A Case Study of a Systematic Attack Design Method for Critical Infrastructure Cyber-Physical Systems

David Grimsman

Brigham Young University

July 6, 2016

American Control Conference, Boston, MA

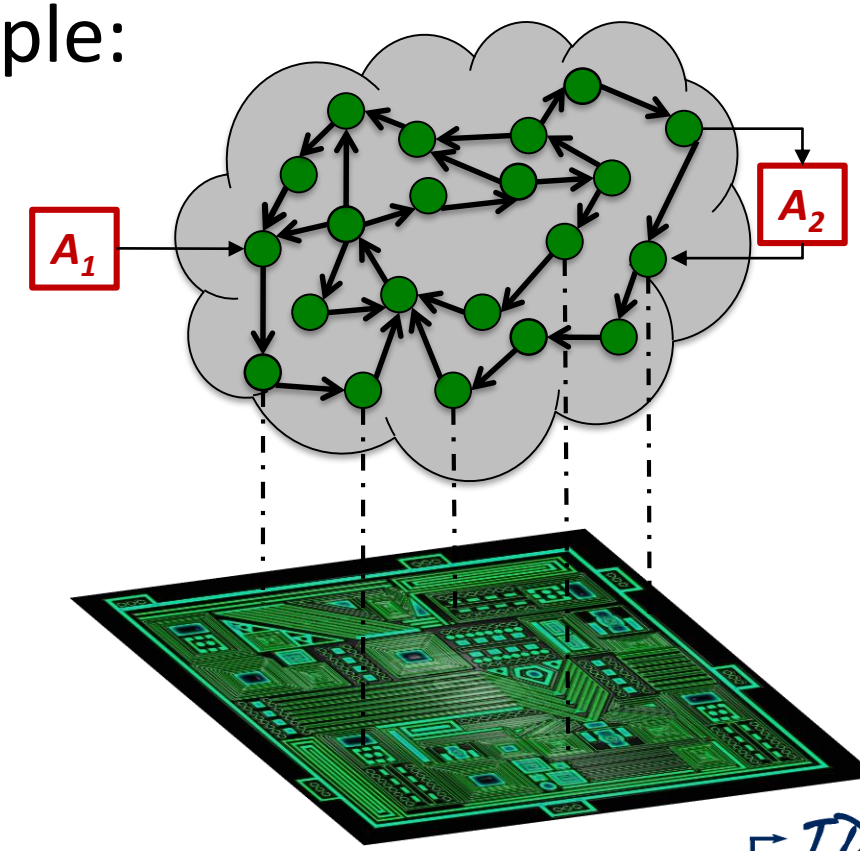
IDeA Labs

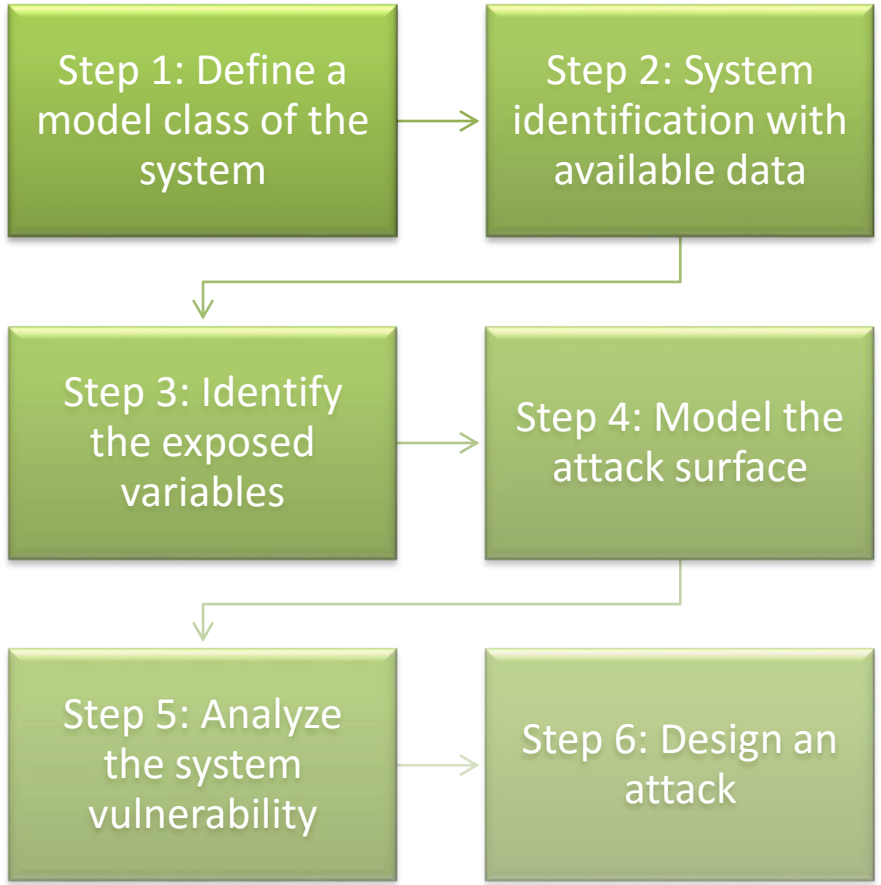
Information & Decision Algorithms Laboratories

