AIR TRANSPORTATION INFRASTRUCTURE ROBUSTNESS ASSESSMENT FOR PROACTIVE SYSTEMIC RISK MANAGEMENT

AIR TRANSPORTATION INFRASTRUCTURE ROBUSTNESS ASSESSMENT FOR PROACTIVE SYSTEMIC RISK MANAGEMENT

BY:
YASSIEN YASSIEN

A THESIS SUBMITTED TO THE SCHOOL OF GRADUATE STUDIES
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE
MASTER OF APPLIED SCIENCE
MCMASTER UNIVERSITY
APRIL 2020

McMaster University MASTER OF APPLIED SCIENCE (2018) Hamilton, Ontario, (Civil Engineering)

TITLE: Air Transportation Infrastructure Robustness Assessment for Proactive Systemic Risk Management

AUTHOR: Yassien Yassien

FIRST SUPERVISOR: Dr. Moataz Mohamed
SECOND SUPERVISOR: Dr. Wael El-Dakhakhni

NUMBER OF PAGES: 48

ABSTRACT

A key attribute of resilience, robustness serves as a predictor of infrastructure system performance under disruptions, thus informing proactive infrastructure risk management. A literature review indicated that previous studies did not consider some key factors that can influence the robustness of Air Transportation Infrastructure Networks (ATIN) and thus their (system-level cascade) *systemic* risk management processes. In this respect, the current study first assesses existing and then develops a new methodology to quantify the robustness of ATIN. Specifically, based on integrating travel time and flight frequency, the study develops alternative best route and link weight approaches to assess key ATIN robustness measures and relevant operating cost losses (OCL). In order to demonstrate the practical use of the developed methodology, the robustness and the associated OCL of the Canadian Domestic Air Traffic Network are evaluated under random failures (i.e., disruptive events that occur randomly) and targeted threats (i.e., disruptive events that occur deliberately). The analysis results show that the network robustness is influenced by the utilized evaluation approach, especially after 20% of the network components become nonoperational. Overall, the methodology developed within this study is expected to provide ATIN policymakers with the means to quantify the network robustness and OCL, and thus enable ATIN resilience-guided proactive risk management in the face of natural or anthropogenic hazard realizations.

ACKNOWLEDGMENT

I would like to express my sincere gratitude to my supervisors, Dr. Moataz Mohamed and Dr. Wael El-Dakhakhni, for their continuous support and guidance. I would like to thank the rest of the members of my examination committee, Dr. Mike Tait, Dr. Zoe Li, and Dr. Mohamed Hussein for their time and insightful comments. Also, I want to thank Dr. Mohamed Ezzeldin for his help, support, and his time for consultation.

Finally, I would like to gratitude my family for making all these possible and their encouragement and support that brought me in the place I am now.

CO-AUTHORSHIP

This thesis has been prepared in accordance with the regulations for a sandwich thesis format or as a compilation of research papers stipulated by the faculty of graduate studies at McMaster University. This research presents analytical work carried out solely by Yassien Yassien. Advice and guidance were provided for the whole thesis by the academic supervisors Drs. Wael El-Dakhakhni and Moataz Mohamed, in addition to support from Dr. Mohamed Ezzeldin. Information presented from outside sources, which has been used towards analysis or discussion, has been cited where appropriate; all other materials are the sole work of the author.

CONTENTS

TABLES

FIGURES

CHAPTER 1: INTRODUCTION

Risk Definition

The term 'risk' defines as the possibility of meeting danger or of suffering loss or harm (Hornby 1995). But, in general, this definition is not applicable for civil infrastructure systems (Ettouney and Alampalli, 2016; Lee et al., 2013 and Chiara, 2009). For civil infrastructures, it is key to define risk in a practical way to address the needs of civil infrastructure stakeholders and to also accommodate relevant uncertainties and management priorities. The literature shows that risk is often defined as the relationship between the hazards that may possibly debase infrastructure's performance and the associated consequences (Gutteling and Wiegman 1996). This last definition seems to be useful for the civil infrastructure field. It can be modified slightly as a description of the outcome of an unfavorable, uncertain event, which might degrade the performance of a single civil infrastructure (Ettouney and Alampalli, 2016).

Risk can be generally divided into three fundamental elements namely: threat, vulnerability, and consequences (Renfroe and Smith, 2010; Cox and Anthony, 2008; Pipattanapiwong et al., 2004; OECD, 2003; Al - Bahar and Crandall 1990). A threat indicates a situation that can affect a particular system or component and has the potential to cause system performance degradation. As a basic element of risk function, it is clear that threat is directly proportional to infrastructure risk (Cox and Anthony, 2008) because of the potential damaging consequences such threats can leave in such infrastructures. It indicates the susceptibility of the system or one of its components to a particular degrading event or group of events (Aven, 2011). Vulnerability is a subjective measure that is useful in the case of considering subjective situations that cannot be described in an objective manner. Risk is directly proportional to vulnerability, similar to threats. It describes the impact or results of a particular event (Aven, 2011; Cox and Anthony, 2008). The consequences are directly related to the asset, such as repair costs or indirectly related to the asset such as the social or economic impacts of disrupting a specific infrastructure due to confronting a disruptive event (Renfroe and Smith, 2010).

Systemic Risk

Systemic risk refers to a risk on an entire system rather than the failure of an individual component (Lee et al., 2013 and Chiara, 2009). In an infrastructural context, systemic risk denotes the system cascading failure risk, caused by linkages among the system components, resulting in a severe decline in system performance/functionality (Taylor et al., 2006). Transportation networks, the internet, and electric power grids are all examples of infrastructure systems in which connectivity among system components is essential. Because of such connectivity, catastrophic cascading failure of the components can occur when the system faces a catastrophic shock, especially if the affected component is critical (e.g., represents a hub station in transportation network) (Huang et al., 2013). Subsequently, in order to minimize the systemic risk, infrastructure systems should be designed to be robust to such devastating shocks. In the wake of the recent disasters, increased attention has been given to infrastructure systems and to systemic risk in particular. The widespread impact of the current disasters (natural such as climate change consequences, or anthropogenic such as terrorist attacks) demonstrated that infrastructure systems became increasingly interconnected, and such disastrous events can provoke global cascading failure that stalemates the system for a prolonged period of time (Zhou et al., 2012; Taylor et al., 2006). Thus, policymakers are supposed to implement safety measures to prevent/mitigate systemic impacts and their cascading failures.

There are five main functions that can be utilized in risk assessment. These are Reliability, Exposure, Likelihood, Sustainability, and Resilience (Ettouney and Alampalli, 2016; Ayyub, 2014). First, reliability is a function in the capacity of the system and the demands on that system (Rausand, 2004). Second, exposure is defined as the function of a combination of hazards and their impact. In other words, exposure is a subjective estimate of the combined effects of the hazard and the system vulnerability to that hazard (Cardona, 2012). Third, likelihood depends, as a function, mainly on both vulnerability and hazard (Ayyub, 2014). Fourth, sustainability is defined as the system ability to operate within acceptable and renewable limits, having respect for available natural resources (Sustainable Measures 2014). Fifth, resilience is defined, as will be illustrated in more detail later, the ability of the system to withstand major disruptions within acceptable degradation range and recover within an acceptable time. Even with the aforementioned five functions to assess risk, the risk assessment process involves some trade-offs due to risk complexity (Renfroe and Smith, 2010). For this reason, in the literature, risk models are simplified and do not account of “real world” boundaries, especially of the various pathways through which a hazard develops. Risk models cannot consider all aspects of human behaviour. In addition, risk models cannot integrate all the indirect consequences of a hazard, which often result from unanticipated linkages between system components (Cox and Anthony, 2008). Risk assessment, therefore, needs to understand the determinants of hazards and vulnerability, and better evaluation of externalities (Ayyub, 2014).

Risk Management

Risk management is concerned with the identification, evaluation, and analysis of risks confronting the underlying infrastructure to prioritize these risks followed by properly allocating resources to minimize, monitor, mitigate, and control the impact of disruptive events (Choudhry et al., 2012; Hubbard et al., 2009). Risk management process adopts two strategies, namely, proactive risk management and reactive risk management. Proactive risk management ranks the identified risks according to their expected negative consequences relevant to the importance of the infrastructure considered (Taylor et al., 2006). Reactive risk management is focused on disaster realization and problem-solving rather than problem-prevention (Attarzadeh et al., 2011; Schatteman et al., 2008). Also, risk management can be divided into four different steps namely, in order: identification, assessment/analysis, response/decision-making, and monitoring (Choudhry et al., 2012; Hubbard et al., 2009; Schatteman et al., 2008).

Risk identification step is applied in the overall risk management plan, the infrastructure objective, and the chronicled hazard exposed to the infrastructure. Other useful sources of risk identification are regulators, operators, design standards, and events related to the infrastructure operation. In general, the main objectives associated with the risk identification process are focused on cost, time and quality (Al - Bahar and Crandall 1990).

In terms of the risk assessment/analysis process, the main variables are the probability of the risks and the associated impacts on the infrastructure. Risk assessments can be generally classified into qualitative and quantitative assessments. The qualitative risk assessment includes risk description, risk occurrence stages, the affected elements, risk occurrence factors, relation with other risks, risk occurrence likelihood, and how the risk can affect the infrastructure. Whereas the quantitative risk assessment can be conducted using one of the techniques that include simulation-, scenario-, probability-, correlation-, and sensitivity analysis (Schatteman et al., 2008).

Whilst the responses/decisions can be classified into four actions: acceptance, reduction, avoidance, and transfer. In acceptance/retention decisions, the risk will be accepted with no actions to face or reduce its impact. The adoption of risk acceptance may be conscious or unconscious (Pipattanapiwong et al., 2004). In conscious risk retention, the risk is recognized without reduction or transferring. Whilst the unconscious related with unperceived risks. Risk reduction can be implemented through loss prevention or recovery after event occurrence (Mansouri et al., 2009). The target of the loss prevention is to prevent the loss occurred due to the risk, while the recovery aimed to suppress the severity of the losses. However, loss prevention is highly effective if the loss can be completely eliminated (Mansouri et al., 2009; OECD, 2003), it is impossible to prevent all possible risks which is more costly than the losses themselves. Avoidance is employed when individuals or organizations refuse to accept risk where the exposure to risk in not permitted. Risk can be passed or transferred from organization to another which is able to deal with it.

Continuous monitoring is needed as well to keep an eye on the changing risks that should be detected and managed and the changes/updates in risk response actions to cope with risk changes (Schatteman et al., 2008). Risk monitoring continues for the life of the infrastructure to keep tracking of the identified-, residual-, and new risks, in addition to monitoring planned-strategy enforcement for the identified risks and evaluating its effectiveness. The risks change as the infrastructure matures because of the new risks' development or anticipated risks' disappearance. Also, risk ratings/prioritizations can change during the infrastructure lifecycle (Tang et al., 2007).

Resilience

Resilience as one of the essential functions used to assess infrastructure risk, contributes to risk analysis and making decisions. Infrastructure resilience has gained substantial attention in recent years especially after experiencing multiple low-probability and high-consequence disruptions such as extreme weather events and terroristic attacks. Because of the essential role that civil infrastructure systems play in social security, safety, and welfare, continuous efforts from governments, private sector, and society are needed to operate and develop such valuable infrastructural assets (Wang et al., 2018; Bruneau et al., 2003). Also, more understanding of resilience applications of civil infrastructure systems can result in more efficient critical infrastructure protection. Generally, infrastructure system resilience should consider system performance within the following different three stages: prior, during, and following a destructive event occurrence (Bruneau et al., 2003).

The origin of the word 'resilience' is the Latin 'resilio', that has two parts; 're' (again) and 'salire' (spring or jump) and means 'to bounce back'. The term 'resilience' was utilized earlier in elasticity theory to represent the energy stored in elastically deformed materials. In 1940, the term 'resilience' was also utilized in psychology as the individual's ability to recover from trauma (Masten et al., 1990). A work that widespread remarkably the concept of resilience was the work by Holling (1973) in ecology. After applications on ecology and psychology, resilience was integrated in other fields such as industrial processes (Wei and Ji, 2010), economics (Vugrin et al., 2010), engineering (Blackmore and Plant, 2008), business management (Hamel and Valikangas, 2003), etc. Despite the common agreement among the prementioned fields that resilience is the system's ability to 'bounce back' from disruptions, different definitions exist depending on the adopted application (Manyena, 2006).

Now, the concept of resilience gained great awareness in applications of planning, operation, and maintenance of civil infrastructure networks (Santora and Wilson, 2008; O'Rourke, 2007). Resilience of civil infrastructure networks is frequently measured using performance metrics (Santora and Wilson, 2008; O'Rourke, 2007). Fig. 1.1 illustrates a performance-based resilience functionality curve which represents the network performance change over time (Kammouh et al., 2017; Bruneau et al., 2003). Therefore, the reduction on infrastructure performance due to the disruptive event is assumed to be represented by the line that connects point A with point B. While the line B-C represents the recovery, which is assumed linear in that case. Linearity assumptions in lines A-B and B-C are not inherently true in every case. For instance, it could have a trend like the 'dashed' line or 'dash dot' line (Cimellaro et al., 2008). The dashed line in Fig. 1.1 refers to an initially slow recovery, while the dashed dot line represents rapid recovery processes. In Fig. 1.1, the network performance returns back to the pre-disruption performance level and remains stable with time, after recovery.

