Network Security Games

Saurabh Amin

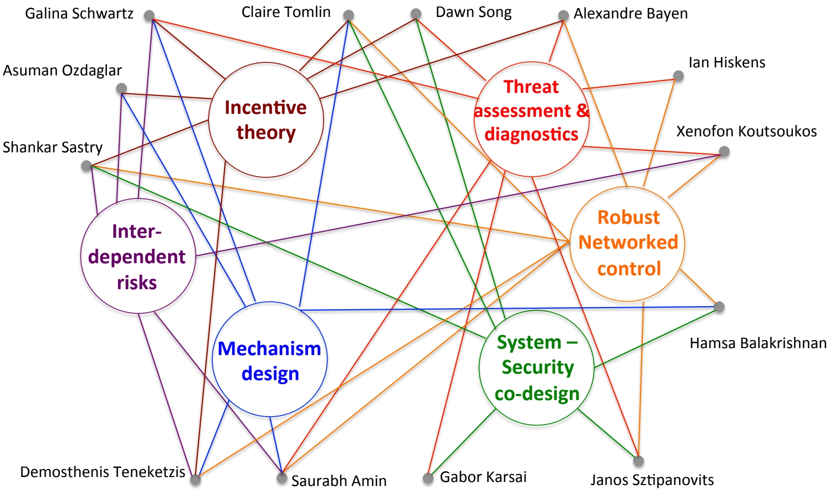
Massachusetts Institute of Technology

ACCESS-FORCES CPS workshop
KTH, October 26-27, 2015

FORCES
FOUNDATIONS OF RESILIENT
CYBER-PHYSICAL SYSTEMS

FORCES

National Science Foundation (NSF) sponsored CPS Frontiers project



<u>Collaborative Research</u>: MIT, UC Berkeley, UMich, Vanderbilt University

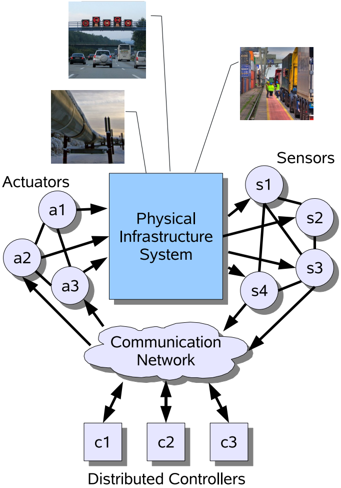
FORCES motivation: Resilient CPS

Attributes

1. Functional correctness by design
2. Robustness to reliability failures (faults)
3. Survivability against security failures (attacks)

Tools [Traditionally disjoint]

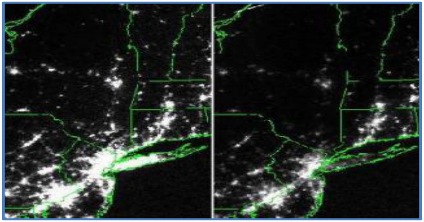
- Resilient Control (RC) over sensor-actuator networks
- Economic Incentives (EI) to influence strategic interaction of individuals within systemic societal institutions



Cyber-Physical Systems (CPS)

Reliability failures

Local disruptions to cascading failures (blackouts)



weather events ⇒ limited situational awareness ⇒ inadequate operator response ⇒ network failures

Security failures: cyber-attacks & Stuxnet

Maroochy Shire sewage plant *(2000)*

Los Angeles traffic control *(2008)*

Tehama Colusa canal system *(2007)*

Cal-ISO system computers *(2007)*

Failures in CPS

- Simultaneous faults [**reliability failures**]
  - Common-mode failures
  - Random failures due to nature
  - Operator errors
- Simultaneous attacks [**security failures**]
  - Targeted cyber-attacks
  - Non-targeted cyber-attacks
  - Coordinated physical attacks
- Cascading failures
  - Failure of nodes in one subnet $\Rightarrow$ progressive failures in other subnets

Observation #1:

Due to cyber-physical interactions, it is extremely difficult to distinguish reliability & security failures using *imperfect* diagnostic information.

Operations and control of CPS

- Multi-agent systems (e.g., infrastructure control systems with multiple entities)
- Agents have different information about CPS (both private and public uncertainties)
- Agents are strategic and have different objectives
- Need to coordinate or influence the agents' strategies so as to maximize the CPS' utility to its users

Observation #2:

Asymmetric information and strategic behavior are key features of CPS.

