THE UNIVERSITY OF TEXAS AT AUSTIN
RADIONAVIGATION LABORATORY

Secure Perception for Autonomous Systems

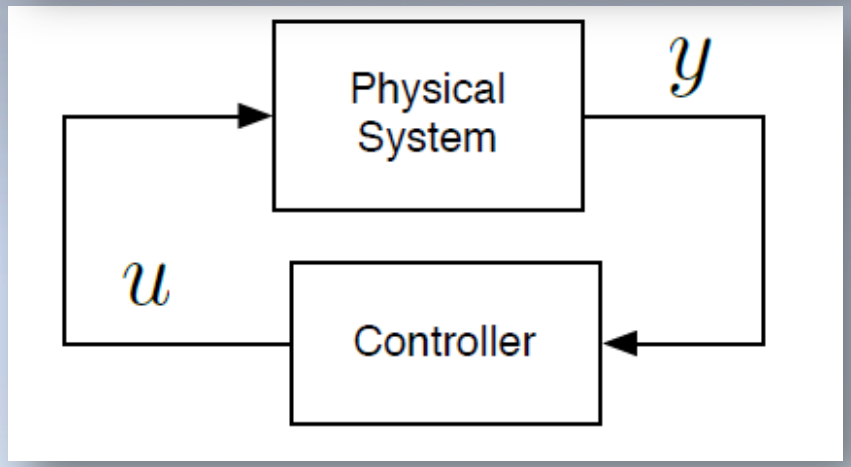
Todd Humphreys | Aerospace Engineering
The University of Texas at Austin

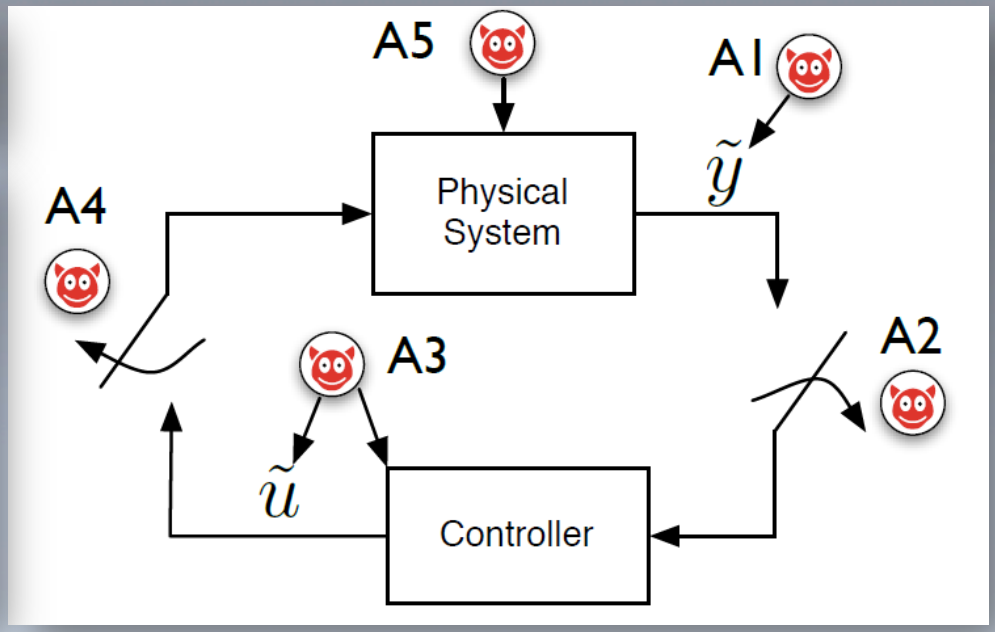
NSF PI Meeting | November 16, 2015

Autonomous Control System Security

Secure Control: Towards Survivable Cyber-Physical Systems*

Alvaro A. Cárdenas Saurabh Amin Shankar Sastry
University of California, Berkeley 2008





