Attack Detection in Wireless Localization

Yingying (Jennifer) Chen

Dept. of Computer Science, Rutgers University
Wireless Information Network Laboratory (WINLAB)
Alcatel-Lucent Technologies

Joint work with Prof. Wade Trappe and Prof. Richard P. Martin

WOCC 2007

Introduction

- What is localization?
  - Simply to find the position of a wireless device or a sensor node.
- Why wireless localization?
  - Public
    - Healthcare monitoring
    - Wildlife animal habitat tracking
    - Emergency rescue/recovery
  - Enterprise
    - Location-based access control
    - Location-aware content delivery
    - Asset tracking

Motivation: Secure Localization

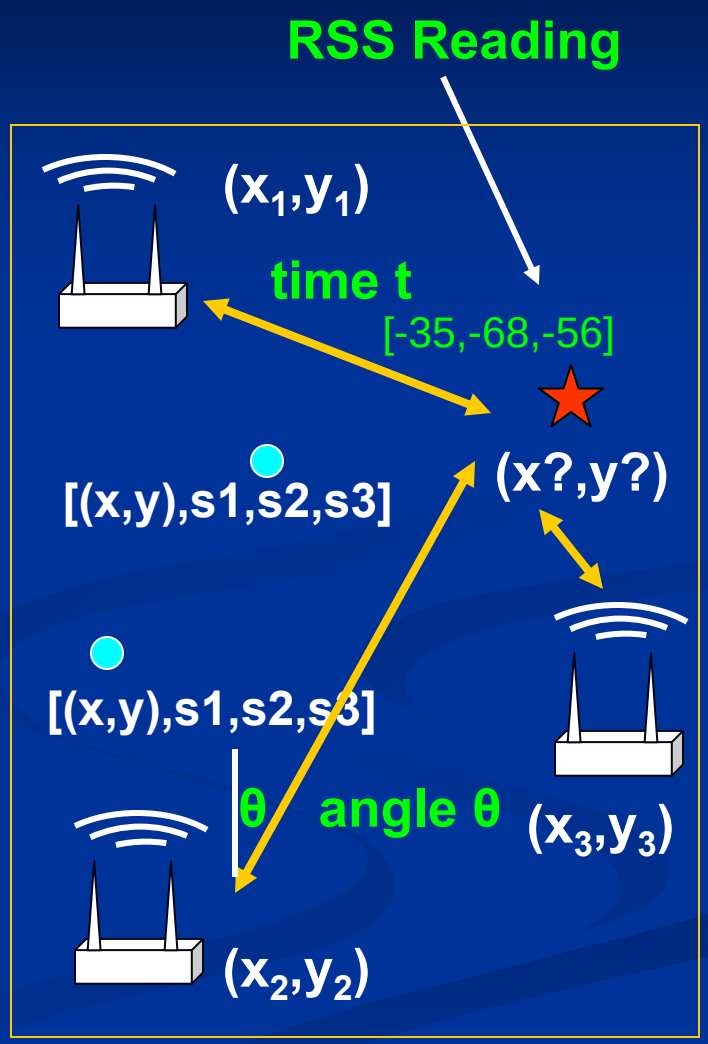
- Attention is on Received Signal Strength (RSS)-based localization techniques
  - Reuse the existing communication infrastructure
  - Tremendous cost saving
  - 802.11, 802.15.4, and Bluetooth support the technology
  - Reasonable accuracy (median error 1 ~ 5 m)
- The localization infrastructure can become the target of malicious attacks
  - Location-based services becoming more prevalent
  - Non-conventional security threats (non-cryptographic attacks)

Outline

- Introduction and motivation
- Background
- A generalized attack detection model
- Common features in RSS-based methods
- Test statistic in multilateration methods
- Experimental evaluation
- Conclusion
- Related work

Background

- Transmit packets at unknown location
- Landmarks Receive packets
- Or the other way around
- Modality
  - Received Signal Strength (RSS)
  - Time-Of-Arrival (TOA)
  - Angle-Of-Arrival (AOA)
- Principle to compute position
  - Lateration
  - Angulation
  - Scene (fingerprint) matching
    - Training data/radio map
  - Probabilistic
- Return location estimation



Generalized Attack Detection Model

- Formulate as statistical significance testing
  - Null hypothesis:
    - $\mathcal{H}_0$: normal (no attack)
- Test statistic $\mathbf{T}$
  - Acceptance region Ω
    - If $\mathbf{T}^{\mathbf{obs}} \in \Omega$, no attack
    - If $\mathbf{T}^{\mathbf{obs}} \notin \Omega$, declare an attack is present
- Significance testing with significance level α

