Reliable Distribution Nets

Polina Sela, Devendra Shelar, Saurabh Amin
MIT Department of CEE

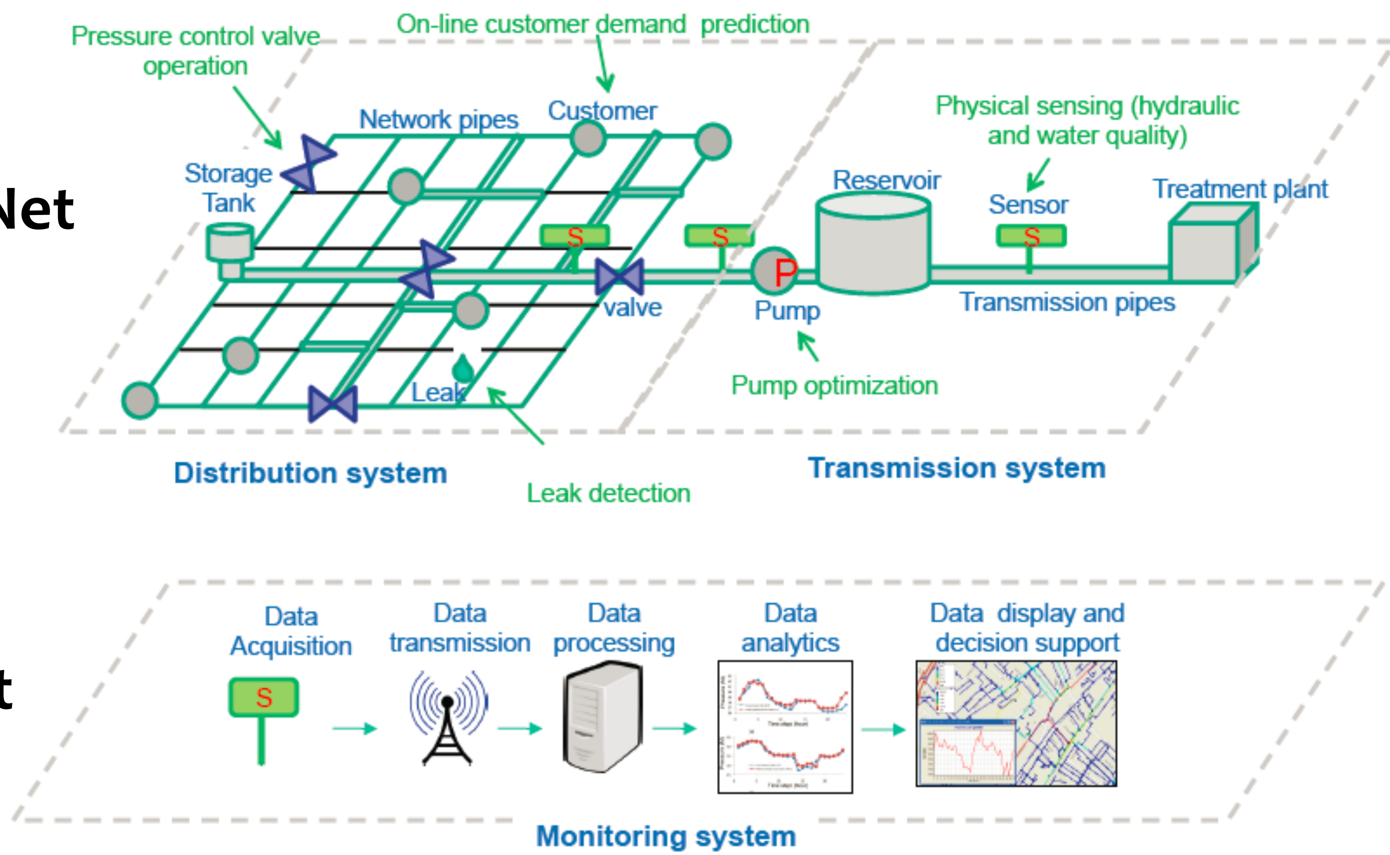
Smart Distribution Nets

Components	Electrical network	Water network
Transmission system	Transfer energy	Transfer water
Distribution system	Delivery to consumers	
Structure	Elevated	Mostly underground
Side sources	Solar panels, wind turbines	Wells, desalination plants
Storage	Not practical	Local storage tanks
Large scale	Large geographical areas, many nodes and links	
Dynamic	Time varying, e.g. supply and demand	
Uncertainty	Inherent uncertainty, e.g. demand	
