Resilient Monitoring and Control Algorithms for Distribution Networks

Saurabh Amin
Massachusetts Institute of Technology

Joint work with Devendra Shelar, Lina Sela (MIT), Galina Schwartz (UCB), Waseem Abbas, and Xenofon Koutsoukos (VU)

Map of research themes

CPS domain	Robust control (**RC**) of networks	Game theory (**GT**) and economic incentives (**EI**)
Flow network operations & control	Proactive incident control	Strategic user choices, Untrusted information
Electricity distribution	Vulnerability analysis, Optimal defense	Demand management, Security incentives

Software tools under development

- JAUNT: Joining Analytics based Units for Network Trustworthiness;
- CYPRS: Multi-model simulation tool to assess cyber-physical security threats on distribution networks.

Outline

Interdiction algorithms for electricity networks

Resilient fault diagnosis for flow networks

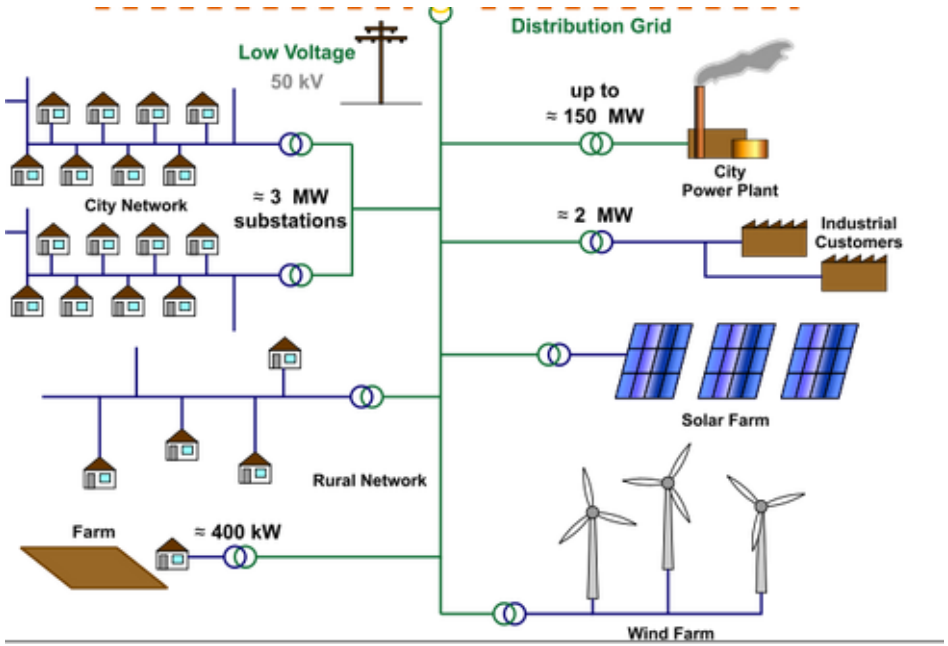
Electricity distribution network vulnerabilities

Motivation

- Management of distributed generation (DGs) in distribution networks need deployment of IT systems for monitoring & control
- IT risks $\Rightarrow$ new vulnerabilities

Our focus

- Worst case attack plans:
  1. Denial-of-service (DoS) attacks on DGs and loads
  2. Manipulation of protection equipment
- Secure network control
- Design secure CPS architecture



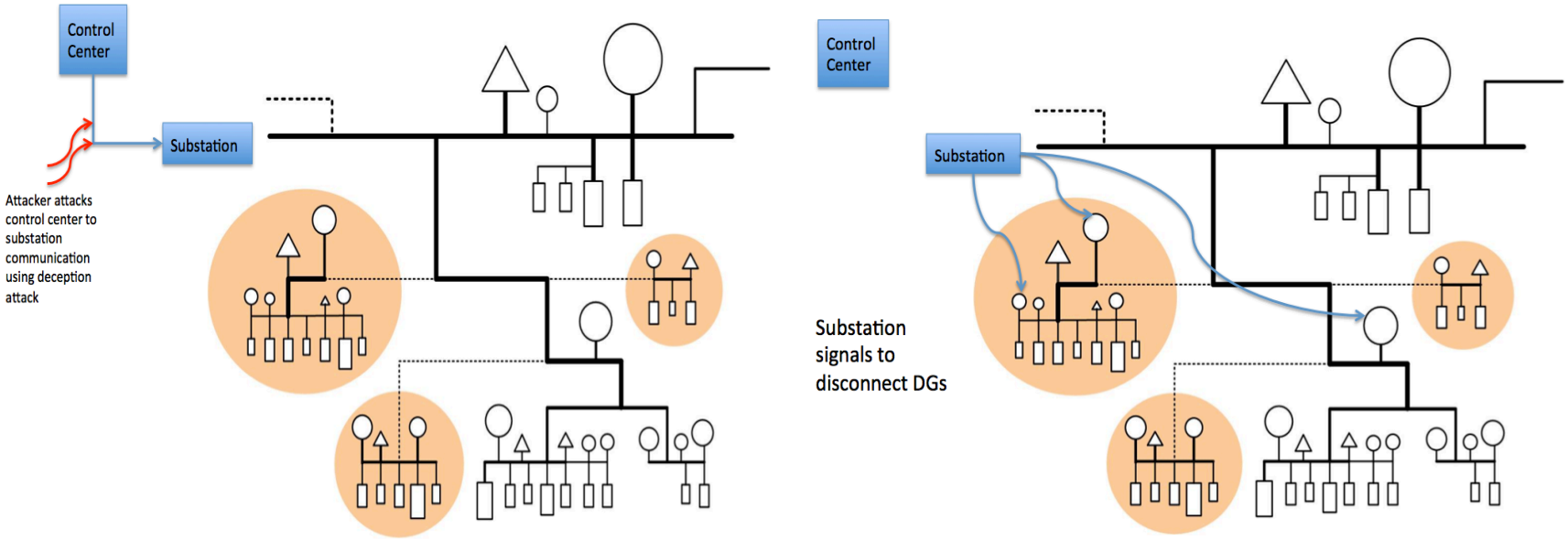
Distribution network with DGs

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Current practice

An example scenario (NESCOR report, EPRI '13)