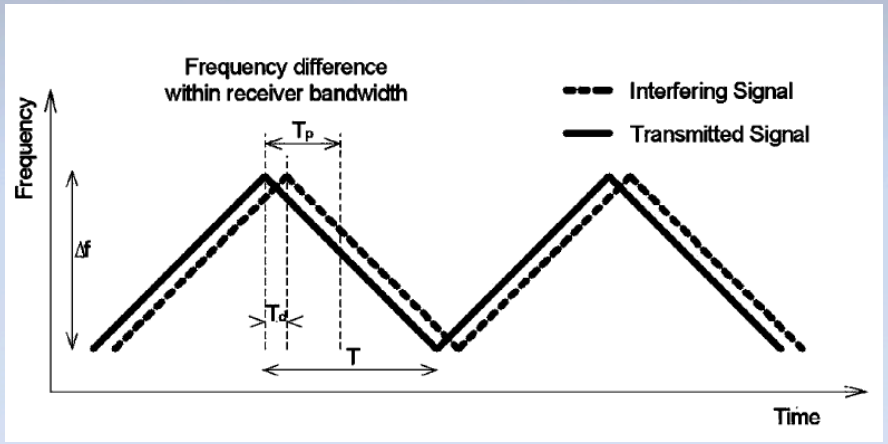
The general secure control problem envisions arbitrary manipulation of y and u (e.g, deception and DoS attacks)

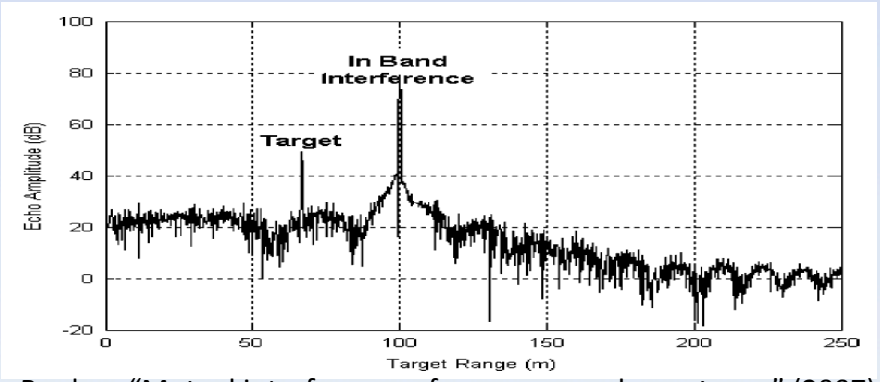
The UT Radionavigation Laboratory's approach to the secure control problem:

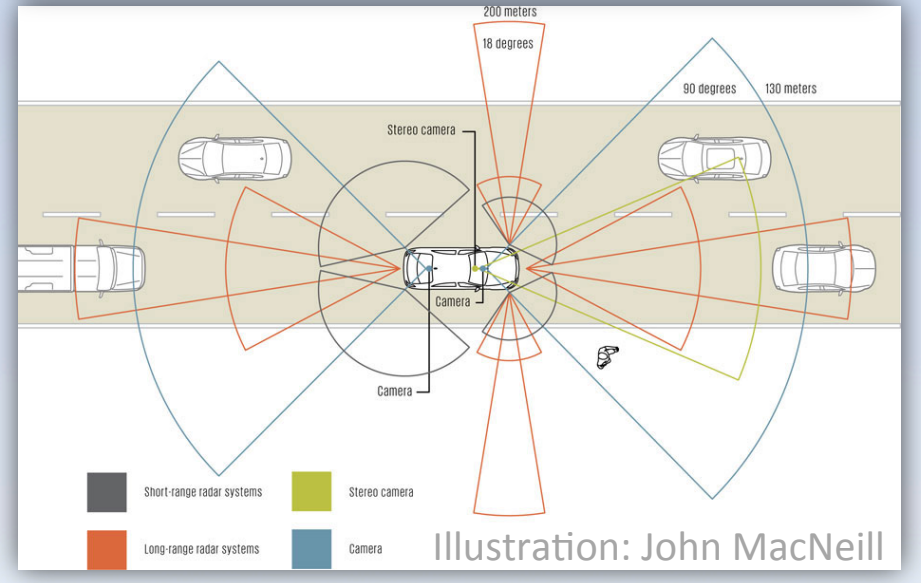
Focus on *field attacks:* attacks on the physical fields (e.g., electromagnetic, acoustic, pressure, etc.) measured by system sensors – especially navigation and timing system sensors.

