Diagnosability of Hybrid Dynamical Systems

Maria Domenica Di Benedetto

University of L'Aquila
Many thanks!

• Elena De Santis
• Giordano Pola
• Gabriella Fiore
• Andrea Balluchi
• Luca Benvenuti
• Alberto Sangiovanni Vincentelli
Outline

• Motivation
  • Cyber-Physical Systems (CPS)
  • Security for CPS

• Modeling CPS as hybrid systems

• Secure state estimation for hybrid systems
  • Observability and diagnosability
  • Secure mode distinguishability
  • Secure diagnosability
  • Approximate diagnosability

• Conclusions and future work
Cyber-Physical Systems (CPSs) integrate physical processes, computational resources and communication capabilities.

Many applications: smart grids, water distribution networks, unmanned (aerial, ground, underwater) vehicles, biomedical and health care devices, air traffic management systems, and many others.
Security of CPS

What Stuxnet's Exposure As An American Weapon Means For Cyberwar

Cyberattack Inflicts Massive Damage on German Steel Factory

Keeping your car safe from hacking
Automakers and NHTSA scramble to protect your privacy and safety

FBI: Hacker claimed to have taken over flight's engine controls

Security Experts Hack Teleoperated Surgical Robot

The first hijacking of a medical telerobot raises important questions over the security of remote surgery, say computer security experts.
Security of CPSs

Security measures protecting only the computational and communication layers are **necessary but not sufficient** for guaranteeing the safe operation of the entire system.

Exploit also system dynamics to
- assess correctness and compatibility of measurements,
- ensure robustness and resilience with respect to malicious attacks.

[Q. Zhu and T. Basar, 2015]
CPSs modeled as hybrid systems

Management Layer

Supervisory Layer

Network Layer

Communication Layer

Control Layer

Physical Layer

\[ q_1 \xrightarrow{} q_2 \xrightarrow{} q_3 \xrightarrow{} q_4 \]

\[ t_0 \xrightarrow{} t_1 \xrightarrow{} t_2 \xrightarrow{} t_3 \xrightarrow{} t_4 \]

DISMA, Torino, 23-27 sept. 2019
• Motivation
  • Cyber-Physical Systems (CPS)
  • Security for CPS

• Modeling CPS as hybrid systems

• Secure state estimation for hybrid systems
  • Observability and diagnosability
  • Secure mode distinguishability
  • Secure diagnosability
  • Approximate diagnosability

• Conclusions and future work
Linear Hybrid systems

\[ \dot{x} = A_1 x + B_1 u \]
\[ y = C_1 x \]

\[ \dot{x} = A_2 x + B_2 u \]
\[ y = C_2 x \]

\[ \dot{x} = A_3 x + B_3 u \]
\[ y = C_3 x \]

\[ x^+ \in R(x^-, e_1) \]
\[ x^+ \in R(x^-, e_3) \]

\[ x^+ \in R(x^-, e_2) \]
**Definition.** An H-system is a tuple: 

\[ \mathcal{H} = (\Xi, \Xi_0, \Upsilon, h, S, E, G, R, \delta, \Delta) \]

- \( \Xi = Q \times X \) hybrid state space
- \( \Xi_0 \subseteq \Xi \) set of initial hybrid states
- \( \Upsilon = Y_d \times \mathbb{R}^p \) hybrid output space
- \( h: Q \to Y_d \) discrete output function
- \( S \) associates to each discrete state a dynamical system \( S(i) \) described by:
  \[
  \begin{cases}
  \dot{x}_i = A_i x(t) + B_i u(t) \\
  y(t) = C_i x(t)
  \end{cases}
  \]
- \( E \subseteq Q \times Q \) admissible discrete transitions
- \( G: E \to 2^X \) guard
- \( R: E \times X \to 2^X \) reset
- \( \delta: Q \to \mathbb{R}^+ \) minimum dwell time associated to \( i \in Q \)
- \( \Delta: Q \to \mathbb{R}^+ \cup \{\infty\} \) maximum dwell time associated to \( i \in Q \)

DISMA, Torino, 23-27 sept. 2019
Definition: A **hybrid time basis** is a sequence of intervals $\tau = \{I_0, I_1, \ldots, I_N\} = \{I_i\}_{i=0}^N$, with $N < \infty$ or $N = \infty$, $I_i = [t_i, t'_i]$ for all $i < N$ such that

- if $N < \infty$ then either $I_N = [t_N, t'_N]$ or $I_N = (t_N, t'_N)$
- $t_i \leq t'_i = t_{i+1}$ for all $i$
Discrete State Evolution

$\begin{align*}
q_1 & \rightarrow q_2 \\
q_2 & \rightarrow q_3 \\
q_3 & \rightarrow q_1 \\
q_1 & \rightarrow q_2
\end{align*}$

$t'_0 = t_1 \\
t'_1 = t_2 \\
t'_2 = t_3 \\
t'_3 = t_4$
Observed output

\( h: Q \rightarrow Y \) is the **discrete output function**, where \( Y \) is the discrete output space
Observability and diagnosability of H-systems

- **Observability**: possibility of determining the current discrete state and the continuous state, on the basis of the observed output information.

