Twelfth USA/Europe Air Traffic Management Research and Development Seminar (ATM2017)

Vulnerability Metrics for the Airspace System

Sandip Roy and Mengran Xue
sroy@eecs.wsu.edu, morashu@mail.com

Banavar Sridhar
bensridhar@gmail.com

***Abstract*—Simple topological vulnerability metrics are defined for the air transportation system, that are meant to reflect the impact levels of potential disruptions including severe weather and man-made threats (e.g., cyber attacks). Specifically, a flow-vulnerability metric is defined using the Laplacian matrix of the air traffic network's graph. In turn, event and total vulnerability metrics are posited. The main focus of this study is evaluate and parameterize these metrics using simulations of flow-level models of the airspace system, together with some formal analysis. These simulations suggest that the vulnerability metrics show promise as indicators of disruption impact.**

Keywords-air traffic management, security and resilience, weather impact, threat assessment

I. INTRODUCTION

The United States' air transportation network, collectively known as the National Airspace System (NAS), is an enormously complex agglomeration of engineered devices, cyber systems, and human stakeholders. The NAS is being subject to an increasing diversity of disruptions. Weather remains a primary threat, but man-made events including cyber failures and attacks, kinetic attacks on facilities, and new operational paradigms (e.g., space-vehicle operations, unmanned-system integration) are of increasing concern [1-9]. These disruptions can impact the NAS at several time horizons. At short look-ahead times (a few minutes or less), some disruptions may hinder guidance of traffic by controllers, directly causing degradation of safety and also potentially influencing workload. Meanwhile, the operational changes necessitated by the disruptions (e.g., closure or reduced capacity of Sectors or airports, rerouting of traffic, perhaps staffing changes) may incur impacts on the *tactical management* of regional traffic by the Air Route Traffic Control Center (ARTCC or Center), over a time frame of minutes to a couple of hours. These regional impacts may include delay, increased fuel cost, congestion, and indirectly perhaps safety concerns remote from the event site. The disruptions to Center operations eventually may have propagative impacts across the NAS over a multi-hour period, requiring *strategic management* of traffic (as implemented by traffic management initiatives or TMIs). Thus, the disruptions may cause delays and congestion, necessitate ad hoc decision-making among stakeholders, and increase fuel costs. Indeed, several recent non-weather disruptions, such as the closure of the Washington DC Center (ZDC) in summer 2015, had propagative impacts across the NAS.

At the shorter time horizons, resolving disruptions depends on the procedures and tools used for air traffic control, along with fast remediation of the disruption cause if possible. Because of the potential safety implications, much effort has been made to robustify the air traffic network to disruption impacts at this fast time scale [10,11]. While catastrophic short-term impacts of disruptions remain a grave concern, the protocols in place have been consistently successful in preventing such impacts for the recent man-made disruption events. In contrast, the recent disruptions have incurred significant impacts at the longer tactical and strategic horizons, and severe weather also routinely degrades NAS performance at these look-ahead horizons. Further, disruptions at the longer horizons are primarily addressed by human decision-making rather than fixed procedures and automation, hence making the decisions both amenable to improvement and subject to second-guessing. The economic costs of these longer-horizon impacts are significant, and continue to grow as traffic densities increase and disruptions become more varied.

The challenges associated with regional and NAS-wide traffic management have motivated a vibrant research and development effort, which is primarily focused on decision-support for management in the face of severe weather [12-25]. Recently, engineers have also recognized the possible impacts of other man-made disruptions [7,10,26,27], and some preliminary efforts are underway to examine and resolve these impacts. Broadly, tools for analysis and management design depend on models for the traffic in the NAS. For regional tactical management, detailed models that track individual aircraft can be used to evaluate performance of management schemes, and optimal management design typically resolves to a scheduling problem. At the NAS-wide scale and strategic (full-day) horizon, the extent of uncertainty and problem scope often dictates the use of flow-level or Eulerian models for design of management, whereupon more detailed models can be used for simulation. Model-driven analyses of air traffic management are now well established and efforts to design management initiatives using the models have also been fruitful, although the translation of the results to field operations is still piecemeal. While the focus of this literature has been on severe weather, some of the simulation tools can be adapted for analysis of man-made disruptions also.

The methods for analyzing and designing against disruptions depend on some forecast knowledge about the threat, such as a stochastic forecast of severe-weather futures [15,28-31]. As the threats to the transportation network become increasingly varied, and include entirely unpredictable events like cyber-system failures, analysis and design of management strategies that operate robustly across the ensemble of possible threats and traffic futures is made difficult. Additionally, even in the case of forecast disruptions like weather, there is a need for management procedures and strategies that are effective over many operational scenarios; current approaches struggle to achieve such robust designs and even to evaluate and monitoring design performance across operational scenarios. Analysis of robustness is further complicated by the difficulty inherent to quantifying performance, which requires weighing and combining multiple factors (e.g., delay, fuel cost, implementability, etc). In short, these concerns make direct model-based analysis and design of robust strategies difficult.

An alternative approach for evaluating robustness and building robust designs is based on simple metrics. The idea is that disruption impacts are roughly tied to simple structural features of the NAS, and the location of the disruption relative to the structure. Robustness or conversely vulnerability metrics that encapsulate these salient features can be compute from limited knowledge of the network, and subsequently robust designs can be found based on these metrics. In this way, robustness/ vulnerability can be understood in a way that that is abstracted from the specific modality of the disruption, and the details of the infrastructure dynamics.

The focus of this study is to establish easy-to-compute, topology-based vulnerability metrics for the air traffic management system. The metrics that we explore are meant to distinguish the following characteristics:

1) The relative vulnerabilities of different traffic flows, or sets of traffic flows, to disruptions.

2) The spatial and temporal extent of the impact incurred by a disruption to a set of flows.

3) The overall susceptibility of the network to completely unknown or stochastically-modeled disruptions.

The metrics that we propose are based on matrix-theoretic and graph-theoretic representations of traffic flows in the NAS. The rationale underlying the proposed metrics is very simple: disruption of a traffic flow has large impact if 1) the nominal flow is large, 2) the flow path is subject to congestion, and 3) good alternative paths are not available. Based on this simple rationale, robustness metrics for vulnerabilities of individual flows are defined based on Laplacian matrix representations of the traffic flow network, and nominal traffic flows. These metrics can then be combined to capture overall vulnerability. We notice that metrics are aligned with the *weather-impacted traffic index (WITI)* [45], but differ in 1) capturing mixed weather and man-made disruptions and 2) explicitly considering impacts on traffic flows.

This initial study on robustness metrics is focused on defining the metrics (Section 2), and then testing them using more detailed simulations of mixed man-made and weather disruptions to an air traffic network as well as limited formal analysis (Section 3). The study is then briefly concluded.

II. Vulnerability metrics

Air traffic managers primarily view the airspace at the resolution of traffic flows. Given this perspective, it is natural to define building-block metrics for *robustness* or conversely *vulnerability* in terms of traffic flows, specifically how tolerant the airspace is to disruption of individual flows. Here, simple flow vulnerability metrics are defined, that are meant to capture the impact (delay, rerouting, workload) caused by blockage of individual traffic flows. In turn, these flow-level metrics are used to define aggregate vulnerability metrics for wider NAS-relevant events (e.g., closure of a Sector, or delay of an airline's fleet due to a cyber problem), as well as a metric of overall network vulnerability.

