

Robustness of Airline Alliance Route Networks

Abstract

The aim of this study is to analyze the robustness of the three major airline alliances' (i.e., Star Alliance, oneworld and SkyTeam) route networks. Firstly, the normalization of a multi-scale measure of vulnerability is proposed in order to perform the analysis in networks with different sizes, i.e., number of nodes. An alternative node selection criterion is also proposed in order to study robustness and vulnerability of such complex networks, based on network efficiency. And lastly, a new procedure –the inverted adaptive strategy– is presented to sort the nodes in order to anticipate network breakdown. Finally, the robustness of the three alliance networks are analyzed with (1) a normalized multi-scale measure of vulnerability, (2) an adaptive strategy based on four different criteria and (3) an inverted adaptive strategy based on the efficiency criterion. The results show that Star Alliance has the most resilient route network, followed by SkyTeam and then oneworld. It was also shown that the inverted adaptive strategy based on the efficiency criterion –inverted efficiency– shows a great success in quickly breaking networks similar to that found with betweenness criterion but with even better results.

Keywords: Alliance route network, Complex networks, Robustness, Airline alliances, Airport disclosure, Intentional attacks

1. Introduction

The restructuring of airline activities into alliances has been one of the major traits of this industry since the beginning of the 90s, and over the last decade most Full-Service Carriers and regional airlines have participated in an airline alliance. Airlines join alliances for several reasons (Gaggero and Bartolini, 2012). First, alliance members can benefit from economies of scale and density: without having to increase investment in aircraft, alliance members can extend their route network and offer a wider range of frequency to customers on selected routes. Furthermore, alliance members can

explore easier ways to collaborate with other members through codesharing, joint-ventures or even merger and acquisitions. Finally, alliance members can benefit from the joint venture by offering benefits to customers (e.g., frequent-flyer programs) or from the joint purchase of supplies such as fuel. In respect to consumer welfare, airline alliances lower the fares of interline flights, which compensates for the fare increases on interhub flights (Brueckner, 2001; Brueckner et al., 2011). However, it must be noted that the competence of alliance members to coordinate routes and fares is an important requirement for passengers to realize these benefits (Wan et al., 2009).

When an airline joins an alliance, the reliability of its services offered to customers not only depends on the flights the airline operates, but also on the operations of the rest of the alliance members, since most of the routes offered by alliances are operated on a hub-and-spoke basis. Although airline alliances have been formed for operational and competitive reasons, the attachment to an alliance can determine the robustness of the airline network.

The *Airline alliance route networks* (AARNs) are constructed as an aggregation of the airlines' route networks belonging to the alliance. These networks can be considered as a multilayered network (Cardillo et al., 2013), and constitute an intermediate level of analysis of air transport networks, between airline route networks and global or regional networks (Lordan et al., 2014a). The aim of the present study is to analyze the vulnerability of AARNs to errors (i.e., the random isolation of an airport) and attacks (i.e., isolation of well-connected airports with the aim of causing the maximum damage to the route network). This assessment is performed by two different approaches: first, using a multi-scale measure of vulnerability (Boccaletti et al., 2007), and second, examining the effect of the disconnection of a fraction f of well-connected nodes on the size of the overall giant component. This study can shed light on the robustness of real networks not only for the special case of airline alliances but also for networks sharing similar topological properties.

2. Methods

2.1. Vulnerability

In Boccaletti et al. (2007), a multi-scale measure of the vulnerability of a graph G is defined by introducing the coefficient p to the characteristic formula of the average edge betweenness as:

$$b_p(G) = \left(\frac{1}{|E|} \sum_{l \in E} b_l^p \right)^{1/p} \quad (1)$$

where $|E|$ is the number of edges, and b_l is the betweenness of the edge l calculated as:

$$b_l = \sum_{i \neq j} \frac{n_{ij}(l)}{n_{ij}} \quad (2)$$

where $n_{ij}(l)$ is the number of geodesics (i.e., shortest paths) from node i to node j that contain the edge l , and n_{ij} is the total number of shortest paths. The scale parameter $p > 0$ acts as an exponent of each value of edge betweenness, and its inverse value as an exponent of the sum of all (powered) edge betweenness. For instance, $b_2(G)$ is the square root of the average square edge betweenness of the graph G .

To compare the vulnerability of two networks G and G' with similar structural properties, the first step is to compute b_1 for both graphs. If $b_1(G) < b_1(G')$, then G is more robust (less vulnerable) than G' . If $b_1(G) = b_1(G')$, then the values of b_p for values of $p > 1$ must be computed until $b_p(G) \neq b_p(G')$. Then, the network with the smallest value of b_p will be the most robust one. In general, the full multi-scale sequence of betweenness coefficients $(b_p(G))_{p \geq 1}$ must be considered in order to get an accurate approach to the robustness of the network (Boccaletti et al., 2007).

