Analysis on Perfect Location Spoofing Attacks Using Beamforming

Ting Wang and Yaling Yang

Virginia Tech, Dept. of ECE

Background

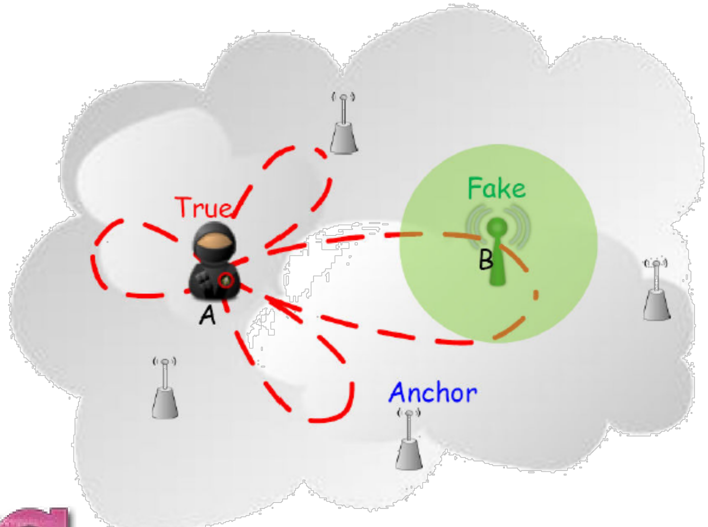
- Location information is critical
  - *Location-based access control*
  - *Identity spoofing detection*
- Threats
  - *Location concealing*
  - *Location spoofing with targeted fake location*
    - More threatening

Road Map

- Attack Model and Objective
- Problem Formulation
- Algorithm
- Simulation Results
- Conclusion

Attack Model

- Perfect Location Spoofing (PLS)
  - *Falsify the RSS measurements to be almost the same as for the targeted fake location*
  - *Using carefully designed beamforming pattern*



Objective

- By answering the questions below:
  - Is PLS attack possible?
  - Under what situations will PLS be feasible?

- Provide:
  - Suggestions for defending PLS attacks

Road Map

- *Attack Model and Objective*
- Problem Formulation
  - How PLS attack works
  - Requirement of PLS attack
  - PLS feasibility problem
- Algorithm
- Simulation Results
- Conclusion

Beamforming

- Circular array

$$G(\theta) = \sum_{i=1}^{N_{ant}} w_i \exp[j\frac{2\pi}{\lambda} R\cos(\theta - \phi_i)]$$

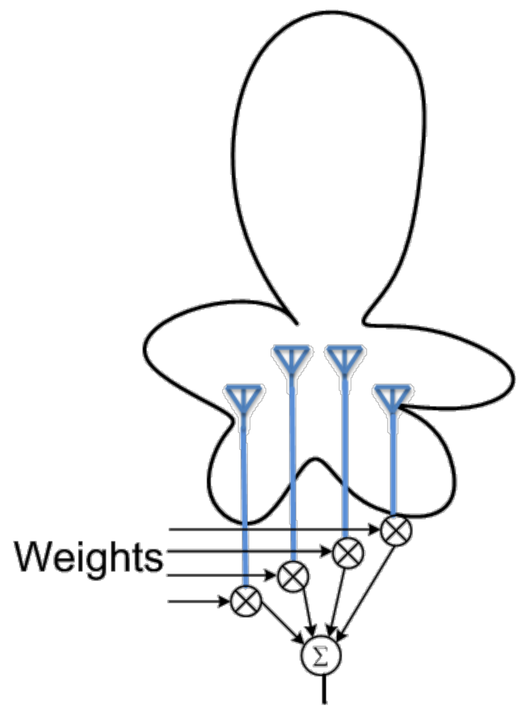
Complex weight

Antenna geometry

Variables to be optimized:

