Secure Trajectory Planning Against Spoofing Attacks

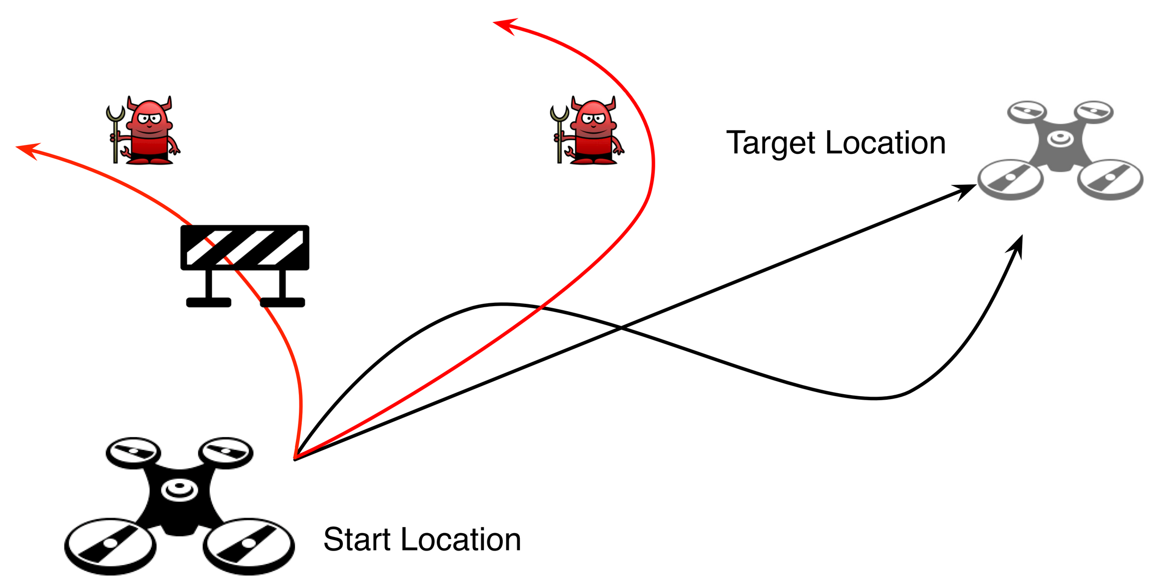
Gianluca Bianchin, Yin-Chen Liu, and Fabio Pasqualetti

Department of Mechanical Engineering, University of California Riverside

Secure Trajectory Planning

Attacks are intentional changes of:

- Received localization signals
- Control inputs to the robot



Attacker vs Defender: Objectives

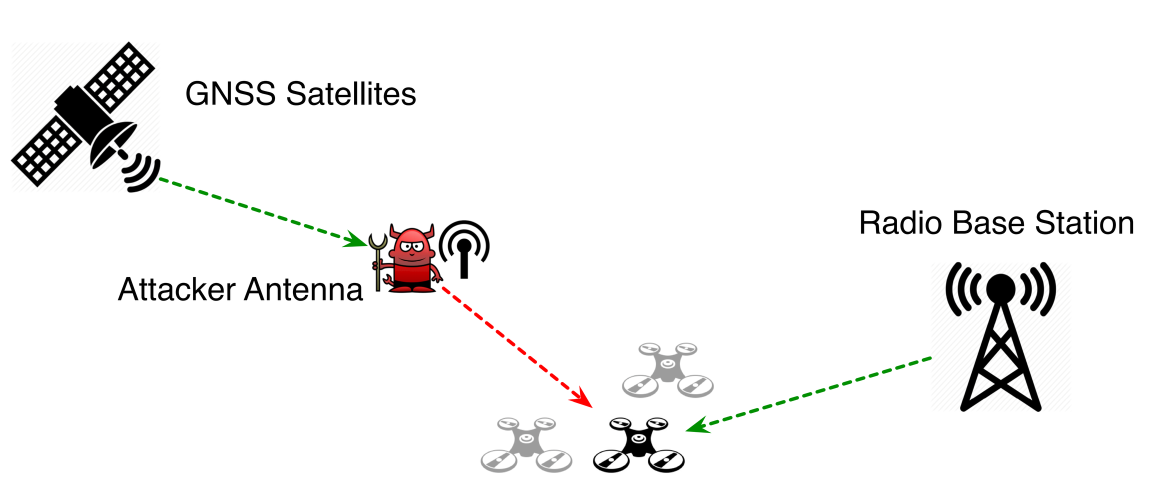
Attacker: Design spoofing and control so that