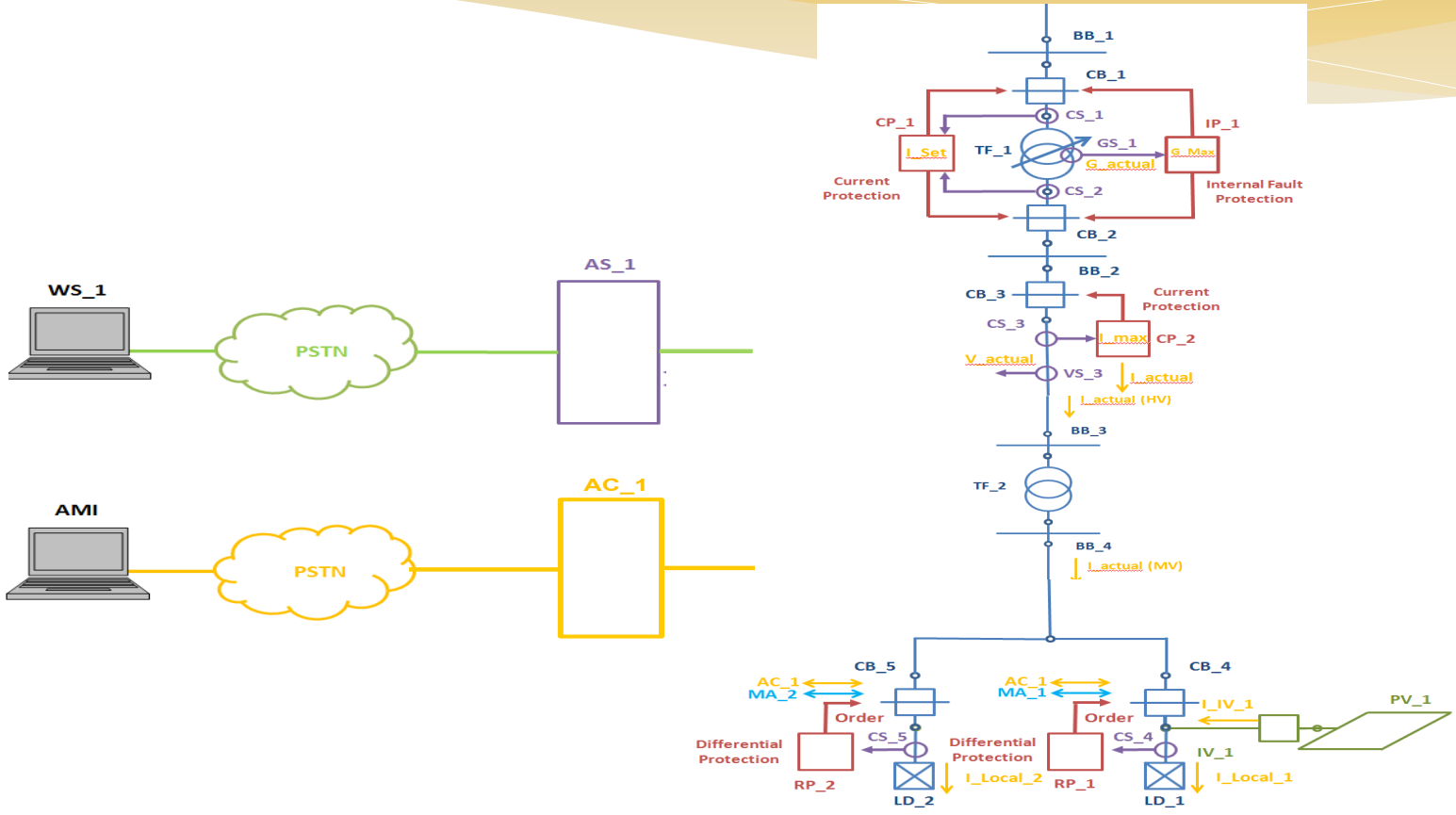
DGs are shutdown by spoofed SCADA control commands



Challenge

How to assess vulnerabilities for worst-case attacks?

First use cases obtained from EPRI experts

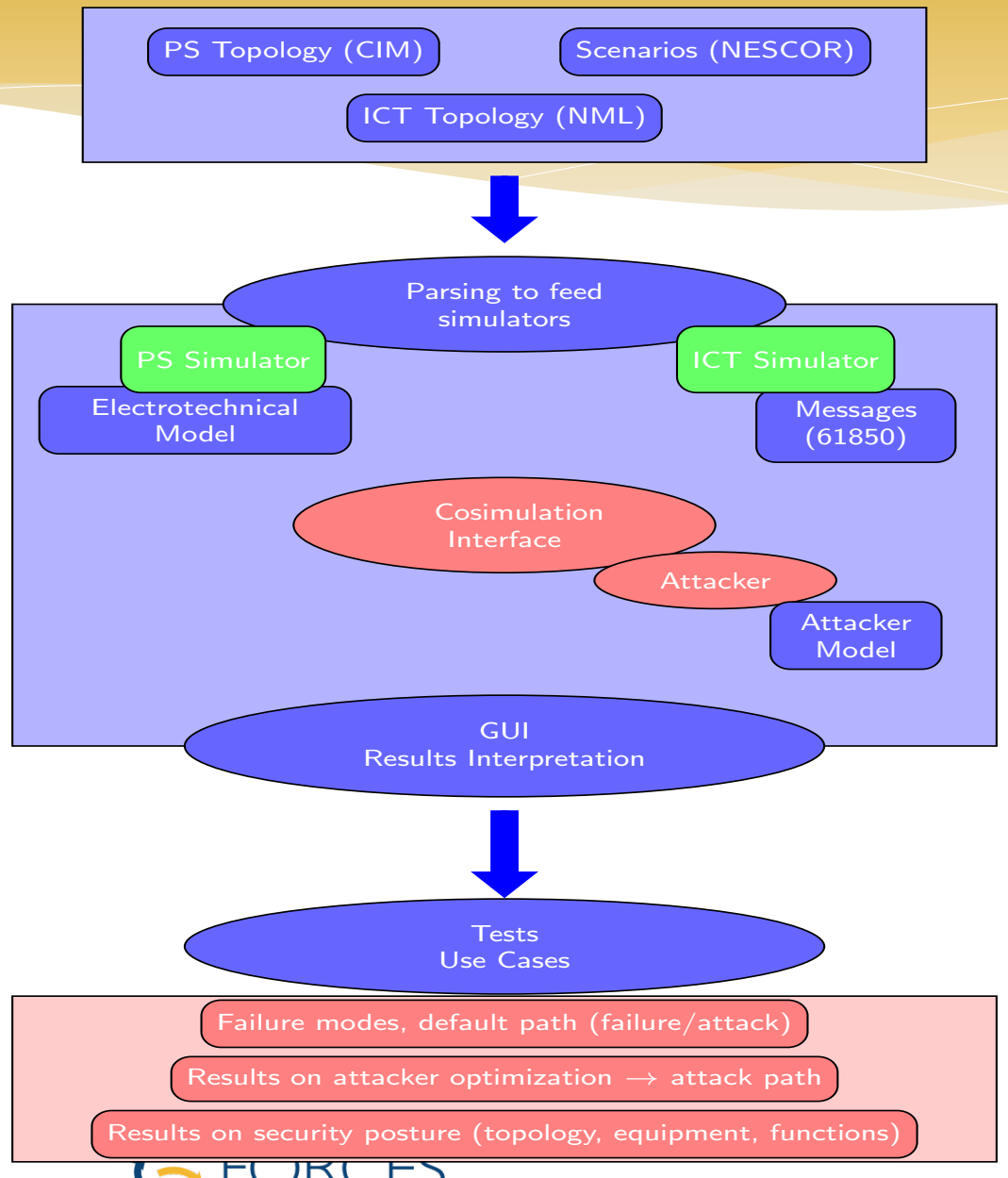


Electric single line diagram (General View)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

CYPRS co-simulation testbed

- Inputs
  - Power System
  - ICT
  - Scenarios: Which scenarios to simulate?
- Models
  - Simulations
- Outputs
  - Failure Modes
  - Optimization
  - Security



Network interdiction

Network interdiction problems can be viewed as perfect information leader-follower game: attacker moves first and defender moves next.

Problem statement:

1. Determine attacker's interdiction plan (compromise DGs) to maximize the sum of loss of voltage regulation and load shedding, given that under defender choices:
   - Inverters provide reactive power (VAR) control;
   - Demand at consumption nodes may be partly satisfied;
   - Ratings of protection equipment are satisfied
2. Determine attacker's interdiction plan (compromise DGs) to cause loss of voltage regulation, given that under defender choices:
   - Inverters provide reactive power (VAR) control;
   - Demand and rating constraints may or may not be satisfied.

