Secure Location Verification with Hidden and Mobile Base Stations

S. Capkun, K.B. Rasmussen - Department of Computer Science, ETH Zurich
M. Cagalj – FESB, University of Split
M. Srivastava – EE Department, UCLA

Presenter - Imran Shah

Outline

- Introduction
- Model
- Infrastructure Centric Localization
- Node Centric Localization
- Sensor Networks with Mobile Base Stations
- Mobile Ad Hoc Networks
- Analysis
- Conclusion

Overview

- Determining node location and ranging is used to implement location based routing and location related functions including access control
- Techniques rely on measurement of radio time of flight (RF ToF), ultrasound time of flight (US ToF), measurement of received strength of radio signals (RF RSS)
- Techniques are vulnerable to attacks

Introduction - Overview

Approach

- Proposed methods do not require fast processing at the prover and works with use of any kind of ranging
- Approach relies on Covert Base Stations (CBS) – location unknown to attacker when localization is performed. CBS is typically passive
- Goal – prevent a node from lying about position

Introduction - Approach

System Model

- Localization infrastructure consists of set of CBSs and Public Base Stations (PBS)
- Assumptions:
  -Attacker can not tamper with CBS location or compromise a CBS
  -Every node shares a secret key with each PBS or each PBS holds authentic public key of node
  -CBS can measure signal strength and perform ranging
  -Communication between CBS and PBS is through channel that preserves location privacy (e.g. wired or infrared)
  -Nodes have a limited number of attempts to prove location

Model - System Model

Attacker Model

- Two types of attacks:
  -Internal - Dishonest or compromised node provides a false location
  -External – External attacker is able to spoof an honest node's position
- Two types of localization systems:
  -Node centric – Node computes its own location
  -Infrastructure centric – Infrastructure computes location of nodes

Model - Attacker Model

Infrastructure Centric Localization w/ CBS

- System based on utilizing time difference of arrival (TDOA) and CBSs

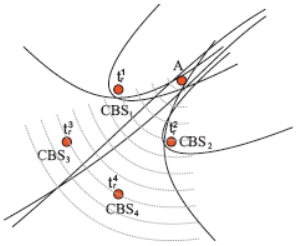


Fig. 1. An example of positioning with Time Difference Of Arrival. The base stations CBS measure the differences of signal arrival times, and compute the position of node A.

TDOA with hidden base stations

1 $PBS(t_s) \rightarrow A: N$
2 $A \rightarrow *:$ m $= \{A, N, \text{sig}_{K_A}(A, N)\}$
3 CBS_n : receive m at t_r^n
: with $t_r^1, \ldots, t_r^n$, compute p with TDOA
: if $\sum_{i>j}(|t_r^i - t_r^j| - h(p,i,j))^2 \leq \Delta$ and $\max_i(t_r^i - t_s) \leq T$
then $p_A = p$; else reject p

$$p = \arg\min_{p^*} \sum_{i>j} (|t_r^i - t_r^j| - h(p^*, i, j))^2$$

Infrastructure Centric Localization-Model

Infrastructure Centric Localization w/ CBS

- To cheat attacker needs to know, or correctly guess, location of CBSs
- Precision of Δ is key
- Wormhole attacks are partially mitigated through use of nonce and time period in which response is expected
- Node location privacy is not preserved as PBS is not authenticated

Infrastructure Centric Localization-Security Analysis

Node Centric Localization - Model

- Node computes its own position, reports it to infrastructure through radio and ultrasonic messages, infrastructure verifies.

