Robustness analysis metrics for worldwide airport network: A comprehensive study

SUN Xiaoqian\textsuperscript{a,b,c}, Volker GOLLNICK\textsuperscript{d}, Sebastian WANDELT\textsuperscript{a,b,c,*}

\textsuperscript{a}School of Electronic and Information Engineering, Beihang University, 100191 Beijing, China
\textsuperscript{b}Beijing Key Laboratory for Network-based Cooperative ATM, Beijing 100191, China
\textsuperscript{c}Beijing Laboratory for General Aviation Technology, Beijing 100191, China
\textsuperscript{d}Institute of Air Transportation Systems, German Aerospace Center, Blohmstrasse 18, 21079 Hamburg, Germany

Received 14 June 2016; revised 9 September 2016; accepted 24 November 2016

Abstract

Robustness of transportation networks is one of the major challenges of the 21st century. This paper investigates the resilience of global air transportation from a complex network point of view, with focus on attacking strategies in the airport network, i.e., to remove airports from the system and see what could affect the air traffic system from a passenger’s perspective. Specifically, we identify commonalities and differences between several robustness measures and attacking strategies, proposing a novel notion of functional robustness: unaffected passengers with rerouting. We apply twelve attacking strategies to the worldwide airport network with three weights, and evaluate three robustness measures. We find that degree and Bonacich based attacks harm passenger weighted network most. Our evaluation is geared toward a unified view on air transportation network attack and serves as a foundation on how to develop effective mitigation strategies.

Keywords: Airport network; robustness measure; attacking strategy; air transportation systems; resilience
1 Introduction

Air transportation is one critical network infrastructure for a nation and it is becoming extremely important for public policy considerations. Disruptions of air transportation systems, either due to extreme weather conditions or terrorist attacks, can lead to huge economic losses. The eruption of Eyjafjallajökull volcano in 2010 caused airline losses of approximately 1.7 billion US dollars and more than 10 million passengers were affected. An overnight snowstorm on March 12, 2013 disrupted the transport across northwestern Europe; in particular, Frankfurt airport was closed and airlines canceled about 700 flights. In order to avoid such high socio-economic costs, it is extremely critical to assess the robustness of air transportation systems against natural or intentional disruptions.

Complex network theory provides powerful tools to understand the structures and dynamics of air transportation systems. Airport networks have often been analyzed, where nodes are airports and links exist between two airports if there are flight connections. Several research focused on how delay is propagated in airport networks. Based on fuzzy soft sets, evaluated the airport importance and network efficiency with US and China’s airport networks as case studies, and the vulnerability of these two networks was also compared. showed that the vast majority of all Intra-European passengers travel direct and the directness of the overall system increased from 2002 to 2012. studied the robustness of US airport network, using attacking strategies based on betweenness, closeness, hyperlink-induced topic search (HITS), and degree, with giant component as robustness measure. studied the resilience of European air transport network against random flight failures, based on a multiplex network formalism, where the set of flights for each airline is considered as an interdependent network. Robustness of Australian network, based on degree, betweenness, strength, and random attacks, with giant component and network reachability robustness measures was investigated. The worldwide airport network was studied under random attacks as well as degree and betweenness-based attacks with the shortest average path length and giant component as robustness measures.

In air transportation networks, random failures correspond to the closure of an airport (node failure) or the cancellation of a flight (link failure) randomly, while targeted attacks correspond to the closure of an airport or the cancellation of a flight based on certain criteria. For instance, Beijing Capital International Airport (PEK) has the largest number of passengers (77531486) in 2013 in the whole world (Data source: http://www.airdi.net). Such hub nodes are critical for the structure of air transportation and they are inherently priorities for targeted attacks. One might think that airline routes are impermanent and links come and go all the time, and therefore robustness analysis is less important for this type of network than for other types of network with a more static structure, e.g., electricity or road networks. However, it is a long process to establish a new route for an airline. Before setting up a new route, the airline network planning department needs to spend considerable amount of time to analyze the profitability of the new route. Several factors need to be considered, for instance, market demand forecasting, competitor analysis, aircraft capacity planning, and passenger spill model. Ultimately, the reason for studying the resilience of the system resides in the time frame associated with an attack to an airport. It is true that, if a route is closed (for instance because of adverse weather), alternative solutions can be found fast. Nevertheless, an attack to an airport may have long-term important consequences as in the recent case of 2016 Brussels bombings. It is thus important to prevent such attacks. In this research, we perform a systematic robustness analysis for the worldwide airport network against random failures and targeted attacks, with focus on several attacking strategies and robustness measures.

Several research on the robustness of the worldwide airport network has been conducted in the past years. presented a methodology for the detection of critical airports in the worldwide airport network, and the network robustness was measured by the size of giant component. The airports are isolated based on several node selection criteria, and especially a novel criterion, Bonacich power centrality, has been tested. introduced the flight route addition/deletion problem and compared three different methods to optimize the robustness of the airport network, with algebraic connectivity as the robustness measure; the Virgin America network was used as a case study with the link failure probability as weight. Wang et al. compared the behavior of two real networks and two synthetic networks under degree based attacks using the size of giant component. proposed to reroute a series of flights within certain distances of original destination airports in order to improve the robustness of the worldwide airport network under degree targeted attacks, where robustness is measured by an estimation of the number of stranded passengers in the giant component. analyzed the resilience of the worldwide airport network and revealed that it is a redundant and resilient network for long distance air travel, otherwise it breaks down completely due to removal of short insignificant connections. Woolley-Meza et al. investigated the eruption of Eyjafjallå-
jökull volcano, September 11th terrorist attacks, and geographical disruptions in the worldwide airport network; effective distance was used to quantify the impact of disasters on the network. Wuellner et al. analyzed the individual structures of seven US largest passenger airline networks and examined the networks' resilience to random/degree/betweenness targeted node deletion. Lordan et al. also analyzed the robustness of three major airline/alliances route networks. Wei et al. also studied the optimization of the robustness of the airport network, with algebraic connectivity as the robustness measure. The effective distance is based on the idea that a small fraction of traffic is effectively equivalent to a large distance, and vice versa. The size of giant component and travel cost in the giant component were used to quantify the network performance under various deletion processes. Moreover, the design of a robust hub network has also been studied. Kotegawa et al. measured the robustness of airline service route network topology under random and targeted disruptions.

