62nd IEEE Conference on Decision and Control

# A Robustness Analysis to Structured Channel Tampering over Secure-by-design Consensus Networks

Marco Fabris and **Daniel Zelazo**

December 13th, 2023

Università degli Studi di Padova

TECHNION
Israel Institute of Technology

# Overview and preliminaries

# Cyber-attacks and Multi-Agent Systems (MASs)

**Cyber-attacks**: malicious and deliberate attempts to breach the information system of an individual or organization.

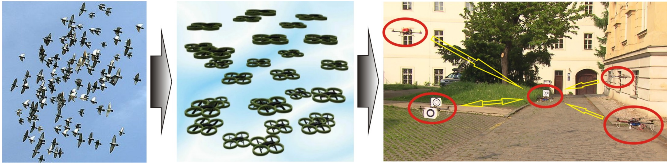
Example of cyber-attacks target: *networked control systems*

# Cyber-attacks and Multi-Agent Systems (MASs)

**Cyber-attacks**: malicious and deliberate attempts to breach the information system of an individual or organization.

Example of cyber-attacks target: *networked control systems*

**MAS**: set of agents situated in a shared environment, constituting a networked control system having the purpose to attain a common task.

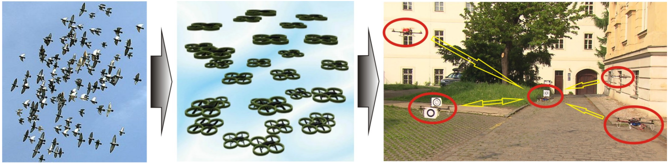


# Cyber-attacks and Multi-Agent Systems (MASs)

**Cyber-attacks**: malicious and deliberate attempts to breach the information system of an individual or organization.

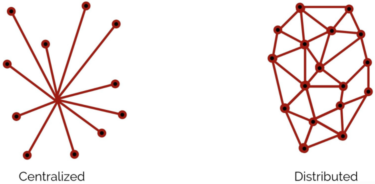
Example of cyber-attacks target: *networked control systems*

**MAS**: set of agents situated in a shared environment, constituting a networked control system having the purpose to attain a common task.



Distinctive features:

- distributed architecture
- autonomy
- scalability
- robustness to failure

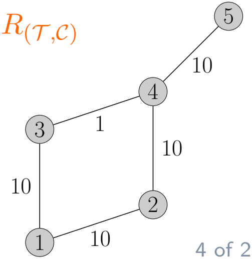


# Graph-based network model

The secure smart networks under analysis are defined as $n$-agent systems modeled through graph theoretical tools.

Notation

- weighted undirected graph: $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{W})$, $|\mathcal{V}| = n$, $|\mathcal{E}| = m$
- vertex set: $\mathcal{V} = \{1, \ldots, n\}$
- edge set: $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$
- $i$-th neighborhood: $\mathcal{N}_i = \{j \in \mathcal{V} \setminus \{i\} \mid (i,j) \in \mathcal{E}\}$
- a spanning tree: $\mathcal{T} \subseteq \mathcal{G}$
- the cut-set matrix of $\mathcal{G}$ w.r.t. $\mathcal{T}$ and $\mathcal{C} = \mathcal{G} \setminus \mathcal{T}$: $R_{(\mathcal{T},\mathcal{C})}$
- weight on edge $(i,j)$: $w_{ij} \in \mathbb{R}$ if $(i,j) \in \mathcal{E}$
- weight matrix: $W$ s.t. $[W]_{kk} = w_{ij}$, $k = (i,j)$
- incidence matrix: $E \in \mathbb{R}^{n \times m}$
- weighted Laplacian matrix: $L(\mathcal{G}) = EWE^\top$



# Weighted consensus protocol

- $n$ homogeneous agents with dyanmic state $x_i = x_i(t) \in \mathbb{R}^D$, $i = 1, \ldots, n$
- ensemble state: $\mathbf{x} = \mathrm{vec}_{i=1}^{n}(x_i) \in X \subset \mathbb{R}^N$, with $N = nD$

# Weighted consensus protocol

- $n$ homogeneous agents with dyanmic state $x_i = x_i(t) \in \mathbb{R}^D$, $i = 1, \ldots, n$
- ensemble state: $\mathbf{x} = \mathrm{vec}_{i=1}^n(x_i) \in X \subset \mathbb{R}^N$, with $N = nD$

**Definition (Weighted Consensus)**

An $n$-agent network achieves consensus if $\lim_{t\to+\infty} \mathbf{x}(t) \in \mathcal{A}$, where $\mathcal{A} = (\mathrm{span}(\mathbb{1}_n) \otimes \omega)$, $\omega \in \mathbb{R}^D$, is called *agreement set*.

# Weighted consensus protocol

- $n$ homogeneous agents with dyanmic state $x_i = x_i(t) \in \mathbb{R}^D$, $i = 1, \dots, n$
- ensemble state: $\mathbf{x} = \mathrm{vec}_{i=1}^{n}(x_i) \in X \subset \mathbb{R}^N$, with $N = nD$

**Definition (Weighted Consensus)**

An $n$-agent network achieves consensus if $\lim_{t \to +\infty} \mathbf{x}(t) \in \mathcal{A}$, where $\mathcal{A} = (\mathrm{span}(\mathbb{1}_n) \otimes \omega)$, $\omega \in \mathbb{R}^D$, is called *agreement set*.

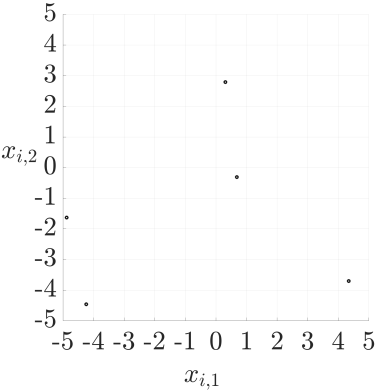
**Proposition**

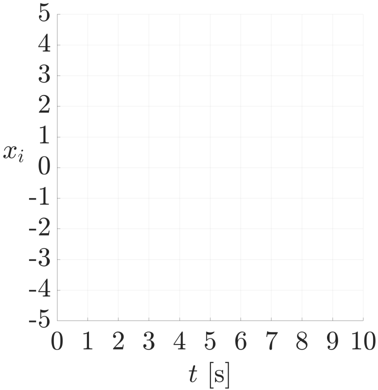
For a MAS described by an undirected and connected graph $\mathcal{G}$ the network state $\mathbf{x}$ driven by dynamics

$$\dot{\mathbf{x}} = -\mathbf{L}(\mathcal{G})\mathbf{x}, \qquad \text{with } \mathbf{L}(\mathcal{G}) = L(\mathcal{G}) \otimes I_D,$$

fulfills weighted consensus.

# Weighted consensus protocol: classic example



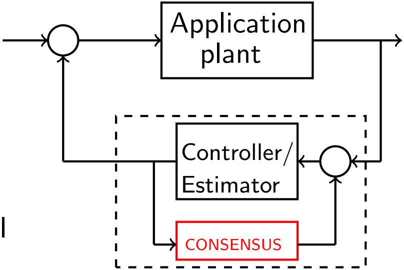

Rendez-vous, $n = 5$, $D = 2$.

# The Secure-by-Design Consensus Protocol

# Edge weight encryption: motivations

Edge weight values affect convergence performances of consensus.
**Practical motivations** suggesting their encryption:

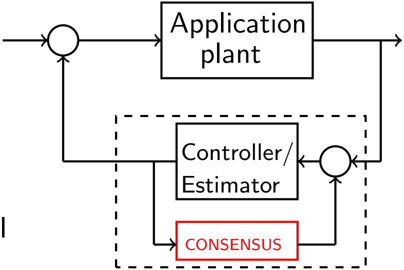
- **preserving privacy**, in general;
- **ensuring performances of existing applications**, e.g. decentralized estimation, opinion dynamics;
- **achieving synchronization** for a group of agents subject to Byzantine attacks through learning-based control techniques.



# Edge weight encryption: motivations

Edge weight values affect convergence performances of consensus.
**Practical motivations** suggesting their encryption:

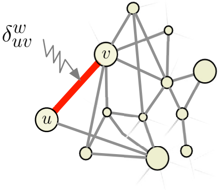
- **preserving privacy**, in general;
- **ensuring performances of existing applications**, e.g. decentralized estimation, opinion dynamics;
- **achieving synchronization** for a group of agents subject to Byzantine attacks through learning-based control techniques.

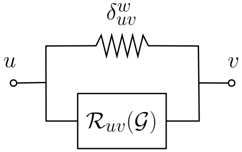



**We want to embed edge weight encryption into consensus networks and study the related robustness**

# "Robustness" within consensus networks

Meaning: **robust stability to small-magnitude perturbations** altering the agent dynamics

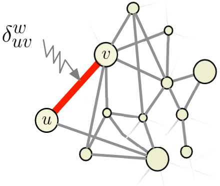


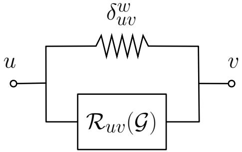




Effective resistance (EF): $\mathcal{R}_{uv}(\mathcal{G}) = [L^\dagger(\mathcal{G})]_{uu} - 2[L^\dagger(\mathcal{G})]_{uv} + [L^\dagger(\mathcal{G})]_{vv}$

# "Robustness" within consensus networks

Meaning: **robust stability to small-magnitude perturbations** altering the agent dynamics



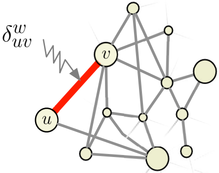

Effective resistance (EF): $\mathcal{R}_{uv}(\mathcal{G}) = [L^{\dagger}(\mathcal{G})]_{uu} - 2[L^{\dagger}(\mathcal{G})]_{uv} + [L^{\dagger}(\mathcal{G})]_{vv}$

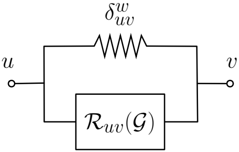
Generalized EF w.r.t. the subset $\mathcal{E}_{\Delta} \subseteq \mathcal{E}$ of uncertain edges:

$$\mathcal{R}_{\mathcal{E}_{\Delta}}(\mathcal{G}) = \left\| P^{\top} R_{(\mathcal{T},\mathcal{C})}^{\top} (R_{(\mathcal{T},\mathcal{C})} W R_{(\mathcal{T},\mathcal{C})}^{\top})^{-1} R_{(\mathcal{T},\mathcal{C})} P \right\|$$

# "Robustness" within consensus networks

Meaning: **robust stability to small-magnitude perturbations** altering the agent dynamics




Effective resistance (EF): $\mathcal{R}_{uv}(\mathcal{G}) = [L^{\dagger}(\mathcal{G})]_{uu} - 2[L^{\dagger}(\mathcal{G})]_{uv} + [L^{\dagger}(\mathcal{G})]_{vv}$

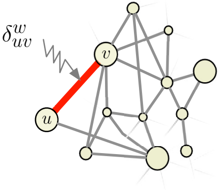
Generalized EF w.r.t. the subset $\mathcal{E}_{\Delta} \subseteq \mathcal{E}$ of uncertain edges:

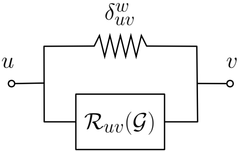
$$\mathcal{R}_{\mathcal{E}_{\Delta}}(\mathcal{G}) = \left\| P^{\top} R_{(\mathcal{T},\mathcal{C})}^{\top} (R_{(\mathcal{T},\mathcal{C})} W R_{(\mathcal{T},\mathcal{C})}^{\top})^{-1} R_{(\mathcal{T},\mathcal{C})} P \right\|$$

**Uncertain consensus protocol**: $\dot{\mathbf{x}} = -L(\mathcal{G}_{\Delta^W})\mathbf{x}$, where $\Delta^W$ is a (structured diagonal) disturbance and $L(\mathcal{G}_{\Delta^W}) = E(W + \Delta^W)E^{\top}$

# “Robustness” within consensus networks

Meaning: **robust stability to small-magnitude perturbations** altering the agent dynamics




Effective resistance (EF): $\mathcal{R}_{uv}(\mathcal{G}) = [L^\dagger(\mathcal{G})]_{uu} - 2[L^\dagger(\mathcal{G})]_{uv} + [L^\dagger(\mathcal{G})]_{vv}$

Generalized EF w.r.t. the subset $\mathcal{E}_\Delta \subseteq \mathcal{E}$ of uncertain edges:

$$\mathcal{R}_{\mathcal{E}_\Delta}(\mathcal{G}) = \left\| P^\top R^\top_{(\mathcal{T},\mathcal{C})} (R_{(\mathcal{T},\mathcal{C})} W R^\top_{(\mathcal{T},\mathcal{C})})^{-1} R_{(\mathcal{T},\mathcal{C})} P \right\|$$

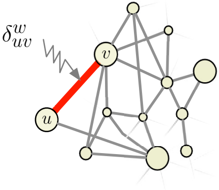
**Uncertain consensus protocol**: $\dot{\mathbf{x}} = -L(\mathcal{G}_{\Delta^W})\mathbf{x}$, where $\Delta^W$ is a (structured diagonal) disturbance and $L(\mathcal{G}_{\Delta^W}) = E(W + \Delta^W)E^\top$

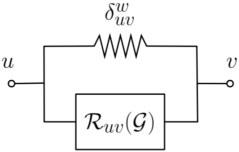
For the uncertainty $\Delta^W$ on $\mathcal{E}_\Delta$ then **robust consensus** is guaranteed if

$$\|\Delta^W\| < \mathcal{R}^{-1}_{\mathcal{E}_\Delta}(\mathcal{G})$$

# “Robustness” within consensus networks

Meaning: **robust stability to small-magnitude perturbations** altering the agent dynamics




Effective resistance (EF): $\mathcal{R}_{uv}(\mathcal{G}) = [L^\dagger(\mathcal{G})]_{uu} - 2[L^\dagger(\mathcal{G})]_{uv} + [L^\dagger(\mathcal{G})]_{vv}$
Generalized EF w.r.t. the subset $\mathcal{E}_\Delta \subseteq \mathcal{E}$ of uncertain edges:

$$\mathcal{R}_{\mathcal{E}_\Delta}(\mathcal{G}) = \left\| P^\top R^\top_{(\mathcal{T},\mathcal{C})} (R_{(\mathcal{T},\mathcal{C})} W R^\top_{(\mathcal{T},\mathcal{C})})^{-1} R_{(\mathcal{T},\mathcal{C})} P \right\|$$

**Uncertain consensus protocol**: $\dot{\mathbf{x}} = -L(\mathcal{G}_{\Delta^W})\mathbf{x}$, where $\Delta^W$ is a (structured diagonal) disturbance and $L(\mathcal{G}_{\Delta^W}) = E(W + \Delta^W)E^\top$

For the uncertainty $\Delta^W$ on $\mathcal{E}_\Delta$ then **robust consensus** is guaranteed if

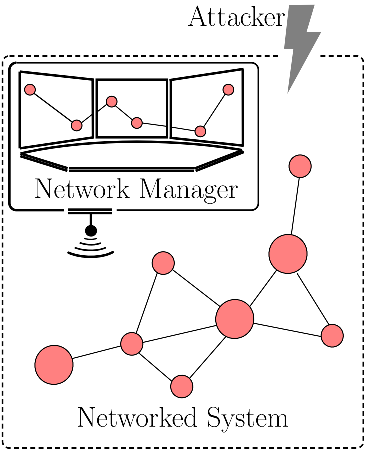
$$\boxed{\|\Delta^W\| < \mathcal{R}^{-1}_{\mathcal{E}_\Delta}(\mathcal{G})}$$

known small-gain theorem result

[D. Zelazo and M. Bürger, *On the Robustness of Uncertain Consensus Networks*, TCNS, 2017]

# Introduction of the network manager

One method to increase security among networks is adopting the so-called **network manager**.




The network manager

- is **not** a global controller
- is used **to secure** distributed algorithms running on MASs
- defines tasks: within consensus, the task corresponds to **(encrypted) edge weight selection**
- its goal is to guarantee **robust** consensus convergence

# Objective coding and information localization

**Objective coding**: a task is described by an encoded parameter $\theta \in \mathbb{R}^{n^2}$ called *codeword*. Decoding functions $p_i$ are used by agents to interpret $\theta$.

# Objective coding and information localization

**Objective coding**: a task is described by an encoded parameter $\theta \in \mathbb{R}^{n^2}$ called *codeword*. Decoding functions $p_i$ are used by agents to interpret $\theta$.

Assumptions on the structure of codeword and decoding functions:

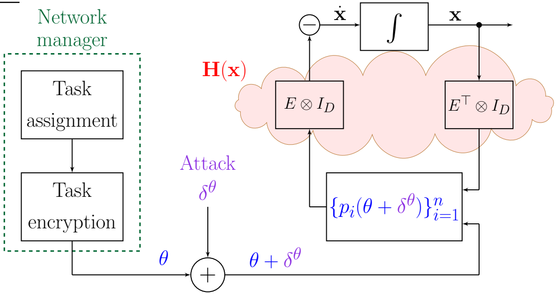
- $\theta^{(k)} := [\theta_i]_j = \theta_{ij}$ such that $\theta_{ij} = \theta_{ji}$, for $k = 1, \ldots, m$
- $\theta^{(k)}$ is meaningful if $k = (i, j) \in \mathcal{E}$
- $\theta_{ii}$ takes arbitrary value
- $p_{ij}(\theta) = p_{ij}(\theta_{ij})$

# Objective coding and information localization

**Objective coding**: a task is described by an encoded parameter $\theta \in \mathbb{R}^{n^2}$ called *codeword*. Decoding functions $p_i$ are used by agents to interpret $\theta$.

Assumptions on the structure of codeword and decoding functions:

- $\theta^{(k)} := [\theta_i]_j = \theta_{ij}$ such that $\theta_{ij} = \theta_{ji}$, for $k = 1, \ldots, m$
- $\theta^{(k)}$ is meaningful if $k = (i,j) \in \mathcal{E}$
- $\theta_{ii}$ takes arbitrary value
- $p_{ij}(\theta) = p_{ij}(\theta_{ij})$

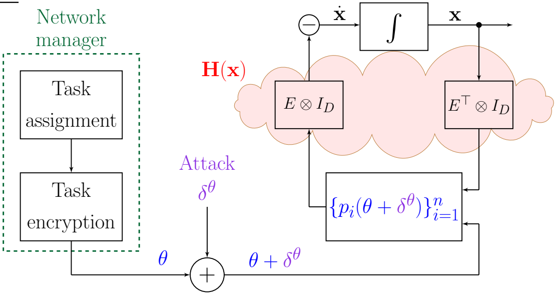


# Objective coding and information localization

**Objective coding**: a task is described by an encoded parameter $\theta \in \mathbb{R}^{n^2}$ called *codeword*. Decoding functions $p_i$ are used by agents to interpret $\theta$.

Assumptions on the structure of codeword and decoding functions:

- $\theta^{(k)} := [\theta_i]_j = \theta_{ij}$ such that $\theta_{ij} = \theta_{ji}$, for $k = 1, \ldots, m$
- $\theta^{(k)}$ is meaningful if $k = (i,j) \in \mathcal{E}$
- $\theta_{ii}$ takes arbitrary value
- $p_{ij}(\theta) = p_{ij}(\theta_{ij})$




**Information localization**: $h_{ij}(\mathbf{x}) := \mathrm{col}_j[h_i(\mathbf{x})] = \begin{cases} x_i - x_j, & (i,j) \in \mathcal{E} \\ \mathbf{0}_D, & \text{otherwise} \end{cases}$

$\mathbf{H}(\mathbf{x}) = \mathrm{diag}_{i=1}^n(h_i(\mathbf{x}))$

# Secure-by-design consensus dynamics

Assume that decoding functions $p_i$, $i = 1, \ldots, n$, obey this rule:

$$[p_i(\theta)]_j = p_{ij}(\theta) = \begin{cases} w_{ij}, & (i,j) \in \mathcal{E} \\ 0, & \text{otherwise} \end{cases}$$

# Secure-by-design consensus dynamics

Assume that decoding functions $p_i$, $i = 1, \ldots, n$, obey this rule:

$$[p_i(\theta)]_j = p_{ij}(\theta) = \begin{cases} w_{ij}, & (i,j) \in \mathcal{E} \\ 0, & \text{otherwise} \end{cases}$$

Then the **nominal consensus protocol** can be thus rewritten as

$$\dot{x}_i = -\sum_{j \in \mathcal{N}_i} p_{ij}(\theta) h_{ij}(\mathbf{x}), \quad i = 1, \ldots, n$$

# Secure-by-design consensus dynamics

Assume that decoding functions $p_i$, $i = 1, \dots, n$, obey this rule:

$$[p_i(\theta)]_j = p_{ij}(\theta) = \begin{cases} w_{ij}, & (i, j) \in \mathcal{E} \\ 0, & \text{otherwise} \end{cases}$$

Then the **nominal consensus protocol** can be thus rewritten as

$$\dot{x}_i = -\sum_{j \in \mathcal{N}_i} p_{ij}(\theta) h_{ij}(\mathbf{x}), \quad i = 1, \dots, n$$

or, equivalently, setting $\mathbf{p} = \mathrm{vec}(p_i)$ and recalling that $\mathbf{H}(\mathbf{x}) = \mathrm{diag}(h_i(\mathbf{x}))$

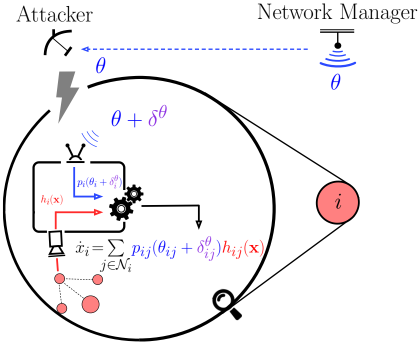
$$\dot{\mathbf{x}} = -\mathbf{H}(\mathbf{x})\mathbf{p}(\theta)$$

# Model for the channel tampering

Attack is a codeword deviation: $\delta^\theta \in \mathbf{\Delta}^\theta = \left\{\delta^\theta \ : \ \left\|\delta^\theta\right\|_\infty \leq \bar{\delta}^\theta\right\}$

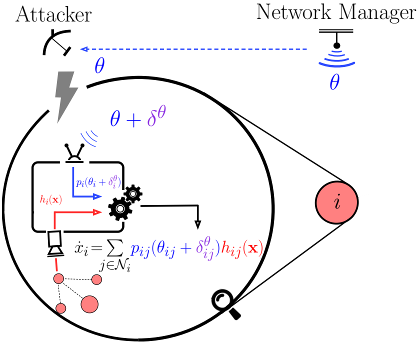
# Model for the channel tampering

Attack is a codeword deviation: $\delta^\theta \in \mathbf{\Delta}^\theta = \left\{\delta^\theta \ : \ \left\|\delta^\theta\right\|_\infty \leq \bar{\delta}^\theta\right\}$



# Model for the channel tampering

Attack is a codeword deviation: $\delta^\theta \in \mathbf{\Delta}^\theta = \left\{ \delta^\theta \ : \ \left\| \delta^\theta \right\|_\infty \leq \bar{\delta}^\theta \right\}$




Then the **perturbed consensus protocol** (PCP) can be described by

$$\dot{x}_i = - \sum_{j \in \mathcal{N}_i} p_{ij}(\theta_{ij} + \delta_{ij}^\theta) h_{ij}(\mathbf{x}), \qquad i = 1, \ldots, n$$

where $\delta_{ij}^\theta = [\delta_i^\theta]_j$ and $\delta_i^\theta$ satisfies $\delta^\theta = \mathrm{vec}(\delta_i^\theta)$.

# Channel tampering: multi-edge attack problem

<u>Problem</u>

Design $p_{ij}$ such that the PCP reaches agreement

- independently from the value of $\theta$
- while the MAS is subject to an attack $\delta^{\theta}$ striking all the edges in $\mathcal{E}_{\Delta}$, that is $\delta^{\theta}_{ij} = 0$ for all $(i, j) \in \mathcal{E} \setminus \mathcal{E}_{\Delta}$

# Channel tampering: multi-edge attack problem

Problem

Design $p_{ij}$ such that the PCP reaches agreement

- independently from the value of $\theta$
- while the MAS is subject to an attack $\delta^{\theta}$ striking all the edges in $\mathcal{E}_{\Delta}$, that is $\delta^{\theta}_{ij} = 0$ for all $(i, j) \in \mathcal{E} \setminus \mathcal{E}_{\Delta}$

Moreover, provide resilience guarantees for a given perturbation set $\boldsymbol{\Delta}^{\theta}$ in terms of the maximum allowed magnitude (say $\rho^{\theta}_{\Delta}$) for the norm of $\delta^{\theta}$.

# Robustness to channel tampering

Further (crucial!) assumptions on the decoding functions:

# Robustness to channel tampering

Further (crucial!) assumptions on the decoding functions:

$(i)$ values $[p_i(\theta)]_j = p_{ij}(\theta_{ij})$, with $\theta_{ij} = [\theta_i]_j$, satisfy

$$p_{ij}(\theta) = \begin{cases} w_{ij}, & \text{if } (i,j) \in \mathcal{E} \\ 0, & \text{otherwise} \end{cases}$$

for all $(i,j) \in \mathcal{E}$ and are **not constant** w.r.t. $\theta_{ij}$.

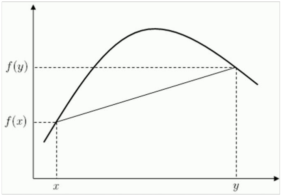
# Robustness to channel tampering

Further (crucial!) assumptions on the decoding functions:

$(i)$ values $[p_i(\theta)]_j = p_{ij}(\theta_{ij})$, with $\theta_{ij} = [\theta_i]_j$, satisfy

$$p_{ij}(\theta) = \begin{cases} w_{ij}, & \text{if } (i,j) \in \mathcal{E} \\ 0, & \text{otherwise} \end{cases}$$

for all $(i,j) \in \mathcal{E}$ and are **not constant** w.r.t. $\theta_{ij}$.




$(ii)$ $p_{ij}(\theta)$ is **concave** for all admissible $\theta$

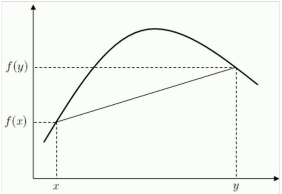
# Robustness to channel tampering

Further (crucial!) assumptions on the decoding functions:

$(i)$ values $[p_i(\theta)]_j = p_{ij}(\theta_{ij})$, with $\theta_{ij} = [\theta_i]_j$, satisfy

$$p_{ij}(\theta) = \begin{cases} w_{ij}, & \text{if } (i,j) \in \mathcal{E} \\ 0, & \text{otherwise} \end{cases}$$

for all $(i,j) \in \mathcal{E}$ and are **not constant** w.r.t. $\theta_{ij}$.




$(ii)$ $p_{ij}(\theta)$ is **concave** for all admissible $\theta$

$(iii)$ $p_{ij}$ is **Lipschitz continuous and differentiable** w.r.t. $\theta$, implying

$$\exists K_{ij} \geq 0\text{: } |p'_{ij}(\theta_{ij})| \leq K_{ij},\ \forall (i,j) \in \mathcal{E}$$

# Robustness to channel tampering (cont'd)

With the previous assumptions holding and setting $K_\Delta := \max_{(u,v)\in\mathcal{E}_\Delta} \{K_{uv}\}$:

**Theorem (Agreement of the PCP under single edge perturbation)**

For an injection attack $\delta^\theta$ on edge all the edges in $\mathcal{E}_\Delta$ the PCP achieves agreement if

$$\left\|\delta^\theta\right\|_\infty < \rho_\Delta^\theta = \left(K_\Delta \mathcal{R}_{\mathcal{E}_\Delta}(\mathcal{G})\right)^{-1},$$

independently from the values taken by any admissible codeword $\theta$.

# Robustness to channel tampering (cont'd)

With the previous assumptions holding and setting $K_\Delta := \max_{(u,v)\in\mathcal{E}_\Delta} \{K_{uv}\}$:

**Theorem (Agreement of the PCP under single edge perturbation)**

For an injection attack $\delta^\theta$ on edge all the edges in $\mathcal{E}_\Delta$ the PCP achieves agreement if

$$\left\|\delta^\theta\right\|_\infty < \rho_\Delta^\theta = (K_\Delta \mathcal{R}_{\mathcal{E}_\Delta}(\mathcal{G}))^{-1},$$

independently from the values taken by any admissible codeword $\theta$.

Sketch of the proof: follows immediately from $\left\|\Delta^W\right\| < \mathcal{R}_{\mathcal{E}_\Delta}^{-1}(\mathcal{G})$.
The three assumptions $(i)$-$(iii)$ are sufficient and necessary to figure out the worst case scenario in which the absolute slope of each $p_{uv}$, $(u,v) \in \mathcal{E}_\Delta$, is maximum, i.e. the absolute slope reaches $K_\Delta$ for any given $\theta$.

# Robustness to channel tampering (cont'd)

With the previous assumptions holding and setting $K_\Delta := \max_{(u,v)\in\mathcal{E}_\Delta} \{K_{uv}\}$:

**Theorem (Agreement of the PCP under single edge perturbation)**

For an injection attack $\delta^\theta$ on edge all the edges in $\mathcal{E}_\Delta$ the PCP achieves agreement if

$$\left\|\delta^\theta\right\|_\infty < \rho^\theta_\Delta = (K_\Delta \mathcal{R}_{\mathcal{E}_\Delta}(\mathcal{G}))^{-1},$$

independently from the values taken by any admissible codeword $\theta$.

Sketch of the proof: follows immediately from $\left\|\Delta^W\right\| < \mathcal{R}^{-1}_{\mathcal{E}_\Delta}(\mathcal{G})$.
The three assumptions $(i)$-$(iii)$ are sufficient and necessary to figure out the worst case scenario in which the absolute slope of each $p_{uv}$, $(u,v) \in \mathcal{E}_\Delta$, is maximum, i.e. the absolute slope reaches $K_\Delta$ for any given $\theta$.

Up to minor changes this result is also valid for **discrete-time** consensus.

# Further analysis and numerical results

# A trade-off: information hiding vs robust stability

Observation: if $\mathcal{E}_\Delta = \{(u,v)\}$, the Lipschitz constant $K_{uv}$ plays a crucial role in either improving information hiding or robust stability!

> Considering $p_{uv}(\theta_{uv}) = b_{uv}\theta_{uv}$, the perturbation on $\theta_{uv}$ is directly "amplified" by $K_{uv} = |b_{uv}|$. Let's focus on this case.

# A trade-off: information hiding vs robust stability

<u>Observation</u>: if $\mathcal{E}_\Delta = \{(u,v)\}$, the Lipschitz constant $K_{uv}$ plays a crucial role in either improving information hiding or robust stability!

Considering $p_{uv}(\theta_{uv}) = b_{uv}\theta_{uv}$, the perturbation on $\theta_{uv}$ is directly "amplified" by $K_{uv} = |b_{uv}|$. Let's focus on this case.

- if $K_{uv}$ increases then the image of $p_{uv} = b_{uv}\theta_{uv}$ reaches more values w.r.t. to some fixed neighborhood of $\theta_{uv}$

$K_{uv} \uparrow$ then encrpytion capabilities of $p_{uv} \uparrow$

# A trade-off: information hiding vs robust stability

<u>Observation</u>: if $\mathcal{E}_\Delta = \{(u, v)\}$, the Lipschitz constant $K_{uv}$ plays a crucial role in either improving information hiding or robust stability!

Considering $p_{uv}(\theta_{uv}) = b_{uv}\theta_{uv}$, the perturbation on $\theta_{uv}$ is directly "amplified" by $K_{uv} = |b_{uv}|$. Let's focus on this case.

- if $K_{uv}$ increases then the image of $p_{uv} = b_{uv}\theta_{uv}$ reaches more values w.r.t. to some fixed neighborhood of $\theta_{uv}$

$$K_{uv} \uparrow \quad \text{then encrpytion capabilities of } p_{uv} \uparrow$$

- if $K_{uv}$ increases then the value of $\rho^{\theta}_{uv} = (K_{uv}\mathcal{R}_{uv}(\mathcal{G}))^{-1}$ decreases

$$K_{uv} \uparrow \quad \text{then robust stability of PCP} \downarrow$$

# The resilience gap

Let us define the quantities: $\mathcal{R}^{\star}_{\mathcal{E}_\Delta}(\mathcal{G}) = \max_{(u,v)\in\mathcal{E}_\Delta} \{\mathcal{R}_{(u,v)}(\mathcal{G})\}$;

$$\mathcal{R}^{tot}_{\mathcal{E}_\Delta}(\mathcal{G}) = \mathrm{tr}\left[P^\top R^\top_{(\mathcal{T},\mathcal{C})}(R_{(\mathcal{T},\mathcal{C})} W R^\top_{(\mathcal{T},\mathcal{C})})^{-1} R_{(\mathcal{T},\mathcal{C})} P\}\right].$$

It is known that:

$$\mathcal{R}^{\star}_{\mathcal{E}_\Delta}(\mathcal{G}) \leq \mathcal{R}_{\mathcal{E}_\Delta}(\mathcal{G}) \leq \mathcal{R}^{tot}_{\mathcal{E}_\Delta}(\mathcal{G})$$

[D. Zelazo and M. Bürger, *On the Robustness of Uncertain Consensus Networks*, TCNS, 2017]

# The resilience gap

Let us define the quantities:

$$\mathcal{R}^{\star}_{\mathcal{E}_\Delta}(\mathcal{G}) = \max_{(u,v)\in\mathcal{E}_\Delta} \{\mathcal{R}_{(u,v)}(\mathcal{G})\};$$

$$\mathcal{R}^{tot}_{\mathcal{E}_\Delta}(\mathcal{G}) = \mathrm{tr}\left[P^\top R^\top_{(\mathcal{T},\mathcal{C})}(R_{(\mathcal{T},\mathcal{C})} W R^\top_{(\mathcal{T},\mathcal{C})})^{-1} R_{(\mathcal{T},\mathcal{C})} P\}\right].$$

It is known that:

$$\mathcal{R}^{\star}_{\mathcal{E}_\Delta}(\mathcal{G}) \leq \mathcal{R}_{\mathcal{E}_\Delta}(\mathcal{G}) \leq \mathcal{R}^{tot}_{\mathcal{E}_\Delta}(\mathcal{G})$$

[D. Zelazo and M. Bürger, *On the Robustness of Uncertain Consensus Networks*, TCNS, 2017]

The following ratio is named *resilience gap*

$$g(\mathcal{G}, \mathcal{E}_\Delta) = 1 - \frac{\mathcal{R}^{\star}_{\mathcal{E}_\Delta}(\mathcal{G})}{\mathcal{R}_{\mathcal{E}_\Delta}(\mathcal{G})} \in [0, 1).$$

This quantity measures the **emerging amount of conservatism** related to the fact that multiple edges are under attack.

# The resilience gap

Let us define the quantities: $\mathcal{R}^{\star}_{\mathcal{E}_\Delta}(\mathcal{G}) = \max_{(u,v)\in\mathcal{E}_\Delta} \{\mathcal{R}_{(u,v)}(\mathcal{G})\}$;

$$\mathcal{R}^{tot}_{\mathcal{E}_\Delta}(\mathcal{G}) = \mathrm{tr}\left[P^\top R^\top_{(\mathcal{T},\mathcal{C})}(R_{(\mathcal{T},\mathcal{C})} W R^\top_{(\mathcal{T},\mathcal{C})})^{-1} R_{(\mathcal{T},\mathcal{C})} P\}\right].$$

It is known that:

$$\mathcal{R}^{\star}_{\mathcal{E}_\Delta}(\mathcal{G}) \leq \mathcal{R}_{\mathcal{E}_\Delta}(\mathcal{G}) \leq \mathcal{R}^{tot}_{\mathcal{E}_\Delta}(\mathcal{G})$$

[D. Zelazo and M. Bürger, *On the Robustness of Uncertain Consensus Networks*, TCNS, 2017]

The following ratio is named *resilience gap*

$$g(\mathcal{G}, \mathcal{E}_\Delta) = 1 - \frac{\mathcal{R}^{\star}_{\mathcal{E}_\Delta}(\mathcal{G})}{\mathcal{R}_{\mathcal{E}_\Delta}(\mathcal{G})} \in [0, 1).$$

This quantity measures the **emerging amount of conservatism** related to the fact that multiple edges are under attack.

Observation

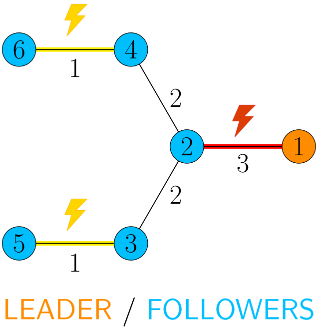
If i) $|\mathcal{E}_\Delta| = 1$, or
ii) $2 \leq |\mathcal{E}_\Delta| \leq n-1 = |\mathcal{E}|$ then $g(\mathcal{G}, \mathcal{E}_\Delta) = 0$

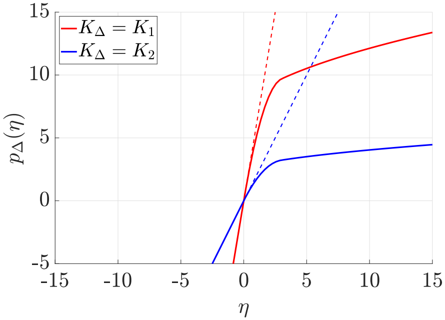
# Numerical simulations

Decoding function: $$p_\Delta(\eta) = \begin{cases} K_\Delta\left(\frac{4}{13}\sqrt{\eta+1}+1\right), & \text{if } \eta \geq 3; \\ K_\Delta\left(-\frac{2}{13}\eta^2+\eta\right), & \text{if } 0 \leq \eta < 3; \\ K_\Delta \eta, & \text{if } \eta < 0; \end{cases}$$

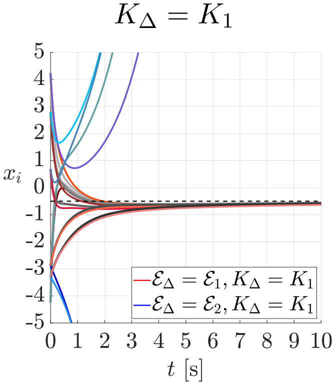
Edges under attack: $\mathcal{E}_1 = \{(1,2)\}$, $\mathcal{E}_2 = \{(1,2),(3,5),(4,6)\}$

Couple of values for $K_\Delta$: $K_1 = 2$, $K_2 = 6$



# Numerical simulations (cont'd)




**Semi-autonomous network** dynamics:

$$\dot{\mathbf{x}} = (L_B(\mathcal{G}) \otimes I_D)\mathbf{x} + (B \otimes I_D)\mathbf{u},$$

where $L_B(\mathcal{G}) = L(\mathcal{G}) + \mathrm{diag}(B\mathbb{1}_{|\mathcal{V}_l|})$ and $B \in \mathbb{R}^{n\times|\mathcal{V}_l|}$ such that $[B]_{i\ell} > 0$, if agent $i$ belongs to the leader set $\mathcal{V}_l = \{1\}$; $[B]_{i\ell} = 0$, otherwise.

# Conclusions

# Final remarks

- the **secure-by-design consenus protocol** rests on novel methods (e.g. network manager, objective coding, information localization) to preserve integrity, synchronization and performance of networks
- the previously devised single-edge attack case has been broadened to a scenario with **multiple threats**
- **small-gain-theorem-based stability guarantees** based on the effective resistance are given, which depend on both network topology and encryption system employed
- **trade-off** between information hiding & robust stability is discussed
- the **conservatism** arising from a multiplicity of threats is addressed
- **future works**: extending this approach to nonlinear consensus and formation control protocols

# THANK YOU FOR YOUR ATTENTION

# References


- J. Lunze, *Networked control of multi-agent systems*, Edition MoRa, 2019
- D. Zelazo and M. Bürger, *On the Robustness of Uncertain Consensus Networks*, TCNS, 2017
- M. Fabris and D. Zelazo, *Secure Consensus via Objective Coding: Robustness Analysis to Channel Tampering*, IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2022
- D.J. Klein and M. Randić, *Resistance distance*, Journal of Mathematical Chemistry, 1993
- M. Fabris, G. Michieletto and A. Cenedese, *A General Regularized Distributed Solution for the System State Estimation from Relative Measurements*, IEEE L-CSS, 2022
- A. Chapman, *Semi-Autonomous Networks: Effective Control of Networked Systems through Protocols, Design, and Modeling*, Springer, 2015