Position verification with hidden base stations

1 $PBS(t_s) \rightarrow A: N$

2 $A \rightarrow$ (rf)$*$: $m_{rf} = p_F, \text{sig}_{K_A}(\text{rf}, p_F, N)$

(us) : $m_{us} = p_F, \text{sig}_{K_A}(\text{us}, p_F, N)$

3 CBS : receive m_{rf} at t_{rf} and m_{us} at t_{us}

: $d_F^e = d(p_F, p_{CBS})$

: $d_F^m = (t_{us} - t_{rf})s$

: if $|d_F^e - d_F^m| \leq \Delta$ and $(t_{rf} - t_s) \leq T$ then $p_A = p_F$; else reject p_A

Node Centric Localization-Model

Node Centric Localization - Attacks

- Internal attack –
  False position report - CBS checks accuracy of reported distance
- External attack – Include spoofing, jamming, replay – Partially prevented through the use of time limit on responses
- Cloning attack not addressed, and again location privacy is not preserved (but could be)

Node Centric Localization-Attacks

Sensor Networks with MBSs

- Method for secure localization using MBSs
- Sensors compute their location on their own
- An MBS securely knows its own location
- Each MBS shares a secret key with each sensor

Model

- An MBS sends a verification request to a node from a location and then waits for a response at a different location

Position verification with mobile base stations

1 (t_1) $MBS \rightarrow A$: MBS, N, T_R
2 (t_2) S $\rightarrow *$ (rf) : p, $\text{MAC}_K(\text{rf}, p, \text{MBS}, N)$
(us) : p, $\text{MAC}_K(\text{us}, p, \text{MBS}, N)$
3 MBS : receive (rf) at t_{rf} and (us) at t_{us}
: $d_S^e = d(p, p_{MBS})$
: $d_S^m = (t_{us} - t_{rf})s$
: if $|d_1^e - d_1^m| \leq \Delta$ and $(t_{rf} - t_1) \leq T_R$
: then $p_S = p$; else reject p_S

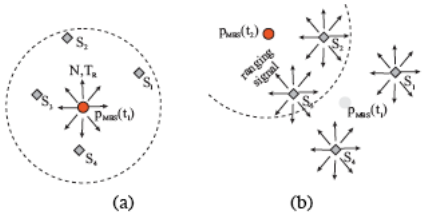
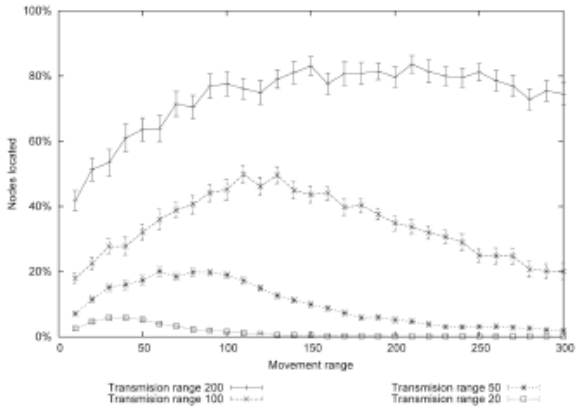


Fig. 4. Position verification in sensor networks. A mobile base station (MBS) verifies positions of nodes; (a) at time t_1 MBS challenges sensor nodes; (b) at time $t_2 > t_1$ the sensors reply to the challenge and their positions are verified by MBS.

Coverage and Simulation

- If sensors are uniformly distributed and at each motion step the MBS moves within the circle defined by its power range it will hear at least 39% of the sensors in its power range at previous time interval



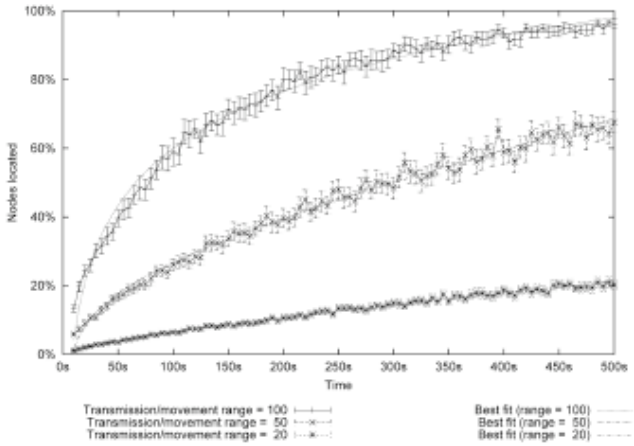


Fig. 10. MBS coverage as a function of time. Every point on the graph is the average result of 50 simulations, whereas the vertical bars indicate the 95 percent confidence interval.