This procedure can be used to assess differences in vulnerability between airline alliance route networks (AARNs). As shown in Table 1, AARNs have really different numbers of nodes and edges, so the measures of vulnerability have to be normalized in order to be able to compare graphs. One possible normalization procedure can be defined by using the graphs of N nodes with minimum and maximum vulnerability: the complete and the string graphs, respectively. A *complete graph* of N nodes is a fully connected graph where each node has $N - 1$ edges. It is easy to see that the complete graph has a minimum vulnerability, which is $b(G_{complete}) = 1$. On the other hand, a *path graph* of N nodes can be defined as a string of nodes attached to its neighbors. Each node has two edges, except the two end nodes of the string that just have one. This graph has the highest vulnerability among all graphs of N nodes. Mishkovski et al. (2011) proposed a normalization for $b(G)$ as:

$$b_{nor}(G) = \frac{b(G) - b(G_{complete})}{b(G_{path}) - b(G_{complete})} = \frac{b(G) - 1}{\frac{N(N+1)}{6} - 1} \quad (3)$$

This normalization can be extended for other scales of vulnerability where $p \neq 1$. Considering the multi-scale approach on a complete graph, one can easily see that $(b_p(G_{complete}))_{p \geq 1} = 1$. For the path graph, although it is known that $b_1(G_{path}) = \frac{N(N+1)}{6}$, this simplification cannot be extended for $p > 1$. Despite that, it is easy to see that $b_p(G_{complete}) \leq b(G) \leq b_p(G_{path})$. As a consequence, the normalization of the multi-scale measure of the vulnerability of a graph is defined as:

$$b_{p,nor}(G) = \frac{b_p(G) - b_p(G_{complete})}{b_p(G_{path}) - b_p(G_{complete})} = \frac{b_p(G) - 1}{b_p(G_{path}) - 1} \quad (4)$$

where G_{path} and $G_{complete}$ have the same number of nodes as G .

2.2. Size of the giant component

An alternate method to assess robustness is to examine the decrease of the size of the giant component when a fraction f of nodes is isolated through an strategy-specific approach (Grubestic et al., 2008). To test network tolerance to errors, the nodes to isolate are selected at random and to test the network's tolerance to attacks the selected nodes must play a vital role in maintaining network connectivity (Albert et al., 2000). The simulation of an attack on an air transport network allows us to detect its critical airports in terms of network connectivity (Lordan et al., 2014b). To select the nodes to isolate, several node selection criteria can be adopted. For instance, Jahanpour and Chen (2013) define criteria based on degree, betweenness, closeness and eigenvector centralities. In this study the robustness to intentional attacks for each AARN attack will be analyzed using six different node selection criteria: *degree*, *betweenness*, *modal analysis* (Petreska et al., 2010), *damage* (Latora and Marchiori, 2005), *Bonacich power* (Bonacich, 1987) and *inverted efficiency*. For the first five criteria an adaptive strategy is adopted: each time a node is isolated the measure for node selection is recalculated for all the nodes that are still connected and the node with the highest value is selected to be disconnected in the following step. This analysis uses a new way to analyze the robustness of a network, named as *inverted efficiency*. For this purpose two new features are introduced altogether: the use of efficiency for assessing the robustness of a complex network and how to invert the adaptive strategy.

2.2.1. Efficiency

Latora and Marchiori (2001, 2003) introduced the efficiency of a network as an indicator of its own traffic capacity as:

$$E = \frac{1}{N(N-1)} \sum_{i \neq j} \frac{1}{d_{ij}} \quad (5)$$

In the robustness analysis carried out on the global air transport network (Lordan et al., 2014b) observed that the decrease in the efficiency of the network has a similar evolution to the decrease in the size of the giant component. Therefore, a promising criterion of node selection for maximizing attack effectiveness could be selecting the node whose disconnection causes the maximal decrease in efficiency. If an adaptive strategy is used, the decrease in efficiency caused by the isolation of each of the remaining nodes must be recalculated for the next iteration. Previous research (Petreska et al., 2010; Jahanpour and Chen, 2013; Lordan et al., 2014b) has used and created criteria based on node measures to attack the network. To our knowledge this is the first criterion that uses network measure for node isolation.