Precise evaluation of disruption impacts requires simulations of detailed air traffic models (e.g. [11]), however our aim here is to develop abstract metrics that are based on the connectivity of the NAS and nominal flow densities. Specifically, our metrics are defined from a *flow graph* of the full NAS, or a region in the NAS of interest, along with nominal flow densities. Formally, traffic flows among a network of n waypoints or *nodes*, labeled $1, \dots n$, are considered. We notice that these nodes may be chosen at the appropriate level of aggregation required for the decision-making task. In particular, they may represent specific waypoints used in reality in the traffic system, or may be aggregate constructs representing a set of waypoints. For regional and NAS-wide management problems, often it is appropriate to aggregate traffic flows to the Sector resolution, in particular using nodes to represent Sector boundaries and midpoints [11]. If arrival and departure flows at major airports are of interest in the vulnerability analysis, then additional nodes can be introduced for each airport.

Regardless of the chosen model resolution, the *flow graph* Γ is defined as a digraph with n vertices, which correspond to the n network nodes. A directed edge is drawn from vertex i to vertex j if and only if direct traffic flow is possible from node i to node j. Thus, the flow graph Γ captures the connectivity of the airspace. The flow graph is typically symmetric since bidirectional flows are allowed (i.e., if traffic flows are permitted between two waypoints in one direction, traffic flows in the alternate direction are also permitted at a different elevation). The nominal forecasted traffic flow from node i to node j during a time period of interest is denoted by f_{ij}. Even though the flow graph is typically symmetric, the flow densities f_{ij} and f_{ji} are usually different.

In this work, the flow vulnerability metrics are defined solely from the flow graph and the nominal traffic flows. Particularly, the *Laplacian matrix* L of the flow graph is used to define the metrics. The Laplacian matrix is a useful construct for measuring vulnerability, for two reasons. First, the Laplacian is known to directly identify connectivity properties of networks [32] that play a key role in deciding vulnerability (e.g., the availability of alternative traffic paths for a disrupted flow). Second, the Laplacian matrix defines linear flow or diffusion dynamics in networks, and hence can be used to approximate disruption impacts to network flow processes [33]. Formally, the Laplacian matrix of the flow graph is an nxn matrix, whose entries are specified as follows. The entry L_{ij} at row i and column j where $i \neq j$ is set to -1 if there is an edge from vertex i to vertex j in the flow graph, and is set to 0 otherwise. Meanwhile, the diagonal entries of the directed Laplacian matrix are chosen so that each row sums to zero, i.e. $L_{ii} = -\sum_{j \neq i} L_{ij}$. Thus, the directed Laplacian matrix captures the connectivity of the airspace, analogously with the flow graph. For the traffic network, the Laplacian is typically symmetric. The Laplacian matrix has been used in several previous studies of the air traffic system, e.g. [34].

The connectivity properties of the flow graph, and hence in our case the traffic network, are well known to be related to the spectrum (eigenvalues, eigenvectors) of the Laplacian L. Specifically, for a connected graph,, the Laplacian matrix is known to have a single eigenvalue at the origin in the complex plane, while the remaining eigenvalues are in the open right half plane (i.e., have real parts strictly greater than zero). In the case where the Laplacian matrix is symmetric (which is typical in our context), the remaining eigenvalues of the Laplacian are real and positive. Further, the right eigenvector $\boldsymbol{v}$ associated with the smallest nonzero eigenvalue λ of the Laplacian matrix (called the Fiedler or subdominant eigenvalue), normalized to unitl length, is known to characterize the connectivity properties of the flow graph. Relevant to the metric definitions pursued here, the absolute difference $|v_i - v_j|$ between entries i and $j$of the Fiedler vector is an indicator of the presence or absence of alternative short paths between vertices i and j in the graph, and hence between nodes i and j in the traffic network. Specifically, if the absolute difference $|v_i - v_j|$ is small, many short paths are present; conversely, if the difference is large, then only sparse and long paths are available. In the case that the Laplacian matrix is asymmetric, its eigenvalues are not necessarily real. In this case, the absolute difference in eigenvector components $|v_i - v_j|$ for the eigenvector associated with the smallest-magnitude non-zero eigenvalue can be used as a measure of connectivity.

The vulnerability of a traffic flow to disruption is closely connected to the nominal density of the flow, and the alternate paths available for the flow. In particular, as the nominal density increases and fewer short alternative paths are available, the disruption of the flow should have larger impact (more constriction and rerouting of traffic, hence larger delays and costs). Thus, this vulnerability can be naturally measured in terms of the eigenvector-entry difference for the two ends of the flow, along with the nominal flow density. This motivates the following vulnerability metric for the traffic flow from node i to node j:

$$V_{ij} = {f_{ij}}^{\alpha} |v_i - v_j|^{\beta} \,, \tag{1}$$

where the constants α and β are positive integers that weight the sensitivity of the metric to the flows and eigenvector-component differences, respectively. In the subsequent simulations and formal analysis, we will consider several choices for the weighting parameters α and β. In particular, simulations and formal analysis will show that $\alpha = 1$ is often the appropriate choice, while there is a rationale for choosing β as either 1 or 2. We notice that the flow vulnerability metric is a nonnegative quantity, with larger values corresponding to higher vulnerability.

Most disruptions to the air traffic system, whether man-made or natural, impact a set of flows rather than a single one, and also often are probabilistic in nature at the decision-making horizon. For instance, convective weather may close an airport or runway, or reduce the capacity of a Sector thus constraining all associated flows. There is significant uncertainty in this capacity impact at a strategic or even tactical look-ahead. Likewise, the recent cyber- disruptions to the airspace system have impacted flows across a wide area (e.g., closure of a Center's airspace, modification of an airline's traffic flows). Generically, a disruption event E can be modeled as constraining a set of flows S (where each flow in the set is identified by a pair of nodes). Abstractly, the event can be viewed as constraining a fraction of the flow, or constraining the flow with some probability. We designate the fraction or probability of impact as p_{ij}.The overall impact of the disruption event can be estimated by weighting and summing the impact due to each constrained flow, as specified by the flow vulnerability metric. Specifically, an *event vulnerability metric* is defined as follows:

$$V_E = \textstyle\sum_{(i,j)\in S} p_{ij} V_{ij} = \sum_{(i,j)\in S} p_{ij} {f_{ij}}^{\alpha} |v_i - v_j|^{\beta}. \tag{2}$$

The event vulnerability metric approximates the total impact of multiple flow disruptions as the sum of the individual impacts. In this sense, it does not explicitly capture higher-order interactions among the disruptions; nevertheless, we contend that the metric is a good indicator of disruption vulnerability.

Finally, a *total vulnerability metric* which represents the overall sensitivity of the network to disruption, or the expected impact level of a completely unmodeled disruption, can be defined. At first glance, it seems natural to define the total-vulnerability by summing the vulnerabilities of each flow in the network. However, the flow vulnerability metric only captures the relative impacts of different flow disruptions: since the metric is based on eigenvector components, absolute information about the vulnerability of one traffic network configuration compared to another may be lost. To capture the total vulnerability, it is therefore useful to also incorporate a measure of the overall connectivity of the network. The overall connectivity is reflected in the Fiedler eigenvalue of the Laplacian matrix, with smaller eigenvalues corresponding to less connected (and hence more vulnerable) networks. This observation motivates the following total vulnerability metric:

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

where the summation is taken over all flows in the airspace system, and c is a positive constant that will be tuned later based on later simulations and formal analysis.

