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

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

Variables to be optimized:

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

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

Complex weight

Antenna geometry
How PLS attack works

- Compensating path loss differences using beamforming

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

- \( \theta_k \): direction of the \( k^{th} \) anchor

Real path loss

Beamforming directional gain

Path loss from fake location

\( (x_1, y_1) \)
\( (x_2, y_2) \)
\( (x_3, y_3) \)
\( (x_4, y_4) \)
\( \hat{x} \)
\( \hat{y} \)
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 (\( \delta \) dB).

\[
|10 \log_{10}(v_k |G(\theta_k)|^2) - 10 \log_{10}(\hat{v}_k)| \leq \delta (\text{dB})
\]

\[
|G'(\theta_k)|^2 = |w^H h_k|^2
\]
NP-hard

\[
\begin{align*}
\text{find any } & \quad w^H \\
\text{s.t.} & \quad |w^H f_k|^2 \leq \delta \\
& \quad |w^H f_k|^2 \geq \frac{1}{\delta} \\
& \quad k = 1, 2, \cdots, K.
\end{align*}
\]

\[f_k = \left( \frac{v_k}{\hat{v}_k} \right)^{\frac{1}{2}} h_k\]

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

Complex weighting vector which defines the beamforming pattern

Antenna array geometry
Road Map

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

- Add quadratic objective function to the PLS problem:

\[
\min_w \quad obj = \sum_{k=1}^{K} (\text{trace}(XQ_k) - 1)^2
\]

s.t. \[\begin{align*}
\text{trace}(XQ_k) &\leq \delta \\
\text{trace}(XQ_k) &\geq \frac{1}{\delta} \\
k & = 1, 2, \cdots, K \\
X &\succeq 0 \\
\text{rank}(X) & = 1.
\end{align*}\]

\[Q_k = f_k f_k^H\]

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

\[|w^H f_k|^2 = \frac{v_k |G(\theta_k)|^2}{\hat{v}_k} = 1\]
Semidefinite Relaxation

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

\[
\begin{align*}
\min_{w} & \quad \sum_{k=1}^{K} (\text{trace}(XQ_k) - 1)^2 \\
\text{s.t.} & \quad \text{trace}(XQ_k) \leq \delta \\
& \quad \text{trace}(XQ_k) \geq \frac{1}{\delta} \\
& \quad k = 1, 2, \ldots, K \\
& \quad X \succeq 0
\end{align*}
\]
Road Map

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

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

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

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

- Anchor
- Fake location
- SDR feasible
- Spoof feasible
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?