Related work

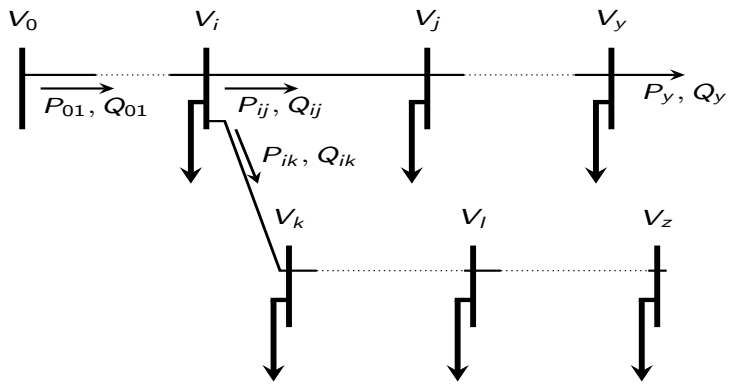
- Steven Low, *et al.*: Convex optimal power flow (on tree networks)
- Konstantin Turitsyn *e. al.*, Ian A. Hiskens. *et. al.*: Distributed optimal VAR control balancing voltage regulation and line losses
- Ross Baldick, Kevin Wood: Interdiction for transmission networks
- Daniel Bienstock, *et al.*: Cascading failures with linear power flow

Our Contribution

- Optimal attacker's interdiction plans under different inverter VAR control and load shedding strategies of defender;

Power flow over 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
- $r_{ij} + \mathbf{j}x_{ij}$ - impedance on line (i, j)



Power flow over tree networks

- Power flow constraints

$$\text{Conservation of real power} \quad P_{ij} = \sum_{k:(j,k)\in\mathcal{E}} P_{jk} + r_{ij} \underbrace{\frac{P_{ij}^2 + Q_{ij}^2}{\nu_i}}_{\text{real power loss}} + \overbrace{p_j^c - p_j^g}^{\text{net real power injected}} \tag{1a}$$

$$\text{Conservation of reactive power} \quad Q_{ij} = \sum_{k:(j,k)\in\mathcal{E}} Q_{jk} + x_{ij}\frac{P_{ij}^2 + Q_{ij}^2}{\nu_i} + q_j^c - q_j^g \tag{1b}$$

$$\text{Ohm's Law} \quad \nu_j = \nu_i - 2(r_{ij}P_{ij} + x_{ij}Q_{ij}) + (r_{ij}^2 + x_{ij}^2)\frac{P_{ij}^2 + Q_{ij}^2}{\nu_i} \tag{1c}$$

$$\text{Current = Power/Voltage} \quad \ell_{ij} = \frac{P_{ij}^2 + Q_{ij}^2}{\nu_i} \tag{1d}$$

- Voltage constraints

$$\underline{\nu}_i \leq \nu_i \leq \overline{\nu}_i \tag{2}$$

Loss Function

- Cost due to loss of voltage regulation

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

- Cost incurred due to load shedding

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

- Composite loss function

$$L(\delta, \gamma) = L_{\text{LOVR}} + L_{\text{LL}}$$

Trade offs: Voltage Reg. vs. Line Losses vs. Lost load

- Ignoring the line losses w.r.t. power flows, Ohm's Law can be approximated as
  $\nu_j \approx \nu_i - 2(r_{ij}P_{ij} + x_{ij}Q_{ij})$
- Voltage Regulation
  - $\nu_j \approx \nu_i \implies Q_{ij} = -\frac{r_{ij}}{x_{ij}}P_{ij}$
- Line Losses
  - $Q_{ij} = 0$
- $\frac{r}{x}$ ratio : Typical values $\frac{1}{2}$ - $\frac{1}{5}$
- Varying q^g has more effect than variations of p^g

Similar trade-offs between loss of voltage regulation and value of lost load

Attacker and defender models

Attacker

- Disrupt DGs

$$\delta_i = \begin{cases} 0 & \text{if } i^{th} \text{ DG is disrupted} \\ 1 & \text{otherwise} \end{cases}$$

- Satisfy resource constraint

$$\sum_{i=1}^{n} \delta_i \geq n - M \qquad (3)$$

Defender

- Control DGs: p_i^g and/or q_i^g
- Shed load

$$\gamma_i \in [\underline{\gamma}_i, 1], \text{where } \underline{\gamma}_i \in [0, 1]$$

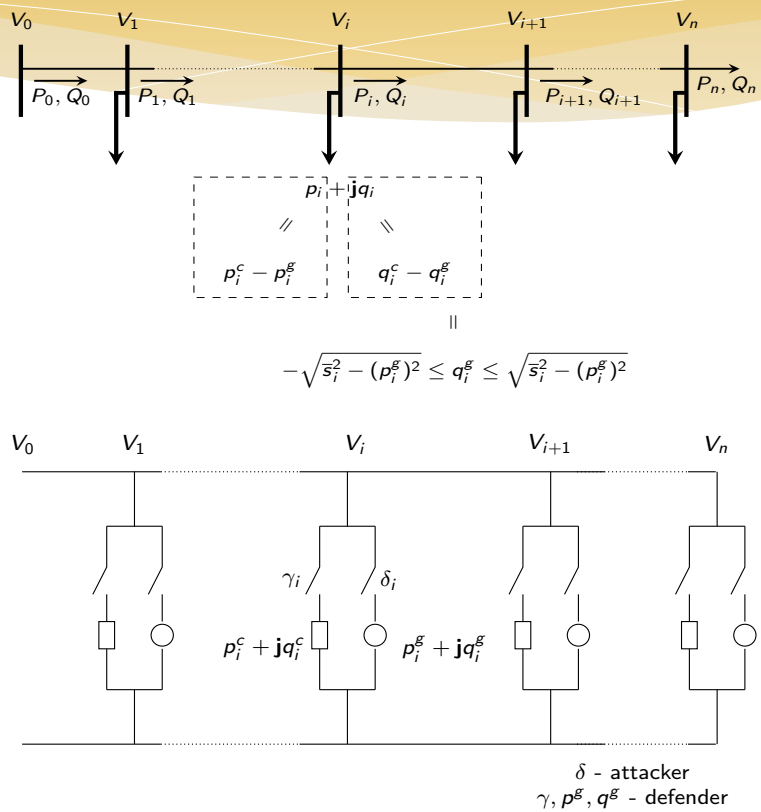


Figure : Linear network representation

Problem statement

Find attacker's interdiction plan to maximize loss of voltage regulation and load shedding, given that defender optimally responds (VAR & load control)

$$\max_{\delta} \quad \min_{u} \quad -\min_{i \in \mathcal{N}_0} w_i(\nu_i - \underline{\nu}_i) + \sum_{i \in \mathcal{N}_0} (1 - \gamma_i) C_i$$

$$\text{s.t. } (1) - (3)$$

$$u := (P, Q, p^g, p^c, q^g, q^c, \nu, \ell, \gamma)$$

$$\delta \in \{0,1\}^n, \gamma \in [\underline{\gamma}_i, 1]^n$$

Simple case

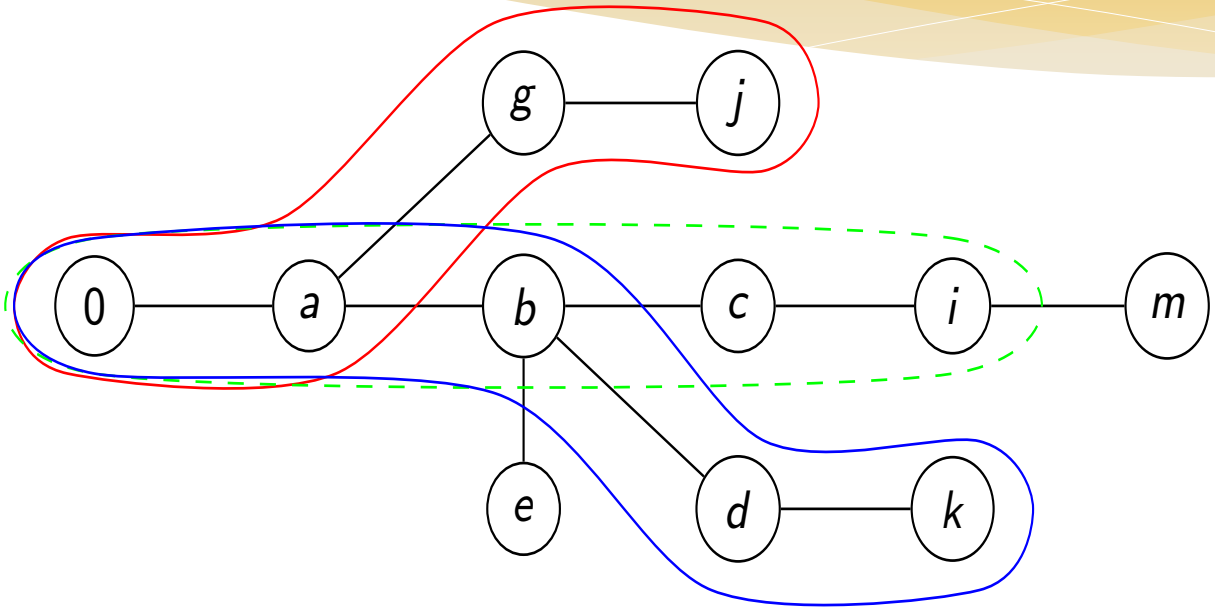
Aforementioned bilevel-problems are hard!

