Netw Spat Econ (2015) 15:235–251
DOI 10.1007/s11067-014-9267-1

Network Hub Structure and Resilience

Morton E. O'Kelly

Published online: 18 September 2014

Abstract This article draws together specific results and facts relevant to a variety of networks (cyber and air) in the context of hubs and with a particular focus on their vulnerability and resilience. The paper highlights the features of networks that are exploitable to either detect or deter intrusions. This paper examines the vulnerability of hub interconnection points. The research points to parts of a network that require strengthened defenses to prevent loss or damage on a broader scale. A key aspect of the review is its emphasis on spatial organization.

Keyword Hub networks · Resilience · Vulnerability

1 Some Preliminary Definitions

Hubs are concentrator nodes that are critical to the continued operation of transportation and communication systems. The potential to disrupt a large amount of traffic by attacking hubs makes them a tempting target. It is clear that these potential disruptions impact businesses that rely on commercial interaction for business-to-business (B2B) and other critical communications (Campbell and O'Kelly 2012). This paper examines the vulnerability of hub interconnection points. The research points to parts of a network that require strengthened defenses to prevent loss or damage on a broader scale. While there have been numerous comprehensive reviews of many aspect of the vulnerability and resilience of complex networks, there are some important connections to be made from the perspective of hub network design. Much research is focused on complexity and physical transport infrastructure (Lordan et al. 2014) but with a broader perspective, it is apparent that significant contributions have been made by clusters of academics with a more general spatial view. These include groups such as Schintler et al. (2005 and 2007); Reggiani and Nijkamp and collaborators (see for example Reggiani and Nijkamp 2009 and 2012); and Murray and Grubesic and collaborators (see for example Murray and Grubesic 2007).

M. E. O'Kelly (✉)
Department of Geography, Center for Urban and Regional Analysis, The Ohio State University, Columbus, OH 43210, USA
e-mail: okelly.1@osu.edu

In defining concepts related to vulnerability, [e.g. robustness, resilience, redundancy, and reliability] there is a need to tolerate ambiguity and to recognize that what might appear to be end members of a continuum sometimes have subtle differences in interpretation, depending on the field of application. In broad terms vulnerability "is the state of susceptibility to harm from exposure to stresses associated with environmental and social change and from the absence of capacity to adapt" (Adger 2006). In the context of electric power grids, Holmgren (2007) states that "vulnerability is described as a susceptibility (sensitivity) to threats and hazards that substantially will reduce the ability of the system to maintain its intended function." The key to both views is that any attack that prevents the system from operating smoothly is problematic and the system's inability to adapt to this attack is at the heart of its vulnerability. Vulnerability and robustness are typically seen as complementary concepts; for example Sullivan et al. (2009) present a review related to the field of network-disruption analysis, including measures of network robustness and vulnerability. Others view robustness as a capability to withstand normal errors whereas vulnerability is a systemic weakness to determined attack (Barabási 2003, 118). Resilience according to the national infrastructure protection plan (Department of Homeland Security 2013), on the other hand, is "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions… [it] includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents." In a general sense then vulnerability is a lack of resilience or robustness (see also Holmgren 2007).

Reggiani (2013) provides a summary of the important terms such as network vulnerability, robustness, resilience, scale-free network and so on. For example, redundancy can mean wasteful excess but also has a close bearing on the idea of back up coverage and protection from exposure to a single bottleneck. A system with some built-in redundancy is capable of providing a good work-around in the event of a failure. A system with some redundancy can provide resilience (Fiksel 2003) leading to its longer term sustainability. Cardoso and Diniz (2009) show that there is a critical level of additional capacity that can protect vulnerable hubs. The availability of back-up solutions is dependent on the system operator providing something more than a bare bones infrastructure and in this sense redundant alternatives contribute to the system's resilience. There is a view that a little redundancy (which is the opposite of complete efficiency) gives networks a chance to survive (Reggiani et al. 2002). The paper referenced below has an interesting counter position – networks evolution rewards modularity, and that connected modules that are sparsely linked to distant modules are easy to repair (Clune et al. 2013). With these terms in hand, it is now possible to consider whether systems can be both vulnerable and resilient, or whether vulnerability itself is an antonym for resilience. Further discussion of this point in the context of actual networks follows below.

2 Types of Vulnerability

The goal is to learn about the resilience of the network, either in terms of links (such as bridges), or nodes (such as hubs), or both. Recognize that terms such as bridge, gateway, and hub can refer to both real physical transport infrastructure as well as

virtual entities that perform these functions in a more abstract way. Murray et al. (2008) provide a methodological overview for evaluating network infrastructure for potential vulnerabilities. Most network measurement and graph-theoretic analysis tools can be used to assess criticality (Grubesic et al. 2008).

2.1 Link Vulnerability

The reduction of a network's capability in response to selective deletion of one or more links is well-known and has been reported in Taaffe et al. (1996) as a fundamental problem in network analysis. A simple method of prioritizing links, for example, would be to count the number of times a link is needed as part of the critical paths between all pairs of nodes. A more technical idea would be to see the selection of the most critical link as the one whose removal would do the most damage – in other words this is a game played between the system operator and a malevolent opponent. Bell (2003) devises a very nice linear program for the non-congested case, and provides a convergent heuristic for the case with flow related costs. An interesting association is to consider the response of traffic flows to disruption and a return to equilibrium (Connors and Watling 2014).

Ip and Wang (2011, 189), while primarily discussing a road network; define survivability as dependent on the number of paths between nodes:

> "Thus, the resilience of a city node can be evaluated by the weighted average number of reliable passageways with all other city nodes in the networks. The network resilience can then be calculated by the weighted sum of the resilience of all nodes. To identify critical road lines or hub cities in networks, the concept of friability is proposed. This is defined as the reduction in total resilience upon removal of an edge or hub city."

The basics of network reliability are captured quite well in the preceding quotation. In fact since the earliest designs for ARPANET, the goals of survivable *connectivity* have been at the forefront of network architecture (see Kim 2012; Lei 2013). There are trade-offs of course. A complete set of connections (a clique) gives a node an easy way to reach every other node, and even if a few links are removed, there is a very high likelihood of a path remaining between nodes, over the surviving links. On the other hand a tree is exceptionally easy to break, as there is a critical role for every link in spanning the nodes.