Example: Adaptive Cruise Control

The security of current automotive radar systems against deliberate attack is weak because the FMCW waveform is almost perfectly predictable







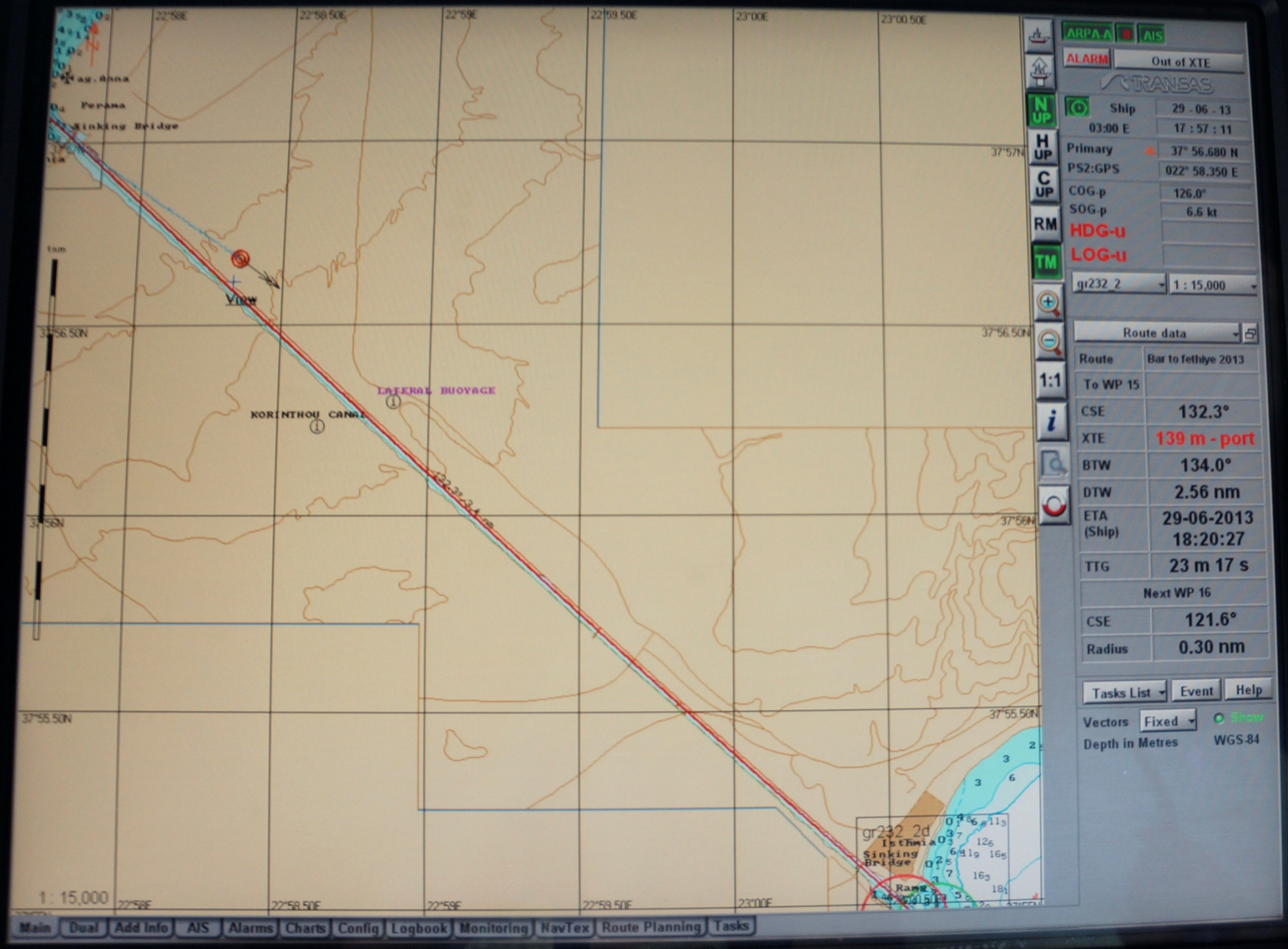
Booker, "Mutual interference of mm-wave radar systems." (2007)

Accurate and trustworthy perception is perhaps *the most difficult challenge* of autonomous vehicles. Lidar, radar, and GPS must all be secured against interference and deception.

Shepard, Bhatti, Humphreys, Fansler, "Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks," Proc. ION GNSS, Nashville, TN, 2012

Follow-on demonstration:
From onset of attack to crash in 20 seconds


WHITE ROSE OF DRACHS


ARPA A
AIS
ALARM
Out of XTE
TRANSAS
Ship
29 - 06 - 13
03:00 E
17 : 57 : 11
Primary
37° 56.680 N
PS2:GPS
022° 58.350 E
COG-p
126.0°
SOG-p
6.6 kt
HDG-u
LOG-u
gr232_2
1 : 15,000
Route data
Route
Bar to fethiye 2013
To WP 15
CSE
132.3°
XTE
139 m - port
BTW
134.0°
DTW
2.56 nm
ETA (Ship)
29-06-2013 18:20:27
TTG
23 m 17 s
Next WP 16
CSE
121.6°
Radius
0.30 nm
Tasks List
Event
Help
Vectors
Fixed
Show
Depth in Metres
WGS-84
N UP
H UP
C UP
RM
TM
1:1
LATERAL BUOYAGE
KORINTHOU CANAL
VIEW
Nav.Aana
Perama
Sinking Bridge
gr232_2d
Isthmia
Sinking Bridge
1 : 15,000
Main
Dual
Add Info
AIS
Alarms
Charts
Config
Logbook
Monitoring
NavTex
Route Planning
Tasks

Three recent developments ...

(1) Cost-Ranked GNSS Attack/Detection Matrix

TABLE I: Cost-Ranked Matrix of GNSS Spoofing Attack and Detection Techniques

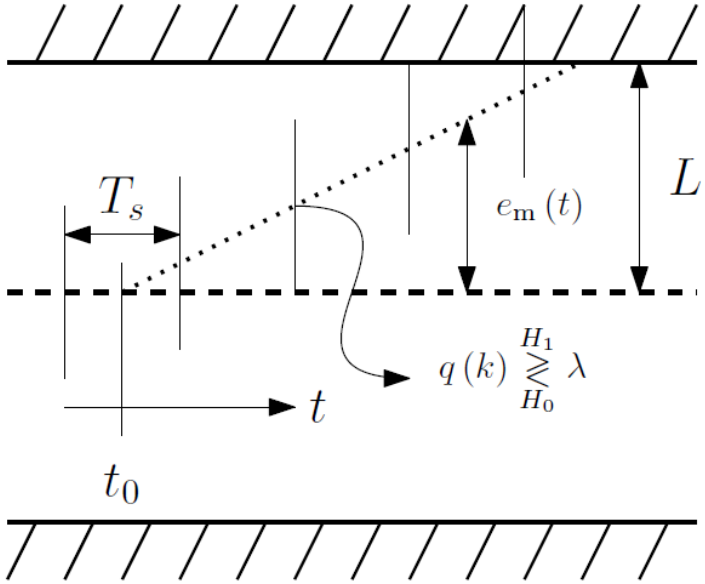
Detection Techniques	Attack Techniques												
	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13
D1	X	X	X	X	X	X	X	X	X	X	X	X	X
D2	~	✓	X	X	~	X	X	X	X	X	X	X	X
D3	~	~	~	~	~	X	X	~	~	~	~	X	X
D4	~	✓	~	~	~	~	~	~	~	~	~	~	~
D5	✓	✓	✓	✓	✓	~	~	✓	✓	✓	✓	~	~
D6	X	✓	✓	X	X	✓	X	✓	✓	X	X	✓	X
D7	X	✓	✓	~	X	✓	~	✓	✓	~	X	✓	~
D8	X	✓	✓	~	X	✓	~	✓	✓	~	X	✓	~
D9	~	✓	✓	✓	~	✓	✓	✓	✓	✓	~	✓	✓
D10	✓	✓	✓	✓	✓	✓	✓	✓	~	~	~	~	~
D11	✓	✓	✓	✓	✓	✓	✓	X	~	~	~	~	~
D12	X	✓	✓	~	X	✓	~	✓	✓	~	X	✓	~
D13	X	✓	✓	~	X	✓	~	✓	✓	~	X	✓	~

	Attack Techniques Key
A1	Meaconing, single RX ant., single TX ant.
A2	Open-loop signal simulator
A3	RX/SP, single TX ant., no SCER
A4	RX/SP, single TX ant., SCER
A5	Meaconing, multi. RX ants., single TX ant.
A6	Nulling RX/SP, single TX ant., no SCER
A7	Nulling RX/SP, single TX ant., SCER
A8	RX/SP, single TX ant., sensing of victim ant. motion
A9	RX/SP, multi. TX ants., no SCER
A10	RX/SP, multi. TX ants., SCER
A11	Meaconing, multi. RX ants., multi. TX ants.
A12	Nulling RX/SP, multi. TX ants., no SCER
A13	Nulling RX/SP, multi. TX ants., SCER

	Detection Techniques Key
D1	Pseudorange-based RAIM
D2	Observables and RPM
D3	Correlation function distortion monitoring
D4	Drift monitoring (clock offset, IMU/position)
D5	Observables, RPM, distortion, and drift monitoring
D6	NMA*
D7	NMA* and SCER detection
D8	Delayed symmetric-key SSSC*
D9	NMA*, SCER detection, RPM, and drift monitoring
D10	Multiple RX antennas
D11	Moving RX antenna
D12	Dual-RX keyless correlation of unknown SSSC codes
D13	Symmetric-key SSSC* [e.g., P(Y) equiv.]

Psiaki & Humphreys, "GNSS Spoofing and Detection," IEEE Proc. (invited), submitted for review

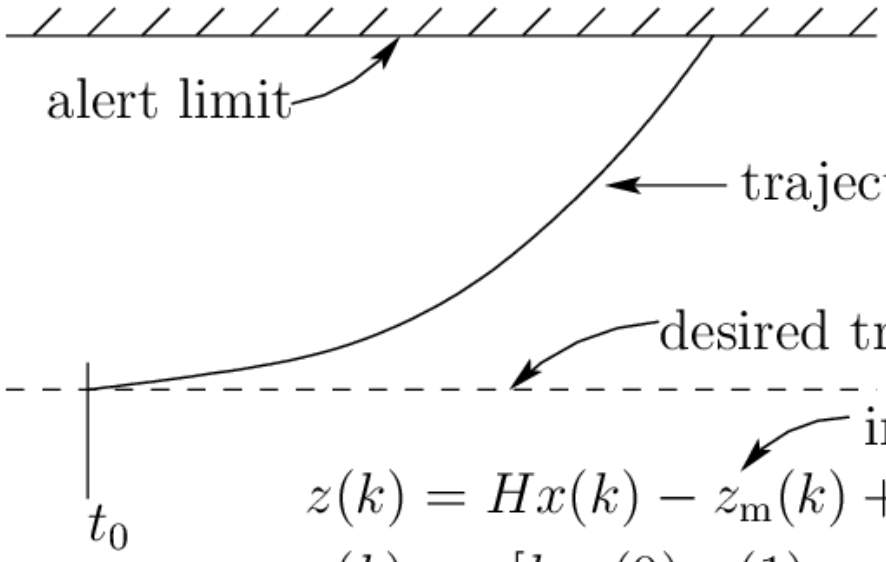
(2) Estimator-Level Detection of Position Deception: Optimization of Time Between Measurements



Measurement interval can be optimized by solving a minimax problem on the mean integrity risk

Bhatti & Humphreys, "Hostile control of ships via false GPS signals: Demonstration and Detection," *Navigation*, submitted for review

(3) Open Problem: Optimal Detection Statistic



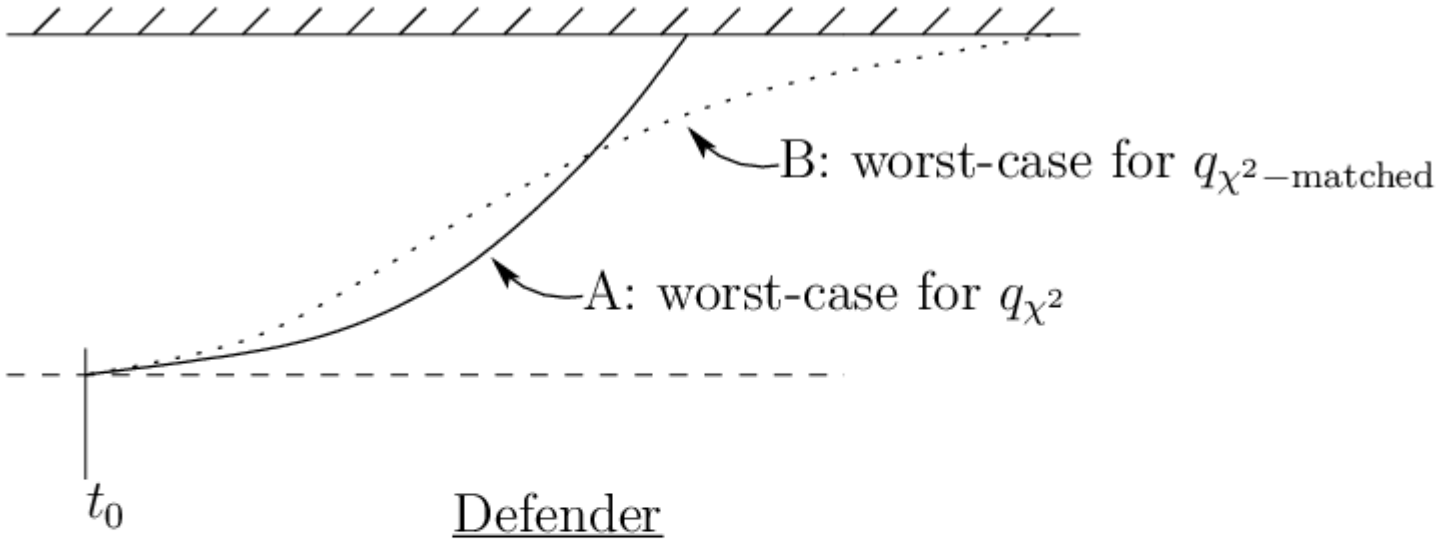
$$z(k) = Hx(k) - z_{\mathrm{m}}(k) + w(k)$$

$$q(k) = q[k, z(0), z(1), ..., z(k)]$$

$$\text{e.g., } q(k) = \sum_{j=k-K}^{k} \nu^T(j) S^{-1}(j) \nu(j) \leftarrow \chi^2 \text{ statistic}$$

Q: Is there a saddle point equilibrium for the differential game involving the induced trajectory and the detection statistic?

(3) Progress: Saddle Point "In the Large"



Defender

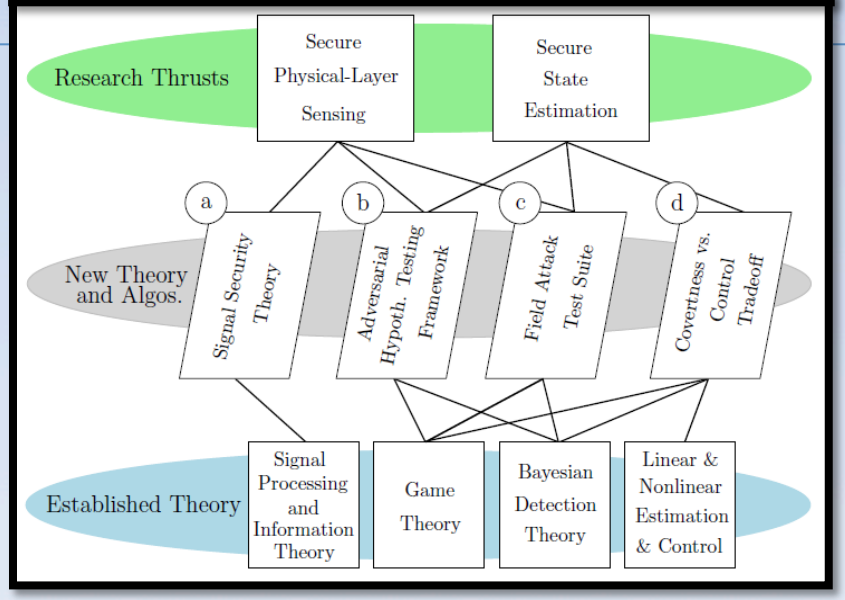
Attacker	q_{χ^2}	$q_{\chi^2-\text{matched}}$
A	0.7	0.5
B	0.6	0.9

cost to defender in terms of integrity risk

Secure Perception for Autonomous Systems

Challenge:

Ensure that autonomous systems are secure against sensor deception



Scientific Impact:

- Theoretical basis for measuring security of time-bearing signals
- Framework for adversarial hypothesis testing
- Suite of detection tests

Solution:

- Physics of attack imposes fundamental difficulties on attack
- Physical layer: Exploit interaction with authentic signal
- State estimation: Optimize detection test for attack

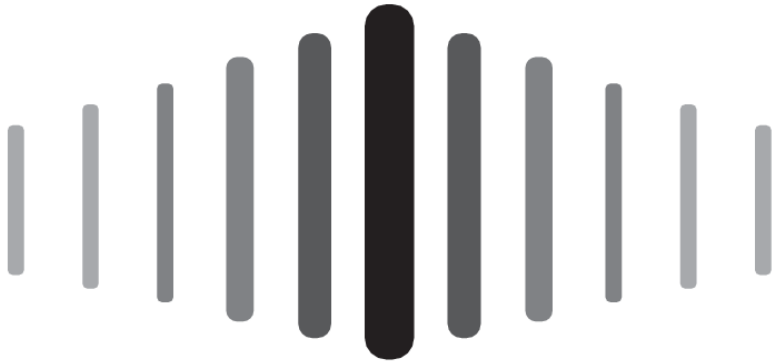
Broader Impact:

- Secure perception crucial for autonomous vehicles to safely enter airspace, roads, waterways across the globe
- $100B market depends on trustworthy autonomy
- "Machine Games" testbed being developed at UT will lay bare problem of secure perception to next generation of engineers

Focus: Secure navigation, timing, and collision avoidance

NSF CAREER award grant 1454474

PI: Todd Humphreys
The University of Texas at Austin



THE UNIVERSITY OF TEXAS AT AUSTIN

RADIONAVIGATION LABORATORY

radionavlab.ae.utexas.edu