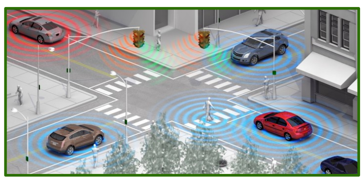
Analysis and Design of Secure Cyber-Physical Systems

Fabio Pasqualetti

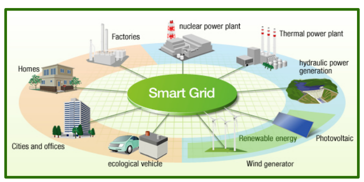
Department of Mechanical Engineering
University of California, Riverside

Outline

Cyber-physical systems, opportunities and challenges



Computation
+
Communication
+
Control



Connectivity enables advanced applications, yet is a source of vulnerability

Security is one of the biggest challenges to realize the CPS vision

Cyber-physical systems are next target of cyber warfare

Stuxnet worm 'targeted high-value Iranian assets'

By Jonathan Fildes
Technology reporter, BBC News

23 September 2010

One of the most sophisticated pieces of malware ever detected was probably targeting "high value" infrastructure in Iran, experts have told the BBC.

Replay attack as "out of the movies":
- Infect controllers via USB device
- Observe and take control
- Deceive and damage centrifuges

Cyber attack on Saudi plant designed to cause explosion

Details emerge of Triton attack against plant safety system which caused shutdown in August

Tags: Cyber crime, Mandiant Corp (www.mandiant.com), Saudi Arabia, Schneider Electric

PRINT E-MAIL TEXT SIZE

By Mark Sutton
Published March 17, 2018

A cyberattack against a petrochemical company in Saudi Arabia could have caused serious physical damage, according to news reports.

The attack, which was detected in August, appears to have been designed to cause safety controllers to stop working, which could have caused an explosion at the plant.

An unnamed petrochemical plant in Saudi Arabia was targeted by the Triton or Trisis malware. (picture for illustrative purposes only).

The attack apparently only failed due to a flaw in the coding of the malware, causing equipment to shut down instead.

Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks

OCTOBER 11, 2017 // AUTHORS: DONGHUI PARK, JULIA SUMMERS, MICHAEL WALSTROM

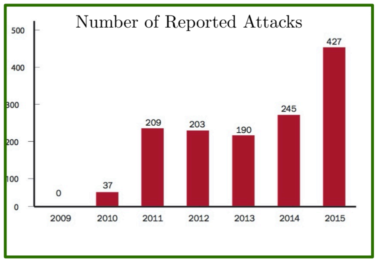
Commercial drones highly vulnerable to cyber-attacks and criminal misuse

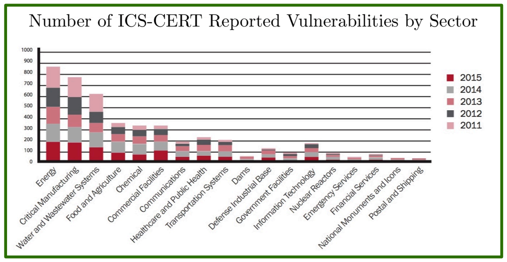
31 July 2017 | Author: Jay Jay

Mysterious GPS glitch telling ships they're parked at airport may be anti-drone measure

Elizabeth Weise, USATODAY Published 1:41 p.m. ET Sept. 26, 2017 | Updated 3:03 p.m. ET Oct. 3, 2017

Severity and scale of the cyber-physical security problem

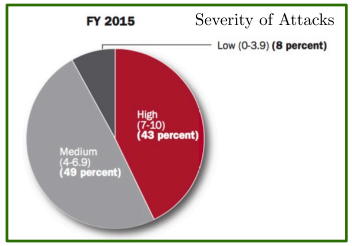




ICS-CERT Annual Report, 2015

- Self-reported incidents, likely more
- Critical infrastructures are key target
- CPS security is of National interest
- Economic, political, criminal drivers
- Attacks are easy to cast, yet severe

Symantec: "Expect more of these threats"



