Vulnerability Metrics for the Airspace System

Sandip Roy and Mengran Xue, Washington State University

Banavar Sridhar, NASA Ames Research Center

Twelfth USA/Europe ATM R&D Seminar, Seattle, WA, 6/29/2017
Disruptions to Airspace Systems

• Air traffic is subject to disruption:
  – Severe weather
  – “Man-made” disruptions: cyber failures, cyber/kinetic attacks, operator fatigue
  – Space-vehicle and UAS integration

• Disruptions are growing in diversity, impact, and perhaps frequency.
Disruption Impacts and Resolution

• Disruptions impact ATC/ATFM, and hence airspace-system performance.

• Impacts at several scales:
  1. Local impact to safety and workload in ATC.
     • Prevent safety-impacting threats.
     • Depend on ATC procedures and tools to resolve.
  2. Consequent impact to tactical and strategic ATFM.
     • Capacities are reduced, which causes various impacts.
     • Still rely on human expertise to resolve, particularly for strategic decision making.
Decision Support for Strategic ATFM

• Vibrant research effort on strategic ATFM.
  – Weather and weather-impact forecasting.
  – Flow-level models for air traffic and traffic management initiatives (TMI).
  – Planning of TMI: optimization

• Deployment of advanced tools is still challenging.
  – Modeling/forecasting is hard, especially for man-made disruptions.
  – Computational (scalability) issues.
  – Optimizations tend to be black box, don’t give insight into good strategies.
  – Operator buy-in.
Simple Metrics for Disruption Impacts?

• Rather than pursuing detailed modeling, is it possible to get simple insights into potential impacts of disruptions?
  – Disruptions constrain flows or reduce capacity.
  – These cause propagative impacts.
  – Can we measure *vulnerability* to a constraint?
    • How much traffic would be disrupted?
    • How hard would it be to resolve?
    • What is the spatial impact pattern?
  – Can we measure event-specific or system-wide vulnerability?
Previous Work on Metrics

• Weather-impacted traffic index (WITI):
  \[ \sum_{i \in R} W(i)T(i) \]

• Graph-theoretic resiliency metrics.
Proposed Metrics: Concept

• Metrics for *link vulnerability, event vulnerability, and total vulnerability.*

• The proposed metrics aims to capture three drivers of vulnerability:
  – Nominal traffic density on a flow.
  – Local congestion.
  – Availability of alternate routes.

Related to the structure of the network.
Link Vulnerability Metric: Concept

What is the (relative) impact on traffic if each link is blocked?
Link-Vulnerability Metric: Definition

\[ V_{ij} = f_{ij}^\alpha |v_i - v_j|^{\beta} \]

Traffic density on the link during a period of interest.

Laplacian-Fiedler-eigenvector difference across the flow: reflects "importance" of flow (congestion, alternatives)

\[
L = \begin{bmatrix}
2 & -1 & -1 \\
-1 & 2 & -1 \\
-1 & -1 & 3 \\
-1 & 3 & -1 \\
3 & -1 & -1 \\
-1 & 3 & -1 \\
-1 & 2 & -1 \\
-1 & -1 & 3 \\
\end{bmatrix}
\]

\[
eig(L)=
\begin{bmatrix}
0.0000 \\
0.3588 \\
2.2763 \\
3.0000 \\
3.5892 \\
3.0000 \\
4.7757 \\
\end{bmatrix}
\]

\[
v_F=
\begin{bmatrix}
-0.4801 \\
-0.4801 \\
0.1471 \\
0.3482 \\
0.3482 \\
0.4244 \\
0.3482 \\
\end{bmatrix}
\]
Event Vulnerability Metric

• Disruption events often impact multiple flows.
  – Cyber- failure may shut down a Center, weather reduces a Sector’s capacity, etc.
  – Impact on each flow may be partial.
  – Also, impacts may be uncertain at the decision-making horizon.

• The event vulnerability metric captures the (relative) impacts of forecasted events.

\[ V_E = \sum_{(i,j) \in S} p_{ij}V_{ij} = \sum_{(i,j) \in S} p_{ij}f_{ij}^\alpha |v_i - v_j|^\beta \]
Total Vulnerability Metric

- A total airspace vulnerability metric is also defined.
  - Captures overall sensitivity to disruption.

\[ V_T = \frac{\sum_{(i,j)} V_{ij}}{\lambda^c} = \frac{\sum_{(i,j)} f_{ij}^\alpha |v_i - v_j|^\beta}{\lambda^c} \]

Fiedler eigenvalue: captures overall connectivity (eigenvectors only give relative information).
Possible Uses of the Metrics

• Evaluating joint impact of weather and cyber disruptions.