Closely related works are summarized in terms of robustness measures, attacking strategies, and network weights in Table 1.

Table 1: Summary of related works and proposed approach on robustness of worldwide airport network

<table>
<thead>
<tr>
<th>Reference</th>
<th>Robustness measure</th>
<th>Attacking strategy</th>
<th>Network weight</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Size of giant component</td>
<td>Degree targeted attack</td>
<td>Unweighted</td>
</tr>
<tr>
<td></td>
<td>Algebraic connectivity</td>
<td>Betweenness targeted attack</td>
<td>Geographical distance</td>
</tr>
<tr>
<td></td>
<td>Survived links</td>
<td>Closeness targeted attack</td>
<td>Number of passengers</td>
</tr>
<tr>
<td></td>
<td>Unaffected passengers with rerouting</td>
<td>Eigenvector targeted attack</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bonacich targeted attack</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Damage targeted attack</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Our work</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In this research, which was motivated by the work of Ref., we extract data from the Sabre
Airport Data Intelligence (ADI) (http://www.airdi.net) to build the worldwide airport network, and an excerpt is shown in Figure Error! Reference source not found.. Each node is one airport, and the size of a node is proportional to its degree, which is weighted by the number of passengers. In this figure, we only show the links which have more than 100000 passengers travelling per year. Note that spherical links are not always drawn as the shortest connection, but go through the center of the projected map. We consider the network as directed and weighted; two different weights are used for this study: geographical distances and the number of passengers travelling between two airports. Given a consistent view on the worldwide airport network, the goal of this research is to make clear, through comparison, which attacking strategy harms the network most and which robustness measure is more appropriate for the network under disruptions.

We are interested in the robustness of air transportation systems under disruption from the function point of view, i.e., transferring passengers from their origins to destinations. We use unaffected passengers with rerouting as a baseline measure from the passenger stakeholder’s perspective: if an airport is closed due to convective weather or intentional human disruptions, how many passengers can still make their journeys? We compare our baseline metric to three other robustness measures: the size of giant component, algebraic connectivity, and survived links. Formal definitions of these robustness measures can be found in Section 2.3.

In our research, we only consider the robustness of the worldwide airport network as single mode transportation, i.e., passengers are not allowed to take any alternative transportation means, such as buses or trains. We think that it is necessary to understand this single mode case first. Another important reason for this hypothesis is that working with the world network, alternative transportation means are not usually available. For instance, if a passenger has to go from Europe to China and the flight is canceled, a bus is not really an option in this case. Previous research on the robustness of airport networks mainly focused on topological robustness measures, for instance, the size of giant component and algebraic connectivity. Furthermore, a multitude of attacking strategies were proposed based on different network metrics. Given a consistent view on the worldwide airport network (related work techniques were evaluated on largely different datasets), our research aims at presenting an overview of the state-of-the-art in single mode air transportation robustness and provides the starting point for future research on the robustness of multi-modal air transportation.

This paper is organized as follows. Section 2 presents our methodology to assess the robustness of air transportation systems, and German airport network is used as a small running network example to explain our methodology. In Section 3, we present the results of robustness analysis for the whole worldwide airport network. Finally, conclusions are drawn in Section 4.

2 Methodology

In this section, we describe how airport networks can be attacked. We formally define the notation of weighted networks and the attack on weighted networks in Section 2.1. In Section 2.2, we present several attacking strategies in our attack model. We define a set of appropriate robustness measures in Section 2.3. In each section, we use the German airport network as a running example, since it is helpful to explain our methodology using an example based on a smaller network. We report on our evaluation for the worldwide airport network in Section 3.

2.1 Attacks on airport networks

**Definition 1 (weighted networks).** A weighted network $\text{WN}$ consists of a set of nodes, denoted with nodes(WN) and a set of weighted links between nodes, denoted with links(WN). Each weighted link is represented as a tuple $(u, v, w)$, where $u$ is the source of the link, $v$ the target of the link, and $w$ the link’s weight. A link is called outgoing $(u, v, w)$ for node $u$ and incoming for node $v$. The weight of a link between two nodes $u$ and $v$ is denoted with weight$(u, v)$. Please note that our functional notation of weights assumes at most one link per pair of nodes. This improves readability, but is no severe restriction on our robustness analysis. The length of a path (a sequence of nodes $(u_1, u_2, \cdots, u_n)$) is defined as the sum of the weights, i.e. weight$(u_1, u_2)+\ldots+\text{weight}(u_{n-1}, u_n)$. A shortest path in a weighted network between two nodes $u$ and $v$ is a sequence of nodes with the shortest length. The number of the shortest paths between nodes $u$ and $v$ is denoted with $\sigma_{u,v}$.