2.2.2. The inverted adaptive strategy: Inverting the procedure

When following an adaptive strategy, the usual (direct) procedure to attack a network consists of starting with the connected network, and then disconnecting nodes one by one –selected following a criterion recalculated for each disconnection– that might bring a decrease in the size of the giant component which is as large as possible, recalculating the value of the criterion for all remaining nodes each time a node is isolated. For each criterion it is possible to construct an inverted procedure, beginning with an isolated network and adding –*activating*– nodes and keeping the giant component as small as possible. The edges considered for computing the size of the giant component are those between activated nodes and the process ends when all the nodes in the original network are activated. The direct adaptive strategy starts with the original network and aims to disconnect the most central or important nodes *as soon as possible*, while the *inverted adaptive strategy* (IAS) presented starts from an empty network and aims to connect the most important nodes *as late as possible*.

A good starting point for an IAS is to compute the betweenness centrality for the nodes of the whole network and select, for activation, the nodes with

betweenness centrality equal to zero. These nodes are among the last ones to be disconnected with the usual direct procedures, and the network obtained by considering the edges linking these nodes should have a giant component with a value of zero or one. The node selection procedure will be different for criteria based on node measures and on network measures:

- *Node measures*: for node measures such as degree or betweenness the node to be selected in each step is the one that, when activated, has the smallest value of the measure among the non-activated nodes.
- *Network measures*: in the straight version of the network measures criteria, the node to be disconnected is the one whose disconnection minimizes network efficiency. For the IAS, the node to be activated will be the one whose activation maximizes network efficiency.

In the first activations of the IAS there can be a lot of equal measures between nodes. A possible criterion for distinguishing between these equal measures is to select the node with the lowest value of betweenness centrality in the initial network. For illustrative purposes, Figure 1 exemplifies this procedure, showing each step of an IAS based on the degree criterion. The graph to study is the one shown in Figure 1a. The first step is to take its nodes and generate an empty graph (see Figure 1b), where all nodes are deactivated. To initiate the process, the betweenness for all nodes of the original graph is calculated: $b_i = (26, 0, 0, 0, 0, 25, 8, 0, 0, 0)$. Then, all nodes with zero betweenness are activated (see Figure 1c).

Following the IAS, in each iteration the non-activated node with *minimum* degree has to be activated. For instance, in the first iteration the non-activated nodes are A, F and G (see Figure 1c). If A were activated its resulting degree would be 4 with A-B, A-C, A-J and A-I connections. In the same way the degrees of F and G would be 2 (F-E and F-D) and 1 (G-H) in this iteration, respectively. As G is one of the nodes with minimum degree it is the node to be activated in the first iteration (see Figure 1d) and only adding the connection G-H.

For the second iteration the non-activated nodes are only A and F. If activated, A would have a degree of 4 and F a degree of 3. Therefore, F is the node to activate in the second step (see Figure 1e). Finally, there is just A left to activate (see Figure 1f) and the process ends since all nodes have been activated.

3. Results

3.1. Topology of alliances' route networks

The three current global airline alliances (Star Alliance, SkyTeam and oneworld) have been included in the study. These three alliances offer around 9,136 routes, which represents 36% of the routes IN the global ATN. It must be said, however, that the routes offered by all alliances represent around two-thirds of total industry capacity (Gaggero and Bartolini, 2012). Therefore, routes operated by alliances are among the most important in terms of passengers and revenue in the entire airline industry.

An AARN has been constructed for each alliance in which the edges are the routes where at least one of the alliance members acts as the marketing airline and the nodes are the airports covered by the set of routes. Air route data have been obtained from the Schedule Reference Service (SRS), a neutral database of scheduled flights compiled by IATA (<http://www.iata.org/publications/srs/Pages/index.aspx>). Codesharing flights have been included considering that alliances are formed by airlines from all around the world and it would be difficult to find an area where they are not operating. Therefore, it has been considered that alliances have no spoke airports that depend on an intermediate hub. Airports are selected as nodes rather than cities, given that airports are the likely target of an intentional attack. The set of marketed routes is the route portfolio that the alliance offers to its customers and it therefore makes more sense to assess the robustness of this set instead of the smaller set of operating routes.

To define the network, a time horizon has been considered that includes the period from December 2011 to March 2012 and all alliances have a stable number of members. In this period three changes to alliance membership took place: Ethiopian Airlines (ET) became a member of Star Alliance in December 2011; in April 2012 bmi British Midland (BD) left Star Alliance; and Air Berlin (AB) entered oneworld. Therefore, the routes marketed by each AARN between December 2011 and March 2012 define the edges of each network that link to the operating airports. These routes have been obtained from the SRS database. As the majority of connections are reciprocal, the three alliance networks have been treated as an undirected network (Guimerà et al., 2005). The AARNs have been considered as unweighted networks, since the purpose of this research is to assess the effect of a total disconnection of airports from the alliance network.