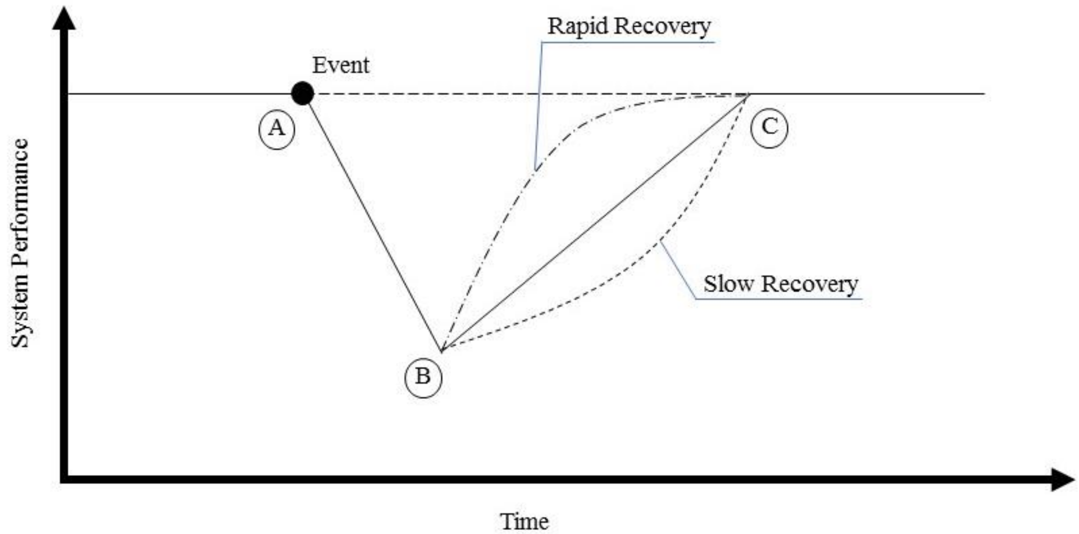

Fig. 1.1: Resilience Function

Through the literature, the Multidisciplinary Center for Extreme Events Research proposed the most commonly used framework for the application of resilience methodologies and methods in civil infrastructure network (MCEER, 2005; Bruneau et al., 2003). This framework represents the network resilience by four functions known as the four R’s (R4): robustness, redundancy, resourcefulness and rapidity (MCEER, 2005). First, robustness is defined as the system ability to withstand stress without suffering degradation or functionality loss. Second, redundancy is defined as the extent to which the system is substitutable, i.e., have the capability to satisfy functional requirements in the case of disruptive events. Third, resourcefulness is defined as the capacity of defining risks, establishing priorities, and mobilizing all/some resources to confront disruptive system events. In other words, resourcefulness includes the ability to utilize the available physical, monetary, technological, and informational materials in addition to human resources to meet determined priorities and reach the aspired objectives. Fourth, rapidity is defined as the ability to meet the determined priorities and achieve the aspired objectives in a timely manner to avoid both future losses and disruptions.

Importance of Air Transportation Infrastructure Networks

As a key critical infrastructure system, Air Transportation Infrastructure Networks (ATIN) play a key role in people and goods mobility as well as its great role in boosting international trade prosperity. Therefore, this thesis is focused on studying the ATIN robustness assessment. Aviation has continued to expand. It has withstood disastrous crises in addition to demonstrating long-term resilience, becoming an indispensable means of transport. Historically, and according to the International Civil Aviation Organization (ICAO) (2015), worldwide airlines carried 3.8 billion passengers achieving annual revenue of 7.1 trillion revenue passenger kilometers. Also, 53 million tons of freight were transported by air. On a daily scale, around 100,000 flights transport over 10 million passengers and around $18 billion worth of goods. Largely, air transport has double-sized every 15 years and has grown faster in comparison with most other industries. Also, ATIN contribute to employment sector through providing direct employment opportunities. Once ATIN are operational, work opportunities and services vary between airport operations/management, maintenance, charter services, storage facilities, and leasing activities. For instance, and to show how ATIN have a massive impact on labor power, the Los Angeles Times reported that the Dallas/Fort Worth (DFW) International Airport has created significant job opportunities since its establishment in the 1970s. Quoting statistics from the US Department of Commerce, the US daily reported that the four countries surrounding the DFW airport had witnessed 148% rise in employment by the turn of the century. In addition, ATIN provide accessibilities, which has a high positive impact on the tourism sector by growing the number of visitors. Therefore, it can notice that the developments of airports have boosted the national economy.

Giant Component Method and Complex Network Theory

The study aims at assessing ATIN robustness using the Giant Component method (calculating and comparing the number of functional system components in the largest component of the network prior to and after disruptions) through adopting Complex Network Theory (CNT) measures (Julliard et al. 2015; Berche et al. 2010). In giant component method (Solé et al., 2008; Beygelzimer et al., 2005), only a fraction of system components remains after an attack or failure, and only the components in a giant connected component of each network remain functional. The goal is to find the fraction of components of each network/infrastructure which remains functional and compare it to the original connected components before the disastrous event (Huang et al., 2013; Zhou et al., 2012).

In recent years, CNT has been gaining significant attention that resulted in developments and applications in various fields. CNT has been implemented in simulating different real networks including road transportation (Tsiotas and Polyzos, 2017; Tian et al., 2016), internet (Barabási, 2013), telecommunications (Grubesic and Murray, 2005), etc. Several network classification-models have been developed in the literature to study the characteristics of complex networks (Barabási, 2013; Lordan et al., 2014). However, three types of complex network models are frequently implemented and hence discussed in the current study. These include Small World- (Watts and Strogatz, 1998), Random- (Erdos and Rényi, 1959), and Scale-free (Barabási, 2013) networks. A Small World network is defined as a highly clustered network with a relatively short average path length (Watts and Strogatz, 1998). In such networks, nodes are typically close to one another and connected through only a small number of links. Conversely, the Random network has a Poisson distribution of nodal degree (the number of links that connects to the node with neighbouring nodes) (Newman, 2010). The third type of networks is the Scale-free, which follows a power-law degree distribution and features a small number of hubs (nodes with a large degree). The World Wide Web is a perfect example of a Scale-free network (Barabási, 2013).

CHAPTER 2: AIR TRANSPORTATION INFRASTRUCTURE ROBUSTNESS ASSESSMENT FOR PROACTIVE SYSTEMIC RISK MANAGEMENT

Abstract: A key attribute of resilience, robustness serves as a predictor of infrastructure system performance under disruptions, thus informing proactive infrastructure risk management. A literature review indicated that previous studies did not consider some key factors that can influence the robustness of Air Transportation Infrastructure Networks (ATIN) and thus their (system-level cascade) *systemic* risk management processes. In this respect, the current study first assesses existing and then develops a new methodology to quantify the robustness of ATIN. Specifically, based on integrating travel time and flight frequency, the study develops alternative best route and link weight approaches to assess key ATIN robustness measures and relevant operating cost losses (OCL). In order to demonstrate the practical use of the developed methodology, the robustness and the associated OCL of the Canadian Domestic Air Traffic Network are evaluated under random failures (i.e., disruptive events that occur randomly) and targeted threats (i.e., disruptive events that occur deliberately). The analysis results show that the network robustness is influenced by the utilized evaluation approach, especially after 20% of the network components become nonoperational. Overall, the methodology developed within this study is expected to provide ATIN policymakers with the means to quantify the network robustness and OCL, and thus enable ATIN resilience-guided proactive risk management in the face of natural or anthropogenic hazard realizations.

Keywords: Air traffic network, Complex Network Theory, Proactive Risk Management, Resilience, Robustness.

Background

Civil infrastructure systems, such as roads, railways, airports, water supply facilities, and wastewater networks, usually require large capital investment and operating/maintenance costs (West et al., 2018; Taylor et al., 2006). Disruptions to such critical infrastructure systems may result in devastating impacts on the national security, economic prosperity and public health and safety. Because the operations of such large infrastructure networks extend spatially and evolve temporally, multiple risks generated by natural (e.g., hurricanes and earthquakes) or anthropogenic (e.g., terrorism and industrial accidents) hazards can significantly affect the former's system-level performance (Padgett et al., 2013; Taylor et al., 2006). Such (system-level) *systemic* risks are defined as the consequences of interdependence-induced failures that would cause cascade-type failures across the entire system (Ezzeldin and El-Dakhakhni, 2019). Systemic risks are further amplified as most modern civil infrastructure systems have become more complex (e.g., cover large spatial areas with extensive interlinkage), more sophisticated (e.g., in terms of their operations and their mutual interdependence), continuously advancing in terms of technology adoption, and the ever-increasing user expectations of around-the-clock reliable service. Therefore, enhancing the safety and reliability of such systems in the face of unforeseen (hyper) risks (Helbing, 2013) has been a key driver in the area of infrastructure disaster risk management (Lee et al., 2013 and Chiara, 2009).

Within the context of the current study, risk management is concerned with the identification, evaluation, and prioritization of risks confronting the underlying infrastructure followed by coordinated and economical application of resources to minimize, monitor, mitigate, and control the probability or impact of what otherwise would be disruptive events (Choudhry et al., 2012; Hubbard et al., 2009). Over the past decade, the increased number of infrastructure disruptive events, and the long-term consequences of such disruptions, have been influencing pertinent risk management strategies (Lee et al., 2013; Del Cano et al., 2002). Such strategies include *proactive risk management* which focuses on ranking the identified risks according to their expected negative consequences relevant to the importance of the infrastructure considered (Taylor et al., 2006). The strategies also encompass reactive risk management which is key in the event of disaster realization (Attarzadeh et al., 2011; Schatteman et al., 2008) as the latter then focuses on problem-solving rather than problem-prevention.

As a process, proactive risk management builds on the decision-maker's intuition and experience in a systematic, effective, rational, logical, prevention-focused and priority-based approach (Taylor et al., 2006). As shown in Fig. 2.1, such a process consists of four main steps: identification, analysis, responding/decision-making, and monitoring of risk (Schatteman et al., 2008; Tang et al., 2007; Del Cano et al., 2002). First, risk identification is the step of systematically and continuously identifying, categorizing, and assessing the initial significance of risks (Tang et al., 2007; Zou et al., 2009). Second, the risk analysis step is the vital link between systematic identification of risks and rational management of the most critical risks. Specifically, this step aims at evaluating the consequences associated with different risks and assessing the impact of such risks through several analyses and measurement techniques (Wang et al., 2016; Zou et al., 2009). Third, the risk response step deals with providing the most efficient responses to the identified and analyzed risks. In this latter step, decision-makers consider how the risk should be managed, for example, by assessing alternative resolutions to either transfer the risk to other parties or to tolerate/mitigate it (Pipattanapiwong et al., 2004). Finally, the step of risk monitoring, where risk consequences are monitored, tracked and reviewed after a decision is taken (Schatteman et al., 2008; Tang et al., 2007).

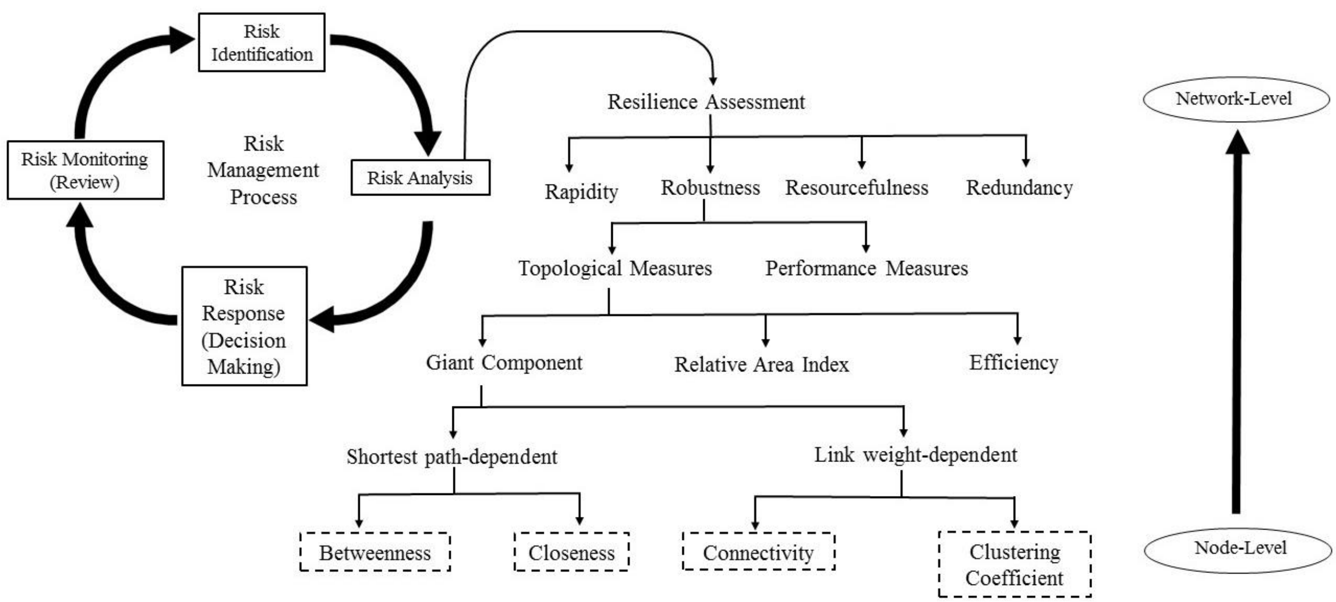

Fig. 2.1: Risk Management Process

The second step of the proactive risk management process (i.e., risk analysis) has been carried out in previous studies (Sánchez-Silva 2018) through a resilience-guided approach, as shown in Fig. 2.1. Such an approach facilitates guiding infrastructure managers to make a tangible difference in preparedness to deal with risks by focusing on the system *resilience*—defined as the system's ability to 'bounce back' following exposure to a disruptive event (Lounis et al., 2016; Carpenter 2014). In other words, resilience assessment is key for infrastructure contingency analysis and proactive risk management (Wang et al., 2018; Kammouh et al., 2017; Wang et al., 2016; Schatteman et al., 2008). In this respect, resilience has been hypothesized to relate to four different attributes: robustness, redundancy, resourcefulness, and rapidity (Bruneau et al., 2003), as shown in Fig. 2.1. Robustness and rapidity are known as the resilience ''ends'', whereas resourcefulness and redundancy are known as the ''means''.

Among critical infrastructure systems, Air Transportation Infrastructure Networks (ATIN) play a major role in the mobility processes of people and goods as well as the international trade. ATIN also link the global economy through supporting and enhancing supply chains and international markets. Subsequently, a disruption to the ATIN has the potential of creating significant cascade economic and social impacts beyond predictions. Globally, ATIN have experienced different forms of disruptions triggered by either natural or anthropogenic hazards that influenced their operations (Lundin, 1995). More recently, in December 2017, a power outage (an anthropogenic hazard) in Atlanta's Hartsfield-Jackson International airport in the USA lasted for only 11 hours yet resulted in cancelling more than 1,000 flights, affecting 30,000 passengers, and causing more than $50 million of economic losses (Cable News Network, 2017). The April 2010 volcanic eruptions of Eyjafjallajökull in Iceland is another disruptive event, albeit due to a natural hazard, that resulted in cancelling an unprecedented number of flights within Europe, creating the highest level of global air travel disruption since the Second World War (Bye et al., 2011). In total, about 20 countries closed their airspace to commercial air traffic, which affected approximately 10 million travelers due to the cancellation of around 4,000 flights (British Broadcasting Corporation News 2010). Such clear cases of systemic risk realizations evidently demonstrate the importance of robustness assessment of ATIN for proactive systemic risk management towards achieving significant economic savings under disruptive events.