Airport networks (AN) are instances of weighted networks, so that the nodes are a set of airports $(a_1, a_2, \cdots, a_n)$ and the links represent relationships between airports, for instance, geographical distances or the
We select the origin-destination (OD) airports with at least 6 passengers travelling per month to build the airport network for Germany. We further explain our selection in Section 3.1. The German airport network (OD pairs, January 2013) consists of 25 nodes and 187 links (Fig. Error! Reference source not found.). The strength of a link grows with the number of travelling passengers. Note that among the three airports in Berlin, only TXL is shown in the map, and the other two airports (BER and SXF) overlap with TXL. On average, a link is weighted with 6529 passengers. The minimum number of passengers for a link is 6 (for instance, DUS → CGN) and the maximum is 53618 (TXL→ MUN). The median number of passengers is 1239 and standard deviation is 12222.

Fig.2 German airport network in January 2013.

One can distinguish two types of passenger weights: number of passengers from direct flights and number of passengers from flight intentions (OD pairs). The first type is considered from the physical network point of view: the number of passengers travelling between any two airports; passengers with multiple intermediate stops are counted for each connecting airport separately. The latter type is considered from the function point of view: the number of passengers travelling between origin/destination airports; passengers with multiple intermediate stops are not counted for the connecting airports.

If an airport is closed down, all direct flight connections from/to this airport are directly affected. However, the conclusion that all these passengers will not travel anymore is wrong. In Fig. Fig.3, we show a simple example for the German airport network: a passenger travels from HAM to STR, via two connecting airports FRA and MUC. Although this example might look unrealistic, since Lufthansa offers a direct flight from HAM to STR, six passengers booked this kind of travel with Lufthansa in January 2013. We suppose that MUC closes down because of an attack, and then one will conclude from direct flight passenger data that six passengers cannot travel from FRA to MUC and six more passengers cannot travel from MUC to STR. This conclusion is misleading for two reasons. First, the passengers can still travel from HAM to STR (via another direct flight, FRA, or any other scheduled airport connection). Second, if one really wants to assume that these passengers cannot travel anymore, one also needs to remove the six passengers for the flight from HAM to FRA.

Therefore, in this paper we use the number of passengers from direct flights as the link weight, while we use the unaffected number of passengers from origin-destination pairs as a baseline measure for the robustness of the world-wide airport network. With flight intentions, the unaffected passenger problem boils down to the question whether
two airports are still connected via another scheduled flight.

Fig. 3 One example of an origin-destination pair with passengers travelling through two connecting airports.

**Definition 2 (network attack).** Given an airport network \( AN \), an attack is a sequence of nodes \( A = (u_1, u_2, \ldots, u_n) \), such that 1) each \( u_i \in \text{nodes}(AN) \) and 2) for each \( i, j \) we have that \( u_i \neq u_j \). An attack \( A \) is called complete for \( AN \), if \( A \) contains \( \mid \text{nodes}(AN) \mid \) different nodes. An attack sequence to a network is applied from left to right. The first step of an attack \( A = (u_1, u_2, \ldots, u_n) \) removes node \( u_1 \) from the network and yields a network with nodes as \( \text{nodes}(AN) \setminus \{u_1\} \), links as \( \text{links}(AN) \setminus \{v, w.(u_1, v, w) \in \text{links}(AN)\} \cup \{v, w.(u, v_1, w) \in \text{links}(AN)\} \). In the second step, \( u_2 \) is removed from the network, etc.

In order to design an attack on a network, one can follow different strategies. A very simple strategy is a so-called random attack, where the sequence of removed nodes is chosen randomly. The effectiveness of such an attack (measured in the degradation of the network performance, see below) is usually rather low on average. One heuristic is to select the sequence of removed nodes based on certain network metrics. We discuss such attacks in Section 2.2.

Intuitively, one can distinguish two types of attacks in a network: strong attacks and weak attacks. Strong attacks refer to attacking important nodes first, while weak attacks refer to attacking unimportant nodes first. Strong attacks often require more knowledge about the targeted network: not only concerning topological properties, but also the traffic.

### 2.2 Attacking strategies

In addition to attacking a network randomly, attacks can also be based on the values of network metrics. In the following, we briefly review six chosen standard network metrics.

1. **Weighted degree**: The degree of a node \( u \) is the sum of all weights for the incoming and outgoing links of \( u \).

2. **Betweenness centrality**: \( B(u) = \sum_{s \neq t, s \neq u} \frac{\sigma_{st}(u)}{\sigma_{st}} \), where \( \sigma_{st}(u) \) is the number of the shortest paths going from node \( s \) to node \( t \) and passing through node \( u \) \( ^{12} \).

3. **Closeness centrality**: \( C(u) = \frac{1}{\sum_{j \neq u, j \neq u} d_G(u, j)} \), where \( d_G(u, j) \) denotes the length of a shortest path between node \( u \) and node \( j \). \( n = \mid \text{nodes}(WN) \mid \) is the number of nodes, and \( n-1 \) is a normalizing constant. This metric is the average distance from a given starting node to all other nodes in the network.

4. **Eigenvector centrality**: It is the eigenvector of the largest eigenvalue of the adjacency matrix. This metric measures the influence of a node in the network. Nodes with high eigenvector centrality also connect to other nodes which have high eigenvector centrality.

