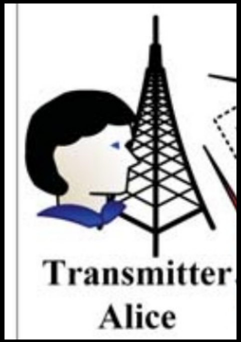
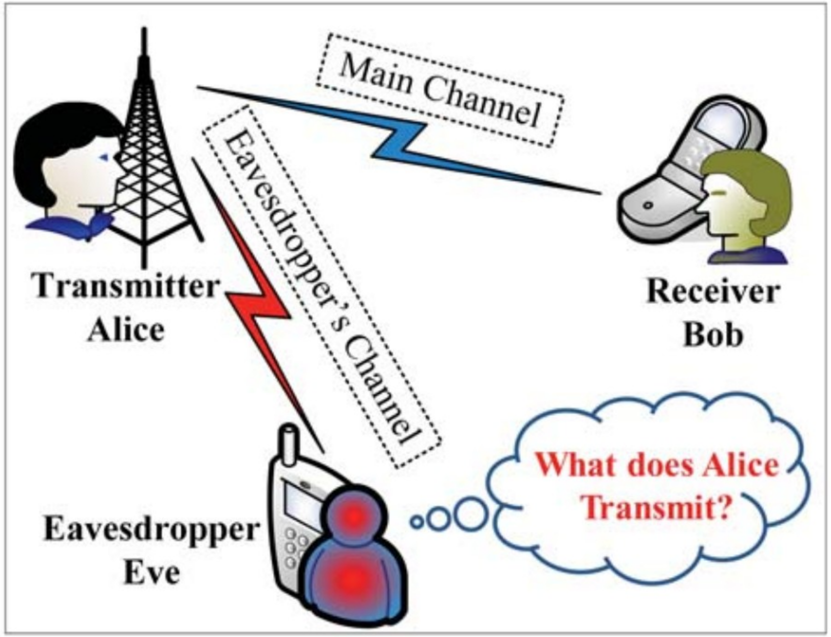
Quantifying Covertness in Communications Systems

Lucas Rooyakkers

What is Covert Communications?

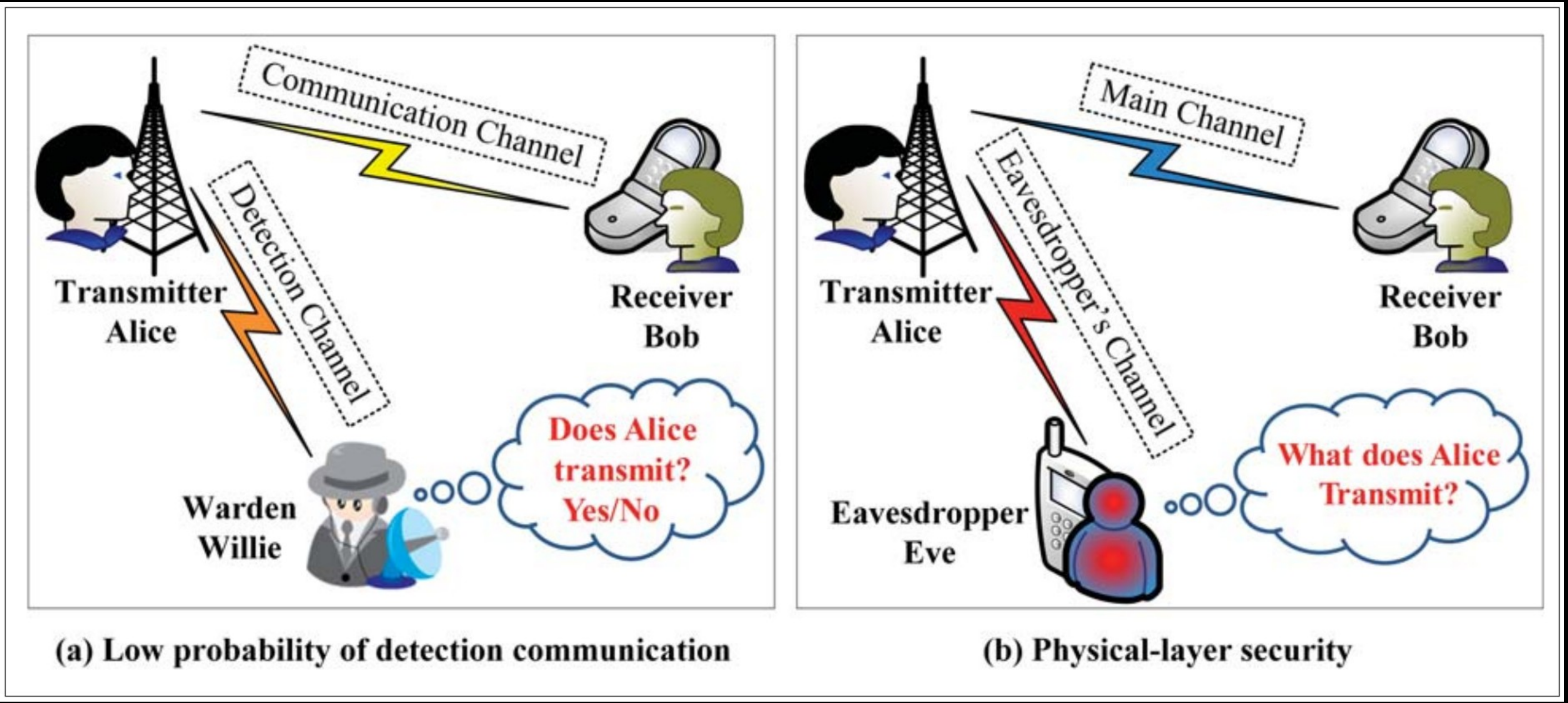


What is Covert Communications?



(b) Physical-layer security

What is Covert Communications?



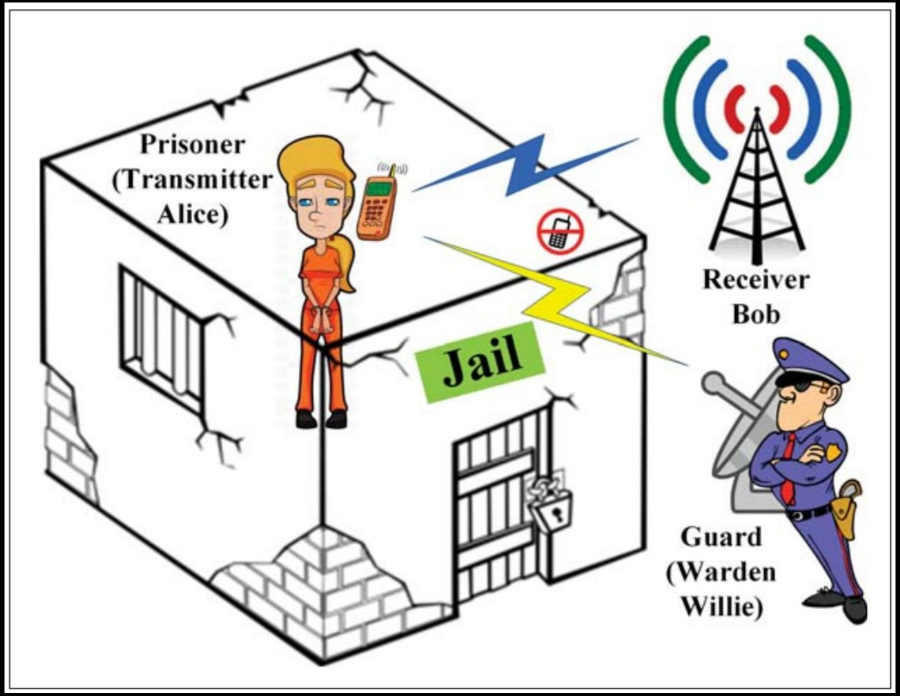
Also Known As

- Low Probability of Detection (LPD)
  - Used by Information Theorists
  - Often formal, mathematical definition