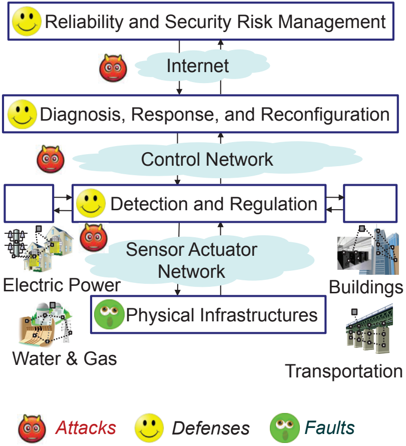
Separation of RC and EI is not suited for CPS resilience

RC tools

- Threat assessment & detection
- Fault-tolerant networked control
- Real-time / predictive response
- Fundamental limits of defenses

EI tools

- Incentive theory for resilience
- Mechanisms to align individually optimal allocations with socially optimum ones
- Interdependent risk assessment



FORCES research plan: hierarchical approach

Upper layer

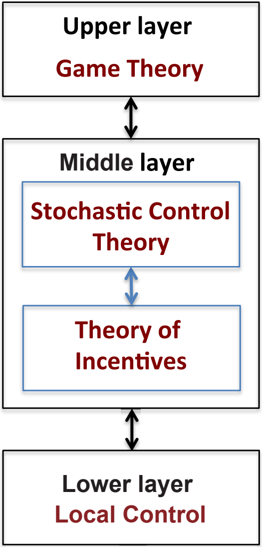
- How the collection of CPS's agents deal with external strategic adversary(-ies)
- Network games that model both security failures and reliability failures

Middle layer

- How strategic agents contribute to CPS efficiency and safety, while protecting their conflicting individual objectives
- Joint stochastic control and incentive-theoretic design, coupled with the outcome of the upper layer game

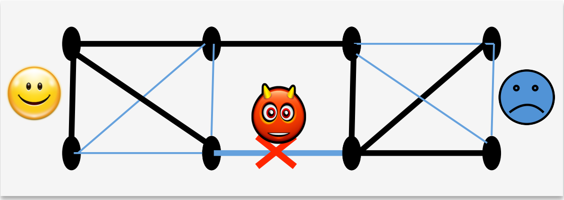
Lower layer

- Control at each individual agent's site.



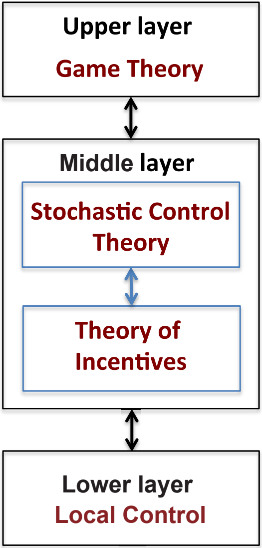
This talk: Upper hierarchical layer

Game with security failures



Game played on a graph representing the topological structure of CPS

- Attacker: Strategic adversary
- Defender: CPS network designer



Related work

Control of networks

- S. Low, N. Li, J. Lavaei: Distributed control and optimization
- F. Bullo, F. Dörfler: Distributed control, oscillations, microgrids
- P. Khargonekar, K. Poolla, P. Varaiya: Selling random wind
- K. Turitsyn, I. Hiskens: Distributed optimal VAR control

Resilience and security of networked systems

- H. Sandberg, K. Johansson: Secure control, networked control
- R. Baldick, K. Wood, D. Bienstock: Network Interdiction, Cascades
- T. Başar, C. Langbort: Network security games
- J. Baras: Network security games and trust

Outline: Network security games (upper layer)

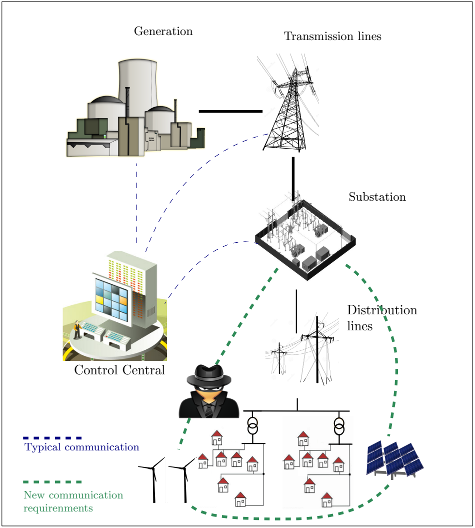
1. Distribution network control under node disruptions
2. Network flow routing under link disruptions