ATIN robustness was quantified in the literature according to a pre-defined measure that evaluates the change in the system prior to- and following the realization of disruptive events. ATIN robustness is often assessed based on random failures of network components and/or targeted threat analyses (on specific critical components within the network). For example, the ATIN robustness assessment was proposed to comprise of three steps (Zhou et al., 2019): 1) defining a topological or a performance measure for the ATIN (Fig. 2.1); 2) quantifying such a measure for the

ATIN before and after different disruptive scenarios; and 3) assessing the ATIN robustness based on the changes of this measure. An example of performance measures utilization is the work of Cardillo et al. (2013) to assess ATIN robustness using *passenger flow* as the ATIN performance indicator. Topological measures on the other hand typically represent the structure of the entire network (Lordan et al., 2016), including Efficiency (Zhou et al., 2019), Relative Area Index (Pien et al., 2015), and Giant Component (Lordan et al., 2016). Table 2.1 summarizes details of reported studies that focused on the ATIN robustness assessment.

Table 2.1: Applications of robustness assessment and CNT in air transportation networks

Author	**Aim**	**Context**	**Measures**	**Case Study (number of nodes, number of links)**
(Malik et al., 2019)	Analyzing the network characteristics	Pakistan	Betweenness, Closeness, Degree	(24, 84)
(Ren et al., 2019)	Analyzing the topology of the air sector (region) network	China	Degree, Betweenness, Closeness	(108, 241)
(Wandelt et al., 2019)	Reviewing and comparing the evolution of eight domestic airport networks during the period 2002–2013	Australia, Brazil, Canada, China, India, Russia, the US, and Europe	Assortativity, Clustering coefficient, Degree	Eight different domestic airport networks
(Zhou et al., 2019)	Proposing a novel efficiency and robustness metric for weighted air transport networks	Australia, Brazil, Canada, China, Europe, India, Russia, USA	Robustness, Efficiency, Betweenness, Degree, Strength	Eight domestic air traffic networks
(Dai et al., 2018)	Studying the topological and spatial changes in the network over the period 1979-2012	Southeast Asia	Clustering coefficient Degree	(237, 602)
(Zhang et al., 2018)	Analyzing flight conflicts in the Chinese air traffic network	China	Betweenness Degree	(1499, 2242)
(Hossain and Alam, 2017)	Analyzing the network structure and characteristics	Australia	Closeness Betweenness Clustering coefficient Degree	(131, 596)
(Sun et al., 2017)	Studying the network at different levels of aggregation	Global	Betweenness Clustering coefficient Degree Modularity Density	(3097, 50694)
(Zhu et al., 2018)	Comparing the connectivity of cities in the network	China	Connectivity	23 Chinese cities
(Lordan et al., 2016)	Analyzing route networks for full- and low-cost carriers	Multiple	Robustness, Clustering coefficient, Degree	Routes for 13 airlines in Europe, North America, and China
(Pien et al., 2015)	Conducting topological and operational analyses of the European air traffic network.	Europe	Robustness, Betweenness	784 airports
(Wandelt et al., 2015)	Proposing new exploration search technique for efficient attacking strategy	Australia, Argentina, Germany, Iceland	Robustness, Betweenness, Degree, closeness	Australia (149, 567), Argentina (41, 184), Germany (28, 170), Iceland (5, 7)
(Wandelt and Sun, 2015)	Analyzing the evolution of the network.	Global	Degree Clustering coefficient Betweenness Density Closeness	144 countries

Author	**Aim**	**Context**	**Measures**	**Case Study (number of nodes, number of links)**
(Marzuoli et al., 2014)	Examining the robustness of the American ATIN	USA	Robustness, Betweenness, Degree	(37, 86)
(Wang et al., 2014)	Comparing between the impact of damage-guided attack and degree-guided attack on ATIN's robustness	USA	Robustness, Degree	(332, 2126)
(Wang et al., 2011)	Exploring the network structure and nodal centralities	China	Betweenness Clustering coefficient Closeness Average path length Degree	(144, 1018)
(Paleari et al., 2010)	Investigating the network characteristics and level of service	Multiple	Clustering coefficient Degree Shortest-path length	Europe (467, 5544) US (657, 5488) China (144, 1329)
(Wuellner et al., 2010)	Analyzing the structure of the networks for the operating carriers in the USA	USA	Robustness, Betweenness, Degree	Seven largest passenger carriers in the USA
(Zhang et al., 2010)	Studying the network topological characteristics	China	Degree Clustering coefficient Betweenness	The evolution of the Chinese air traffic network from 1950 to 2010
(Bagler, 2008)	Analyzing the characteristics of weighted and unweighted network	India	Clustering coefficient Degree Node Strength Shortest-path length	(79, 442)
(Guida and Maria, 2007)	Analyzing the network structure	Italy	Degree Betweenness Clustering coefficient	(42, 310)
(Guimera et al., 2005)	Network characteristics evaluation	Global	Degree Betweenness	(3883, 27051)
(Chi et al., 2003)	Analyzing the network's probability distributions to investigate the corresponding characteristics	USA	Clustering coefficient Degree Shortest-path length	(215, 116725)

Scope and Objectives

The current study assesses ATIN robustness using the Giant Component method (calculating the number of airports in the largest component of the network prior to and following disruptions) (Julliard et al., 2015; Berche et al., 2010; Berche et al., 2009; Hu et al., 2008) based on specific Complex Network Theoretic (CNT) measures. For example, *betweenness* refers to the position of an airport in a network and its functionality as a bridge in the shortest paths between all other airports, whereas *closeness* describes the proximity of an airport to the rest of the network airports and is evaluated by the shortest path (Freeman, 1978). *Connectivity* refers to the total weight of in- and out-links connected to an airport, thus indicating such airport importance (Zhu et al., 2018). *Clustering coefficient*, on the other hand, is an indication of the redundancy in the network (Wasserman et al., 1994), whereas neighboring airports (within the cluster) remain interconnected even after one airport becomes nonoperational. Full details of previous studies that applied CNT measures on the ATIN are presented in Table 2.1. As shown in Fig. 2.1, betweenness and closeness are *shortest path*-dependent (i.e., their calculations depend on the shortest paths selected), whereas connectivity and clustering coefficient are *link weight*-dependent (i.e., their calculations depend on the link weight assigned).

Throughout published literature, the estimation of shortest path was based on of the following factors: 1) the number of links needed in order to travel between two airports (e.g., Paleari et al., 2010; Dai et al., 2018; Ren et al., 2019); 2) the travel distance (e.g., Wandelt and Sun, 2015; Sun et al., 2017; Wandelt et al., 2019); 3) the travel time (e.g., Zhu et al., 2018); or 4) the travel velocity (e.g., Zhu et al., 2018). Whereas link weight estimation was based on flight frequency (e.g., Hossain and Alam, 2017; Malik et al., 2019) and flight capacity (e.g., Muriel-Villegas et al., 2016; Zhu et al., 2018; Hossain and Alam, 2017). However, none of the previous studies considered the combinations of all such factors in influencing the ATIN robustness. As such, an effective risk management strategy might require the inclusion of such factors when the ATIN topological characteristics and robustness are evaluated (Wandelt et al., 2019). In addition, only a very limited number of research studies has been conducted on small-size national ATIN of less than 80 airports (Guida and Maria, 2007; Bagler, 2008), compared to their larger-size regional counterparts (Chi et al., 2003; Guimera et al., 2005; Wang et al., 2011). As network size usually influences its characteristics, there remains a need to investigate the relevant measures and the corresponding topological properties of small size ATIN (e.g., such as the specific network analyzed within the current manuscript later).

The objective of the current study is thus to address the research gap of not considering all the above key factors and their combinations in assessing ATIN robustness. In this respect, a robustness quantification methodology based on key CNT measures is developed. To demonstrate the proposed methodology, the robustness of the Canadian domestic air traffic network was assessed under random failures and targeted threats. Afterwards, the study focuses on evaluating the operating cost losses due to different disruption scenarios of the studied ATIN. Finally, key managerial insights are presented, followed by concluding remarks.

Robustness Quantification Methodology

This study aims at assessing existing and developing new methodologies for evaluation of ATIN robustness under random failures and targeted threats based on CNT measures including clustering coefficient, betweenness, connectivity, and closeness. Although other researchers adopted the notion of shortest path to account for the travel distance (Lordan et al., 2015; Wandelt and Sun, 2015; Zhu et al., 2018), the current study uses the term "*best route*" to more accurately represent the aspects that has little to do with the distance (e.g., flight capacity). The best route (Dia 2002; Jou et al. 2007; Ben-Elia et al. 2013) is thus the route that maximizes the underlying utility (e.g., least travel time, least travel distance, most flight capacity, and most travel velocity) among all available routes within the network.

The link weight has also been quantified using various approaches including flight frequency (Hossain and Alam, 2017; Zhu et al., 2018), flight capacity (Zhu et al., 2018; Muriel-Villegas et al., 2016; Wandelt and Sun, 2015), and the multiplication of flight capacity and travel velocity (Zhu et al., 2018). However, the current study adopts the approach of combining flight capacity and travel time or integrating flight capacity and travel distance to investigate the effect of considering these factors and their combinations on the ATIN robustness performance. Therefore, the following two subsections focus on the development of approaches to evaluate the shortest path and link weight, as the first step to quantify the connectivity, betweenness, closeness, and clustering coefficient.

Shortest Path

In previous studies, the best route was calculated using three distinct approaches based on the path that exhibits: 1) the minimum number of links (d_{ij}^{l}) (Eq.1) (Lordan et al., 2015; Wandelt and Sun, 2015; Barabási, 2013); 2) the minimum travel time (d_{ij}^{t}) as shown in Eq.2 (Zhu et al., 2018); and 3) the minimum travel distance (d_{ij}^{d}) as shown in Eq.3 (Wandelt and Sun, 2015). However, such three approaches typically result in three different values of the best route between the same pair of airports in the network. Thus, none of these three approaches minimizes the number of links, travel time, and distance simultaneously.

$$d_{ij}^{l} = min \sum_{l \in L} l \qquad \text{Eq. 1}$$

$$d_{ij}^{t} = min \sum_{l \in L} t_l \qquad \text{Eq. 2}$$

$$d_{ij}^{d} = min \sum_{l \in L} d_l \qquad \text{Eq. 3}$$

Where l: is the link that belongs to a set of links (L) in the network.

t_l: is the travelling time on a link (l) that belongs to a set of the total links (L) in the network.

d_l: is the travelling distance on a link (l) that belongs to a set of the total links (L) in the network.

The proposed estimation approaches for the best route, presented in Eqs. 4-6, maximize the utility of the route according to the considered parameters. More specifically, the first approach (d_{ij}^{ft}) integrates flight capacity and travel time (Eq.4) through selecting the route that yields both the minimum travel time and the maximum flight capacity. In the second approach, (d_{ij}^{fd}) is calculated based on the flight capacity and the travel distance (Eq.5) by choosing the route that concurrently combines the minimum travel distance and the maximum flight capacity. Finally, in the third approach, d_{ij}^{fv} presented in Eq. 6, aims at identifying the route with the maximum travel velocity and flight capacity among all the possible routes. The proposed three estimation approaches of the shortest path all share one common factor, namely the flight capacity. This is mainly to investigate the influence of considering flight capacity with travel time, travel distance, and travel velocity when the shortest path is evaluated. It is also worth mentioning that as real origin-destination matrix is currently designated as sensitive data, the aircraft capacity was utilized instead herein when estimating d_{ij}^{ft}, d_{ij}^{fd}, and d_{ij}^{fv}.

$$d_{ij}^{ft} = min \sum_{l \in L} \frac{t_l}{f_l \, . N_{p,f}} \qquad \text{Eq. 4}$$

$$d_{ij}^{fd} = min \sum_{l \in L} \frac{d_l}{f_l \, . N_{p,f}} \qquad \text{Eq. 5}$$

$$d_{ij}^{fv} = min \sum_{l \in L} \frac{1}{v_l . f_l \, . N_{p,f}} \qquad \text{Eq. 6}$$

where, t_l is the travelling time on a link (l), $l \in L$.

d_l is the travelling distance on a link (l), $l \in L$.

f_l is the flight frequency on a link (l), $l \in L$.

v_l is the travelling velocity on a link (l), $l \in L$.

$N_{p,f}$ is the number of the passengers in a flight that travels on a link (l), $l \in L$.

Link weight

Link weight was estimated in previous studies using three distinct approaches: 1) flight frequency (w_{ij}^{n}), as shown in Eq.7 (Hossain and Alam, 2017; Zhu et al., 2018); 2) flight frequency multiplied by the aircraft capacity (w_{ij}^{f}), as shown in Eq.8 (Muriel-Villegas et al., 2016; Wandelt and Sun, 2015); and 3) a combination of flight frequency, aircraft capacity, and travel velocity (w_{ij}^{fv}), as shown in Eq. 9 (Zhu et al., 2018). However, these previous approaches excluded the influence of travel time and distance in their estimations. Whenever travel time and/or travel distance to a certain airport increase, the airport connectivity is negatively affected and thus the weighted clustering coefficient. As such, two new approaches, w_{ij}^{ft} and w_{ij}^{fd}, are developed in the current study to address this aspect, as shown in Eqs. 10 and 11, respectively. The two approaches of the link weight include two different combinations, namely travel time with flight capacity, and travel distance with flight capacity.

$$w_{ij}^{n} = f_l \qquad \text{Eq. 7}$$

$$w_{ij}^{f} = f_l \,.\, N_{p,f} \qquad \text{Eq. 8}$$

$$w_{ij}^{fv} = f_l \,.\, N_{p,f} \,.\, v_l \qquad \text{Eq. 9}$$

$$w_{ij}^{ft} = \frac{f_l \,.\, N_{p,f}}{t_l} \qquad \text{Eq. 10}$$

$$w_{ij}^{fd} = \frac{f_l \,.\, N_{p,f}}{d_l} \qquad \text{Eq. 11}$$

Network Measures

The airport degree (k_i) (Eq.12) reflects the number of links connected to an airport (Erdös and Rényi, 1959; Watts and Strogatz, 1998; Barabási, 2013).

$$k_i = \sum_{j=1}^{N} a_{ij} \qquad \text{Eq. 12}$$

where a_{ij} represents the linkage between two neighbour airports. In other words, a_{ij}=1 if a linkage between airports i and j exists, otherwise, a_{ij}=0.

