

Wireless Network Security and Privacy

Physical Layer Threats; Jamming

Xiaoyu Ji 冀晓宇

Department of Electrical Engineering
Zhejiang University

2025 Autumn

PHY

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.

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

How to deal with a noise or imperfect wireless channels?

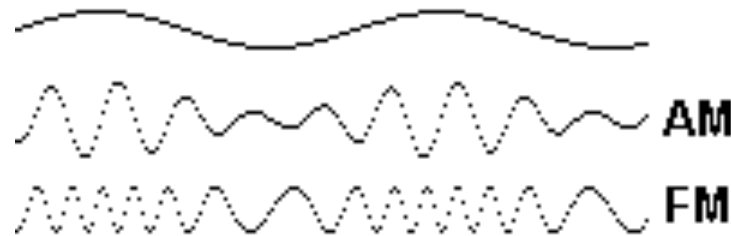
MODULATION

Baseband vs. Carrier Modulation

- **Modulation:** is the process of varying one or more properties of a periodic waveform, called the **carrier signal**, with a separate signal called the **modulation signal** that typically contains information to be transmitted.
- Baseband modulation: send the “bare” signal
- Carrier modulation: use the signal to modulate a higher frequency signal (carrier).
 - Can be viewed as the product of the two signals
 - Corresponds to a shift in the frequency domain

Modulation

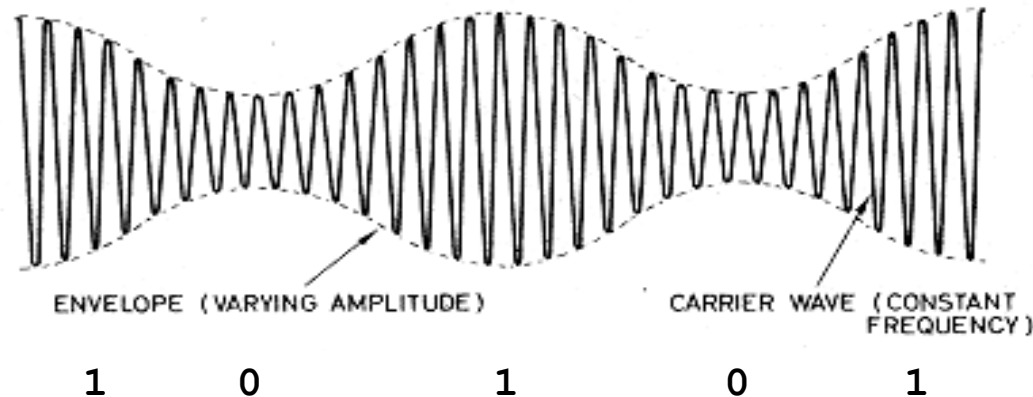
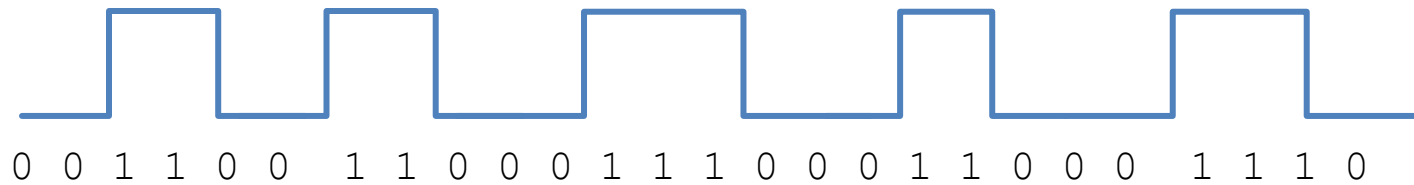
- Changing a signal to convey information
- Ways to modulate a sinusoidal wave
 - Volume: Amplitude Modulation (AM)
 - Pitch: Frequency Modulation (FM)
 - Timing: Phase Modulation (PM)



- In our case, modulate signal to encode a “0” or a “1”. (multi-valued signals sometimes)

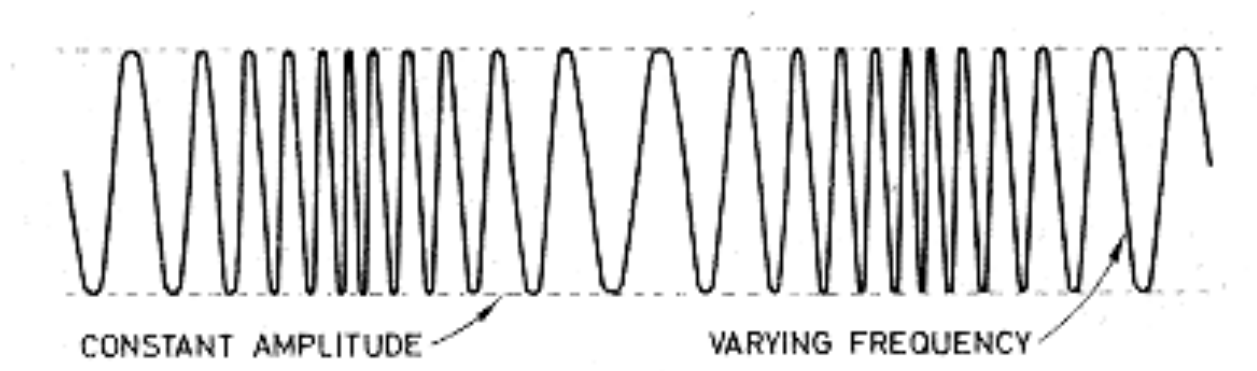
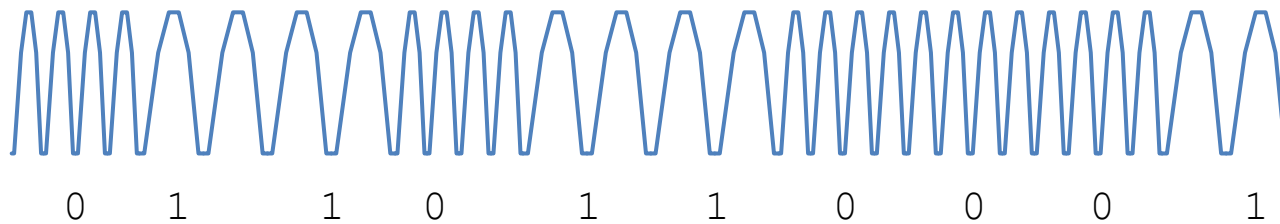
Amplitude Modulation

- AM: change the strength of the signal.
- Example: High voltage for a 1, low voltage for a 0



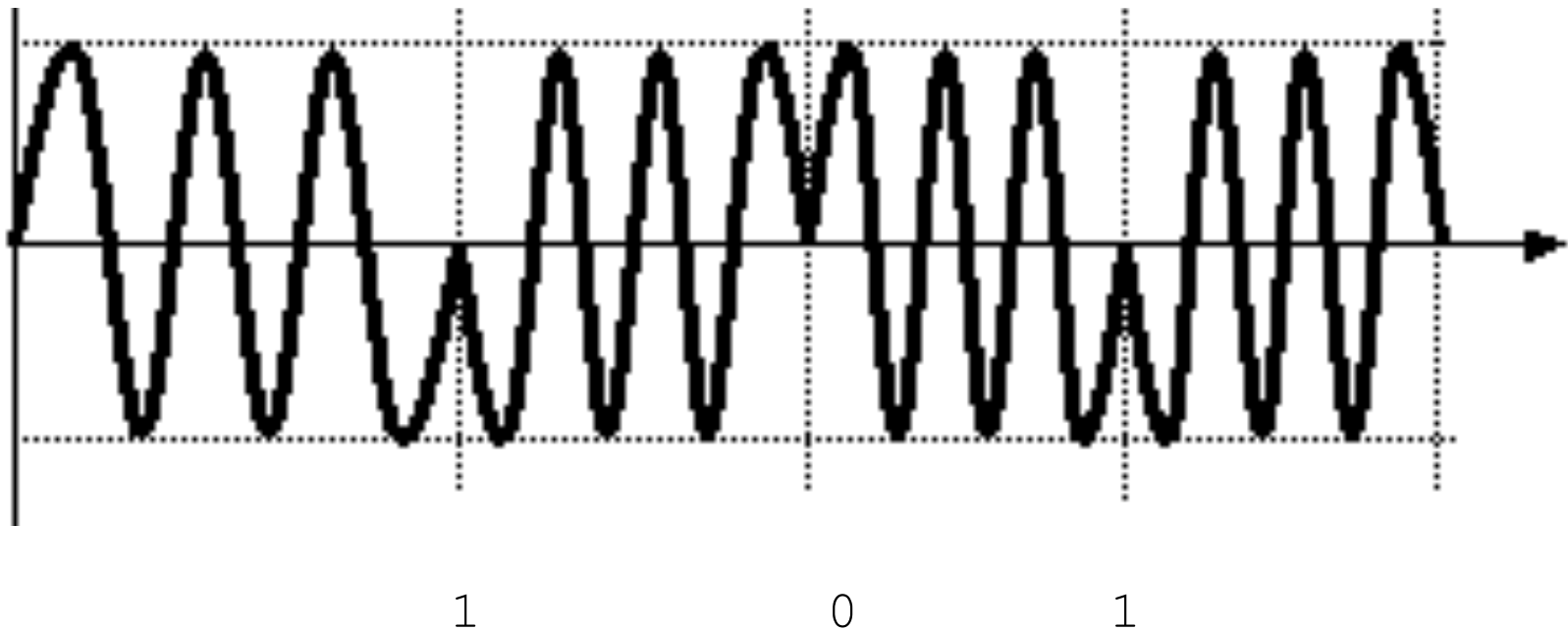
Frequency Modulation

- FM: change the frequency



Phase Modulation

- PM: Change the phase of the signal



How wo regulate wireless vendors?

WIRELESS STANDARDS

Standards

- Availability of interoperable equipment from **multiple vendors**
- Prevents a “Tower of Babel” situation
 - Equipment from different vendors will interoperate if it complies with the standard
 - Alliances and certification bodies assure interoperability
 - Wi-Fi for 802.11
- Lowers costs to consumers
 - Both through competition and economies of scale
- Fight for standards from countries, e.g, in 5G.

IEEE 802 Standards

Maintained by IEEE 802 LAN/MAN Standards Committee (LMSC):

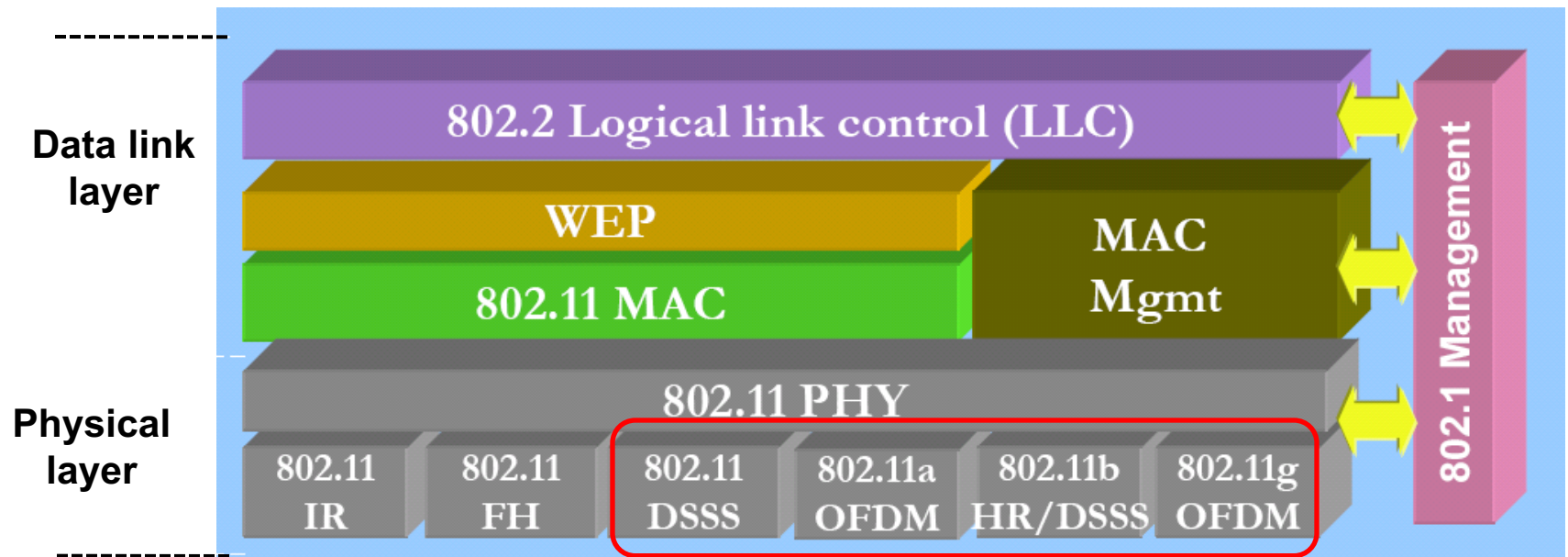
- 802.1 Overview, Architecture, Internetworking and Management
- 802.2 Logical Link Control
- **802.3 Ethernet (CSMA/CD PHY and MAC)**
- 802.5 Token Ring PHY and MAC
- **802.11 Wireless LAN-Wi-Fi**
- 802.12 Demand Priority Access
- **802.15 Wireless PAN**
- **802.16 Broadband Wireless Access**
- 802.17 Resilient Packet Ring
- 802.18 Radio Regulatory
- 802.19 Coexistence
- **802.20 Mobile Broadband Wireless Access**
- 802.21 Media Independent Handoff
- 802.22 Wireless Regional Area Network

Typical Standards and Protocols

802.11 Wi-Fi as an example

802.11

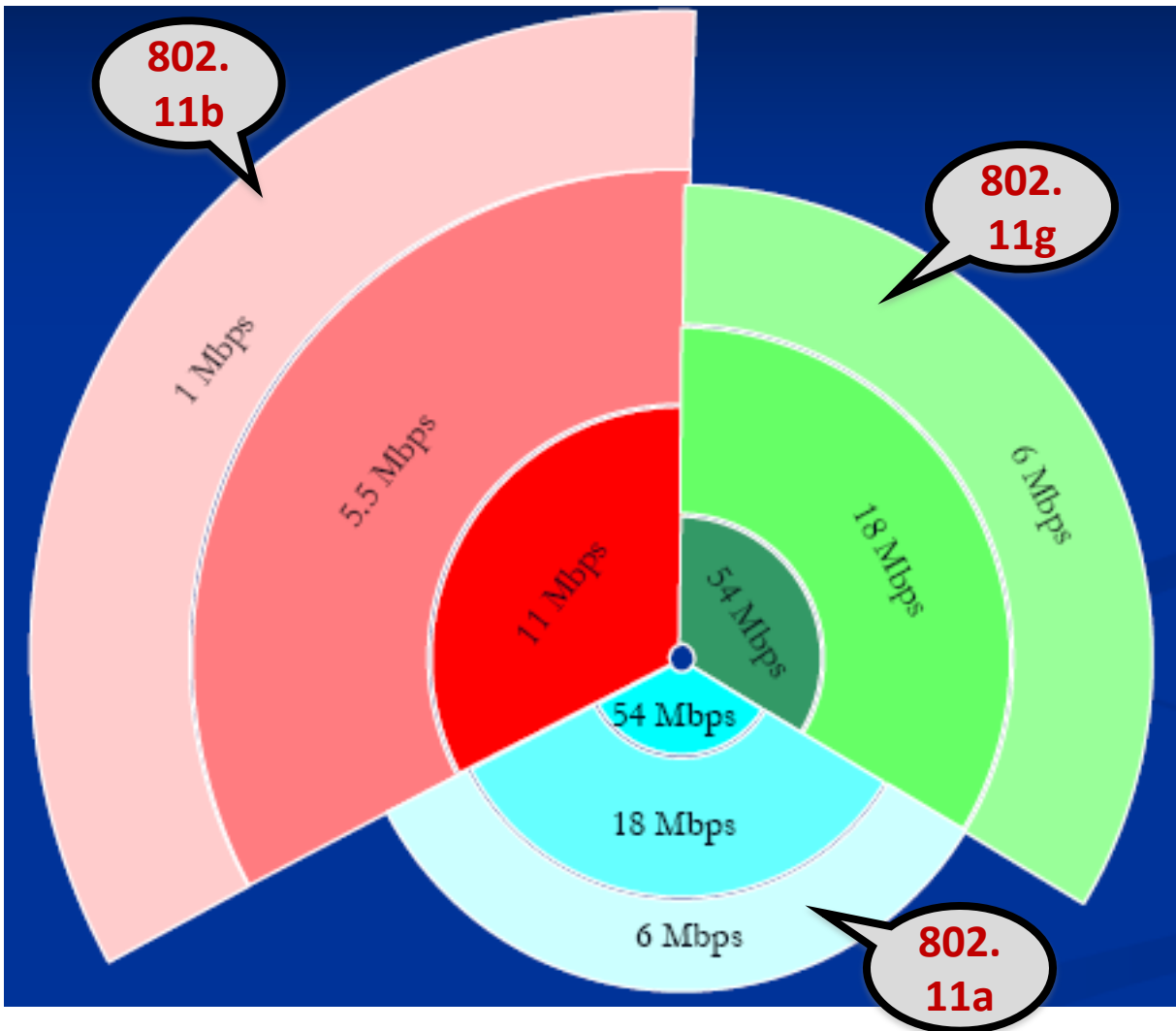
- 802.11 data link and physical layer have a lot of members...



Wireless “Alphabet Soup”

- Q: What is Wi-Fi?
- A: Wi-Fi is a family of wireless network protocols based on the IEEE 802.11 family of standards, especially with specially designed physical layers, including:
 - 802.11b:
 - Most common wireless protocol. Uses 2.4GHz frequency, with 1, 2, 5.5, 11 Mbps bandwidth. (5 Mbps is more typical).
 - 802.11a:
 - Uses 5.5GHz range, 54 Mbps bandwidth (~20 Mbps is typical performance). Produces too much radio power to be certified in medical areas.
 - 802.11g:
 - Uses 2.4GHz band and is compatible with 802.11b. Also 54 Mbps bandwidth (~20 Mbps typical)
- Almost a~z are all used!

802.11 Range



802.11 b	
1	410 ft
5.5	310 ft
11	160 ft
802.11 g	
6	300 ft
18	210 ft
54	90 ft
802.11 a	
6	210 ft
18	150 ft
54	60 ft

What are the basic threats
faced at the PHY layer?

Back to the Party



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

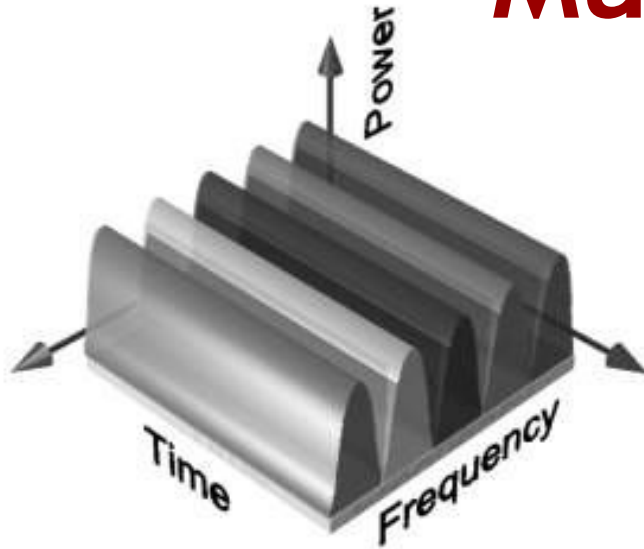
Challenges

- 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

Spread Spectrum

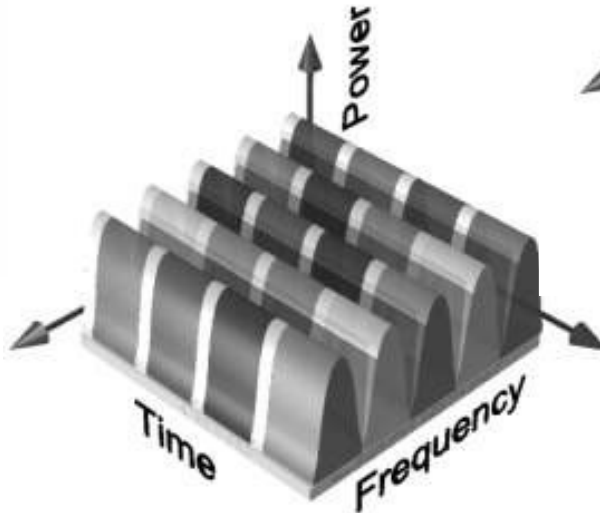
- Spread spectrum is an extension of multiplexing that uses randomization to increase diversity and improve performance in various ways
 - Frequency-hopping spread spectrum (FHSS) builds on FDM allowing devices to pseudo-randomly move among frequency channels
 - If one channel is particular good or bad, 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

Multiplexing

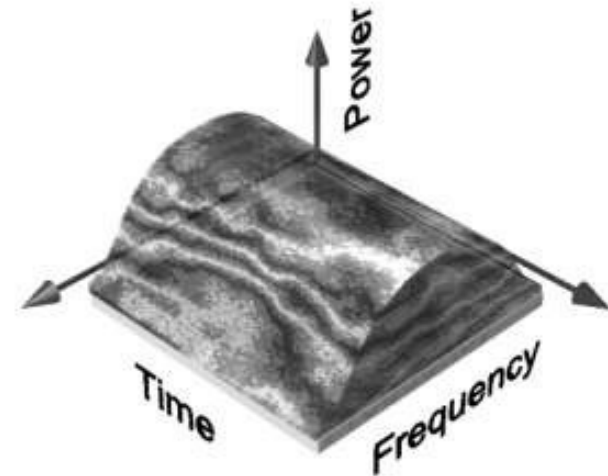


FDM - frequency
division multiplexing

TDM - time division
multiplexing (flip x-y)



TDM + FDM
as in GSM

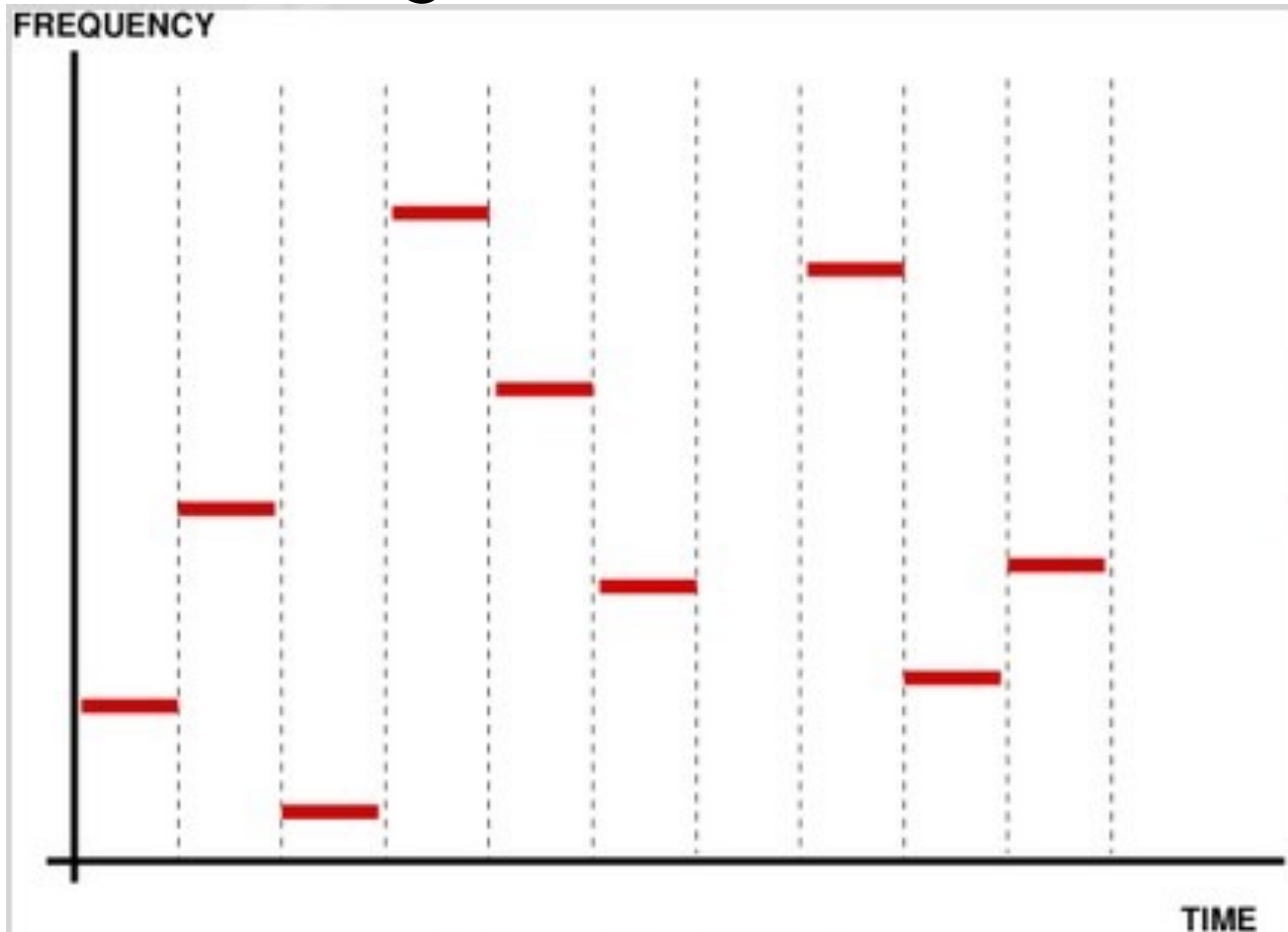


CDM - code division
multiplexing

images from [Erik Lawrey; SkyDSP.com]

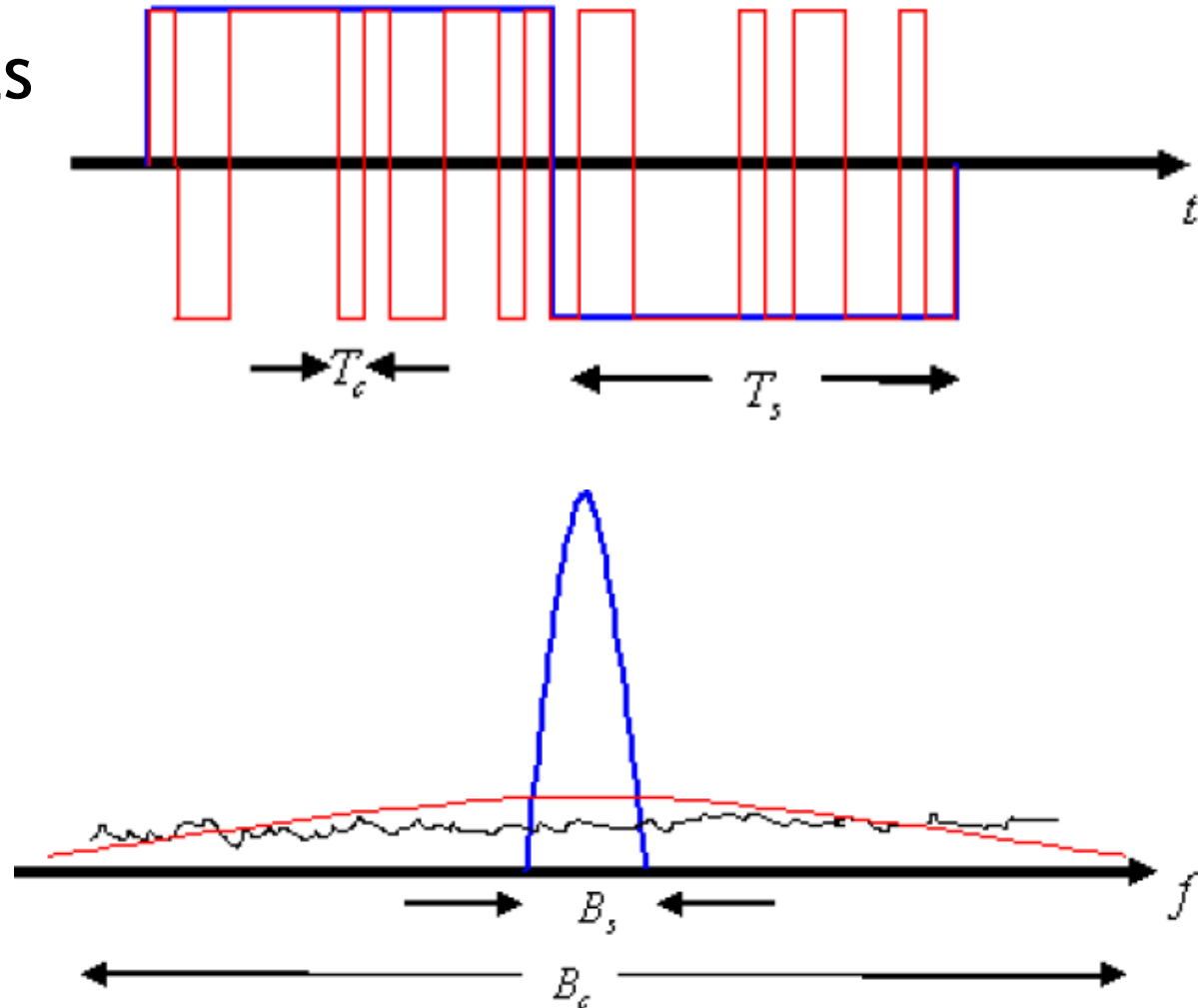
FHSS

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



DSSS Encoding

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



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

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 pseudo random number generator (PRNG) makes the hopping schedule or code sequence secret
- In both cases, this requires symmetric key management, which has its own issues

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

Further Hardening the PHY

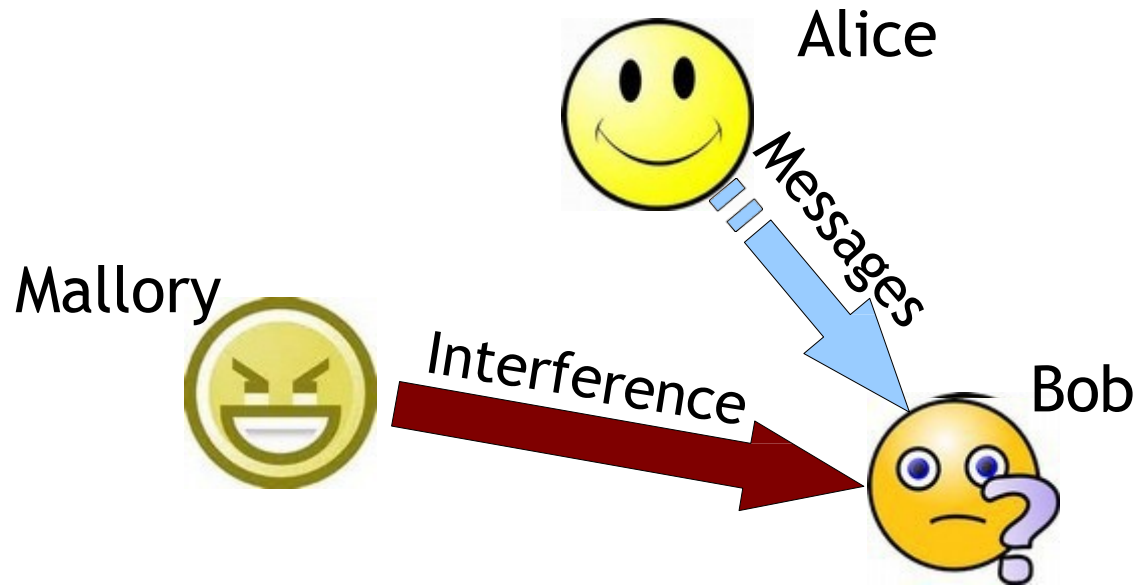
- If spread spectrum isn't enough, what else?
 - Multiple diversity can protect against multiple threats at numerous levels
 - Implementations must consider the threat models and adapt to unexpected behaviors
 - Prevent statistical analysis, adapt to learning adversaries

Let's focus on Jamming

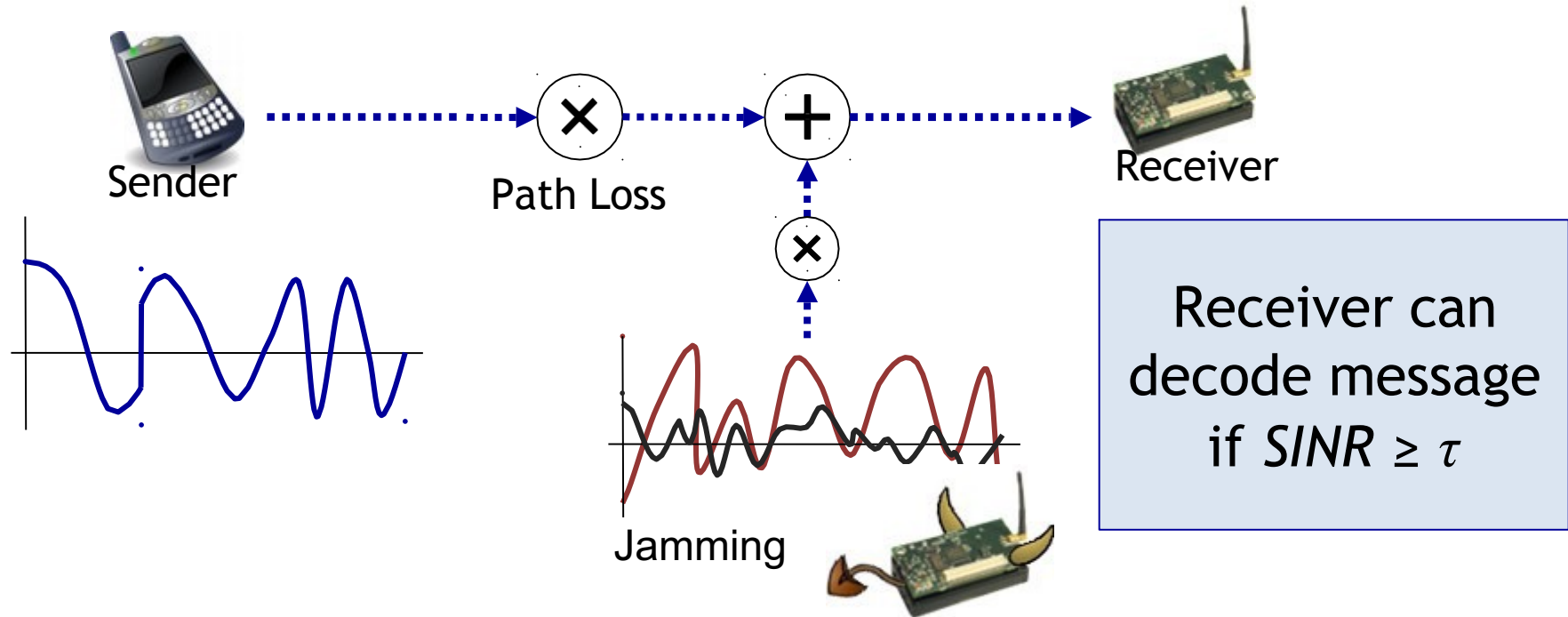


Jamming

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



How Does Jamming Work?



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

But, it's much more complicated than that...

Geometry Matters



Attacker can be MUCH
quitter than the speaker



SINR metric **captures effects** of geometry

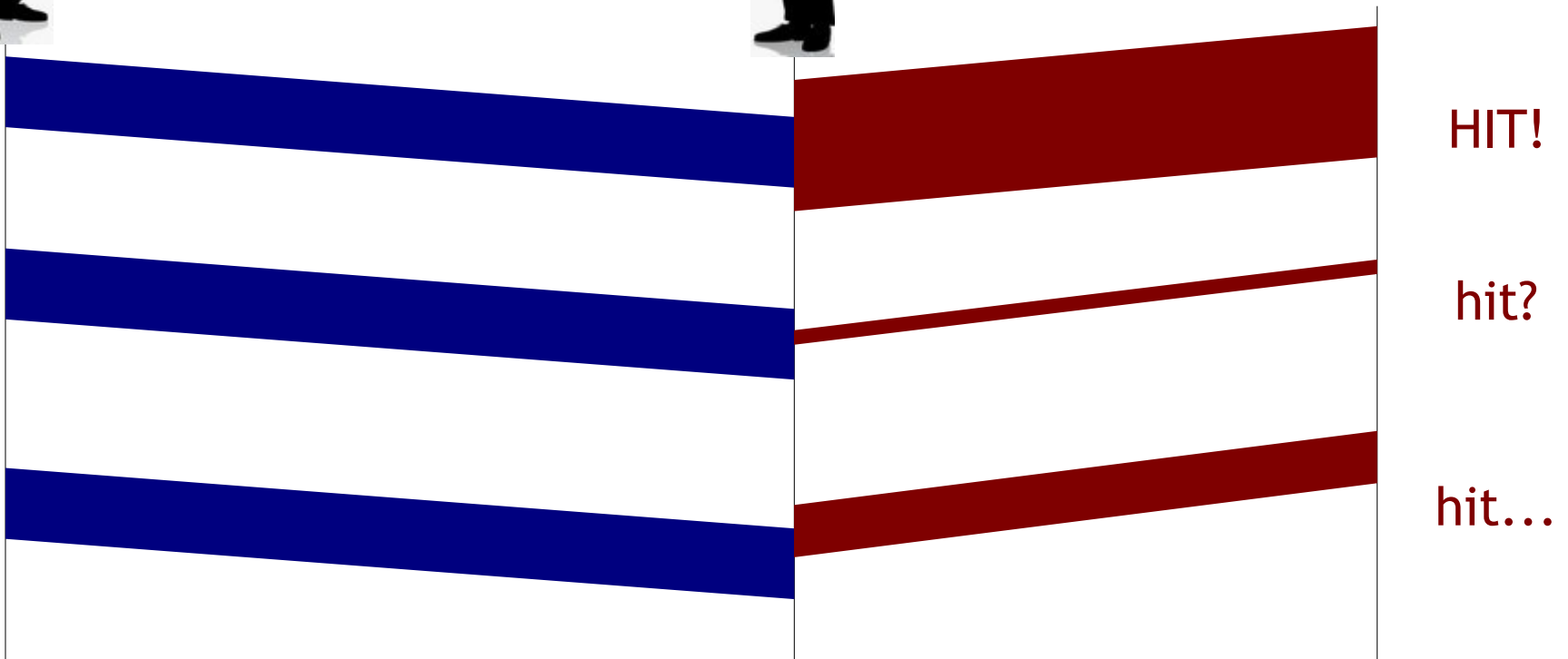
$\text{SINR} = (\text{Rx signal power}) / (\text{noise power} + \text{Rx jamming power})$

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

Typically random
variable N_0

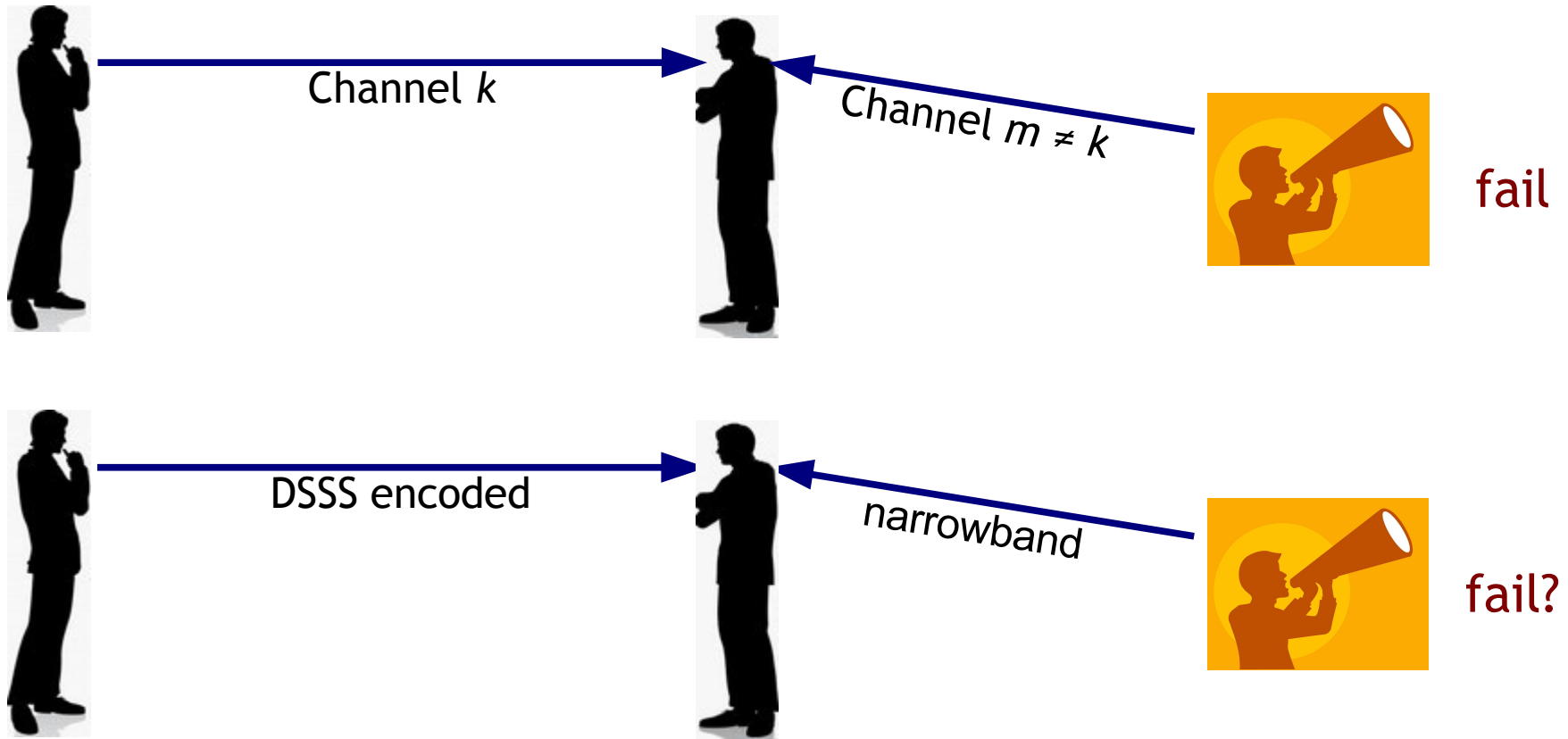
Often modeled
as $P_{jr} = k_j P_j d_{jr}^{-\alpha}$

Timing Matters



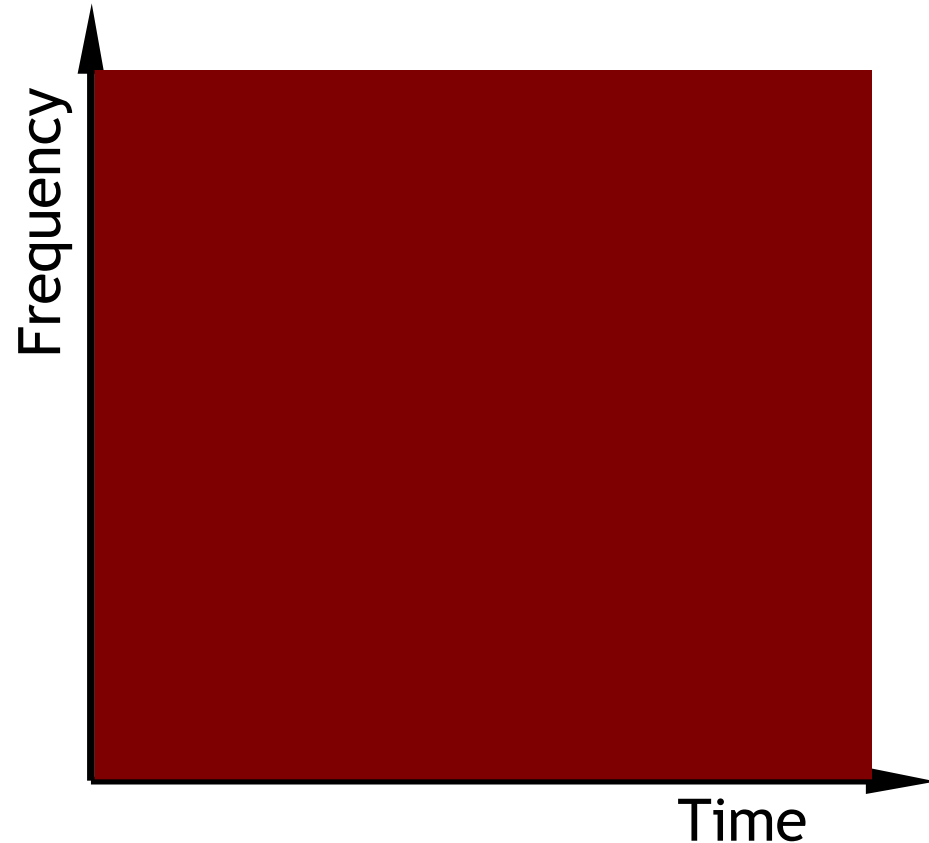
Can be modeled as a (random) multiplier in the “I” term of the SINR metric

Orthogonality Matters



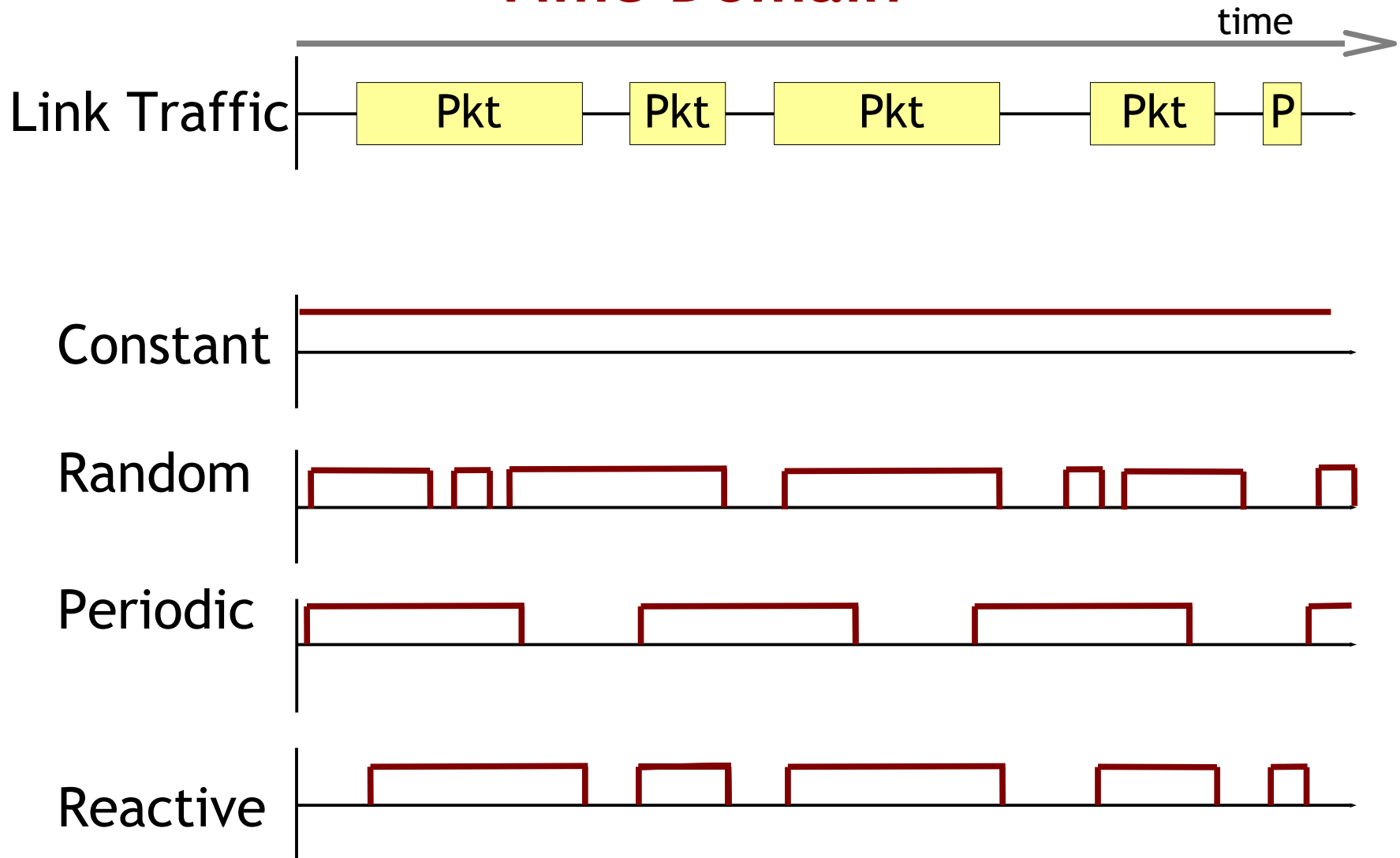
Generalized Jamming

- 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

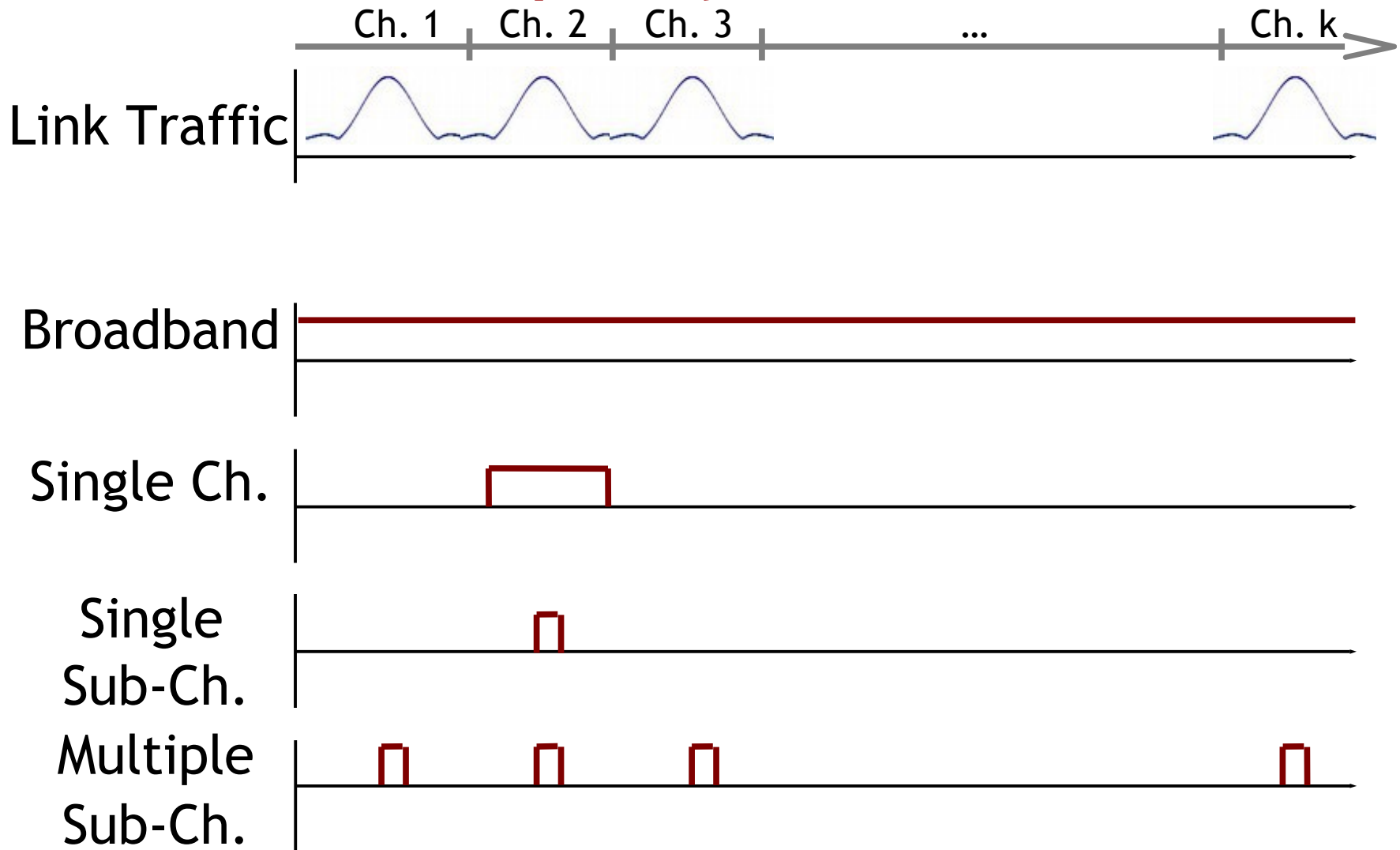
Time Domain



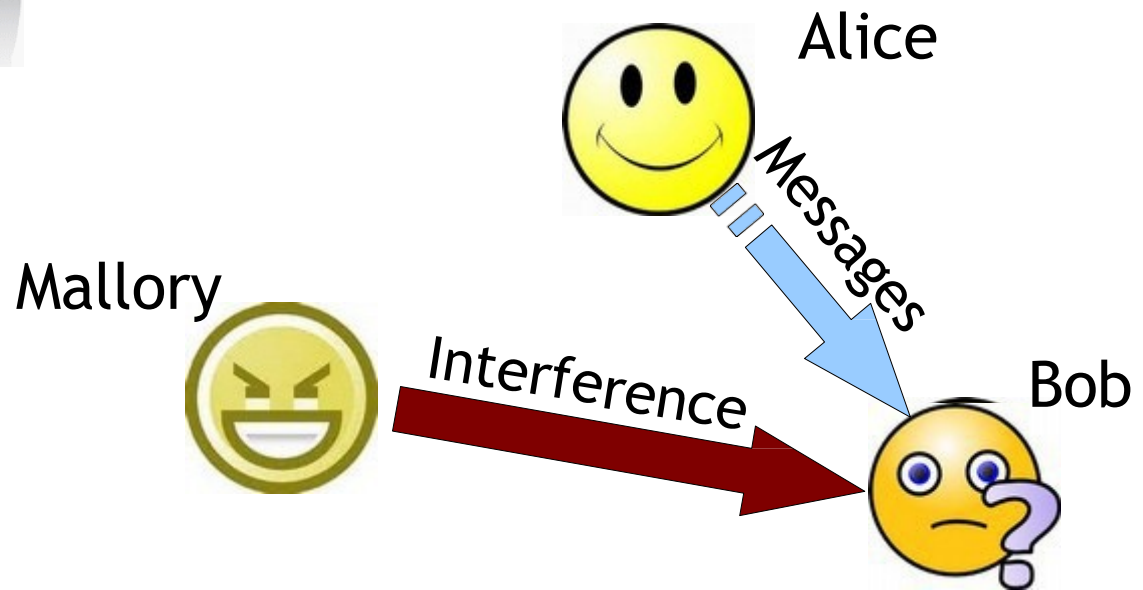
[Xu et al., 2006; Mpitziopoulos et al., 2009]

Jamming Strategies

Frequency Domain



Jamming



How can we protect against jamming?

Jamming Detection & Defense

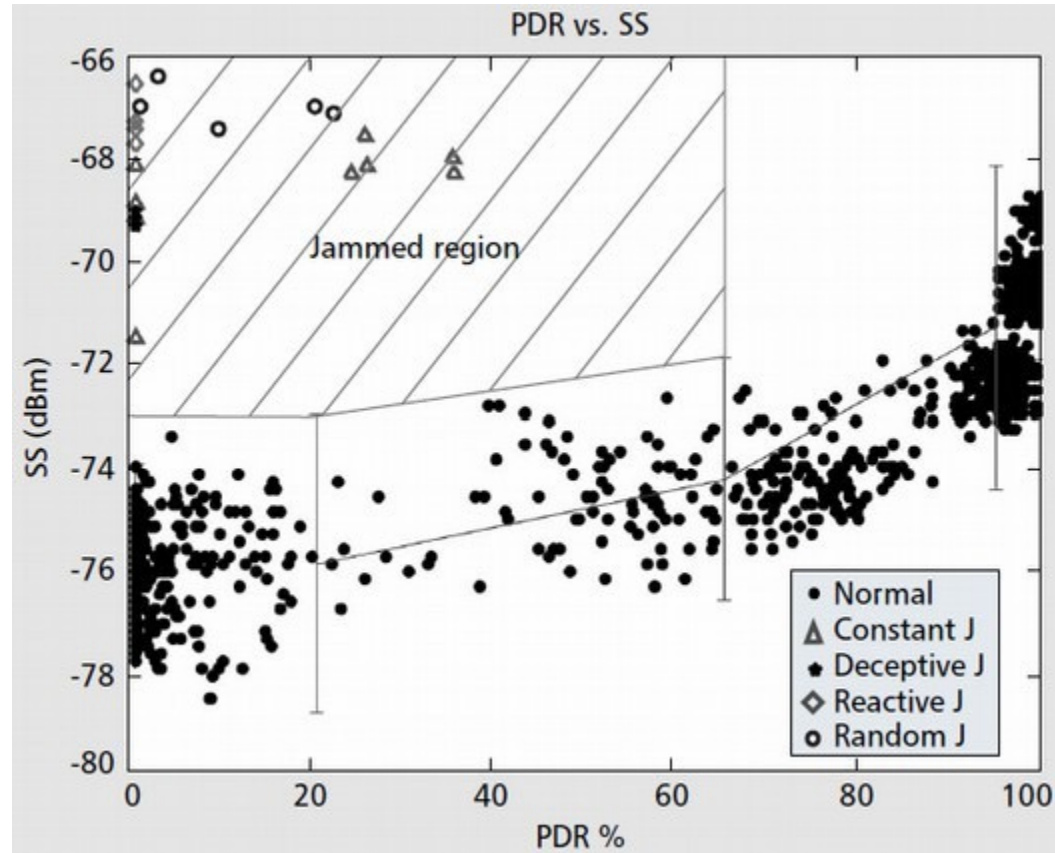
- **Goal:** detect and localize jamming attacks, then evade them or otherwise respond to them
- **Challenge:** distinguish between adversarial and natural behaviors (poor connectivity, battery depletion, congestion, node failure, etc.)
 - Certain level of detection error is going to occur
 - Appropriate for deployment in wireless networks
- **Approach:** coarse detection based on packet observation

Basic Detection Statistics

- Received signal strength (RSSI)
 - Jamming signal will affect RSSI measurements
 - Very difficult to distinguish between jamming/natural
- Carrier sensing time
 - Helps to detect jamming as MAC misbehavior
 - Doesn't help for random or reactive cases
- Packet delivery ratio (PDR)
 - Jamming significantly reduces PDR (to ~ 0)
 - Robust to congestion, but other dynamics (node failure, outside comm range) also cause $PDR \rightarrow 0$

Advanced Detection

- Combining multiple statistics in detection can help
 - High PDR + High RSSI → OK
 - Low PDR + Low RSSI → Poor connectivity
 - Low PDR + High RSSI → ? → Jamming attack?

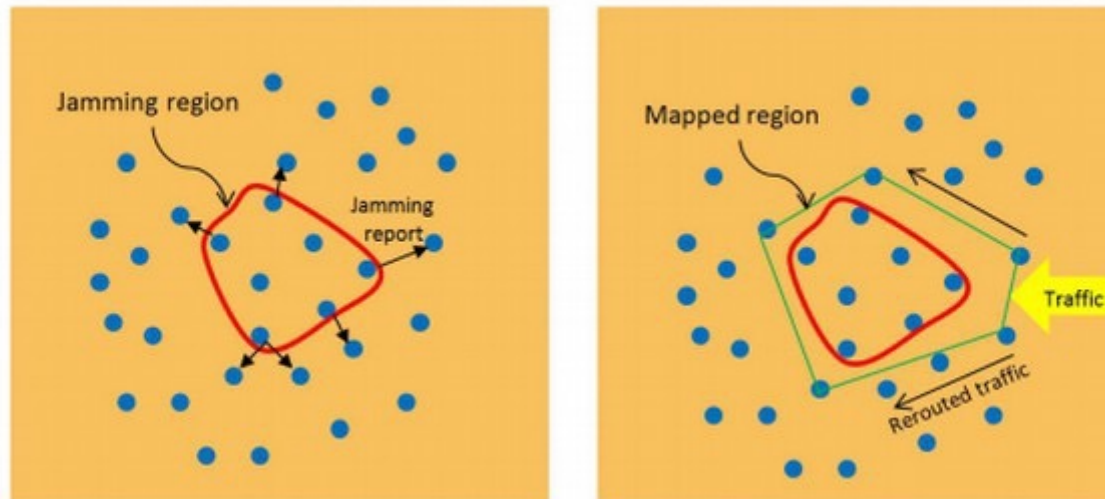


Caveat: this assumes RSSI can be accurately measured

See [DeBruhl & Tague, SECON 2013]

Jammed Area Mapping

- Based on advanced detection technique, nodes can figure out when they are jammed
- At the boundary of the jammed area, nodes can get messages out to free nodes
- Free nodes can collaborate to **perform boundary detection** using location information



Evading Jamming

- Nodes in the jammed region can evade the attack, either spectrally or spatially
 - **Spectral evasion** → “channel surfing” to find open spectrum and talk with free nodes
 - **Spatial evasion** → mobile retreat out of jammed area
 - Need to compensate for mobile jammers ability to partition the network (see figure in paper)

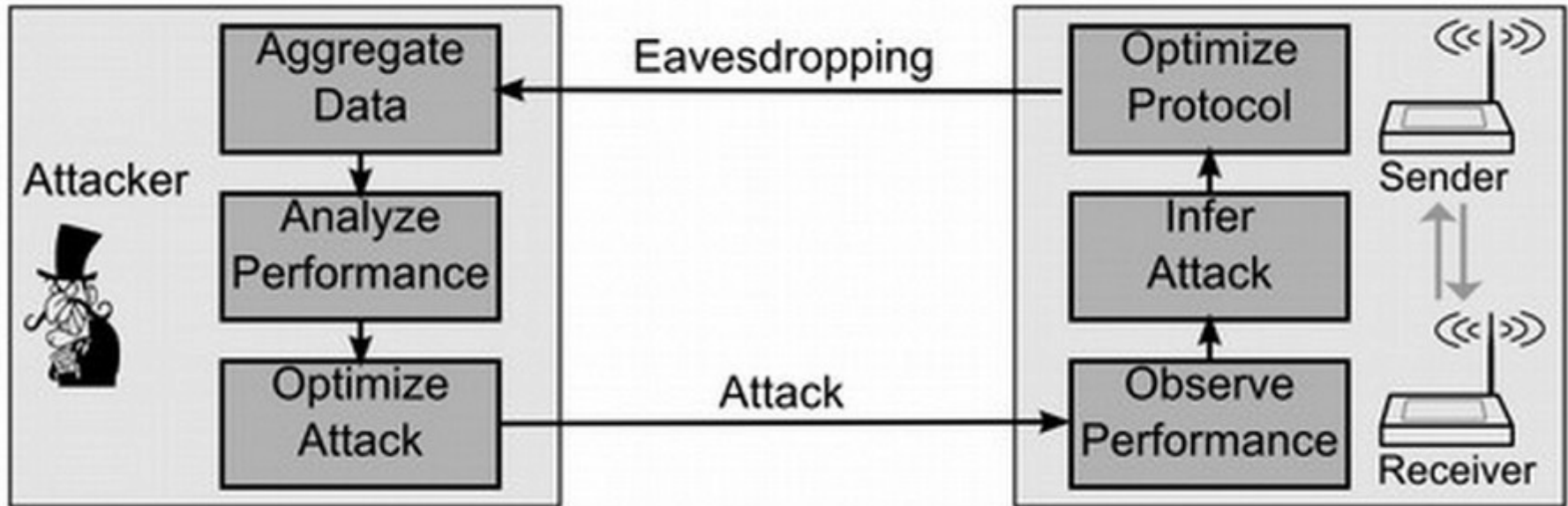
What about dynamic attack and defense strategies?

Optimal Jamming & Detection

- **Problem setup:** each of the network and the jammer have **control over random jamming and transmission probabilities**
 - Network parameter γ is probability each node will transmit in a time slot
 - Attack parameter β is probability the jammer will transmit in a time slot
- Opponents can learn about goals through observation and optimize for min-max/max-min

Jamming Games

- What if both the attacker and defender are freely adapting in response to each other?



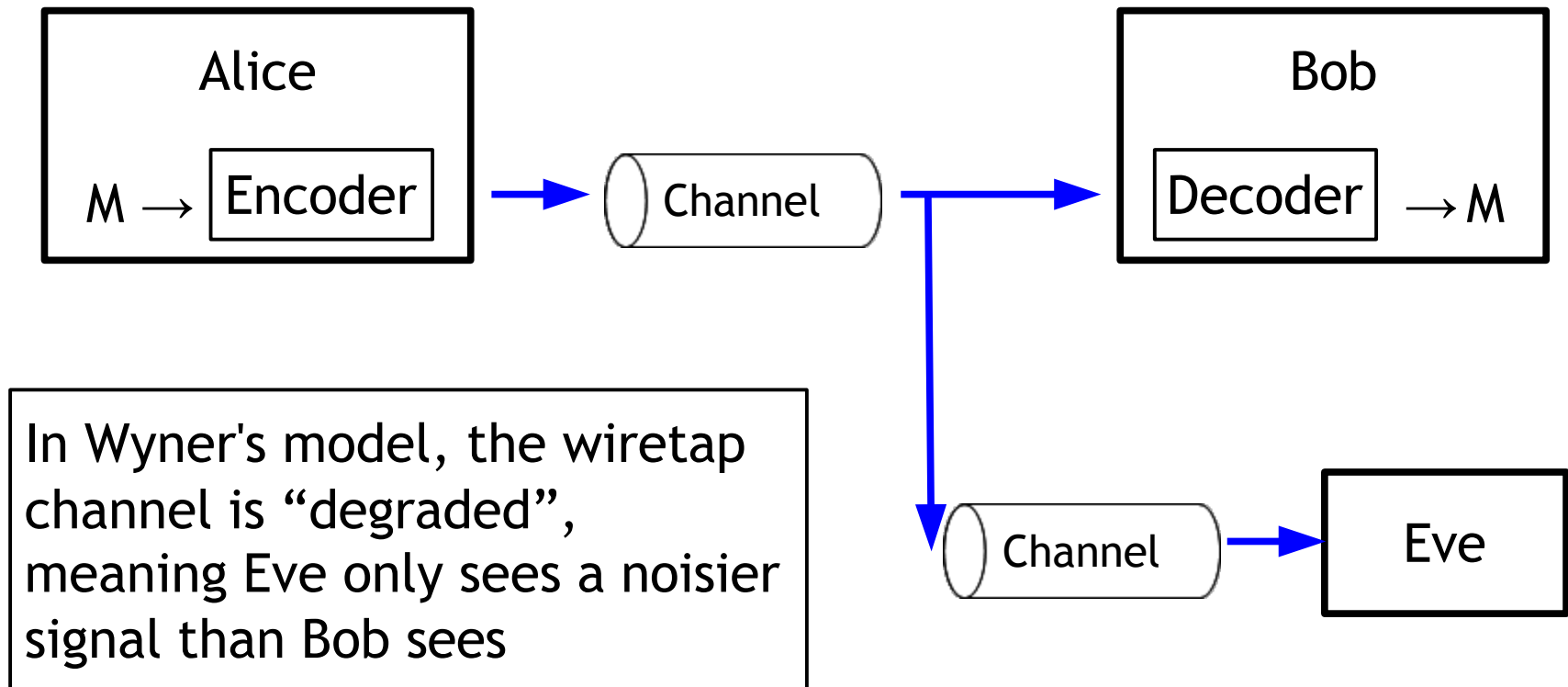
Eavesdropping / Snooping



How can the properties of the wireless medium actually **help** to achieve secure communication?

“Wiretapping”

- In 1975, A. D. Wyner defined the wiretap channel to formalize eavesdropping



Secrecy Capacity

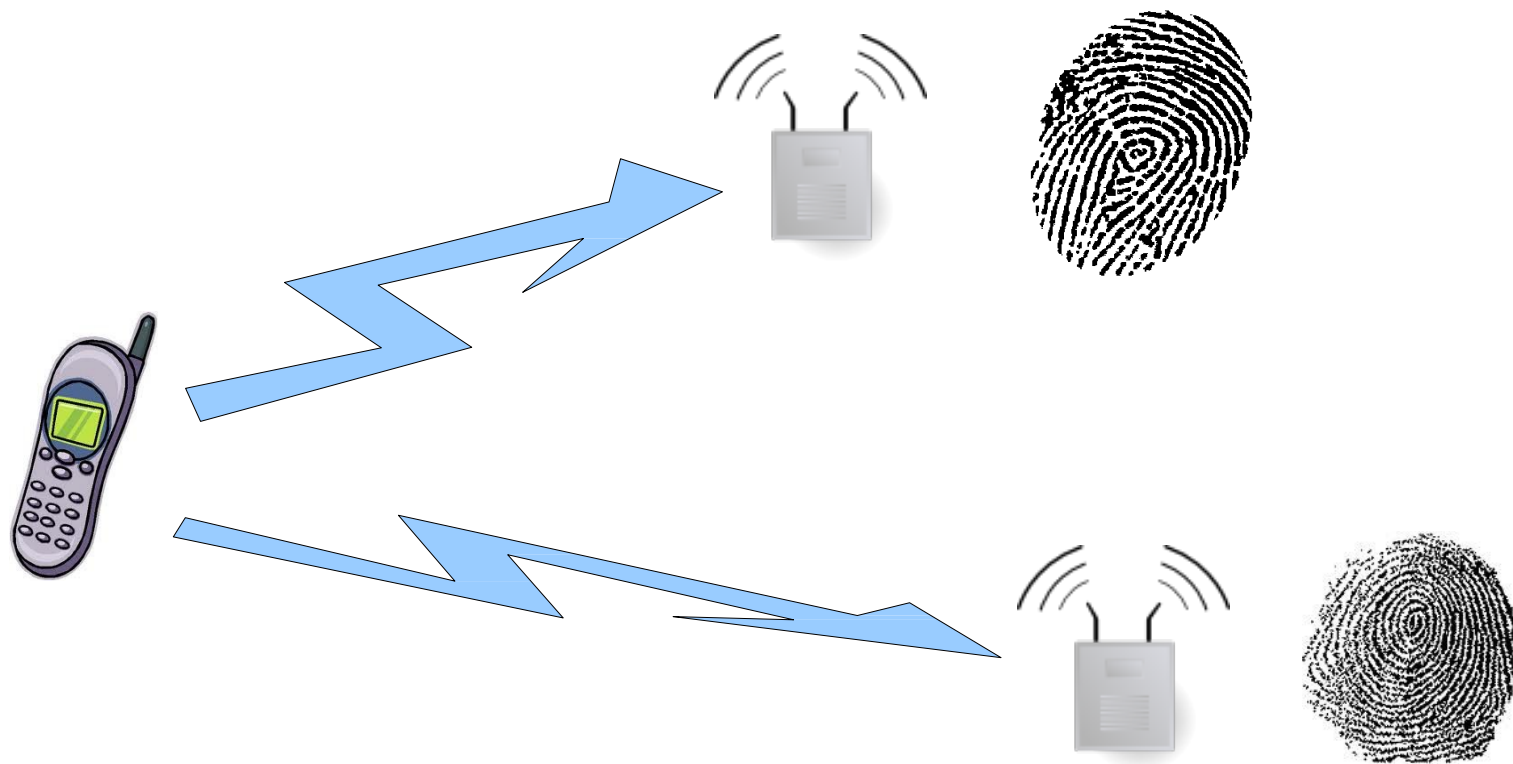
- Since the Alice $\rightarrow$ Eve channel is noisier than the Alice $\rightarrow$ Bob channel:
 - Eve can't decode everything that Bob can decode
 - i.e., there exists an encoding such that Alice can encode messages that Bob can decode but Eve can't
 - There's a really nice Information Theory formalization of the concept of secrecy capacity, namely the amount of secret information Alice can send to Bob without Eve being able to decode
 - I'll leave the details for you to explore

Degraded Eavesdropper?

- In a practical scenario, is it reasonable to assume the eavesdropper's signal is more degraded than the receiver's?
 - Probably not.
- What else can we do to tip the scales in the favor of the Alice-Bob channel?

Diversity of Receivers

The signal emitted by a transmitter looks “different” to receivers in distinct locations



Measurement + Feedback

- Channel State Information (CSI):
 - CSI is the term used to describe measurements of the channel condition
 - If Alice knows the CSI to Bob and to Eve, she can find an appropriate encoding using the CSI measurements
 - If Alice and Bob interact repeatedly, the measurement and feedback actually increase the secrecy capacity
 - This can allow for secrecy capacity >0 even if Eve's channel is less noisy than Bob's channel

Jamming a autonomous car

- Attacker can jam the ultrasound of the car, making the obstacle “disappear”, or even generate a fake obstacle, e.g., a person