Effectiveness of Attack Detection

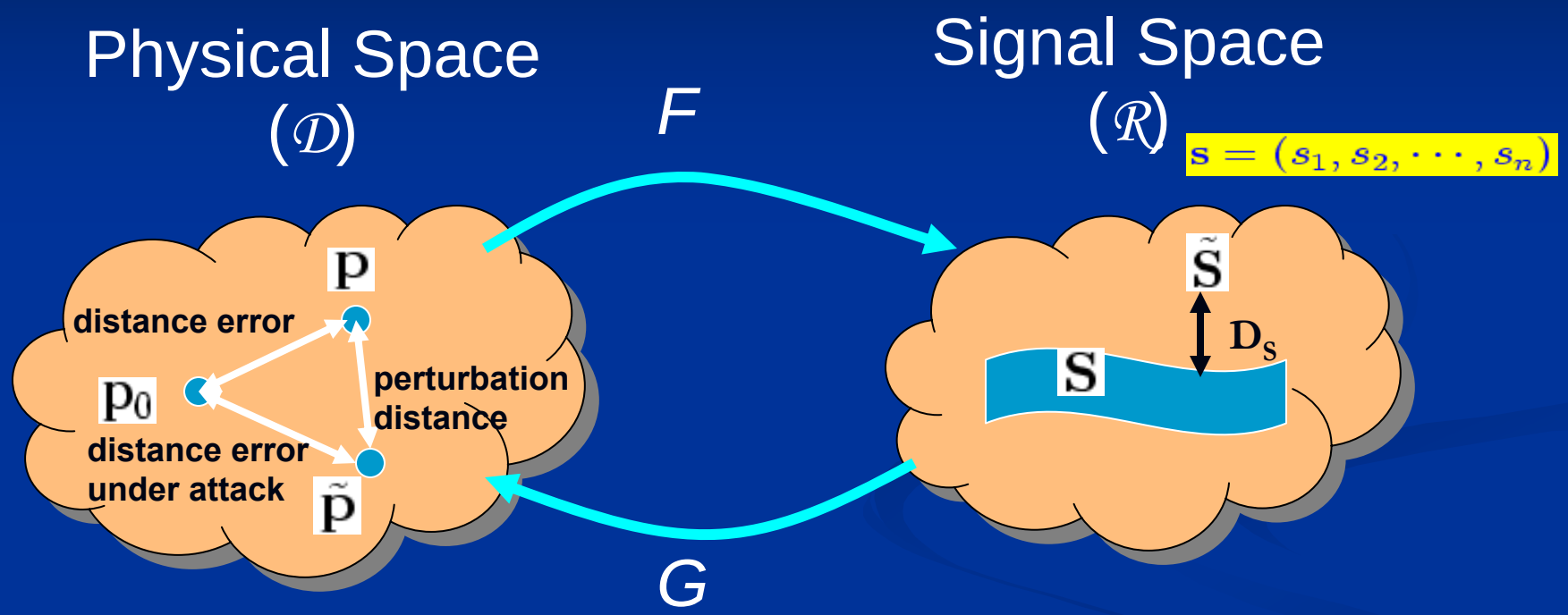
- Cumulative Distribution Function (CDF) of the test statistic $\mathbf{T}$
- Detection Rate (DR) $DR = \frac{N_{attack}}{N_{total}}$
  - Under attack, $DR = P_d$
  - Under normal, $DR = P_{fa}$
- Receiving Operating Characteristic (ROC) curve
  - Plot of attack detection accuracy against the false positive rate
  - Measure the tradeoff between the false-positive and correct detections

Choosing a Test Statistic

- Signal-strength based algorithms – range-based and scene matching
  - Common feature: distance in signal space
  - Area based Probability (ABP)
    - Bayes' rule to compute the likelihood of an RSS matching a fingerprint for each area
  - Bayesian Networks (BN)
    - Use Bayesian Graphical Model to predict the sampling distribution of the possible location
- Multilateration methods – single and multi-hop range-based
  - Non-linear Least Squares (NLS)
  - Linear Least Squares (LLS)

Test Statistic: Distance in Signal Space

Key advantage - attack detection before localization



$\mathbf{p}_0$ true location

$\mathbf{p}$ estimation under normal

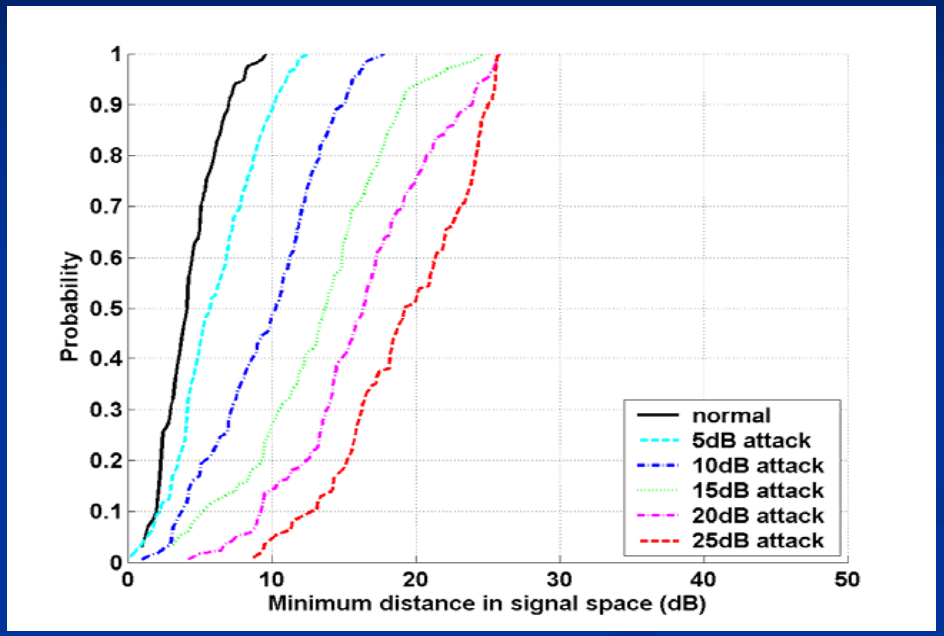
$\tilde{\mathbf{p}}$ estimation under attack

Localization:

$$\mathbf{p} = G_{alg}(\mathbf{s})$$

$$\tilde{\mathbf{p}} = G_{alg}(\tilde{\mathbf{s}})$$

Finding Thresholds



- D_S as a test statistic
- If $D_S > \tau$ for a given α, RSS readings under attack
- Choosing a threshold (τ):
  - empirical methodology vs. statistical modeling

Test Statistic for Multilateration Methods - Using Least Squares

- Ranging step:
  - Distance estimation between unknown node and landmarks
  - Various methods available: RSS, TOA, hop count
- Lateration step:
  - Traditional: Non-linear Least squares (NLS)

$$(\hat{x}, \hat{y}) = arg \min_{x,y} \sum_{i=1}^{N} [\sqrt{(x_i - x)^2 + (y_i - y)^2} - d_i]^2$$

  - Linear Least squares (LLS)

$$\mathbf{Ax} = \mathbf{b}$$

$$\mathbf{x} = (\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T\mathbf{b}$$

Test Statistic: The Residuals

- Localization with LLS
  - Linear regression: $\mathbf{b} = \mathbf{A}\mathbf{x} + \mathbf{e}$
  - Location estimation: $\hat{\mathbf{x}} = (\mathbf{A}^T A)^{-1}\mathbf{A}^T\mathbf{b}$
- Define the residuals

  $\hat{\mathbf{e}} = \mathbf{b} - \hat{\mathbf{b}} = [1 - \mathbf{A}(\mathbf{A}^T A)^{-1}\mathbf{A}^T]\mathbf{b}$
- Follow a Gaussian distribution: ~N(μ, Σ)
- Choose the residuals as the test statistic $\mathbf{T}$ for attack detection

The Detection Scheme

- Perform after the localization phase
- An observed value: $\hat{\mathbf{e}}^{\mathbf{obs}}$
- Model the residuals as multivariate Gaussian random variables:

$$f(\hat{\mathbf{e}}) = \frac{1}{(\sqrt{2\pi})^n |\Sigma|^{\frac{1}{2}}} e^{-\frac{1}{2}(\hat{\mathbf{e}}-\mu)^{\mathbf{T}} \boldsymbol{\Sigma}^{-\mathbf{1}} (\hat{\mathbf{e}}-\mu)}$$

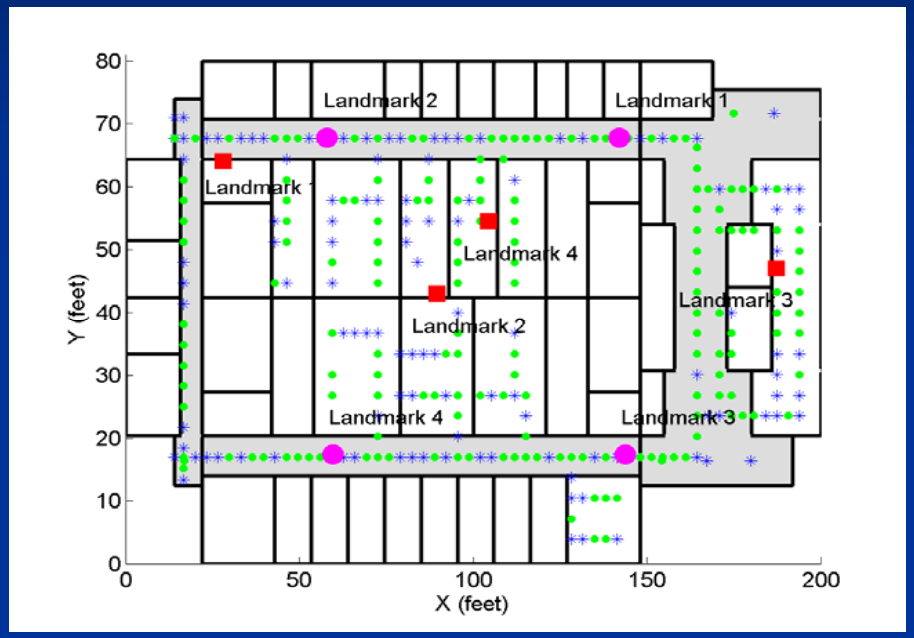
- Acceptance Region:

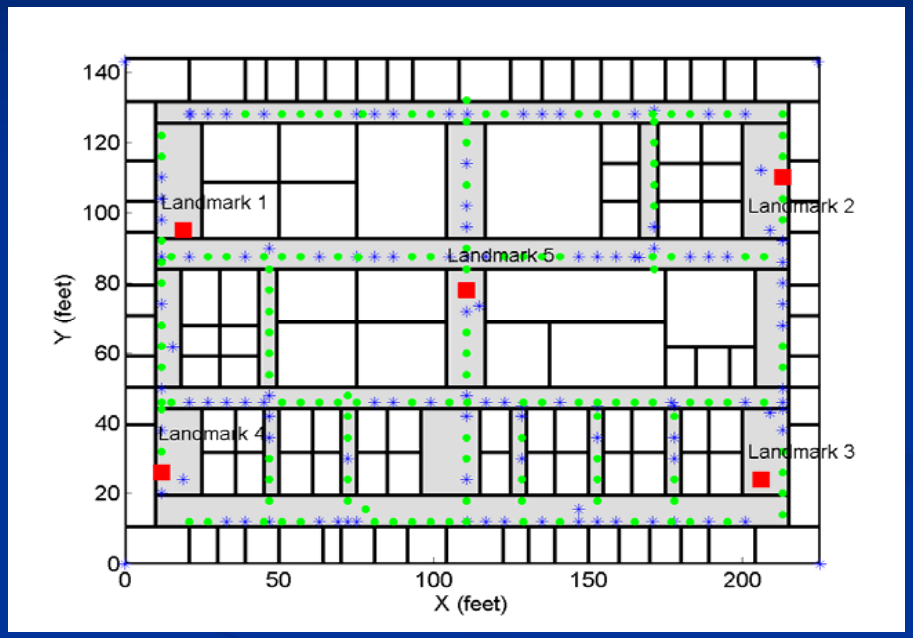
$$\Omega = \{\hat{\mathrm{e}} : Pr(\{\mathrm{T} : (\mathrm{T}-\mu)^T \Sigma^{-1} (\mathrm{T}-\mu) > (\hat{\mathrm{e}}-\mu)^T \Sigma^{-1} (\hat{\mathrm{e}}-\mu)\}) > \alpha\}.$$

- Under attack, if $P = 1 - M < \alpha$ (significance level)

$$\mathbf{M} = \frac{\Gamma(\mathbf{n}/2, \mathbf{X}/2)}{\Gamma(\mathbf{n}/2)}$$

Experimental Setup:
(Two buildings: CoRE Building and Industrial Lab)



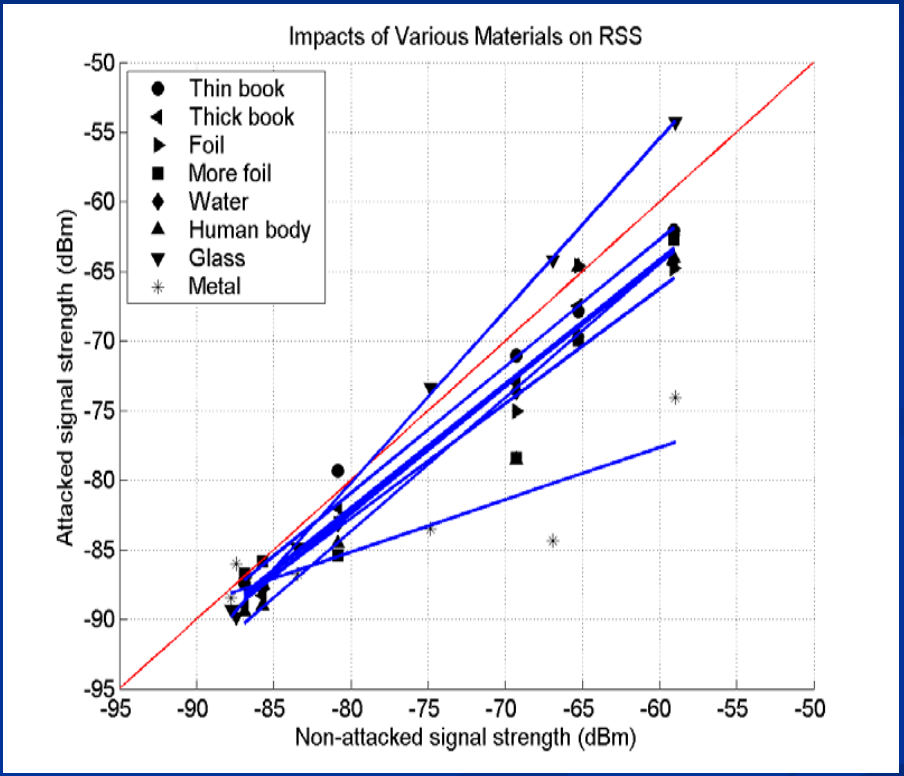


- Floor plan: 200ft x 80ft (16000 ft^2)
- 802.11 (WiFi) Network
- 802.15.4 (ZigBee) Network

- Floor plan: 225ft x 144ft (32400 ft^2)
- 802.11 (WiFi) Network

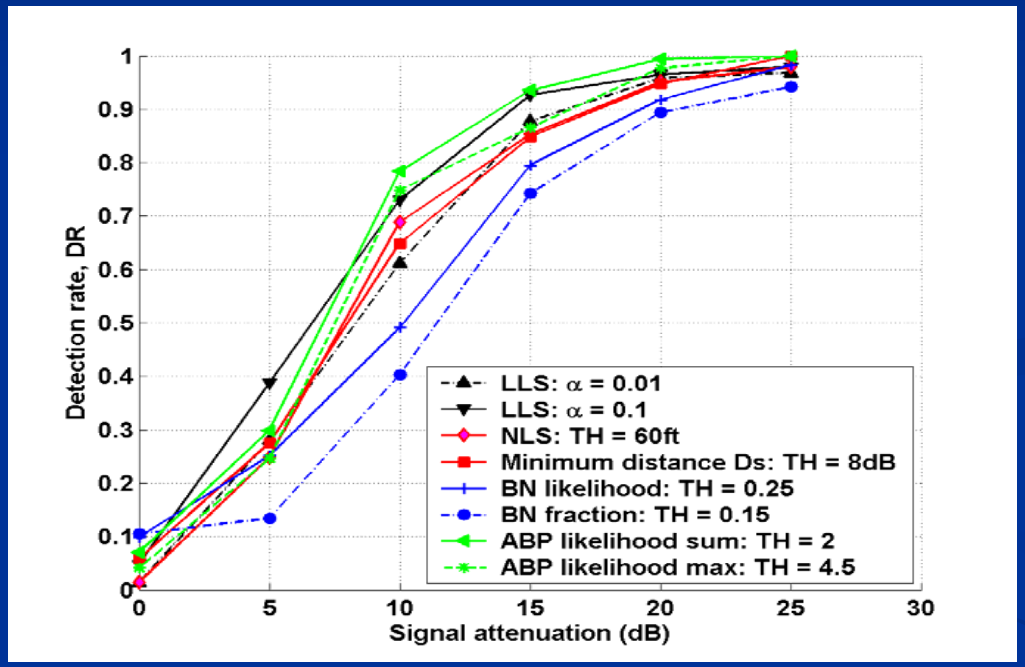
Experimental Evaluation
- Using Signal Strength Attacks