- Low Probability of Intercept (LPI)
  - Used by Waveform Designers
  - Describes signals that are “hard” to intercept

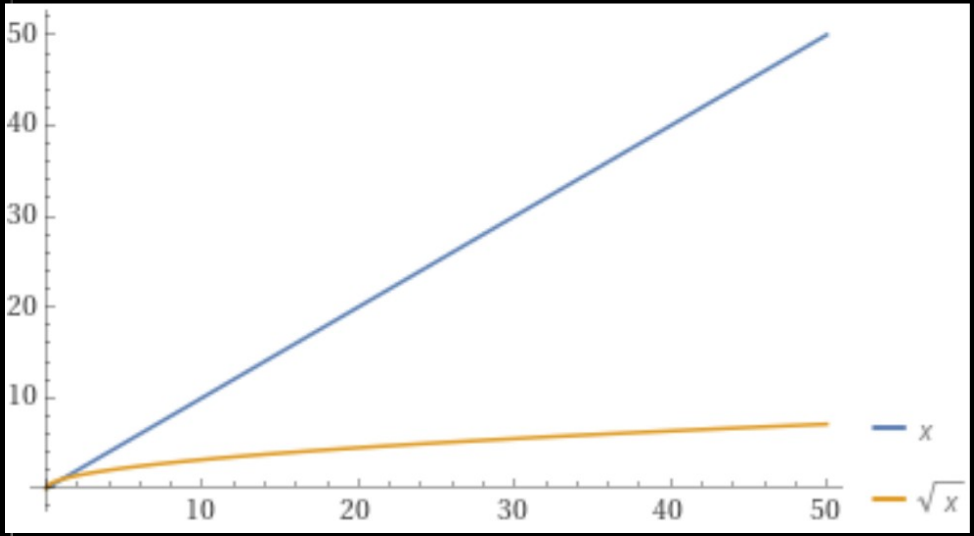
Fundamental Limits: Square Root Law

- Alice can transmit $O(\sqrt{n})$ bits for every n channel uses.
- Alice and Bob need a pre-shared key of $O(\sqrt{n})$



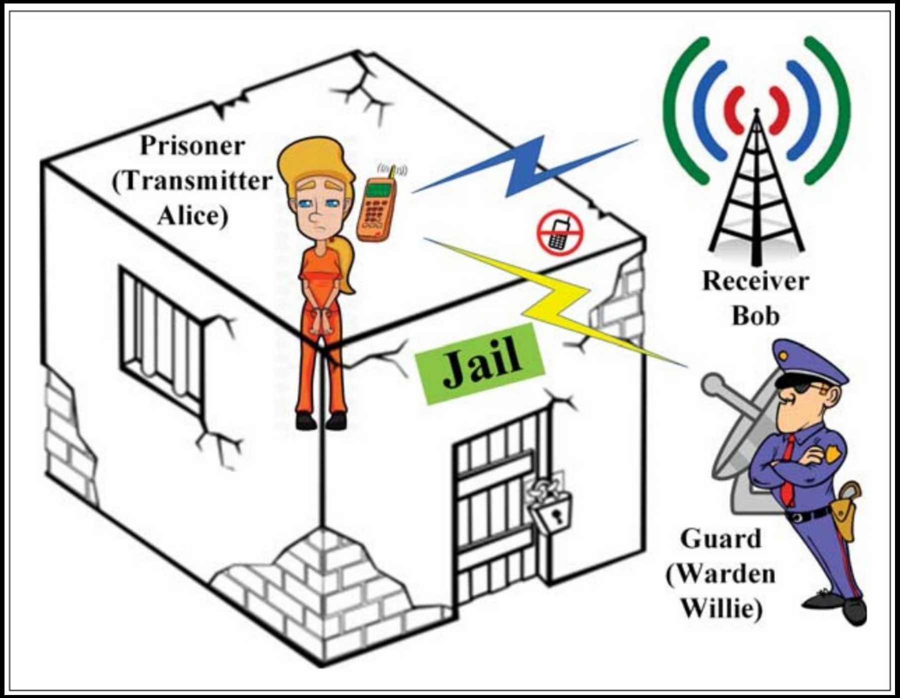
Fundamental Limits: Square Root Law

- Comes from Steganography
- Doesn't grow very fast
- Assumes Willie knows *everything*, except secret key



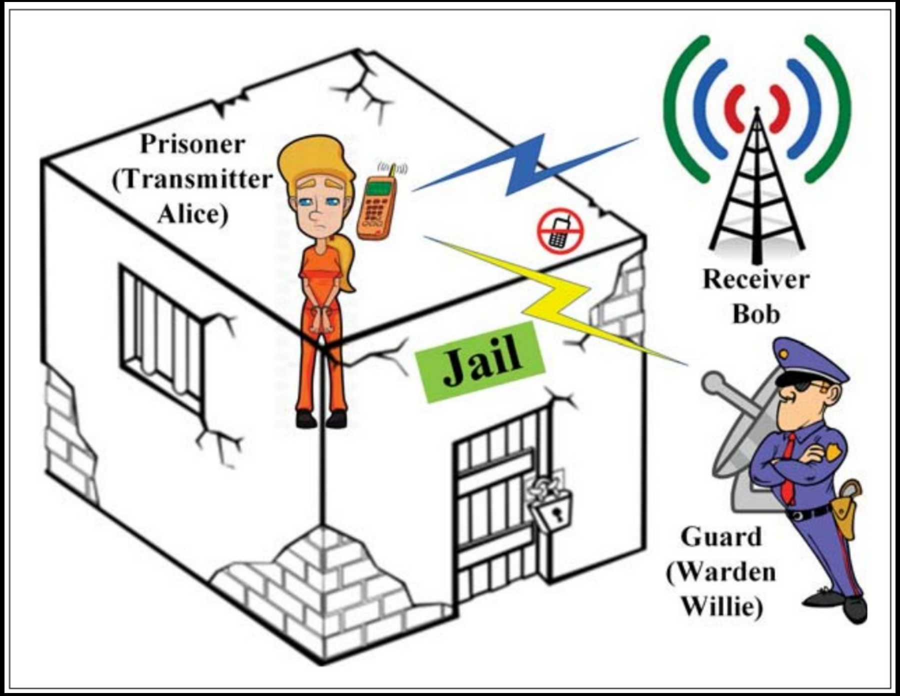
Fundamental Limits: Positive Capacity

- Alice can transmit *O*(*n*) bits when:



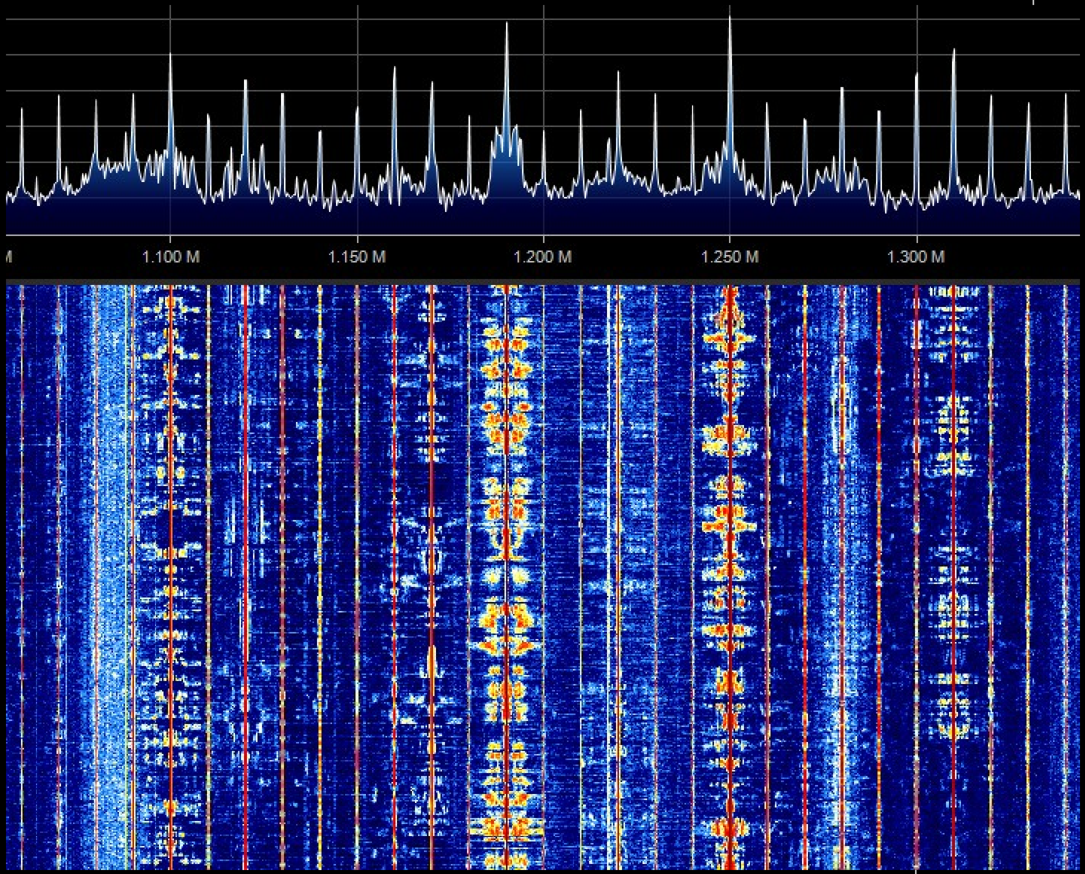
Fundamental Limits: Positive Capacity

- Alice can transmit *O(n)* bits when:
  - Willie doesn't know the noise level exactly
  - Jammers are used
  - There are public spectrum users



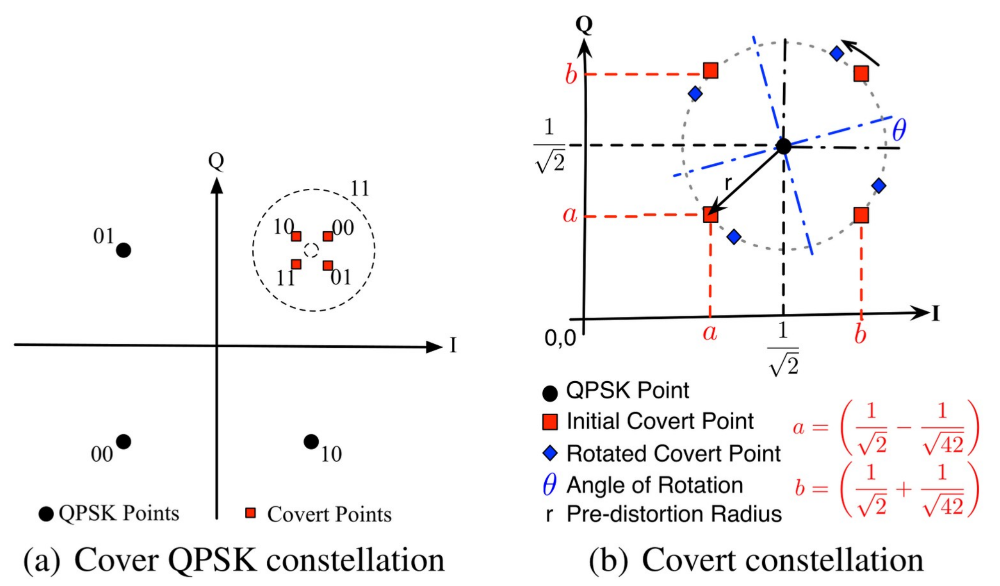
Public Messages

- Alice can hide *among* public messages
  - Willie must filter out every public message to detect Alice
  - More public users means lower probability of detection

