Wireless Network Security
Spring 2016

Patrick Tague

Class #4 – Physical Layer Threats; Jamming

©2016 Patrick Tague

Class #4

- PHY layer basics and threats
- Jamming

 ©2016 Patrick Tague

PHY

©2016 Patrick Tague

Wireless PHY

- The wireless PHY is responsible for delivering a bit stream from a transmitter to one or more receivers. It's not as easy as it sounds.

- Tx/Rxs need to be coordinated in time, space, frequency, phase, encoding/language

- Wireless means there are many sources of error, reasons for failure, etc.

PHY Standards

- In WiFi networks, IEEE 802.11 defines several versions of the PHY, including extensions for mesh, vehicular, etc.
- In telecom, the GSM 05.xx series defines the Um physical layer, and other standards build on it, including ITU-T standards like 4G.
- In PANs, standards like 802.15.1 (Bluetooth), .3 (high-rate, e.g., UWB), and .4 (low-rate, e.g., Zigbee) all define their own PHY models.

©2016 Patrick Tague

Wireless PHY Services

- Various parts of PHY operation:
  - Radio interface: spectrum allocation, signal strength, bandwidth, carrier sensing, phase sync, …
  - Signal processing: equalization, filtering, training, pulse shaping, signaling, …
  - Coding: channel coding, bit interleaving, fwd error correction, …
  - Modulation (mapping bits to signals)
  - Topology, antennas, duplex/simplex, multiplexing, and so much more
- PHY is typically the most complex part of a wireless network

©2016 Patrick Tague

What are the basic threats faced at the PHY layer?

©2016 Patrick Tague

Back to the Party

©2016 Patrick Tague

Physical Layer Misbehavior

- Open, shared medium is vulnerable
  - Anyone can "talk" → greedy or malicious nodes can easily interfere
    - Prevention/degradation of communication via jamming
    - Cutting off available resources influences network control, operation, and performance
  - Anyone can "listen" → curious or malicious nodes can easily eavesdrop on communication
    - Recovery of information exchanged by neighbors (violation of data, identity, operation/intention privacy)
    - Inference/learning, tracking, observing

©2016 Patrick Tague

Challenges

- How can we prevent a curious or malicious party from eavesdropping on wireless transmissions at the physical layer?
- How can we prevent a greedy or malicious party from interfering with PHY transmission and reception?
- For both:
  - Short answer, we can't
  - However, we can make it much more difficult