A network’s vulnerability to errors and attacks depends on its topology. Scale-free networks, that is, networks whose degree distribution follows a power law, are usually resilient to errors but have low tolerance to attacks (Zanin and Lillo, 2013). Table 1 shows the values of the main topological properties for the three alliances. When compared with the global ATN (Lordan et al., 2014b), the AARNs have smaller values of average path length and L and higher values of clustering coefficient C (the ATN has $L = 3.94$ and $C = 0.64$). Thus, all the AARNs have the small-world property and also a high clustering coefficient.

Figure 2 shows the degree and betweenness cumulative distributions for each AARN, in a log-log scale. The three AARNs have a similar cumulative degree distribution (that is, the probability that a given node has a degree of value k), which follows a truncated power-law distribution but with a less stark truncation than that obtained for the global ATN. Similarly, the cumulative betweenness distribution but similar for the three AARNs, and also follows a truncated power-law distribution thus showing the presence of a subset of airports with high values of betweenness centrality for each alliance. Degree and betweenness cumulative distributions of alliances could be smoother than the ones for the global ATN for two reasons: on the one hand, a large set of airports with low degree (i.e., with few connections) present in the global ATN are not covered by airline alliances, and on the other hand, each alliance has a subset of airports with a high number of connections and high betweenness centrality, compared to the global ATN which includes all of them.

A distinctive feature for Star Alliance is shown in Figure 3, which compares the betweenness and the degree for each airport and each alliance. The Star Alliance graph shows a similar pattern to that observed for the global ATN (considering nodes as airports or nodes as cities as in Guimerà et al. (2005)): the appearance of nodes with a high value of betweenness and a low value of degree. In the other two graphs, however, a strong correlation between degree and betweenness can be observed, with no airports showing a pattern of low degree and high betweenness. On the other hand, Star Alliance has a more continuous distribution of degree and betweenness, while the other two alliances have airports with values of degree and betweenness that are much higher than the rest (i.e., one in the case of oneworld and three for SkyTeam).

3.2. Robustness of airline alliance route networks

Figure 4 shows the multi-scale vulnerability measures for the three alliances for values of p ranging from 1 to 50. In order to compare the vulnerability of each alliance the values of the multi-scales measures have been normalized following the procedure described in subsection 2.1. The results show that Star Alliance is the alliance with lowest values of vulnerability, followed by SkyTeam and oneworld, respectively. Therefore, according to this measure, oneworld seems to have the most vulnerable network and Star Alliance the most robust one.

Figure 5 shows an alternative assessment of the robustness of the alliances route network: the evolution of the size of the giant component when a fraction f of the nodes is isolated. The criteria used to select the nodes are described in subsection 2.2: *betweenness*, *degree*, *Bonacich power*, *damage*, *modal analysis* and *inverted efficiency*. As all node criteria disconnect the networks when $f > 9\%$, this value has been adopted as the threshold for Figure 5. At first glance, it can be seen that while node selection criteria give different results for Star Alliance and SkyTeam the results for all criteria are quite similar for oneworld. A possible explanation for the behavior of oneworld comes from its topological properties: Figure 3 shows that oneworld is the alliance whose betweenness and degree are most correlated as all its nodes with high degree have also high betweenness. It can also be observed that oneworld appears to be as the least robust network, as for $f \simeq 2.5$ the giant component has decreased significantly.

As for Star Alliance and SkyTeam, thenode selection criteria offer different results, with a similar pattern to the one obtained for the global ATN. The most effective criteria to select nodes to attack the Star Alliance and SkyTeam networks turns out to be betweenness and inverted efficiency (see Figure 5). In fact, it can be observed that inverted efficiency anticipates the significant falls in size of the giant component obtained with betweenness. For values of f around 2% and 2.5% inverted efficiency is the most effective criteria in both networks. The greater performance of betweenness compared to the rest of the criteria, except inverted efficiency for Star Alliance and SkyTeam can also be explained in terms of the degree vs betweenness graphs in Figure 3. Figure 6 shows the detailed decrease in the size of the giant component for $f \leq 2\%$. For low values of f , damage is the most effective way of attacking all AARN. More precisely, in all cases damage overcomes

the rest of the node selection criteria until the first break is obtained through betweenness and inverted efficiency.

The Star Alliance topology replicates, to some extent, a property observed in Guimerà et al. (2005) for the global ATN: the existence of central (i.e., high betweenness), low-connected (i.e., low degree) nodes. This property is less salient in the case of SkyTeam, but nevertheless this alliance also has a multicomunity structure where there are some central airports with a connectedness lower than expected, considering its network centrality.

