Securing Wireless Localization: Living with Bad Guys

Zang Li, Yanyong Zhang, Wade Trappe

Badri Nath

WINLAB
WIRELESS INFORMATION NETWORK LABORATORY

Talk Overview

- Wireless Localization Background
- Attacks on Wireless Localization
  - Time of Flight
  - Signal Strength
  - Angle of Arrival
  - Region Inclusion
  - Hop Count
  - Neighbor Location
- Coping with Localization Threats
  - Multimodal Localization Strategies
  - Robust Statistics
- Conclusions and Future Directions

What is Localization?

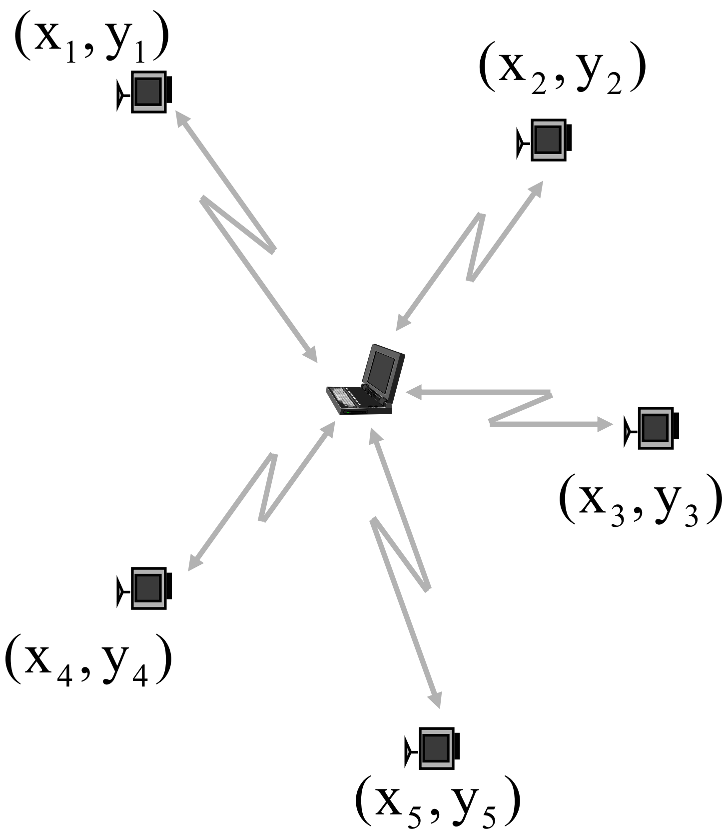
- Localization is important for facilitating location-based services
- **Goal:** Determine the location of one or more wireless devices based on some form of measurements
- Useful measurements:
  - Time of flight (TOA)
  - Time difference of flight (TdOA)
  - Energy of flight (DoA based on Signal Strength)
  - Phase of flight (AoA = Angle of arrival from fixed stations)
  - Perspective of flight (Visual Cues)
  - Hop count to anchors: Correlated with distance
  - Neighbor Location: Find regions
- Examples…

Use Neighbor Locations: Centroids

- Scenario:
  - A set of anchor nodes with known locations are deployed as infrastructure for localization
- Wireless devices localize by calculating the centroid of the anchor points they hear:

$$(\hat{x}, \hat{y}) = \left(\frac{x_1 + x_2 + \cdots + x_n}{n}, \frac{y_1 + y_2 + \cdots + y_n}{n} \right)$$

- Refine by averaging the values of the other nodes within the signal range

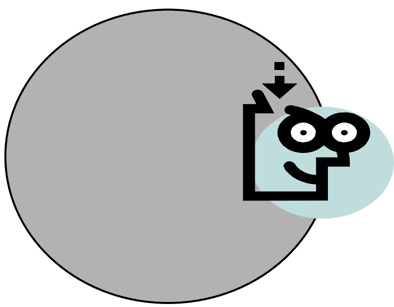


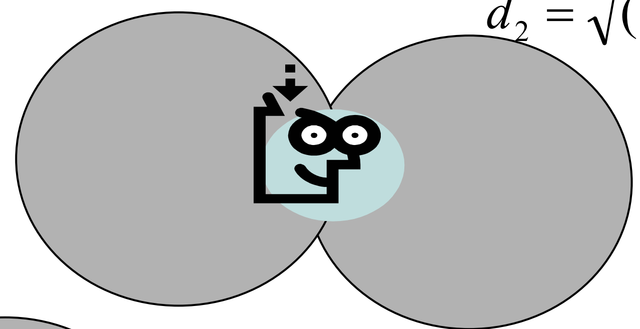
WINLAB
WIRELESS INFORMATION NETWORK LABORATORY

Time of Flight (S=R) Localization

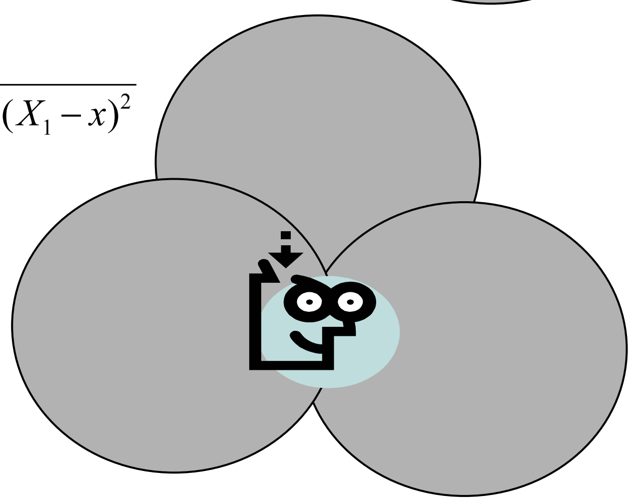
- Send a signal to receiver and back
- Measure RTT, know velocity of propagation
- Calculate Distance -

$$d_1 = \sqrt{(Y_1 - y)^2 + (X_1 - x)^2}$$
$$d_2 = \sqrt{(Y_2 - y)^2 + (X_2 - x)^2}$$





$$d_1 = c(rtt) = \sqrt{(Y_1 - y)^2 + (X_1 - x)^2}$$



$$d_1 = \sqrt{(Y_1 - y)^2 + (X_1 - x)^2}$$
$$d_2 = \sqrt{(Y_2 - y)^2 + (X_2 - x)^2}$$
$$d_3 = \sqrt{(Y_3 - y)^2 + (X_3 - x)^2}$$