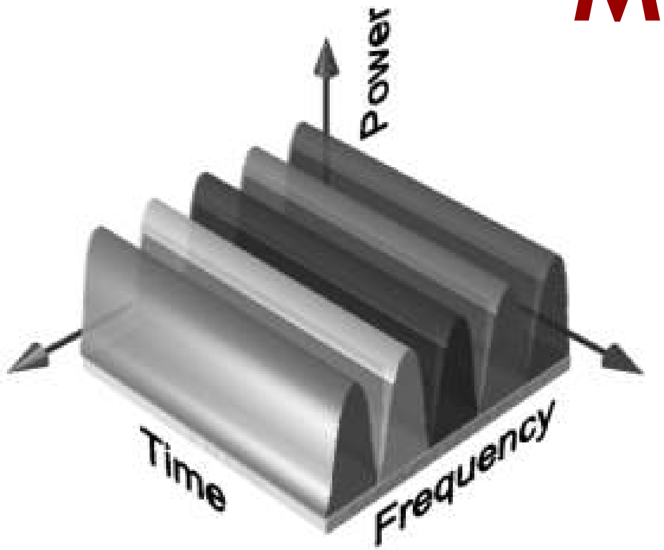
©2016 Patrick Tague

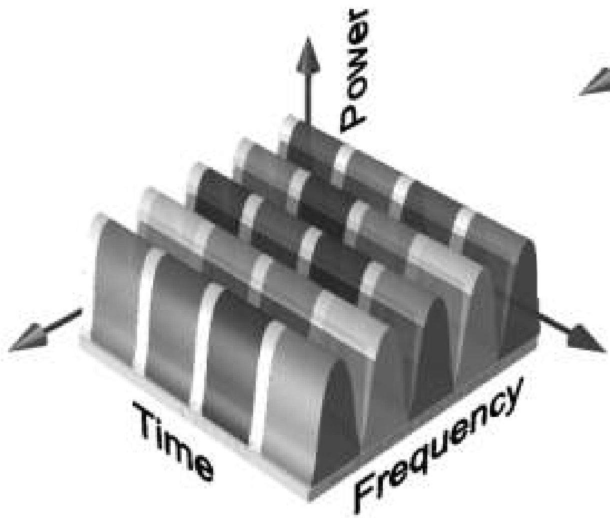
Spread Spectrum

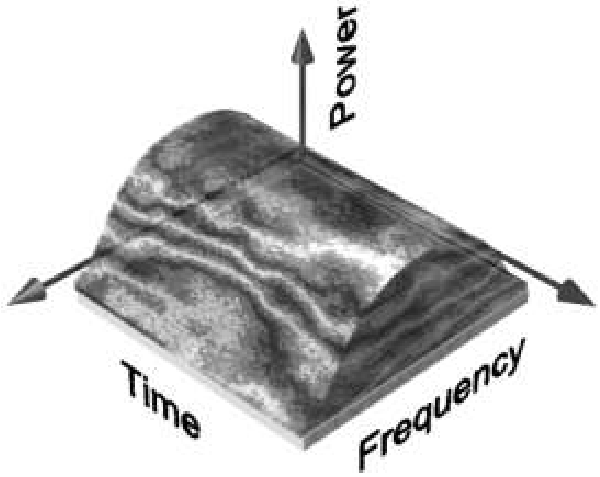
- Spread spectrum is an extension of multiplexing that uses randomization to increase diversity and improve performance in various ways
  - Frequency-hopping spread spectrum (FHSS) builds on FDM allowing devices to pseudo-randomly move among frequency channels
    - If one channel is particular good or bad, everyone shares it randomly
  - Direct-sequence spread spectrum (DSSS) builds on CDM allowing devices to pseudo-randomly move among different code spaces
    - Code spaces are analogous to frequency bands

©2016 Patrick Tague

Multiplexing







FDM – frequency division multiplexing

TDM – time division multiplexing (flip x-y)