Devendra Shelar

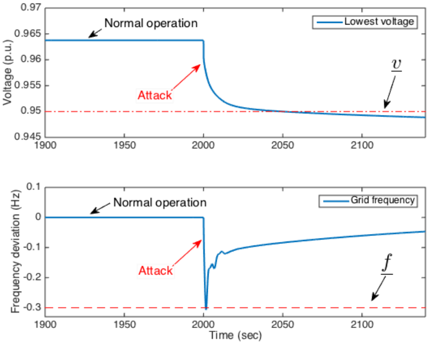
Mathieu Dahan

Model of DER disruptions

Vulnerability(-ies) published by EPRI



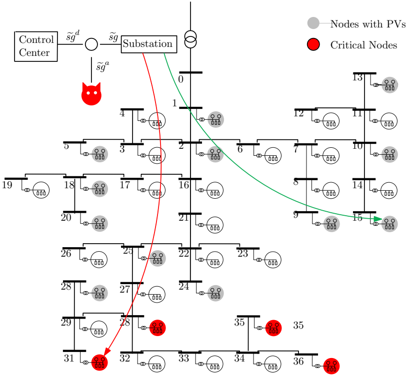
- Hack substation communications
- Introduce incorrect set-points and disrupt DERs
- Create supply-demand mismatch
- Cause voltage & freq. violations
- Induce cascading failures



Main questions

When malicious entities (or random failures) compromise DERs/PVs:

- How to perform security threat assessment of distribution networks under DER/PV disruptions?
- How to design decentralized defender (network operator) strategies?



Attacker-defender interaction

Stackelberg game model (bilevel optimization)

- Leader: Attacker compromises a subset of DERs/PVs;
- Follower: Defender response via network control.

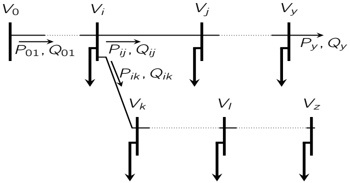
Problem statement:

- Determine worse-case attack plan (compromise DERs/PVs) to induce:
  - loss of voltage regulation
  - loss due to load shedding
  - loss of frequency regulation [esp., for large PV installations]
- Best defender response (reactive control):
  - Non-compromised DERs provide active and reactive power (VAR)
  - Load control: demand at consumption nodes may be partly satisfied

Network model

Tree networks

- $\mathcal{G} = (\mathcal{N}, \mathcal{E})$ - tree network of nodes and edges
- $\nu_i = |V_i|^2$ - square of voltage magnitude at node i
- $\ell_{ij} = |I_{ij}|^2$ - square of current magnitude from node i to j
- $z_{ij} = r_{ij} + \mathbf{j}x_{ij}$ - impedance on line (i,j)
- P_{ij}, Q_{ij} - real and reactive power from node i to node j
- $S_{ij} = P_{ij} + \mathbf{j}Q_{ij}$ - complex power flowing on line $(i,j) \in \mathcal{E}$



Power flow and operational constraints

- Generated power: $sg_i = pg_i + jqg_i$
- Consumed power: $sc_i = pc_i + jqc_i$
- Power flow

$$P_{ij} = \sum_{k:j\to k} P_{jk} + r_{ij}\ell_{ij} + pc_j - pg_j$$

$$Q_{ij} = \sum_{k:j\to k} Q_{jk} + x_{ij}\ell_{ij} + qc_j - qg_j$$

$$\nu_j = \nu_i - 2(r_{ij}P_{ij} + x_{ij}Q_{ij}) + (r_{ij}^2 + x_{ij}^2)\ell_{ij}$$

$$\ell_{ij} = \frac{P_{ij}^2 + Q_{ij}^2}{\nu_i}$$

- Voltage (and frequency limits)

$$\underline{\nu}_i \le \nu_i \le \bar{\nu}_i \quad \text{and} \quad \underline{f} \le f \le \bar{f}$$

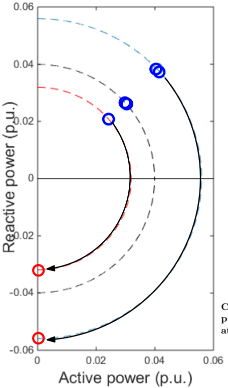
- Maximum injected power

$$-\sqrt{\overline{sg}_i^2 - (pg_i)^2} \le qg_i \le \sqrt{\overline{sg}_i^2 - (pg_i)^2}$$

Attacker model

Attacker strategy: $\psi = (\delta, \widetilde{pg}, \widetilde{qg})$

- δ is a vector, with elements $\delta_i = 1$ if DER i is compromised and zero otherwise;
- $\widetilde{pg}^a$: Active power set-points induced by the attacker;
- $\widetilde{qg}^a$: Reactive power set-points induced by the attacker.
- Satisfy resource constraint $\sum_{i=1}^{n} \delta_i \leq M$ (attacker's budget)



