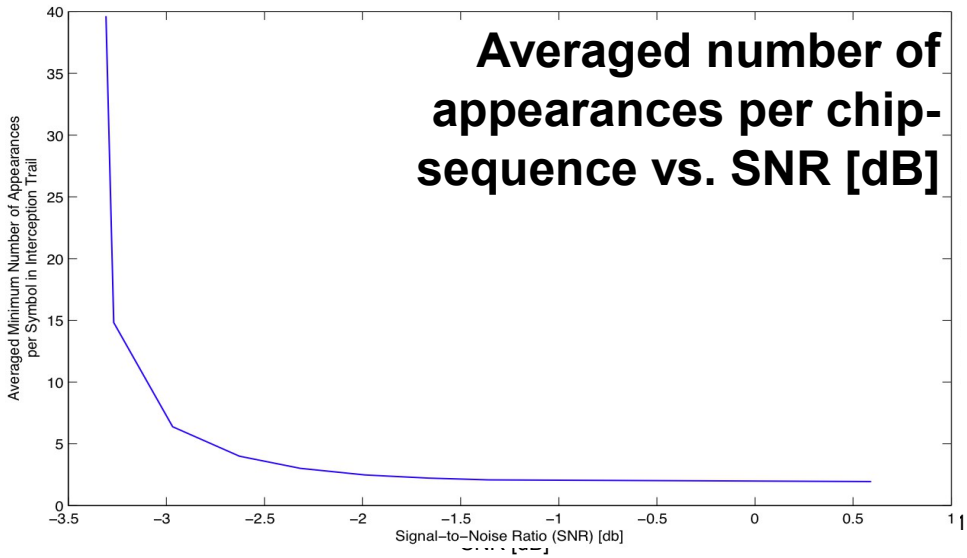
- Worst Case Attacker:
  - Protocol parameters assumed to be known (its FOSS)
  - Adapted m-ary DSSS attack [Wang, ICC, 2008]

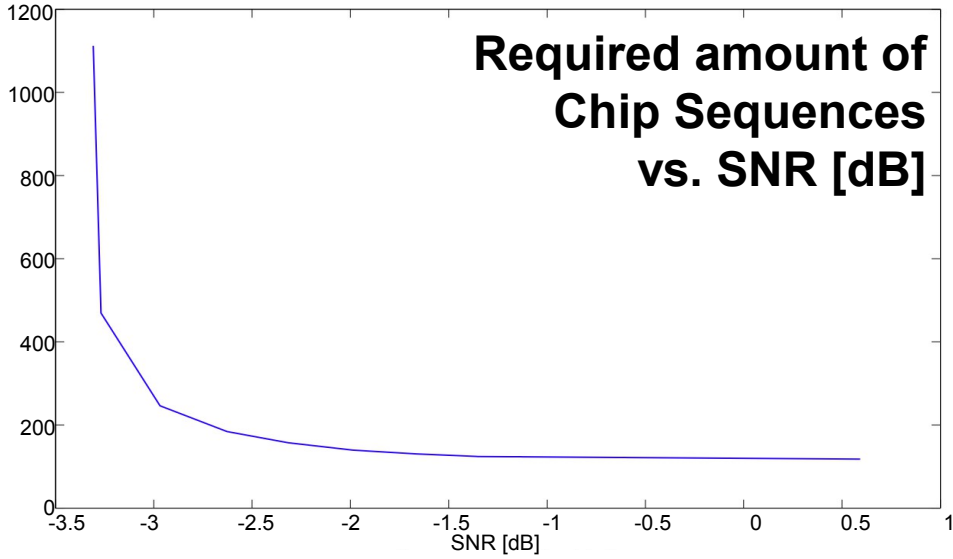
- Attacker Strategy:
  1. Record chip stream from channel

     As synchronization assumed this results in a list of intercepted chip-sequences
  2. K-means Clustering to eliminate chip errors
  3. Collect centroids / Compare with true Codes

➔ **Measure** performance of attacker
➔ Determine **how often each individual chip sequence is needed**
➔ Determine **required amount of chip sequences**

Attacking the Secrecy of the Codes (con't)





- The lower the SNR (the higher the chip error rate) the more often each individual chip sequence is required
- Asymptote:
  - No Chip Errors ➔each once
  - E[each Chip Seq. received once] ≅54 (if uniform distributed)