Lateration

- very
- common
- local
- triangulation
- solve [Ax=b]

Signal Strength

- Underlying Principle: Signal strength (RSSI) is a function of distance
  - Free Space Propagation Model

$$P_r = P_t \left[\frac{\sqrt{G_l}\lambda}{4\pi d} \right]^2$$

  - Two-Path (Single Ground Reflection Model)

$$P_r = P_t \left[\frac{\sqrt{G_l} h_t h_r}{d^2} \right]^2$$

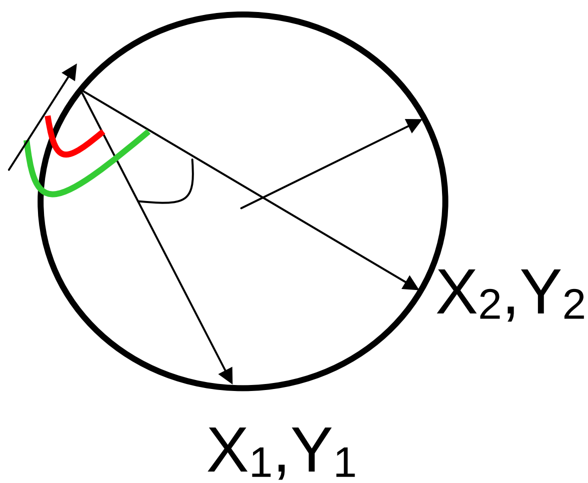
  - Generalized Path Loss Model

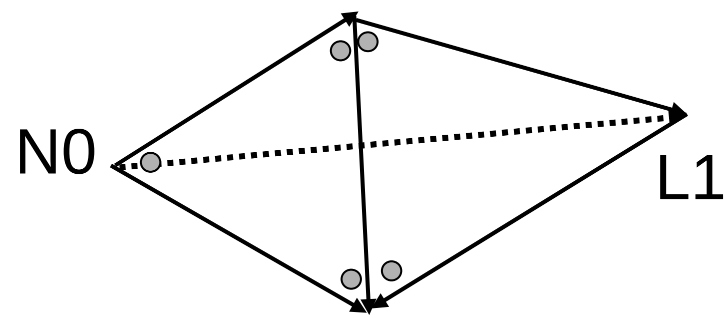
$$P_r = P_t K \left[\frac{d_0}{d} \right]^\gamma$$

- Use known landmark locations and RSSI-Distance relationship to setup a least squares problem

Angle of Arrival Localization

- One can determine an orientation w.r.t a reference direction
- Angle of Arrival (AoA) from two different points and their distances
- You can locate a point on a circle. Similar AoA from another point gives you three points. Then triangulate to get a position





a/sinA=b/sinB=c/sinC

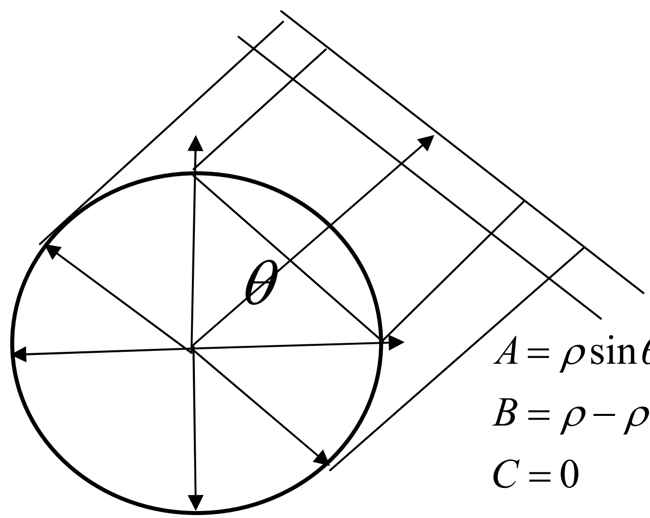
"Ad Hoc Positioning System (APS) Using AOA", D. Niculescu and B. Nath, Infocom 2003

AoA capable nodes

- Cricket Compass (MIT Mobicom 2000)
  - Uses 5 ultra sound receivers
  - 0.8 cm each
  - A few centimeters across
  - Uses tdoa (time difference of arrival)
  - +/- 10% accuracy
- Medusa sensor node (UCLA node)
  - Mani Srivatsava et.al
- Antenna Arrays

AoA Using Visual Cues

- Color cylinder
- Determine proportion of colors



$$A = \rho\sin\theta + \rho\cos\theta$$
$$B = \rho - \rho\cos\theta$$
$$C = 0$$
$$D = \rho - \rho\sin\theta$$

Taking the ratios A/D and A/B and solving for theta

$$\sin\theta = (A + B - D)/(A + B + D)$$
$$\cos\theta = (A - B + D)/(A + B + D)$$
$$\theta = \arctan((A + B - D)/(A - B + D))$$

“Mobile robot localization by remote viewing of color cylinder”, Volpe et al In IROS Aug 1995

Attacks on Localization

- Most security and privacy issues for wireless networks are best addressed through cryptography and network security
- **End of Day Analysis:** Not all security issues can be addressed by cryptography!
- Non-cryptographic attacks on wireless localization:
  - Adversaries may affect the measurements used to conduct localization
  - Adversaries may physically pick up and move devices
  - Adversaries may alter the physical medium (adjust propagation speed, introduce smoke, etc.)
  - Many, many more **crazy** attacks…
- New Field: Securing Wireless Localization
  - "Secure Verification of Location Claims," Sastry and Wagner
  - "Secure Positioning in Sensor Networks," S. Capkun and J.P. Hubaux
  - "SeRLoc: Secure range-independent localization for wireless networks," L. Lazos and R. Poovendran
  - "Securing Wireless Localization: Living with Bad Guys," Z. Li, Y. Zhang, W. Trappe and B. Nath (expanded version under submission)

