Security Games on Flow Networks

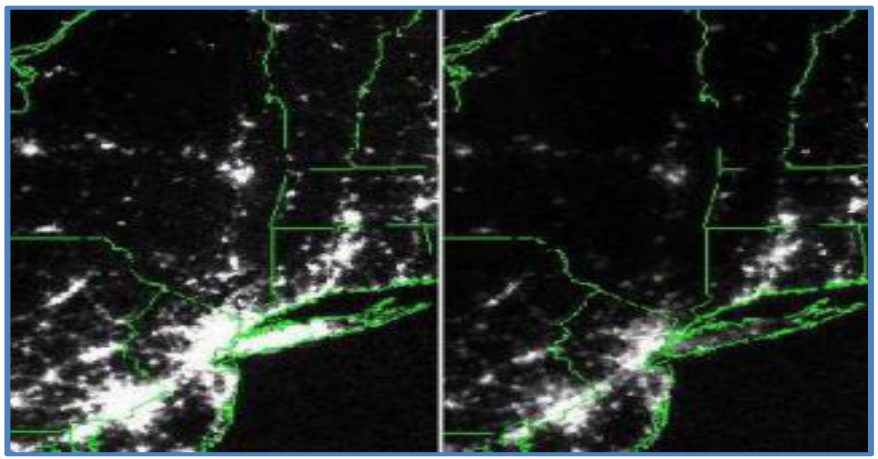
Structural Results and Practical Implications

Saurabh Amin
(Joint work with Devendra Shelar and Mathieu Dahan)

Support: NSF FORCES, NSF CAREER, ARFL SURE Lablet

Science of Security of CPS, CPSWeek 2016
Vienna, April 11th, 2016

Reliability failures



Weather/random events

⇒Limited situational awareness

⇒Network failures

⇒ Local or common mode failures

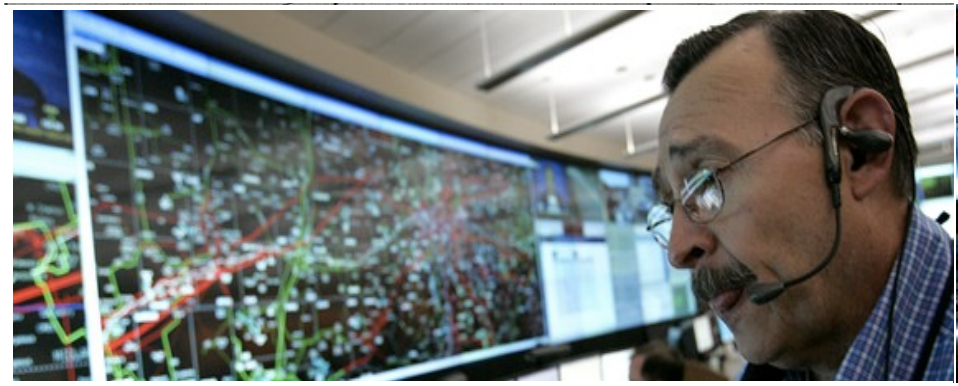
⇒ Inadequate operator response

⇒ Cascades (blackout)

Security failures: cyber-attacks (post-Stuxnet)

Sniper attack: PG&E's Metcalf substation (2013)

Dragonfly: DERs give backdoor entry (2013)



Cyberspies: hacking into US electric grid (2009)

HAVEX: Hacks control system software (2012)

Hack substation/ DERs/ meters

$\Rightarrow$Disrupt DERs/ protection equip.

$\Rightarrow$Cause voltage & freq. violations

$\Rightarrow$ Introduce incorrect set-points

$\Rightarrow$ Create supply-demand mismatch

$\Rightarrow$ Cascades (blackout)

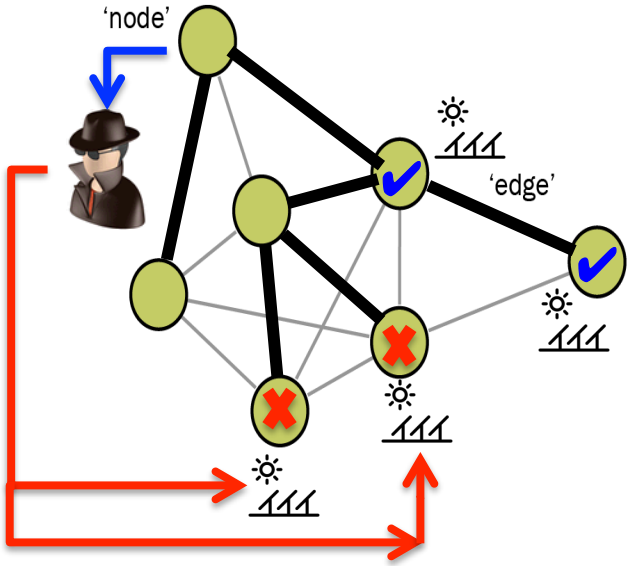
Resilient Infrastructure Networks: Key issues

1. *IT security tools: necessary but not sufficient*
   - Operator(s) need capabilities to deal with external strategic adversaries who can compromise control data
2. *Reliability failures (faults) ≠ Security failures (attacks)*
   - Due to cyber-physical interactions, it is extremely difficult to distinguish reliability & security failures using available information.
3. Agents (operators and users) have different information about the network, both private and public uncertainties
4. Need mechanisms to coordinate or influence the agents' strategies so as to maximize the network's utility to its users

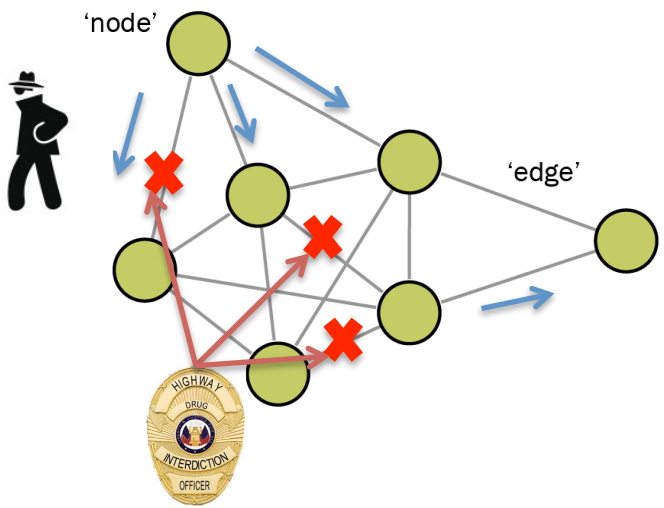
This talk: Game on a graph representing the structure of the network:

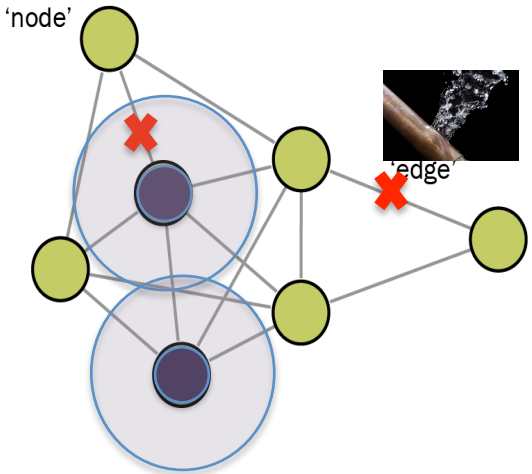
- Attacker: Strategic resource-constrained adversary
- Defender: CPS network designer facing physical constraints

Security games: our focus



Classical result: Optimal power flow problem
Our focus: Malicious DER node disruptions in electricity DNs (Shelar and SA. '15)





Classical result: Minimum set cover problem
Our focus: Optimal sensing for strategic link disruptions in water networks
(Sela, Dahan, Liu, SA. '15)

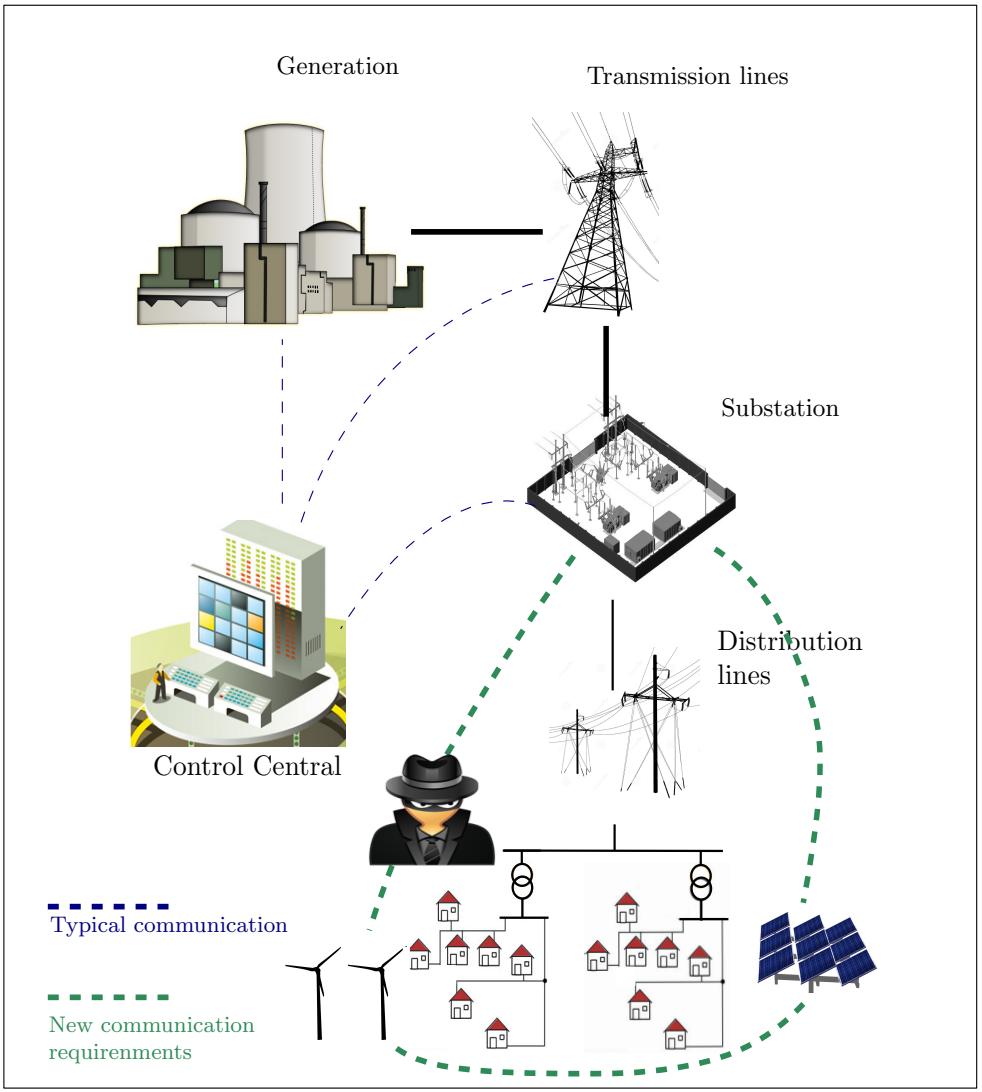
Classical result: Max-flow min transportation cost problem; max-flow min-cut theorem
Our focus: Network flow routing under strategic link disruptions (Dahan, SA. '15)