- Need **Code Change every packet** to defend against Worst Case Attacker

➔ $b \leq 27$ bytes

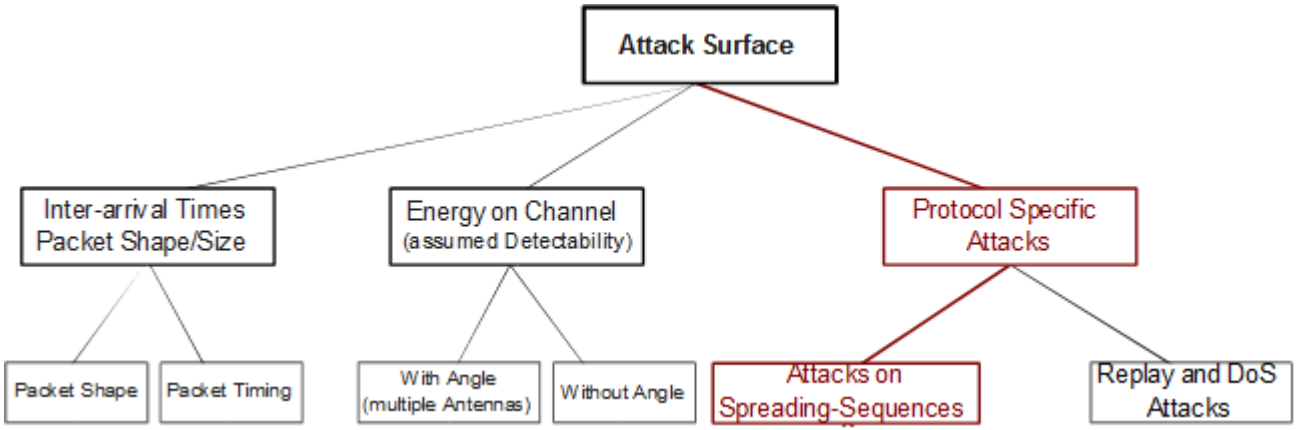
➔ Code Change every packet (average packet size of 22 bytes)

Evaluation: Secret Codes

- Initial protocol tests using GnuRadio SDR
  - Secret and dynamically changing but only 32-bit codes instead of the publicly known 16-bit codes in 802.15.4
- Packet Error Rate increase < 13%
- Protocol overhead < 1%
- Worst Case Attacker requires **only 27 bytes** to break the secrecy of the Codes

Possible Ways to Decrease PHY Attack Surface

- Cryptographic primitive changes
- Entropy maximization of packet timings, size and dynamic spreading factor
- Burst frame improvements
- Combine DS + FH



Low Detectability

- Often cited attribute for SS and CDMA
  - Only valid if spread code and/or seed remain secret
  - Static PRNG seeds may be discovered by theft or tampering

QRP Amateur Radio Protocols

- WSJT weak signal software
  - Excellent, OS, signal processing
  - JT65 (VHF-UHF) EME and QRP (MF-HF, 10,15,20m USB) IM
  - WSPR (MF-HF) beacons: reporting worldwide ionospheric “skip” conditions
    - 6000km HackRF (10mW) packet received
  - JT9 (LF-HF) can operate > 40 dB (10,000-fold) below noise floor of band
- Compatible with all common ham gear
  - Very power efficient: LED flash-light power can offer international coverage
  - Bandwidth efficient: ~15 Hz (JT9-1), <0.5 Hz (JT9-30)
  - Not strictly covert but can be very difficult to detect w/o a priori knowledge
- QRSS (spread temporal)
  - Morse code “dit” of 10-30 seconds (or even longer) commonly used
  - Long distance communications possible with << 1mW power

Long-Wire & Dipole HF Antennas

- Dipole
  - Simple and cheap
  - Hidden in attics
  - Broadband & low efficiency
  - Usually horizontally polarized
- Longwire

Small Resonant Loop (SRL)

- Small (1/10 – 1/4 wave circumference)
- Efficient for narrow-band but can require careful tuning
- High immunity to nearby noise and out-of-band signals
- Somewhat directional
- Excellent for NVIS (when vertical) and skip

- Needed: wideband capable, HF, “efficient”, travel, transmit magloop for QRP
  - Status: research