- Attenuate or amplify RSS
- Materials – easy to access
- Attacks – simple to perform with low cost
  - Attack the wireless node
  - Compromise the landmarks
- Linear relationship - linear attack model



Comparison

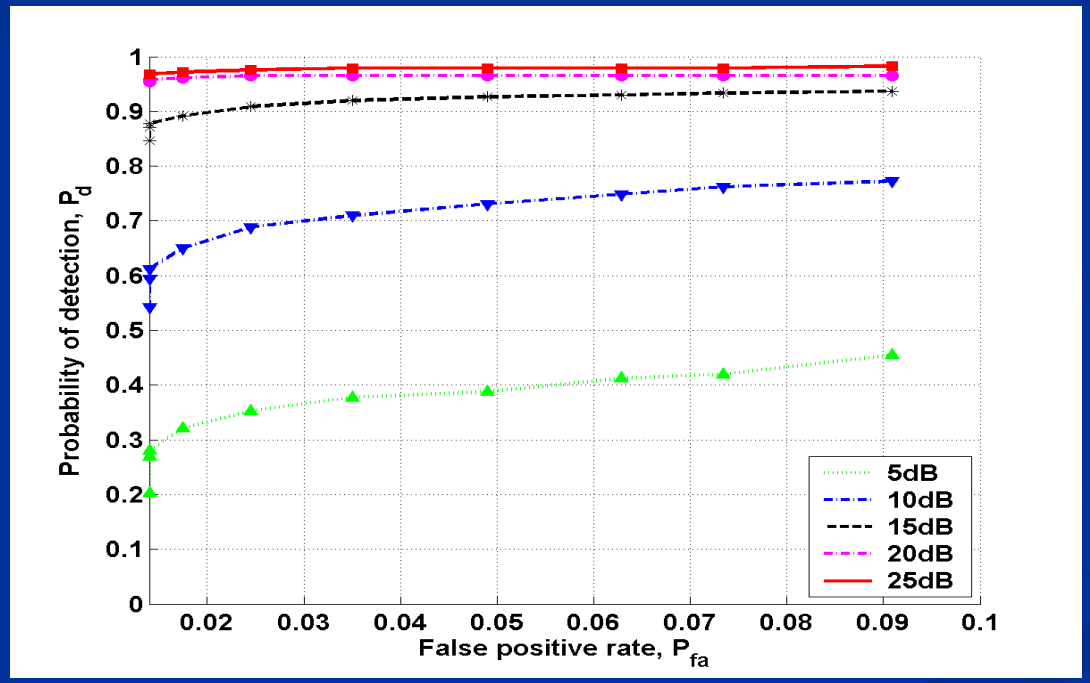
Statistical Significance Testing: generic and specific test statistics



Performance: similar detection rates!

Receiving Operating Characteristic (ROC) - Using LLS Residuals

A closer look: CoRE, 802.11 network, $\alpha = 0.01$



Impact of small attacks: ~ 1.55 ft/dB

Summary

- Generic approach
  - Across algorithms, networks, and buildings
- Effectiveness of our attack detection schemes
  - High detection rates, over 95% (attacks > 15dB)
  - Low false positive rates, below 5%
- Different localization systems have similar attack detection capabilities

Related Work

- Cryptographic threats
  - Use traditional security services - authentication [Bohge WiSe 2003, Wu IPDPS 2005, Zhu MWN 2003]
- Non-cryptographic threats
  - Distance bounding protocols [Brands 1994, Sastry 2003]
  - Verifiable multilateration mechanisms [Capkun Infocom 2005]
  - Hidden and mobile base stations [Capkun Infocom 2006]
  - Directional antennas and distance bounding [Lazos IPSN 2005]
  - Eliminate attack efforts using data redundancy or neighbor information [Li IPSN 2005, Liu IPSN 2005, Liu ICDCS 2005, Du IPDPS 2005]

Thank you

&

Questions