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

For fixed defender choices:

$$\max_{\delta} \quad -\min_{i \in \mathcal{N}_0} w_i(\nu_i - \underline{\nu}_i)$$
$$\text{s.t. } (1) - (3)$$

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 of b is ancestor of k

Main result: Optimal interdiction plan

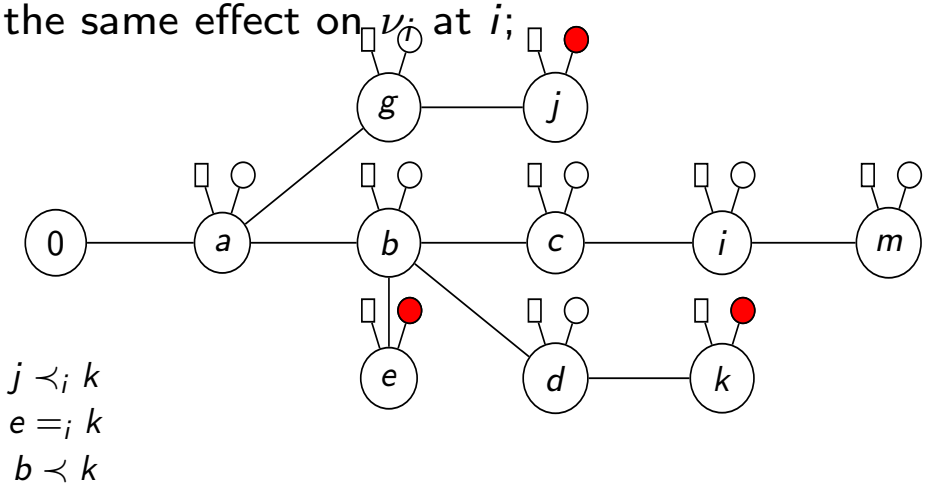
- Let ν_i^{old}/ν_i^{new} be $|V_i|^2$ before/after the attack
- $\Delta(\nu_i) = \nu_i^{old} - \nu_i^{new}$

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;
- 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;

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



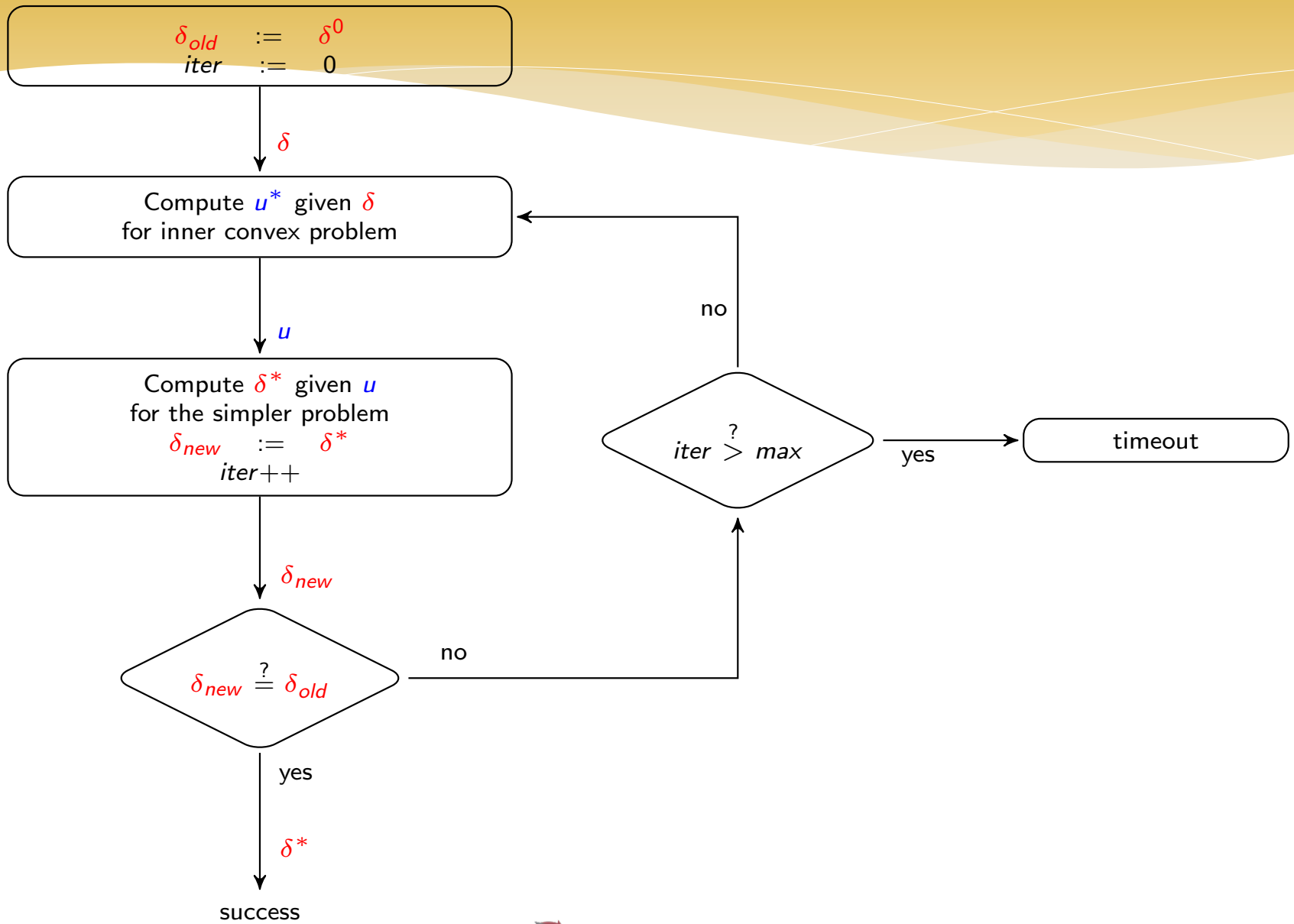
$j \prec_i k$
$e =_i k$
$b \prec k$

Optimal attack under 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
  $k := \arg\min_{i \in \mathcal{N}_0} \quad \nu_i - \Delta_{J_i^*}(\nu_i)$
  return $J^* := J_k^*$ (Pick J_i^* which violates voltage constraint the most)
end procedure