Change on set-points due to the attack

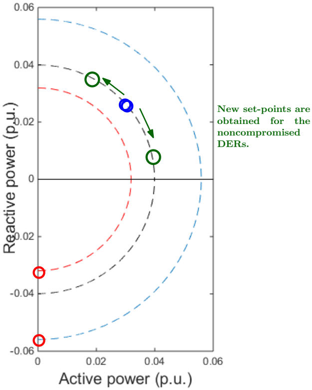
Power injected by each DER constrained by:

$$-\sqrt{\overline{sg}_i^2 - (\widetilde{pg}_i^a)^2} \leq \widetilde{qg}_i^a \leq \sqrt{\overline{sg}_i^2 - (\widetilde{pg}_i^a)^2}$$

Defender model

Defender response: $\phi = (\gamma, \widetilde{pg}^d, \widetilde{qg}^d)$

- $\gamma \in [0,1]$ the portion of controlled loads;
- $\widetilde{pg}^d$: New active power set-points set by defender;
- $\widetilde{qg}^d$: New reactive power set-points set by the defender.



Power injected by each DER constrained by:

$$-\sqrt{\overline{sg}_i^2 - (\widetilde{pg}_i^d)^2} \leq \widetilde{qg}_i^d \leq \sqrt{\overline{sg}_i^2 - (\widetilde{pg}_i^d)^2}$$

How to choose the defender response (set-points)?

Losses

- Loss of voltage regulation

$$L_{\text{LOVR}} \equiv \max_{i \in \mathcal{N}_0} w_i (\underline{\nu}_i - \nu_i)_+$$

- Cost incurred due to load control

$$L_{\text{LL}} \equiv \sum_{i \in \mathcal{N}_0} C_i (1 - \gamma_i)$$

Composite loss function

$$L(\psi, \phi) = L_{\text{LOVR}} + L_{\text{LL}}$$

Problem statement

Find attacker's interdiction plan to maximize composite loss $L(\psi,\phi)$, given that defender optimally responds

$$\max_{\psi} \quad \min_{\phi} \quad \left(\max_{i \in \mathcal{N}_0} w_i (\underline{\nu}_i - \nu_i)_+ + \sum_{i \in \mathcal{N}_0} C_i (1-\gamma_i) \right)$$
$$\text{s.t. Power flow, DER constraints, and resource contraints}$$

- Can add loss of frequency regulation $L_{LOFR} \equiv \tilde{w}(\underline{f}_{dev} - f_{dev})_+$

This bilevel-problem is hard!

- Outer problem: integer-valued attack variables
- Inner problem: nonlinear in control variables

Simple case

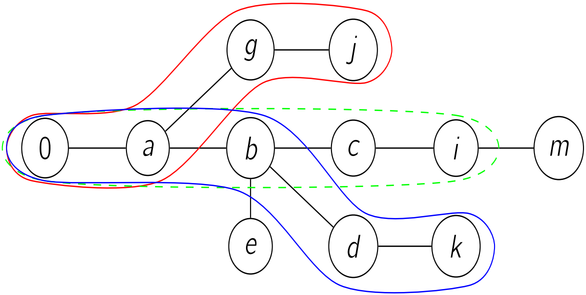
For a fixed defender choice and ignoring loss of freq. regulation:

$$\max_{\delta} \quad \left(\max_{i \in \mathcal{N}_0} w_i (\underline{\nu}_i - \nu_i)_+ \right)$$

s.t. Power flow, DER constraints, and resource contraints

Results for this simple case also extend to the case when R/X ratio is homogeneous and defender responds with only DER control.

Precedence description



In the above figure

- $j \prec_i k$: Node j is before node k with respect to node i
- $e =_i k$: Node e is at the same level as node k with respect to node i
- $b \prec k$: Node b is before node k because b is ancestor of k

Optimal interdiction plan

Theorem

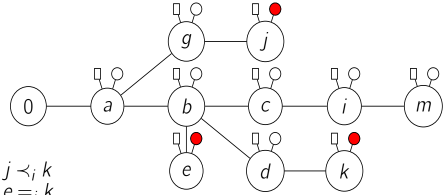
For a tree network, given nodes i (pivot), $j, k \in \mathcal{N}_0$:

- If DGs at j, k are homogenous and j is before k w.r.t. i, then DG disruption at k will have larger effect on ν_i at i (relative to disruption at node j);
- If DGs at j, k are homogenous and j is at the same level as k w.r.t. i, then DG disruptions at j and k will have the same effect on ν_i at i;

  Let ν_i^{old}/ν_i^{new} be $|V_i|^2$ before/after the attack

  $\Delta(\nu_i) = \nu_i^{old} - \nu_i^{new}$

$$\Delta_j(\nu_i) < \Delta_k(\nu_i)$$
$$\Delta_e(\nu_i) \approx \Delta_k(\nu_i)$$