III. Evaluating the Metrics: Simulations of Cyber- and Weather Disruptions

The vulnerability metrics are evaluated using a layered dynamical model for the air traffic system, which captures traffic at the resolution of flows, cyber and other man-made disruptions, and severe weather. The layered model, which was originally introduced in [7,12,26], is reviewed (Section III.A). Then, simulations and formal analysis of the model are used to evaluate the effectiveness of the link vulnerability metric (Section III.B). Finally, the performance of the event and total vulnerability metrics is evaluated, via simulation of the layered model for complex cyber and weather disruptions (Section III.C). Several examples are considered in the section.

A. Layered Network Model

A network model with three layers is considered: 1) a traffic layer which captures air traffic at the resolution of major flows and also major controls (e.g. traffic management initiatives such as GDPs and AFPs); 2) a cyber- layer that abstractly represents the information flow among stakeholders (airline dispatch offices, Centers, ATCSCC) required for operations, and the impacts of this information flow on traffic; and 3) a weather layer that tracks forecasted severe weather impacts on traffic and capacities. The model as whole comprises a multi-layer nonlinear flow and queueing network model, which has structured interfaces between the layers (Figure 1). The presentation of the layered network model closely follows the development in [26], but the discussion is enhanced slightly to give a common framework for the influence of weather and cyber events on traffic flows.

The models for traffic flow and weather considered here have been widely studied in the literature, hence we only briefly review them here. Specifically, two models for the traffic and management layer are considered here, which were introduced in [11,13,35,36]. The models fall within the broad class of flow- and queueing- models, or Eulerian models, that represent aggregate flow densities or traffic counts rather than individual aircraft positions [14]. The more sophisticated model considered here represents traffic at the resolution of inter-Sector flow densities in an *area of interest* with high congestion or severe weather, and at a lower resolution outside the area of interest. Specifically, traffic is modeled using overlaid flow networks for different origin-destination (OD) pairs, see Figure 1a. Flows are routed at aggregate ``waypoints", which represent Sector boundaries in the area of interest and are even more aggregate outside. Structured queueing elements are used to represent traffic management initiatives such as ground-delay programs, airspace flow programs, miles-in-trail or minutes-in-trail. Queues also are used to model intrinsic capacity restrictions on airspace resources (e.g., Sector capacities, arrival and departure rate constraints). Demand is modeled as having a deterministic component which represents scheduled traffic, and a stochastic component which reflects schedule uncertainty and pop-up traffic [19]. Resource capacities are modulated by forecasted weather dynamics, see discussion on the weather layer below. Model parameters – including the flow-network structure, demand profiles, possible traffic management initiatives, and nominal capacities – are obtained from archived data along with day-of-operations data. The queueing model has been evaluated for several historical bad-weather days, and has been shown to provide adequate forecasting of traffic characteristics. The model has also been used for tuning of traffic management initiatives [20,21]. We refer to the model in brief as the nonlinear queueing-network model for the airspace system.

A simpler linear Eulerian model for the airspace system is also considered [35]. This model follows on the Eulerian models for traffic flow densities and regional aircraft counts developed in [13,14,36]. Specifically, traffic flows or densities are modeled at the Sector resolution, as with the queueing model. However, routing and traffic management actions are not modeled in detail; instead, traffic is fractionally routed at waypoints, and can be viewed as diffusing through the network. The simpler model can be obtained through a stochastic linearization of the queueing network model, and takes the form of a driven resistive-capacitive circuit model (Figure 1a). The linear model has been shown to be effective in estimating the spatial and temporal impact of disruptions, see [35]. We refer to the model as *the linear Eulerian model*.

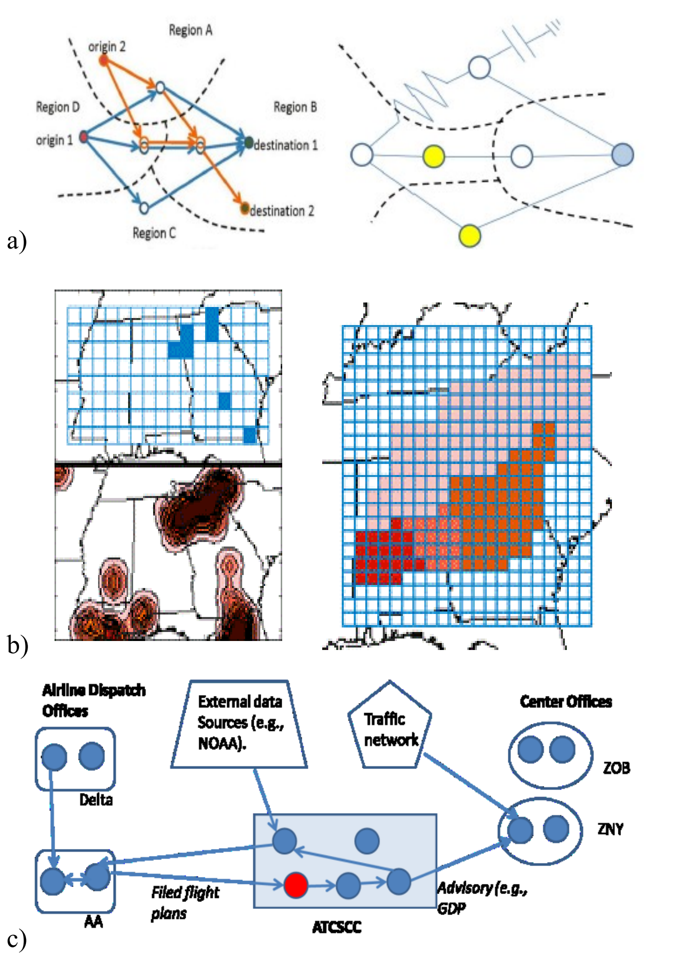

Figure 1: a) Nonlinear queueing-network model and linear Eulerian model; b) A stochastic automaton is used to generate weather-impact (capacity reduction) scenarios that match ensemble forecasts; c)

Weather significantly modulates *en route* and terminal area air traffic, and hence modeling the traffic management system requires modeling of forecast weather. At the longer decision-making horizons, weather is subject to significant uncertainty, and hence appropriate statistical forecasts of weather are needed. Although statistical weather forecasting tools are available in the public domain , these tools often do not output weather data at the proper resolution for traffic management, and also do not capture the regional-scale variabilities and uncertainties in forecast weather. In our previous work, we have used a stochastic automaton network known as the influence model [27-31] to represent the spatiotemporal progression of severe convective weather, so as to forecast *en route* capacity impacts. The main idea is to parameterize the influence model to statistically match public-domain forecasts at snapshot times, whereupon the model can be run and analyzed to get interpolated forecasts at desired resolutions and to capture small-scale variabilities in weather evolution. The convective coverage predicted by the model can then be translated to a reduction in the en route capacity. Meanwhile, airport capacity trajectories can be computed from local wind, ceiling, and convection variables in ensemble forecasts or terminal aerodrome forecasts. The weather layer of the proposed model includes the spatiotemporal models for weather evolution, and their translation to airport and en route capacities, see Figure 1b. The weather layer is interfaced with the traffic layer in that causes probabilistic reductions in en route and terminal area capacities; for the queueing model, the reductions are applied explicitly to capacity or queueing variables, while for the linear Eulerian model the reductions translate to blockages or reductions on link flows (reduction of link conductances, from the circuit equivalent standpoint).