- COTS transmit varieties narrowband only and over-designed for QRP

Hiding the Signal Below the Noise Approach #2

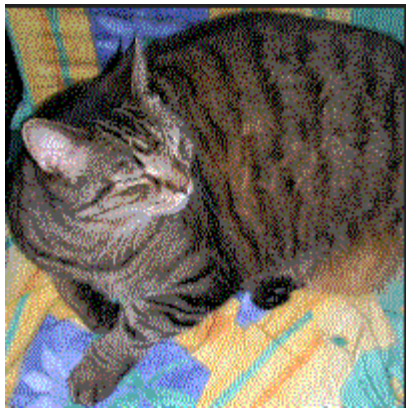
Idea: Random Code DSSS + enhanced WSPR beacons (LF-HF) to help coordinate p-t-p links between Alice and Bob

- Medium range using NVIS (MF-HF) or ground wave
- Long range via ionospheric skip
- Asynchronous CDMA for efficient band-sharing
- Specialized antennas for portable use (in development)
- Low-moderate cost
- Regulatory issues
- Probably **invulnerable** even to well-equipped adversaries
- Only low-speed data
- Status: planned

Steganography: Hiding below or within another Signal

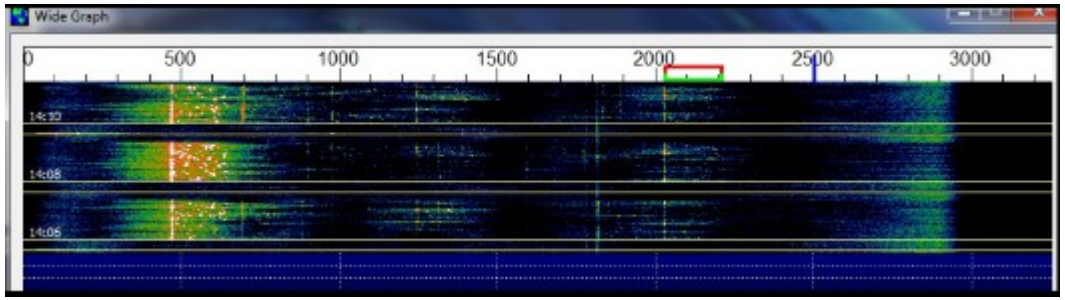
- Physical forms used since ancient times
- Commercially used for watermarking content
- Simplest use LSB of noisy images or sounds
- Most breakable with COTS software
- Some forms (e.g., noiseless) may be near impossible to break from a purely technical standpoint

-->



Steganographic Approach #1

Idea: Modify JT65 timing or injecting errors (e.g., in the FEC)

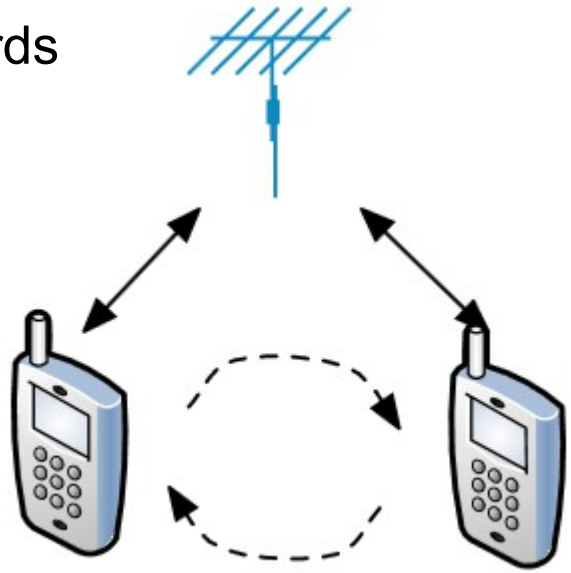


- Can, in theory, provide a long-distance capable, short message, platform
- Not tested OTA due to regulatory issues
- Probably **vulnerable** to well-equipped adversaries