From the results of the analysis reported in Figure 5, the most robust AARN to intentional attacks is the Star Alliance network, followed by SkyTeam and oneworld. Using the betweenness or inverted efficiency node selection criteria, the first network break –a significant decrease in the size of the giant component– occurs for values of $f \simeq 1.5\%$ for oneworld, $f \simeq 2\%$ for SkyTeam and $f \simeq 2.5\%$ for Star Alliance (for the first two alliances, the first break can be observed in detail in Figure 6). When attacked the size of the giant component of Star Alliance falls abruptly with one single break, while for the other alliances the disruption of the giant component occurs in two steps. Interestingly, the results of ranking the robustness of alliances by a decrease in size of the giant component are the same as the standardized multi-scale vulnerability (see Figure 4).

4. Conclusions

Airline alliances are an idiosyncratic mode of coordinating airline operations that allow airlines to provide customers worldwide mobility through collaboration with other airlines. The routes marketed by any of the members of the alliance define the airline alliance route network, or AARN. Although no alliance covers the entire global air transport network (ATN), all three alliances have a global reach and their routes are among the most important in the ATN, both by revenue and passengers transported. The AARNs are networks with a truncated power-law distribution, the small-world property (i.e., low average path length) and a high clustering coefficient. The Star Alliance network is the most similar to the global ATN, since it includes central airports (i.e., airports with high betweenness centrality) with low connectedness (i.e., with low degree). For SkyTeam and oneworld a strong correlation between node degree and betweenness is observed.

The robustness of AARNs has been analyzed through two methods: the multi-scale measure of vulnerability, defined in Boccaletti et al. (2007), and the study of the effect on the size of giant component of the isolation of a fraction f of the airports covered by the alliance following several node selection criteria. In order to allow a network vulnerability comparison, a normalization procedure has been defined for multi-scale vulnerability. To perform the latter analysis, the inverted adaptive strategy (IAS) for defining node selection criteria has been defined. Rather than starting with the connected network and trying to disconnect it *as soon as possible*, IAS starts with a disconnected network, and adds new nodes in order to connect the original network *as late as possible*. From the results of this robustness analysis of the global ATN, it is considered convenient to define a IAS in the analysis based on reducing network efficiency.

Both methods of assessing network vulnerability coincide in that the most robust AARN is the Star Alliance route network, followed by SkyTeam and oneworld. In all cases, the node selection criterion based on damage is the most effective for low values of f (around 2%), while betweenness and inverted efficiency are most effective for higher values of f (between 2% and 9%). The latter criteria disconnect the networks through breaks (abrupt reductions in the giant component). In fact, betweenness and inverted efficiency are the most effective for values of f when the first break occurs. The merit of the inverted efficiency criterion is that breaks appear before the betweenness criteria. Therefore, the former is the most effective for some ranges of f . Interestingly, Star Alliance has a single break of the giant component for $f \simeq 2.5\%$, while in the other two AARNs two breaks occur and of a size of around half the value of the break in Star Alliance.

Airline alliances have appeared for economic and operational reasons, since they allow airlines to benefit from economies of scale and density. A deeper insight into how AARNs are formed can include criteria based on robustness in the decisions shaping alliance evolution. Airlines seeking participation in an alliance should take into account the gain or loss of robustness of their marketed route network after joining an alliance. On the other hand, alliances seeking partners should balance the gain in coverage across the network with the variation in robustness of their AARN.

The results of the analysis reported in this study allow for the comparison of the results of robustness of the alliance route networks with those of the global ATN. The next step is to assess the robustness of individual airlines

route network. It must be noted that individual airlines have features that should make their network different from the AARNs and the global ATN. First, airline route networks do not have the global scope of alliances and second, airline route networks depend on the business model adopted by each airline.

References

- Albert, R., Jeong, H., Barabási, A.L., 2000. Error and attack tolerance of complex networks. *Nature* 406, 378–82. URL: <http://www.ncbi.nlm.nih.gov/pubmed/10935628>, doi:10.1038/35019019.
- Boccaletti, S., Buldú, J., Criado, R., Flores, J., Latora, V., Pello, J., Romance, M., 2007. Multiscale vulnerability of complex networks. *Chaos (Woodbury, N.Y.)* 17, 043110. URL: <http://www.ncbi.nlm.nih.gov/pubmed/18163774>, doi:10.1063/1.2801687.
- Bonacich, P., 1987. Power and centrality: A family of measures. *American journal of sociology* 92, 1170–1182. URL: <http://www.jstor.org/stable/10.2307/2780000>.
- Brueckner, J.K., 2001. The economics of international codesharing: an analysis of airline alliances. *International Journal of Industrial Organization* 19, 1475–1498. URL: <http://linkinghub.elsevier.com/retrieve/pii/S0167718700000680>, doi:10.1016/S0167-7187(00)00068-0.
- Brueckner, J.K., Lee, D.N., Singer, E.S., 2011. Alliances, Codesharing, Antitrust Immunity, and International Airfares: Do Previous Patterns Persist? *Journal of Competition Law and Economics* 7, 573–602. URL: <http://jcle.oxfordjournals.org/cgi/doi/10.1093/joclec/nhr005>, doi:10.1093/joclec/nhr005.
- Cardillo, A., Zanin, M., Gómez-Gardeñes, J., Romance, M., García del Amo, A.J., Boccaletti, S., 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, 23–33. URL: <http://link.springer.com/10.1140/epjst/e2013-01712-8>, doi:10.1140/epjst/e2013-01712-8.