In terms of moving material through a network of links, the maximum flow between a source and sink over a capacitated network is known to be the capacity of the minimum cut disconnecting the pair of places. Clearly two nodes can be disconnected if everything between them is obliterated, but the minimum cut result will indicate the *smallest* amount of capacity removal to accomplish the task (see Matisziw et al. 2007). Networks are sensitive to critical blocking points and analysis can identify bottlenecks that are especially critical locations on such networks (see recent work of Medal et al. 2011, on studies to reduce the risk of disruption to critical networked infrastructures). It is important to model and simulate these highest priority connections (see also Church and Scaparra 2007). The related idea of optimally splitting a budget between preparedness and recovery is discussed in Miller-Hooks et al. (2012).

2.2 Nodal Vulnerability

Research has also focused on the idea of *nodal* vulnerability. It is clear that damage to a node is, at least initially, a local effect. But, to the extent that the node plays a critical role in the operation of the entire network, the loss of that node is potentially harmful at the network or sector level. Furthermore, the network is vulnerable to the extent that the node that is damaged is a point of sorting, amalgamation, concentration, or distribution. As stated by the National Infrastructure Strategy [White House 2003]:

> "the challenges and uncertainties presented by critical nodes and single-points-of-failure within infrastructures, as well as increasing interdependencies that exist among the various infrastructure sectors both nationally and internationally. These interdependencies and key nodes are often difficult to identify and resolve, as are the cascading and cross-sector effects associated with their disruption."

Co-location of several important critical items can pose added challenges as shown in the discussion of critical Korean infrastructure (O'Kelly and Kim 2007). In the co-location case, flows between many origin–destination pairs are impacted. The special case of the port (a node which serves as a gateway) is analyzed in a creative fashion in Rose and Wie (2013) who develop a methodology for estimating the total economic consequences of a seaport disruption, factoring in the major types of resilience. The paper adds to the methodological toolkit by including input–output effects. A node with high importance might be expected to have high "betweenness" (Guimerà et al. 2005). A very useful assessment of nodal classification is in Fortunato (2010, 156) reviewing the work of Guimerà and Amaral (2005). While their conceptual analysis was not in a spatial context, their ideas of peripheral and central nodes resonate extremely well with actual air networks, as seen in the follow up work on air (Guimerà et al. 2005).

A particular technical aspect of network resilience is that networks might have the advantage of a form of combinatoric self-protection. The idea here is that a network has so many parts, that the effective selection of a large subset of these that would do serious damage is somewhat unlikely. The chances that the attacker could identify the best (from their view the most damaging) subset would require the enumeration of a large array of items. The range of impacts from most to least critical impact has been defined in work by O'Kelly and Kim (2007) as a type of resilience arising from the variance of the amount of damage that can be done to a portfolio.

2.3 Hub Vulnerability

Intense activity levels are inherent in a basic hub and spoke network (O'Kelly 1986). Hub networks exhibit a non-random pattern of node "degree" with some nodes exhibiting very high connectivity (the hubs) while most nodes have quite low numbers of links. An attack at a node chosen at random would most likely do little damage (because of the preponderance of low degree nodes); but a deliberately concerted effort to disable one of the very high degree nodes could be devastating (Albert et al. 2000). Hub nodes also have internal interaction between gates or termini (see O'Kelly 2010) which provides both a target and an opportunity for heightened scrutiny.

Hubs are not only the most obvious targets, but also are complex enough to contain the kinds of redundant systems that may make for quick recovery, assuming we view the hub as part of a larger metropolitan agglomeration. On 9/11, Manhattan suffered a lethal blow, and some networks [notably Verizon] were directly impacted, but at the same time the adjacency to replacement systems, and the cluster of technical workers in the greater metro area, provided strong evidence of the resilience of these networks. It is a fundamental business viability question to assess the location of nodes that need to be protected (as potential targets). This, in broad overview, is a key question in the rapidly emerging field of complex network analysis. Such concepts have been applied to the vulnerability of internet backbones as well as air transport systems. It is also clear that with the major shake-up in the telecomm industry, the number and location (and peering arrangements) between surviving telecomms in major markets makes the issue of redundancy and connectivity ever more important and consequential for business development. In fact, despite the reported benefits of peering arrangements, competitive disputes can lead to de-peering and "going it alone" by providing private networks (notably Google).

The hub and spoke system design has served well for several forms of transportation and communication as will be seen in some examples later in the paper. But it is obvious, now that security issues are heightened, that the exposure of large fractions of interactions to passage through a few key nodes, or along a single path, requires assessment in terms of risk and probability of failure (Kim and O'Kelly 2009). Any risk situation is a combination of the probability of the failure, the likely consequences of that failure, and the frequency of occurrence. It is also highly likely that risk and consequences are interdependent, especially for a malicious agent, as it is very probable that the attack would prioritize the highest valued targets.

Lewis (2006) argues that nodes (especially hubs and gateways) are more critical than links; the loss of a single hub located at the center of a star-shaped network will result in the complete failure of the connection. However, links that bridge (join two gateways) are also very critical to the interconnection of two sectors of the network. An issue that has also been relatively under-examined in the context of hubs is that the resulting sparse and efficient network gives an obvious shortest path, but pays no attention to the availability of back up routes. Thus, an added vulnerability of the hub system (at least in the pure single allocation form) is that there is a lack of redundant (or backup) alternatives. It is also extremely easy to use the assignment variables to know which links will be busy, and what pairs of interactions flow on them. This could make targeted disruption of key connections quite easy.

3 Complex Networks and Implications for Hubs

It is clear that hubs have higher connectivity than expected in a random network, and are critical connecting points. Lewis (2006) argues that the hub structure of most sectors is important to the goal of protecting critical infrastructure: networks are studied to reveal useful information to enhance security and safety. One of the critical observations is that hubs have much higher degrees and that is consistent with the "fat tail" in a power law. There is some confusion however about what useful properties networks have when they are "scale free" or what advantage a network might possess from

having an empirical power law function fitted to its degree distribution. There are also potential sources of confusion from results devised in Cyber networks versus those applicable to other physical networks.

The first step here is to consider the process by which hubs emerge (sometimes referred to as preferential attachment). Hub-based networks have numerous high degree nodes. The most straightforward argument is that the network begins with some small number of nodes, and new portions of the system are built to join onto the existing clusters. We see this in the evolutionary examples presented by Levinson (2005) and when existing structures merge. An early effort on this front was developed by O'Kelly and Grubesic (2002) at the time of the first wave of internet backbone expansion through added networks.

