# The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks

Authors: Wenyuan XU, Wade Trappe, Yanyong Zhang and Timothy Wood

# OUTLINE

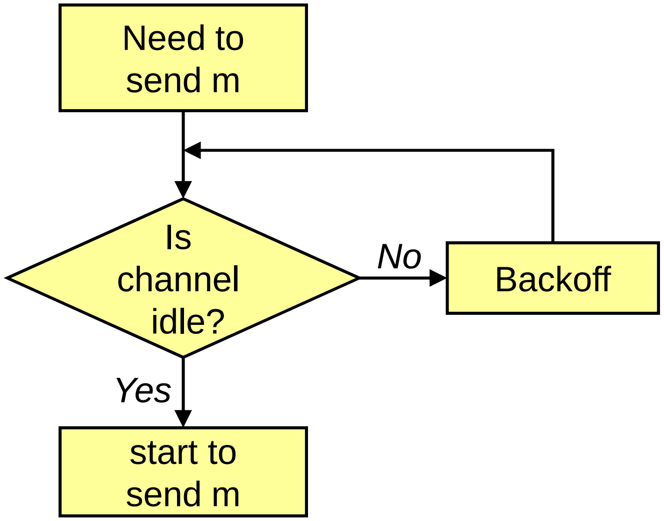
1. Introduction
2. Jamming Attack Models
3. Statistics for detecting jamming attacks
4. Jamming Detection with consistency checks
5. Related Work
6. Conclusion

# INTRODUCTION

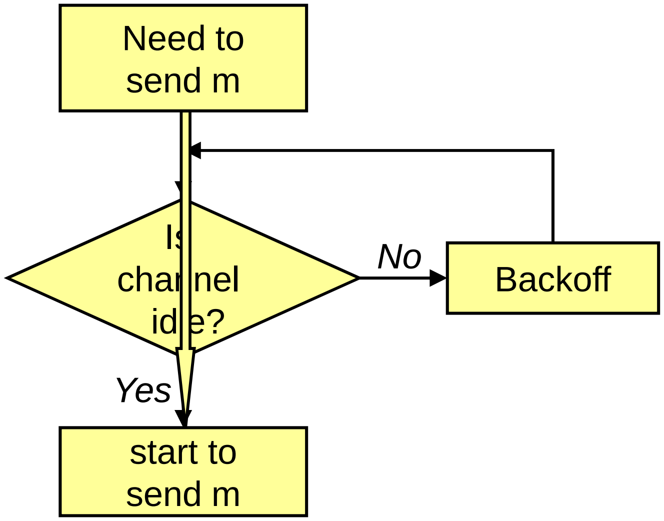
- Wireless networks have gained great popularity. Is providing security is a critical issue??
- An Adversary is empowered to launch a severe DoS attack by blocking the wireless medium. **Jamming**
- The first stage in defense is understanding the types of **Jamming** attacks and …..

# Jammer Attack Models

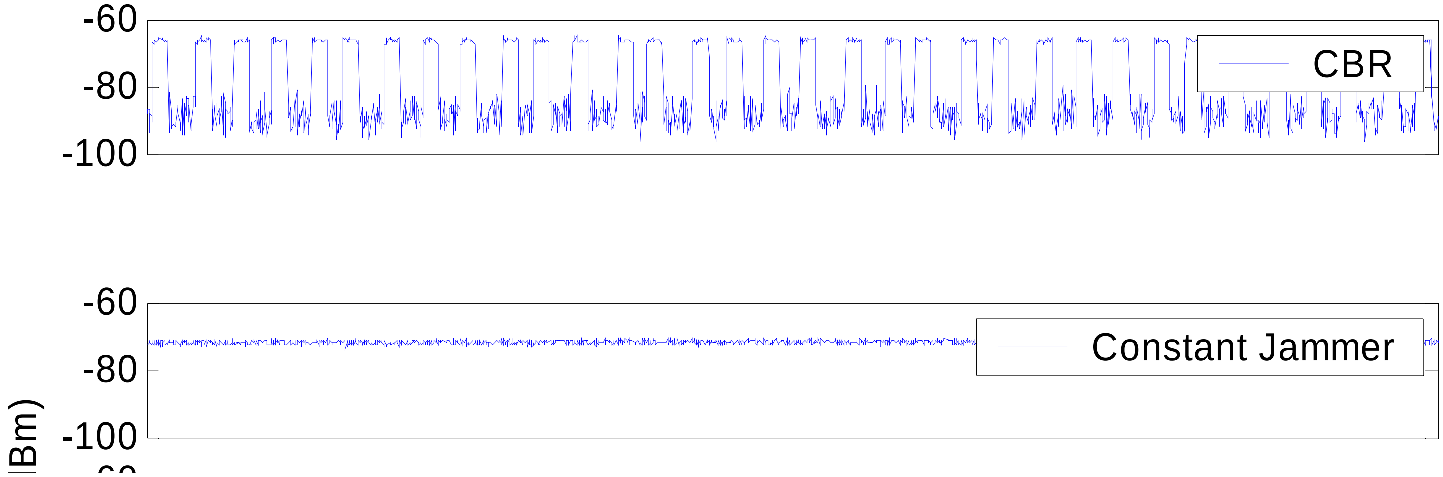
*Normal MAC protocol:*



*Jammer:*

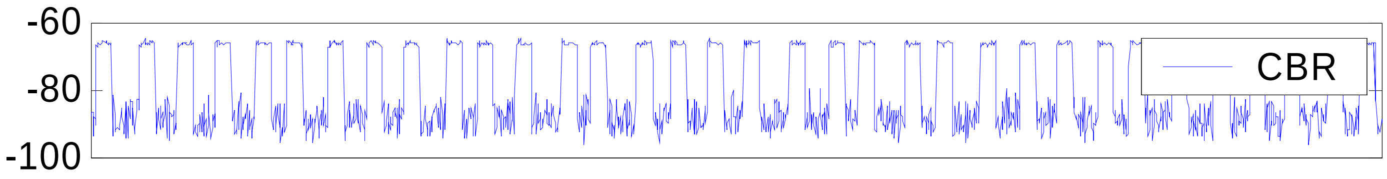


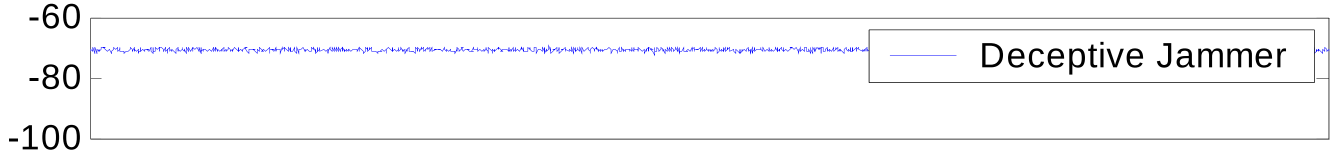
# Constant Jammer



- **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 .

