ROPE:
Robust Position Estimation in wireless sensor networks

Wireless Sensor Networks (IN4181)

Venkatraman Iyer

2006-2007

Localization

Estimating the position of a sensor in the wireless network.

Applications

- **Routing,** based on physical location of nodes.
- **Querying** nodes over a geographical area.
- **Coverage** study of a network.

Different Approaches to Localization

Distance Estimation Techniques

- Received signal strength indicator (RSSI)
- Time (Difference) of arrival. (ToA, TdoA)
- Angle of arrival. (AoA)

Combining Techniques

- Tri-lateration/Multilateration
- Triangulation
- Maximum Likelihood Estimate (ML)

What is Localization lacking?

SECURITY !!!

An attacker can

- Disrupt distance estimates .
- Replay beacons to a different region (Mafia Frauds.)

Objectives of a Secure Localization System

- Achieve robust estimates.
- Ability to verify a location.

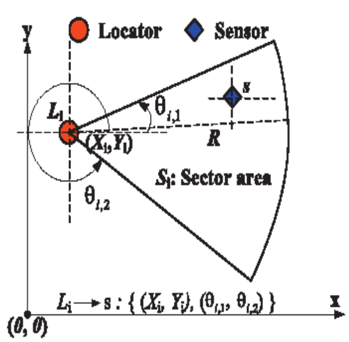
The ROPE Positioning System

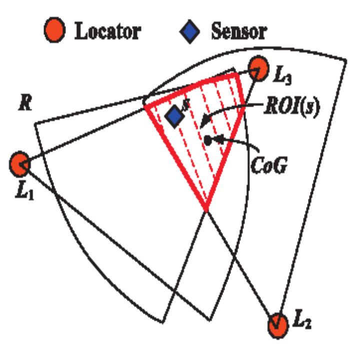
- A de-centralized, range-free, robust positioning system.
- Can verify location of sensors.

Key features

- ***Distance Bounding:*** **bounds an attacker's ability to spoof a sensor.**
- ***Verifiable Multilateration (VM): Multilateration with validity checks.***
- ***Secure Range Independent Localization***
    - ***Verifiers/Locators with predetermined locations.***
    - ***Directional Antennas for longer range.***
    - ***Use of pair-wise keys between sensors and locators.***

Range-free Localization principle





Threats handled

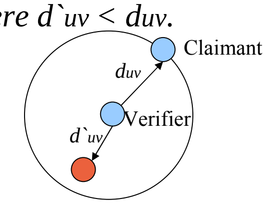
- **Wormhole**
  - Record information at one point, replay at another.
  - Can not be detected by message authentication codes.
- **SYBIL**
  Impersonation of nodes.
- **Jamming**
  Enlarges distance estimates.

TU Delft

Distance Bounding Principle(1)

Concept

- A claimant node at a distance *duv from a verifier cannot claim to be at a distance d`uv from it, where d`uv < duv.*



- *Exchange of RF signals between the claimant and the verifier.*

TU Delft

Distance Bounding Principle(2)

Distance bounding protocol

- The claimant ***u*** commits to a random nonce Nu.
  i.e. Generate commitment (c,d) = commit(Nu),
  send c to verifier.

- The verifier sends a challenge Nv, and starts a timer.

- The claimant responds by sending Nv Θ Nu (Θ = EX-OR).

- The verifier on receiving the challenge response, calculates *dvu*.

2006-2007 9

TUDelft

Distance Bounding Principle(3)

Distance bounding protocol(contd.)

- ***The claimant sends the decommit value d thorough an encrypted pairwise key Kvu.***

Assumptions/Requirements

- ***Binding and Hiding commitment scheme.***

- **Nanosecond precision for time measurement and computations.**

2006-2007 10

TUDelft

Verifiable Multilateration (VM)

Principle

- At least three reference points.
- Central Authority estimates sensor position and runs the verification checks.
- Prevents spoofing of honest nodes, and nodes from lying about their positions.

