ECE 495 – Electromagnetic Warfare and Survivability

Block 2: RF Electronic Warfare

Lesson 16: EP for Communications

Juan Jurado, Col, USAF, Ph.D.
Permanent Professor and Head
Electrical and Computer Engineering

Fall 2026

Where We Left Off

L15 protected the **radar**: emit less, spread, hop, and police the side-lobes.

Frequency agility was a hint of the bigger idea — a signal that refuses to sit still in the spectrum. Push that idea all the way and you get **spread spectrum**.

Today: EP for our **links** — keeping comms alive when the enemy jams the band.

Lesson Objectives

By the end of this lesson, you will be able to:

- Explain why a **narrowband link** is easy to jam and intercept
- Describe **DSSS** and **FHSS** as spread-spectrum techniques
- Compute **processing gain** and relate it to a survivable J/S
- Explain how a signal can hide **below the noise floor**

A Link Is a Target Too

A datalink only helps if the message gets through. A plain narrowband signal makes that easy to stop:

- All its energy sits in one small band — **easy to find** and intercept
- A jammer puts all its power on that band — **easy to deny**
- Encryption hides the *message*, not the *signal* — the link still gets jammed

You can encrypt what you say and still be silenced.

Spread Spectrum: The Big Idea

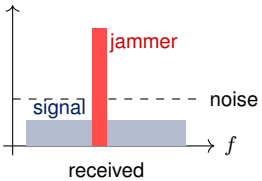
Take the signal and **smear** it across a band far wider than the data needs, using a code both ends share.

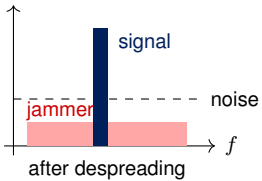
- The code (the “key”) spreads energy until the signal looks like **noise**
- No single slice of spectrum carries much power — hard to find, hard to jam
- Only a receiver with the *same code* can pull the signal back together

Two ways to do it: spread in **code** (DSSS) or spread in **frequency** (FHSS).

Processing Gain

$$G_p = 10\log_{10}\frac{B_{\text{spread}}}{B_{\text{data}}} = 10\log_{10} N_{\text{chips}} \qquad \text{(typically 10–60 dB)}$$





Despreading **concentrates the signal** and **spreads the jammer** — so the link survives even when J/S is positive.

DSSS: Direct Sequence

Multiply each data bit by a fast **pseudo-noise (PN)** chip sequence.

- N chips per bit spreads the bandwidth by N — and sets the processing gain
- The receiver multiplies by the *same* PN code and integrates per bit
- Signal chips line up and add; the jammer, uncorrelated with the code, gets spread

Same code at both ends: the signal re-collapses, the jammer smears out.

FHSS: Frequency Hopping

Instead of spreading every instant, **hop** the carrier across many channels on a code-driven schedule.

- The transmitter and receiver hop together; an eavesdropper sees only fragments
- A spot jammer cannot follow — the same lose-lose we built in L15
- Spread is over *time and frequency*, not code — but the payoff is the same J/S relief

DSSS and FHSS are two routes to one goal: a moving, noise-like signal.

Below the Noise Floor

With enough processing gain, a signal can live *below* the noise floor.

- **GPS** arrives below the noise floor; the code digs it back out
- If the threat cannot *find* the signal, it cannot intercept or jam it well
- This is **low probability of detection** — the comms cousin of LPI radar

You cannot jam what you cannot find.

Today's Interactive Demo: Beat the Jammer with Code

Today's interactive demo.

- Send bits over a narrowband link with a jammer **12 dB above** the signal — it dies
- Spread the same bits with a 64-chip PN code, then despread
- Watch the bit error rate collapse — $10 \log_{10} 64 \approx 18$ dB of processing gain

Companion script: `L16_DSSSProcessingGain.m`

The jammer never loses a watt. The code wins anyway.

Quick Exercise / Type-along: Size the Gain

A protected B-21 datalink uses DSSS. Reason about each:

1. The code runs 1000 chips per bit. What is the processing gain in dB?
2. A jammer sits 20 dB above your signal. With that gain, can the link close?
3. The enemy cannot even detect your transmission. Which EP property is that?
4. Why does encrypting the message not, by itself, defeat a jammer?

Wrap-Up

Key ideas:

- A narrowband link is easy to find and easy to jam
- Spread spectrum hides the signal in a wide, noise-like band
- Processing gain $= 10 \log_{10} N$ — it buys a survivable J/S
- DSSS spreads in code, FHSS in frequency; both can hide below the noise

Next lesson:

- **L17: Electromagnetic Attack** — jamming taxonomy, J/S, burn-through range
- Pre-flight quiz for L17 due before class