# Local Identification of Sensor Attack and Distributed Resilient State Estimation for Linear Systems

**Junsoo Kim**, Jin Gyu Lee, Chanhwa Lee,
Hyungbo Shim, and Jin H. Seo

Seoul National Univ., Korea

Control & Dynamic Systems Lab.

The 57th IEEE Conference on Decision and Control

December 17, 2018

# Control systems under sensor attack

plant:

$$
\begin{aligned}
\dot{x}(t) &= Ax(t) && \in \mathbb{R}^n \\
\begin{bmatrix} y_1(t) \\ y_2(t) \\ \vdots \\ y_p(t) \end{bmatrix} &= \begin{bmatrix} C_1 \\ C_2 \\ \vdots \\ C_p \end{bmatrix} x(t) + \begin{bmatrix} a_1(t) \\ a_2(t) \\ \vdots \\ a_p(t) \end{bmatrix} && \in \mathbb{R}^p \\
&= Cx(t) + a(t)
\end{aligned}
$$

The attack $a(t) = \left[a_1(t), a_2(t), \cdots a_p(t)\right]^T$

- is unknown, might be arbitrarily large
- might be carefully designed not to be detected at the controller (e.g. zero-dynamics attack[1])

[1] Teixeira, Shames, Sandberg, and Johansson, AUT 2015

# As a defender: resilient state estimation

plant having $p$-sensors:

$$\begin{aligned} \dot{x} &= Ax && \in \mathbb{R}^n \\ y &= Cx + a && \in \mathbb{R}^p \end{aligned}$$

up to $q$-sensors are attacked out of $p$-sensors
(attack resource is limited in usual)

objective:

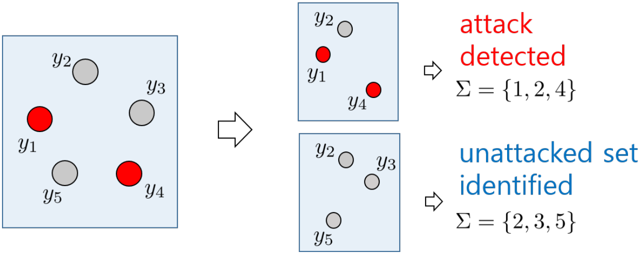
identification of unattacked $p - q$ sensors (out of $p$-sensors)
$\rightarrow$ state estimation with identified sensors

# An existing scheme for identification of unattacked sensors[1]

e.g. $p = 5, \; q = 2 \quad \Longrightarrow \quad$ finding $(p - q = 3)$-unattacked sensors

1. prepare a detection scheme for each $(p - q = 3)$-sensors s.t.

attack alarm rings $\Longleftrightarrow$ indicated $(p - q = 3)$-sensors include an attacked sensor

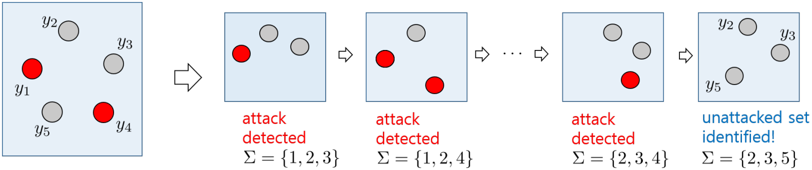



[1]Kim, Lee, Shim, Eun, and Seo, TAC 2018 (early access)

# A scheme for identification of unattacked sensors[1]

e.g. $p = 5, \;\; q = 2 \quad \Longrightarrow \quad$ finding $(p - q = 3)$-unattacked sensors

2. inspect $\binom{p}{q} = \binom{5}{2} = 10$ cases




Applying the detection scheme for each selection one by one, it eventually finds out a set of unattacked sensors.

[1] Kim, Lee, Shim, Eun, and Seo, TAC 2018 (early access)

# The scheme is valid for $2q$-redundant observable[1] systems.

"$2q$-redundant observable $\iff$ observable with any $p-2q$ sensors"

## Definition

The pair $(A, C)$ is $2q$-redundant observable iff

$$\operatorname{rank}\begin{bmatrix} C' \\ C'A \\ \vdots \\ C'A^{n-1} \end{bmatrix} = n$$

for any $C'$: $2q$-rows removed from $C$.

## Theorem

Every injection of $q$-sensor attacks is identifiable if
the pair $(A, C)$ is $2q$-redundant observable.

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

# Solutions based on $2q$-redundant observability

However, the problem is generally NP-hard, and is combinatorial in nature[1] in most cases.

e.g.

- observer-based approach
  assumption: $2q$-redundant observability
  $\rightarrow$ Chong, Wakaiki, and Hespanha, ACC 2015
  $\rightarrow$ constructs $\binom{p}{q} \times \binom{p-q}{q}$ observers
  $\rightarrow$ Lee, Shim, and Eun, ECC 2015
  $\rightarrow$ cardinality of searching space for optimization $= \binom{p}{q}$

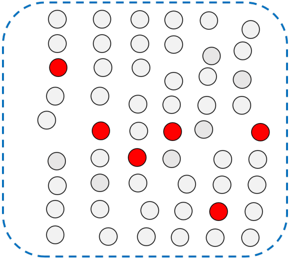
- nonlinear generalization
  assumption: $2q$-redundant observability for uniformly observable nonlinear systems
  $\rightarrow$ Kim, Lee, Shim, Eun, and Seo, TAC 2018 (early access)
  $\rightarrow$ $\binom{p}{q}/2$ inspections expected when attack detected

...so they require a substantial computational effort as $p \uparrow$

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

# Countermeasure: Local identification of sensor attack[1]

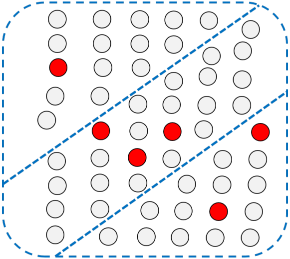
e.g. $p = 45$, $q = 6$:



(centralized)

$$\binom{p}{q} = \binom{45}{6}$$

$= 8145060$ cases



(distributed, 3-local groups)

$$3 \times \binom{p/3}{q} = 3 \times \binom{15}{6}$$

$= 15015$ cases

computational complexity: $\binom{p}{q} = \binom{\sum_{l=1}^{k} p_l}{q} \gg \sum_{l=1}^{k} \binom{p_l}{q}$

[1] Pasqualetti, Dorfler, and Bullo, CDC 2015

# So, we propose distributed resilient state estimation.

$p$-sensors partitioned into $k$-local groups:

$$\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_p \end{bmatrix} = Cx + a \qquad \rightarrow \qquad \begin{cases} y_{P_1} = C_{P_1}x + a_{P_1} \\ y_{P_2} = C_{P_2}x + a_{P_2} \\ \qquad\vdots \\ y_{P_k} = C_{P_k}x + a_{P_k} \end{cases}$$

where

$$\{1, 2, \cdots, p\} = \bigcup_{l=1}^{k} P_l \qquad \text{and} \qquad P_i \cap P_j = \emptyset, \quad \text{if } i \neq j$$

For each $l$-th local sensor group,

- local output $y_{P_l}$: a subset of $\{y_1, \cdots, y_p\}$
- $a_{P_l}$: up to $q$-local attack
- Note: $(A, C_{P_l})$ may not be observable (even though $(A, C)$ is observable)

# So, we propose distributed resilient state estimation.

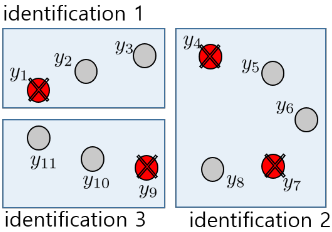
## problem formulation

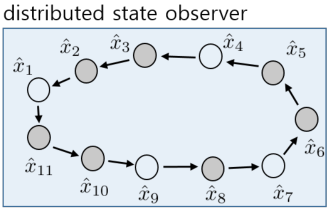
plant:

$$\dot{x} = Ax$$
$$y_{P_l} = C_{P_l} x + a_{P_l}, \quad l = 1, \ldots, k$$

objective:

1. local identification of unattacked sensors for each $y_{P_l}$
2. state estimation with identified sensors in a distributed manner
   $\because$ not observable from $y_{P_l}$



# Contents

- Distributed resilient state estimation problem
- Observability notion for local identification of sensor attack
- Design of distributed resilient state observer

# Observability notion for local identification of sensor attack

Q. centralized attack identification $\rightarrow$ $2q$-redundant observability

distributed attack identification $\rightarrow$ ???

A1. $2q$-redundant observability from each local sensor group

$\rightarrow$ (restrictive) The system is generally not even observable from a local sensor group.

... then, what if it requires sensing redundancy only and does not require full state observability?

# A2. the notion of $2q$-redundant sensors

We introduce the local version of redundancy condition which does not require observability.

plant with $p_l$-local sensors:

$$\dot{x} = Ax$$
$$y_{P_l} = C_{P_l} x + a_{P_l} \in \mathbb{R}^{p_l}$$

**Definition**

The pair $(A, C_{P_l})$ is said $2q$-redundant if

$$\operatorname{rank} \begin{bmatrix} C'_{P_l} \\ C'_{P_l} A \\ \vdots \\ C'_{P_l} A^{n-1} \end{bmatrix} = \operatorname{rank} \begin{bmatrix} C_{P_l} \\ C_{P_l} A \\ \vdots \\ C_{P_l} A^{n-1} \end{bmatrix} \leq n$$

for any $C'_{P_l}$: $2q$-rows removed from $C_{P_l}$.

Meaning:
It has $2q$-redundant local sensors so that
it does not lose its observability rank removing any $2q$-sensors.

## A2. the notion of $2q$-redundant sensors

We introduce the local version of redundancy condition which does not require observability.

plant with $p_l$-local sensors:

$$\dot{x} = Ax$$
$$y_{P_l} = C_{P_l} x + a_{P_l} \in \mathbb{R}^{p_l}$$

There is no need of full state observability
for local identification of sensor attack.

**Theorem**

Every injection of $q$-local attacks is locally identifiable iff the pair $(A, C_{P_l})$ is $2q$-redundant.

# Contents

- Distributed resilient state estimation problem
- Observability notion for local identification of sensor attack
- Design of distributed resilient state observer

## First, design "partial" observer for each $y_i \in \mathbb{R}$, $i = 1, 2, \cdots, p$.

Kalman observable decomposition for $i$-th output $y_i \in \mathbb{R}$:

$$\begin{aligned} \dot{x} &= Ax \\ y_i &= C_i x + a_i \\ (i &= 1, \cdots, p) \end{aligned} \quad \Longrightarrow \quad \begin{aligned} \dot{z}_i &= \Phi_i A \Phi_i^T z_i \\ \dot{z}_i' &= \Psi_i A \Phi_i^T z_i + \Psi_i A \Psi_i^T z_i' \\ y_i &= C_i \Phi_i^T z_i + a_i \end{aligned}$$

Luenberger observer for observable sub-state $z_i = \Phi_i x$:

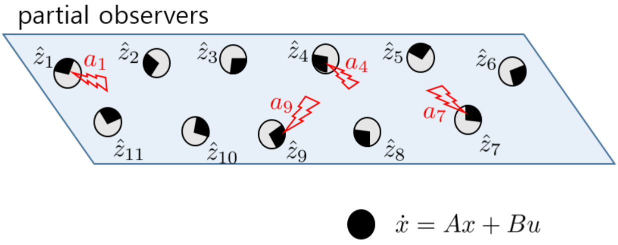
$$\dot{\hat{z}}_i = \Phi_i A \Phi_i^T \hat{z}_i + L_i(y_i - C_i \Phi_i^T \hat{z}_i), \quad i = 1, \cdots, p$$

so that $\hat{z}_i \to z_i$ if $y_i$ is not attacked

> Benefit:
>
> this yields un-corrupted (partial) estimates $\hat{z}_i$ as many as the number of unattacked sensors.

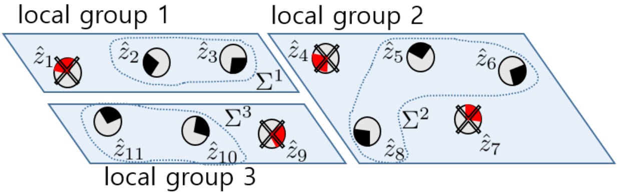
# Proposed distributed resilient state observer (overview)

1. design of partial observers for each $z_i = \Phi_i x$



# Proposed distributed resilient state observer (overview)

2. attack identification for each local group

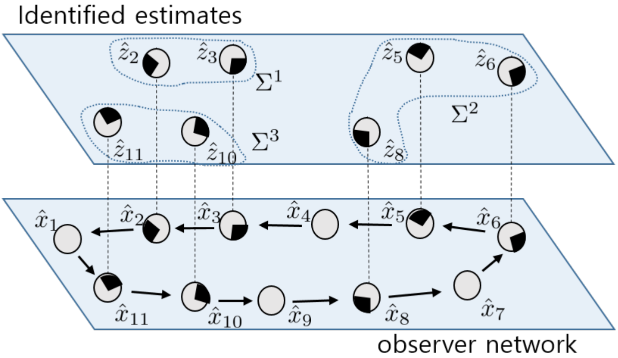



identification result:
$\Sigma^1 = \{2, 3\}$, $\Sigma^2 = \{5, 6, 8\}$, $\Sigma^3 = \{10, 11\}$

The identification algorithm in [Kim *et al.*, TAC 2018 (early access)] is applied for each local group.

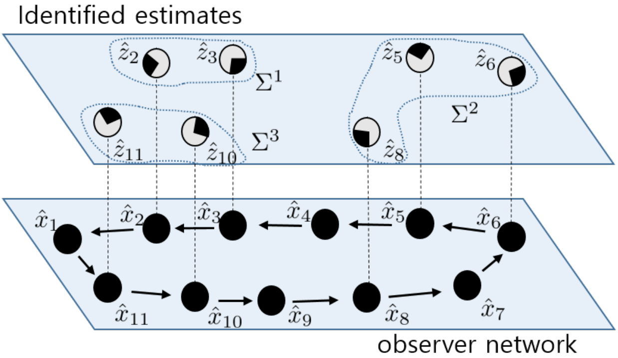
# Proposed distributed resilient state observer (overview)

3. identified partial estimates fed into observer network



# Proposed distributed resilient state observer (overview)

4. Through the communication, $x$ is recovered in every node $i$.



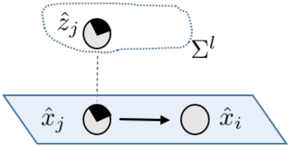
# Design of distributed state observer

state observer in the node $i$, $\quad i = 1, \cdots, p$ :

$$\dot{\hat{x}}_i = A\hat{x}_i + \gamma \sum_{j \in N_i} (\hat{x}_j^{\text{net}} - \hat{x}_i)$$

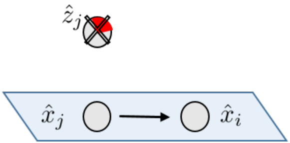
- $N_i$: neighbors of node $i$, $\qquad \gamma$: coupling gain
- $\hat{x}_j^{\text{net}}$: state information transmitted from node $j$

case 1: $j \in \Sigma^l$ for some $l$




$$\hat{x}_j^{\text{net}} = (\Phi_j^T \hat{z}_j - \Phi_j^T \Phi_j \hat{x}_j) + \hat{x}_j$$

case 2: $j \notin \Sigma^l$ for all $l$




$$\hat{x}_j^{\text{net}} = \hat{x}_j$$

partial estimate $\hat{z}_j$ is fed into the observer network
only when it is identified as attack free

# Main result

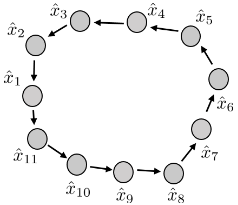
proposed distributed resilient state observer:

$$\dot{\hat{z}}_i = \Phi_i A \Phi_i^T \hat{z}_i + L_i(y_i - C_i \Phi_i^T \hat{z}_i)$$
$$\dot{\hat{x}}_i = A\hat{x}_i + \gamma \sum_{j \in N_i} (\hat{x}_j^{\text{net}} - \hat{x}_i), \qquad i \in \{1, \cdots, p\}$$

## Assumptions

- $(A, C)$ is observable.
- For each local $y_{P_l}$, $(A, C_{P_l})$ is $2q$-redundant.
- The communication graph is directed and strongly connected.

e.g., ring network:



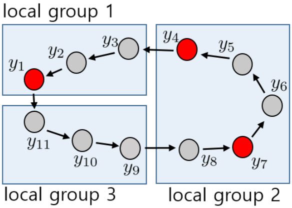

## Theorem

Under up to $q$-sensor attacks,

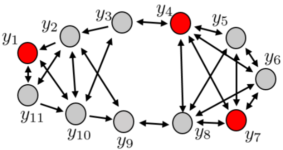
$$\|\hat{x}_i(t) - x(t)\| \to 0 \quad \text{as} \quad t \to \infty, \quad \forall i = 1, ..., p$$

provided that $\gamma$ is sufficiently large.

# Comparison with an existing result




our solution




[Mitra and Sundaram, CDC 2016]

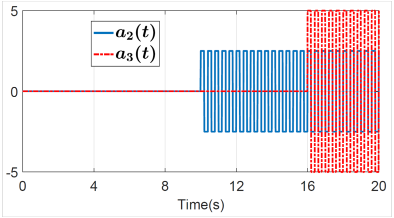
- local attack identification
- $2q$-redundant sensors + network connectivity
- no restriction for matrix $A$

- identification by each node
- at least $2q$ neighbors for each node + $\alpha$
- assumes $A$ has simple eigenvalues

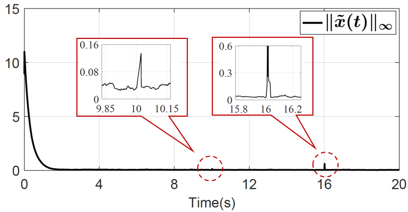
# A simulation result

- $\#$ of sensors $= 60$, $\#$ of local groups $= 10$
  $2$-attacks in one local group
- The system is not observable from each sensor group, but each group has $4$-redundant sensors.
  $\rightarrow$ every $2$-attacks are locally identifiable

computational complexity:
(centralized) $\binom{60}{2} = 1700$ v.s. (distributed) $10 \times \binom{6}{2} = 150$




sensor attacks injected at $t = 10, 16$




maximum norm of estimation error

# Conclusion

- For local identification of sensor attack, $2q$-redundant observability can be relaxed as $2q$-redundant sensors condition.

  $\rightarrow$ Full state observability is not necessary for local attack identification.

- distributed solution to resilient state estimation

  $\rightarrow$ reduced computational complexity

$$\binom{p}{q} = \binom{\sum_{l=1}^{k} p_l}{q} \gg \sum_{l=1}^{k} \binom{p_l}{q}$$

Thank you for your time!

email: kjs9044@cdsl.kr