CPS: Synergy: Collaborative Research: Threat-Assessment Tools for Management-Coupled Cyber and Physical Infrastructures

Senior Investigators: **Sandip Roy, Hans Van Dongen, Ali Mehrizi Sani, and Adam Hahn, Washington State University; Yan Wan, University of Texas at Arlington; Sajal Das, Missouri University of Science and Technology**

Students/Postdocs: **Amirkhosro Vosughi, Samantha Riedy, Ali Tamimi, Shameek Bhattacharjee**

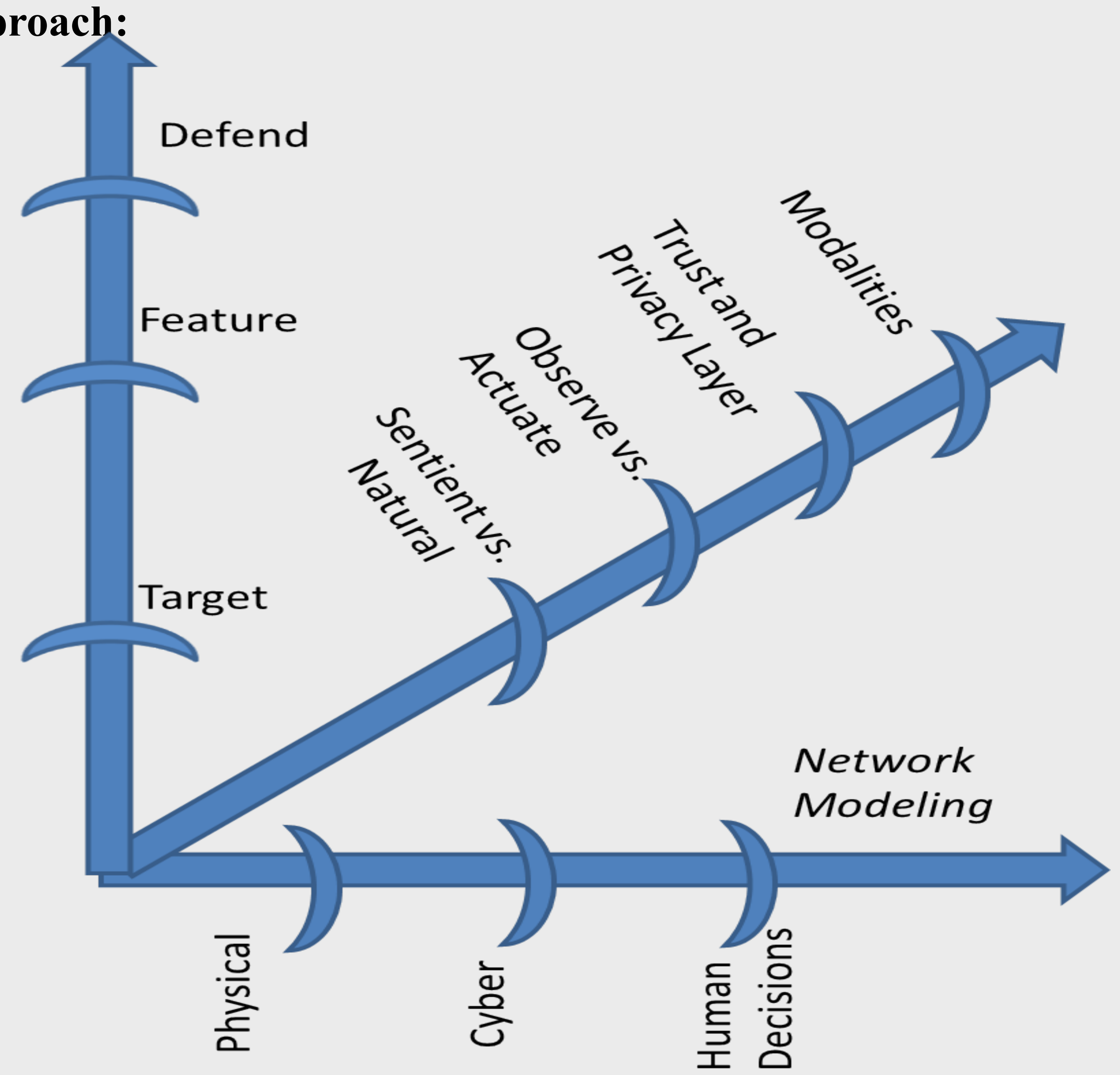
Synopsis

Context: Decision-making in infrastructures often involves human operators, who are sandwiched between cyber and physical assets.

Goal: To develop a threat-assessment framework for these *Management-Coupled Cyber- and Physical- Infrastructures (MCCPIs).*

Application: strategic air traffic management**.**

Approach:



Full Project Period: 9/1/2015-8/31/2018.

Outcomes for the second project year (FY17):

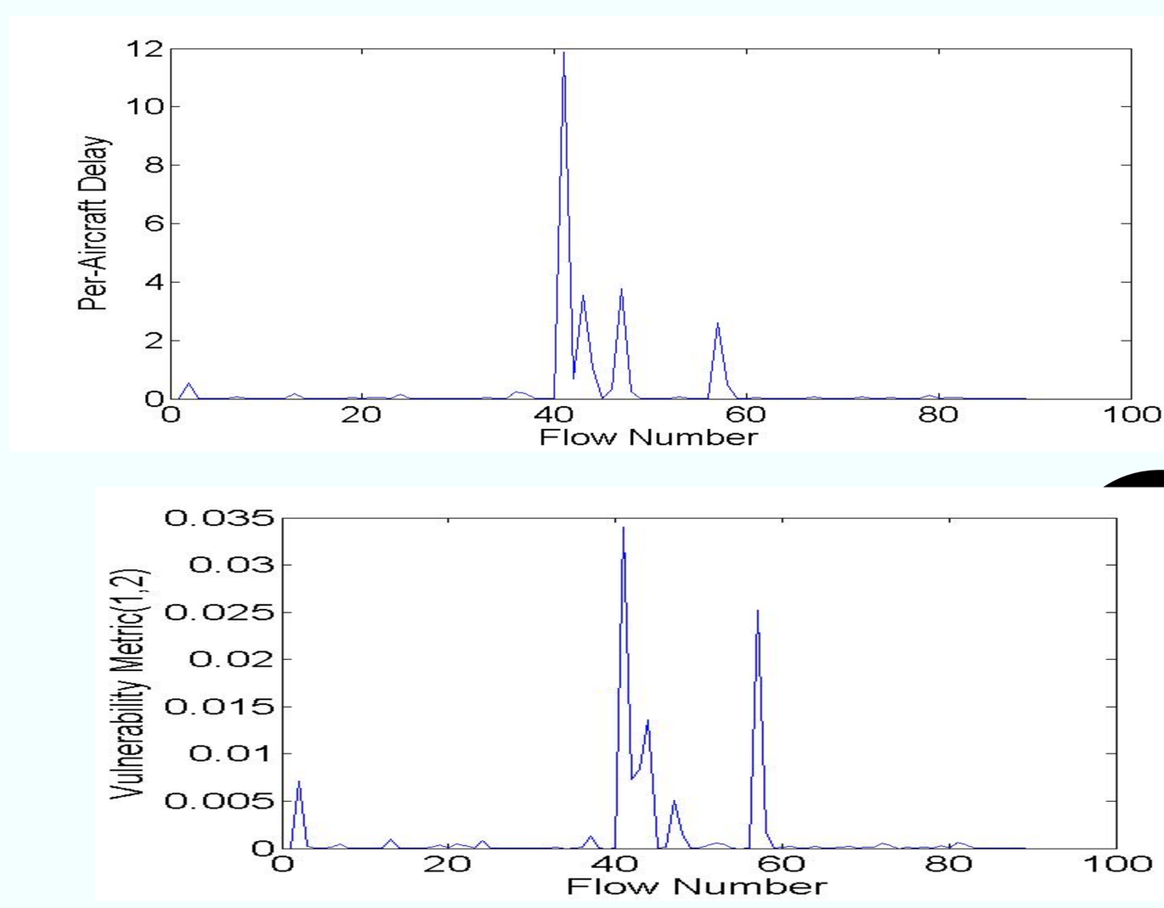
1) Global vulnerability metrics for MCCPIs.
2) Detailed modeling of cyber-threat impacts on air traffic.
3) Human decision-making modeling.
4) Trust modeling
4) 15+ publications in the aviation, control systems, and cyber-physical systems literatures.
5) Presentations and initial technology transfer to NASA, DHS, and FAA.
6) Training of students and postdoctoral researchers.
7) Exploratory application to IoT.

Sample Publications

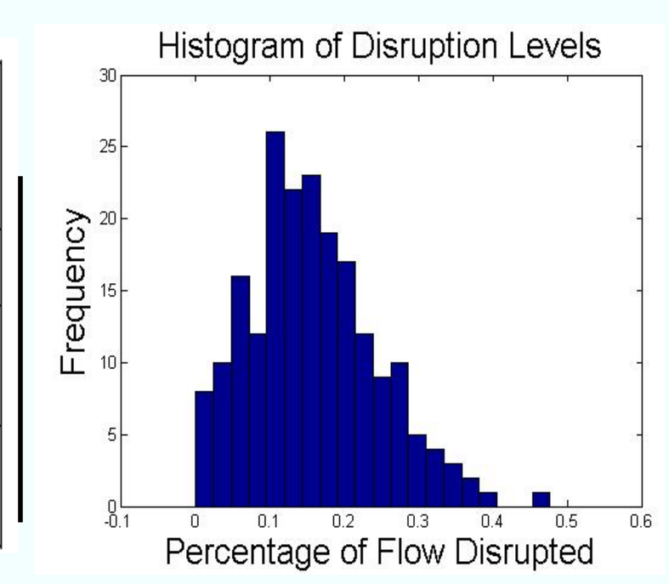
- S. Roy, M. Xue, and B. Sridhar, ``Vulnerability metrics for the airspace system," in *Proceedings of the 2017 FAA/Eurocontrol Air Traffic Management R&D Seminar*, Seattle, WA.
- . J. Abad Torres and S Roy, ``Dominant eigenvalue minimization with trace-preserving diagonal perturbation: subset design problem," to appear in *Automatica.*

Vulnerability Metrics: A Global View

- Defined a network metric for the vulnerability of a traffic flow
  - Agnostic to the source of the disruption (cyber, physical, or human).
  - Captures "ripple".