Outline

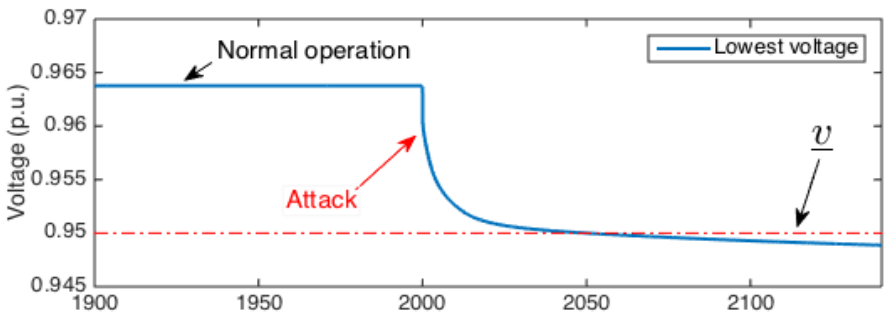
1. Network control under node disruptions
2. Network routing under link disruptions

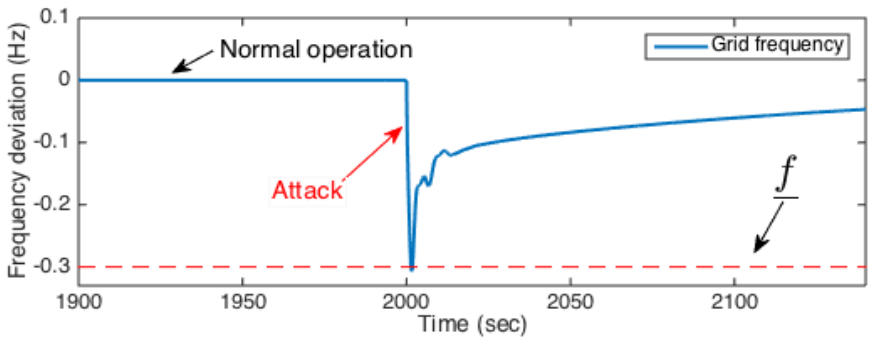
Model of DER disruptions

NESCO Vulnerabilities (EPRI):



Authorized Employee Issues Invalid Mass Remote Disconnect
Invalid Access Used to Install Malware Enabling Remote Internet Control
Meter Authentication Credentials are Compromised and Posted on Internet
Weak Encryption Exposes AMI Device Communication
Known but Unpatched Vulnerability Exposes AMI Infrastructure
Inadequate Access Control of DER Systems Causes Electrocution
DER SCADA System Issues Invalid Commands
Denial of Service Attack Impairs NTP Service

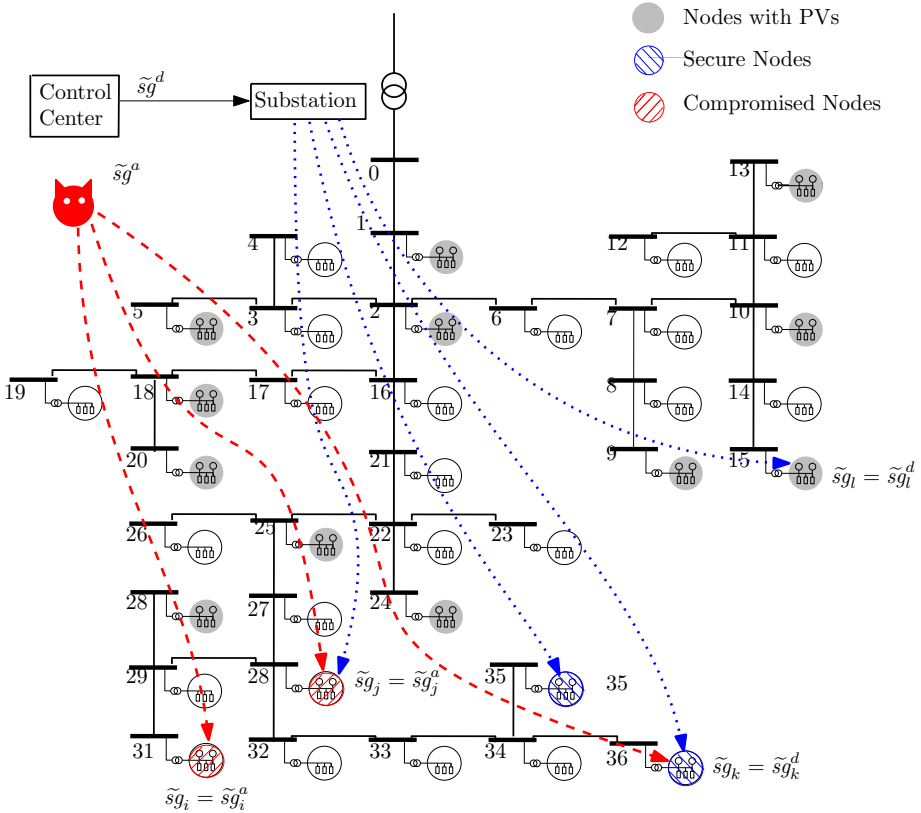




Main questions

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 resource-constrained attack plan (compromise DERs/PVs) to maximize:
  - loss of voltage regulation
  - loss due to load shedding
  - line losses [classical objective in OPF problems]
  - *loss of frequency regulation* [esp., for large DER installations]
- Compute best defender response (reactive control):
  - Non-compromised DERs provide active and reactive power (VAR)
  - Load control: demand at consumption nodes may be partly satisfied

Related work

Control of electricity networks

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

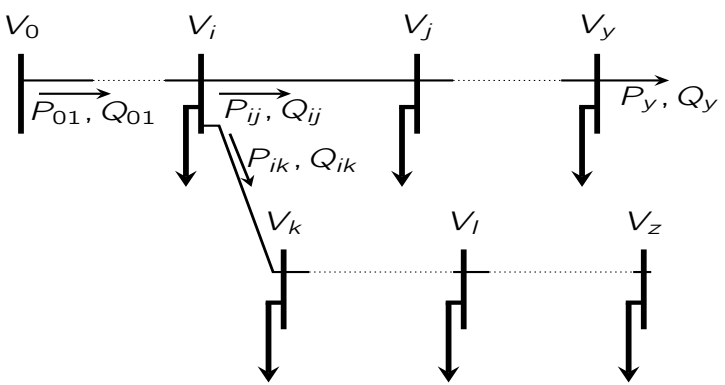
Resilience and security of networked control systems

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

Network model

Power flow on 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 limits (hard safety constraints)

$$\underline{\mu} \leqslant \nu_i \leqslant \overline{\mu}$$

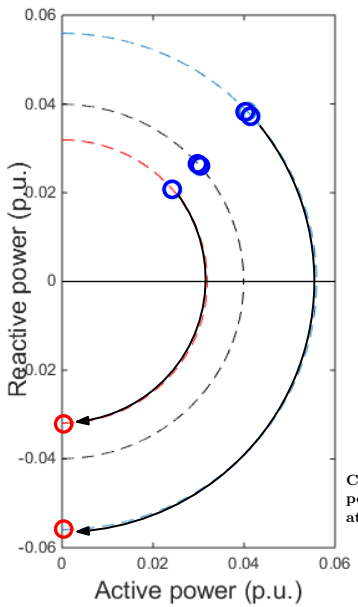
- Maximum injected power

$$-\sqrt{\overline{\mathrm{sp}}_i^2 - (pg_i)^2} \leqslant qg_i \leqslant \sqrt{\overline{\mathrm{sp}}_i^2 - (pg_i)^2}$$

Attacker model

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

- δ: attack vector, with $\delta_i = 1$ if DER i is compromised and zero otherwise
- Satisfy resource constraint $\sum_{i=1}^{n} \delta_i \leqslant M$ (attacker's budget)
- For compromised DERs, attacker chooses incorrect set-points:
  - $\widetilde{pg}^a$: False active power set-points
  - $\widetilde{qg}^a$: False reactive power set-points



