# Wireless Security

Why is Security More of a Concern in Wireless?

- No inherent physical protection
  - physical connections between devices are replaced by logical associations
  - sending and receiving messages do not need physical access to the network infrastructure (cables, hubs, routers, etc.)
- Broadcast communications
  - wireless usually means radio, which has a broadcast nature
  - transmissions can be overheard by anyone in range
  - anyone can generate transmissions, which will be received by other devices in range
  - which will interfere with other nearby transmissions and may prevent their correct reception (jamming)
- Eavesdropping is easy
- Injecting bogus messages into the network is easy
- Replaying previously recorded messages is easy
- Illegitimate access to the network and its services is easy
- Denial of service is easily achieved by jamming

Overview

Understand Attacks → **Detect Attacks** → **Defend**
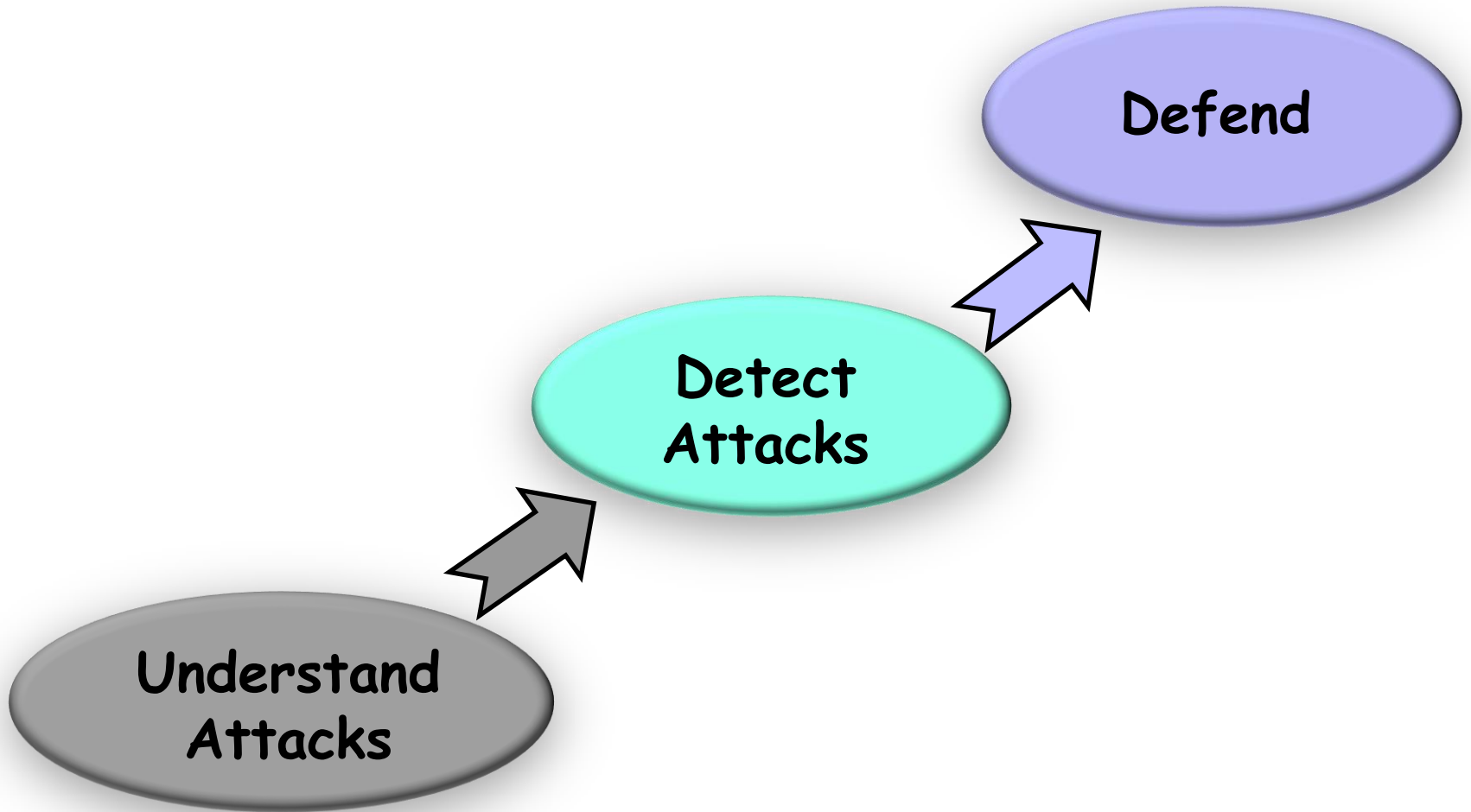
Attacking Wireless Networks

Attack 1: CSMA Selfish Behaviors

❑ **Carrier sense:** When a node wishes to transmit a packet, it first waits until the channel is idle

❑ **Backoff Interval:** used to reduce collision probability

❑ When transmitting a packet, choose a backoff interval in the range [0,cw]: cw is contention window

❑ Count down the backoff interval when medium is idle

  ○ Count-down is suspended if medium becomes busy

❑ When backoff interval reaches 0, transmit

❑ IEEE 802.11 DCF: contention window cw is chosen dynamically depending on collision occurrence

Binary Exponential Backoff

❑ When a node faced a transmission failure, it increases the contention window
  ○ cw is doubled (up to an upper bound)

❑ When a node successfully completes a data transfer, it restores cw to cw_{min}

❑ cw follows a sawtooth curve
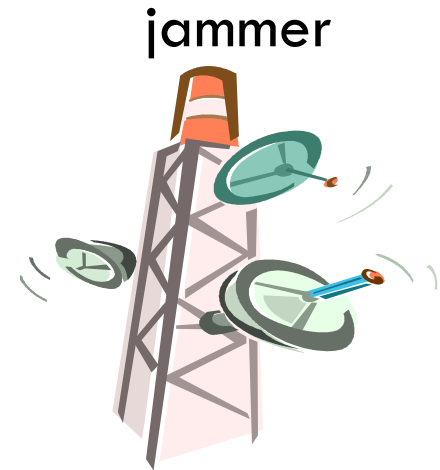
Attack 1: CSMA Selfish Behaviors
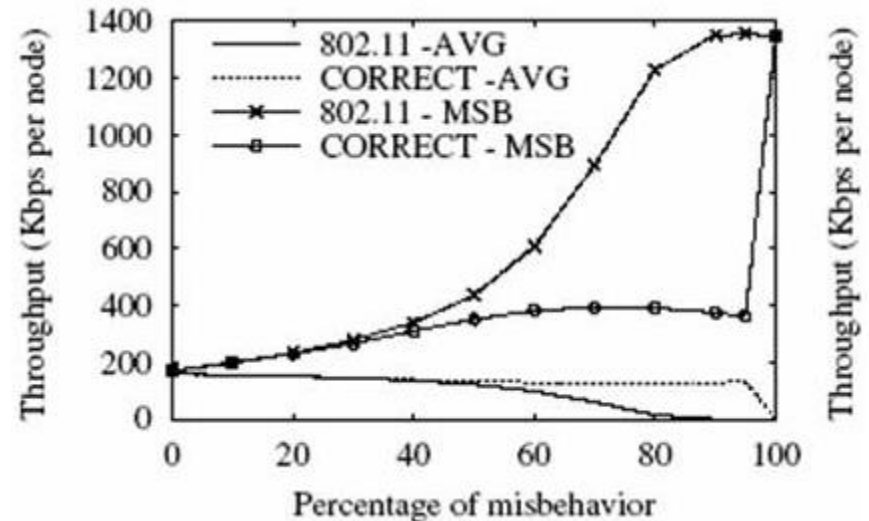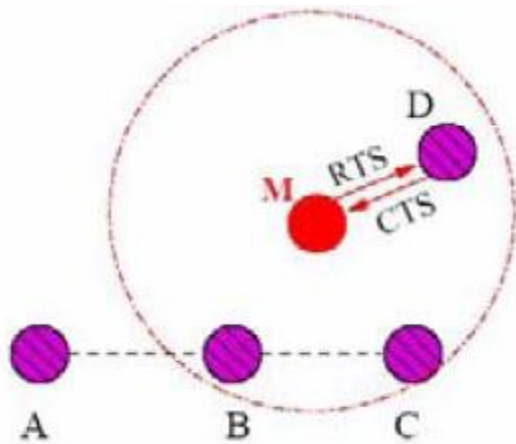
- ❑ Use smaller backoff window
  - ○ Transmit with you should not
    - • Attacker gets more bandwidth
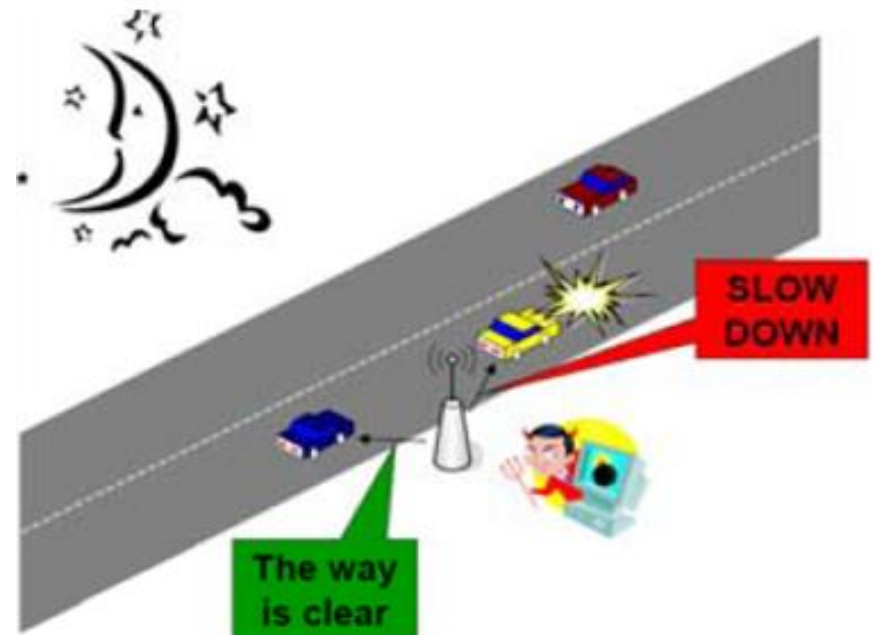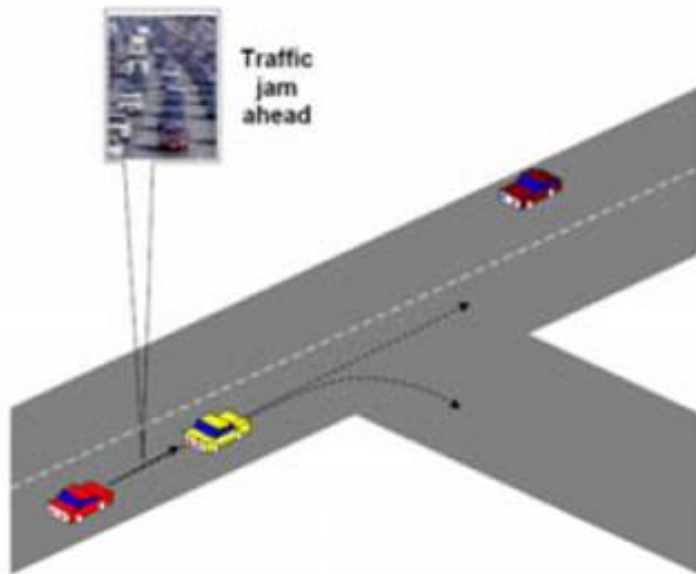 - ○ Cause collisions to others