5. **Bonacich power centrality**: This centrality is based on the idea that the status of a node is influenced by the status of his neighbors. \( C(\alpha, \beta) = \alpha(I - \beta A)^{-1} A \), where \( \alpha \) is a scaling factor, \( \beta \) the degree to which a node’s status is influenced by his neighbors’ status, \( I \) the identity matrix.
matrix, \( A \) the adjacency matrix, and \( 1 \) a matrix of all ones. When \( \beta > 0 \), Bonacich power centrality increases if one’s neighbors have many connections; When \( \beta = 0 \), Bonacich power centrality only considers direct connections; When \( \beta < 0 \), Bonacich power centrality increases if one’s neighbors have few connections, i.e., having weak neighbors is a source of power. In this paper, we choose \( \beta = -0.995^* \frac{1}{\text{largest eigenvalue of the adjacency matrix}} \), since we are interested in the power-dependence of the network. 

(6) **Damage:** This attacking strategy is proposed by Latora and Marchiori, and the importance of a node is measured by the drop of the network performance caused by deactivation of that node. The performance of the network is measured by \( \text{Efficiency} = \frac{1}{n(n-1)} \sum_{i \neq j \in N} \frac{1}{d_{ij}} \), where \( d_{ij} \) is the smallest sum of the links throughout all possible paths in the network from a node \( i \) to a node \( j \). When the network is unweighted, \( d_{ij} \) is just the minimum number of links traversed from node \( i \) to node \( j \); when the links in the network are weighted (for instance geometrical distance), the smallest sum of the links represents the shortest weighted path from \( i \) to \( j \).

**Table 2.** Top 10 ranked German airports according to descending order of six network metrics

<table>
<thead>
<tr>
<th>distance weighted network metrics</th>
<th>passenger weighted network metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top degree betweenness closeness eigenvector bonacich damage</td>
<td>Top degree betweenness closeness eigenvector bonacich damage</td>
</tr>
<tr>
<td>MUC</td>
<td>HAM</td>
</tr>
<tr>
<td>HAM</td>
<td>MUC</td>
</tr>
<tr>
<td>STR</td>
<td>NUE</td>
</tr>
<tr>
<td>TXL</td>
<td>STR</td>
</tr>
<tr>
<td>FRA</td>
<td>MUC</td>
</tr>
<tr>
<td>CGN</td>
<td>FKB</td>
</tr>
</tbody>
</table>

Each of these metrics can be exploited as a strategy for attacking a network by either removing nodes in the order of descending metric values or ascending metric values. A common practice is, for instance, to attack nodes in decreasing order of degree. The intuition is that nodes with a high degree - often called hubs - are important for the network structure and therefore the removal of high-degree nodes harms the network most. In our study, we provide a complete picture of possible attacks: random attacks, strong attacks (descending values of metrics), and weak attacks (ascending values of metrics).

Table 2 shows the top 10 ranked nodes in the German airport network based on the descending order of the six network metrics. Two different weights are used: geographical distances between two airports and the number of passengers travelling between two airports. All of the metric orders yield a different ranking. Therefore, it is interesting to further investigate which attacking strategy harms the network most.

### 2.3 Robustness measures

In this section, we use the unaffected passengers with rerouting as a baseline measure for the robustness of air transportation systems. Further, we introduce another robustness measure: survived links. For the purpose of comparison, we also briefly review two existing robustness measures: giant component and algebraic connectivity.

The unaffected passengers with rerouting (UPR) captures how many passengers still can travel when an airport is closed, with the reallocation of the passengers taken into account; this is denoted as dynamic robustness in Ref. Note that our analysis focuses on the connectivity of the airports: passengers between certain OD pairs can still make their trips as long as the OD airports are connected via other airports from the original schedule.

**Definition 3 (unaffected passengers with rerouting).** **UPR for a network AN against a base-
line network $AN_{base}$ is defined as $R = \sum_{(u,v,w) \in \text{links}(AN)} \text{rerouting}(u,v,w)$ and we let $\text{rerouting}(u,v,w) = w$, if connected($AN,u,v$) and 0 otherwise.

Fig.4 presents the scatter plot between the number of passengers and revenue in the year 2013 (Each circle represents one ticket sold in year 2013.). There is a general trend that the revenue increases with the number of passengers (Power law correlation: Revenue$=882.45 \times \text{Passengers}^{0.8694}$, $R^2=0.8458$). Intuitively, the revenue would be higher with more passengers travelling. We also investigate another robustness measure: Unaffected Revenue with Rerouting (URR). However, since the number of passengers and the revenue are highly correlated, the two measures yield very similar results. Therefore, we only present the results using UPR as the baseline robustness measure for the worldwide airport network.

The survived links (SL) is the number of remaining connections between airports after an attack on the network.

![Fig.4 Number of passengers versus revenue in worldwide airport network in 2013](image)

**Definition 4 (survived links).** SL for a network $AN$ against a baseline network $AN_{base}$ is defined as

$$\frac{\text{links}(AN)}{\text{links}(AN_{base})},$$

i.e., the ratio of links after nodes are removed from the network to the number of links in the original network.

In a network, the Giant Component (GC) is a group of connected nodes where every node is reachable from all other nodes. $\text{Error! Reference source not found.}$

**Definition 5 (giant component).** GC for a network $AN$ against a base network $AN_{base}$ is defined as

$$\frac{\max(|\text{nodes}(c)|\{c \in \text{connectedComponents}(AN)\})}{\max(|\text{nodes}(c)|\{c \in \text{connectedComponents}(AN_{base})\})},$$

i.e., the ratio of the new size of GC after nodes are removed from the network to the GC of the original network.