The betweenness measure of an airport is the ratio between the number of best routes that pass through this airport to the total number of best routes in the network (Freeman, 1978). Thus, the estimation approach of the best route directly influences the betweenness measure. The betweenness of airport i is $C_B(i)_s$ (Eq. 13), which can be calculated based on the different estimation approaches of the best route.

$$C_B(i)_s = \frac{n(i)_s}{M} \qquad \text{Eq. 13}$$

where, $n(i)_s$ is the number of the best routes that pass through airport i, and s refers to the utilized approach (Eqs. 1-6) in calculating the best route, as illustrated in the Appendix in Table A-1. While M is the total number of best routes in the entire network (Eq.13).

The airport closeness evaluates the extent to which one airport is close to all other airports in the network (Freeman, 1978). Similar to the betweenness, the closeness measure $C_C(i)_s$ relies also on the different estimation approaches of the best route (Eq. 14).

$$C_C(i)_s = \frac{N-1}{\sum_{i \neq j} d_{ij}^s} \qquad \text{Eq. 14}$$

where, N is the total number of airports in the network and d_{ij}^s is the best route from airport i to airport j and s refers to the utilized approach (Eqs. 1-6) used in calculating the best route, as illustrated in Table A-1 in the Appendix.

The clustering coefficient of airport i is the ratio between the number of existing links between the neighbours of this airport to the maximum possible number of these links (Wasserman et al., 1994). It can be divided into: 1) unweighted clustering coefficient $C(i)$ (Eq.15 by Hossain and Alam (2017)); and 2) weighted clustering coefficient $C(i)_{ws}$ (Eq. 16 by Barrat et al. (2004)).

$$C(i) = \frac{1}{k_i(k_i - 1)} \sum_{i \neq j \neq k} a_{ij}\, a_{jk}\, a_{ik} \qquad \text{Eq. 15}$$

where, k_i is the degree measure for airport i and a_{ij}, a_{jk}, and a_{ik} are binary variables that represent the development of linkage in the triangle made up of airport i, j, and k.

$$C(i)_{ws} = \frac{1}{C(i)_s(k_i - 1)} \sum_{i \neq j \neq k} \frac{1}{< w_i^s >} \frac{w_{ij}^s + w_{ik}^s}{2} a_{ij}\, a_{jk}\, a_{ik} \qquad \text{Eq. 16}$$

where, w_{ij}^s and w_{ik}^s are the weights of links (i-j) and (i-k), respectively, $< w_i^s >$ is the average link weight of airport i, w refers to the weighted clustering coefficient, and s refers to the utilized approach (Eqs. 7-11) used in calculating the link weight, as illustrated in Table A-1 in the Appendix.

The connectivity measure describes the reachability of an airport from its neighbouring airports (Galil et al., 1995). This measure (Eq. 17) was identified in previous studies based on the flight frequency (Hossain and Alam, 2017; Zhu et al., 2018), flight capacity (Muriel-Villegas et al., 2016; Wandelt and Sun, 2015), and travel velocity (Zhu et al., 2018).

$$C(i)_s = \sum_{n=1}^{k_i} w_{ij}^s \qquad \text{Eq. 17}$$

where, $C(i)_s$ is the connectivity measure for airport i which depends on the link weight (w_{ij}^s), and s refers to the approach (Eqs. 7-11) utilized in calculating the link weight (Eq.17), as illustrated in Table A-1 in the Appendix. It is worth mentioning that airport connectivity is essentially the same measure utilized by Barrat et al. (2004) designated as “airport strength” and by Bagler (2008) referred to as the “weighted degree”.

To assess the ATIN robustness, the study adopts the Giant Component (i.e., defined as the largest connected group of airports) method (Lordan et al., 2014; Huang et al., 2013; Zhou et al., 2012; Tanizawa et al., 2012; Gao et al., 2011; Solé et al., 2008; Beygelzimer et al., 2005; Callaway et al., 2000). In this method, the network robustness (R) is quantified as the ratio between the giant component size following the failure initiation, N_{gc}, to the total number of airports, N, as presented in Eq. 18.

$$R = \frac{N_{gc}}{N} \qquad Eq. 18$$

Application on the Canadian Domestic Air Traffic Network

In order to demonstrate the application of the proposed methodology, the current study utilizes a dataset of the Canadian Domestic Air Traffic Network (CDATN). The dataset was collected from public sources (https://www.wegotravel.ca/schedules/ca/canada-flight-schedules) during the period of September 10th to October 25th, 2018 reflecting typical airline weekly schedule within this period, as presented in Table 2.2. Within this dataset, the inclusion of airports was subject to the following criteria: 1) only airports designated for civilian passenger flights; 2) airports with regular flight schedules; and 3) airports with publicly accessible data. Therefore, the dataset excluded airports that are used solely for military and freight purposes as well as airports without regular trips or inaccessible data. In this respect, the analysis dataset is based on a total of 47 airports in Canada, as illustrated in Fig. 2.2. In addition, in Fig. 2.2, the route popularity (i.e., number of weekly flights between each two Canadian airports) is represented by the thickness of the link connecting such two airports. The total number of undirected routes (links) between the airports is 123 routes. The rationale behind adopting undirected links (i.e., the connected airports influence each other), rather than directed links (i.e., one airport influences the other connected airport), is attributed to the fact that the number of flights for *go* and *return* directions on each network link/route is usually similar (Rocha, 2017; Li et al., 2004). The capacity of flights between airports is considered in the analysis to represent the flight capacity on a specific route, as mentioned earlier. Therefore, the CDATN is analyzed as a weighted yet undirected network. Comprised of 47 airports and 123 routes, the CDATN dataset yielded 8,380 weekly domestic flights in Canada. Table 2.3 provides a sample of the data for John C. Munro Hamilton International Airport.

Table 2.2: Analytical data for the CDATN

Variables	Number of flights per route (flight)	Flight capacity (passenger/flight) *	Flight velocity (km/hr)	Travel time (minutes)	Travel distance (km)
Max	188	355	807	310	3690
Min	6	20	146	15	48
Mean	35	152	477	120	1062
Standard deviation	35	110	166	60	1347

* Flight capacity is calculated based on aircraft type with an assumed occupancy rate of 100%.

Table 2.3: Sample data for the YHM airport in Hamilton from September 10th to October 25th, 2018

From	To	Weekly flights (flight)	Travel time (minutes)	Travel distance (km)
Hamilton - YHM	Calgary – YYC	13	220	2625
	Edmonton - YEG	12	215	2690
	Winnipeg - YWG	12	140	1510
	Halifax – YHZ	10	130	1313
	Montreal - YUL	13	80	560

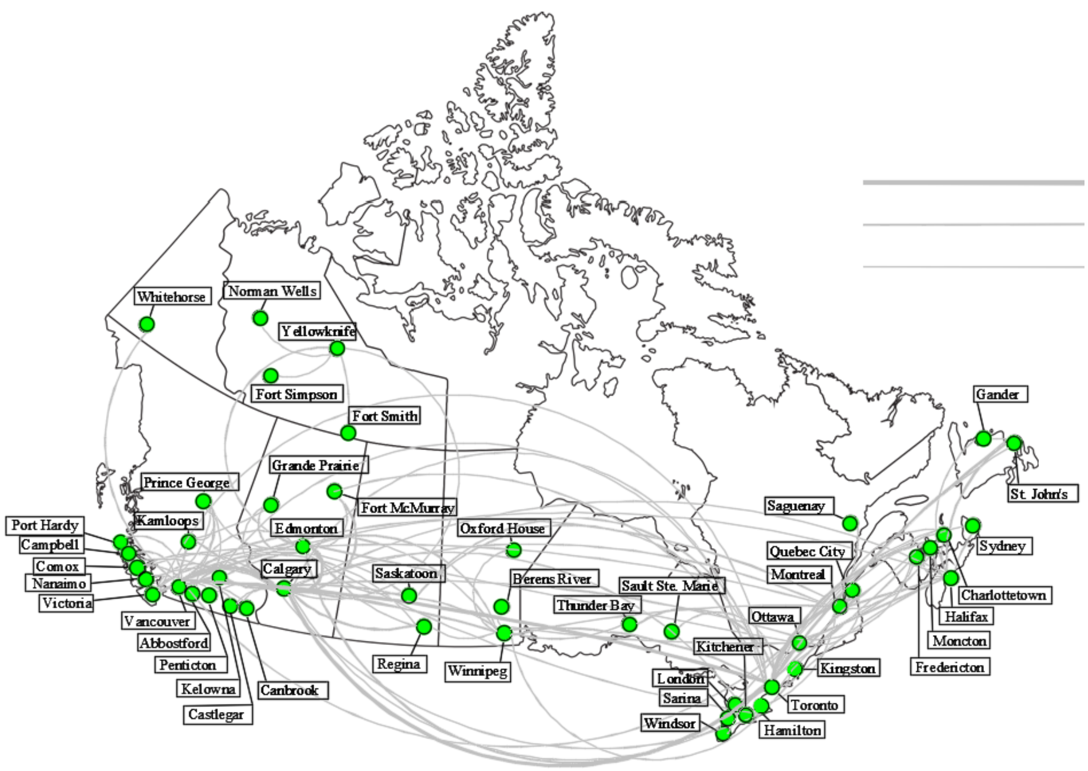

Fig. 2.2: Distribution of the Canadian cities included in the CDATN

Network Classification

The CDATN possesses several topological characteristics that can be used to identify the network type. First, the cumulative degree centrality distribution, shown in Fig. 2.3 (on a logarithmic scale), demonstrates that the CDATN follows a multi-regime power-law (Double Pareto Law) distribution (Guida and Maria, 2007) with two different exponents. One regime has an exponent γ_1 of -0.82, while the other regime has an exponent γ_2 of -2.27. The turning point, as identified by Li et al. (2004), between these two regimes occurs at a critical degree k_c= 12. As such, the discrete degree centrality distribution P (k) is derived based on the k_c value, as illustrated in Eq.19.

$$P(k) = \frac{\partial P\ (K > k)}{\partial k} \sim \begin{cases} k^{-(0.82+1)}, & for\ k\ \leq\ k_c; \\ k^{-(2.27+1)}, & for\ k\ >\ k_c, \end{cases} \qquad \text{Eq. 19}$$

From Eq. 19, the exponents of the probability distributions with the average deviations from the fitting regime, γ_1' and γ_2' are 1.81 ± 0.12 and 3.27 ± 0.12, respectively. These values are very close to the limits for scale-free networks (i.e., $2 < \gamma < 3$) (Barabási, 2013). Through evaluating the network characteristics, it can also be inferred that the CDATN has a very large degree variance $<k^2>=105$ compared to the network average degree $<k>=5.25$. In addition, it is clear that the CDATN has only three main hub airports namely: Calgary International Airport, Toronto Pearson Airport, and Vancouver International Airport; with degree centrality values equal to 25, 24, and 20, respectively. Moreover, more than 77% of the airports have degree centrality values less than 5. The CDATN's small-world property, where the average best route of the network = 2.32 < ln N = 3.85 (Watts and Strogatz, 1998), confirms also the proximity between any pair of airports in the network. Considering these topological characteristics, the CDATN can be designated as a scale-free network. Being a scale-free network indicates that the CDATN is robust (i.e., connectedness retention) under random failures but fragile against targeted threats (Barabási, 2013). Such behavior is attributed to the fact that random failures would typically remove any of the many airports with a small degree centrality value, that contributes little to the CDATN robustness. Conversely, the removal of even a small fraction of *hub* airports is sufficient to break the CDATN into a disconnected airport network.

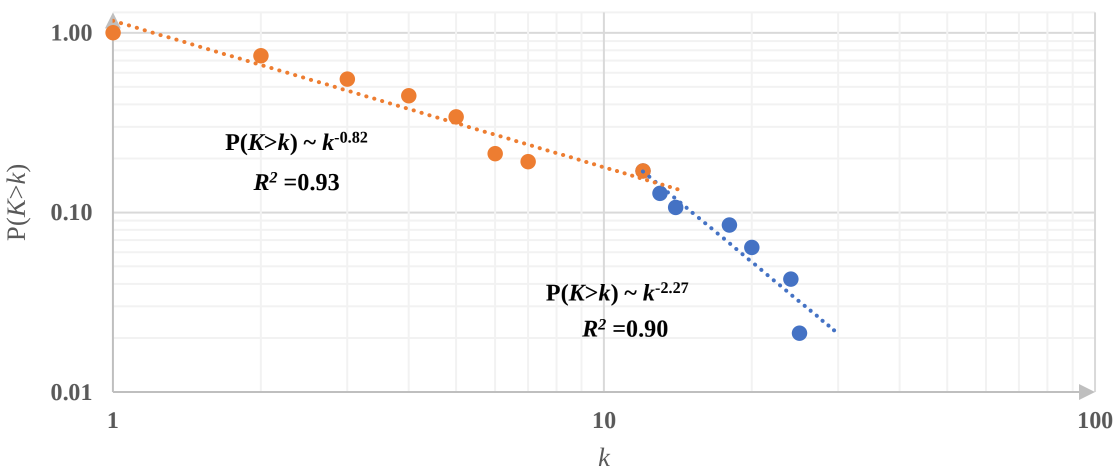

Fig. 2.3: Cumulative degree centrality distribution for the CDATN

The power-law probability distribution indicates also that the low-degree airports belong to interconnected communities (Arenas, 2010; Bagler, 2008). Therefore, the hub airports mentioned earlier have a crucial role in connecting the communities of low-degree airports. Furthermore, hub airports provide connectivity to multiple low-degree airports. This can be attributed that cities with low-administrative airports (airports that have few runways and handle smaller traffic volumes in comparison to that of the CDATN hub airports) tend to link with network hubs (Hossain and Alam, 2017; Wang et al., 2011).

Assortativity, as well, is an indicator of the network robustness and network model. Assortativity is a key measure that demonstrates the relationships among the network nodes in terms of their degree measure values. Therefore, the assortativity of the network can be detected through the correlation between the degree measure and the average degree for the neighbour nodes (knn-Avg) (Bagler, 2008; Wang et al., 2011; Hossain and Alam, 2017). It is evident that there is a negative correlation between the degree and the average degree measures in the CDATN as shown in Fig. 2.4. The negative slope of the trend line indicates that the CDATN is a dis-assortative network, where relatively high-degree cities tend to be connected to the low-degree cities. This dis-assortativity feature was also observed in other air traffic networks such as the Australian air traffic network (Hossain and Alam, 2017), the Indian air traffic network (Bagler, 2008), and the Chinese air traffic network (Wang et al., 2011; Chi et al., 2004). In general, the dis-assortativity indicates that the network is robust against random failures, but vulnerable to targeted threats (Kitsak, 2007).

Also, the cumulative betweenness probability distribution P (B > b) follows a truncated double-regime distribution. Fig. 2.4 shows the average double-regime for the six betweenness measures ($C_B(i)_l$, $C_B(i)_t$, $C_B(i)_d$, $C_B(i)_{ft}$, $C_B(i)_{fd}$, and $C_B(i)_{fv}$). The first part of that regime has an exponent of -0.32, whereas the second part of the regime has an exponent of -2.47. The exponents for all regimes in the cumulative probability distributions for the six betweenness measures are shown in Table 2.4. To compare the CDATN topology to that of a random network of the same size (same number of nodes and links), the upper regime in Fig. 2.5 shows the cumulative betweenness probability distribution for the corresponding random network with exponents of -0.51 and -2.50. It is clear that the CDATN betweenness cumulative distribution function does not follow that of a random network.

Table 2.4: Various exponents for betweenness measure according to the different betweenness measures

Measure	$C_B(i)_l$	$C_B(i)_t$	$C_B(i)_d$	$C_B(i)_{ft}$	$C_B(i)_{fd}$	$C_B(i)_{fv}$
Exponent of the first regime	-0.20	-0.21	-0.11	-0.49	-0.46	-0.47
Exponent of the second regime	-1.40	-2.17	-2.25	-2.41	-3.11	-3.49

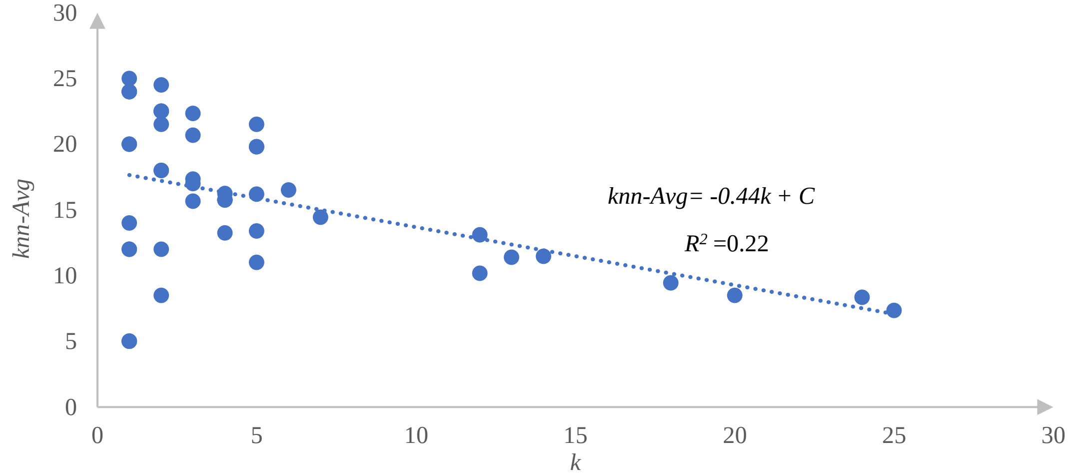

Fig. 2.4: Relationship between the degree centrality and the average degree for the neighbour airports in the CDATN

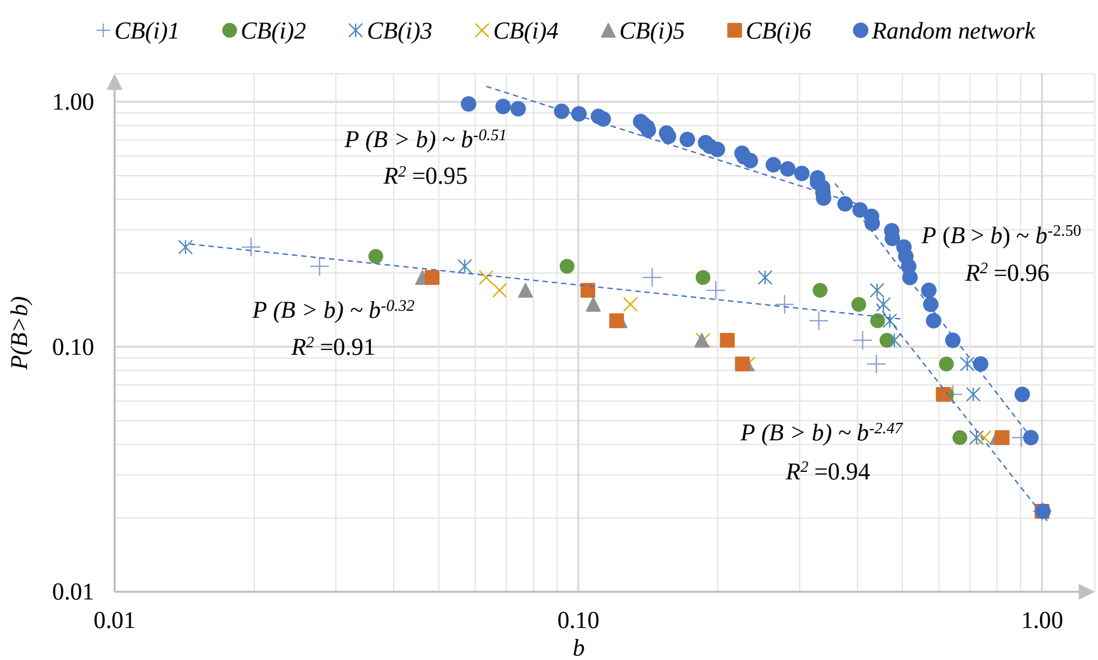

Fig. 2.5: Cumulative distribution function for betweenness measure in the CDATN

Robustness Assessment

The CDATN robustness under targeted threats is evaluated based on targeting airports with the highest attributes of clustering coefficient (Fig. 2.6), betweenness (Fig. 2.7), connectivity (Fig. 2.8) and closeness (Fig. 2.9). As can be seen in Fig. 2.6, the use of the different approaches to evaluate the clustering coefficient has almost the same influence on the corresponding robustness value. For example, in Fig. 2.6, the CDATN robustness is almost 0.6 and 0.1 corresponding to a fraction of removed airports, f, of 0.125 and 0.2, respectively, regardless of the approach used to evaluate the clustering coefficient. On the other hand, the CDATN robustness under targeted threats is sensitive to the approach used to estimate the betweenness (Fig. 2.7) and connectivity (Fig. 2.8) measures especially after eliminating 20% of the network airports (f=0.2). For instance, in Fig. 2.6, the CDATN robustness has values of 0.025 and 0.125 at f = 0.4 according to measures $C_B(i)_l$ and $C_B(i)_{ft}$, respectively, whereas in Fig. 2.9, the CDATN robustness has values of 0.1 and 0.3 at f = 0.4 according to measures $C_C(i)_{fd}$ and $C_C(i)_d$, respectively. This observation indicates that targeting airports with the highest $C_C(i)_d$ does not influence the size of the giant component regardless of the high-closeness (i.e., in terms of travel distance only) that these targeted airports have to all other airports. Targeting airports with the highest $C_C(i)_{fd}$ diminishes the CDATN robustness rapidly when the flight capacity and travel distance are considered in the closeness estimation. These discrepancies between the robustness values in Fig. 2.9 (i.e., based on the closeness) indicate how alternative best route estimation approaches significantly affect the measures used to assess network robustness.

The robustness of the CDATN was also assessed under random failures (i.e., based on 20 realizations) as shown in Figs. 2.6 to 2.8 and compared to that under targeted threats in the same figures. The figures confirm the network class assessment (i.e., the CDATN being a scale-free network) thus the network robustness under random failures, vulnerability to targeted threats. For example, as shown in Fig. 2.7, the CDATN robustness is 0.8 and 0.1, on average, at f = 0.2 (i.e., 20% of the airports are eliminated from the network) under random failures and targeted threats, respectively, based on the betweenness measure. As shown also in Figs. 2.6 to 2.8, the CDATN robustness under random failures has a density spread that increases gradually with the increase of the fraction of removed airports (f). For instance, at f = 0.2, R ranges between 0.67 to 0.82, While, at f = 0.5, R ranges between 0.21 to 0.52.

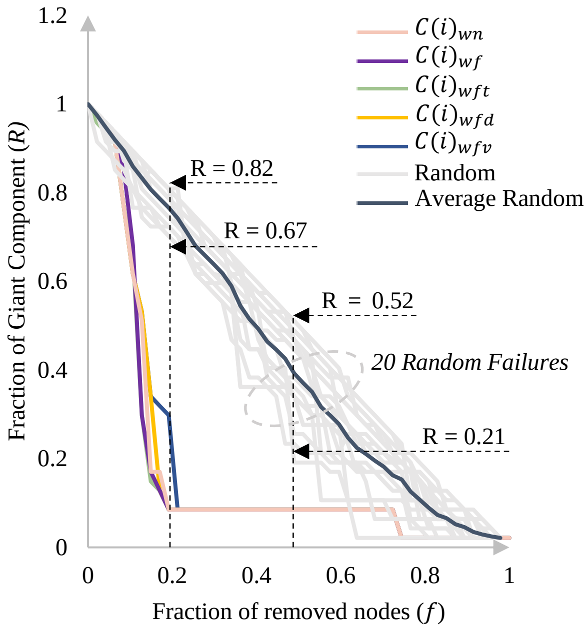

Fig. 2.6: Targeted threats according to weighted clustering coefficients and random failures

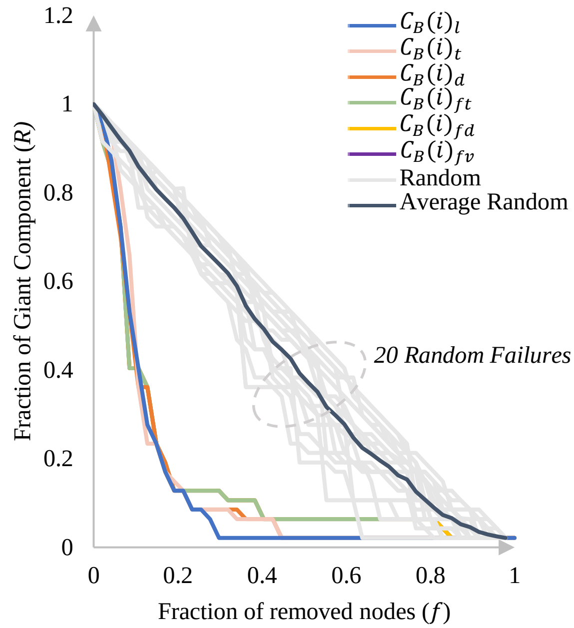

Fig. 2.7: Targeted threats according to betweenness measures and random failures

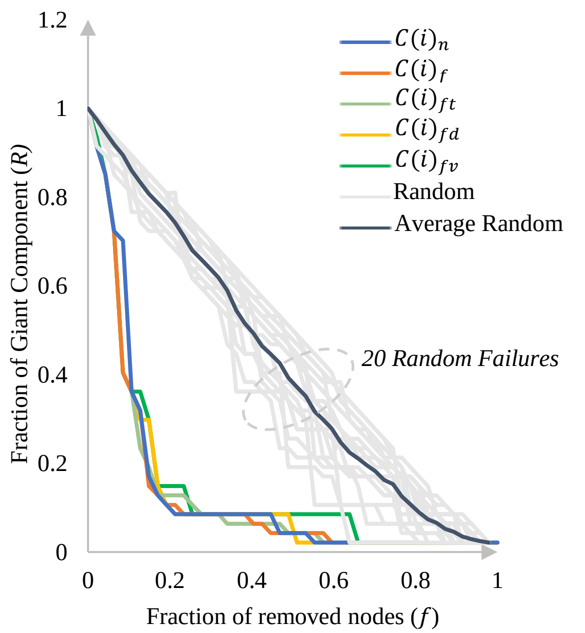

Fig. 2.8: Targeted threats according to connectivity measures and random failures

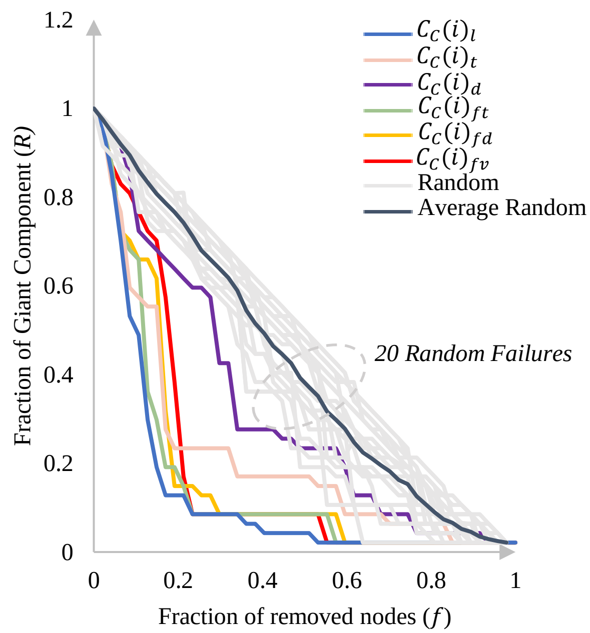

Fig. 2.9: Targeted threats according to closeness measures and random failures

Direct Operating Cost Loss Prediction

The robustness results are quantified in terms of monetary values in Figures 2.10 to 2.13 assuming a \$ 2,481 per block hour operating cost of airline according to the International Civil Aviation Organization (https://www.icao.int/Pages/default.aspx). Figures 2.10 to 2.13 show the CDATN operating cost losses (OCL) corresponding to airport removals according to the clustering coefficient, betweenness, connectivity, and closeness measures, respectively. For the first three measures, the losses increase sharply and essentially plateau at the removal of 20% of the network airports according to the different existing and developed measures. For example, at f = 0.2, the OCL are on average \$4.90, \$4.85 and \$4.85 million based on the measures of clustering coefficient (Fig. 2.10), betweenness (Fig. 2.11) and connectivity (Fig. 2.12), respectively.

However, the OCL follow different trends according to the closeness measures, as shown in Fig. 2.13. Varying from measure $C_C(i)_l$, that depends on the number of links, and $C_C(i)_d$, that depends on travel distance, shows the highest and lowest losses rate in operating costs, respectively. For example, at f = 0.2, the OCL vary between \$4.8 and \$3.0 million based on $C_C(i)_l$ and $C_C(i)_d$, respectively, as shown in Fig. 2.13. It is worth mentioning that although both measures depend on the best routes selected in their calculations, the OCL trends based on the closeness (Fig. 2.13) are different from those based on the betweenness (Fig. 2.11). This is because the estimated values of the best route are considered in the calculations of closeness measures (Eq. 14), while only the numbers of best routes are adopted in the calculations of betweenness measures (Eq. 13).

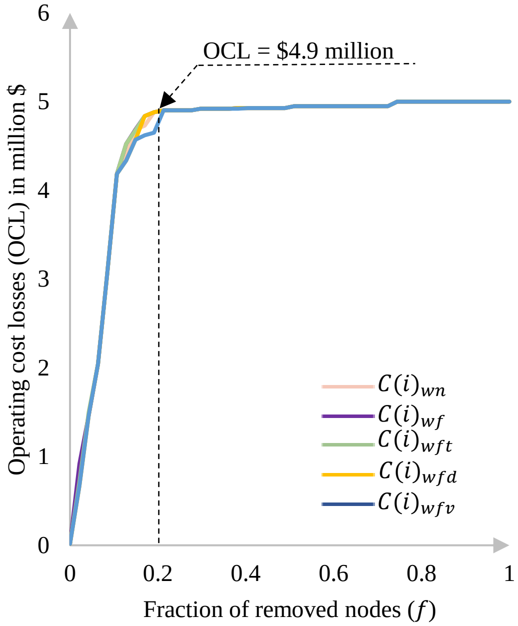

Fig. 2.10: Operating cost losses after targeted threats according to weighted clustering coefficient

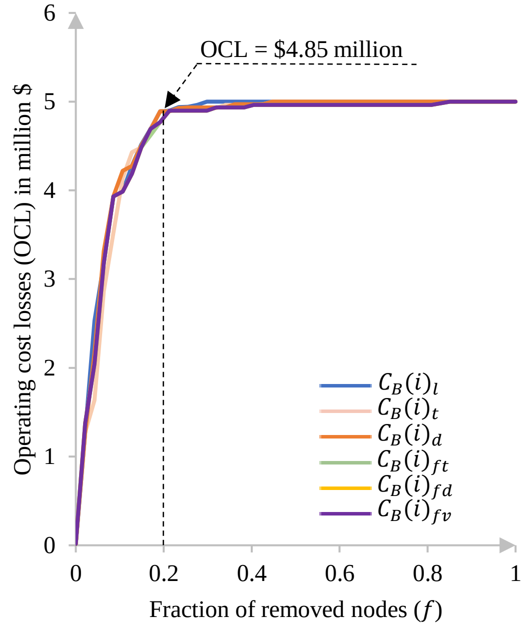

Fig. 2.11: Operating cost losses after targeted threats according to betweenness measures

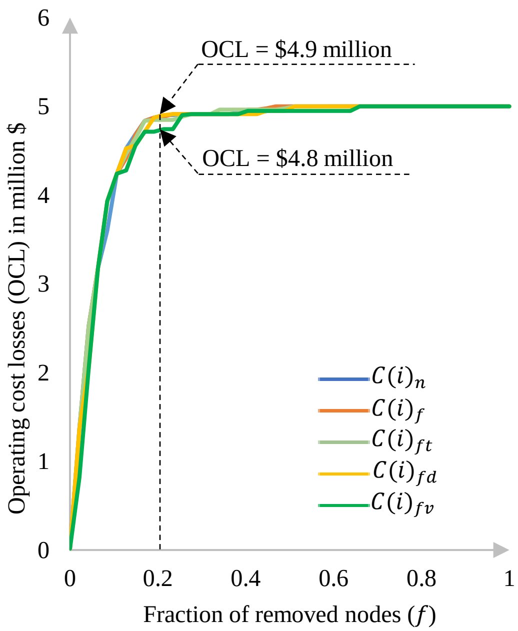

Fig. 2.12: Operating cost losses after targeted threats according to connectivity measures

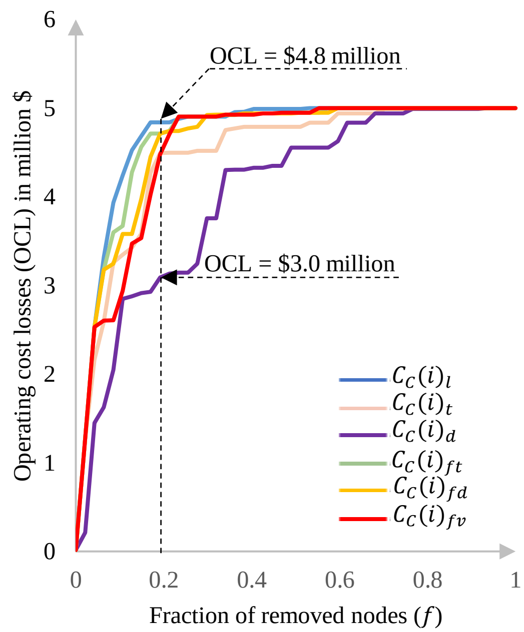

Fig. 2.13: Operating cost losses after targeted threats according to closeness measures

Managerial Insights

Investments in infrastructure resilience planning and management coupled with an in-depth understanding of the specific infrastructure network behavior under systemic risks are key for effective proactive risk mitigation strategies. Principally, the goal of resilience planning is to ensure the infrastructure's continued performance and protection from significant and non-reversible (disastrous) deterioration under disruptive events. This can be performed by defining an immediate *recovery strategy* (Fig. 2.14) that includes, for example, the rapid availability of *a sufficient* number of components within the considered infrastructure network to maintain its functionality under disruptions.

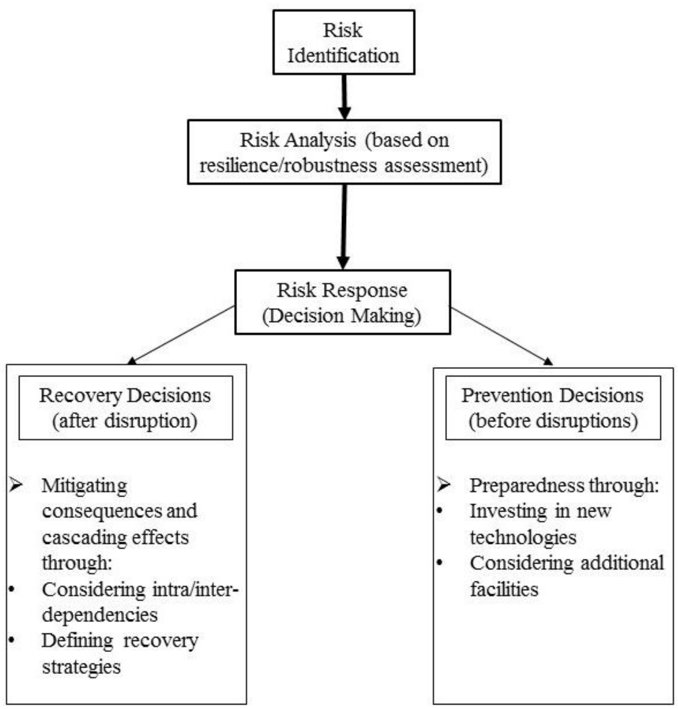

Fig. 2.14: Managerial Decision-Making process

It is also key to acknowledge that the performance of most components depends not only on their own functions but also on that of other components within the same network due to their mutual interdependence. Such interdependence needs to be also addressed during the process of setting the infrastructure network resilience-guided performance goals (e.g., robustness and rapidity) in order to mitigate systemic risks with proper means (e.g., via resourcefulness and redundancy). Infrastructure systemic risk mitigation must also consider the nature of interdependence within the same infrastructure system (that might result in an *intra*system cascading failures) or between multiple interdependent infrastructure systems (that might result in an *inter*system cascading failures). For example, within the current study focus, the loss of service within a specific airport can cause delays in the routes connected to this dysfunctional airport and subsequently can isolate other airports within the ATIN (i.e., *intra*system cascading failures) that are connected to that first-out-of-service airport. On the other hand, power network outage and subsequent depletion of auxiliary/emergency power systems can also halt the operation (i.e., *inter*system cascading failures) of an airport, and may thus affect the whole ATIN.

Investments in new technologies and more advanced tools (e.g., control towers, command posts, and radars) with high-level of reliability can be also considered for resilience-guided proactive risk management strategies (Fig. 2.14). The implementation of strategies that promote network robustness and redundancy has the potential to significantly reduce the systemic risk of OCL for ATIN stakeholders on the long term. For example, within the context of the current study, decision-makers can mitigate independence-induced risks through considering additional key facilities (Fig. 2.14) by increasing the capacities of specific existing airports/terminal or ensuring the operation of alternative (hub) airports in the event of disruption occurrence.

Based on the conducted analyses on the CDATN in the current study, the adoption of the existing and developed clustering coefficients, betweenness, and connectivity measures have almost the same effect on network robustness and the OCL. However, when the closeness measures are adopted, it was obvious that the measure $C_C(i)_l$ is the most critical measure and the measure $C_C(i)_d$ is the least critical one in estimating both, network robustness and the OCL.

Conclusions

Resilience planning and management of air transportation infrastructure networks (ATIN) aim at ensuring that external shocks do not exhibit lasting damage to the functionality of the components in this system. Robustness is one of the resilience attributes that can be assessed using various methods, including the giant component method utilized in this study. Robustness assessment and enhancement provide policymakers and infrastructure managers with upfront (proactive) defense (risk management) in the face of different forms of hazards. In this context, the current study contributes to assessing existing and developing new approaches for the evaluation of ATIN robustness and operating cost losses (OCL) under random failures and targeted threats based on key complex network theoretic measures (e.g., clustering coefficient, betweenness, connectivity, and closeness). The study adopts the notion of the *best route* to estimate the measures of betweenness and closeness. In addition, the study also adopted the flight capacity as an alternative link weight to estimate both connectivity and clustering coefficient. Finally, the Canadian Domestic Air Traffic Network (CDATN) was used as an application to demonstrate the proposed methodology.

Based on the robustness analysis, it was concluded that the CDATN is vulnerable to targeted threats and robust to random failures regardless of the underlying measure. The discrepancies between the robustness and the OCL values indicated that the different estimation approaches significantly affected the network robustness assessment, especially the closeness measures. Furthermore, the CDATN class is found to correspond to that of a scale-free network with small-world properties. Such a network class pertains to a high level of robustness against random failures but is vulnerable to targeted threats. The CDATN was also shown to possess large hubs that serve not interconnected small cities. This means that targeted threats on a hub node/city can divide the network into isolated clusters (islands) confirming the network vulnerability to targeted threats.

It is worth noting that the current study focused on only one technique of risk analysis, namely resilience-guided risk analysis. As such, comparisons with other risk analysis techniques (e.g., probability analysis, sensitivity analysis, scenario analysis, simulation analysis, correlation analysis) might result in further managerial insights. In addition, the developed methodology adopted a static undirected network, and therefore, future consideration of the temporal variation influence within ATIN, as well as its directionality might improve our understanding of the network (dynamic) behavior. Finally, as most global ATIN are connected, it is also important to evaluate how the robustness, or lack thereof, of one network can cascade (present systemic-risks) to affect other ATIN by conducting networks-of-networks type of analysis.

Overall, system-level infrastructure management is centered around optimally allocating the resources needed to enhance the system operation continuity and functionality against potential systemic risks. Towards achieving this optimal goal, the current study provides a practical tool for airspace managers and planners, supported by risk of operating cost losses, to advance the ATIN robustness assessment following effective proactive systemic risk management strategies.

CHAPTER 3: DISCUSSIONS AND CONCLUSIONS

The current study considers key factors and their combinations in assessing robustness for a specific type of civil infrastructure which is air transportation infrastructure networks (ATIN). The Canadian Domestic Air Traffic Network (CDATN) was used as an application to demonstrate the proposed methodology. The CDATN consists of 47 nodes (airports) and 123 links (routes), which accounts for 8,380 weekly domestic flights. The criteria for data collection included: 1) airports for civilian passenger flights; 2) airports with regular flight schedules; 3) and airports with accessible data.

Resilience is key to face disruptions, i.e. random failure, natural disasters, technical failures and human errors. Resilience can be assessed by measuring the "ability to prepare, absorb, recover from, and successfully adapt to adverse events" (National Academy of Sciences, 2012). Thus, resilience depends on several functions, such as shock absorption, adapting to new conditions and rapid recovery assets (Wang et al., 2018; Bruneau et al., 2003). Furthermore, it considers the mounting complexity of the networks resulting from increasing interdependencies as well as the changes in unforeseen unexpected events (Santora and Wilson, 2008; O'Rourke, 2007).

For summarization, the destructive events, along the disruption time, results in a system performance losses or "downward-trend" or, that followed by a bounce-back or "upward-trend", represented the network recovery behaviour (Santora and Wilson, 2008; Bruneau et al., 2003). This resilience curve provides a theoretically appropriate description of the several resilience functions which can be analyzed by quantitative performance attribute (O'Rourke, 2007). Worth mentioning that the less the performance loss ("downward-trend") and the rapidly the bounce back ("upward-trend") of a network after a disruptive event indicates the higher network resilience (Ganin et al., 2016). Therefore, it is not very sound to evaluate the overall network resilience with a single, aggregated network performance attribute, as it is obvious that resilience function depends on multiple phases that can be calculated by other attributes. So, a group of attributes is utilized to demonstrate the different stages/phases of resilience and different network behaviours (Ganin et al., 2016; Haimes et al., 2008; Bruneau et al., 2003). The resilience framework proposed by MCEER (2005) considers 4R attributes as resilience attributes including robustness, redundancy, resourcefulness and rapidity.