- Deviation between desired trajectory and actual trajectory is maximized
- Attack remains undetected

Defender: Design secure, open-loop, control inputs that guarantee

- In the absence of attacks, the robot achieves a desired final state at minimum time
- In the presence of attacks, available sensors allow attack detection

Spoofing Mechanism



Contact Information

- Email: gianluca@engr.ucr.edu
- Web: sites.google.com/a/ucr.edu/gbianchin

Robot Dynamics

Double integrator dynamics moving on a 2-D plane

$$\underbrace{\begin{bmatrix}\dot p_{\rm n}\\ \dot v_{\rm n}\end{bmatrix}}_{\dot x_{\rm n}} = \underbrace{\begin{bmatrix}\mathbf{0}_2 & I_2\\ \mathbf{0}_2 & \mathbf{0}_2\end{bmatrix}}_{A}\underbrace{\begin{bmatrix}p_{\rm n}\\ v_{\rm n}\end{bmatrix}}_{x_{\rm n}} + \underbrace{\begin{bmatrix}\mathbf{0}_2\\ I_2\end{bmatrix}}_{B} u_{\rm n}$$

Bound on largest robot acceleration

$$\|u_{\rm n}\| \leq u_{\max}$$

Sensor readings

$$y_{\rm n}^{\rm GNSS} = p_{\rm n} \qquad y_{\rm n}^{\rm RSSI} = p_{\rm n}^{\mathsf T} p_{\rm n}$$

Attacker Model

Attackers can simultaneously:

1. Compromise the nominal control input $u_{\rm n}$

$$\underbrace{\begin{bmatrix}\dot p\\ \dot v\end{bmatrix}}_{\dot x} = \underbrace{\begin{bmatrix}\mathbf{0}_2 & I_2\\ \mathbf{0}_2 & \mathbf{0}_2\end{bmatrix}}_{A}\underbrace{\begin{bmatrix}p\\ v\end{bmatrix}}_{x} + \underbrace{\begin{bmatrix}\mathbf{0}_2\\ I_2\end{bmatrix}}_{B} u \qquad \|u\| \leq u_{\max}$$

2. Spoof the received GNSS signal

$$y^{\rm GNSS} = p + u^{\rm GNSS} \qquad y^{\rm RSSI} = p^{\mathsf T} p$$

Attack Undetectability

$$y^{\rm GNSS} = y_{\rm n}^{\rm GNSS} \qquad y^{\rm RSSI} = y_{\rm n}^{\rm RSSI}$$

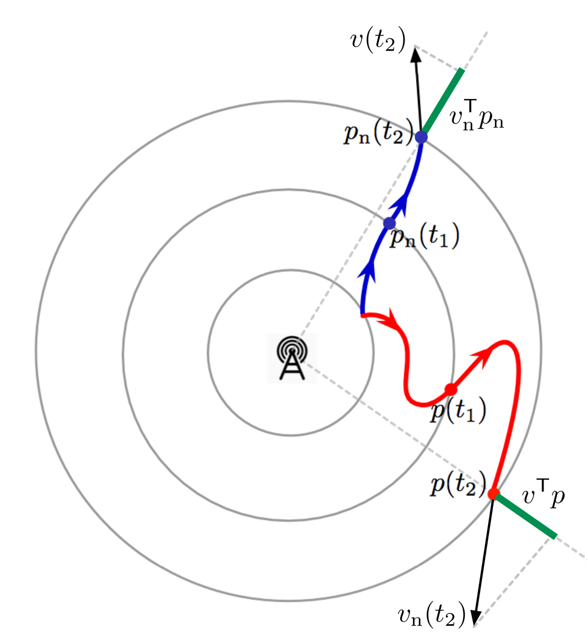
That is, sensor readings are compatible with each other and follow the nominal dynamics

Double Integrator Robots

Undetectable Trajectories

Position and velocity satisfy, for all times,

$$p^{\mathsf T} p = p_{\rm n}^{\mathsf T} p_{\rm n} \qquad v^{\mathsf T} p = v_{\rm n}^{\mathsf T} p_{\rm n}$$



Undetectable Control Inputs

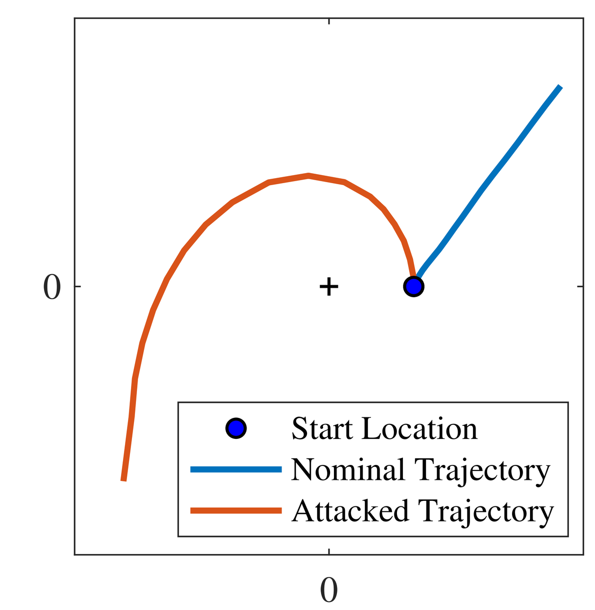
The attack undetectability constraints the radial acceleration of the robot

$$\text{Radial Acc.} = \frac{u_{\rm n}^{\mathsf T} p_{\rm n} + \|v_{\rm n}\|^2 - \|v\|^2}{\|p\|^2}$$

Attacker Control Problem

$$\begin{aligned}\max_{u,x} \quad & (x(T) - x_{\rm n}(T))^{\mathsf T} Q (x(T) - x_{\rm n}(T))\\ \text{subject to} \quad & \dot x = Ax + Bu\\ & \text{Radial Acc.} = \frac{u_{\rm n}^{\mathsf T} p_{\rm n} + \|v_{\rm n}\|^2 - \|v\|^2}{\|p\|^2}\\ & \|u\| \leq u_{\max}\end{aligned}$$

Control of Tangential Acceleration



Secure Trajectory Planning

Given initial position $p_{\rm I}$ and desired final position $p_{\rm F}$, determine $u_{\rm n}$ and the control horizon $[0, T]$ s.t.

$$p_{\rm n}(0) = p_{\rm I} \qquad p_{\rm n}(T) = p_{\rm F}$$

and, for any undetectable attack, either

1. $p = p_{\rm n}$ for all $t \in [0, T]$
2. If $p \neq p_{\rm n}$ then the attack is detectable

Secure Control Inputs

A control input is secure if and only if

$$u_{\rm n} = \kappa \frac{p_{\rm n}}{\|p_{\rm n}\|} u_{\max}$$

where $\kappa : \mathbb{R}_{[0,T]} \to \{-1, 1\}$

Secure control inputs accelerate the robot with the maximum admissible acceleration

Secure Trajectory Planning

$$\begin{aligned}\min_{\kappa,T} \quad & T + (x_{\rm n}(T) - x_{\rm D})^{\mathsf T} Q (x_{\rm n}(T) - x_{\rm D})\\ \text{subject to} \quad & \dot x_{\rm n} = Ax_{\rm n} + Bu_{\rm n}\\ & u_{\rm n} = \kappa \frac{p_{\rm n}}{\|p_{\rm n}\|} u_{\max}\end{aligned}$$

$\Rightarrow$ Two-point boundary value problem

$\Rightarrow$ Bang-Bang optimal control $\kappa^* = -\operatorname{sgn}(\lambda^{\mathsf T} B p_{\rm n})$

Control of Radial Acceleration