Cyber Threat Impact Analysis to Air Traffic Flows Through Dynamic Queue Networks

ALI TAMIMI, ADAM HAHN, and SANDIP ROY, Washington State University

Air traffic control (ATC) increasingly depends on information and communication technology to manage traffic flow through highly congested and increasingly interdependent airspace regions. Although these systems are critical to ensuring the efficiency and safety of our airspace, they are also increasingly vulnerable to cyber threats that could potentially lead to reduction in capacity and/or reorganization of traffic flows. In this article, we model various cyber threats to ATC systems and analyze how these attacks could impact the flow of aircraft through the airspace. To perform this analysis, we consider a model for wide-area air traffic based on a dynamic queuing network model. Then we introduce three different attacks (Route Denial of Service, Route Selection Tampering, and Sector Denial of Service) to the ATC system and explore how these attacks manipulate the sector flows by evaluating the queue backlogs for each sector's outflows. Furthermore, we explore graph-level vulnerability metrics to identify the sectors that are most vulnerable to various flow manipulations and compare them to case-study simulations of the various attacks. The results suggest that Route Denial of Service attacks have a significant impact on the target sector and lead to the largest degradation to the overall air traffic flows. Furthermore, the impact of Sector Denial of Service attack impacts are primarily confined to the target sector, whereas Route Selection Tampering impacts are mostly confined to certain aircraft.

CCS Concepts: • **Security and privacy → Systems security**; • **Applied computing → Transportation**; • **Computer systems organization → Embedded and cyber-physical systems**;

Additional Key Words and Phrases: Dynamic queuing network, air traffic control system, cyber physical system, cybersecurity

ACM Reference format:
Ali Tamimi, Adam Hahn, and Sandip Roy. 2020. Cyber Threat Impact Analysis to Air Traffic Flows Through Dynamic Queue Networks. *ACM Trans. Cyber-Phys. Syst.* 4, 3, Article 26 (March 2020), 22 pages.
https://doi.org/10.1145/3377425

1 INTRODUCTION

Air traffic control (ATC) systems are responsible for ensuring the safety and efficiency of airspace. The primary function of ATC systems is to guide each aircraft from the departure gate to the arrival gate along planned routes, in such a way as to avoid conflicts. At longer time horizons, ATC systems are also responsible for scheduling and routing aircraft to match demand with capacity, in a way that is efficient for the stakeholders—this additional function is known as *air traffic management*. Traffic control requires continuous communication between each aircraft and a number

This work was supported by the National Science Foundation under award CNS-1545104.
Authors' addresses: A. Tamimi, A. Hahn, and S. Roy, School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA 99163; emails: ali.tamimi@wsu.edu, {ahahn, sroy}@eecs.wsu.edu.

2378-962X/2020/03-ART26 $15.00
https://doi.org/10.1145/3377425

of ATC facilities (towers, control centers) during different phases of the flight. In addition, for both traffic control and management, various facilities (including towers and control centers, as well as airline dispatch offices and central command elements) must communicate to decide aircraft flight plans, enact modifications, and exchange information about traffic.

ATC has historically been dependent on radar and VHF-based voice communication; however, modern ATC systems are increasingly using digital technology to enhance the control and awareness of the airspace. For example, the U.S. Federal Aviation Administration (FAA) is working on the transition to the Next Generation Air Transportation System (NextGen). NextGen intends to modernize ATC to increase the capacity and reliability of the airspace while also improving safety and security, and minimizing the environmental impact of aviation [4]. NextGen expands the use of digital communication through the Automatic Dependent Surveillance-Broadcast (ADS-B) system, which requires that aircraft broadcast their location rather than depending on radars. In addition, NextGen envisions a host of new decision-support tools for traffic control and management, which will require automated communication and ingestion of data sources (e.g. ensemble weather forecasts) from public-domain websites. Although these advances should ideally lead to improved control and fewer delays, they also expand the system's attack surface and expose the system to threats of digital manipulation.

NextGen technologies increase data sharing throughout the National Airspace System (NAS) to improve system operations, yet this also introduces additional cybersecurity challenges [36]. The threat of cyber attack to ATC has been well documented in both government reports and in academic literature. The FAA reports identify the need to improve the cybersecurity and resilience of the NAS [14], whereas the National Academy of Sciences recommend the development of improved threat models to explore the risk of air transportation system architectures [13]. In addition, the U.S. Government Accountability Office (GAO) has released numerous reports identifying potential vulnerabilities in these systems [6, 37]. There have also been real-world intrusions to ATC, as reports suggest attacks targeting British ATC attempted to manipulate the voice (VHF) communications [11], whereas sophisticated cyber attacks also infiltrated Sweden's ATC [26]. Beyond cyber attacks, a number of high-profile failures and a physical-world attack have impacted the cyber infrastructure associated with the ATC system.

The potential impacts of cyber attacks and failures to ATC are multifacted, as the recent events have demonstrated. First, such events may directly impact system safety by interfering with controllers' ability to guide aircraft. In addition, however, these events have cascading impacts on the wide-area management of traffic, thus complicating scheduling and routing, reducing system efficiency, increasing controller workload, and potentially indirectly degrading safety at remote locations. Safeguards are in place to reduce the risk of direct safety impacts, but the wide-area impacts of cyber attacks on traffic control and management are not well understood and are a crucial concern. Although current academic literature has explored ATC system security and vulnerabilities, most of this work has focused on identifying technical vulnerabilities in ATC protocols, but it has not yet explored how such vulnerabilities impact system-level aircraft routing and flows. However, models for system-level air traffic flows and their management have been developed, but none of these studies realistically model the cyber system and associated attack surface. This work aims to bridge the gap by modeling the impact of cyber attacks on air traffic flows and analyzing attack impacts on regional air traffic management. To perform this analysis, we present a model for air traffic flows management based on the dynamic queuing network (DQN) introduced in Wan et al. [34]. We then model various attacks from previous literature within this network and calculate the impacts of these various attacks on air traffic flows. Moreover, we apply the metric presented in Roy et al. [21] to identify vulnerable routes and sectors in air traffic flows.

1.1 Problem Statement, Contribution, and Outline

The primary objective of this work is to analyze the impacts of cyber attacks on air traffic flows. While previous work has explored both general disruptions to ATC flows and cyber vulnerabilities within ATC systems, no research has yet explored the impact and severity of these threats based on ATC control structures and flow properties. Toward this goal, we pursue integrated modeling of queueing-based models of wide-area traffic flow, and explore simulation-based and graph-theoretic approaches to evaluate attack impacts. The specific contributions include the following:

- This is the first work that explores the application of previously identified cybersecurity threats to explore their impacts to ATC traffic flows. The approach extends previous work on ATC flow analysis, based on DQN models [18, 20, 21], by modeling and analyzing known cyber vulnerabilities within the communications infrastructure [5, 15–17, 23].
- This work's results compare different ATC system attacks, including route and sector tampering and denial of service (DoS) based on their impact, attack vector, and difficulty to implement. The results suggest that route-based DoS attacks present the highest risk due to their ability to shutdown sectors, routes, and resulting flows.
- Finally, this work presents a vulnerability metric to estimate which ATC routes/sector have the greatest impact to overall flows and therefore are inherent to the most risk from potential attacks. The proposed metrics can be used to identify the sectors that should be most concerned with cyber threats, along with where mitigations should be prioritized.

The article is organized as follows.

Section 2 reviews previous work related to the analysis of ATC traffic flows and cybersecurity vulnerabilities within ATC communication architectures. It then provides an overview of current ATC system operations, including Air Route Traffic Control Centers (ARTCCs), their communication with aircraft, and previously defined DQN models used to analyze air traffic flows.

Section 3 investigates the lack of security in ADS-B that sends aircraft information such as altitude, airspeed, and location to other aircraft and ground stations. Based on the security issues of ADS-B, we model various cyber threats to ATC systems and analyze how these attacks could impact the flow of aircraft through the airspace. To perform this analysis, we extend previously defined DQN models for wide-area air traffic and incorporated three attacks (Route Denial of Service (RDOS), Route Selection Tampering (RST), and Sector Denial of Service (SDOS)) to enable flow-based analysis.

Section 4 presents case studies to evaluate the impacts of the previously introduced attacks on air traffic flows within a single region. Each case study presents a single attack on the simplified network. We investigate how different attacks impact flows between ARTCCs and their their functionality, and we evaluate its propagating impacts on the region.

Section 5 provides system-level risk analysis metrics to identify the sectors and regions most vulnerable to attacks. Section 4 demonstrates simulation studies of a specific attack; however, this technique is not scalable for risk assessment within a large-scale network. We present graph-level vulnerability metrics to identify the sectors that are most vulnerable to various flow manipulations and compare them to case-study simulations of the various attacks.

Section 6 provides a discussion on the resulting risk from the proposed attacks and introduces potential mitigations. The results suggest that RDOS attacks will have the most significant impact on the target sector and lead to the largest degradation to the overall air traffic flows. Furthermore, the impact of SDOS attack impacts are primarily confined to the target sector, whereas the RST impacts are mostly confined to certain aircraft.