In our recent work [26], flow-level models for the airspace system have been extended to abstractly represent the cyber infrastructure, with the goal of modeling disruptions that arise via the cyber system. The cyber model is discussed in detail here. To begin, we note that the modern air traffic system uses numerous networked cyber assets for traffic control and management. Relevant to this effort, control of aircraft for collision avoidance is undertaken by human controllers located in about 20 regional offices, known as Air Route Traffic Control Centers (ARTCCs or Centers), which are each responsible for a partition of the United States' airspace. At each Center, a small group of controllers (typically 3-5) are assigned to each Sector in the Center's airspace, and are responsible for the control of aircraft in the Sector. The controllers for each Center rely on a number of cyber- systems, including radar displays of aircraft and weather, collision alert tools, and computer systems that provide directives from traffic managers. In similar fashion, controllers for the Terminal Radar Approach Control facilities (TRACONs) associated with major airports, as well as airport-control tower personnel, have numerous cyber tools which provide radar data, filed flight plans, and relevant weather data. Meanwhile, wider-area and longer-term traffic management is undertaken via coordination of traffic managers at the regional offices, the central command center (Air Traffic Control Strategic Command Center or ATCSCC), and major commercial airlines. The personnel involved in traffic management also use numerous cyber tools, including weather and traffic data sources, telephone as well as web-based communication, simulators, etc.

Holistically, the cyber system acting in support of the air traffic system can be viewed as transmitting the information that is necessary for effective traffic management and control. This cyber system comprises a mixture of specialized information transfers for the air traffic system and generic information gathering from the broader Internet (e.g., public-domain weather forecasts). The systems used by traffic managers are very often networked to the broader web, whether for required data transmission or for convenience. To the best of our knowledge, cyber systems used in the airspace system use only standard protection technologies (e.g., standard firewalls and virus-checking software, limited or no encryption). They may be subject both to failures and to deliberate software and hardware attacks, and indeed both types of threats have been observed.

In this work, we abstractly model the cyber system as a network of information resources that are necessary for control and management of traffic, see Figure 1c. Under nominal conditions, each piece of information is modeled as being present, which then allows control and management. The main purpose of our cyber-layer model is to represent disruptions to the needed information resources (which are the nodes in our network model). These disruptions then cause changes to the traffic network, which are modeled as the interface between the cyber and traffic layers.

Formally, an information network with m nodes labelled $i = 1, \dots, m$ is considered, which each node represents an information resource needed for traffic management and control (e.g., the flight manifest data that are needed by a Center's traffic managers, etc). Each node is modeled has having a nominal state `Normal' or `N', which indicates that the information content is available and uncorrupted. During a particular operational period of interest, each node may transition to a failed state (`Failure' or `F') which indicates that the information content associated with the node is unavailable, whether due to a failure or an attack. The state of node i during the period of interest is referred to as $x(i)$.

Two probabilistic models for failure are considered. In the simpler model, an attack or failure event is modeled as causing the state $x(i)$ of each network node to be `F' with probability $p(i)$, independently of all other nodes. This simple model for failures is descriptive of independent component failures, which cause individual information resources to become unavailable. The model also encompasses structured deterministic failure scenarios where the failure of a fixed set of information resources needs to be evaluated (e.g., during post-processing after a failure or event, or for common failure paradigms). The model further captures certain cyber-attacks, for which information resources are independently impacted. For instance, phishing attacks wherein an attacker sends an e-mail with a computer-virus file attached to many recipients may be modeled in this way. In this scenario, personnel who are responsible for traffic control each have some probability of independently receiving and opening the attack e-mail using a particular cyber system, causing failure of the system for a period of time. Thus, a model where each cyber resource is independently disrupted with some probability is apt.

A second, more sophisticated model for cyber disruptions is also considered. This second model reflects that information flows among resources according to a specified network, and hence disruptions of information flow may be correlated. Specifically, the model captures that information disruptions may propagate through the cyber network. This type of propagative disruption in cyber systems has been studied widely, in the context of computer-virus spread, cascading failure modeling, and other contexts [38-40]. Numerous probabilistic models for propagation or spread have been proposed. Here, a stochastic percolation model for disruption propagation is considered. Specifically, first each node i in the network is modeled as probabilistically being infected (having a failed status) with some probability, say $p_0(i)$; this is the initial stage (stage *k=0)* of the infection. In further stages of the infection, each node that has just been infected has some probability of infecting further nodes. Specifically, at stage k, each node i that was infected at stage $k\text{-}1$ infects any neighboring node j with probability $p_k(j,i)$, where the neighbors of a node are specified by the digraph Γ. The infection process continues until no new infections are produced. We notice that the percolation model generalizes the simple probabilistic-failure model, by capturing cascading impacts of failures in the information-flow network. The percolation model is useful when the failure of one cyber system implicates an impact on other information resources used in traffic control and management: for instance, the failure of systems which store flight manifests may simultaneously impact information resources at multiple Centers.

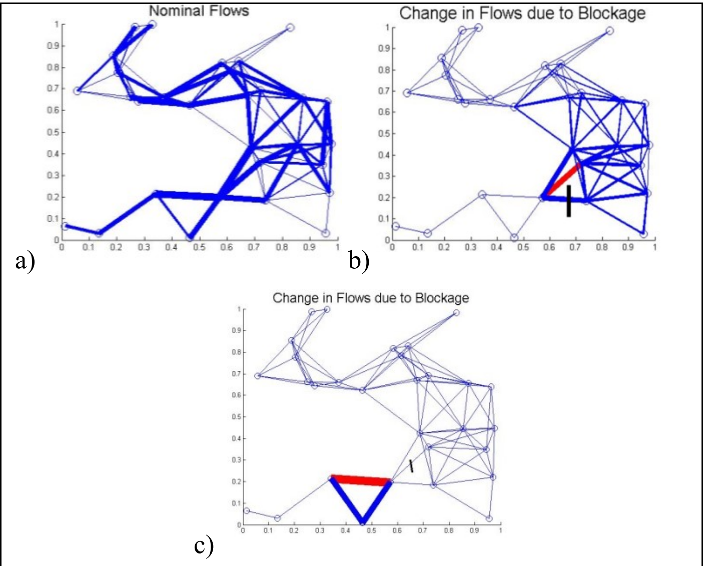
Nominal Flows
Change in Flows due to Blockage
Change in Flows due to Blockage
a)
b)
c)

Figure 2: a) Nominal traffic flow densities are diagrammed, in a small constructed network with 30 waypoints. b) c) The redistribution of traffic caused by the blockage of a flow is shown, for two different flows (red colored edge in the graph).

The cyber- layer of the model is interfaced with the traffic layer as follows. Each information resource is viewed as being necessary for operation of some airspace resources over a time period of interest– for instance, a major flow or jet route, a sector or group of sectors, or one airline's traffic. Thus, information-resource failures modulate the associated traffic resources' parameters for their nominal values. Specifically, airspace resources such as Sector or flow capacities may be curtailed, demand patterns may be altered, traffic management initiatives parameters (e.g., rates, scope) may be modified, etc. Thus, the traffic models parameters and inputs are changed over an interval in reflection of the information-layer failures.

B. Evaluation of the Link-Vulnerability Metric

Simulations of the traffic network model are undertaken to evaluate whether the defined link-vulnerability metric is indicative of the impacts caused by flow disruptions. Two examples are considered, one based on the linear Eulerian model and the second based on the detailed queueing-network model. For each, the total impact of individual flow blockages, as measured by integrated change in traffic flows across the network and the delay imposed, is computed. These simulated impacts are compared with the link-vulnerability metric for each flow blockage. In addition to the examples, a formal analysis of the linear Eulerian model is undertaken to give insight into the vulnerability metric.

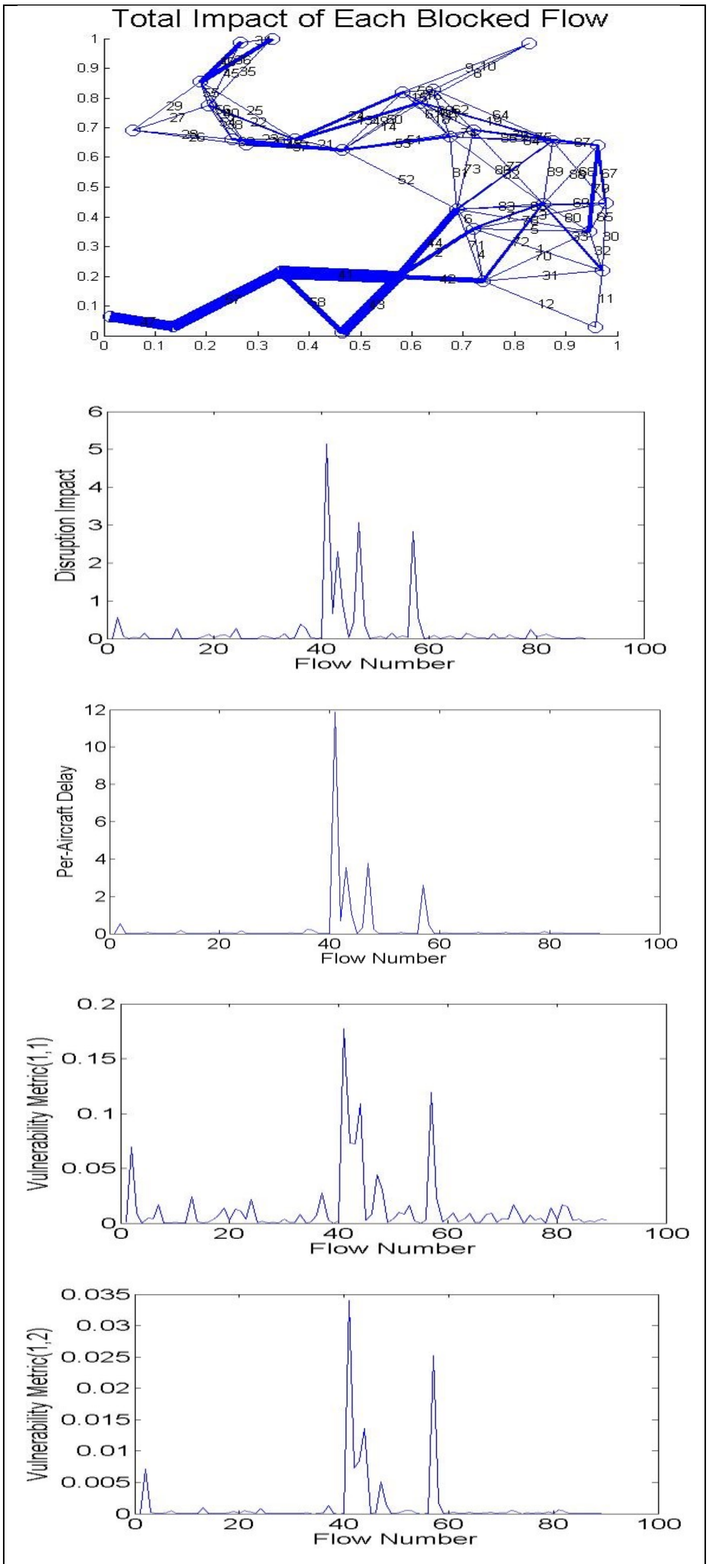

Figure 3: a) The total disruption impact, in terms of total squared deviation in traffic, is illustrated for blockage of each flow in the network. b) The disruption impact is plotted vs. blocked flow number. c) The delay incurred is plotted vs. the blocked flow number. d),e) The flow vulnerability metric is plotted vs flow number, for two choices of the parameters.

B.1. Linear Eulerian Model

First, traffic flow on a constructed network with 30 waypoints is simulated using the linear Eulerian model, see Figure 2a. Traffic to three destination airports from 10 origin points (which may represent either origin airports or points at which flows enter from outside the modeled region) is considered. The nominal flow densities on the links are shown in Figure 2a.

The spatial impacts on network-wide traffic of two individual flow disruptions are shown in Figure 2. Specifically, Figures 2b and 2c show the magnitudes of the changes in flow densities due to blockage of a particular flow. Simulations of this sort indicate that the most drastic changes occur on flows that are proximal to impacted flow, and particularly on routes that are alternatives of the blocked flow. The transient responses indicate a traveling-wave phenomenon, wherein alternative routes are quickly impacted, immediate downstream flows show a fast bimodal response (i.e., decrease followed by increase), and locations further away have a more limited and slower transient. The spatial characteristics of the simulated disruptions suggest that, indeed, disruptions of large flows with few alternative paths have larger impacts, which the defined flow-vulnerability metric should capture.

In Figure 3, the total flow disruption caused by a blockage on each link is compared with the defined flow vulnerability metric, for the constructed network. Figure 3a illustrates the disruption impact caused by the blockage of each flow. Specifically, the disruption impact is computed by finding the integrated squared deviation between the traffic density for each flow without and with the blockage, and then summing over the flows. Figures 3b-e compare these disruption impact levels as well as delays incurred by the disruption with the vulnerability metric for two choices of α and β. Figure 3b shows the disruption impacts for each flow, and Figure 3c shows the approximate delay per aircraft for each flow blockage (please see [13,35] for the estimation of delays from linear Eulerian models). Figure 3d shows the vulnerability metric for $\alpha = 1$ and $\beta = 1$, and Figure 3e shows the vulnerability metric for for $\alpha = 1$ and $\beta = 2$. The plots show that both metrics correctly identify the five most vulnerable flows, i.e. the five flows which incur the largest deviations and cause the most additional delay. While both metrics are able to distinguish vulnerable flows, the metric for $\alpha = 1$ and $\beta = 2$

better predicts the relative magnitudes of the disruption impacts caused by each flow blockage. Likewise, this form of the metric better predicts the excess delay caused by the blockage. Based on the simulations of the linear Eulerian model, the flow vulnerability metrics appear promising as indicators of flow disruption impacts.

B.2. Detailed Queueing-Network Model

The flow-vulnerability metrics are also evaluated using the detailed queueing-network model for traffic flow. Evaluation using the more sophisticated model is important, since this model has been validated as a tool for predicting delays and congestion, and also designing traffic management schemes. Here, an example network with 16 waypoints within 6 Sectors is considered (Figure 4), which was originally developed by Wan and co-workers in [26], and has been considered in several further works (e.g., [7,26]). The example uses a realistic demand model for traffic between four origin-destination pairs, captures Sector and link-level traffic constraints, and allows representation of flow-management actions (including ground and en route holding, as well as rerouting).