Such a process naturally confers very strong benefits to the members of the structure who are already there (assuming this is a benign network) or alternatively exposes them to more harm if the added nodes bring more disease or malicious intent. The process is defined on a set of ever expanding nodes, and at each time the incremental nodes join with other new or existing nodes. Nodes may start out as "percolated" isolated clusters that perhaps join with random partners in their group, but over time these clusters find ways to reach out to the other emerging clusters (forming small worlds). The nodes begin to have strong incentives to attach to clusters of existing strong nodes, especially to make sure that there is a path to other major users.

3.1 Various Interpretations of Scale Free

Barabási's scale-free networks are networks where most nodes are connected to a small number of hub nodes. The modal degree of an individual node is small (i.e. it has a small number of links). A few super nodes (hubs) become highly focused points of interconnection (Memphis in the Fed Ex system, or Atlanta in the Delta system). A potential process that leads to scale-free networks occurs when joining nodes; by repeatedly applying an organizing principle that favors nodes with more than average number of links super hubs emerge (Barabási 2003). This is variously described as a rich club phenomenon; or more precisely as a result of network economies. But these hubs are not the only major nodes, and large scale hub networks often have additional hubs that are interlinked by a high capacity backbone.

Reggiani's (2013) use of the term scale free is perhaps best related to the literature on self-organizing (and fractal) systems where the same pattern slope is demonstrated whether one looks at the curve in the macro sense or zooms in to a small patch of it. Another way the term scale free arises is to note that the power function is invariant under a multiplicative change of units (a fact noted by Fotheringham and O'Kelly (1989) as a useful feature of the power distance decay function in spatial interaction; for example the gravity model with a power function will yield the same results whether the units are in kilometers or miles). Note that such a property does not hold for exponential decay; those functions are invariant under an additive transformation of the values (as opposed to a multiplicative one).

3.2 Small World?

Watts (1999) defines a small world network as a network that is (1) large, (2) sparse, (3) lacking a single dominant node but with clusters of nodes, and (4) there are relatively

short paths from one node to another. They are also characterized by the well-known idea that there are connections between every node and others in the system by surprisingly few steps, e.g. no more than 6 links separate every pair of nodes. Many hubs-based airline passenger networks have the majority of pairs connected by even fewer steps. A recent air access[1] map shows that about 2/3rds of US air passengers reach their destinations on non-stop trips, which may appear high but is related to the percentage of traffic originating at major hub cities with excellent air service [Source: Q1 BTS data for 2011; air access web site]. Most other passengers have a one stop trip, and only the most peripheral small regional airports require multiple steps to reach destinations. The reason this occurs is that all these systems benefit from a local structure that is connected by short cuts to the rest of the world. The bridge lines that connect systems through gateways are arguably the most important points of pressure in a small world system. Interrupting these links could destroy the small-world property. Without the short cuts, the system degrades to a series of locally connected neighborhoods; see Newman, 2006b.

3.3 Where do Hub Networks Fit In?

One compromise interpretation is to see transport hub networks as a hybrid of both small world and power law systems. Kuby et al. (2009) point out that the general problems are complex networks systems, of which small world and power law networks are separate instances with their own generating mechanisms. Clarification of whether these concepts are directly applicable to the hub network, and its vulnerability / resilience, is part of the overall aim of this paper.

As expected from consideration of real world aviation and other transportation economic factors, the idealized networks from first principles do not necessarily match well to actual systems. Actual hub networks in air systems (particularly air express) are like a series of trees rooted at the hubs (stars) but in turn interconnected to each other. As explained for example in Barthelemy's (2011) comprehensive review, there are many complicating factors in making path length or connection calculations for an open region. Some nodes have extensive connections to the rest of the world, confounding the effects of very long range paths. Barthelemy (2011) points out those large hubs, with many intercontinental connections to other hubs, can distort results for a regional analysis. Hubs of these systems are precisely the nodes likely to be connected to other hubs (see O'Kelly 2014 for a map of the interhub connection backbone network of FedEx). A clear illustration of this issue occurs in Fagiolo et al. (2009, 116) where the hubs are not directly connected to each other, in general, and indeed tend to require a connection through other non-hub nodes. The absence of a special backbone connecting the hubs is a critical omission from a transport point of view.

A hub based system is notably vulnerable at the points of convergence. It is hard to imagine a skilled attacker making a random attack on such a network: they are very likely to have targeted attacks on (i) central nodes (D'Agostino and Scala 2014, 21); (ii) the inter-hub links; or, (iii) the channels to the nerve center of the network. For this reason, papers that talk about efforts to protect, harden, or to prevent percolation or interdiction

[1] Accessibility mapping system: http://www.geography.osu.edu/aviation/main/accessibility_map.html.

are quite relevant. Nevertheless, Lewis (2009) shows that networks with protected hubs are the least susceptible to percolation and breakage, because (a) they can easily survive random (ineffective) attacks, and (b) more significantly, they can be protected against the inevitable focused attack on the hub. (See also Cardoso and Diniz 2009.)

3.4 Spatial Aspects of the Network

As is well-known, a star network (basically a one-hub design) random node removal will destroy global connectivity if the single hub is removed or when almost all the spoke-nodes are removed. Paul, Sreenivasan and Stanley (2005) carefully examine the fraction of nodes which must be randomly removed before global connectivity is lost. A nice extension of this idea to what basically amounts to a "protocol A" network (all nodes are connected to one out of a number of fully interconnected hubs; these hubs have higher degrees [O'Kelly and Miller 1994). The issue of the network failure is basically the question of whether the entire set of spoke cities can be expected to fail before the subset of higher degree hubs fail. However, O'Kelly, Kim and Kim (2006) conducted a study of internet reliability (in 2003) that modified the usual simple assumption that network nodes are vulnerable to closure by accidents or attacks. Instead of an all-or-nothing assumption, a form of cooperative peering was used, making it less likely that an entire network node could be disabled. Initial studies that sought the ease of breaking a scale free network, as reported by Barabási, show that power law governed scale free networks, with an exponent parameter less than 3, is basically unbreakable until almost all the nodes are removed. This result is perhaps over-interpreted by Lewis (2006) when he reports the results but ignores the restriction on the parameter. In fact many of the sample networks in Lewis have parameter values that are widely different from the theoretical norms (a fact that is acknowledged in the text). In some ways Lewis and others get the results right but without necessarily pinning down the appropriate mechanisms. It seems that hubs are both the source of resilience and the focus of vulnerability.

So, unifying the results, and essentially confirming the idea of Barabási, a node failure with sufficiently high criticality can cause immense damage, but a large number of nodes can be taken out with only low impact effects. The goal would be to disguise the criticality of the node, or to spread the risk by mirroring / replication of the system and enhanced peering to maximize resilience.

3.5 Survivability

Other work has examined the probability that focused attack on subsets of the key nodes would render the network inoperable. O'Kelly, Kim and Kim (2006) showed that the Internet has great resilience against accidental disruption or even targeted attacks by terrorists; they found that because of connections within and between Internet nodes, connectivity could be maintained.

The relatively small number of global domain name server (DNS) locations offers the potential to attack the entire system. However, the internet has demonstrated resilience against accidental and deliberate attempts at disruption; one noted example was a failed effort to swamp major routers because the un-attacked set survived (Slater 2002). Networks in a geo-spatial context have clues that can lead to enhanced security

and safety; this is something that is obvious from studying networks with critical nodes. A number of authors in a variety of disciplines have stressed the emergence of spatial networks as providing a very rich source of hypotheses as well as action items for protection of such networks (e.g. Morris and Barthelemy 2014; on complex networks; Barthelemy, 2011 on spatial networks; Newman (2006a, b), on the structure and function of networks; Beauguitte and Ducruet (2011) on relevant geographic theory; and recent work of Ducruet and Beauguitte (2014) on spatial science and network science).

If the network is required to provide an almost independent or redundant second path, these networks have what might be best thought of as meshed neighbors, where the degrees of separation are in fact 2 or 3. As networks are allowed to be less than fully connected (e.g. a partial backbone) it is not surprising that there are some path lengths that increase to 3, 4, or even 5 stages. Linking assets with secure, reliable and redundant communications requires a focus on network design that exploits the efficiency of centralized hubs. Some advantages of co-location and protection are afforded by secure "telecom hotels" but at the same time there is a need to prevent placing all the assets in the same easy-to-identify target. A study of Korean internet backbones suggests that the system had that kind of exposure to concentrated attack, and subsequent attacks confirm the vulnerability (Kim and O'Kelly 2009).

The failure, so far, of simultaneously knocking out the global system of top level DNS has provided a testimony to the physical design and structural benefits of the internet (Grubesic et al. 2003). On the other hand, the ease with which software exploits can infiltrate the system has only been reinforced over time. Despite the recognition at high levels of cybersecurity and telecommunications within the Department of Homeland Security (DHS) hardly a week goes by without renewed concern over the perils of hacking, cyber theft, and disruptive DOS attacks. The disconnect between resilient hardware and network architecture was foreshadowed by Malecki (2002) and Gorman (2004). A detailed study of the issues is in Tranos (2013).

4 Examples

This section provides some brief examples from cyber-networks and air transportation. While both systems use networks that are highly relevant to the theme of this paper, there are some particular aspects of their set-up that allow some generalizations to be drawn. In the case of cyber networks, interconnections between brands of network occur at peering points. In the case of aviation the network attracts users (passengers) to the system, in part on the basis of its convenience. For that reason the network has to provide more types of connections than the minimum. Hubs for air express are delivery systems under the unified routing and control of a single planner / operator, and so may very well provide the most clear cut examples of cost minimization. The implications for the resilience (or otherwise) may be determined from fairly simple analysis of the degree distributions.

4.1 Cyber-Networks and Peering

Simulations of a realistic set of closure scenarios, including partial and multiple simultaneous attacks are now routinely examined in the literature, including a very

useful empirical demonstration of simultaneous attacks on root servers (Slater 2002). When we seek to examine the impact of a series of different closures, it is important to be able to examine the closure without permanently removing the node or altering the data structure. In principle all linked networks can potentially be connected, yet these may be also partially disconnected as a result of attack or damage. When two networks share a common node, the easiest case is to assume that both can connect (peer) there. Unfortunately, that crude assumption only allows for all-or-nothing functionality at a node, and as mentioned in the introduction, large interconnection nodes actually have diverse connections, which can be an advantage in terms of recovery. An improved strategy is to create an artificial set of interconnection links at the node and examine the connectivity with both the default full connection assumption, and some partial (probabilistically controlled) closure assumptions. This is somewhat like a technique in traffic engineering where intersections and junctions are modeled as a set of dummy links with weights to reflect the turn penalties. In essence, if the turn penalty is increased to a very large level, one can block selected movements. The sub-networks within a city/metro region can be modeled as a set of connections – the maximum fully meshed (all peer) assumption is a simple special case.

The literature has begun to address a more realistic probabilistic failure model. A plausible simulation scenario is that the networks' ability to interconnect is stochastically degraded. A city where three networks have linkages, and hence act as an interchange point, could technically be limited to a subset of these interconnections. How many (or what fraction) of the peering arrangements would have to be disrupted to make a network begin to break into disconnected components? This is an extension to "percolation" as studied by Barabási and Bonabeau (2003). Simulations by Kim (2012) and others have tackled the issue of multiple types of networks and their spatial coincidence in a few key cities together with a means to block fractions of the inter-net linkages.

4.2 Passenger Transport Hubs

Air passenger transportation increasingly relies on hubs to provide a one- or two-stop path between almost all the interacting nodes at a continental scale. Such a high level of service would not be viable without the switching and routing functions of hubs. The placement of these hubs in cities that are also major traffic generators and attractors means that many hub based airlines can accommodate a large portion of their hub-originating traffic with excellent service (e.g. Chicago, Atlanta, …). Hubs are among the highest hierarchical level facilities, with many more linkages than the standard spoke cities. Useful analysis of these services can be accomplished with various power laws. Advice on the empirical analysis of various forms of the functions fitted to these data is provided in Adamic and Huberman (2002), Adamic (2006) and Reggiani and Nijkamp (2012). In addition there are comprehensive empirical cases (e.g. for Lufthansa: Reggiani et al. 2009) and also good overviews of related comparative results (Lordan et al. 2014).