Change on set-points due to the attack

Power injected by each DER constrained by:

$$-\sqrt{\overline{\mathrm{sp}}_i^2 - (\widetilde{pg}_i^a)^2} \leqslant \widetilde{qg}_i^a \leqslant \sqrt{\overline{\mathrm{sp}}_i^2 - (\widetilde{pg}_i^a)^2}$$

Attacker strategy

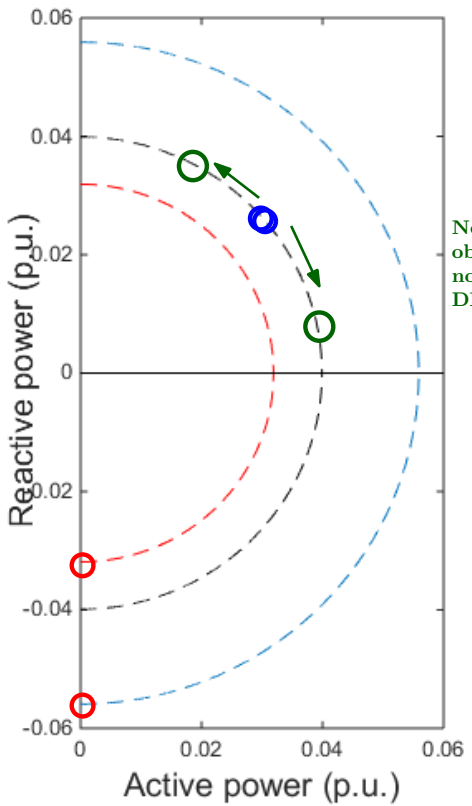
Which DERs to compromise?

What are the optimal attacker set-points?

Defender model

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

- $\gamma \in [0, 1]$: proportion of controlled loads
- For non-compromised DERs, defender chooses new set-points:
  - $\widetilde{pg}^d$: New active power set-points
  - $\widetilde{qg}^d$: New reactive power set-points



New set-points are obtained for the noncompromised DERs.

Power injected by each DER constrained by:

$$-\sqrt{\overline{\mathrm{sp}}_i^2 - (\widetilde{pg}_i^d)^2} \leqslant \widetilde{qg}_i^d \leqslant \sqrt{\overline{\mathrm{sp}}_i^2 - (\widetilde{pg}_i^d)^2}$$

Defender response

How to configure the non-compromised DERs?

How much load control should be exercised?

Losses

- Loss of voltage regulation

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

  - $\underline{\nu}_i > \underline{\mu}$: lower bound on voltage quality
- 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

$$\mathcal{L} := \max_{\psi} \quad \min_{\phi} \quad \left(\max_{i \in \mathcal{N}_0} w_i (\underline{\nu}_i - \nu_i)_+ + \sum_{i \in \mathcal{N}_0} C_i (1 - \gamma_i) \right)$$

$$\text{s.t. Nonlinear power flow, DER constraints,}$$

$$\text{and attacker's resource constraints}$$

This bilevel-problem is hard!

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

Assumptions and Optimal attacker set-points

Assumptions

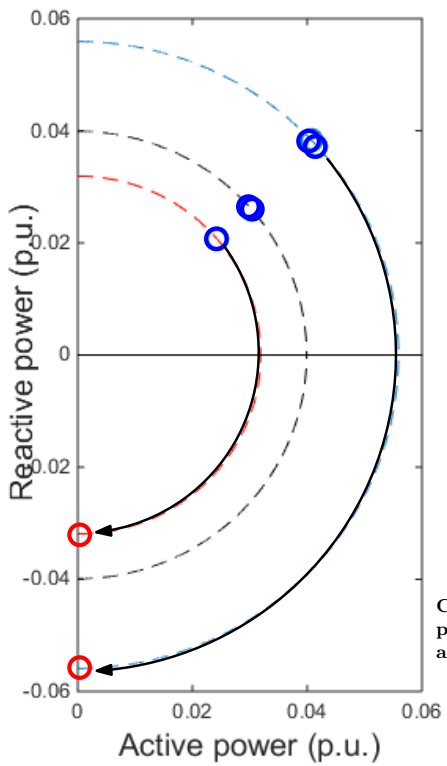
- **No reverse power flows:** power flows from substation to downstream nodes
- **Small line losses:** in comparison to the power flows
- **Small impedances:** sufficiently small resistances & reactances

What are optimal attacker set-points?

Theorem

For a defender action ϕ, and given attacker choice of DERs δ, the optimal attacker set-point is given by:

$$\widetilde{pg}_i^a = 0, \quad \widetilde{qg}_i^a = -\overline{\mathrm{sp}}_i$$



Change on set-points due to the attack

Two simpler problems!

Attacker-Defender problem under linear models:

$$\widehat{\mathcal{L}} \text{ (LPF model)} \qquad \breve{\mathcal{L}} \text{ (}\epsilon\text{-LPF model)} \quad := \begin{cases} \max\limits_{\delta} \ \min\limits_{\phi} \ L(\delta, \phi) \\ \text{s.t. DER constraints, resource contraints} \\ \text{and Linear power flow (LPF) or } (\epsilon\text{-LPF}) \end{cases}$$

LPF state: $\widehat{\mathrm{x}} = [\widehat{\nu}, \widehat{\ell}, sc, sg, \widehat{S}] \in \widehat{\mathcal{X}}$

$$\widehat{S}_j = \sum_{k:(j,k)\in\mathcal{E}} \widehat{S}_k + s_j + \cancel{z_j \ell_j}$$
$$\widehat{\nu}_j = \widehat{\nu}_i - 2\mathbf{Re}(\bar{z}_j \widehat{S}_j) + \cancel{|z_j|^2 \ell_j}$$

ϵ-LPF state: $\breve{\mathrm{x}} = [\breve{\nu}, \breve{\ell}, sc, sg, \breve{S}] \in \breve{\mathcal{X}}$

$$\breve{S}_j = \sum_{k:(j,k)\in\mathcal{E}} \breve{S}_k + (1+\epsilon) s_j$$
$$\breve{\nu}_j = \breve{\nu}_i - 2\mathbf{Re}(\bar{z}_j \breve{S}_j)$$

- $s_j = sc_j - sg_j$ (net power consumed at node j)
- ϵ: chosen based on size of tree network and the max. ratio of line losses to power flows

Main result

Theorem

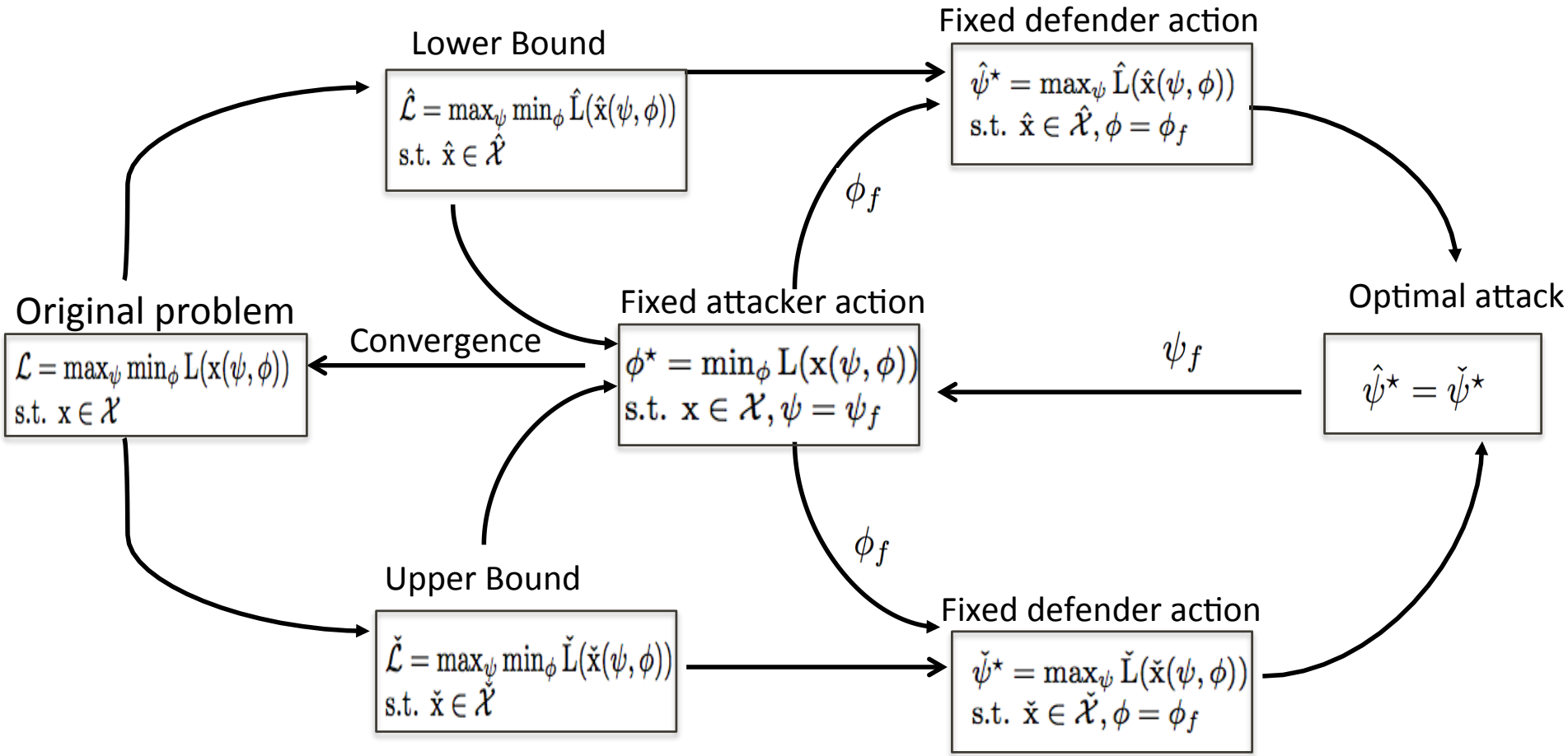
Let (ψ^*, ϕ^*), $(\widehat{\psi}^*, \widehat{\phi}^*)$ *and* $(\breve{\psi}^*, \breve{\phi}^*)$ *be optimal solutions to attacker-defender game under NPF, LPF, and* ϵ*-LPF respectively; and denote the optimal losses by* $\mathcal{L}$, $\widehat{\mathcal{L}}$, *and* $\breve{\mathcal{L}}$, *respectively. Then,*

$$\widehat{\mathcal{L}} \leqslant \mathcal{L} \leqslant \breve{\mathcal{L}} + \frac{\underline{\mu} N}{2\underline{\mu} + 4}.$$

