CCS 2021 Satellite Symposium

Data-based diagnosis of Networked Dynamical Systems

27th October 2021, Lyon, France

DETECTING SALIENT FEATURES OF NETWORK DYNAMICAL SYSTEMS FROM TIME SERIES

Pietro De Lellis

University of Naples Federico II

(joint-work with Maurizio Porfiri, New York University)

Understanding Complex Systems

- We are experiencing a rapid increase of data storage - digital data will reach 175 ZB by 2025!
- Paradoxically, our understanding and ability to control complex systems is often hampered by inherent limitations in the available data

Understanding Complex Systems

- We are experiencing a rapid increase of data storage - digital data will reach 175 ZB by 2025!

- Paradoxically, our understanding and ability to control complex systems is often hampered by inherent limitations in the available data

- Despite the success of the network dynamical systems paradigm, when collecting and analyzing data of complex systems, we are hindered by

  - Limited spatial resolution
  - Non-stationarity
  - Hidden units
  - Restricted access to data
  - Paucity of the dataset
  - Noise plaguing the dynamics

- Often, we only have at our disposal a single, noisy time series, from which it is hard to identify the *salient features* of the system

Salient Features of Complex Systems

- How many units compose the system? Can we detect the presence of hidden units in the system?

(Haehne, Casadiego, Peinke, & Timme, *Physical Review Letters*, 2019)

Salient Features of Complex Systems

- How many units compose the system? Can we detect the presence of hidden units in the system?

How do we detect the presence
(and effect) of unobserved neurons?

Salient Features of Complex Systems

- How many units compose the system? Can we detect the presence of hidden units in the system?

How do we detect the presence
(and effect) of unobserved neurons?

- Can we determine key / influential / vulnerable nodes in the system

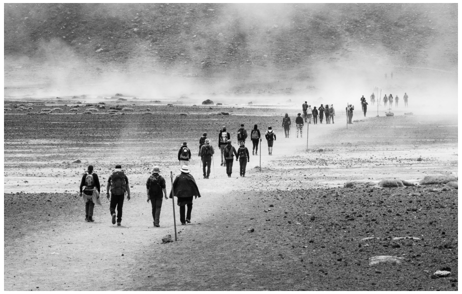
Salient Features of Complex Systems

- How many units compose the system? Can we detect the presence of hidden units in the system?

How do we detect the presence
(and effect) of unobserved neurons?

- Can we determine key / influential / vulnerable nodes in the system

Human migrations:
how do we identify most vulnerable
districts to climate change?



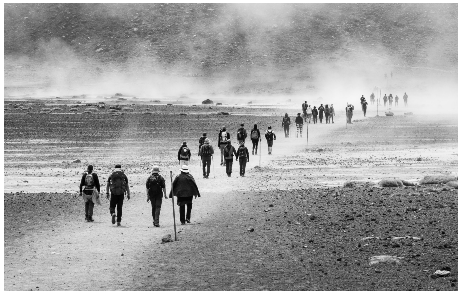
Salient Features of Complex Systems

- How many units compose the system? Can we detect the presence of hidden units in the system?

How do we detect the presence
(and effect) of unobserved neurons?

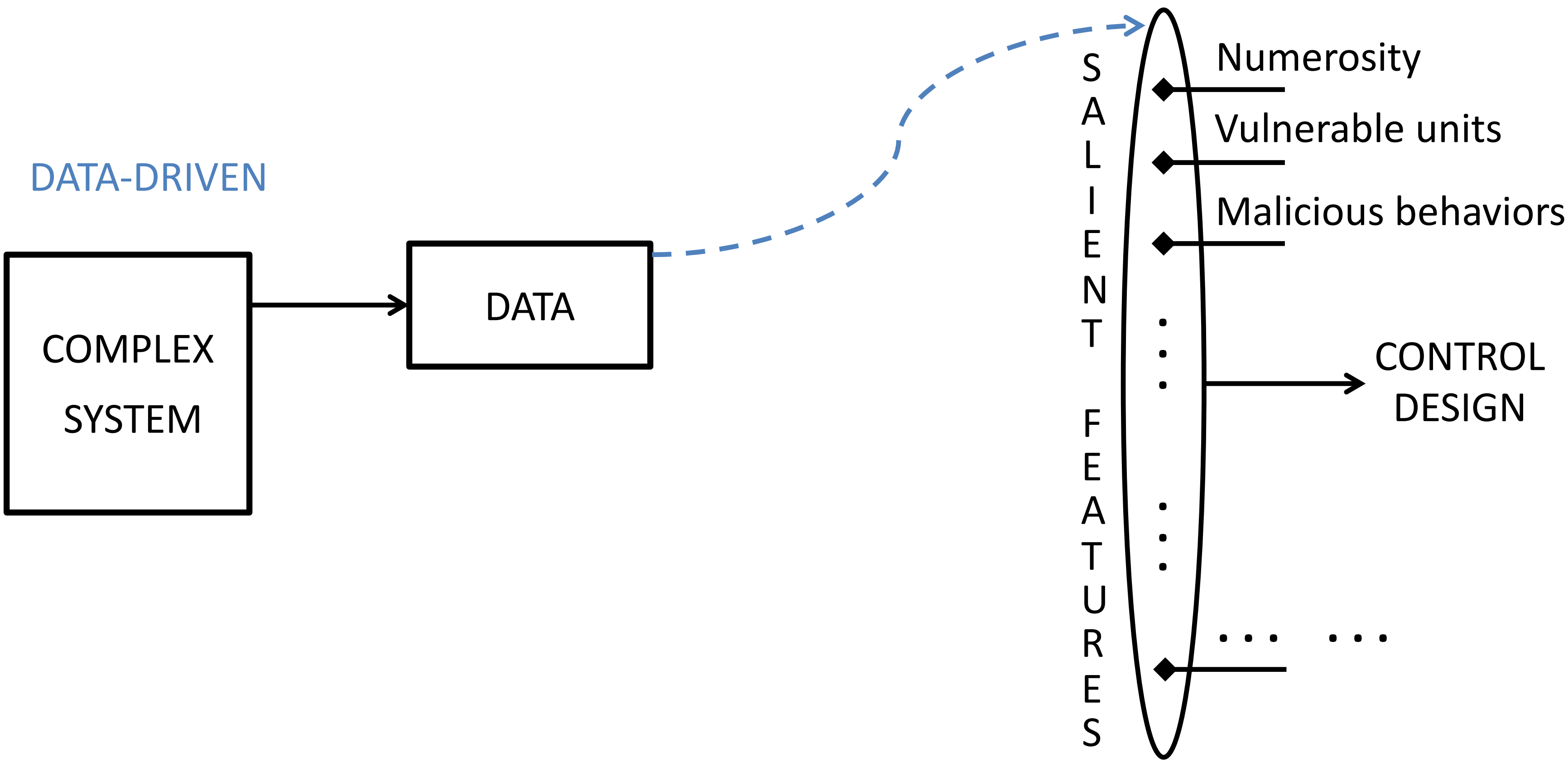
- Can we determine key / influential / vulnerable nodes in the system

Human migrations:
how do we identify most vulnerable
districts to climate change?

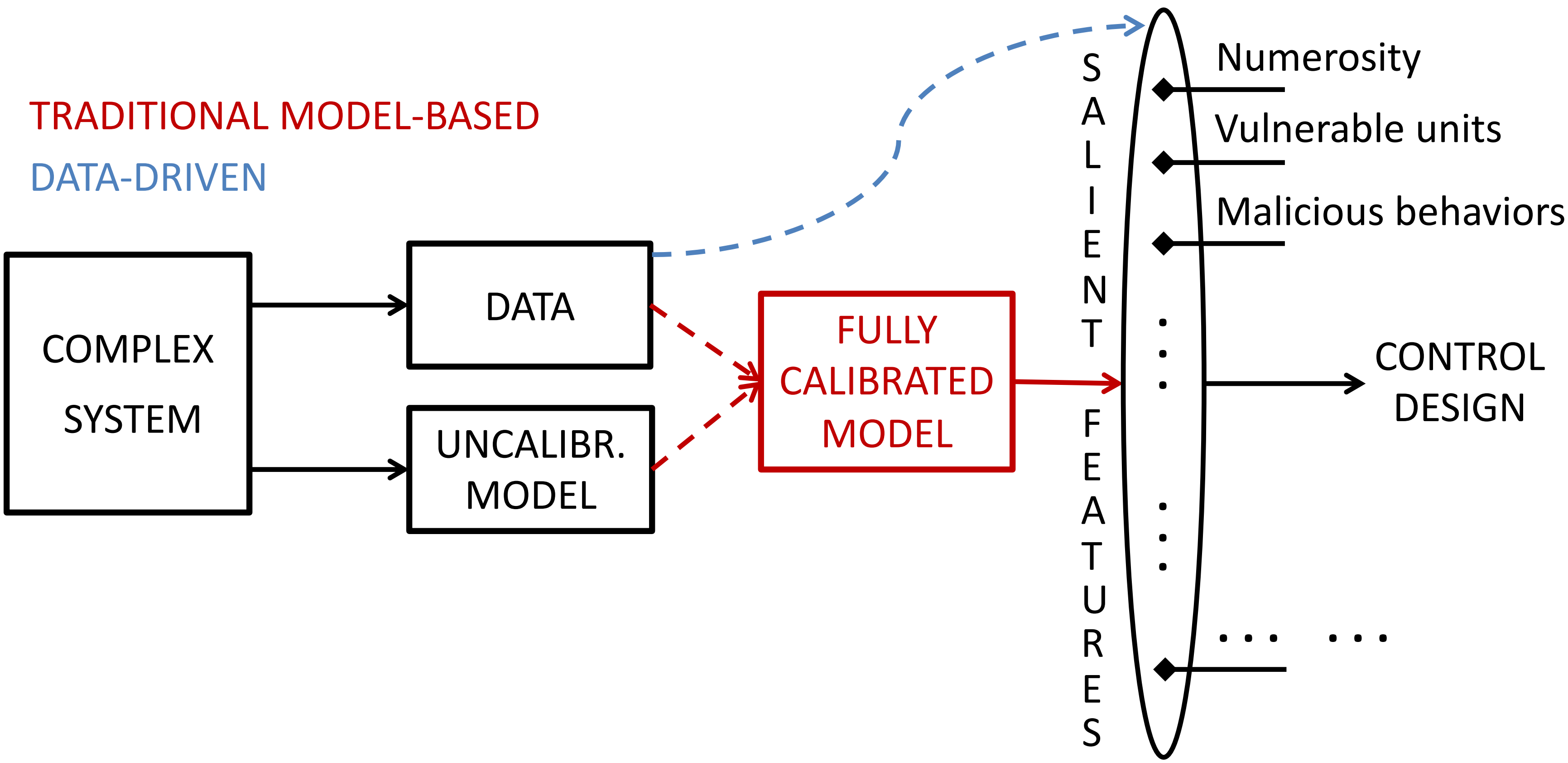


Power grids:
what are the nodes that would trigger
cascading effects on the network?

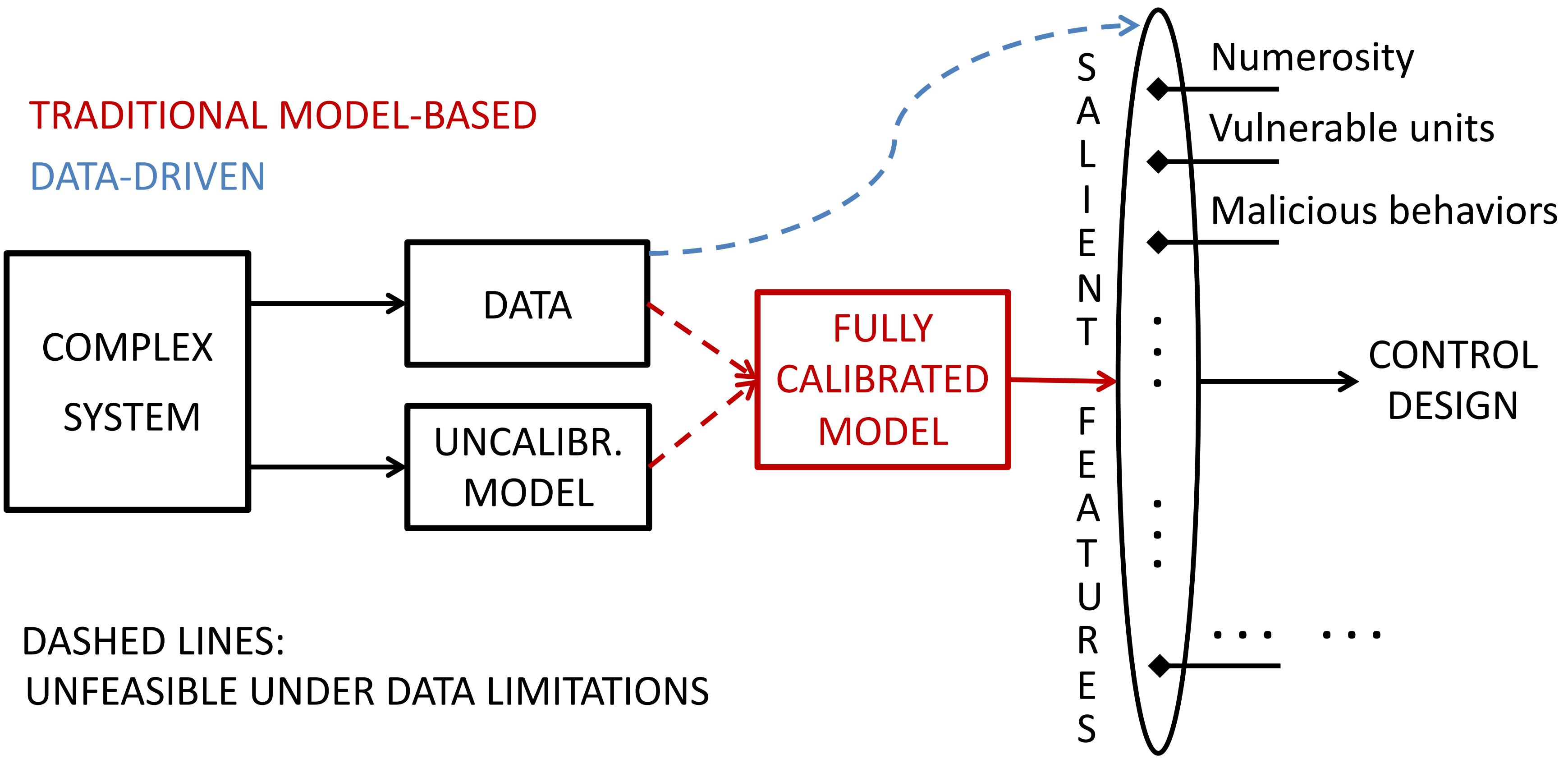
Detecting Salient Features of Complex Systems



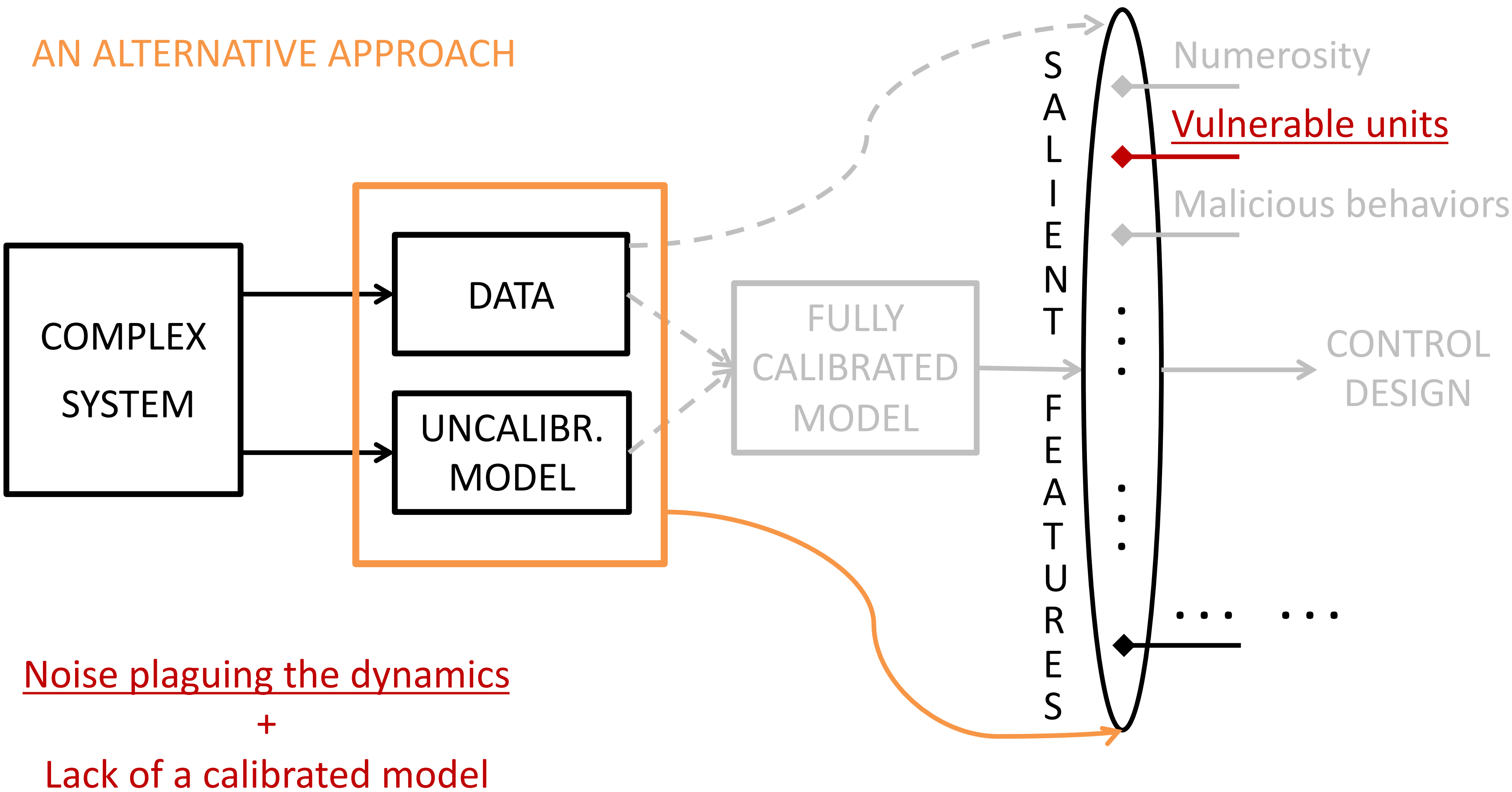
Limitations on the available data



Limitations on the available data



Limitations on the available data



Vulnerability: Select Findings and Open Problems

- Peripheral nodes play a key role on the overall network dynamics in power grids (Tyloo et al., *Science Advances*, 2019)

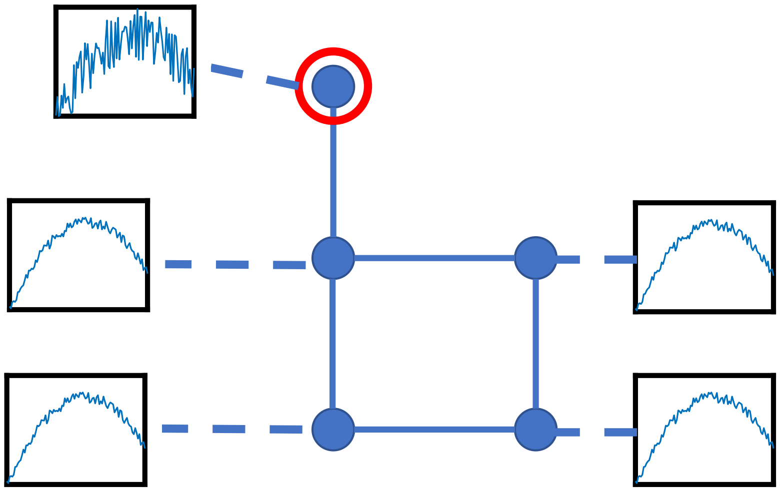
- An inverse correlation was observed between node resistance centrality and transient stability of the European power grid

- Similar results have been observed when assessing vulnerability in the classical consensus problem (Porfiri and Frasca, *IEEE TCNS*, 2018)

Vulnerability: Select Findings and Open Problems

- Peripheral nodes play a key role on the overall network dynamics in power grids (Tyloo et al., *Science Advances*, 2019)
- An inverse correlation was observed between node resistance centrality and transient stability of the European power grid
- Similar results have been observed when assessing vulnerability in the classical consensus problem (Porfiri and Frasca, *IEEE TCNS*, 2018)
- Regardless of the performance metric, evaluating vulnerability requires assessing how specific manipulation at one node translate into network-level performance

Ideal versus Real Experiment

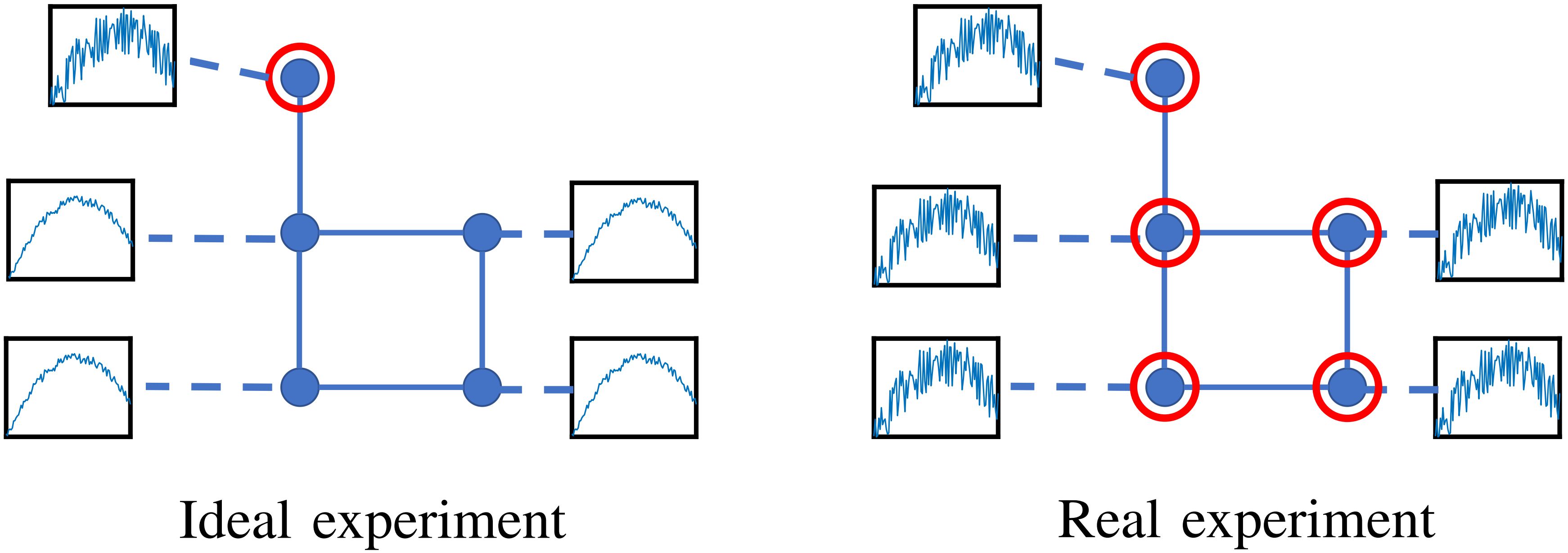


Ideal experiment

Vulnerability can be assessed via ideal experiments, where the researcher selectively inject a perturbation at each node, by means of

- Calibrated mathematical models
- Experiments where dynamics can be freely manipulated

Ideal versus Real Experiment



- In real experimental observations noise plagues each node
- Can we pinpoint causal influence from time-series of experimental observations? (without calibrated model / targeted experimental manipulations)

The Network Dynamical System

- *A priori knowledge* on the network system:
  - Interactions are bidirectional (the network topology is undirected)
  - Diffusion dynamics are taking place

The Network Dynamical System

- *A priori knowledge* on the network system:
  - Interactions are bidirectional (the network topology is undirected)
  - Diffusion dynamics are taking place
- We consider a network of N diffusively coupled linear systems

$$x_{k+1}^i = F x_k^i - \sum_{j=1}^{N} l_{ij} \Gamma x_k^j + q_i B \eta_k^i$$

Individual dynamics

State of the i-th unit

Element ij of the Laplacian matrix

Inner coupling matrix

The Network Dynamical System

- *A priori knowledge* on the network system:
  - Interactions are bidirectional (the network topology is undirected)
  - Diffusion dynamics are taking place
- We consider a network of N diffusively coupled linear systems

$$x_{k+1}^i = F x_k^i - \sum_{j=1}^{N} l_{ij} \Gamma x_k^j + q_i B \eta_k^i$$

positive if node i is affected by noise
0 otherwise

i.i.d. noise with 0 mean
and covariance matrix Σ_η

Determines how noise diffuses
on the state variables

The Network Dynamical System

- *A priori knowledge* on the network system:
  - Interactions are bidirectional (the network topology is undirected)
  - Diffusion dynamics are taking place
- We consider a network of N diffusively coupled linear systems

$$x_{k+1}^i = F x_k^i - \sum_{j=1}^{N} l_{ij} \Gamma x_k^j + q_i B \eta_k^i$$

- We are not aware of the individual dynamics, network topology, that is, the model is uncalibrated
- Available data (encoded by the output function)
- State not fully accessible

$$y_k = (I_N \otimes C) x_k$$

Vulnerability of Network Dynamical Systems

- Let us introduce the steady-state covariance matrix

$$\Xi_{\infty}^{\boxed{Q}} = \lim_{k\rightarrow+\infty} \mathrm{E}\left[\xi_k \xi_k^{\mathrm{T}}\right]$$

$$\mathrm{diag}\left\{q_1, \ldots, q_N\right\}$$

Vulnerability of Network Dynamical Systems

- Let us introduce the steady-state covariance matrix

$$\Xi_{\infty}^{Q} = \lim_{k\to+\infty} \mathrm{E}\left[\xi_k \xi_k^{\mathrm{T}}\right]$$

- To study vulnerability to an attack at the i-th unit we would need to consider an ideal experiment where noise is only injected at unit i $\longrightarrow$ $Q = \mathbb{e}_i \mathbb{e}_i^{\mathrm{T}}$

