SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks

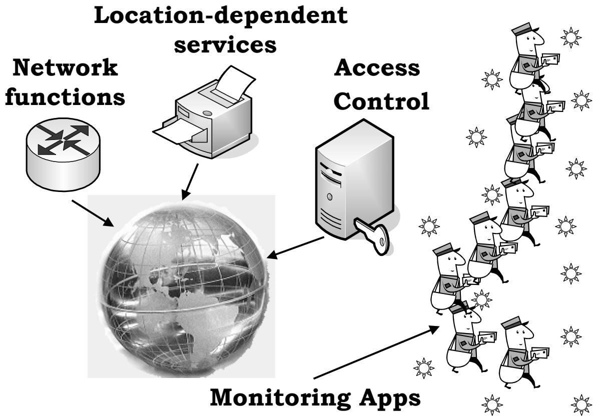
Loukas Lazos
Advisor: Radha Poovendran
Network Security Lab
University of Washington

Outline

- **Motivation**
- **Secure Localization Problem**
- **SeRLoc**
- **Threats and defenses**
- **Performance Evaluation**
- **Conclusions**

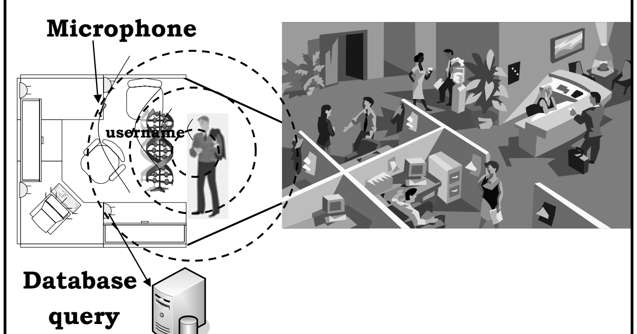
2

Why do we need location in WSN?



3

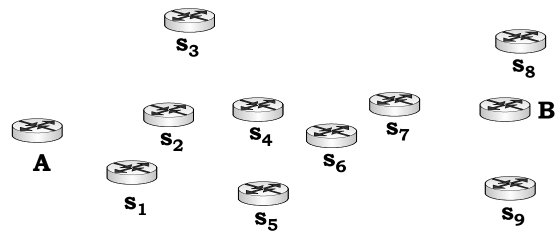
Location-based Access Control



Access is decided based on the location of the user. Different privileges for various areas

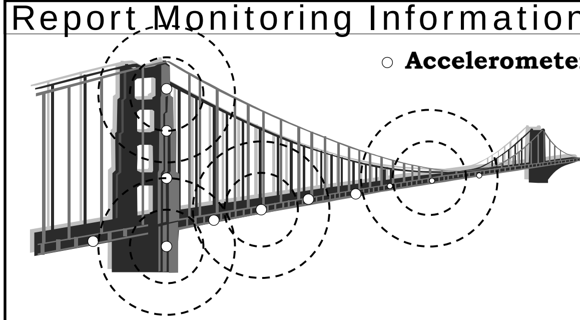
4

Geographical Routing



- A wants to send a message to B
- Each node forwards the message to the neighbor closest to the destination.

Report Monitoring Information



Monitor the structural health of the bridge

Sensors associate their location with the reporting data

Localization Problem

Localization: Sensor Location Estimation

- How do sensors become aware of their position when they are randomly deployed or mobile?
- Algorithm Design considerations
  - What type of localization is required?
    - Coarse or Fine Grain?
  - Where is the WSN deployed?
    - Indoors or Outdoors
  - What are the capabilities of the sensors?
    - Hardware and Power Constraints

Classification of Loc. Schemes

- Indoors vs. Outdoors:
  - GPS, VOR, Centroid (outdoors),
  - RADAR, Active Bat, AhLos, (indoors).
- Infrastructureless (I-L) vs. Infrastructure based (I-B):
  - AhLos, Amorphous, DV-Hop (I-L),
  - RADAR, Active Bat, AVL (I-B).
- Range-based (R-B) vs. Range-Independent (R-I):
  - Radar, Ahlos, GPS, Active Bat, VOR (R-B),
  - APIT, DV-Hop, Amorphous, Centroid (R-I).

Localization in un-trusted environment

- Previous schemes assumed trusted nodes and no external attacks, but
- WSN may be deployed in hostile environments
- Several threats in WSN localization:
  - Replay attacks,
  - Node Impersonation attacks,
  - Compromise of network entities.

