Threat-Assessment Tools for Management-Coupled Cyber- and Physical- Infrastructures

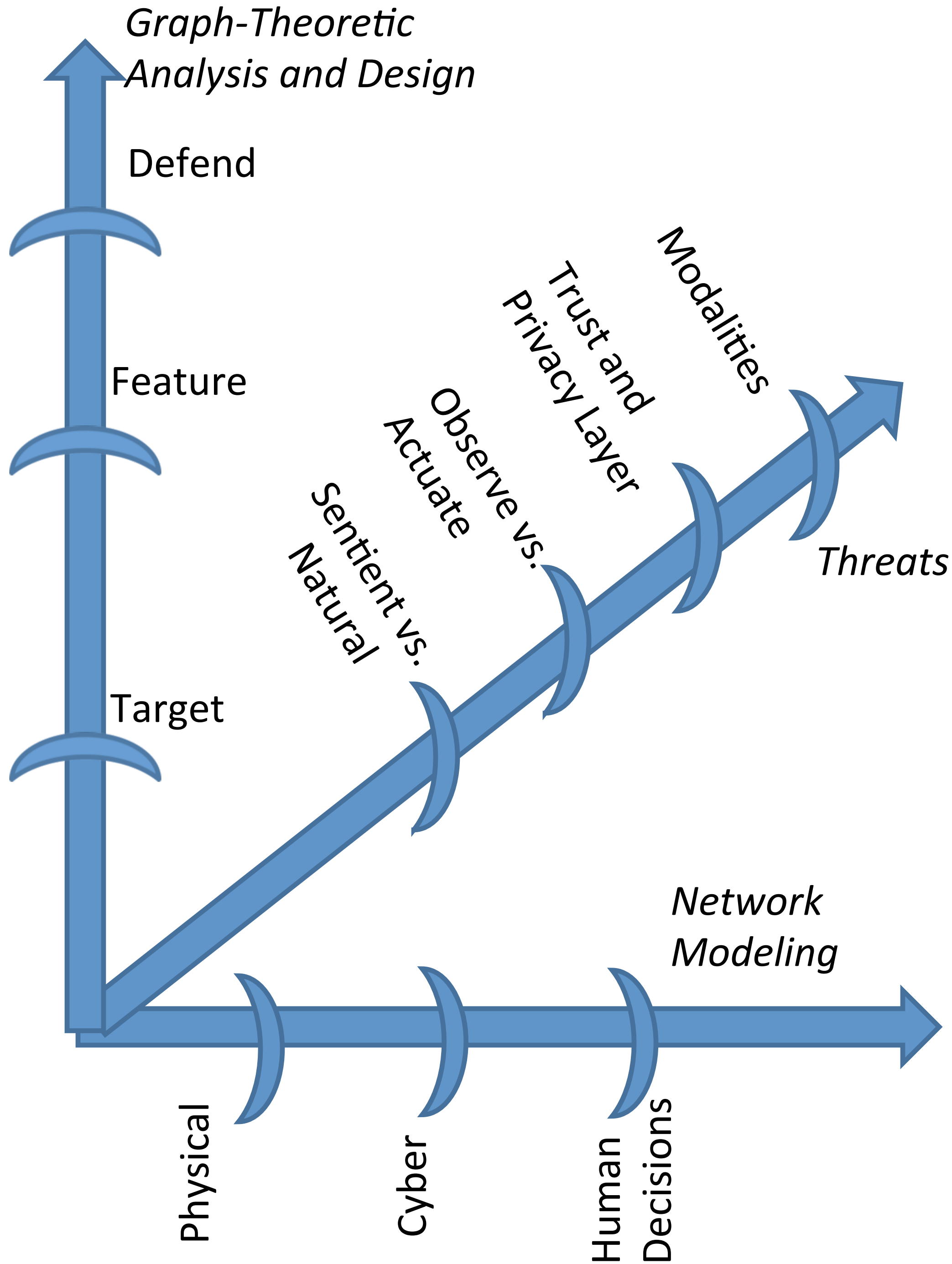
Sandip Roy, Washington State University

Sajal Das, Missouri University of Science and Technology

Yan Wan, University of Texas at Arlington

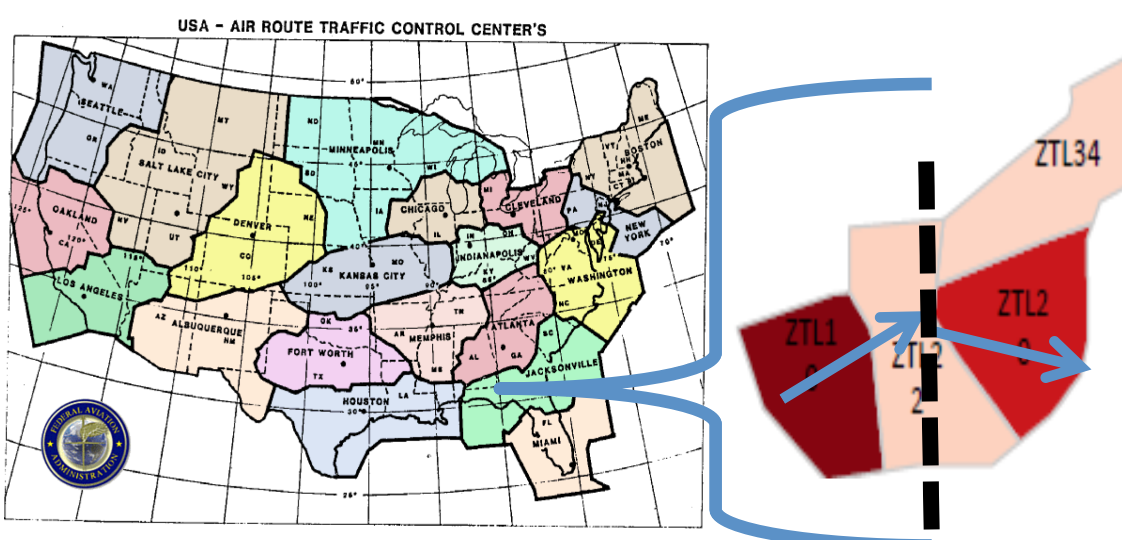
- **Context:** Decision-making in infrastructures often involves human operators, who are sandwiched between cyber and physical assets.

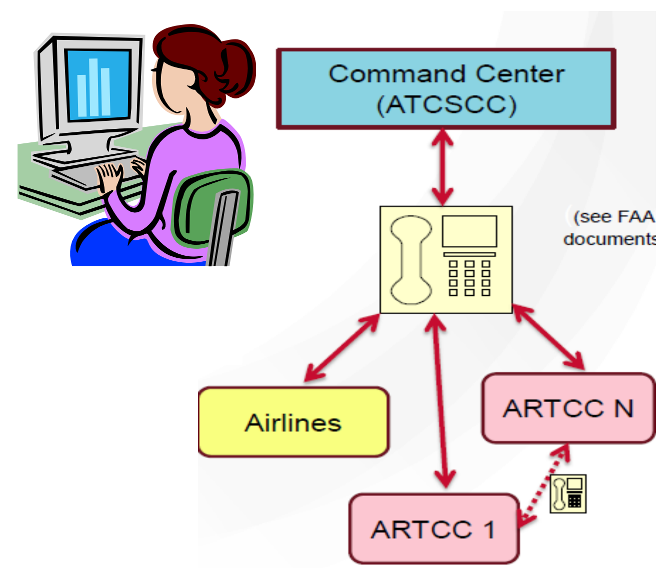
- **Goal:** To develop a threat-assessment framework for these *Management-Coupled Cyber- and Physical-Infrastructures (MCCPIs).*
  - Application: strategic air traffic management.



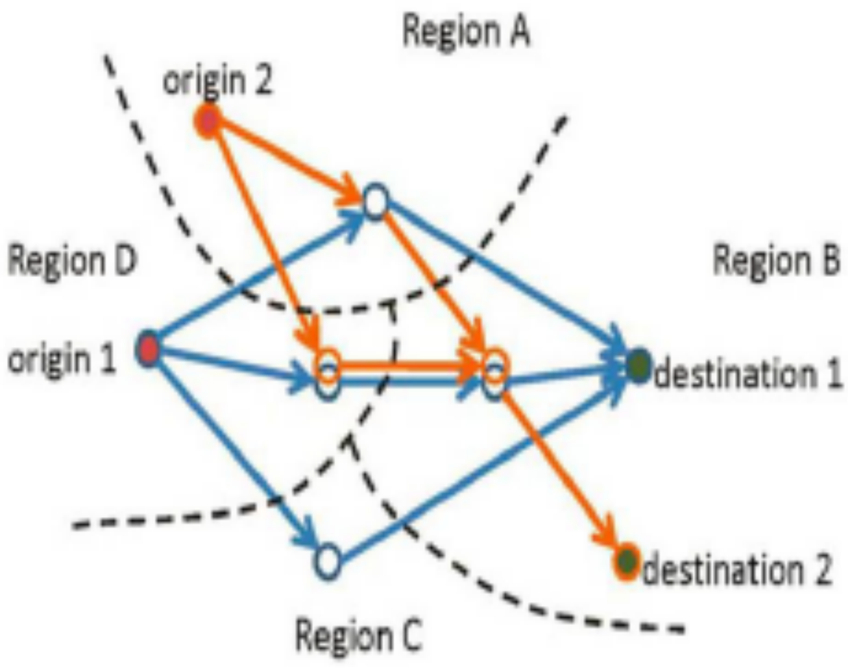
Air Traffic Management: Background

- Human decision-makers are responsible for guiding traffic, using cyber-tools. Several scales:
  - Trajectory guidance to pilots (air traffic control), Sector scale, minutes.
  - Regional guidance (tactical management), Center scale, 0.5-2hours.
  - ***Airspace-wide flow management (strategic), 2-15 hrs.***
- Growing concern about ``man-made” disruptions in addition to weather.
  - Cyber failures and attacks, operator fatigue, new operational paradigms (space vehicles, UAS)

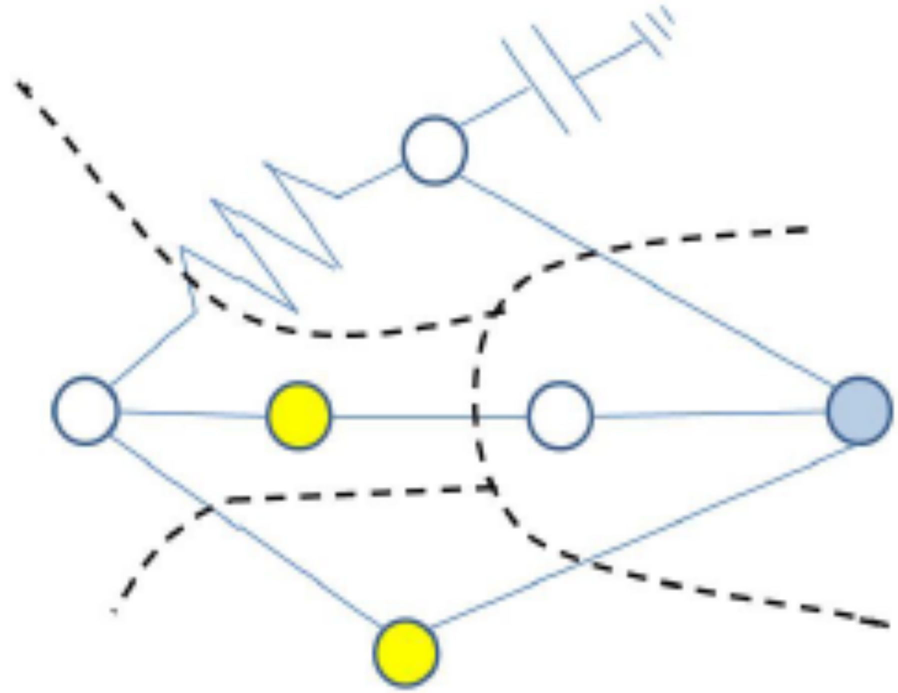




Network Modeling: Physical (Traffic)



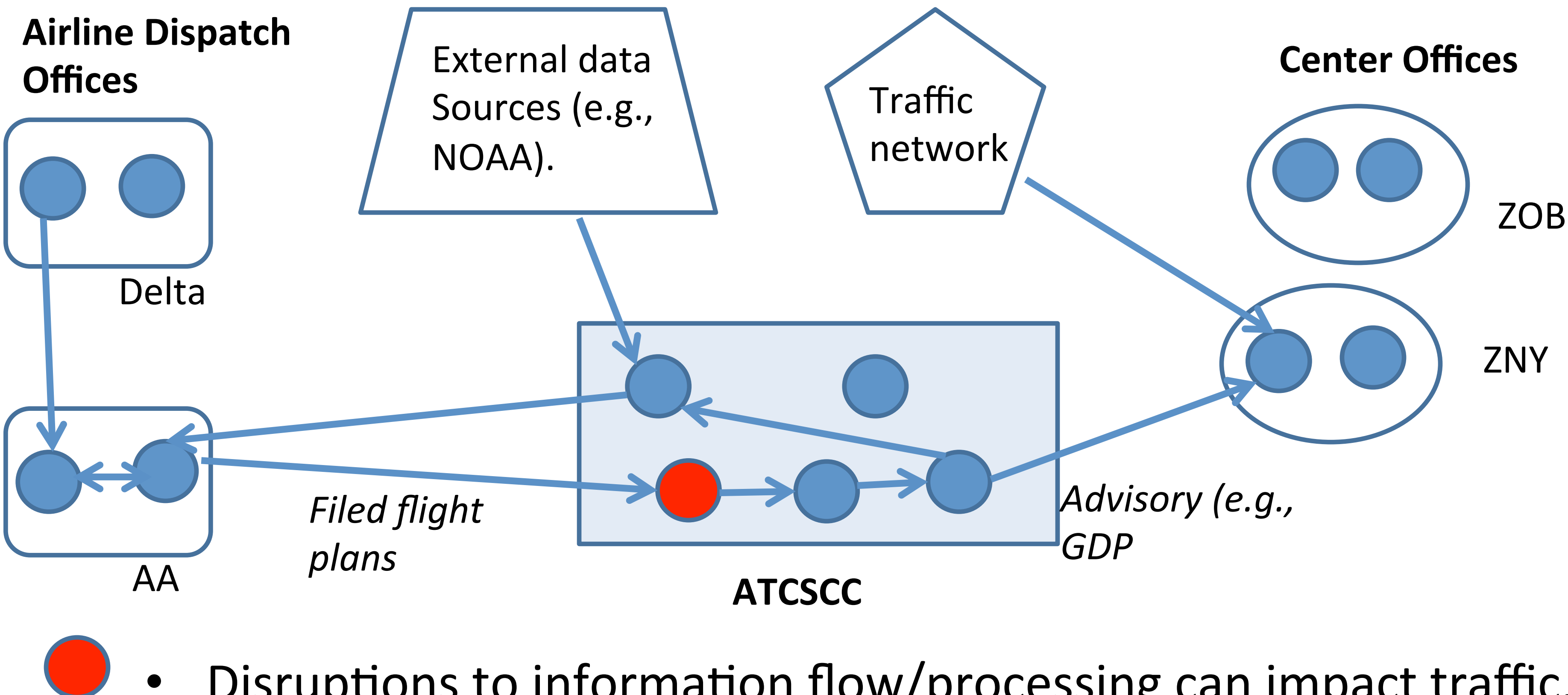
Flow and Queueing Model
(Y. Wan et al, 2012)



RC Circuit Approximation

Network Modeling: Cyber

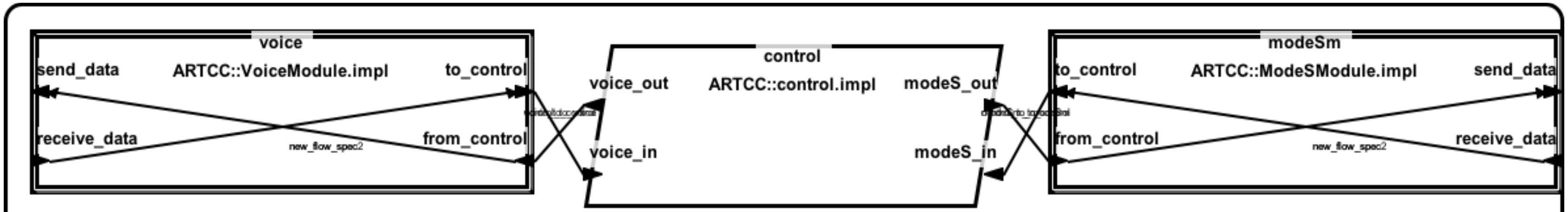
- Abstractly, operation of the air traffic system depends on information flow between stakeholders.



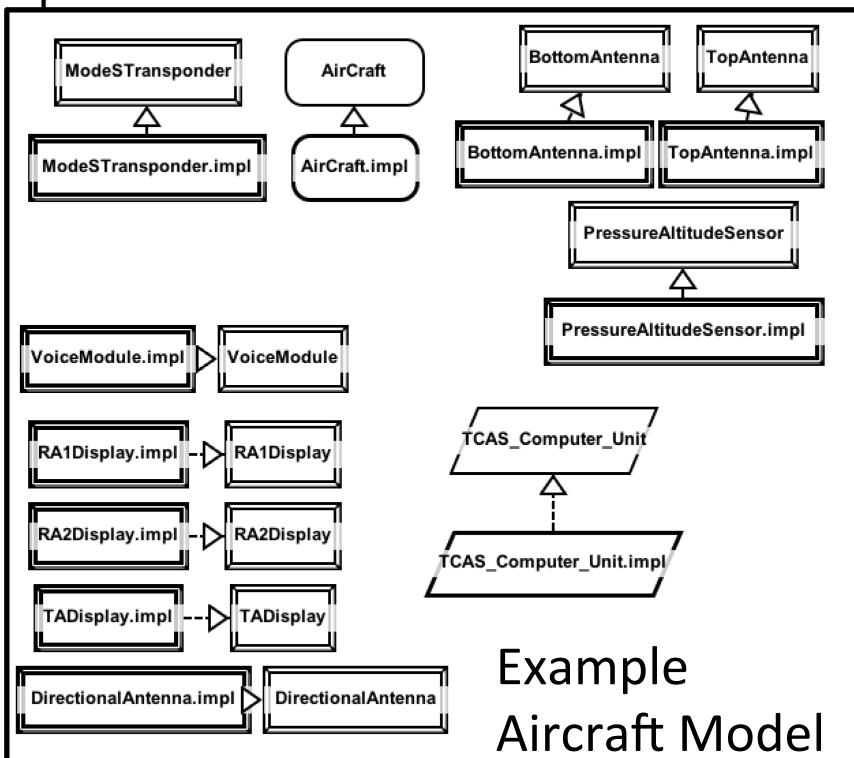
- Disruptions to information flow/processing can impact traffic.

(Roy et al, 2016)

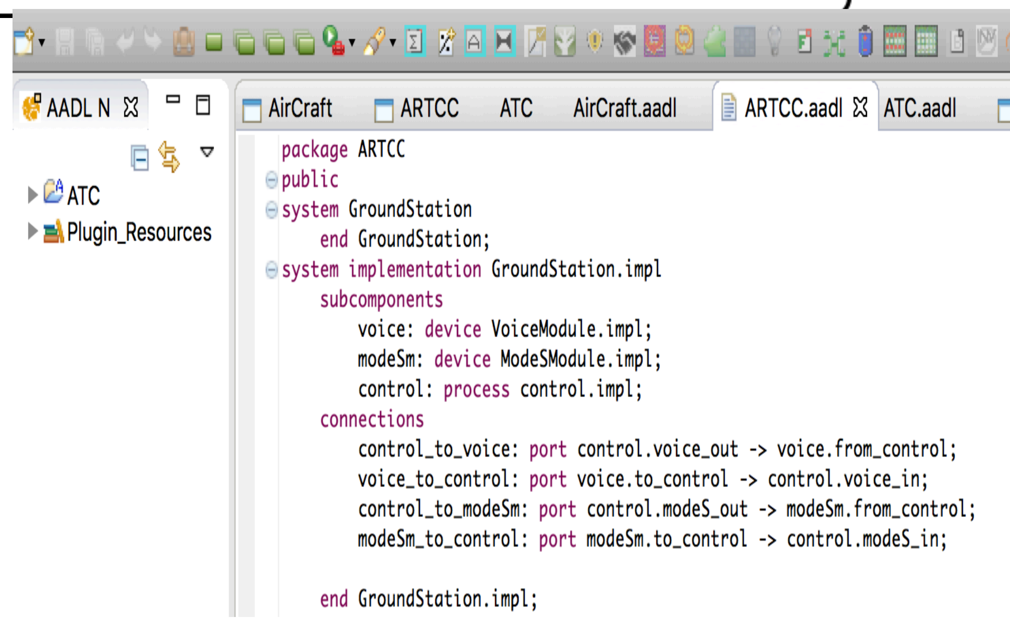
Cyber Network: AADL Modeling



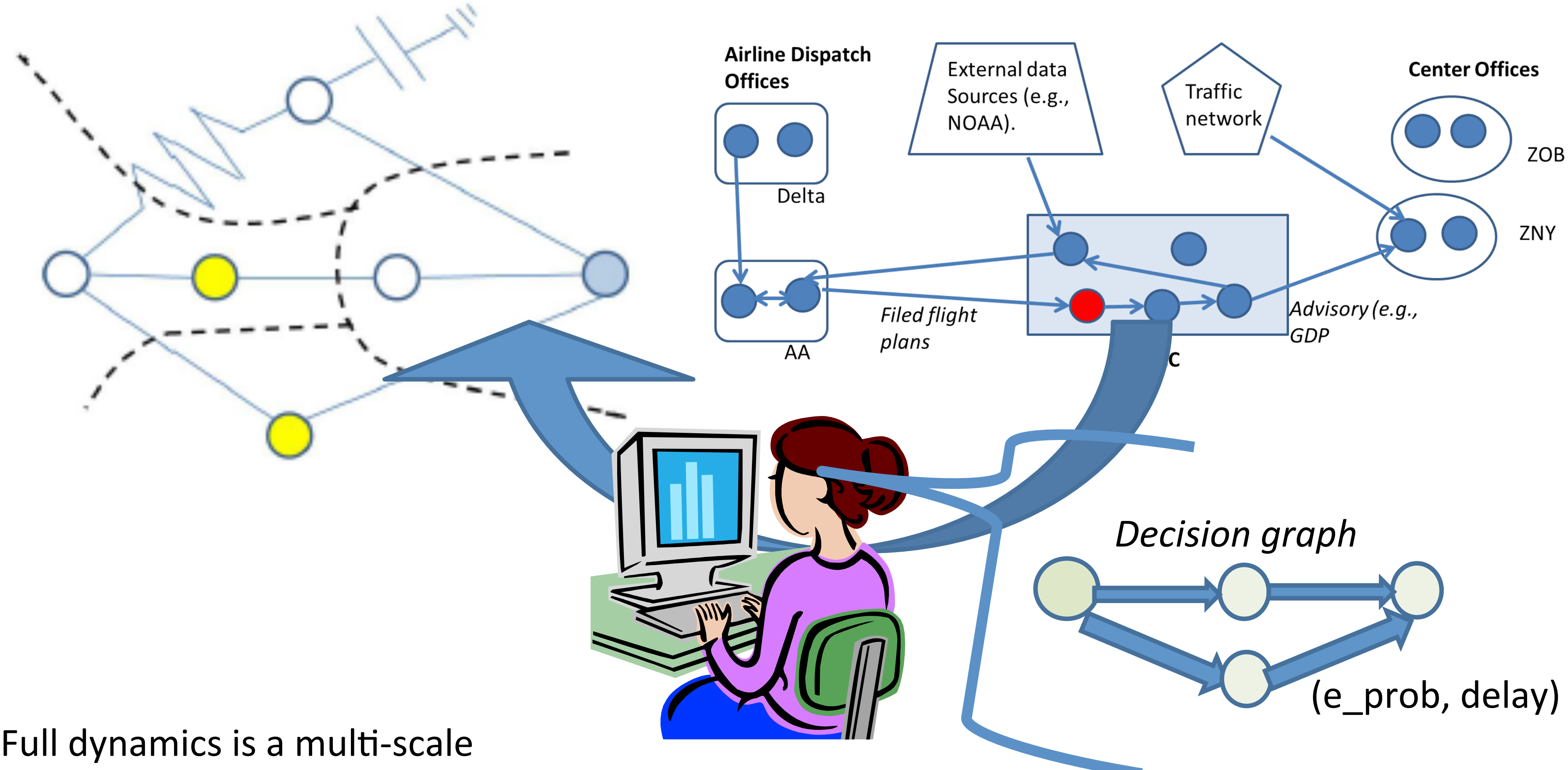
Air Route Traffic Control Center Model



Example Aircraft Model



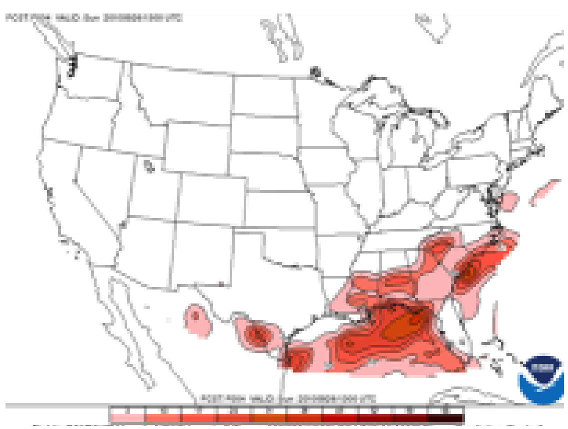
Management Coupling and Full MCCPI

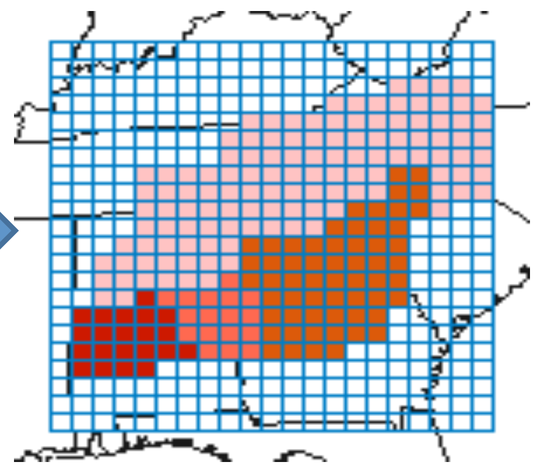


Full dynamics is a multi-scale *layered* network model (Dhal et al, submitted, 2016)

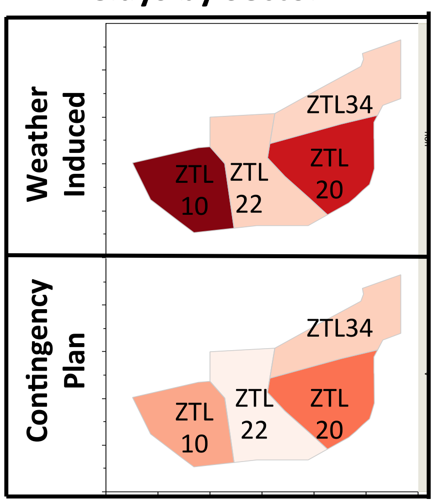
Threat Modeling by Modality

- Environmental Disruptions: Severe Weather
  - Disrupts traffic flows, reduces capacities.
  - Extensive literature in this area, key challenge is to capture uncertainty.
  - Stochastic automaton models that use commercially-available forecasts, and identify capacity reductions (Xue et al 2012).



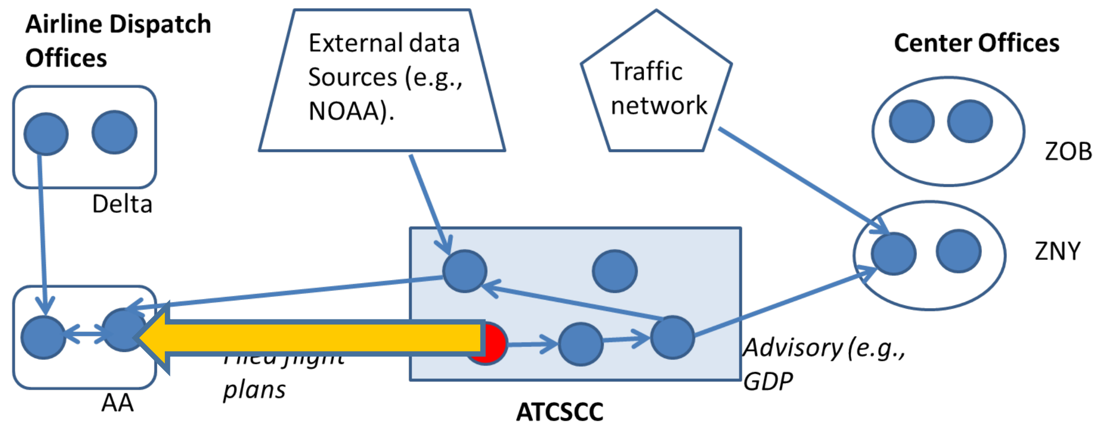


Delays by Sector

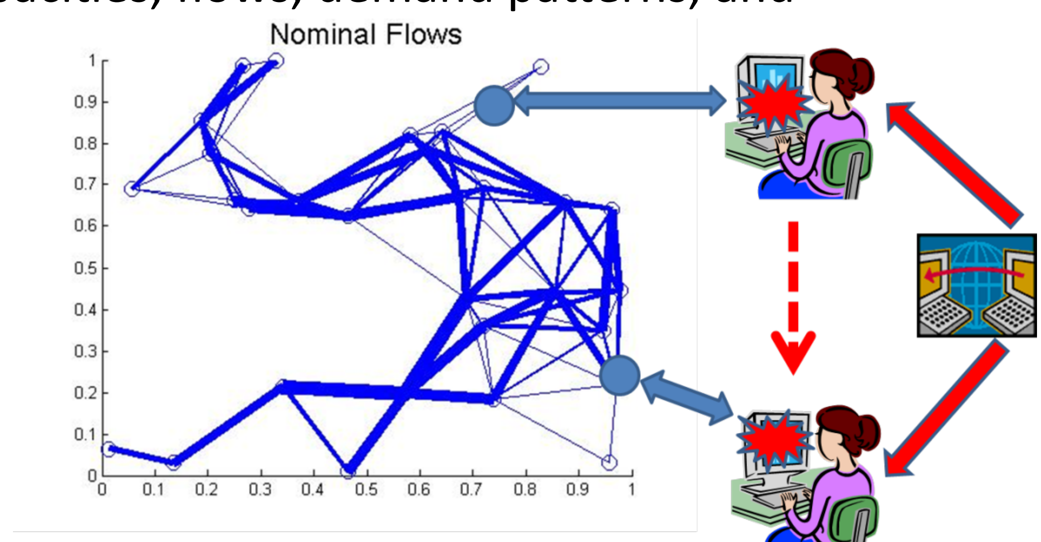


Threat Modeling by Modality

- Cyber- attacks (sentient) and failures (natural)
  - **Full model:** random-chance or percolation model in cyber layer.
  - Diverse exploits: phishing, denial-of-service, false data injection.

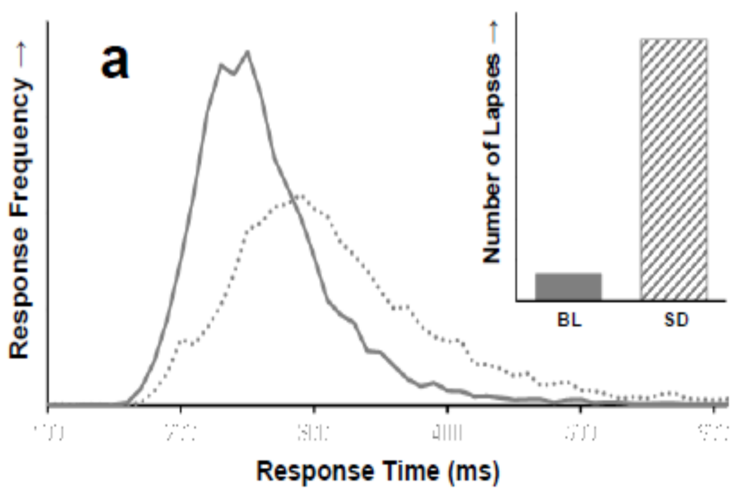


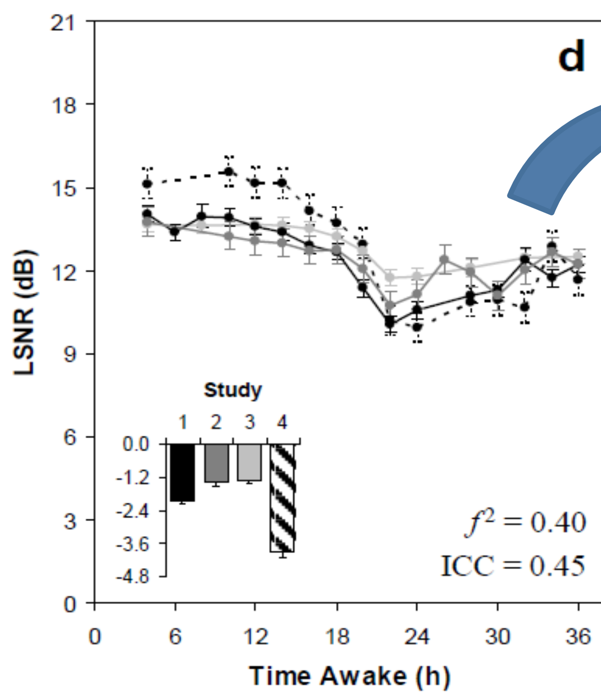
  - **Reduced model:** impact capacities, flows, demand patterns, and controls in physical layer.
  - Gain information about flows/controls.
  - May aim to control, learn, disrupt.
  - Reduction?

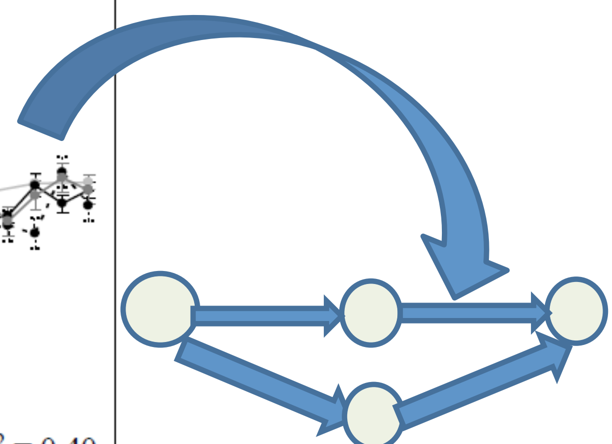


Threat Modeling by Modality

- Human-in-the-loop threats: fatigue increases variability and duration of delay (d), and probability of incorrect delay (e_prob).
  - One-choice diffusion-model is predictive of variability
  - *SNR formulation facilitates network analysis* (Chavali et al, 2016).
- These threats may affect capacities and flow densities in the airspace system.







Decision graph

A Trust Layer

- A defender's perspective: understanding the trustworthiness of measured data.
  - Need to be able to differentiate between legitimate operational changes, impacting threats, and data manipulation.
- Exploring trust models that capture:
  - Fidelity of sensors
  - Laws governing physical-world behaviors.
- A double-weighted approach is being pursued.

An Application-Independent Framework

- Multi-time-scale layered network model for MCCPI dynamics, e.g.:

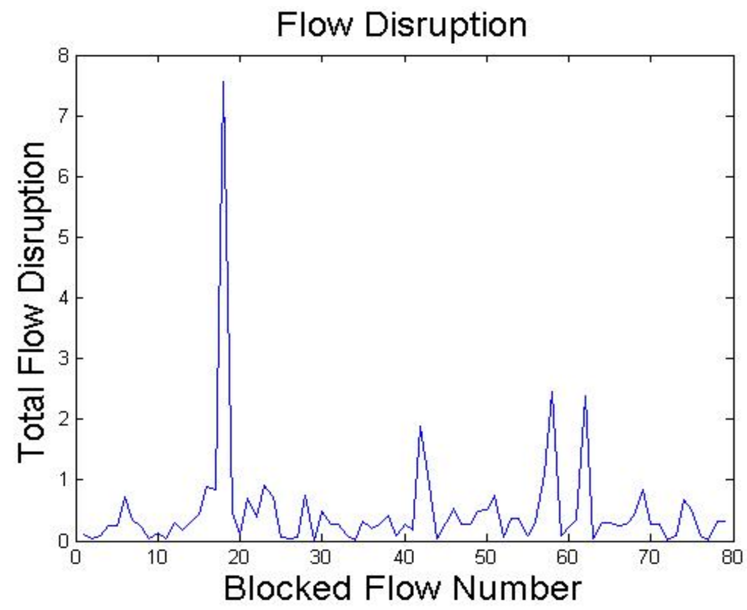
$$\begin{bmatrix} x_t[k+1] \\ x_c[k+1] \end{bmatrix} = \begin{bmatrix} G_{tt}(\Gamma_t) & G_{ct}(\Gamma_{ct}) \\ ?? & G_{cc}(\Gamma_c) \end{bmatrix} \begin{bmatrix} x_t[k] \\ x_c[k] \end{bmatrix} + \begin{bmatrix} 0 \\ B_c \end{bmatrix} u[k]$$

- Broadly, threats: 1) actuate the dynamics, 2) change network-model parameters, or 3) alter observations.
- Assessment metrics: targeted manipulability/controllability, observability, disruptiveness, trust, privacy (coming soon).

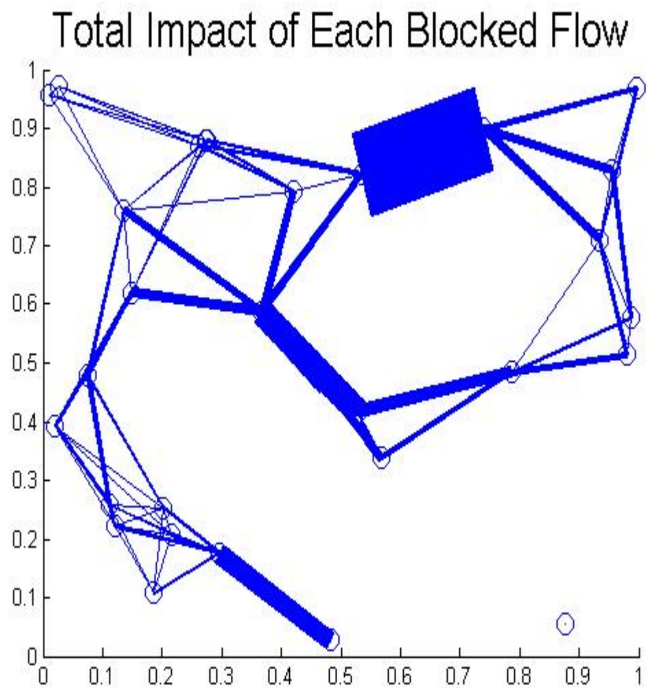
- **Assessment principle:** Attacks have propagative impact across cyber, physical, and human components of an MCCPI. Assessment requires understanding this.
  - Can be evaluated through simulation.
  - Or, we can develop **graph-theoretic** insights which enable defense and mitigation.