In practice, there are many complications in the data. Most US airports have multiple serving airlines, and many nodes are connected to one or more of the hubs of each airline. In other words the nodes (even the non-hub nodes) have a large number of connections, once the services of several carriers are combined. In addition, it makes

sense to analyze the specific degree of the node on a particular carrier (say Delta Airlines) and perhaps in aggregate for all carriers. (See the excellent work of Cardillo et al. 2013, who analyze the combined properties of networks in combination for European systems.) A very simple attempt to fit a power law to the resulting degree distribution (i.e. the proportion of nodes with degree 1, 2, …) shows that a power law fits quite well (see Fig. 1). The links column shows how many of the links are accounted for by nodes with degree 1, 2, 3, …: of the 1849 links in the system, 208 originate at Atlanta, clearly two orders of magnitude greater than the lowest nodes. In the specific case of Delta, as well as one very large node there are significant numbers of nodes with much higher degree than expected from the power law (see the departures above the trend line on the left side of Fig. 1). These are listed as the top rated nodes in Table 1. It seems that the hub and spoke system is not perfectly suited to the power law scale free hypothesis but the fitted parameter falls well within the range of the standard model. Particularly notable is the heavy concentration of observations with lower degrees (the right hand tail of the chart in Fig. 1).

The results fit the case of Paul, Sreenivasan and Stanley (2005) who modified the power law idea to include two types of nodes – a large number of lower degree nodes and a small number of higher degree hubs. This seems much more relevant to the air hub system, and the hub-property of such a system is useful; a very high proportion of the nodes have degree 1, 2, or 3 (meaning that Delta only flies from these nodes to a few places). For this strategy to work in providing connectivity, these nodes have to join some common interchange points – hubs where passengers can be routed to their actual destination.

4.3 Freight Transport Hubs

Real networks for aviation have multiple nodes with very high degree. The recent paper of O'Kelly (2014) shows maps of several Federal Express Hubs each of which is connected to multiple origin cities as well as meshed together with the other hubs (see Table 1). The resultant paths are typically no more than 2 or 3 hops from origin to destination, so that the network has a more intensive small world property than the social networks studied by Watts (1999). [For another air freight example see: Dang and Peng 2012.] The short cuts between systems might be thought of as the intercontinental long range gateway-to-gateway connections (e.g. Memphis (MEM) to Paris (CDG)). An especially useful review of these long range paths, and their importance, is given in Bowen (2012).

A new analysis, computed for this paper, shows the following characteristics of the Fed Ex System, from actual daily operational data over 1 year, (180,000 flights). The data include the out degree from each city to any place that is connected, so long as the origin is in the US or its territories. (Thus the network has only a partial view of the rest of the world.)

The method is to count the number of links from each origin, and then to count the number of places with degree 1, 2, 3. The nodes column shows how many of the $n=$ 162 vertices, 154 have degree of 8 or less. The links column shows how many of the links are accounted for by nodes with degree 1, 2, 3. Of the 775 links in the system, 140 originate at Memphis, clearly two orders of magnitude greater than the lowest nodes, as

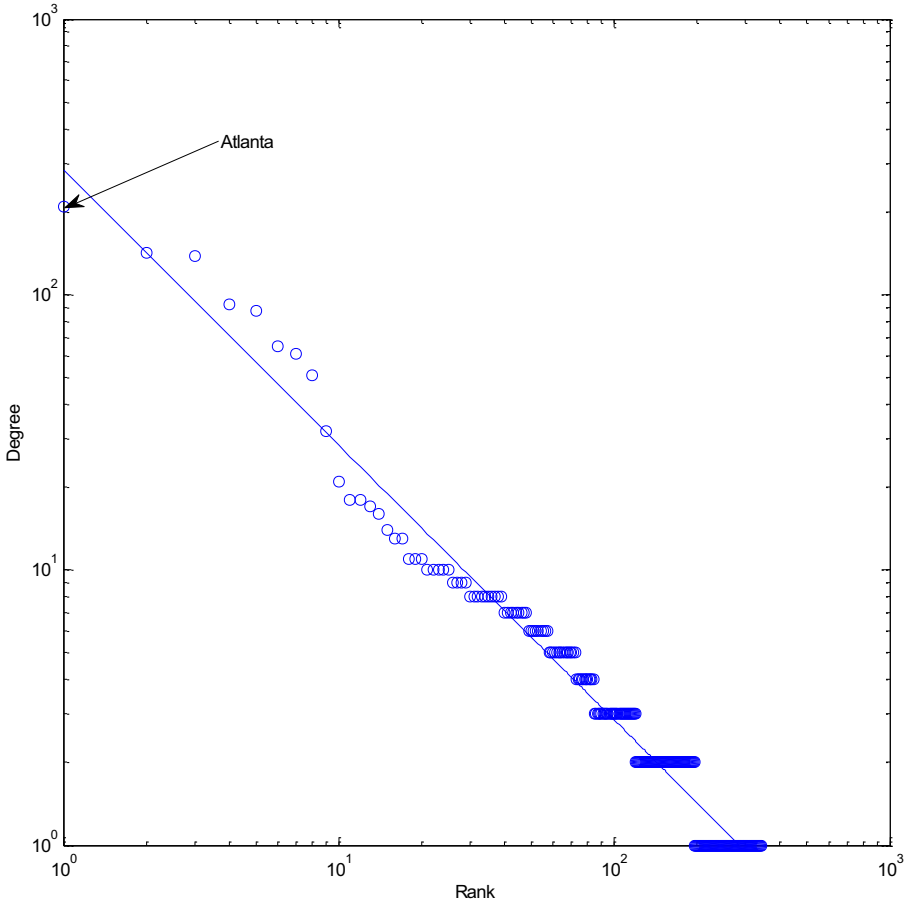

Fig. 1 Delta N=342 nodal degree distribution vs rank (Zipf) fitted with a power function. Source: Author's calculations from OAG data. Slope=−0.9980 which is consistent with a power law shape parameter of (1+1/0.998)=2.002. R-square is 0.9693

shown in Table 1 and Fig. 2. About half of all the links originate at places with degree less than 6. Such networks, provided they are not dominated by just a single hub, are in a class of networks that are both well connected and capable of survival. A dominant hub in air passenger transport (such as Atlanta) or air freight (such as Memphis) is clearly vital to the operation of their respective networks. Air transport systems have made some effort to guard against these vulnerabilities, for example in the case of FedEx having a second major hub in the same general region as the first (i.e. Indianapolis).