2 RELATED WORK AND ATC SYSTEM BACKGROUND

2.1 Related Work

There have been many previous efforts exploring cybersecurity vulnerabilities within an ATC system, along with work exploring the vulnerability of ATC sectors and flows to traditional disruptions (e.g., weather). Key efforts that explored the cybersecurity of ATC include work by Strohmeier [27] and Strohmeier et al. [29], which introduced a survey of the communication devices used in ATC and identified vulnerabilities for each device. Further work by Costin and Francillon [5] explored cyber vulnerabilities within the NextGen platform, specifically the ADS-B communications, and then explored potential threat impacts based on the aircraft locations and attacker goals. In other work, they simulated an environment including an air traffic model, existing surveillance systems, ADS-B systems, and a wireless channel model to investigate communication infrastructure of next generation air traffic management and evaluate the performance of communication and optimize it [15, 16]. A variety of other works have also explored vulnerabilities within ADS-B. Schäfer et al. [23] evaluated ADS-B attacks and quantified various factors, such as the attacker's location and the signal strength, based on the attacker's ability to manipulate various aircraft messages. Purton et al. [17] explored different potential attacks against ADS-B systems, including network intrusions, message spoofing, and communication malfunction, and analyzed each based on their threats, attack opportunities, weaknesses, and strengths. Broader ADS-B attack taxonomies and potential impacts are identified by McCallie et al. [9], including the techniques required for exploitation and their difficulty. A model-based approach that investigates various physical and cyber vulnerabilities of ADS-B from different aspects is presented by Thudimilla and McMillin [32].

Other related work has explored theoretic models and analysis techniques to evaluate how interruptions within air traffic sectors impact the broader system-level flows, such as the flow management function of the ATC system. Gwiggner and Nagaoka [7] reviewed recent models of air traffic flow analysis and then explored queuing networks, traffic flow theory, and cellular automata methods to discover relationships between system variables. They concluded that the combination of model-based flow analysis and analysis of flight data leads to new insight into the air traffic congestion mechanisms. Sridhar et al. [25] categorized the traffic flow models into three groups, including linear dynamic system models, other Eulerian models, and partial differential equation models, which can enable simplified analysis of wide-area dynamics. Furthermore, work by Bayen et al. [3], Menon et al. [10], and Roy et al. [19] explored Eulerian network models for air traffic flows. These flow-level models for air traffic were later enhanced to represent traffic at varied resolutions, to explicitly capture multiple origin-destination pairs, and to model management initiatives as queueing elements [30, 34]. Finally, agent-based modeling was explored by Wang et al. [35], where each flight and control agent is defined as an agent and used to analyze different system properties such as throughput, capacity, delay, delay jitter, and congestion. Furthermore, domain-specific multiagent system models have also been explored in the domain of air traffic management to provide constructs (which can be instantiated to implement specific tasks and procedures in air traffic management domain) for different scenarios [22]. Building on these studies, a series of recent works have begun to assess the propagative impacts of traffic flow restrictions—whether due to cyber events, weather, or other causes (e.g., space vehicle operations) [18, 20, 21].

2.2 ATC System Operations

ARTCCs are the facilities primarily responsible for en route management of aircraft. ARTCCs are required to support each phase of a flight, including preflight, takeoff, departure, en route, descent, approach, and landing [33]. The main function of ARTCCs is to ensure appropriate aircraft

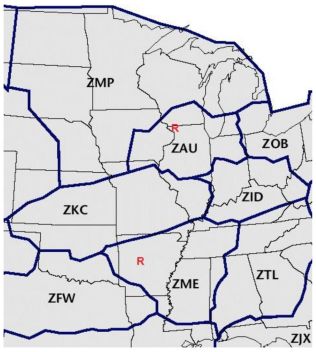


Fig. 1. A part of the map of ARTCCs.

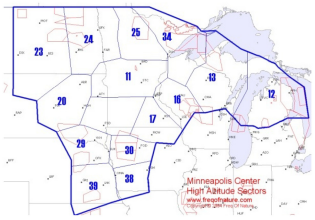


Fig. 2. Sectors of Minneapolis ARTCC (ZMP).

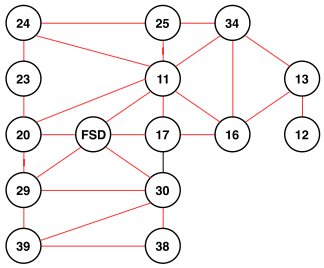


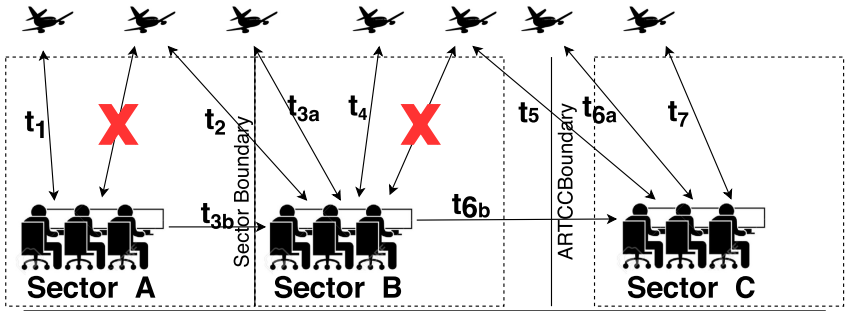
Fig. 3. ZMP ARTCC graph model.

separation and the safety of the various sector routes, as well as maintenance of sector capacities to meet controller workload constraints [12]. ARTCCs accept aircraft and pass them to other ARTCCs or terminal control centers. Based on an FAA report [1], more than 36,000 flights were held by ARTCCs for different reasons such as traffic congestion or weather conditions in 2018, which was a 3.5% increase from that in 2017. During holding, an aircraft is flying in a repeating rotational pattern deliberately. There are 22 ARTCCs located in 19 states [2]. Figure 1 shows a partition of the U.S. airspace, where the airspace managed by each ARTCC is given a unique name (e.g., ZMP refers to Minneapolis ARTCC). Each ARTCC's airspace consists of several sectors. For instance, Figure 2 shows the sectors within the ZMP ARTCC. This work will utilize queueing-theoretic and graph-theoretic approaches to model and analyze traffic flows and cyber disruptions. A graphical representation of a ZMP ARTCC is shown in Figure 3.

Let us first provide an overview of how ARTCCs manage the flow of en route aircraft through sectors, as a starting point for understanding the potential impacts of cyber attacks. When an aircraft enters a sector, it communicates to the corresponding sector controller. Each sector is controlled by one or a team of controllers and is responsible for separating of the aircraft. At the sector boundary, they are responsible for transferring control from the previous controller. The process of transferring control and transferring communication is called the *hand-off*. Figure 4 shows the communications during en route flight. The explanation of each time interval is as follows:

- *Over sector*: The aircraft flies over the sector and is controlled by that current sector; its only communication is with the current sector in this phase.
- *Com transfer*: The aircraft is close to the sector boundary and is still controlled by current sector, but the transfer of communications to the next sector is initiated before it reaches the boundary.
- *In boundary*: The aircraft flies over the boundary and keeps the communication with next sector.
- *Ctrl transferring*: The aircraft flies over the boundary, and the control is passed from the current sector to the next sector.

Based on the preceding explanation, Figure 4 shows the communication of an aircraft during en route travel as it passes to different sectors and ARTCCs. The figure also includes a table that relates the aircraft's location between sectors with its communication to sector controllers and the controlling sector. At t_1, the aircraft communicates with sector A, which is responsible for



Time	Name	Src/Dst	Plane Position	Communication with	Controlled by
t_1	over sector	aircraft/sector	Sector A	Sector A	Sector A
t_2	com transferring	aircraft/sector	Sector A	transferring	Sector A
t_{3a}	in boundary	aircraft/sector	Boundary	Sector B	transferring
t_{3b}	ctrl transferring	sector/sector	Boundary	Sector B	transferring
t_4	over sector	aircraft/sector	Sector B	Sector B	Sector B
t_5	com transferring	aircraft/sector	Sector B	transferring	Sector B
t_{6a}	in boundary	aircraft/sector	Boundary	Sector C	transferring
t_{6b}	ctrl transferring	sector/sector	Boundary	Sector C	transferring
t_7	over sector	aircraft/sector	Sector C	Sector C	Sector C

Fig. 4. Communications in the en route phase when an aircraft routes between the sectors and a table that shows when and where each communication is established.

controlling the aircraft. Before leaving sector A (t_2), the communication is transferred to sector B. Although in this step the communication is transferred to sector B, the aircraft is still controlled by sector A. The time t_3 corresponds to the aircraft passing the boundary of two sectors: sector A passes control of aircraft to sector B. The times t_4, t_5, and t_6 are analogous to the times t_1, t_2, and t_3, respectively, but at t_5 and t_6, the communication and control are passed to a sector in another ARTCC.

2.3 DQN Model for Air Traffic Flow Management

In this section, we present an air traffic flow model based on DQN, whereas in the next section, we describe how the model can be used to evaluate the previous three attack scenarios.

The proposed model is based on the queuing-network modeling paradigm introduced by Wan et al. [34], which is part of a recent literature on flow-level or Eulerian modeling of air traffic for the purpose of strategic air traffic management (also see Bayen et al. [3] and Roy et al. [19]). The network model by Wan et al. [34] represents traffic at the resolution of aggregate traffic flow densities between high-altitude sectors (either sector-midpoint to midpoint or sector-midpoint to boundary) in an area of interest and at lower resolution outside this area. Each flow is modeled as an assimilation of traffic for multiple origin-destination pairs, each with associated fixed or stochastically selected routes. The nominal (free-flow) dynamics of the traffic are specified by link delays (which capture sector crossing times) and flow-conservation equations at nodes (sector midpoints or boundaries where flows may merge or split). These nominal dynamics are modulated by flow constraints, which may arise either because of intrinsic capacity constraints of airspace sectors or traffic management initiatives that are deliberately placed to manage congestion. These flow constraints are modeled as queues of various sorts—we refer the reader to the work by Wan et al. [34] for the queuing models used to represent various constraints. Additionally, rerouting protocols are represented within the model. Finally, environmental or operational factors that alter flow

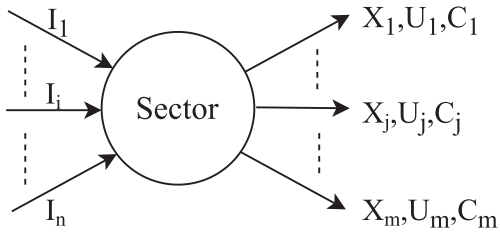


Fig. 5. DQN model parameters.

constraints (e.g., sector = capacity reductions due to weather) then are modeled as time variations in the queuing parameters. Simulation of the model then allows characterization of local and aggregate performance, including en route and terminal-area backlog and delay. It is worth noting that some formal analysis of the model is also possible for simplified graph architectures (e.g., for a sequence of two congested regions); however, these analyses are largely limited to majorizations and qualitative graph-theoretic characterizations rather than quantitative bounds.

Our aim here is to understand the differential impact of potential cyber attacks on traffic-system performance. Thus, we focus on a specialization of the queuing-network model, with the goal of comparing uncongested traffic flows to cyber attack–impacted flows. Specifically, we model a portion of the airspace (e.g., a single ARTCC's scope) at a sector resolution, whereas the remainder of the airspace is modeled as a single node that is a traffic source/destination. Sector capacities are imposed as queuing elements, but other flow constraints (e.g., management initiatives, rerouting) are excluded, and time variations due to environmental conditions are also ignored. The cyber attacks are modeled as incurring additional time-varying flow constraints, as described in the following section. For readability, we present the simplified model explicitly and directly rather than referring to the more general formulation of Wan et al. [34].

Formally, the DQN model is defined on a graph, for which each node represents an en route sector, and directed edges are used to capture traffic flows—if there is traffic flow from sector A to sector B, then a directed edge is drawn from node A to node B.

Figure 5 illustrates the queuing dynamics associated with one node in the graph, representing traffic flows to and from a single center. The queuing dynamics are modeled in discrete time, with each time interval capturing the average time required for traffic to transit a sector. The dynamic variable $I_i(t)$, $i = 1, \ldots, n$, captures an inflow from another sector (i.e., the number of aircraft entering the sector per discrete time interval). Each aircraft in inflow I_i leaves the sector via one of the outflows, based on its flight profile. The dynamic variable $U_j(t)$, $j = 1, \ldots, m$ captures the inflow traffic from other sectors that leave this sector through the outflow j; therefore,

$$\sum_{i=1}^{n} I_i(t) = \sum_{j=1}^{m} U_j(t),$$

where n is the number of inflows and m is the number of outflows. Each outflow j has a parameter C_j that is the capacity of outflow, which indicates the number of aircraft that can be served by the sector through the outflow j in each time interval. Since the sector cannot serve all aircraft in its outflows, it is possible that some aircraft are waiting to be served in next time interval(s). The number of aircraft waiting in the queue in each time interval is the backlog, which is represented by the dynamic variable $X_j(t)$. Based on the described dynamic variables and parameters c, we model the backlog for outflow i as evolving as follows:

$$X_i(t) = \max(X_i(t-1) + U_i(t) - C_i, 0), \tag{1}$$

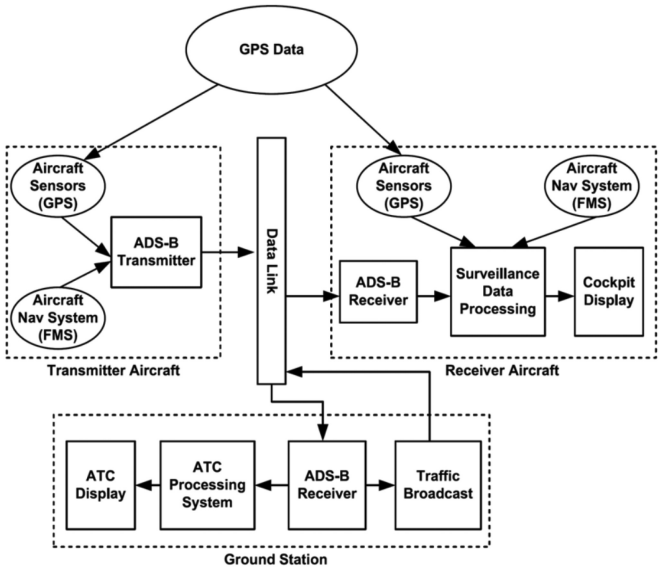


Fig. 6. ADS-B System Architecture [23].

where

- $X_i(t)$ is the backlog of the sector for the outflow i at time t,
- C_i is the number of aircraft that can be served at the outflow i in each time interval, and
- $U_i(t)$ is the number of aircraft that come to sector at time t, and based on their flight (routing) profile, that will leave the sector through the outflow i.

The equation captures the conservation of flow in the sector, subject to the additional queueing constraint that each outflow is subject to a capacity constraint. We note that the sector flow model on the DQN follows the nominal queueing model for a sector given in Wan et al. [34]. We note that the max() function in the equation serves to ensure that planes are queued only if the total flow demand exceeds the capacity.

3 ATC SYSTEM THREATS: CONCEPTS AND MODEL

3.1 En Route Communications Threats

ADS-B is the foundation of the NextGen ATC infrastructure and will become mandatory in the United States by 2020 [5, 23]. The main function of ADS-B is to improve aircraft surveillance by having planes broadcast their altitude, airspeed, and location to other aircraft and ground stations, as shown in Figure 6 [23]. ADS-B uses GPS to determine their location and then advertises the aircraft's status (e.g., position, velocity) through a 1,090-MHZ data link.

A core problem of ADS-B is the lack of security, specifically message encryption and authentication. Recent research has suggested that attackers could exploit these vulnerabilities to manipulate the ARTCC operations [5] through the following attacks:

- *Ghost Injection*: In this attack, the attacker broadcasts ADS-B messages for a nonexisting aircraft (ghost aircraft). This results in nonexisting aircraft appearing on the ground station radar screen. During such an attack, it may not be possible for the ground station to distinguish between the real aircraft and nonexisting aircraft. This confusion may lead to a station-level DoS attack, as controllers can no longer correctly serve existing aircraft.

Table 1. Attacks Properties

Attack	Mechanisms	Target	Summary	Immediate Impact	Long-Term Goal
RDOS	Ghost Injection	Sector	Attacker broadcasts fake ADS-B messages so that the sector controller cannot distinguish between real and ghost aircraft	Shutdown route or sector	Delay airspace flows from the targeted sector
RST	Virtual Trajectory Modification	Aircraft & Sector	Attacker jams the signal to the targeted aircraft and then spoofs the ADS-B message using an aircraft's ID	Provide the sector controller with a fake route for the targeted aircraft	Decrease safety of airspace
SDOS	Flood Denial	Sector	Attacker jams the sector to prevent the sector controller from sending future instructions	Bypass queuing of a sector	Delay airspace flows from sectors after the targeted sector

- *Flood Denial*: In this attack, the attacker produces a jamming signal that disrupts the 1,090-MHz data link. As a result, the ground station cannot receive an aircraft's ADS-B messages, causing the aircraft to disappear from the ground station controller screen. Therefore, the ground station is unable to send future messages to the aircraft, ensuring that the aircraft will remain on its current route.
- *Virtual Trajectory Modification*: By selectively jamming an aircraft's signals and replacing them with modified messages, an attacker can inject the wrong aircraft location. Therefore, the ground station will have nonexisting aircraft on its screen and the controller will manage the flows based on nonexisting aircraft.

Based on these previously introduced threats, we propose three attack scenarios to identify how each threat impacts ARTCC flows. In the next section, we explain how these attacks influence air traffic flows using the DQN model. Figure 7 shows the schema of our attacks, whereas Table 1 shows the description of attacks.

Scenario 1: RDOS. An attacker injects spoofed aircraft in a specific route using the Ghost Injection attack. Therefore, the air traffic controller sees a combination of real and ghost aircraft on the display. Since the controller is unable to distinguish between real and ghost aircraft, the controller cannot serve the real aircraft and will shut down the targeted route to prevent any spacing violations. Therefore, additional aircraft cannot be served and must stay in their current sectors. The attack will be referred to as a partial RDOS (P-RDOS) if it targets only one route and complete RDOS (C-RDOS) if it targets all outflows of a sector.

Scenario 2: RST. In the second scenario, the attacker modifies the ADS-B message of an aircraft using the Virtual Trajectory Modification attack. Therefore, the controller will view nonexisting aircraft instead of the true aircraft.

Scenario 3: SDOS. In this scenario, the attacker applies a Flood Denial attack to a sector. The attacker sends the jamming signal to the VHF channel of a sector controller, and the controller cannot send any instruction related to queue management to the aircraft. Therefore, all aircraft continue their routes without queuing management, thus increasing traffic on all outgoing routes. As such, the next sectors face increased traffic and delays due to growing backlog queues.

3.2 Threat Analysis

In this part, we demonstrate the attack scenarios introduced in Section 3.1 on the proposed DQN model and explore their air traffic flow impacts.

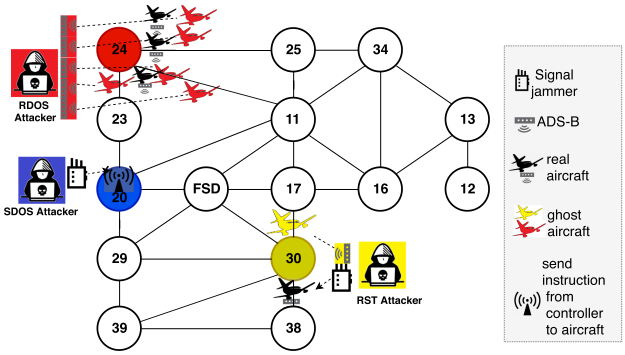


Fig. 7. Attack demonstration in a flow graph.

