Recent Advances in Safety, Optimization, and Control

Ricardo Sanfelice
Department Electrical and Computer Engineering
University of California

CoE Review @ Duke University - December 7, 2023

Outline of Recent Results

1. **Safety**
   - Safety Certificates
     ACC23a, CDC23a, CDC23b,
     TAC (provisionally accepted) w/ Warren Dixon
   - Applications of Safety to Security
     CCTA22a and ACC23b
2. **Optimization**
   - Dynamical systems approach
     ACC23c, Optimization journal (almost ready)
     Automatica 2023, ACC23d w/ Matt Hale
   - Optimization with Computational Constraints
     CPSWeek-IoT 23 Workshop
3. **Motion Planning for Hybrid Systems**
   - RRT for feasibility and optimality
     CDC22, CCTA22b, CDC23c, ADHS24 (work in progress)

Outline of Recent Results

1. **Safety**
   - Safety Certificates

     ACC23a, CDC23a, CDC23b,

     TAC (provisionally accepted) w/ Warren Dixon
   - Applications of Safety to Security

     CCTA22a and ACC23b
2. **Optimization**
   - Dynamical systems approach

     ACC23c, Optimization journal (almost ready)

     Automatica 2023, ACC23d w/ Matt Hale
   - Optimization with Computational Constraints

     CPSWeek-IoT 23 Workshop
3. **Motion Planning for Hybrid Systems**

New MS student (Ryan Rodriguez) and postdoc (Himadri Basu)

Visited S. Phillips at AFRL/RV

Released new version of Hybrid Equations Toolbox (v3.0) for Matlab

UF UNIVERSITY of FLORIDA · Duke UNIVERSITY · TEXAS The University of Texas at Austin · UC SANTA CRUZ

An Observer-based Switching Algorithm for Safety under Sensor Denial-of-Service Attacks

Santiago J. Leudo, Kunal Garg*, Ricardo G. Sanfelice, and Alvaro A. Cardenas

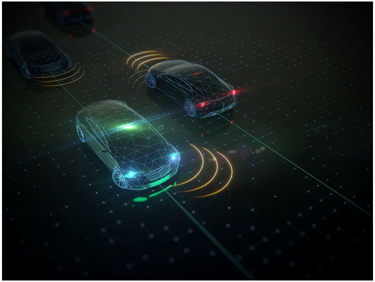
University of California, Santa Cruz, CA
*Massachusetts Institute of Technology, Cambridge, MA

CoE Review @ Duke University

December 7, 2023

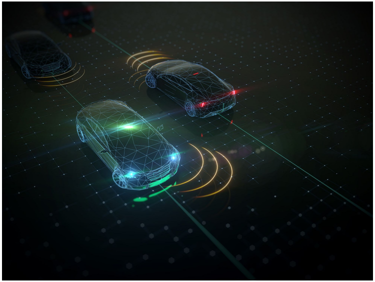
HYBRID SYSTEMS LABORATORY

Security of a CPS from a Control-Theoretic Perspective



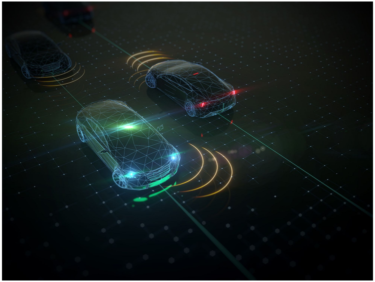
- Attacks: Sensor data.

Security of a CPS from a Control-Theoretic Perspective



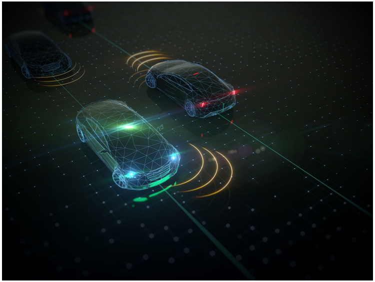
- Attacks: Sensor data.
- Attackers can disable the transmission of signals between devices: a Denial of Service (DoS) attack.

Security of a CPS from a Control-Theoretic Perspective



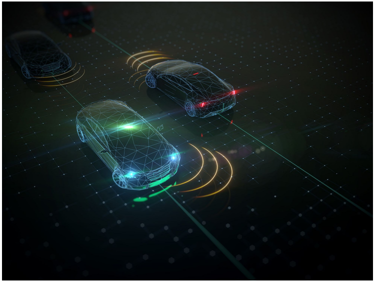
- Attacks: Sensor data.
- Attackers can disable the transmission of signals between devices: a Denial of Service (DoS) attack.
- Potential violation of safety requirements.

Security of a CPS from a Control-Theoretic Perspective



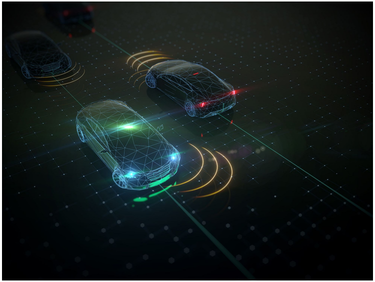
Goal: Keep a system's trajectories in a safe set even under DoS attacks.

Security of a CPS from a Control-Theoretic Perspective



Goal: Keep a system's trajectories in a safe set even under DoS attacks.
Approach: Control scheme to bound the impact of an attack based on the **information available** to guarantee **safety**.

Security of a CPS from a Control-Theoretic Perspective



Goal: Keep a system's trajectories in a safe set even under DoS attacks.
Approach: Control scheme to bound the impact of an attack based on the **information available** to guarantee **safety**.
Assumption: **Finite duration** attacks, succeeded by intervals without attacks.

Safety Definitions

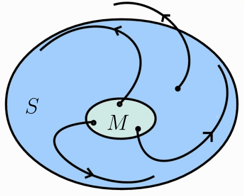
Consider the nonlinear system with state x and output y:

$$\mathcal{F}_n : \begin{cases} \dot{x} & = & F(t,x) \\ y & = & H(t,x) \end{cases}$$

- F is the *flow map*
- H is the *output map*

Safety Definitions

Consider the nonlinear system with state x and outp



$$\mathcal{F}_n : \begin{cases} \dot{x} &= F(t,x) \\ y &= H(t,x) \end{cases}$$

- F is the *flow map*
- H is the *output map*

Definition: (Conditional invariance)

A closed set $S \subset \mathbb{R}^n$ is said to be *conditionally invariant* for $\mathcal{F}_n$ with respect to $M \subset S$ if, for each $x_0 \in M$, any solution to $\mathcal{F}_n$ from x_0 remains in S.

