Cooperative Anomaly Detection in Dynamic Spectrum Access Networks

Rutgers, The State University of New Jersey

www.winlab.rutgers.edu

Song Liu, Larry J. Greenstein, Wade Trappe, Yingying Chen

song@winlab.rutgers.edu

Content

- Background and Motivation
- Network Structure with Spectrum Policy Enforcement
- Anomaly Detection Using Significance Testing
- Distributed Detection Using Energy Fingerprint
- Summary and Ongoing Work

Motivation

- Openness of the Lower-layer Protocol in Cognitive Radio (CR)
  - A flexible solution to dynamic spectrum access (DSA)
  - Target for adversaries and susceptible to reckless users

- Spectrum etiquette enforcement is critical to effectiveness and correctness of a DSA system
  - Detection
  - Localization
  - Elimination

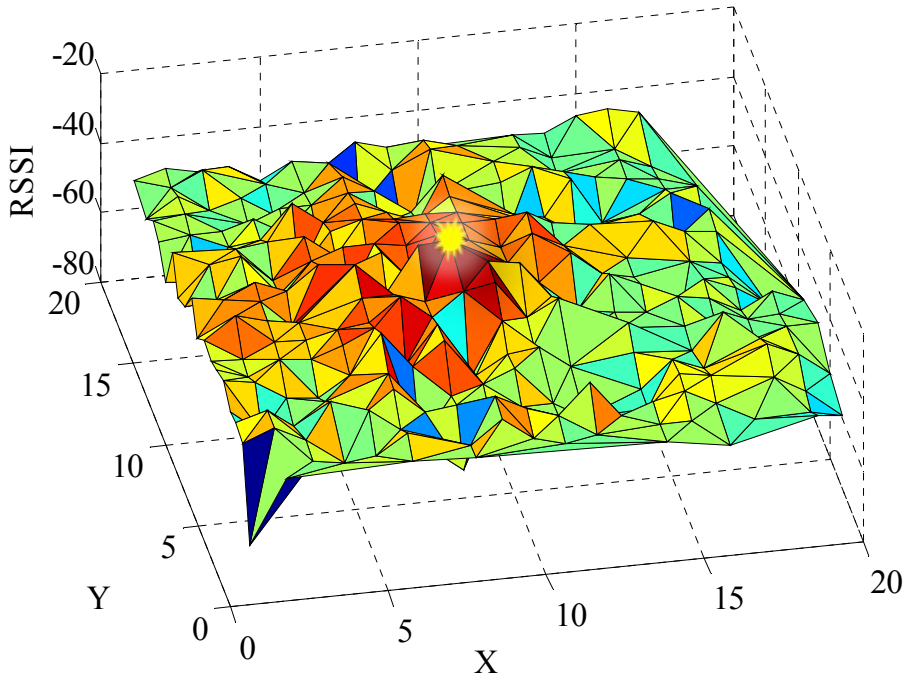
Detection of Anomalous Usage

- Spectrum Anomaly: a spectrum usage that is not authorized by the DSA protocol and therefore can interfere with authorized (primary) users.