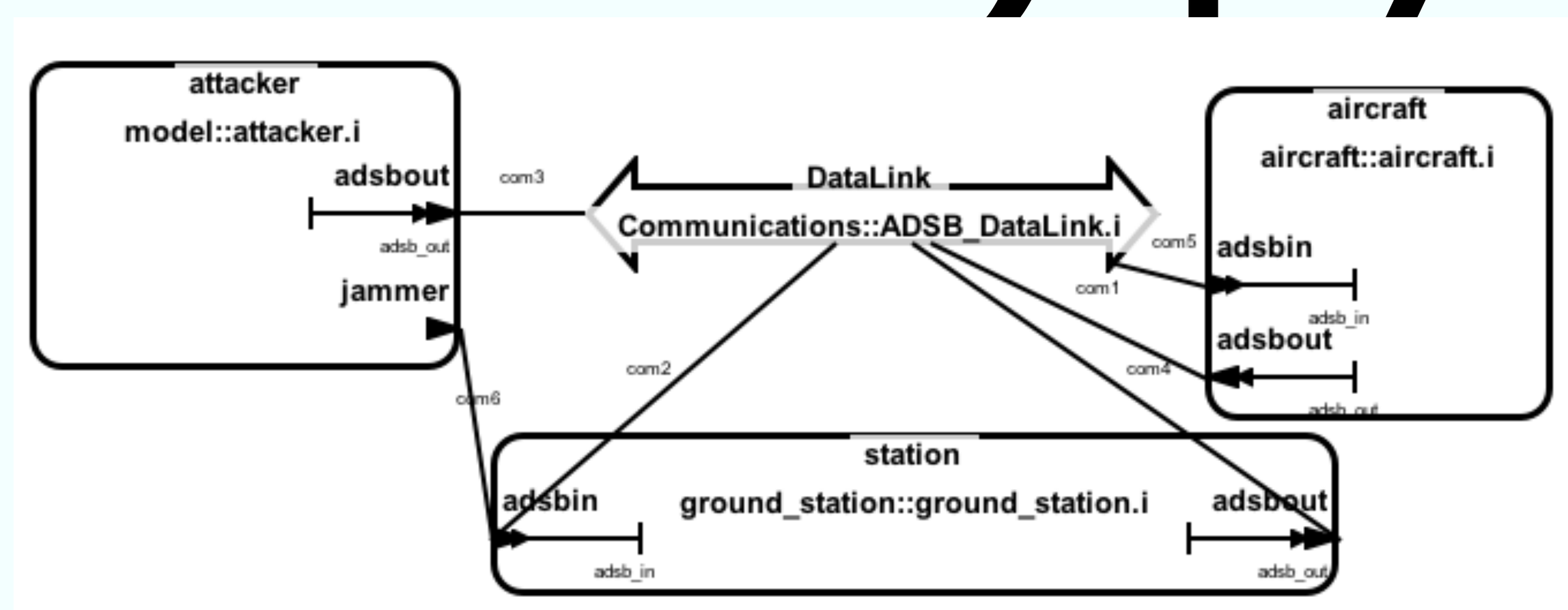


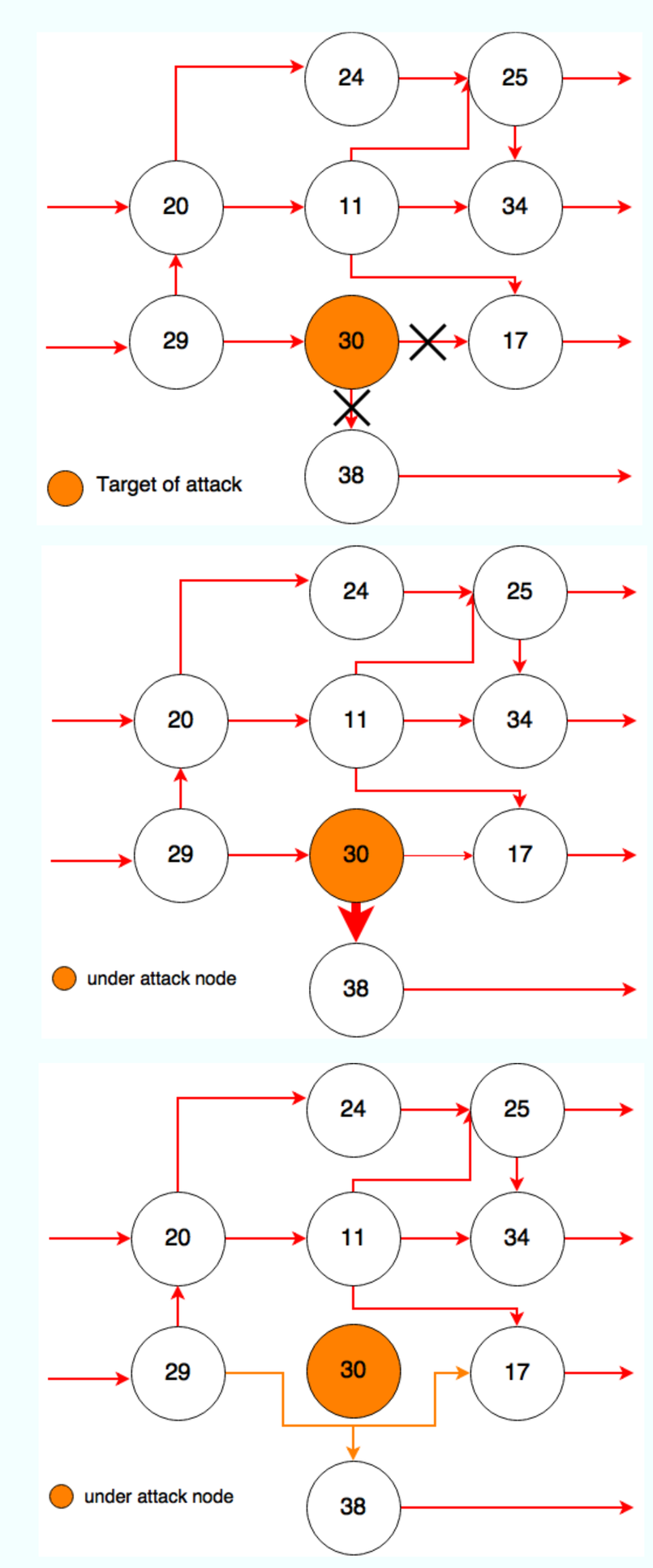
	Delay	Total Squared Deviation	Metric ($\alpha = 1, \beta = 1$)	Metric ($\alpha = 1, \beta = 2$)
Nominal	17.7	0	N/A	N/A
Flow 1-4 blocked	67	7.6E3	0.60	.144
Flow 1-7 blocked	19.2	3.2E3	0.19	.028



Cyber-Attack Modeling

- Modeling Air Traffic Control using Architecture Analysis & Design Language
- Defining and modeling cyber attacks on Air Traffic Control System.
- Investigating the impacts of attacks on air traffic flows using graph modeling