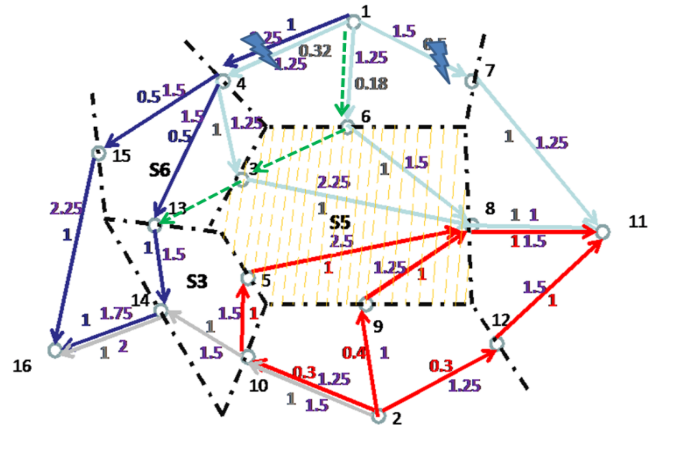

Figure 4: The flow-vulnerability metrics are evaluated using the nonlinear detailed queueing-network model, for the example shown here (with 16 waypoints, 6 sectors, and 4 O-D pairs). The flow disruption and delay caused by the failure of two links are evaluated, and compared with the flow-vulnerability metric.

The flow-vulnerability metric has been computed for the 24 links in the network. The metric indicates that the three most vulnerable flows are 10-14, 1-4, and 2-10, see Figure 4. To evaluate the metric, we compare the performance degradation due to the blockage of one of these vulnerable flows (1-4) with the degradation caused by another less vulnerable link (1-7), see Figure 4. For each link blockage, a realistic traffic management strategy involving re-routing is implemented. Specifically, blockage of the flow 1-4 requires re-routing of traffic for two O-D pairs (1-11 and 1-16). This traffic is distributed on alternate routes that are already being used, as well as via the new route shown with green dashed arrows. When the flow 1-7 is blocked, only traffic for the OD-pair 1-11 needs to be rerouted; this traffic is distributed on the available alternate routes. These strategies reflect the corrective actions that might be taken in response to an unexpected flow restriction (which might arise e.g. because of weather or communication problems between Sector controllers). The total deviation in traffic flows from nominal and the total delay are compared. The results are shown in Table 1.

The analysis shows that the vulnerability metrics are promising. In particular, both vulnerability metrics are significantly larger for Flow 1-4 as compared to Flow 1-7, and indeed the blockage of Flow 1-4 causes a more significant impact as compared to the blockage of Flow 1-7. Specifically, the blockage to Flow 1-4 causes an overall modification of flows that is about twice as large as the blockage of Flow 1-7. Also, the blockage of Flow 1-7 only causes minor excess delay, (about 10% more delay), while the blockage of Flow 1-4 causes much larger delay (almost 300% excess delay). The metrics readily capture the significant increase in the impact. It is worth noting that the flow vulnerability metric with $\alpha = 1$ and $\beta = 1$ scales comparably to the total flow deviation. However, the excess delay is much more sensitive to the blocked flow. The high sensitivity is expected, since delays grow in a nonlinear fashion with the flow density when a capacity threshold is exceeded. While our initial effort has focused on two flows for comparison, a comprehensive study of all flow disruptions will be undertaken in a final draft.

	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

Table 1: The flow vulnerability metric is compared with the delay and total squared flow deviation resulting from blockage of the flow.

B.3. A Formal Justification of the Metric

The two examples show that the link-vulnerability metric is surprisingly effective as an indicator of the impact caused by a flow blockage or disruption, particularly for the parameters $\alpha = 1$ and $\beta = 2$. The linear Eulerian model enables a formal analysis of the link-vulnerability metric, which gives some insight into why the metric is predictive of disruption.

The disruption impact of a link failure can be computed for the linear Eulerian model precisely because of its linear and diffusive structure. In particular, because of the model's linearity, the flow deviation across the network caused by a link blockage can be computed via a superposition argument, considering only the flow that is blocked. In particular, it is easy to check that total squared deviation of flows across the network due to blockage of the flow between nodes i and j is given by:

$$D = f_{ij}(e_{ij}^T Z^{-1} e_{ij})$$

where e_{ij} is an $n\,x\,1$ column vector whose ith entry is 1, jth entry is -1, and all other entries are zero; Z is the $n\,x\,n$ diffusive state matrix governing the Eulerian dynamics, $(\ )^T$ represents the transpose of a vector, and the matrix inverse is in fact a pseudo-inverse (notice here that a diffusive matrix does not have full rank), see [41,42]. For the Eulerian model, the state matrix Z has exactly the same zero pattern and structure as the Laplacian matrix L, except for the blocked flow. In fact, the state matrix can be roughly approximated by the Laplacian matrix, which yields that the total squared deviation is given by:

$$D \approx f_{ij}(e_{ij}^T L^{-1} e_{ij})$$

where the inverse is again technically a pseudo-inverse. By substituting the eigenvalue decomposition for L into the expression and performing simple matrix algebra, the total squared deviation can be written as:

$$D \approx f_{ij} \sum_{q=1}^{n-1} \frac{(v_{qi} - v_{qj})^2}{\lambda_q}$$

where $\lambda_1, \dots, \lambda_{n-1}$ are the nonzero eigenvalues of L, $v_1, \dots, v_{n-1}$ are the corresponding eigenvectors, and $\lambda_1 = \lambda$ and $v_1 = v$ are the Fiedler eigenvalue and corresponding eigenvector. We notice that λ_1 is smaller than $\lambda_2, \dots, \lambda_{n-1}$ by definition, and is significantly smaller for many planar graphs which are representative of the air traffic network [44]. Thus, the total squared deviation can be further approximated as

$$D \approx \frac{f_{ij}(v_i - v_j)^2}{\lambda}.$$

This expression shows that the relative disruption impact, as measured by the total flow deviation, is proportional to$f_{ij}(v_i - v_j)^2$. Thus, the flow vulnerability metric with $(\alpha = 1, \beta = 2)$ is justified.

C. Evaluation of the Event and Total Vulnerability Metrics

The event and total vulnerability metrics are also evaluated using simulations. Three examples are considered. The first example is concerned with probabilistic cyber attacks on the constructed 30-waypoint network. The second example, briefly developed, is concerned with probabilistic weather and cyber disruptions in the Atlanta Center. The third example compares the total vulnerabilities of constructed networks with different topologies.

C.1. Cyber-Attack Vulnerability Assessment

The constructed 30-waypoint example developed in Section III.B.1 is studied. Specifically, the linear network model is overlaid with the cyber-disruption model, as described in Section III.A. The independent-failure model for cyber events described in Section 2 is considered here, as a means to capture a phishing attack. Information disruptions in the cyber system are assumed to block flows in the traffic network. Specifically, for the example considered here, each information resource corresponds to an individual flow in the traffic network. The information resource is modeled as failing, according to the random-choice or percolation-type model described before. The probability of blockage of each flow in the traffic network can be computed via formal analysis of the percolation model, and hence the event vulnerability metric can be computed.

Monte Carlo simulations have been undertaken of attacks with two virulence levels (probabilities of failure of individual information resources). The event vulnerability metric has also been computed in each case, for $\alpha = 1$ and $\beta = 2$. The event vulnerability metric for the more virulent attack is a factor of 1.5 larger than the event vulnerability metric for the less virulent attack. In Figure 5, histograms of the percentage flow disruption are shown for each attack (using 100 Monte Carlo simulations). The expected flow disruption increases from 5% to 13%, which is a similar scaling to the vulnerability metric. We notice that the shape of the histogram changes significantly between the low- and high- virulence attacks, even though the vulnerability metric and expected disruption scale commensurately.