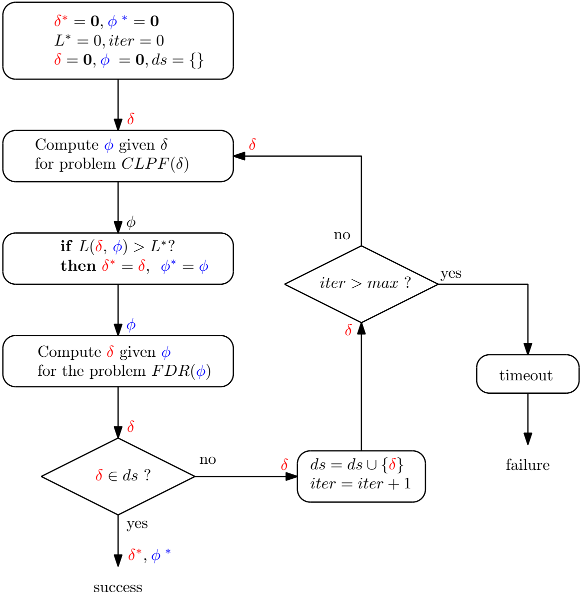
$j \prec_i k$
$e =_i k$
$b \prec k$

Computing optimal attack: fixed defender choices

procedure Optimal Attack Plan
  for $i \in \mathcal{N}_0$ **do**
    for $j \in \mathcal{N}_0$ **do**
      Compute $\Delta_j(\nu_i)$
    end for
    Sort js in decreasing order of $\Delta_j(\nu_i)$ values
    Compute J_i^* by picking js corresponding to top M $\Delta_j(\nu_i)$ values.
  end for
  $k := w_i \arg\min_{i \in \mathcal{N}_0} \nu_i - \Delta_{J_i^*}(\nu_i)$
  return $J^* := J_k^*$ (Pick J_i^* which violates voltage constraint the most)
end procedure

- $\mathcal{O}(n^2 log\ n)$

Greedy algorithm for optimal attack: defender response



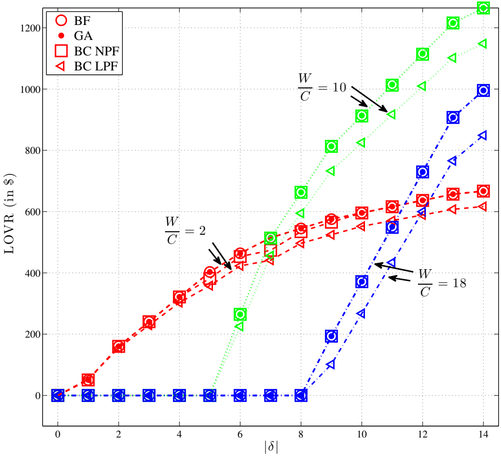
Main results

- Results using greedy algorithm compare very well with results from (more computationally intensive) brute force and Bender's cut;
- Optimal attack plans with defender response (using both DER control and load control) show downstream preference;

Effect of attack on loss of voltage regulation

Optimal defender response under DER/PV disruptions

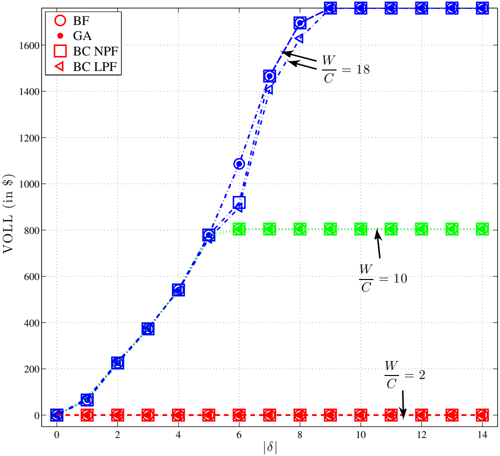
- Voltage regulation can be improved by selective load control
- If load control is costly, defender permits loss of voltage regulation



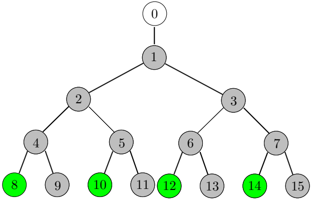
Effect of attack on cost of load control

Optimal defender response under DER/PV disruptions

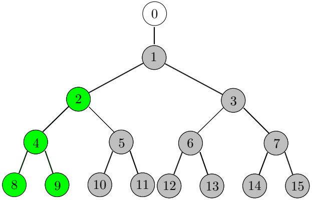
- For small intensity attack, load control limits losses
- For high intensity attack, load control not effective



Secure network designs: which DERs/PVs to secure?