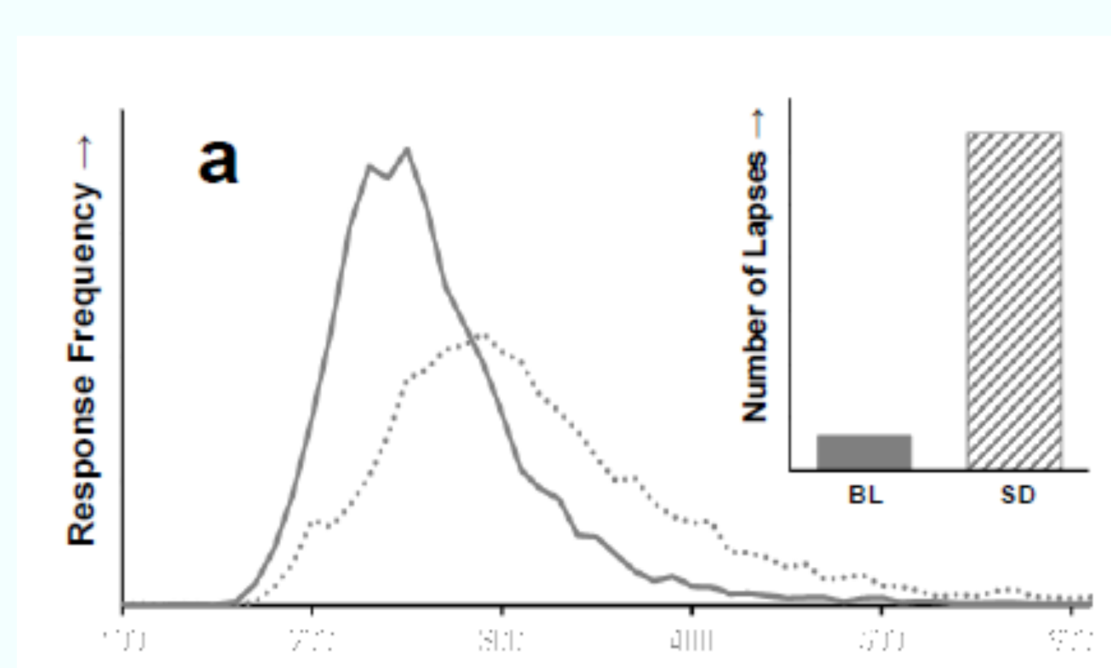


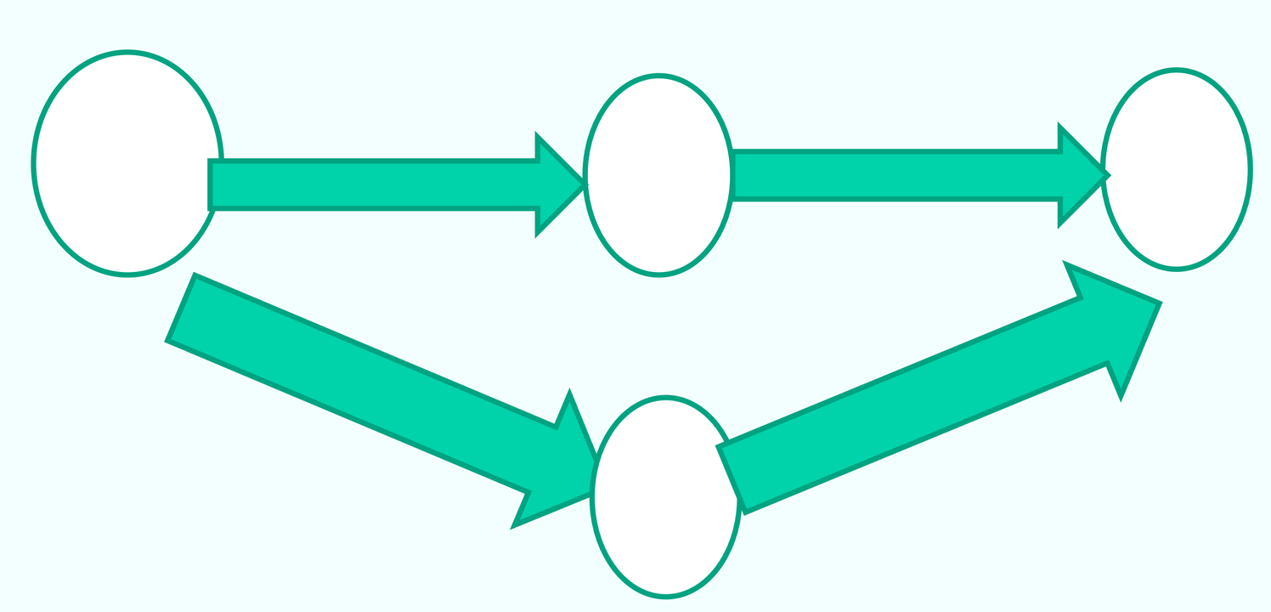


Attack	Goal	Impact
Route Denial of Service	Inject ghost aircrafts to controllers and aircrafts screen	Shutdown the sector controller or a route
Route Selection Tampering	Change the route of aircraft	Disturbance of flow management
Sector Denial of Service	Remove the aircrafts from controller screen	Loss of control over aircrafts

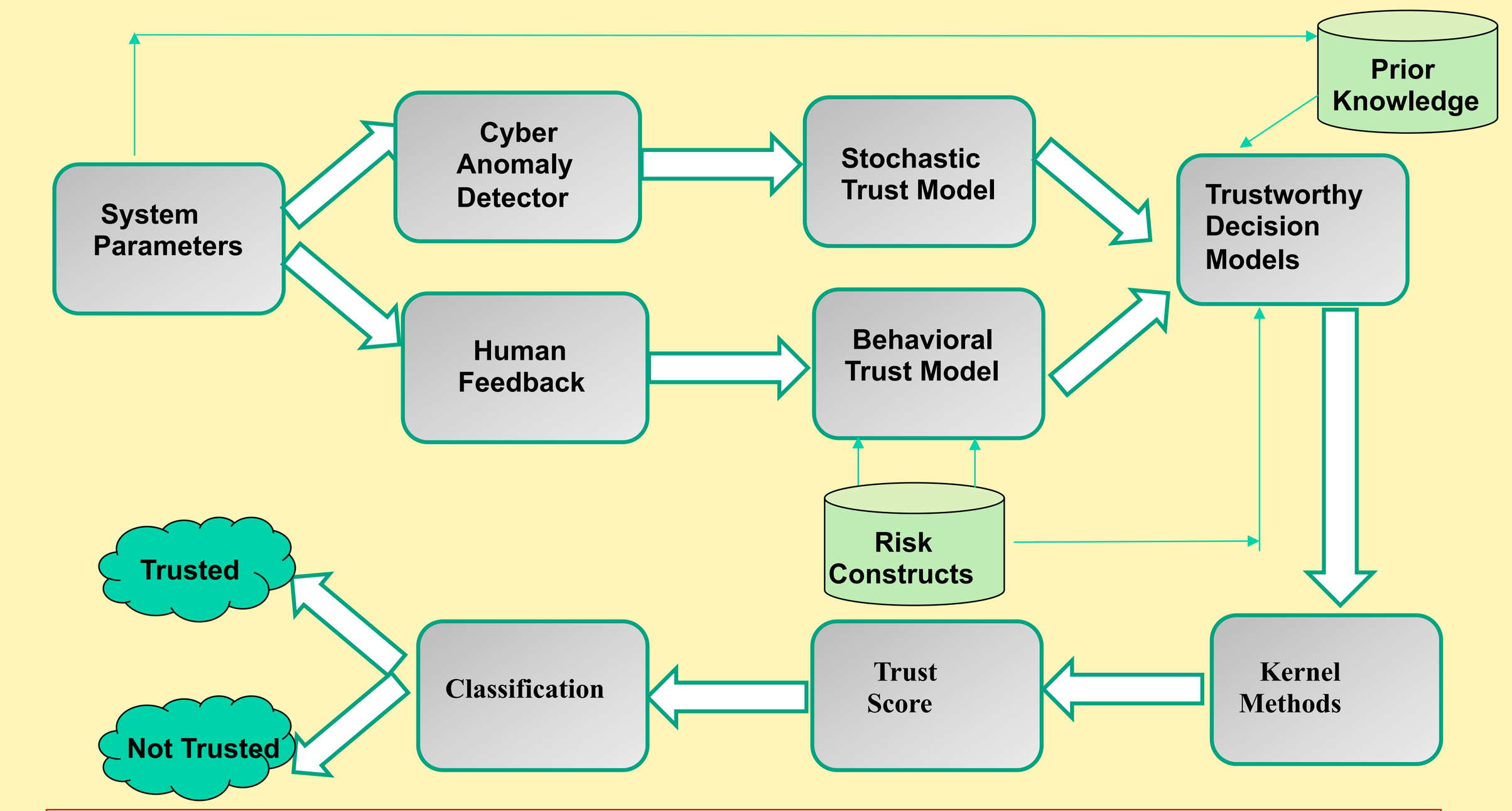
The Human Element

- Diffusion model for decision-making under fatigue.
- Relationship between decision signal-to-noise ratio and fatigue level (published by H. Van Dongen et al in *Sleep*).
- Modeling of air traffic control as a sequential decision task.