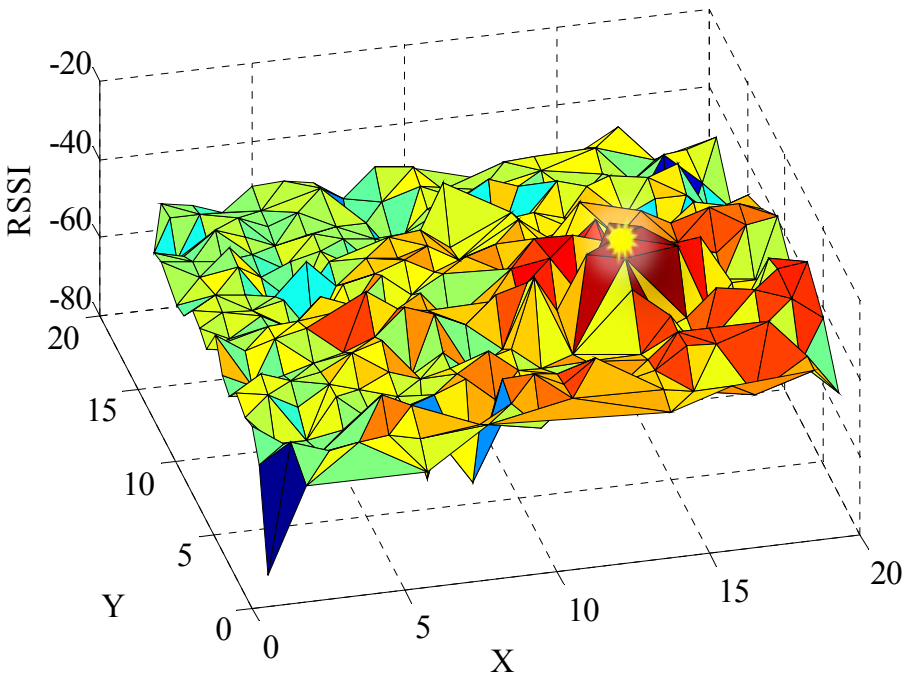
- Distinguishing bad (unauthorized) transmissions from good (authorized) ones
  - **Challenge**: Conventional signal processing techniques are insufficient
  - **Goal**: Effective detection mechanism relying on non-programmable features

Radio Energy Based Fingerprint Detection

- Transmitters at different locations yield different "power maps"
  - **Fingerprint**: spatial distribution of the received signal strength
  - Its robustness has been shown in fingerprint localization [RADAR]



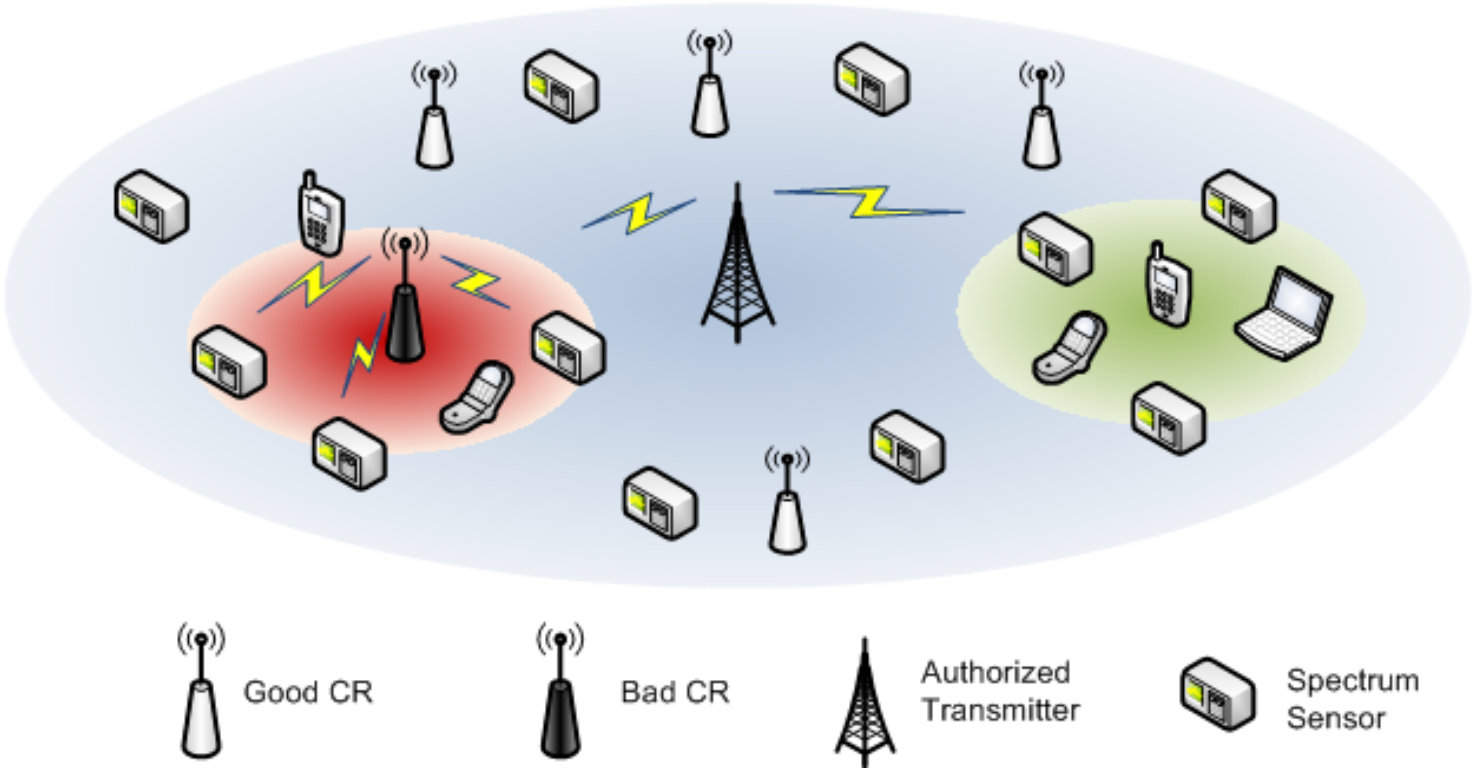
Tx = (9, 10)



