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

Why do we need location in WSN?

Location-dependent services

Network functions

Access Control

Monitoring Apps

Location-based Access Control

Microphone

Database query

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

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].

Outline

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

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.
Network Model Assumptions (1)

Two-tier network architecture

- **Omnidirectional Antennas**
  - Sensor range \( r \)

- **Directional Antennas**
  - Locator range \( R \)

- **Beamwidth** \( \theta \)

Locator\hspace{1cm} Sensor

\( (X_1, Y_1) \hspace{1cm} (X_2, Y_2) \)

\( (X_3, Y_3) \hspace{1cm} (X_4, Y_4) \)

\( (X_5, Y_5) \)

Network Model Assumptions (2)

- **Locator deployment**: Homogeneous Poisson point process of rate \( \rho_L \) \( \rightarrow \) Random spatial distribution.

- **Sensor deployment**: Poisson point process of rate \( \rho_s \) independent of locator deployment.

- Or can be seen as Random sampling with rate \( \rho_s \).

\[
P(LH_s = k) = \frac{(\rho_s \pi R^2)^k}{k!} e^{-\rho_s \pi R^2}
\]

\( LH_s \): 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.

<table>
<thead>
<tr>
<th>Locators</th>
<th>Coordinates</th>
<th>Slopes</th>
</tr>
</thead>
<tbody>
<tr>
<td>( L_1 )</td>
<td>([X_1, Y_1])</td>
<td>([\theta_{1,1}, \theta_{1,2}])</td>
</tr>
<tr>
<td>( L_2 )</td>
<td>([X_2, Y_2])</td>
<td>([\theta_{2,1}, \theta_{2,2}])</td>
</tr>
<tr>
<td>( L_3 )</td>
<td>([X_3, Y_3])</td>
<td>([\theta_{3,1}, \theta_{3,2}])</td>
</tr>
<tr>
<td>( L_4 )</td>
<td>([X_4, Y_4])</td>
<td>([\theta_{4,1}, \theta_{4,2}])</td>
</tr>
</tbody>
</table>

- \( (0, 0) \)
**SeRLoc – Step 2: Search area**

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

\[
\text{Define: } X_{\text{min}} = \min \{ X_i \in L_{H_s} \} \\
Y_{\text{min}} = \min \{ Y_i \in L_{H_s} \} \\
X_{\text{max}} = \max \{ X_i \in L_{H_s} \} \\
Y_{\text{max}} = \max \{ Y_i \in L_{H_s} \}
\]

**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:
    \[
    C_1 : \| g - L \| \leq R, \\
    C_2 : \theta_{1,2} \leq \theta \leq \theta_{1,2}
    \]
- If test positive increase score value by one.

**SeRLoc – Step 4: ROI computation**

- 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.

**SeRLoc - Security mechanisms**

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

  \[ L_i : \{ (X_i, Y_i) \mid \theta_{i,1}, \theta_{i,2} \mid \{ H^n(PW_i) \} \} R \]

  - Locator's coordinates
  - Slopes of the sector
  - Shared symmetric key

  \[ PW_i \xrightarrow{H} H^1(PW_i) \xrightarrow{H} H^2(PW_i) \ldots H^n(PW_i) \]

  - Hash chain
  - One-way hash function
  - A sensor can authenticate all locators that are within its range (one-hop authentication).

**SeRLoc - Wormhole Attack**

- 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 $L_{H_S} \{ L_1 \ldots L_8 \}$.
- No compromise of integrity, authenticity of the communication or crypto protocols.
- Direct link allows replay of the beacons in a timely fashion.

**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

\[ P(SG) = P(LH_{\geq 1}) = 1 - e^{-n_i} \]
**Wormhole attack detection (2)**

Communication range constraint property.

- Sensor
- Locator
- Attacker

Locators heard by a sensor cannot be more than \(2R\) apart.

\[ \|L_i - L_j\| \leq 2R \]

\(R\): locator-to-sensor communication range.

\[ P(CR) \geq \left(1 - e^{-\gamma_i \cdot \delta} \right) \left(1 - e^{-\gamma_j \cdot \delta} \right) \]

**Wormhole attack detection (3)**

Probability of wormhole detection

- Sensor
- Locator
- Attacker

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

\[ P_{\text{det}} = P(SG \cup CR) = P(SG) + P(CR) - P(SG)P(CR) \]

\[ \geq \left(1 - e^{-\gamma_i \cdot \delta} \right) + e^{-\gamma_i \cdot \delta} \left(1 - e^{-\gamma_j \cdot \delta} \right)^2 \]

**Wormhole attack detection (4)**

Probability of wormhole detection

A lower bound on \(P_{\text{det}}\).

\[ P_{\text{det}} \geq 99.48\% \]

**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 \(s\) \(\rightarrow\): Broadcasts a nonce \(\eta\).
2. Locator \(L_i\) \(\rightarrow\): Reply with a beacon + the nonce \(\eta\), encrypted with the pairwise key \(K_{s,L_i}\).
3. Sensor \(s\) \(\rightarrow\): Identify the locator \(L_c\) with the first authentic reply.
4. Sensor \(s\) \(\rightarrow\): 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 $|L_{Hs}|$ locators impersonated.

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

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:

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

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

Probability of false alarm

Probability of Sybil attack detection

• Design goal: Given security requirement $\delta$, minimize false alarm probability $\varepsilon$.

Sybil Attack detection - Defense

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

$$P(|L_{Hs}| > k) = 1 - \sum_{i=1}^{k} \left( \frac{p_i}{\beta} \right) e^{-\frac{p_i}{\beta}}$$

99% Detection probability

Once the Sybil Attack is detected: Execute ACLA

26 locators

52 locators

5% False alarm

Detection probability vs. Maximum number of allowable locators $L_{max}$
Enhanced location determination algorithm

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

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 $\rho_L$.
  - Random sensor distribution with density 0.5.
- Performance evaluation metric:

  $$LE = \frac{1}{|S|} \sum_{i=1}^{M} \left| \frac{s_i'} - s_i \right|$$

  - $s_i'$: 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

<table>
<thead>
<tr>
<th>Sector</th>
<th>LE vs. LH</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 sectors</td>
<td>0.8</td>
<td>Higher number of directional antennas (narrower sectors) reduces LH.</td>
</tr>
<tr>
<td>4 sectors</td>
<td>0.6</td>
<td></td>
</tr>
<tr>
<td>6 sectors</td>
<td>0.5</td>
<td></td>
</tr>
<tr>
<td>9 sectors</td>
<td>0.4</td>
<td></td>
</tr>
<tr>
<td>16 sectors</td>
<td>0.3</td>
<td></td>
</tr>
</tbody>
</table>

- 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 $LH \geq 6$.

### 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
  - \( \text{GPSE} = 1.8r \); Avg. LE = 1.1r; requires
    - \( \text{SeRLoc} \) needs LH = 3;
    - \( \text{Dv-Hop} \) needs LH = 5, no GPSE;
    - \( \text{APIT} \) needs LH = 12, no GPSE;
- Communication cost;
  - \( \text{APIT} \) requires \(|S| + |L|\)
  - \( \text{SeRLoc} \) requires \(|L|^M\)

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

### Conclusions

- We need to secure location estimation to claim secure location-dependent functions/apps.
- \( \text{SeRLoc: SEcure Range-independent LOCalization} \)
- 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

---

**Thank you for your time!**

**Any Questions**