TDM + FDM as in GSM

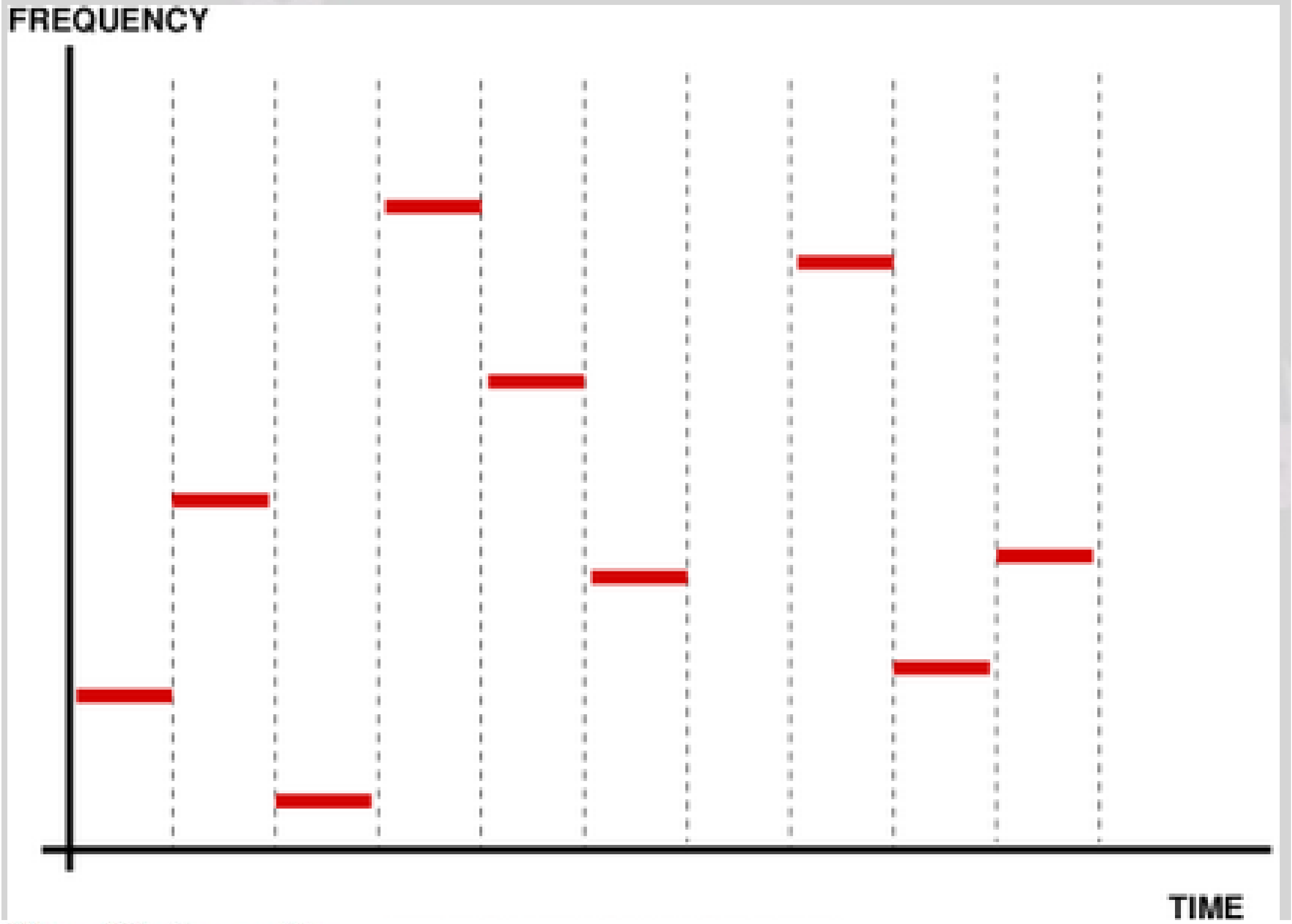
CDM – code division multiplexing

images from [Erik Lawrey; SkyDSP.com]

©2016 Patrick Tague

FHSS

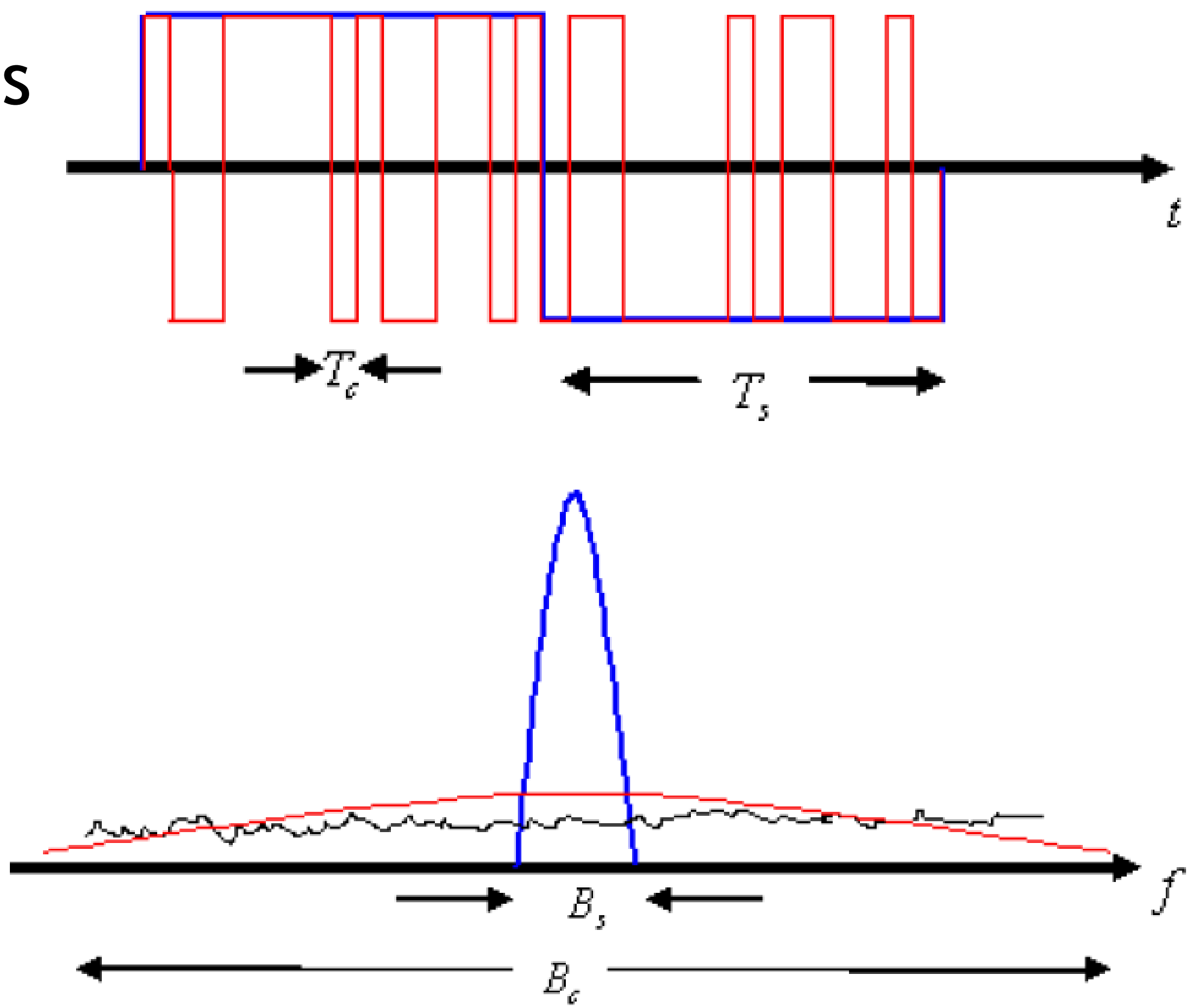
- FHSS: Sender and receiver synchronize a hopping pattern over a large bandwidth