9

Secure Localization Problem

- Secure Localization: Ensure robust location estimation even in the presence of adversaries.
- Related work:
  - An Asymmetric Security Mechanism for navigation signals [Kuhn 2004].
  - Secure Positioning of Wireless Devices with Application to Sensor Networks (SPINE) [Capkun et al, Infocom 2004].

10

Outline

- Motivation
- Problem Description
- SeRLoc
- Threats and defense
- Performance
- Conclusions

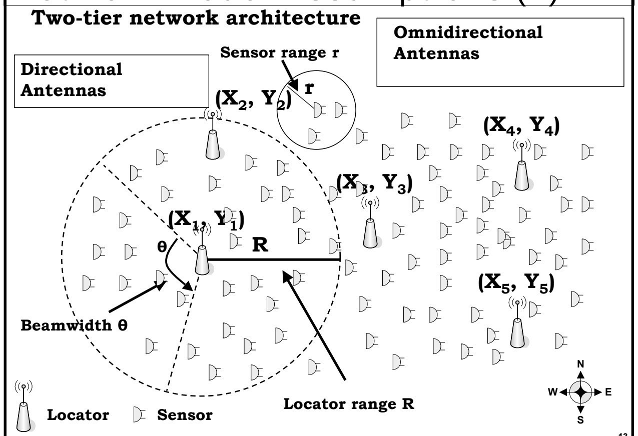
11

Our Approach: SeRLoc

- SeRLoc: SEcure Range-independent LOCalization
- SeRLoc features
  - Passive Localization,
  - Robust against sources of error,
  - Decentralized Implementation, Scalable.
  - Robust against attacks - Lightweight security.

12

Network Model Assumptions (1)



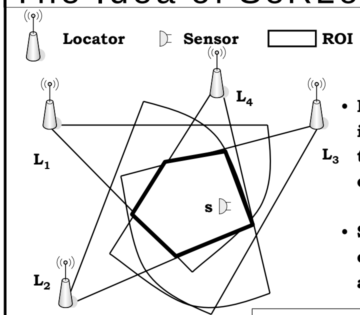
Network Model Assumptions (2)

- **Locator deployment: Homogeneous Poisson point process of rate ρ_L → Random spatial distribution.**
- **Sensor deployment: Poisson point process of rate ρ_s *independent* of locator deployment**
- **Or can be seen as Random sampling with rate ρ_s.**

$$P(LH_s = k) = \frac{(\rho_L \pi R^2)^k}{k!} e^{-\rho_L \pi R^2}$$

LH_s: Locators heard at a sensor s

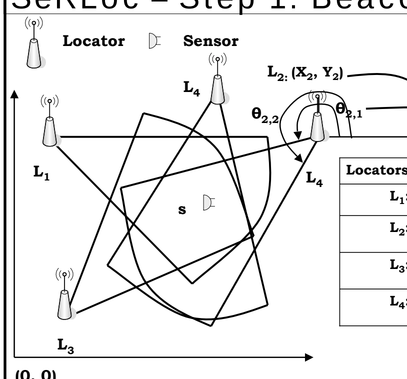
The Idea of SeRLoc



- **Each locator L_i transmits information that defines the sector S_i, covered by each transmission.**
- **Sensor s defines the region of intersection (ROI), from all locators it hears.**

$$ROI = \bigcap_{i=1}^{|LH_s|} S_i$$

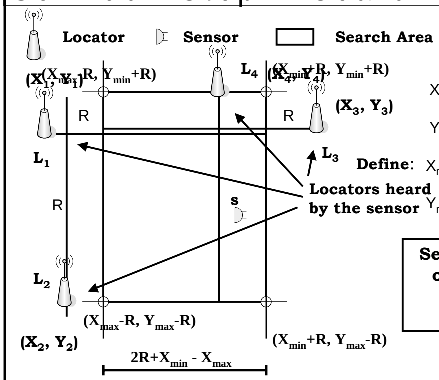
SeRLoc – Step 1: Beacon reception



The sensor collects information from all the locators that it can hear.

Locators	Coordinates	Slopes
L_1:	(X_1, Y_1)	$[\theta_{1,1}, \theta_{1,2}]$
L_2:	(X_2, Y_2)	$[\theta_{2,1}, \theta_{2,2}]$
L_3:	(X_3, Y_3)	$[\theta_{3,1}, \theta_{3,2}]$
L_4:	(X_4, Y_4)	$[\theta_{4,1}, \theta_{4,2}]$

SeRLoc – Step 2: Search area



Define:

$X_{min} = \min \{ X_i \; i \in LH_s \}$

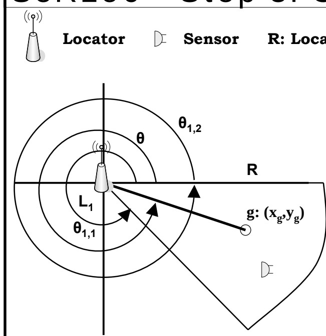
$Y_{min} = \min \{ Y_i \; i \in LH_s \}$

$X_{max} = \max \{ Y_i \; i \in LH_s \}$

$Y_{max} = \max \{ Y_i \; i \in LH_s \}$

Sensor places a grid of equally spaced points into the search area

SeRLoc – Step 3: Grid-sector test



— **Sensor holds a Grid Score Table (GST) initialized at zero.**

— **For every point in the grid and every sector heard, perform**

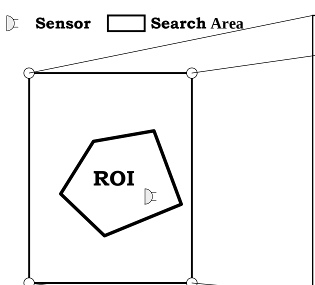
— **Grid sector test:**

$$C_1 : \|g - L_i\| \le R,$$

$$C_2 : \theta_{1,1} \le \theta \le \theta_{1,2}$$

— **If test positive increase score value by one.**

SeRLoc – Step 4: ROI computation



GRID Score Table (GST)

0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
…
1 1 1 2 3 3 3 3 4 4 4 3 3 3 3 3 3
1 1 2 2 2 3 4 4 4 4 4 4 4 3 3 2 2
1 1 2 2 4 4 4 4 4 4 4 4 4 3 3 2
2 2 2 2 3 4 4 4 4 4 4 4 4 3 2 2 2
2 2 3 3 3 3 4 4 4 4 4 3 3 2 2 2
2 2 2 3 3 3 3 4 4 4 4 3 3 2 2 2 2
1 2 2 2 3 3 3 3 4 4 3 2 2 2 3 4 3
2 2 2 3 3 3 3 3 2 2 2 2 1 1 1 1 1
…
0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 0

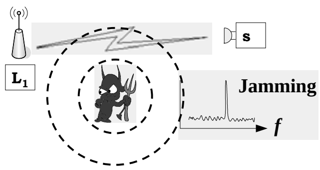
•**Majority vote: Points with highest score define the ROI.**
•**Error introduction due to discrete computation.**
•**Accuracy vs. Complexity tradeoff.**

Outline

- **Motivation**
- **Problem**
- **SeRLoc**
- **Threats and defense**
- **Performance**
- **High resolution localization: HiRLoc**
- **Conclusions**

Attacker Model

- **Attacker aims at displacing the sensors.**
- **Attacker must remain undetected.**
- **No DoS attacks.**
- **No jamming of the communication medium.**

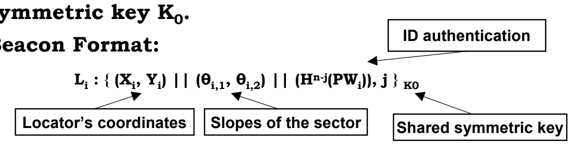


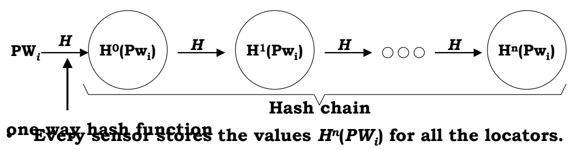
21

SeRLoc - Security mechanisms

- **Message Encryption: Messages encrypted with a symmetric key K_0.**
- **Beacon Format:**

$$L_i : \{ (X_i, Y_i) \,||\, (\theta_{i,1}, \theta_{i,2}) \,||\, (H^{n-j}(PW_i)), j \}_{K0}$$

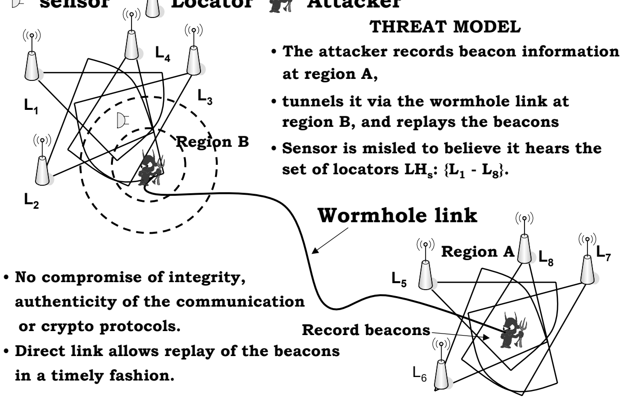




- **Every sensor stores the values $H^n(PW_i)$ for all the locators.**
- **A sensor can authenticate all locators that are within its range (one-hop authentication).**

22

SeRLoc – Wormhole Attack



THREAT MODEL

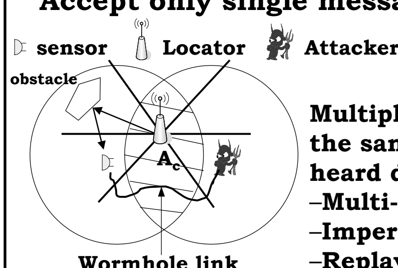
- **The attacker records beacon information at region A,**
- **tunnels it via the wormhole link at region B, and replays the beacons**
- **Sensor is misled to believe it hears the set of locators LH_s: $\{L_1 - L_8\}$.**

- **No compromise of integrity, authenticity of the communication or crypto protocols.**
- **Direct link allows replay of the beacons in a timely fashion.**

23

Wormhole attack detection (1)

Accept only single message per locator



Multiple messages from the same locator are heard due to:

- **Multi-path effects**
- **Imperfect sectorization**
- **Replay attack**

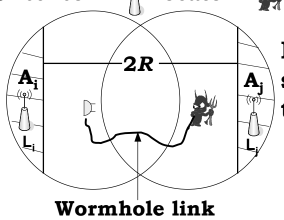
$$P(SG) = P(LH_{A_c} \geq 1) = 1 - e^{-\rho_L A_c}$$

24

Wormhole attack detection (2)

Communication range constraint property.

sensor   Locator   Attacker



Locators heard by a sensor cannot be more than 2*R* apart.

$$\|L_i - L_j\| \le 2R$$

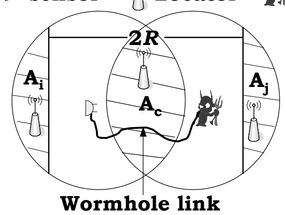
***R*: locator-to-sensor communication range.**

$$P(CR) \ge \left(1-e^{-\rho_L A_i}\right)\left(1-e^{-\rho_L A_j}\right)$$

Wormhole attack detection (3)

Probability of wormhole detection

sensor   Locator   Attacker

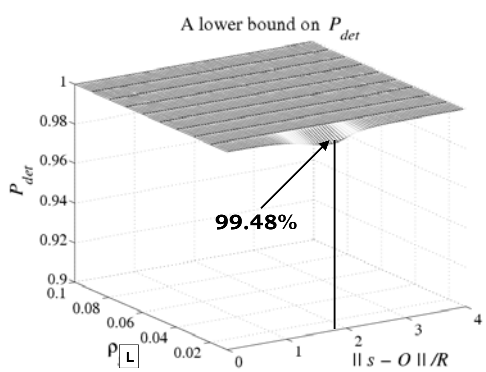


The events of a locator being within any region A_i, A_j, A_c are independent (Regions do not overlap).

$$P_{\det} = P\left(SG \bigcup CR\right) = P(SG) + P(CR) - P(SG)P(CR)$$
$$\ge \left(1-e^{-\rho_L A_c}\right) + e^{-\rho_L A_c}\left(1-e^{-\rho_L A_i}\right)^2$$

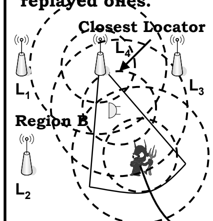
Wormhole attack detection (4)

Probability of wormhole detection



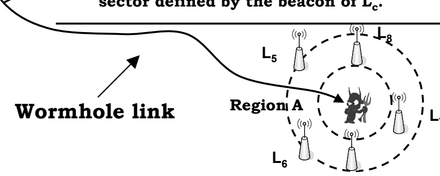
Resolution of location ambiguity

A sensor needs to distinguish the valid set of locators from the replayed ones.



Attach to Closest Locator Algorithm (ACLA)

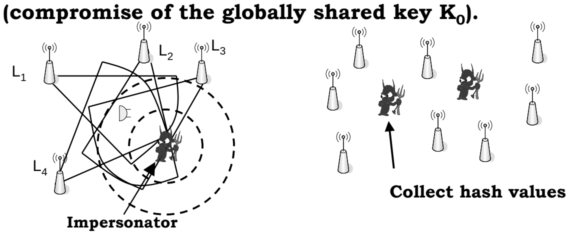
1. **Sensor s → : Broadcasts a nonce η.**
2. **Locator L_i→ : Reply with a beacon + the nonce η, encrypted with the pair-wise key $K_{s,Li}$.**
3. **Sensor s → : Identify the locator L_c with the first authentic reply.**
4. **Sensor s → : A locator L_i belongs to the valid set, only if it overlaps with the sector defined by the beacon of L_c.**



SeRLoc – Sybil Attack

THREAT MODEL

- The attacker impersonates multiple locators (compromise of the globally shared key K_0).



- Attacker can fabricate arbitrary beacons.
- Hence, compromise the majority-based scheme, if more than $|LH_s|$ locators impersonated.

Sybil Attack detection(1)

- In a Sybil attack, the sensor hears at least twice the number of locators.
- Define a threshold L_{max} as the maximum allowable number of locators heard, such that:

$$P(|LH_s| > L_{\max}) = \varepsilon,$$

Probability of false alarm

$$P(|LH_s| > \frac{L_{\max}}{2}) = 1 - \delta$$

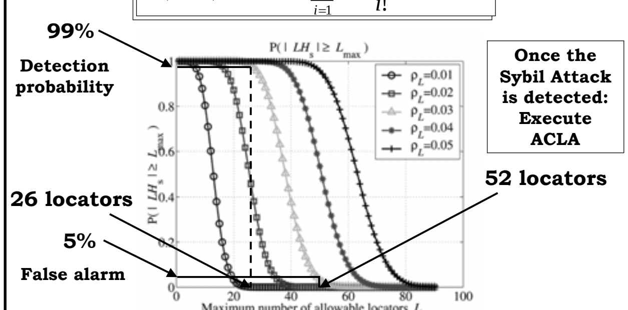
Probability of Sybil attack detection

- Design goal: Given security requirement δ, minimize false alarm probability ε.

Sybil Attack detection - Defense

- Random locator deployment we can derive the L_{max} value:

$$P(|LH_s| > k) = 1 - \sum_{i=1}^{k} \frac{(\rho_L \pi R^2)^i}{i!} e^{-\rho_L \pi R^2}$$



SeRLoc – Compromised entities

THREAT MODEL

- Compromised network entities: Attacker gains:
  1. Knowledge of all cryptographic quantities
  2. Full control over the behavior of the entity.
- Compromise of a sensor → reveals the globally shared key K_0.
- Compromise of a locator → reveals K_0, master key K_{Li}, and the hash chain of the locator.
- Impersonate the Closest Locator → Compromise the ACLA algorithm → Displace any sensor

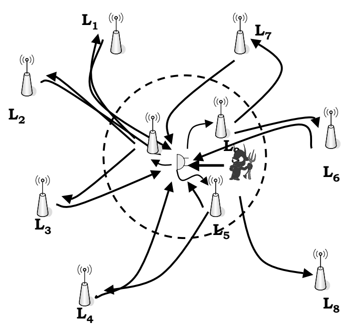
Enhanced location determination algorithm

1. The sensor transmits a nonce with his ID and set LH_s

2. Locators within r from the sensor relay the nonce.

3. Locators within R reply with a beacon + the nonce.

4. Sensor accepts first L_{max} replies.



- **Attacker has to compromise more than $L_{max}/2$ locators, AND**
- **Replay before authentic replies arrive at s.**

Outline

- **Motivation**
- **Secure Localization Problem**
- **SeRLoc**
- **Threats and defenses**
- **Performance Evaluation**
- **Conclusions**