- **Diagnosability**: possibility of detecting the occurrence of particular subsets of hybrid states, for example faulty states, on the basis of the observations, within a finite time interval.

\[ \Xi = Q \times X \]
Outline

• Motivation
  • Cyber-Physical Systems (CPS)
  • Security for CPS

• Modeling CPS as hybrid systems

• Secure state estimation for hybrid systems
  • Observability and diagnosability
  • Secure mode distinguishability
  • Secure diagnosability
  • Approximate diagnosability

• Conclusions and future work
Observability and resilience: example 1

\[ x(t + 1) = -Lx(t) + Bu(t) \]
\[ y = Cx(t) \]

\[ l_{ij} = \begin{cases} 1 & j \in \mathcal{N}_i \\ -|\mathcal{N}_i| & j = i \\ 0 & \text{otherwise} \end{cases} \]

\[ L = \begin{bmatrix} -2 & 1 & 1 & 0 \\ 1 & -3 & 1 & 1 \\ 1 & 1 & -3 & 1 \\ 0 & 1 & 1 & -2 \end{bmatrix} \]
\[ B = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \]
\[ C = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \end{bmatrix} \]
**Observability and resilience: example 1**

\[ x(t + 1) = -\mathbf{L}x(t) + Bu(t) \]
\[ y = Cx(t) \]

Link disconnection:

\[ l_{ij} = \begin{cases} 
1 & j \in \mathcal{N}_i \\
-|\mathcal{N}_i| & j = i \\
0 & \text{otherwise}
\end{cases} \]

\[
\mathbf{L} = \begin{bmatrix}
-2 & 1 & 1 & 0 \\
1 & -2 & 0 & 1 \\
1 & 0 & -2 & 1 \\
0 & 1 & 1 & -2
\end{bmatrix}
\]

\[
B = \begin{bmatrix} 1 \\
0 \\
0 \\
0 \end{bmatrix}
\]

\[
C = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 \end{bmatrix}
\]

DISMA, Torino, 23-27 sept. 2019
Observability and resilience: example 1

Node disconnection:

\[ x(t + 1) = -\bar{L}x(t) + \bar{B}u(t) \]
\[ y = \bar{C}x(t) \]

\[ l_{ij} = \begin{cases} 
1 & j \in \mathcal{N}_{i} \\
-|\mathcal{N}_{i}| & j = i \\
0 & \text{otherwise}
\end{cases} \]

\[ \bar{L} = \begin{bmatrix} 
-1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 \\
1 & 0 & -2 & 1 \\
0 & 0 & 1 & -1 
\end{bmatrix} \quad \bar{B} = \begin{bmatrix} 
1 \\
0 \\
0 \\
0 
\end{bmatrix} \quad \bar{C} = \begin{bmatrix} 
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 
\end{bmatrix} \]
Observability and resilience: example 2

Objectives:

- Extract the maximum available power from renewable sources
- Provide/absorb the power when needed by means of the battery
- Stabilize grid and load voltage (also in case of disturbances)

[lovine et al. 2017]
Linearized digital model

\[ S = \begin{cases} 
  x(k + 1) = Ax(k) + [B_b \ D] \begin{bmatrix} b(k) \\ d_x(k) \end{bmatrix} = Ax(k) + Bu(k) \\
  y(k) = Cx(k) + w(k) 
\end{cases} \]

\[ \text{Sparse attack } \quad w(k) \in \mathbb{S}\sigma^p \]

\[ x(k) \in \mathbb{R}^n, \; u(k) \in \mathbb{R}^m, \; y(k) \in \mathbb{R}^p \]
Observability of H-systems

**Definition.** The system H is **observable** if there exists a function \( \hat{\xi}: \Upsilon \times U \rightarrow \Xi \) which, by setting \( \hat{\xi}(\eta|_{[0,t]}, \hat{u}|_{[0,t]}) = (\hat{q}(t), \hat{x}(t)) \) satisfies the following condition:

- there exists \( \hat{t} > 0 \) such that:
  - \( \hat{q}(t) = q(t) \) \( \forall \ t > \hat{t} \)
  - \( ||\hat{x}(t) - x(t)|| = 0 \) \( \forall \ t > \hat{t} \)

for any generic input \( \hat{u} \in U \), for any execution \( \chi \) with \( u = \hat{u} \).
For an input $u \in \mathcal{U}$, with $\mathcal{U}$ set of piecewise continuous functions, define the norm of $u$ as:

$$
\|u\| = \sup_{t \in \mathbb{R}} \|u(t)\|
$$

where $\|u(t)\|$ standard Euclidean norm of the vector $u(t)$ in the space $\mathbb{R}^m$.

A generic input $\hat{u} \in \mathcal{U}$ is any input function that belongs to a dense subset of the set $\mathcal{U}$ equipped with the above defined norm.
Is observability of each pair \((A_i, C_i)\) necessary and sufficient for the observability of \(H\)?

Example:

\[
\begin{align*}
\dot{x} &= A_1 x \\
y &= C_1 x
\end{align*}
\]

\[
\begin{align*}
\dot{x} &= A_2 x \\
y &= C_2 x
\end{align*}
\]

\[
\begin{align*}
x &\in \mathbb{R}^2, \Delta(i) = \Delta \neq \infty \\
h(i) &= i, \quad \forall i \in Q \\
S(1) &= \begin{cases} 
\dot{x}_1 = x_1 \\
\dot{x}_2 = x_2 \\
y = x_1
\end{cases} \\
A_1 &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\
C_1 &= \begin{bmatrix} 1 & 0 \end{bmatrix}
\]

\[
\begin{align*}
S(2) &= \begin{cases} 
\dot{x}_1 = x_1 \\
\dot{x}_2 = x_2 \\
y = x_2
\end{cases} \\
A_2 &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\
C_2 &= \begin{bmatrix} 0 & 1 \end{bmatrix}
\]

The pairs \((A_i, C_i)\) are not observable, however \(H\) is observable!
Role of reset, graph topology

Example:

\[ R_{e_1} = I \]
\[ R_{e_3} = 0 \]
\[ R_{e_2} = I \]

\[ x \in \mathbb{R}^2, \Delta(i) = \Delta \neq \infty \]
\[ h(i) = i, \quad \forall i \in Q \]

The pairs \((A_i, C_i)\) are not observable.

At most after \(3\Delta\) units of time the state is equal to 0 because of the reset function definition. Hence, H is observable!
State estimation of H-systems

HYBRID SYSTEM

\[ x^{k+1} = A_1 x^k + B_1 u^k \]
\[ y^k = C_1 x^k \]

\[ x^{k+1} = A_2 x^k + B_2 u^k \]
\[ y^k = C_2 x^k \]

\[ x^{k+1} = A_3 x^k + B_3 u^k \]
\[ y^k = C_3 x^k \]

\[ x^{k+1} = A_4 x^k + B_4 u^k \]
\[ y^k = C_4 x^k \]

\[ \hat{\xi} = (\hat{q}, \hat{x}) \]

DISMA, Torino, 23-27 sept. 2019
Goal: Determine current discrete state of H by using discrete output information either independently from continuous output evolution or by using also continuous evolution.
Finite state machine associated to $H$

HYBRID SYSTEM $\quad H = (\Xi = (Q, X), \Xi_0 = (Q_0, X_0), \mathcal{Y} = (\mathcal{Y}, \mathbb{R}^P), h, S, E, G, R, \delta, \Delta)$

Nondeterministic **finite state machine** (FSM) that abstracts the dependence of the discrete dynamics of $H$ from its continuous evolution:

$$M = (\mathcal{Q}, Q_0, \mathcal{Y}, h, E)$$
Finite state machine associated to H

\[ M = (Q, Q_0, Y, h, E) \]

Given the evolution in time of the H-system \( \chi = (q_0, \tau, q) \), where \( \tau \) is a time basis with \( \text{card}(\tau) = L \), the event-based evolution of the FSM is a string \( \sigma \):

- **State execution of M:**
  \[ \sigma(1) \in Q \]
  \[ \sigma(k) = q(t_{k-1}), \quad k = 1, 2, \ldots, L \]
  \[ \sigma(k + 1) \in \text{succ}(\sigma(k)), \quad k = 1, \ldots, L - 1 \]