©2016 Patrick Tague

DSSS Encoding

- DSSS encoding maps long symbols to sequences of short chips
- Shorter chip duration means wider bandwidth



©2016 Patrick Tague

Benefits

- FHSS:
  - Narrow-band interference only has an effect for a small fraction of the time
  - Single-channel eavesdroppers can't "follow" the signal, need to use much wider bandwidth to hear everything
- DSSS:
  - Narrow-band interference is "despread" at the receiver, more like quiet wide-band noise
  - Other signals are (nearly) orthogonal
  - Eavesdropper has to know/guess code to decode

©2016 Patrick Tague

Cryptographic SS

- Building off basic spread spectrum, we can add cryptographic randomization to make hopping schedule and code sequences secret
  - Using a symmetric key as a seed to a PRNG makes the hopping schedule or code sequence secret

- In both cases, this requires symmetric key management, which has its own issues

©2016 Patrick Tague

Issues with Spread Spectrum

- To be effective against curiosity/greed/malice, hopping sequences (FHSS) and spreading codes (DSSS) must be **private**
  - In many implementations, these codes are given to all group members – if becoming a group member is easy, there's no barrier
  - If group membership is tightly guarded, can it be bought or stolen?
- If codes can't be obtained, can they be learned?
  - Code reuse allows for statistical analysis and recovery

©2016 Patrick Tague

Further Hardening the PHY

- If spread spectrum isn't enough, what else?
  - Multiple diversity can protect against multiple threats at numerous levels
  - Implementations must consider the threat models and adapt to unexpected behaviors
    - Prevent statistical analysis, adapt to learning adversaries