The robustness attribute clarifies the network's ability to withstand or resist disruption events within acceptable damage levels. The robustness corresponds to the concept of reliability and is similar to the elasticity threshold limit in material science (Masten et al., 1990). While the distinction between the event occurrence, including system degradation, and the lowest point of the "downward-trend" is often expressed using redundancy and resourcefulness functions (Bruneau, et al., 2003). Redundancy is the extent system components can be substituted and have the capability to satisfy functional requirements in the disruption event. In case simulating the studied system as a network including the nodes that represent the various system components and the links that represent the linkage between system components, the redundancy attribute can be calculated based on CNT clustering coefficient (in this study both, weighted and unweighted clustering coefficient can be utilized) (Jing et al., 2019; Yazdani and Jeffery, 2011). This can be applied by calculating the average clustering coefficient after the occurrence of the disastrous event. However, resourcefulness represents the ability to recognize problems, set priorities, and allocate resources in disruption cases. Recovery behaviours, in the "upward-trend" phase, are assessed using rapidity function (Haimes et al., 2008) that measures the ability to achieve performance targets in a timely manner to suppress damage impact and prevent potential disruption. Largely, and through the literature, system resilience for critical infrastructures can be calculated by different methodologies. The most utilized methodology is to calculate it depending on the 4R attributes or any other attributes utilized to determine it (Vurgin et al., 2011; Haimes et al., 2008; Bruneau et al., 2003) through calculating the arithmetic mean the attribute values (Rehak et al., 2019; Shin et al., 2018; Vurgin et al., 2011).

Largely, for an integrated risk management process in a multidisciplinary infrastructure, it is very important to diversify the capabilities of system components and enhance the dialogue between multiple disciplines. As the dialogue will result in cooperation between these different regimes and could, in turn, boost regulatory effectiveness. This should be in parallel with the efforts exerted by the authorities and the private sector to define, apply and enforce the appropriate regulations. In other words, exploiting the synergies between the public regulators and the private industries will help effectively to overcome the challenges rooted from risks and achieve the aspired goals. Therefore, awareness of risk issues among people and organizations is a prerequisite for an efficient risk management process. Therefore, educating, training, communicating, adequately articulating self-organization, and centralized risk management are all so crucial for achieving the improvement of civil infrastructure performance.

Finally, it is important to highlight some of the limitations in this study that might need to be addressed in future work. For example, the network routes can be modeled as directed links to give more flexibility to the network simulation in case outbound and inbound routs are not identical under the disruptive events. Temporal changes in the network topology can also be addressed in the further studies. A temporal network (time-varying network) is a network with links that can be active or inactive throughout different points in time. Once a link is active, its characteristics (e.g., its weight) is considered in the network simulation and will thus affect the network topology and the analysis results. Different attack probability profiles may also be considered for the network components (nodes and links) to give different perspectives of the system behaviour under different risk scenarios (e.g., sequential cyberattacks). Finally, an integration between the entire decision-making and the risk analysis processes and their interaction, although challenging, would show the extent of systemic risk and its best management strategy solutions for the infrastructure mangers and regulators (e.g., Transport Canada or the US Federal Aviation Adminstration).

In conclusion, Risk is multidimensional because several aspects affect its components: hazards, exposure, and vulnerability. Even such aspects are more diverse in a world where economic, physical, informational connections/linkages are increasing on a daily base. Therefore, tailoring up a systemic risk policy entails integrating the complex interactions of these aspects. In many fields, risk assessment approaches are supposed to go beyond traditional occurrence/consequence probabilities and contemplate environmental and social factors that affect hazard exposure/transmission. In addition to considering the effects induced by risk management policies on the linkages among the different system components to blunt the effectiveness of the adopted policies. So, it is crucial to bring together specialized knowledge in every aspect including engineering applications, sociology and economics to broaden risk issues' perspective.

REFERENCES

Al-Bahar, J. F., and K. C. Crandall. 1990. "Systematic risk management approach for construction projects." Journal of Construction Engineering and Management 116, no. 3 (1990): 533-546.

Arenas, A., J. Duch, S. Gómez, L. Danon, and A. Díaz-Guilera. 2010. "Communities in complex networks: Identification at different levels." Complex Networks (2010): 197.

Attarzadeh, M., D. K. H. Chua, and M. Beer. 2011. "Risk Management of Long Term Infrastructure Projects" PPP-BOT Projects" by Using Uncertainty, Probabilistic and Stochastic Methods, and Models." In Vulnerability, Uncertainty, and Risk: Analysis, Modeling, and Management, pp. 360-367.

Aven, T. 2011. "On some recent definitions and analysis frameworks for risk, vulnerability, and resilience." Risk Analysis: An International Journal 31, no. 4 (2011): 515-522.

Ayyub, B.M. 2014. "Risk Analysis in Engineering and Economics, 2nd ed., CRC, Boca Raton, FL.

Sustainable Measures. 2014. Available at http://www.sustainablemeasures.com/node/35 (accessed April 7, 2014).

Bagler, G. 2008. "Analysis of the airport network of India as a complex weighted network." Physica A: Statistical Mechanics and its Applications 387, no. 12 (2008): 2972-2980.

Barabási, A. 2013. "Network science." Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences371, no. 1987 (2013): 20120375.

Barrat, A., M. Barthelemy, R. Pastor-Satorras, and A. Vespignani. 2004. "The architecture of complex weighted networks." Proceedings of the national academy of sciences101, no. 11 (2004): 3747-3752.

Ben-Elia, E., R. D. Pace, G. N. Bifulco, and Y. Shiftan. 2013. "The impact of travel information's accuracy on route-choice." Transportation Research Part C: Emerging Technologies 26 (2013): 146-159.

Berche, B., C. V. Ferber, T. Holovatch, and Y. Holovatch. 2010. "Public transport networks under random failure and directed attack." arXiv preprint arXiv:1002.2300 (2010).

Berche, B., C. V. Ferber, T. Holovatch, and Y. Holovatch. 2009. "Resilience of public transport networks against attacks." The European Physical Journal B 71, no. 1 (2009): 125-137.

Beygelzimer, A., G. Grinstein, R. Linsker, and I. Rish. 2005. "Improving network robustness by edge modification." Physica A: Statistical Mechanics and its Applications 357, no. 3-4 (2005): 593-612.

Blackmore, J. M., and R. A. Plant. 2008. "Risk and resilience to enhance sustainability with application to urban water systems." Journal of Water Resources Planning and Management 134, no. 3 (2008): 224-233.

Bruneau, M., S. E. Chang, R. T. Eguchi, G. C. Lee, T. D. O'Rourke, A. M. Reinhorn, M. Shinozuka, K. Tierney, W. A. Wallace, and D. V. Winterfeldt. 2003. "A framework to quantitatively assess and enhance the seismic resilience of communities." Earthquake spectra 19, no. 4 (2003): 733-752.

Bye, Bente L. 2011. "Volcanic eruptions: Science and risk management." Science 2, no. 27.05 (2011).

Callaway, D., M. E. Newman, S. H. Strogatz, and D. J. Watts. 2000. "Network robustness and fragility: Percolation on random graphs." Physical review letters 85, no. 25 (2000): 5468.

Cardillo, A., M. Zanin, J. Gómez-Gardenes, M. Romance, A. J. García del Amo, and S. Boccaletti. 2013. "Modeling the multi-layer nature of the European Air Transport Network: Resilience and passengers re-scheduling under random failures." The European Physical Journal Special Topics 215, no. 1 (2013): 23-33.

Cardona, O.D., V. Aalst, M.K. Birkmann, J. Fordham. 2012. "Determinants of Risk: Exposure and Vulnerability. In: Managing the Risk of Extreme Events and Disasters to Advance Climate Change Adaptation".

Carpenter, A. M. 2014. "Critical Infrastructure Resilience: A Baseline Study for Georgia." In ICSI 2014: Creating Infrastructure for a Sustainable World, pp. 186-197.

Chi, L., W. Ru, S. Hang, X. Xin-Ping, Z. Jin-Song, L. Wei, and C. Xu. 2003. "Structural properties of US flight network." Chinese physics letters 20, no. 8 (2003): 1393.

Chiara, N. 2009. "Infrastructure Risk Management in Renewable Energy Projects Using Risk Flexibility Theory." In Construction Research Congress 2009: Building a Sustainable Future, pp. 1174-1183.

Choudhry, R., and K. Iqbal. 2012. "Identification of risk management system in construction industry in Pakistan." Journal of Management in Engineering 29, no. 1 (2012): 42-49.

Cimellaro, G. P., C. Fumo, A. Reinhorn, and M. Bruneau. 2008. "Seismic resilience of health care facilities." In 14th World Conference on Earthquake Engineering (14WCEE), Beijing, China, Oct, pp. 12-17. 2008.

Cox, J., L. Anthony. 2008. "Some limitations of “Risk= Threat× Vulnerability× Consequence” for risk analysis of terrorist attacks." Risk Analysis: An International Journal 28, no. 6 (2008): 1749-1761.

Dai, L., B. Derudder, and X. Liu. 2018. "The evolving structure of the Southeast Asian air transport network through the lens of complex networks, 1979–2012." Journal of Transport Geography 68 (2018): 67-77.

Del Cano, A., and M. P. de la Cruz. 2002. "Integrated methodology for project risk management." Journal of construction engineering and management 128, no. 6 (2002): 473-485.

Dia, H. 2002. "An agent-based approach to modelling driver route choice behaviour under the influence of real-time information." Transportation Research Part C: Emerging Technologies 10, no. 5-6 (2002): 331-349.

Erdös, P., and A. Rényi. 1959. "On random graphs', Math." Debrecen 6 (1959): 290-297.

Ettouney, Mohammed M., and S. Alampalli. 2016. “Risk Management in Civil Infrastructure”. CRC Press, 2016.

Ezzeldin, M., and W. E. El-Dakhakhni. 2019. "Robustness of Ontario power network under systemic risks." Sustainable and Resilient Infrastructure (2019): 1-20.

Francis, R., & B. Bekera. 2014. “A metric and frameworks for resilience analysis of engineered and infrastructure systems”. Reliability Engineering & System Safety, 121, pp. 90-103.

Freeman, L. 1978. "Centrality in social networks conceptual clarification." Social networks 1, no. 3 (1978): 215-239.

Galil, Z., and X. Yu. 1995. "Short length versions of Menger's theorem." In Annual ACM Symposium on Theory of Computing: Proceedings of the twenty-seventh annual ACM symposium on Theory of computing, vol. 29, pp. 499-508.

Ganin, A. A., E. Massaro, A. Gutfraind, N. Steen, J. M. Keisler, A. Kott, R. Mangoubi, and I. Linkov. 2016. "Operational resilience: concepts, design and analysis." Scientific reports 6 (2016): 19540.

Gao, J., S. V. Buldyrev, S. Havlin, and H. E. Stanley. 2011. "Robustness of a network of networks." Physical Review Letters 107, no. 19 (2011): 195701.

Grubesic, Tony H., and A. T. Murray. 2010. "Spatial–historical landscapes of telecommunication network survivability." Telecommunications Policy29, no. 11 (2005): 801-820. DOI: 10.1016/j.telpol.2005.06.011.

Guida, M., and F. Maria. 2007. "Topology of the Italian airport network: A scale-free small-world network with a fractal structure?." Chaos, Solitons & Fractals 31, no. 3 (2007): 527-536.

Guimera, R., S. Mossa, A. Turtschi, and L. N. Amaral. 2005. "The worldwide air transportation network: Anomalous centrality, community structure, and cities' global roles." Proceedings of the National Academy of Sciences102, no. 22 (2005): 7794-7799.

Gutteling, J., and O. Wiegman. 1996.” Exploring Risk Communications, Kluwer Academic, Dordrecht, The Netherlands. Halpin, D.W.

Haimes, Y. Y., Crowther, K., & Horowitz, B. M. 2008. Homeland security preparedness: Balancing protection with resilience in emergent systems. Systems Engineering, 11(4), pp. 287-308.

Hamel, G., and L. Valikangas. 2003. "The quest for resilience." Revista Icade. Revista de las Facultades de Derecho y Ciencias Económicas y Empresariales 62 (2004): 355-358.

Helbing, D. 2013. "Globally networked risks and how to respond." Nature 497, no. 7447 (2013): 51-59.

Holling, C. S. 1973. "Resilience and stability of ecological systems." Annual review of ecology and systematics 4, no. 1 (1973): 1-23.

Hornby, A. S., A. P. Cowie, and A. C. Gimson. 1974. “Oxford advanced learner's dictionary of current English.” Vol. 1428. Oxford: Oxford university press, 1974.

Hossain, M. M., and S. Alam. 2017. "A complex network approach towards modeling and analysis of the Australian Airport Network." Journal of Air Transport Management 60 (2017): 1-9.

Hu, Y., Q. Wu, and D. Zhu. 2008. "Topological patterns of spatial urban street networks." In 2008 4th International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1-4. IEEE, 2008.

Huang, X., S. Shao, H. Wang, S. V. Buldyrev, H. E. Stanley, and S. Havlin. 2013. "The robustness of interdependent clustered networks." EPL (Europhysics Letters)101, no. 1 (2013): 18002.

Hubbard, D. W. 2009. “The failure of risk management: Why it's broken and how to fix it.” John Wiley & Sons.

Jing, W., X. Xu, and Y. Pu. 2019. "Route Redundancy-Based Network Topology Measure of Metro Networks." Journal of Advanced Transportation 2019 (2019).

Jou, R., D. A. Hensher, and K. Chen. 2007. "Route choice behaviour of freeway travellers under real-time traffic information provision–Application of the best route and the habitual route choice mechanisms." Transportation Planning and Technology 30, no. 6 (2007): 545-570.

Julliard, R., P. J. Yun, and R. Rado. 2015. "Robustness of transportation networks: The case of Madagascar’s road network." International Journal of Advancements in Research & Technology 4, no. 5 (2015): 1-4.

Kammouh, O., G. Dervishaj, and G. P. Cimellaro. 2017. "Quantitative framework to assess resilience and risk at the country level." ASCE-ASME Journal of risk and uncertainty in engineering systems, part A: civil engineering 4, no. 1 (2017): 04017033.

Kitsak, M., S. Havlin, G. Paul, M. Riccaboni, F. Pammolli, and H. E. Stanley. 2007. "Betweenness centrality of fractal and nonfractal scale-free model networks and tests on real networks." Physical Review E 75, no. 5 (2007): 056115.

Lee, N., and J. E. Schaufelberger. 2013. "Risk management strategies for privatized infrastructure projects: Study of the build–operate–transfer approach in east Asia and the Pacific." Journal of management in engineering 30, no. 3 (2013): 05014001.

Li, W., and X. Cai. 2004. "Statistical analysis of airport network of China." Physical Review E 69, no. 4 (2004): 046106.