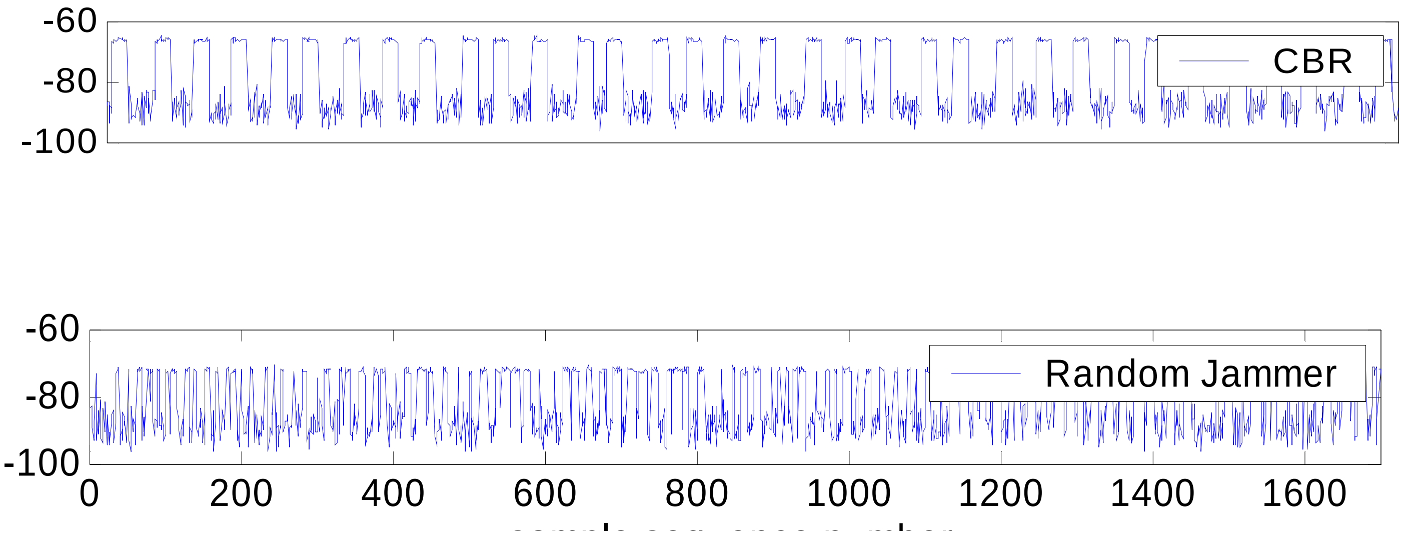
# Deceptive Jammer





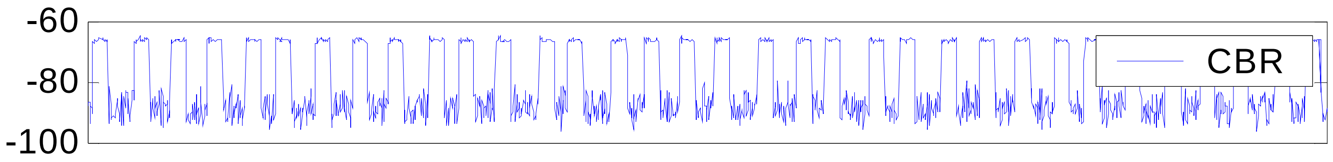
- **Deceptive Jammer-** constantly injects regular packets with no gap between packets. A normal device will remain in the receive state and cannot switch to the send state because of the constant stream of incoming packets.

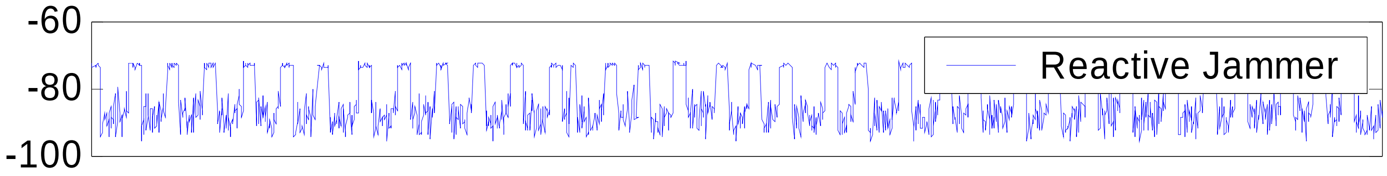
# Random Jammer



- **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.

# How do we measure Communication?

- Packet Sent Ratio (PSR)-the ratio of packets successfully sent by a legitimate sender

  - MAC protocols, Carrier-Sensing and signal strength comparison causing buffered and dropped packets