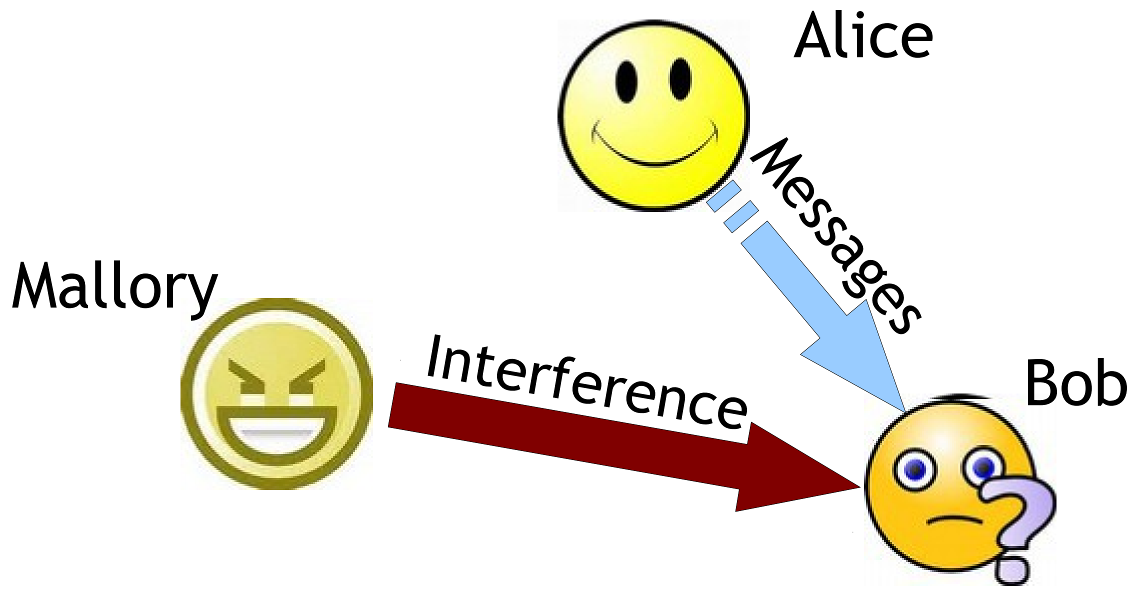
©2016 Patrick Tague

Let's focus on Jamming

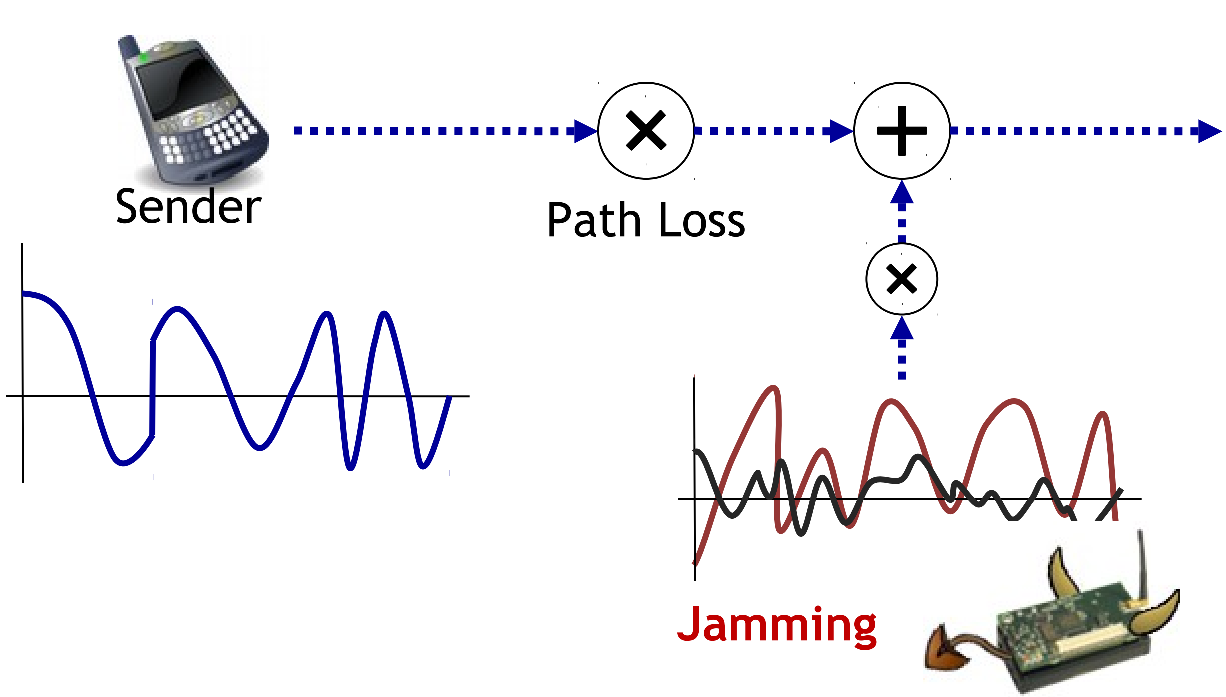
©2016 Patrick Tague

Jamming

- Conceptually, jamming is a physical layer denial-of-service attack that aims to prevent wireless communication between parties



How Does Jamming Work?



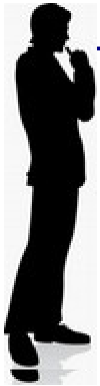
Receiver can decode message if *SINR* ≥ τ

Jamming decreases *SINR*, causes ***decoding failure*** and ***packet loss***

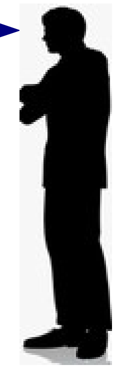
But, it's much more complicated than that…

©2016 Patrick Tague

Geometry Matters



Attacker can be MUCH quieter than speaker



SINR metric captures effects of geometry

SINR = (Rx signal power) / (noise power + Rx jamming power)