Attack Design Methodology

Concerned with physical consequences

Example:

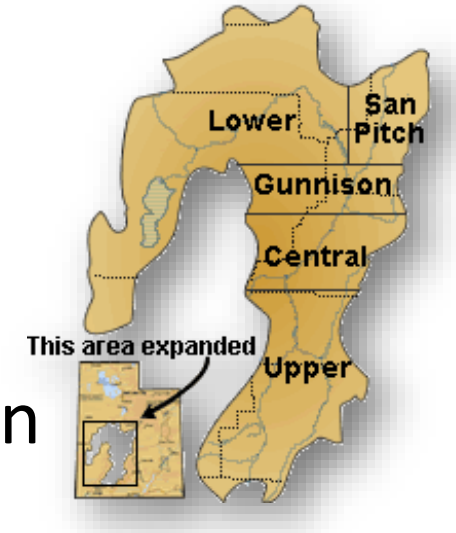




IDeA Labs
Information & Decision Algorithms Laboratories

The Sevier River

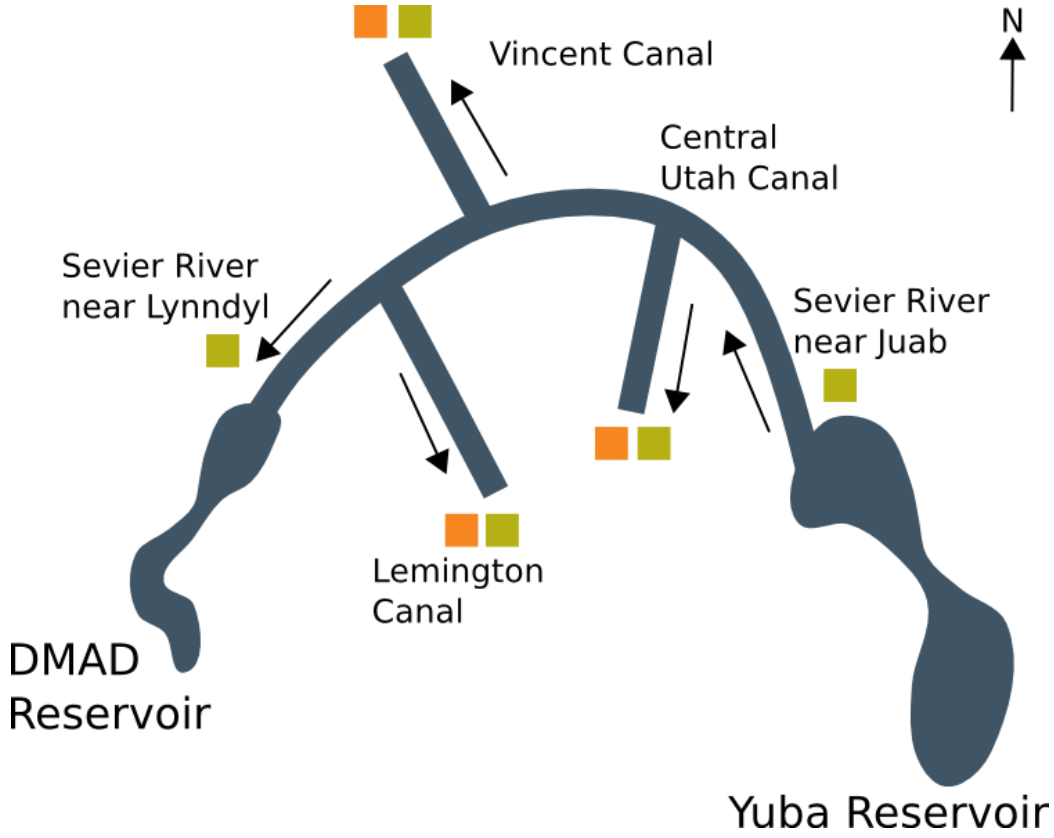
- Runs through Central Utah
- Irrigates over 286,600 acres of farmland – mostly alfalfa
- Has a series of reservoirs
- Farmers request water from canal companies who request it from reservoirs
- **Goal: keep this system safe**
- Destroying even 1 cut per season could cost about **$70 million**