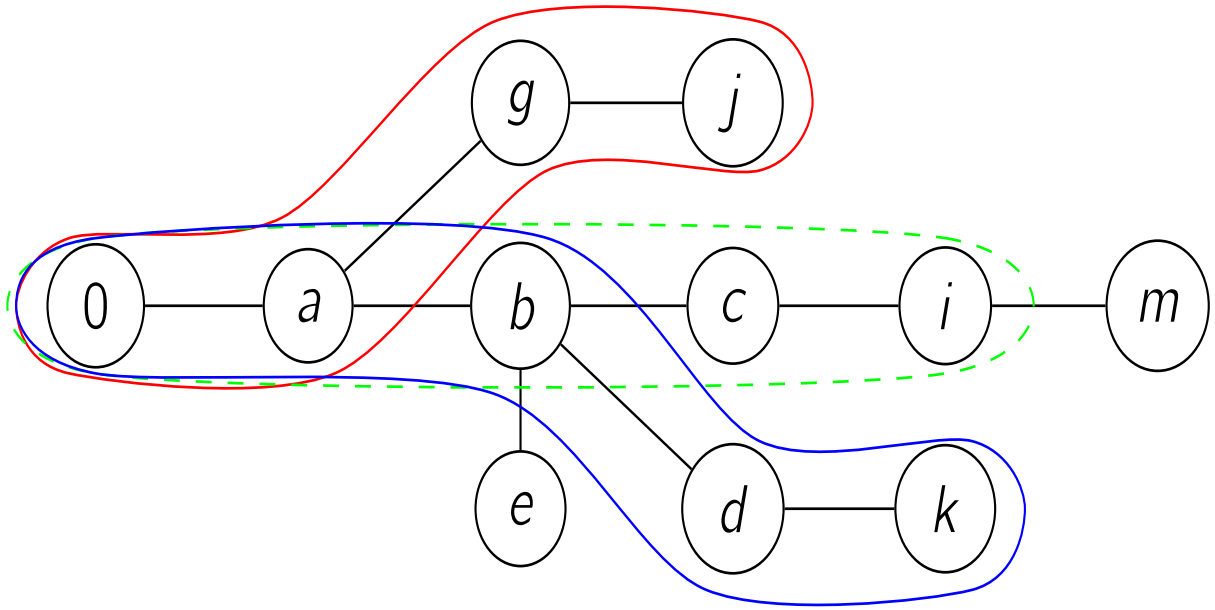
Computational results

- All results for the LPF model also hold for the ϵ-LPF model. The optimal attacker strategy is identical for both LPF and ϵ-LPF.

Summary of our approach



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: fixed defender choices

Theorem

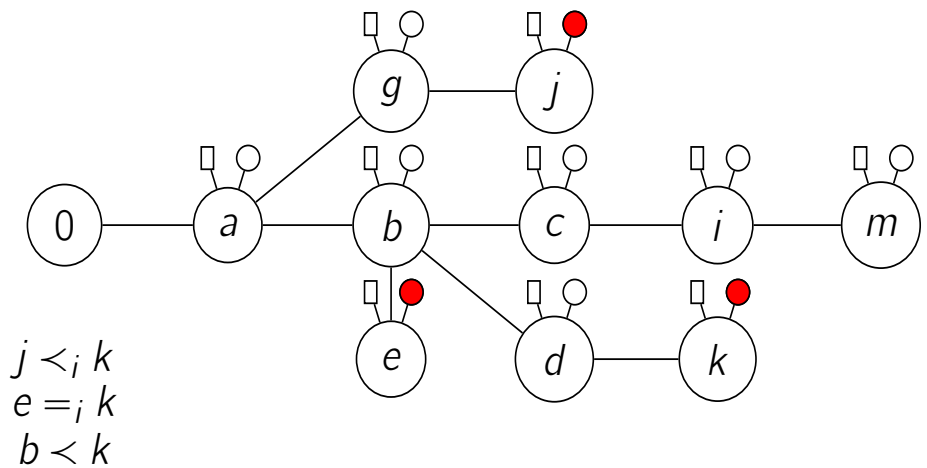
For a tree network, given nodes i (pivot), $j, k \in \mathcal{N}_0$:

- 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

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

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

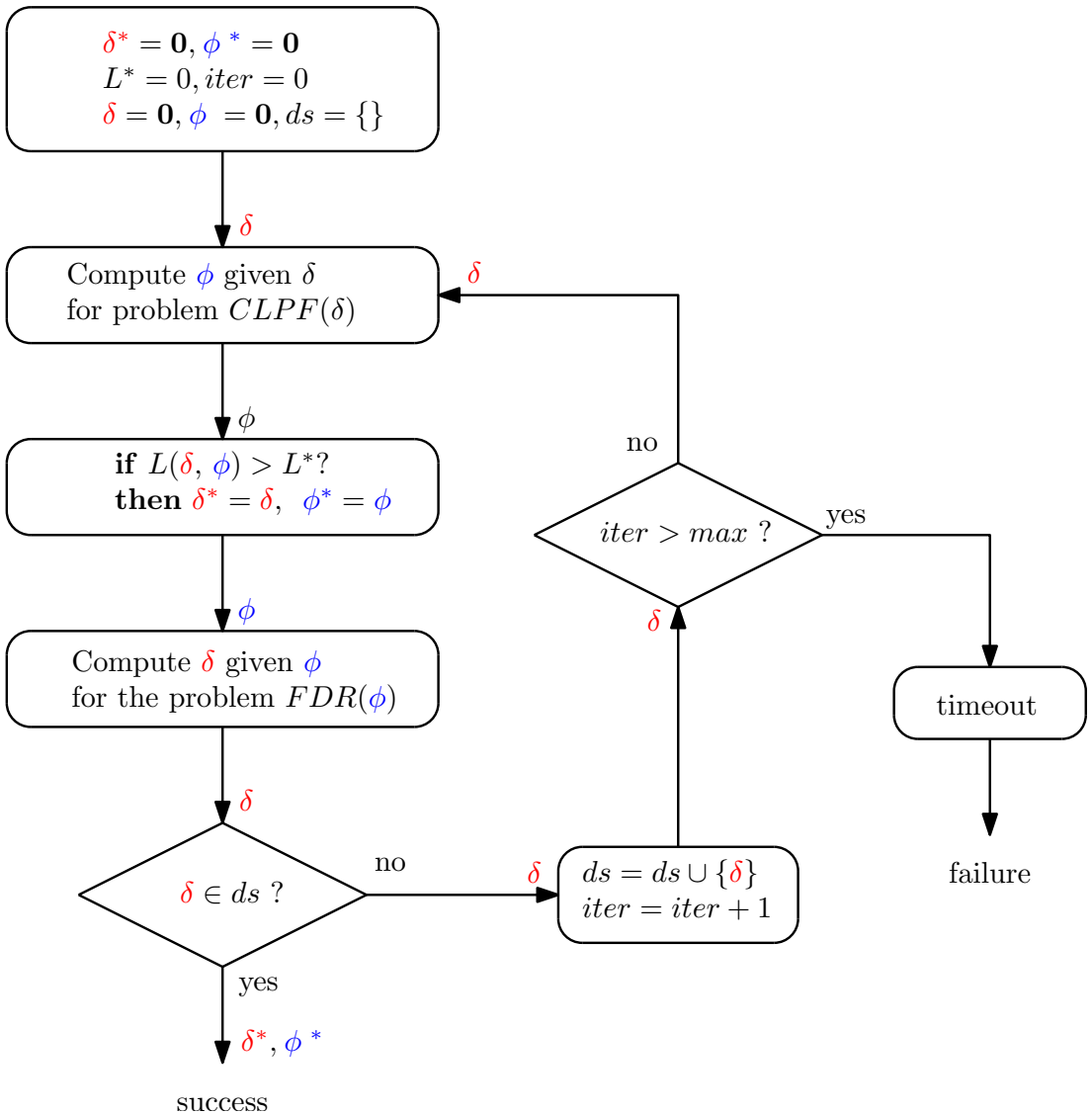


Computing optimal attack: fixed defender choices

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
  $k := \arg\min_{i \in \mathcal{N}_0} \; w_i \left(\nu_i - \Delta_{J_i^*}(\nu_i) \right)$
  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

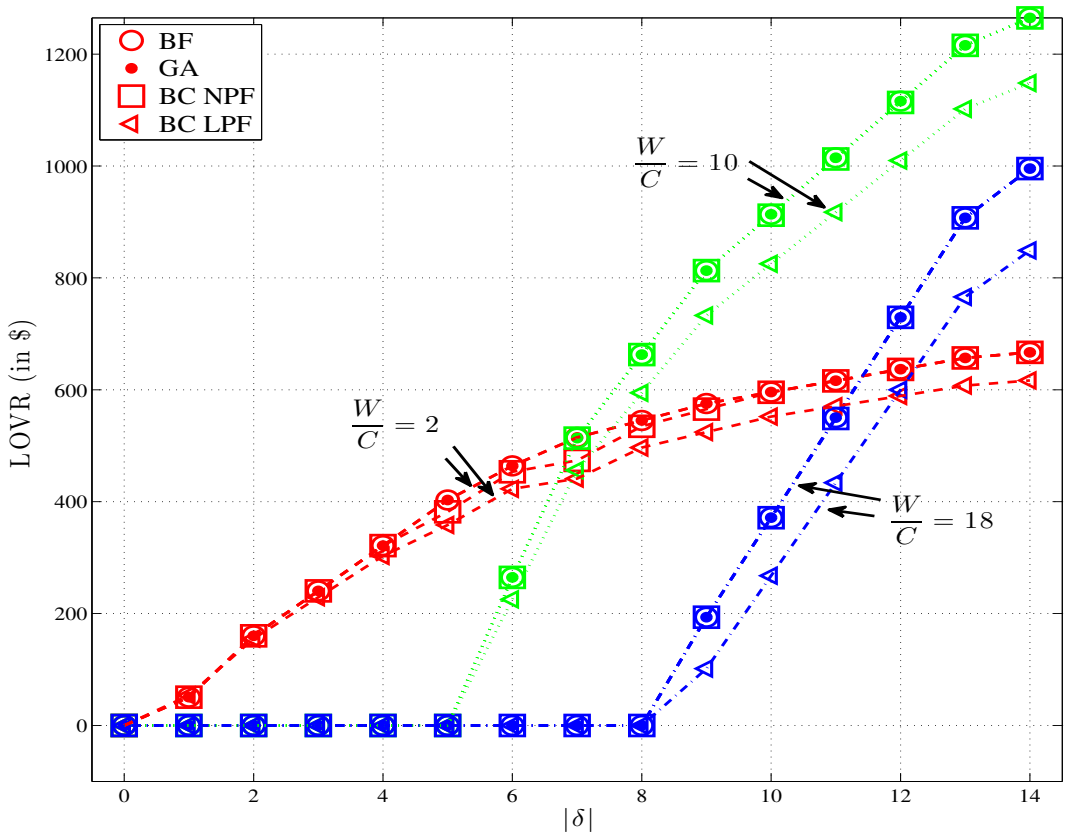


- Results compare very well with results from (more computationally intensive) Bender's cut
- Optimal attack plans with defender response show downstream preference

Effect of attack on loss of voltage regulation

Optimal defender response under DER/PV disruptions

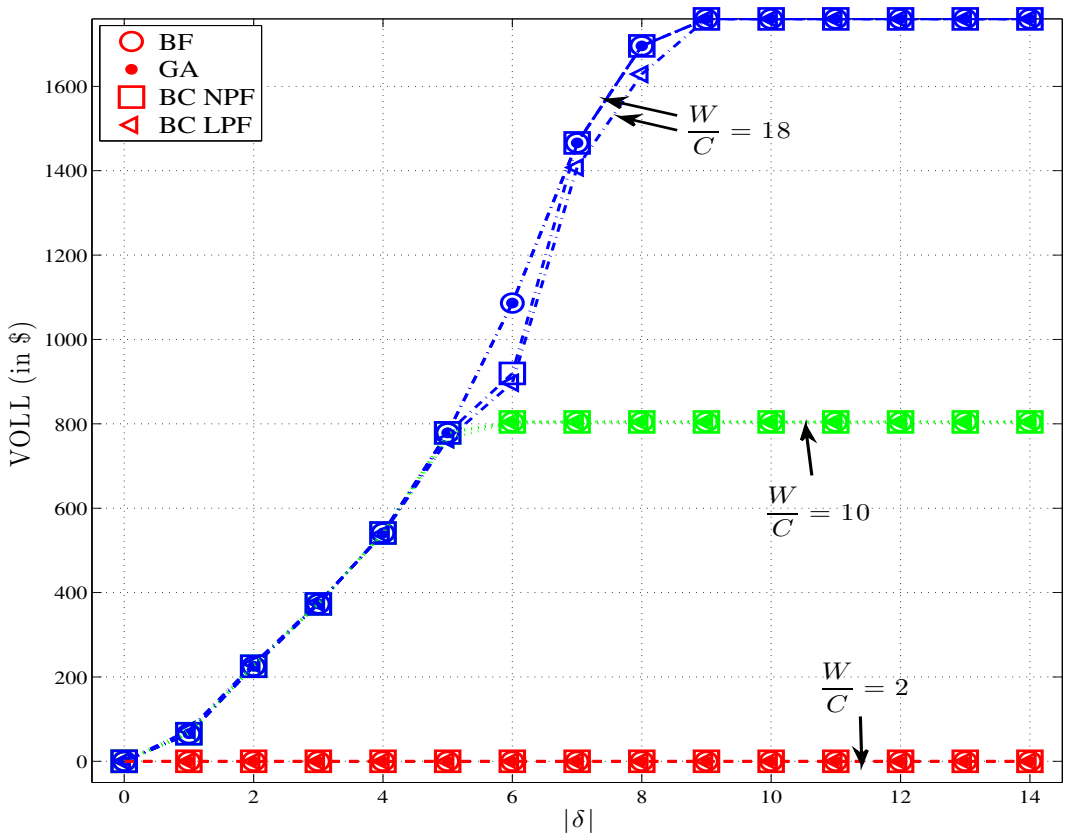
- Marginal impact of each DER/PV compromise decreases as attack intensity increases (i.e., more downstream nodes are compromised)
- Voltage regulation can be improved by selective load control
- If load control is costly, defender permits loss of voltage regulation



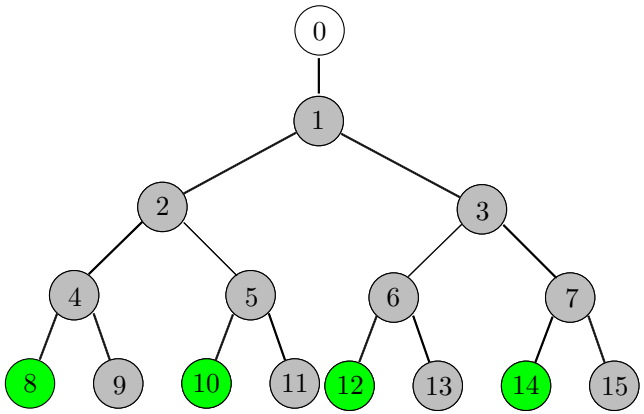
Effect of attack on cost of load control

Optimal defender response under DER/PV disruptions

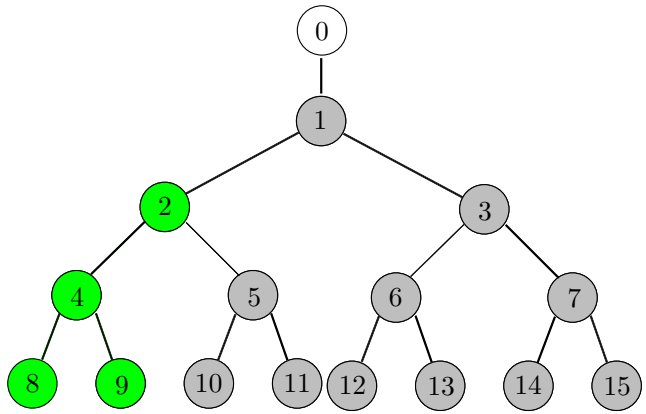
- Defender exerts load control until the load control capability of "beneficial" downstream loads is exhausted
- For small intensity attack, load control limits losses
- For high intensity attack, load control not effective



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:

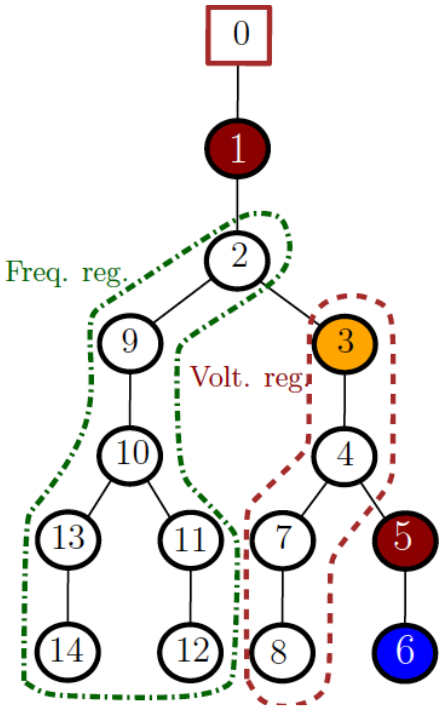
1. **Security**: Centralized control strategy undesirable if CC-SS communication is vulnerable
2. **Compensation to owners**: Upstream DERs/PVs likely to be owned by distribution utilities $\Rightarrow \uparrow$ costs when set-points change for larger DERs (esp. $\downarrow$ real power production)
3.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

We propose a distributed 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

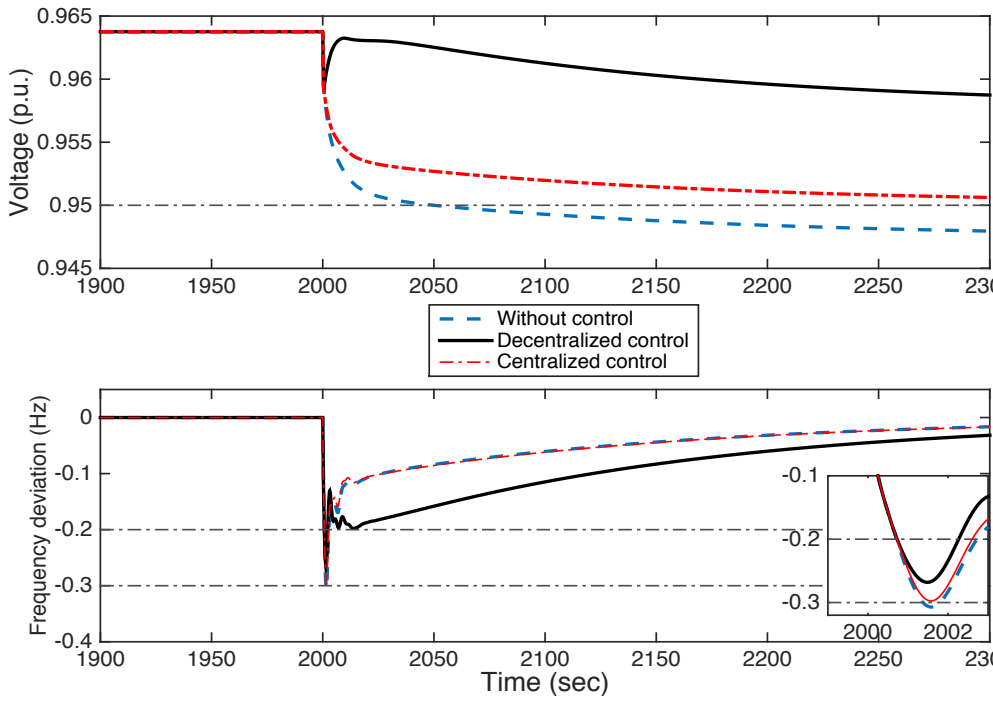


Attacker-Defender interaction

- 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

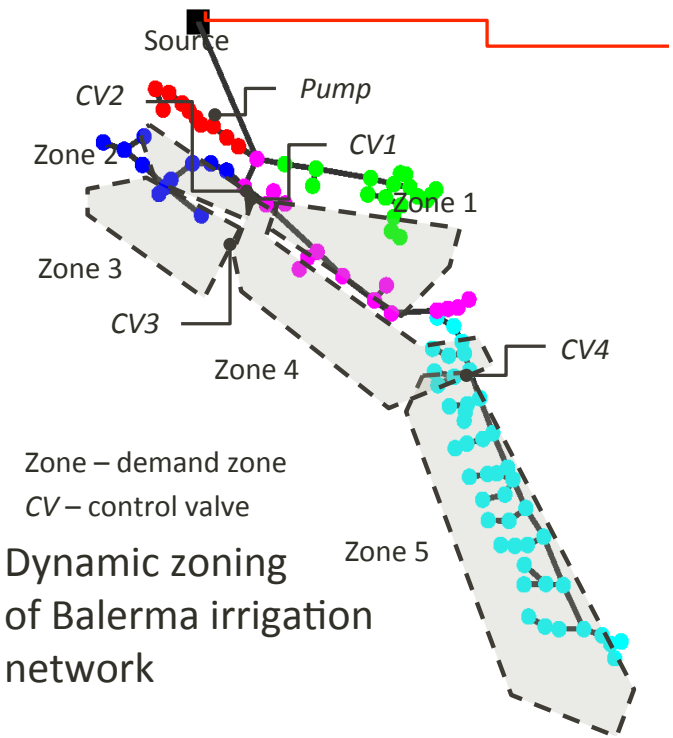
Results

- 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).

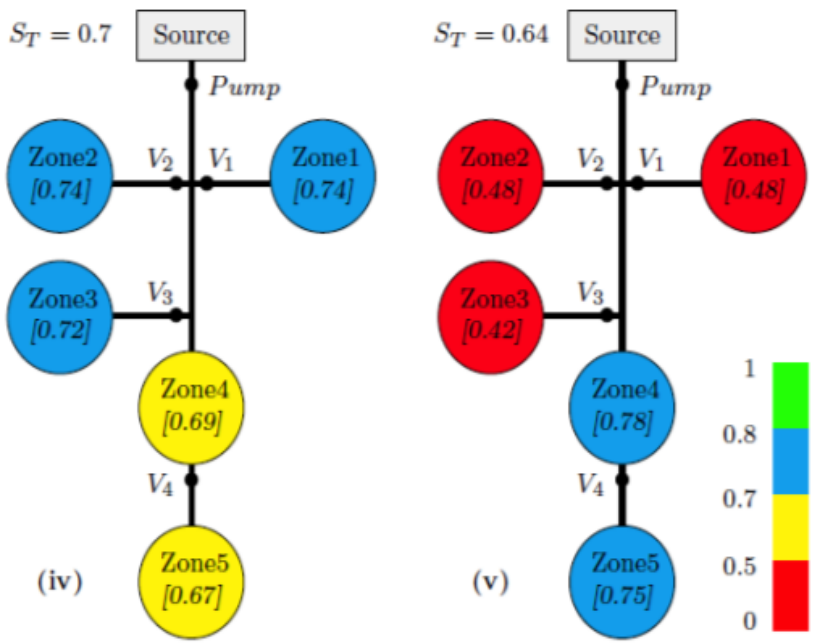
Extension: water network control under node disruptions

Objective: Minimize supply-demand mismatches in water networks created during contingencies subject to

- Nonlinear network flow
- Pump and valve constraints
- Available supply resource & demand specifications



Dynamic zoning of Balerma irrigation network



Controlling supply and shaping demand

Outline

1. Network control under node disruptions
2. Network routing under link disruptions

Network routing in the face of disruptions

Network flow routing

- Max-flow problem [Fulkerson '56]
- Max-flow min-cut theorem [Fulkerson '56]
- Min-cost max-flow problem [Edmonds and Karp '72]

(Q): Network routing when the operator faces strategic link disruptions?

- Network interdiction problems [Washburn '95, Bertsimas '13]
- Network security games [Wooders '10, Gueye '10, Goyal '14]
- We formulate a simultaneous network security game
  - Both transportation and attack costs
  - Attacker simultaneously disrupts multiple edges
  - Defender strategically chooses a flow but no re-routing after attack.

Recall: (Min-cost) max-flow problem

Max-flow problem

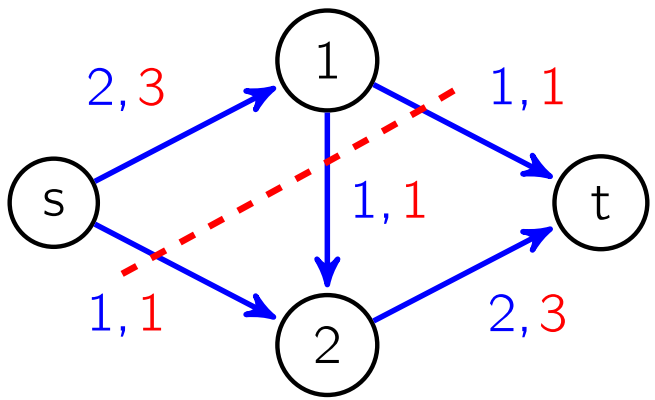
$$(\mathcal{P}_1): \quad \begin{array}{ll} \text{maximize} & \mathrm{F}(x) \\ \text{subject to} & x \in \mathcal{F}, \end{array}$$

Min-cost max-flow problem

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

- $\mathrm{F}(x)$: Value of flow x
- $\mathrm{C}_1(x)$: 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.



Game

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

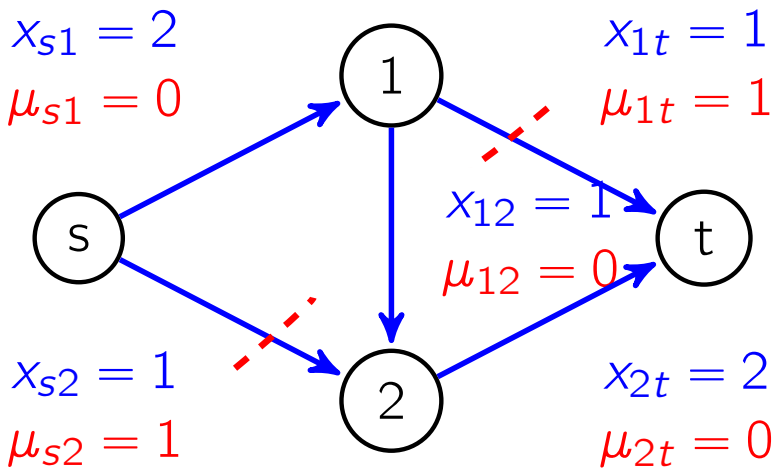
- Directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, and for every $(i,j) \in \mathcal{E}$:
  - Edge capacity c_{ij}.
  - Edge transportation cost b_{ij}.
- Player 1 (Defender) chooses a feasible flow $x \in \mathcal{F}$.
- Player 2 (Attacker) chooses the edges to disrupt through an attack $\mu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

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

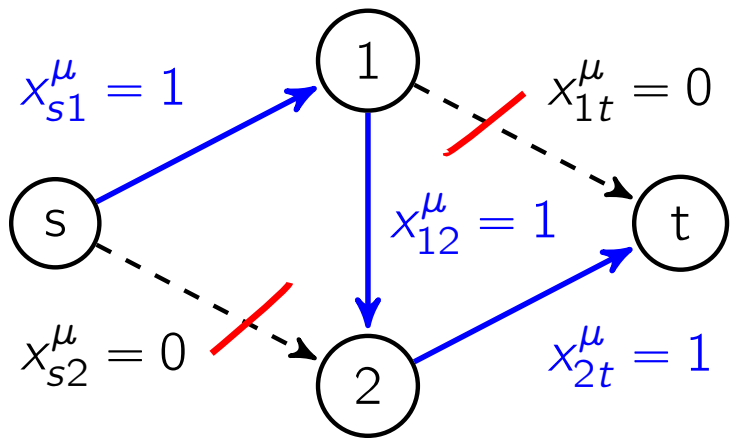
- 1 single $s-t$ pair.