Often modeled as $P_{tr} = k_t P_t d_{tr}^{-\alpha}$

Typically random variable N_0

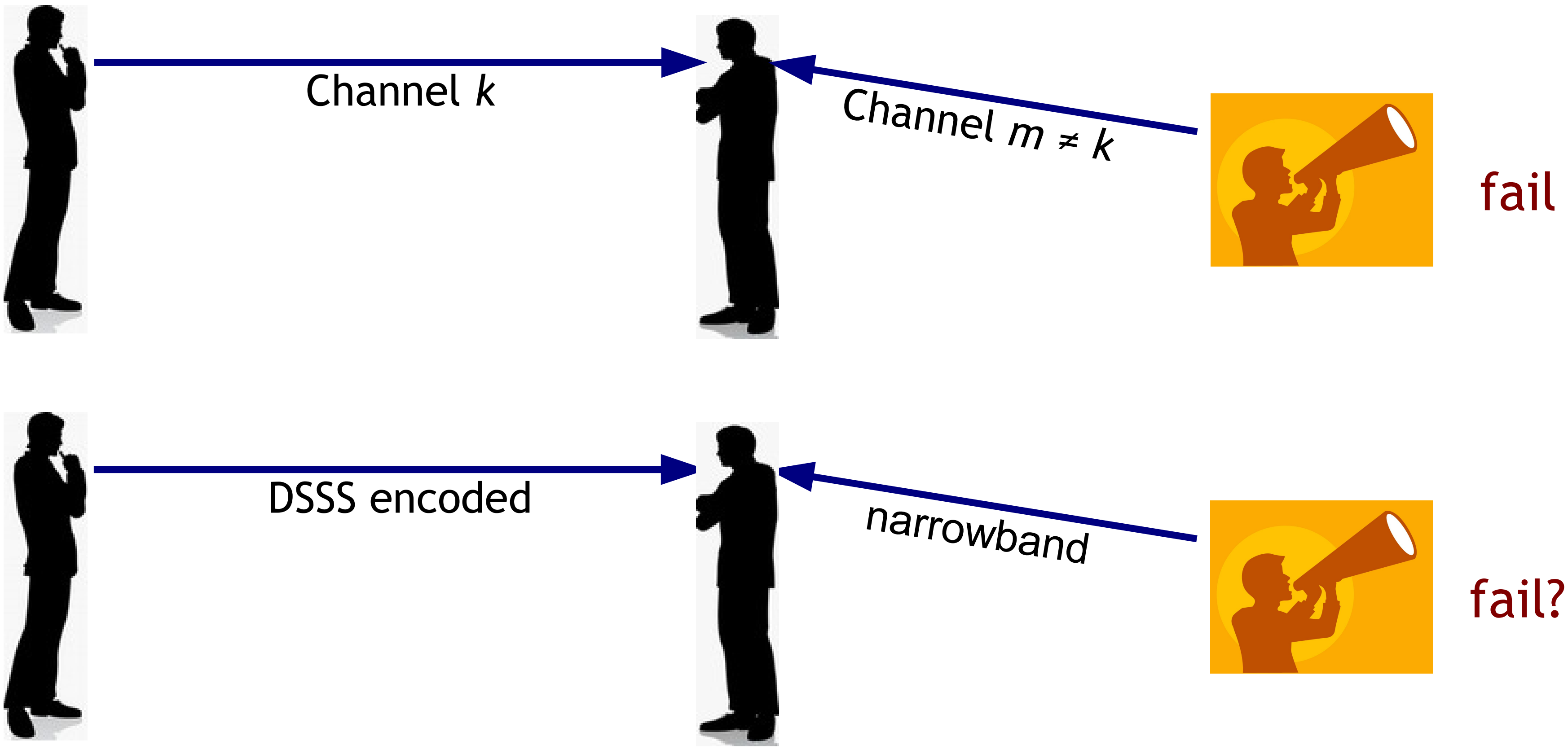
Often modeled as $P_{jr} = k_j P_j d_{jr}^{-\alpha}$