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

Computing "optimal" attack plan under defender response



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

An Illustration

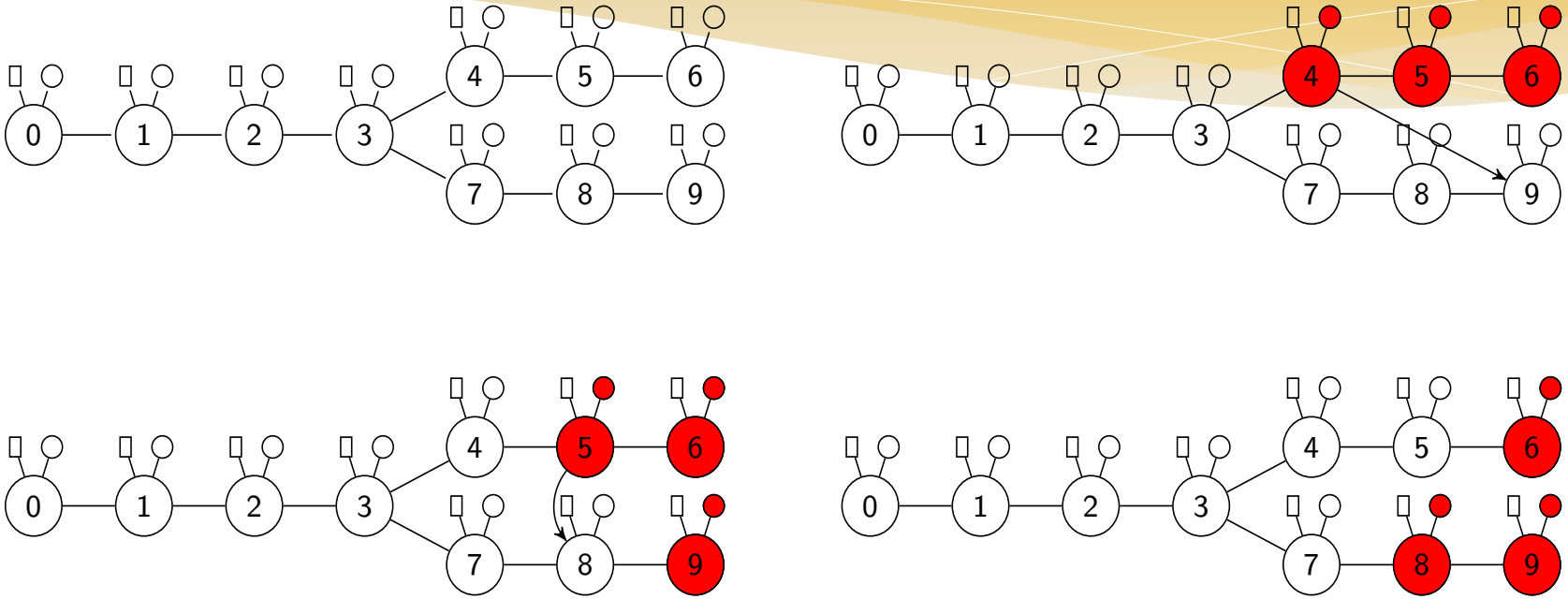
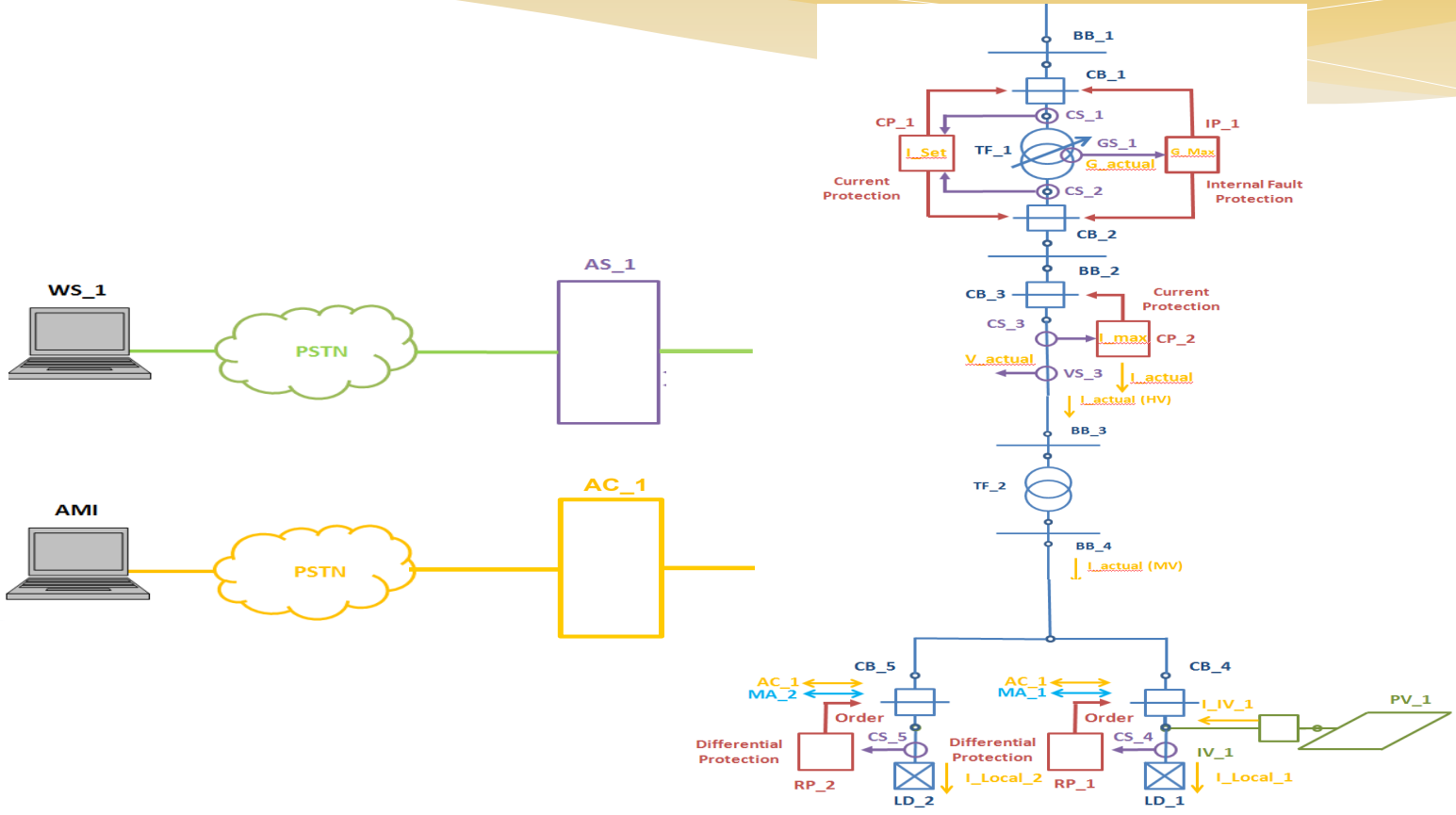


Figure : Heuristic for update of δ

- Defender actions : γ, p^g, q^g
- Non-uniqueness of solutions

Ongoing work: implementation of optimal attacks on EPRI use cases



Electric single line diagram (General View)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Related work: Game theoretic analysis for energy diversion

A game-theoretic model of distribution utility and consumers

- Sequential game; distributor moves first
- Consumer choice: the amount of electricity to steal
- Consumer theft is lower if
  - (i) fines are higher
  - (ii) detection prob. is higher
- Distribution utility investment in theft prevention is higher if
  - (i) its costs of monitoring are lower
  - (ii) user theft is higher

Conclusions

- Monopolist distributor: low investment in detection [suboptimal]
- Regulated distributor: low investment in detection [suboptimal]
- Lax monitoring = High theft

Incentives + Control

- Distributors: via regulatory reform [Incentives]
- Consumers: via increase of fines, shaming [Control]

Outline

Interdiction algorithms for electricity networks

Resilient fault diagnosis for flow networks

Resilient Water Networks

Water nets as CPS

Network sensing

- Monitor pressure and water quality
- Data acquisition and telemetry

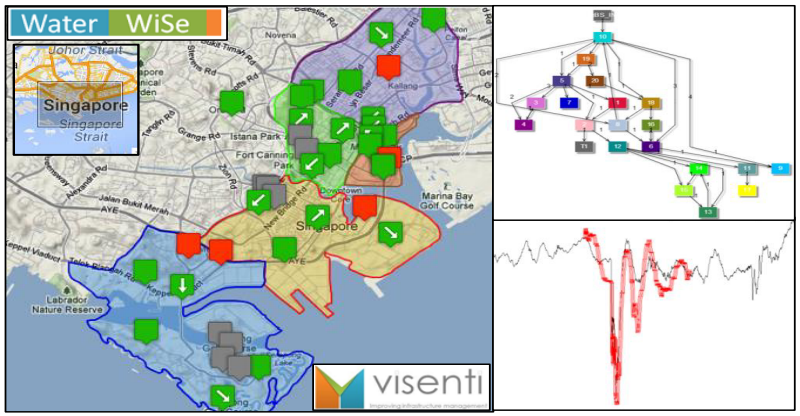
Analytics

- Hydraulic modeling and simulation
- Event detection, localization, and classification
- Data visualization

Research scope

- Vulnerability assessment: use Network interdiction
- Network control: Lina Sela's talk
- Resilient sensor placement: This talk

