Real-time Situational Awareness of Risk to EDS To Cyber Attack

Exploring Security Metrics for Electric Grid Networks

Panini Patapanchala, Chen Huo, Rakesh B. Bobba, Eduardo Cotilla-Sanchez

GOALS

- Understand the impact of cyber attacks on EDS operations
- Develop tools for real-time situational awareness of risks to EDS

FUNDAMENTAL QUESTIONS/CHALLENGES

- What sequence of events can lead to catastrophic failures?
- Can such sequences be triggered by cyber attacks?
- Can we design models to study such cyber attack pathways?
- What metrics can be used to describe the difficulty or ease of traversing such pathways?
- Can such metrics be presented to an operator in a meaningful manner?
- Can this analysis be done in real-time?

RESEARCH PLAN

- Modeling and simulations to identify catastrophic failure scenarios
- Develop cyber-physical models that capture cyber-physical dependencies of EDS
- Identify cyber assets potentially linked with failure scenarios
- Develop methodology and algorithms to assess the difficulty or ease of reaching critical cyber assets
- Develop algorithms to assess the risk or compute metrics to indicate the risk of proximity to cyber-attack induced failures

CYBER-PHYSICAL MODELING AND ASSESSMENT

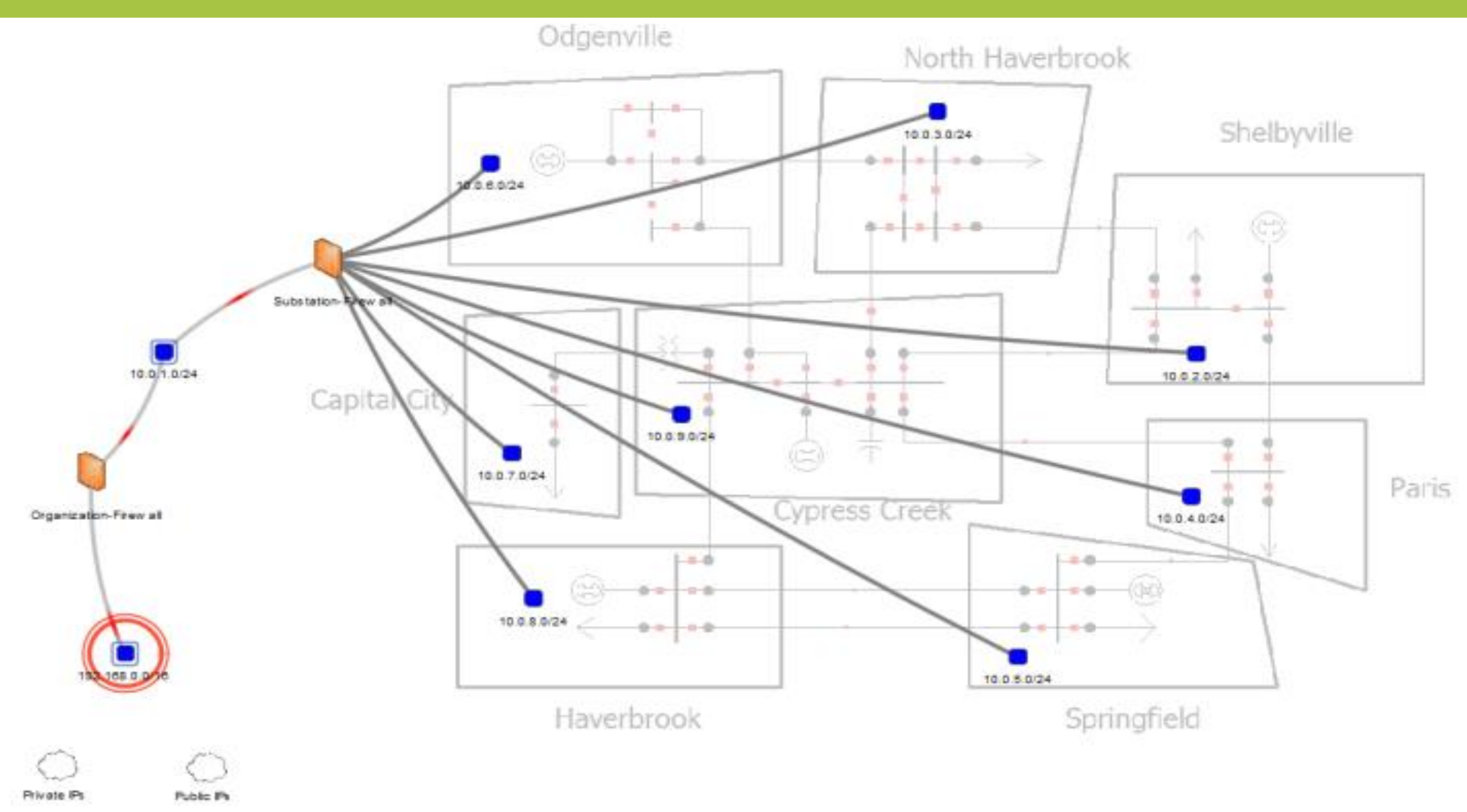
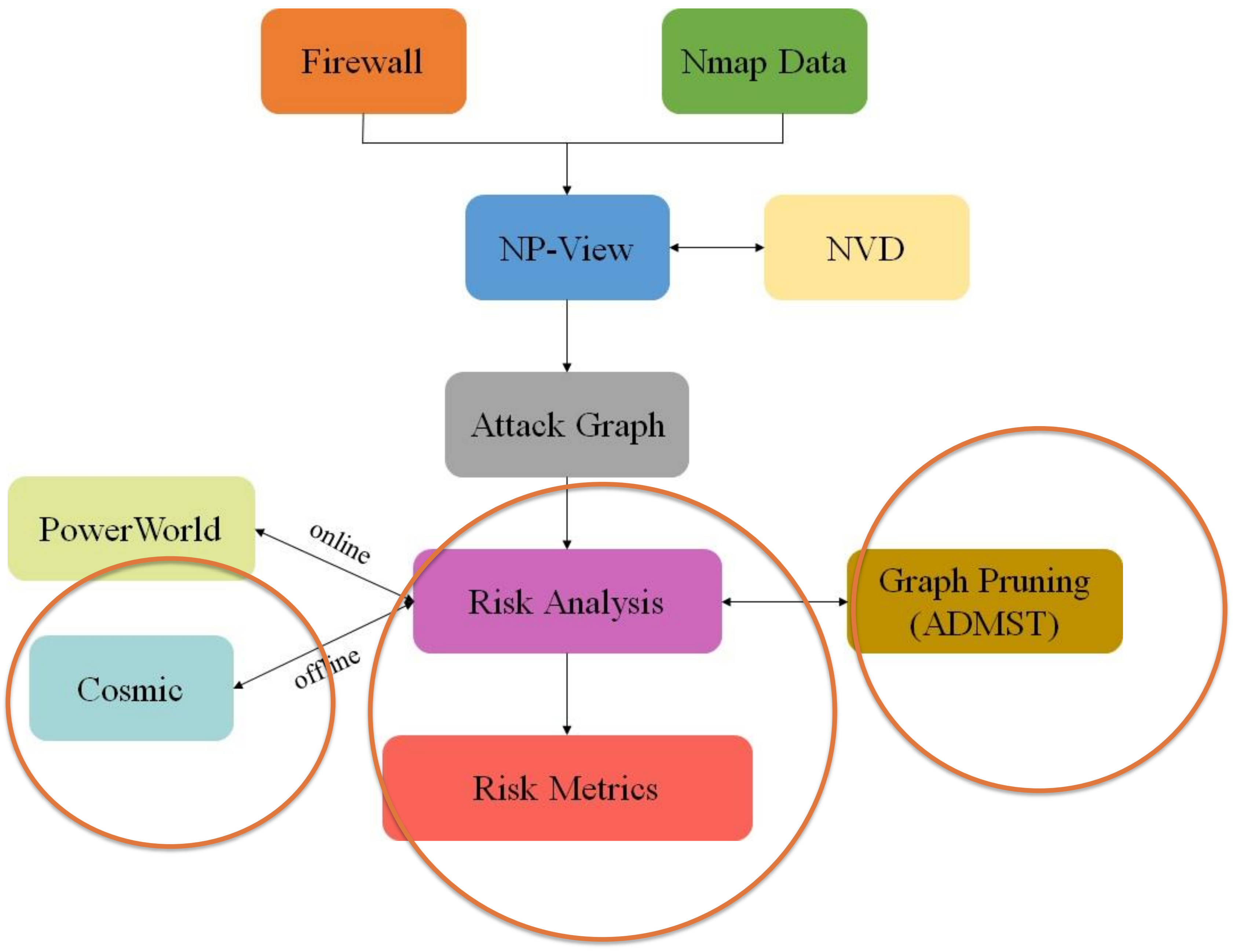


Figure 1: A Sample Cyber-Physical Model

Source: CyPSA Project


Firewall

Nmap Data

NP-View

NVD

Attack Graph

PowerWorld

online

Risk Analysis

Graph Pruning (ADMST)