Tx = (14, 8)

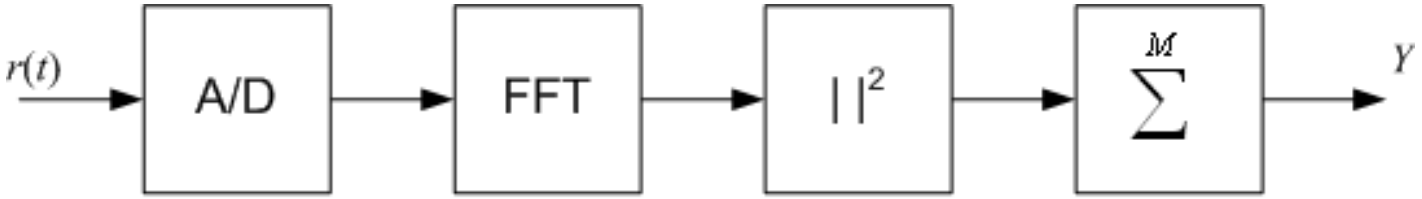
Sensor Assisted Anomaly Detection

- Network Structure for Anomaly Detection
  - Primary (authorized) transmitter is stationary
  - Distributed detection by a 3rd-party sensor network
    - *sensors collaborate locally.*



Energy Detection Model

- FFT implementation of an energy detector



- A lognormal approximation of the energy detector output
  - **Assumption**: signal bandwidth is sufficiently large so that M frequency samples are i.i.d.

$$Y_n = Y_{0,n} + Y_{R,n}, \quad \text{(dB)}$$

  - $Y_{0,n}$: path loss and shadow fading (correlated over space)
  - $Y_{R,n}$: multipath fading, independent (but may not be identical) over space

Anomaly Detection Using Significance Testing

- Statistics of the energy measurement only known under the normal condition:

$$\mathcal{H}_0 : r(t) = s(t) + w(t), \qquad \text{normal usage,}$$
$$\mathcal{H}_1 : r(t) = s(t) + x(t) + w(t), \qquad \text{anomalous usage}$$

  - s(t): authorized signal
  - x(t): unauthorized signal – *unknown!*
  - w(t): AWGN