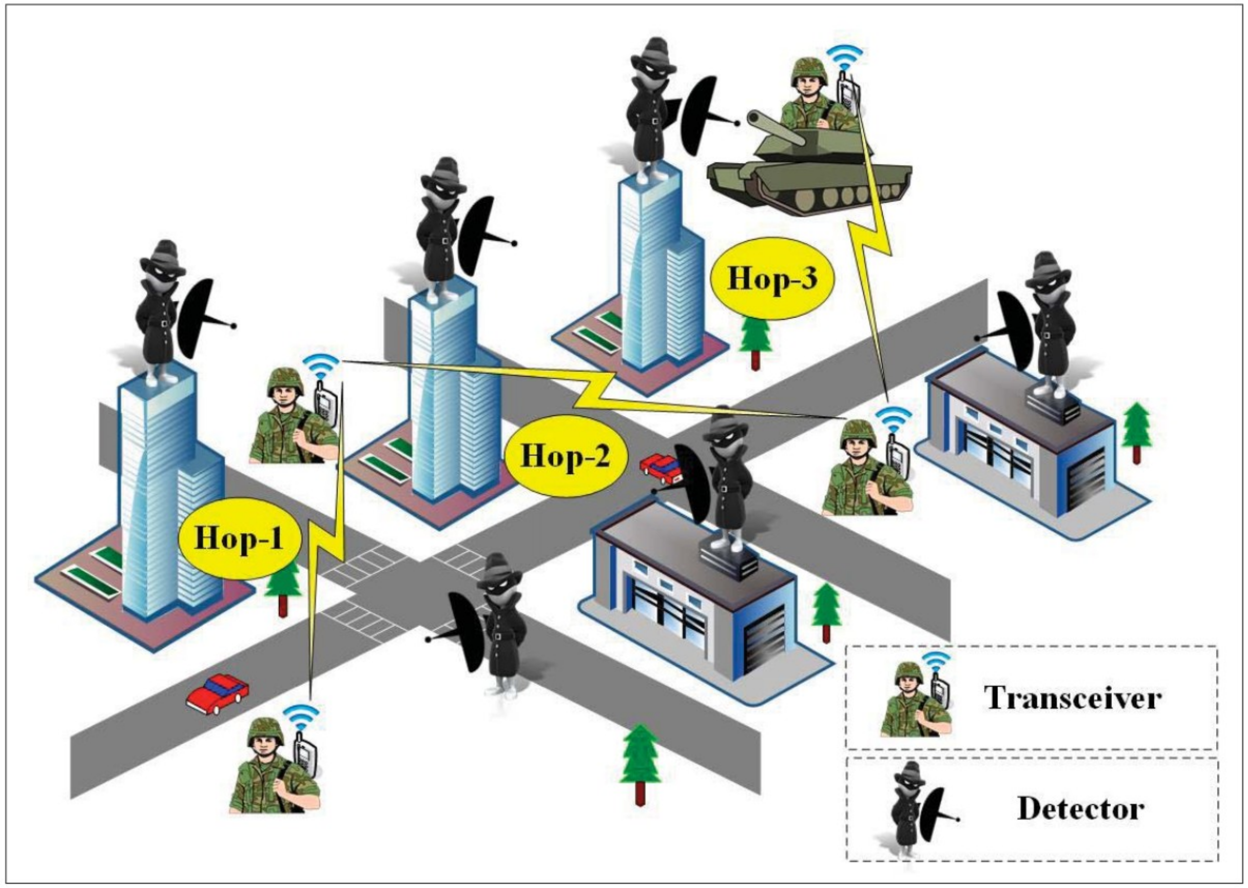


Public Messages

- Alice can hide *within* public messages
  - Alice mush know structure of public message
  - Willie must filter out *every* public message to detect Alice

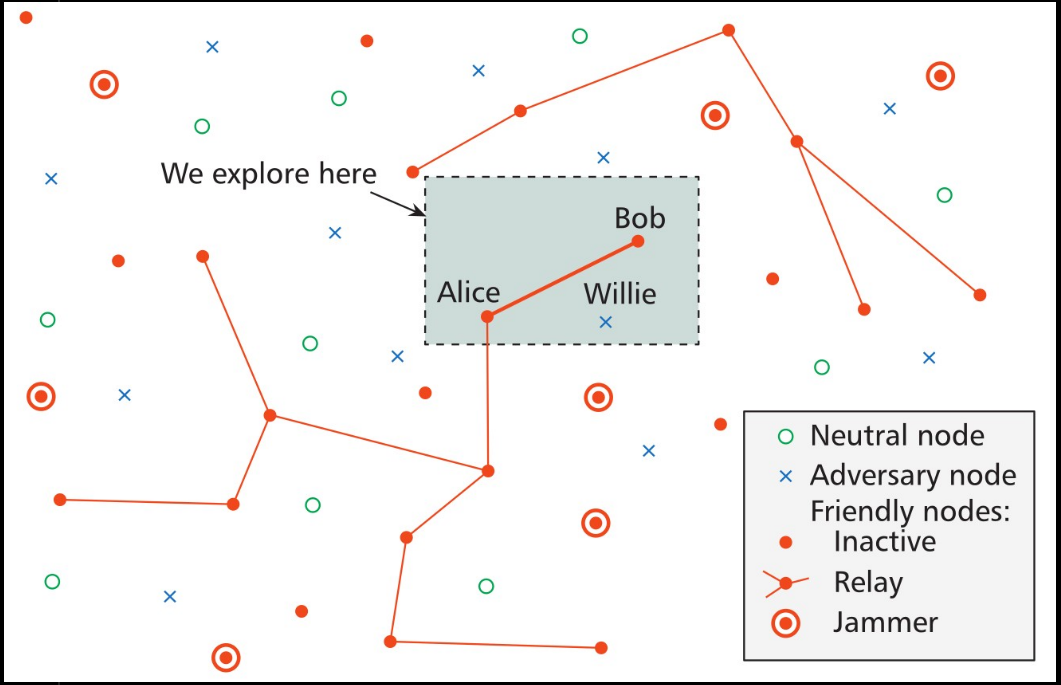


Shadow Networks



Shadow Networks

- O(√*n*) when using undirected antennae
- O(*n*) with beamforming, directed antennae, MIMO



Detector Theory: Willie’s Test

Detector Theory: Willie's Test

- Null Hypothesis: Only Noise
  - H_0: r(t) = n(t)

- Alternative Hypothesis: Alice's Signal and Noise
  - H_1: r(t) = n(t) + s(t)

Detector Theory: Detectors

- A detector takes the received signal and outputs a test statistic to be compared to a threshold:

$$\mathcal{D}(r(t)) = \lambda \underset{H_1}{\overset{H_0}{\lessgtr}} \lambda_0$$

Detector Theory: Error Types

- Type I (False Alarm)
- Type II (Missed Detection)

$$\mathcal{P}_{\mathrm{FA}} = \mathbb{P}(\lambda > \lambda_0 | H_0)$$

$$\mathcal{P}_{\mathrm{MD}} = \mathbb{P}(\lambda < \lambda_0 | H_1)$$

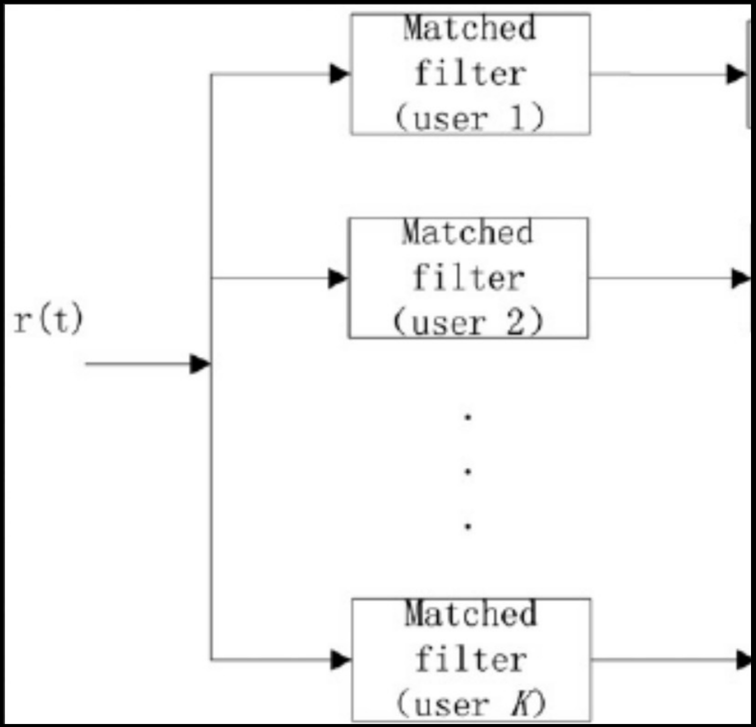
Optimal Detectors: The Radiometer

- Compare measured power to noise estimate
- Optimal for completely unknown signal, on an AWGN channel
- Struggles with interference

$$\int_0^T r(t)^2 dt$$

Optimal Detectors: Matched Filters

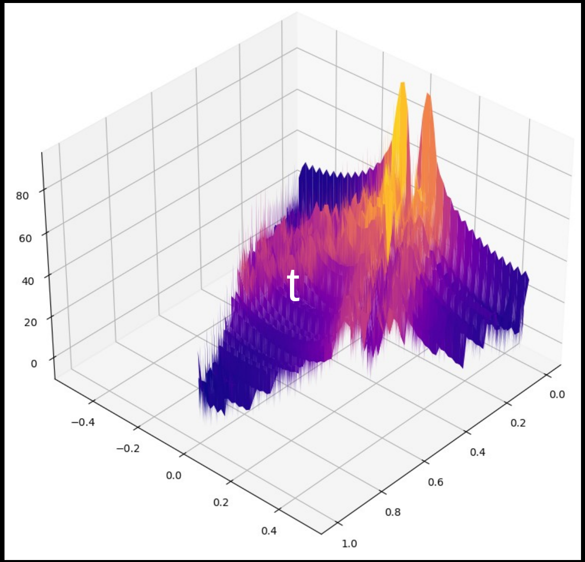
- Signal properties must be known
- Can be used in a bank in parallel