Trust Modeling

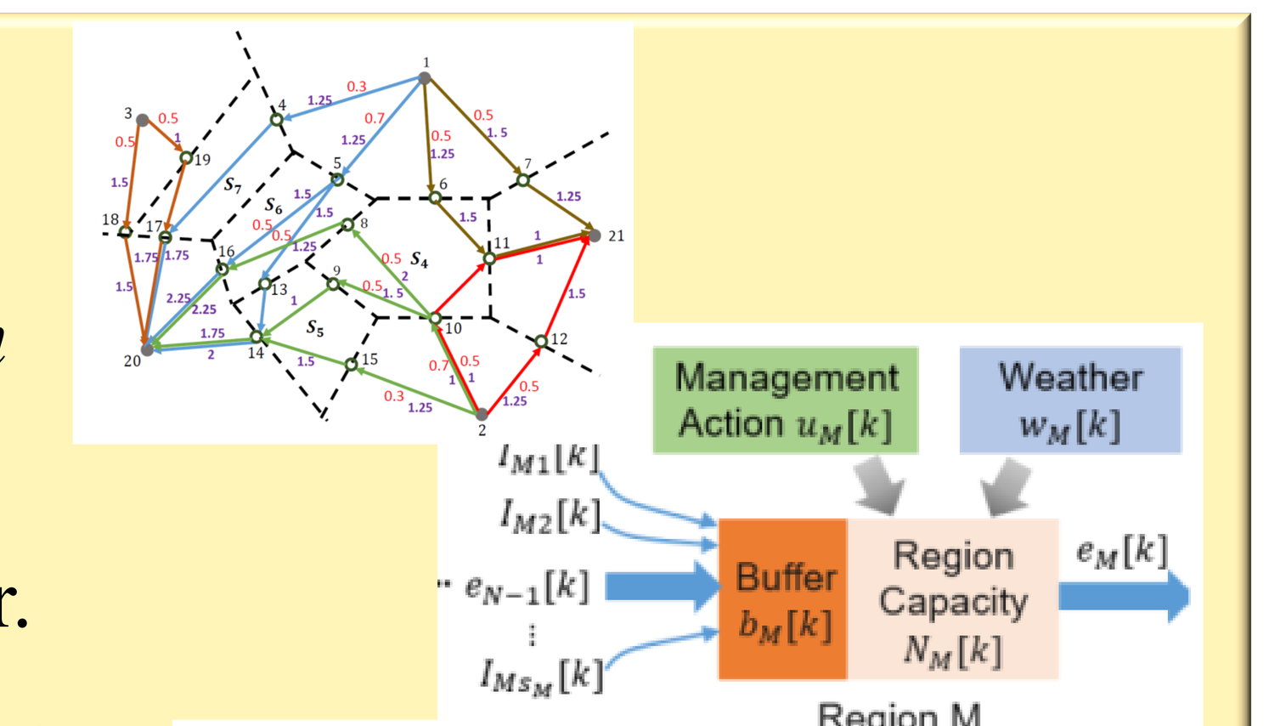


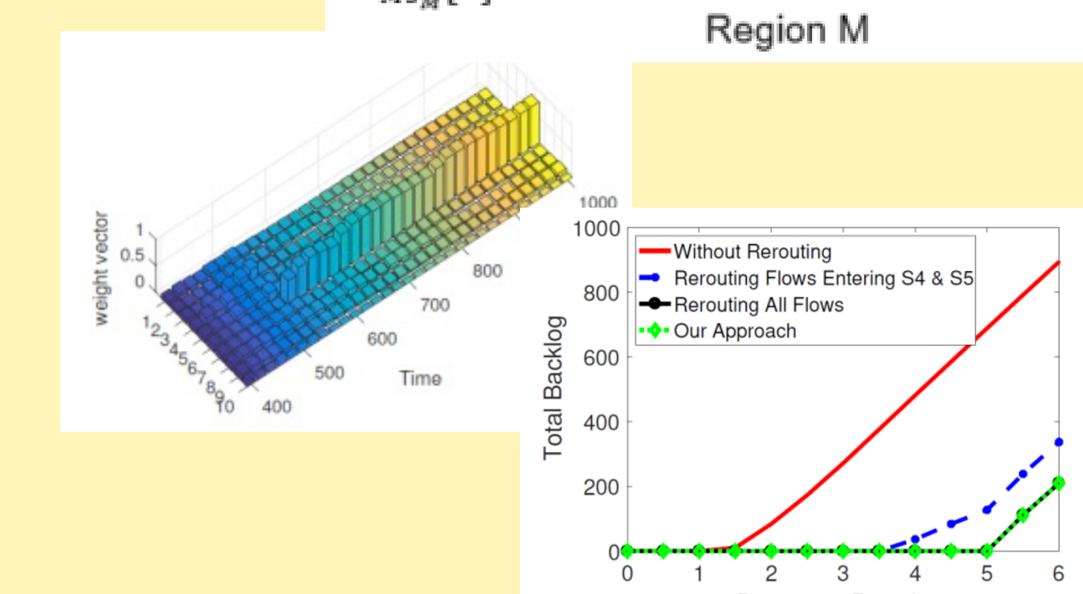
--Each event is associated with a trust metric calculated as regression score with non-linear weights to positive and uncertain indicators.
--Positive indicators' weights are incremental change process modeled by generalized Richard's curve.
--Uncertain indicators' weights are transformational change process modeled by Richard's curve)and decreasing Kohlsrausch relaxation function.
--Regression score is combined with risk aware value functions.

- Trustworthy collaboration among various stakeholders in air traffic control systems.
  - Focus on the TMI selection problem