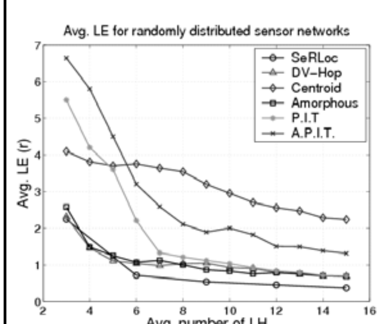
Performance Evaluation

- **Simulation setup:**
  - **Random locator distribution with density ρ_L.**
  - **Random sensor distribution with density 0.5.**
- **Performance evaluation metric:**

$$\overline{LE} = \frac{1}{|S|}\sum_{i=1}^{|S|}\frac{\left\|s_i^{est} - s_i\right\|}{r}$$

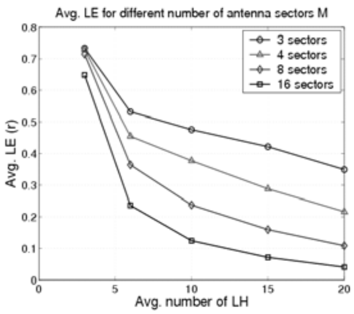
- s_i^{est} **: Sensor location estimation.**
- s_i **: Sensor actual location.**
- r **: Sensor-to-sensor communication range.**
- $|S|$ **: Number of sensors.**

Localization Error vs. LH



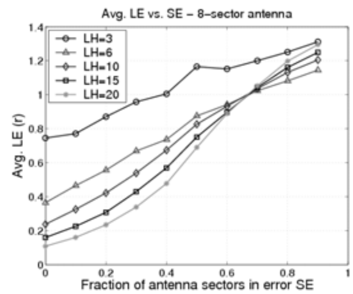
- **Each locator is equivalent to *M* reference points,**
- **M number of antenna sectors**
- **SeRLoc outperforms current schemes for any LH value**

Localization error vs. antenna sectors



- Higher number of directional antennas (narrower sectors) reduces LH.
- More expensive hardware at each locator.

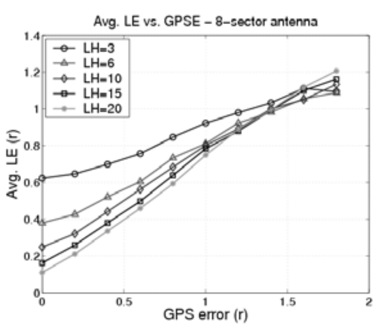
Localization error vs. sector error



- **Sector error: Fraction of sectors falsely estimated at each sensor.**
- **SeRLoc is resilient against sector error due to the majority vote scheme.**

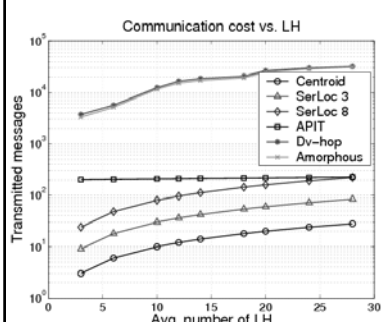
- **Even when 50% of the sectors are falsely estimated, LE < r for LH ≥ 6.**

Localization error vs. GPS error



- **GPS Error (*GPSE*): Error in the locators' coordinates.**
- **For *GPSE = 1.8r* and *LH = 3, LE = 1.1r.***
- **DV-hop/Amorphous: *LE = 1.1r* requires *LH = 5* with no *GPSE.***
- **APIT: *LE = 1.1r* requires *LH = 12* with no *GPSE.***

Communication Cost



- **Communication cost is independent of the number of sensors**
- **Communication cost increases with the locator density, or number of directional antennas at each locator.**

Performance Summary

- Increasing number of sectors
  - Reduction in error and power needed but increased complexity
- Sensitivity to GPSE error
  - GPSE=1.8r; Avg. LE=1.1r; requires
    - SeRLoc needs LH=3;
    - Dv-Hop needs LH=5, no GPSE;
    - APIT needs LH=12, no GPSE;
- Communication cost;
  - APIT requires |S|+|L|
  - SeRLoc requires |L|*M

S: Set of sensors, L: Set of locators, M: # of antennas

41

Conclusions

- We need to secure location estimation to claim secure location-dependent functions/apps.
- SeRLoc: SEcure Range-independent LOCalization
  - Robustly computes the location even in the presence of attacks
  - Better performance than up-to-date range independent localization schemes
  - Decentralized implementation, resilient to sources of error
- Current developments
  - Resistance to jamming attacks
  - Analytical evaluation of error bounds

42

Thank you for your time!

Any Questions

43