Node Centric Location Verification in Mobile Ad Hoc Networks

- No dedicated MBSs rather nodes obtain their own positions and rely on neighbors for verification
- Each node has public/private key pair and shares a secret key with location database server

Protocol

$$
\begin{array}{l}
A: \text{pick } N \leftarrow \{0,1\}^k \\
A \overset{*}{\rightsquigarrow} *: A, P_A, T_A, N, \text{sign}_{K_A}\{A, P_A, T_A, N\} \\
\\
\quad B: d_A^c \leftarrow \text{dist}(P_A, P_B) \\
\quad\quad d_A^m \leftarrow (t_{us} - t_{rf}) \cdot v_s \\
\quad\quad \textbf{if } |d_A^c - d_A^m| \leq \Delta \\
\quad\quad \textbf{then } m \leftarrow \text{enc}_{K_{BS}}(B, A, T_B, P_A, ok) \\
\quad\quad \textbf{else } m \leftarrow \text{enc}_{K_{BS}}(B, A, T_B, P_A, nok) \\
\quad\quad stat_B \leftarrow m, \text{sign}_{K_B}\{m, N\} \\
\\
B \longrightarrow A: stat_B \\
A \longrightarrow S: m
\end{array}
$$

Fig. 12. Node B issues a witness location statement, attesting if A was at location P_A at time T_B. Note that A does not know if B's witness statement is positive *ok* or negative *nok*. A forwards this statement to the server S (in a private message and possibly over multiple hops). A's location P_A is therefore disclosed only to its surrounding nodes (for location verification) and to the location server S and is not disclosed to other network nodes.

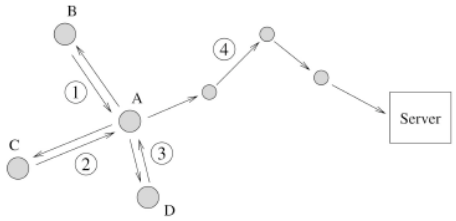


Fig. 11. Node A gathers signed witness statements about its location in order to update a central location database (residing on the server S). Each using the protocol in Fig. 12, nodes B, C, and D first verify the location of A (steps 1, 2, and 3) and then send (to A) signed statements about their locations. A then sends its position, along with the collected witness statements (positive and negative), in a confidential message to the server (step 4).

Analysis

- Authors analyze probability that an internal attacker is able to cheat the proposed methods by guessing location of or distance to CBSs
- Success for attacker is when a false location is reported and the CBS calculates a reported position within the confidence interval that verifies the reported position

$$|d_F^c - d_F^m| \leq \Delta \qquad Pr(|d_F^c - d_F^m| \leq \Delta | p_F \neq p_A)$$

Analysis

Analysis

- Assume localization occurs on a disk (2D) or sphere (3D) to reflect power ranges of devices
- Assume position of base station is uniformly chosen

Analysis

Attacker Average Success Probability

- If attacker and hidden base station are placed uniformly on disk/sphere
- Authors show that the more precise Δ is and the larger the area of the disk/sphere the more secure the position verification becomes.
- An attacker's chance for success can also be reduced by using multiple CBSs for position verification

Attacker Maximum Success Probability

- Which position on the disk/sphere will yield highest probability for success?
- Authors show that highest probability of success is when position is chosen at center of disk/ sphere and false measured distance is

$$d_F^m = R$$

Analysis of Time Difference of Arrival

- When TDOA is used attacker must also guess direction where directional antenna should be pointed to send delayed message to correct base station
- Attacker desires to hit correct CBS and not hit any of the other CBSs
- Maximum probability of success occurs when angle chosen is 1/n where n is the number of base stations which is the max of

$$P_{hit} = \frac{\theta}{\theta_{max}} = \theta_{rel}, \qquad P_{intr} = (1 - \theta_{rel})^{n-1}.$$