For a graph, Algebraic Connectivity (AC) is defined as the second smallest eigenvalue of the Laplacian matrix $L$, and $L = D - A$, where $D$ is the diagonal degree matrix and $A$ the adjacency matrix. $\text{Error! Reference source not found.}$ AC plays a special role in the robustness of complex networks, since it measures the extent to which it is difficult to break a network into disconnected components. $\text{Error! Reference source not found.}$ In the context of air transportation, a network with a larger value of AC has a higher robustness against node (node) and link (flight connection) failure.
Definition 6 (algebraic connectivity). \( AC \) for a network \( \mathbf{AN} \) against a base network \( \mathbf{AN}_{\text{base}} \) is defined as
\[
\frac{\text{AC}_{\mathbf{AN}}}{\text{AC}_{\mathbf{AN}_{\text{base}}}},
\]
i.e., the ratio of the new \( AC \) after nodes are removed from the network to the \( AC \) of the original network.

We generated 1000 complete random attacks for the German airport network. For each of these attacks, we computed the attack traces: robustness measures compared to the percentage of removed nodes during an attack. The results are shown in Fig. 5 (a).

In order to visualize the commonalities of these random attacks, e.g. data points which occur frequently and independently of the chosen attack, we show the two-dimensional kernel density estimation for the percentage of removed nodes against the robustness measures in Fig. 5(b). White areas indicate infrequent/unused points and darker areas represent commonalities. We draw the following conclusions:

- **UPR** is the baseline for the robustness measure. It calculates the percentage of passengers who can still travel after an attack took place. The attack traces are wide-spread. While some attacks are very successful (if important nodes are removed early), under other attacks the network keeps robust (with robustness of 80%) even if 50% of the nodes are removed. The two-dimensional kernel density of UPR shows the commonalities among random attack traces, which can be summarized as follows: 1) if only a few nodes are removed, the network remains robust (dark area in the top-left of the chart) and 2) if more than 60%-70% of the nodes are removed, the network’s robustness is very low (dark area in the bottom-right of the chart). Intuitively, this is correct, since for the range between (say 1%-70%), the random attacks do not have anything else in common.

- **GC-robustness curves** are either on or closely below the diagonal line. For most of the time, each attack can reduce the size of giant component of a network by one or zero, depending on whether the removed node was in the giant component before. Note that there are some cases that an attack can reduce the size of giant component more than one. we consider a network composed of two communities and connected by a central node. If that central node is deleted, the size of giant component would be greatly reduced. Since the size of giant component cannot be larger than the number of remaining nodes, the upper-right triangle of the attack trace area is unused. The two-dimensional kernel density suggests that for GC most of the random attacks have very similar proper-
ties (black diagonal). This conclusion contradicts the observation from UPR.

- A robustness measure should be monotonically descending. However, AC-robustness is increasing with the number of removed nodes. This shows that AC is inappropriate, if node removal is taken into account. AC was originally proposed as an edge-based robustness measure, where the number of nodes remains unchanged. In our attack scenario, AC yields unusable results. Therefore we will disregard AC below. The other three measures are monotonically decreasing.

- SL robustness curves are quite similar to UPR robustness curves. Compared to GC, SL also 1) allows to represent attack traces above the diagonal line and 2) does not (wrongly) suggest very strong commonalities between random attacks.

3 Results

When a network is attacked, it is open how to select the order in which the nodes should be removed [Error! Reference source not found.]. In this study, we apply twelve different attacking strategies to the worldwide airport network with three different weights (unweighted, distance weighted and passenger weighted): removing nodes based on six network metrics (degree, betweenness, closeness, eigenvector, Bonacich and damage) in descending and ascending order separately. We use three robustness measures to detect the decrease of the network performance caused by these attacks. In total we have 108 attacking scenarios (3 weights, 12 attacking strategies and 3 robustness measures). We are interested to find out which attacking strategy harms the network most. We introduce the database in Section 3.1. Section 3.2 presents the results of several attacking strategies to the worldwide airport network with different robustness measures.

3.1 Database

For the application and analysis of the metrics, recent data from 2013 ADI was obtained [Error! Reference source not found.]. The OD Market Section in ADI provides the details of the passenger itineraries: the total number of passengers and the total revenue between the origin and destination airports. For each OD pair, up to three connecting airports are recorded.

From this database, we select the origin and destination airports with at least 72 passengers travelling per year (i.e., 6 passengers travelling per month). Note that there is no standard threshold for the number of passengers or the number of flights between two airports when the airport network is constructed. For instance, Lehner selected the links with at least 600 flights per year (50 flights per month) in the European airport network [Error! Reference source not found.]. Kotegawa et al. selected the links with at least 365 flights per year (i.e., airports are required to have an average of at least one operation per day) in the U.S. airport network [Error! Reference source not found.]. In this study, to our best knowledge, our threshold (72 passengers travelling per year) has the finest granularity.

We consider the worldwide airport network as directed and weighted; three different weights are used: unweighted, geographical distances, and the number of passengers travelling between two airports. In total, there are 3885 nodes and 228080 links. The unweighted worldwide airport network has an average path length of 2.946 and an average clustering coefficient of 0.645. These values are comparable with the worldwide airport network constructed in Ref. [Error! Reference source not found.]: average path length 3.94 and an average clustering coefficient 0.64. On average, there are 11845 passengers per airport connection. The minimum number of passengers is 73 and the maximum is 441200 (CJU: Jeju International Airport, South Korea → GMP: Gimpo International Airport, South Korea). The median number of passengers is 592 and standard deviation is 61986.