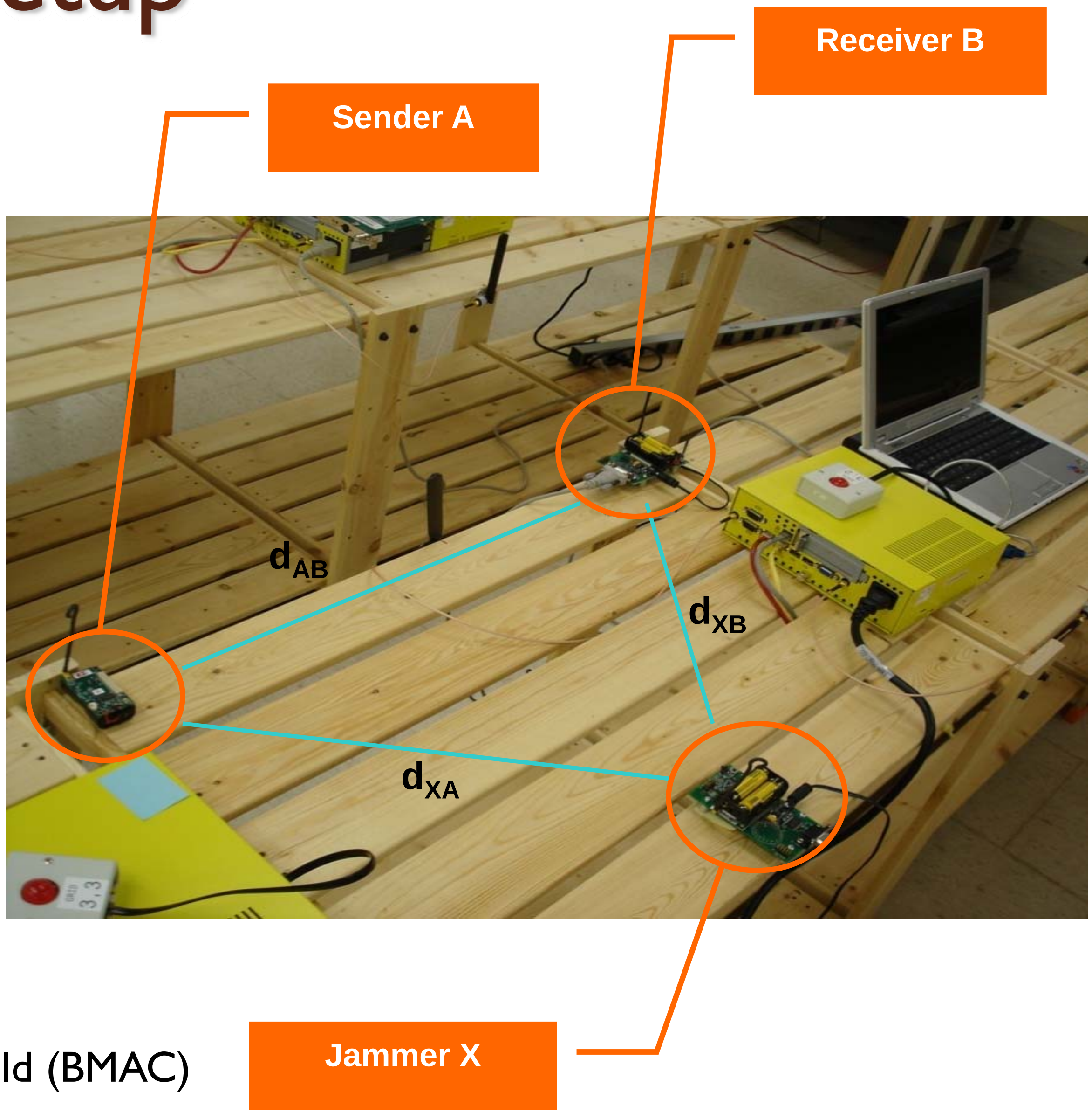
- Packet Delivery Ratio (PDR)- ratio of packets successfully delivered compared to sent(packets may be corrupt even if received)

  - measured by receiver with pass CRC and preamble

  - measured by sender with packets sent and ACK

# 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
    - $P_A = P_B = P_X = -4$dBm
  - MAC
    - Fix MAC threshold
    - Adaptive MAC threshold (BMAC)



# Experiment Results

**Constant Jammer**

| $d_{xa}$ (inch) | BMAC | | FixMAC | |
|---|---|---|---|---|
| | PSR(%) | PDR(%) | PSR(%) | PDR(%) |
| 38.6 | 74.37 | 0.43 | 1.00 | 1.94 |
| 54.0 | 77.17 | 0.53 | 1.02 | 2.91 |
| 72.0 | 99.57 | 93.57 | 0.92 | 3.26 |

**Reactive Jammer**

| $d_{xa}$ (inch) | | BMAC | | FixMAC | |
|---|---|---|---|---|---|
| | | PSR(%) | PDR(%) | PSR(%) | PDR(%) |
| *m* = *7bytes* | 38.6 | 99.00 | 0.00 | 100.0 | 0.00 |
| | 54.0 | 100.0 | 99.24 | 100.0 | 99.87 |
| | 72.0 | 100.0 | 99.35 | 100.0 | 99.87 |
| *m* = *33bytes* | 38.6 | 99.00 | 0.00 | 100.0 | 0.00 |
| | 44.0 | 99.00 | 58.05 | 100.0 | 87.26 |
| | 54.0 | 99.25 | 98.00 | 100.0 | 99.53 |