- Humans vs. Machines: robustness under risk vs objectivity
- Interesting approaches: risk aware behavioral decision theory, prospect theory
- Initial Results to appear in *AIAA SciTech* (S. Bhattacharjee, S. Das, S. Roy).

Numerical Tools

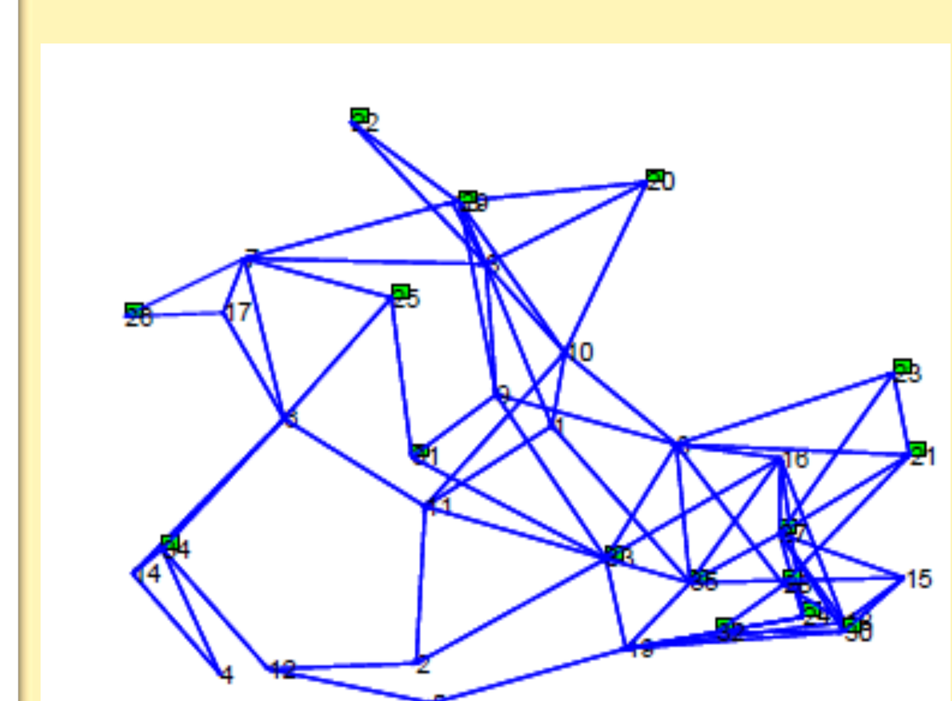
- *Key results by the group at UTA led by Dr. Yan Wan*
  - A discrete-time queuing network simulator and correlation-based network abnormalities detector.
  - A network-condition-centric method to improve the efficiency of rerouting in an uncertain and dynamically changing airspace environment.
  - A scalable sampling-based control method that enables an optimal/robust rerouting and flow restriction design under uncertainty.