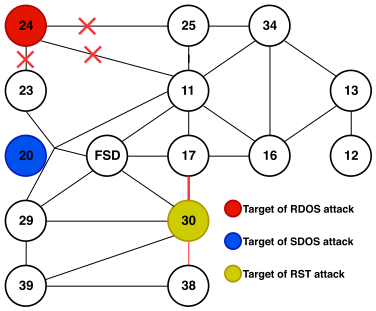


Fig. 8. Attack impact on a flow graph.

3.2.1 Route Denial of Service. The RDOS attack assumes that the attacker may cause a controller screen change by injecting nonexisting aircraft. Since the controller is unable to distinguish between the real and nonexisting aircraft, it leads to shutting down a route or a sector. If there is a route shutdown (P-RDOS), the controller cannot serve the aircraft through the targeted route. Therefore, the targeted route is shutting down for some time interval until the controller resumes its functionality. If there is a sector shutdown (C-RDOS), all routes of the targeted sector are shutting down. We define the attack model for C-RDOS in Equation (2).

$$X_i(t) = \max(X_i(t-1) + U_i(t) - (1 - b(t)) \times C_i, 0) \tag{2}$$

The attack model for P-RDOS is defined in Equation (3), where $\circ$ denotes elementwise multiplication.

$$X_i(t) = \max(X_i(t-1) + U_i(t) - (1 - b_i(t)) \circ C_i, 0) \tag{3}$$

The dynamic variable $b(t)$ is the attack parameter that is defined as a single value (0 or 1) for C-RDOS and as a vector for P-RDOS. For a C-RDOS attack, $b(t)$ is defined as follows.

$$b(t) = \begin{cases} 1, & \text{during complete attack (all routes of the sector are shutdown)} \\ 0, & \text{no attack} \end{cases}$$

For a P-RDOS attack, $b_i(t)$ is defined as follows.

$$b_i(t) = \begin{cases} 1, & \text{partial attack happens in route number } i \text{ at time } t \\ 0, & \text{no attack at route number } i \text{ at time } t \end{cases}$$

In the graph model, the outflow edges that correspond to the targeted sector should be removed. Figure 7 shows a complete RDOS attack on sector 24. Figure 8 shows the structure of the graph after the RDOS attack.

3.2.2 Route Selection Tampering. In an RST attack, an attacker could jam the ADS-B signal of an aircraft and inject new ADS-B messages with a new position using identification parameters of the real aircraft. In this condition, the aircraft maintains the original route; however, there is a route change on the controller screen showing that the aircraft is heading to another sector. In this attack, the targeted sector has an additional aircraft (nonexisting aircraft) in the queue. In this attack, we show vector $b_i(t)$ as follows.

$$b_i(t) = \begin{cases} 1, & \text{a ghost aircraft is injected to outflow } i \\ 0, & \text{no attack} \end{cases}$$

Equation (4) presents the model of the RST attack.

$$X_i(t) = \max(X_i(t-1) + U_i(t) + b_i(t) - C_i, 0) \tag{4}$$

Figure 7 shows the RST attack on sector 30. After leaving sector 30, the attacker jams the ADS-B messages and injects a new aircraft into the route that is heading to sector 17. Therefore, the sector controller should serve an extra aircraft in the outflow queue that is heading to sector 17.

3.2.3 Sector Denial of Service. In the SDOS attack, after establishing voice communication between the aircraft and the receiving sector, the attacker jams this communication. Since the sector cannot send any messages to the aircraft, it continues its route without any instruction from the sector controller regarding queue management. As a result of the SDOS attack, the sector controller cannot inform the aircraft about the over service capacity condition. In other words, all aircraft in the sector continue their routes without waiting in the queues. The consequence of this attack is more visible in the sectors that are in front of the targeted sector. We present the model of this attack as follows. Since the aircraft do not enter the queues, the backlog is equal to zero. Equation (5) presents the SDOS attack model, where $b(t) = 1$ if the sector is under attack and $b(t) = 0$ when there is no attack.

$$X_i(t) = (1 - b(t)) \times [\max(X_i(t-1) + U_i(t) - C_i, 0)] \tag{5}$$

Since the attack hinders queue management, the outflow of the targeted sector increases with no limitation and changes the inflows of the sectors that are after it. Therefore, aircraft will ignore the queues of the targeted sector and continue their routes. In the flow graph model, the node representing the targeted sector is removed and the outflow edges of previous sectors connect to the inflow edges of the next sectors. Suppose that in Figure 7, sector 20 is the target of an SDOS attack. Figure 8 shows the changes in the graph structure after the attack. The major impact of this attack is in the sectors that have an inflow from the targeted sector. In Figure 8, the largest impact is found in sectors 11, 23, and 29 and the FSD (Sioux Falls sector). The number of aircraft in their queues increases, and it needs more time to serve them. This is because there is no queue management in sector 20, and all aircraft are directed to the next sectors without staying in the queues. As a result of this situation, the number of aircraft increases in the queues of sectors 11, 23, and 29 and the FSD.

4 FLOW IMPACT CASE STUDIES

This section investigates the impact of the proposed attacks on a test system to analyze the queue backlogs and resulting delay. It demonstrates a Matlab-based simulation of attacks within a test region (representing the ZMP model introduced in Section 2) to explore how the specific attacks would impact flows. The case study that we use is as follows. At $t = 0$, there are 21 airplanes in the system that are in the queues of the sectors. The origin sectors of the aircraft are defined in Figure 9. The destination of all aircraft is assumed to be sector 12. Figure 9 shows the initial condition of the flow graph, where c represents the capacity of service in each queue and q represents the aircraft number in the queue (e.g., aircraft 16 and 17 are in the outflow of sector 3, which is heading to sector 8, and aircraft 14 and 15 are in the outflow of sector 3, which is heading to sector 7). In the following, we investigate the impacts of different attacks on the flow graph (the routes are as follows: $route1 = [3, 7, 11, 12]$, $route2 = [3, 8, 11, 12]$, $route3 = [4, 8, 11, 12]$, and $route4 = [5, 8, 11, 12]$):

- In the C-RDOS scenario (Figure 10), the attack starts at $t = 1$, targets sector 8, and lasts one time interval. Therefore, sector 8 cannot serve the aircraft at $t = 1$. The RST scenario (Figure 11) starts at $t = 0$ and targets aircraft number 15.

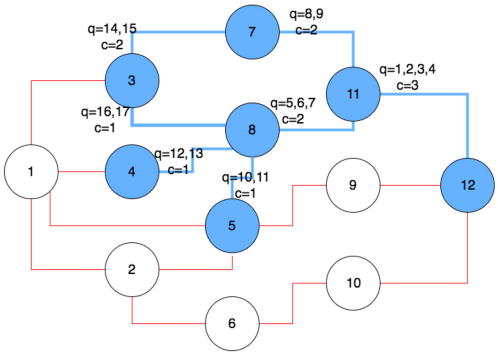


Fig. 9. Air traffic flows of the example system.

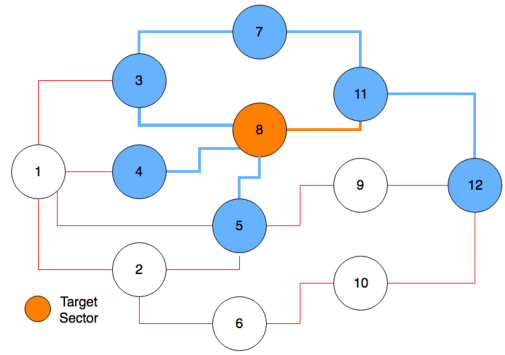


Fig. 10. Scenario of the C-RDOS attack.

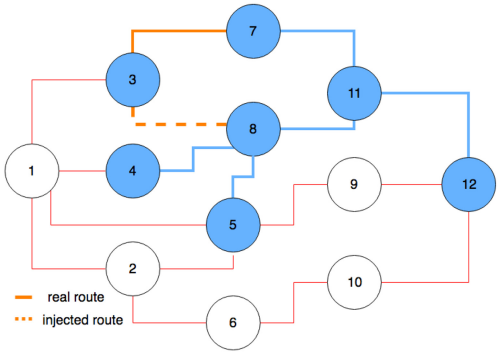


Fig. 11. Scenario of the RST attack.

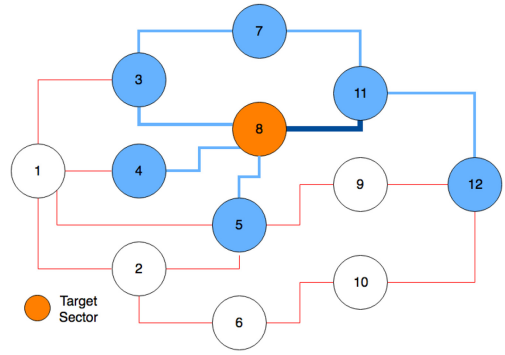


Fig. 12. Scenario of the SDOS attack.

- In the RST scenario (Figure 11), the attack starts at $t = 0$ to show the impact of the attack on sectors 7 and 8 at $t = 1$ and sector 11 at $t = 2$ of attack. The attacker creates a nonexisting (ghost) aircraft using the ID of airplane 15 between sectors 3 and 8. Simultaneously, airplane number 15 vanishes from the radar screen when it travels from sector 3 to sector 7.
- In the SDOS scenario (Figure 12), the attack starts at $t = 2$, targets sector 8, and lasts one time interval.