IDeA Labs
Information & Decision Algorithms Laboratories

The Sevier River

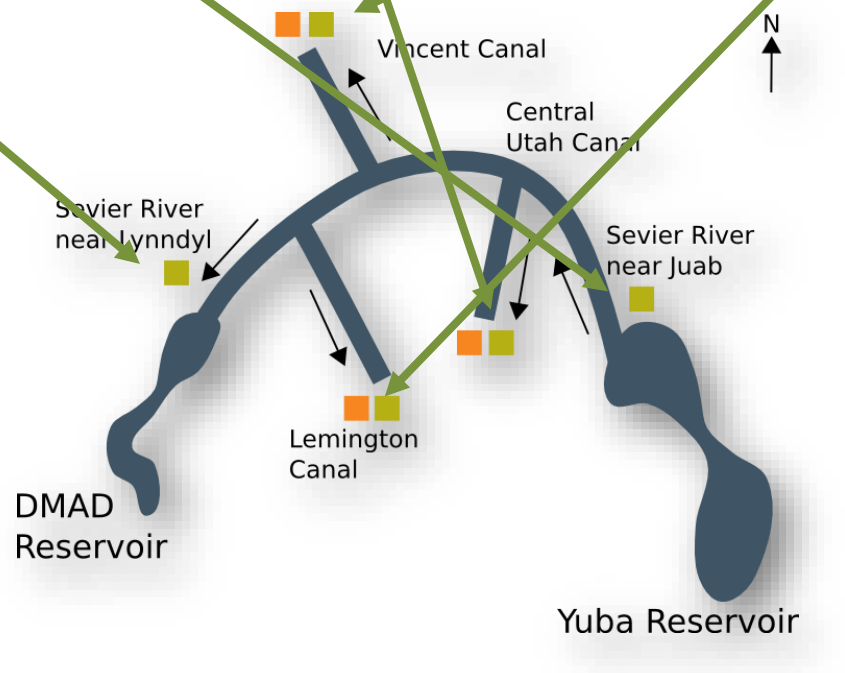
- A small portion of the Sevier River between 2 reservoirs (about 75 mi)
- 3 canals divert water with remotely-controlled gates
- Water commissioner receives requests and releases water accordingly
- Water not diverted empties into DMAD



Step 1: Define a model class of the system

- A simple parameterized mass-balance model
- This model class has been used before on a different section of the river
- The model class is a good choice since sensors are noisy

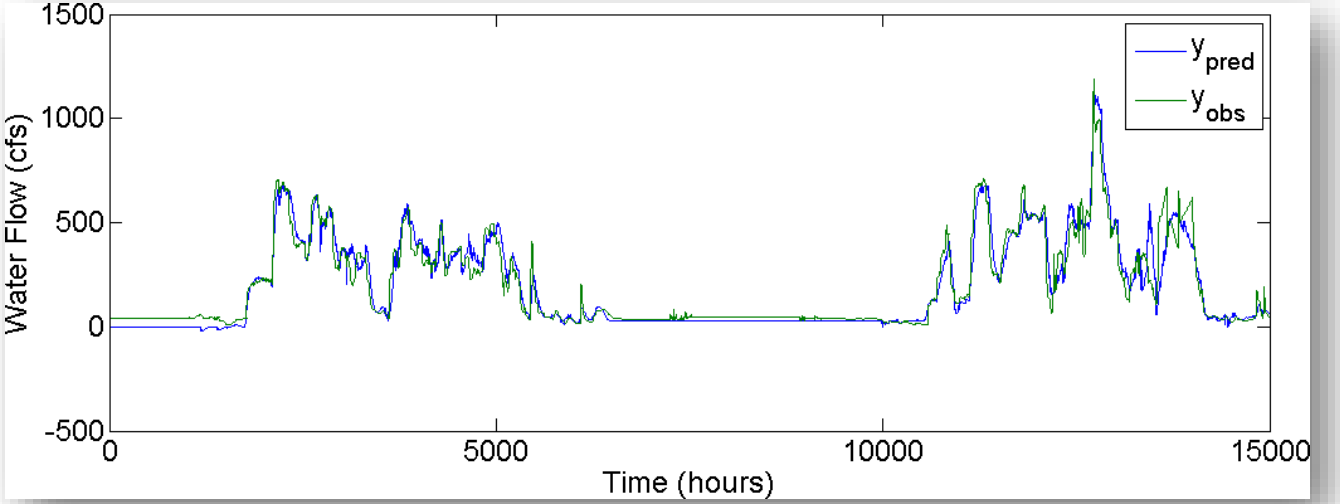
$$y[k] = a_1 w_1[k - l_1] - w_2[k - l_2] - w_3[k - l_3] - w_4[k - l_4]$$



IDeA Labs
Information & Decision Algorithms Laboratories

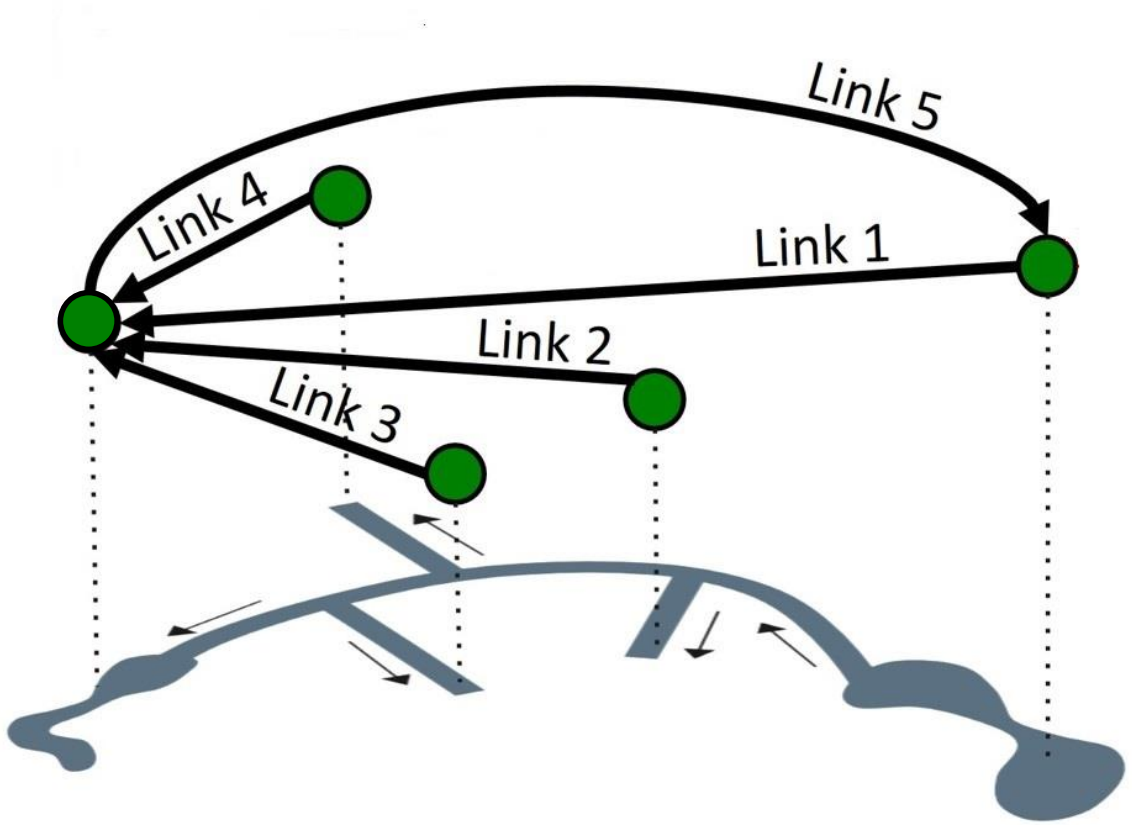
Step 2: System identification with available data

- Use publicly available data from the SRWUA website
  - Gate heights and water flows
- Fit parameters to our mass-balance model using L_1 regression
- Model tested against validation data



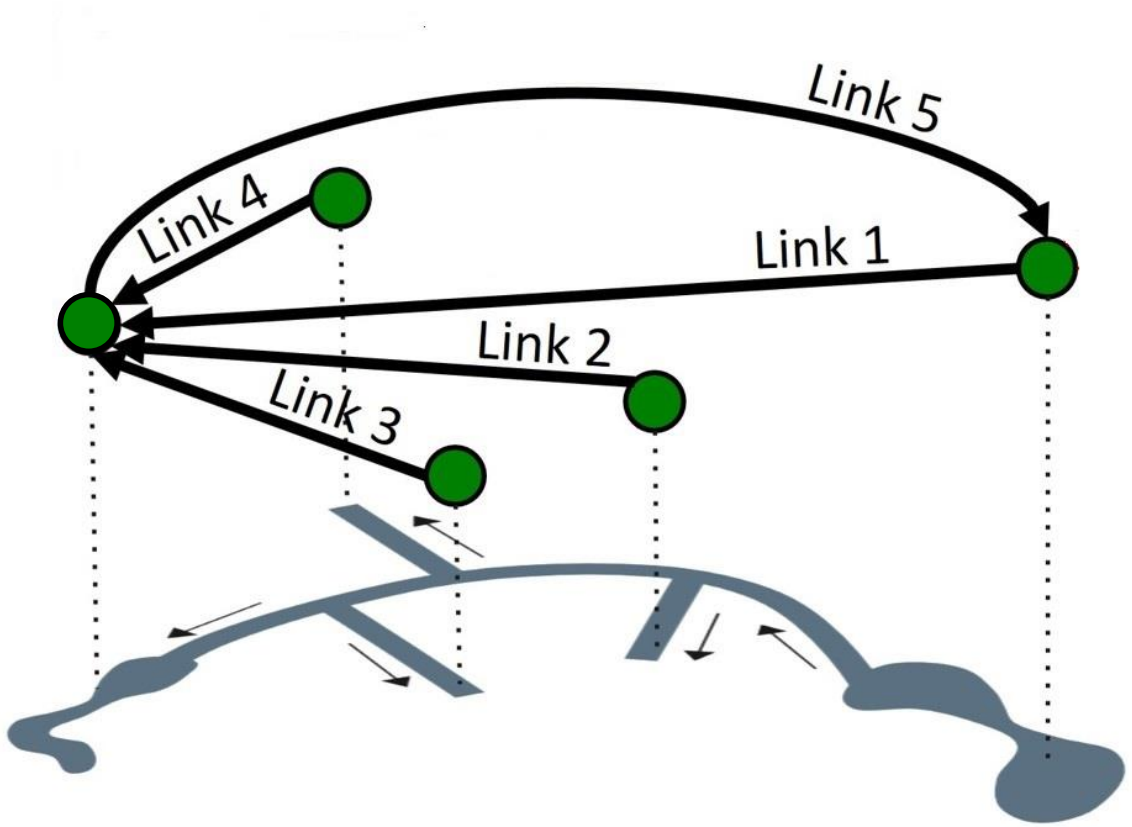
Step 3: Identify the exposed variables

- Variables, or state values, can be considered the water flow at various points along the river
- Exposed variables are those measurements that are publicly available through the SRWUA website



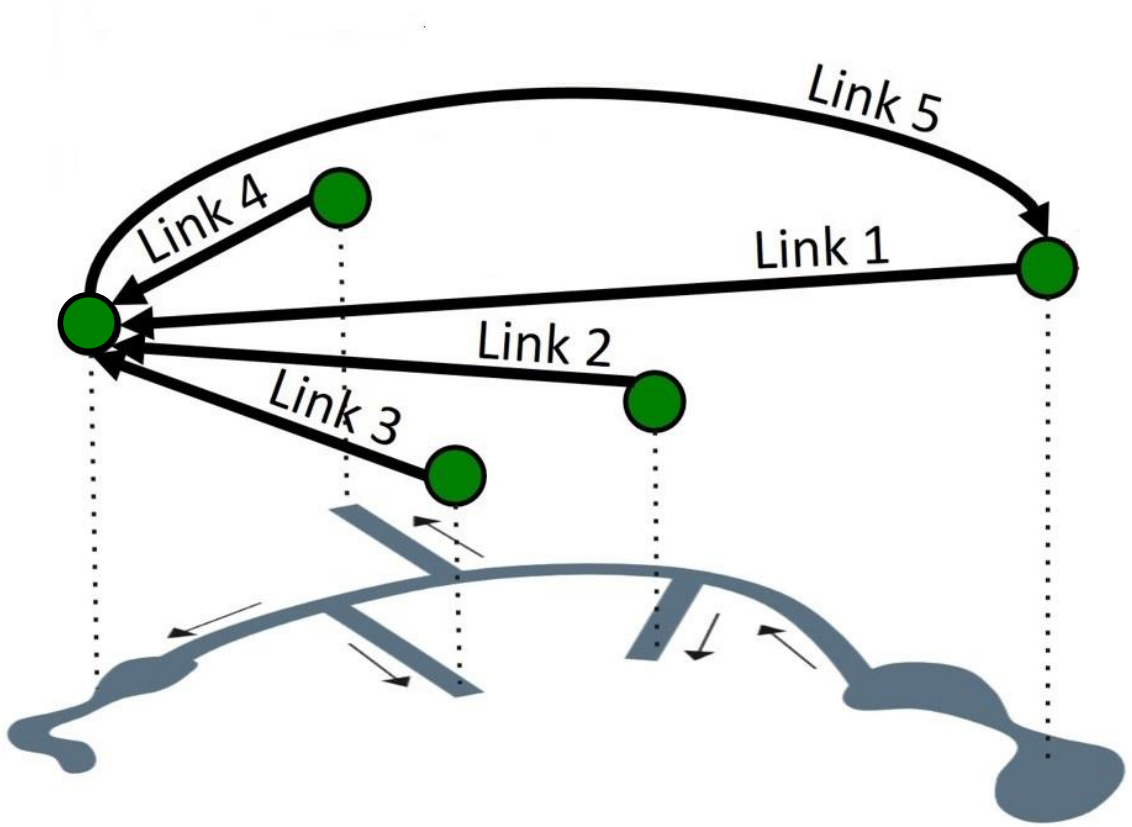
Step 4: Model the attack surface

- Use a signal structure representation, showing how each signal interacts
- In this work, we use the dynamical structure function (DSF)
- The mass-balance model can be converted to a DSF representation



Step 5: Analyze the system vulnerability

- The most vulnerable link is the one with the lowest H_∞ norm
- This is the link where the smallest perturbations can lead to system-wide instability
- Vulnerability is zero on links with not feedback



Step 6: Design Attacks

Downstream manipulation attack (A_m)

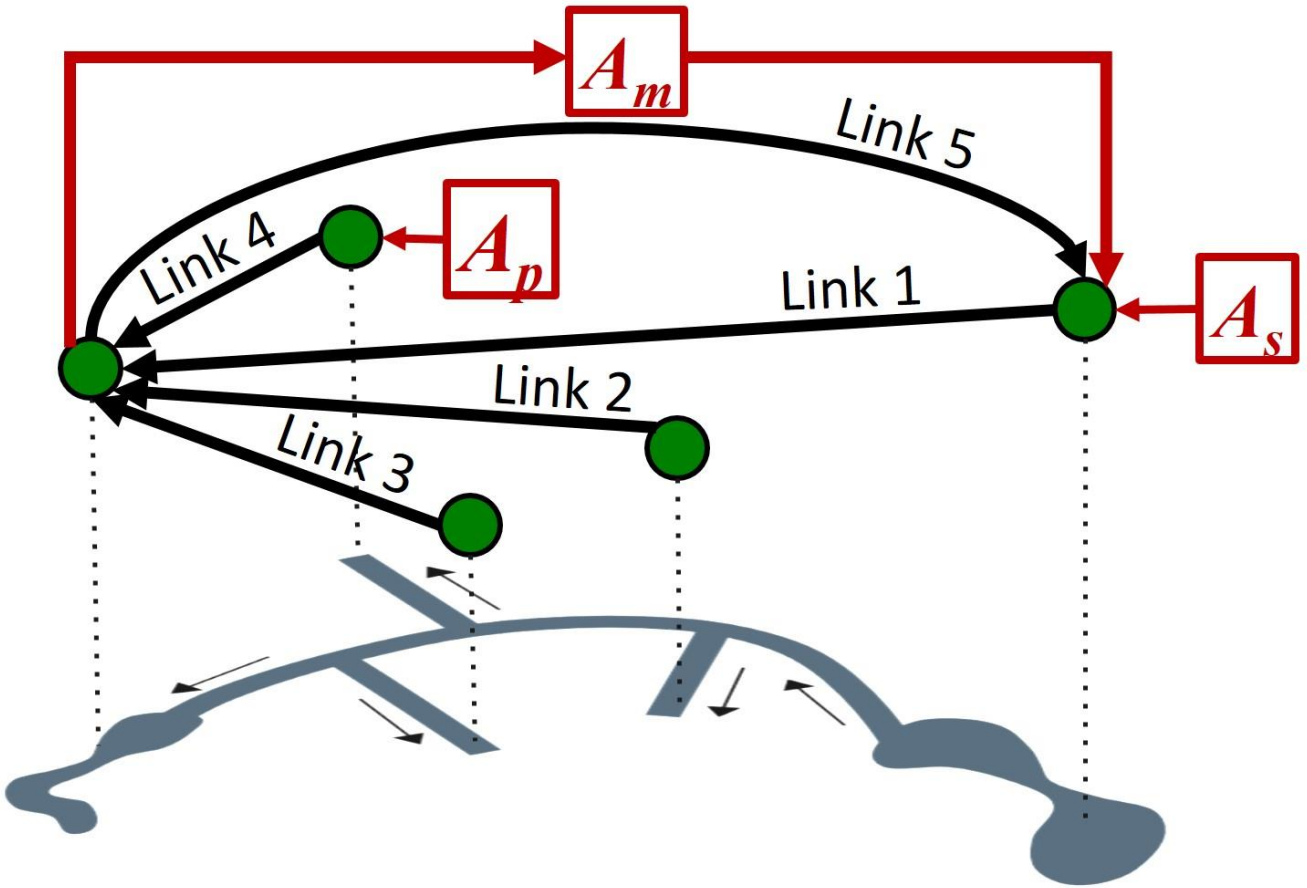
- Manipulate sensor values at bottom reservoir

Physical attack (A_p)

- Tamper with flow sensors at canal heads

Canal request spoofing attack (A_s)

- Intercept SMS requests for water



IDeA Labs
Information & Decision Algorithms Laboratories

Possible countermeasures

Conduct random, unannounced inspections of the sensors used in the canals. This will mitigate damage done using attack A_p.

Secure and encrypt requests from canal companies to the water commissioner. A well-implemented request tool would make attack A_s extremely difficult.

Place redundant sensors along the main river, making only the data from one public. If reported values are too different, an A_m attack could be detected.

Remove critical data from the public website. In the river section studied here, we suggest removing the Lynndyl readings. This would hinder an attacker from creating a useful model.

Future work

- Develop additional attacks using the DSF
- Design attacks specific to other applications
- Develop a visual tool that allows non-experts to identify system vulnerabilities