$$\mathbf{w} = [w_1, w_2, \cdots w_{N_{ant}}]^T$$

- Other geometries
  - Linear array
  - Planer array
  - 3-D array



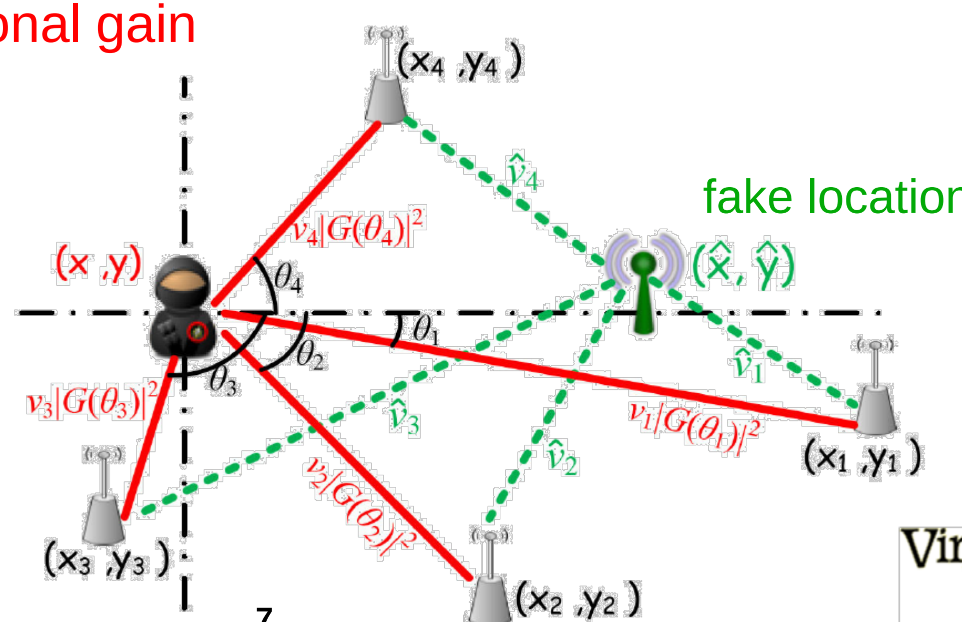
How PLS attack works

- Compensating path loss differences using beamforming

$$v_k|G(\theta_k)|^2 \approx \hat{v}_k, \forall k = 1, 2, \cdots, K.$$

Real path loss — Beamforming directional gain — Path loss from fake location

- θ_k : direction of the k^th anchor



Requirement of PLS Attack

- For each anchor k within coverage, the falsified path loss is almost the same as the normal path loss from the fake location, with a difference no more than the standard deviation of Gaussian noise (δ dB).

$$\left|10\log_{10}(v_k|G(\theta_k)|^2) - 10\log_{10}(\hat{v}_k)\right| \leq \delta(\mathrm{dB})$$

$$|G(\theta_k)|^2 = |\mathbf{w}^H \mathbf{h}_k|^2$$

Complex weight vector

Antenna array geometry

Feasibility Problem of PLS

- NP-hard

$$\begin{aligned} \text{find any} \quad & \mathbf{w}^H \\ \text{s.t.} \quad & |\mathbf{w}^H \mathbf{f}_k|^2 \le \delta \\ & |\mathbf{w}^H \mathbf{f}_k|^2 \ge \frac{1}{\delta} \\ & k = 1, 2, \cdots, K. \end{aligned}$$

Complex weighting vector which defines the beamforming pattern

$$\mathbf{f}_k = \left(\frac{v_k}{\hat{v}_k}\right)^{\frac{1}{2}} \mathbf{h_k}$$

$$\mathbf{h}_k = \begin{bmatrix} \exp[j\frac{2\pi}{\lambda} R\cos(\theta_k - \phi_1)] \\ \exp[j\frac{2\pi}{\lambda} R\cos(\theta_k - \phi_2)] \\ \vdots \\ \exp[j\frac{2\pi}{\lambda} R\cos(\theta_k - \phi_{N_{ant}})] \end{bmatrix}$$

Antenna array geometry

Road Map

- *Attack Model and Objective*
- *Problem Formulation*
- Algorithm
- Simulation Results
- Conclusion