  Unlike the RDOS attack, where the most affected sector is the target sector (sector 8), in the SDOS attack, the most affected sector is sector 11, which is located after the target sector. Therefore, we start the attack at $t = 2$ to be able to compare the effect of different attacks on the same sector at the same time. In other words, by starting the RDOS attack at $t = 1$ and the SDOS attack at $t = 2$, we can see the effect of attacks on sector 11 at the same time.

For each attack, we extract the backlog $x_{11}^{8}(t)$ for sector 8 and $x_{12}^{11}(t)$ for sector 11 that is located after target of attack. $x_j^i(t)$ means the backlog of the outflow of sector i that routes to sector j. Figure 13 and Figure 14 show $x_{11}^{8}(t)$ and $x_{12}^{11}(t)$, respectively, for each of the three attacks.

In the RDOS attack, since the target sector (sector 8) cannot serve the airplanes, the backlog increases. However, decreasing the inflow of sector 11 leads to decreasing the backlog in this sector during the attack. Therefore, the aircraft that come to sector 11 from other inflows (aircraft 15) can be served faster.

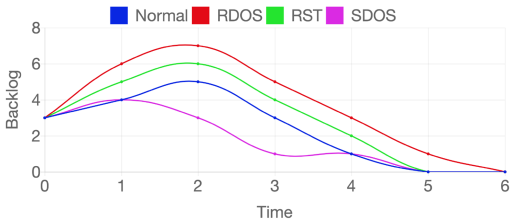


Fig. 13. $x_{11}^{8}(t)$ in normal and attack cases.

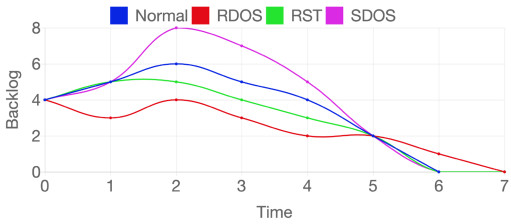


Fig. 14. $x_{12}^{11}(t)$ in normal and attack cases.

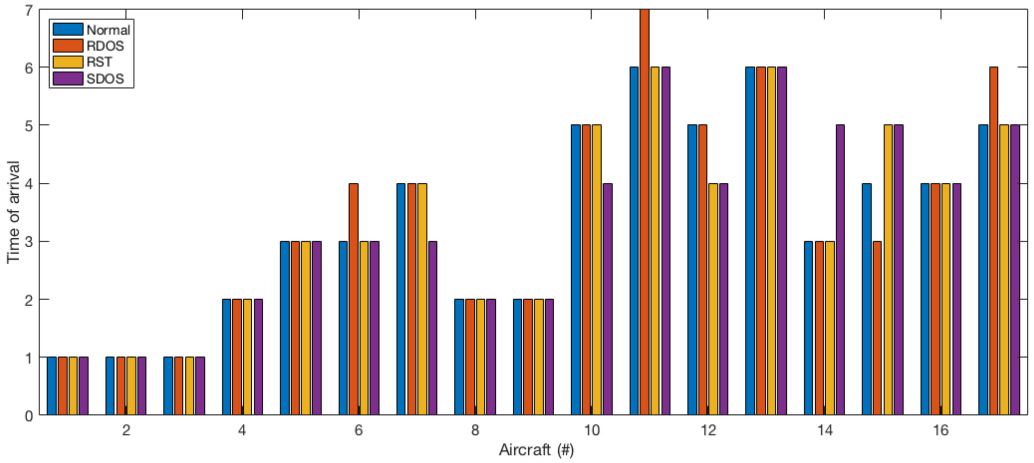


Fig. 15. Arrival time of aircraft in normal and attack conditions.

In the RST attack, there is a nonexisting (ghost) aircraft in the queue that increases the $x_{11}^{8}(t)$. Since sector 8 schedules a nonexisting aircraft, it cannot use all of the outflow capacity that is the inflow of sector 11. This issue leads to a decreased backlog of sector 11. The time of arrival of the target aircraft (aircraft 15) increases. In the SDOS attack, all aircraft in the queue of the target sector (sector 8) fly to the next sector. This leads to a decreased backlog of the target sector. However, since all aircraft that left the target sector arrive at sector 11 together, the backlog of sector 11 increases.

Figure 15 shows the time of arrival of aircraft for the normal and attack cases. There are 17 aircraft in Figure 9. Where, the queue initial values (aircraft numbers) and the capacity are specified for each sector. Aircraft 1 through 4 are located after the attack point, and the attacks do not impact on them. Aircraft 5 through 8 are located on the targeted sector of RDOS and SDOS attacks and after the targeted route of the RST attack. In the RDOS attack, the aircraft face delay in sector 8, which is the target of attack. As a result of the delay in sector 8, sector 11 becomes less crowded in a few timesteps after the attack. However, since aircraft 8, 9, 14, and 15 are not located in attack paths, it is possible that they can be served by sector 11 faster than the normal condition. In the RST attack, since only one aircraft is the target of the attack, it has a minor impact on delays. As Figure 15 shows, the attack only leads to delay in aircraft 15, which is the target of attack. However, as a result of the attack, aircraft 12 reaches sector 11 before aircraft 15 and serves sooner than in the normal condition. In the SDOS attack, since the queue of sector 8 is bypassed, the aircraft pass the sector without waiting in the queue. Therefore, the number of aircraft reaching to sector 11 increases after the attack. Increasing the number of aircraft in sector 11 leads to a crowd in this

sector and takes more time to serve the aircraft. The results show that the RDOS attack presents the greatest impact to aircraft 6, 11, and 17. The RST attack increases the time of arrival of aircraft 15. Finally, the SDOS attack impacts on aircraft 14 and 15.

5 SYSTEM-LEVEL VULNERABILITY ANALYSIS

The previous section only explored threat vulnerability in the context of a small case study; however, risks need to be evaluated at the regional or national scale, which requires analysis of a large network encompassing many sectors. An example of cybersecurity risk assessment of a cyber physical system is presented by Teymouri et al. [31]. For larger-scale risk assessment, exhaustive simulation of potential threats using the DQN becomes cumbersome. Therefore, we are motivated to consider simplified vulnerability metrics, which allow comparison of potential threat impacts without exhaustive simulation. Here, we explore whether the vulnerability metrics proposed by Roy et al. [21] provide a strong indicator of cybersecurity vulnerabilities in the ATC system. Specifically, we estimate the vulnerability to attacks of the sectors and routes of a given system using the metric. We also present a method to evaluate the metric-based assessment of the attacks, using a graph-theoretic argument. Finally, we further investigate the impacts of attacks on the backlog of the airspace system as a means for evaluation/comparison.

5.1 Vulnerability Metric

In this section, we recall a metric that is proposed by Roy et al. [21]. Using the metric, we measure the vulnerability of different sectors and routes. This allows us determine which sectors and routes of the model are more vulnerable to different types of attack.

The vulnerability metric defined by Roy et al. [21] is concerned with estimating the total impact across the airspace system of the blockage or modification of a set of flows (say flows $1, \ldots, n$). The metric is based on the concept that a flow disruption has large impact if (1) the nominal traffic flow on the link is large and (2) there are few good alternative routes for the blocked flow. To capture these two features in a simplified way, the metric incorporates (1) the total nominal flow f_{ij} on each disrupted link (i, j) and (2) a purely graph-theoretic measure of the presence/absence of alternative routes. Specifically, the eigenvector associated with the subdominant eigenvalue of the graph's Laplacian matrix is used to estimate the presence/absence of alternatives, as this vector gives an indication of the connectivity pattern of the network [24].

In the following equation, we formally present the vulnerability metric and then describe the process by which the variables in the metric are found.

$$V_T = \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} \frac{f_{ij}^{\alpha} \mid v_i - v_j \mid^{\beta}}{\lambda^c} \tag{6}$$

The metric is derived from the flow graph and nominal traffic flow. The procedure for calculating the variables in the metric is as follows:

- *Create Laplacian matrix (L)*: This matrix is $n \times n$, where n is the number of vertices (sectors) in the flow graph. If there is an edge (route) between vertex i and vertex j, the value of L_{ij} is equal to −1. Otherwise, it is 0. The value of diagonal elements (L_{ii}) is equal to the value that makes the sum of the row to zero.

$$L_{ij} = \begin{cases} -1 & \text{there is an edge from } i \text{ to } j \\ 0 & \text{there is no edge from } i \text{ to } j \\ -\sum_{j \neq i} L_{ij} & i = j \end{cases} \tag{7}$$

- *Calculate eigenvector*: Calculate the eigenvector v that corresponds to the smallest positive eigenvalue, and scale it to have unit norm.
- *Vulnerability metric*: Equation (8) shows the vulnerability metric for the edge between vertex i and vertex j, where f_{ij} is the flow density (number of aircraft) between sector i and sector j; v_i and v_j are the ith and jth elements of the eigenvector; and the constants α and β are positive integers that weight the flows (f_{ij}) and eigenvector component differences, respectively. Based on the work of Roy et al. [21], different simulation and analysis show that the appropriate value for α is 1 and for β is 1 or 2.

  Based on the preceding computation, the vulnerability of the flow on a link (i, j) is found as

$$V_{ij} = f_{ij}^{\alpha} \mid v_i - v_j \mid^{\beta} . \tag{8}$$

  If we want to find the total vulnerability metric over a set of flows (or for the entire network), we use Equation (6). In the total vulnerability computation, we using a scaling based on λ^c, where λ is the subdominant eigenvalue and c is a tunable constant; this scaling does not depend on the individual flows considered and hence is not necessary for comparison of different flows' vulnerabilities. However, it is helpful to obtain an absolute measure of vulnerability, which, for example, allows comparison of one network to another.

We use Equations (6) and (8) to determine which of the routes and sectors are more vulnerable. In the rest of this section, we explain how this metric is used to evaluate the impact of different attacks.

C-RDOS attack. In a C-RDOS attack, all outflows are blocked such that no aircraft can pass through outflows. Therefore, in the flow graph model, all routes of the target sector should be removed. This change makes the flow graph disconnected, and we cannot show the effect of the target sector in the calculation of the vulnerability metric. For the calculation of the metric in this condition, each time, we keep one edge of the target node and remove others and calculate the metric using Equation (6). The procedure repeats for all edges. If the target node has m edges, we do the procedure m times. In this attack, V_T is the sum of the calculated values. If the target sector t has k routes and $V_{T_{ti}}$ shows the vulnerability metric when the only available route of target sector (t) is ti, Equation (9) shows the total vulnerability metric.

$$V_T = \sum_{i=1}^{k} V_{T_{ti}} \tag{9}$$

P-RDOS attack. In a P-RDOS attack, one of the outflows of the target sector is blocked. For calculating the vulnerability metric, first we remove the edge corresponding to the blocked route from the graph. Then we calculate V_T using Equation (6).

SDOS attack. In the SDOS attack, the outflows of target sector increase and no route is blocked. There is no change in the structure of graph model during this attack, and only f_{ij} of the outflows of the target sector increases. Therefore, we calculate V_T using Equation (6).

5.2 Metric Comparison

In this section, we calculate the presented metric for the routes and sectors of the flow graph shown in Figure 16.

RDOS attack. In this experiment, we investigate the impact of the RDOS attack on different sectors. The example of Figure 16 has 12 sectors. In C-RDOS, each time, one of the sectors is the target of attack and then we calculate the metric. By comparing the values, we can find which sectors or routes are more important in the flow graph. In P-RDOS, each time, we suppose that one of the routes is the target of attack and calculate the metric. In our experiment, each route

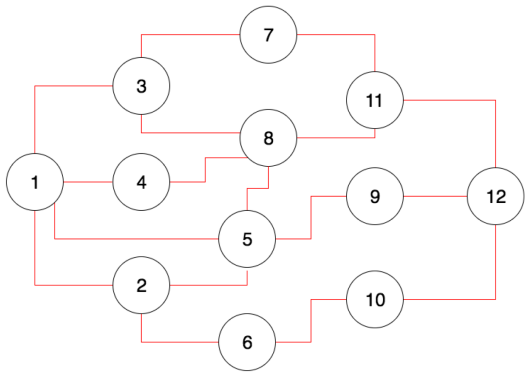


Fig. 16. Example of air traffic flows.

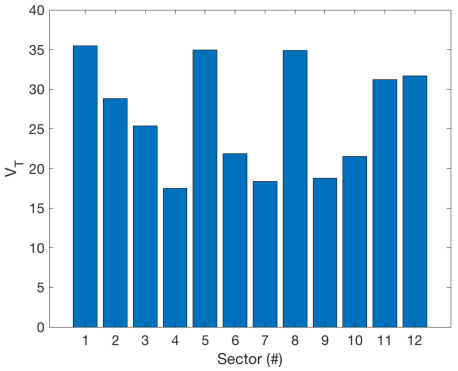


Fig. 17. V_T for each sector that is under a C-RDOS attack.

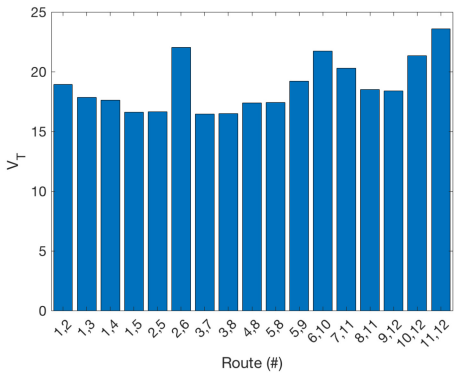


Fig. 18. V_T for each route that is under a P-RDOS attack.

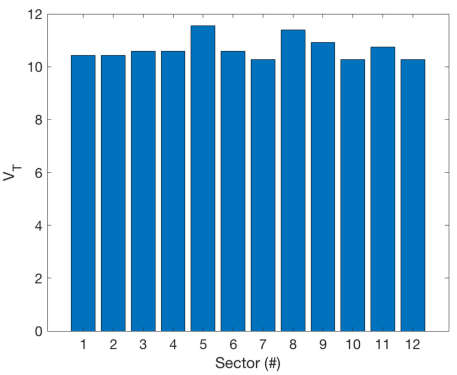


Fig. 19. V_T for each sector that is under an SDOS attack.

is bi-directional. We assume that the value of f for all routes is equal to 2. Figure 17 shows the results of a C-RDOS attack, and Figure 18 shows the results of a P-RDOS attack. The results show that sectors 1, 5, and 8 are more vulnerable than the other sectors. Moreover, the following routes are more vulnerable than other routes: 11,12; 2,6; 6,10; and 10,12.

SDOS attack. In this experiment, we investigate the impact of the SDOS attack on different sectors. We use the example of Figure 16 for this experiment. We repeat this experiment for different sectors. Each time, we select one of the sectors as the target of attack and calculate V_T. We suppose that the number of aircraft in outflows of the targeted sector increases by a factor of 3. In other words, the normal value of f is equal to 2, and the value of f for outflows of the target sector is equal to 6. Figure 19 shows the results.

RST attack. Since the RST attack does not change the structure of the flow graph and has a low impact on changing the value of f, we do not show any results from this analysis.

5.3 Metric Verification for an RDOS Attack

The RDOS attack is the only attack in which the structure of the graph is changed based on the edge removal. In the SDOS attack, the structure of the graph is changed based on the node removal (bypassing of the queues) and the edges keep their connectivity. In the RST attack, only the flow of one (or few) edge is changed. Therefore, it does not impact on the structure of the graph. Since

RDOS is the only attack that leads to a change of graph structure, we focus on the RDOS attack. In this section, we investigate the structure of the flow graph.

We present different parameters and find a formula to compute vulnerability of sectors and paths in air traffic flows. Then we compare our results with the values of the metric presented in the previous section (V_T). For calculating the vulnerability degree in air traffic flows, we need to know how many paths are eliminated after shutting down a sector. First, we introduce two variables, $lostpath_k^n$ and $reducepath_k^n$, as defined next:

- $lostpath_k^n$: If there are X routes with length of n between sector i and sector j, but when sector k is shut down ($k \neq i$ and $k \neq j$) there no longer are any routes with length of n, then $lostpath_k^n(i,j) = X$. This factor demonstrates that when sector k is shut down, all routes with length of n between i and j are eliminated. Then, $lostpath_k^n = \sum_{i \in S} \sum_{j \in S} lostpath_k^n(i,j)$, where S is the set of sectors in air traffic flows. We can use same definition to find the number of routes that are eliminated after shutting down a route. In this condition, k is a path that is shut down.

$$lostpath_k^n(i,j) = \begin{cases} X & \text{if all } X \text{ routes with length of } n \text{ between } i \text{ and } j \text{ are eliminated} \\ 0 & \text{if at least one route with length of } n \text{ remains between } i \text{ and } j \end{cases} \tag{10}$$

- $reducepath_k^n$: If there are X routes with length n between sector i and sector j, and when the target sector k is shut down ($k \neq i$ and $k \neq j$) there remain Υ routes ($0 < \Upsilon < X$) with length n between i and j, $reducepath_k^n(i,j) = X - \Upsilon$. This factor shows that by shutting down a sector, some routes with length n between i and j are eliminated. But $X - \Upsilon$ routes remain. Then, $reducepath_k^n = \sum_{i \in S} \sum_{j \in S} reducepath_k^n(i,j)$. We can use the same definition to find the number of routes that are reduced when a route is shut down. In this condition, k is a path that is shut down.

$$reducepath_k^n(i,j) = \begin{cases} X - \Upsilon & \text{if } \Upsilon \text{ routes of all } X \text{ routes with length } n \text{ between } i \text{ and } j \\ & \text{remain} \\ 0 & \text{if all routes or no routes with length } n \text{ are eliminated between} \\ & i \text{ and } j \end{cases} \tag{11}$$

- $defaultpath^n$: The number of routes with length n in the air traffic flow graph.

Using presented parameters, we can define a measure for vulnerability of air traffic flows.

$$V_k = \sum_{i=1}^{max(n)} (max(n) - i + 1) \frac{[\mu(lostpath_k^i) + (1-\mu)(reducepath_k^i)]}{defaultpath^i}, \tag{12}$$

where V_k is the vulnerability of the air traffic flows when sector k (or route k) is shut down. The term $(max(n) - i + 1)$ defines the weight of the routes based on their length. Since, subject to safety requirement, it is important to minimize cost by appropriate route selection [8], airlines select shorter routes between the source and destination. Therefore, the length of routes plays a crucial role in air traffic flow management. The term $(max(n) - i + 1)$ shows that the impact of losing the shorter routes is greater than losing the longer routes. For example, if the length of the longest route is equal to 7, the weight of losing the route with a length of 2 is 6. However, the weight of losing the route with a length of 5 is 3. The constant μ is $0.5 < \mu < 1$ and weight the sensitivity of lost paths with respect to reduced paths. We use the example of Figure 16 and calculate V_k for each sector and route. We use $\mu = 0.75$ in our calculations. Table 2 shows the comparison between our metric (V_k) and the metric presented by Roy et al. [21] (V_T). The rank column shows which sectors are more vulnerable. The results show that the V_K metric recognizes

Table 2. Compare Metrics for a C-RDOS Attack

Sector	V_K		V_T		Rank Difference
	Rank	Value	Rank	Value	
1	2	15.68	1	35.49	1
2	5	12.1	6	28.82	1
3	7	8.56	7	25.38	0
4	12	3.36	12	17.5	0
5	1	20.48	2	34.95	1
6	8	5.87	8	21.88	0
7	10	5.56	11	18.38	1
8	3	14.92	3	34.9	0
9	11	5.25	10	18.79	1
10	9	5.69	9	21.53	0
11	6	11.71	5	31.2	1
12	4	12.45	4	31.65	0

sector 5 and sector 1. The V_T metric identifies the same sectors as the most vulnerable sectors but in different order (sector 1 as the first rank and sector 5 as the second rank). The main reason is because they have more routes compared to other sectors. Moreover, some of the paths that pass through them are not replaceable by other paths. Both metrics rank sectors 8 and 12 as the third and fourth vulnerable sectors. Sector 8 has four routes (same as sectors 1 and 5); however, it is less vulnerable than sectors 1 and 5. The main reason is because the paths of sector 8 are less critical than the paths of sectors 1 and 5. For example, by shutting down sector 5, we lose a path with a length of 3 between sectors 1 and 12 that is not replaceable by other paths. However, by shutting down sector 8, all paths that pass through this sector could be replaced by other paths. For example, the path between sectors 1 and 11 that goes through sector 8 could be replaced by the path that passes through sectors 3 and 7 and has the same length. By comparing the results, we can find that the difference of the rank in both metrics is at most 1.