- **\( \mathcal{X}^* \)** set of all state executions
- **\( \mathcal{X} \)** set of infinite state executions with \( \sigma(1) \in Q_0 \)
- **Liveness:** \( \text{succ}(i) \neq \emptyset \quad \forall \ i \in Q \)
- **Discrete output of M:**
  \[ h(\sigma(k)) = h(q(t_{k-1})) = y_d(t_{k-1}) \]
- **Output string of M:**
  \[ h : \mathcal{X}^* \to (Y \setminus \{\varepsilon\})^* \]

where for \( \sigma \in \mathcal{X}^* \), \( h(\sigma) = P(s) \), \( s = (h(\sigma(1)) \ldots h(\sigma(|\sigma|))) \)

where for an output string \( s \in Y^* \), \( P(s) \) denotes the string obtained from \( s \) by erasing all \( \varepsilon \) symbols.
**Definition:** The FSM $M$ is **current location observable** if there exists $\bar{k} \in \mathbb{Z}$, such that for any string $\sigma \in \mathcal{X}$ with unknown $\sigma(1) \in Q_0$, the knowledge of the output string $h(\sigma|_{[1,k]})$ makes it possible to infer that $\sigma(k) = i$, for some $i \in Q$, for all $k \geq \bar{k}$.

![Diagram of an FSM](image)

**Current location observable!**

[Ramadge, CDC 1986]
Current location observability

**Theorem.** The FSM $M$ is *current location observable* if and only if for every persistent state $i \in Q_p$ of $M$:

1) $h(i) \neq \varepsilon$;
2) there exists a singleton state $\{i\}$ in the observer $O_M$ and it is the only persistent state of $O_M$ containing $i$.

$M$ and $O_M$ have the same set of persistent states!

$M$

$h(i) \neq \varepsilon$;

$O_M$
Current location observability of $H$ (using discrete output only)

Assuming \textit{finite maximum dwell time}, current location observability of $M$ is equivalent to current location observability of $H$. 
Current location observability of $H$ (using discrete output only)

H-system

FSM

Current location observability

$\Delta < \infty$

Current location observability

What if the maximum dwell time is $\Delta = \infty$?

Critical location observability is needed!
**Definition:** The FSM M is \( \{i\} – \text{critically location observable} \) if, for any \( k \in \mathbb{Z} \), whenever \( \sigma(k) = i \), the knowledge of the output string \( h(\sigma|_{1,k}) \) makes it possible to infer that \( \sigma(k) = i \). If M is \( \{i\} – \text{critically location observable} \) for all \( i \in Q \), then it is called **critically location observable**.

**Theorem:** The FSM M is \( \{i\} – \text{critically location observable} \) only if \( h(i) \neq \varepsilon \).
Observability of critical states

\[ Q_b = \{ \text{unauth. crossing} \} \]
Critical observability of H

**Definition.** The H-system is \(\{i\} -\text{critically location observable}\) if there exists a function \(\dot{\xi}: Y \times U \rightarrow \Xi\) such that, by setting

\[
\dot{\xi}(\eta|_{[0,t]}, \hat{u}|_{[0,t]}) = (\hat{q}(t), \hat{x}(t))
\]

whenever \(q(t_k) = i\)

\[
\hat{q}(t) = i \quad \forall \ t \in (t_k, t_{k+1})
\]

for any generic input \(\hat{u} \in U\) and for any execution \(\chi\) with \(u = \hat{u}\).

The H-system is **critically location observable** if it is \(\{i\}\)-critically location observable for all \(i \in Q\).

**Theorem.** The H-system is **critically location observable** if and only if it is current location observable with \(\hat{t} = 0\).
Current location observability of H
(using discrete output only)

<table>
<thead>
<tr>
<th>H-system</th>
<th>FSM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current location observability</td>
<td>( \Delta &lt; \infty )</td>
</tr>
<tr>
<td>{i} – critical location observability</td>
<td>{i} – critical location observability</td>
</tr>
<tr>
<td>Current location observability</td>
<td>✔ Current location observability</td>
</tr>
<tr>
<td></td>
<td>✔ {i} – critical location observability</td>
</tr>
<tr>
<td>( \Delta = \infty )</td>
<td>( \forall i \in \text{reach}(Q_{\infty}) )</td>
</tr>
</tbody>
</table>

H-system is *current location observable* only if \( h(i) \neq \varepsilon \), for all "persistent in time" states \( i \in Q_p \cup \text{reach}(Q_{\infty}) \).
Current location observability
(mixed continuous and discrete information)

**Question:** What if the discrete output information is not sufficient to estimate the current discrete location?

**Example:**

If the current output symbol is \( b \), we can deduce that the current mode is either \( i \) or \( j \). However, the modes \( i \) and \( j \) cannot be distinguished only on the basis of the discrete output information, although no state is silent.