Consider the nonlinear system with state x and output y:

$$\mathcal{F}_n : \begin{cases} \dot{x} &= F(t,x) \\ y &= H(t,x) \end{cases}$$

- F is the *flow map*
- H is the *output map*

Definition: (Conditional invariance)

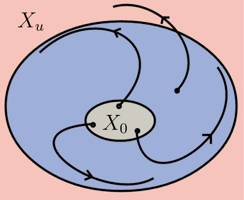
A closed set $S \subset \mathbb{R}^n$ is said to be *conditionally invariant* for $\mathcal{F}_n$ with respect to $M \subset S$ if, for each $x_0 \in M$, any solution to $\mathcal{F}_n$ from x_0 remains in S.

Definition: (Safety)

The system $\mathcal{F}_n$ is said to be *safe* with respect to (X_0, X_u), with $X_0 \subset \mathbb{R}^n \setminus X_u$, if for each $x_0 \in X_0$, any solution to $\mathcal{F}_n$ from x_0 remains in $\mathbb{R}^n \setminus X_u$.

Safety Definitions

Consider the nonlinear system with state x and outp



$$\mathcal{F}_n : \begin{cases} \dot{x} &= F(t,x) \\ y &= H(t,x) \end{cases}$$

- F is the *flow map*
- H is the *output map*

Definition: (Conditional invariance)

A closed set $S \subset \mathbb{R}^n$ is said to be *conditionally invariant* for $\mathcal{F}_n$ with respect to $M \subset S$ if, for each $x_0 \in M$, any solution to $\mathcal{F}_n$ from x_0 remains in S.

Definition: (Safety)

The system $\mathcal{F}_n$ is said to be *safe* with respect to (X_0, X_u), with $X_0 \subset \mathbb{R}^n \setminus X_u$, if for each $x_0 \in X_0$, any solution to $\mathcal{F}_n$ from x_0 remains in $\mathbb{R}^n \setminus X_u$.

System Model

Consider the LTI system with state x, input u and output y:

$$\mathcal{F} : \begin{cases} \dot{z} &= Ax + Bu \\ y &= Cx \end{cases}$$

where $C = \begin{bmatrix} \tilde{C} \\ \bar{C} \end{bmatrix}$.

System Model

Consider the LTI system with state x, input u and output y:

$$\mathcal{F} : \begin{cases} \dot{z} & = & Ax + Bu \\ y & = & Cx \end{cases}$$

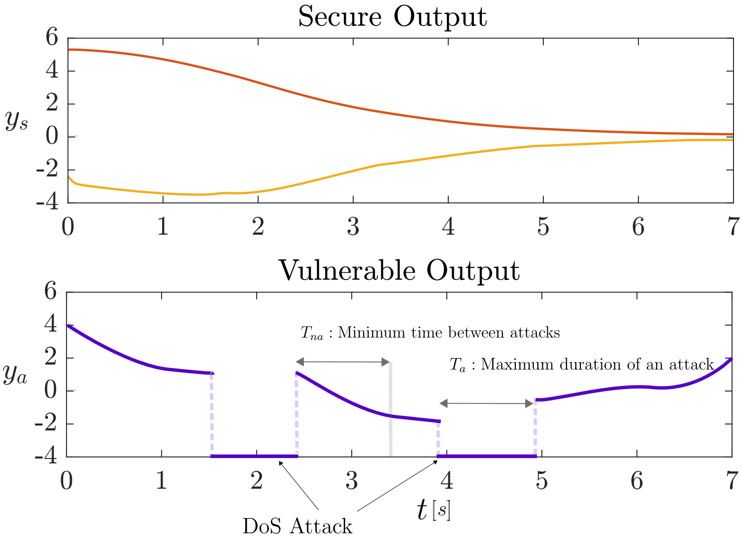
where $C = \begin{bmatrix} \tilde{C} \\ \bar{C} \end{bmatrix}$.

Attack Model (Denial-of-Service (DoS))

The *measured* output: $\bar{y} = \begin{bmatrix} y_s \\ y_a \end{bmatrix}$, where $y_s = \tilde{C}x$, and, along a solution $t \mapsto x(t)$,

$$y_a(t) = \begin{cases} \bar{C}x(t) & \text{if } t \notin \mathcal{T}_a, \\ Y(t, x(t)) & \text{if } t \in \mathcal{T}_a \end{cases}$$

- $\mathcal{T}_a$: the set of times of attack (known)


Secure Output
y_s
6
4
2
0
-2
-4
0
1
2
3
4
5
6
7
Vulnerable Output
y_a
6
4
2
0
-2
-4
T_{na} : Minimum time between attacks
T_a : Maximum duration of an attack
0
1
2
3
4
5
6
7
$t\,[s]$
DoS Attack

Design an algorithm to render the set S conditionally invariant for the system $\mathcal{F}$ with respect to the set X_0 using output measurements only.

Safety Problem

1. Find a set of initial states $X_0 \subset S$, and

Design an algorithm to render the set S conditionally invariant for the system $\mathcal{F}$ with respect to the set X_0 using output measurements only.

Safety Problem

1. Find a set of initial states $X_0 \subset S$, and
2. Design a control law κ that uses the measured output $\bar{y} = (y_s, y_s)$

Design an algorithm to render the set S conditionally invariant for the system $\mathcal{F}$ with respect to the set X_0 using output measurements only.

Safety Problem

1. Find a set of initial states $X_0 \subset S$, and
2. Design a control law κ that uses the measured output $\bar{y} = (y_s, y_s)$

such that, for each $x_0 \in X_0$, $x(0) = x_0$ implies $x(t) \in S$ for all $t \geq 0$.

Problem Statement

Design an algorithm to render the set S conditionally invariant for the system $\mathcal{F}$ with respect to the set X_0 using output measurements only.

Safety Problem

1. Find a set of initial states $X_0 \subset S$, and
2. Design a control law κ that uses the measured output $\bar{y} = (y_s, y_s)$

such that, for each $x_0 \in X_0$, $x(0) = x_0$ implies $x(t) \in S$ for all $t \geq 0$.

Solution Approach:

Design an observer-based feedback law that induces conditional invariance of S with respect to X_0 using the measured output $\bar{y}$.

Problem Statement

Design an algorithm to render the set S conditionally invariant for the system $\mathcal{F}$ with respect to the set X_0 using output measurements only.

Safety Problem

1. Find a set of initial states $X_0 \subset S$, and
2. Design a control law κ that uses the measured output $\bar{y} = (y_s, y_s)$

such that, for each $x_0 \in X_0$, $x(0) = x_0$ implies $x(t) \in S$ for all $t \geq 0$.

Solution Approach:
Design an observer-based feedback law that induces conditional invariance of S with respect to X_0 using the measured output $\bar{y}$.

- System output **under attack** $\rightarrow$ the observer uses the **non-attacked output** components.

Problem Statement

Design an algorithm to render the set S conditionally invariant for the system $\mathcal{F}$ with respect to the set X_0 using output measurements only.

Safety Problem

1. Find a set of initial states $X_0 \subset S$, and
2. Design a control law κ that uses the measured output $\bar{y} = (y_s, y_s)$

such that, for each $x_0 \in X_0$, $x(0) = x_0$ implies $x(t) \in S$ for all $t \geq 0$.

Solution Approach:
Design an observer-based feedback law that induces conditional invariance of S with respect to X_0 using the measured output $\bar{y}$.

- System output **under attack** $\rightarrow$ the observer uses the **non-attacked output** components.
- System output **not attacked** $\rightarrow$ the observer uses the **complete output** vector.

Solution Approach

1. Design functions g_1 and g_2 for the observer

$$\dot{\hat{x}} = \begin{cases} A\hat{x} + Bu + g_1(Cx, C\hat{x}) & \text{if} \quad t \notin \mathcal{T}_a, \\ A\hat{x} + Bu + g_2(\tilde{C}x, C\hat{x}) & \text{if} \quad t \in \mathcal{T}_a, \end{cases}$$

Solution Approach

1. Design functions g_1 and g_2 for the observer

$$\dot{\hat{x}} = \begin{cases} A\hat{x} + Bu + g_1(Cx, C\hat{x}) & \text{if} \quad t \notin \mathcal{T}_a, \\ A\hat{x} + Bu + g_2(\tilde{C}x, C\hat{x}) & \text{if} \quad t \in \mathcal{T}_a, \end{cases}$$

2. design functions κ_1 and κ_2 for the observer-based feedback law

$$\kappa(t, \hat{x}, \bar{y}) = \begin{cases} \kappa_1(\hat{x}, \bar{y}) & \text{if} \quad t \notin \mathcal{T}_a, \\ \kappa_2(\hat{x}, \bar{y}) & \text{if} \quad t \in \mathcal{T}_a, \end{cases}$$

Solution Approach

1. Design functions g_1 and g_2 for the observer

$$\dot{\hat{x}} = \begin{cases} A\hat{x} + Bu + g_1(Cx, C\hat{x}) & \text{if} \quad t \notin \mathcal{T}_a, \\ A\hat{x} + Bu + g_2(\tilde{C}x, C\hat{x}) & \text{if} \quad t \in \mathcal{T}_a, \end{cases}$$

2. design functions κ_1 and κ_2 for the observer-based feedback law

$$\kappa(t, \hat{x}, \bar{y}) = \begin{cases} \kappa_1(\hat{x}, \bar{y}) & \text{if} \quad t \notin \mathcal{T}_a, \\ \kappa_2(\hat{x}, \bar{y}) & \text{if} \quad t \in \mathcal{T}_a, \end{cases}$$

3. and, compute
   - X_0: set of initial states,
   - $\hat{X}_0$: set of estimates before an attack,
   - $\tilde{X}$: set of estimates after an attack,

Solution Approach

1. Design functions g_1 and g_2 for the observer

$$\dot{\hat{x}} = \begin{cases} A\hat{x} + Bu + g_1(Cx, C\hat{x}) & \text{if} \quad t \notin \mathcal{T}_a, \\ A\hat{x} + Bu + g_2(\tilde{C}x, C\hat{x}) & \text{if} \quad t \in \mathcal{T}_a, \end{cases}$$

2. design functions κ_1 and κ_2 for the observer-based feedback law

$$\kappa(t, \hat{x}, \bar{y}) = \begin{cases} \kappa_1(\hat{x}, \bar{y}) & \text{if} \quad t \notin \mathcal{T}_a, \\ \kappa_2(\hat{x}, \bar{y}) & \text{if} \quad t \in \mathcal{T}_a, \end{cases}$$

3. and, compute
   - X_0: set of initial states,
   - $\hat{X}_0$: set of estimates before an attack,
   - $\tilde{X}$: set of estimates after an attack,

- If $x(0) \in X_0, \hat{x}(0) \in \hat{X}_0(x_0) \Rightarrow x(t) \in S$ during attacks.

Solution Approach

1. Design functions g_1 and g_2 for the observer

$$\dot{\hat{x}} = \begin{cases} A\hat{x} + Bu + g_1(Cx, C\hat{x}) & \text{if} \quad t \notin \mathcal{T}_a, \\ A\hat{x} + Bu + g_2(\tilde{C}x, C\hat{x}) & \text{if} \quad t \in \mathcal{T}_a, \end{cases}$$

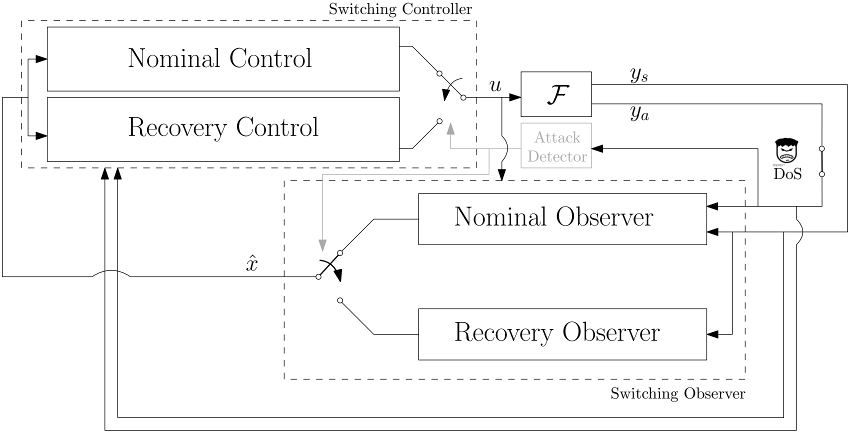
2. design functions κ_1 and κ_2 for the observer-based feedback law

$$\kappa(t, \hat{x}, \bar{y}) = \begin{cases} \kappa_1(\hat{x}, \bar{y}) & \text{if} \quad t \notin \mathcal{T}_a, \\ \kappa_2(\hat{x}, \bar{y}) & \text{if} \quad t \in \mathcal{T}_a, \end{cases}$$

3. and, compute
    - X_0: set of initial states,
    - $\hat{X}_0$: set of estimates before an attack,
    - $\tilde{X}$: set of estimates after an attack,