Modeling	Current, potential, potential drop (linear)	Flow, hydraulic head, headloss (nonlinear)
SCADA	Advanced measuring and control	
Sensing and smart metering	Online sensing, analysis, and transmission	
Losses	Physical (leaks) and apparent (metering errors, theft)	
Security	**Physical and cyber security against an adversary**	

Smart Water Distribution Nets

Physical Net

Cyber Net



Whittle A. J. (2012)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Water Distribution Nets

Research topic:

Using WDS modeling to assist epidemiologic investigations

Challenge:

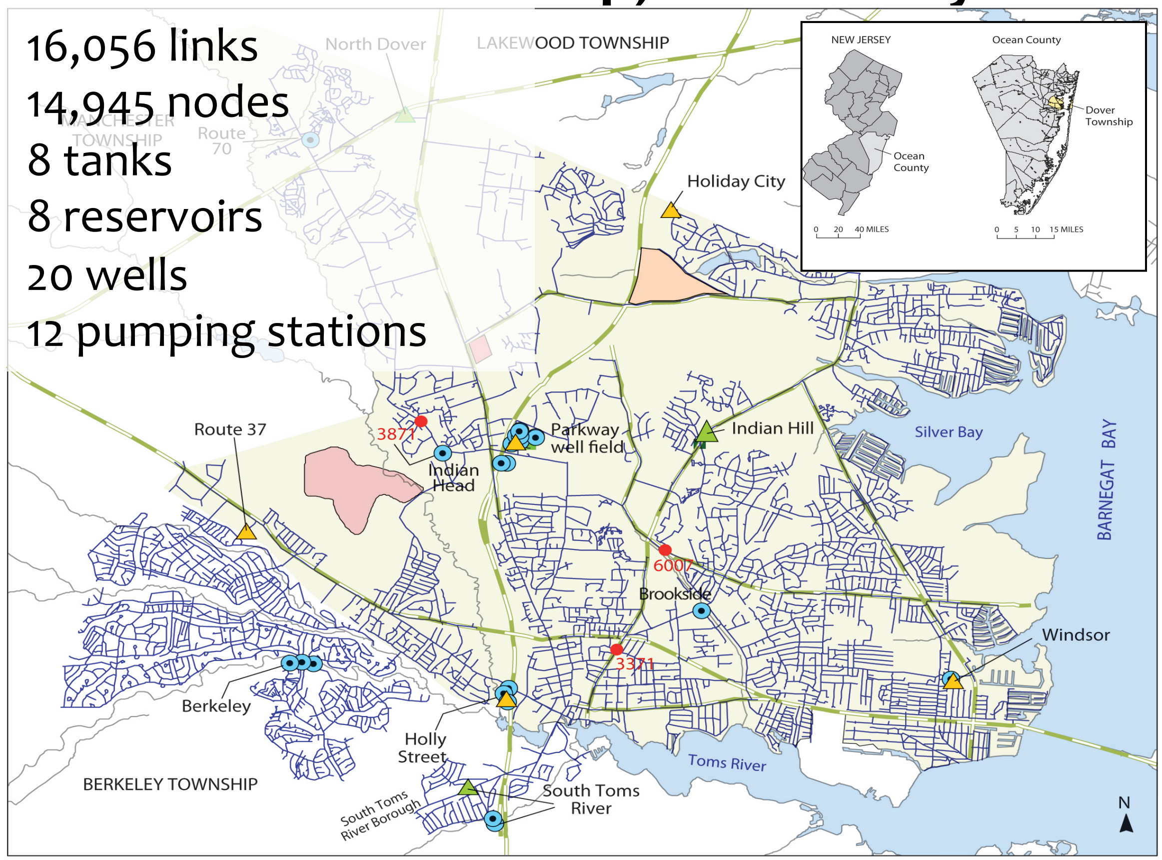
Large-scale, dynamic system, nonlinearity – computational complexity