The average values of the six metrics in the worldwide airport network with three different weights are presented in Table 3. Each of these metrics is exploited as a strategy to attack the network.

Table 3 Average values of six metrics in worldwide airport network using different weights with 3885 nodes and 228080 links.

<table>
<thead>
<tr>
<th>Worldwide airport network</th>
<th>Degree</th>
<th>Betweenness</th>
<th>Closeness</th>
<th>Eigenvector</th>
<th>Bonacich</th>
<th>Efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unweighted</td>
<td>59</td>
<td>0.00048</td>
<td>0.34849</td>
<td>0.08199</td>
<td>0.00563</td>
<td>0.35586</td>
</tr>
<tr>
<td>Distance weighted</td>
<td>231619</td>
<td>0.00069</td>
<td>0.00010</td>
<td>0.00630</td>
<td>0.00318</td>
<td>0.00017</td>
</tr>
<tr>
<td>Passenger weighted</td>
<td>692998</td>
<td>0.00072</td>
<td>0.00052</td>
<td>0.00273</td>
<td>0.00363</td>
<td>0.00201</td>
</tr>
</tbody>
</table>
Fig. 6 Cross-comparison among three robustness measures (UPR, GC and SL) in passenger weighted worldwide airport network with targeted attacks based on descending order of six network metrics.

3.2 System analysis of robustness for worldwide airport network

We perform system analysis of the robustness for the worldwide airport network with three different weights (unweighted, distance weighted and passenger weighted) measured by UPR, GC and SL under attacks, respectively. The comparison of different attacking strategies is presented in Section 3.2.1, while the computational efficiency is compared in Section 3.2.2.

3.2.1 Comparison of attacking strategies

Intuitively, one is more interested in strong attacks (descending order of metric values), since they are more harmful to the network than weak attacks (ascending order of metric values). Fig. 6 presents the robustness measures (UPR, GC and SL) in the passenger weighted worldwide airport network under strong attacks. When UPR is used as the robustness measure, attacks based on Bonacich power centrality and degree are equally most harmful to the network. Bonacich power centrality is better for the initial phase of an attack (up to 7% of removed nodes) and degree is slightly better when more than 7% of the nodes are removed. With comparable attacking effectiveness, the computation of degree is 1-2 orders of magnitude faster than the computation of Bonacich. Since the computation time is often the bottle-neck for large-scale networks, degree is a very good candidate for an effective and lightweight attacking strategy, especially in the case of interactive attacks on large-scale networks.

On the other hand, the attack based on closeness is least harmful to the network. One explanation is that closeness of a node is the reciprocal of the sum of the shortest path distances from this node to all other nodes in the network, and since we use the number of passengers as link weight in the shortest path calculation, the closeness metric might become less meaningful. Regarding GC and SL, Bonacich power centrality is slightly better than degree, while eigenvector is the worst attacking strategy.

Note that there may be no "best" robustness measure or "best" attacking strategy, and results may depend on the objective of a study. The objective of our study is to evaluate the robustness of air transportation systems from passengers' perspective, and we propose to use the unaffected passengers with rerouting as a baseline measure. In opposition to graph-theoretic metrics, this measure directly expresses the impact of airport failure on the traffic - not on (theoretical) properties of the graph.

In order to further investigate the correlation between UPR and other robustness measures, Fig. 7 plots the robustness values of UPR against SL and GC for all six network metrics. The dashed diagonal grey line represents perfect correlation; the red line shows the dependency between pairs of robustness measures. The overlapping of the two curves indicates strong similarity between two robustness measures. We can observe that UPR and GC are least similar; SL is closer to the diagonal line and it is more similar to UPR than GC.
Table 4 presents the most successful targeted attacks based on node degree to worldwide airport network with number of passengers as weight.