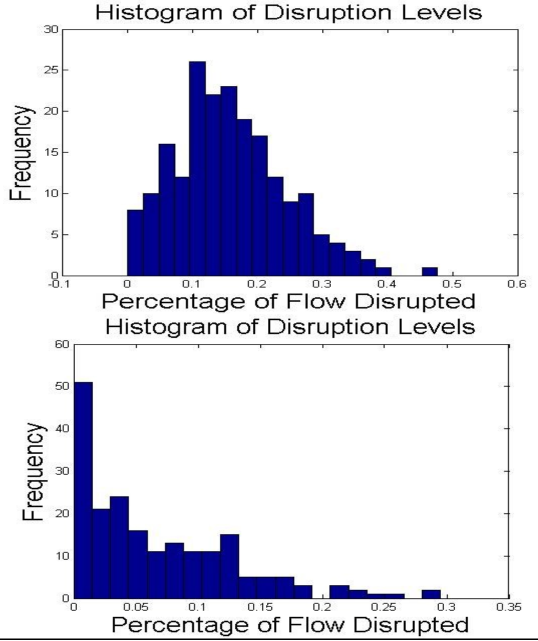

Figure 5: Histograms of the flow disruption percentage are shown based on 50 Monte Carlo simulations of cyber- attacks, for phishing attacks with two virulence levels. The upper plot corresponds to a more virulent attack, and the lower plot to a less virulent attack.

C.2. Weather and Cyber Vulnerability Assessment for ZTL

We are pursuing computation of event vulnerability metrics for ZTL, for cyber- attacks that close high-altitude Sectors as well as for forecast weather disruptions for a historical case-study day. The analysis is being conducted as follows. The ZTL airspace has been modeled at the resolution of Sector-midpoint-to-boundary flows, and the construction of the associated Laplacian matrix then allows computation of the flow-vulnerability metrics. Event vulnerability metrics are then computed from the flow-vulnerability metrics. In particular, cyber-attacks are modeled as closing a Sector's airspace: such closure may result for instance if the radar for the Sector's controllers is attacked, or communications between the controllers and aircraft are targeted. For the weather disruptions, the influence modeling tool has been used to generate representative weather-impact scenarios for a historical weather day, which specify flow-impact fractions for each Sector over a time duration (see [28-31], also Figure 1b). These fractions will be used to compute the event-vulnerability metrics. Results of this analysis, and comparisons with detailed simulation and WITI metrics, will be included in the final draft.

C.3. Total Vulnerability Metric

Three different constructed networks with 30 nodes have been studied to evaluate the total vulnerability metric. Specifically, for the three networks, the linear Eulerian model has been used to determine the expected deviation in flows caused by an entirely unknown disruption to the network. This disruption level is compared with the total vulnerability metric in Table 2. For the metric computation, the parameters used are $\alpha = 1$, $\beta = 2$, and $c = 2$. The value of c was to best capture the scaling in the expected flow deviation among the networks; it was found that c between 2 and 3 best captured the scaling. The least vulnerable network shown in Figure 6, as a comparison to the most vulnerable one (Figure 3a). As expected, sparsely connected networks with limited routing options have higher vulnerability. Indeed the higher vulnerability translates to larger expected flow deviations for unknown disruption, or equivalently to higher sensitivity to disruptions as a whole. While the results here are for small constructed networks, we believe that the total vulnerability metric will prove useful for gauging the vulnerability or conversely robustness of the full NAS, given weather forecasts and planned traffic management strategies.

	Expected Flow Deviation	Metric ($\alpha = 1, \beta = 2$, $c = 2$)	Fiedler Eigenvalue
Network 1	21.06%	3.33	0.19
Network 2	7.43%	1.59	.28
Network 3	15.17%	2.49	.24

Table 2: The expected squared deviation in flows due to an unmodeled disruption is shown, along with the total vulnerability metric and the Fiedler eigenvalue, for three networks.

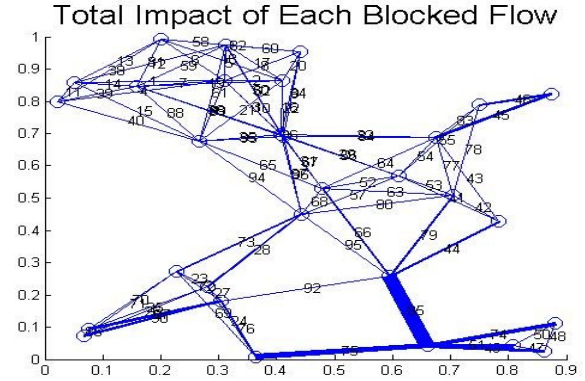

Figure 6: The constructed network shown above has lower total vulnerability compared to the network shown in 3a, per the linear Eulerian model. More alternate routes are available for disrupted flows, which reduces the vulnerability.

Conclusions: Graph-theoretic metrics have been defined, which are meant to give simple insights into the vulnerability of the airspace system to natural or man-made disruptions. Evaluations of the metrics have been undertaken via simulations of flow-level models, and limited formal analysis. These evaluation efforts, while preliminary, suggest that the metrics are indeed promising as indicators of disruption impact. We posit that the metrics may prove to be useful tools for gaining situational awareness about the vulnerability or robustness of traffic management solutions, and in turn the design of robust management strategies.

REFERENCES

[1] S. Gallagher, ``Computer systems outage grounded American Airlines at major hubs," http://arstechnica.com/information-technology/2015/09/computer-systems-outage-grounds-american-airlines-at-major-hubs/ .

[2] "Computer glitch delays hundreds of flights in New York, DC," https://www.rt.com/usa/312554-flights-delay-faa-glitch/ .

[3] ``Computer glitch caused delays at NY's Kennedy Airport," Associated Press, http://www.journalnow.com/news/nation_world_ap/computer-glitch-caused-delays-at-ny-s-kennedy-airport/article_5741a109-85e4-5ad3-a2ed-72987167e3f9.html

[4] M. Bishop, "What is computer security?." *Security & Privacy, IEEE* 1.1 (2003): 67-69.

[5] R. Baheti and H. Gill, "Cyber-physical systems." *The Impact of Control Technology* 12 (2011): 161-166.

[6] R. S. Huang, H. M. Yang, and H. G. Wu. "Enabling Confidentiality for ADS-B Broadcast Messages Based on Format-Preserving Encryption." *Applied Mechanics and Materials*, vol. 543, pp. 2032-2035. 2014.

[7] S. Roy, Y. Wan, and J. Xie, "Proactive and reactive management of non-weather capacity disruption events in the National Airspace System: a flow modeling and design approach," in *Proceedings of the 15th AIAA Aviation Technology, Integration, and Operations Conference*, *AIAA Aviation* Dallas TX, June 2015.

[8] M. C. Aubert et al, "Toward the development of a low-altitude air traffic control paradigm for networks of small, autonomous unmanned aerial vehicles," *Aviation SciTech,* Jan. 2015.

[9] T. J. Colvin, and J. J. Alonso, "Near-elimination of airspace disruption from commercial space traffic using compact envelopes." *AIAA SPACE 2015 Conference and Exposition*, 2015.

[10] Liu, W., Kwon, C., Aljanabi, I., & Hwang, I. (2012). Cyber security analysis for state estimators in air traffic control systems. In *AIAA Guidance, Navigation, and Control Conference* (p. 4929).