Design 1



Design 2

Theorem

A homogeneous DN with optimally secure PVs has following properties:

- If any PV node is secure, secure all its child nodes
- At most one intermediate level with both vulnerable and secure nodes
- In this intermediate level, secure nodes uniformly at random

Resilient defender response

Desirable properties of defender response:

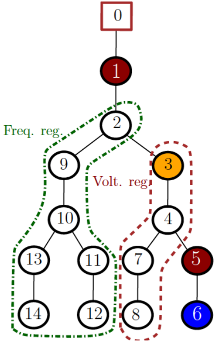
1. **Security**: Centralized control strategy undesirable if CC-SS communication is vulnerable
2. **Compensation to owners**: Upstream DERs/PVs likely to be owned by distribution utilities $\Rightarrow \uparrow$ costs when set-points change for larger DERs (esp. $\downarrow$ real power production)
3. **Flexibility**: Topology of DNs might be variable across time: configuration of worst affected nodes may change.

We propose a decentralized control strategy and find new set-points for non-compromised nodes using

- Information: local measurements (voltage & freq.) and location of the node with lowest voltage;
- Diversification: each node contributes either to voltage or to frequency regulation.

Decentralized defender response

Theorem: Node diversification

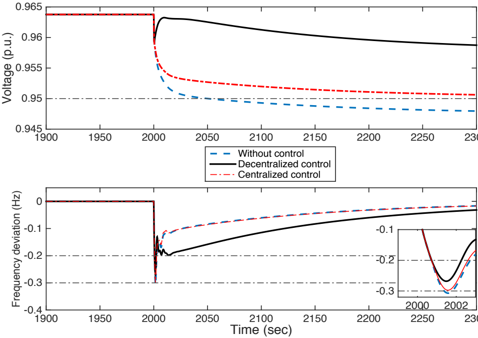


Attacker-Defender interaction

- Attacker: disrupt DERs at 1, 5, 6
- Critical node 3 partitions network:
  - Subnet 1: control frequency
  - Subnet 2: regulate voltage.
- Defender: New set-points

Approach

- Resource-constrained attacker: loss of voltage & freq. regulation
- Worst-case attacks (maximin)
- Compute defender response (Distributed control)



Summary: network control under node disruptions

Questions

- How to assess vulnerability of electricity networks to disruptions of Distributed Energy Resources (DERs)?
- How to design decentralized defender (network operator) strategies?

Approach

Attacker-defender model; Network interdiction formulation;
Characterization of worst-case attacks; Defender strategies

Results

- Interdiction model captures threats to DERs / smart inverters;
- Structural results on worst case attacks that maximize voltage deviations and / or frequency deviation from nominal operation;
- Efficient (greedy) technique for solving interdiction problems with nonlinear power flow constraints;
- Ongoing: Distributed defender control strategy (uses measurements and knowledge of worst affected node).

Outline: Network security games (upper layer)

1. Distribution network control under node disruptions
2. Network flow routing under link disruptions

Network flow optimization problems

Max-flow problem

$$(\mathcal{P}_1): \quad \begin{array}{ll} \text{maximize} & \mathrm{F}(x) \\ \text{subject to} & x \in \mathcal{F}, \end{array}$$

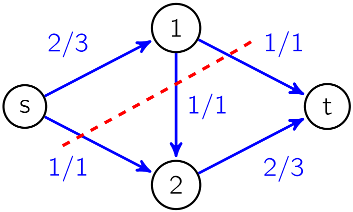
- $\mathrm{F}(x)$: Value of flow x

Max-flow w/ min-transportation cost

$$(\mathcal{P}_2): \quad \begin{array}{ll} \text{minimize} & \mathrm{C}_1(x) \\ \text{subject to} & x \in \mathcal{F} \\ & \mathrm{F}(x) \geq \mathrm{F}(x'), \quad \forall x' \in \mathcal{F} \end{array}$$

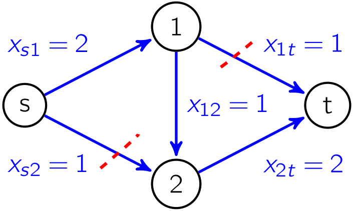
- $\mathrm{C}_1(x)$: Cost of transporting flow x

Max-flow min-cut theorem: the maximum value of an $s-t$ flow is equal to the minimum capacity over all $s-t$ cuts.

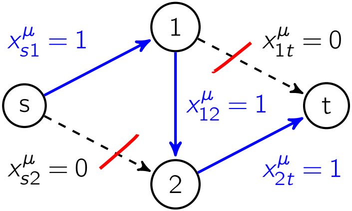


Example

- What if the network is under strategic link disruptions?



Initial flow and attack.



Resulting effective flow

Is it possible to extend classical network optimization results to strategic environments? If so, what are the structural properties?

Our focus

Network routing when the operator faces strategic link disruptions

Simultaneous non-zero sum game

- Both transportation and attack costs
- Attacker simultaneously disrupts multiple edges
- Defender strategically chooses a flow but no re-routing after attack.