<table>
<thead>
<tr>
<th>Nr</th>
<th>Airport</th>
<th>UPR</th>
<th>Nr</th>
<th>Airport</th>
<th>UPR</th>
<th>Nr</th>
<th>Airport</th>
<th>UPR</th>
<th>Nr</th>
<th>Airport</th>
<th>UPR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>PEK (Beijing)</td>
<td>0.971</td>
<td>11</td>
<td>SIN (Singapore)</td>
<td>0.802</td>
<td>21</td>
<td>MNL (Manila)</td>
<td>0.682</td>
<td>31</td>
<td>LGW (London)</td>
<td>0.587</td>
</tr>
<tr>
<td>2</td>
<td>HND (Tokyo)</td>
<td>0.943</td>
<td>12</td>
<td>ORD (Chicago)</td>
<td>0.787</td>
<td>22</td>
<td>SYD (Sydney)</td>
<td>0.671</td>
<td>32</td>
<td>BOS (Boston)</td>
<td>0.581</td>
</tr>
<tr>
<td>3</td>
<td>CGK (Jakarta)</td>
<td>0.924</td>
<td>13</td>
<td>KUL (Kuala Lumpur)</td>
<td>0.775</td>
<td>23</td>
<td>MCO (Orlando)</td>
<td>0.663</td>
<td>33</td>
<td>MEL (Melbourne)</td>
<td>0.575</td>
</tr>
<tr>
<td>4</td>
<td>LHR (London)</td>
<td>0.904</td>
<td>14</td>
<td>SFO (San Francisco)</td>
<td>0.766</td>
<td>24</td>
<td>DEN (Denver)</td>
<td>0.651</td>
<td>34</td>
<td>SEA (Seattle)</td>
<td>0.568</td>
</tr>
<tr>
<td>5</td>
<td>LAX (Los Angeles)</td>
<td>0.886</td>
<td>15</td>
<td>SHA (Shanghai)</td>
<td>0.756</td>
<td>25</td>
<td>SZX (Shenzhen)</td>
<td>0.642</td>
<td>35</td>
<td>AMS (Amsterdam)</td>
<td>0.558</td>
</tr>
<tr>
<td>6</td>
<td>CAN (Guangzhou)</td>
<td>0.87</td>
<td>16</td>
<td>LAS (Las Vegas)</td>
<td>0.746</td>
<td>26</td>
<td>CTU (Chengdu)</td>
<td>0.635</td>
<td>36</td>
<td>FRA (Frankfurt)</td>
<td>0.548</td>
</tr>
<tr>
<td>7</td>
<td>PVG (Shanghai)</td>
<td>0.855</td>
<td>17</td>
<td>ATL (Atlanta)</td>
<td>0.726</td>
<td>27</td>
<td>ICN (Seoul)</td>
<td>0.628</td>
<td>37</td>
<td>NRT (Tokyo)</td>
<td>0.542</td>
</tr>
<tr>
<td>8</td>
<td>JFK (New York)</td>
<td>0.842</td>
<td>18</td>
<td>BKK (Bangkok)</td>
<td>0.717</td>
<td>28</td>
<td>IST (Istanbul)</td>
<td>0.615</td>
<td>38</td>
<td>GRU (Sao Paulo)</td>
<td>0.532</td>
</tr>
<tr>
<td>9</td>
<td>HKG (Hong Kong)</td>
<td>0.828</td>
<td>19</td>
<td>BCN (Barcelona)</td>
<td>0.706</td>
<td>29</td>
<td>DEL (Delhi)</td>
<td>0.605</td>
<td>39</td>
<td>MAD (Madrid)</td>
<td>0.524</td>
</tr>
<tr>
<td>10</td>
<td>CDG (Paris)</td>
<td>0.814</td>
<td>20</td>
<td>DXB (Dubai)</td>
<td>0.691</td>
<td>30</td>
<td>KMG (Kunming)</td>
<td>0.597</td>
<td>40</td>
<td>BOM (Mumbai)</td>
<td>0.517</td>
</tr>
</tbody>
</table>

Table 4 presents the most successful targeted attacks based on node degree, where the first 40 attacked nodes (out of 3885 nodes, less than 1.1%) are listed. These attacks reduce the robustness of the network from 100% down to 50%, i.e., 50% of the passengers cannot travel any more although rerouting is enabled. The first attacked node is PEK, and PEK has the highest weighted degree in the passenger weighted worldwide airport network. Among 3885 airports, when we use the attacking strategy based on weighted degree, one only needs to attack 11 nodes (out of 3885 nodes, less than 0.3%), and then the performance of the network can be degraded to 80%. Especially, there are 7 Asian airports among these 11 attacked nodes. This shows the importance of Asia for the functioning of global air transportation systems.

### 3.2.2 Comparison of computational efficiency

During our experiments, we noticed that the computation time of attacking strategies was rather different ranging from seconds, minutes to hours. Our initial hypothesis was that longer computation time might generate more effective attacking results. Therefore, we compare the computational efficiency of different attacking strategies and robustness measures. The run time for computing the attacking strategies is shown in Fig. 8, while the run time for evaluating the robustness measures is shown in Fig. 9. Note that different scales (seconds, minutes and hours) are used for measuring run time. Computing degree and eigenvector takes only a few seconds, while computing betweenness,
closeness and Bonacich takes up to several minutes. The run time for SL (right panel in Fig.9) is less than 0.2 second. The slowest attacking strategy (computation-wise) is damage, which takes up to three complete days when applied to the initial worldwide network.

In our 108 attacking scenarios, damage did not provide an effective attacking performance, although it took the longest time to compute. We think this counter-intuitive finding should draw more attention. Especially in the context of interactive simulations with larger networks, e.g., what happens in case of any change to the network (node/link addition/deletion), the computational time required for finding interesting (harming) attacks becomes more important.

On the other hand, calculating UPR is the most time-consuming operation. For the initial network, it takes 3-4 seconds to evaluate the robustness. The more nodes are removed, the much time is spent on the rerouting process (up to ten seconds). Only when few nodes are left, the rerouting process speeds up recognizably and the run time decreases. Evaluating GC takes three seconds for the initial network and the run time is decreased when more nodes are removed (because less nodes have to be analyzed for finding the giant component). The fastest robustness measure is SL, which is 1-2 orders of magnitude faster than the other two measures. This is an interesting property in the case of interactive attacks in future research.

4 Conclusions

The safety and reliability of complex air transportation systems are vital for the society. In this study, we performed system analysis for the robustness of air transportation systems, with unaffected passengers with rerouting as a baseline measure. Given the most complete dataset available, we identify commonalities and differences between several robustness measures and attacking strategies for the worldwide airport network. The contributions of the paper are as follows:

Fig.8 Run time for computing attacking strategies regarding six network metrics.