- Gaggero, A.A., Bartolini, D., 2012. The Determinants of Airline Alliances. *Journal of Transport Economics and Policy* 46, 399–414. URL: <http://www.ingentaconnect.com/content/lse/jtep/2012/00000046/00000003/art00006>.
- Grubestic, T.H., Matisziw, T.C., Murray, a.T., Snediker, D., 2008. Comparative Approaches for Assessing Network Vulnerability. *International Regional Science Review* 31, 88–112. URL: <http://irx.sagepub.com/cgi/doi/10.1177/0160017607308679>, doi:10.1177/0160017607308679.
- Guimerà, R., Mossa, S., Turtschi, A., Amaral, L.a.N., 2005. The worldwide air transportation network: Anomalous centrality, community structure, and cities' global roles. *Proceedings of the National Academy of Sciences of the United States of America* 102, 7794–9. URL: <http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=1142352&tool=pmcentrez&rendertype=abstract>, doi:10.1073/pnas.0407994102.
- Jahanpour, E., Chen, X., 2013. Analysis of complex network performance and heuristic node removal strategies. *Communications in Non-linear Science and Numerical Simulation* 18, 3458–3468. URL: <http://linkinghub.elsevier.com/retrieve/pii/S1007570413002050>, doi:10.1016/j.cnsns.2013.04.030.
- Latora, V., Marchiori, M., 2001. Efficient Behavior of Small-World Networks. *Physical Review Letters* 87, 3–6. URL: <http://link.aps.org/doi/10.1103/PhysRevLett.87.198701>, doi:10.1103/PhysRevLett.87.198701.
- Latora, V., Marchiori, M., 2003. Economic small-world behavior in weighted networks. *The European Physical Journal B - Condensed Matter* 32, 249–263. URL: <http://www.springerlink.com/Index/10.1140/epjb/e2003-00095-5>, doi:10.1140/epjb/e2003-00095-5.
- Latora, V., Marchiori, M., 2005. Vulnerability and protection of infrastructure networks. *Physical Review E* 71, 015103. doi:10.1103/PhysRevE.71.015103.
- Lordan, O., Sallan, J.M., Simo, P., 2014a. 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, 112–120. doi:10.1016/j.jtrangeo.2014.04.015.
- Lordan, O., Sallan, J.M., Simo, P., Gonzalez-Prieto, D., 2014b. Robustness of the Air Transport Network. *Transportation Research Part E: Logistics and Transportation Review* doi:10.1016/j.tre.2014.05.011. In press.
- Mishkovski, I., Biey, M., Kocarev, L., 2011. Vulnerability of complex networks. *Communications in Nonlinear Science and Numerical Simulation* 16, 341–349. URL: <http://linkinghub.elsevier.com/retrieve/pii/S1007570410001607>, doi:10.1016/j.cnsns.2010.03.018.
- Petreska, I., Tomovski, I., Gutierrez, E., Kocarev, L., Bono, F., Poljansek, K., 2010. Application of modal analysis in assessing attack vulnerability of complex networks. *Communications in Nonlinear Science and Numerical Simulation* 15, 1008–1018. URL: <http://linkinghub.elsevier.com/retrieve/pii/S1007570409002639>, doi:10.1016/j.cnsns.2009.05.002.
- Wan, X., Zou, L., Dresner, M., 2009. Assessing the price effects of airline alliances on parallel routes. *Transportation Research Part E: Logistics and Transportation Review* 45, 627–641.
- Zanin, M., Lillo, F., 2013. Modelling the air transport with complex networks: A short review. *The European Physical Journal Special Topics* 215, 5–21. URL: <http://link.springer.com/10.1140/epjst/e2013-01711-9>, doi:10.1140/epjst/e2013-01711-9.