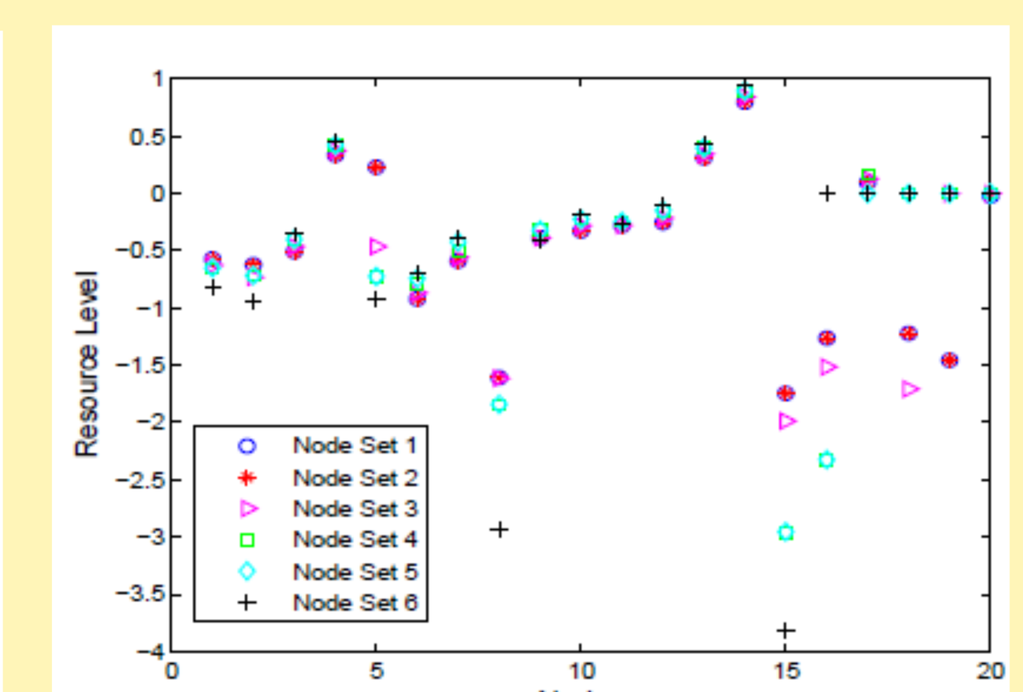


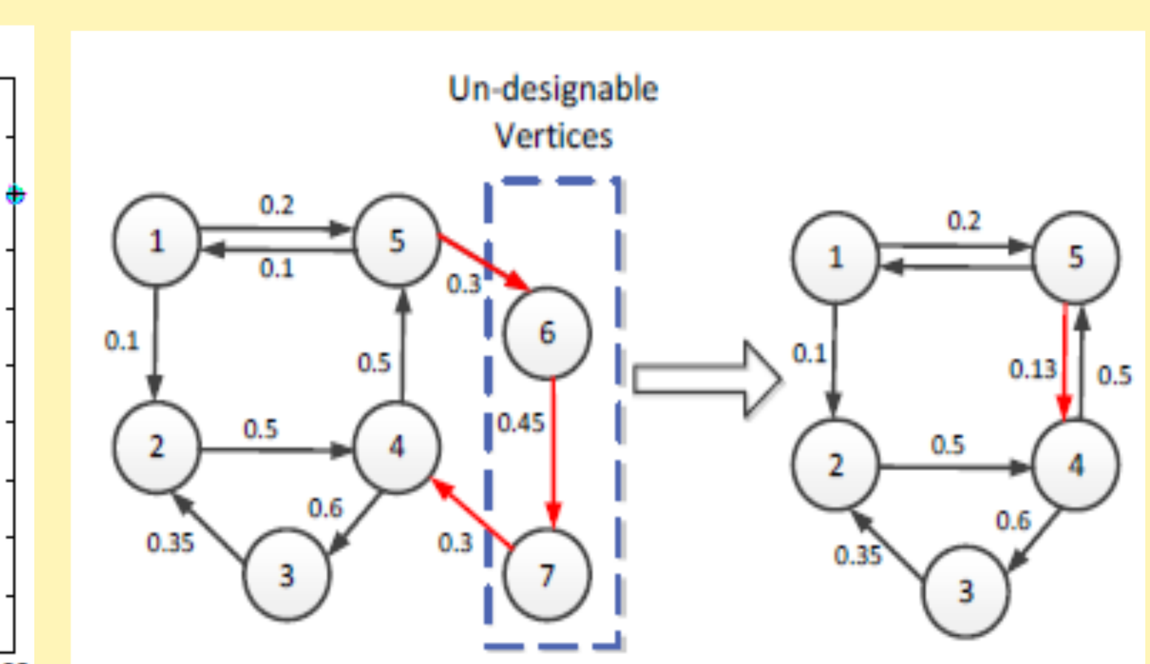


Control Theory for Attack Assessment/Mitigation

- Techniques for understanding attack ripples from a graph-theory perspective.
- Defensive resource allocation in networks.







Broader Impact: Highlights

1) Dissemination to transportation practitioners (FAA, NASA, DHS, airlines).
2) IoT monitoring and security co-application.
   - Published in *IEEE Conference on Control Technologies and Applications* (S. Roy, A. Hahn, M. Xue)
3) Course material development.