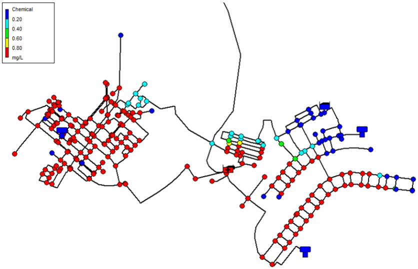
# Synergistic Security for Smart Water Networks: Redundancy, Diversity, and Hardening

Aron Laszka, Waseem Abbas
Yevgeniy Vorobeychik, Xenofon Koutsoukos

VANDERBILT UNIVERSITY

April 21, 2017

# Motivation



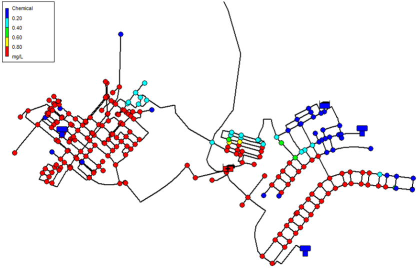

An adversary **attacks** a water distribution network

- by introducing contaminants.
- by disabling sensing devices.

A network can be made **resilient** against attacks by

- by adding more sensors,
- by introducing different types of sensing devices,
- by increasing protection & security of devices.

# Motivation




An adversary **attacks** a water distribution network

- by introducing contaminants.
- by disabling sensing devices.

A network can be made **resilient** against attacks by

- by adding more sensors,
- by introducing different types of sensing devices,
- by increasing protection & security of devices.

What is the **most effective** strategy to make the network resilient against such attacks?

# Contributions

- Cyber-physical attacks in smart water-distribution network.
- To improve resilience against attacks, an optimal defense strategy that combines
  - redundancy, diversity, and hardening approaches.
- Models
  - System model, security investment model, and cyber-physical attack model.
- Problem formulation
- Preliminary results and numerical evaluation

# Cyber-Physical Attack in Smart Water-Distribution Network

**Physical attack**

- Contaminating drinking water
- Example: during the 2016 Olympic games, a terrorist group planned a *biochemical attack* on a water-reservoir.

**Cyber attack**

- Disabling network monitoring system
- Example: disabling sensor devices.

Even without attacks, providing clean drinking water is critical for public health and safety.

# Redundancy, Diversity, and Hardening

## Redundancy

- example: deploying additional sensor devices.
- adversary has to compromise more devices.

## Diversity

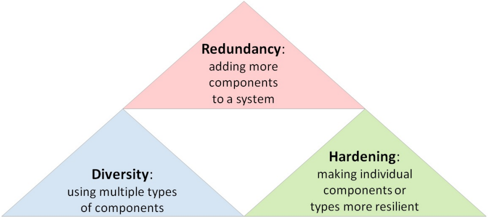
- example: using multiple software/hardware platforms.
- single, common vulnerability cannot be exploited to compromise all devices.

## Hardening

- example: penetration testing, vulnerability discovery for platforms and tamper resistant hardware for devices.
- devices are harder to compromise for adversary.

# Optimal Strategy to Resilience

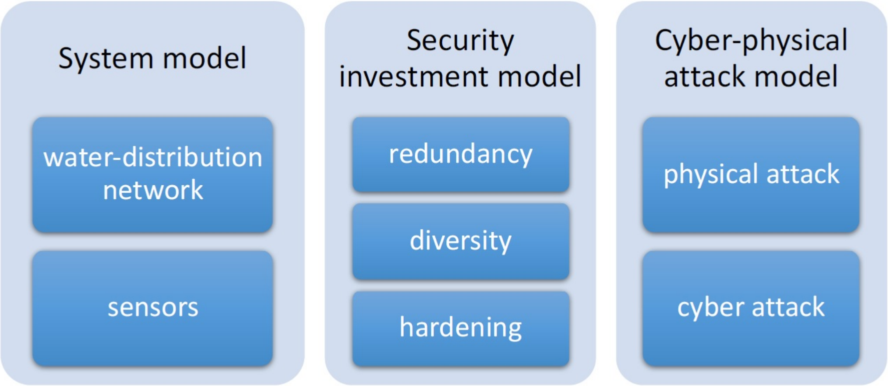
- Each of these approaches has been extensively studied in isolation.
- Example: sensor placement, investment into software security etc.




**Optimal Strategy**

How to combine canonical approaches optimally to improve network resilience against attacks?

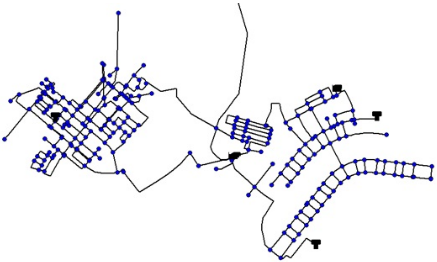
# Model


System model
water-distribution network
sensors
Security investment model
redundancy
diversity
hardening
Cyber-physical attack model
physical attack
cyber attack

# System Model

**Water network** $G(V, E)$

- links $E$ model pipes
- nodes $V$ model junctions of pipes, reservoirs, tanks, consumers, etc.
- every consumer node $v$ has a water-consumption value $U_v$

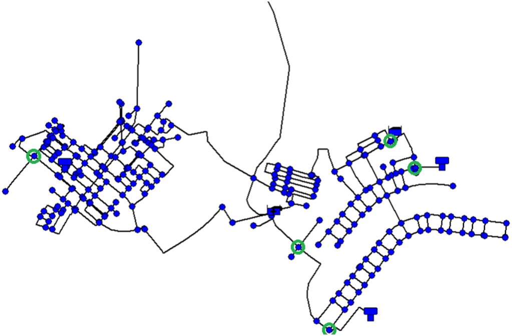


**Sensor devices** $S$

- each sensor $s \in S$ is deployed at node $l_s \in V$,
- every sensor continuously monitors the water at its node, and raises an alarm when the concentration of a contaminant reaches a threshold level $\tau$.

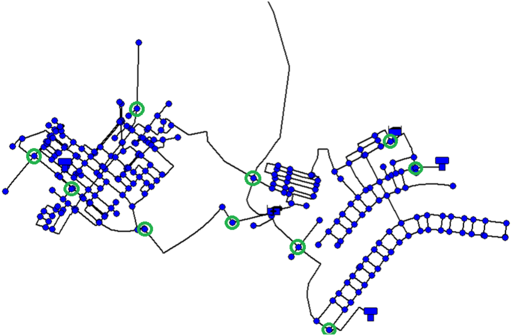
# Security Investment Model – Redundancy

- Minimum number of sensors (for adequate monitoring without attacks) $= S_{min}$
- Level of redundancy: $R = |S| - S_{min}$
- Redundancy investment $= C_R \cdot R$



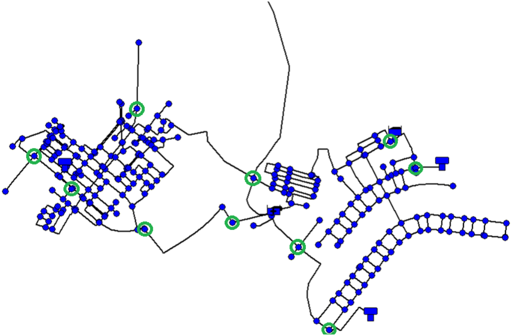
# Security Investment Model – Redundancy

- Minimum number of sensors (for adequate monitoring without attacks) $= S_{min}$
- Level of redundancy: $R = |S| - S_{min}$
- Redundancy investment $= C_R \cdot R$



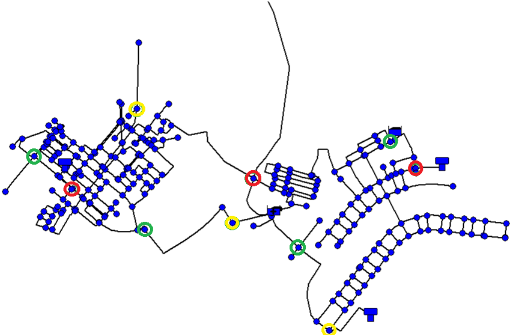
# Security Investment Model – Diversity

- Set of implementation types of sensors $= T$
- Implementation type of sensor $s$ is $t_s \in T$.
- Level of diversity: $D = |T| - 1$
- Diversity investment $= C_D \cdot D$