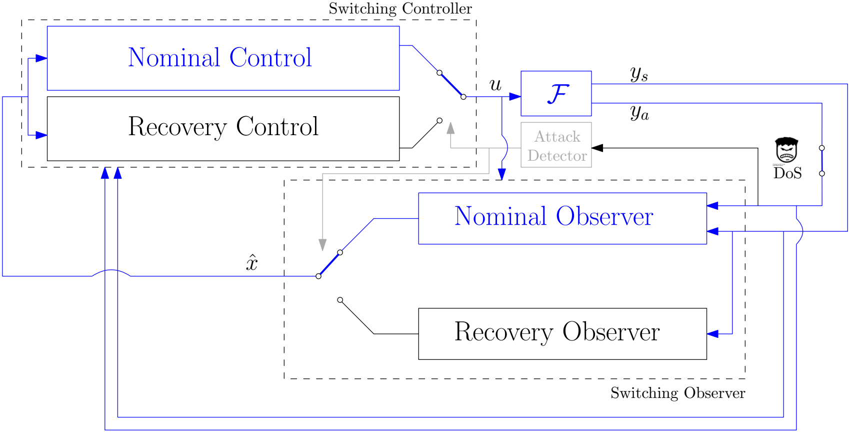
- If $x(0) \in S, \hat{x}(0) \in \tilde{X} \Rightarrow x(t) \in S$ when no attacks and belongs to X_0 at the beginning of the next attack.

Solution Approach

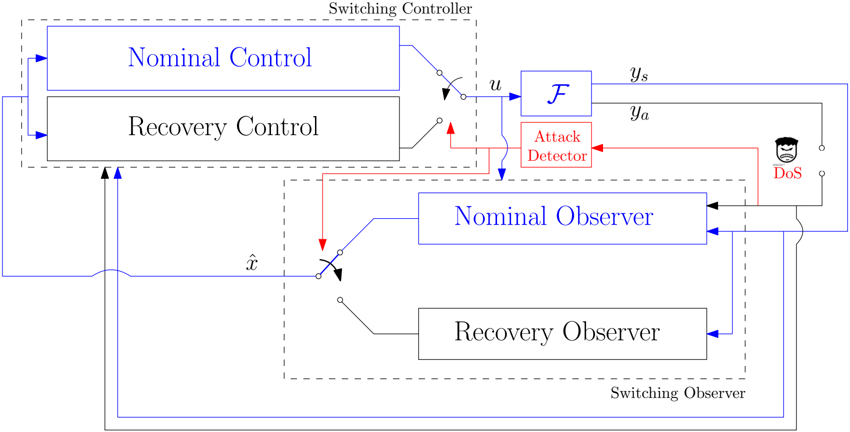


Attack detector [Phillips et al - CDC 17]

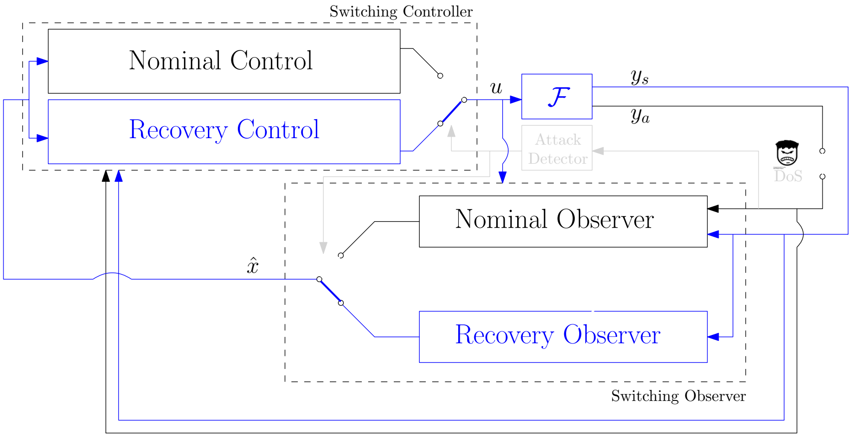
Solution Approach



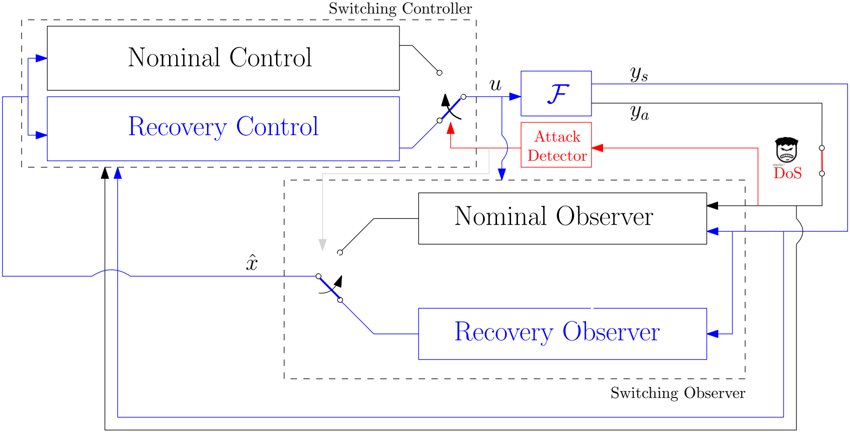
Solution Approach



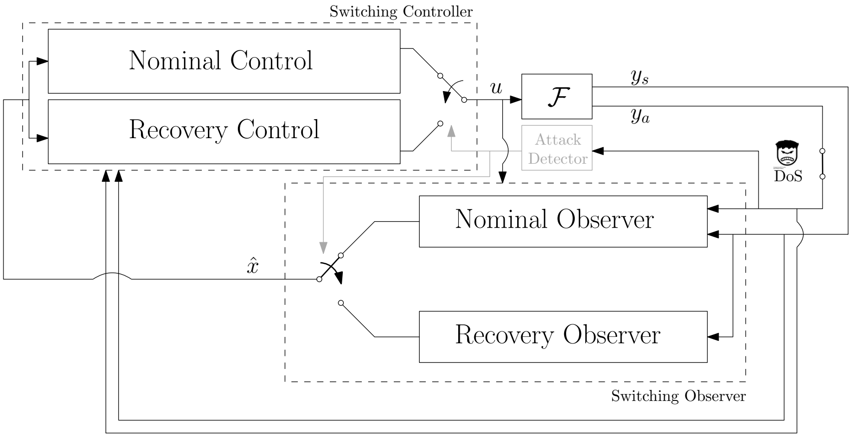
Solution Approach



Solution Approach



Solution Approach



Switching Observer Design

Reconstruction of the state with potential unobservable modes when under attack for feedback control design. The switching observer

$$\dot{\hat{x}} = \begin{cases} A\hat{x} + Bu + L(Cx - C\hat{x}) & \text{if} \quad t \notin \mathcal{T}_a, \\ A\hat{x} + Bu + \tilde{L}(\tilde{C}x - \tilde{C}\hat{x}) & \text{if} \quad t \in \mathcal{T}_a, \end{cases}$$

Reconstruction of the state with potential unobservable modes when under attack for feedback control design. The switching observer

$$\dot{\hat{x}} = \begin{cases} A\hat{x} + Bu + L(Cx - C\hat{x}) & \text{if} \quad t \notin \mathcal{T}_a, \\ A\hat{x} + Bu + \tilde{L}(\tilde{C}x - \tilde{C}\hat{x}) & \text{if} \quad t \in \mathcal{T}_a, \end{cases}$$

Basic Assumptions

- The pair (A, B) is controllable and the pair (C, A) is detectable.
- We design L so that $A - LC$ has all its eigenvalues in the open left-half plane.
- We design $\tilde{L}$ so that $A - \tilde{L}\tilde{C}$ has as many eigenvalues (but not necessarily all of them) as possible in the open left-half plane.