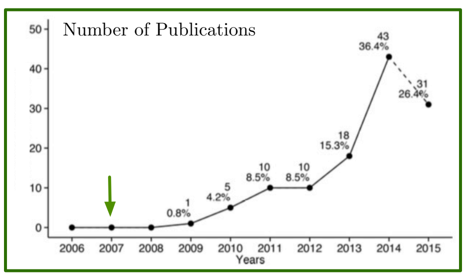
ICS-CERT Annual Report, 2015

Cyber-physical security vs cyber security and fault tolerance

1. Different systems
   - Cyber-physical systems comprise dynamical components
   - Laws of physics → challenges and opportunities for security
   - E.g., patches may be expensive; models give predictive power
2. Different objectives
   - Confidentiality, integrity and availability in addition to safety/resilience
   - Continue operation and guarantee graceful degradation under attack
   - Attacks are intentional/"worst-case", faults accidental/"generic"
3. Different methods
   - Data protection not sufficient, need compatibility with physics (Stuxnet)
   - Can use sensors/actuators for active security, physical watermarking
   - Unlike faults, attackers do not obey assumptions and predefined models

Cyber-physical security $\neq$ cyber security $\oplus$ fault tolerance

An independent and fast-growing research field



Cyber-Physical Systems Security: a Systematic Mapping Study, 2016

F. Pasqualetti, A. Bicchi, F. Bullo "Consensus computation in unreliable networks: A system theoretic approach," in *IEEE Transactions on Automatic Control*, 56(12):90-104, 2011.

S. Sundaram, C. Hadjicostis "Distributed function calculation via linear iterative strategies in the presence of malicious agents," in *IEEE Transactions on Automatic Control*, 56(7):1495-1508, 2011.

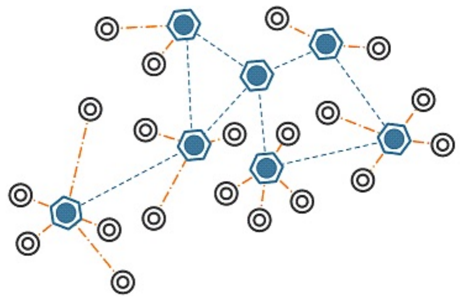
F. Pasqualetti, F. Dörfler, F. Bullo "Attack Detection and Identification in Cyber-Physical Systems," in *IEEE Transactions on Automatic Control*, 58(11):2715-2729, 2013.

F. Hamza, P. Tabuada, and S. Diggavi "Secure estimation and control for cyber-physical systems under adversarial attacks," in *IEEE Transactions on Automatic Control*, 59(6):1454-1467, 2014.

Y. Mo, B. Sinopoli. "Secure Estimation in the Presence of Integrity Attacks," in *IEEE Transactions on Automatic Control*, 60(4):1145-1151, 2015.

Outline

Sensor network



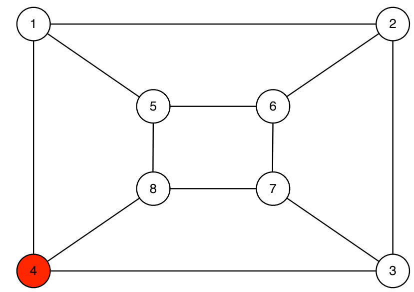
- Nodes update state based on weighted average of neighboring states

$$x_i(t+1) = \sum a_{ij} x_j(t)$$

- Widely used in consensus, estimation, formation control ...
- Misbehaving nodes (faulty, malicious) update their state **arbitrarily**

How many misbehaving nodes can be tolerated (detected/identified)?

Sensor network with misbehaving nodes



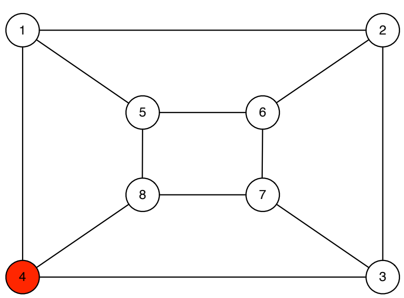
- Graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$
- Weights: $a_{ij} \neq 0 \leftrightarrow (i,j) \in \mathcal{E}$
- Adjacency matrix: $A = [a_{ij}]$
- Misbehaving nodes: $\mathcal{K} \subseteq \mathcal{V}$

$$x(t+1) = Ax(t) + B_{\mathcal{K}} u_{\mathcal{K}}(t)$$

$$y_i(t) = C_i x_i(t)$$

- $B_{\mathcal{K}} \Rightarrow$ location of misbehaving nodes
- $u_{\mathcal{K}} \Rightarrow$ strategy of misbehaving nodes
- $B_{\mathcal{K}}, u_{\mathcal{K}}$ unknown to node $i \notin \mathcal{K}$
- $y_i \Rightarrow$ local measurements of node i