# What attributes will help us detect jamming?

- Signal Strength
- Carrier Sensing Time
- Packet Delivery Ratio

# 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

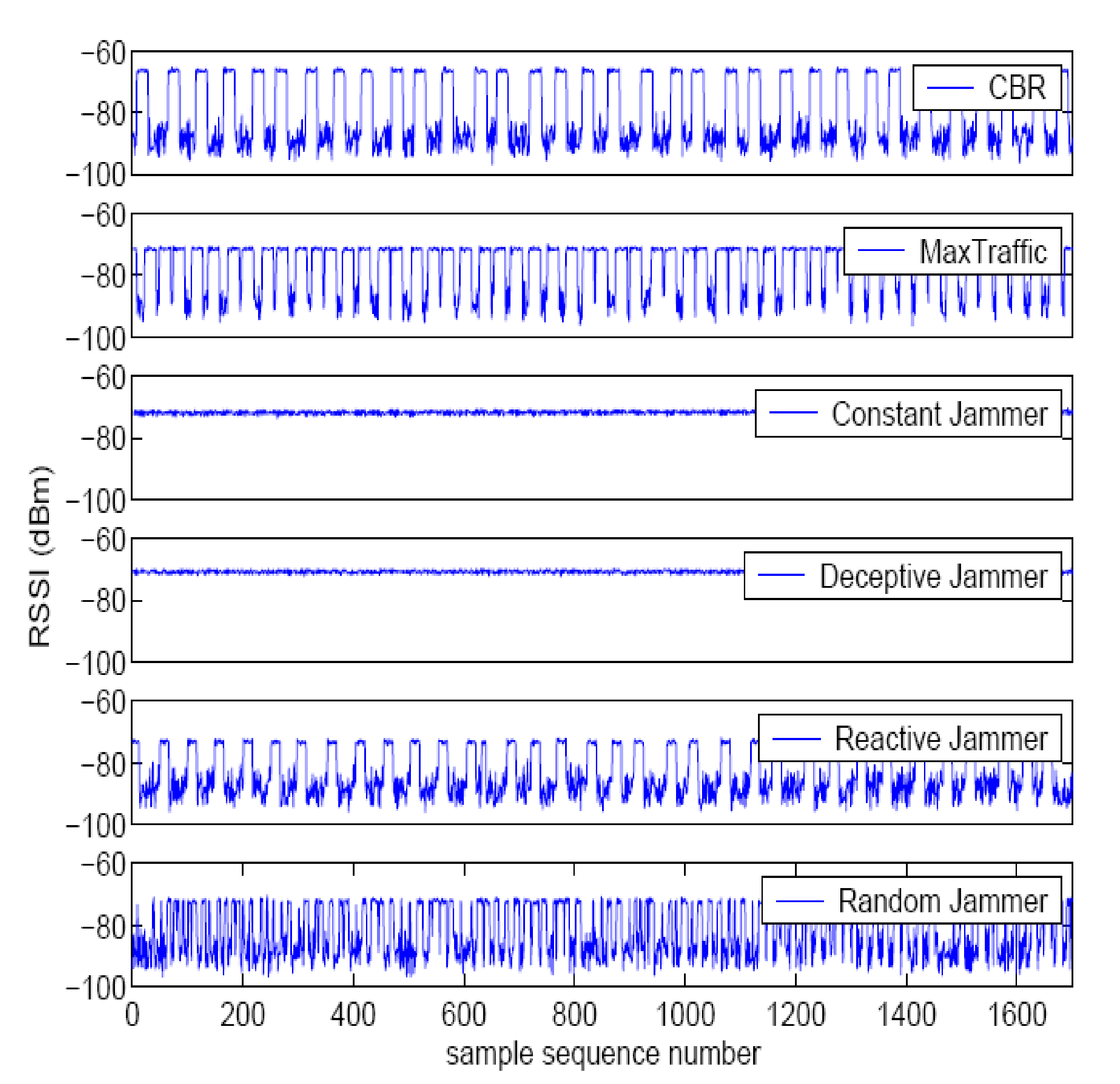
# SIGNAL STRENGTH

-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



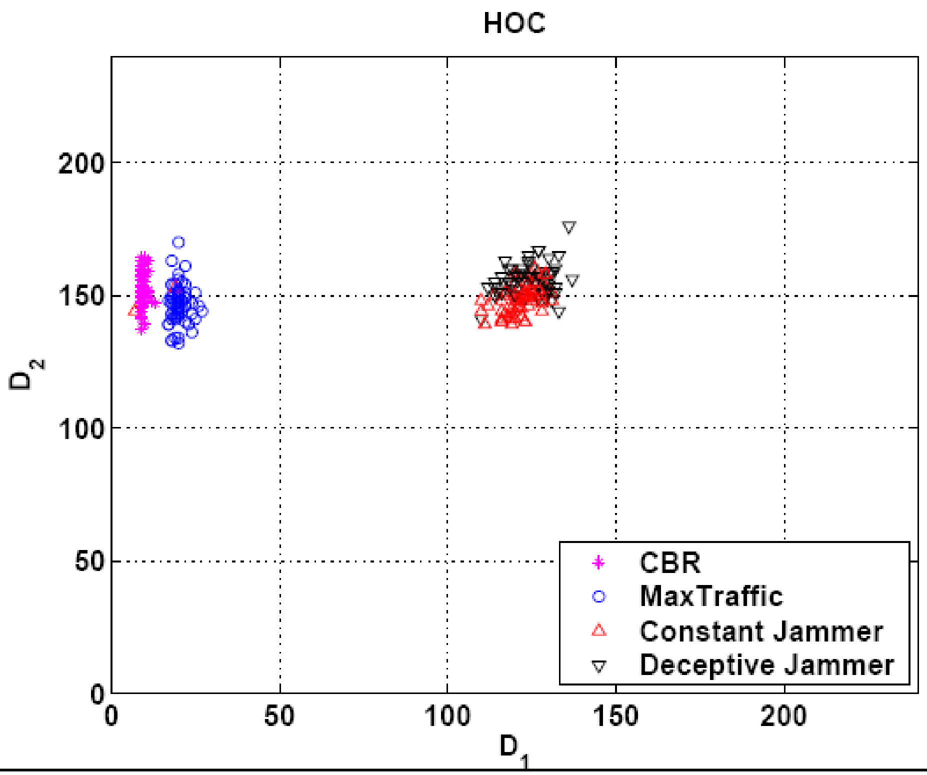
# More on Signal Strength

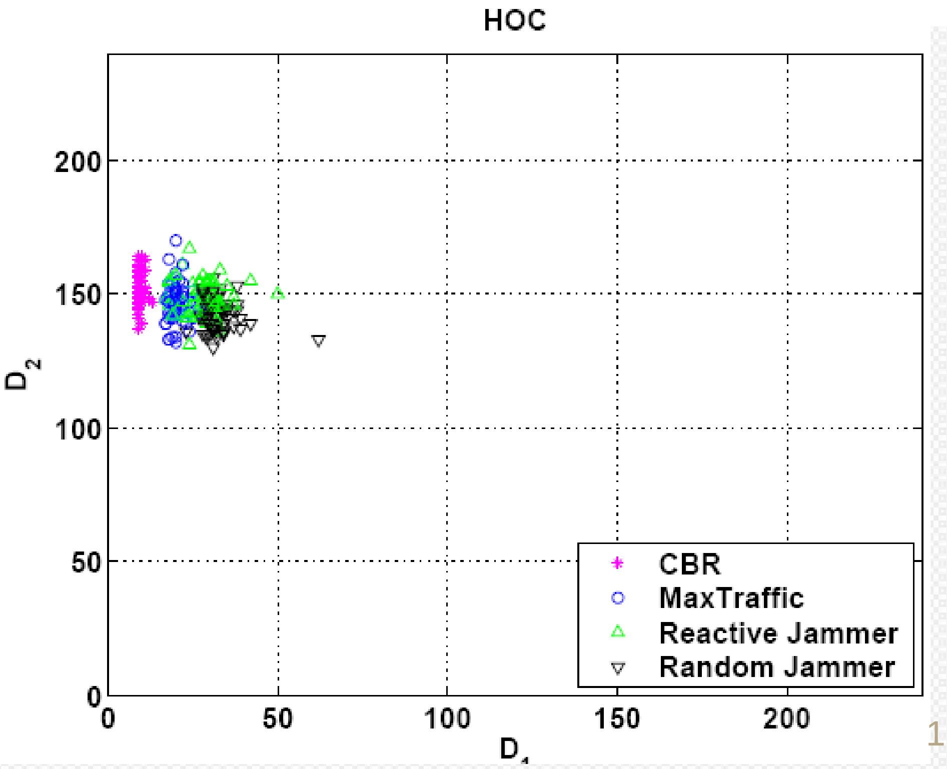
- **Not Successful**

- 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





# Next….Carrier Sensing Time

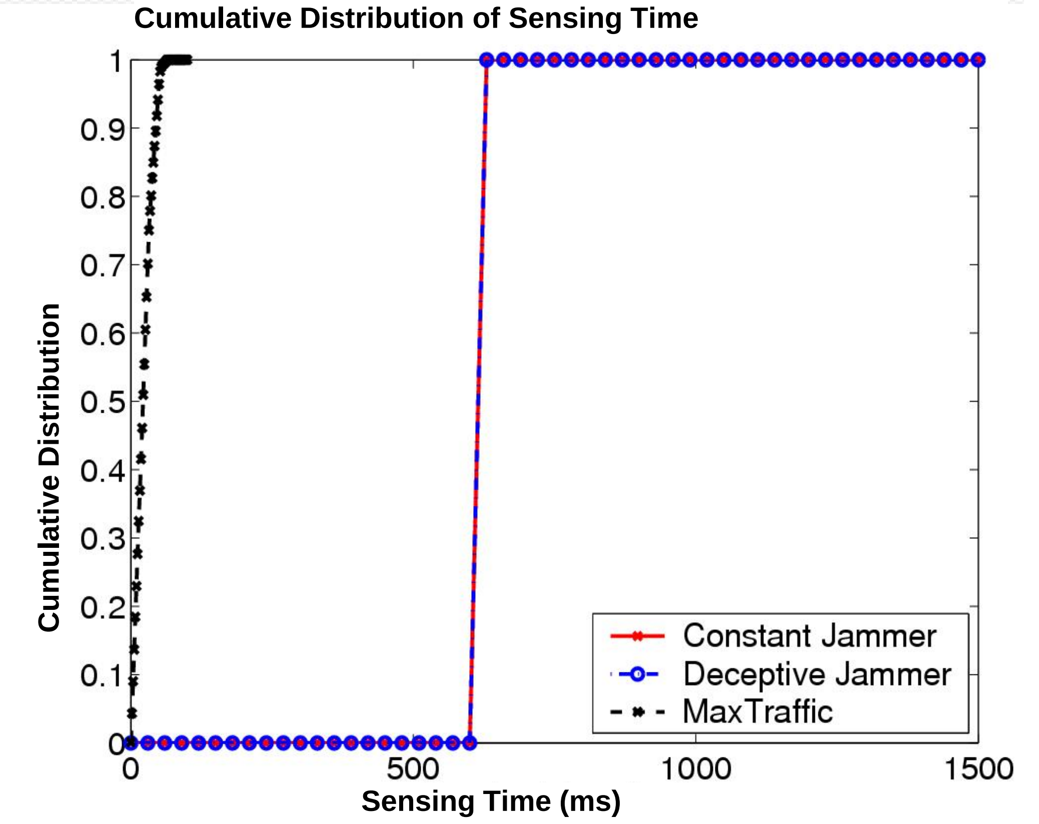
