Networked Control Systems under Cyber Attacks with Applications to Power Networks

André Teixeira, Henrik Sandberg, Karl H. Johansson

ACCESS Linnaeus Centre, Electrical Engineering, Royal Institute of Technology (KTH)

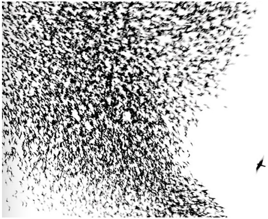
American Control Conference
July 1st, 2010

Outline

Outline

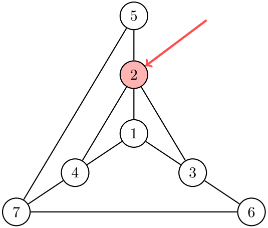
1. Introduction
   - Motivation
   - Fault Detection and Isolation
2. The Consensus Protocol
   - Consensus
   - Consensus in NMAS under Attack on Node
   - Consensus in NMAS under Communication Attacks
   - Reducing the Number of Monitoring Nodes
3. Power Systems
   - Classical Model

- Several agents interacting with each other
  - Information exchange or physical coupling
- Cooperation needed to achieve common goal
- Only local information available
  (*i.e.* from neighbors)
- Decentralized / Distributed Controllers

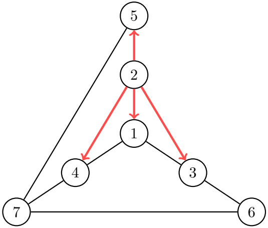


- What happens to the entire network if a single agent misbehaves?
- How can the other agents detect the misbehavior?
- Can the misbehaving node be identified?
- How should the network react?

Attack on Node



Attack on Communications



- How to detect and identify the misbehaving node in a distributed fashion?
- How to distinguish between an attack on a node and an attack on the communications?

- Dynamics of node k under attack in k

$$\dot{x}_k = A_{kk}x_k + \sum_{j \neq k} A_{kj}x_j + f_k$$

- Global dynamics seen from i under attack in k

$$\begin{cases} \dot{\mathbf{x}} = A\mathbf{x} + b_f^k f_k \\ \mathbf{y}_i = C_i\mathbf{x}, \end{cases}$$

where

- $\mathbf{y}_i$ are the measurements available at node i.
- b_f^k is the attack signature
- C_i is a design parameter

- Dynamics of node k under attack in k

$$\dot{x}_k = A_{kk}x_k + \sum_{j\neq k} A_{kj}x_j + f_k$$

- Global dynamics seen from i under attack in k

$$\begin{cases} \dot{\mathbf{x}} = A\mathbf{x} + b_f^k f_k \\ \mathbf{y}_i = C_i\mathbf{x}, \end{cases}$$

where

- $\mathbf{y}_i$ are the measurements available at node i.
- b_f^k is the attack signature
- C_i is a design parameter

- Dynamics of node k under attack in k

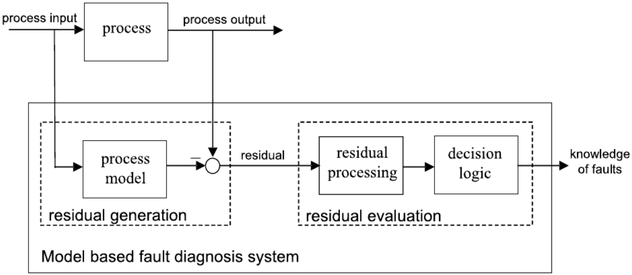
$$\dot{x}_k = A_{kk}x_k + \sum_{j \neq k} A_{kj}x_j + f_k$$

- Global dynamics seen from i under attack in k

$$\begin{cases} \dot{\mathbf{x}} = A\mathbf{x} + b_f^k f_k \\ \mathbf{y}_i = C_i\mathbf{x}, \end{cases}$$

where

- $\mathbf{y}_i$ are the measurements available at node i.
- b_f^k is the attack signature
- C_i is a design parameter



- Basic Ideas:
  - Compute an expected output;
  - Compare and evaluate the real and expected outputs.

Model-based Fault Detection and Isolation

Generalized Observer Scheme

- Implement a Generalized Observer Scheme (GOS) based on a bank of observers such that:
  - Each observer i is insensitive to only one fault element, f_i
  - The residual r_i is then sensitive to all faults except f_i
  - The fault f_i is detected using the following threshold logic:

$$\begin{cases} \|r_i(t)\| < T_{f_i} \\ \|r_k(t)\| \geq T_{f_k} \;, \forall k \neq i \end{cases}$$

Example

Let $f \in \mathbb{R}^3$. Build a bank of 3 observers according to the GOS.

	f_1	f_2	f_3
$\|r_1\|$	0	$+$	$+$
$\|r_2\|$	$+$	0	$+$
$\|r_3\|$	$+$	$+$	0

Unknown Input Observer

- Consider the faulty system:

$$\begin{cases} \dot{\mathbf{x}} = A\mathbf{x} + b_f^k f_k \\ \mathbf{y}_i = C_i\mathbf{x} \end{cases}$$

Definition

A state observer is an unknown input observer (UIO), with respect to f_k, if the state estimation error $e_i^k = \mathbf{x} - \hat{\mathbf{x}}_i^k$ approaches zero asymptotically, regardless of the presence of an unknown input f_k.

- Such UIO for the previous perturbed system has the following dynamics:

$$\begin{cases} \dot{z} = Fz + TBu + K\mathbf{y}_i \\ \hat{x}_i^k = z + H\mathbf{y}_i \end{cases}$$

- Choose the matrices F, T, K, H to satisfy the following conditions:

$$\begin{aligned} F &= A - HC_iA - K_1C_i \\ T &= I - HC_i \\ (HC_i - I)\, b_f^k &= 0 \\ K_2 &= FH \\ K &= K_1 + K_2 \end{aligned}$$

Theorem

The necessary and sufficient conditions for this UIO to exist are:

$$rank\left(C_i b_f^k\right) = rank\left(b_f^k\right) = 1, \quad rank\left(\begin{bmatrix} sI_n - A & b_f^k \\ C_i & 0 \end{bmatrix}\right) = n + 1$$

for all $Re(s) \geq 0$.

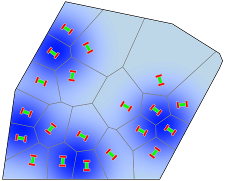
- Estimation error's dynamics and residual when all faults are active

$$
\begin{aligned}
\dot{e}_i^k &= F e_i^k + (I - HC_i) B_f^{-k} f_{-k} \\
r_i^k &= C_i e_i^k
\end{aligned}
$$

- Estimation error's dynamics and residual when all faults are active

$$\begin{aligned}\dot{e}_i^k &= Fe_i^k + (I - HC_i)B_f^{-k} f_{-k}\\ r_i^k &= C_i e_i^k\end{aligned}$$

Outline



- The main objective of such protocol is to achieve an agreement on a certain quantity of interest
- Example of applications:
  - Rendezvous
  - Formation
  - Deployment
  - Load balancing
  - Distributed estimation

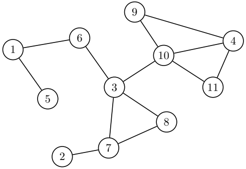
- Agents with single integrator dynamics:

$$\begin{cases} \dot{x}_i = u_i & , \; x_i(0) = x_{i_0} \in \mathbb{R} \\ y_i = x_i \end{cases}$$

- Distributed control law given by:

$$u_i = -\sum_{j \in N_i} (y_i - y_j)$$

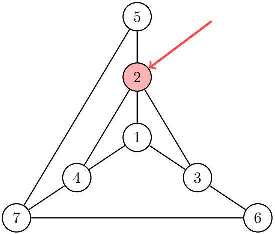
  - Based on local information only
  - Relies on the information transmitted by the neighbors, y_j



- Global dynamics of the network:

$$\dot{\mathbf{x}} = -\mathcal{L}\mathbf{x} \qquad (1)$$

with
$\mathbf{x} = \left[x_1^T \cdots x_N^T\right]^T$



- Dynamics of the attached node k:

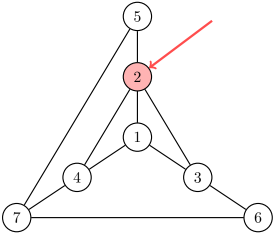
$$\begin{cases} \dot{x}_k & = & -\sum_{j \in N_k} (y_k - y_j) + f_k \\ y_k & = & x_k \end{cases}$$

- Global dynamics of the network:

$$\dot{\mathbf{x}} = -\mathcal{L}\mathbf{x} + b_f^k f_k \qquad (2)$$

  - $b_f^k \in \mathbb{R}^N$ is a vector with the k^{th} component set to 1 and all the others to 0

- The same form as $\dot{x}(t) = Ax(t) + b_f^k f(t)$



- Dynamics of the attached node k:

$$\begin{cases} \dot{x}_k &= -\sum_{j \in N_k} (y_k - y_j) + f_k \\ y_k &= x_k \end{cases}$$

- Global dynamics of the network:

$$\dot{\mathbf{x}} = -\mathcal{L}\mathbf{x} + b_f^k f_k \qquad (2)$$

  - $b_f^k \in \mathbb{R}^N$ is a vector with the k^{th} component set to 1 and all the others to 0

- The same form as $\dot{x}(t) = Ax(t) + b_f^k f(t)$

Assumption

The graph of the network is known by all nodes and it remains constant.

- Distributed scheme:
  - Have each node monitoring all its neighbors using a GOS
- Information available at node i is

$$\mathbf{y}_i = \begin{bmatrix} y_i^T & y_{i_1}^T & \cdots & y_{i_{|N_i|}}^T \end{bmatrix}^T = \begin{bmatrix} x_i^T & x_{i_1}^T & \cdots & x_{i_{|N_i|}}^T \end{bmatrix}^T = C_i \mathbf{x}$$

- For each neighbor k, design a UIO for the global dynamics insensitive only to an attack on node k

$$\begin{cases} \dot{z}_i^k & = & F_i^k z_i^k + K_i^k \mathbf{y}_i \\ \hat{\mathbf{x}}_i^k & = & z_i^k + H_i^k \mathbf{y}_i \end{cases} \qquad (3)$$

- Reminding the necessary and sufficient conditions for the UIO
  1. $\text{rank}\left(C_i b_f^k\right) = \text{rank}\left(b_f^k\right) = 1$
  2. The transmission zeros of $\left(-\mathcal{L}, b_f^k, C_i, 0\right)$ are stable
- Derived results:

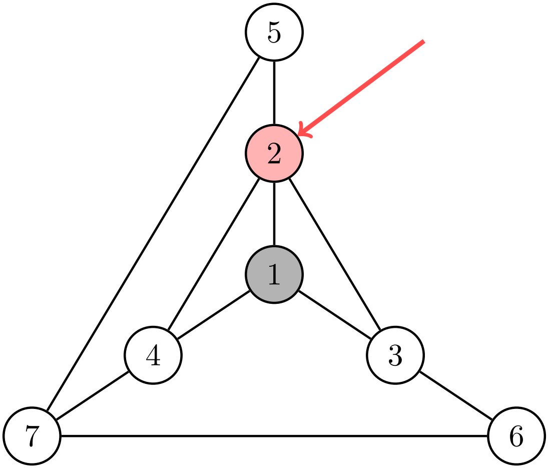
Lemma

If an undirected graph $\mathcal{G}$ is connected, then any principle minor of its Laplacian matrix $\mathcal{L}$, induced by a subset of nodes $\bar{F} \subset \mathcal{V}$, is invertible.

Theorem

There exists a UIO for the system $\left(-\mathcal{L}\left(\mathcal{G}\right), b_f^k, C_i, 0\right)$ if the graph $\mathcal{G}$ is connected and $k \in \mathcal{N}_i$.

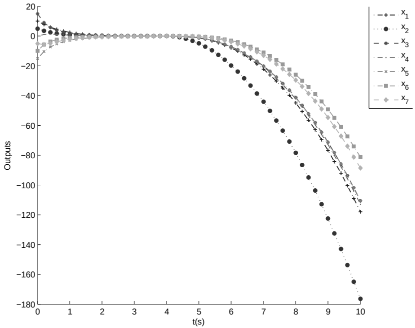
- Attack in node 2 seen from node 1



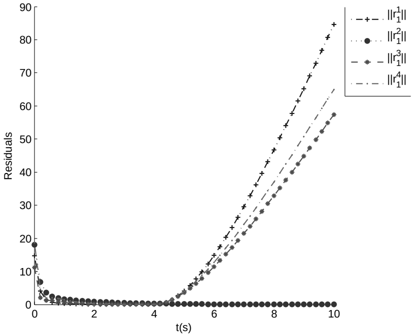
Consensus in NMAS under Attack on Node

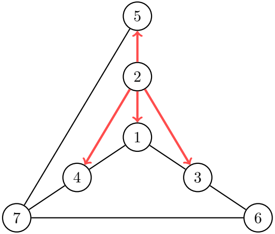
Results 1)

Outputs



Residuals at node 1





- Dynamics of the compromised node k:

$$\begin{cases} \dot{x}_k &= -\sum_{j \in N_k} (w_k - y_j) \\ w_k &= x_k \\ y_k &= x_k + f_k \end{cases}$$

  - w_k is an internal measurement of the state, not being subject to an attack on the communications

- Global dynamics of the network:

$$\begin{cases} \dot{\mathbf{x}} &= -\mathcal{L}\mathbf{x} + \mathcal{I}_{\bar{k}} l^k f_k \\ \mathbf{y} &= \mathbf{x} + b_f^k f_k \\ \mathbf{w} &= \mathbf{x} \end{cases} \tag{4}$$

- Separating the dynamics of the healthy network $\bar{k}$

$$\begin{cases} \dot{\mathbf{x}}_{\bar{k}} = -\mathcal{L}_{\bar{k}}\mathbf{x}_{\bar{k}} - l_{\bar{k}k}y_k \\ \mathbf{y}_{\bar{k}} = \mathbf{x}_{\bar{k}} \end{cases} \tag{5}$$

- Note that y_k is the information transmitted by node k
  - Attack in node k:

$$\begin{cases} \dot{x}_k = -\mathcal{L}_k x_k - l_{k\bar{k}}\mathbf{y}_{\bar{k}} + f_k \\ y_k = x_k \end{cases}$$

  - Communication attack in node k:

$$\begin{cases} \dot{x}_k = -\mathcal{L}_k x_k - l_{k\bar{k}}\mathbf{y}_{\bar{k}} \\ y_k = x_k + f_k \end{cases}$$

- The "healthy" network can not distinguish between both attacks

- Separating the dynamics of the healthy network $\bar{k}$

$$\begin{cases} \dot{\mathbf{x}}_{\bar{k}} &= -\mathcal{L}_{\bar{k}}\mathbf{x}_{\bar{k}} - l_{\bar{k}k}y_k \\ \mathbf{y}_{\bar{k}} &= \mathbf{x}_{\bar{k}} \end{cases} \tag{5}$$

- Note that y_k is the information transmitted by node k
  - Attack in node k:

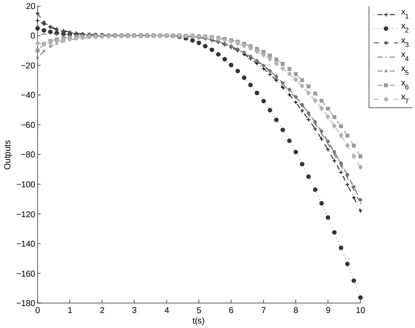
$$\begin{cases} \dot{x}_k &= -\mathcal{L}_k x_k - l_{k\bar{k}}\mathbf{y}_{\bar{k}} + f_k \\ y_k &= x_k \end{cases}$$

  - Communication attack in node k:

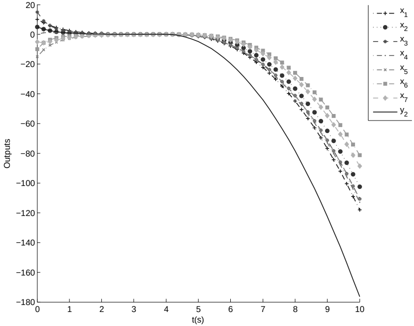
$$\begin{cases} \dot{x}_k &= -\mathcal{L}_k x_k - l_{k\bar{k}}\mathbf{y}_{\bar{k}} \\ y_k &= x_k + f_k \end{cases}$$

- The "healthy“ network can not distinguish between both attacks

Attack in node 2



Communication attack in node 2

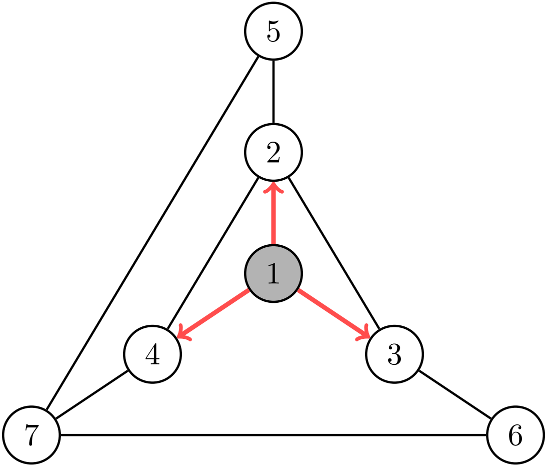


- Key observations:
  - Node k followed the rest of the network under the communication attack
  - Thus it should be able to realize something is wrong
- For node k, it seems all its neighbors are misbehaving in a particular way
- Consider the previous system monitored from node k

$$\begin{cases} \dot{\mathbf{x}} = -\mathcal{L}\mathbf{x} + b_f^k f_k \\ \mathbf{y}_k = C_k \mathbf{x} \end{cases} \tag{6}$$

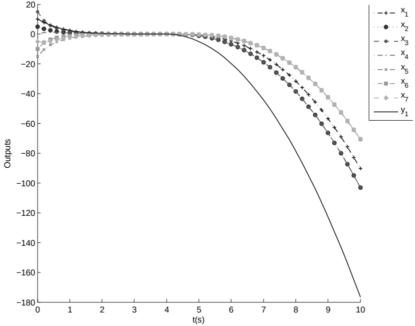
  - with $b_f^k = \mathcal{I}_{\bar{k}} l^k$
  - and $\mathbf{y}_k = \begin{bmatrix} w_k & y_{k_1} & \cdots & y_{k_{|\mathcal{N}_k|}} \end{bmatrix}^T$
- Add an UIO insensitive to b_f^k to the observer bank in node k

- Attack in node 1 seen from node 1

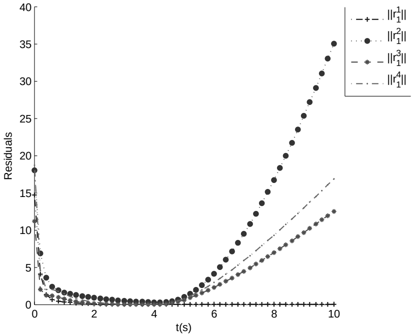


Consensus in NMAS under Communication Attacks
Results 2)

Outputs



Residuals at node 1

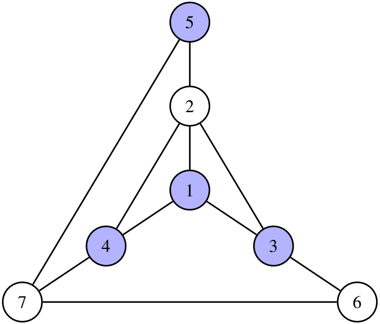


Reducing the Number of Monitoring Nodes

- The problem of reducing the number of observers is related to the set cover:

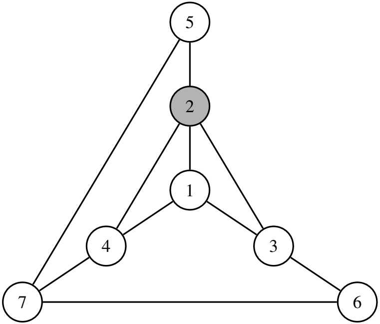
$$\min_{S \subseteq \mathcal{V}} \quad |S|$$
$$\text{s.t.} \bigcup_{i \in S} N_i = \mathcal{V}$$

- Each observer node is monitored by at least one other node.

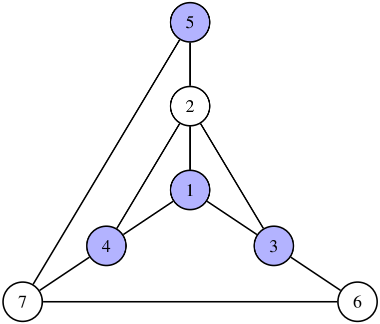


Reducing the Number of Monitoring Nodes

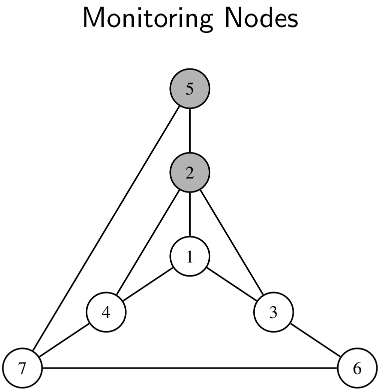
Monitoring Nodes

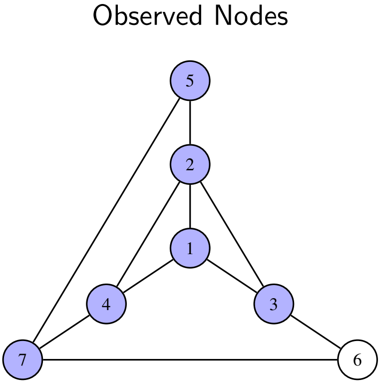


Observed Nodes



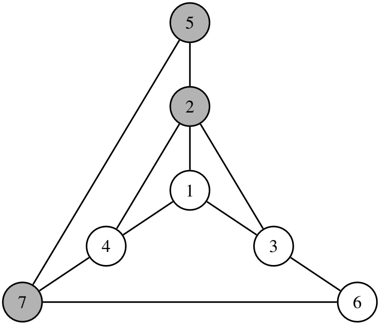
Reducing the Number of Monitoring Nodes



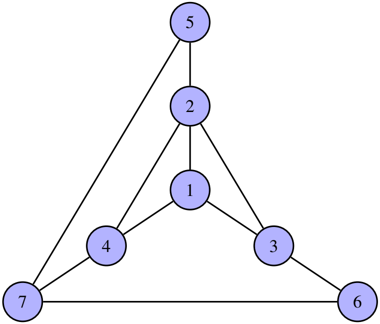


Reducing the Number of Monitoring Nodes

Monitoring Nodes



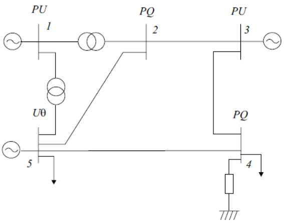
Observed Nodes



Outline

- Active power flow on a loss-less distribution grid.
- Each bus has dynamics given by the "swing equation":

$$M_i\ddot{\delta}_i + D_i\dot{\delta}_i = -\sum_{j\in N_i} w_{ij}\sin(\delta_i - \delta_j) + P_{m_i}$$



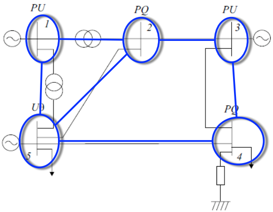
- $\delta_{ij} = \delta_i - \delta_j$ is small, thus $\sin(\delta_i - \delta_j) \approx \delta_i - \delta_j$.

It can be looked at from a multi-agent systems point of view.

- consider δ_i and $\dot{\delta}_i(t)$ to be states of each bus.
- Having $x = [\delta_1, \ldots, \delta_N, \dot{\delta}_1, \ldots, \dot{\delta}_N]$: $\dot{\mathbf{x}}(t) = A\mathbf{x}(t) + B\mathbf{P}_m$.

- Active power flow on a loss-less distribution grid.
- Each bus has dynamics given by the "swing equation":

$$M_i\ddot{\delta}_i + D_i\dot{\delta}_i = -\sum_{j\in N_i} w_{ij}\sin(\delta_i - \delta_j) + P_{m_i}$$



- $\delta_{ij} = \delta_i - \delta_j$ is small, thus $\sin(\delta_i - \delta_j) \approx \delta_i - \delta_j$.

It can be looked at from a multi-agent systems point of view.

- consider δ_i and $\dot{\delta}_i(t)$ to be states of each bus.
- Having $x = [\delta_1, \ldots, \delta_N, \dot{\delta}_1, \ldots, \dot{\delta}_N]$: $\dot{\mathbf{x}}(t) = A\mathbf{x}(t) + B\mathbf{P}_m$.

- Existence of UIO:

Theorem

There exists an UIO for the system $\left(A, b_f^k, C_i, 0\right)$ *if the graph* $\mathcal{G}$ *is connected,* k *is a neighbor of* i *and node* i *measures both the phase-angle and the frequency offset of its neighbors.*

- Infeasibility results:

Theorem

Let the graph $\mathcal{G}$ *be connected and* k *be a neighbor of* i*. No UIO for the system* $\left(A, b_f^k, C_i, 0\right)$ *exists if node* i *only measures either the phase-angle or the frequency offset of its neighbors.*

Summary

- Distributed techniques to detect and isolate attacks on nodes and communication attacks in a network of agent using the *consensus protocol* were proposed and sufficient conditions were also provided
- It was shown that the "healthy network" can not distinguish between the two types of attack, but the misbehaving node can
- A distributed FDI scheme for power systems was proposed