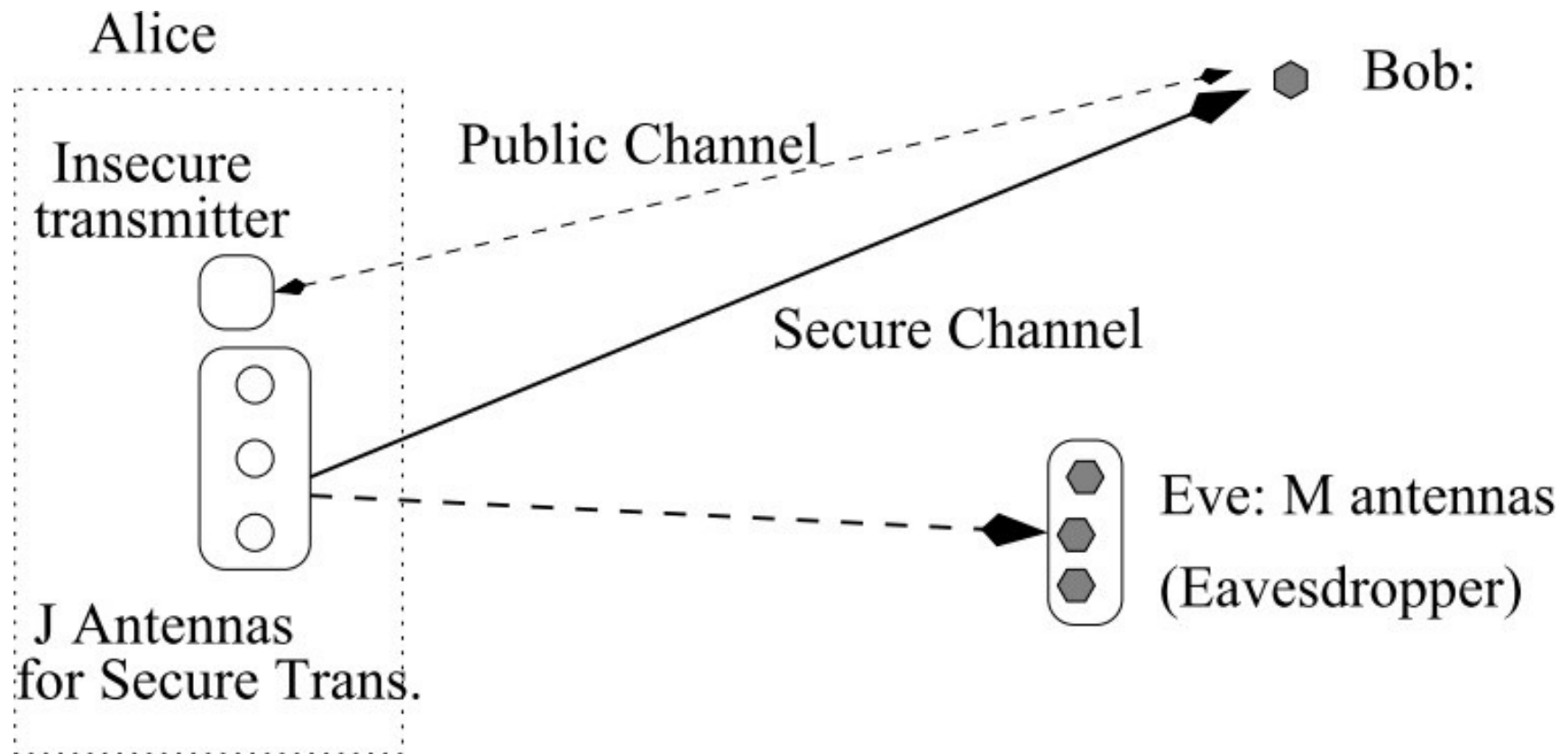


Jamming for Good

- If Alice has diversity in the form of multiple radios or some collaborators:
 - Alice & friends can use a jamming attack to prevent Eve from eavesdropping
 - As long as they don't jam Bob at the same time
 - **Example:** if the deployment geometry is known, Alice can adjust power, antenna config, etc. so Bob's SINR is high but Eve's is low

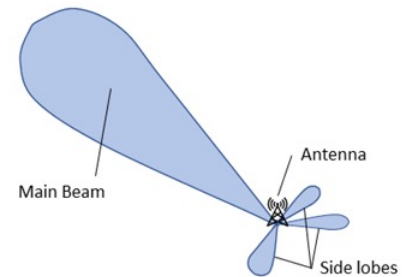
Secure Array Transmission

- **Antenna control** can be used for transmission with *low probability of interception*



Application

- Application 1: Building on secrecy capacity:
 - If two devices can communicate with a high probability guarantee that eavesdroppers cannot hear them, whatever they say is secret
 - BUT how? Probably **beamforming**!



Beamforming Antenna Array

- Application 2: Secret messages → keys!
 - Secret key generation is now possible using inherent properties of the wireless medium

Further Reading

- For a really good summary of secrecy capacity, the formalization, secret key generation, and lots of excellent details:
 - “Physical Layer Security” by Bloch and Barros
 - Available at:
<https://www.cambridge.org/core/books/physicallayer-security/543CF3D1431805B6AE04A7AA72903D09>

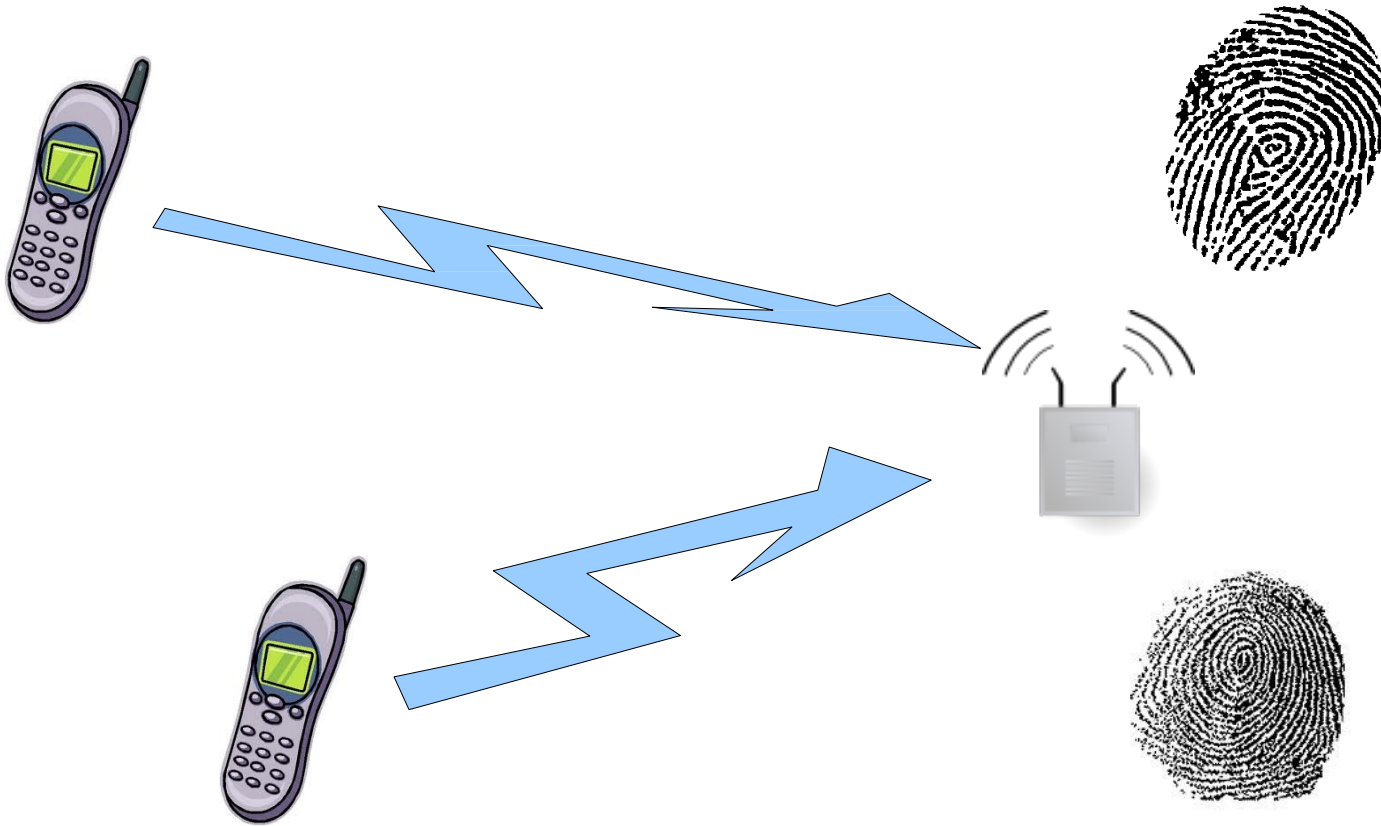
More Benefit for the Party?



Physical layer properties can help
with authentication!

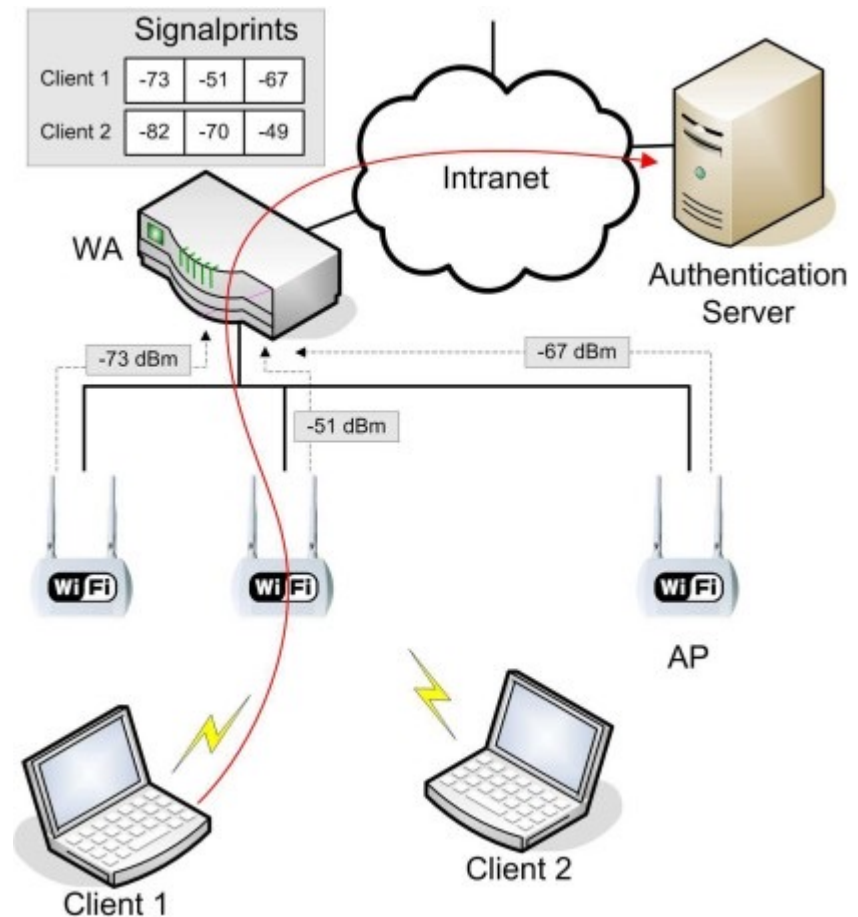
Diversity of Senders

Signals captured by a receiver from senders in
distinct locations look “different”



Signalprints

- In a WLAN with multiple APs, each AP **sees different characteristics of packets** from each sender
 - Each AP can measure various packet features, some of which are relatively static over packets: e.g., **received signal strength**
 - A back-end server can collect measurements and keep history of packets from different senders



Signalprint Properties

- **Difficult to spoof**
 - Spoofing node would require control of medium
 - Transmission power control creates lower RSS at every AP; differential analysis reveals power control, but how?
- **Correlated with physical location**
 - Attacker needs to be physically near target device
- **Sequential packets have similar signalprints**
 - RSSI values are highly correlated for stationary sender and receiver
 - Note: not highly correlated with distance, but very highly correlated with subsequent transmissions

Limitations

- Signalprints with any reasonable matching rule cannot differentiate between nearby devices
 - Masquerading/spoofing attacks are possible if physical proximity is easily achieved
- Low-rate attacks cannot be detected
 - But, low-rate attacks have limited effects
- Multi-antenna attackers can cheat
- Highly mobile devices can't be printed

Summary

Interference and eavesdropping are two of the most fundamental yet least understood vulnerabilities in wireless.

There's still a lot of work to be done.