

Detection of Sensor Attack and Resilient State Estimation for Uniformly Observable Nonlinear Systems

Junsoo Kim*, Chanhwa Lee*, Hyungbo Shim*,
Yongsoon Eun[†], and Jin H. Seo*

Seoul National University*



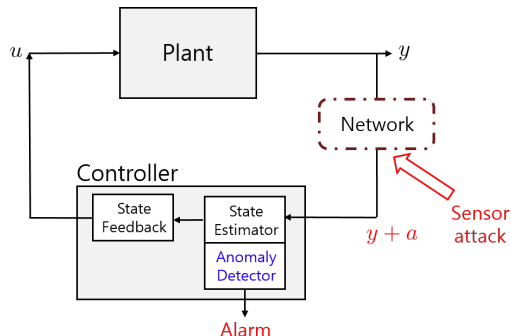
Daegu Gyeongbuk Inst. of Science & Tech[†]



55th IEEE Conference on Decision and Control

December 12, 2016

Feedback control systems under sensor attack



plant:

$$\dot{x} = f(x, u) \quad \in \mathbb{R}^n, u \in \mathbb{R}^m$$

$$y = h(x) + a \quad \in \mathbb{R}^p$$

- one may design anomaly detector to detect the attack (motivated by the fault detection technique)
- but, zero-dynamics attack for estimation error dynamics can deceive the anomaly detector¹

¹e.g., Teixeira, Shames, Sandberg, and Johansson, AUT 2015

Resilient state estimation problem¹

Meaning:

- **detection** of malicious sensor attack
- **identification** of attacked sensors
- **reconstruction** of the state even under sensor attack

Prior research [A, B, C, D, E]

The problem is solvable with the assumptions:

- **sparse attack**: limited attack resource
→ small number of sensors are compromised
- **redundant sensors**: observable despite eliminating several outputs

¹[A] Pasqualetti, Dorfler, and Bullo, TAC 2013
[B] Fawzi, Tabuada, and Diggavi, TAC 2014
[C] Chong, Wakaiki, and Hespanha, ACC 2015
[D] Lee, Shim, and Eun, ECC 2015
[E] Shoukry, Nuzzo, Bezzo, Sangiovanni-Vincentelli, Seshiz, and Tabuada, CDC 2015

Resilient state estimation problem¹

Meaning:

- **detection** of malicious sensor attack
- **identification** of attacked sensors
- **reconstruction** of the state even under sensor attack

Prior research [A, B, C, D, E]

The problem is solvable with the assumptions:

- **sparse attack**: limited attack resource
→ small number of sensors are compromised
- **redundant sensors**: observable despite eliminating several outputs

¹[A] Pasqualetti, Dorfler, and Bullo, TAC 2013

[B] Fawzi, Tabuada, and Diggavi, TAC 2014

[C] Chong, Wakaiki, and Hespanha, ACC 2015

[D] Lee, Shim, and Eun, ECC 2015

[E] Shoukry, Nuzzo, Bezzo, Sangiovanni-Vincentelli, Seshiz, and Tabuada, CDC 2015

Most results are for linear systems

- fundamental limitations in attack detection and identification [A]
 - ▶ includes actuator attack for linear descriptor systems
 - ▶ characterization of undetectable sensor attack
- introduction of redundant observability [B]
 - ▶ inspired by compressed sensing technique
 - ▶ relaxation of l_0 -minimization to convex optimization
- observer-based approach [C, D]
 - ▶ reduced optimization on finite set
 - ▶ design of multiple observers to search unattacked sensor combination

¹[A] Pasqualetti, Dorfler, and Bullo, TAC 2013

[B] Fawzi, Tabuada, and Diggavi, TAC 2014

[C] Chong, Wakaiki, and Hespanha, ACC 2015

[D] Lee, Shim, and Eun, ECC 2015

Shoukry et al. considered nonlinear systems [E]

they studied the case of nonlinear system with assumption of

$$\begin{aligned}x(t) &= \alpha(y(t), \dot{y}(t), \ddot{y}(t), \dots) \\u(t) &= \beta(y(t), \dot{y}(t), \ddot{y}(t), \dots)\end{aligned}\tag{*}$$

- both state and input are determined by measurement output
- state reconstruction without input information

→ strong condition of observability

¹[E] Shoukry, Nuzzo, Bezzo, Sangiovanni-Vincentelli, Seshiz, and Tabuada, CDC 2015

Resilient state estimation for uniformly observable systems

Our contribution

We present an attack-resilient estimation scheme for **uniformly observable nonlinear systems**

Uniformly observable?

⇔ observable for any input

⇔ state is determined by both output and input¹, i.e.,

$$x(t) = \alpha(y(t), \dot{y}(t), \ddot{y}(t), \dots, u(t), \dot{u}(t), \ddot{u}(t), \dots) \quad (**)$$

Note:

- (*) of [E] implies (**)
- obs. LTI sys. satisfies (**)

¹Teel and Praly, SCL 1994

Resilient state estimation for uniformly observable systems

Our contribution

We present an attack-resilient estimation scheme for **uniformly observable nonlinear systems**

Uniformly observable?

⇔ observable for any input

⇔ state is determined by both output and input¹, i.e.,

$$x(t) = \alpha(y(t), \dot{y}(t), \ddot{y}(t), \dots, u(t), \dot{u}(t), \ddot{u}(t), \dots)) \quad (**)$$

Note:

- (*) of [E] implies (**)
- obs. LTI sys. satisfies (**)

¹Teel and Praly, SCL 1994

Resilient state estimation for uniformly observable systems

Our contribution

We present an attack-resilient estimation scheme for **uniformly observable nonlinear systems**

Uniformly observable?