Water CPS, Singapore



MIT, SMART-CENSAM, Visenti Pte., PUB, NRF Singapore

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

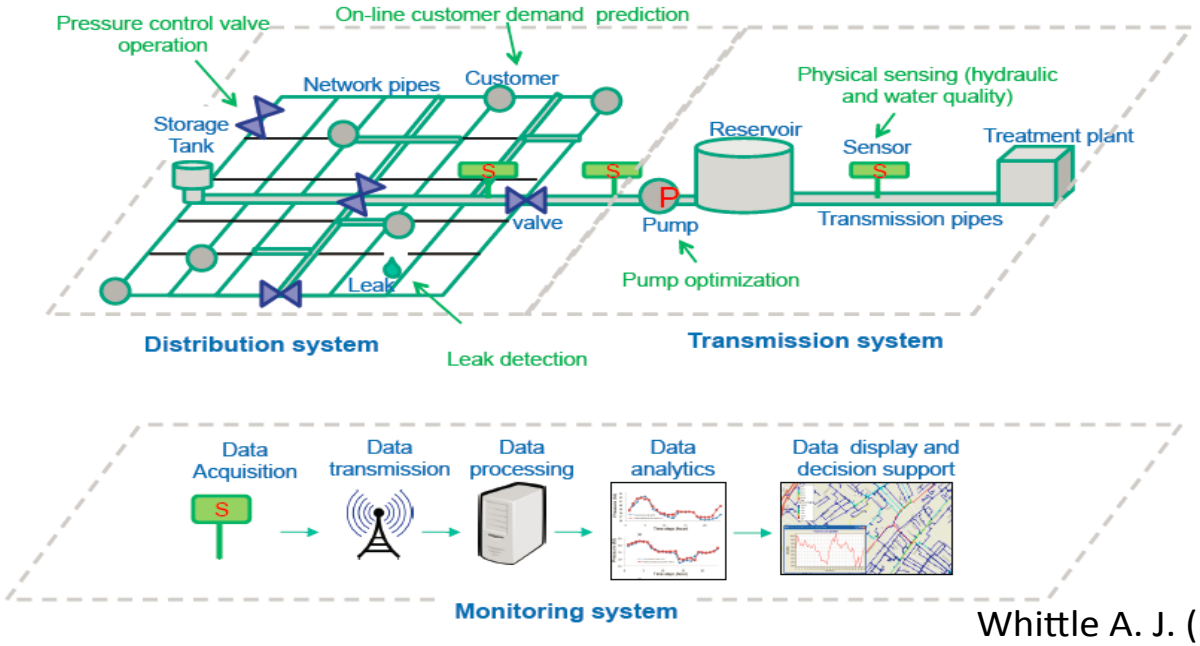
Cyber-physical water supply systems

Physical net:

- Production and treatment,
- Transmission,
- Distribution.

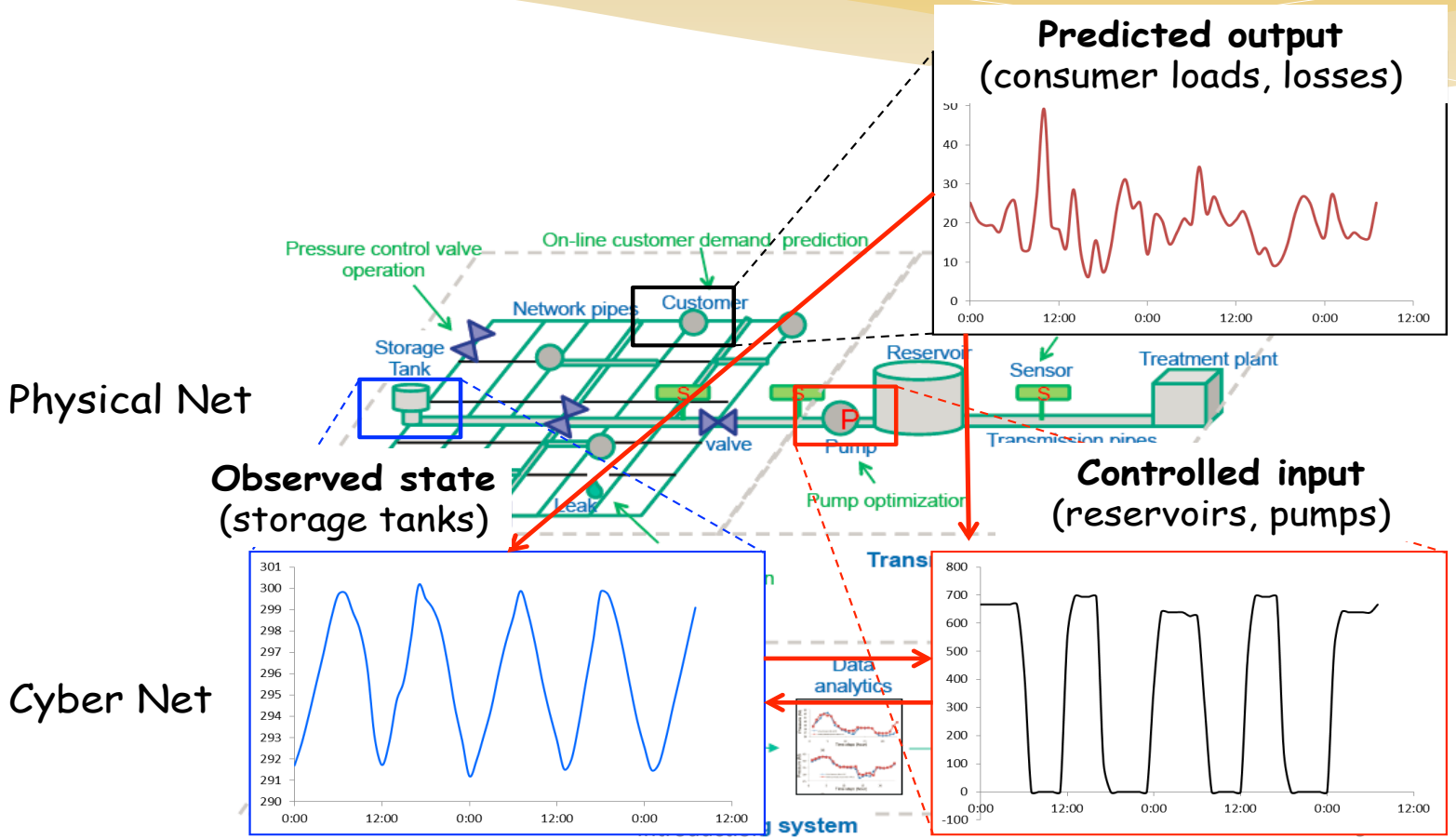
Cyber net:

- Data acquisition,
- Analytics,
- Decision support & control.



Whittle A. J. (2012)

Control of water supply systems



Cyber Physical water system security

Threats to water systems:

- physically or remotely disrupting network assets
  - isolation of pipes in the network,
  - disconnecting one or more sources
- deception:
  - feeding sensors with false information,
  - manipulating actuators' set points.

Our recent work

- Modeling: vulnerability assessment by accounting for effect of:
  - Topological connectivity, and
  - Nonlinear flow dynamics

  on the operational performance of the water networks.
- Optimization: Interdiction model where attacker interdicts supply nodes and/or network links to cause loss of operational performance.

Vulnerability analysis: lessons learned

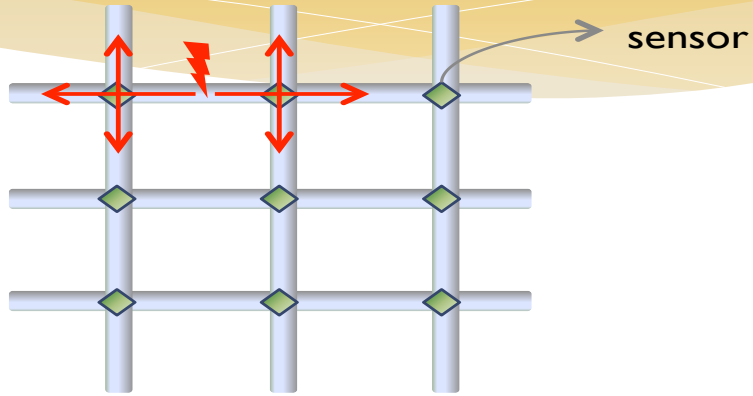
- Network interdiction model: Bi-level optimization problem with convex sub-problem and mixed integer master problem;
- Network nonlinearities play a critical role, in addition to topological connectivity;
- Reinforcing network pipes for mitigating the vulnerabilities is not cost-effective;
- Systems by a single source are highly vulnerable;
- Operational changes (control) for cost-effective resilience needs to be further explored.

Fault diagnosis in flow networks

Objective

Given a flow network, distribute the minimum number of sensors that can

- Detect a link failure
- Localize a link failure (uniquely identify a link failure)



Use

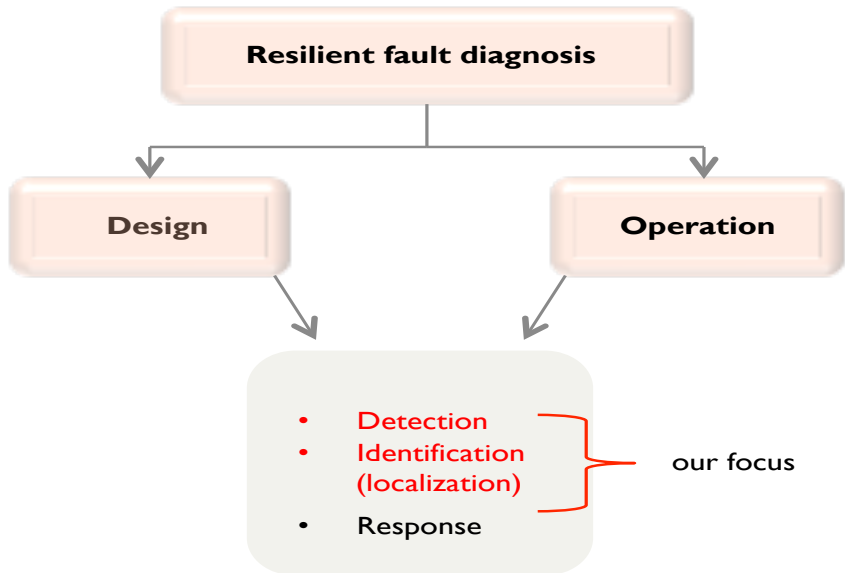
Sensor network design for the detection and identification of faults

Methods

System (flow network, faults, sensor) model, combinatorial optimization

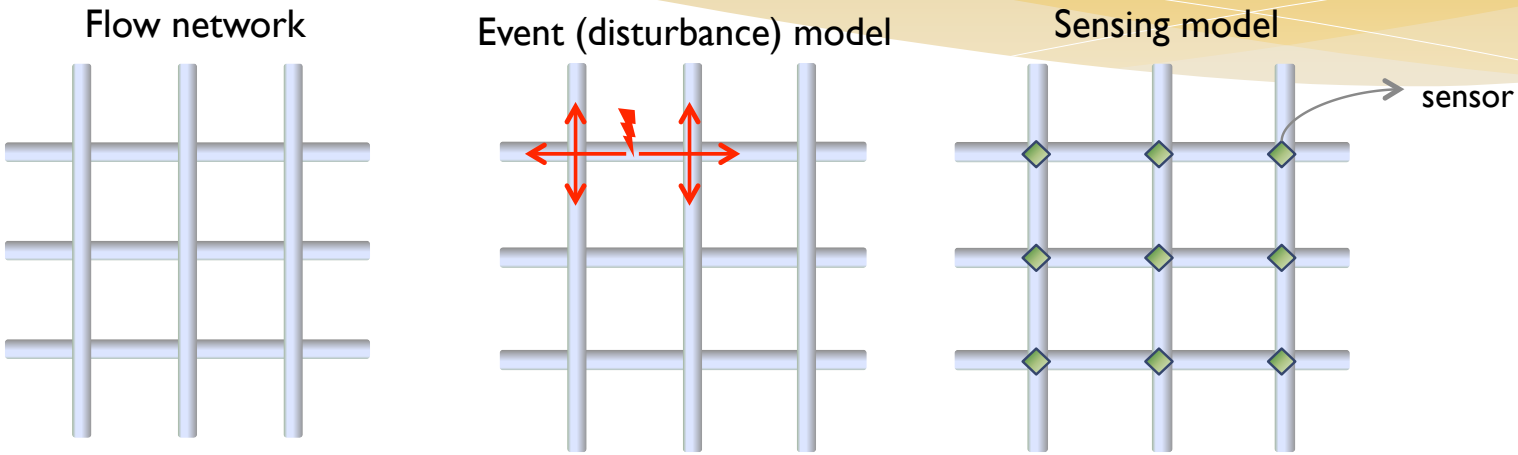
Performance evaluation

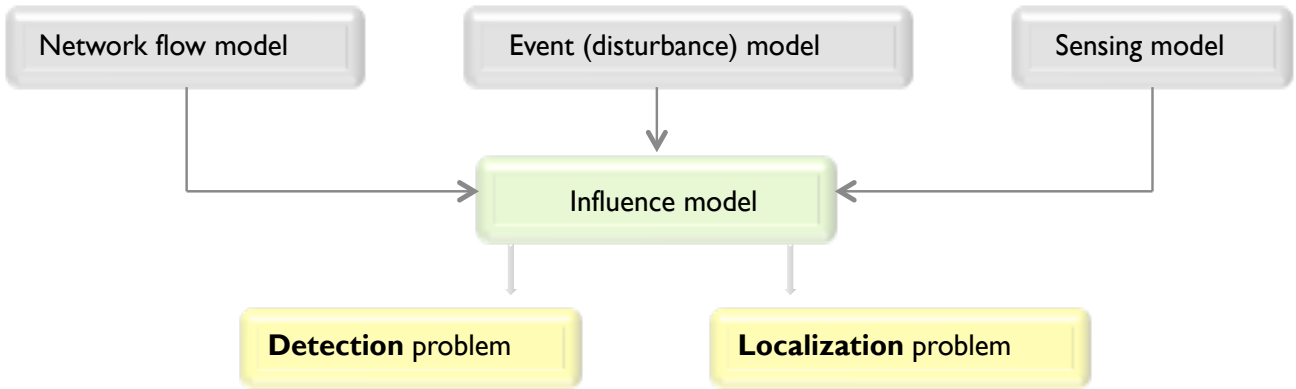
Resilience to random sensor faults and adversarial attacks



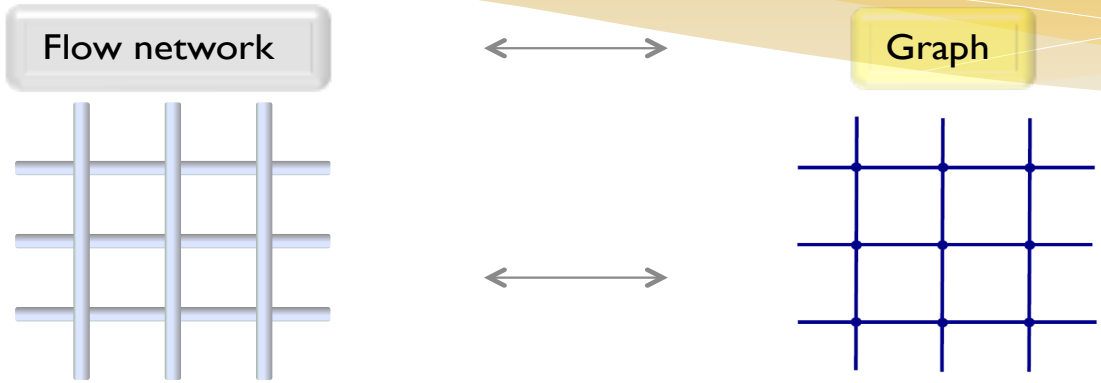
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

System model





Flow network model



Links		Edges
Physical characteristics (e.g., length, material parameters etc.)	⟷	Edge weights
Physical characteristics (e.g., nodal demands etc.)		Node weights

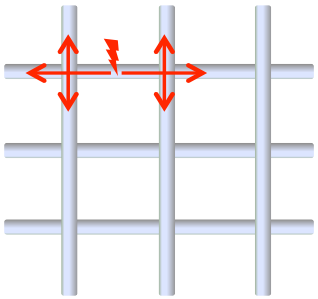
The physical network is defined by

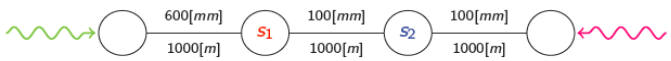
- Network topology (graph): $G = G(V,E)$
- Flow model over the graph G: $f = f(Q,H,G)$

Q = flows over network links
H = heads over network nodes

$$\begin{bmatrix} H = p + z \\ p = \text{pressure} \\ z = \text{elevation} \end{bmatrix}$$

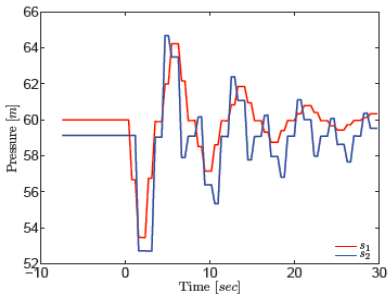
Evidence (Disturbance) model



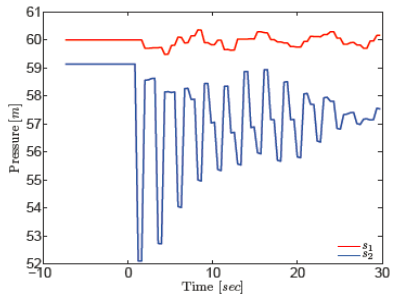


- Event model is comprised of a link failure and its impact
  - Pipe failure (random or induced) and the pressure transient generated.
  - Physically flushing an hydrant causing massive loss of water, increased load on the system and corresponding pressure losses.
  - Remotely closing or opening active elements (pumps, valves) that can cause severe transients in the systems.
- The signal propagates in all directions from the site of failure along the links of the network.

Event 1

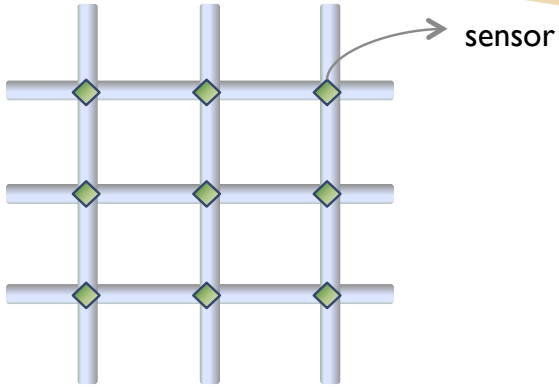


Event 2



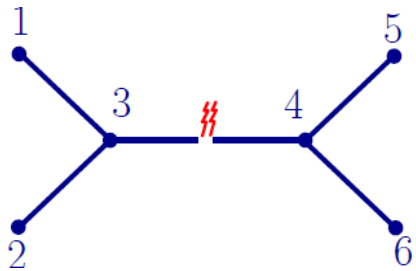
Along with the network topology, the **physical model** defined over the graph also affects the event model

Sensing model



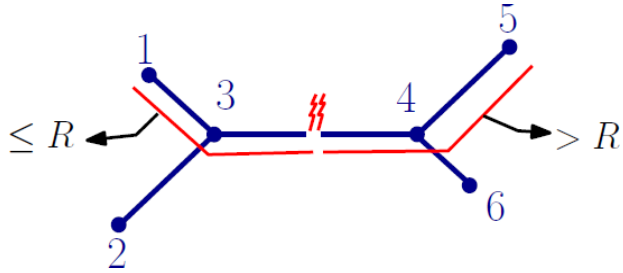
- Sensors are placed at the nodes.
- A sensor can detect the pressure signal from any direction.
- An alarm is raised when a sensor detects a signal.

First-order model:



All sensors at the nodes adjacent to the end nodes of failed link will detect the fault.

R-disk model:



A sensor can detect a fault if and only if fault occurs at a link that lies within the distance R from the failure along the links.

Influence model

- Network flow, event, and sensor model outputs are represented using an **influence matrix** M.
- ℓ_i - i^{th} **row** corresponds to the **event** i.
- θ_j - j^{th} **column** corresponds to the j^{th} **sensor**.
- M_{ij} - j^{th} sensor output in response to the event i.

Example: M is boolean matrix.

Sensor 1's output is 1 when event 2 occurs.

$$
\begin{array}{c}
 & \theta_1 & \theta_2 & \dots & \theta_j & \dots & \theta_n \\
\ell_1 & 0 & 0 & \dots & 1 & 0 & 0 \\
\ell_2 & 1 & 1 & \dots & 0 & 1 & 0 \\
 & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
\ell_i & 1 & 0 & \dots & 1 & 1 & 0 \\
 & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
\ell_m & 0 & 0 & \dots & 1 & 0 & 1
\end{array}
$$

Detection and localization

Detection

Find the minimum number of sensors and their locations so that every link failure can be detected by at least one sensor.

Event set: $\{\ell_1, \ell_2, \cdots, \ell_m\}$

Sensor set: $\{\theta_1, \theta_2, \cdots, \theta_n\}$

Detection set: C_i = Set of links whose failure is detected by the sensor i.

Minimum set cover problem

Localization

Find the minimum number of sensors and their locations so that every link failure can be uniquely identified and can be distinguished from any other link failure.

Event set: $\{\ell_1, \ell_2, \cdots, \ell_m\}$

Sensor set: $\{\theta_1, \theta_2, \cdots, \theta_n\}$

Identification set

Minimum test cover problem

Example

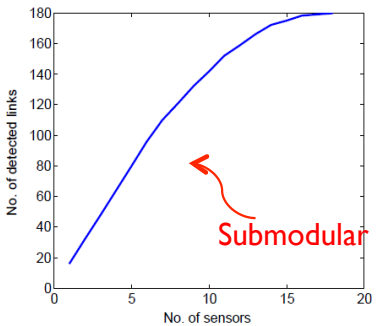
- Consider a 10 by 10 grid network consisting of 100 nodes and 180 links.
- Influence matrix is obtained using the first order influence model.

Detection → (greedy) MSC

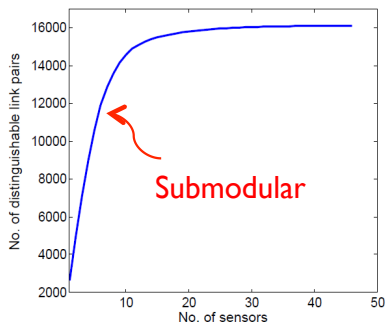
18 sensors are sufficient to **detect** any link failure.

Localization → MTC → (transform) (greedy) MSC

46 sensors are sufficient to **localize** any link failure.



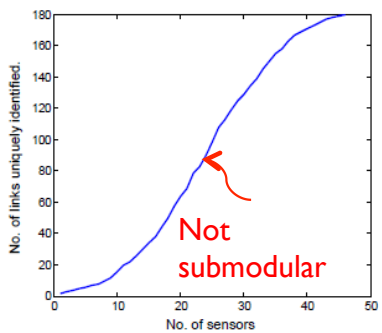
No. of detected links as a function of sensors deployed.



No. of distinguishable link pairs as a function of sensors deployed.

Total no. of link pairs

$$\binom{180}{2} = 16110$$



No. of links that can be uniquely identified as a function of sensors deployed.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Ongoing work

- Incorporate network topology and influence model to design efficient (scalable, improved approximation ratios) algorithms for detection and localization
- Characterize detection and localization of link failures as a function of number of sensors deployed (e.g., submodularity)
- How the detection & localization of link failures are dependent on the influence model and network topologies?
- For a given influence model, what are the (structural) constraints on the network topology such that every link failure can be detected as well as localized?
- Generalizations
  - Associating a probability distribution to the link failures.
  - Detecting (localizing) $k > 1$ simultaneous link failures.
  - Incorporating more generalized sensing and influence model.
- Resilient fault diagnosis $\Rightarrow$ Prof. X. Koutsoukos's talk