[11] Malakis, Stathis, and Tom Kontogiannis. "Cognitive strategies in emergency and abnormal situations training: implications for resilience in air traffic control." In *Proceedings of the 3rd Symposium on Resilience Engineering*. 2008.

[11] Y. Wan et al, "Dynamic queuing network model for flow contingency management." *Intelligent Transportation Systems, IEEE Transactions on* 14.3 (2013): 1380-1392.

[12] M. Xue et al, "Using stochastic, dynamic weather-impact models in strategic traffic flow management." *Proceedings of 91st American Meteorological Society Annual Meeting*, Seattle, WA, Dec. 2011.

[13] S. Roy, B. Sridhar, and G. C. Verghese. "An aggregate dynamic stochastic model for air traffic control." In *Proceedings of the 5th USA/Europe ATM 2003 R&D Seminar, Budapest, Hungary*. 2003.

[14] D. Sun et al, "Eulerian trilogy." *AIAA Guidance, Navigation, and Control Conference and Exhibit*, 2006.

[15] Buxi, Gurkaran, and Mark Hansen. "Generating probabilistic capacity profiles from weather forecast: A design-of-experiment approach." *Proc. of USA/Europe Air Traffic Management Research & Development Seminar*. 2011.

[16] Ramanujam, Varun, and Hamsa Balakrishnan. "Estimation of maximum-likelihood discrete-choice models of the runway configuration selection process." *American Control Conference (ACC), 2011*. IEEE, 2011.

[17] Liu, Pei-chen Barry, Mark Hansen, and Avijit Mukherjee. "Scenario-based air traffic flow management: From theory to practice." *Transportation Research Part B: Methodological* 42, no. 7 (2008): 685-702.

[18] Vossen, Thomas WM, Robert Hoffman, and Avijit Mukherjee. "Air traffic flow management." In *Quantitative problem solving methods in the airline industry*, pp. 385-453. Springer US, 2012.

[19] Wan, Yan, and Sandip Roy. "A scalable methodology for evaluating and designing coordinated air-traffic flow management strategies under uncertainty." *Intelligent Transportation Systems, IEEE Transactions on* 9.4 (2008): 644-656.

[20] Wanke, Craig, et al. "Modeling air traffic demand for a real-time queuing network model of the national airspace system." *AIAA Modeling, Simulation and Technologies Conference, Minneapolis, MN*. 2012.

[21] Wanke, Craig, and Christine Taylor. "Exploring Design Trade-offs for Strategic Flow Planning." *AIAA Aviation* (2013): 12-14.

[22] Taylor, Christine, et al. "Designing Traffic Flow Management Strategies Under Uncertainty." *FAA/Eurocontrol Air Traffic Management Research and Development Forum and Exhibit* (2015).

[23] B. Sridhar and P. Kopardekar, ``Toward autonomous aviation operations: what can we learn from other areas of automation," to appear in *2016 AIAA Aviation Forum, Washington DC* (2016).

[24] Martinez, Stephane, et al. "A weighted-graph approach for dynamic airspace configuration." *Proceedings of the AIAA Conference on Guidance, Navigation, and Control (GNC). American Institute of Aeronautics and Astronautics* (2007).

[25] K. Gopalkrishnan, H. Balakrishnan, and R. Jordan, ``Clusters and communities in air traffic delay networks," to appear in the *2016 American Control Conference, Boston, MA* (2016).

[26] Roy, Sandip, and Banavar Sridhar. "Cyber-Threat Assessment for the Air Traffic Management System: A Network Controls Approach." In *16th AIAA Aviation Technology, Integration, and Operations Conference*, p. 4354. 2016.

[27] Rungta, Neha, Guillaume Brat, William J. Clancey, Charlotte Linde, Franco Raimondi, Chin Seah, and Michael Shafto. "Aviation safety: modeling and analyzing complex interactions between humans and automated systems." In *Proceedings of the 3rd International Conference on Application and Theory of Automation in Command and Control Systems*, pp. 27-37. ACM, 2013.

[28] Xue, Mengran, et al. "Using stochastic, dynamic weather-impact models in strategic traffic flow management." *Proceedings of 91st American Meteorological Society Annual Meeting*. 2011.

[29] Roy, Sandip, et al. "A stochastic network model for uncertain spatiotemporal weather impact at the strategic time horizon." *Proceedings of AIAA Aviation Technology, Integration, and Operations Conference*. 2010.

[30] Xue, Mengran, et al. "Refinement and Enhancement of an Influence-Model-based Weather-Impact Simulator." *Proceedings 2012 AIAA Modeling and Simulation Technologies Conference*. 2012.

[31] Dhal, Rahul, et al. "An Operations-Structured Model for Strategic Prediction of Airport Arrival Rate and Departure Rate Futures." *2014 Aviation Technology, Integration, and Operations Conference*. 2014.

[32] Chung, Fan RK. *Spectral graph theory*. Vol. 92. American Mathematical Soc., 1997.

[33] Wu, Chai Wah, and Leon O. Chua. "Application of Kronecker products to the analysis of systems with uniform linear coupling." *IEEE Transactions on Circuits and Systems I: Fundamental theory and applications* 42, no. 10 (1995): 775-778.

[34] Martinez, Stephane, Gano Chatterji, Dengfeng Sun, and Alexandre Bayen. "A weighted-graph approach for dynamic airspace configuration." In *Aiaa guidance, navigation and control conference and exhibit*, p. 6448. 2007.

[35] Roy, Sandip, and Yan Wan. "Geographical weather-impact sourcing: analytical and data-driven approaches." In *2013 Aviation Technology, Integration, and Operations Conference*, p. 4375. 2013.

[36] R. Dhal and S. Roy, "Layered moment-linear network models as tools for strategic air traffic flow management." *Proceedings of the 2012 AIAA Guidance, Navigation, and Control Conference*, June 2012.

[37] Ramanujam, Varun, and Hamsa Balakrishnan. "Estimation of maximum-likelihood discrete-choice models of the runway configuration selection process." *American Control Conference (ACC), 2011*. IEEE, 2011.

[38] Cohen, Reuven, Shlomo Havlin, and Daniel Ben-Avraham. "Efficient immunization strategies for computer networks and populations." *Physical review letters* 91.24 (2003): 247901.

[39] Wan, Yan, Sandip Roy, and Ali Saberi. "Designing spatially heterogeneous strategies for control of virus spread." *Systems Biology, IET* 2.4 (2008): 184-201.

[40] Saito, Kazumi, Ryohei Nakano, and Masahiro Kimura. "Prediction of information diffusion probabilities for independent cascade model." *Knowledge-based intelligent information and engineering systems*. Springer Berlin Heidelberg, 2008.

[41] Lesieutre, Bernard C., and Sandip Roy. "Power system vulnerability metrics." In *North American Power Symposium (NAPS), 2015*, pp. 1-6. IEEE, 2015.

[42] Roy, Sandip, and Bernie Lesieutre. "Studies in network partitioning based on topological structure." In *32nd Annual North American Power Symposium*. 2000.

[44] Kelner, Jonathan A., et al. "Higher eigenvalues of graphs." *Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on*. IEEE, 2009.

[45] Sridhar, Banavar, and Neil Chen. "Short-term national airspace system delay prediction using weather impacted traffic index." *Journal of guidance, control, and dynamics* 32, no. 2 (2009): 657-662.