- Significance Testing
  - Test statistic **T**: a measure of observed data
  - Acceptance Region Ω: we accept the null hypothesis if T∈Ω
  - Significance level α: probability of false alarm

$$Prob(\mathbf{T} \notin \Omega | \mathcal{H}_0) \leq \alpha$$

Distributed Anomaly Detection

- Each sensor computes the residual error

$$e_n = Y_n - Y_n^c$$

- The residues are exchanged among neighboring sensors
- A *differential fingerprint* is constructed at each sensor

$$\hat{\mathbf{e}} = (\hat{e}_1, \hat{e}_2, \ldots, \hat{e}_{N-1})^T$$

- Based on the lognormal approximation, the residues are jointly normal distributed $\hat{\mathbf{e}} \sim \mathcal{N}(0, \mathbf{\Sigma}_e)$
- An anomaly is declared if the difference is above a threshold
  - Acceptance region:

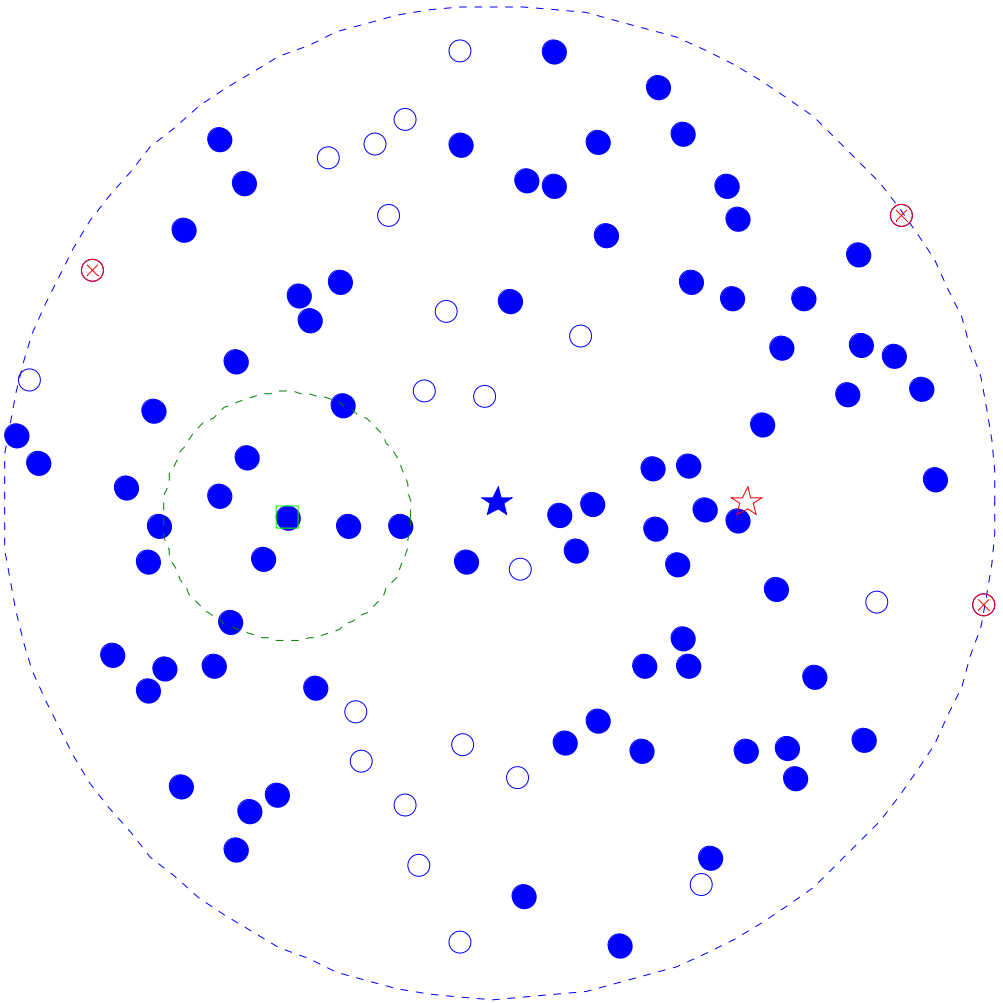
$$\Omega = \{\hat{\mathbf{e}} : f(\hat{\mathbf{e}}) \geq f_T\}$$

  - False alarm rate:

$$Q_F = \frac{\Gamma((N-1)/2, T_c/2)}{\Gamma((N-1)/2)}$$

Simulation Evaluation

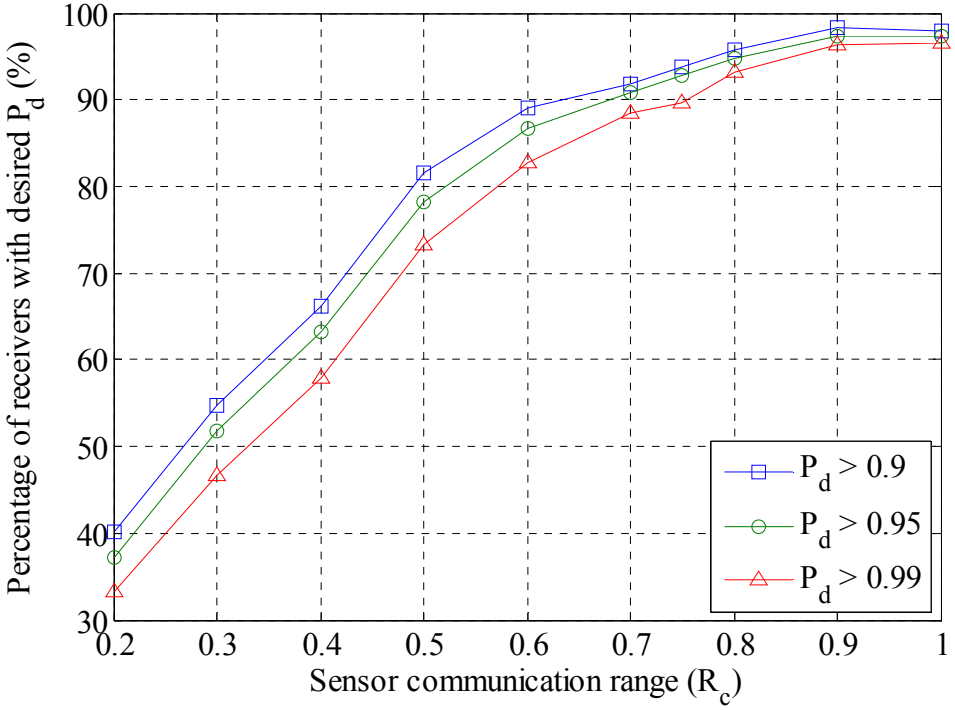
- A detection scenario
  - Path loss $\gamma = 2$
  - Shadowing $\sigma_s = 6$ dB
  - False alarm rate $Q_F = 0.05$
  - Transmission ISR = 0 dB
  - $N = 100$; $R_c = 0.25R$
  - 77 sensors have $Q_D > 0.9$