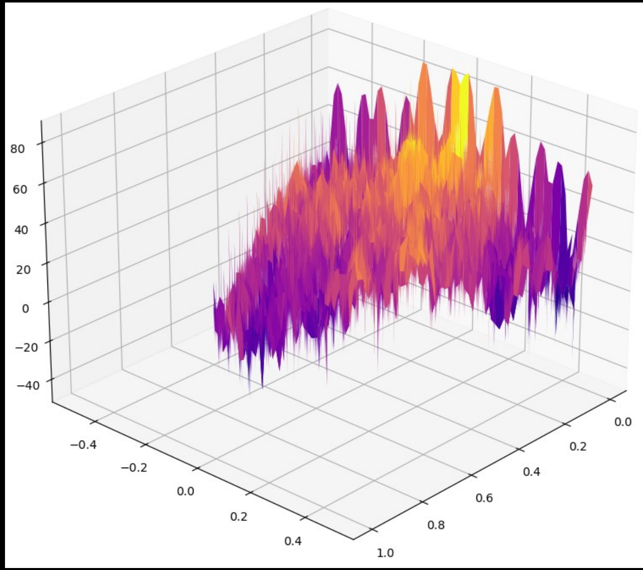
Cyclostationary Detectors

- Checks for periodicity in signals
- Best for weak signals in noise
- No proven “best” metric

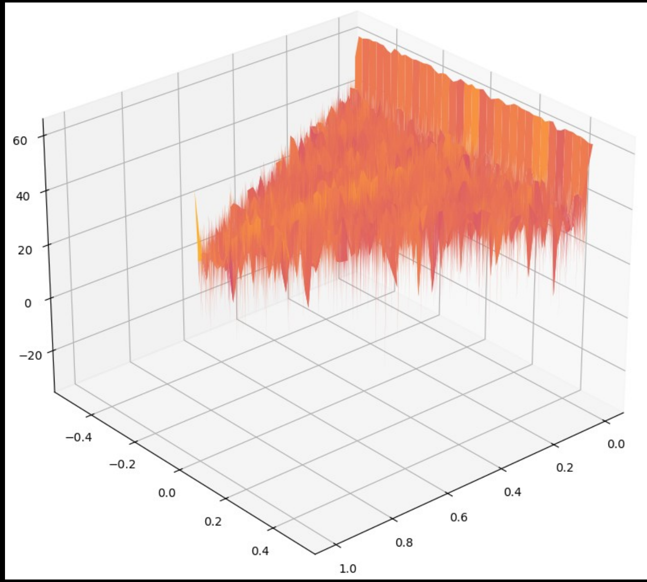
Cyclostationary Detectors



BPSK



CDMA-BPSK



AWGN

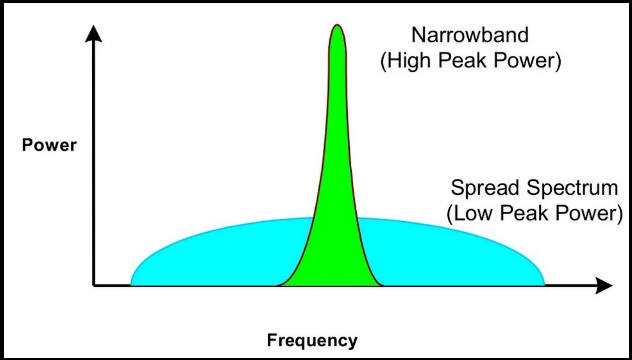
How to Create LPI/LPD Waveforms

How to Create LPI/LPD Waveforms

- Lower the Power (at Willie)

How to Create LPI/LPD Waveforms

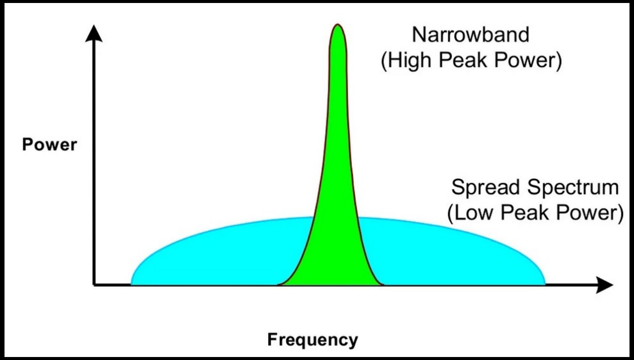
- Lower the Power (at Willie)



- Spread it out in frequency

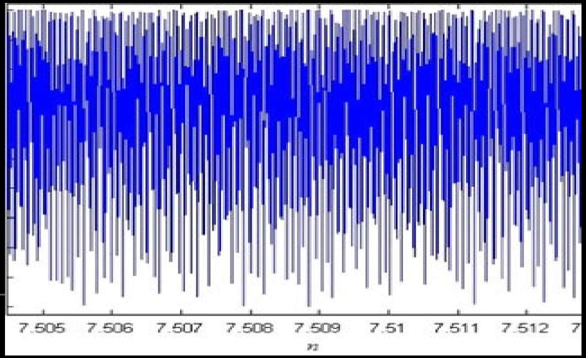
How to Create LPI/LPD Waveforms

- Lower the Power (at Willie)



- Spread it out in frequency

- Make the waveform irregular

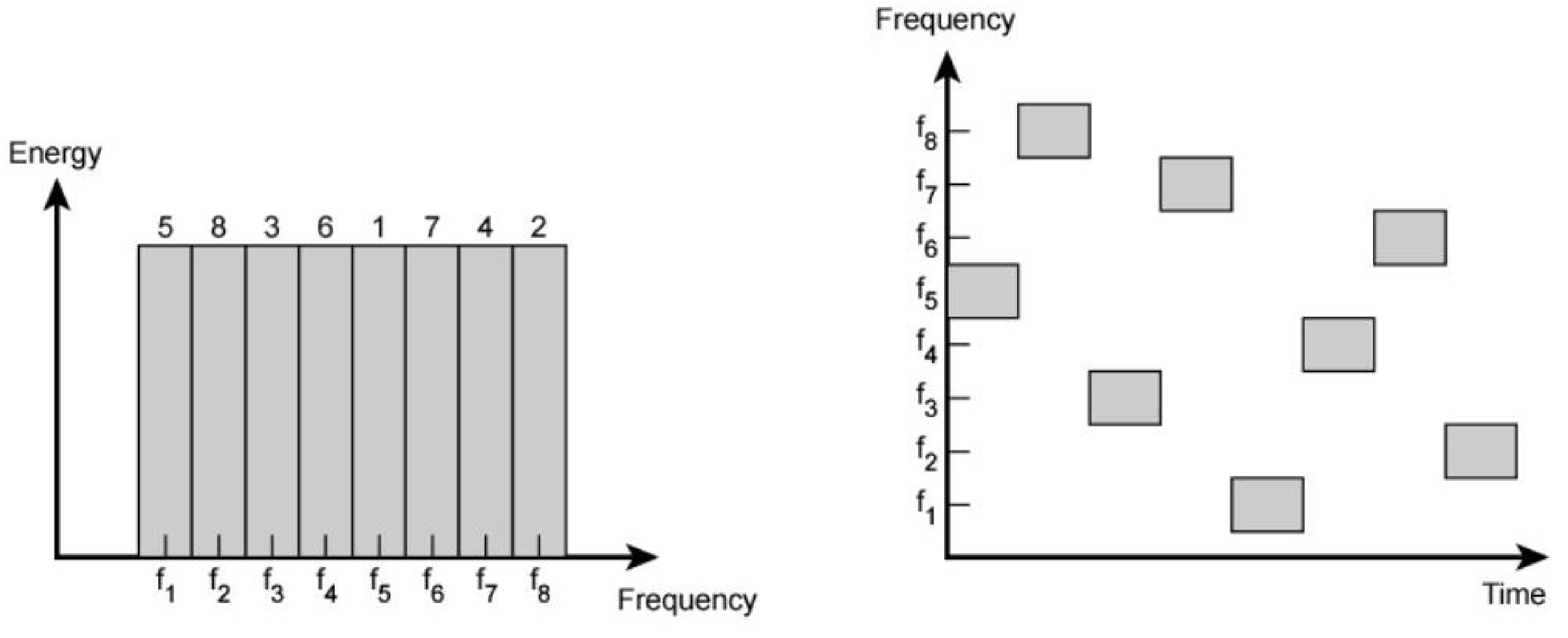


Spread Spectrum

- Frequency Hopping (FHSS)
- Chirp Spread Spectrum (CSS)

- Direct Sequence (DSSS)

Frequency Hopping Spread Spectrum

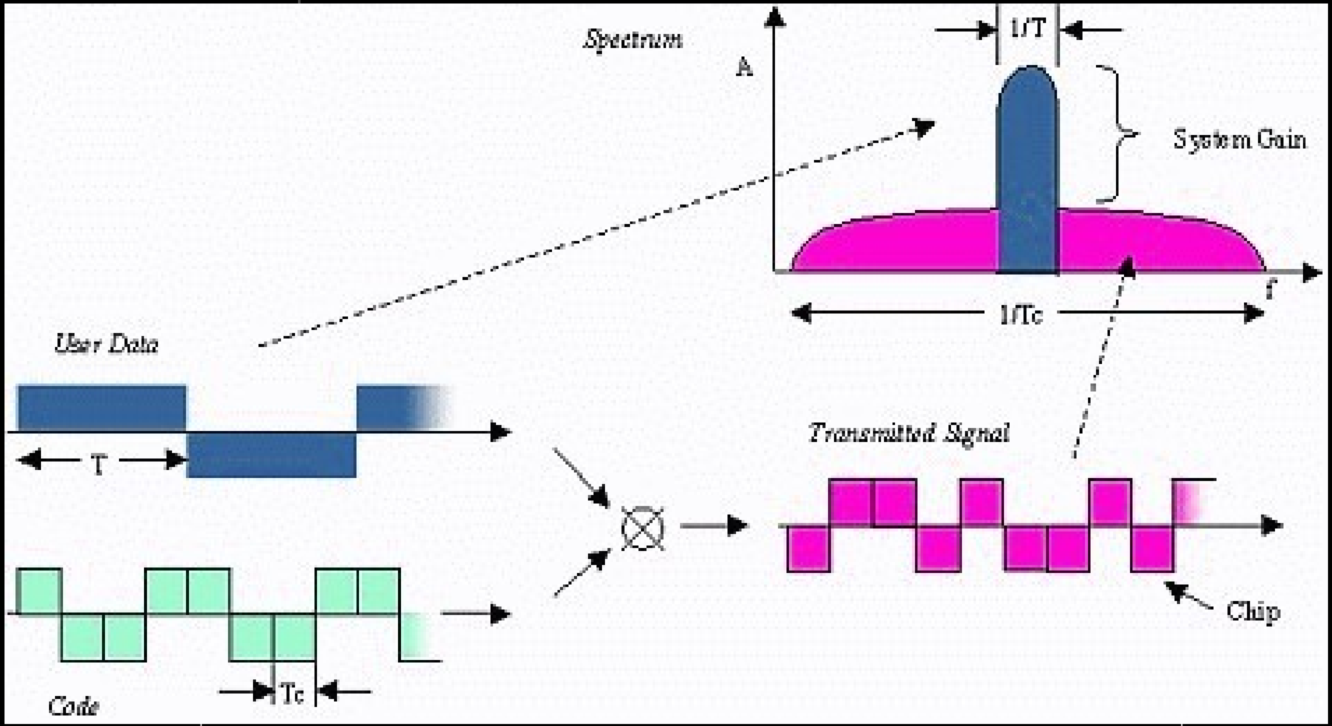


(a) Channel assignment

(b) Channel use

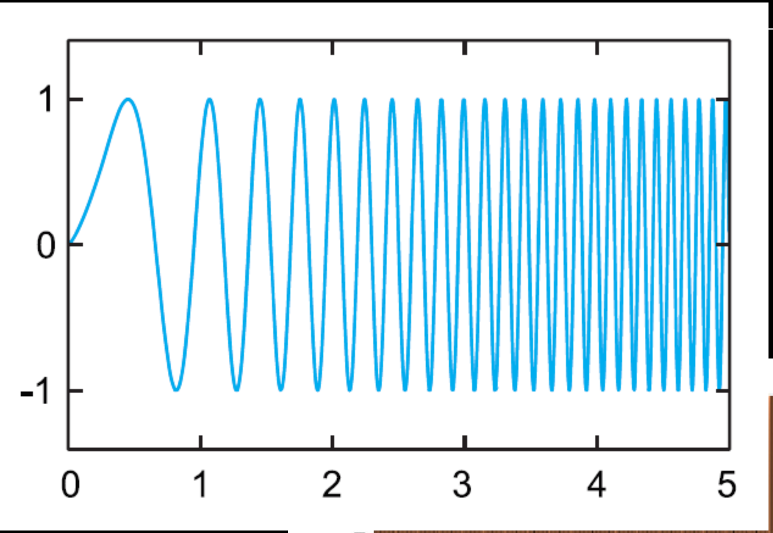
Direct Sequence Spread Spectrum

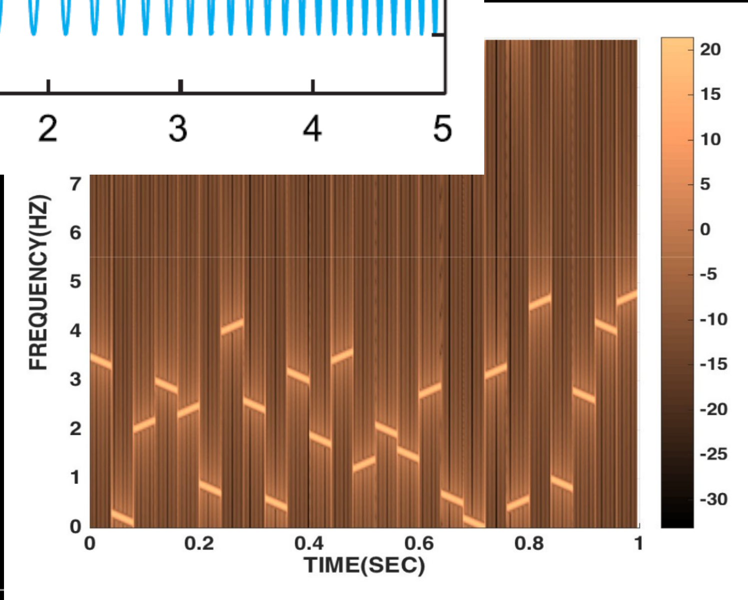
- Multiply signal by spreading sequence
- Flattens frequency spectrum



Chirp Spread Spectrum

- Direction and slope can encode information
- Immune to Doppler shift





Chaos Communications

- A small change to the initial conditions results in a large change to the output.

- Chaos provides an irregular waveform
- Presents synchronization issues

The Situation

The Situation

- Fundamental limits established mathematically

The Situation

- Fundamental limits established mathematically
- Several methods of increase “covertness”

The Situation

- Fundamental limits established mathematically
- Several methods to increase “covertness”
- *No way to evaluate covertness*

The Situation

- Fundamental limits established mathematically
- Several methods of increase “covertness”
- *No way to evaluate covertness*
- *No way to generate optimal covert protocol*

Thesis Question(s)

Thesis Question(s)

- What detection method(s) can Willie employ to best detect LPI/LPD signals?

Thesis Question(s)

- What detection method(s) can Willie employ to best detect LPI/LPD signals?
- Which protocols and techniques can Alice employ to best evade detection (while communicating with Bob with a given probability of error)?

Thesis Proposal

- Create simulation of channel
- Evaluate which techniques increase covertness (while maximizing transmission rate)
- Evaluate which detector(s) work best

Detectors Available to Willie

- Wideband Radiometer (Energy)
- D’Agostino and Pearson’s Normal Test
- Max Cut Detector (Cyclostationary)
- Degree of Cyclostationarity (Cyclostationary)

Detectors Available to Willie

- ✅ Wideband Radiometer (Energy)
- ✅ D’Agostino and Pearson’s Normal Test
- ✅ Max Cut Detector (Cyclostationary)
- ✅ Degree of Cyclostationarity (Cyclostationary)

Protocols Available to Alice and Bob

- Traditional:
  - PSK
  - FSK
  - QAM
- Spread Spectrum
  - CDMA
  - OFDM
  - FH-CSS
- Chaotic
  - Chaotic Multi-Tone (CMT)
  - Differential Chaos Shift Keying (DCSK)
  - FH-OFDM-DCSK
- Other
  - QS-DS-CDMA

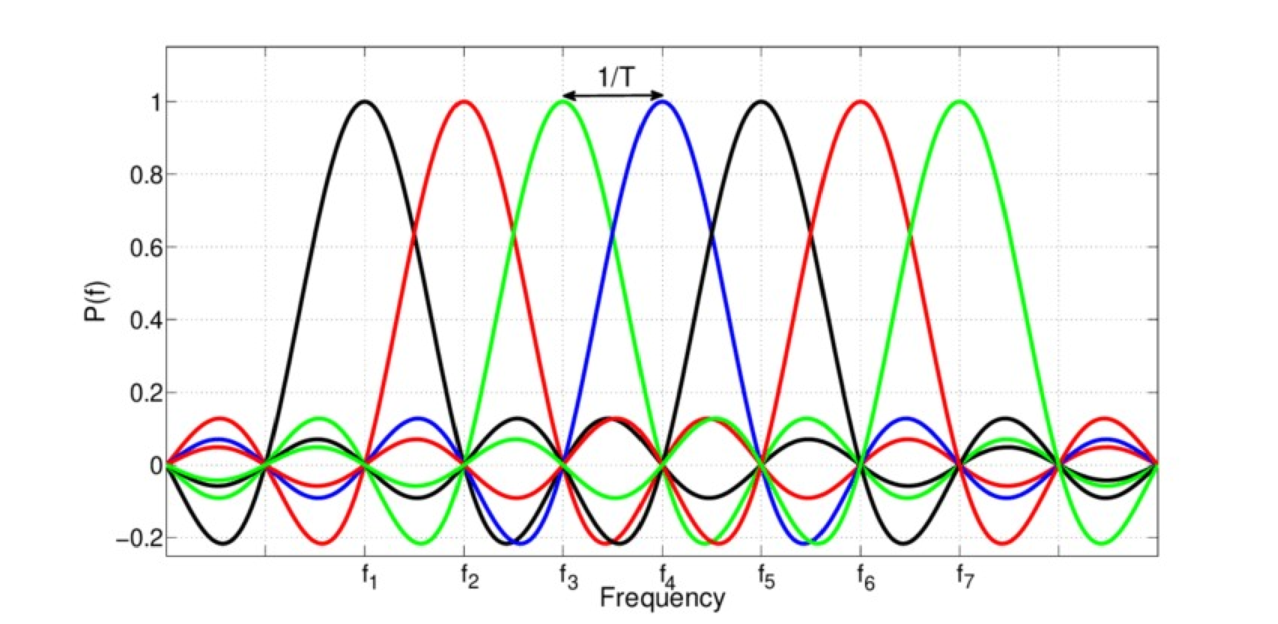
Protocols Available to Alice and Bob

- Traditional:
  - ✅ PSK
  - ✅ FSK
  - ✅ QAM
- Spread Spectrum
  - ✅ CDMA
  - ✅ OFDM
  - FH-CSS
- Chaotic
  - Chaotic Multi-Tone (CMT)
  - ✅ Differential Chaos Shift Keying (DCSK)
  - ✅ FH-OFDM-DCSK
- Other
  - QS-DS-CDMA

Questions?