- 802.11 uses CSMA and RTS/CTS so if the channel is occupied either a time out or stuck in channel sensing
- Establish an average sensing time during normal traffic to allow you to compare when you may be jammed.
- Only works with fixed signal strength not adaptive thresholds such as BMAC.
- Determine when large sensing times are results of jamming by setting a threshold
- Threshold set conservatively to reduce false positive (significance testing)

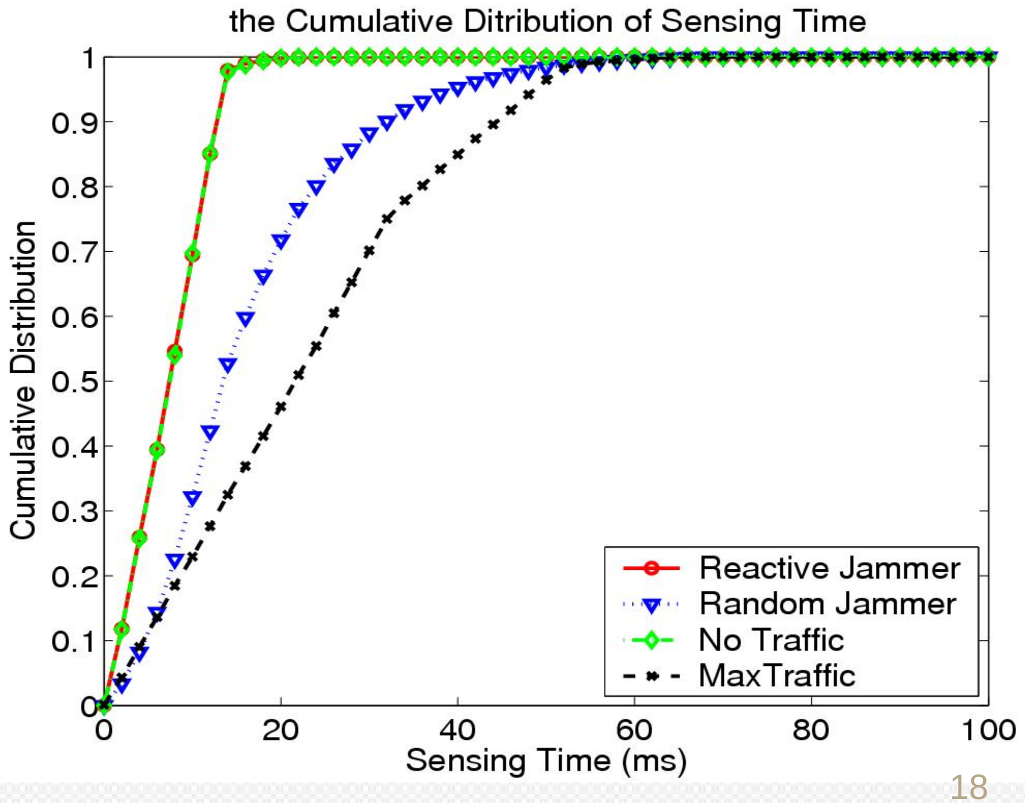
# Carrier Sensing Time Analysis

Observations:

- It detects the Constant and Deceptive Jammer

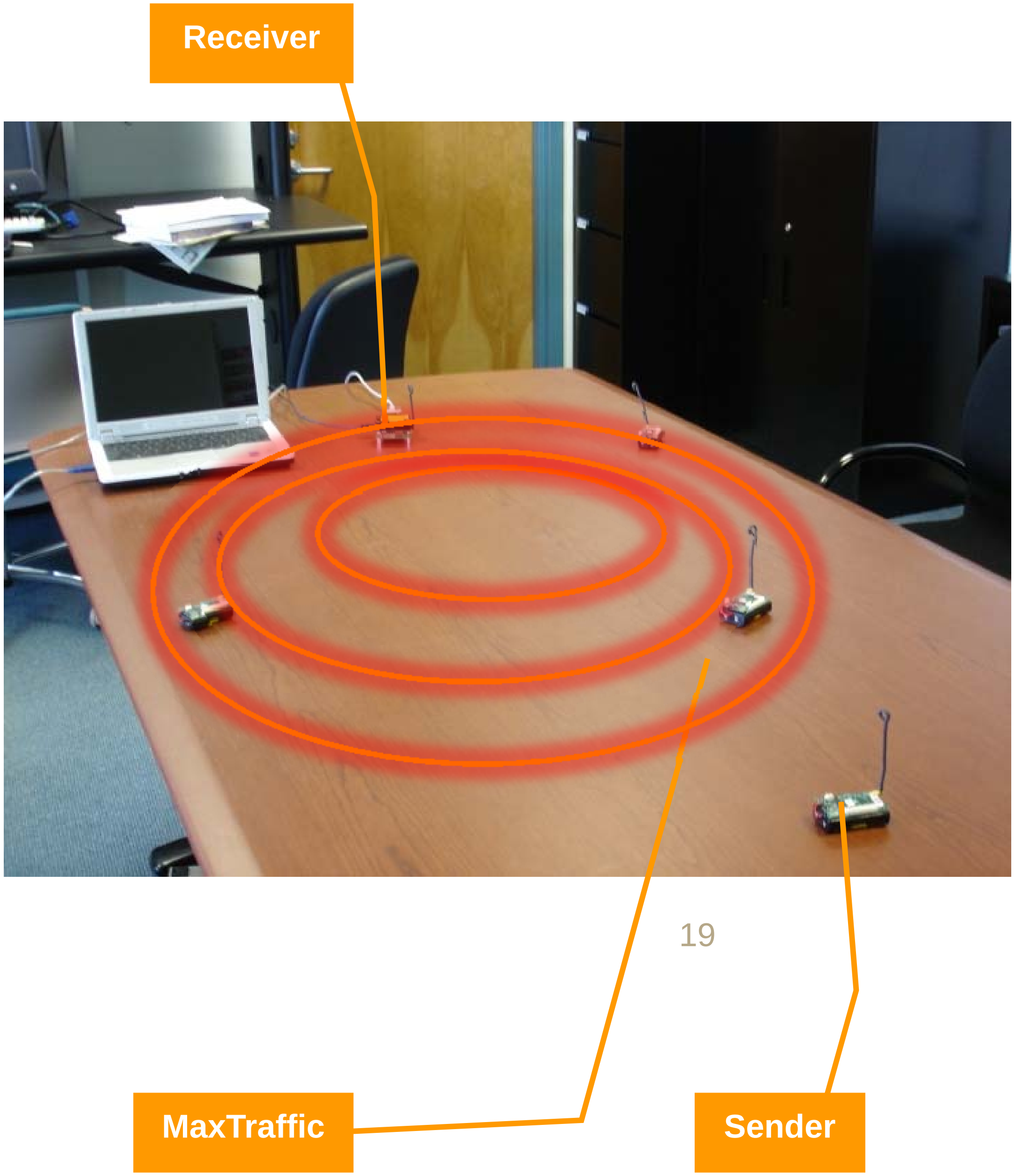
- It does not detect the Reactive or Random Jammer





# Finally, the best for last….Packet Delivery Ratio

- How much PDR degradation can be caused by non-jamming, normal network dynamics, such as congestion?
- Result: PDR 78%
- It can be measured in two ways, by the sender or receiver
- the PDR can be used to differentiate a jamming attack from a congested network.
- A simple threshold based on PDR is a powerful statistic to determine Jamming vs. congestion.
- It can not account for all network dynamics.



# 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.

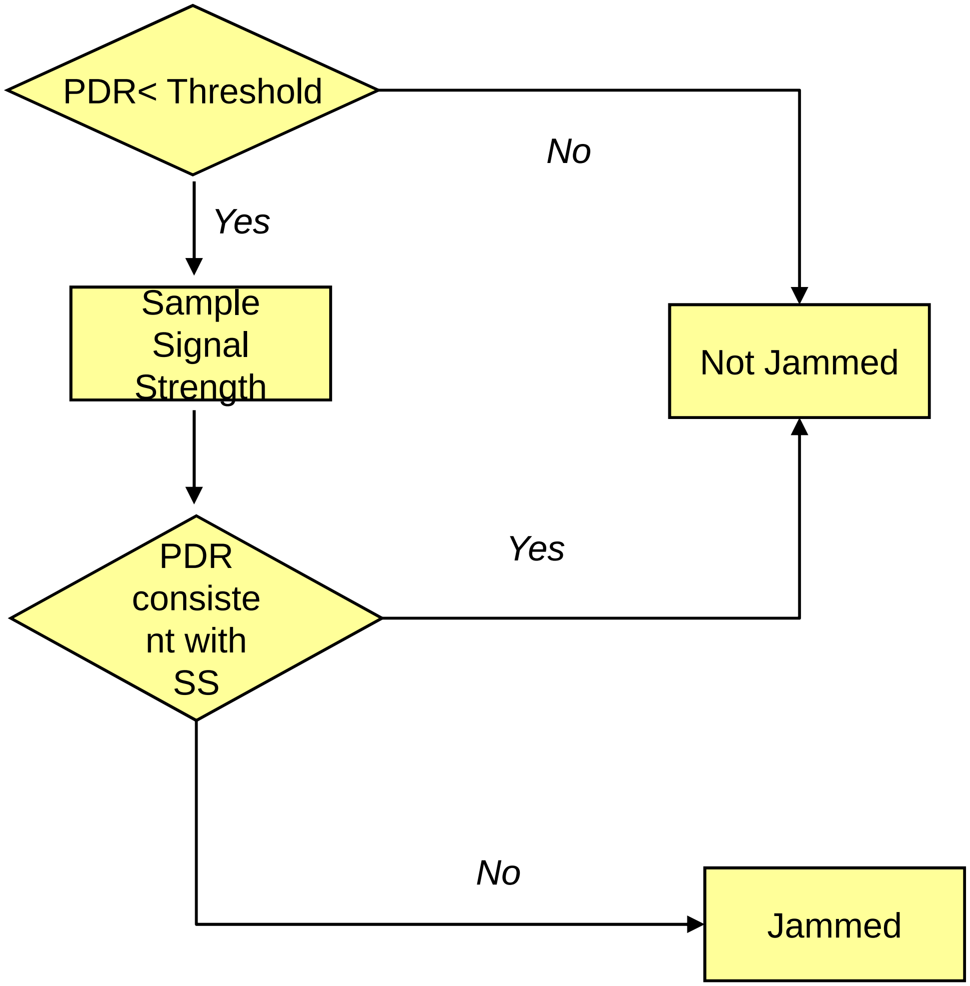
# We need Consistency Checks to be Sure

1. Signal Strength Consistency Checks
2. Location Consistency Checks

Assumptions

- Each node detects whether it is jammed
- Each node maintains a neighbor list from routing layer
- Network deployment is dense so each node has several neighbors
- All legitimate nodes participate by sending heartbeat beacons( allows for reliable estimate of PDR over time)