Attack 2: Jamming
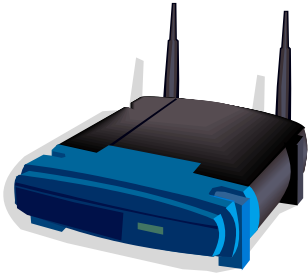
# Attack 3: Injecting Bogus Information

Introduction

❑ Traditionally, Denial of Service (DoS) attacks involve filling receiving buffers and/or bringing down servers

❑ In the wireless domain, DoS is more fundamentally linked with the medium
  - MAC misbehavior or
  - Preventing nodes from even communicating (*i.e., jamming*)

Roadmap

Advanced Detection Mechanisms

Basic Detection Mechanisms

Jamming Models
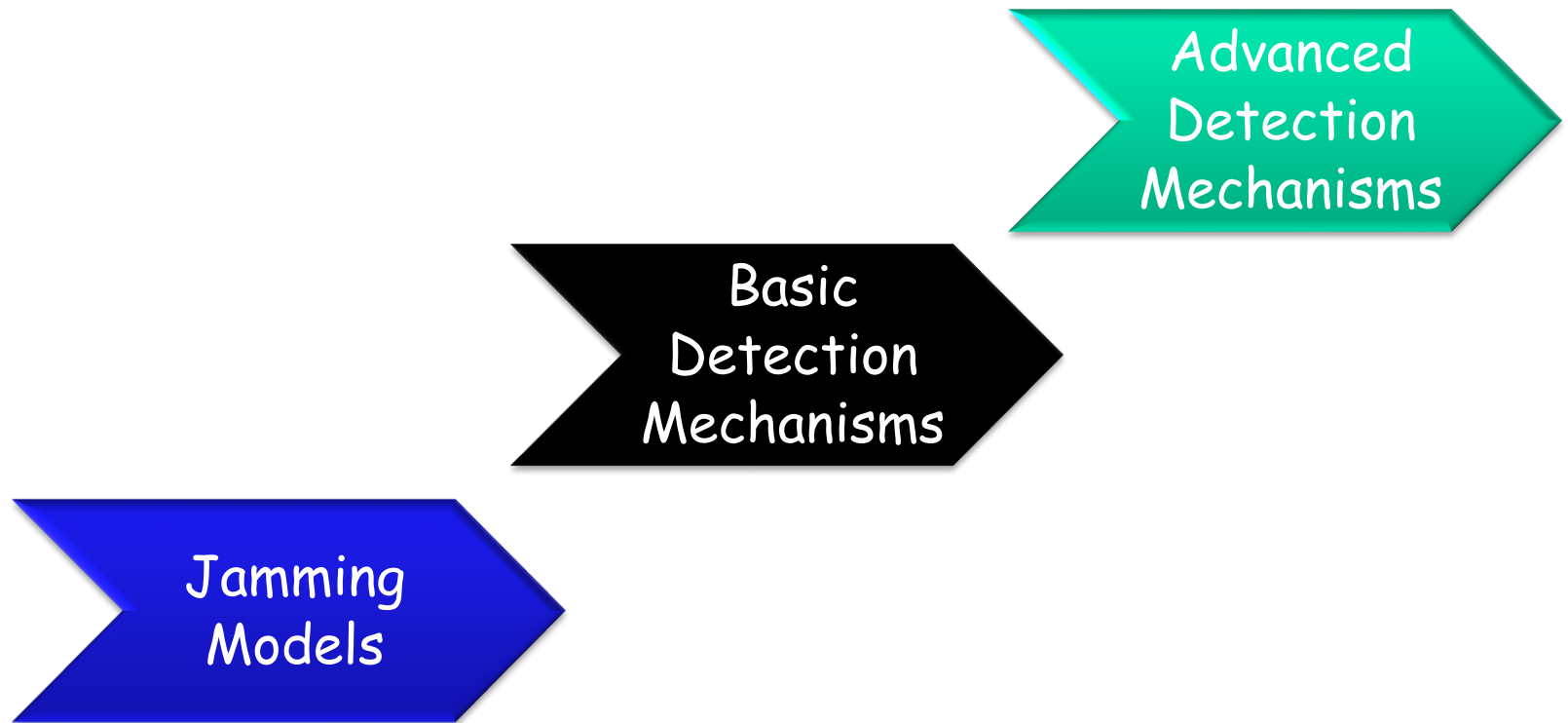
What is a Jammer?

❑ A jammer is purposefully trying to interfere with the physical transmit/receive
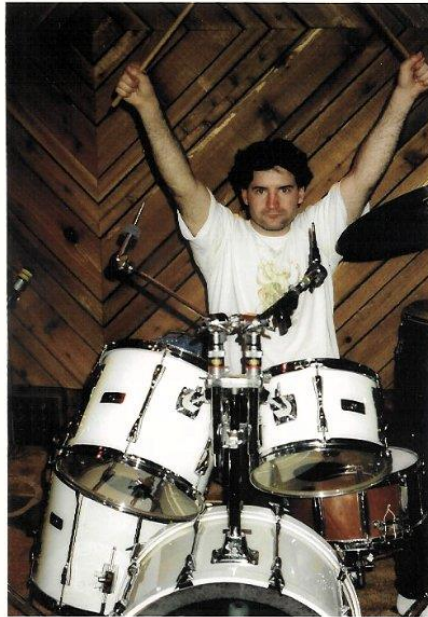
Jammers -- Hardware

- ❏ Cell phone jammer unit
  - ○ Block every cellular phone!!!
- ❏ Signal generator
- ❏ Conventional devices

Goal of Jammer

☐ Interference
- ◘ Prevent a sender from sensing out packets
- ◘ Prevent a receiver from receiving legitimate packets