5.4 Long-Term Impacts on Air Traffic Flow

Factors such as the capacity of outflow (C_i) and the size of the input of queue (U_i) change the impact of an attack in the long term. During the attack, the value of the backlog increases, and after the attack, it does not change, but it is greater than the value before the attack. In this section, we investigate the impacts of attacks in different cases for C-RDOS. In this attack, we consider two different scenarios to compare the results. In one scenario, $U_i(t) < C_i(t)$, and in the second scenario, $U_i(t) = C_i(t)$. We use the flow graph of Figure 16 for our examples. The properties of attack are as follows:

- The attack starts at $t = 3$ and lasts until $t = 6$. For the first case, the routes of sector 5 are the target of attack, and for the second case, the routes of sector 11 are the target of attack. For sector 5, we focus on the outflow to sector 9, and for sector 11, we focus on the outflow to sector 12.
- $X_9^5(0) = X_{12}^{11}(0) = 2$. The initial backlog of the queue for both cases is 2.
- $C_9^5(t) = C_{12}^{11}(t) = 3$. In each time interval, three aircraft are served.
- In the first case, $U_9^5(t) = 3$, and for the second case, $U_{12}^{11}(t) = 2$. It is the number of aircraft that comes to the queue in each time interval.

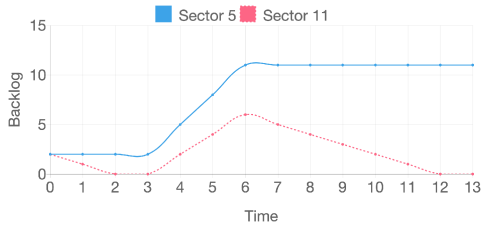


Fig. 20. Backlog when for the outflow of sector 5 $U_i(t) = C_i(t)$ and for the outflow of sector 11 $U_i(t) < C_i(t)$.

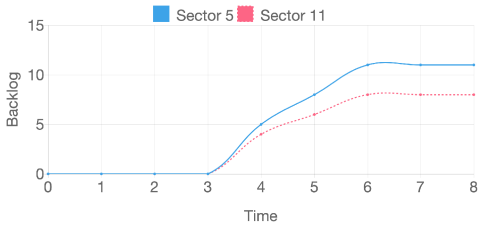


Fig. 21. Backlog when for the outflow of sector 5 $U_i(t) = C_i(t) = 3$ and for the outflow of sector 11 $U_i(t) = C_i(t) = 2$.

Figure 20 shows how the attack affects the backlog. The result shows that if $U_i(t) < C_i(t)$, the sector returns to the normal condition after some time intervals. But if $U_i(t) = C_i(t)$, effects of the attack remain. In another experiment, we investigate the rate of backlog increasing. We keep all properties from the previous experiment and only change $C_{12}^{11} = 2$ for the second case. In both cases, $U_i(t) = C_i(t)$ but have different values. Figure 21 shows how the attack affects the backlog. The results of two experiments show that if $U_i(t) = C_i(t)$, the backlog increases by the rate of $U_i(t)$ during the attack. If $U_i(t) < C_i(t)$, first the backlog decreases with the rate of $U_i(t) - C_i(t)$, and during the attack, it increases with the rate of $U_i(t)$.

6 DISCUSSION AND POTENTIAL MITIGATIONS

The previous sections introduced a combination of analytical attack scenarios and vulnerability metrics to evaluate the impact of attacks to ATC; however, this section will provide further discussion in identifying the key factors contributing to the risk of these attacks based on the significance of the route manipulations. During the C-RDOS attack, all outflows are blocked and all inflows should wait in the queues and increase the backlog of the queues. Therefore, the rate of inflows during the attack has a significant role in the impact of attacks. If the rate of inflows is m aircraft per time interval and the sector has n outflows, the backlog of queues increases by the rate of m/n aircraft per time interval on average. The rate for each outflow i is U_i, which is the input of the queue of outflow. The value of C is an important factor to decrease the impacts of the attack when it is finished. If there are n outflows and $\sum_i^n C_i = c$, the aircraft are served by the rate of c/n per time interval on average. The rate for each outflow is C_i. For the P-RDOS attack, the impact is only on one outflow.

The target of an RST attack is an aircraft. Therefore, there is not any blockage in the inflows or outflows. As the attacker is only injecting a fake route for the target aircraft, the backlog of one of the outflows increases one unit.

For an SDOS attack, as a result of removing the queue management, the outflows increase. If the attack happens, all aircraft in the queue and all new aircraft pass through outflows. After that, there is no aircraft in the queue, and all new aircraft pass to outflows. The rate of increasing the outflow in the first time interval of attack is $b_i + U_i$; after that, it is U_i. This large amount of outflows impacts on the inflows of the next sectors and leads to increasing the backlog of them.

The RDOS attack increases the backlog of the target sector. The RST attack changes the backlog of the original destination and the new destination that is injected by the attacker. In the SDOS attack, the backlog increases for the sectors that have a route from the targeted sector. Table 3 shows a summary of attacks. We know that the value of $U_i(t)$ affects the backlog in different attacks. Figure 22 shows the effects of $U_i(t)$ to the sectors. The blue line shows the effect when $U_i(t) < C_i$. In other words, the number of aircraft that enter the queue is smaller than the number

Table 3. Attacks Impact Summary

Attacks	RDOS	RST	SDOS
Effected by:	Inflow	Outflow (minor)	Outflow
Backlog increase rate	U_i	1	U_i
Impacts on:	Single sector	2 sectors	Multisectors

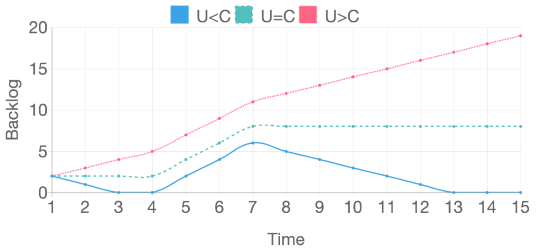


Fig. 22. How the value of $U_i(t)$ affects backlog.

Table 4. Attack Conclusion

Attack	Impact	Difficulty	Attack Vector	Goal
RDOS	High	Medium	Message injecting	Shut down route or sector
RST	Low	High	Message jamming and injecting	Create a fake route
SDOS	Medium-High	Low	Jamming	Bypass queuing

of aircraft that get served. In this condition, the backlog decreases to zero in some time interval after the attack. During the attack, the value of backlog increases. When the attack ends, since $U_i(t) < C_i$, the value of the backlog decreases. The green dashed line shows the effect of the attack when $U_i(t) = C_i$. When the attack happens, the backlog increases. After the attack, since $U_i(t) = C_i$, the value of the backlog remains constant, as the effect of the attack continues. The dotted red line shows the condition that $U_i(t) > C_i$. In this condition, the value of the backlog increases before the attack. During the attack, the value of the backlog continues to increase with the larger rate. When the attack finishes, the rate of increasing returns to the normal value.

Table 4 shows a conclusion of the proposed attacks, including their goal, difficulty, and attack vector.

6.1 Attack Mitigation Techniques

Several countermeasures, such as secure location verification and secure broadcast authentication methods, help increase security of the ADS-B system and avoid these attacks [28]. However, each method has some drawbacks. Secure location verification methods usually need expensive hardware; therefore, systems would not be cost effective at scale. The secure authentication methods face problems such as small ADS-B message length, which limits space for more headers (e.g., message authentication code). Furthermore, the large number of aircraft and their geographic dispersion across multiple countries and ATC domains make key management and distribution more difficult [28]. However, some research into the security of wireless communication in the physical layer (e.g., [38]) may help address these concerns.

Due to the lack of attack protection techniques, rerouting the blocked aircraft could help decrease the backlog in an RDOS attack. In an SDOS attack, increasing the value of c for a short period in the sectors located after the target sector leads to decreasing the backlog at a more significant rate. Using the proposed method, we can evaluate that these techniques are helpful and how much they can reduce the impact on air traffic flows. Moreover, by comparing the metrics for different structures, we can choose the best structure for the system.