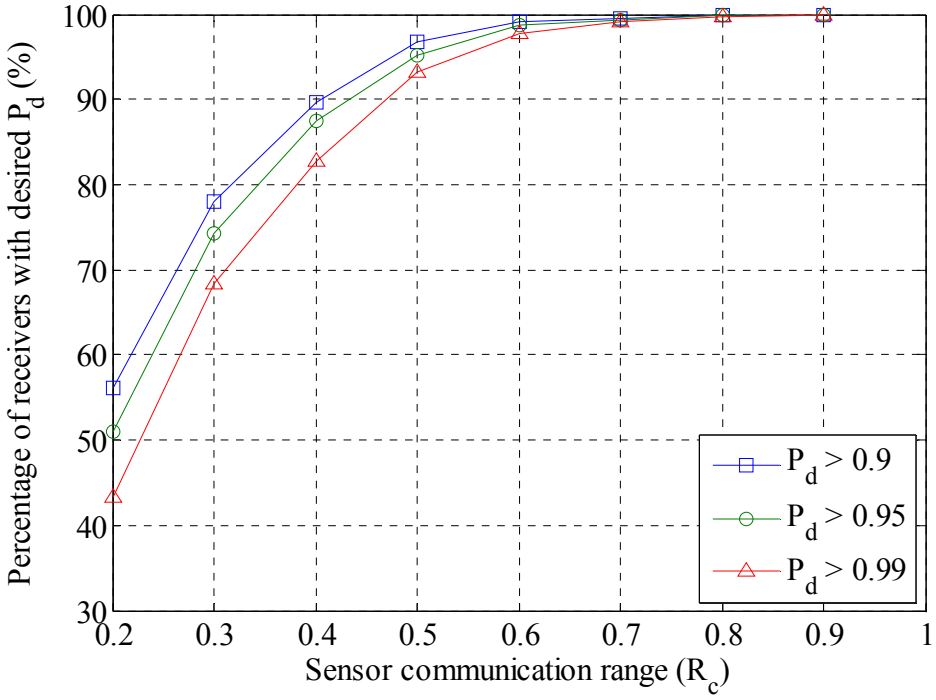
- : sensors with $Q_D > 0.9$
- ○ : sensors with $Q_D \leq 0.9$
- : sensors with <2 neighbors

Simulation Evaluation (2)

- Percentage of sensors with a desired detection probability
  - ISR = -10 dB: > 70% of Pd > 0.99 for $R_c = 0.5R$
  - ISR = 0 dB: > 93% of Pd > 0.99 for $R_c = 0.5R$



ISR = -10 dB



ISR = 0 dB

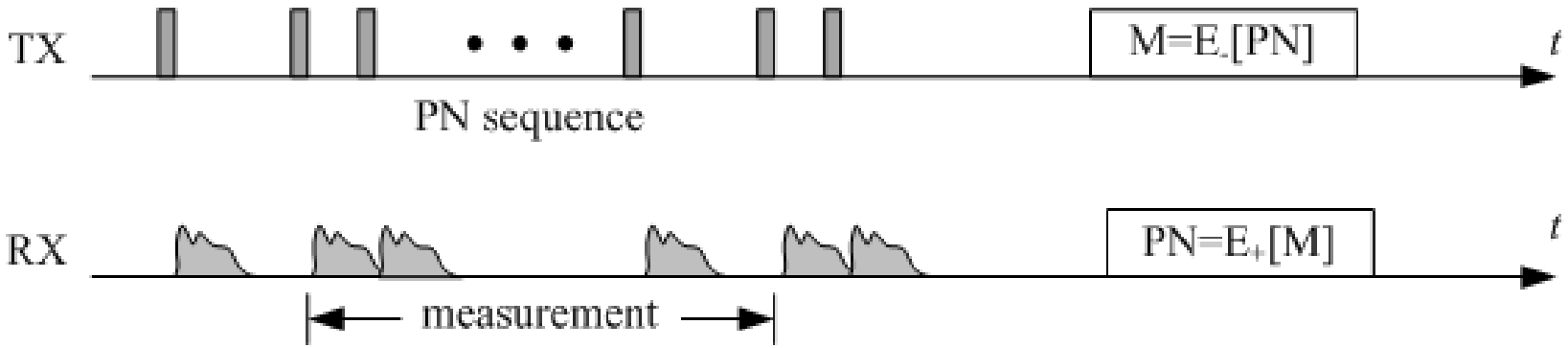
Summary and Ongoing Work

- We propose a cooperative detection method for anomaly detection in a dynamic spectrum access network
  - The method utilizes energy detectors so it is independent of the signal structure.
- The detection is performed by exchanging energy measurements among locally distributed sensors and comparing the difference between two energy fingerprints
- We formulate the detection problem as a significance test
- Ongoing work
  - Empirical based threshold in an imperfect environment
    - *Energy detector output is no long lognormal at low SNR!*
    - *Empirical detection threshold by a learning process*
  - Decision fusion

Thank You!

