Secure location determination and verification in wireless networks

- 1. Lazos, L. and Poovendran, R. 2004. SeRLoc: secure range-independent localization for wireless sensor networks. In Proceedings of the 3rd ACM Workshop on Wireless Security (Philadelphia, PA, USA, October 01 - 01, 2004). WiSe '04.
- 2. S. Ray, R. Ungrangsi, F. D. Pellegrini, A. Trachtenberg, and D. Starobinski. Robust location detection in emergency sensor networks. In Proceedings of IEEE INFOCOM 2003, April 2003.
- 3. Liu, D., Ning, P., and Du, W. K. 2005. Attack-resistant location estimation in sensor networks. In Proceedings of the 4th international Symposium on information Processing in Sensor Networks (IPSN) (Los Angeles, California, April 24 - 27, 2005).
- 4. Ekici, E.; Mcnair, J.; Al-Abri, D., "A Probabilistic Approach to Location Verification in Wireless Sensor Networks," Communications, 2006. ICC '06. IEEE International Conference on , vol.8, no., pp.3485-3490, June 2006.

Attack-Resistant Location Estimation in Sensor Networks

Dependable Computing Systems Laboratory

DongHoon Shin

24 October 2007

Motivation & Goal

- Motivation
  - Most of existing location discovery protocols for wireless sensor networks (WSNs) are vulnerable in hostile environments.
  - Authentication can certainly enhance the security of location discovery, but cannot guarantee it.
    - Replaying beacon packets
    - Forging beacon packets with keys learned through compromised nodes
- Goal
  - Develop attack-resistant location estimation techniques to tolerate the malicious attacks against range-based location discovery in WSNs.

Attack Resistant Location Estimation

- Attack-Resistant Minimum Mean Square Estimation
  - Exploits the inconsistency among location references
  - Employs the minimum mean square estimation (MMSE) to identify and remove malicious location references
- Voting-Based Location Estimation
  - Has location reference "vote" on the cells in which node may reside
  - Provides an iterative refinement of voting results

Assumptions & Threat Model

- All beacon nodes are uniquely identified.
- Each non-beacon node uses at most one location reference derived from the beacon signals sent by each beacon node.
- Distances measured from beacon signals (e.g., with RSSI or TDoA) are used for location estimation.
- A location reference obtained from a beacon signal is denoted as a triple <x, y, δ>.
- An attacker may change any field in a location reference.
- Multiple malicious beacon nodes may collude together to make the malicious location references appear to be consistent.

5/15

Attack-Resistant MMSE

- Algorithm
  1. First, estimate the sensor's location with a existing MMSE-based method, and then assess if the estimation location could be derived from a set of consistent location references.
     - If yes, accept the estimation result
     - Otherwise, identify and remove the most inconsistent location reference, and repeat the above process
  2. The process continues until we find a set of consistent location references or it is not possible to find such a set.
- Mean square error and τ-consistent

Definition 1: Given a set of location references $\mathcal{L} = \{\langle x_1, y_1, \delta_1\rangle, \langle x_2, y_2, \delta_2\rangle, ..., \langle x_m, y_m, \delta_m\rangle\}$ and a location $(\tilde{x}_0, \tilde{y}_0)$ estimated based on $\mathcal{L}$, the *mean square error of this location estimation* is $\varsigma^2 = \sum_{i=1}^{m} \frac{(\delta_i - \sqrt{(\tilde{x}_0 - x_i)^2 + (\tilde{y}_0 - y_i)^2})^2}{m}$.

- If $\varsigma^2 < \tau^2$, L is said to be τ-consistent.