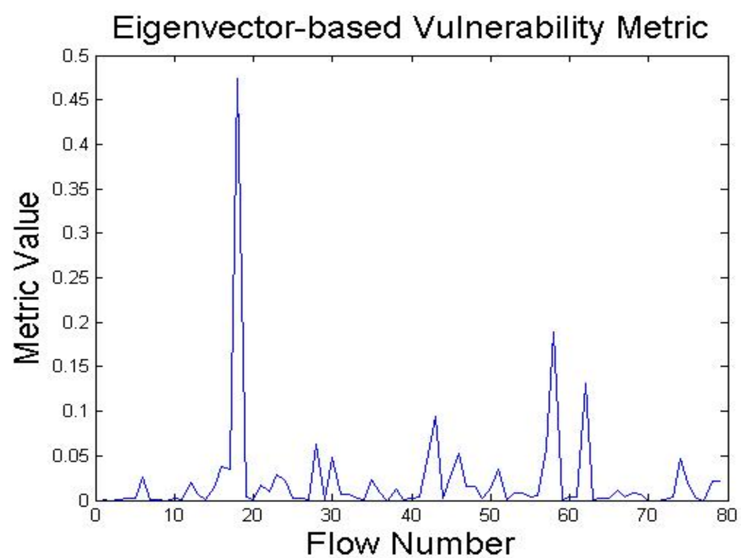
Assessment Tools: *Target*

- Identify where the network is susceptible to attack.



Via simulation



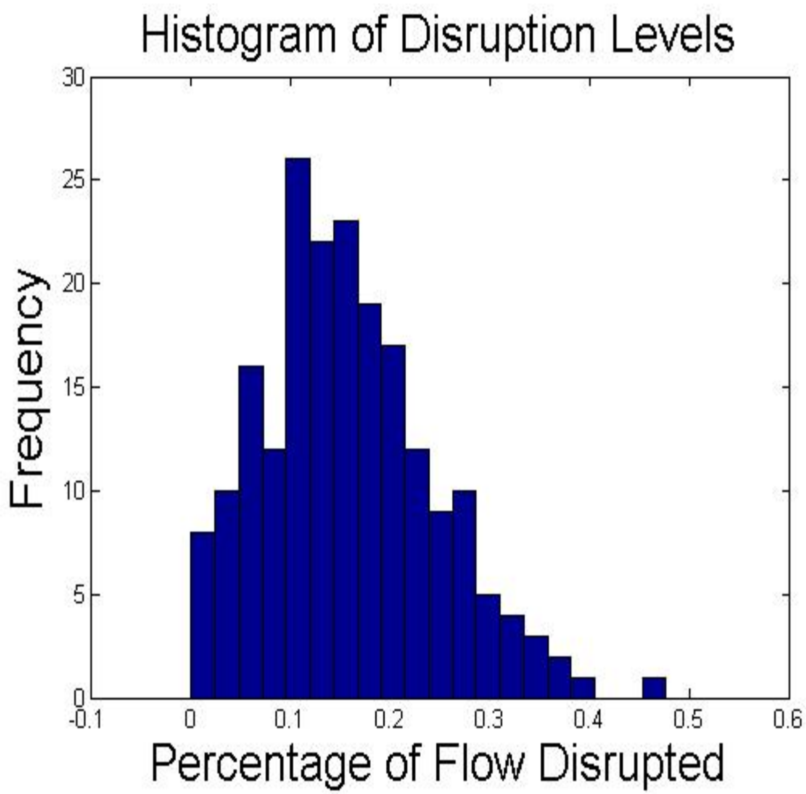


Major flows with few uncongested alternatives are vulnerable.

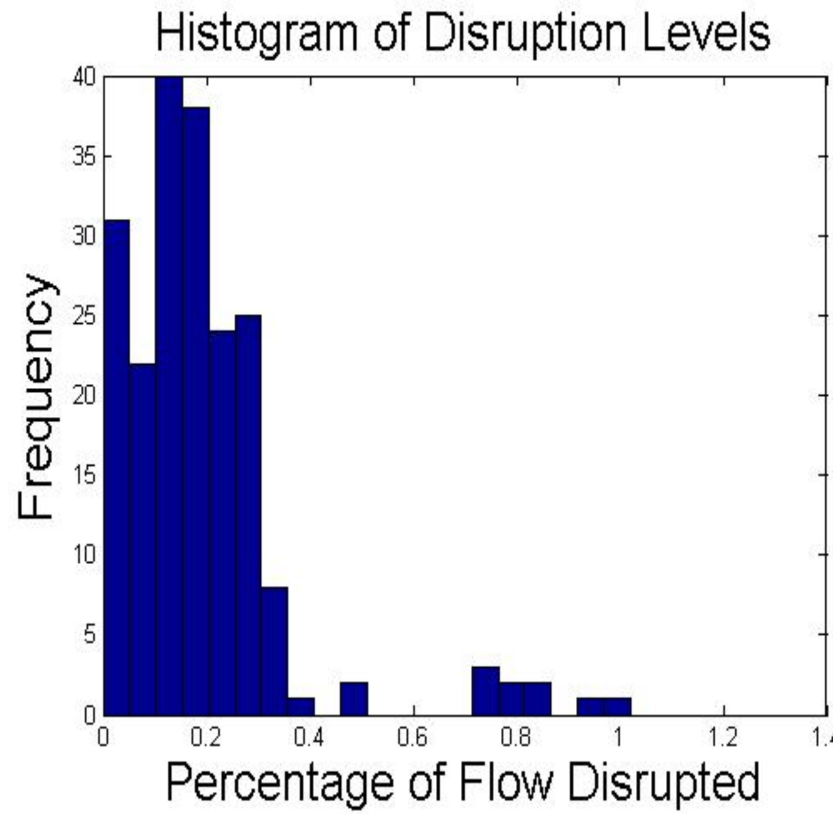
Via a graph-theoretic metric.

Assessment Tools: Feature

- Understand what features of the network decide overall vulnerability.



Uncongested network



Congested network with critical flows

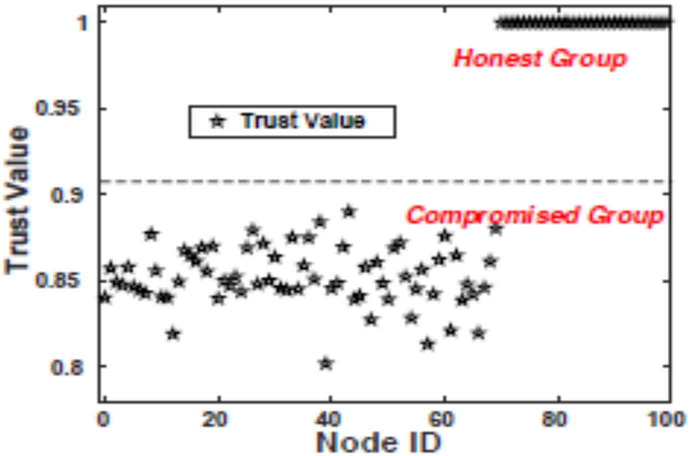
Assessment Tools: Defend

- Statistical techniques for detection of anomalies and attacks.
  - Ratio of the *harmonic mean* (HM) and *arithmetic mean* (AM) is an interesting scale-free measure, that enables lightweight detection of anomalies.
  - Tests using power-meter data show ability to differentiate several type of false-data attacks.