Steganographic Approach #2

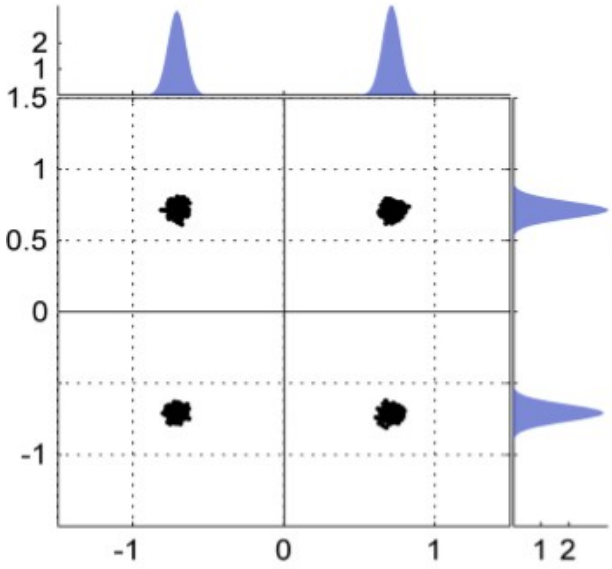
Idea: Add hidden data, as noise, to modulation constellation

- Alice and Bob send innocuous cover traffic through a router
- Mimics noisy signal or hardware impairment
- Changes fall within modulation quality standards
- Hardware/firmware assist to SDR
- Experiments conducted to verify covertness
- Hotspots and private networks

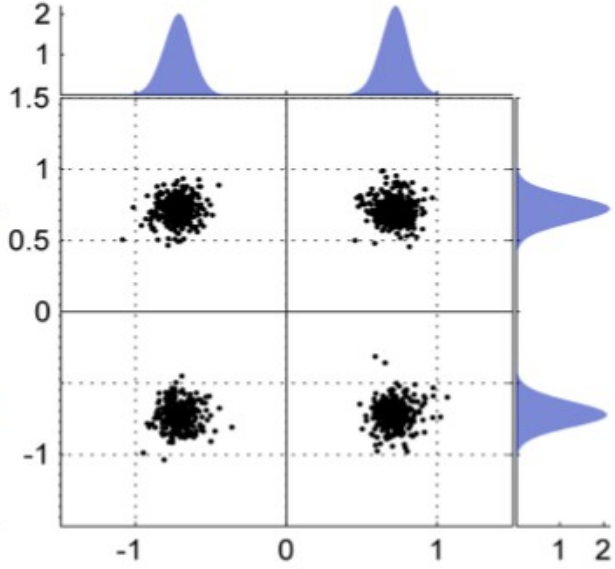


Stego Data Hidden in Noisy Constellations

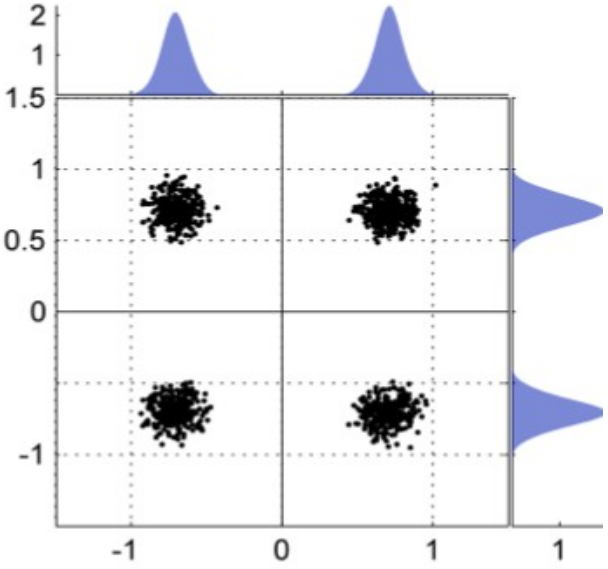
- QPSK and QPSK with hardware impairments are indistinguishable, even at same SNR
- 10dB of modulation error at transmission is allowed in IEEE 802.11 standard



Ideal QPSK



Noisy QPSK



QPSK with Hardware impairments

Key Generation

- Alice and Bob must have a way to generate shared secret key(s) in the presence of Eve
  - Should be computationally efficient
  - For DSSS it seeds the initial random spreading sequences
  - Before any communication detectable by Eve

Key Generation Method #1

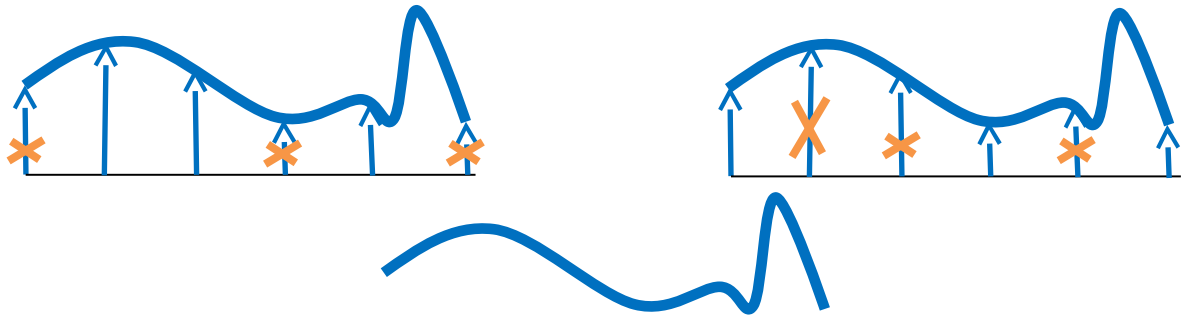
Idea: Use station “addresses” known only to Alice and Bob + randomizing factors (e.g., Time-of-Day)

- Works like a RSA key dongle
- Alice's station device generates a series of unique random addresses (like a bitcoin wallet create a receiving address)
- Bob gets one, Charlie another, etc.
- Generated keys tell each party's device when, what frequency & spreading code to use for a session with Alice
- Enhanced beacons used to improve location and propagation

Key Generation Method #2

Idea: Exploit or create randomness at the wireless physical layer

Cooperative Jamming



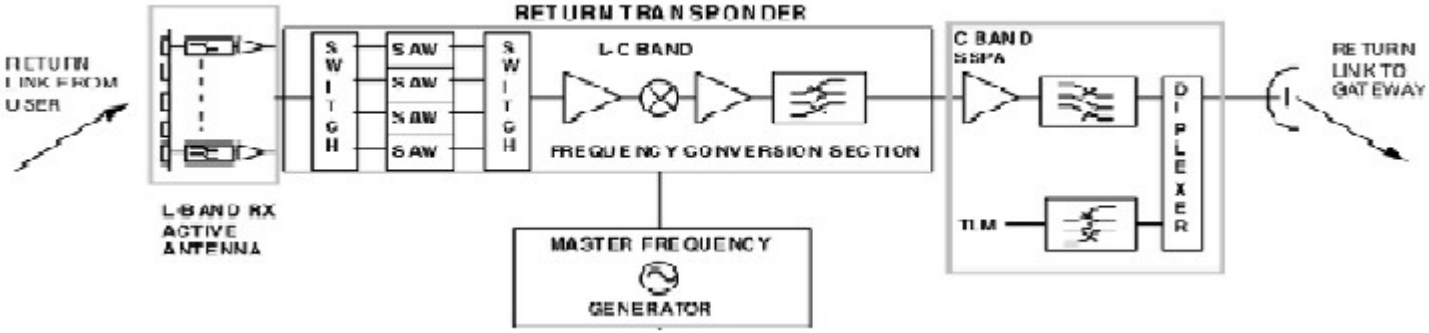
- Practical key needs 2048 bits
- Exploiting existing channel randomness yields only 1-44 bps
- Selective jamming by receiver can yield >3kbps secret bits
- Receiver reconstructs signal by picking clean samples
- May work best when Alice and Bob are near (T.B.D.)

Satellites

- Commercial GEO
  - Older C-band and newer Ku-band
    - Worldwide, 24/7, coverage
    - Easily obtained, innocuous, affordable, up- and down-link equipment
  - Almost all are “bent pipes”
- Commercial LEOs
  - GlobalStar, Iridium
- Military (LEOs)
  - FLTSAT and UFO
  - Brazilian trucker and narco exploits
- Interfering signal
  - Detection based on down-link tuned intercept receiver
  - Direction of Arrival DoA across adjacent satellites

Bent Pipes

- A bent pipe satellite does not demodulate and decode the up-link signal
  - A gateway station on the ground controls the satellite and routes traffic to and from the satellite
  - FFT/IFFT used inside bird to clean-up up-link signals and relay on down-link
  - Unwanted signal blocking limited to narrow-band



Covert Satellite Approach #1

Idea: Random Code DS + C/Ku bands GEO satellites enabling point-to-point links between Alice and Bob

- 24/7 reliability
- Low-moderate station cost using VSAT modem + GR + SDR transceiver
- Ku can use innocuous small dishes like your neighbour's
- Uncoordinated CDMA for covertness and efficient band-sharing
- Supports both voice and low-speed data
- Possibly **invulnerable** to well-equipped adversaries when (prior) DS covert tech is used

Covert Satellite Approach #2

Idea: Random Code DS (e.g., GlobalStar) C-band LEOs enabling point-to-point links between Alice and Bob

- Possible 24/7 reliability
- Moderate station cost using down-converter/LNA +GR + SDR transceiver
- Might enable portable omni antenna or small dishes with alt-az tracking
- Uncoordinated CDMA for efficient band-sharing
- Supports low-speed data
- Possibly **invulnerable** to well-equipped adversaries when (prior) DS covert tech is used

Covert Satellite Approach #3

Idea: Narrow effective up-link beam-width so only one "bird" can see it

- May prevent triangulation and reception by multiple satellites
- Might work with only small- (DTV-VSAT) moderate-size antenna
- Works with all transmitter modulation and protocols
- Inexpensive when manufactured in volume
- Similarity but simpler than Artimis pCell massive MIMO technology
- Can also be used for LoS and troposcatter/ducting
- Status: needs R&D

Anonymously re-purpose an existing service

Pager Networks

- Still widely used worldwide
- Simplex operation = anonymous receiver location
- Cheap and portable simple messaging
- Easily hacked
  - Assume any device ID
  - Group sharing via sub-IDs
- Encrypted messages permitted
- Anon message injection via service's email
- SDR support on Android mobiles via RTL/specialized HW

Thank you for listening...

... any questions?

Resources

- My email: wirelesswarrior@safe-mail.net
- Wireless for the Warrior http://www.wftw.nl/
- Gnu Radio https://en.wikipedia.org/wiki/GNU_Radio
- HackRF http://greatscottgadgets.com/
- BladeRF http://nuand.com/
- USRP http://www.ettus.com/
- FunCube dongle http://www.funcubedongle.com/
- Selected covert wireless tech papers: by request

More Resources

- WSJT http://physics.princeton.edu/pulsar/K1JT/wsjt.html
- QRSS http://www.w0ch.net/qrss/qrss.htm
- Future radio beacons http://www.g4jnt.com/BeaconPres-2.ppt
- Magnetic loop antennas http://www.dxzone.com/catalog/Manufacturers/Antennas/HF/Magnetic_Loop/
- Sat-jacking
  - http://archive.wired.com/politics/security/news/2009/04/fleetcom
  - https://www.blackhat.com/docs/us-15/materials/us-15-Moore-Spread-Spectrum-Satcom-Hacking-Attacking-The-GlobalStar-Simplex-Data-Service-wp.pdf

More Resources

- FireChat
  - Bruce Schneier
    https://www.schneier.com/blog/archives/2014/10/firechat.htm
  - FC's creator
    http://www.wired.co.uk/news/archive/2014-06/25/firechat

Appendicies

Major Feature Receiver Comparison

Receiver	Advantages	Disadvantages	Principal Applications
Wideband crystal video	Simple, inexpensive, instantaneous, High POI in frequency range	No frequency resolution Poor sensitivity and Poor simultaneous signal performance	RWR
Tuned RF Crystal Video	Simple, Frequency measurement Higher sensitivity than wideband	Slow response time Poor POI	Option in RWR, Frequency measurement in hybrid
IFM	Relatively simple Frequency resolution Instantaneous, high POI	Cannot sort simultaneous signals Relatively poor sensitivity	Shipboard ESM, Jammer power management, SIGINT equipment
Narrow-band scanning Superhet	High sensitivity Good frequency resolution Simultaneous signals don't interfere	Slow response time Poor POI Poor against frequency agility	SIGINT equipment Air and ship ESM Analysis part of hybrid
Wide-band Superhet	Better response time and POI	Spurious signals generated Poorer sensitivity	Shipboard ESM Tactical air warning
Channelized	Wide bandwidth, Near instantaneous, Moderate frequency resolution	High complexity, cost; Lower reliability; limited sensitivity	SIGINT equipment Jammer power management
Microscan	Near instantaneous, Good resolution and dynamic range, Good simultaneous signal capability	High complexity, Limited bandwidth No pulse modulation information Critical alignment	SIGINT equipment Applications for fine freq analysis over wide range
Acousto-optic	Near instantaneous, Good resolution, Good simultaneous signal capability Good POI	High complexity; new technology	

Qualitative Comparison of Receivers

Feature	Receiver Type							
	Wide-Band Crystal Video	TRF Crystal Video	IFM	Narrow-Band Superhet	Wide-Band Superhet	Channelized	Microscan	Acousto-optic
Instantaneous Analysis Bandwidth	Very wide	Narrow	Very wide	Narrow	Moderate	Wide	Wide	Moderate
Frequency Resolution	Very poor	Fair	Good	Very good	Poor	Fair	Good	Good
Sensitivity	Poor (No preamp) Fair (preamp)	Fair/ good	Poor (No preamp) Fair (preamp)	Very good	Fair	Fair/ good	Very good	Good
Dynamic Range	Fair	Fair/ good	Good	Very good	Fair	Good	Fair	Poor
Speed of Acquisition	Very Fast	Slow	Very Fast	Slow	Fast	Very Fast	Very Fast	Fast
Short pulse Width Capability	Good	Good	Good	Good	Very good	Good	Fair	Fair
Retention of Signal Character-istics	Fair	Fair	Poor	Good	Fair/ good	Good	Poor	Fair/ good

Qualitative Comparison of Receivers (con't)

Feature	Receiver Type							
	Wide-Band Crystal Video	TRF Crystal Video	IFM	Narrow-Band Superhet	Wide-Band Superhet	Channelized	Microscan	Acousto-optic
Applicability to Exotic Signals	Poor/ fair	Poor	Good	Poor	Fair/ good	Good	Fair/ good	Fair/ good
High signal Density Performance	Poor (high false alarm rate from background)	Fair/ good	Good	Poor	Fair (depending on BW)	Fair/good, depending on architecture & processing	Good	Poor
Simultaneous Signal Capability	Poor	Fair/ good	Poor	Good	Fair (depending on BW)	Good	Good	Good
Processing Complexity	Moderate depending on application	Moderate depending on application	Moderate	Moderate	Moderate	Low-high depending on architecture	Complex	Simple signal processing complex data processing
Immunity to Jamming	Poor	Fair	Poor/ Fair	Good	Poor/ Fair	Good	Good	Good
Power Requirements	Low	Low/ Moderate	Moderate	Moderate	Moderate	High	Moderate	Moderate/ High

Qualitative Comparison of Receivers (con't)

Feature	Receiver Type							
	Wide-Band Crystal Video	TRF Crystal Video	IFM	Narrow-Band Superhet	Wide-Band Superhet	Channelized	Microscan	Acousto-optic
RF Range (GHz)	Multi-octave (0.5-40)	0.15-18 separate	>0.5 to 40	<0.01 to 40	0.5 to 18	0.5 to 60	<0.5 to 8	0.5-4 (0.5-18 channelized and down conversion)
Max Instantane-ous Analysis Bandwidth	Multi-octave (to 17.5 GHz)	As high as desired with equivalent reduction in resolution	Multi-octave (1 octave per unit)	50 MHz	500 MHz	~2 GHz without degradation, 17.5 GHz with degradation	0.5 to 2 depending on PW limitation	1 GHz
Frequency Accuracy	Measurement accuracy no better than analysis BW	Measurement accuracy no better than analysis BW	5-10 MHz	0.5% to 1%	0.5 to 3 MHz	±1 MHz	10 KHz	±1 MHz

Receiver Types vs. Signal Types

Signal Type	Receiver Type							
	Wide-Band Crystal Video	TRF Crystal Video	IFM	Narrow-Band Superhet	Wide-Band Superhet	Channelized	Microscan	Acousto-optic
CW	Special design for CW	Special design for CW	Yes, but interferes with pulsed reception	Yes	Yes	Yes	Yes	Yes
Pulsed	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multiple Frequency	No	No	No	Yes, but won't recognize as same source	No	Yes	Yes	Yes
Frequency Agile	Yes, doesn't measure frequency	No	Yes	No	Yes (within passband)	Yes	Yes	No/Yes, depending on readout time
PRI Agile	Yes	Yes	Yes	No/Yes, depending on scan rate	Yes	Yes	No/Yes, imprecision in TOA	No/Yes, depending on readout time
Chirped	Yes, within acceptance BW	No	Yes	No/Yes, depending on BW	Yes	Yes (reduced sensitivity)	No/Yes, depending on scan rate	Yes (reduced sensitivity)
Spread Spectrum	Yes, within acceptance BW	No	Yes	No	No/Yes, depending on BW	Yes (reduced sensitivity)	Yes (reduced sensitivity)	Yes (reduced sensitivity)