5 Summary and Conclusion

Hubs can provide a place where the "normal" trade dyads are stable and well-understood; (passengers transit through a hub from A to B in normal traffic). Hubs are the obvious

Table 1 Delta (N=342) and FedEx (N=162) nodal degree distribution

DELTA			FEDEX		
Name or Count of nodes	Rank	Degree	Name or Count of nodes	Rank	Degree
Atlanta	1	208	Memphis	1	140
Detroit	2	142	Indianapolis	2	58
Minn-St Paul	3	138	Oakland	3	24
JFK	4	92	Newark	4	23
Salt Lake City	5	87	Dallas/Fort Worth	5	20
LaGuardia	6	65	LA	6	15
Memphis	7	61	Anchorage	7	13
Cincinnati	8	51	Denver	8	12
	…			…	
35 nodes	85…119	3	27 nodes	63…89	3
76 nodes	120…195	2	36 nodes	90…125	2
147 nodes	196… 342	1	37 nodes	126…162	1

Source: Author's calculations from OAG for Delta and the FlightAware 1 year data reported in O'Kelly (2014) for FedEx

place to assess and measure the highest levels of interaction, and intercept movement, as well as the useful by-product of protecting the hub as a destination in its own right. Perhaps an even more important node is the gateway – a special node that acts as an entry or exit point to or from a region. Typically these are major points of embarkation and have customs/immigration officials at each end. (Amsterdam=KLM gateway to Europe; MSP=a significant gateway for the former NWA (now Delta) with historically very strong ties to Asia). They can therefore provide excellent barrier point to control inflow.

Hubs … "determine the structural stability, dynamic behavior, robustness, and error and attack tolerance of real networks. They stand as proof of the highly important organizing principles that govern network evolution" Barabási (2003, 72). As is expected by geographers, hubs are central switching points and represent locations through which a great deal of the interaction in a system connects.

The probability of finding nodes with a large number of links is significant, in contrast to random networks, where it is rare to find a node with a large number of links. In random nets, most nodes have a few links; power law distributions are characteristic of internet backbones. In retrospect, and as discussed in Barabási, it really never made much sense to expect that the Erdos/Renyi random connection model would apply to physical internet backbones, where a significant number of backbone nodes have a large number of links and the average number of links is not especially significant (hence Barabási and Bonabeau (2003) call such networks "scale free").

A hub is vulnerable to a non-random attack (because of its high degree). It is important to note that simply labeling the network as scale free is not essential to the analysis of the network's resilience. We can certainly surmise some important properties if the network complies exactly with the process, but one is often left with the impression that the scale free property is somewhat of a magical numerical code. Many analyses of scale free networks consider the nodes degree of connection to other nodes,

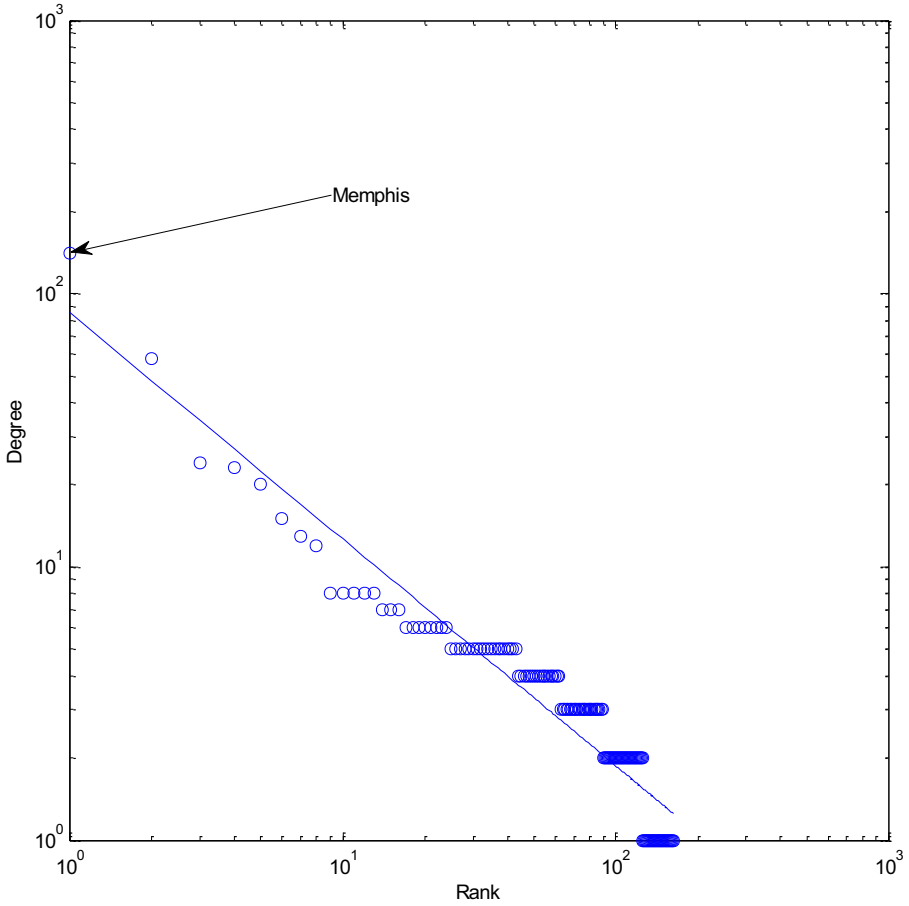

Fig. 2 FedEx $N=162$ nodal degree distribution vs rank (Zipf) fitted with a power function. Source: Author's calculations from the FlightAware 1 year data reported in O'Kelly (2014). Slope=−0.8296 which is consistent with a power law shape parameter of (1+1/.8296)=2.2054. R-square is 0.9077

and do not model the fact that the highly connected nodes (hubs) act as switching points for flows through the hubs. Power law obeying networks have resilience to random attack. This paper has shown that air passenger, air freight, and other actual transportation systems have strong features drawn from complex scale free networks. There remains a question, however, whether a scale free power law provides any real process explanation for nodes (the hubs) with high degree. It would seem to be very important to have a spatial explanation for how these special nodes are located, what their degree might be, and how they are connected to other nodes. In short, the network may provide both the target and the solution to the problem of security: as long as there are alternative paths to work around a disruption, failure, or compromised link, the network can continue to operate.

At the conclusion of the research, which has covered a rather wide range of material, one is left with a strong sense that much work remains to develop tactics and strategies for mitigating network problems. These efforts can range over identifying critical infrastructure, (Lei 2013); halting the spread of viruses in the networks (Dezso and

Barabási 2002); and, restoration of service in the aftermath of a problems (Matisziw et al. 2010). The high level of attention paid to these issues across an extremely wide array of disciplines is a positive sign that there is keen interest in solutions to handle many of these issues, such as assessment of architecture (Barrat et al. 2004) and halting epidemics in highly connected systems (Pastor-Satorras and Vespignani 2001). In general, the theme in Schintler et al. (2007) of moving from protection to resiliency sums up the problem rather well.

Acknowledgments Thanks to Yongha Park for excellent research assistance. Research on hubs is funded by Nextrans (086OY04 Air freight hubs and fuel use) and the National Science Foundation BCS-1125840. The author is especially grateful for the constructive comments from the referees.

References

Adamic LA (2006) Zipf, Power-laws, and Pareto - a ranking tutorial. Information Dynamics Lab, HP Labs, at http://www.hpl.hp.com/research/idl/papers/ranking/

Adamic LA, Huberman BA (2002) Zipf's law and the Internet. Glottometrics 3:143–150

Adger WN (2006) Vulnerability. Glob Environ Chang 16(3):268–281

Albert R, Jeong H, Barabási AL (2000) Error and attack tolerance of complex networks. Nature 406:378–382

Barabási AL (2003) Linked: how everything is connected to everything else and what it means for business, science, and everyday life. Plume, New York

Barabási AL, Bonabeau E (2003) Scale-free networks. Sci Am 288(5):60–69

Barrat A, Barthélemy M, Pastor-Satorras R, Vespignani A (2004) The architecture of complex weighted networks. Proc Natl Acad Sci 101:3747–3752

Barthélemy M (2011) Spatial networks. Phys Rep 499:1–101

Beauguitte L, Ducruet C (2011) Scale-free and small-world networks in geographical research: a critical examination. 17th European Colloquium on Theoretical and Quantitative Geography (ECTQG), Athens, pp 2–5

Bell Michael GH (2003) The use of game theory to measure the vulnerability of stochastic networks. IEEE Trans Reliab 52(1):63–68

Bowen JT (2012) A spatial analysis of FedEx and UPS: hubs, spokes, and network structure. J Transp Geogr 24:419–431

Campbell J, O'Kelly ME (2012) Twenty-Five Years of Hub Location Research. Transp Sci 46(2):153–169

Cardillo A, Gómez-Gardeñes J, Zanin M, Romance M, Papo D, Pozo F, Boccaletti S (2013) Emergence of network features from multiplexity. Sci Rep 3:1–6. doi:10.1038/srep01344

Cardoso JMP, Diniz PC (2009) Making Telecommunications Networks Resilient against Terrorist Attacks. In: Bier VM, Azaiez MN (eds) Game Theoretic Risk Analysis of Security. Springer, US, pp 1–23

Church RL, Scaparra MP (2007) Protecting Critical Assets: The r-Interdiction Median Problem with Fortification. Geogr Anal 39(2):129–146

Clune J, Mouret J-B, Lipson H. (2013) The evolutionary origins of modularity. Proc R Soc B 280: 1–9. 20122863, http://dx.doi.org/10.1098/rspb.2012.2863

Connors RD, Watling DP (2014) Assessing the Demand Vulnerability of Equilibrium Traffic Networks via Network Aggregation. Netw Spat Econ. doi:10.1007/s11067-014-9251-9 (forthcoming)

D'Agostino G, Scala A (2014) Networks of Networks: The Last Frontier of Complexity. Springer International, Switzerland

Dang Y, Peng L (2012) Hierarchy of Air Freight Transportation Network Based on Centrality Measure of Complex Networks. J Transp Syst Eng Inf Technol 12(3):109–114

Department of Homeland Security (2013) National Infrastructure protection plan (NIPP). Washington

Dezso Z, Barabási AL (2002) Halting viruses in scale-free networks. Phys Rev E 65(5):055103

Ducruet C, Beauguitte L (2014) Spatial Science and Network Science: Review and Outcomes of a Complex Relationship. Netw Spat Econ. doi:10.1007/s11067-013-9222-6 (forthcoming)

Fagiolo G, Valente M, Vriend NJ (2009) A Dynamic Model of Segregation in Small-World Networks. In: Ahmad K, Naimzada AK, Stefani S, Torriero A (eds) Networks, Topology and Dynamics. Springer, Berlin Heidelberg, pp 111–126