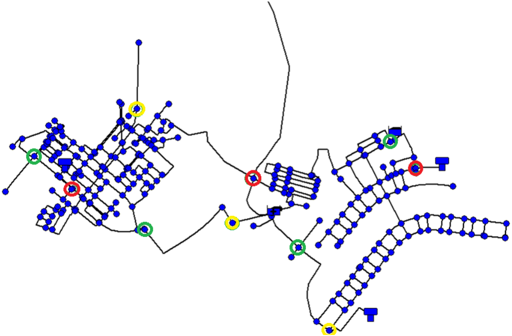
# Security Investment Model – Diversity

- Set of implementation types of sensors $= T$
- Implementation type of sensor $s$ is $t_s \in T$.
- Level of diversity: $D = |T| - 1$
- Diversity investment $= C_D \cdot D$



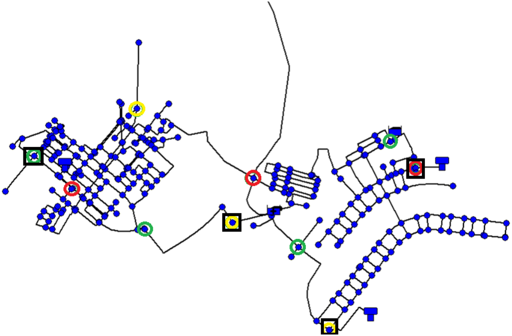
# Security Investment Model – Hardening

- Investment into hardening implementation type $t$ is $h_t$.
- Investment into hardening sensor $s$ is $h_s$.
- Hardening investment: $H = \sum_{t \in T} h_t + \sum_{s \in S} h_s$



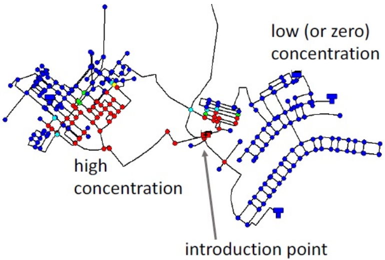
# Security Investment Model – Hardening

- Investment into hardening implementation type $t$ is $h_t$.
- Investment into hardening sensor $s$ is $h_s$.
- Hardening investment: $H = \sum_{t \in T} h_t + \sum_{s \in S} h_s$



# Physical-Attack Model

- **Water-supply contamination**
  - adversary can introduce a contaminant at one of the introduction points $P$
  - discrete-time spread model: from introduction point $p \in P$, after $n$ time steps, the concentration at node $v$ is $\mathcal{C}_p(n, v)$




- **Detection time $L_p$**

$$L_p(S) = \min \left\{ n \in N \mid \exists s \in S : \mathcal{C}_p(n, l_s) \geq \tau \right\}$$

detection threshold

- **Physical impact $I_p$**

$$I_p(S) = \sum_{n=1}^{L_p(S)} \sum_{v \in V} U_v \cdot \mathcal{C}_p(n, v)$$

water consumption

concentration

# Cyber-Attack Model

- Adversary finds a common vulnerability in implementation type $t \in T$

$$\text{Pr [finding a vulnerability in type t]} = \boldsymbol{V_t \cdot e^{-h_t / C_H^T}}$$

  - all devices of this type are disabled by the adversary
- Adversary compromises each sensor device $s \in S$ with probability

$$\text{Pr [compromising sensor s]} = \boldsymbol{V_s \cdot e^{-h_s / C_H^S}}$$

  - each compromised device is disabled by the adversary
- $S_A$ is the set of sensors that have not been disabled, then

$$\text{Expected impact of cyber-physical attack} = \mathop{\mathbb{E}}_{\boldsymbol{S_A}} \left[ \boldsymbol{I_p(S_A)} \right]$$

# Problem Statement

**Worse-case attack**

adversary mounts worst-case attack

$$\operatorname*{argmax}_{p \in P} \mathop{\mathrm{E}}_{S_A} \left[ I_p(S_A) \right].$$

# Problem Statement

**Decision variables:**

- Set of sensors: $S$
- Set of implementation types: $T$
- For each sensor $s \in S$
  - location $l_s$
  - implementation type $t_s$
  - hardening investment $h_s$
- For implementation type $t \in T$
  - hardening investment $h_t$.

# Problem Statement

**Decision variables:**

- Set of sensors: $S$
- Set of implementation types: $T$
- For each sensor $s \in S$
  - location $l_s$
  - implementation type $t_s$
  - hardening investment $h_s$
- For implementation type $t \in T$
  - hardening investment $h_t$.