Sensor network with misbehaving nodes



- Graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$
- Weights: $a_{ij} \neq 0 \leftrightarrow (i,j) \in \mathcal{E}$
- Adjacency matrix: $A = [a_{ij}]$
- Misbehaving nodes: $\mathcal{K} \subseteq \mathcal{V}$

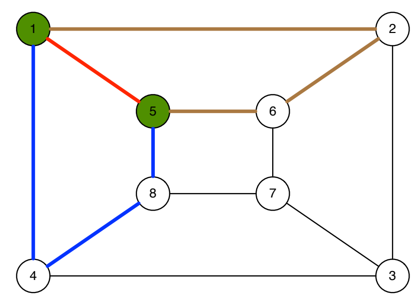
$$x(t+1) = Ax(t) + B_{\mathcal{K}} u_{\mathcal{K}}(t)$$

$$y_i(t) = C_i x_i(t)$$

$$B_4 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}^T$$

$$C_1 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}^T$$

How many misbehaving nodes can a network tolerate?



- Graph connectivity: $\kappa(\mathcal{G})$
- $\kappa(\mathcal{G})$: max number of disjoint paths between any two vertices
- Knowing A and y_i, how many nodes $\mathcal{K}$ can be detected?

Fundamental detection bound

Generically, any well-behaving node can detect $\kappa(\mathcal{G}) - 1$ misbehaving nodes

- Detection: recognize that $u_{\mathcal{K}} \neq 0$ from measurements
- Identification: reconstruct the attack matrix $B_{\mathcal{K}}$ from measurements

Undetectable misbehaving nodes

The misbehaving nodes $\mathcal{K}$ remain undetected by node i if and only if

$$y_i(x_0, B_{\mathcal{K}} u_{\mathcal{K}}, t) = y_i(\bar{x}_0, 0, t)$$

Equivalently, if and only if

$$y_i(\tilde{x}_0, B_{\mathcal{K}} u_{\mathcal{K}}, t) = 0.$$

Undetectability of misbehaving nodes $\Leftrightarrow$ zero dynamics

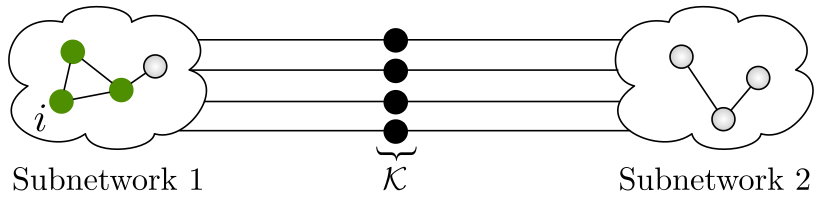
The misbehaving nodes $\mathcal{K}$ remain undetected by node i if and only if $u_{\mathcal{K}}$ excites only the zero dynamics of $(A, B_{\mathcal{K}}, C_i)$, for some initial state $\tilde{x}_0$.

- Invariant zero structure determines undetectable attack strategies
- Solution to: $(sI - A)x_0 - B_{\mathcal{K}} g = 0$ and $Cx_0 + D_{\mathcal{K}} g = 0$

At most $\kappa(\mathcal{G}) - 1$ misbehaving nodes can be detected

Fundamental detection bound

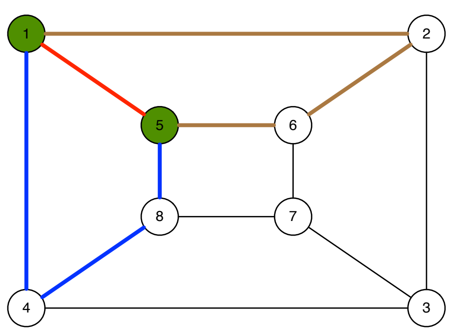
Generically, any well-behaving node can detect $\kappa(\mathcal{G}) - 1$ misbehaving nodes



Misbehaving nodes update their state to cancel interconnection signal
$\Leftrightarrow$
zero dynamics

- $\text{Im}(A_{12}) \subseteq \text{Im}(B_{\mathcal{K}})$, $x_1(t+1) = A_{11}x_1(t) + A_{12}x_2(t) + B_{\mathcal{K}} u_{\mathcal{K}}(t)$

How many misbehaving nodes can a network tolerate?