☐ How to measure their effectiveness:
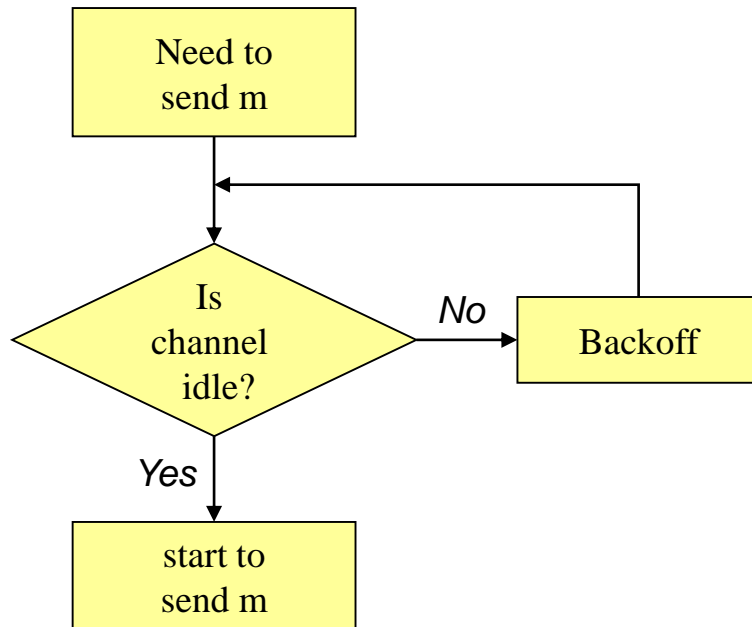- ◘ Packet Send Ratio (PSR):
  - ■ Ratio of actual # of packets sent out versus # of packets intended
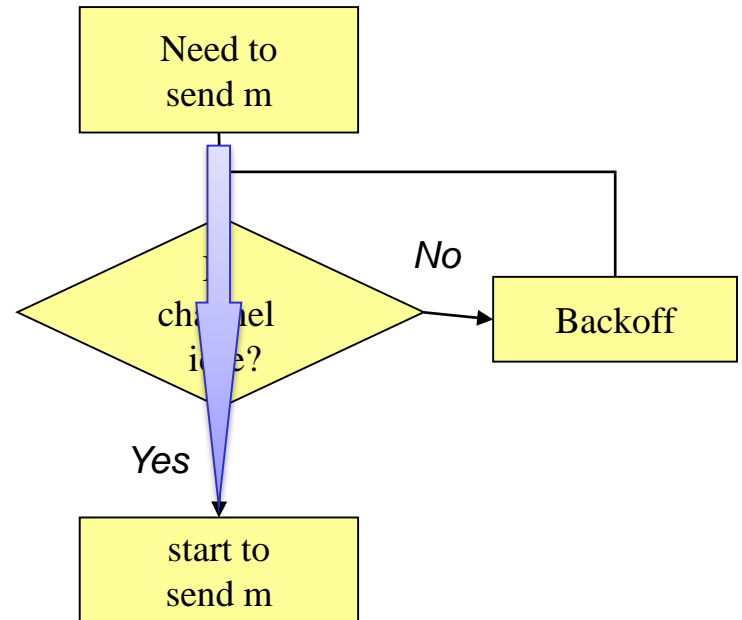- ◘ Packet Delivery Ratio (PDR):
  - ■ Ratio of # of successfully delivered packets versus # of packets sent out
  - ■ Measured at sender [ACKs] or receiver [CRC check]

Jammer Attack Models

Normal MAC protocol:

Jammer:

Jamming Models

- ☐ Constant Jammer
  - ◘ Continuously emits radio signal (random bits, no MAC-etiquette)
- ☐ Deceptive Jammer
  - ◘ Continuously sends regular packets (preamble bits) without gaps in transmission
  - ◘ Targeting sending
- ☐ Random Jammer
  - ◘ Alternates between sleeping and jamming states.
  - ◘ Takes energy conservation into consideration
- ☐ Reactive Jammer:
  - ◘ Reacts to a sent message
  - ◘ Targeting reception;
  - ◘ Harder to detect

Constant Jammer
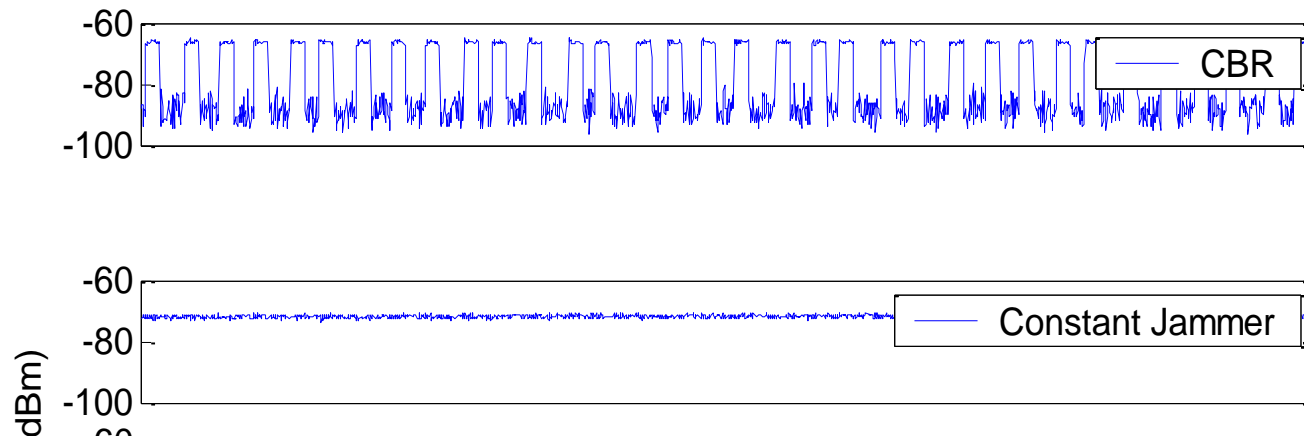
□ Constant Jammer - continually emits a radio signal (noise). The device will not wait for the channel to be idle before transmitting. Can disrupt even signal strength comparison protocols .

Deceptive Jammer
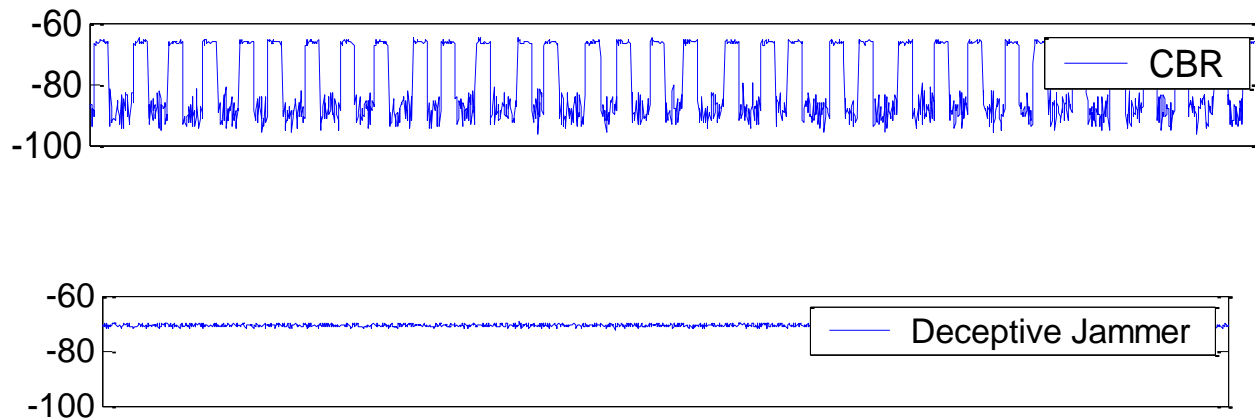

□ Deceptive Jammer - constantly injects regular packets with no gap between packets. A normal device will remain in the receive state and cannot switch to the send state because of the constant stream of incoming packets.