Figure 1: Example of the inverted adaptive strategy. *Grey circles*: activated; *white squares*: deactivated

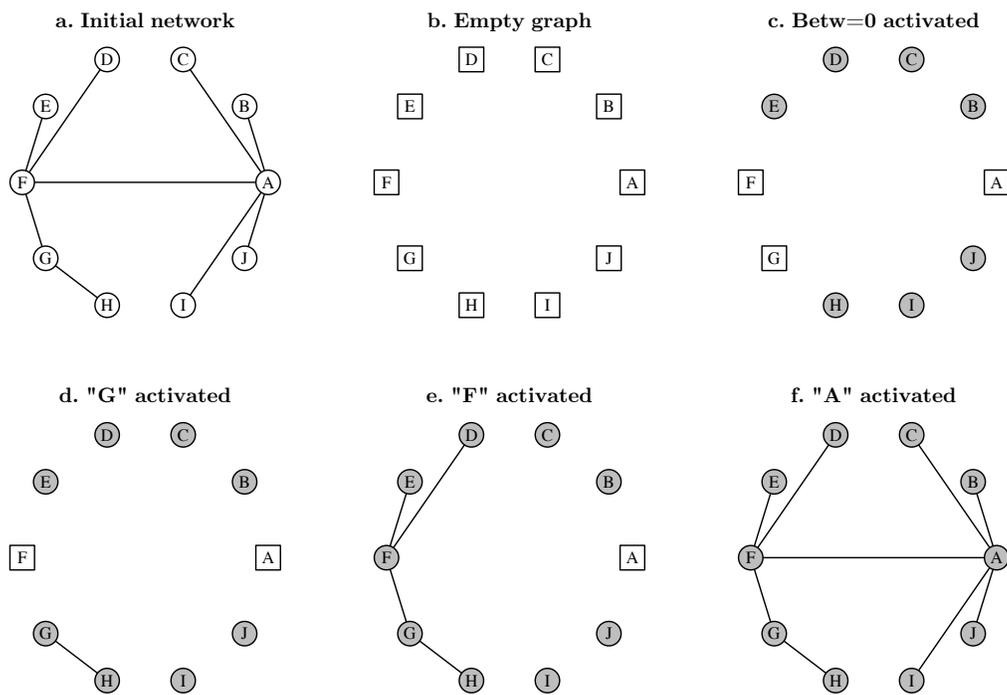
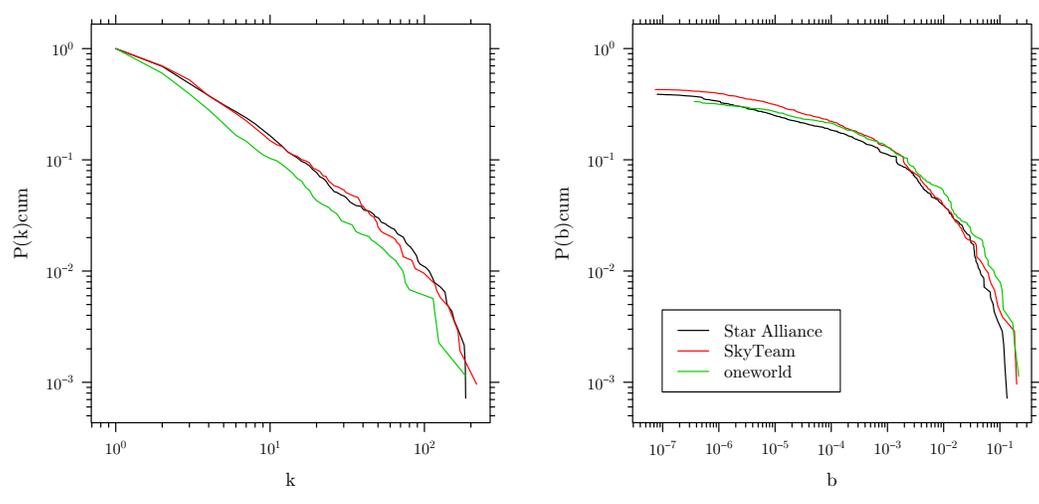


Figure 2: Degree (k) and betweenness (b) cumulative distributions for each alliance



	N	E	$\langle k \rangle$	L	C	ν
Star Alliance	1,150	4,240	7.37	3.24	0.77	< 0
SkyTeam	896	3,226	7.20	3.13	0.74	< 0
oneworld	741	1,670	4.51	3.28	0.71	< 0

Table 1: Main topological properties of AARNs. The quantities measured are: number of vertices N , number of edges E , characteristic path length L , clustering coefficient C , average degree $\langle k \rangle$, and type of correlations.