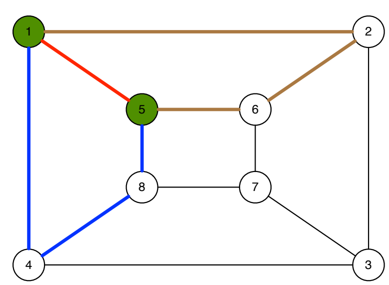
- Graph connectivity: $\kappa(\mathcal{G})$
- Knowing A and y_i, how many nodes $\mathcal{K}$ can be identified?

Fundamental identification bound

Generically, any well-behaving node can identify $\left\lfloor \frac{\kappa(\mathcal{G})-1}{2} \right\rfloor$ misbehaving nodes

- Identifiability $\Leftrightarrow$ zero dynamics of $(A, [B_{\mathcal{K}}\ B_{\mathcal{R}}], C_i)$

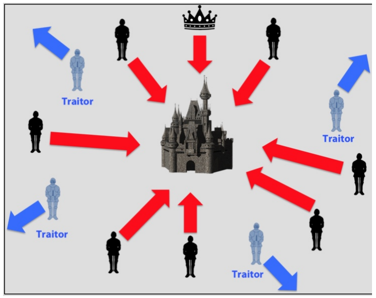
An example, and some considerations



- Connectivity $\kappa(\mathcal{G}) = 3$
- Generically, 2 misbehaving node can be detected
- Generically, 1 misbehaving node can be identified

- To remain undetected/unidentified, attacks must be chosen carefully
- Faults are generic; different bounds (security $\neq$ fault tolerance)
- Genericity: bounds hold for "almost all" choices of edge weights
- Tradeoff between connectivity and security (system design, more later)

Connections to Byzantine Generals problem, and extensions



The Byzantine Generals Problem

LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE
SRI International

The Byzantine Generals Strike Again*

DANNY DOLEV†

Computer Science Department, Stanford University, Stanford, California 94305

Received March 10, 1981

Can unanimity be achieved in an unreliable distributed system? This problem was named the "Byzantine Generals Problem" by L. Lamport, R. Shostak, and M. Pease (Technical Report 54, Computer Science Laboratory, SRI International, March 1980). The results obtained in the present paper prove that unanimity is achievable in *any* distributed system *if and only if* the number of faulty processors in the system is: (1) less than one-third of the total number of processors; and (2) less than one-half of the connectivity of the system's network. In cases where unanimity is achievable, algorithms for obtaining it are given. This result forms a complete characterization of networks in the light of the Byzantine Problem.

Connections to Byzantine Generals problem, and extensions

Our bounds are in accordance to results for Byzantine Generals. Moreover,

1. "zero dynamics" ⇔ "resilience" ⇔ "Byzantine bounds"
2. linear protocols are maximally resilient to misbehaving nodes

In fact, our bounds include and generalize many existing security notions:

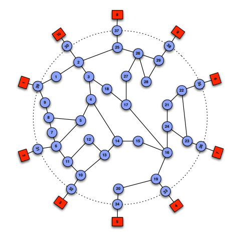
- "zero dynamics" ⇒ "2s-observability" (secure estimation) ...
  [P. Tabuada et al. 2014]
- "zero dynamics" ⇒ "securable subspace" (as unobs. subspace) ...
  [P. R. Kumar et al. 2018]
- "zero dynamics" ⇒ other undetectable attacks "stealthy", "covert" ...
  [S. Sastry et al. 2011], [R. Smith 2015], [B. Sinopoli et al. 2017]
- "zero dynamics" ⇒ remedial controls against stealthy attacks ...
  [K. Johansson et al. 2015]

Outline

Model of power network

Small-signal structure-preserving power network model:

1. transmission network: generators ■, buses ●, DC load flow assumptions, and network susceptance matrix $Y = Y^T$

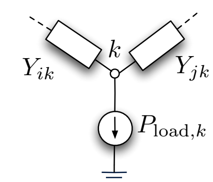


2. generators ■ modeled by swing equations:

$$M_i\ddot{\theta}_i + D_i\dot{\theta}_i = P_{\text{mech.in},i} - \sum_j Y_{ij}\cdot(\theta_i - \theta_j)$$