Random Jammer
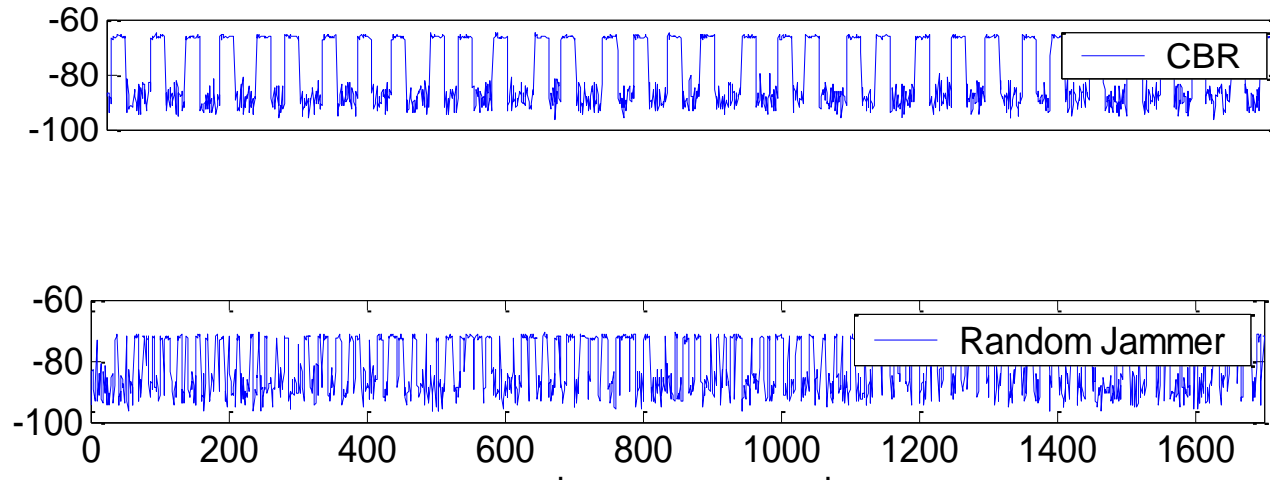
☐ Random Jammer - alternates between sleeping and jamming. Can act as constant or deceptive when jamming. Takes energy conservation into consideration.
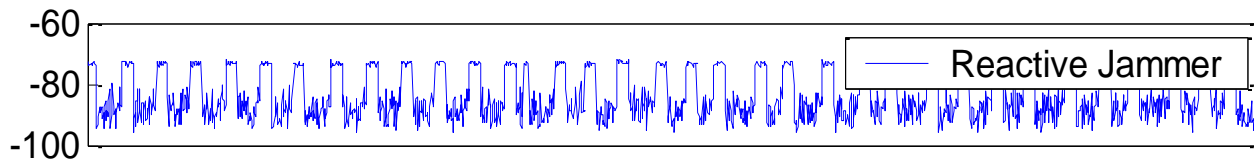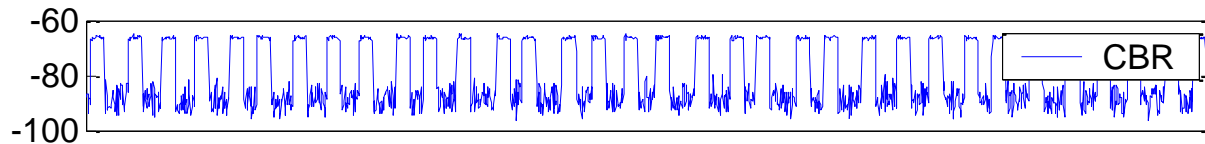
Reactive Jammer

☐ Reactive Jammer - other three are active this is not. It stays quiet until there is activity on the channel. This targets the reception of a message. This style does not conserve energy however it may be harder to detect.

Basic Jamming Detection

What attributes will help us detect jamming?

- ❑ Signal strength (PHY-layer detection)
- ❑ Carrier sense (MAC layer detection)
- ❑ Packet Delivery Ratio
  - ○ Detects all jamming models
  - ○ Differentiates jamming from congestion
  - ○ Cannot differentiate jamming from node failure, battery loss, departure, etc.

Detection 1: Analyzing Signal Strength

How can we use Signal Strength to detect Jamming?

❑ Signal strength distribution may be affected by the presence of a jammer

❑ Each device should gather its own statistics to make its own decisions on the possibility of jamming

❑ Establish a base line or build a statistical model of normal energy levels prior to jamming of noise levels….But how??

Two Methods for Signal Strength

1. Basic Average and Energy Detection
   - We can extract two statistics from this reading, the average signal strength and the energy for detection over a period of time

2. Signal Strength Spectral Discrimination
   - A method that employs higher order crossings (HOC) to calculate the differences between samples
   - This method is practical to implement on resource constrained wireless devices, such as sensor nodes

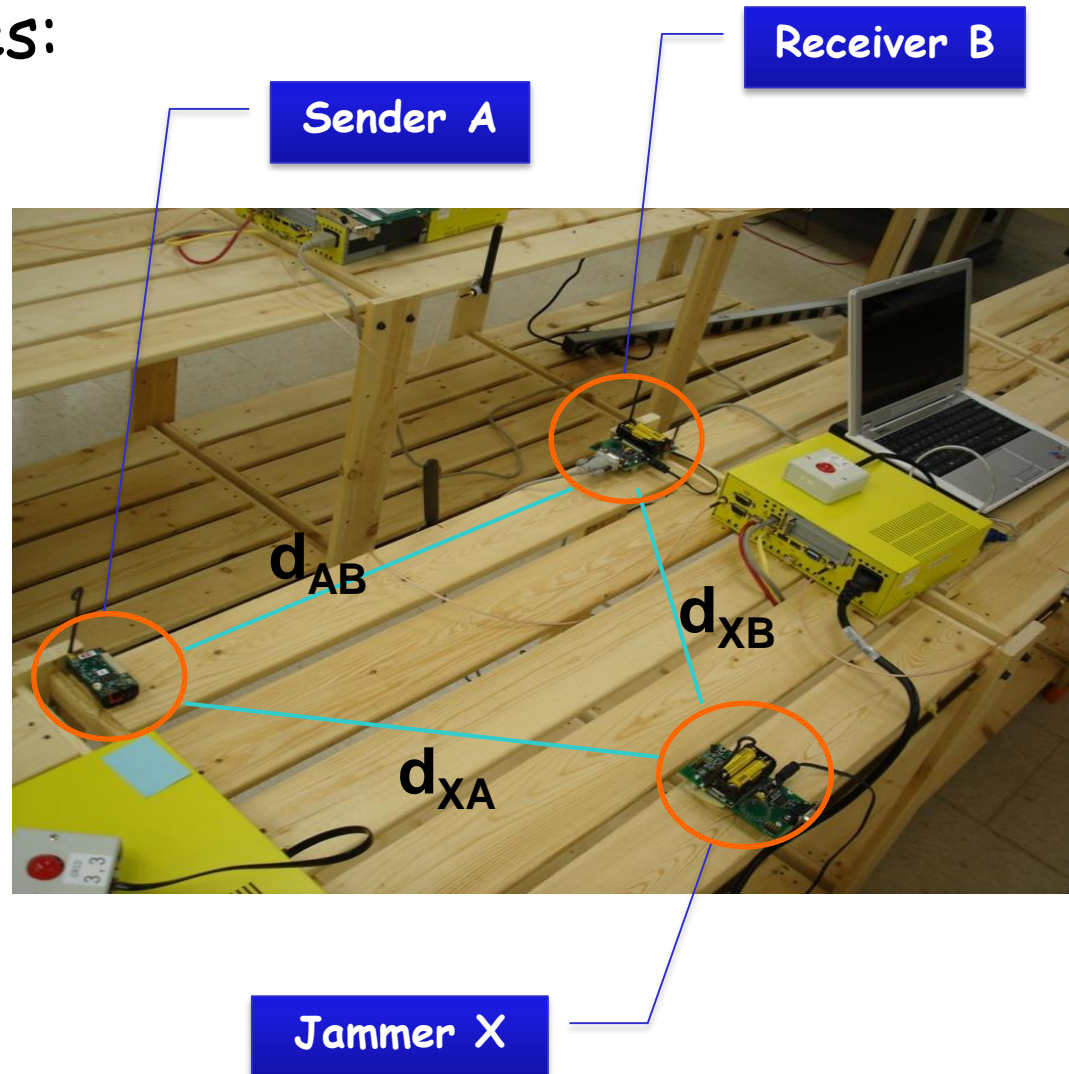# Experiment Setup

❑ **Involving three parties:**
- Normal nodes:
 - Sender A
  - Receiver B
- Jammer X

❑ **Parameters**
- Four jammers model
- Distance
  - Let $d_{XB} = d_{XA}$
  - Fix d_{AB} at 30 inches
- Power
  - $P_A = P_B = P_X = -4dBm$

Signal Strength

□ The average values for the constant jammer and the MaxTraffic source are roughly equal

□ The constant jammer and deceptive jammer have roughly the same average values

□ The signal strength average from a CBR source does not differ much from the reactive jammer scenario

□ These results suggest that we may not be able to use simple statistics such as average signal strength to identify jamming