Vulnerability of Network Dynamical Systems

- Let us introduce the steady-state covariance matrix

$$\Xi_\infty^Q = \lim_{k\to+\infty} \mathrm{E}\left[\xi_k \xi_k^{\mathrm{T}}\right]$$

- To study vulnerability to an attack at the i-th unit we would need to consider an ideal experiment where noise is only injected at unit i $\longrightarrow$ $Q = \mathbb{e}_i \mathbb{e}_i^{\mathrm{T}}$
- Vulnerability could be then quantified as

$$\mathrm{Vul}(i, M) = \mathrm{Tr}\left[(M^{\mathrm{T}} \otimes C)\Xi_\infty^{\mathbb{e}_i \mathbb{e}_i^{\mathrm{T}}}(M \otimes C^{\mathrm{T}})\right]$$

where $M = \mathrm{diag}\left\{m_1, \ldots, m_N\right\}$ weights the relevance of each node in the network;

- Unfortunately, from time-series of the real experiment we can only estimate $\Sigma_\infty^Q = \lim_{t\to+\infty} \mathrm{E}\left[y_k y_k^{\mathrm{T}}\right]$ and not $\Xi_\infty^{\mathbb{e}_i \mathbb{e}_i^{\mathrm{T}}}$

Reconciling Ideal and Real Experiments

- Ideal and real experiments can be reconciled due to two classical principles in circuit theory, the superposition and reciprocity principles

1. From the model linearity, the response of the system to noise injected at all nodes can be obtained as the sum of the responses to noise individually injected at each node

Reconciling Ideal and Real Experiments

- Ideal and real experiments can be reconciled due to two classical principles in circuit theory, the superposition and reciprocity principles

1. From the model linearity, the response of the system to noise injected at all nodes can be obtained as the sum of the responses to noise individually injected at each node
2. Being the network undirected, we proved that the reciprocity principle carries over to the context of network dynamical systems:

The effect of noise injected at node i on node j is equivalent to the effect of noise injected at node j on node i

$$\left(\Xi_{\infty}^{\mathbb{e}_i \mathbb{e}_i^{\mathrm{T}}}\right)_{jj} = \left(\Xi_{\infty}^{\mathbb{e}_j \mathbb{e}_j^{\mathrm{T}}}\right)_{ii}$$

Vulnerability from Time-Series

- By applying the superposition and reciprocity principles, we can exactly infer vulnerability when $M = Q$

$$\boxed{\mathrm{Vul}(i, M) = \mathrm{Tr}\left((R \otimes I_p)\Sigma_\infty^Q (R \otimes I_p)\right)_{ii}}$$

where $R = I_N - \mathbb{1}_\mathbb{N} \mathbb{1}_N^\mathrm{T} / N$

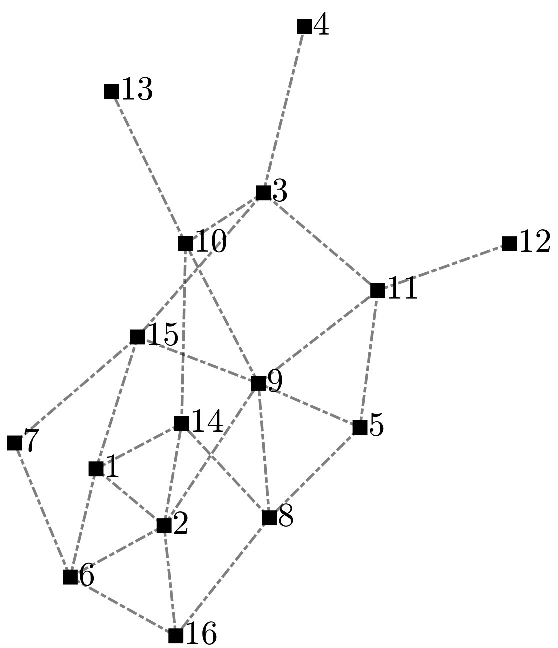
- Vulnerability can be then estimated from the sample covariance matrix of the network output y_k

- The result can be extended to the case of non diagonal M
- When instead M and Q are different, lower and upper bound for the vulnerability can be computed instead

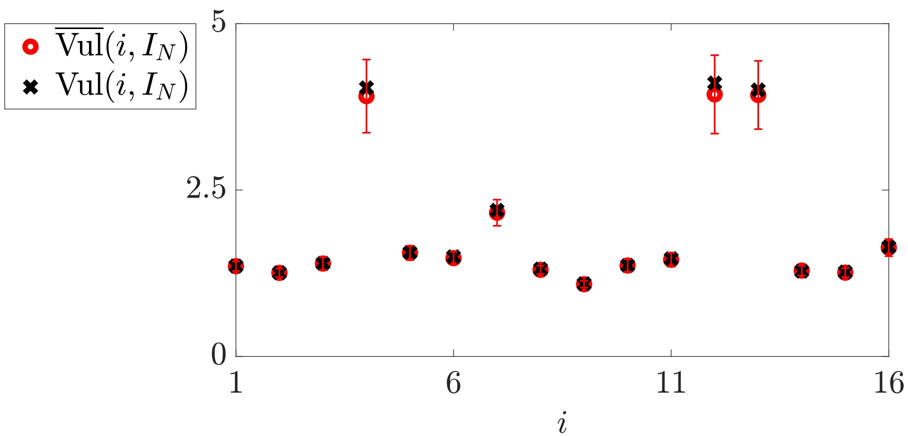
Verification on Synthetic Data

- We consider the same network examined in (Fitch, Leonard, 2015), with

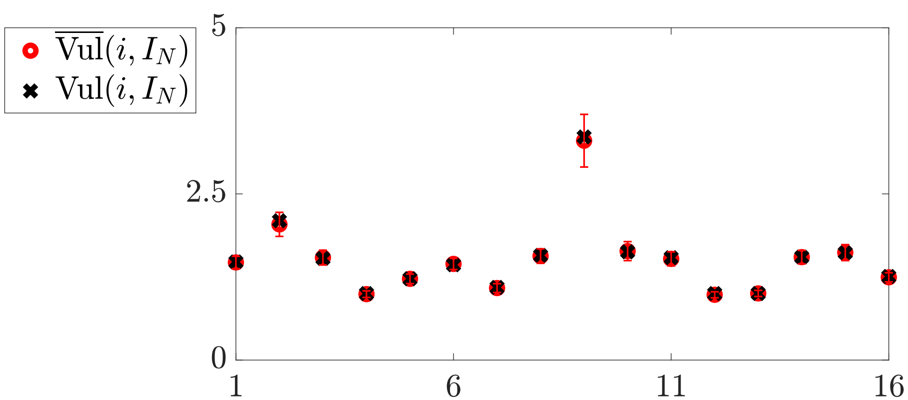
$$x_{k+1}^i = \alpha x_k^i - \sum_{j=1}^{N} l_{ij} \beta x_k^j + q_i \eta_k^i, \quad y_k^i = x_k^i$$



Graph topology



$\alpha = 1$
$\beta = 0.159$



$\alpha = -0.1$
$\beta = 0.1$

Firearm Prevalence in the U.S.

- Firearm acquisition in the U.S. has an inherent network structure (Porfiri et al., 2020)
- Firearm acquisitions in any State are influenced by acquisitions in other States

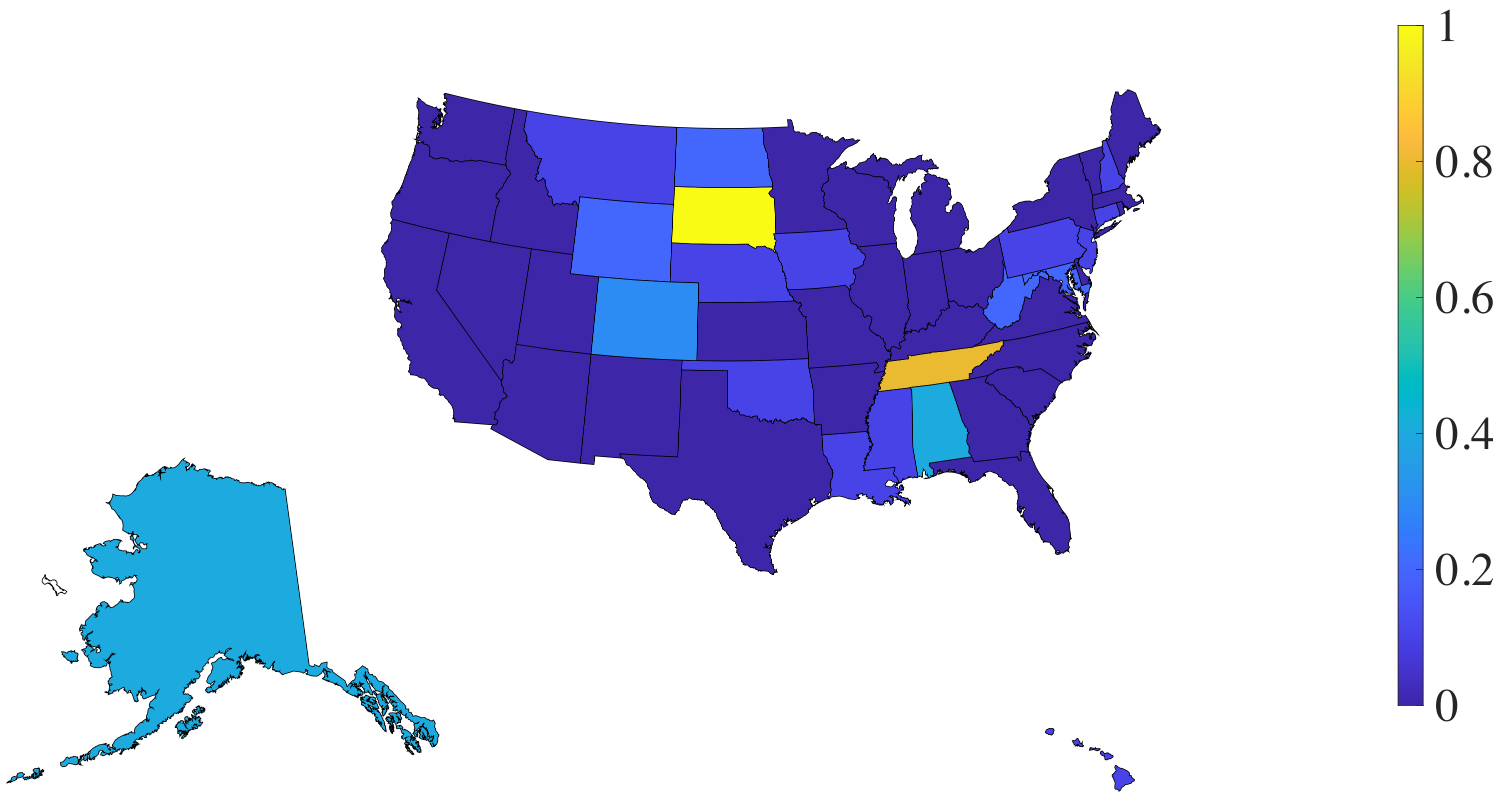
Firearm Prevalence in the U.S.

- Firearm acquisition in the U.S. has an inherent network structure (Porfiri et al., 2020)
- Firearm acquisitions in any State are influenced by acquisitions in other States
- Background checks are a proxy of firearm acquisitions
- We analyzed data from 1999 to 2017
- The time-series has been detrended and seasonally adjusted

Firearm Prevalence in the U.S.

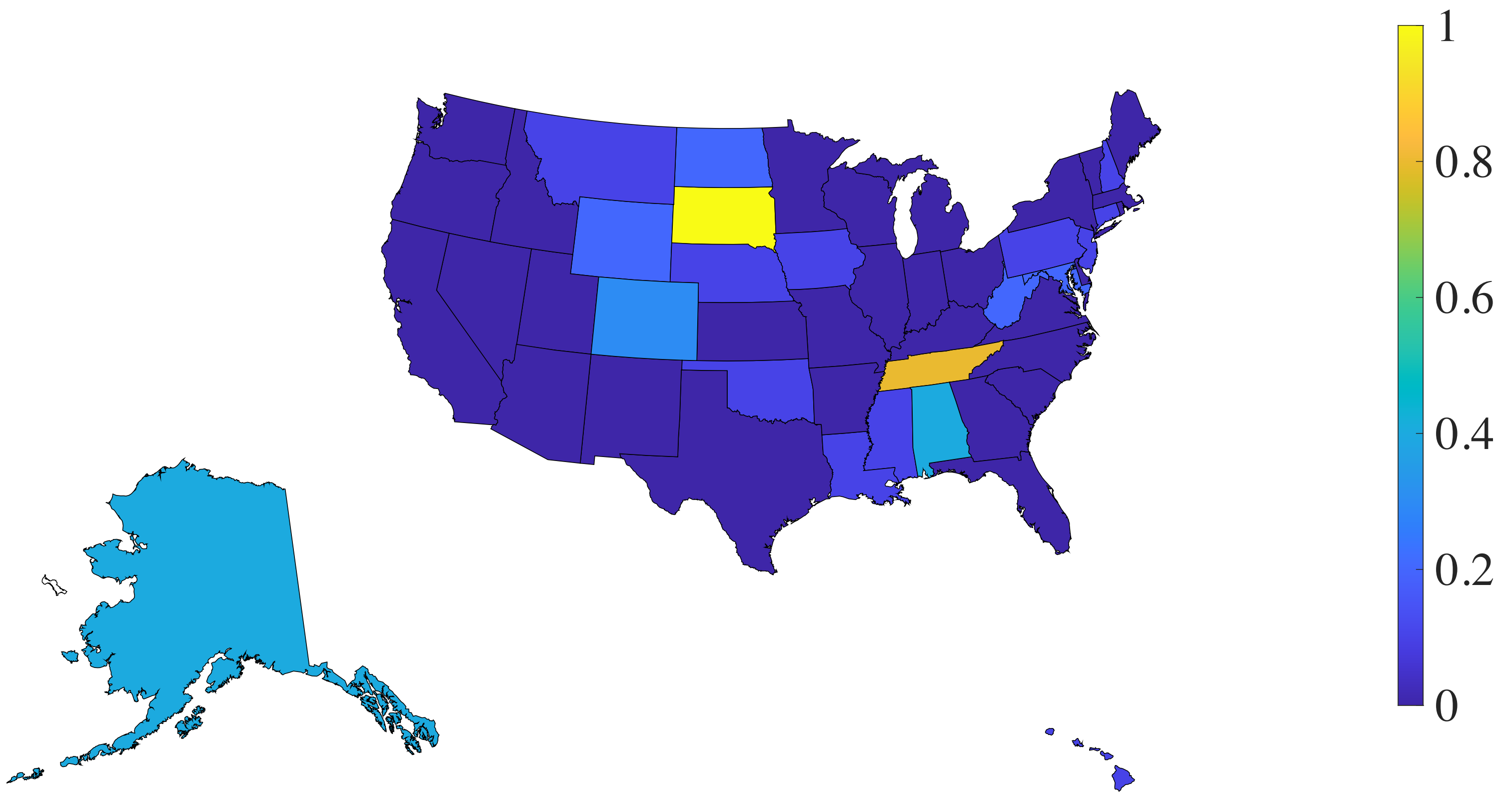
- Firearm acquisition in the U.S. has an inherent network structure (Porfiri et al., 2020)
- Firearm acquisitions in any State are influenced by acquisitions in other States
- Background checks are a proxy of firearm acquisitions
- We analyzed data from 1999 to 2017
- The time-series has been detrended and seasonally adjusted
- We then calculated the sample mean covariance matrix associated to the pre-processed time-series
- Assuming that noise enters all the States in the same manner, we estimated the vulnerability index we defined

Firearm Prevalence in the U.S.



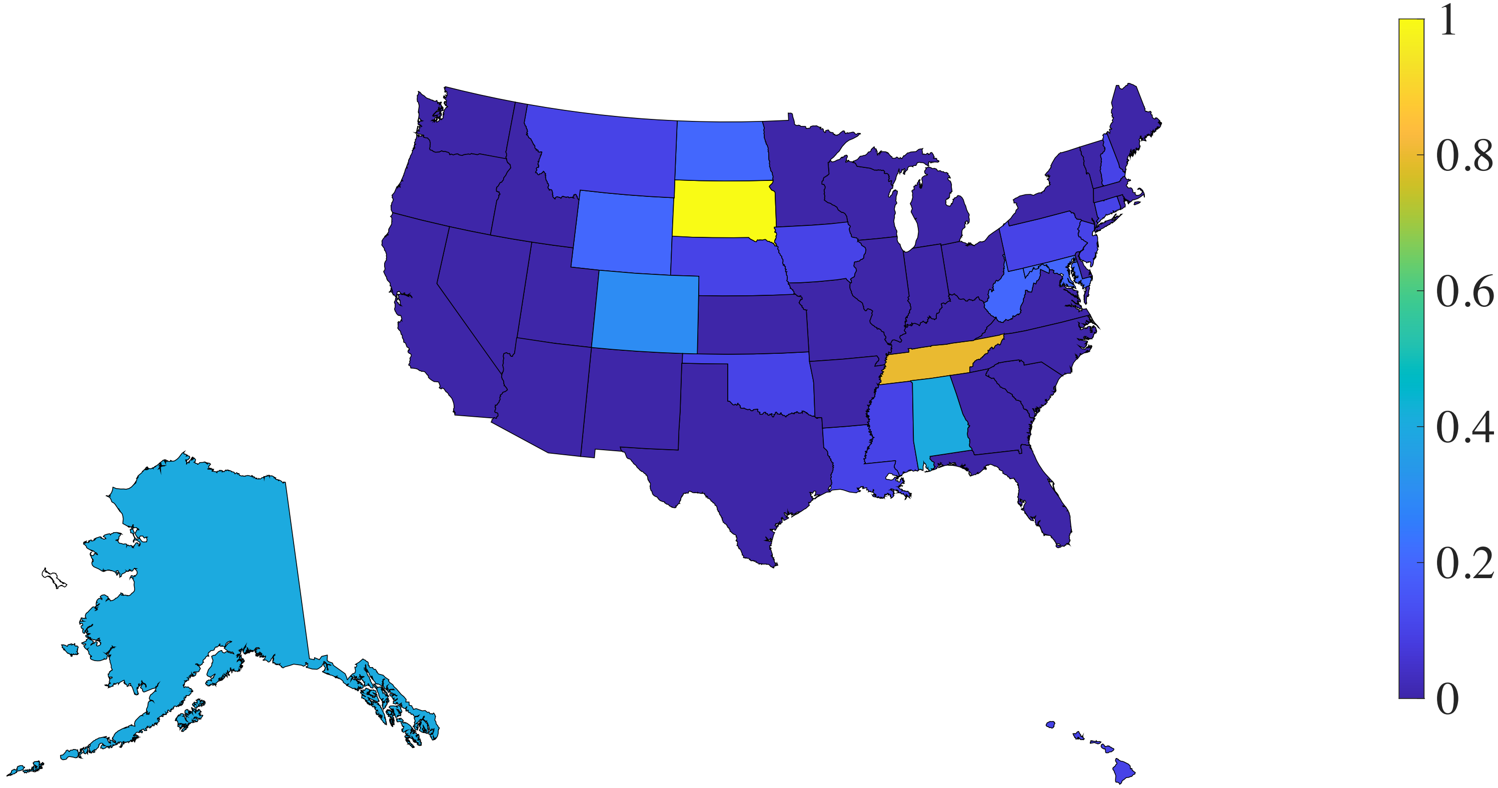
- The 5 most influential states are South Dakota, Tennessee, Alaska, Alabama, and Colorado

Firearm Prevalence in the U.S.



- These states are among those with the most permissive legal environment (quantified as the fraction of firearm safety law in effect)

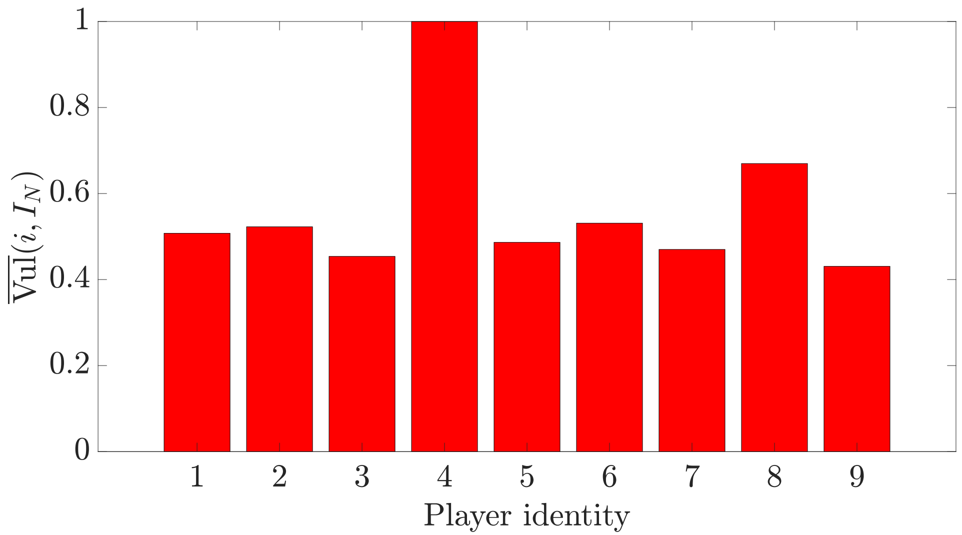
Firearm Prevalence in the U.S.



- States in which it is easier to purchase a firearm might have a higher connectivity in the network: other States may use them as proxy of potential changes in firearm regulations

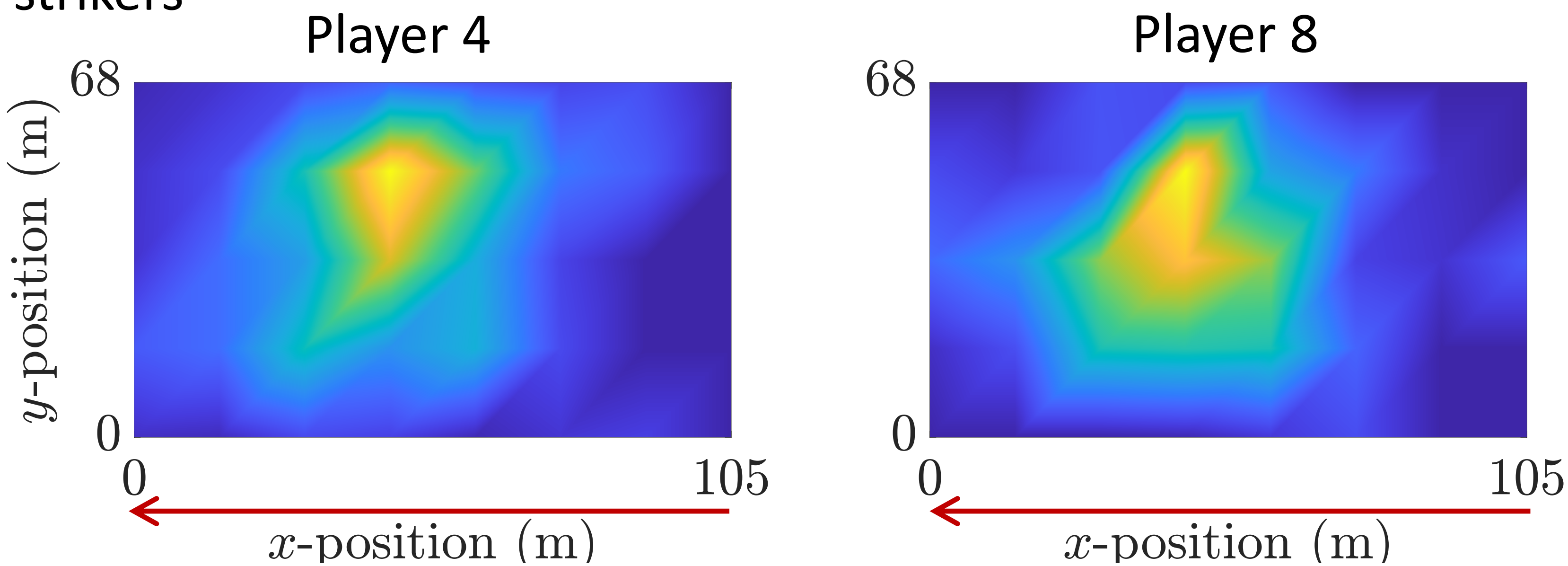
Analysis of a Soccer Dataset

- We examine a dataset of the positions of 9 soccer players in a soccer game
- We focus on the time series of speed and compute vulnerability
- In this context, vulnerability is associated to lack of coordination
- Player 4 and 8 appear to be the key players in the team



Analysis of a Soccer Dataset

- Player 4 acts behind the strikers, while Player 8 is one of the two strikers



- A reduction in the coordination of either of these two players could hinder the coordination of the whole team
- Interesting, they are among the player with the least ball possession (movements off the ball are crucial)

Discussion

- We established a novel approach to identify influential nodes in network dynamical systems from time-series of real experiments
- We focused networks of time-invariant, diffusively coupled linear systems that synchronize against added noise
- For this class of problems, the influence of a node is defined as the extent to which adding noise at that particular node affects the steady-state covariance of the disagreement dynamics
- We demonstrate that the influence of each of the nodes can be effectively inferred from time series
- The chief reason for the correspondence between ideal and real experiments lies in the reciprocity principle

Ongoing and Future Research

- In the same setting, can we identify other salient features (e.g. numerosity, hidden units)?

- Devise methodologies for inferring influence from real experiments in which nodes have heterogeneous nodal dynamics

- The entire methodology assumes that the network is undirected. which allows for deriving modal equations that would be not feasible in the case of directed networks.

- The mathematical treatment is presently limited to time-invariant linear dynamics, thereby calling for further research on temporal networks and nonsmooth dynamics.

References and Contacts

- P. De Lellis, M. Porfiri, "Detection of influential nodes in network dynamical systems from time series", IEEE Transactions on Control of Network Systems, 8(3), 1249-1260, 2021.
- P. De Lellis, M. Ruiz Marin, M. Porfiri, Modeling human migration under environmental change: a case study of the effect of sea level rise in Bangladesh, Earth's Future, 9(4), e2020EF001931, 2021.

- https://sites.google.com/site/pierodelellis/home
- pietro.delellis@unina.it

- Acknowledgement. ACROSS project: Analysis and ContRol of emerging properties in evolving complex networks Of Stochastic Systems (funder: Compagnia di San Paolo – Fondazione Banco di Napoli)