⇔ observable for any input

⇔ state is determined by both output and input¹, i.e.,

$$x(t) = \alpha(y(t), \dot{y}(t), \ddot{y}(t), \dots, u(t), \dot{u}(t), \ddot{u}(t), \dots) \quad (**)$$

Note:

- (*) of [E] implies (**)
- obs. LTI sys. satisfies (**)

¹Teel and Praly, SCL 1994

Resilient state estimation for uniformly observable systems

Our contribution

We present an attack-resilient estimation scheme for **uniformly observable nonlinear systems**

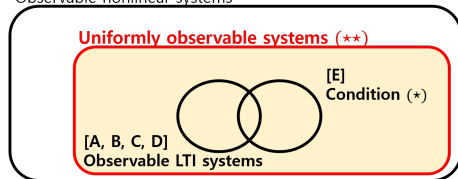
Uniformly observable?

⇔ observable for any input

⇔ state is determined by both output and input¹, i.e.,

$$x(t) = \alpha(y(t), \dot{y}(t), \ddot{y}(t), \dots, u(t), \dot{u}(t), \ddot{u}(t), \dots) \quad (**)$$

Observable nonlinear systems



Note:

- (*) of [E] implies (**)
- obs. LTI sys. satisfies (**)

¹Teel and Praly, SCL 1994

Contents

1. Preliminaries
2. Problem formulation & assumptions
3. Constructive design
 - 3.1. Partial high gain observers
 - 3.2. Attack-resilient state recovery with monitoring system
4. Conclusion

1. Preliminaries: a new way of observer construction¹

observable LTI system: $\dot{x} = Ax + Bu, \quad x \in \mathbb{R}^n, \quad u \in \mathbb{R}^m$
 $y_i = C_i x, \quad i \in [p] := \{1, 2, \dots, p\}$

- consider i -th measurement y_i only \implies may not be observable from y_i
- coordinate change with Kalman observable decomposition

$$\dot{z}_i = F_i z_i + G_i u$$

$$\dot{z}'_i = F'_{i,1} z_i + F'_{i,2} z'_i + G'_i u \implies \text{(Luenberger observer for } z_i\text{-subsystem)}$$

$$y_i = H_i z_i$$

$$\dot{\hat{z}}_i = F_i \hat{z}_i + G_i u + L_i (y_i - H_i \hat{z}_i)$$

- state recovery

$$\text{define } \Phi x := \begin{bmatrix} z_1 \\ \vdots \\ z_p \end{bmatrix} \implies \hat{x} = \Psi \begin{bmatrix} \hat{z}_1 \\ \vdots \\ \hat{z}_p \end{bmatrix}$$

where Ψ : left inverse matrix of Φ

¹Tanwani, Shim, and Liberzon, TAC 2013

1. Preliminaries: a new way of observer construction¹

observable LTI system: $\dot{x} = Ax + Bu, \quad x \in \mathbb{R}^n, \quad u \in \mathbb{R}^m$
 $y_i = C_i x, \quad i \in [p] := \{1, 2, \dots, p\}$

- consider i -th measurement y_i only \implies may not be observable from y_i
- coordinate change with **Kalman observable decomposition**

$$\dot{z}_i = F_i z_i + G_i u$$

$$\dot{z}'_i = F'_{i,1} z_i + F'_{i,2} z'_i + G'_i u \implies$$

(Luenberger observer for z_i -subsystem)

$$\dot{\hat{z}}_i = F_i \hat{z}_i + G_i u + L_i (y_i - H_i \hat{z}_i)$$

$$y_i = H_i z_i$$

- state recovery

$$\text{define } \Phi x := \begin{bmatrix} z_1 \\ \vdots \\ z_p \end{bmatrix} \implies \hat{x} = \Psi \begin{bmatrix} \hat{z}_1 \\ \vdots \\ \hat{z}_p \end{bmatrix}$$

where Ψ : left inverse matrix of Φ

¹Tanwani, Shim, and Liberzon, TAC 2013

1. Preliminaries: a new way of observer construction¹

observable LTI system: $\dot{x} = Ax + Bu, \quad x \in \mathbb{R}^n, \quad u \in \mathbb{R}^m$
 $y_i = C_i x, \quad i \in [p] := \{1, 2, \dots, p\}$

- consider i -th measurement y_i only \implies may not be observable from y_i
- coordinate change with **Kalman observable decomposition**

$$\dot{z}_i = F_i z_i + G_i u$$

$$\dot{z}'_i = F'_{i,1} z_i + F'_{i,2} z'_i + G'_i u \implies \text{(Luenberger observer for } z_i\text{-subsystem)}$$

$$\dot{\hat{z}}_i = F_i \hat{z}_i + G_i u + L_i (y_i - H_i \hat{z}_i)$$

$$y_i = H_i z_i$$

- state recovery

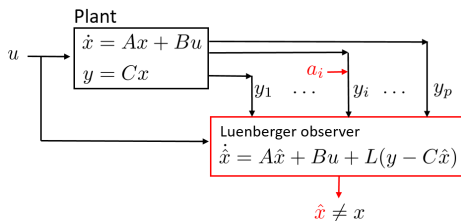
$$\text{define } \Phi x := \begin{bmatrix} z_1 \\ \vdots \\ z_p \end{bmatrix} \implies \hat{x} = \Psi \begin{bmatrix} \hat{z}_1 \\ \vdots \\ \hat{z}_p \end{bmatrix}$$

where Ψ : **left inverse** matrix of Φ

¹Tanwani, Shim, and Liberzon, TAC 2013

Benefit arises when sparse sensor attack exists¹

classical state observer

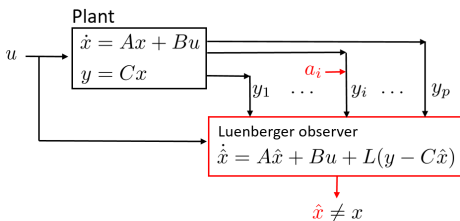


- one observer for p outputs
- even sparse attack
⇒ estimation fails

¹[D] Lee, Shim, and Eun, ECC 2015

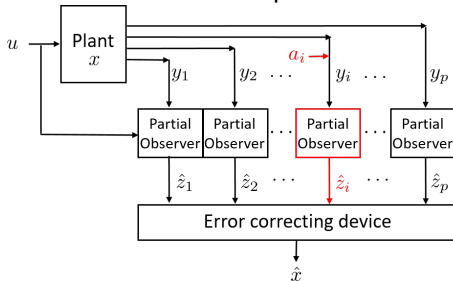
Benefit arises when sparse sensor attack exists¹

classical state observer



- one observer for p outputs
- even sparse attack
⇒ estimation fails

observers for each output



- p -partial observers for each output
- can preserve many unattacked observers
- so, enables some error correcting algorithm