Approach:

System aggregation for hydraulic and water quality analysis

Dover Township, New Jersey

16,056 links
14,945 nodes
8 tanks
8 reservoirs
20 wells
12 pumping stations



Roads, hydrography, and boundaries based on 1995 TIGER/Line data

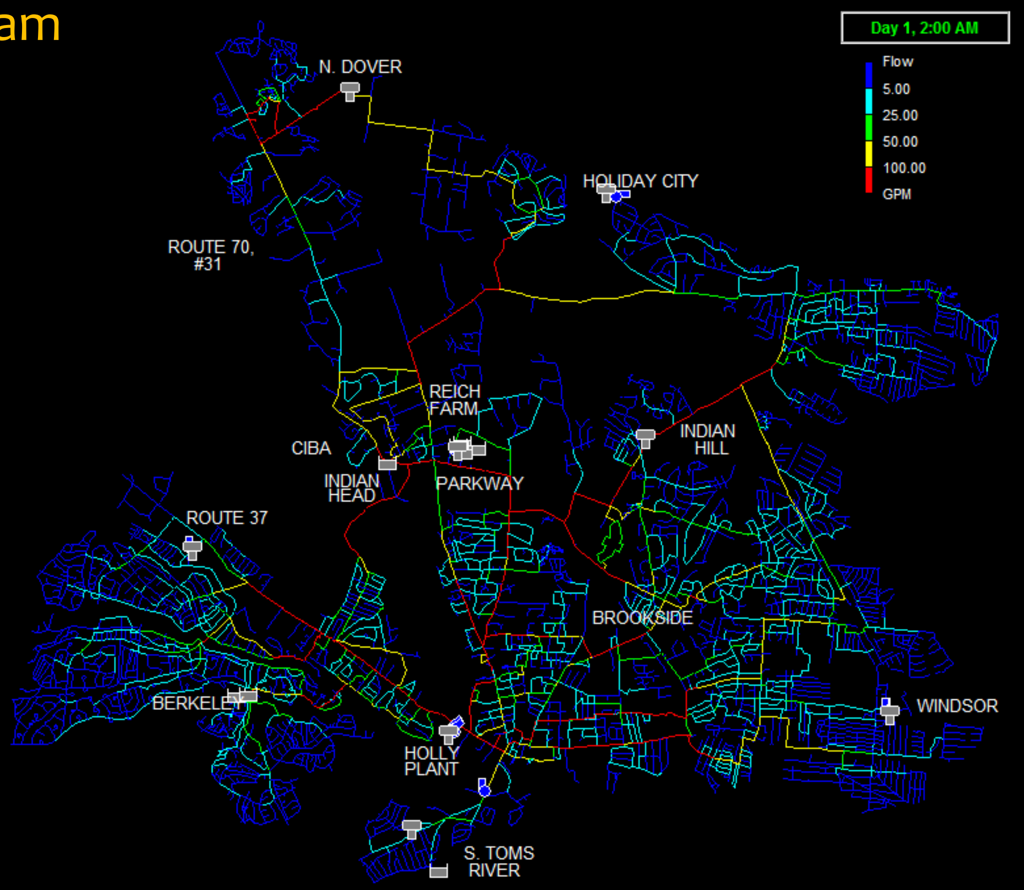
0 1 2 3 MILES

FORCES FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Maslia et al 2000

Dynamic complex large-scale nets

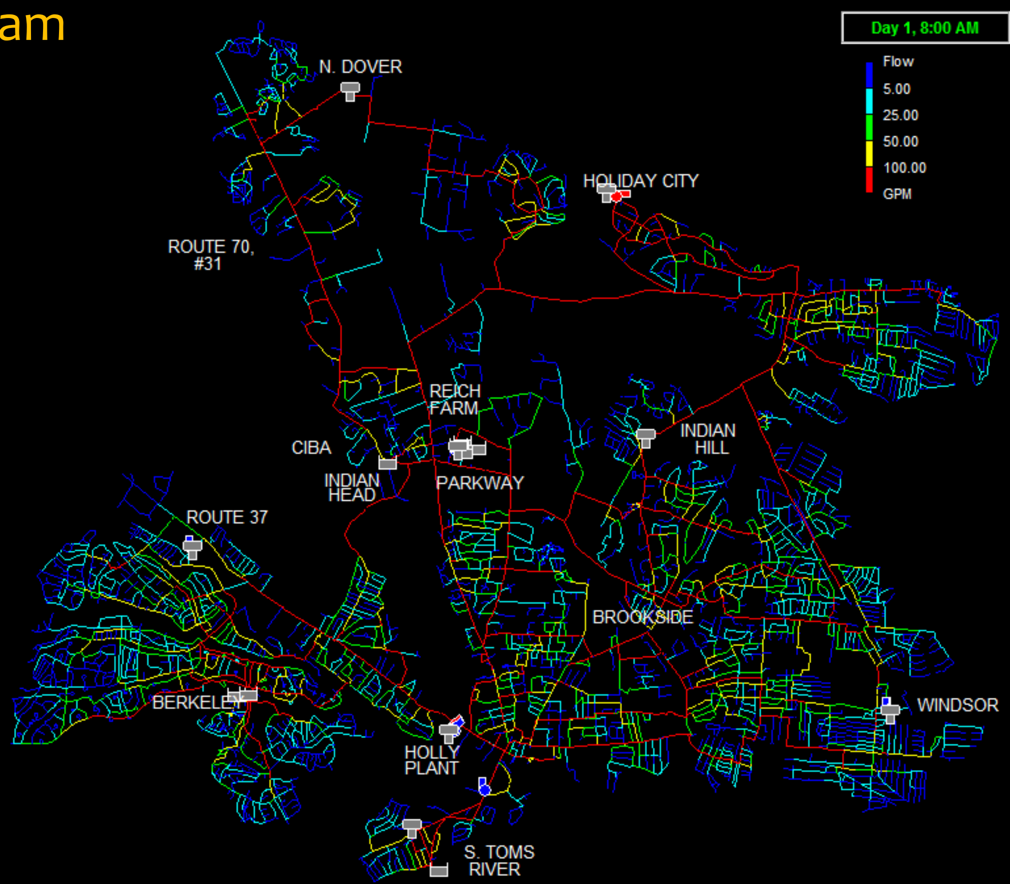
Flow simulation – 2am



Sela et al (2008)