# PRD/Signal Strength Consistency



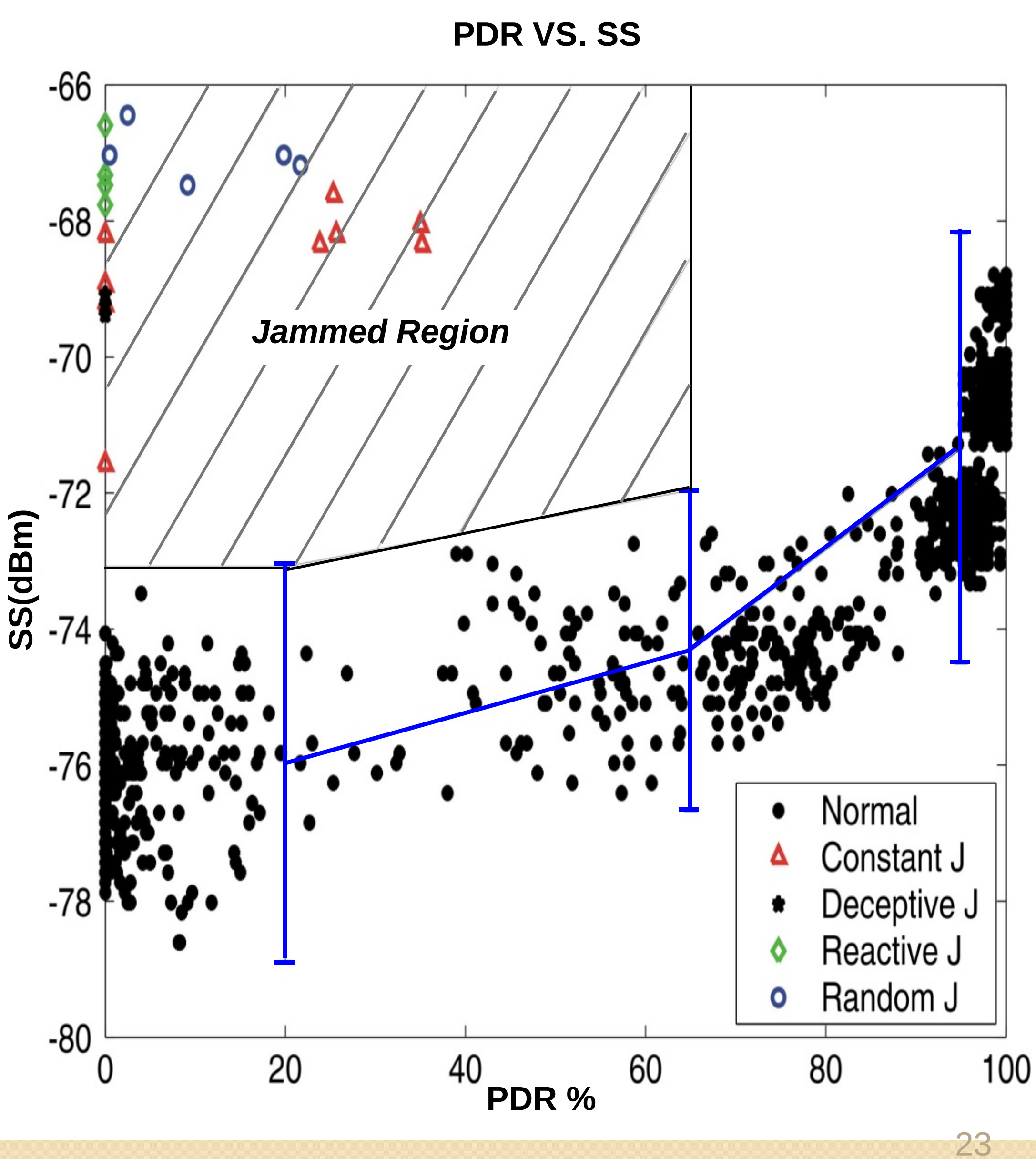
# 4.1 Signal Strength Consistency Checks

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 DISTANCE

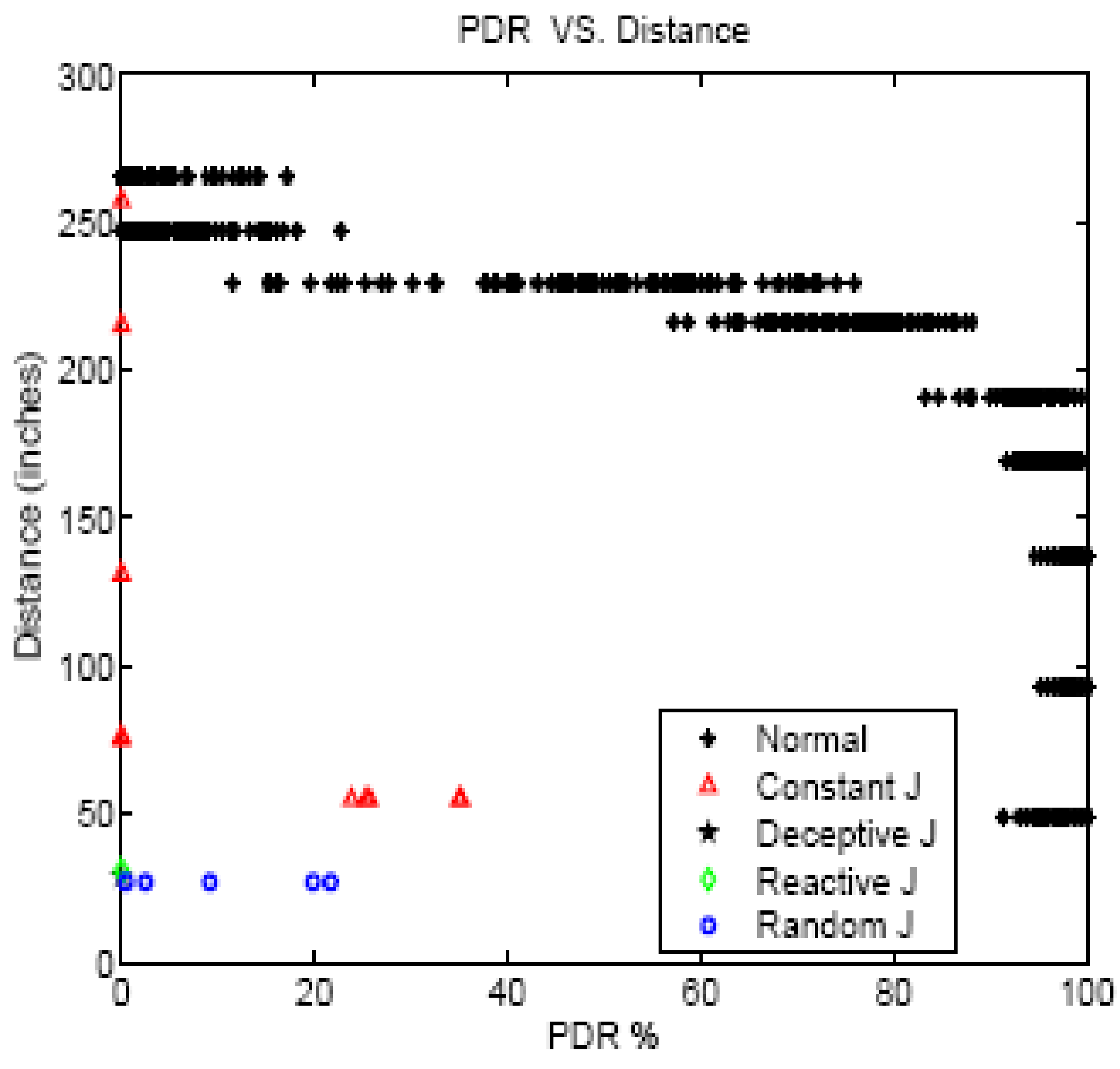
**Observations:**

- Neighbors that are close should have high PDR values, if they have low PDR values they are Jammed

- All nodes advertise their current location and their PDRs to their neighbors to ensure there is a minimum amount of traffic to establish PDR. Thus PDR = 0 if no packets received

- Similar to the SS consistency check. An initial baseline to represent the profile of a normal environment (PDR,d) for each node.

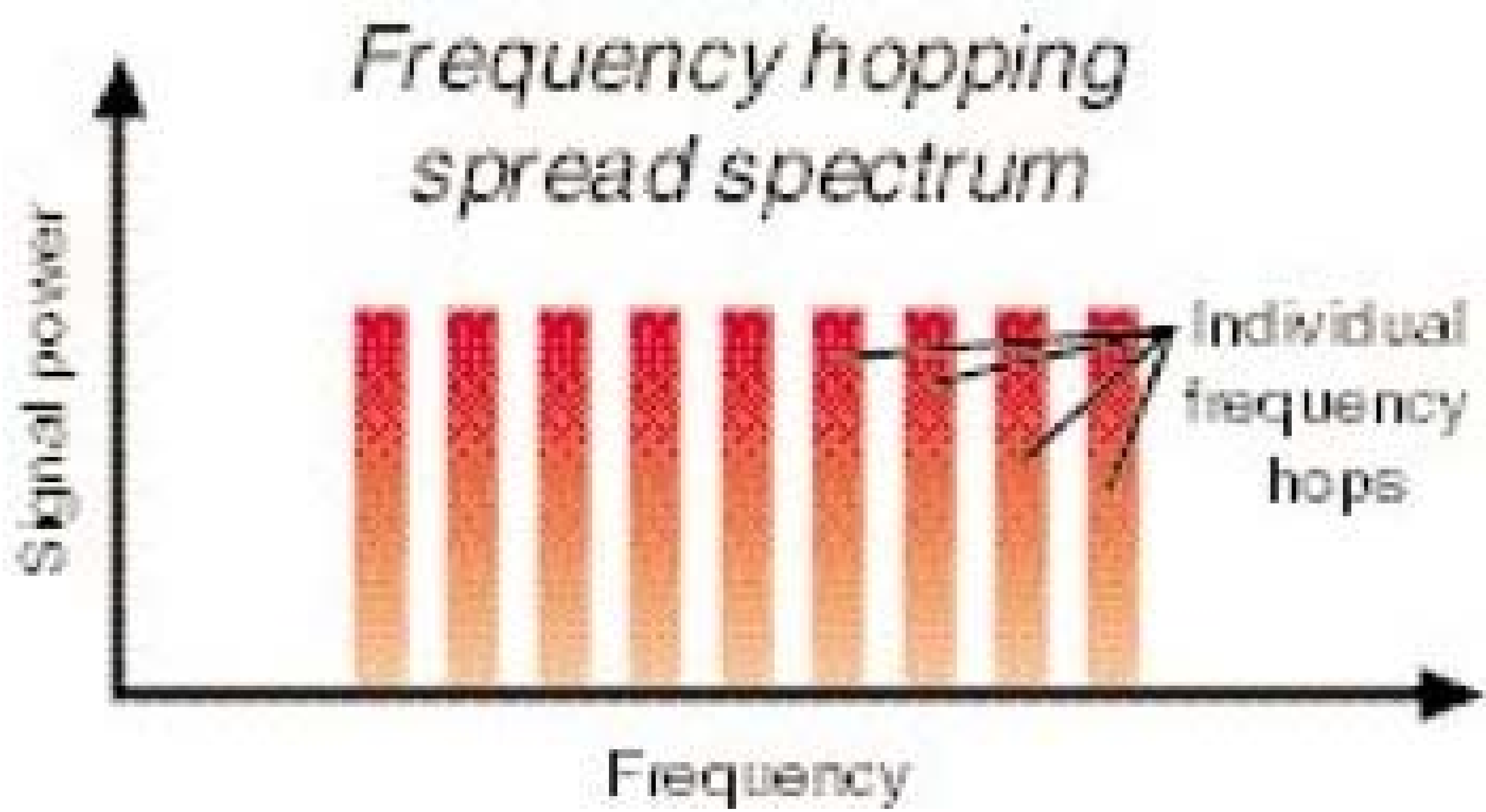
- If a lower PDR is observed than should be for a given distance under normal radio conditions than the node declares it is Jammed.



# 5. RELATED WORK

- This work focuses on being able to detect and under stand attacks. Do you understand that you are under attack??

- Countermeasures : Physical layer design technologies such as spread spectrum work but have not found wide spread deployment in commodity wireless devices.



- The use of Low density parity check codes, Reed-Solomon codes, channel surfing or on demand link layer frequency hopping and spatial retreats….yes, Run Away!!

# 6. CONCLUSIONS

- Protecting our wireless networks is important
- Jamming is a viable threat
- Detecting Jamming is the first step in defeating it