Reformulation

- Add quadratic objective function to the PLS problem:

$$
\begin{aligned}
\min_{\mathbf{w}} \quad & obj = \sum_{k=1}^{K} (\mathrm{trace}(\mathbf{X}\mathbf{Q}_k) - 1)^2 \\
\text{s.t.} \quad & \mathrm{trace}(\mathbf{X}\mathbf{Q}_k) \le \delta \\
& \mathrm{trace}(\mathbf{X}\mathbf{Q}_k) \ge \frac{1}{\delta} \\
& k = 1, 2, \cdots, K \\
& \mathbf{X} \succeq 0 \\
& \mathrm{rank}(\mathbf{X}) = 1.
\end{aligned}
$$

Non-convex constraint

$$\mathbf{Q}_k = \mathbf{f}_k \mathbf{f}_k{}^H$$

obj reaches 0 when the beamforming pattern is ideal, which means:

$$|\mathbf{w}^H \mathbf{f}_k|^2 = \frac{v_k |G(\theta_k)|^2}{\hat{v}_k} = 1$$

Semidefinite Relaxation

- Ignore the non-convex constraint "$\text{rank}(\mathbf{X}) = 1$" and we get the following SDR (semidefinite relaxation) problem, which is convex:

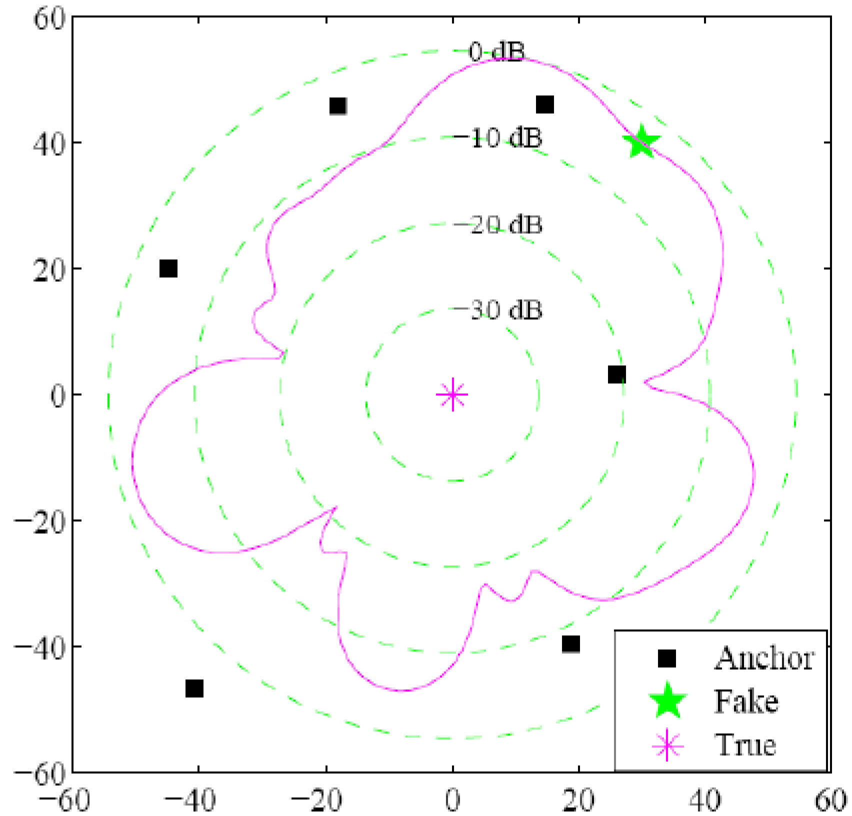
$$\begin{array}{ll} \min\limits_{\mathbf{w}} & \sum\limits_{k=1}^{K} (\text{trace}(\mathbf{X}\mathbf{Q}_k) - 1)^2 \\ \text{s.t.} & \text{trace}(\mathbf{X}\mathbf{Q}_k) \leq \delta \\ & \text{trace}(\mathbf{X}\mathbf{Q}_k) \geq \frac{1}{\delta} \\ & k = 1, 2, \cdots, K \\ & \mathbf{X} \succeq 0 \end{array}$$

Road Map

- *Attack Model and Objective*
- *Problem Formulation*
- *Algorithm*
- Simulation Resultst
- Conclusion

PLS Beamforming Pattern

- Anchors are randomly generated in a 200*200 m^2 2-D space
- Attacker's location: (0, 0)
- Fake location: (30, 40)

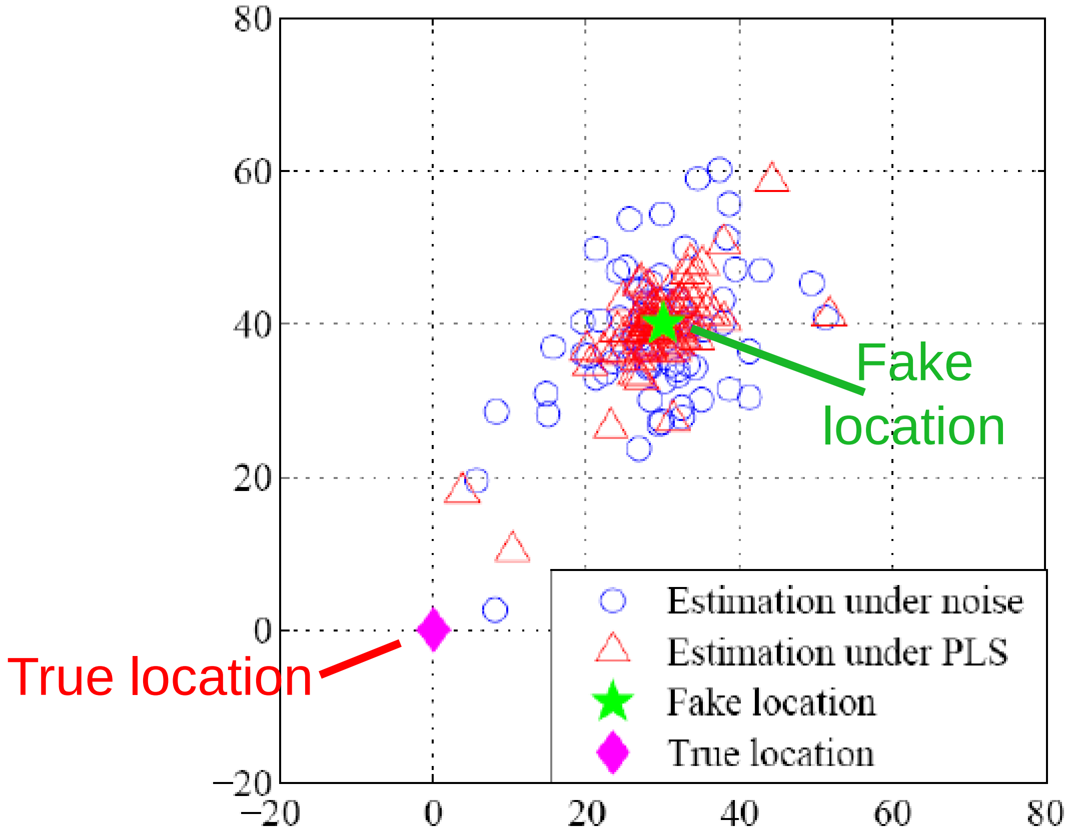


Success Rates of PLS

- (# of feasible PLS / # of feasible SDR) out of 200 simulations
  - # of feasible PLS – lower bound
  - # of feasible SDR – upper bound