Cosmic

offline

Risk Metrics

Figure 2: Extended Cyber-Physical Security Assessment (CyPSA) Workflow

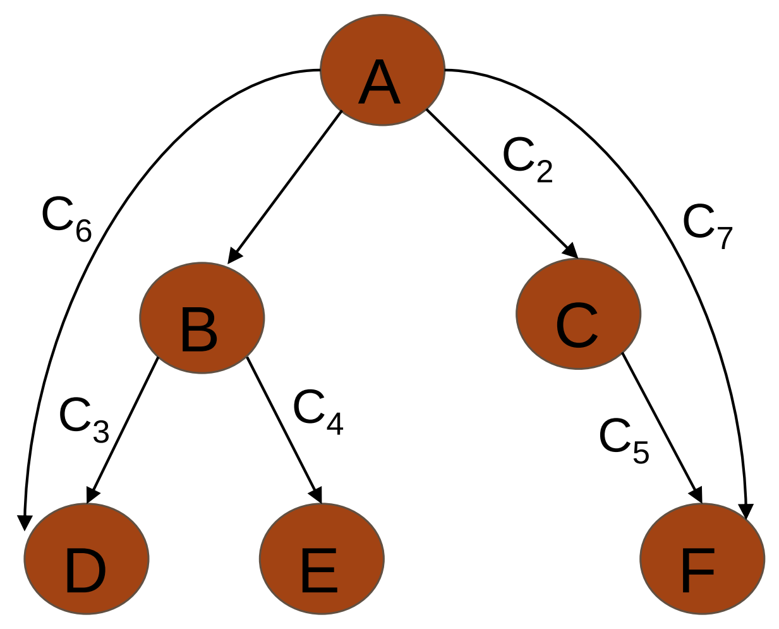
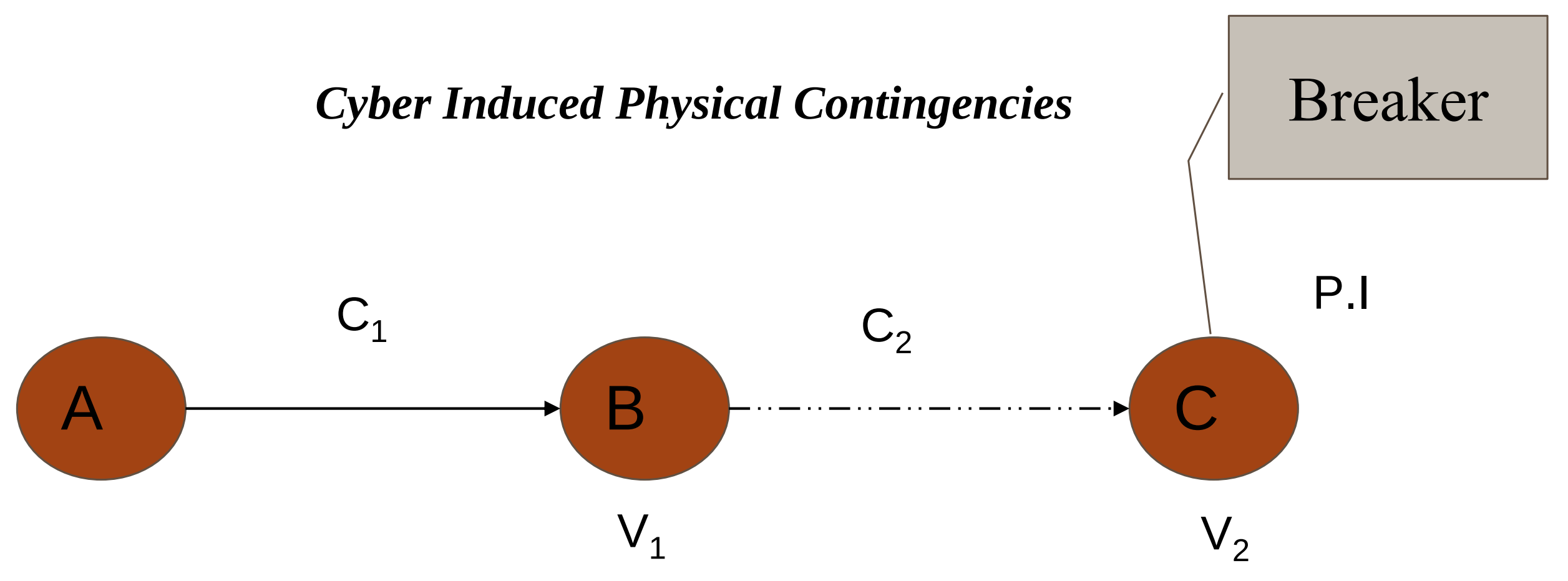