TUDelft

Range Independent Localization(1)

Features

- **De-centralized Passive localization.**
- ***Two tier network architecture. Locators i.e. reference points and sensors,***
- ***Sensor collects beacons from all locators within range, determines regions of intersection (ROI).***

TUDelft

Position Estimation in ROPE (1)

Network Model

- **Sensors.**
  - **Randomly deployed with density ρs.**
  - **Sensor-sensor Communication range of *r***
- **Locators.**
  - **randomly deployed with density ρL << ρs.**
  - **M directional antennas, each of beamwidth 2π/M.**
  - **Locator-sensor Communication range of *R*.**
  - ***Sensor-locator communication range*** $r_{SL} = rG^{\frac{1}{\gamma}}$
- **Key based security.**
  - Each sensor shares pair-wise key with every locator.

TUDelft

Position Estimation in ROPE (1)

Secure Localization

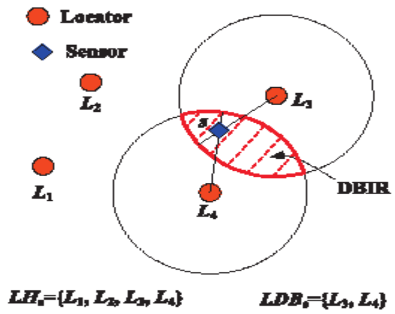
- **Sensor broadcasts Id with a random Nonce.**
- **Locators in the sensor's range perform distance bounding**
- **Sensor performs VM, when it has distance bounds with at least three locators. Notify neighbouring locators on completion.**
- **Compute Distance Bounding Intersection Region (DBIR) if multilateration is not feasible.**

TUDelft

Position Estimation in ROPE (2)

Secure Localization(contd.)

Distance Bounding Intersection Region (DBIR)



- **Meanwhile, Locators wait for a notification.**

Position Estimation in ROPE (3)

Secure Localization(contd.)

- **Locators that do not hear the notification re-broadcast the sensor Id, the original Nonce , with their Id.**
- **Re-transmission covers all locators within sensor's range.**
- **A locator on hearing the broadcast transmits the**

$$\left\langle M_j^k, MAC_{K_{L_j}^s}(M_j^k) \right\rangle,$$

$$M_j^k : Id_{L_j} \parallel (X_j, Y_j) \parallel (\theta_{j,1}^k, \theta_{j,2}^k) \parallel N_s,$$

M_j^k **:message transmitted by**

(X_j, Y_j) **:position of locator j**

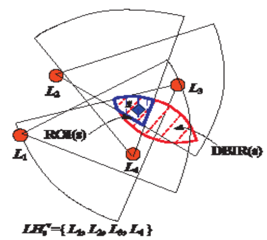
$(\theta_{j,1}^k, \theta_{j,2}^k)$ **:slopes of the sector boundary.**

$MAC_{K_{L_j}^s}(M_j^k)$ **: Message Authentication code.**

Position Estimation in ROPE (4)

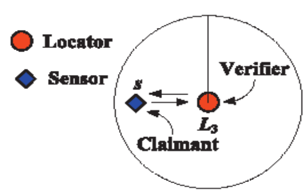
Secure Localization(contd.)

- **Collect beacons within the range *after* a time-out, and build a set of locators.**
- **Region of Intersection (ROI) determined**
- **Centre of gravity yields position estimate**



Position Verification in ROPE

- **Locators also operate as data collectors.**



- **Achieved through distance bounding.**

Attacks and the ROPE system(1)

Types of attacks

- **Wormhole**
  Record information at one point, replay at another.
- **SYBIL**
  Impersonation of nodes.

Metric for analyzing robustness

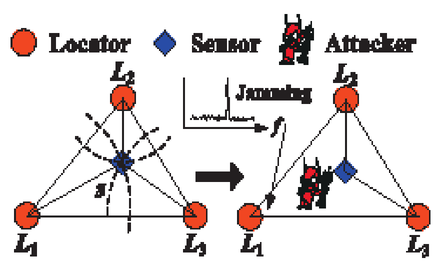
Maximum Spoofing Impact (MSI)*: *The maximum distance between the actual sensor position and the faulty position.