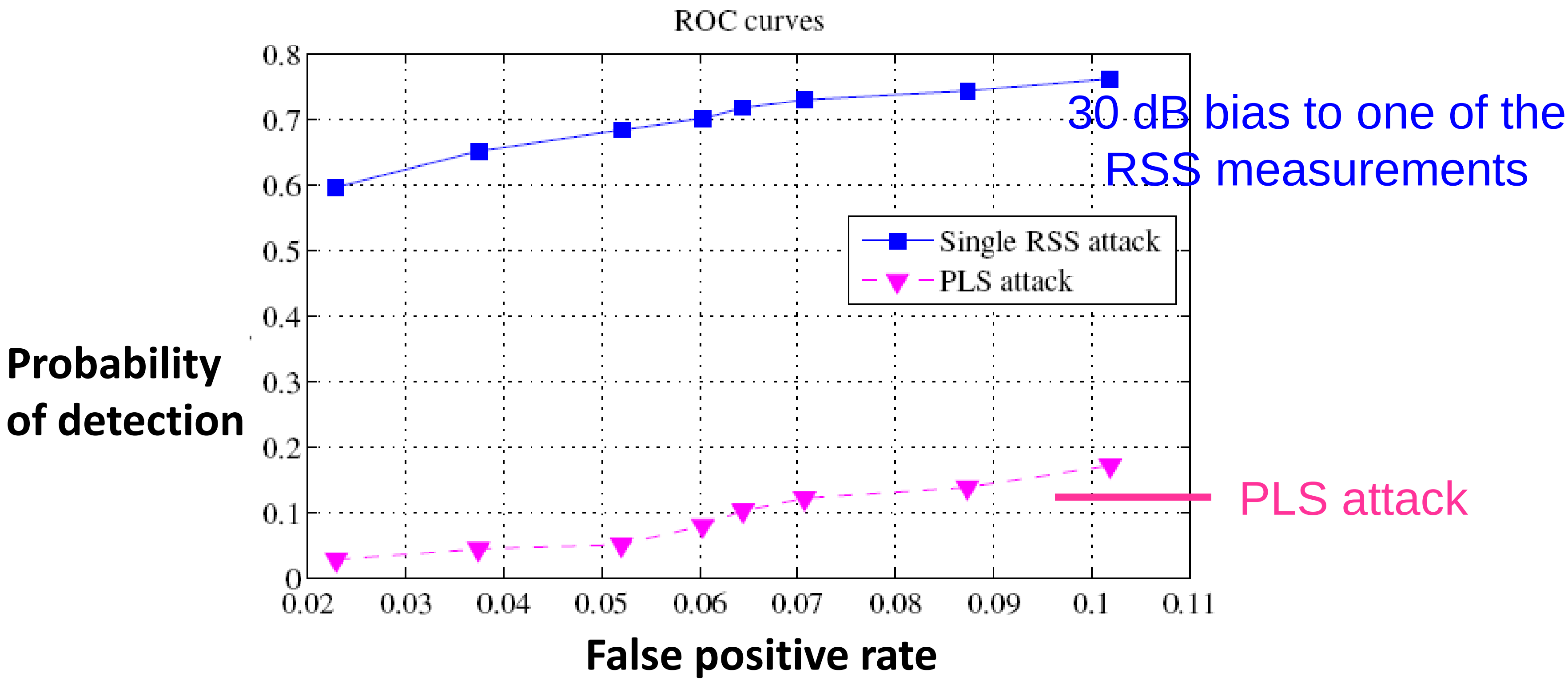
δ	K	N_{ant}=6	N_{ant}=8	N_{ant}=10	N_{ant}=12
1dB	4	66/70	142/160	170/181	175/192
	5	4/7	78/97	93/152	106/182
	6	0/0	20/34	43/97	31/162
	7	0/0	0/5	16/64	9/95
	8	0/0	0/0	3/29	1/33
2dB	4	96/96	129/129	171/172	180/181
	5	10/11	105/107	148/148	165/170
	6	0/0	55/56	110/110	134/141
	7	0/0	15/15	81/84	97/107
	8	0/0	1/1	43/50	74/78
3dB	4	80/84	144/145	169/169	186/188
	5	15/16	117/120	148/152	170/176
	6	0/0	60/62	117/120	133/145
	7	0/0	18/20	99/100	100/107
	8	0/0	0/1	44/47	78/86

Spoofed localization



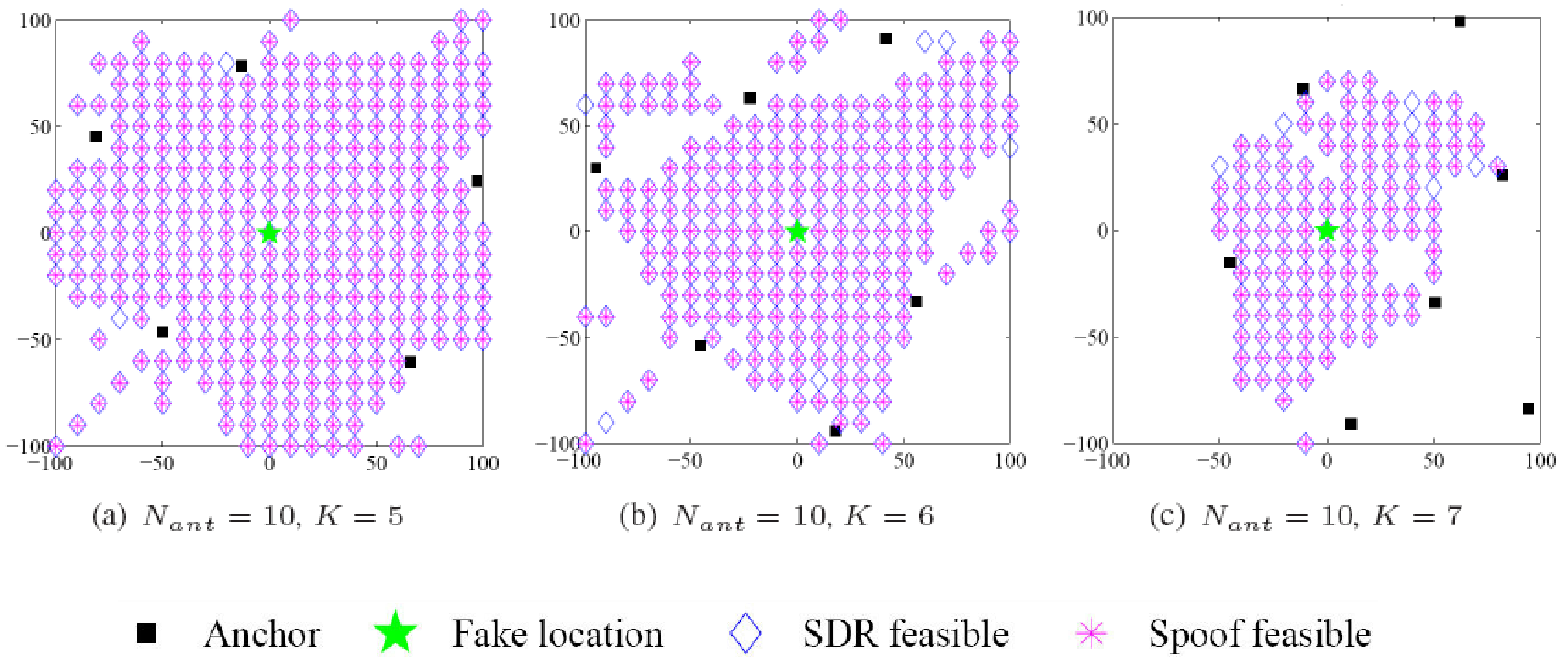
Spoofed location estimations overlapping with noised localization results around the fake location

PLS Attacks are Difficult to Detect



Attack detection algorithm introduced in:
Y. Chen, W. Trappe, and R. P. Martin, “Attack detection in wireless localization,” in Proceedings of IEEE INFOCOM, 2007.

Fixed Anchor Deployment



(a) $N_{ant} = 10,\ K = 5$ (b) $N_{ant} = 10,\ K = 6$ (c) $N_{ant} = 10,\ K = 7$

Road Map

- *Attack Model and Objective*
- *Problem Formulation*
- *Algorithm*
- *Simulation Results*
- Conclusion

Conclusion

- Anchor deployment with higher density lowers the success rate of PLS attacks.

- Guard against PLS attacks
  - Increase anchor density near critical area
  - Use mobile anchors

Thanks!

Questions?