6/15

Attack-Resistant MMSE

- Given a set L of n-location references and a threshold τ, find the largest set of τ-consistent location references
  - Naïve approach: check all subsets of L with i location references about τ-consistency
    - i starts from n and drops until a subset of L is found τ-consistent or it is not possible to find such a set
    - If the largest set consists of m elements, # of MMSE method to be used is at least, $1+{}_nC_{m+1}+ \cdots +{}_nC_n$ times, e.g. if n=10 and m=5, 387 times are needed to perform the MMSE method.
  - Greedy Algorithm
    - In first round, starts with the set of all location references
    - In each round, it first verifies if the current set of location references is τ-consistent
      - If yes, the algorithm outputs the estimated location and stops.
      - Otherwise, it considers all subsets of location with one fewer location reference, and chooses the subset with least mean square error as input to the next round.
    - Uses a MMSE method at most $1+n+(n-1)+ \cdots + 4$ times when m=5. For the earlier example, performs MMSE operations for about 50 times.

7/15

Attack-Resistant MMSE

- Determine threshold τ
  - τ depends on the measurement error model
  - Assume the measurement error model will not change
  - Performs simulation off-line and determine an appropriate τ
  - The measurement error of a benign location reference $<x_i, y_i, \delta_i>$ can be given by $e_i = \delta_i - \sqrt{(x_0 - x_i)^2 + (y_0 - y_i)^2}$
  - Obtain the distribution of the mean square error through following Lemma1

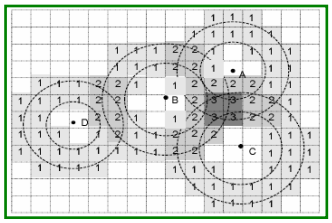
Lemma 1: Let $\{e_1, ..., e_m\}$ be a set of independent random variables, and μ_i, σ_i^2 be the mean and the variance of e_i^2, respectively. If the estimated location of a sensor node is its real location, the probability distribution of ς^2 is $\lim_{m\to\infty} \mathrm{F}[\varsigma^2 \le \varsigma_0^2] = \Phi(\frac{m\varsigma_0^2 - \mu'}{\sigma'})$, where $\mu' = \sum_{i=1}^{m} \mu_i$, $\sigma' = \sqrt{\sum_{i=0}^{m} \sigma_i^2}$, and $\Phi(x)$ is the probability of a standard normal random variable being less than x.

  - Choose a value of τ corresponding to a high cumulative probability

8/15

Voting-Based Location Estimation

- Basic Scheme
  - Determine the target field
    - First, identifies the minimum rectangular that covers all the locations declared in location references
    - Extend this rectangular by the transmission range of a beacon signal
  - Divide the target field into M small squares (cells) with same side length L
  - Keeps a voting state variable for each cell, initially set to 0
  - Find a candidate ring at (x, y)
    - For a benign location reference <x, y, δ>, this location reference must be in a ring centered at (x, y), with inner radius max{δ-ε,0} and outer radius δ+ε
  - Identifies the cells that overlap with the corresponding candidate ring
    - Increments the voting variables for these cells by 1



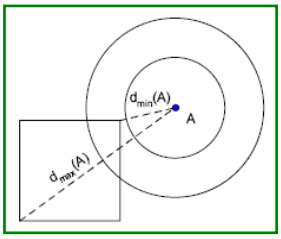
9/15

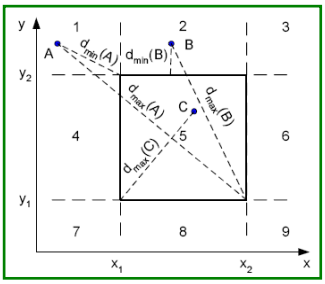
Voting-Based Location Estimation

- Overlap of Candidate Rings and Cells
  - Check if the candidate ring at A overlaps with a cell
    - The candidate ring does not overlaps with the cell only when

$$d_{min}(A) > r_o \text{ or } d_{max}(A) < r_i$$

  - Compute d_{min} and d_{max}

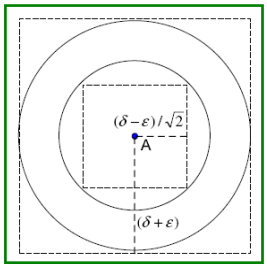




10/15

Voting-Based Location Estimation

- Overlap of Candidate Rings and Cells (con't)
  - Limit the examinations of cells