Main contributions

- Structural insights on the set of Nash equilibria
- Relation to classical network routing problems
- Network vulnerability under strategic attacks

Game

$\Gamma := \langle \{1,2\}, (\mathcal{F}, \mathcal{A}), (u_1, u_2) \rangle$

- Directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, and for every $(i,j) \in \mathcal{E}$:
  - Edge capacity c_{ij}.
  - Edge transportation cost b_{ij}.
- Player 1 (Defender) chooses a feasible flow $x \in \mathcal{F}$.
- Player 2 (Attacker) chooses the edges to disrupt through an attack $\mu \in \mathcal{A}$.

$$\forall (i,j) \in \mathcal{E},\ \mu_{ij} = \begin{cases} 1 & \text{if } (i,j) \text{ is disrupted,} \\ 0 & \text{otherwise.} \end{cases}$$

- Given a flow x and an attack μ, x^{μ} is the **effective flow**.

Payoffs

$\Gamma := \langle \{1,2\}, (\mathcal{F}, \mathcal{A}), (u_1, u_2) \rangle$

- 1 single $s-t$ pair.

$$u_1(x,\mu) = p_1 \underbrace{\mathsf{F}(x^\mu)}_{\text{amount of effective flow}} - \underbrace{\mathsf{C}_1(x)}_{\text{transportation cost}}$$

$$u_2(x,\mu) = p_2 \underbrace{\mathsf{F}(x - x^\mu)}_{\text{amount of lost flow}} - \underbrace{\mathsf{C}_2(\mu)}_{\text{cost of attack}}$$

- Mixed-extension:

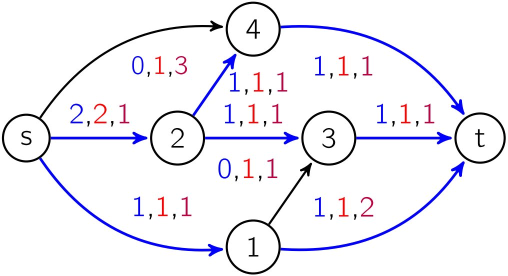
$$U_1(\sigma^1, \sigma^2) = \mathbb{E}[u_1(x,\mu)], \quad U_2(\sigma^1, \sigma^2) = \mathbb{E}[u_2(x,\mu)]$$

  where $(\sigma^1, \sigma^2) \in \Delta(\mathcal{F}) \times \Delta(\mathcal{A})$
- $\mathcal{S}_\Gamma$ is the set of Nash Equilibria.

Simplification

Assumption

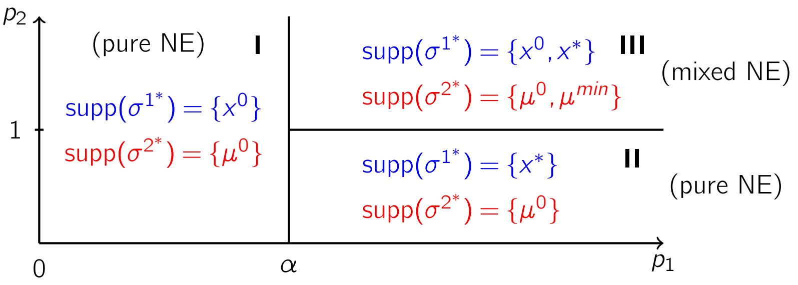
There exists a max-flow with min-transp. cost, x^*, that only takes $s-t$ paths that induce the lowest marginal transportation cost, denoted α.



- $\alpha = 3$

- Simplifying assumption without any loss of generality.
- α plays an important role in the results.

What properties does S_Γ satisfy?



Proposition (Regime **III**)

If $p_1 > \alpha$ and $p_2 > 1$, then Γ has no pure NE. Furthermore, $\exists \sigma_0 = (\sigma_0^1, \sigma_0^2) \in \mathcal{S}_\Gamma$ such that $U_1(\sigma_0^1, \sigma_0^2) = U_2(\sigma_0^1, \sigma_0^2) = 0$. σ_0 is defined by:

- $\sigma^1_{x^0} = 1 - \dfrac{1}{p_2}, \quad \sigma^1_{x^*} = \dfrac{1}{p_2},$
- $\sigma^2_{\mu^0} = \dfrac{\alpha}{p_1}, \quad \sigma^2_{\mu^{min}} = 1 - \dfrac{\alpha}{p_1}$