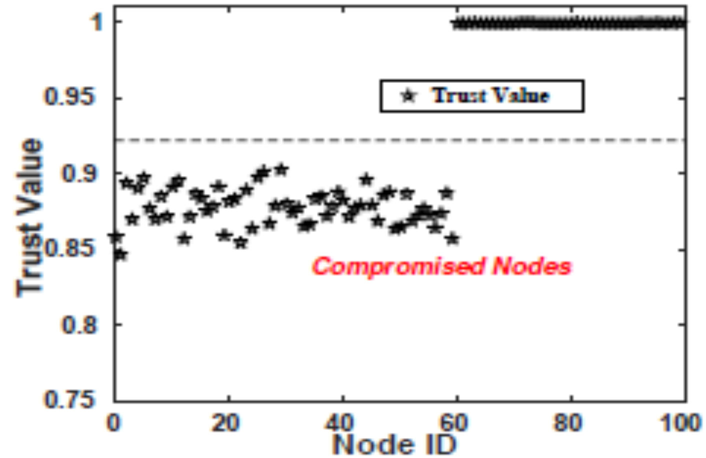
(Bhattacharjee et al, 2016)

HM/AM Ratio-based detection

Real Data sets from Light Intensity Sensors and Smart Meter Power Consumptions

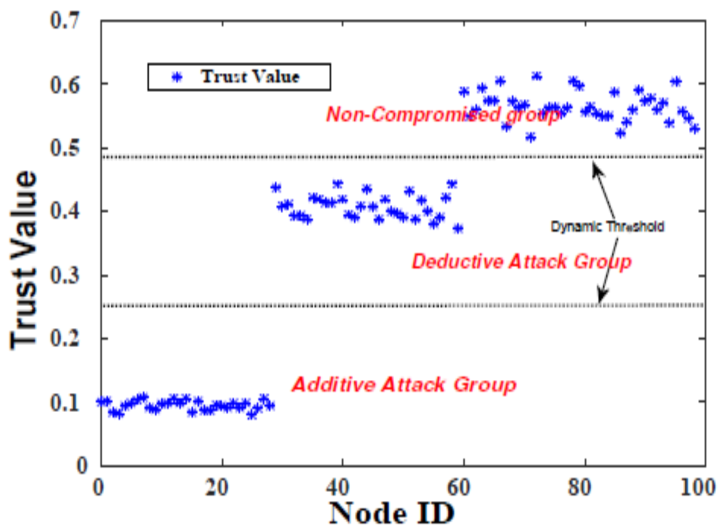


(a) Additive : 70% compromised

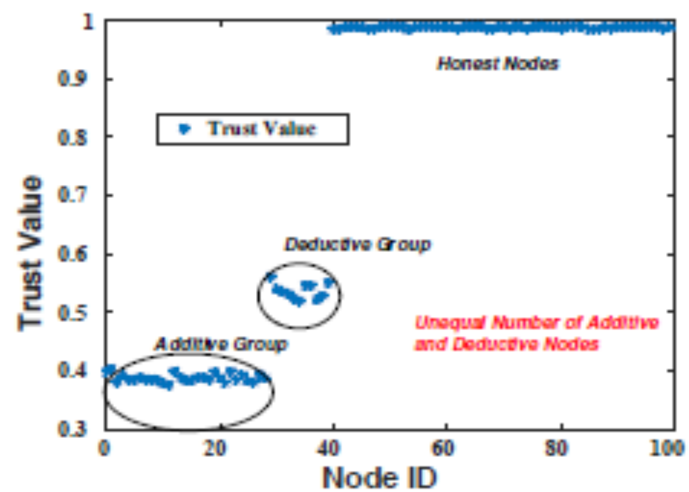


(b) Deductive: 60% compromised

Emulated Attacks using real data set fed to simulated network



(a) Camouflage : 60% compromised



(b) Conflict : 40% compromised

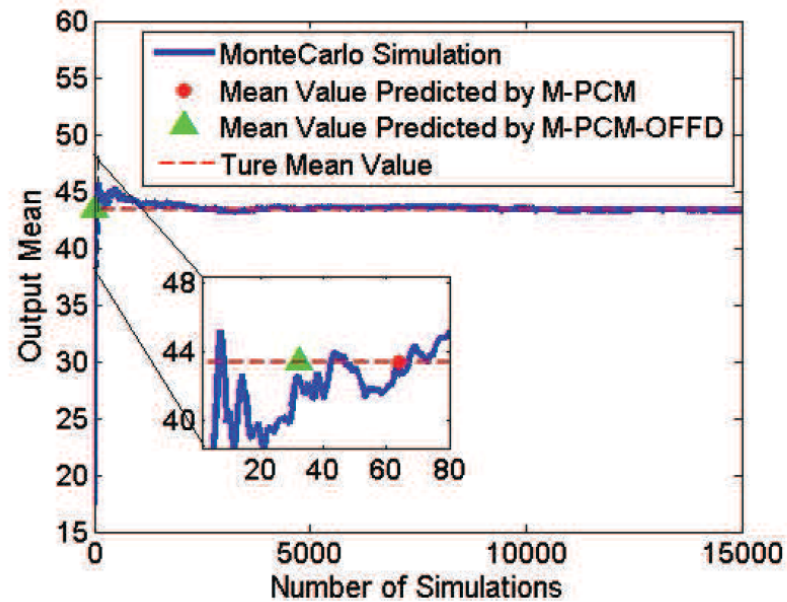
Clear Difference between trust score of compromised and honest sensors

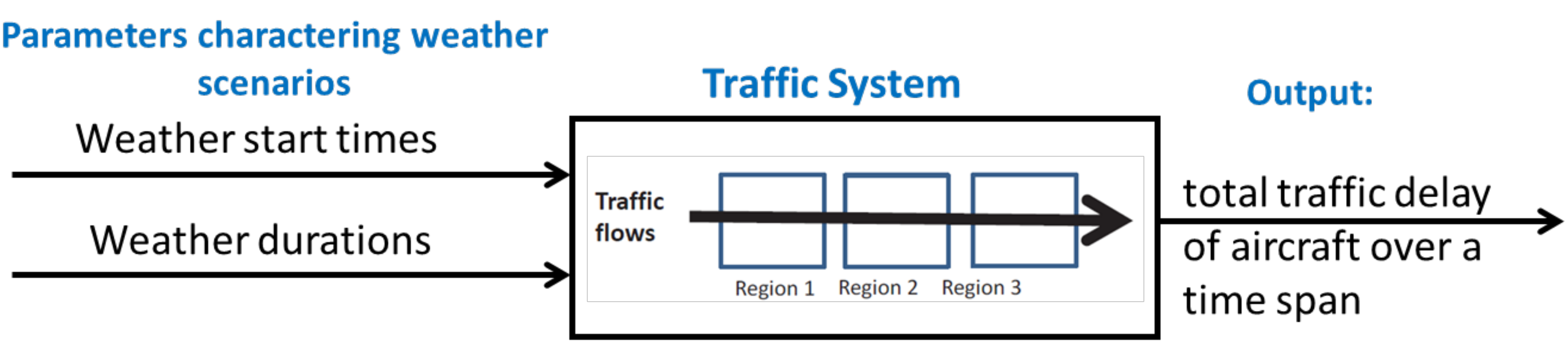
Assessment tools: Defend

- Jump-Markov approximations for statistical evaluation and design of traffic management initiatives.

- Smart simulation techniques for evaluation of and design against uncertainties.
  - Based on the probabilistic collocation method.