**Resulting investments:**

- Redundancy: $R = |S| - S_{min}$
- Diversity: $D = |T| - 1$
- Hardening: $H = \sum_{t \in T} h_t + \sum_{s \in S} h_s$

**Constraint:**

- Investment budget: C

$$C_R \cdot R + C_D \cdot D + H \leq C$$

# Problem Statement

**Decision variables:**

- Set of sensors: $S$
- Set of implementation types: $T$
- For each sensor $s \in S$
  - location $l_s$
  - implementation type $t_s$
  - hardening investment $h_s$
- For implementation type $t \in T$
  - hardening investment $h_t$.

**Resulting investments:**

- Redundancy: $R = |S| - S_{min}$
- Diversity: $D = |T| - 1$
- Hardening: $H = \sum_{t \in T} h_t + \sum_{s \in S} h_s$

**Constraint:**

- Investment budget: C

$$C_R \cdot R + C_D \cdot D + H \leq C$$

## Optimal defense

$$\min_{S, T, \langle l_s, t_s, h_s \rangle_{s \in S}, \langle h_t \rangle_{t \in T}} \max_{p \in P} \mathop{\mathrm{E}}_{S_A} \left[ I_p(S_A) \right]$$

$$\text{subject to, } C_R \cdot R + C_D \cdot D + H \leq C$$

# Preliminary Results

- Finding an optimal defense is computationally hard.

**Problem complexity**

Given a fixed amount of security investment $C$ and a threshold expected impact $K$, determining if there exists a defense that results in expected impact less than or equal to $K$ is an **NP-hard problem**.

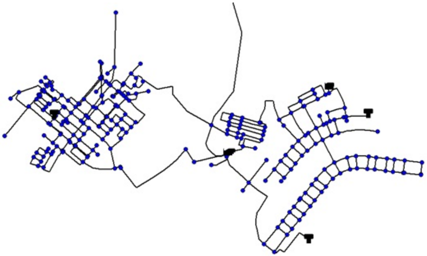
Most variants and subproblems are also computationally challenging.

- We use a greedy heuristic to find placements, type assignments, and distributions of hardening expenditure

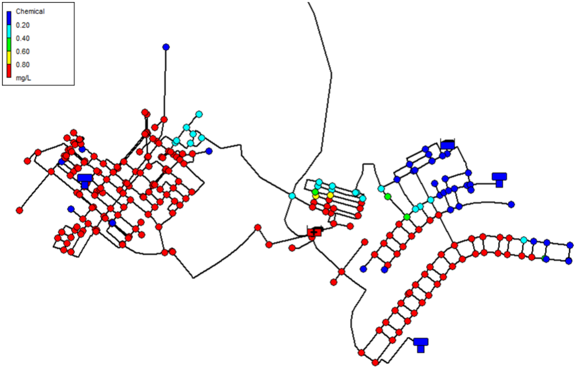
# Numerical Illustration

- Based on a real-world water-distribution network from Kentucky
  - obtained from the Water Distribution System Research Database at uky.edu
  - contains topology and water-demand values

- Simulating physical attacks
  - contaminant may be introduced at one of six nodes $P$ (3 tanks and 3 reservoirs);
  - for each node $p \in P$, we simulated the spread of a contaminant using EPANET (epa.gov/water-research/epanet)



# Simulation Example

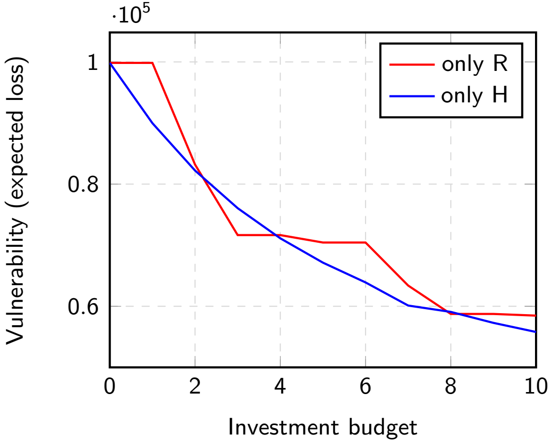


# Numerical Setup

- Physical system parameters
  - topology $G$: from real-world data,
  - contaminant concentrations $\mathcal{C}_p(n, v)$: from simulations,
  - impact $I_p$: from concentrations $\mathcal{C}_p(n, v)$ and real-world data.
- Cyber system parameters
  - to study various combinations of $R$, $D$, and $H$, we let
    minimum number of sensors: $S_{min} = 1$
    cost of hardening types: $C_H^T = 100$
    cost of hardening devices: $C_H^D = 1$.

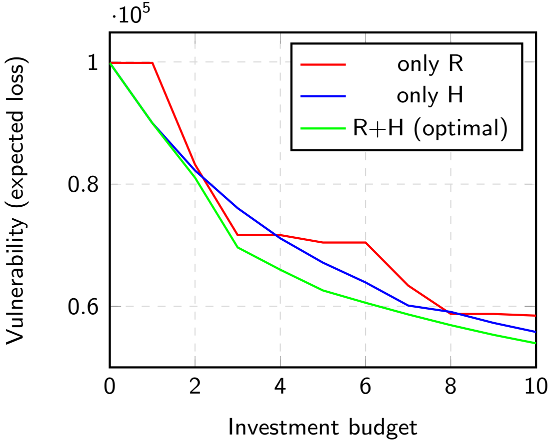
# Numerical Results

**Comparison of security investment strategies**



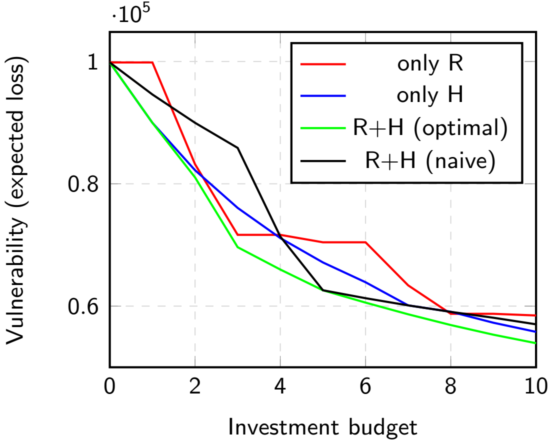
# Numerical Results

**Comparison of security investment strategies**

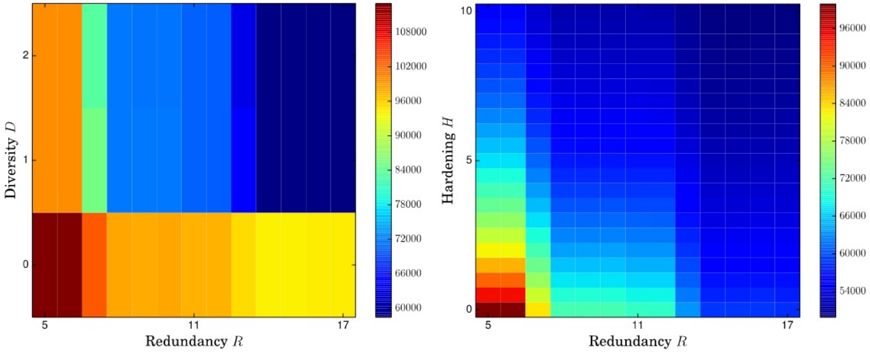


# Numerical Results

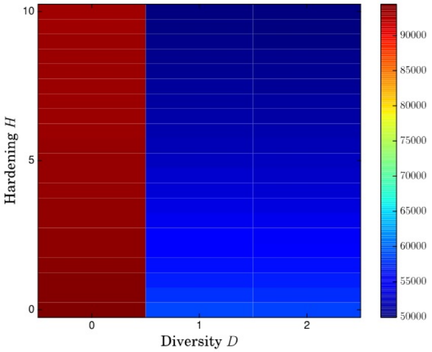
**Comparison of security investment strategies**



# Numerical Results



# Numerical Results contd.



# Conclusions

- Theoretical foundations for studying redundancy, diversity, and hardening in an integrated framework.
- Numerical results show that the three approaches can be significantly more effective when combined.
- Finding optimal defense is computationally challenging.
- **Future work**
  - consider a wider range of CPS (e.g., smart grids, transportation networks).
  - provide efficient algorithms for finding optimal defense.
  - establish general principles for secure and resilient CPS design.

## Acknowledgments

- National Science Foundation (CNS-1238959)
- Air Force Research Laboratory (FA 8750-14-2-0180)

# Thank You