Switching Observer Design

Reconstruction of the state with potential unobservable modes when under attack for feedback control design. The switching observer

$$\dot{\hat{x}} = \begin{cases} A\hat{x} + Bu + L(Cx - C\hat{x}) & \text{if} \quad t \notin \mathcal{T}_a, \\ A\hat{x} + Bu + \tilde{L}(\tilde{C}x - \tilde{C}\hat{x}) & \text{if} \quad t \in \mathcal{T}_a, \end{cases}$$

Basic Assumptions

- The pair (A, B) is controllable and the pair (C, A) is detectable.
- We design L so that $A - LC$ has all its eigenvalues in the open left-half plane.
- We design $\tilde{L}$ so that $A - \tilde{L}\tilde{C}$ has as many eigenvalues (but not necessarily all of them) as possible in the open left-half plane.

Define the estimation error as $e = x - \hat{x}$ with

$$\dot{e} = \begin{cases} (A - LC)e & \text{if} \quad t \notin \mathcal{T}_a, \\ (A - \tilde{L}\tilde{C})e & \text{if} \quad t \in \mathcal{T}_a. \end{cases}$$

Estimation Error Bounds

Lemma 1. Under No Attacks

For given $T_{na}, \bar{e}_0 > 0$, if at the end of an attack the norm of **the estimation error** $e = x - \hat{x}$ is bounded by $\bar{e}_0$, then

$$|e(t)| \leq \gamma_1(t)\bar{e}_0 \qquad \forall t \in [0, T_{na}]$$

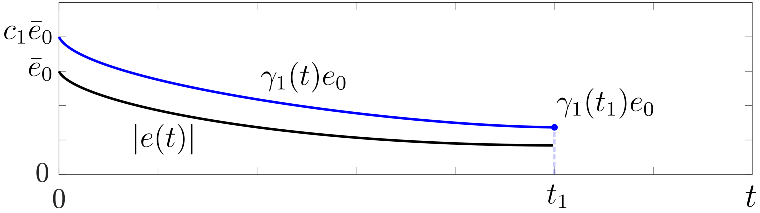
where $\gamma_1(t) := c_1 \exp\left(-\bar{\lambda}_1 t\right)$ with $c_1, \bar{\lambda}_1 > 0$.

Lemma 1. Under No Attacks

For given $T_{na}, \bar{e}_0 > 0$, if at the end of an attack the norm of **the estimation error** $e = x - \hat{x}$ is bounded by $\bar{e}_0$, then

$$|e(t)| \leq \gamma_1(t)\bar{e}_0 \qquad \forall t \in [0, T_{na}]$$

where $\gamma_1(t) := c_1 \exp\left(-\bar{\lambda}_1 t\right)$ with $c_1, \bar{\lambda}_1 > 0$.



Lemma 2. Under Attacks

For given $T_a, \bar{e}_0 > 0$, if at the beginning of an attack the norm of **the estimation error** e is bounded by $\bar{e}_0$, then

$$|e(t)| \leq \gamma_2(T_a)\bar{e}_0 \qquad \forall t \in [0, T_a]$$

where $\gamma_2(T_a) := \max_{t \in [0, T_a]} \hat{c}_1 \exp\left(-\hat{\lambda}_1 t\right) + \hat{c}_2 \exp\left(\hat{\lambda}_2 t\right)$

with $\hat{c}_1, \hat{\lambda}_1, \hat{c}_2, \hat{\lambda}_2 > 0$.

Estimation Error Bounds

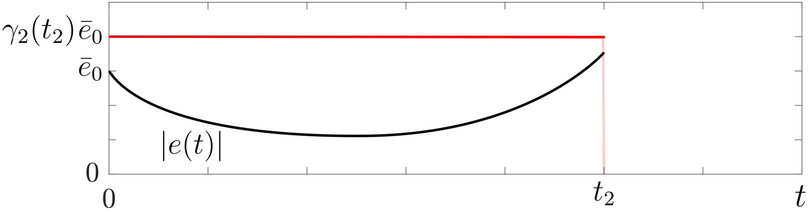
Lemma 2. Under Attacks

For given $T_a, \bar{e}_0 > 0$, if at the beginning of an attack the norm of **the estimation error** e is bounded by $\bar{e}_0$, then

$$|e(t)| \leq \gamma_2(T_a)\bar{e}_0 \qquad \forall t \in [0, T_a]$$

where $\gamma_2(T_a) := \max_{t\in[0,T_a]} \hat{c}_1 \exp\left(-\hat{\lambda}_1 t\right) + \hat{c}_2 \exp\left(\hat{\lambda}_2 t\right)$

with $\hat{c}_1, \hat{\lambda}_1, \hat{c}_2, \hat{\lambda}_2 > 0$.



UF UNIVERSITY of FLORIDA Duke UNIVERSITY TEXAS The University of Texas at Austin UC SANTA CRUZ

Global Bound on Estimation Error

Theorem 1.

Given $\bar{E}, T_{na}, T_a > 0$, if the initial estimation error $e(0)$ satisfies $|e(0)| \leq \bar{E}$ and $\gamma_1(T_{na})\gamma_2(T_a) \leq 1$, then

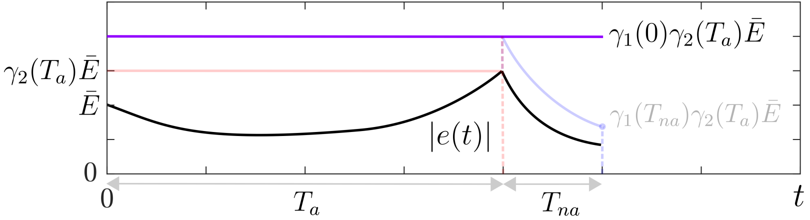
$$|e(t)| \leq \gamma_1(0)\gamma_2(T_a)\bar{E} \qquad \forall t \geq 0$$

Global Bound on Estimation Error

Theorem 1.

Given $\bar{E}, T_{na}, T_a > 0$, if the initial estimation error $e(0)$ satisfies $|e(0)| \leq \bar{E}$ and $\gamma_1(T_{na})\gamma_2(T_a) \leq 1$, then

$$|e(t)| \leq \gamma_1(0)\gamma_2(T_a)\bar{E} \qquad \forall t \geq 0$$

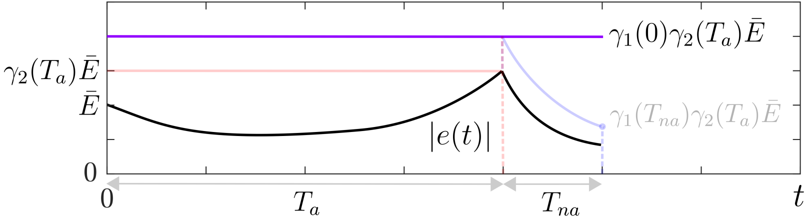


Global Bound on Estimation Error

Theorem 1.

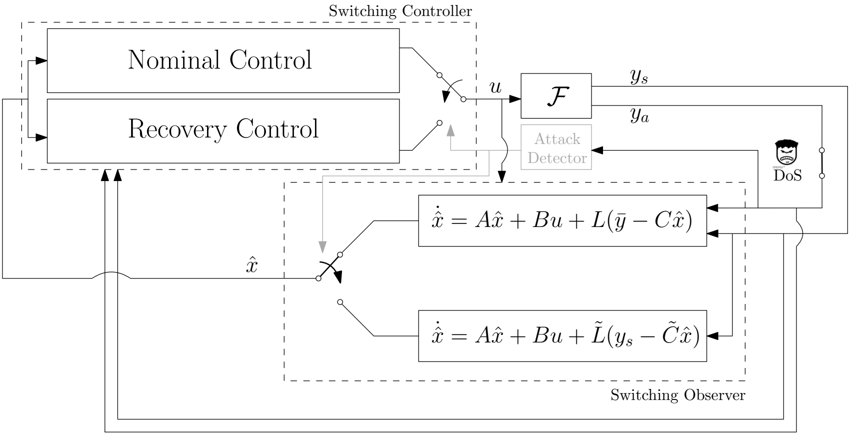
Given $\bar{E}, T_{na}, T_a > 0$, if the initial estimation error $e(0)$ satisfies $|e(0)| \leq \bar{E}$ and $\gamma_1(T_{na})\gamma_2(T_a) \leq 1$, then

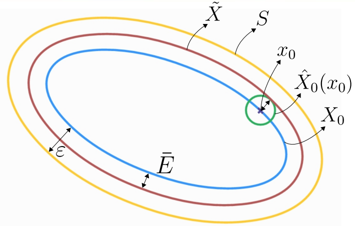
$$|e(t)| \leq \gamma_1(0)\gamma_2(T_a)\bar{E} \qquad \forall t \geq 0$$



Using the proposed observer, **the norm of the error always remains bounded**.

Switched Observer

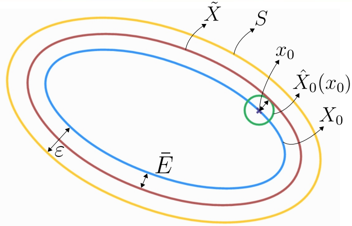




Construction of Sets of Initial Conditions

Pick $\varepsilon > (1 + \gamma_1(0)\gamma_2(T_a))\bar{E}$

- Set of initial states: $X_0 := S \setminus (\partial S + \varepsilon\mathbb{B})$
- Set of initial estimates: $\hat{X}_0(x_0) := x_0 + \bar{E}$
- Allowed initial estimates: $\tilde{X} := X_0 + \bar{E}\mathbb{B}$



Construction of Sets of Initial Conditions

Pick $\varepsilon > (1 + \gamma_1(0)\gamma_2(T_a))\bar{E}$

- Set of initial states: $X_0 := S \setminus (\partial S + \varepsilon\mathbb{B})$
- Set of initial estimates: $\hat{X}_0(x_0) := x_0 + \bar{E}$
- Allowed initial estimates: $\tilde{X} := X_0 + \bar{E}\mathbb{B}$

Lemma 3

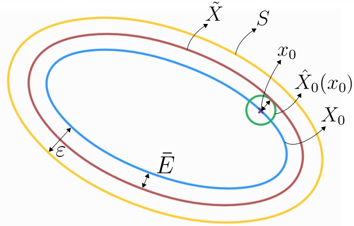
With **bounded estimation error** and $x(0) \in X_0, \hat{x}(0) \in \hat{X}_0(x_0)$:

Observer-based Feedback Law Design

Construction of Sets of Initial Conditions

Pick $\varepsilon > (1 + \gamma_1(0)\gamma_2(T_a))\bar{E}$

- Set of initial states: $X_0 := S \setminus (\partial S + \varepsilon\mathbb{B})$
- Set of initial estimates: $\hat{X}_0(x_0) := x_0 + \bar{E}$
- Allowed initial estimates: $\tilde{X} := X_0 + \bar{E}\mathbb{B}$



Lemma 3

With **bounded estimation error** and $x(0) \in X_0, \hat{x}(0) \in \hat{X}_0(x_0)$:

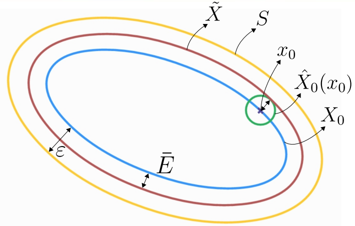
If $\hat{x}(t) \in \tilde{X}$ for all $t \geq 0$, then $x(t) \in S$ for all $t \geq 0$.

Observer-based Feedback Law Design

Construction of Sets of Initial Conditions

Pick $\varepsilon > (1 + \gamma_1(0)\gamma_2(T_a))\bar{E}$

- Set of initial states: $X_0 := S \setminus (\partial S + \varepsilon \mathbb{B})$
- Set of initial estimates: $\hat{X}_0(x_0) := x_0 + \bar{E}$
- Allowed initial estimates: $\tilde{X} := X_0 + \bar{E}\mathbb{B}$



Lemma 3

With **bounded estimation error** and $x(0) \in X_0, \hat{x}(0) \in \hat{X}_0(x_0)$:

If $\hat{x}(t) \in \tilde{X}$ for all $t \geq 0$, then $x(t) \in S$ for all $t \geq 0$.

- The sets X_0 and $\hat{X}_0$ are defined such that the $|e(0)| \leq \bar{E}$.
- Forward invariance of $\tilde{X}$ for the observer implies conditional invariance of the set S for $\mathcal{F}$ with respect to X_0.

QP-based Feedback Law Synthesis

Control barrier function (CBF)-based approach for control design.

Control Objective

Enforce the estimate $\hat{x}$ in the set $\tilde{X}$ to guarantee safety of S.

QP-based Feedback Law Synthesis

Control barrier function (CBF)-based approach for control design.

Control Objective

Enforce the estimate $\hat{x}$ in the set $\tilde{X}$ to guarantee safety of S.

Zero sublevel set representation of a set $\bar{X}$ based on function $h : \mathbb{R}^n \to \mathbb{R}$

$$\bar{X} \coloneqq \{\hat{x} \mid h(\hat{x}) \leq 0\} \subset \tilde{X}$$

QP-based Feedback Law Synthesis
Control barrier function (CBF)-based approach for control design.

Control Objective

Enforce the estimate $\hat{x}$ in the set $\tilde{X}$ to guarantee safety of S.

Zero sublevel set representation of a set $\bar{X}$ based on function $h : \mathbb{R}^n \to \mathbb{R}$

$$\bar{X} := \{\hat{x} \mid h(\hat{x}) \leq 0\} \subset \tilde{X}$$

Sufficient: Design an observer-based feedback law κ such that for each $\hat{x}(0) \in \bar{X}$, the estimate $\hat{x}(t) \in \bar{X} \subset \tilde{X}$, for all $t \geq 0$.

Observer-based Feedback Law Design

QP-based Feedback Law Synthesis
Control barrier function (CBF)-based approach for control design.

Control Objective

Enforce the estimate $\hat{x}$ in the set $\tilde{X}$ to guarantee safety of S.

Zero sublevel set representation of a set $\bar{X}$ based on function $h : \mathbb{R}^n \to \mathbb{R}$

$$\bar{X} := \{\hat{x} \mid h(\hat{x}) \leq 0\} \subset \tilde{X}$$

Sufficient: Design an observer-based feedback law κ such that for each $\hat{x}(0) \in \bar{X}$, the estimate $\hat{x}(t) \in \bar{X} \subset \tilde{X}$, for all $t \geq 0$.

CBF Conditions

Under no attacks:

$$\frac{\partial}{\partial \hat{x}} h(\hat{x}(t)) \left(A\hat{x}(t) + B\kappa_1(\hat{x}(t), \bar{y}(t)) + L(\bar{y}(t) - C\hat{x}(t))\right) \leq \alpha_1(-h(\hat{x}(t))),$$

Under attack:

$$\frac{\partial}{\partial \hat{x}} h(\hat{x}(t)) \left(A\hat{x}(t) + B\kappa_2(\hat{x}(t), \bar{y}(t)) + \tilde{L}(\bar{y}_s(t) - \tilde{C}\hat{x}(t))\right) \leq \alpha_2(-h(\hat{x}(t))).$$

Observer-based Feedback Law Design

QP-based Feedback Law Synthesis

Control barrier function (CBF)-based approach for control design.

Quadratic Programming (QP) Formulation to Compute Input u

Synthesize the control input via solving:

- For each $\hat{x} \in \bar{X}$ and $\bar{y}$ such that $x \in S$ when there is no attack:

$$\min_{(v,\eta)} \quad \frac{1}{2}|v - K\hat{x}|^2 + \frac{1}{2}\eta^2$$

$$\text{s.t.} \qquad \frac{\partial}{\partial \hat{x}} h(\hat{x}) \left(A\hat{x} + Bv + L(\bar{y} - C\hat{x})\right) \leq -\eta h(\hat{x}),$$

- For each $\hat{x} \in \bar{X}$ and $y_s = \tilde{C}x$ such that $x \in S$ when under attack:

$$\min_{(v_s,\zeta)} \quad \frac{1}{2}|v_s - K\hat{x}|^2 + \frac{1}{2}\zeta^2$$

$$\text{s.t.} \qquad \frac{\partial}{\partial \hat{x}} h(\hat{x}) \left(A\hat{x} + Bv_s + \tilde{L}(y_s - \tilde{C}\hat{x})\right) \leq -\zeta h(\hat{x}).$$

where K is the optimal LQR gain for the pair (A, B).

QP-based Feedback Law Synthesis
Control barrier function (CBF)-based approach for control design.

Theorem 2. Main Result

Under feasible QPs for all $\hat{x} \in \tilde{X}$:

QP-based Feedback Law Synthesis

Control barrier function (CBF)-based approach for control design.

Theorem 2. Main Result

Under feasible QPs for all $\hat{x} \in \tilde{X}$:

For each $x_0 \in X_0$ and $\hat{x}_0 \in \bar{X} \cap \hat{X}_0(x_0)$,

$$\hat{x}(t) \in \bar{X} \text{ and } x(t) \in S \text{ for all } t \geq 0.$$

QP-based Feedback Law Synthesis

Control barrier function (CBF)-based approach for control design.

Theorem 2. Main Result

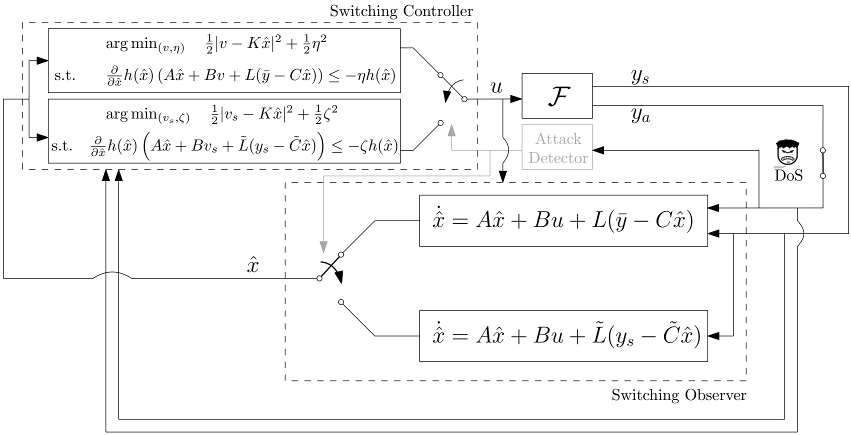
Under feasible QPs for all $\hat{x} \in \tilde{X}$:

For each $x_0 \in X_0$ and $\hat{x}_0 \in \bar{X} \cap \hat{X}_0(x_0)$,

$$\hat{x}(t) \in \bar{X} \text{ and } x(t) \in S \text{ for all } t \geq 0.$$

- Feasibility of the QPs with proper state initialization renders the estimate $\hat{x}(t) \in \bar{X}$ at all times.
- Then **the state x remains in S at all times.**