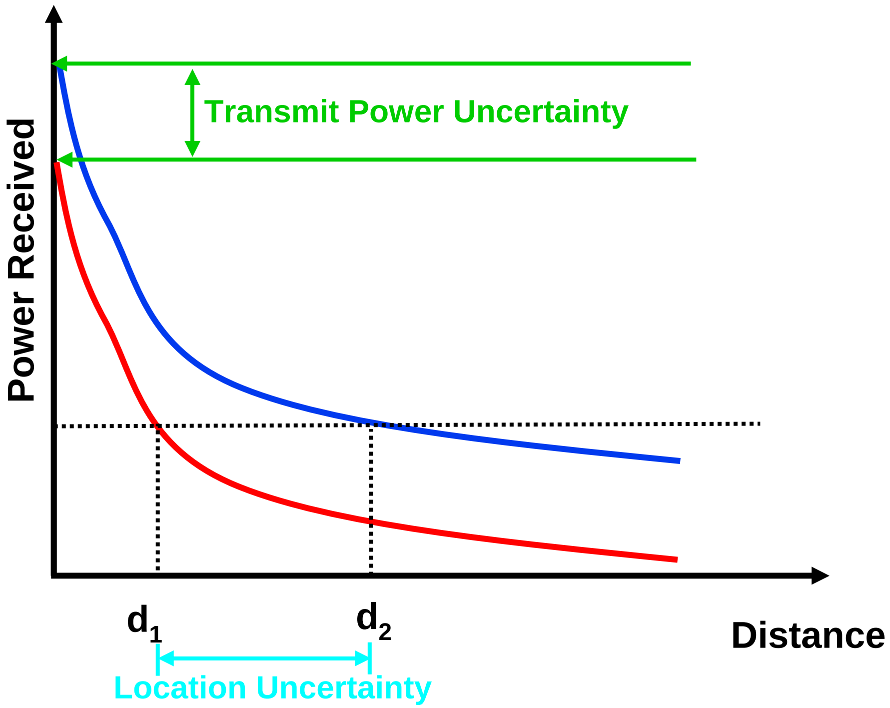
Possible Attacks vs. Localization Algorithms

Property	Example Algorithms	Attack Threats
Time of Flight	Cricket	➢ Remove direct path and force radio transmission to employ a multipath; ➢ Delay transmission of a response message; ➢ Exploit difference in propagation speeds (speedup attack, transmission through a different medium).
Signal Strength	RADAR, SpotON, Nibble	➢ Remove direct path and force radio transmission to employ a multipath; ➢ Introduce different microwave or acoustic propagation loss model; ➢ Transmit at a different power than specified by protocol; ➢ Locally elevate ambient channel noise
Region Inclusion	APIT, SerLoc	➢ Enlarge neighborhood by wormholes; ➢ Manipulate the one-hop distance measurements; ➢ Alter neighborhood by jamming along certain directions

Property	Example Algorithms	Attack Threats
Angle of Arrival	APS	➢ Remove direct path and force radio transmission to employ a multipath; ➢ Change the signal arrival angel by using reflective objects, e.g., mirrors; ➢ Alter clockwise/counter-clockwise orientation of receiver (up-down attack)
Hop Count	DV-Hop	➢ Shorten the routing path between two nodes through wormholes; ➢ Lengthen the routing path between two nodes by jamming; ➢ Alter the hop count by manipulating the radio range; ➢ Vary per-hop distance by physically removing/displacing nodes
Neighbor Location	Centroid, SerLoc	➢ Shrink radio region (jamming); Enlarge radio region (transmit at higher power, wormhole); ➢ Replay; Modify the message; Physically move locators; ➢ Change antenna receive pattern

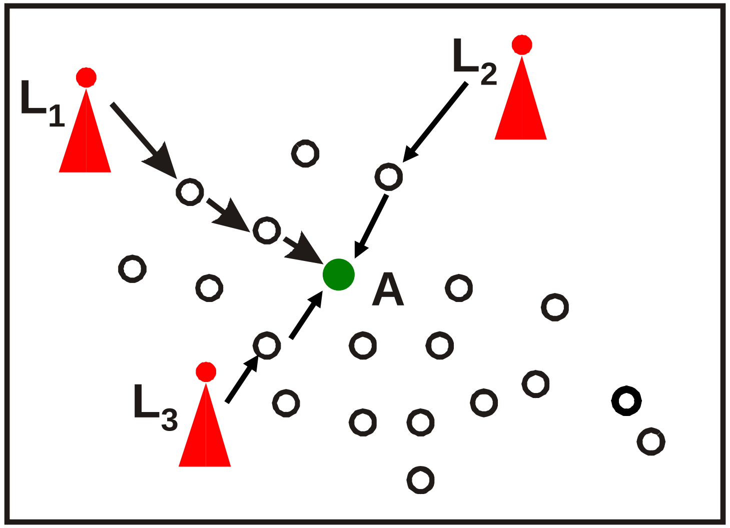
Signal Strength Attack on Localization

- Signal strength wireless localization are susceptible to power-distance uncertainty relationships
- Adversary may:
  - Alter transmit power of nodes
  - Remove direct path by introducing obstacles
  - Introduce absorbing or attenuating material
  - Introduce ambient channel noise



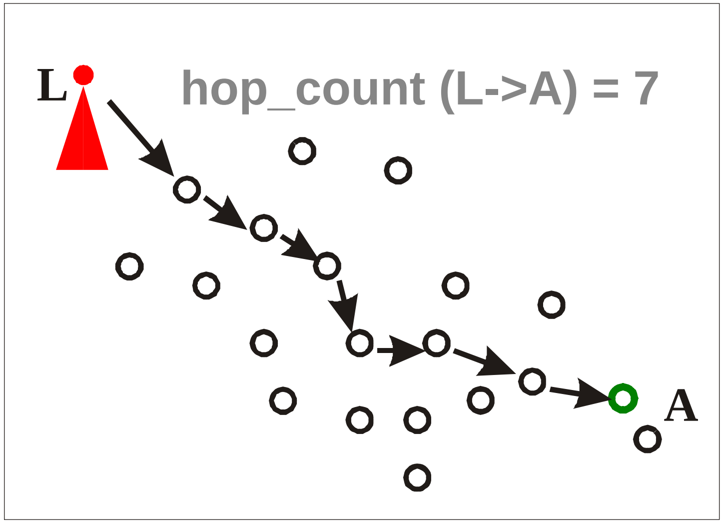
Attacks on Hop-Count Methods

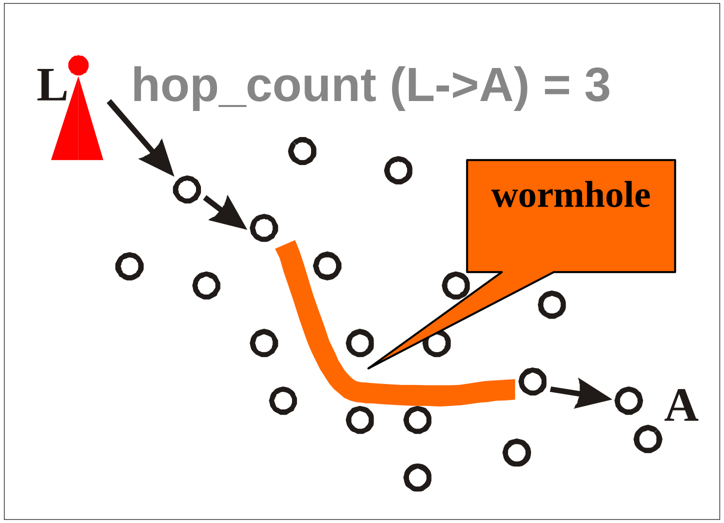
- DV-hop localization algorithm:
- Obtain the hop counts between a sensor node and several locators.
- Translate hop counts to actual distance.
- Localize using triangulation.

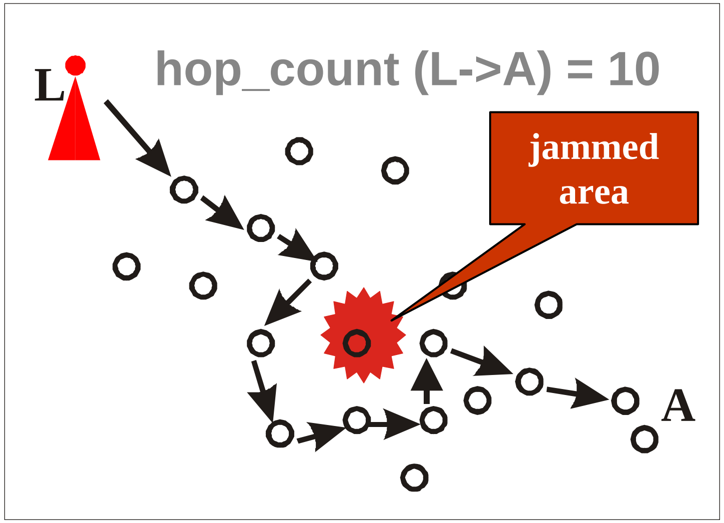


It is critical to obtain the correct hop counts between sensor nodes and every locator.

Attacks on Hop-Count Methods, pg. 2





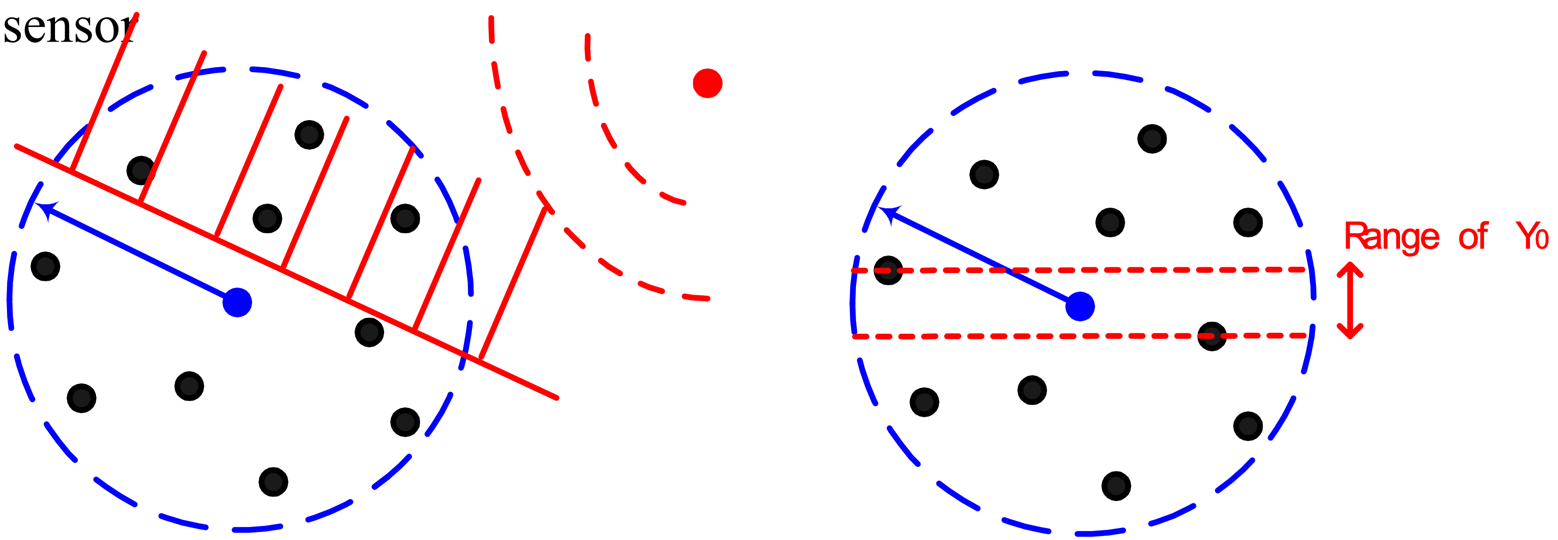


Defenses for Wireless Localization

- **Multimodal Localization:**
  - Most localization techniques employ a single property
  - Adversary only has to attack one-dimension!!!
  - **Defense Strategy:** Make the adversary have to attack several properties simultaneously
  - Example: Do signal strength measurements correspond to TOF measurements?
- **Robust Statistical Methods:**
  - **Defense Strategy:** Ignore the wrong values introduced by adversaries
  - Develop robust statistical estimation algorithms and data cleansing methods
  - Interesting behavior: Its best for the adversary not to be too aggressive!

Multimodal Techniques

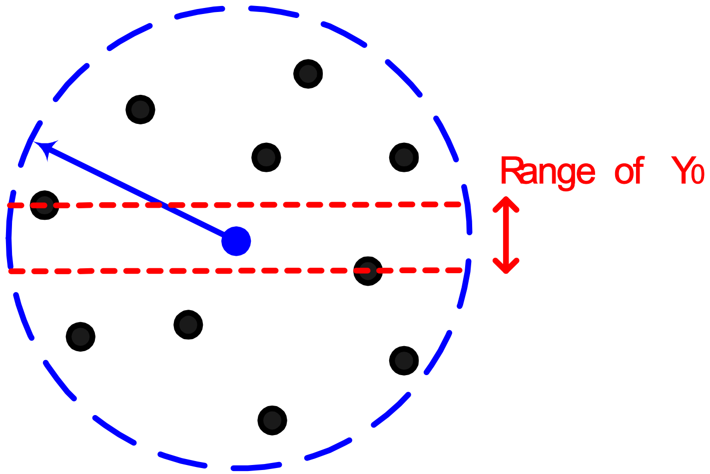
- Multimodal localization strategies: exploiting several properties simultaneously to corroborate each other and improve robustness
- Example: Centroid
  - **Attacks**: generally involve modifying neighboring list
  - **Defense**: use both neighbor location and a two-sector antenna on each sensor



$$\hat{x}_0 = \frac{1}{N}\sum_{i=1}^{N} x_i, \quad \hat{y}_0 = \frac{1}{N}\sum_{i=1}^{N} y_i$$

Multimodal Technique

- Only the neighbors that are closest to the sensor in the x-coordinate or y-coordinate will affect the estimation
- Robust to wrong neighbor information
- Neighbor coordinates rule: the neighbors in the upper sector have larger Y coordinates than the neighbors in lower sector
  - Ensure correct orientation
  - Detect existence of attacks



WINLAB
WIRELESS INFORMATION NETWORK LABORATORY

Robust: Localization with Anchor Nodes

- Anchor nodes have their positions $\{(x, y)\}$ known
- Distances to anchor nodes d are estimated through DV-hop or signal strength or other distance estimation methods
- $\{(x, y, d)\}$ values map out a parabolic surface $d(x, y)$ whose minimum value (x_0, y_0) is the wireless device location
- Least squares (LS) algorithm can be used to find $(\hat{x}_0, \hat{y}_0)$

$$(\hat{x}_0, \hat{y}_0) = \arg\min_{(x_0, y_0)} \sum_{i=1}^{N} \left(\sqrt{(x_i - x_0)^2 + (y_i - y_0)^2} - d_i\right)^2$$

WINLAB
WIRELESS INFORMATION NETWORK LABORATORY

What if Attacks Exist?

- Adversary can alter the distance measurement through wormholes or jamming attacks
- One significant deviation of distance measurement may drive the location estimation far from the true value
- The fundamental reason for this vulnerability to attacks is that

Least squares algorithm is not robust to outliers!

- The misinformation produced by the adversary are outliers in the location estimation problem
- Redundancy within network can be exploited to combat attacks

Robust Statistics

- Least median squares (LMS) algorithm

$$(\hat{x}_0, \hat{y}_0) = \arg\min_{(x_0, y_0)} \operatorname{med}\left(\sqrt{(x_i - x_0)^2 + (y_i - y_0)^2} - d_i\right)^2$$

- Proposed by Rousseeuw
- With a robust cost function, a small fraction of outliers won't affect the cost function significantly
- In the absence of noise, LMS algorithm can tolerate up to 50 percent outliers
- Exact calculation of LMS solution is computational expensive

Least Median Squares Algorithm

- Solve random subsets of $\{(x_i, y_i, d_i)\}$ values to get several candidate $(\hat{x}_0, \hat{y}_0)$
- Choose the candidate with the least median residue squares
- Identify the inliers and outliers according to the least median squares subset estimate

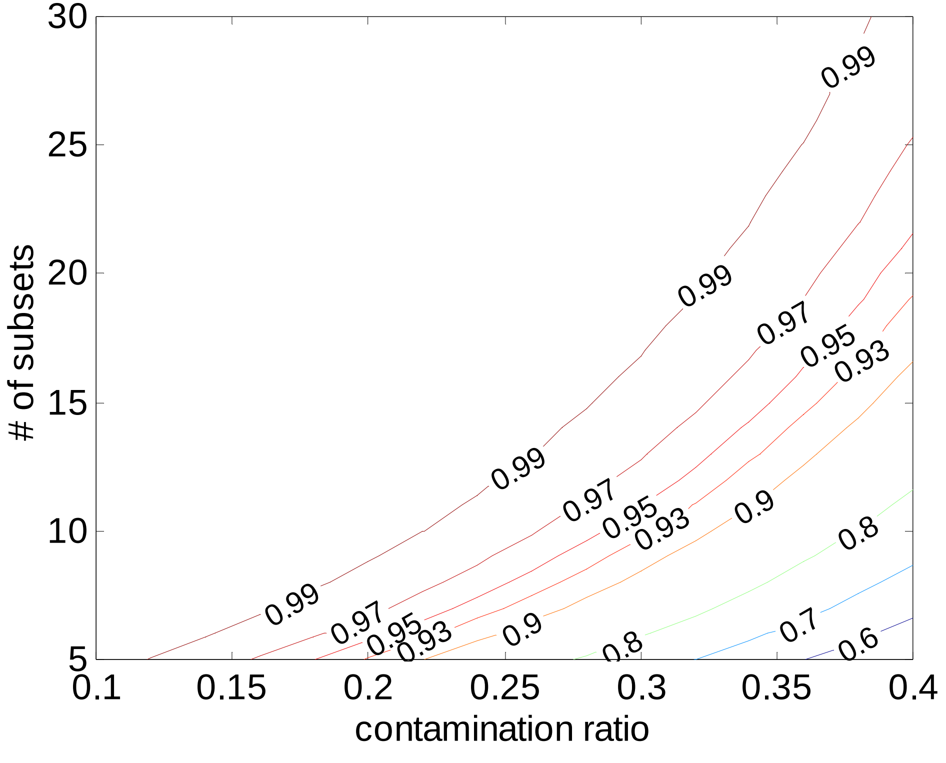
$$s_0 = 1.4826\left(1 + \frac{5}{N - p}\right)\sqrt{\text{med } r_i^2} \qquad w_i = \begin{cases} 1, & |r_i / s_0| > \gamma \\ 0, & otherwise \end{cases}$$

- Do a reweighted least squares algorithm to get the final estimate $(\hat{x}_0, \hat{y}_0)$