Fig.9 Run time for three different robustness measures when partial attacks are executed on worldwide network.
1. We applied twelve different attacking strategies (degree, betweenness, closeness, eigenvector, Bonacich and damage in ascending and descending order) to the worldwide airport network with three different weights (unweighted, distance and passenger) and evaluated three different robustness measures (UPR, GC and SL). All experiments were evaluated on the same dataset and give a consistent view on attacking airport networks. In total, we investigated 108 attacking scenarios.

2. We find that GC is a rather bad robustness measure, since (1) it cannot represent weak attacks appropriately, and (2) it overestimates robustness for very strong attacks. SL is an alternative which solves (1), and reduces the effects of (2)). Furthermore, SL is 1-2 orders of magnitude faster to compute than GC, which is an interesting property in the case of interactive attacks.

3. The attacking strategies: degree and Bonacich are the best methods for attacking the worldwide airport network with passenger weights using UPR. Bonacich is better for the initial phase of an attack (up to 7% of removed nodes) and degree is slightly better when more than 7% of the nodes are removed. With comparable attacking effectiveness, the computation of degree is 1-2 orders of magnitude faster than the computation of Bonacich. Since the computation time is often the bottle-neck for large-scale networks, degree is a very good candidate for an effective and lightweight attacking strategy, especially in the case of interactive attacks on large-scale networks. Furthermore, closeness is the worst strategy for the robustness measure UPR. For GC/SL, Bonacich is slightly better than degree. Eigenvector is the worst attacking strategy. In our experiments, damage took the longest time to compute, but did not provide effective attacking performance.

4. Our analysis shows that knowledge of an attacker significantly influences the effectiveness of attacking strategies. When the attacker is aware of the number of passengers travelling on routes (passenger-weighted network), the attack is more successful than that conducted by less informed attacker (unweighted or distance-weighted network).

5. We analyze the computational resources required for each attacking technique on the same airport network. While these resources are often neglected in related work, we show that the time to compute an attack is sometimes orders of magnitude faster/slower, while providing similar results. Given that many graph problems are not efficiently solvable, i.e. solutions do not scale up with the size of the graph, we advocate the use of simple, yet efficient attacking strategies for future robustness analysis of air transportation networks. In particular, running interactive robustness analysis on large networks is only feasible with short response time, if the attacking strategies can be computed efficiently.

In this study, we analyzed the robustness of the worldwide airport network under node random failure and targeted attacks with several attacking strategies and robustness measures. Our research provides a unified view on attacking air transportation networks and serves as a starting point to further explore effective mitigation strategies to defend against disruptions.

In the following, we discuss some limitations of our initial study, which can be addressed in future work. 1) While our research focused on static attack generators, in practice, attacks can also have a dynamic nature. Thus, future work should take into account the iterative calculation of metric values: after each single-node attack to a network, the network metric is recomputed for the remaining nodes and the node with the highest/lowest value is removed next, since it was shown that this recalculation of metrics can be more effective than the pre-computation of a static attack. 2) One assumption of our study is that intentional failures in airports can happen all over the world, which is impossible to coordinate in practice, if many airports have to be affected. Therefore, future research could investigate other attacking scenarios, where local regions are affected, instead of widely distributed nodes. 3) Similarly, we neglect the effect of regional airport system, where multiple airports serve the same metropolitan regions. We did not consider the case of multi-modal transportation in a sense that passengers could connect to other airports by other means of transportation, e.g., using train or bus connections. We would like to address this problem in future work. 4) Furthermore, our analysis relied on the connectivity of the airports: passengers between certain OD pairs can still make their trips as long as the OD airports are connected via other airports from the original schedule. Capacity constraints should be taken into account in future work. 5) Rerouting passengers after a global air transport failure assumes that all passengers still want to travel. Experiences with past terrorist attacks indicate that the passengers often cancel their travel plans. Analyzing and modeling such psychological effects can further help to understand and improve the robustness of the network.

Acknowledgements
This study was supported by the National Natural Science Foundation of China (Nos. 61650110516, 61601013 and 61521091). The authors would like to thank Sabre Airport Data Intelligence (ADI) and German Aerospace Center (DLR) for providing the data in this study. The authors would like to particularly acknowledge Klaus Luetjens and Niclas Dzikus for providing us with the way to download the data from ADI. The authors also thank Stephan Lehner...
for the initial discussion on robustness in air transportation systems.

References

34. Wei, P., Sun, D.. Weighted algebraic connectivity: An application to airport transportation network. In: *18th IFAC World Congress Milano (Italy)*, 2011.

**SUN Xiaoqian** is an associate professor with School of Electronic and Information Engineering at Beihang University, Beijing, China. She obtained her Ph.D. degree in aerospace engineering from Hamburg University of Technology in 2012. Her research interests mainly include air transportation networks, multi-modal transportation, and multi-criteria decision analysis.

E-mail: sunxq@buaa.edu.cn
Volker Gollnick is a full professor at Hamburg University of Technology and director of Institute of Air Transportation Systems at German Aerospace Center since 2007. He received his Diplom-degree in mechanical and aerospace engineering in 1991. In 2004, he received his Ph.D. degree at the TU Munich. His research interests are integrated aircraft design, air transport operation and processes, as well as avionics systems.
E-mail: volker.gollnick@dlr.de

Sebastian Wandelt is a full professor at School of Electronic and Information Engineering, Beihang University, Beijing, China. He received the Ph.D. degree in computer science from Hamburg University of Technology in 2011. His research interests are transportation systems, scalable data management, and compressing/searching large collections of objects.
E-mail: wandelt@buaa.edu.cn