Effective flow

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



Initial flow and attack.



Resulting effective flow

Payoffs

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

- $u_1(x,\mu) = p_1 \mathsf{F}(x^\mu) - \mathsf{C}_1(x)$
- $u_2(x,\mu) = p_2 \mathsf{F}(x - x^\mu) - \mathsf{C}_2(\mu)$

where:

- $\mathsf{F}(x^\mu) = \sum_{\{i \,|\, (i,t) \in \mathcal{E}\}} x^\mu_{it}$: **amount of effective flow**.
- $\mathsf{C}_1(x) = \sum_{(i,j)\in\mathcal{E}} b_{ij} x_{ij}$: **transportation cost**.
- $\mathsf{C}_2(\mu) = \sum_{(i,j)\in\mathcal{E}} c_{ij} \mu_{ij}$: **attacking cost**.
- $\mathsf{F}(x - x^\mu) = \mathsf{F}(x) - \mathsf{F}(x^\mu)$: **amount of lost flow**.

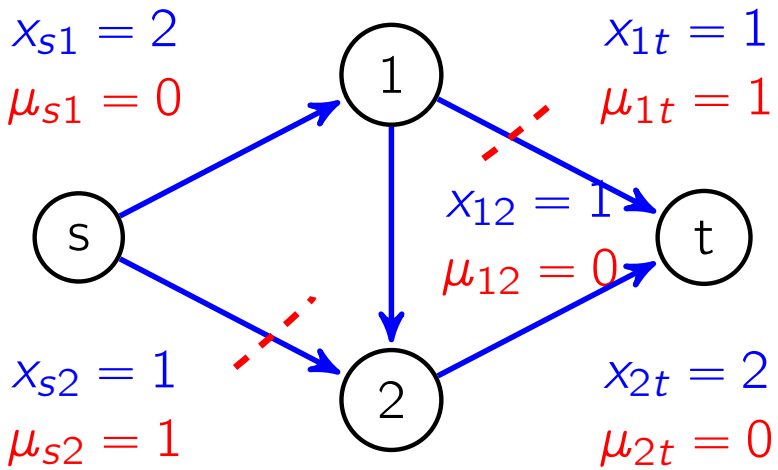
- Mixed-extension: for $(\sigma^1, \sigma^2) \in \Delta(\mathcal{F}) \times \Delta(\mathcal{A})$:

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

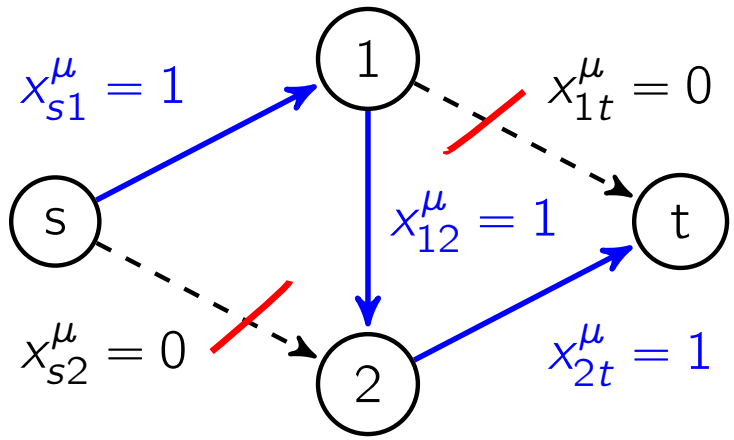
- $\mathcal{S}_\Gamma$ is the set of Nash Equilibria.

Example

$\forall (i,j) \in \mathcal{E},\ b_{ij} = 1.$



Initial flow and attack.



Resulting effective flow

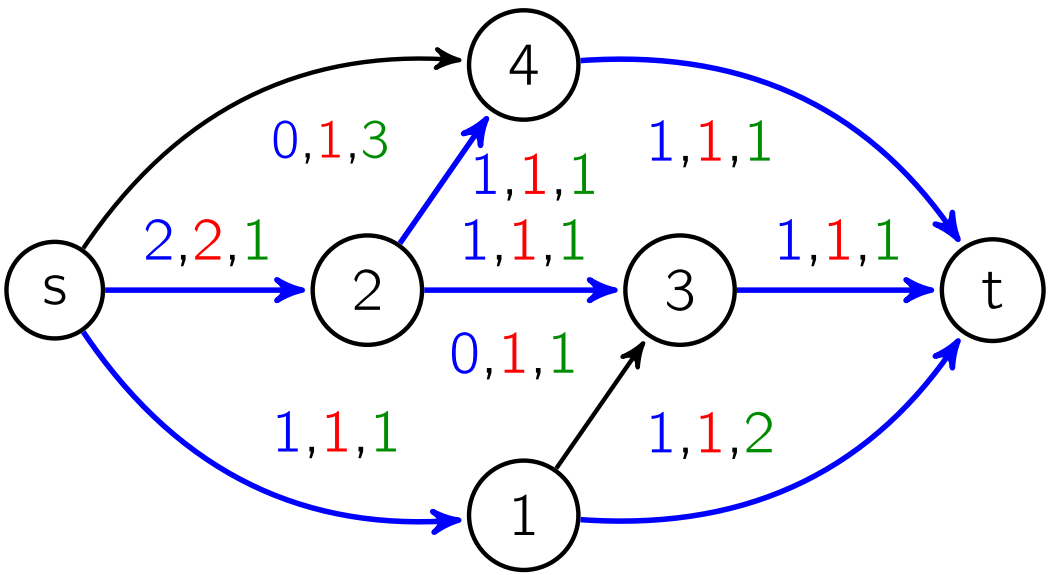
- $u_1(x,\mu) = p_1 - 7$
- $u_2(x,\mu) = 2p_2 - 2.$

What properties does $\mathcal{S}_\Gamma$ satisfy?

Simplification

Assumption 1

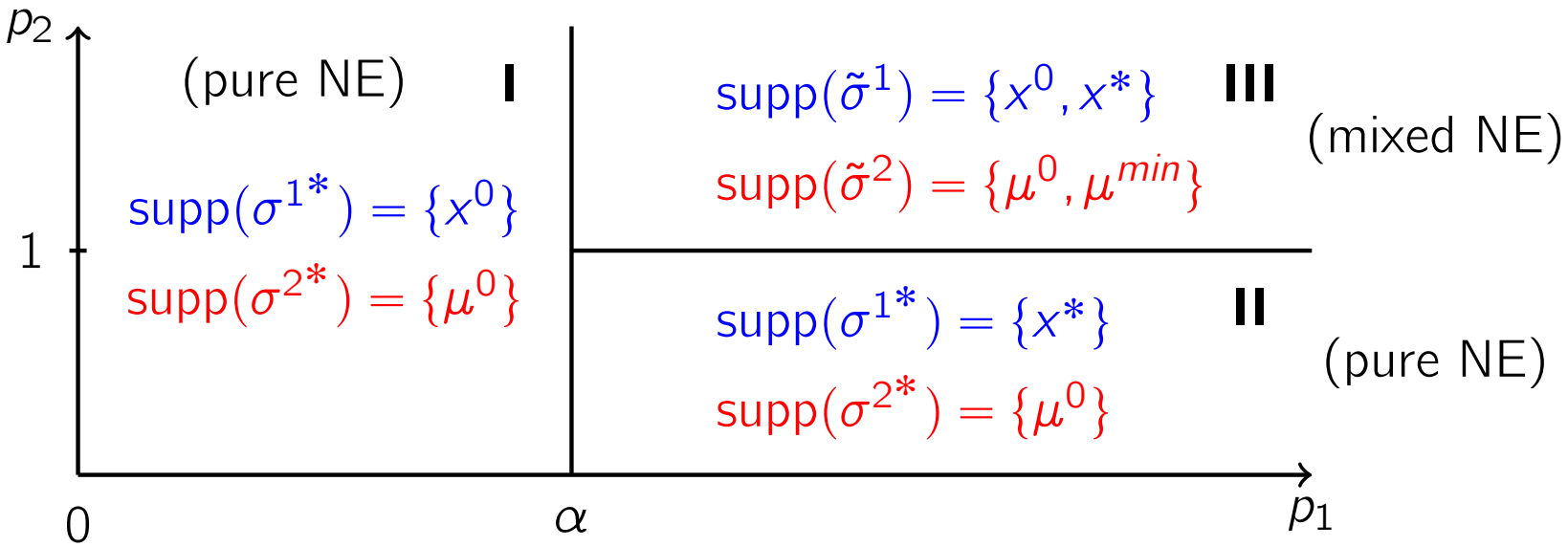
There exists a min-cost max-flow x^* that only takes $s-t$ paths that induce the lowest marginal transportation cost, denoted α.



- $\alpha = 3$

- α plays an important role in the results.

Regimes



Proposition (Regime **III**)

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

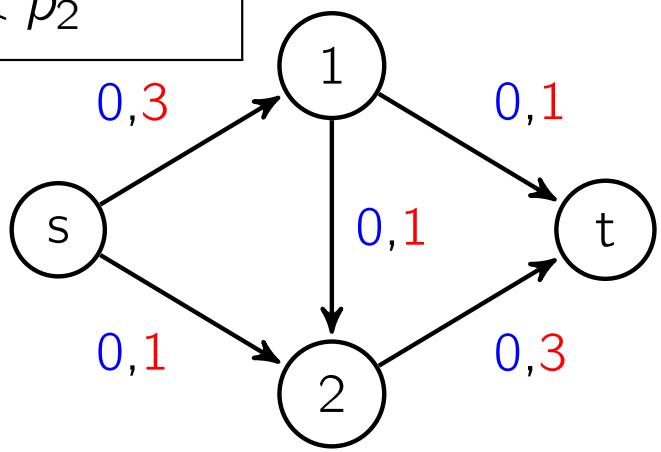
- $\tilde{\sigma}^1_{x^0} = 1 - \dfrac{1}{p_2}, \quad \tilde{\sigma}^1_{x^*} = \dfrac{1}{p_2},$
- $\tilde{\sigma}^2_{\mu^0} = \dfrac{\alpha}{p_1}, \quad \tilde{\sigma}^2_{\mu^{min}} = 1 - \dfrac{\alpha}{p_1}$

Illustration of the Regimes

- Example: Every path induces the same transportation cost

I

$0 < p_1 < \alpha$
$0 < p_2$

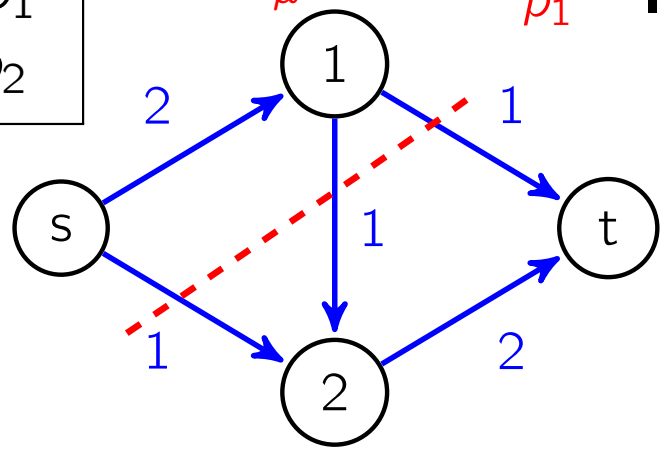


III

$\alpha < p_1$
$1 < p_2$

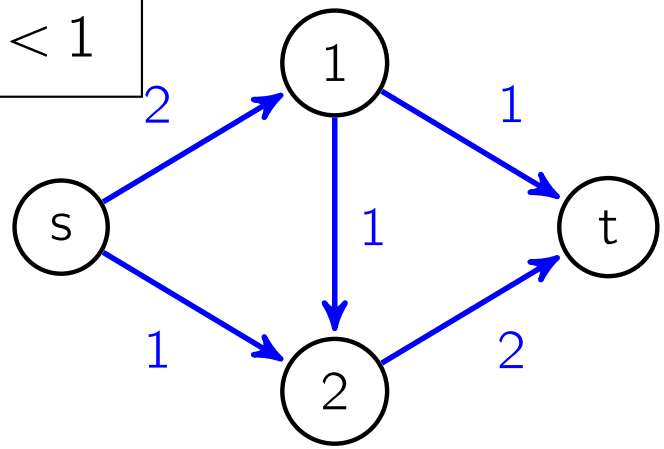
$\tilde{\sigma}^2_{\mu^{min}} = 1 - \frac{3}{p_1}$

$\tilde{\sigma}^1_{x*} = \frac{1}{p_2}$



II

$\alpha < p_1$
$0 < p_2 < 1$



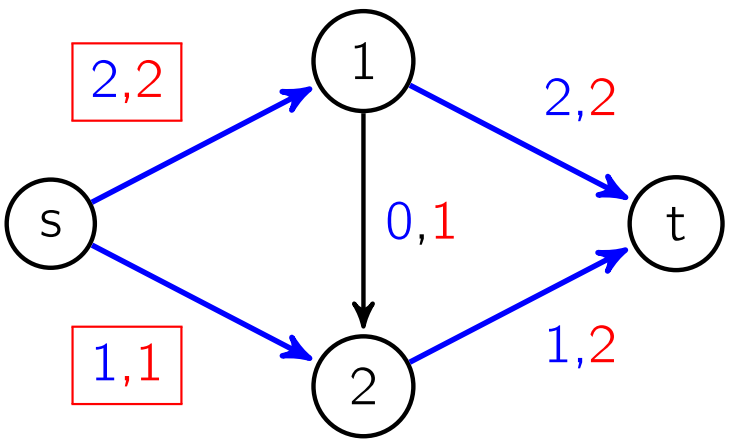
Necessary conditions

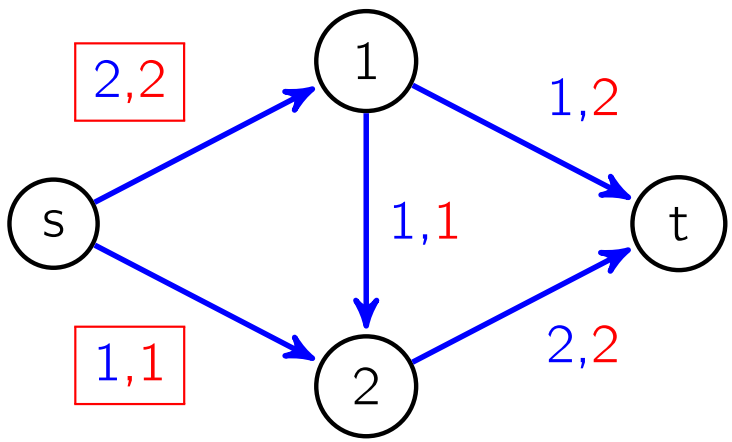
Attacker strategy σ^{2*} and $(\mathcal{P}_2)$

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

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

Example: every path induces the same transportation cost.





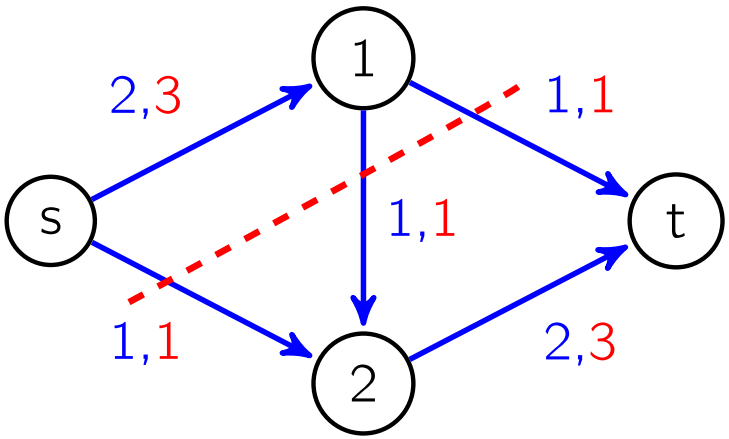
Necessary conditions

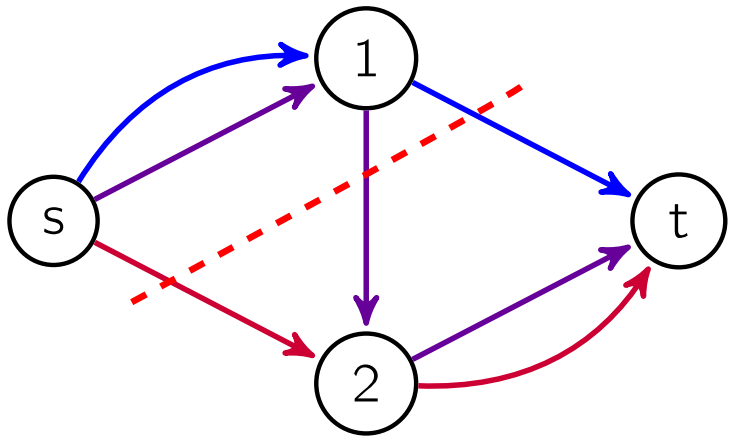
Defender strategy σ^{1*} and min-cut sets

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

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

Example:





Main results

$\overline{f} = \mathsf{F}(x^*)$: Optimal value of the max-flow problem.

Theorem (Regime **III**)

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

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

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

- *The expected amount of flow sent in the network is given by:*

$$\mathbb{E}_{\sigma^*}\left[\mathsf{F}(x)\right] \equiv \frac{1}{p_2}\overline{f}$$

- *Expected cost of attack:*

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

- *Expected transportation cost:*

$$\mathbb{E}_{\sigma^*}\left[\mathsf{C}_1(x)\right] \equiv \frac{\alpha}{p_2}\overline{f}$$

- *The expected amount of effective flow (that reaches t) is given by:*

$$\mathbb{E}_{\sigma^*}\left[\mathsf{F}(x^\mu)\right] \equiv \frac{\alpha}{p_1 p_2}\overline{f}$$

Summary: network routing under link disruptions

Results

- Modeled a simultaneous network security game on flow networks
- Obtained structural insights on the NE
- Related the NE to min-cost max-flows and min-cut sets
- Applied the analysis to a larger class of graphs
- Extended the results to a budget-constrained game

Future work

- Imperfect information game with both reliability and security failures
- Repeated game with incomplete information on one side

References

Sunghoon Hong and Myrna Wooders (2010)
Strategic Network Interdiction

Ford, L. R., D. R. Fulkerson (1956)
Maximal Flow through a Network

Assane Gueye, Jean C. Walrand, Venkat Anantharam (2010)
Design of network topology in an adversarial environment.

Alan Washburn and Kevin Wood (1995)
Two-Person Zero-Sum Games for Network Interdiction

Jack Edmonds and Richard M. Karp (1972)
Theoretical Improvements in Algorithmic Efficiency for Network Flow Problems

Dimitris Bertsimas, Ebrahim Nasrabadi, James B. Orlin (2013)
On the Power of Randomization in Network Interdiction.

Sanjeev Goyal, Adrien Vigier (2014)
Attack, Defense, and Contagion in Networks.