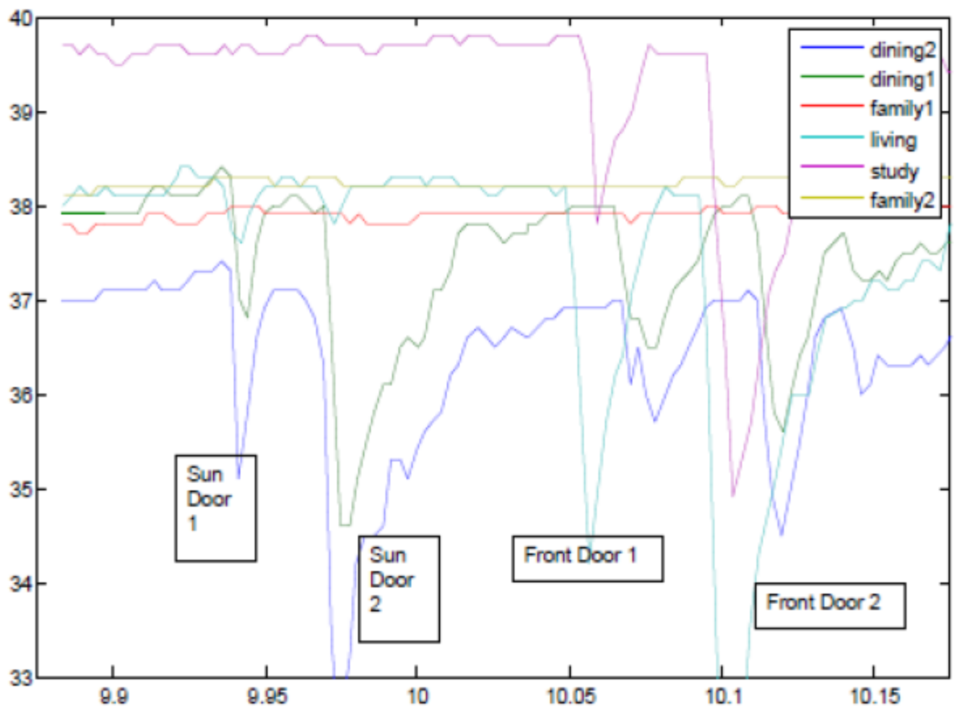
- The methods have proved effective for designing against severe weather.
  - Next task: addressing cyber and human disruptions.

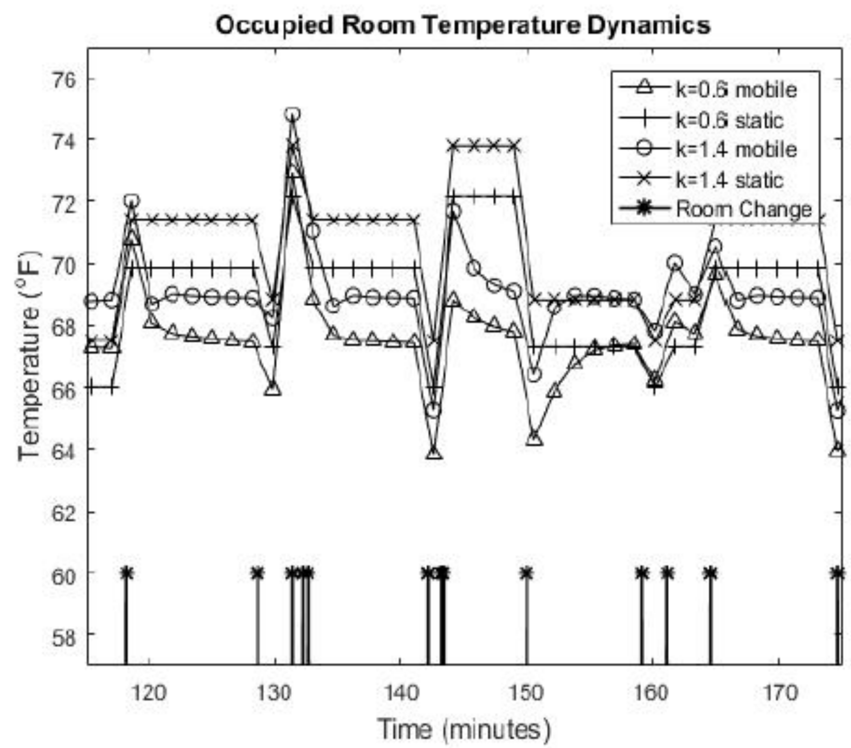




Broader-Impact Activities

1) Dissemination to transportation practitioners (FAA, NASA, DHS, airlines).
2) Cross-domain application to the electric power industry.
3) IoT applications (anomaly detection and resident-location-catered control for HVAC) : student training.
4) Course material development.





Project Participants

Sandip Roy (PI, WSU)
Sajal Das (PI, MST)
Yan Wan (PI, UTA)
Adam Hahn (co-PI, WSU)
Hans Van Dongen (co-PI, WSU)
Ali Mehrizi-Sani (co-PI, WSU)
Amirkhosro Vosughi (graduate student, WSU)
Samantha Riedy (graduate student, WSU)
Ali Tamimi (graduate student, WSU)
Shameek Bhattacharjee (PostDoc, MST)

Threat-Assessment Tools for Management-Coupled Cyber- and Physical- Infrastructures

Sandip Roy, Yan Wan, and Sajal Das

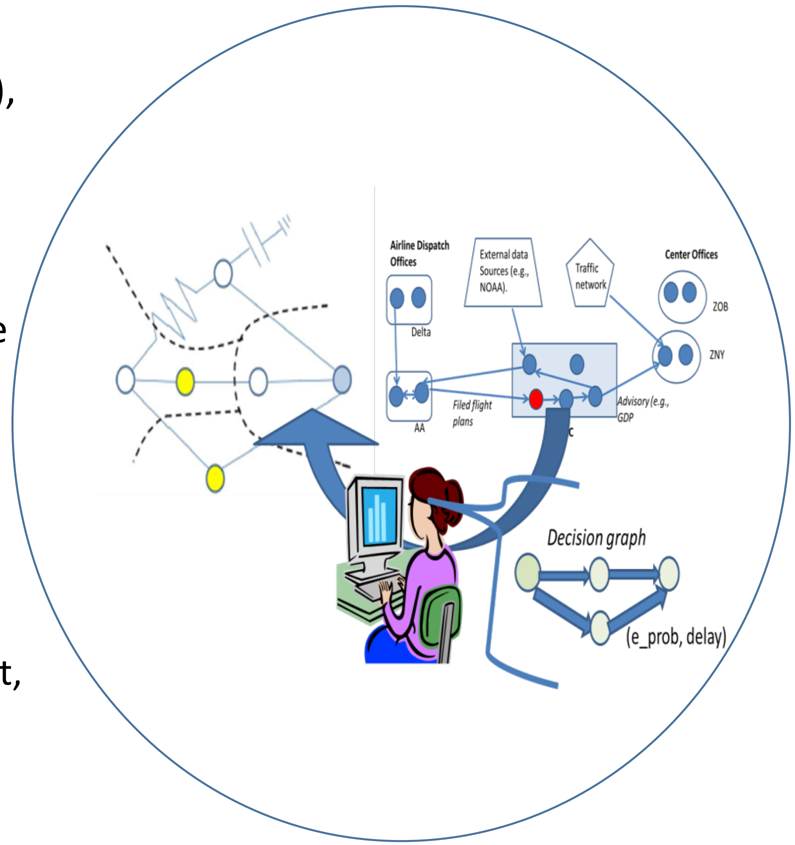
Challenge:

- In critical infrastructures (e.g. the air traffic network), threats have wide-area propagative impacts across cyber, physical, and human components.
- Need to assess and manage threats!

Solution:

- Model management-coupled cyber and physical infrastructures.
- Represent threats
- Assessment tools: target, feature, and defend

Washington State U. (CNS-1545104), U. of Texas at Arlington (CNS-1544863), Missouri S&T (CNS-1545050)



Scientific Impact:

- Development of layered network models; cyber, cognitive, and environmental threat models; and sparse network control theory for assessment.
- Tools and software for air traffic management.
- These can be ported to other infrastructures, and Internet-of-Things applications.

Broader Impact:

- Improve response to cyber and fatigue events in the air traffic system (6-10 such events over last year!)
  - Pursuing Technology transfer.
- Student training on IoT, and course curriculum development.
- Power-system applications.