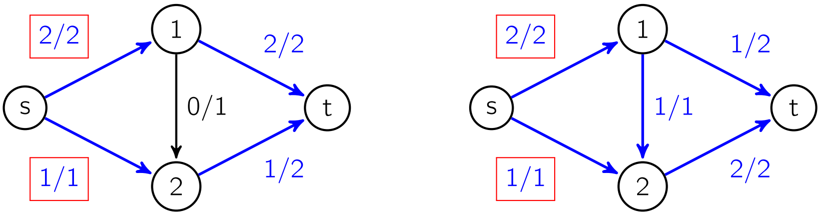
Necessary conditions

Attacker strategy σ^{2^*} and max-flow with min-transp. cost problem

For any NE $(\sigma^{1^*}, \sigma^{2^*})$, any μ in the support of σ^{2^*} disrupts edges that are saturated by every max-flow with minimum transportation cost.

$$\forall(\sigma^{1^*}, \sigma^{2^*}) \in \mathcal{S}_\Gamma, \forall \mu \in \text{supp}(\sigma^{2^*}), \forall (i,j) \in \mathcal{E}, \mu_{ij} = 1 \Longrightarrow \forall x^* \in \Omega_2,\ x^*_{ij} = c_{ij}$$

Example: every path induces the same transportation cost.



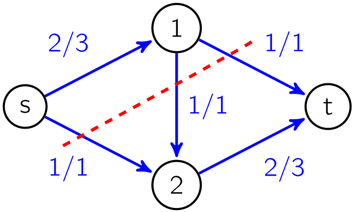
Necessary conditions

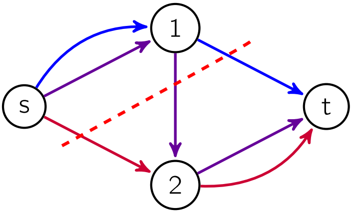
Defender strategy σ^{1^*} and min-cuts

For every NE $(\sigma^{1^*}, \sigma^{2^*})$, any edge of any min-cut must be taken by at least one flow x in the support of σ^{1^*}.

$$\forall (\sigma^{1^*}, \sigma^{2^*}) \in \mathcal{S}_\Gamma, \ \forall \text{ min-cut } E(\{S, T\}), \ \forall (i,j) \in E(\{S, T\}),$$
$$\exists x \in \mathrm{supp}(\sigma^{1^*}) \mid x_{ij} > 0$$

Example:





Main Results

$\Theta_1 = \mathrm{F}(x^*)$: Optimal value of the max-flow problem.
$\Theta_2 = \mathrm{C}_1(x^*)$: Optimal value of the max-flow min-cost problem.

Theorem: Regime **III**

If $p_1 > \alpha$, $p_2 > 1$, and under Assumption 1, then for any $\sigma^* \in \mathcal{S}_\Gamma$:

1. Both players' equilibrium payoffs are equal to 0, i.e.:

$$U_1(\sigma^{1^*}, \sigma^{2^*}) \equiv 0, \quad U_2(\sigma^{1^*}, \sigma^{2^*}) \equiv 0$$

2. The expected amount of flow sent in the network is given by:

$$\mathbb{E}_{\sigma^*}[\mathrm{F}(x)] \equiv \frac{1}{p_2}\Theta_1$$

and the expected transportation cost is given by:

$$\mathbb{E}_{\sigma^*}[\mathrm{C}_1(x)] \equiv \frac{1}{p_2}\Theta_2$$

Main Results

$\Theta_1 = \mathsf{F}(x^*)$: Optimal value of the max-flow problem.
$\Theta_2 = \mathsf{C}_1(x^*)$: Optimal value of the max-flow min-cost problem.

Theorem: Regime **III**

3. The expected cost of attack is given by:

$$\mathbb{E}_{\sigma^*}[\mathsf{C}_2(\mu)] \equiv \Theta_1 - \frac{1}{p_1}\Theta_2 = \left(1 - \frac{\alpha}{p_1}\right)\Theta_1$$

4. The expected amount of effective flow (that reaches t) is given by:

$$\mathbb{E}_{\sigma^*}[\mathsf{F}(x^\mu)] \equiv \frac{1}{p_1 p_2}\Theta_2$$

   $\mathbb{E}_{\sigma^*}[\mathsf{F}(x^\mu)]$ decreases with both p_1 and p_2!

5. The yield is given by:

$$\frac{\mathbb{E}_{\sigma^*}[\mathsf{F}(x^\mu)]}{\mathbb{E}_{\sigma^*}[\mathsf{F}(x)]} \equiv \frac{\Theta_2}{p_1 \Theta_1}$$

Summary: network routing under link disruptions

Results

- Modeled a simultaneous non-zero sum network game
- Obtained structural insights on the NE
- Related the NE to max-flow min-cost and min-cut
- Determined the vulnerability of a graph under strategic attack

Ongoing

- Nash equilibria (NE) of the one-stage game within the class of mixed strategies under link disruptions caused due to either reliability or security failures
- Equilibria for the finitely or infinitely repeated game