©2016 Patrick Tague

Timing Matters

Can be modeled as a (random) multiplier in the "I" term of the SINR metric

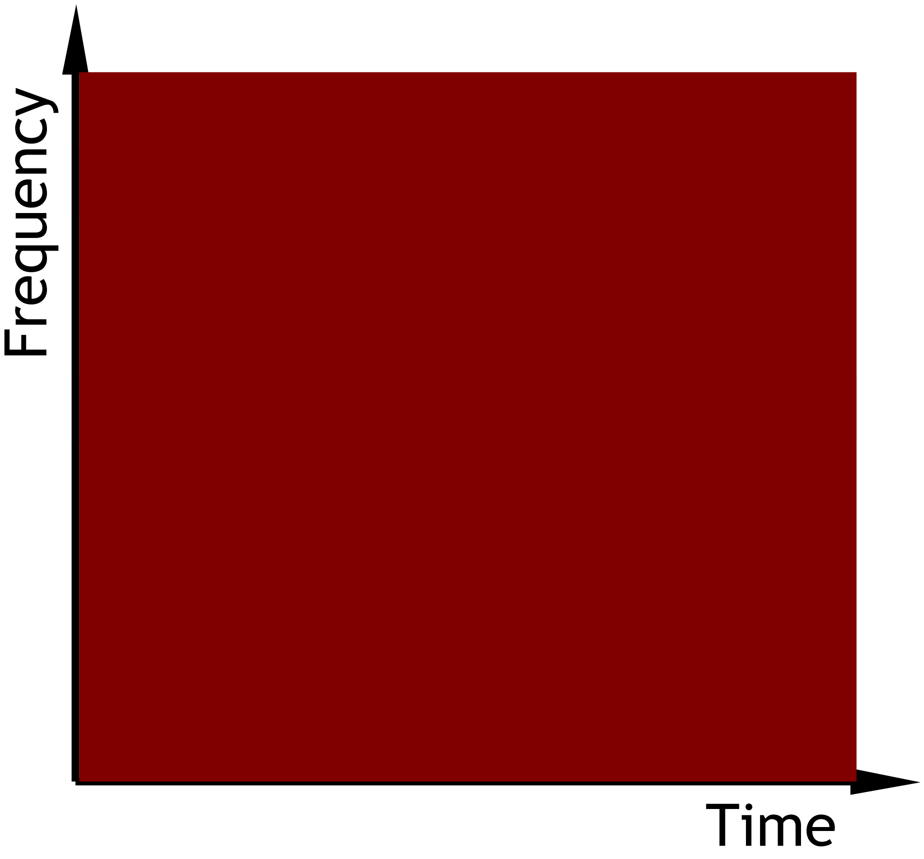
Orthogonality Matters



©2016 Patrick Tague

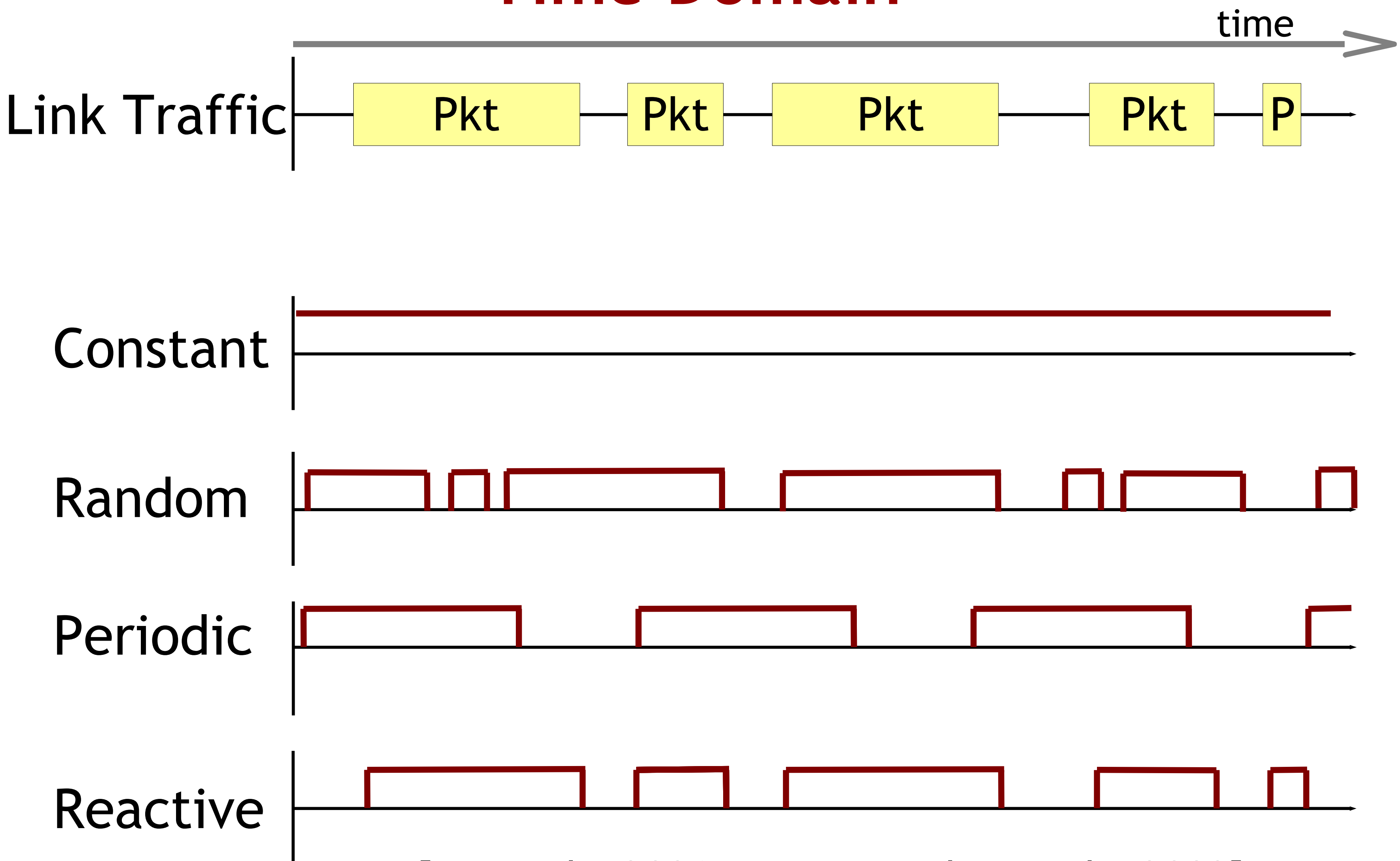
Generalized Jamming

- A jammer allocates energy/signal to diverse time, freq, etc. resources according to an attack strategy *S*
  - Effect *E*(*S*) of the attack
  - Cost *C*(*S*) of the attack
  - Risk *R*(*S*) of being detected / punished
  - With other metrics, an optimization emerges



Jamming Strategies

Time Domain

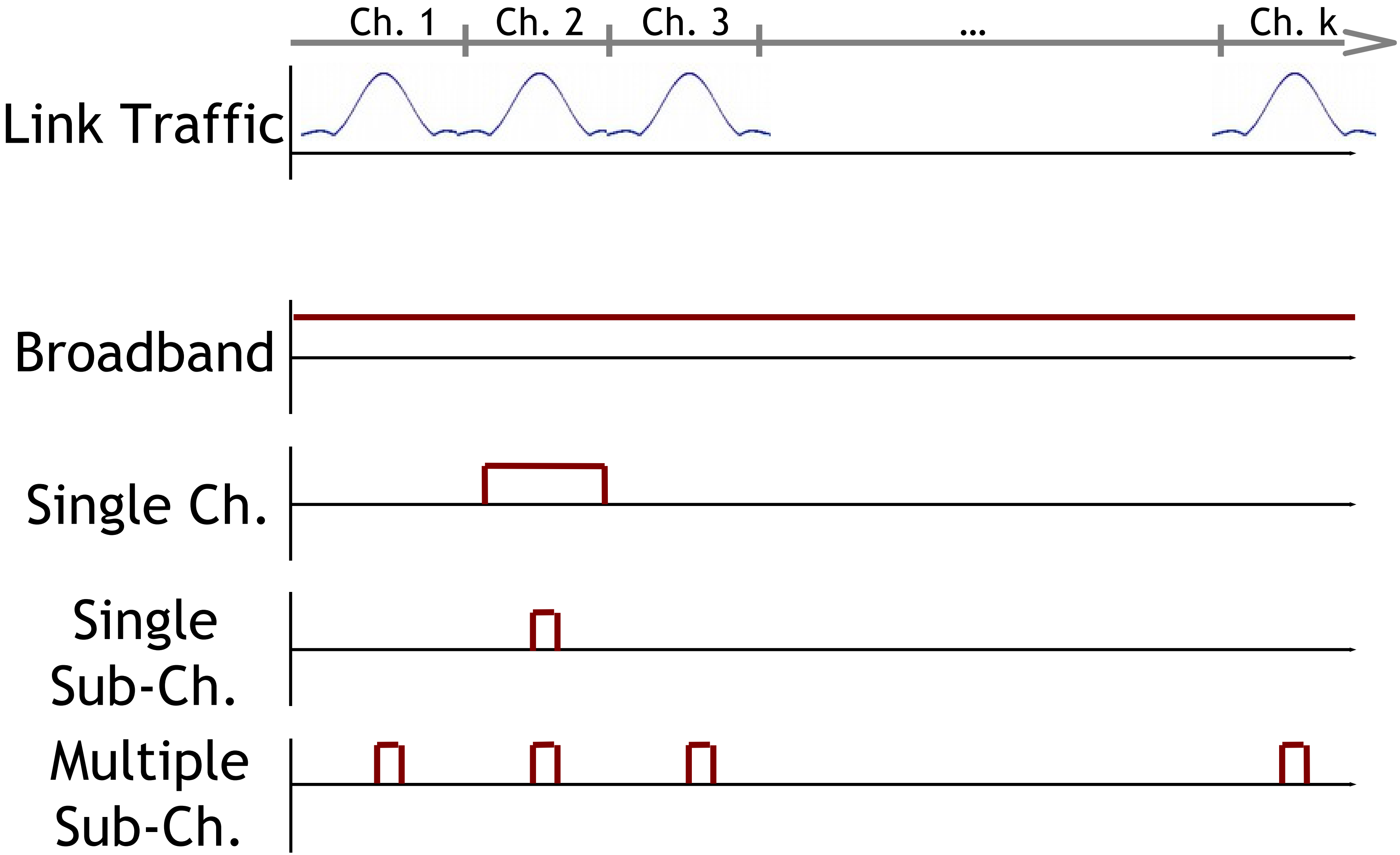


[Xu et al., 2006; Mpitziopoulos et al., 2009]

©2016 Patrick Tague

Jamming Strategies

Frequency Domain



©2016 Patrick Tague

January 26:
Jamming (cont'd); Physical Layer Security

©2016 Patrick Tague