7 CONCLUSION

In this article, we explained three different attack scenarios (RST, RDOS, SDOS) to ATC systems and developed a formal DQN model to evaluate their impact on a simplified model. The RDOS attack

is launched by injecting the ADS-B message of nonexisting aircraft into the air traffic system. Although the controllers cannot distinguish real and injected aircraft, they do not serve the aircraft and the routes of the sector are shut down. As a result of this attack, the outflows are blocked and the aircraft have to wait to be served. The RST attack blocks the ADS-B message from a valid aircraft and injects a manipulated ADS-B message for the airplane. This attack affects on two outflows of the sector and makes changes in queue management of the sector controller. The SDOS attack is lunched by jamming the messages near the sector controller. As a result of this attack, aircraft are unable to receive the commands of the sector about queue management and pass the sector without waiting in the queue. Based on this analysis, we demonstrate that the RDOS attack provides the greatest impact to the ATC routes and will likely introduce the greatest delays, whereas the SDOS and RST attacks maintain more confined impact to specific planes and routes.

REFERENCES

[1] Federal Aviation Administration. 2019. Air Traffic By the Numbers. Retrieved February 10, 2020 from https://www.faa.gov/air_traffic/by_the_numbers/.

[2] Federal Aviation Administration. 2013. Air Route Traffic Control Centers (ARTCC). Retrieved February 10, 2020 from https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/air_traffic_services/artcc/.

[3] Alexandre M. Bayen, Robin L. Raffard, and Claire J. Tomlin. 2004. Eulerian network model of air traffic flow in congested areas. In *Proceedings of the 2004 American Control Conference*, Vol. 6. IEEE, Los Alamitos, CA, 5520–5526.

[4] Akshay Belle, Dominic McConnachie, and Philippe Bonnefoy. 2015. A methodology for environmental and energy assessment of operational improvements. In *Proceedings of the 11th USA/Europe Air Traffic Management Research and Development Seminar*.

[5] Andrei Costin and Aurélien Francillon. 2012. Ghost in the air (traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. In *Proceedings of Black Hat USA 2012*. 1–12.

[6] Gerald L. Dillingham, Gregory C. Wilshusen, and Nabajyoti Barkakati. 2015. GAO-15-221: FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen. Retrieved February 10, 2020 from https://www.gao.gov/assets/670/669627.pdf.

[7] Claus Gwiggner and Sakae Nagaoka. 2008. 2B10 Recent Models in the Analysis of Air Traffic Flow. Retrieved February 20, 2020 from https://lix.polytechnique.fr/~gwiggner/Pubs/JSASS08.pdf.

[8] K. C. Khurana. 2009. *Aviation Management: Global Perspectives*. Global India Publications.

[9] Donald McCallie, Jonathan Butts, and Robert Mills. 2011. Security analysis of the ADS-B implementation in the Next Generation Air Transportation System. *International Journal of Critical Infrastructure Protection* 4, 2 (2011), 78–87. DOI: https://doi.org/10.1016/j.ijcip.2011.06.001

[10] P. K. Menon, G. D. Sweriduk, T. Lam, G. M. Diaz, and Karl D. Bilimoria. 2006. Computer-aided Eulerian air traffic flow modeling and predictive control. *Journal of Guidance, Control, and Dynamics* 29, 1 (2006), 12–19.

[11] D. Morgan. 2016. Hackers Attack Air Traffic Control. Retrieved February 10, 2020 from http://abcnews.go.com/US/story?id=95993&page=1.

[12] Michael Nolan. 2010. *Fundamentals of Air Traffic Control*. Cengage Learning.

[13] The National Academy of Sciences. 2015. *A Review of the Next Generation Air Transportation System: Implications and Importance of System Architecture*. National Academies Press, Washington, DC.

[14] U.S. Department of Transportation. Federal Aviation Administration. 2016. The Future of the NAS. Retrieved February 10, 2020 from https://www.faa.gov/nextgen/media/futureofthenas.pdf.

[15] Pangun Park and Claire Tomlin. 2012. Investigating communication infrastructure of next generation air traffic management. In *Proceedings of the IEEE/ACM 3rd International Conference on Cyber-Physical Systems (ICCPS'12)*. IEEE, Los Alamitos, CA, 35–44.

[16] Pangun Park and Claire Tomlin. 2015. Performance evaluation and optimization of communication infrastructure for the Next Generation Air Transportation System. *IEEE Transactions on Parallel and Distributed Systems* 26, 4 (2015), 1106–1116.

[17] Leon Purton, Hussein Abbass, and Sameer Alam. 2010. Identification of ADS-B system vulnerabilities and threats. In *Proceedings of the Australian Transport Research Forum, Canberra*. 1–16.

[18] Sandip Roy and Banavar Sridhar. 2016. Cyber-threat assessment for the air traffic management system: A network controls approach. In *Proceedings of the 16th AIAA Aviation Technology, Integration, and Operations Conference*. 4354.

[19] Sandip Roy, Banavar Sridhar, and George C. Verghese. 2003. An aggregate dynamic stochastic model for an air traffic system. In *Proceedings of the 5th Eurocontrol/Federal Aviation Agency Air Traffic Management Research and Development Seminar*.

[20] Sandip Roy, Ali Tamimi, Adam Hahn, Mengran Xue, Sajal Das, Amirkhosro Vosughi, and Sean Warnick. 2018. A modeling framework for assessing cyber disruptions and attacks to the National Airspace System. In *Proceedings of the 2018 AIAA Modeling and Simulation Technologies Conference*. 0109.

[21] Sandip Roy, Mengran Xue, and Banavar Sridhar. 2017. Vulnerability metrics for the airspace system. In *Proceedings of the 12th USA/Europe Air Traffic Management Research and Development Seminar (ATM'17)*.

[22] Neha Rungta, Eric G. Mercer, Franco Raimondi, Bjorn C. Krantz, Richard Stocker, and Andrew Wallace. 2016. Modeling complex air traffic management systems. In *Proceedings of the IEEE/ACM 8th International Workshop on Modeling in Software Engineering (MiSE'16)*. IEEE, Los Alamitos, CA, 41–47.

[23] Matthias Schäfer, Vincent Lenders, and Ivan Martinovic. 2013. Experimental analysis of attacks on next generation air traffic communication. In *Proceedings of the International Conference on Applied Cryptography and Network Security*. 253–271.

[24] Daniel A. Spielman and Shang-Hua Teng. 2007. Spectral partitioning works: Planar graphs and finite element meshes. *Linear Algebra and Its Applications* 421, 2–3 (2007), 284–305.

[25] Banavar Sridhar, Shon R. Grabbe, and Avijit Mukherjee. 2008. Modeling and optimization in traffic flow management. *Proceedings of the IEEE* 96, 12 (2008), 2060–2080.

[26] Kjetil Stormark. 2016. Sweden issued cyber attack alert. *Aldrimer*. Retrieved February 10, 2020 from https://www.aldrimer.no/sweden-issued-cyber-attack-alert-as-its-air-traffic-reeled/.

[27] Martin Strohmeier. 2016. *Security in Next Generation Air Traffic Communication Networks*. Ph.D. Dissertation. University of Oxford.

[28] Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. 2015. On the security of the Automatic Dependent Surveillance-Broadcast protocol. *IEEE Communications Surveys & Tutorials* 17, 2 (2015), 1066–1087.

[29] M. Strohmeier, M. Schafer, R. Pinheiro, V. Lenders, and I. Martinovic. 2016. On perception and reality in wireless air traffic communication security. *IEEE Intelligent Transportation Systems Society* 18, 6 (Oct. 2016), 1338–1357.

[30] Christine Taylor, Craig Wanke, Yan Wan, and Sandip Roy. 2012. A decision support tool for flow contingency management. In *Proceedings of the AIAA Guidance, Navigation, and Control Conference*. 4976.

[31] Armin Teymouri, Ali Mehrizi-Sani, and Chen-Ching Liu. 2018. Cyber security risk assessment of solar PV units with reactive power capability. In *Proceedings of the 44th Annual Conference of the IEEE Industrial Electronics Society (IECON'18)*. IEEE, Los Alamitos, CA, 2872–2877.

[32] Anusha Thudimilla and Bruce McMillin. 2017. Multiple security domain nondeducibility air traffic surveillance systems. In *Proceedings of the IEEE 18th International Symposium on High Assurance Systems Engineering (HASE'17)*. IEEE, Los Alamitos, CA, 136–139.

[33] Federal Aviation Administration. 2015. En route operations. In *Instrument Procedures Handbook*. Federal Aviation Administration.

[34] Yan Wan, Christine Taylor, Sandip Roy, Craig Wanke, and Yi Zhou. 2013. Dynamic queuing network model for flow contingency management. *IEEE Transactions on Intelligent Transportation Systems* 14, 3 (2013), 1380–1392.

[35] Chao Wang, Jing Ge, and Xiaohao Xu. 2009. Analysis of air traffic flow control through agent-based modeling and simulation. In *Proceedings of the International Conference on Computer Modeling and Simulation (ICCMS'09)*. IEEE, Los Alamitos, CA, 286–290.

[36] James Williams and T. L. Signore. 2010. National Airspace System Security Cyber Architecture. Retrieved February 10, 2020 from https://www.mitre.org/sites/default/files/publications/10_4169.pdf.

[37] Gregory C. Wilshusen, Nabajyoti Barkakati, and Gerald L. Dillingham. 2015. *GAO-15-370: FAA Needs to Address Weaknesses in Air Traffic Control Systems*. Government Accountability Office, Washington, DC.

[38] Mustafa Harun Yılmaz, Ertuğrul Güvenkaya, Haji M. Furqan, Selçuk Köse, and Hüseyin Arslan. 2017. Cognitive security of wireless communication systems in the physical layer. *Wireless Communications and Mobile Computing* 2017 (2017).

Received October 2018; revised November 2019; accepted December 2019