• Identifying bottlenecks or choke points.

• Supporting resource planning.

• Designing TMI strategies.
Metric Evaluation and Validation

• In this initial study, we have focused on evaluating/validating the metrics.

• How?
  – Compare the metrics with predictions from flow-level models of air traffic.
Flow Models for Air Traffic

• Significant effort on flow models of air traffic during the last 15 years.
  – Appealing for STFM because: account for uncertainties, simpler to simulate, naturally represent TMIs.
• Here, a queueing model (Y. Wan, C. Taylor, et al, 2013) and linear approximation (S. Roy et al, 2015) are considered.
Link Vulnerability Metric: Evaluation

- We first study the link-vulnerability metric for a 30-waypoint constructed network.
  - Use the linear flow model.

![Diagram: Total Impact of Each Blocked Flow](image.png)
Evaluation using the Queueing Model

<table>
<thead>
<tr>
<th></th>
<th>Delay</th>
<th>Total Squared Deviation</th>
<th>Metric ($\alpha = 1$, $\beta = 1$)</th>
<th>Metric ($\alpha = 1$, $\beta = 2$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nominal</td>
<td>17.7</td>
<td>0</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Flow 1-4</td>
<td>67</td>
<td>7.6E3</td>
<td>0.60</td>
<td>0.144</td>
</tr>
<tr>
<td>Flow 1-7</td>
<td>19.2</td>
<td>3.2E3</td>
<td>0.19</td>
<td>0.028</td>
</tr>
</tbody>
</table>
Event Metric: Modeling Disruptions

**Weather:** probabilistic models based on ensemble forecasts; Translated to capacity impacts.

**Cyber:**
- Network of information resources needed for management.
- Cyber events disrupt information, hence traffic.
- Simple percolation-type model for blunt cyber disruptions considered here.
Percolation model for cyber threats
Event-Vulnerability Metric: Evaluation

**High-Vulnerability Attack**

*Histogram of Disruption Levels*

Expected flow disruption: 13%

**Low-Vulnerability Attack**

*Histogram of Disruption Levels*

Expected flow disruption: 5%

Event-vulnerability metric: decreases by a factor of 1.5.
Comparing Weather vs. Cyber

• Initial comparison of event vulnerability metrics, for weather vs. cyber events.
  – Model for ZTL.
  – Influence model for weather.
  – Percolation model for cyber threats.

• Preliminary result: much greater variability among event vulnerability metrics for cyber events vs weather ones.
Total Vulnerability Metric: Evaluation

**Total Impact of Each Blocked Flow**

<table>
<thead>
<tr>
<th>Network</th>
<th>Expected Flow Deviation</th>
<th>Metric ($\alpha = 1$, $\beta = 2$, $c = 2$)</th>
<th>Fiedler Eigenvalue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network 1</td>
<td>21.06%</td>
<td>3.33</td>
<td>0.19</td>
</tr>
<tr>
<td>Network 2</td>
<td>7.43%</td>
<td>1.59</td>
<td>.28</td>
</tr>
<tr>
<td>Network 3</td>
<td>15.17%</td>
<td>2.49</td>
<td>.24</td>
</tr>
</tbody>
</table>
For a linear flow model, the perturbation caused by removal of a link can be computed:

\[ D = f_{ij}(e_{ij}^T Z^{-1} e_{ij}) \approx f_{ij}(e_{ij}^T L^{-1} e_{ij}) \], where \( D \) is the total-squared deviation in the flow.

The perturbation can be rewritten as:

\[ D \approx f_{ij} \sum_{q=1}^{n-1} \frac{(v_{qi} - v_{qj})^2}{\lambda_q} \], and can be further approximated as

\[ D \approx \frac{f_{ij}(v_i - v_j)^2}{\lambda} \] provided that the Fiedler eigenvalue is small compared to the others.

Thus, the link perturbation impact is (approximately) proportional to \( V_{ij}(1,2) \).
Cyber Threat Assessment Framework

Detailed Models of Cyber-Architecture/Threats (AADL)

Modeling Cyber-Threats as Queueing-Network Perturbations

Weather-Impact Modeling

Queueing Network-based Threat Assessment and Resolution

Human Operator Threats

Metrics Analysis

Counterfactual “What-if” Analysis

Collaborators: A. Hahn, S. Warnick, S. Das, Y. Wan
Acknowledgements

• This work was partially supported by the U.S. National Science Foundation under grant CNS-1545104, and by the U.S. Department of Homeland Security.

• Questions?

• Contact: Sandip Roy, sroy@eeecs.wsu.edu