**Solution:** Continuous inputs and outputs can be used to obtain some additional information that may be useful for the identification of the plant current location.
Location detector

\[ \xi = (q, x) \]

PLANT HYBRID MODEL

LOCATION DETECTOR

LOCATION OBSERVER

\[ \hat{y} \]

\[ \hat{q} \]
**Theorem.** The FSM $M$ is **current location observable** if and only if for every persistent state $i \in Q_p$ of $M$:

1) $h(i) \neq \varepsilon$;  

2) there exists a singleton state $\{i\}$ in the observer $O_M$ and it is the only persistent state of $O_M$ containing $i$.

There exists persistent state of $M$ having unobservable output. $\mathcal{L}_H$ has to produce an output event $\gamma$.

**Example:**
Theorem. The FSM $M$ is **current location observable** if and only if for every persistent state $i \in Q_p$ of $M$:

1) $h(i) \neq \varepsilon$;

2) there exists a singleton state $\{i\}$ in the observer $O_M$ and it is the only persistent state of $O_M$ containing $i$.

There exist persistent states of $M$ that are not **distinguishable** by using only discrete output information.

**Question:** Is it possible to **distinguish** those states by using continuous information?

Example:
**Goal:** Determine the current **discrete state** of a linear H-system by using only the **continuous output** information.

**Definition:** Two linear systems $S_1$ and $S_2$ are **input generic distinguishable** if, given an arbitrarily small $t > 0$, for all $(x_1(0), x_2(0))$ and for a generic input $u \in \mathcal{U}$, $y_1|_{[0,t]} \neq y_2|_{[0,t]}$.

\[
\dot{x} = A_1 x + B_1 u \\
y_1 = C_1 x(t) \\
\dot{x} = A_2 x + B_2 u \\
y_2 = C_2 x(t) \\
\]

\[
A_{12} = \begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix} \quad B_{12} = \begin{bmatrix} B_1 \\ B_2 \end{bmatrix} \quad C_{12} = \begin{bmatrix} C_1 & -C_2 \end{bmatrix}
\]

\[A_i \in \mathbb{R}^{n \times n} \quad i = 1,2 \]
\[B_i \in \mathbb{R}^{n \times m} \quad i = 1,2 \]
\[C_i \in \mathbb{R}^{p \times n} \quad i = 1,2 \]
Sparse attacks

- Physical process modeled as a linear dynamic system:
  \[
  x(t + 1) = Ax(t) + Bu(t) \\
  y(t) = Cx(t) + e(t)
  \]
  with \( t \in \mathbb{N}, x(t) \in \mathbb{R}^n, u(t) \in \mathbb{R}^m, y(t) \in \mathbb{R}^p \), where \( e_i(t) \neq 0 \) (some sensors are attacked)

Sparse attacks [Fawzi and Tabuada, 2014]:

- \( e_i(t) \) can be arbitrary (no stochastic model, no boundedness, …)
- set of attacked sensors is fixed, but unknown
- the attacker has only access to a subset of sensors (whose cardinality is at most equal to \( \sigma \))

Notation:
- \( e(t) \in \mathbb{S}_\sigma^p \quad \sigma = \|e(t)\|_0 < p \)
- \( e|_{[0,3]} \in \mathbb{C}\mathbb{S}_{\sigma}^{4p} \)
Secure distinguishability

\[
x(t + 1) = A_q x(t) + B_q u(t) \quad q = i, j
\]
\[
y_q(t) = C_q x(t) + w_q(t)
\]
\[
w_q(t) \in S^p_\sigma: \text{sparse attack}
\]
\[
w_q(t)|_{[0,\tau-1]} \in \mathbb{CS}^{p\tau}_s: \text{collecting } \tau \text{ samples}
\]

\[
A_{ij} = \begin{bmatrix} A_i & 0 \\ 0 & A_j \end{bmatrix} \quad \quad B_{ij} = \begin{bmatrix} B_i \\ B_j \end{bmatrix} \quad \quad C_{ij} = [C_i \quad -C_j]
\]

**Definition:** \( S_i \) and \( S_j \) are \( \sigma 0 \) –securely distinguishable (w.r.t. generic inputs and for all \( \sigma \) –sparse attacks on sensors) if there exists \( \tau \in \mathbb{N} \) s. t.