TU Delft

Prevention of attacks in ROPE (1)

- Attacker can either jam the transmissions or replay beacons after a delay.

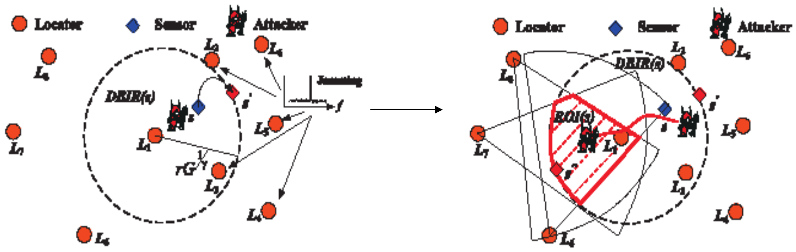
- If VM can be performed, distance bounding thwarts the attack.



TU Delft

Prevention of attacks in ROPE (2)

Wormhole attack



Cost of an attack makes it prohibitive.

Prevention of attacks in ROPE (3)

SYBIL attack

- **Infeasible to find (M',K') such tha** $MAC_{K'}(M')=MAC_{K^s_{L_i}}(M_i^k)$
- **A sensor can perform distance bounding with *Kmin* *locators to mitigate impact of a single locator compromise.***
- ***Trade-off between security, and locator density.***

Performance Evaluation(1)

Experiment Setup

- Sensors deployed in an area 100m X 100m with density $\rho_s = 0.5$.
- Varying density ρ_L of locators.

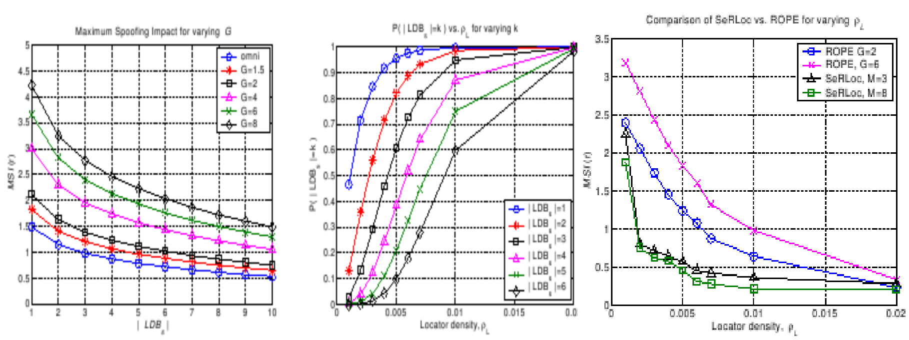
Metric for analyzing robustness

Maximum Spoofing Impact (MSI)*: *The maximum distance between the actual sensor position and the faulty position.

$$MSI = \max_{p \in DBIR} \|s - p\|.$$

TU Delft

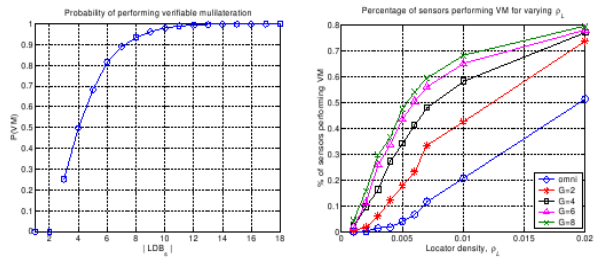
Performance Evaluation(2)



(a) (b) (c)

TU Delft

Performance Evaluation(3)



(a) (b)

TU Delft

Conclusions

- ROPE performs a robust and verifiable localization using distance bounding and VM.
- Resists wormhole attacks, impersonation and jamming.
- Limits MSI even for low locator densities.

TU Delft