Solution Scheme



Integrator with Nondetectable Modes under Attack

System $\mathcal{F}$ with state $x = (x_1, x_2) \in \mathbb{R}^2$, input $u \in \mathbb{R}$, and dynamics

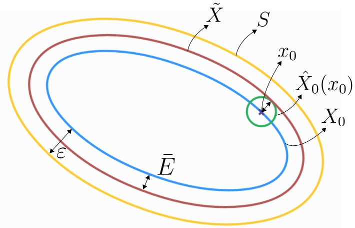
$$\begin{aligned} \dot{x}_1 &= \frac{x_1}{2} + x_2 \\ \dot{x}_2 &= u \\ y &= (x_1, x_2) \end{aligned}$$

Integrator with Nondetectable Modes under Attack

System $\mathcal{F}$ with state $x = (x_1, x_2) \in \mathbb{R}^2$, input $u \in \mathbb{R}$, and dynamics

$$\begin{aligned}\dot{x}_1 &= \frac{x_1}{2} + x_2 \\ \dot{x}_2 &= u \\ y &= (x_1, x_2)\end{aligned}$$

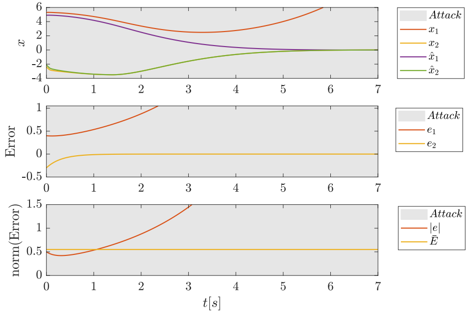
- $y_a = x_1$ is only available when there are no attacks.
- Attacks of max. $T_a = 1.6$s. No attacks for min. $T_{na} = 0.05$s.



Integrator with Nondetectable Modes under Attack

System $\mathcal{F}$ with state $x = (x_1, x_2) \in \mathbb{R}^2$, input $u \in \mathbb{R}$, and dynamics

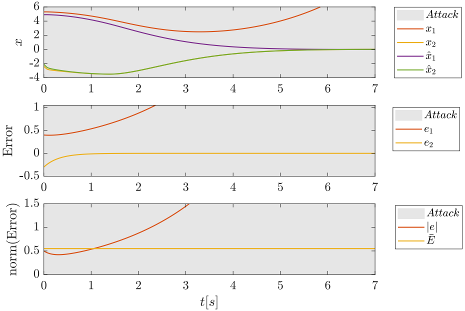
$$\dot{x}_1 = \frac{x_1}{2} + x_2$$
$$\dot{x}_2 = u$$
$$y = (x_1, x_2)$$

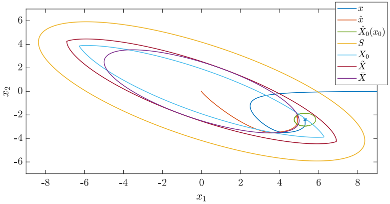


Integrator with Nondetectable Modes under Attack

System $\mathcal{F}$ with state $x = (x_1, x_2) \in \mathbb{R}^2$, input $u \in \mathbb{R}$, and dynamics

$$\begin{aligned}\dot{x}_1 &= \frac{x_1}{2} + x_2\\ \dot{x}_2 &= u\\ y &= (x_1, x_2)\end{aligned}$$



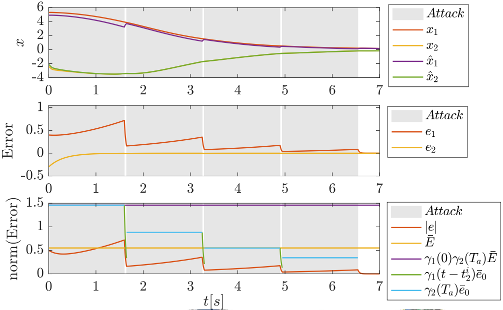


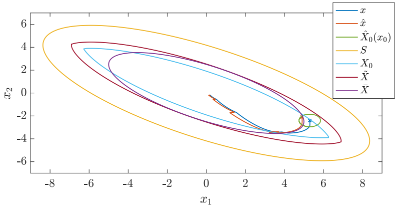
Numerical Example

Integrator with Nondetectable Modes under Attack

System $\mathcal{F}$ with state $x = (x_1, x_2) \in \mathbb{R}^2$, input $u \in \mathbb{R}$, and dynamics

$$\dot{x}_1 = \frac{x_1}{2} + x_2$$
$$\dot{x}_2 = u$$
$$y = (x_1, x_2)$$



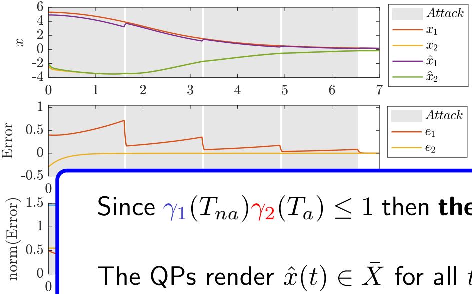


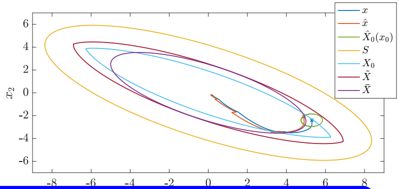
Numerical Example

Integrator with Nondetectable Modes under Attack

System $\mathcal{F}$ with state $x = (x_1, x_2) \in \mathbb{R}^2$, input $u \in \mathbb{R}$, and dynamics

$$
\begin{aligned}
\dot{x}_1 &= \frac{x_1}{2} + x_2 \\
\dot{x}_2 &= u \\
y &= (x_1, x_2)
\end{aligned}
$$





Since $\gamma_1(T_{na})\gamma_2(T_a) \leq 1$ then **the error is bounded at all times.**

The QPs render $\hat{x}(t) \in \bar{X}$ for all t, then $x(t) \in S$ for all t.

Conclusion

- **Switched controller** design with a **switched observer** that ensures a LTI system to recover *safely* from finite-time DoS attacks in some of the system outputs.
- Conditional invariance of a set with respect to a subset of initial conditions by employing a **barrier function** approach and **bounding the estimation error at all times**.

Conclusion

- **Switched controller** design with a **switched observer** that ensures a LTI system to recover *safely* from finite-time DoS attacks in some of the system outputs.
- Conditional invariance of a set with respect to a subset of initial conditions by employing a **barrier function** approach and **bounding the estimation error at all times**.

Future Work

- Finite-time observer and tighter bound to relax the conservatism.

Aknowledgements This research has been partially supported by the Air Force Office of Scientific Research under Grant no. FA9550-19-1-0169