\[
y_i|_{[0,\tau-1]} \neq y_j|_{[0,\tau-1]}
\]

for any pair of initial states \( x_{0i} \) and \( x_{0j} \), for any pair of \( \sigma \)–sparse attack vectors \( w_i(t)|_{[0,\tau-1]} \in \mathbb{CS}^{p\tau}_\sigma \) and \( w_j(t)|_{[0,\tau-1]} \in \mathbb{CS}^{p\tau}_\sigma \), and for any generic input sequence \( u|_{[0,\tau-1]} \), and \( u \in \mathcal{U} \).
Secure distinguishability

\[ M_{ij} = \begin{bmatrix}
C_{ij}B_{ij} & 0 & \ldots & 0 \\
C_{ij}A_{ij}B_{ij} & C_{ij}B_{ij} & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
C_{ij}A_{ij}^{2n-2}B_{ij} & C_{ij}A_{ij}^{2n-3}B_{ij} & \ldots & C_{ij}B_{ij}
\end{bmatrix} \quad \mathcal{O}_{ij} = \begin{bmatrix}
C_{ij} \\
C_{ij}A_{ij} \\
\vdots \\
C_{ij}A_{ij}^{2n-1}
\end{bmatrix} = \begin{bmatrix}
\mathcal{O}_i \\
-\mathcal{O}_i
\end{bmatrix}

Given the set \( \Gamma \subset \{1, \ldots, p\}, |\Gamma| \leq 2\sigma \), let \( M_{ij,\Gamma} \) be the matrix obtained by the triples \((A_i, B_i, \tilde{C}_{i,\Gamma})\) and \((A_j, B_j, \tilde{C}_{j,\Gamma})\), where \( \tilde{C}_{i,\Gamma} \) is the matrix obtained from \( C_i \) by removing the rows contained in \( \Gamma \).

**Theorem:** \( S_i \) and \( S_j \) are \( \sigma 0 \)-securely distinguishable if and only if for any set \( \Gamma \) with \( \Gamma \subset \{1, \ldots, p\}, |\Gamma| \leq 2\sigma \), the matrix \( M_{ij,\Gamma} \neq 0 \).
Definition: $S_i$ and $S_j$ are $\sigma\rho$ - securely distinguishable (w.r.t. generic inputs, generic $\rho$ - sparse attacks on actuators, and for all $\sigma$ - sparse attacks on sensors) if there exists $\tau \in \mathbb{N}$ s. t.

\[
\left. y_i \right|_{[0, \tau-1]} \neq \left. y_j \right|_{[0, \tau-1]}
\]

for any pair of initial states $x_{0i}$ and $x_{0j}$, for any pair of $\sigma$ - sparse attack vectors $w_i(t)|_{[0,\tau-1]} \in \mathbb{C}\mathbb{S}_{\sigma}^{p\tau}$ and $w_j(t)|_{[0,\tau-1]} \in \mathbb{C}\mathbb{S}_{\sigma}^{p\tau}$, and for any generic $(u, v_i, v_j) \in \mathcal{U} \times \mathbb{S}_\rho^m \times \mathbb{S}_\rho^m$.
Location detector design

Examples:

Distinguishability of \((S_i, S_j)\) allows distinguishing mode \(i\) and mode \(j\), despite the same output symbol.

Distinguishability of \((S_i, S_j), (S_h, S_i)\) and \((S_h, S_j)\) ensures current location observability even though the persistent states \(i\) and \(j\) are silent.
When only discrete output information is used, current location observability of H can be checked on the FSM M.

H is transformed into an «equivalent» hybrid system $H'$ with purely discrete output information and with no silent states by translating the continuous output information into discrete output signals.
1. If $i \in Q_p$ is a persistent state, then either it is not silent ($h(i) \neq \varepsilon$) or the pair of dynamical systems $(S_i, S_j)$ is distinguishable for any other state $j$ such that $j$ belongs to $\text{succ}(i)$.

Example:

State $i$ is a persistent state and it is silent, thus distinguishability of pairs $(S_i, S_k)$ and $(S_i, S_h)$ is necessary.
2. If \( i \in \text{reach}(Q_\infty) \setminus Q_0 \), then either it is not silent \((h(i) \neq \varepsilon)\) or the pair of dynamical systems \((S_j, S_i)\) is distinguishable for any other state \(j\) predecessor of \(i\).

Example:

\[
Q_\infty = \{2\}
\]

State \(i\) is a persistent state and it is silent, thus distinguishability of pairs \((S_i, S_k)\) and \((S_i, S_h)\) is necessary.