Fiksel J (2003) Designing resilient, sustainable systems. Environ Sci Technol 37:5330–5339
Fortunato S (2010) Community detection in graphs. Phys Rep 486(3):75–174
Fotheringham AS, O'Kelly ME (1989) Spatial interaction models: formulations and applications. Kluwer, Dordrecht
Gorman SP (2004) Networks, complexity, and security: the role of public policy in critical infrastructure protection. Dissertation, George Mason University
Grubesic TH, O'Kelly ME, Murray AT (2003) A geographic perspective on commercial Internet survivability. Telemat Inform 20:51–69
Grubesic TH, Matisziw TC, Murray AT, Snediker D (2008) Comparative Approaches for Assessing Network Vulnerability. Int Reg Sci Rev 31(1):88–112
Guimerà R, Amaral LAN (2005) Functional cartography of complex metabolic networks. Nature 433(7028): 895–900
Guimerà R, Mossa S, Turtschi A, Amaral LAN (2005) The Worldwide Air Transportation Network: Anomalous Centrality, Community Structure, and Cities' Global Roles. Proc Natl Acad Sci US Am 102(22):7794–7799
Holmgren AJ (2007) A Framework for Vulnerability Assessment of Electric Power Systems. In: Murray AT, Grubesic TH (eds) Critical Infrastructure. Springer, Berlin Heidelberg, pp 31–55
Ip WH, Wang D (2011) Resilience and friability of transportation networks: Evaluation, analysis and optimization. Syst J, IEEE 5(2):189–198
Kim H (2012) P-hub protection models for survivable hub network design. J Geogr Syst 14(4):437–461
Kim H, O'Kelly ME (2009) Reliable p-Hub Location Problems in Telecommunication Networks. Geogr Anal 41(3):283–306
Kuby MJ, Roberts TD, Upchurch CD, Tierney S (2009) Network Analysis. In: Kitchin R, Thrift N (eds) International Encyclopedia of Human Geography (Vol. 7). Elsevier, Oxford, pp 391–398
Lei TL (2013) Identifying Critical Facilities in Hub-and-Spoke Networks: A Hub Interdiction Median Problem. Geogr Anal 45(2):105–122
Levinson D (2005) The Evolution of Transport Networks. In: Button KJ, Hensher DA (eds) Handbook of Transport Strategy, Policy & Institutions: (Volume 6, Handbooks in Transport). Elsevier, Oxford, pp 175–188
Lewis TG (2006) Critical Infrastructure Protection in Homeland Security: defending a networked nation. Wiley, Hoboken
Lewis TG (2009) Network science: Theory and applications. Wiley, Hoboken
Lordan O, Sallan JM, Simo P (2014) Study of the topology and robustness of airline route networks from the complex network approach: a survey and research agenda. J Trans Geog 37:112–120
Malecki EJ (2002) The Economic Geography of the Internet's Infrastructure. Econ Geogr 78(4):399–424
Matisziw TC, Murray AT, Grubesic TH (2007) Bounding network interdiction vulnerability through cutset identification. In: Murray AT, Grubesic TH (eds) Critical Infrastructure: Reliability and Vulnerability (Advances in Spatial Science), Springer, Berlin, pp 243–256
Matisziw TC, Murray AT, Grubesic TH (2010) Strategic Network Restoration. Netw Spat Econ 10(3):345–361
Medal H, Sharp SJ, Pohl E, Rainwater C, Mason SJ (2011) Models for reducing the risk of critical networked infrastructures. Int J Risk Assess Manag 15(2):99–127
Miller-Hooks E, Zhang X, Faturechi R (2012) Measuring and maximizing resilience of freight transportation networks. Comput Oper Res 39(7):1633–1643
Morris RG, Barthelemy M (2014) Spatial Effects: Transport on Interdependent Networks. In: D'Agostino G, Scala A (eds) Networks of Networks: The Last Frontier of Complexity. Springer International, Switzerland, pp 145–162. doi:10.1007/978-3-319-03518-5_7
Murray AT, Grubesic TH (eds) (2007) Critical Infrastructure: Reliability and Vulnerability. Springer, Berlin Heidelberg
Murray AT, Matisziw TC, Grubesic TH (2008) A Methodological Overview of Network Vulnerability Analysis. Growth and Change 39(4):573–592
Newman MEJ (2006a) Power laws, Pareto distributions and Zipf's law. Contemp Phys 46(5):321–351
Newman MEJ (2006b) Modularity and community structure in networks. Proc Natl Acad Sci 103(23):8577–8582
O'Kelly ME (1986) Activity levels at hub facilities in interacting networks. Geogr Anal 18(4):343–356
O'Kelly ME (2010) Routing Traffic at Hub Facilities. Netw Spat Econ 10(2):173–191
O'Kelly ME (2014) Air Freight Hubs in the FedEx System: Analysis of Fuel Use. J Air Transp Manag 36:1–12
O'Kelly ME, Miller HJ (1994) The hub network design problem: a review and synthesis. J Transp Geogr 2(1): 31–40
O'Kelly ME, Grubesic TH (2002) Backbone topology, access, and the commercial Internet, 1997–2000. Environ Plan B 29(4):533–552

O'Kelly ME, Kim H (2007) Survivability of commercial backbones with peering: a case study of Korean networks. In: Murray AT, Grubesic TH (eds) Critical Infrastructure: Reliability and Vulnerability (Advances in Spatial Science). Springer, Berlin, pp 107–128

O'Kelly ME, Kim H, Kim C (2006) Internet reliability with realistic peering. Environ Plan B 33(3):325–343

Pastor-Satorras R, Vespignani A (2001) Epidemic spreading in scale-free networks. Phys Rev Lett 86(14): 3200–3203

Paul G, Sreenivasan S, Stanley HE (2005) Resilience of Complex Networks to Random Breakdown. Phys Rev E 72(5):056130. doi:10.1103/PhysRevE.72.056130

Reggiani A (2013) Network resilience for transport security: Some methodological considerations. Transp Policy 28(2):63–68

Reggiani A, Nijkamp P (eds) (2009) Complexity and Spatial Networks: In Search of Simplicity (Advances in Spatial Science). Springer, Berlin

Reggiani A and Nijkamp P (2012) Did Zipf anticipate socio-economic spatial networks, Quaderni Working Paper DSE No. 816.

Reggiani A, De Graaff T, Nijkamp P (2002) Resilience: An Evolutionary Approach to Spatial Economic Systems. Netw and Spat Econ 2(2):211–229

Reggiani A, Nijkamp P, Cento A (2009) Connectivity and Competition in Airline Networks: A Study of Lufthansa's Network. In: Vervest PHM, Liere VDW, Zheng L (eds) The Network Experience: New Value from Smart Business Networks. Springer, Berlin, pp 141–164

Rose A, Wei D (2013) Estimating the Economic Consequences of a Port Shutdown: The Special Role of Resilience. Econ Syst Res 25(2):212–232

Schintler LA, Gorman S, Reggiani A, Patuelli R, Gillespie A, Nijkamp P, Rutherford J (2005) Complex Network Phenomena in Telecommunication Systems. Netw and Spat Econ 5(4):351–370

Schintler LA, Gorman S, Kulkarni R, Stough R (2007) Moving from Protection to Resiliency: A Path to Securing Critical Infrastructure. In: Murray AT, Grubesic TH (eds) Critical Infrastructure: Reliability and Vulnerability (Advances in Spatial Science), Springer, Berlin, pp 291–307

Slater III, WF (2002) The Internet outage and attacks of October 2002. Chicago Chapter of the Internet Society 1–14. Nov 7

Sullivan J, Aultman-Hall L, Novak D (2009) A review of current practice in network disruption analysis and an assessment of the ability to account for isolating links in transportation networks. Transp Lett 1(4): 271–280

Taaffe EJ, Gauthier HL, O'Kelly ME (1996) Geography of transportation. Prentice Hall, Upper Saddle River

Tranos E (2013) The Geography of the Internet: Cities, Regions and Internet Infrastructure in Europe. Edward Elgar Publishing, Northampton

Watts DJ (1999) Networks, Dynamics, and the Small-World Phenomenon. Am J Soc 105(2):493–527

White House (2003) The national strategy for the physical protection of critical infrastructures and key assets. Washington DC. http://www.whitehouse.gov/pcipb/physical_strategy.pdf