Figure 3: Attack Graph Structure

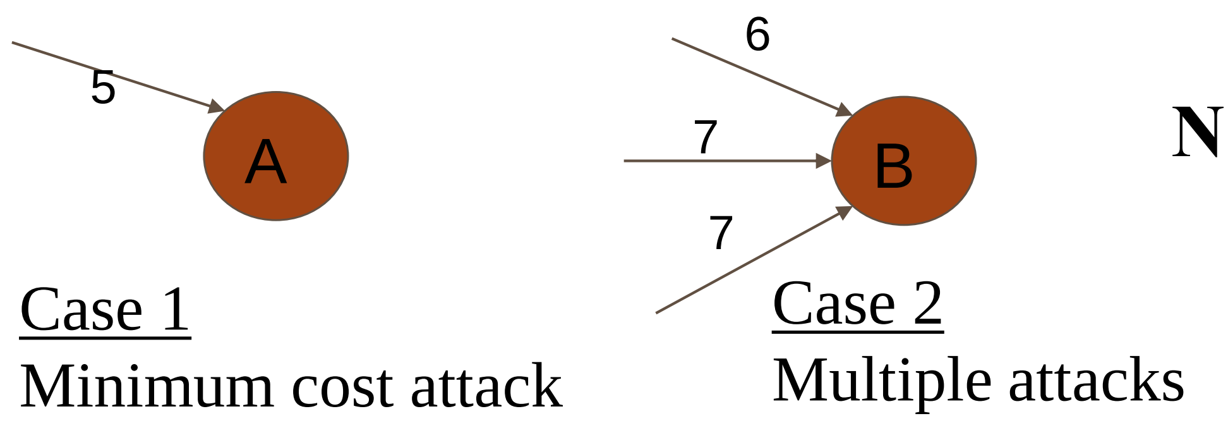
SECURITY METRICS



$$S.I = P.I * \frac{1}{C_1 + C_2}$$

S.I – Security Index of an attack from *A* to *C* through *B*
P.I – Physical impact of losing control of asset *C*
C= C_1+C_2 – path cost to reach asset *C* from a source *A*

Limitations



Need to capture both cases!!

Proposed Graph-Inspired Metrics

- **Target / Asset Metrics**
  - M1 - Minimum cost attack path and impact per target
  - M2 - Number of attack paths, cost and impact per target
- **Intermediate nodes – Stepping stones**
  - M3 - Shortest attack path through the node
  - M4 - All attack paths through the node
- **Attacker / Source**
  - M5 - Attack paths from a source with minimum cost and impact
  - M6 - Number of attack paths, cost and impact per attacker / source
- **Total Security Metric**
  - M7 – Capture overall system exposure
- **Coordinated Attack**
  - M8 - Set of targets, minimum cost paths and associated impact

Example --- M2: Target Node Security Index

$$T.N.S.I_t(i) = P.I_i * \sum_{j \in S} \frac{1}{C_{min_{ji}}}$$

BROADER IMPACT

- If successful, will provide decision support for cyber security investments
- Will help track cyber security improvements
- Will help with real-time cyber security assessment

INTERACTION WITH OTHER PROJECTS

- This work builds on the CyPSA project that was funded by ARPA-E.
- It is related to the following CREDC activities
  - Cyber-resilience metrics being done at Old Dominion
  - Measuring cyber-resiliency activity at WSU
  - Rare event risk estimation work being done at MIT

FUTURE EFFORTS

- Complete Cyber-Physical Model for IEEE 96-RTS system
- Apply the proposed metrics to analyze the IEEE 96-RTS system cyber-physical model
- Find an industry partner to validate the metrics and evaluate their value

RELATED PUBLICATIONS

- Patapanchala, P., Huo, C., Bobba, R., Cotilla-Sanchez, E. “Exploring Security Metrics for Electric Grid Infrastructures Leveraging Attack Graphs.” IEEE Conference on Technologies for Sustainability (SusTech), 2016.
- Weaver, G. A., Davis, K., Davis, M., Rogers, E. J., Bobba, R. B., Zonouz, S. A., Berthier, R., Sauer, P. W., Nicol, D. M. “Cyber-Physical Models for Power Grid Security Analysis: 8-Substation Case.” IEEE International Conference on Smart Grid Communications (SmartGridComm), Sydney, Australia, 2016, pp. 140-146.
- Davis, K.R., Davis, C.M., Zonouz, S.A., Bobba, R.B., Berthier, R.A., Garcia, L. and Sauer, P.W., "A Cyber-Physical Modeling and Assessment Framework for Power Grid Infrastructures," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2464 - 2475, Sep. 2015.

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY