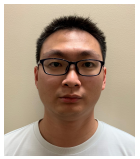
# Secure Navigation of Robots in Adversarial Environments

**Gianluca Bianchin**, Yin-Chen Liu, and Fabio Pasqualetti

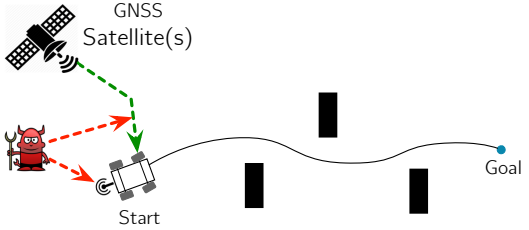




Department of Mechanical Engineering
University of California, Riverside

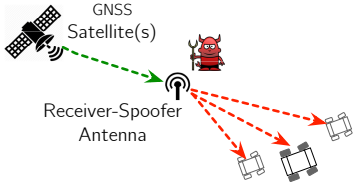
58th IEEE Conference on Decision and Control
December 12, 2019 | Nice, France



## Secure Navigation in Adversarial Environments

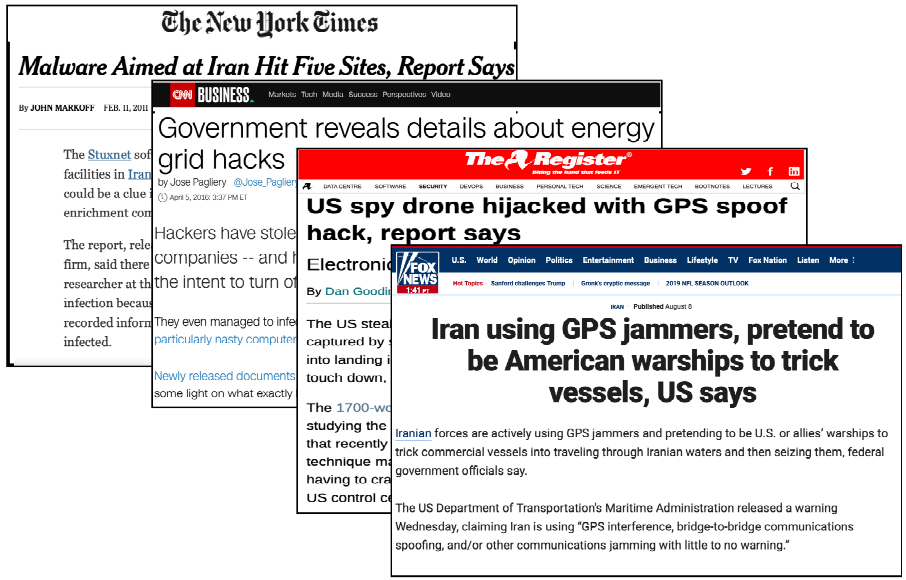



- Navigate from start position to goal
- Despite unknown and arbitrary attacks
- Vulnerability: wireless communication
- e.g. GPS spoofing






## Security of Cyber-Physical Systems and Spoofing



The New York Times

*Malware Aimed at Iran Hit Five Sites, Report Says*

By JOHN MARKOFF FEB. 11, 2011

The Stuxnet sof
facilities in Iran
could be a clue
enrichment con

The report, rele
firm, said there
researcher at th
infection becaus
recorded inform
infected.

CNN BUSINESS Markets Tech Media Success Perspectives Video

Government reveals details about energy grid hacks

by Jose Pagliery @Jose_Pagliery

Hackers have stole
companies -- and
the intent to turn o

They even managed to infe
particularly nasty computer

Newly released documents
some light on what exactly

The Register

**US spy drone hijacked with GPS spoof hack, report says**

Electronic

By Dan Goodi

The US steal
captured by
into landing
touch down.

The 1700-w
studying the
that recently
technique ma
having to cra
US control c

FOX NEWS 24/7

U.S. World Opinion Politics Entertainment Business Lifestyle TV Fox Nation Listen More

Hot Topics Sanford challenges Trump Gronk's cryptic message 2019 NFL SEASON OUTLOOK

IRAN Published August 8

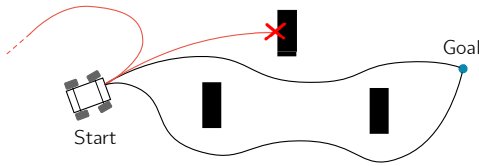
**Iran using GPS jammers, pretend to be American warships to trick vessels, US says**

Iranian forces are actively using GPS jammers and pretending to be U.S. or allies' warships to trick commercial vessels into traveling through Iranian waters and then seizing them, federal government officials say.

The US Department of Transportation's Maritime Administration released a warning Wednesday, claiming Iran is using "GPS interference, bridge-to-bridge communications spoofing, and/or other communications jamming with little to no warning."



## Can We Make Robotic Navigation Secure?




1. Can an attacker modify the trajectory and escape detectability?

✓ Yes, under appropriate design

2. Can we design trajectories are secure?

✓ Yes, there is a tradeoff between security and control energy

## Secure Trajectory Planning: Model

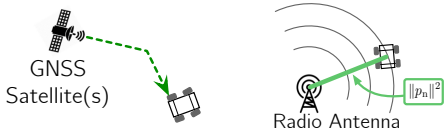
**Nominal Robot**

Double integrator on 2-D plane

$$\underbrace{\begin{bmatrix}\dot{p}_\mathsf{n}\\ \dot{v}_\mathsf{n}\end{bmatrix}}_{\dot{x}_\mathsf{n}} = \underbrace{\begin{bmatrix} & 1\\ & \end{bmatrix}}_{A}\underbrace{\begin{bmatrix}p_\mathsf{n}\\ v_\mathsf{n}\end{bmatrix}}_{x_\mathsf{n}} + \underbrace{\begin{bmatrix}\\ 1\end{bmatrix}}_{B} u_\mathsf{n}$$

Localization via GNSS and RSSI

$$y_\mathsf{n}^{\mathsf{GNSS}} = p_\mathsf{n} \qquad y^{\mathsf{RSSI}} = \|p_\mathsf{n}\|^2$$




**Robot Under Attack**

Attackers compromise the controls

$$\underbrace{\begin{bmatrix}\dot{p}\\ \dot{v}\end{bmatrix}}_{\dot{x}} = \underbrace{\begin{bmatrix} & 1\\ & \end{bmatrix}}_{A}\underbrace{\begin{bmatrix}p\\ v\end{bmatrix}}_{x} + \underbrace{\begin{bmatrix}\\ 1\end{bmatrix}}_{B} u$$

And spoof the GNSS signal

$$y^{\mathsf{GNSS}} = p + u^{\mathsf{SPOOF}} \qquad y^{\mathsf{RSSI}} = \|p\|^2$$



## Secure Trajectory Planning: Model

**Nominal Robot**

Double integrator on 2-D plane

$$\underbrace{\begin{bmatrix}\dot{p}_\mathsf{n}\\ \dot{v}_\mathsf{n}\end{bmatrix}}_{\dot{x}_\mathsf{n}} = \underbrace{\begin{bmatrix} & 1\\ & \end{bmatrix}}_{A}\underbrace{\begin{bmatrix}p_\mathsf{n}\\ v_\mathsf{n}\end{bmatrix}}_{x_\mathsf{n}} + \underbrace{\begin{bmatrix}\\ 1\end{bmatrix}}_{B} u_\mathsf{n}$$

Localization via GNSS and RSSI

$$y_\mathsf{n}^{\mathsf{GNSS}} = p_\mathsf{n} \qquad y^{\mathsf{RSSI}} = \|p_\mathsf{n}\|^2$$

**Robot Under Attack**

Attackers compromise the controls

$$\underbrace{\begin{bmatrix}\dot{p}\\ \dot{v}\end{bmatrix}}_{\dot{x}} = \underbrace{\begin{bmatrix} & 1\\ & \end{bmatrix}}_{A}\underbrace{\begin{bmatrix}p\\ v\end{bmatrix}}_{x} + \underbrace{\begin{bmatrix}\\ 1\end{bmatrix}}_{B} u$$

And spoof the GNSS signal

$$y^{\mathsf{GNSS}} = p + u^{\mathsf{SPOOF}} \qquad y^{\mathsf{RSSI}} = \|p\|^2$$