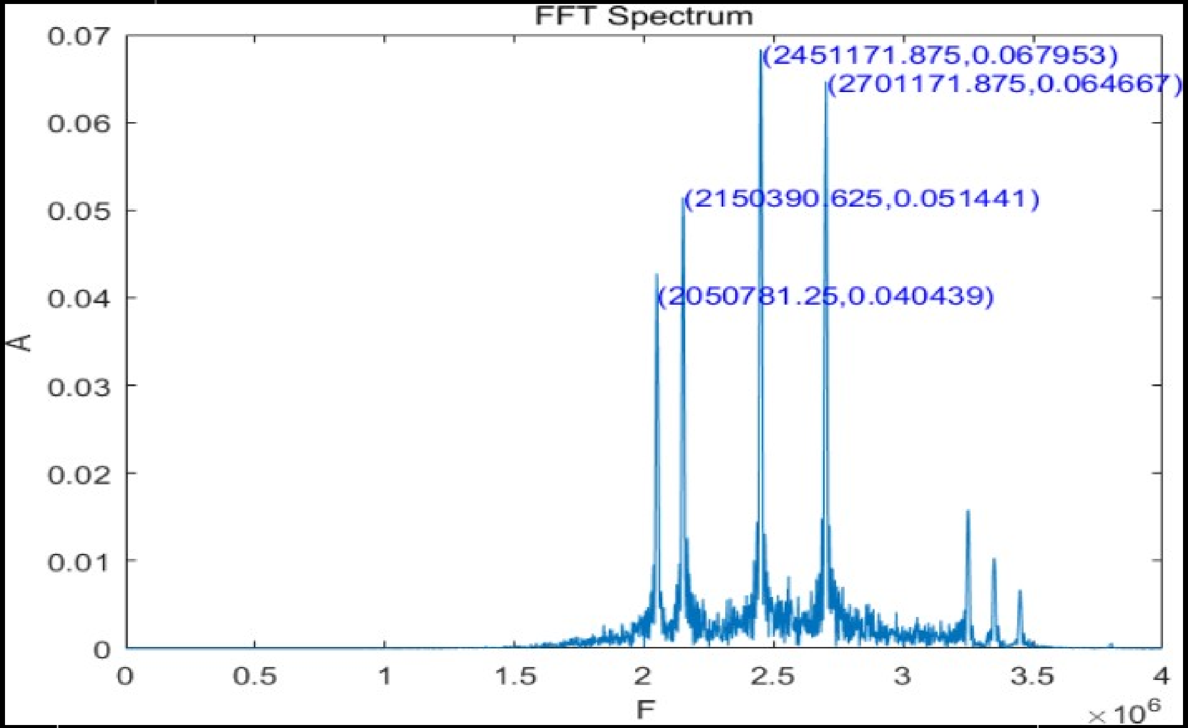
OFDM

- Multiplex bits across orthogonal subcarriers
- Flattens frequency spectrum
- Helps mitigate FSF



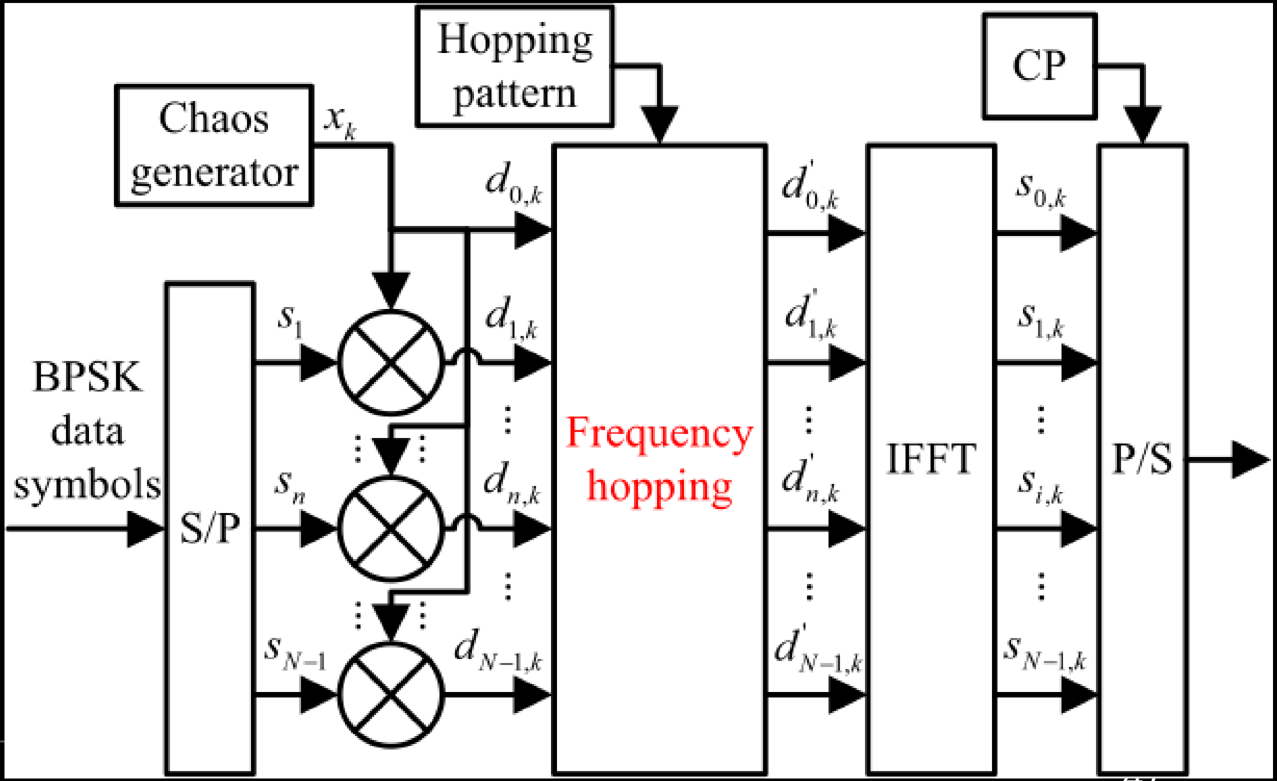
Chaotic Multi Tone

- Chaotically select tone groups to transmit information
- Signal is very random

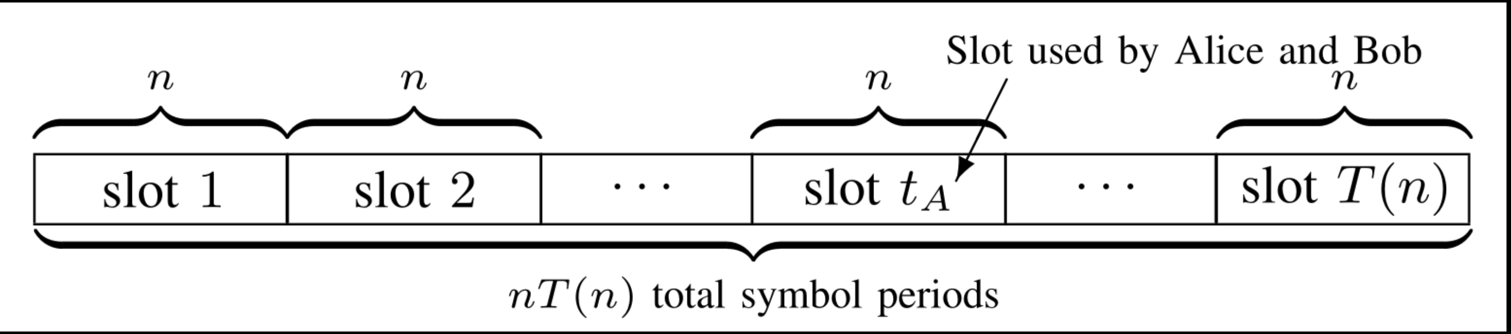


FH-OFDM-DCSK

- Frequency Hopped OFDM Differential Chaos Shift Keying



When Willie Doesn't Know When



- Alice picks one slot out of *T(n)* slots
- She can transmit *O(√n log(T(n)))* bits
- Willie has to monitor every slot.