¹[D] Lee, Shim, and Eun, ECC 2015

2. Problem formulation & assumptions

$$\begin{aligned} \text{plant:} \quad \dot{x} &= f(x) + g(x)u, & x &\in \mathbb{R}^n, \quad u \in \mathbb{R} \\ y_i &= h_i(x) + a_i(t), & i &\in [p] = \{1, 2, \dots, p\} \end{aligned}$$

Assumption (input & state boundedness)

$$\exists R_x > 0, R_u > 0 \quad \text{s.t.} \quad \|x(t)\| \leq R_x, \quad |u(t)| \leq R_u, \quad \forall t \geq 0$$

Assumption (q -sparse attack)

up to q sensors are attacked and $2q < p$

Let σ_{unattack} be the set of indices of unattacked sensors:

$$\sigma_{\text{unattack}} := \{i \in [p] : a_i(t) \equiv 0\}$$

Uniformly observable decomposition³ for each sensor

Assumption (uniformly observable decomposition)

For each y_i , system is diffeomorphic to the form

$$\begin{aligned}\dot{z}_i &= F_i(z_i) + G_i(z_i)u \\ \dot{z}'_i &= F'_i(z_i, z'_i) + G'_i(z_i, z'_i)u \\ y_i &= H_i(z_i)\end{aligned}$$

where z_i -subsystem with y_i is uniformly observable.

By uniform observability, w.l.o.g., z_i -subsystem takes² the form of

$$\dot{z}_i = \begin{bmatrix} \dot{z}_{i,1} \\ \dot{z}_{i,2} \\ \vdots \\ \dot{z}_{i,n_i} \end{bmatrix} = \begin{bmatrix} z_{i,2} \\ \vdots \\ z_{i,n_i} \\ \alpha_i(z_i) \end{bmatrix} + \begin{bmatrix} \beta_{i,1}(z_{i,1}) \\ \beta_{i,2}(z_{i,1}, z_{i,2}) \\ \vdots \\ \beta_{i,n_i}(z_{i,1}, \dots, z_{i,n_i}) \end{bmatrix} u$$
$$y_i = z_{i,1}$$

²Gauthier, Hammouri, and Othman, TAC 1992

³Shim and Tanwani, IJRN 2014

Observability for state recovery by collecting observable parts

To recover x from the partial estimates of observable substate z_i , we need a certain observability.

Let Φ be the mapping from x to the observable substates:

$$\begin{bmatrix} z_1 \\ \vdots \\ z_p \end{bmatrix} = \Phi(x).$$

Then, required observability is the **existence of a left inverse Ψ of Φ** :

$$x = \Psi \left(\begin{bmatrix} z_1 \\ \vdots \\ z_p \end{bmatrix} \right)$$

- If Φ is **injective immersion** or **Bi-Lipschitz** on the domain of interest, then \exists a left inverse Ψ of Φ .
- w.l.o.g., Ψ can be taken to be globally Lipschitz.

Redundant observability

For state recovery under sensor attack, we need in fact stronger observability.

Let

σ : the index subset of $[p]$ whose cardinality is $p - q$

$$\Phi^\sigma(x) := \text{stack}_{i \in \sigma} \{z_i\}$$

Definition

The system is **q -redundant observable** if

$$\exists \text{ left inverse } \Psi^\sigma \text{ of } \Phi^\sigma, \quad \forall \sigma \subset [p]$$

Assumption (redundant observability)

The system is $2q$ -redundant observable.

This means the system is still observable with any $p - 2q$ sensors.

Redundant observability

For state recovery under sensor attack, we need in fact stronger observability.

Let

σ : the index subset of $[p]$ whose cardinality is $p - q$

$$\Phi^\sigma(x) := \text{stack}_{i \in \sigma} \{z_i\}$$

Definition

The system is **q -redundant observable** if

$$\exists \text{ left inverse } \Psi^\sigma \text{ of } \Phi^\sigma, \quad \forall \sigma \subset [p]$$

Assumption (redundant observability)

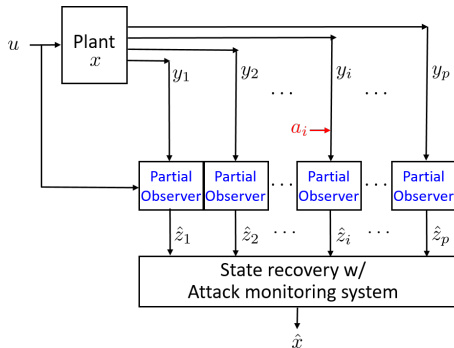
The system is **$2q$ -redundant observable**.

This means the system is still observable with any $p - 2q$ sensors.

3. Constructive design

3.1. Partial high gain observers

3.2. Attack-resilient state recovery with monitoring system



Partial high gain observers

Uniformly observable decomposition assumption immediately yields the high-gain observer for each observable sub-state z_i from y_i .

Lemma (High gain observer¹)

for each z_i , $\exists \theta_i \gg 1$, $L_i(\theta_i) \in \mathbb{R}^{n_i \times 1}$, $k_i(\theta_i) \in \mathbb{R}$ s.t. the observer

$$\dot{\hat{z}}_i = \begin{bmatrix} \dot{\hat{z}}_{i,1} \\ \dot{\hat{z}}_{i,2} \\ \vdots \\ \dot{\hat{z}}_{i,n_i} \end{bmatrix} = \begin{bmatrix} \hat{z}_{i,2} \\ \vdots \\ \hat{z}_{i,n_i} \\ \alpha_i(\hat{z}_i) \end{bmatrix} + \begin{bmatrix} \beta_{i,1}(\hat{z}_{i,1}) \\ \beta_{i,2}(\hat{z}_{i,1}, \hat{z}_{i,2}) \\ \vdots \\ \beta_{i,n_i}(\hat{z}_{i,1}, \dots, \hat{z}_{i,n_i}) \end{bmatrix} u - L_i(\theta_i)(\hat{z}_{i,1} - y_i)$$

guarantees

$$\|\hat{z}_i(t) - z_i(t)\| \leq k_i(\theta_i)e^{-\frac{\theta_i}{4}t} \quad \text{for } i \in \sigma_{\text{unattack}}$$

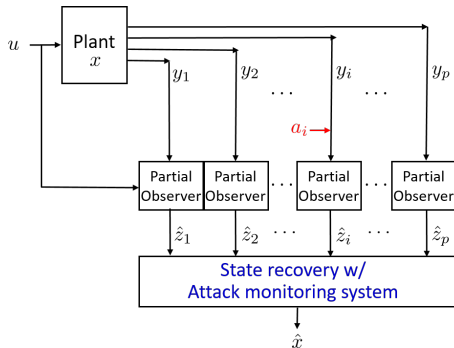
where $\hat{z}_i(0) := 0$ and $z_i(0)$: bounded.

¹Gauthier, Hammouri, and Othman, TAC 1992

3. Constructive design

3.1. Partial high gain observers

3.2. Attack-resilient state recovery with monitoring system



Idea for attack detection & finding unattacked sensors

- $z^\sigma(t) := \text{stack}_{i \in \sigma} \{z_i(t)\} \in \text{Im}(\Phi^\sigma)$ for all σ and $t \geq 0$
- $z^\sigma \in \text{Im}(\Phi^\sigma) \iff z^\sigma = \Phi^\sigma(\Psi^\sigma(z^\sigma))$
- $\hat{z}_i(t) \rightarrow z_i(t)$ for $i \in \sigma_{\text{unattack}}$ & $\hat{z}_i(t) \not\rightarrow z_i(t)$ for $i \notin \sigma_{\text{unattack}}$

Proposition

Under assumptions of q -sparse attack and $2q$ -redundant observability,

no attack on the sensors y_i , $\forall i \in \sigma$



$$\lim_{t \rightarrow \infty} \|\hat{z}^\sigma(t) - \Phi^\sigma(\Psi^\sigma(\hat{z}^\sigma(t)))\| = 0$$



- once an index set $\sigma \subset \sigma_{\text{unattack}}$ is identified, state is recovered by

$$\hat{x}(t) := \Psi^\sigma(\hat{z}^\sigma(t))$$

- in practice,  is not implementable

Idea for attack detection & finding unattacked sensors

- $z^\sigma(t) := \text{stack}_{i \in \sigma} \{z_i(t)\} \in \text{Im}(\Phi^\sigma)$ for all σ and $t \geq 0$
- $z^\sigma \in \text{Im}(\Phi^\sigma) \iff z^\sigma = \Phi^\sigma(\Psi^\sigma(z^\sigma))$
- $\hat{z}_i(t) \rightarrow z_i(t)$ for $i \in \sigma_{\text{unattack}}$ & $\hat{z}_i(t) \not\rightarrow z_i(t)$ for $i \notin \sigma_{\text{unattack}}$

Proposition

Under assumptions of q -sparse attack and $2q$ -redundant observability,

no attack on the sensors y_i , $\forall i \in \sigma$




$$\lim_{t \rightarrow \infty} \|\hat{z}^\sigma(t) - \Phi^\sigma(\Psi^\sigma(\hat{z}^\sigma(t)))\| = 0$$



- once an index set $\sigma \subset \sigma_{\text{unattack}}$ is identified, state is recovered by

$$\hat{x}(t) := \Psi^\sigma(\hat{z}^\sigma(t))$$

- in practice, () is not implementable

Implemented attack detection

Define

$$\text{residual}^\sigma(t) := \|\hat{z}^\sigma(t) - \Phi^\sigma(\Psi^\sigma(\hat{z}^\sigma(t)))\|$$

$$\text{threshold}^\sigma(t) := (\text{Lip}(\Phi^\sigma \circ \Psi^\sigma) + 1) \max_{i \in [p]} \{k_i(\theta_i) e^{-\frac{\theta_i}{4}t}\},$$

(Lip(\cdot) : Lipschitz const)

Theorem (attack detection)

Under assumptions of q -sparse attack and $2q$ -redundant observability,

- $\exists t, \text{residual}^\sigma(t) > \text{threshold}^\sigma(t) \Rightarrow \exists$ attacked sensor in $\sigma \subset [p]$
- $\forall t, \text{residual}^\sigma(t) \leq \text{threshold}^\sigma(t) \Rightarrow$

$$\|\hat{x}(t) - x(t)\| \leq \max_{i \in [p]} \{M k_i(\theta_i) e^{-\frac{\theta_i}{4}t}\} \rightarrow 0$$

as $t \rightarrow \infty$ where $M > 0$: a constant

Attack-resilient state recovery with monitoring system

Let $\sigma(j)$, $j = 1, 2, \dots, \binom{p}{p-q}$, be the index subset of $[p]$ whose cardinality is $p - q$.

Theorem (Resilient state estimation)

Under assumptions of $2q$ -sparse attack and q -redundant observability, monitor the sensor attack by

$$j \leftarrow j + 1 \quad \text{if residual}^{\sigma(j)}(t) > \text{threshold}^{\sigma(j)}(t),$$

and construct the estimate by

$$\hat{x}(t) = \Psi^{\sigma(j)}(\hat{z}^{\sigma(j)}(t)).$$

Then, $\|\hat{x}(t) - x(t)\| \leq \max_{i \in [p]} \{Mk_i(\theta_i)e^{-\frac{\theta_i}{4}t}\} \rightarrow 0$ as $t \rightarrow \infty$.

- unlike [A,B], no need to solve optimization at every time step
- unlike [C], there are just p observers

³[A] Pasqualetti et al., 2013 / [B] Fawzi et al., 2014 / [C] Chong et al., 2013

Attack-resilient state recovery with monitoring system

Let $\sigma(j)$, $j = 1, 2, \dots, \binom{p}{p-q}$, be the index subset of $[p]$ whose cardinality is $p - q$.

Theorem (Resilient state estimation)

Under assumptions of $2q$ -sparse attack and q -redundant observability, monitor the sensor attack by

$$j \leftarrow j + 1 \quad \text{if residual}^{\sigma(j)}(t) > \text{threshold}^{\sigma(j)}(t),$$

and construct the estimate by

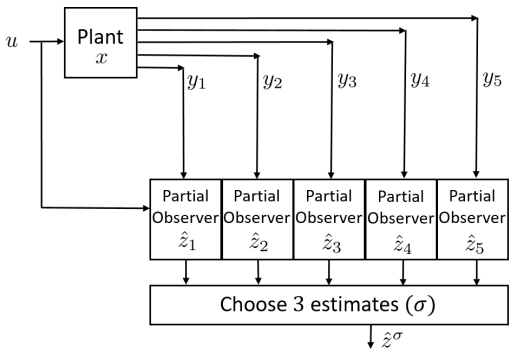
$$\hat{x}(t) = \Psi^{\sigma(j)}(\hat{z}^{\sigma(j)}(t)).$$

Then, $\|\hat{x}(t) - x(t)\| \leq \max_{i \in [p]} \{Mk_i(\theta_i)e^{-\frac{\theta_i}{4}t}\} \rightarrow 0$ as $t \rightarrow \infty$.

- unlike [A,B], no need to solve optimization at every time step
- unlike [C], there are just p observers

³[A] Pasqualetti et al., 2013 / [B] Fawzi et al., 2014 / [C] Chong et al., 2013

example: $p = 5, q = 2 \Rightarrow \binom{5}{5-2} = 10$ cases



$$\sigma = \{1, 2, 3\}$$

$$\downarrow$$

$$\{1, 2, 4\}$$

$$\downarrow$$

$$\{1, 2, 5\}$$

$$\downarrow$$

$$\{1, 3, 4\}$$

$$\downarrow$$

$$\{1, 3, 5\}$$

$$\downarrow$$

$$\{1, 4, 5\}$$

$$\downarrow$$

$$\{2, 3, 4\}$$

$$\downarrow$$

$$\{2, 3, 5\}$$

$$\downarrow$$

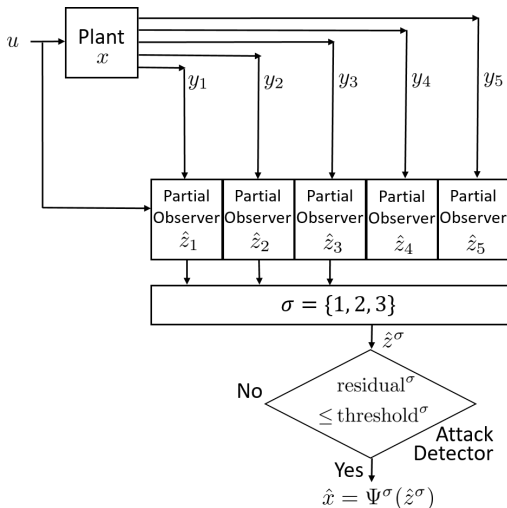
$$\{2, 4, 5\}$$

$$\downarrow$$

$$\{3, 4, 5\}$$

- no alarm \Rightarrow just monitoring & state recovery
- next residual immediately available
- does not consider all cases at each time step

example: $p = 5, q = 2 \Rightarrow \binom{5}{5-2} = 10$ cases



$\sigma = \{1, 2, 3\}$

\downarrow
 $\{1, 2, 4\}$

\downarrow
 $\{1, 2, 5\}$

\downarrow
 $\{1, 3, 4\}$

\downarrow
 $\{1, 3, 5\}$

\downarrow
 $\{1, 4, 5\}$

\downarrow
 $\{2, 3, 4\}$

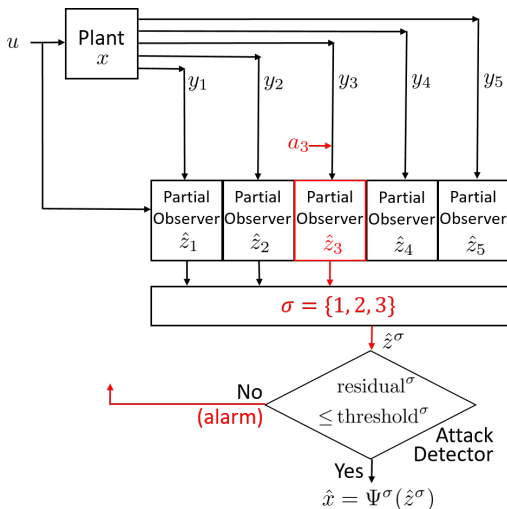
\downarrow
 $\{2, 3, 5\}$

\downarrow
 $\{2, 4, 5\}$

\downarrow
 $\{3, 4, 5\}$

- no alarm \Rightarrow just monitoring & state recovery
- next residual immediately available
- does not consider all cases at each time step

example: $p = 5, q = 2 \Rightarrow \binom{5}{5-2} = 10$ cases



$\sigma = \{1, 2, 3\}$

\downarrow
 $\{1, 2, 4\}$

\downarrow
 $\{1, 2, 5\}$

\downarrow
 $\{1, 3, 4\}$

\downarrow
 $\{1, 3, 5\}$

\downarrow
 $\{1, 4, 5\}$

\downarrow
 $\{2, 3, 4\}$

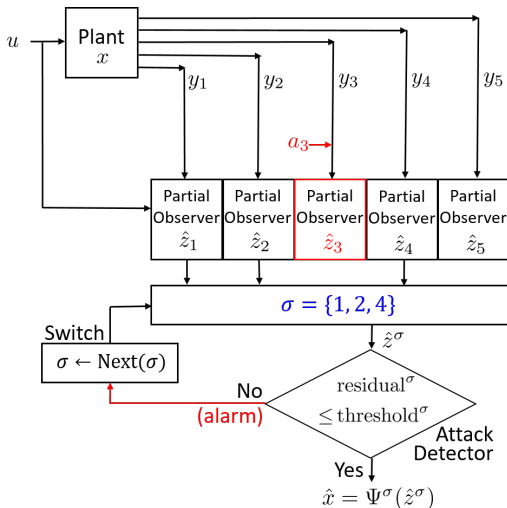
\downarrow
 $\{2, 3, 5\}$

\downarrow
 $\{2, 4, 5\}$

\downarrow
 $\{3, 4, 5\}$

- no alarm \Rightarrow just monitoring & state recovery
- next residual immediately available
- does not consider all cases at each time step

example: $p = 5, q = 2 \Rightarrow \binom{5}{5-2} = 10$ cases



$\sigma = \{1, 2, 3\}$

↓

$\{1, 2, 4\}$

↓

$\{1, 2, 5\}$

↓

$\{1, 3, 4\}$

↓

$\{1, 3, 5\}$

↓

$\{1, 4, 5\}$

↓

$\{2, 3, 4\}$

↓

$\{2, 3, 5\}$

↓

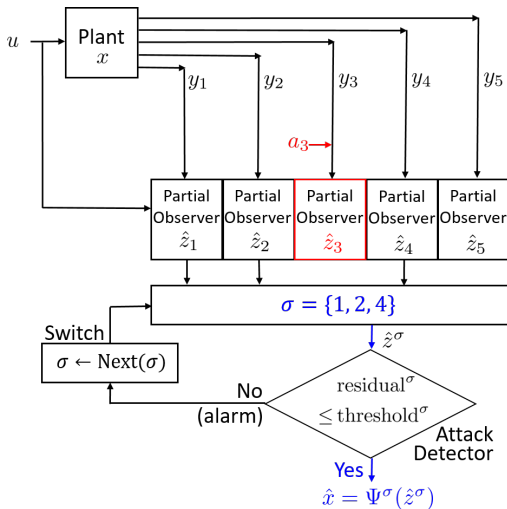
$\{2, 4, 5\}$

↓

$\{3, 4, 5\}$

- no alarm \Rightarrow just monitoring & state recovery
- next residual immediately available
- does not consider all cases at each time step

example: $p = 5, q = 2 \Rightarrow \binom{5}{5-2} = 10$ cases



$\sigma = \{1, 2, 3\}$

↓

$\{1, 2, 4\}$

↓

$\{1, 2, 5\}$

↓

$\{1, 3, 4\}$

↓

$\{1, 3, 5\}$

↓

$\{1, 4, 5\}$

↓

$\{2, 3, 4\}$

↓

$\{2, 3, 5\}$

↓

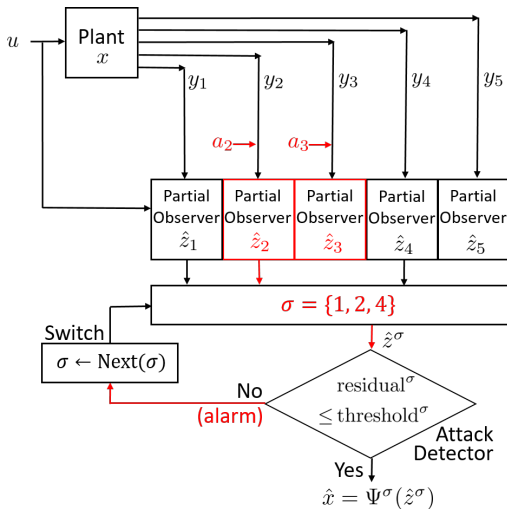
$\{2, 4, 5\}$

↓

$\{3, 4, 5\}$

- no alarm \Rightarrow just monitoring & state recovery
- next residual immediately available
- does not consider all cases at each time step

example: $p = 5, q = 2 \Rightarrow \binom{5}{5-2} = 10$ cases



$$\sigma = \{1, 2, 3\}$$

↓

$$\{1, 2, 4\}$$

↓

$$\{1, 2, 5\}$$

↓

$$\{1, 3, 4\}$$

↓

$$\{1, 3, 5\}$$

↓

$$\{1, 4, 5\}$$

↓

$$\{2, 3, 4\}$$

↓

$$\{2, 3, 5\}$$

↓

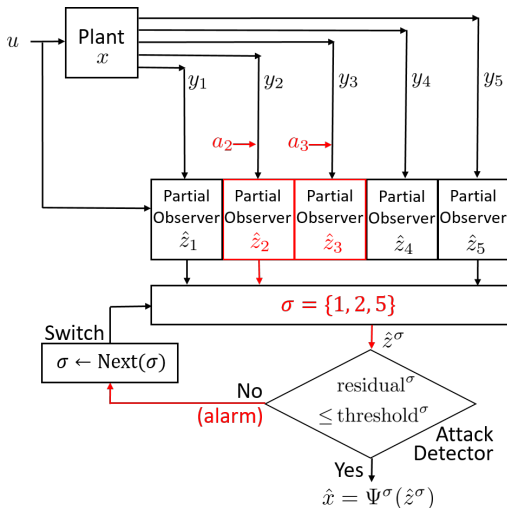
$$\{2, 4, 5\}$$

↓

$$\{3, 4, 5\}$$

- no alarm \Rightarrow just monitoring & state recovery
- next residual immediately available
- does not consider all cases at each time step

example: $p = 5, q = 2 \Rightarrow \binom{5}{5-2} = 10$ cases



$\sigma = \{1, 2, 3\}$

$\{1, 2, 4\}$

$\{1, 2, 5\}$

$\{1, 3, 4\}$

$\{1, 3, 5\}$

$\{1, 4, 5\}$

$\{2, 3, 4\}$

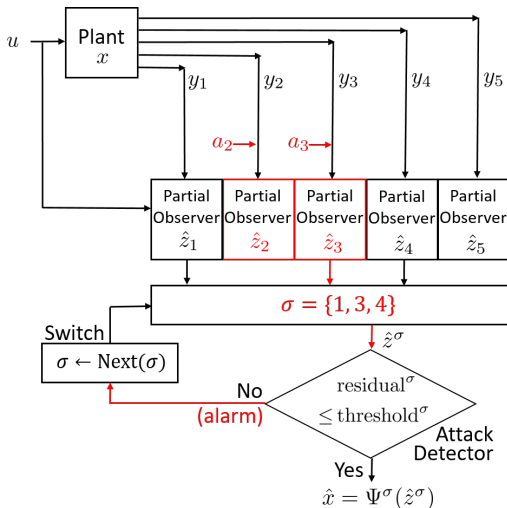
$\{2, 3, 5\}$

$\{2, 4, 5\}$

$\{3, 4, 5\}$

- no alarm \Rightarrow just monitoring & state recovery
- next residual immediately available
- does not consider all cases at each time step

example: $p = 5, q = 2 \Rightarrow \binom{5}{5-2} = 10$ cases



$\sigma = \{1, 2, 3\}$

\downarrow
 $\{1, 2, 4\}$

\downarrow
 $\{1, 2, 5\}$

\downarrow
 $\{1, 3, 4\}$

\downarrow
 $\{1, 3, 5\}$

\downarrow
 $\{1, 4, 5\}$

\downarrow
 $\{2, 3, 4\}$

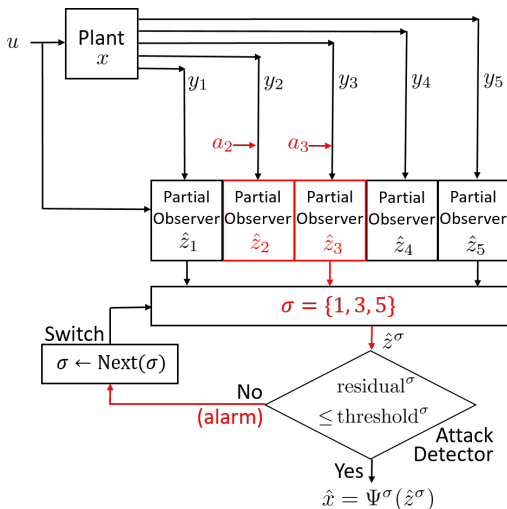
\downarrow
 $\{2, 3, 5\}$

\downarrow
 $\{2, 4, 5\}$

\downarrow
 $\{3, 4, 5\}$

- no alarm \Rightarrow just monitoring & state recovery
- next residual immediately available
- does not consider all cases at each time step

example: $p = 5, q = 2 \Rightarrow \binom{5}{5-2} = 10$ cases



$\sigma = \{1, 2, 3\}$

$\{1, 2, 4\}$

$\{1, 2, 5\}$

$\{1, 3, 4\}$

$\{1, 3, 5\}$

$\{1, 4, 5\}$

$\{2, 3, 4\}$

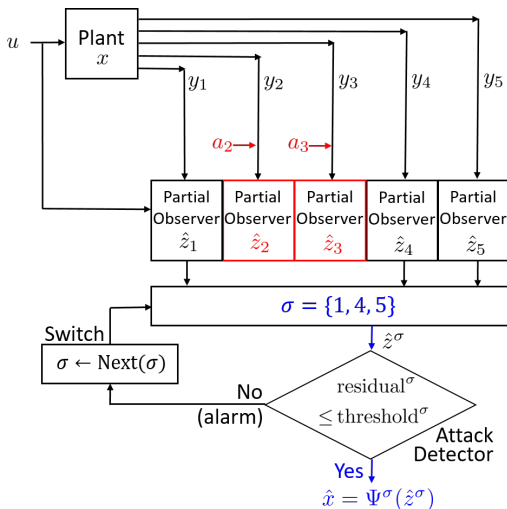
$\{2, 3, 5\}$

$\{2, 4, 5\}$

$\{3, 4, 5\}$

- no alarm \Rightarrow just monitoring & state recovery
- next residual immediately available
- does not consider all cases at each time step

example: $p = 5, q = 2 \Rightarrow \binom{5}{5-2} = 10$ cases



$$\sigma = \{1, 2, 3\}$$

$$\downarrow$$

$$\{1, 2, 4\}$$

$$\downarrow$$

$$\{1, 2, 5\}$$

$$\downarrow$$

$$\{1, 3, 4\}$$

$$\downarrow$$

$$\{1, 3, 5\}$$

$$\downarrow$$

$$\{1, 4, 5\}$$

$$\downarrow$$

$$\{2, 3, 4\}$$

$$\downarrow$$

$$\{2, 3, 5\}$$

$$\downarrow$$

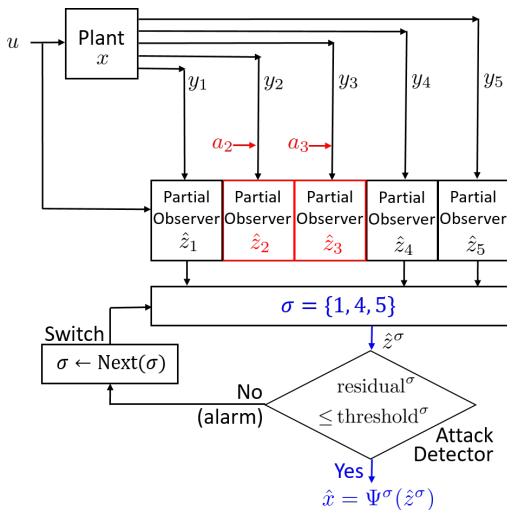
$$\{2, 4, 5\}$$

$$\downarrow$$

$$\{3, 4, 5\}$$

- no alarm \Rightarrow just monitoring & state recovery
- next residual immediately available
- does not consider all cases at each time step

example: $p = 5, q = 2 \Rightarrow \binom{5}{5-2} = 10$ cases



$$\sigma = \{1, 2, 3\}$$

$$\downarrow$$

$$\{1, 2, 4\}$$

$$\downarrow$$

$$\{1, 2, 5\}$$

$$\downarrow$$

$$\{1, 3, 4\}$$

$$\downarrow$$

$$\{1, 3, 5\}$$

$$\downarrow$$

$$\{1, 4, 5\}$$

$$\downarrow$$

$$\{2, 3, 4\}$$

$$\downarrow$$

$$\{2, 3, 5\}$$

$$\downarrow$$

$$\{2, 4, 5\}$$

$$\downarrow$$

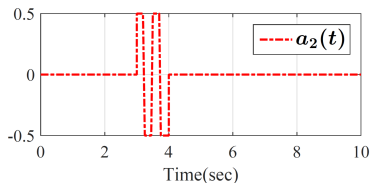
$$\{3, 4, 5\}$$

- no alarm \Rightarrow just monitoring & state recovery
- next residual immediately available
- does not consider all cases at each time step

Simulation for toy example

- case of $p = 4$ outputs, $q = 1$ sparse sensor attack

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = \begin{bmatrix} -2x_1 \\ -x_1 - x_2 \\ -(x_1 - x_2)^2 - x_3 \end{bmatrix} + \begin{bmatrix} 1 \\ 2 \\ 2(x_2 - x_1) \end{bmatrix} u$$
$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} = \begin{bmatrix} x_2 + x_3 - (x_1 - x_2)^2 \\ x_1 - x_3 + (x_1 - x_2)^2 \\ x_2 - 2x_1 \\ x_1 - x_2 + x_3 - (x_1 - x_2)^2 \end{bmatrix} + \begin{bmatrix} 0 \\ a_2 \\ 0 \\ 0 \end{bmatrix}$$



a_2 injected in y_2 at $t = 3$

- system is 2-red. observable: any 2 selection of z_i 's are left invertible

$$z_1 = \begin{bmatrix} x_2 + x_3 - (x_1 - x_2)^2 \\ -x_1 - x_2 - x_3 + (x_1 - x_2)^2 \end{bmatrix}$$

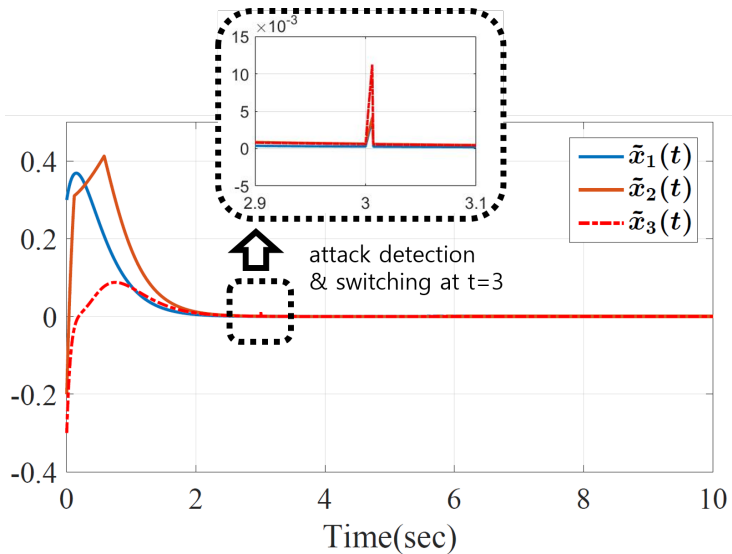
$$z_2 = \begin{bmatrix} x_1 - x_3 + (x_1 - x_2)^2 \\ x_3 - 2x_1 - (x_1 - x_2)^2 \end{bmatrix}$$

$$z_3 = \begin{bmatrix} x_2 - 2x_1 \\ 3x_1 - x_2 \end{bmatrix}$$

$$z_4 = x_1 - x_2 + x_3 - (x_1 - x_2)^2$$

\therefore resilient state estimation available!

Simulation result: plot of $\tilde{x}(t) = \hat{x}(t) - x(t)$



Conclusion

Our contribution

We present an attack-resilient estimation scheme for uniformly observable nonlinear systems

1. nonlinear generalization of resilient estimation scheme

	LTI system	Uniformly observable system
decomposition	Kalman obs. decomp.	Uniformly obs. decomp.
state observer	Luenberger observer	High gain observer
redundancy notion	red. full.col.rank	red. injective immersion

2. computationally efficient monitoring system

- ▶ residual & threshold analysis \Rightarrow detects every influential attacks
- ▶ simple switching logic: searching another estimate candidate only when attack alarm rings

Thank you for your time! (kjs9044@cdsl.kr)