Lordan, O., J. M. Sallan, N. Escorihuela, and D. Gonzalez-Prieto. 2016. "Robustness of airline route networks." Physica A: Statistical Mechanics and its Applications 445 (2016): 18-26.

Lordan, O., J. M. Sallan, and P. Simo. 2015. "Study of the topology and robustness of airline route networks from the complex network approach: a survey and research agenda." Journal of Transport Geography 37 (2015): 112-120.

Lordan, O., J. M. Sallan, P. Simo, and D. Gonzalez-Prieto. 2014. "Robustness of the air transport network." Transportation Research Part E: Logistics and Transportation Review 68 (2014): 155-163.

Lounis, Z., and T. P. McAllister. 2016. "Risk-based decision making for sustainable and resilient infrastructure systems." Journal of Structural Engineering 142, no. 9 (2016): F4016005.

Lundin, T. 1995. "Transportation disasters: A review." Journal of traumatic stress.

Malik, H. A. M., N. Mahmood, M. H. Usman, K. Rziwan, and F. Abid. 2019. "Analysis of Airport Network in Pakistan Utilizing Complex Network Approach." network 10, no. 1 (2019)

Mansouri, M., R. Nilchiani, and A. Mostashari. 2009. "A risk management-based decision analysis framework for resilience in maritime infrastructure and transportation systems." In 2009 3rd Annual IEEE Systems Conference, pp. 35-41. IEEE, 2009.

Manyena, S. B. 2006. "The concept of resilience revisited." Disasters 30, no. 4 (2006): 434-450.

Marzuoli, A., E. Feron, and E. Boidot. 2014. "Resilience of the national airspace system structure: A data-driven network approach." In 2014 IEEE/AIAA 33rd Digital Avionics Systems Conference (DASC), pp. 1D2-1. IEEE, 2014.

Muriel-Villegas, J. E., K. C. Alvarez-Uribe, C. E. Patiño-Rodríguez, and J. G. Villegas. 2016. "Analysis of transportation networks subject to natural hazards–Insights from a Colombian case." Reliability Engineering & System Safety 152 (2016): 151-165.

Masten, A. S., Karin M. Best, and N. Garmezy. 1990. "Resilience and development: Contributions from the study of children who overcome adversity." Development and psychopathology 2, no. 4 (1990): 425-444.

Newman, M. E. J. 2010. "Networks: an introduction. Oxford; New York: Oxford University Press", 2010.

OECD, I. 2003. "Emerging risks in the 21st century: an agenda for action." (2003): 290.

O'Rourke, T. D. 2007. "Critical infrastructure, interdependencies, and resilience." BRIDGE-Washington-National Academy of Engineering- 37, no. 1 (2007): 22.

Padgett, J. E., and C. Tapia. 2013. "Sustainability of natural hazard risk mitigation: Life cycle analysis of environmental indicators for bridge infrastructure." Journal of Infrastructure Systems 19, no. 4 (2013): 395-408.

Paleari, S., R. Redondi, and P. Malighetti. 2010. "A comparative study of airport connectivity in China, Europe and US: which network provides the best service to passengers?." Transportation Research Part E: Logistics and Transportation Review 46, no. 2 (2010): 198-210.

Pien, K., K. Han, W. Shang, A. Majumdar, and W. Ochieng. 2015. "Robustness analysis of the European air traffic network." Transportmetrica A: Transport Science11, no. 9 (2015): 772-792.

Pipattanapiwong, J. 2004. "Development of multi-party risk and uncertainty management process for an infrastructure project." (2004).

Rausand, M. 2004. "System Reliability Theory: Models, Statistical Methods, and Applications", John Wiley &

Sons, Hoboken, NJ.

Ren, G., C. Lu, J. Zhu, and X.i Liu. 2019. "Analyzing the topological characteristic and key nodes of Chinese air sector network." International Journal of Modern Physics B (2019): 1950100.

Renfroe, N. A., and J. L. Smith. 2010. "Threat/vulnerability assessments and risk analysis." Applied Research Associates, Inc (2010).

Rehak, D., P.l Senovsky, M. Hromada, and T. Lovecek. 2019. "Complex approach to assessing resilience of critical infrastructure elements." International Journal of Critical Infrastructure Protection 25 (2019): 125-138.

Rocha, L. E. 2017. "Dynamics of air transport networks: A review from a complex systems perspective." Chinese Journal of Aeronautics 30, no. 2 (2017): 469-478.

Santora, M., and R. Wilson. 2008. "Resilient and sustainable water infrastructure." Journal-American Water Works Association 100, no. 12 (2008): 40-42.

Schatteman, D., W. Herroelen, S.V. de Vonder, and A. Boone. 2008. "Methodology for integrated risk management and proactive scheduling of construction projects." Journal of construction engineering and management 134, no. 11 (2008): 885-893.

Shin, S., S. Lee, D. R. Judi, M. Parvania, E. Goharian, T. McPherson, and S. J. Burian. 2018. "A systematic review of quantitative resilience measures for water infrastructure systems." Water 10, no. 2 (2018): 164.

Solé, R. V., M. Rosas-Casals, B. Corominas-Murtra, and S. Valverde. 2008. "Robustness of the European power grids under intentional attack." Physical Review E 77, no. 2 (2008): 026102.

Sun, X., V. Gollnick, and S. Wandelt. 2017. "Robustness analysis metrics for worldwide airport network: A comprehensive study." Chinese Journal of Aeronautics 30, no. 2 (2017): 500-512.

Sánchez-Silva, M. 2018. "Managing Infrastructure Systems through Changeability." Journal of Infrastructure Systems 25, no. 1 (2018): 04018040.

Tang, W., M. Qiang, C. F. Duffield, D. M. Young, and Y. Lu. 2007. "Risk management in the Chinese construction industry." Journal of construction engineering and management 133, no. 12 (2007): 944-956.

Tanizawa, T., S. Havlin, and H. E. Stanley. 2012. "Robustness of onionlike correlated networks against targeted attacks." Physical Review E 85, no. 4 (2012): 046109.

Taylor, C., and E. Vanmarcke. 2006. “Infrastructure risk management processes: Natural, accidental, and deliberate hazards.” Vol. 1. ASCE Publications.

Tian, Zhao, L. Jia, H. Dong, F. Su, and Z. Zhang. 2016. "Analysis of urban road traffic network based on complex network." Procedia engineering 137 (2016): 537-546.

Tsiotas, D., and S. Polyzos. 2017. "The topology of urban road networks and its role to urban mobility." Transportation research procedia24 (2017): 482-490. DOI: 10.1016/j.tre.2014.08.005.

Vugrin, E. D., D. E. Warren, M. A. Ehlen, and R. C. Camphouse. 2010. "A framework for assessing the resilience of infrastructure and economic systems." In Sustainable and resilient critical infrastructure systems, pp. 77-116. Springer, Berlin, Heidelberg, 2010.

Vugrin, E. D., D. E. Warren, and M. A. Ehlen. 2011. "A resilience assessment framework for infrastructure and economic systems: Quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane." Process Safety Progress 30, no. 3 (2011): 280-290.

Wandelt, S., and X. Sun. 2015. "Evolution of the international air transportation country network from 2002 to 2013." Transportation Research Part E: Logistics and Transportation Review 82 (2015): 55-78.

Wandelt, S., X. Sun, and X. Cao. 2015. "Computationally efficient attack design for robustness analysis of air transportation networks." Transportmetrica A: Transport Science 11, no. 10 (2015): 939-966.

Wandelt, S., X. Sun, and J. Zhang. 2019. "Evolution of domestic airport networks: a review and comparative analysis." Transportmetrica B: Transport Dynamics 7, no. 1 (2019): 1-17.

Wang, H., J. Huang, X. Xu, and Y. Xiao. 2014. "Damage attack on complex networks." Physica A: Statistical Mechanics and its Applications 408 (2014): 134-148.

Wang, J., H. Mo, F. Wang, and F. Jin. 2011. "Exploring the network structure and nodal centrality of China’s air transport network: A complex network approach." Journal of Transport Geography 19, no. 4 (2011): 712-721.

Wang, J., R. Dou, R. R. Muddada, and W. Zhang. 2018. "Management of a holistic supply chain network for proactive resilience: Theory and case study." Computers & Industrial Engineering 125 (2018): 668-677.

Wang, T., W. Tang, L. Du, C. F. Duffield, and Y. Wei. 2016. "Relationships among risk management, partnering, and contractor capability in international EPC project delivery." Journal of management in engineering 32, no. 6 (2016): 04016017.

Wasserman, S., and K. Faust. 1994. “Social network analysis: Methods and applications.” Vol. 8. Cambridge university press, 1994.

Watts, D. J., and S. H. Strogatz. 1998. "Collective dynamics of ‘small-world’networks." nature 393, no. 6684 (1998): 440.

Wei, D., and K. Ji. 2010. "Resilient industrial control system (RICS): Concepts, formulation, metrics, and insights." In 2010 3rd International symposium on resilient control systems, pp. 15-22. IEEE, 2010.

West, C., S. Kenway, M. Hassall, and Z. Yuan. 2018. "Integrated Project Risk Management for Residential Recycled-Water Schemes in Australia." Journal of Management in Engineering 35, no. 2 (2018): 04018063.

Wuellner, D. R., S. Roy, and R. M. D’Souza. 2010. "Resilience and rewiring of the passenger airline networks in the United States." Physical Review E 82, no. 5 (2010): 056101.

Yazdani, A., and P. Jeffrey. 2011. "Applying network theory to quantify the redundancy and structural robustness of water distribution systems." Journal of Water Resources Planning and Management 138, no. 2 (2011): 153-161.

Zhang, J., X. Cao, W. Du, and K. Cai. 2010. "Evolution of Chinese airport network." Physica A: Statistical Mechanics and its Applications 389, no. 18 (2010): 3922-3931. DOI: 10.1016/j.physa.2010.05.042.

Zhang, M., B. Liang, S. Wang, M. Perc, W.o Du, and X. Cao. 2018. "Analysis of flight conflicts in the Chinese air route network." Chaos, Solitons & Fractals 112 (2018): 97-102.

Zhou, D., H. E. Stanley, G. D'Agostino, and A. Scala. 2012. "Assortativity decreases the robustness of interdependent networks." Physical Review E 86, no. 6 (2012): 066103.

Zhou, Y., J. Wang, and G. Q. Huang. 2019. "Efficiency and robustness of weighted air transport networks." Transportation Research Part E: Logistics and Transportation Review 122 (2019): 14-26.

Zhu, Z., A. Zhang, and Y. Zhang. 2018. "Connectivity of intercity passenger transportation in China: A multi-modal and network approach." Journal of Transport Geography 71 (2018): 263-276.

Zou, P., Y. Chen, and T. Chan. 2009. "Understanding and improving your risk management capability: Assessment model for construction organizations." Journal of Construction Engineering and Management 136, no. 8 (2009): 854-863.

APPENDIX

Table A-1: The formula for the different measures in the CDATN

Measure	*Formula*	*Measure*	*Formula*
$\boldsymbol{C_B(i)_l}$	$\frac{n(i)_l}{M}$	$C_C(i)_{fv}$	$\frac{N-1}{\sum_{i\neq j} d_{ij}^{fv}}$
$\boldsymbol{C_B(i)_t}$	$\frac{n(i)_t}{M}$	$C(i)_{wn}$	$\frac{1}{k_i(k_i-1)}\sum_{i\neq j\neq k}\frac{1}{< w_i^n >}\frac{w_{ij}^n+w_{ik}^n}{2}a_{ij}\,a_{jk}\,a_{ik}$
$\boldsymbol{C_B(i)_d}$	$\frac{n(i)_d}{M}$	$\boldsymbol{C(i)_{wf}}$	$\frac{1}{k_i(k_i-1)}\sum_{i\neq j\neq k}\frac{1}{< w_i^f >}\frac{w_{ij}^f+w_{ik}^f}{2}a_{ij}\,a_{jk}\,a_{ik}$
$\boldsymbol{C_B(i)_{ft}}$	$\frac{n(i)_{ft}}{M}$	$\boldsymbol{C(i)_{wft}}$	$\frac{1}{k_i(k_i-1)}\sum_{i\neq j\neq k}\frac{1}{< w_i^{ft} >}\frac{w_{ij}^{ft}+w_{ik}^{ft}}{2}a_{ij}\,a_{jk}\,a_{ik}$
$\boldsymbol{C_B(i)_{fd}}$	$\frac{n(i)_{fd}}{M}$	$\boldsymbol{C(i)_{wfd}}$	$\frac{1}{k_i(k_i-1)}\sum_{i\neq j\neq k}\frac{1}{< w_i^{fd} >}\frac{w_{ij}^{fd}+w_{ik}^{fd}}{2}a_{ij}\,a_{jk}\,a_{ik}$
$\boldsymbol{C_B(i)_{fv}}$	$\frac{n(i)_{fv}}{M}$	$\boldsymbol{C(i)_{wfv}}$	$\frac{1}{k_i(k_i-1)}\sum_{i\neq j\neq k}\frac{1}{< w_i^{fv} >}\frac{w_{ij}^{fv}+w_{ik}^{fv}}{2}a_{ij}\,a_{jk}\,a_{ik}$
$\boldsymbol{C_C(i)_l}$	$\frac{N-1}{\sum_{i\neq j} d_{ij}^{l}}$	$\boldsymbol{C(i)_n}$	$\sum_{n=1}^{k_i} w_{ij}^n$
$\boldsymbol{C_C(i)_t}$	$\frac{N-1}{\sum_{i\neq j} d_{ij}^{t}}$	$\boldsymbol{C(i)_f}$	$\sum_{n=1}^{k_i} w_{ij}^f$
$\boldsymbol{C_C(i)_d}$	$\frac{N-1}{\sum_{i\neq j} d_{ij}^{d}}$	$\boldsymbol{C(i)_{ft}}$	$\sum_{n=1}^{k_i} w_{ij}^{ft}$
$\boldsymbol{C_C(i)_{ft}}$	$\frac{N-1}{\sum_{i\neq j} d_{ij}^{ft}}$	$\boldsymbol{C(i)_{fd}}$	$\sum_{n=1}^{k_i} w_{ij}^{fd}$
$\boldsymbol{C_C(i)_{fd}}$	$\frac{N-1}{\sum_{i\neq j} d_{ij}^{fd}}$	$\boldsymbol{C(i)_{fv}}$	$\sum_{n=1}^{k_i} w_{ij}^{fv}$