CBR: 20 packets per second
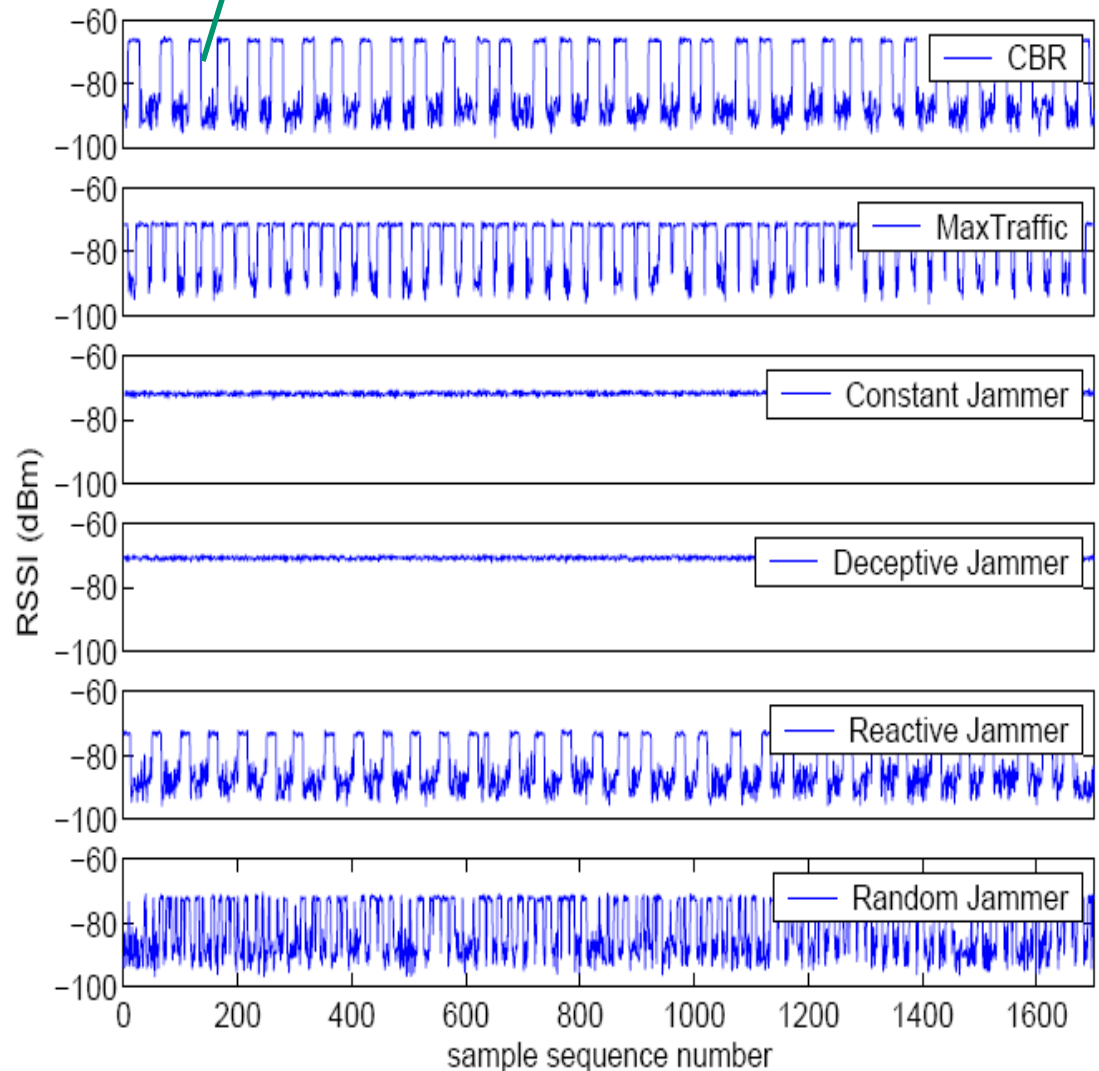
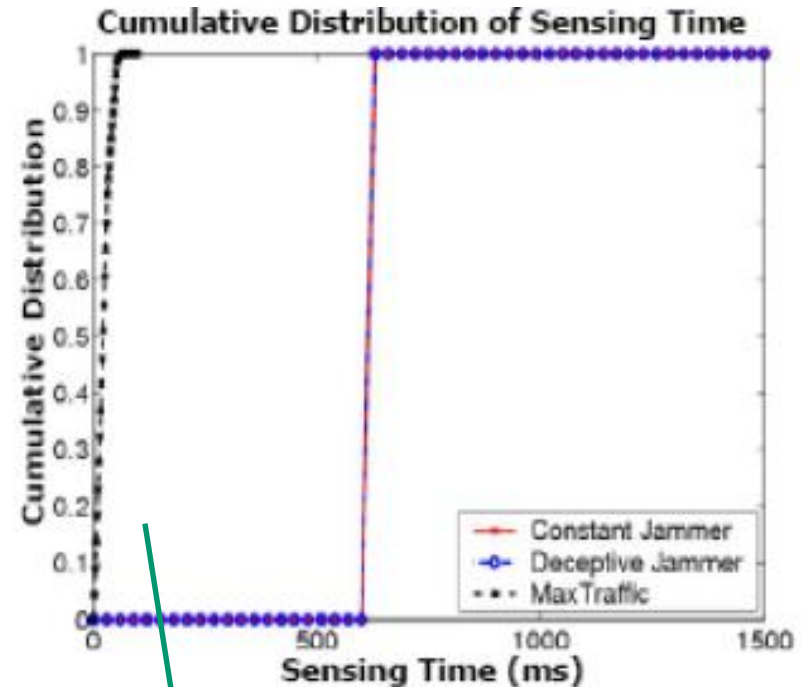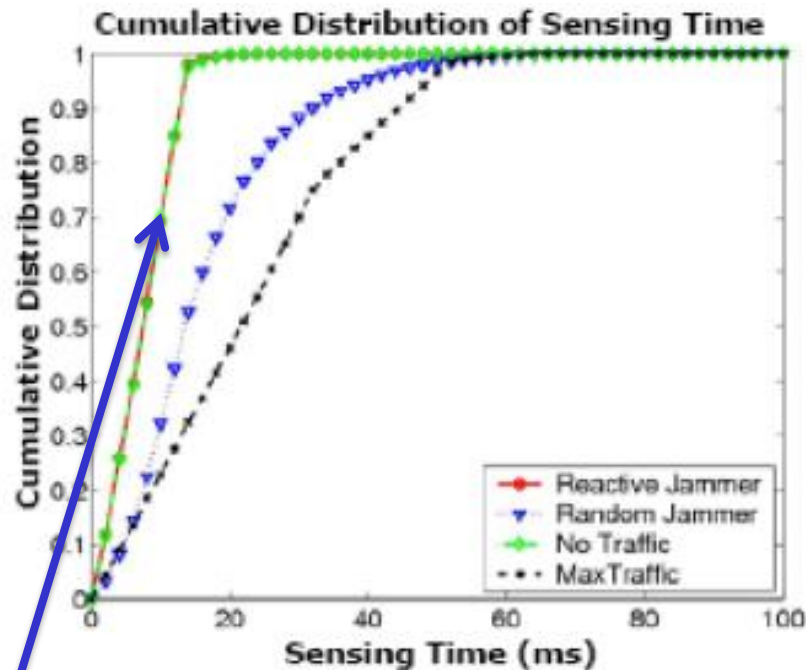# Signal-Strength: Higher Order Crossing

- We can not distinguish the reactive or random jammer from normal traffic
- A reactive or random jammer will alternate between busy and idle in the same way as normal traffic behaves
- HOC will work for some jammer scenarios but are not powerful enough to detect all jammer scenarios

Not working well….
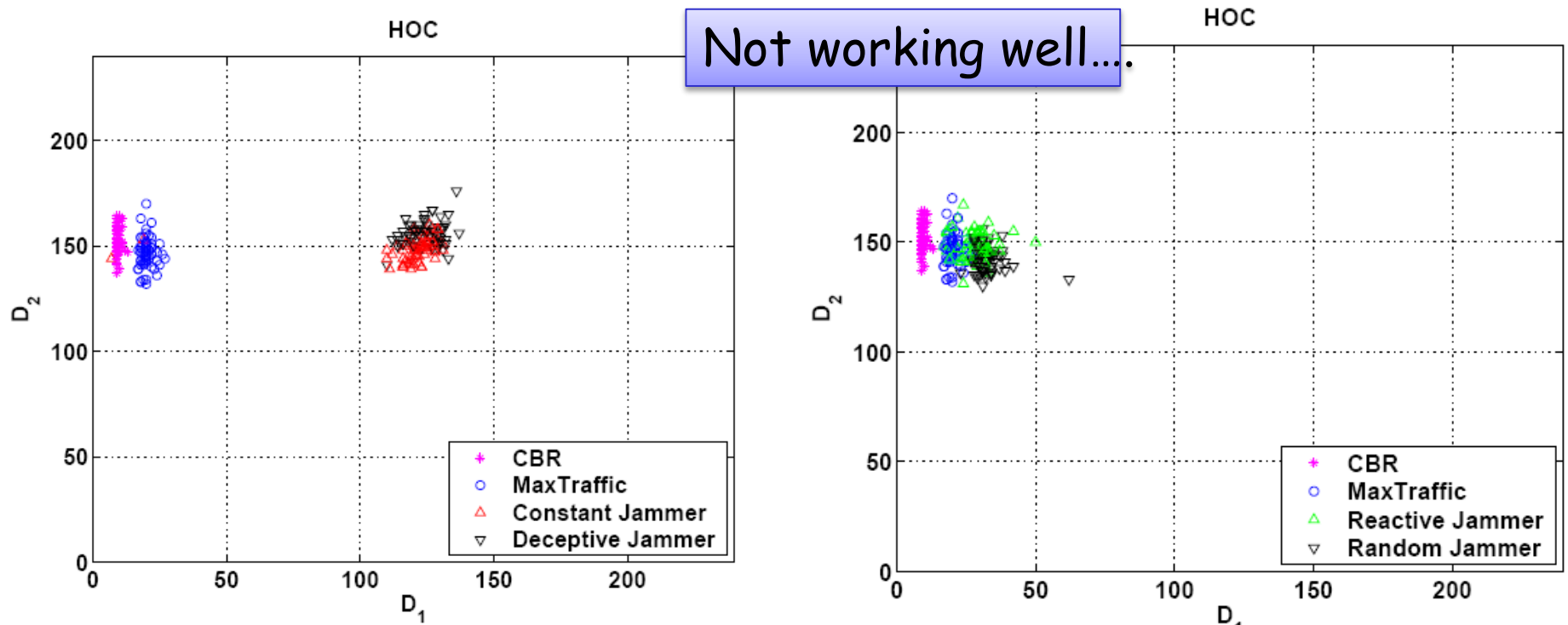
Detection 2: Analyzing Carrier Sensing Time

❑ A jammer can prevent a legitimate source from sending out packets ← channel might appear constantly busy to the source

❑ Keep track of the amount of time it spends waiting for the channel to become idle (carrier sensing time)

   ○ Compare it with the sensing time during normal traffic operations to determine whether it is jammed

   ○ Only true if MAC protocol employs a fixed signal strength threshold to determine whether channel is busy

❑ Determine when large sensing times are results of jamming by setting a threshold

❑ Threshold set conservatively to reduce false positive

Detection 2: Analyzing Carrier Sensing Time

Cumulative Distribution of Sensing Time

- Reactive Jammer
- Random Jammer
- No Traffic
- MaxTraffic

Cumulative Distribution of Sensing Time

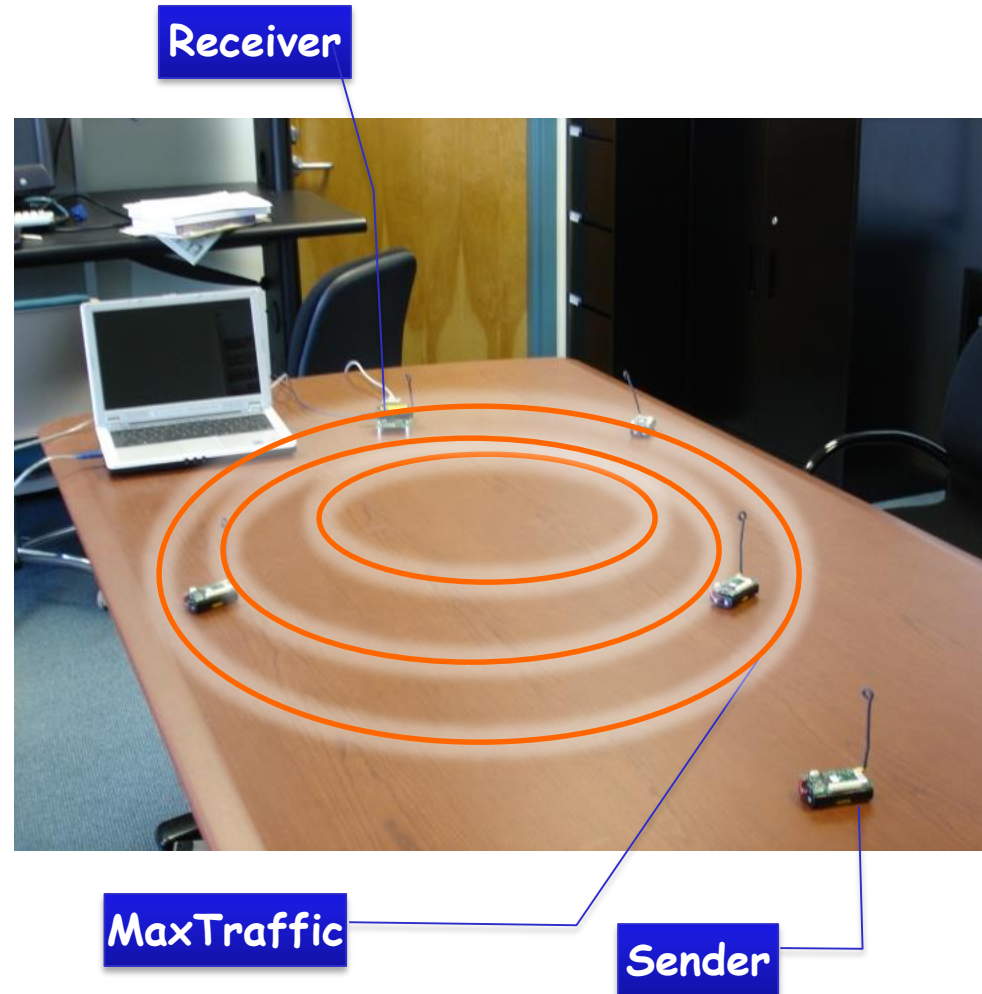- Constant Jammer
- Deceptive Jammer
- MaxTraffic

Hard to detect a reactive jammer

It detects the Constant and Deceptive Jammer

Detection 3: Analyzing Packet Delivery Ratio

- ❑ How much PDR degradation can be caused by non-jamming, normal network dynamics, such as congestion? (PDR 78%)

- ❑ A jammer causes the PDR drop significantly, almost to 100%

- ❑ A simple threshold based on PDR is a powerful statistic to determine Jamming vs. congestion

- ❑ PDR can not differentiate non-aggressive jamming attacks from poor channel quality…

Receiver

MaxTraffic

Sender

Basic Statistics Summary

❑ Both Signal Strength and Carrier Sensing time can only detect the constant and deceptive jammer

❑ Neither of these two statistics is effective in detecting the random or the reactive jammer

❑ PDR is a powerful statistic to determine Jamming vs. congestion
  ○ It can not account for all network dynamics

Solution: Consistency Checks

☐ PDR is relatively good
- ◘ Normal scenario:
  - ■ High signal strength → high PDR
  - ■ Low signal strength → low PDR
- ◘ Low PDR in real life
  - ■ Poor channel quality
  - ■ Jamming attacks → high signal strength