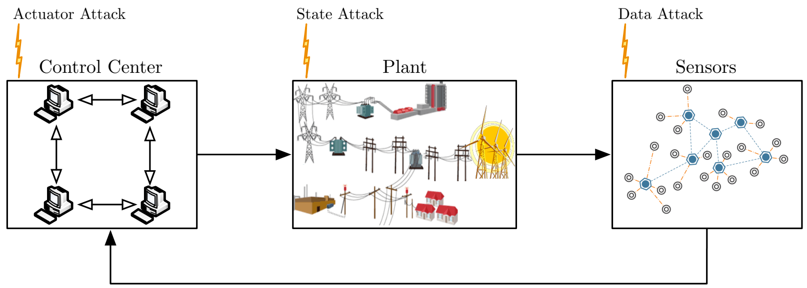
3. buses ● with constant real power demand:

$$0 = P_{\text{load},i} - \sum_j Y_{ij}\cdot(\theta_i - \theta_j)$$



⇒ Linear differential-algebraic sys: $E\dot{x} = Ax + P$

Models of attackers and monitors

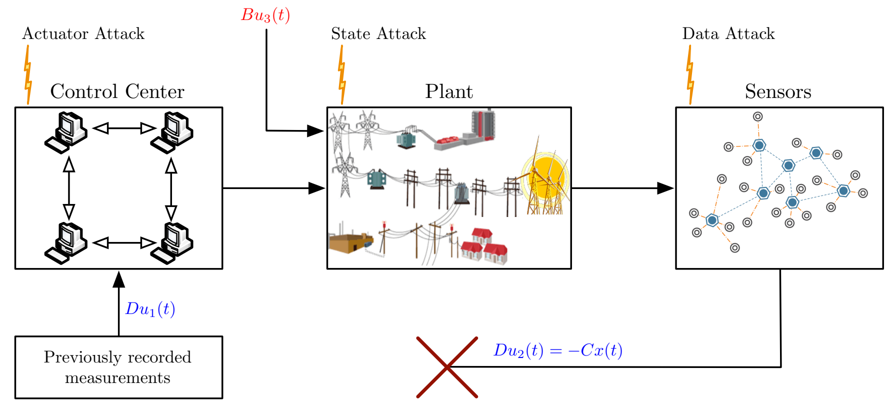


$$E\dot{x}(t) = Ax(t) + Bu(t) \qquad \text{(state and actuator attack)}$$

$$y(t) = Cx(t) + Du(t) \qquad \text{(data substitution attack)}$$

- Attackers are colluding and omniscient (model, params, state)
- Attackers aim to change physical state and mislead monitors
- Monitors aim to detect/identify attacks via measurements

Modeling Stuxnet with unknown inputs and matrices



System dynamics:

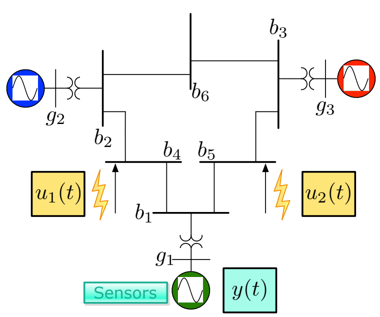
$$E\dot{x}(t) = Ax(t) + Bu_3(t)$$

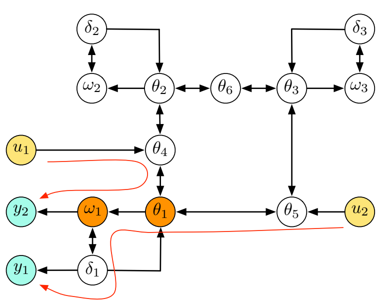
$$y(t) = Cx(t) + Du_1(t) + Du_2(t)$$

Undetectable attacks in power systems

Equivalent characterizations of undetectable attacks:

1. **Vulnerability:** undetectable attack $y(x_1, 0, t) = y(x_2, u, t)$
2. **System theory:** intruder/monitor system has invariant zeros
3. **Graph theory:** # attack signals $>$ size of input/output linking

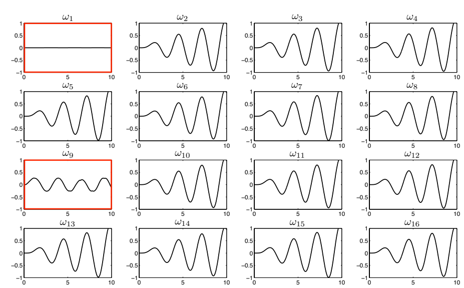


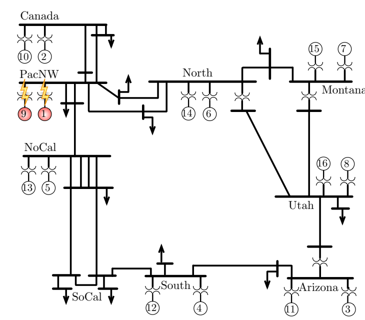


Design of targeted attacks

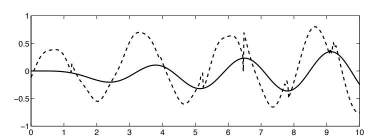
- Targeted attack design via geometric / optimal control (dual to detection)
- Malicious coalition: $\{1, 9\}$ (PacNW)
- Attack input minimizes $\|\omega_9(t)\|_{\mathcal{L}_\infty}$ subject to $\|\omega_{16}(t)\|_{\mathcal{L}_\infty} \geq 1$ (Utah)

$\Rightarrow$ non-colluding generators are damaged





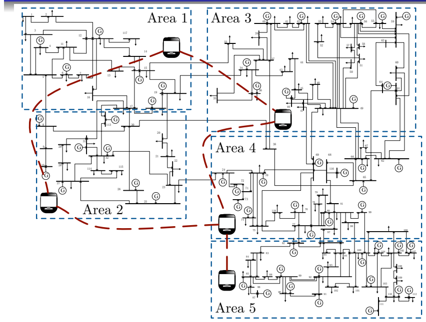
Reduced WECC grid



Governor control input

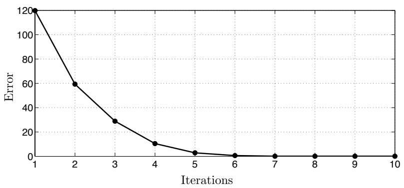
(not a fault signal!)

Distributed monitor design

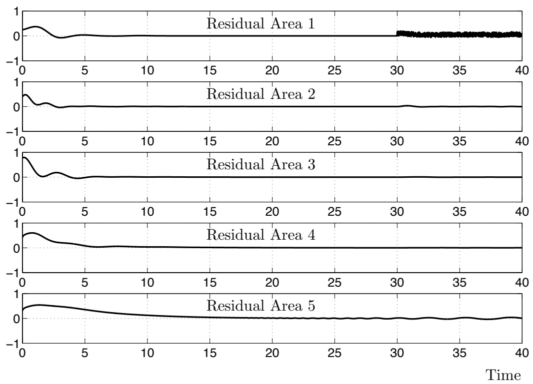


- Detection/identification of attacks
- Centralized geometric filters
- Decentralized filters via waveform relaxation and distributed UIO

Waveform iteration error:

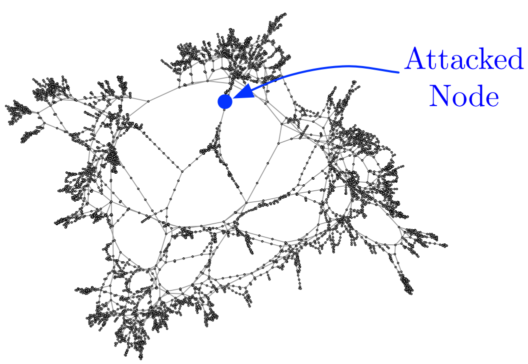


Residuals $r_i^{(k)}(t)$ for $k = 100$:



Outline

Mitigating attacks

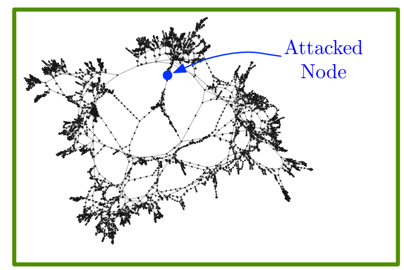


How to limit the effect of attacks on the system?

Controller redesign, containment strategy, design for security ...

Resilience of large network systems

- Network size $\gg$ attacked nodes
- $\dot{x} = Ax + Bu$
- $A \rightarrow$ interaction graph
- $B \rightarrow$ attacked nodes



Controllability Gramian: $\mathcal{W} = \int_0^\infty e^{At} B B^\mathsf{T} e^{A^\mathsf{T} t}\, dt$

Small $\lambda_{\min}(\mathcal{W})$ $\Leftrightarrow$ **Small controllability degree**

Large $\lambda_{\min}(\mathcal{W})$ $\Leftrightarrow$ **Large controllability degree**

Large networks are resilient to few attacked nodes

Upper bound on controllability degree

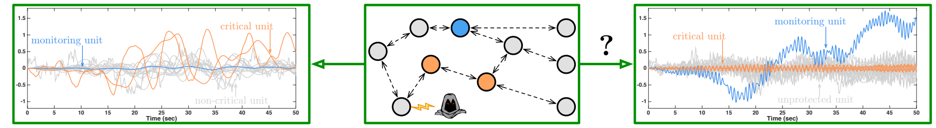
Let A be diagonalizable as $A = V \Lambda V^{-1}$. Then,

$$\lambda_{\min}(\mathcal{W}) \leq \frac{\kappa^4(V)}{2s(A)} \, \rho^{\frac{\#\text{nodes}}{\#\text{attacked nodes}}}$$

- $\kappa(V) = \sigma_{\max}(V)/\sigma_{\min}(V)$ (condition number; non-normality degree)
- $s(A) = -\max \Re(\lambda(A))$ (stability margin)
- $\rho = \max \left| \frac{\lambda_i(A) - \lambda_j(A)}{\lambda_i^*(A) + \lambda_j(A)} \right|^2$ (< 1 when A is stable)

- Resilience increases exponentially with $\frac{\#\text{nodes}}{\#\text{attacked nodes}}$
  (bounded non-normality degree and stability margin)
- Certain network modes could still be controllable by attacker

Gramian assignment for selective network resilience



How to choose the network weights to protect critical nodes and facilitate attack detection from monitoring nodes?

- Fixed set $\mathcal{S}$ of vulnerable nodes $\Rightarrow B$
- Effect of attack on node $i \Rightarrow \mathcal{H}_2^2(A, B, e_i^{\mathsf{T}}) = \mathcal{W}_{ii}$
  (energy impulse response from B to i = i-th diagonal entry Gramian)

Network design for Gramian assignment

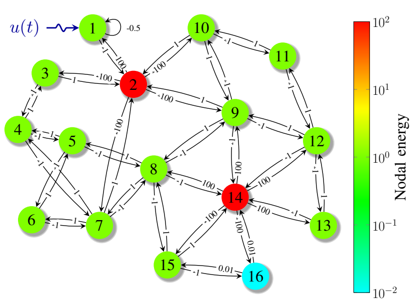
Given a graph $\mathcal{G}$, $\{\omega_1, \dots, \omega_n\} > 0$, and an input matrix B, find a weighted adjacency matrix A such that the Gramian $\mathcal{W}$ of A, B satisfies $\mathcal{W}_{ii} = \omega_i$.

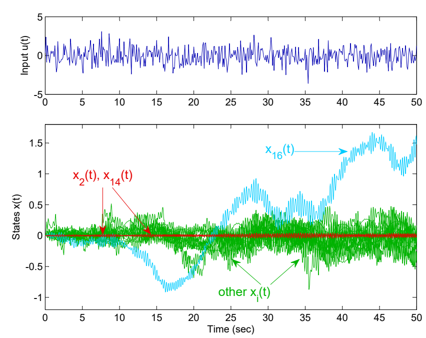
Network design for selective security

Network design for Gramian assignment

If A is stable and "uniformly input-connected" with control impacts β_i,

$$\mathcal{W}_{ii} = \beta_i.$$





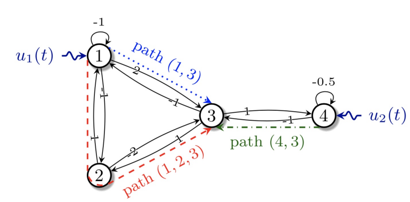
Select weights to assign control impacts $\Rightarrow$ Network resilience by design

Network design for selective security

Network design for Gramian assignment

If A is stable and "uniformly input-connected" with control impacts β_i,

$$\mathcal{W}_{ii} = \beta_i.$$



Control impact along a path

The control impact along $(i_1, i_2, \dots i_p)$ is

$$\beta_{i_1,\dots i_p} = \frac{1}{|a_{i_1 i_1}|} \left| \frac{a_{i_2 i_1}}{a_{i_1 i_2}} \right| \left| \frac{a_{i_3 i_2}}{a_{i_2 i_3}} \right| \cdots \left| \frac{a_{i_p i_{p-1}}}{a_{i_{p-1} i_p}} \right|$$

Network design for selective security

Network design for Gramian assignment

If A is stable and "uniformly input-connected" with control impacts β_i,

$$\mathcal{W}_{ii} = \beta_i.$$

Uniformly input-connected network

A network is *uniformly input-connected* if

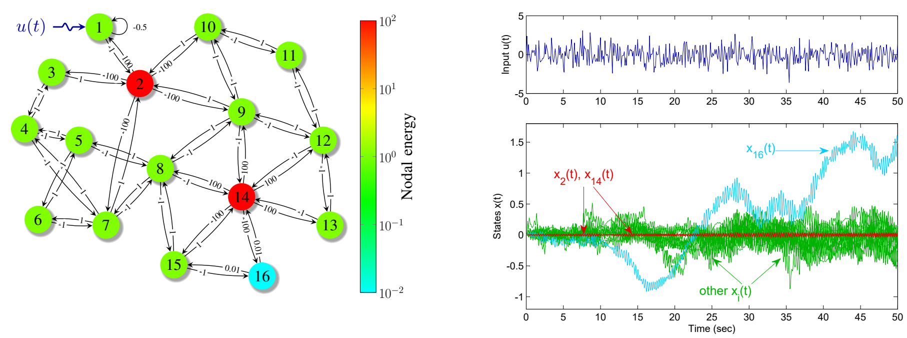
- it is sign-skew-symmetric ($a_{ij}a_{ji} < 0$, $a_{ii} < 0$ for $i \in \mathcal{S}$), and
- for every node i, all control impacts to i are equal to $\beta_i \in \mathbb{R}_{>0}$.

Network design for selective security

Network design for Gramian assignment

If A is stable and "uniformly input-connected" with control impacts β_i,

$$\mathcal{W}_{ii} = \beta_i.$$



Select weights to assign control impacts ⇒ Network resilience by design

Summary

1. Fundamental security limitations
   - A link between cyber and cyber-physical security
   - Attacks and monitors for power systems
2. Security countermeasures
   - Asymptotic bounds of network resilience
   - Network design for selective security

F. Pasqualetti, A. Bicchi, F. Bullo "Consensus computation in unreliable networks: A system theoretic approach," in *IEEE Transactions on Automatic Control*, 56(12):90-104, 2011.

F. Pasqualetti, F. Dörfler, F. Bullo "Attack Detection and Identification in Cyber-Physical Systems," in *IEEE Transactions on Automatic Control*, 58(11):2715-2729, 2013.

F. Pasqualetti and S. Zampieri and F. Bullo "Controllability Metrics, Limitations and Algorithms for Complex Networks," in *IEEE Transactions on Control of Network Systems*, 1(1):40-52, 2014.

G. Bianchin, P. Frasca, A. Gasparri, F. Pasqualetti, "The Observability Radius of Networks," in *IEEE Transactions on Automatic Control*, 62(6):3006-3013, 2017.

S. Zhao and F. Pasqualetti "Networks with Diagonal Controllability Gramians: Analysis, Graphical Conditions, and Design Algorithms," in *Automatica*, Submitted, 2018.

Other results in CPS security

3. Security for the smart grid

F. Pasqualetti, R. Carli, F. Bullo "Distributed Estimation via Iterative Projections with Application to Power Network Monitoring," in *Automatica*, 48(5):747-758, 2012.

S. Amini and F. Pasqualetti and H. Mohsenian-Rad "Dynamic Load Altering Attacks Against Power System Stability: Attack Models and Protection Schemes," in *IEEE Transactions on Smart Grid*, 1-5, 2015.

S. Amini, F. Pasqualetti, M. Abbaszadeh, H. Mohsenian-Rad "Hierarchical Location Identification of Destabilizing Faults and Attacks in Power Systems: A Frequency-Domain Approach," in *IEEE Transactions on Smart Grid*, To appear, 2017.

4. Security vs privacy vs performance tradeoff in distributed systems

V. Katewa and F. Pasqualetti and V. Gupta "On Privacy vs Cooperation in Multi-agent Systems," in *International Journal of Control*, 1-15, 2017.

5. Security limitations and tradeoffs in stochastic control systems

C-Z. Bai and F. Pasqualetti and V. Gupta "Data-injection attacks in stochastic control systems: Detectability and performance tradeoffs," in *Automatica*, 82:251-260, 2017.

C-Z. Bai and F. Pasqualetti and V. Gupta "On Kalman Filtering with Compromised Sensors: Attack Stealthiness and Performance Bounds," in *IEEE Transactions on Automatic Control*, 62(12):6641-6648, 2017.