**Trajectory planner**: selects $u_\mathsf{n}$

**Attackers**: choose $(u, u^{\mathsf{SPOOF}})$

Gianluca Bianchin (UC Riverside) Secure Navigation of Robots Dec 12, 2019 4 / 16

## Undetectable Attacks

An **Undetectable Attack** is:

Pair $(u, u^{\mathsf{SPOOF}})$ that is not "visible" from the sensors:

$$y_\mathsf{n}^{\mathsf{GNSS}} = y^{\mathsf{GNSS}}, \qquad y_\mathsf{n}^{\mathsf{RSSI}} = y^{\mathsf{RSSI}} \qquad \text{(at all times)}$$

An attack is undetectable **if and only if**

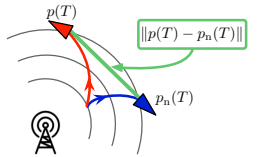
$$u^\mathsf{T} p = u_\mathsf{n}^\mathsf{T} p_\mathsf{n} + \|v_\mathsf{n}\|^2 - \|v\|^2$$
$$u^{\mathsf{SPOOF}} = p_\mathsf{n} - p$$

Can be computed given the nominal state at all times



## Computing Optimal Undetectable Attacks

$$\begin{aligned} \max_{u} \quad & \|p(T) - p_\mathsf{n}(T)\| \\ \text{s.t.} \quad & \dot{x} = Ax + Bu \\ & u = \text{undetectable} \\ & \|u\| \le u_{\max} \end{aligned}$$




Optimal solutions are:

$$u = a_\mathsf{r}\, p + w$$

where $w^\mathsf{T} p = 0$, and

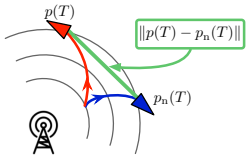
$$a_\mathsf{r} = (u_\mathsf{n}^\mathsf{T} p_\mathsf{n} + \|v_\mathsf{n}\|^2 - \|v\|^2)\|p\|^{-2}$$
$$w = -\operatorname{sgn}(\lambda^\mathsf{T} BWx)\sqrt{u_{\max}^2/\|p\|^2 - a_\mathsf{r}^2}\, Wx$$

and $(\lambda, x)$ = solve a two-point BVP

- $a_\mathsf{r}$= radial accel.
- $w$= tangential accel.
- Bang-Bang control
- Can be computed by solving BVP offline

## Computing Optimal Undetectable Attacks

$$\begin{aligned} \max_{u} \quad & \|p(T) - p_{\mathsf{n}}(T)\| \\ \text{s.t.} \quad & \dot{x} = Ax + Bu \\ & u = \text{undetectable} \\ & \|u\| \le u_{\max} \end{aligned}$$




For single integrator robots ($A = 0$), **BVP can be solved explicitly**:

Optimal solutions are:

$$u = a_{\mathsf{r}}\, p + w$$

where $w^{\mathsf{T}} p = 0$, and

$$a_{\mathsf{r}} = u_{\mathsf{n}}^{\mathsf{T}} p_{\mathsf{n}} \|p\|^{-2}$$

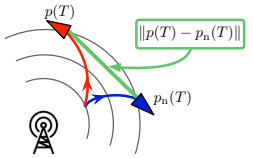
$$w = -\gamma \sqrt{u_{\max}^2 / \|p\|^2 - a_{\mathsf{r}}^2}\, W x$$

$\phi \leftarrow$ Angle between $x(t)$ and $-x_{\mathsf{n}}(T)$;
**if** $\phi = 0$ **then**
  $\gamma \leftarrow 0$;
**else if** $0 < \phi \le \pi$ **then**
  $\gamma \leftarrow 1$;
**else**
  $\gamma \leftarrow -1$;

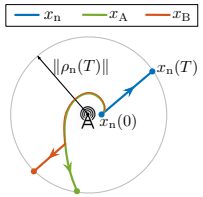


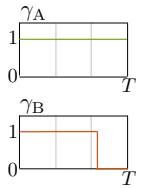
## Computing Optimal Undetectable Attacks

$$\begin{aligned} \max_{u} \quad & \|p(T) - p_{\mathsf{n}}(T)\| \\ \text{s.t.} \quad & \dot{x} = Ax + Bu \\ & u = \text{undetectable} \\ & \|u\| \le u_{\max} \end{aligned}$$




For single integrator robots ($A = 0$), **BVP can be solved explicitly**:



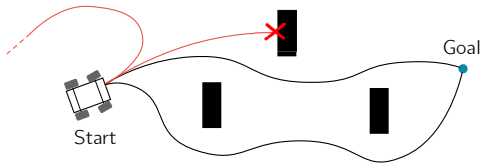




$\phi \leftarrow$ Angle between $x(t)$ and $-x_{\mathsf{n}}(T)$;
**if** $\phi = 0$ **then**
  $\gamma \leftarrow 0$;
**else if** $0 < \phi \le \pi$ **then**
  $\gamma \leftarrow 1$;
**else**
  $\gamma \leftarrow -1$;

State-feedback law



## Can We Make the Navigation Secure?




1. Can an attacker modify the trajectory and escape detectability?

✓ Yes, under appropriate design

2. Can we design trajectories are secure?

✓ Yes, there is a tradeoff between security and control energy

A **Secure Trajectory** is:

1. Navigate from start to destination
2. Any attack can be detected ($\nexists$ undetectable attacks)



## Designing Controls that are Secure

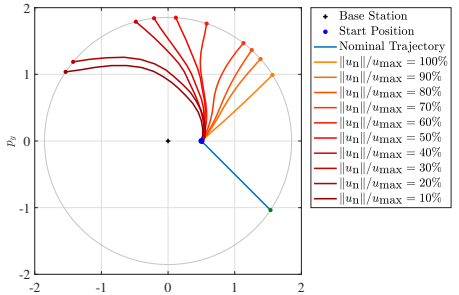
Assume max. acceleration is bounded: $\|u_{\mathsf{n}}\| \le u_{\max}$

A trajectory is secure **if and only if**

$$u_{\mathsf{n}} = \kappa \frac{p_{\mathsf{n}}}{\|p_{\mathsf{n}}\|} u_{\max} \qquad \kappa : \mathbb{R}_{\ge 0} \to \{-1, 1\}$$

- State-feedback law
- Maximum energy at all times

What if we chose **controls that are not secure**?



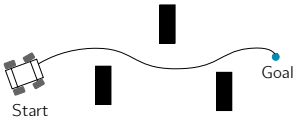

There is a tradeoff between control energy and security

Existence of undetectable attacks depends upon the nominal inputs

## Computing Minimum-Time Secure Trajectories

Given initial and final positions $p_{\mathsf{I}}$, $p_{\mathsf{F}}$

$$\begin{aligned} \min_{\kappa,T} \quad & T \;+\; \|p_{\mathsf{n}}(T) - p_{\mathsf{F}}\| \\ \text{s.t.} \quad & \dot{x}_{\mathsf{n}} = Ax_{\mathsf{n}} + Bu_{\mathsf{n}} \\ & u_{\mathsf{n}} = \kappa \frac{p_{\mathsf{n}}}{\|p_{\mathsf{n}}\|} u_{\max} \end{aligned}$$




Optimal solutions satisfy:

$$\kappa^* = -\operatorname{sgn}(\lambda^{\mathsf{T}} B p_{\mathsf{n}}), \qquad T^* = \xi$$

where $(\lambda, p_{\mathsf{n}}, \xi)$ = solve a two-point BVP

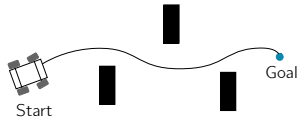
- Bang-Bang control
- Open-loop input
- Computed offline



## Computing Minimum-Time Secure Trajectories

Given initial and final positions $p_{\mathsf{I}}$, $p_{\mathsf{F}}$

$$\begin{aligned} \min_{\kappa,T} \quad & T \;+\; \|p_{\mathsf{n}}(T) - p_{\mathsf{F}}\| \\ \text{s.t.} \quad & \dot{x}_{\mathsf{n}} = Ax_{\mathsf{n}} + Bu_{\mathsf{n}} \\ & u_{\mathsf{n}} = \kappa \frac{p_{\mathsf{n}}}{\|p_{\mathsf{n}}\|} u_{\max} \end{aligned}$$



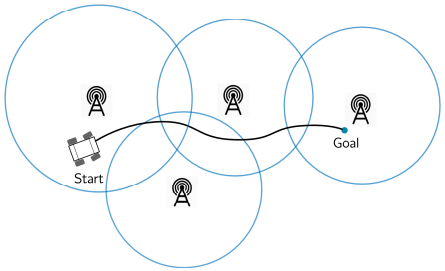

**Emerging Difficulty:**

What are the configurations $\mathcal{S}$ that are reachable via secure inputs?