- Probability of aiming N directional antennas at N CBSs without hitting any wrong CBSs $\prod_{n=1}^{N} \frac{1}{n}\left(1 - \frac{1}{n}\right)^{n-1}$
- Best case probability to cheat with 4 CBSs is 9.6 * 10^-9
- Attacker's probability of success can also be decreased by placing CBSs around the localization areas

Analysis

Sensitivity

- Desire to set Δ such that it minimizes false negatives and false positives
- Two sources of error – error in reported position and error in distance measurement
- Assuming errors are normally distributed total error $|d_F^c - d_F^m|$ is $error \sim N(0, \sigma^2 = \sigma_P^2 + \sigma_R^2)$
- Let $\Delta = k\sigma$ and $(\sigma = \sqrt{\sigma_P + \sigma_R})$
- s is defined as $1/k$ and is a measure of sensitivity

Analysis

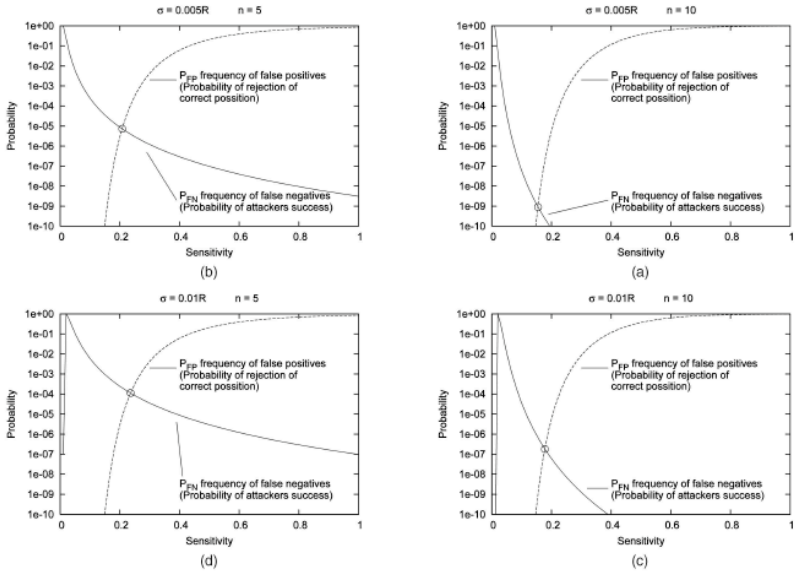


Fig. 17. The frequency of false positives and false negatives, and a crossover error rate for (a) $\sigma = 0.005R$ and $n = 5$, (b) $\sigma = 0.005R$ and $n = 10$, (c) $\sigma = 0.01R$ and $n = 5$, (d) $\sigma = 0.01R$ and $n = 10$. $s = 1/k$ is the sensitivity. $\Delta = k\sigma$ is the tolerated localization and ranging error. σ is the standard deviation of the localization and ranging error. Note that the probability axis is logarithmic.

Further Improvement

- If frequency of false positives is set to 1%

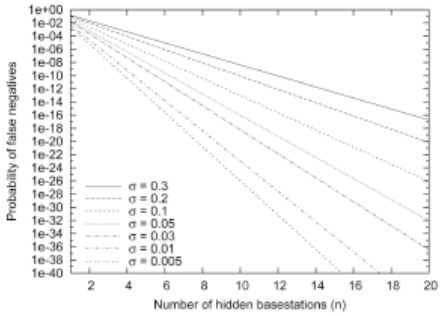


Fig. 18. The frequency of false negatives (the probability of the attacker's success) if the frequency of false positives is set to 1 percent.

Analysis

Conclusion

- Approach proposes secure localization using CBSs in infrastructure centric and node centric scenarios
- Secure localization is also presented for secure localization in sensor networks with mobile base stations and for location verification in mobile ad hoc networks
- Future work will focus on implementation and will look into privacy