Questions?

A Secure Method for Energy Calibration



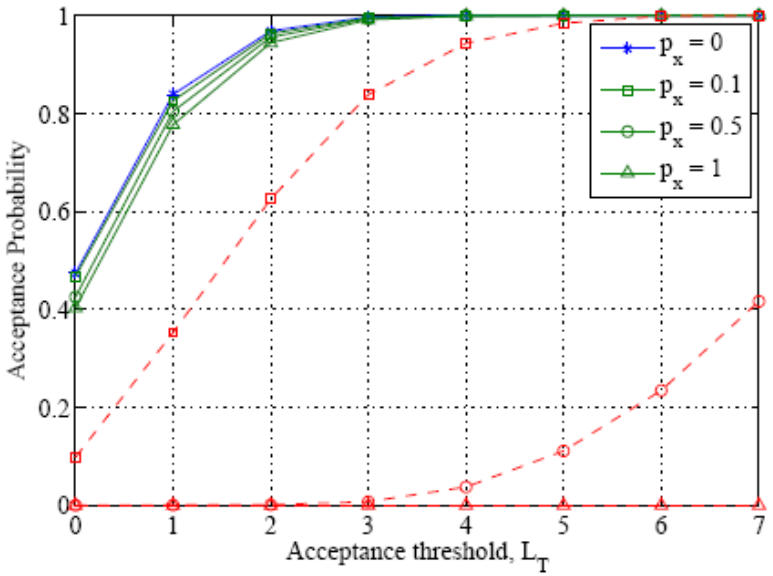
- Calibration signal: a PN sequence using On-Off-Key
- A scheme analog to *delayed key disclosure*
  - The sequence is unknown to sensors during transmission
  - The exact sequence is announced a short time later via a public authentication channel between the authorized transmitter and sensors
- **Assumptions**:
  - sensors can store and decode the sequence from the secret channel
  - Sensors are synchronous with the primary transmitter

A Secure Method for Energy Calibration

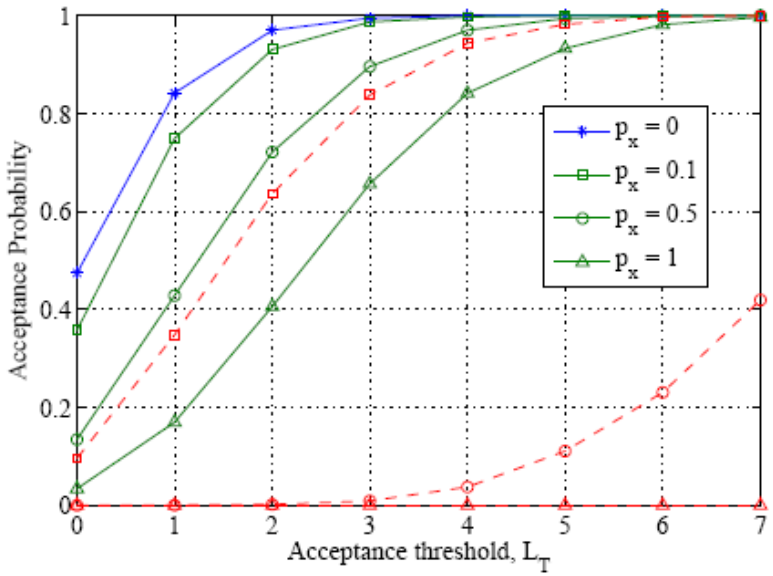
- A maximum-length sequence (m-sequence) is sent twice
  - A sensor receives a cyclic shifted version of the m-sequence

$$\rho(k) = \begin{cases} N, & k = 0 \\ -1, & 0 < k < N \end{cases}$$

- Probability of accepting the calibration sequence (ISR=-10 & 0 dB)



SNR = 0 dB



SNR = 10 dB