3. If step 1 and step 2 are possible, \(H\) is current location observable if \(H'\) (with purely discrete output and no silent states) is current location observable, and this can be checked on the FSM associated to \(H'\).
Hybrid observer design

\[ \xi = (q, x) \]

PLANT HYBRID MODEL

CONTINUOUS INPUT \( u \)

LOCATION DETECTOR

LOCATION OBSERVER

CONTINUOUS OBSERVER

DISCRETE OUTPUT \( y_d \)

CONTINUOUS OUTPUT \( y \)

\[ \hat{q} \]

\[ \hat{x} \]
Diagnosability of $M$

$M = (Q, Q_0, Y, h, E)$  \hspace{1cm} \text{Critical set:} \hspace{0.5cm} \Omega \subset Q$

$\Omega$—diagnosability describes the possibility of inferring that the state belongs to $\Omega$, on the basis of the output execution

For any infinite state execution $\sigma \in \mathcal{X}$ two cases are possible:

i. $\sigma(k) \notin \Omega$, $\forall \ k \in \mathbb{Z}$

ii. $\sigma(k) \in \Omega$, for some $k \in \mathbb{Z}$ (crossing event)

If (ii) holds, let $k_\sigma$ be the minimum value of $k$ such that $\sigma(k) \in \Omega$, otherwise $k_\sigma = \infty$
Definition: M is parametrically $\Omega$–diagnosable if there exist $\tau \in \mathbb{Z}$, $\delta \in \mathbb{Z}$, and $T \in \mathbb{Z} \cup \{\infty\}$ such that for any string $\sigma \in \mathcal{X}$ with finite $k_\sigma$, whenever $\sigma(k) \in \Omega$ and $k \in [\max\{k_\sigma, (\tau + 1)\}, k_\sigma + T]$, it follows that for any string $\hat{\sigma} \in y^{-1}(y(\sigma|_{[1, k+\delta]}))$, $\hat{\sigma}(l) \in \Omega$ for some $l \in [\max\{1, (k - \gamma_1)\}, k + \gamma_2]$ and for some $\gamma_1, \gamma_2 \in \mathbb{Z}, \gamma_2 \leq \delta$.

- $\gamma = \max\{\gamma_1, \gamma_2\}$: uncertainty radius in the reconstruction of the step at which the crossing event occurred
- $\delta \in \mathbb{Z}$: delay of the crossing event detection
- $\tau \in \mathbb{Z}$: initial time interval in which the crossing event is not required to be detected
- $T \in \mathbb{Z} \cup \{\infty\}$: time interval in which the occurrence of the crossing event must be detected
Parametrical $\Omega$ – Diagnosability

Parameters $\tau, T, \delta, \gamma$

1. $\max\{k_\sigma, (\tau + 1)\} = (\tau + 1)$

2. $\max\{k_\sigma, (\tau + 1)\} = k_\sigma$

3. No detection is required.
Parametrical $\Omega$ –Diag: Special cases

- **$\Omega$ – current state observability**
  - time interval within which the occurrence of the crossing event must be detected: $T = \infty$
  - initial time interval where the crossing event is not required to be detected: $\tau > 0$
  - delay of the crossing event detection: $\delta = 0$

- **critical $\Omega$ – observability**
  - time interval within which the occurrence of the crossing event must be detected: $T = \infty$
  - initial time interval where the crossing event is not required to be detected: $\tau = 0$
  - delay of the crossing event detection: $\delta = 0$

- **$\Omega$ – initial state observability.** $T = 0, \tau = 0, \delta \geq 0, \Omega \subset Q_0, \gamma_1 = \gamma_2 = 0$
  - The crossing event is detected the first time it occurs, with delay $\delta \geq 0$

- **$\Omega$ – diagnosability.** $T = 0, \tau = 0.$ If $\delta = 0,$ **$\Omega$ – observability**
{3}-diagnosability: For any $\tau$ there exists an execution that crosses for the first time after the interval $\tau$, and it is not possible to detect the set $\Omega$ nor immediately neither with a delay, nor uncertainty.

- $\Omega = \{3\}$: $M$ is not {3}-diag!
- $\Omega = \{2\}$: $M$ is {2}-diag!
Checking $\Omega$ – Diagnosability

- The set-membership formalism and the derived algorithms are very simple and intuitive, and allow checking the diagnosability properties without constructing an observer.

- We can check diagnosability of a critical event, such as a faulty event, and at the same time compute
  - delay of the diagnosis with respect to the occurrence of the event,
  - the uncertainty about the time at which that event occurred,
  - the duration of a possible initial transient where the diagnosis is not possible or not required.

[De Santis, Di Benedetto, 2017]
Secure diagnosability of hybrid systems

**Definition:** A linear hybrid system is $\sigma$–securely $\Omega$–diagnosable if there exists $T \in \mathbb{N}$ and a function $D : (\mathcal{U} \times \mathcal{Y} \times S^{p}_\sigma) \to \{0,1\}$, called diagnoser, s.t.

1. if $\xi(\hat{t}) \in \Omega \land (\hat{t} = 0 \lor (\xi(t) \notin \Omega, \forall t \in [0,\hat{t} - 1], \hat{t} > 0))$ then 
   
   $D(u|_{[0,\hat{t}+T-1]}, \eta|_{[0,\hat{t}+T]}) = 1$, with $\eta|_{[0,\hat{t}+T]} = (y_d|_{[0,\hat{t}+T]}, y|_{[0,\hat{t}+T]} + w|_{[0,\hat{t}+T]})$, for any generic input sequence $u|_{[0,\hat{t}+T-1]}$, with $u \in \mathcal{U}$, and for any attack sequence $w|_{[0,\hat{t}+T]} \in CS^{(\hat{t}+T)p}_\sigma$

2. if for any generic input sequence $u|_{[0,\hat{t} - 1]}$, with $u \in \mathcal{U}$, and for any attack sequence $w|_{[0,t]} \in CS^{tp}_\sigma$, $D(u|_{[0,t-1]}, \eta|_{[0,t]}) = 1$ and 
   
   $\left(t = 0 \lor \left( D \left(u|_{[0,t'-1]}, \eta|_{[0,t']} \right) = 0, \forall t' \in [0,t - 1], t > 0 \right) \right)$ then $\xi(\hat{t}) \in \Omega$, for some $\hat{t} \in [\max\{0,t - T\}, t]$. 

\[\text{DISMA, Torino, 23-27 sept. 2019}\]
Abstracting procedure

If with $\Omega = Q_C \times \mathbb{R}^n$, and discrete information is not sufficient to identify the discrete state, continuous output information is needed.

The abstracting procedure leads to a hybrid system with purely discrete information, that is equivalent to $H^{(1)}$ with respect to the secure diagnosability property.
Abstracting procedure

**Theorem:** Let the linear hybrid system $H^{(1)}$ be given, with $\delta(q) \geq \delta_{\text{min}}$, $\Delta(q) \neq \infty$, $\forall q \in Q$. If $H^{(3)}$ is $Q_C$-diagnosable, then $H^{(1)}$ is $\sigma$-securely $\Omega$-diagnosable with $\Omega = Q_C \times \mathbb{R}^n$. 

DISMA, Torino, 23-27sept. 2019
Approximate diagnosability

Let $F \subseteq X$ be a set of faulty states, $\rho \geq 0$ a desired accuracy, $\Omega = Q_C \times F$

- If one is able to construct a symbolic metric system approximating a continuous or hybrid control system $\Sigma$ (with an infinite number of states) in the sense of approximate simulation, we can check approximate diagnosability of $\Sigma$ on the symbolic system

- Symbolic models approximating continuous or hybrid control systems are extensively investigated. Papers working with approximate simulation that fit the framework of our contribution:

  - [Pola et al., TAC-16; Pola et al., Autom-08]
  - [Zamani et al., TAC-12], for possibly unstable nonlinear systems
  - [Girard et al., TAC-10], for incrementally stable switched systems
  - [Pola & Di Benedetto, TAC-14], for piecewise affine systems
Introduction
  • Cyber-Physical Systems (CPS)
  • Security for CPS

Modeling CPS as hybrid systems

Secure state estimation for hybrid systems
  • Observability and diagnosability
  • Secure mode distinguishability
  • Secure diagnosability
  • Approximate diagnosability

Conclusions and future work
Conclusions and ongoing work

- Secure state estimation problem for hybrid systems
- Predictability for hybrid systems
- Malicious attacks on both continuous and discrete output information
- More general representation of attacks
- Application of the results
Some references


Some references

- A. Grastien, L. Travé-Massuyès, and V. Puig. Solving diagnosability of hybrid systems via abstraction and discrete event techniques, 20th World Congress of the International Federation of Automatic Control (IFAC), 2017
- P. Caines et al., Current-state tree, CDC 1988.

DISMA, Torino, 23-27 sept. 2019
Some references


Thank you!