- Iterative Refinement
  - Number of cells M is a critical parameter
    - The larger M, the more precise the location is, but more storage required
  - Granularity of the partition is limited by memory size
  - Iterative refinement
    1. M is chosen according to the memory constraint.
    2. After the first round, a sensor node find the cells having the largest vote.
    3. In the next round, performs the voting process for the smallest rectangle that contains all cell having the largest vote.
    4. The iterative refinement process continues until a desired precision is reached or the estimation cannot be refined.

11/15

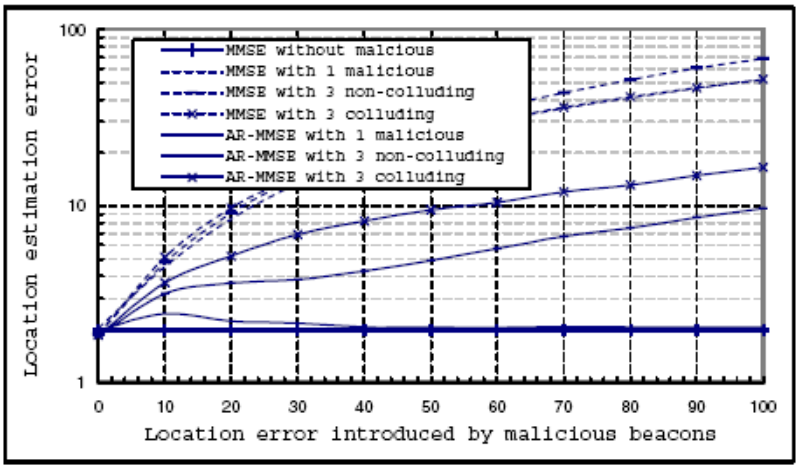
Simulation Evaluation

- Three Attack Scenarios
  - A single malicious location reference
    - Declares a wrong location e meters away from the beacon node's real location
  - Multiple non-colluding malicious location references
    - Each of them independently declares a wrong location.
  - Multiple colluding malicious location references
    - Malicious location references declare false locations.
    - Coordinate with each other so that the malicious location references may appear to be consistent to a victim node.

12/15

Simulation Evaluation

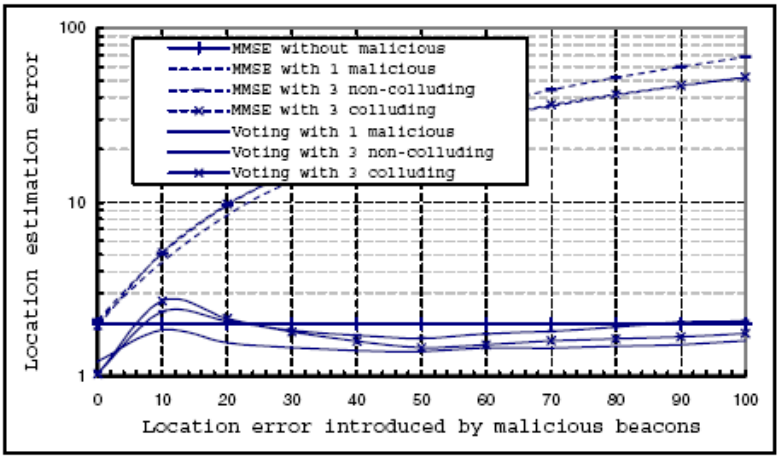
- Evaluation of Attack-Resistant MMSE



13/15

Simulation Evaluation

- Evaluation of Voting-Based Scheme



14/15

Future Research

- Study the techniques that utilize location references from non-beacon nodes that already estimated their locations
  - Investigate the effect of “error propagation” due to the estimation errors at non-beacon nodes
- Study how to combine the proposed techniques with other protection mechanisms such as wormhole detection

15/15