☐ Consistency check
- ◘ Look at transmissions from neighbors
- ◘ If at least one neighbor has high PDR
- ◘ If all have low PDR → check signal strength → high → I am being jammed!
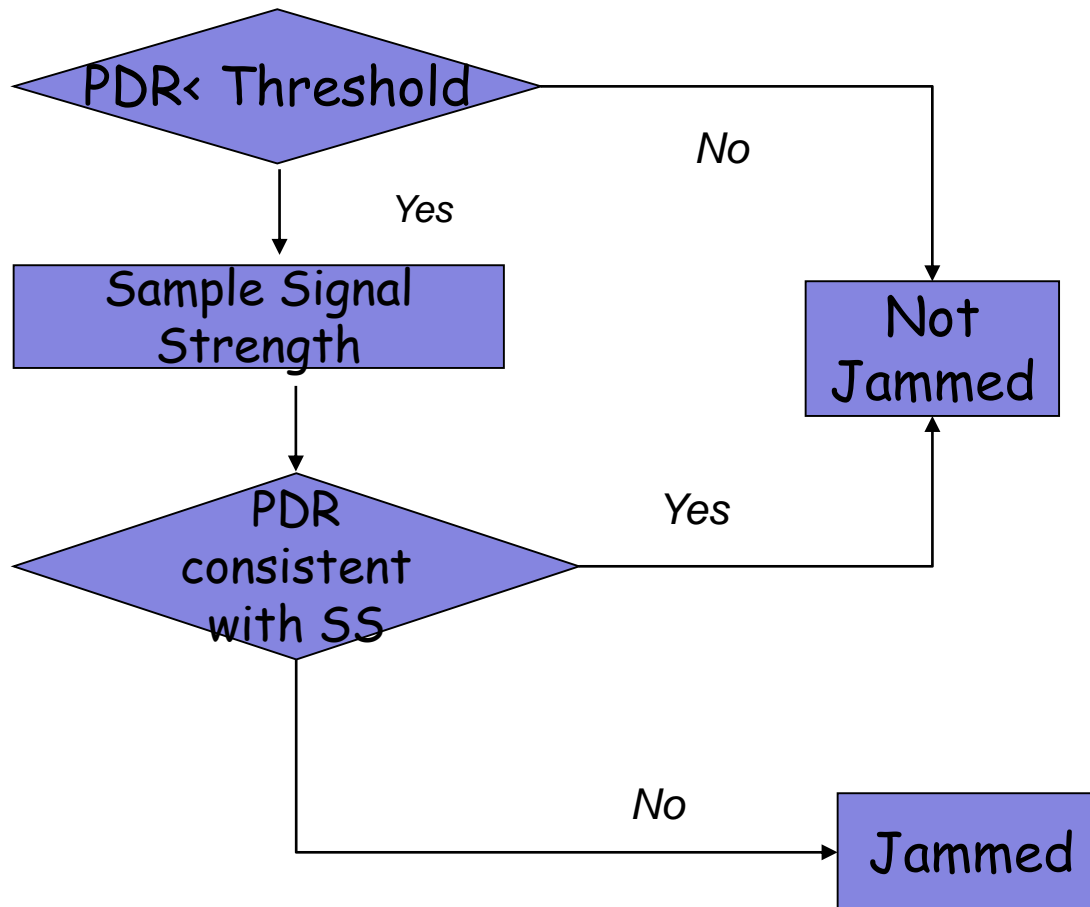
Location-Based Consistency Check

❑ Concept:
  ○ Close neighbor nodes → high PDR
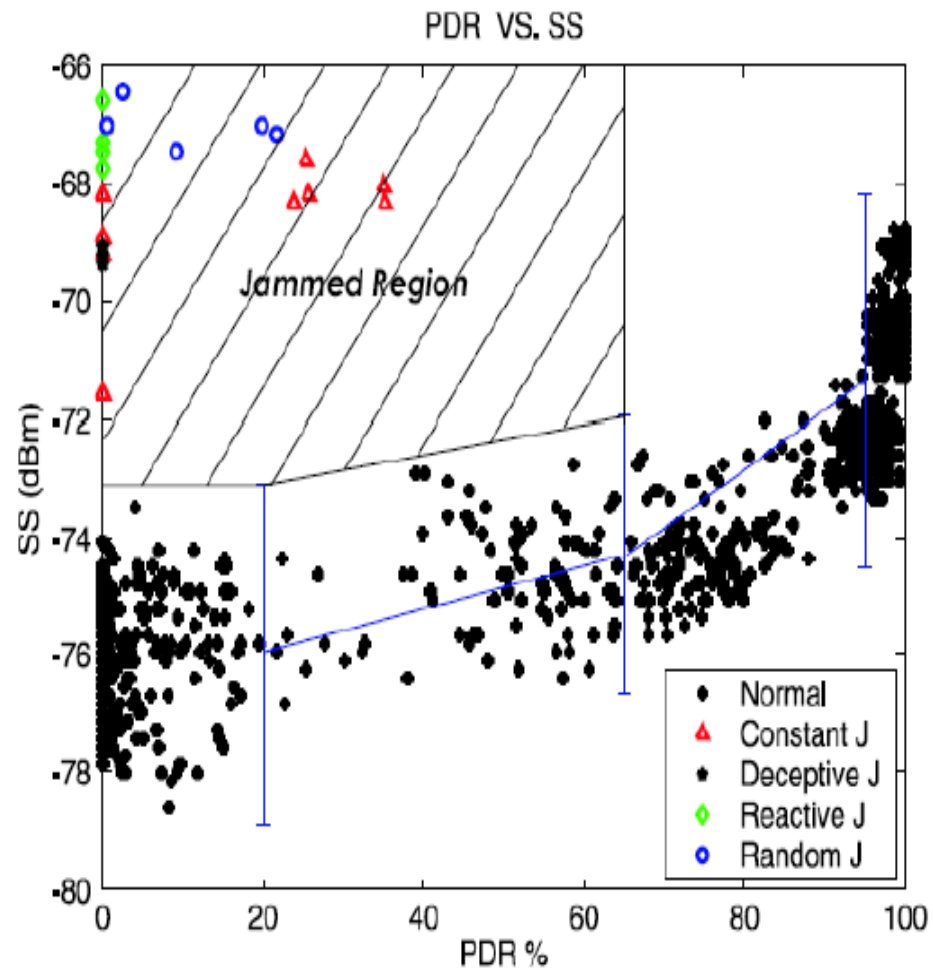 ○ Far neighbor nodes → lower PDR
❑ If all nearby neighbors exhibit low PDR
  → jammed!

PRD/Signal Strength Consistency

Results

- Observed Normal relationships
  - High signal strength yields a high PDR
  - Low signal strength yields a low PDR
- Jammed scenario: a high signal strength but a low PDR
- The Jammed region has above 99% signal strength confidence intervals and whose PDR is below 65%

PDR VS. SS

Jammed Region

SS (dBm)

PDR %

Legend:
- Normal
- Constant J
- Deceptive J
- Reactive J
- Random J

What Happens After Detection??

❑ This work has identified jamming models and described a means of detection

❑ Prevention? Reaction?

  ○ Channel surfing and spatial retreats
  ○ SSCH
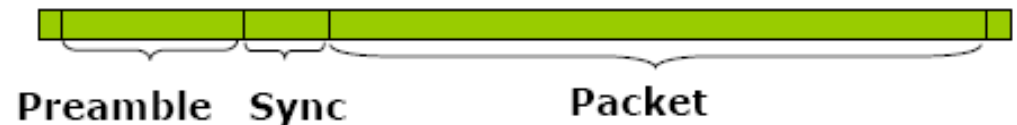
Our Jammers

❑ MAC-layer Jammer
  - Mica2 Motes (UC Berkeley)
    - 8-bit CPU at 4MHz
    - 512KB flash, 4KB RAM
    - 916.7MHz radio
    - OS: TinyOS
  - Disable the CSMA
  - Keep sending out the preamble

❑ PHY-layer Jammer
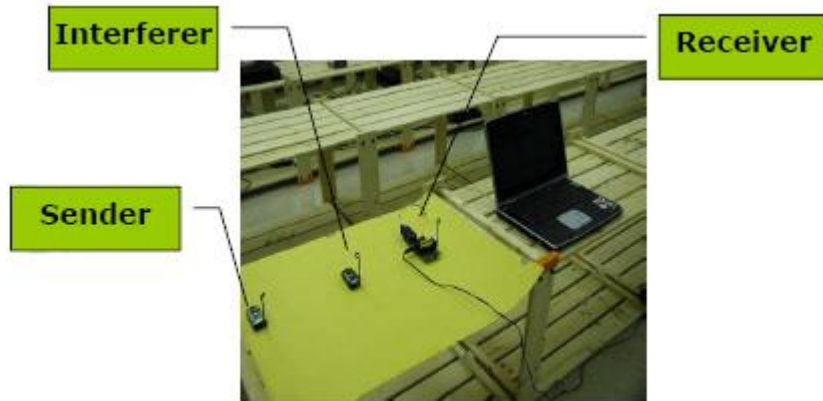 - Waveform Generator
  - Tune frequency to 916.7MHz

Preamble   Sync   Packet

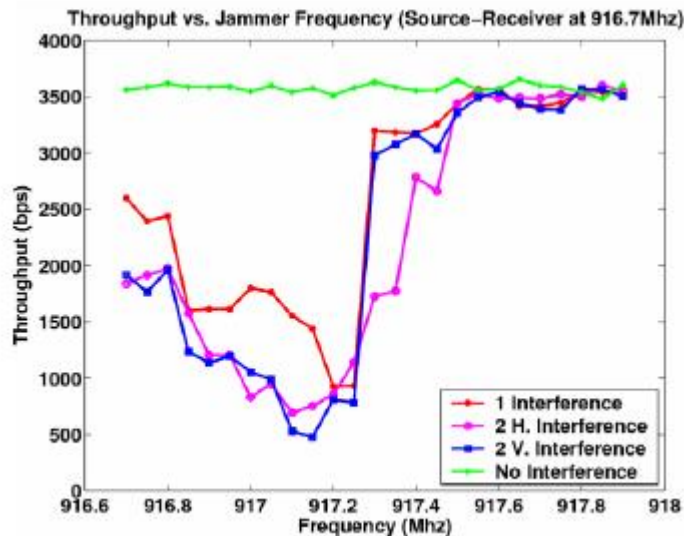# Escaping From Jamming Attacks

❑ **Channel Surfing**

- ○ Utilize frequency hopping if a node detects that it is being jammed it just switches to another channel

  - Inspired by frequency hopping techniques, but operates at the link layer

- ○ System Issues: Must have ability to choose multiple "orthogonal" channels

  - Practical Issue: PHY specs do not necessarily translate into correct "orthogonal" channels

 - Example: MICA2 Radio recommends: "choose separate channels with a minimum spacing of 150KHz" but…..