1. In general: no systematic way to characterize $\mathcal{S}$
2. Single-Integrator dynamics: $\mathcal{S} = \{x \;:\; x = \alpha x_{\mathsf{n}}(0), \alpha \in \mathbb{R}_{>0}\}$



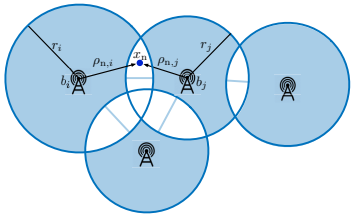
## Secure Navigation: Waypoint Design




How do we plan trajectories when RSSI readings change over time?



## Existence of Undetectable Attacks



- If robot is in the range $r_i$ of station $i$

$$\|x_{\mathsf{n}} - b_i\| \leq r_i$$

- Then, $i$-th RSSI reading is available

$$y^{\mathsf{RSSI}}_{\mathsf{n},i} = \|x_{\mathsf{n}} - b_i\|^2, \quad y^{\mathsf{GNSS}}_{\mathsf{n}} = x_{\mathsf{n}}$$

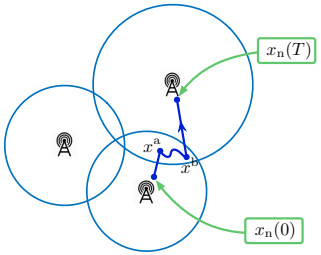
There exist undetectable attacks **only if**

$$\operatorname{Rank}(\begin{bmatrix} x_{\mathsf{n}} - b_{i_1}, & x_{\mathsf{n}} - b_{i_2}, & \cdots & x_{\mathsf{n}} - b_{i_s} \end{bmatrix}) < 2$$

at some time $t$

## Secure Navigation: Waypoint Design

**Given:** $x_{\mathrm{n}}(0)$ and $x_{\mathrm{n}}(T)$
**Goal:** Navigate from $x_{\mathrm{n}}(0)$ to $x_{\mathrm{n}}(T)$




1. Chose $x^{\mathrm{a}}_{\mathrm{n}}$ s.t.
   - $\operatorname{Rank} \mathcal{R}(x^{\mathrm{a}}_{\mathrm{n}}) \geq 2$
   - $x^{\mathrm{a}}_{\mathrm{n}} \in \mathcal{S}(x_{\mathrm{n}}(0))$
2. Navigate from $x_{\mathrm{n}}(0)$ to $x^{\mathrm{a}}_{\mathrm{n}}$ via secure trajectories
3. Chose $x^{\mathrm{b}}_{\mathrm{n}}$ s.t.
   - $\operatorname{Rank} \mathcal{R}(x^{\mathrm{b}}_{\mathrm{n}}) \geq 2$
   - $x^{\mathrm{b}}_{\mathrm{n}} \in \mathcal{S}(x_{\mathrm{n}}(T))$
4. Navigate from $x^{\mathrm{a}}_{\mathrm{n}}$ to $x^{\mathrm{b}}_{\mathrm{n}}$
5. Navigate from $x^{\mathrm{b}}_{\mathrm{n}}$ to $x_{\mathrm{n}}(T)$ via secure trajectories



## Summary

Two emerging questions:

1. Can an attacker modify the trajectory and escape detectability?

✓ Yes, under appropriate design

2. Can we design trajectories that ensure detectability of attacks?

✓ Yes, there is a tradeoff between security and control energy

Control input design affects security in systems with nonlinear dynamics

Generalizations

- Methods applicable to any system with nonlinear dynamics
- Challenge in characterizing secure reachable sets