Robust Localization with LMS

- How to choose M, the number of subsets and n, the size of a subset?
  - Hopefully, at least one subset among all subsets does not contain any contaminated sample

$$P = 1 - (1 - (1 - \varepsilon)^{n})^{M}$$



- In our simulation:
  - ✓ n = 4
  - ✓ M=20

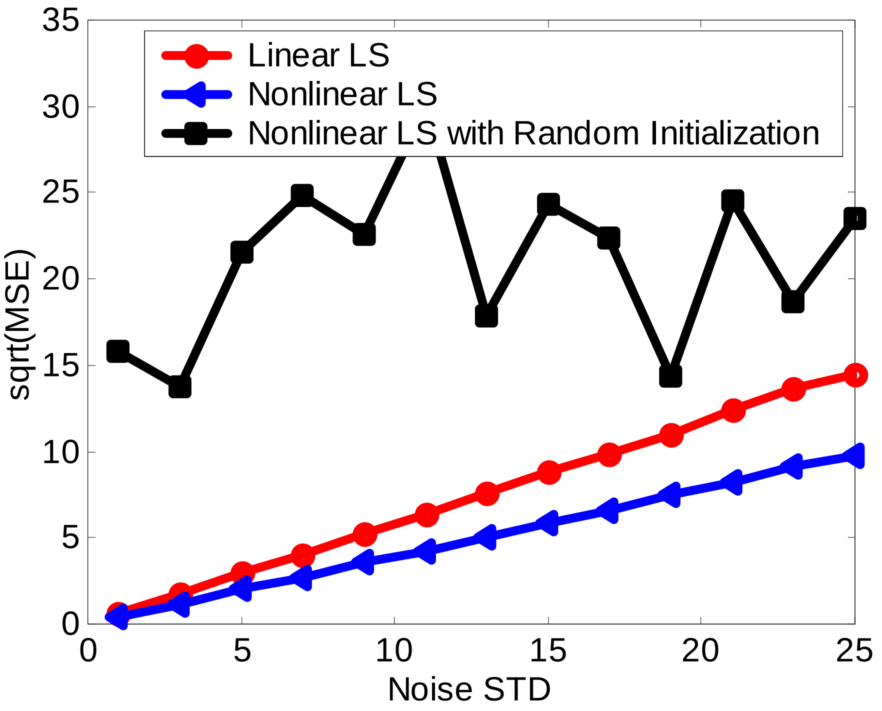
Robust Localization with LMS (ctd.)

- How to estimate the location from the samples with reduced computation?
  - Linearization: suboptimal, but less complexity

$$(x_1 - x_0)^2 + (y_1 - y_0)^2 = d_1^{\,2}$$
$$\vdots$$
$$(x_N - x_0)^2 + (y_N - y_0)^2 = d_N^{\,2}$$

$$\Downarrow$$

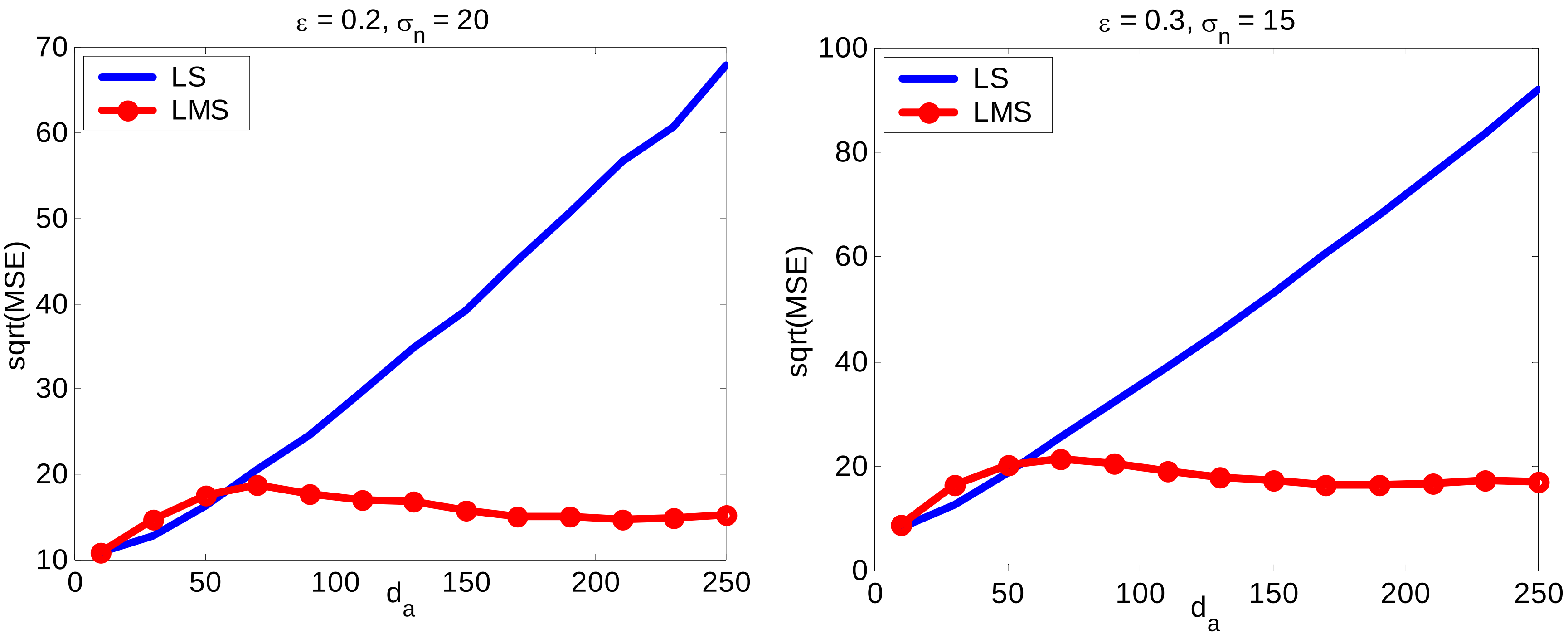
$$\frac{1}{N}\sum_{i=1}^{N}[(x_i - x_0)^2 + (y_i - y_0)^2] = \frac{1}{N}\sum_{i=1}^{N} d_i^{\,2}$$



Attack Model

- The adversary successfully gains the power to arbitrarily modify the distance measurements to a fraction ε of the total anchor nodes
- The contamination ratio $\varepsilon \leq 0.5$
- The adversary coordinates the tampering of measurements so that they will push the estimate toward the same wrong location (x_a, y_a)
- d_a, distance between (x_a, y_a) and (x_0, y_0), is used to indicate the strength of the attack

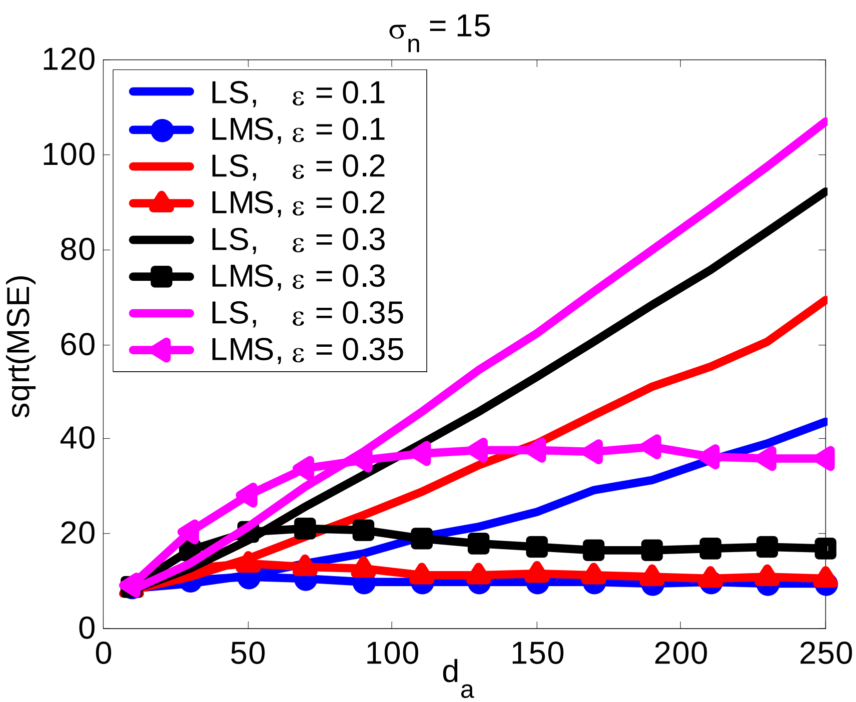
Performance of the LMS Algorithm

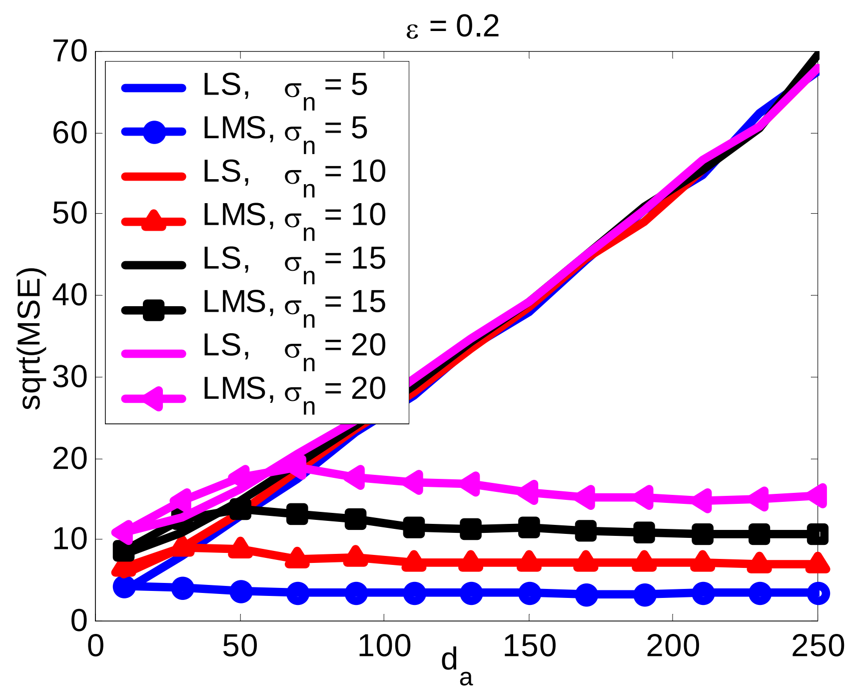


- MSE of LS algorithm increases as d_a increases
- MSE of LMS algorithm does not increase unboundedly with d_a

WINLAB
WIRELESS INFORMATION NETWORK LABORATORY

Performance of the LMS Algorithm (ctd.)



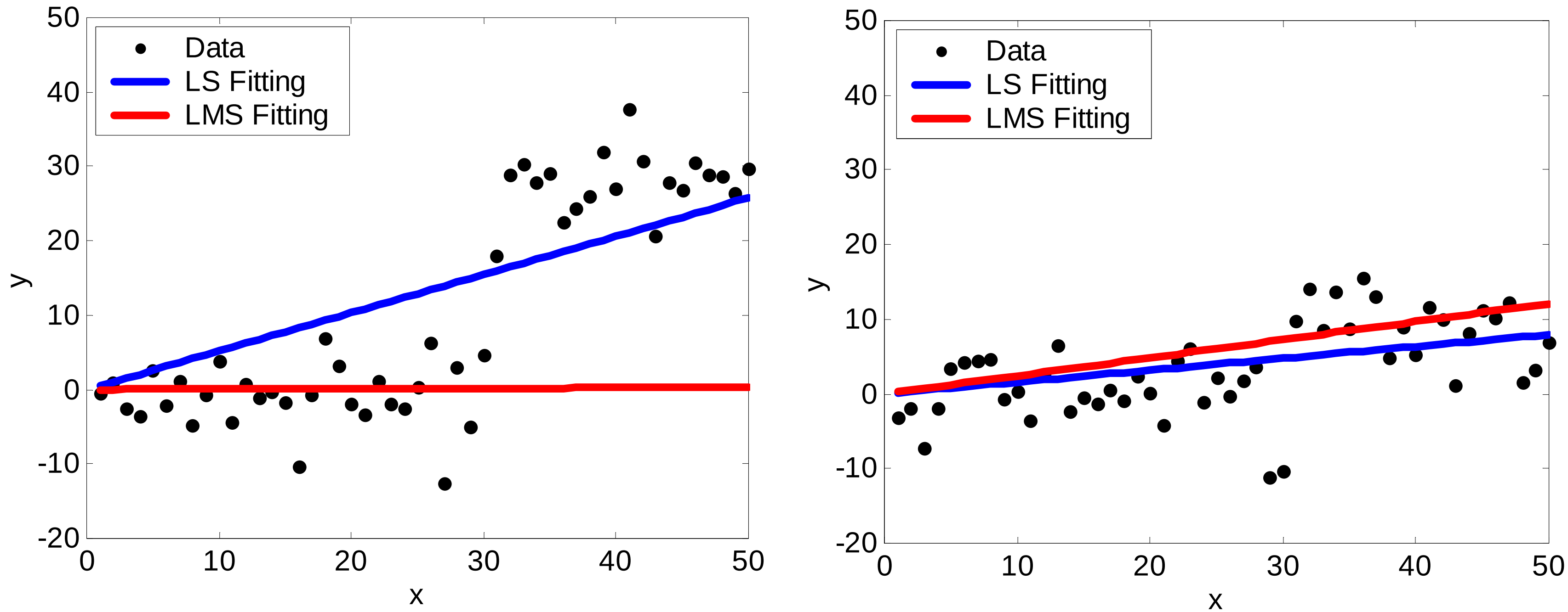


- The larger contamination ratio, the worse the performance
- The larger the measurement noise level, the worse the performance

WINLAB WIRELESS INFORMATION NETWORK LABORATORY

When to Use LMS?

- At small d_a, LS performs better than LMS at a lower computational cost



(Conceptual Figures)

When to Use LMS? (ctd.)

- Observation: the variance of the data with outliers is larger than that of the data without outliers
- Variance expansion indicates the attacking strength
- Estimate the variance in data using LS

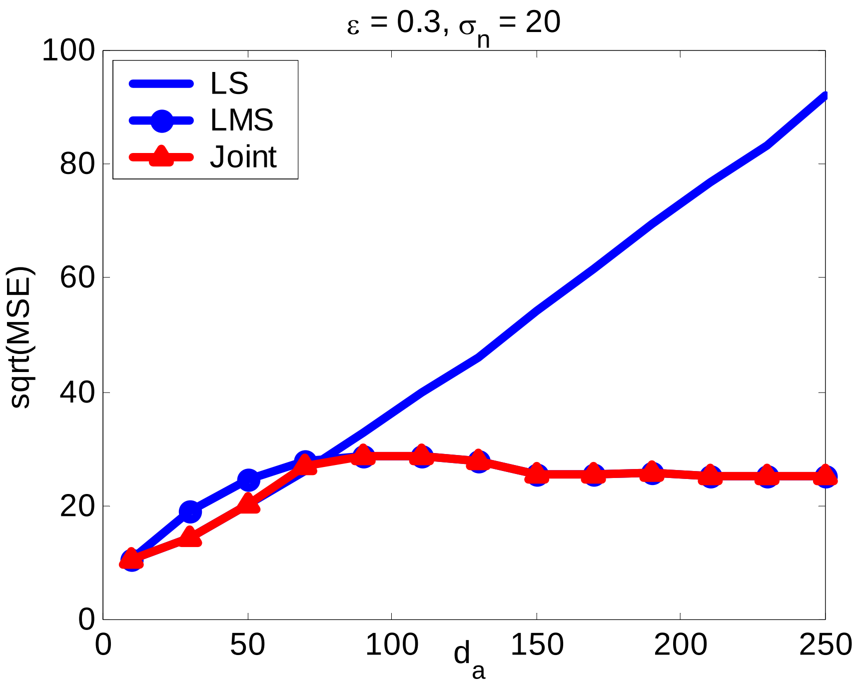
$$\hat{\sigma}_n = \sqrt{\frac{\sum r_i^2}{N-2}}$$

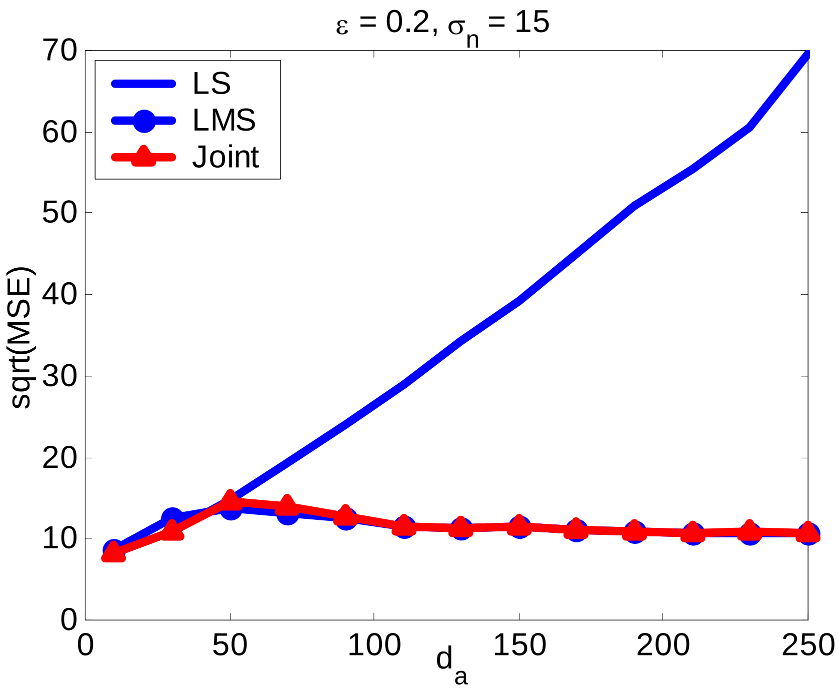
- Assume the actual measurement noise level σ_n is known
- Use LMS only when

$$\frac{\hat{\sigma}_n}{\sigma_n} > T$$

Performance of Joint LS and LMS Algorithm

- Empirically, T = 1.5 is a good choice across all (ε, σ_n) pairs





This improvement is achieved and we save computational complexity!!!

Conclusion and Remarks

- Wireless localization algorithms are important to future location-based services
- Several (non-cryptographic) attacks unique to wireless localization were identified
- We presented two strategies to cope with the effects of attacks on localization
  - Multimodal Localization
  - Robust Statistical Localization