Throughput VS. Channel Assignment

Interferer · Receiver · Sender

Throughput vs. Jammer Frequency (Source–Receiver at 916.7Mhz)

- 1 Interference
- 2 H. Interference
- 2 V. Interference
- No Interference

- ❑ Sender sends the packet as fast as it can
- ❑ Receiver counts the packet and calculates the throughput
- ❑ The radio frequency of the sender and receiver was fixed at 916.7MHz
- ❑ Increased the interferer's communication frequency by 50kHz each time
- ❑ When the Jammer's communication frequency increases to 917.5MHz, there is almost no interference

Is Channel Surfing Feasible??
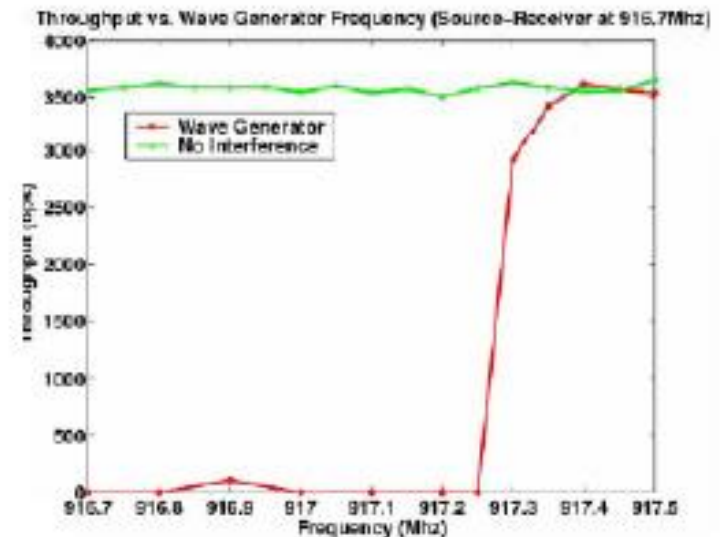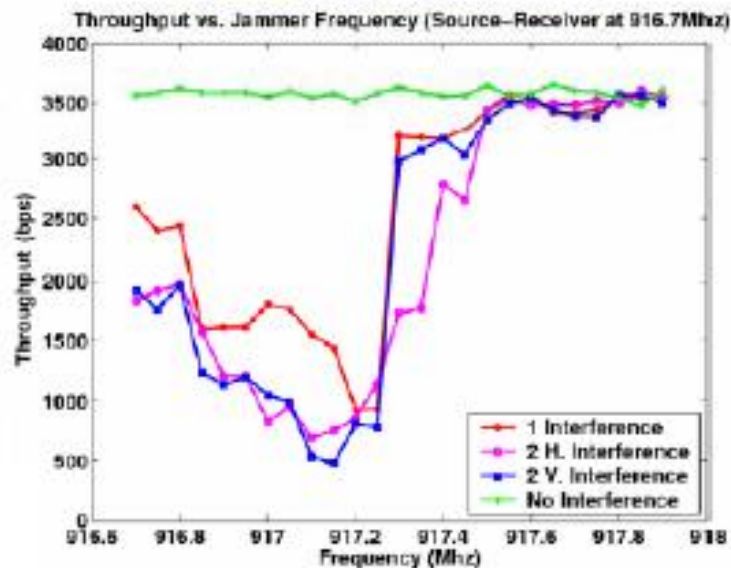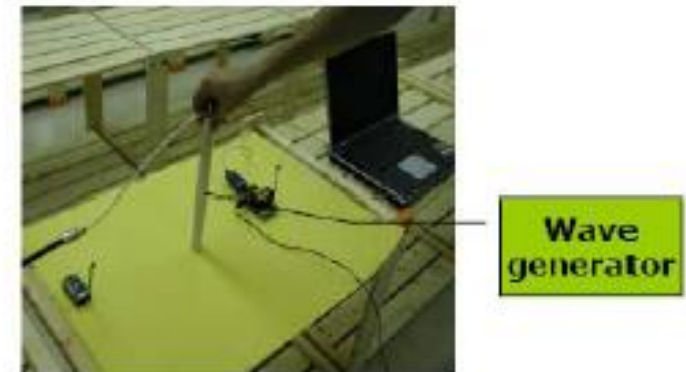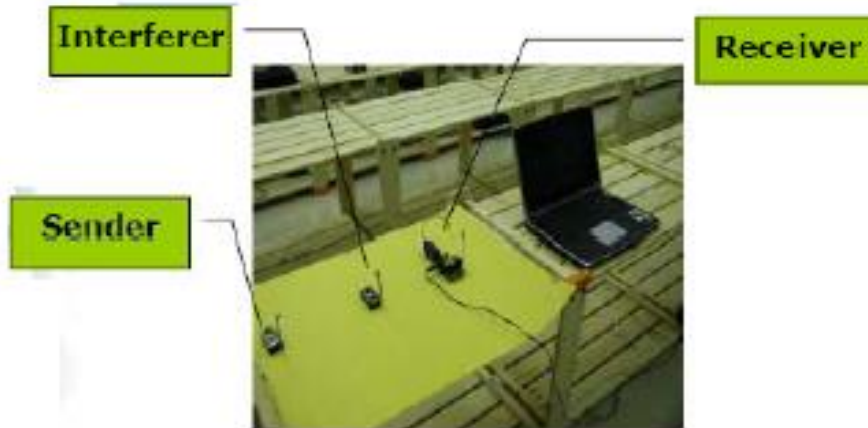
Escaping From Jamming Attacks

❑ "Orthogonal" channels

  ○ The fact is that we need at least 800KHz to escape the interference

  ○ Therefore, explicit determination of the amount of orthogonal channels is important

❑ Channel Surfing

  ○ Target: maximize the delay before the attacker finds the new channel

  ○ Solution: use a (keyed) pseudo-random channel assignment between nodes

Escaping from Jamming Attacks

❑ Spatial Retreats:
  ○ If a node is jammed move spatially (physically) to another location
  ○ When a node changes location, it needs to move to a new location where it can avoid being jammed but minimize network degradation
  ○ Sometimes a spatial retreat will cause a network partition
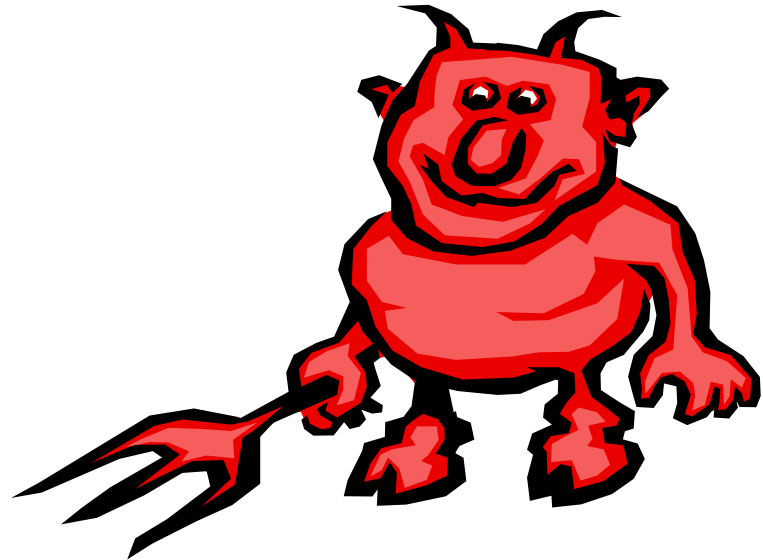
❑ Two different strategies to defend against jamming
  ○ Channel-surfing: changing the transmission frequency to a range where there is no interference from the attacker
  ○ Spatial retreat: moving to a new location where there is no interference

Jammers will be Punished

❑ A man skilled in the operation of commercial wireless Internet networks was sentenced for intentionally bringing down wireless Internet services across the region of Vernal, Utah.

❑ Ryan Fisher, 24, was sentenced to 24 months in prison to be followed by 36 months of supervised release, and to pay $65,000 in restitution.

❑ In total, more than 170 customers lost Internet service, some of them for as long as three weeks

Bottom Line

Don't be Evil !!