Figure 3: Betweenness (b) as a function of degree (k) for each alliance

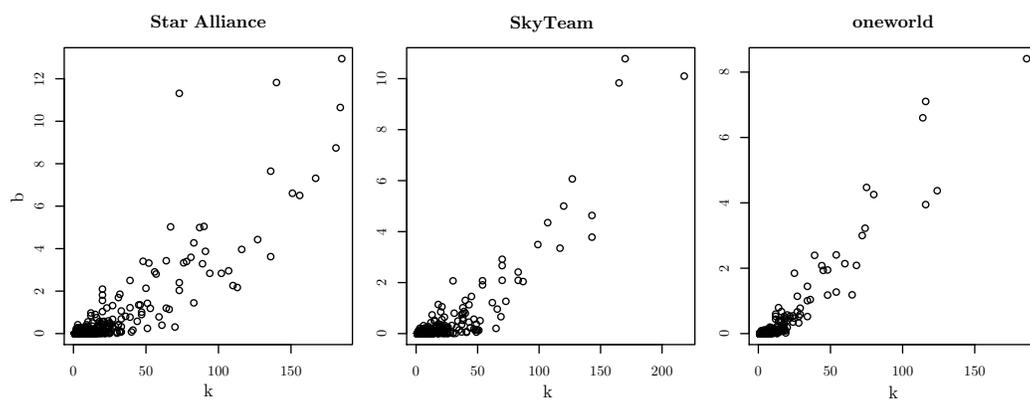


Figure 4: AARNs multi-scale vulnerability comparison

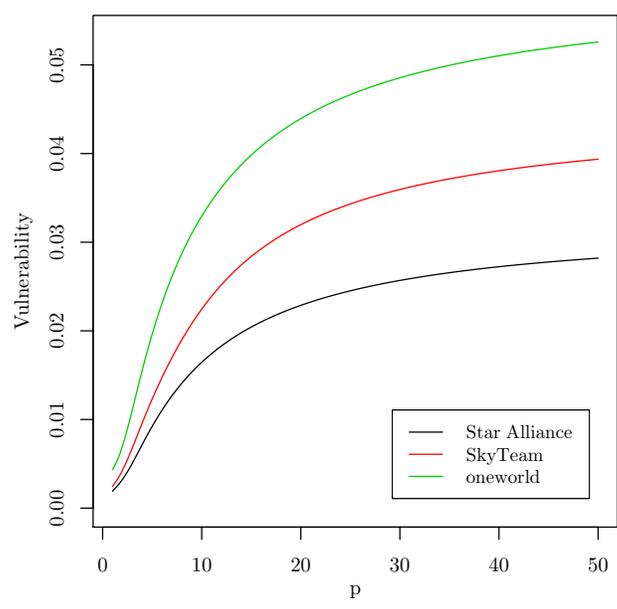


Figure 5: Vulnerability of AARNs $f \leq 9\%$

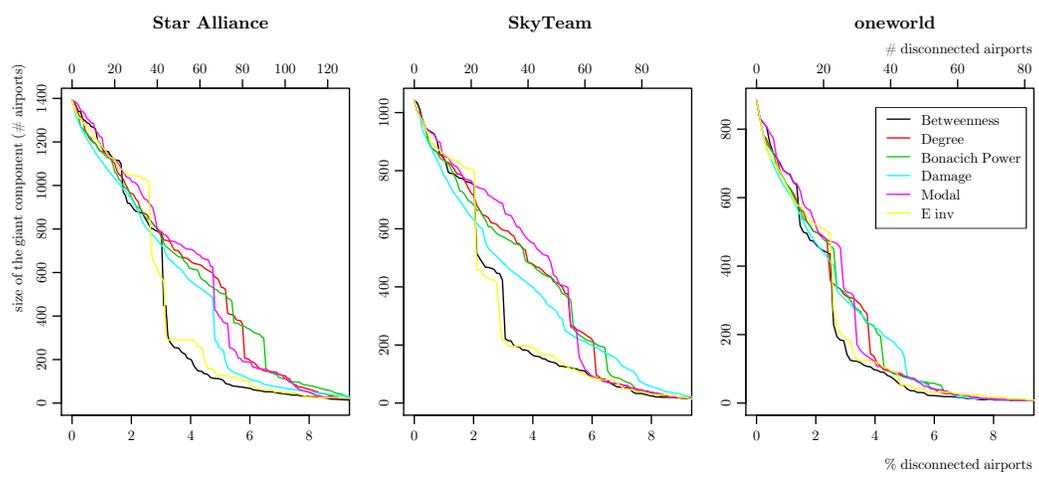


Figure 6: Vulnerability of AARNs. Detail: $f \leq 2\%$