Dynamic complex large-scale nets

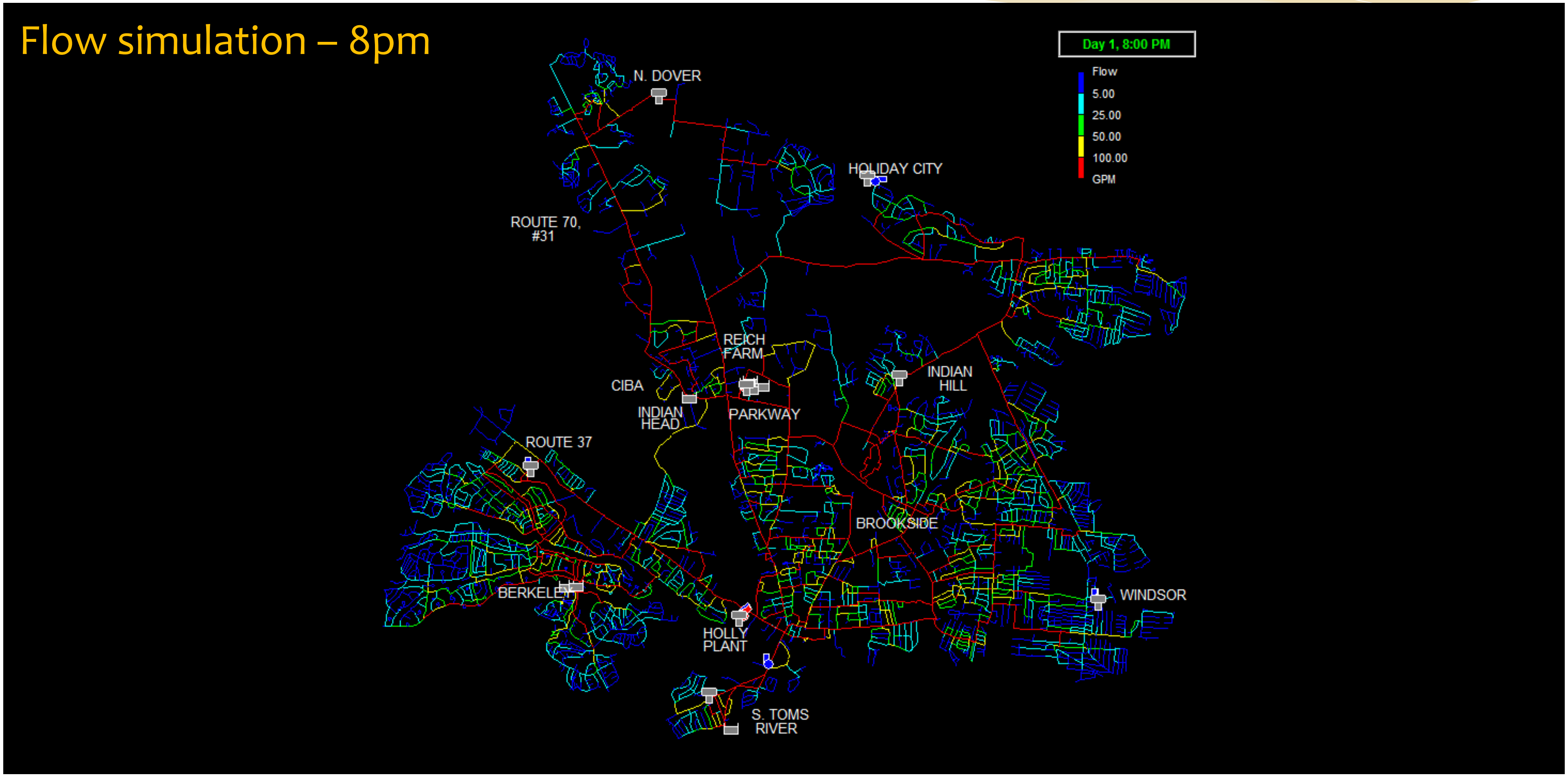
Flow simulation – 8am



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Sela et al (2008)

Dynamic complex large-scale nets



Sela et al (2008)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Failures in Water Nets

Pressurized pipeline flows

Gignac Le canal victime d'actes de vandalisme à répétition

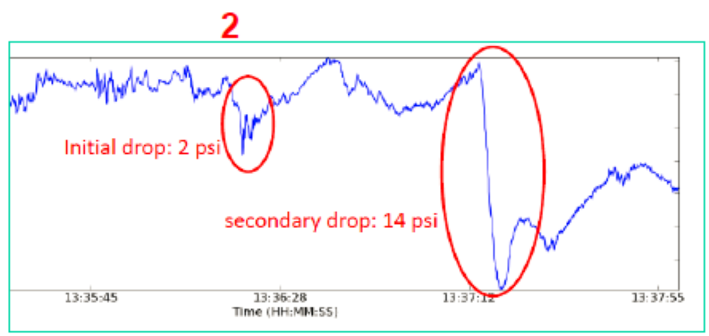
Depuis le 21 juin, le canal de Gignac est victime d'actes malveillants sur l'ouvrage de l'aqueduc de l'Aurelle (derrière le lagunage de Popian) : effondrement du radier du canal puis dégradation des réparations mises en place (retrait des boulots de serrage, mettant gravement en péril la pérennité de l'aqueduc).
L'ouvrage de l'Aurelle permet la continuité du transport de l'eau vers les parcelles du périmètre irrigué situé sur les communes de Pouzols, Le Pouget, Tressan et Puilacher, soit près de 900 ha, pour lesquels l'apport d'eau estival est essentiel.
Ces agissements ont fait l'objet de constats par les brigades de gendarmerie et de plaintes contre X. Il est à noter que l'intégralité du patrimoine de l'Association syndicale autorisée du canal de Gignac est un ouvrage public, dont la destruction, la dégradation ou la détérioration peuvent faire l'objet de poursuites et être punies de trois ans d'emprisonnement et de 45 000 € d'amende.

Open channel flows

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Failures in Water Nets

Event detection from multiple data streams



Whittle A. J. (2012)

Failures in Water Nets

Problem description:

1. 90% of the leaks are nonvisible, buried underground, hard to detect.
2. Catastrophic damage from pipe burst – damage to infrastructure (water, roads, sewer, telecommunication), isolation of consumers.
3. High cost reactive maintenance – taken out of operation for repair.

Enhancing physical reliability: re-active approach

1. Detection of bursts events.
2. Localization of source of the event.
3. Response to failure events.

Enhancing physical reliability: pro-active approach

1. Assessing vulnerability of the network.
2. Operational changes for cost effective reliability.

Vulnerability Assessment

1. Assess **vulnerability** of the distribution system.
2. Characterize **attacker** – vandalism, theft, terrorism.
3. Identify security measures of the **defender** – operational changes.
4. Determine adversary's **attack strategy** based on available information about the system and budget constraints.
5. Determine defender's **security strategy** based on threats and security measures.
6. **Game theoretic** tools to model interactions between attacker and defender and identify optimal strategies.
7. **Interdiction models** (Stackelberg game) of attacker-defender interactions.
8. Extension to **simultaneous** play strategic games.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Vulnerability Assessment

Optimal distribution problem

$$\underset{x}{\text{minimize}} \quad \sum_{j \in A} \int_0^x \phi(t)\, dt$$

$$\text{subject to} \quad \sum_{j \in A} e(i,j)\, x(j) = b(i) \qquad \forall i \in N$$

$$0 \le x(j) \le u(j) \qquad \forall j \in A$$

x – water flow,
b – supply/demand
e– connectivity matrix
u – capacity
$\phi(x)$ – flow cost function
N – set of nodes
A – set of links

Set flow cost as $\phi(x) = \Delta h(x) = Rx^e$ the nonlinear headloss function (potential drop) and $R(D,L,C)$ pipe's conductance as a nonlinear function of its diameter, length, and friction.

The solution of the network equilibrium problem (Kirchhoff's laws I&II) satisfies the KKT conditions of the optimal distribution problem, where the Lagrangian multipliers represent nodal heads.

Vulnerability Assessment

Nonlinear network interdiction formulation

Network interdiction problems has been studied extensively in the context of maximum flow/shortest path mainly with transportation and supply applications using linear cost-flow models (Alderson et al 2013).

$$\underset{z}{\text{maximize}} \begin{Bmatrix} \underset{x}{\text{minimize}} & \sum_{j\in A}\int_0^x \phi(t,z)\,dt + \sum_{i\in N}\psi\big(x(i)-b(i)\big) & \\ \text{subject to} & \sum_{j\in A} e(i,j)\,x(j) \ge b(i) & \forall i\in N \\ & 0 \le x(j) \le u(j) & \forall j\in A \end{Bmatrix}$$

$$\sum_{z\in A} z(j) \le N_z$$

$$z\in\{0,1\}$$

Defender model

x – water flow,
b – supply/demand
e – connectivity matrix
u – capacity
$\phi(x)$ – flow cost function
N – set of nodes
A – set of links

Attacker model

z – attack on a link
N_Z – attacker budget
$\psi(x)$ – dissatisfaction function of undelivered demand

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Vulnerability Assessment

Research plan:

Find efficient solution techniques for the nonlinear network interdiction problem

Incorporate dynamics of the water distribution system in the network interdiction problem.

Model more realistic failure/attack strategies. For example, partial link interdiction, node interdiction, contaminant intrusion.

Model more realistic operator/defender strategies. For example, segment isolation (cluster of pipes) instead of single link, detection and localization capabilities of the attack.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS