Strategic Network Disruption

B. Hoyer[*,a], K. De Jaegher[b]

[a] Utrecht School of Economics, Utrecht University, Janskerkhof 12, 3512 BL, Utrecht, the Netherlands
[b] Utrecht School of Economics, Utrecht University, Janskerkhof 12, 3512 Bl, Utrecht, the Netherlands

Abstract

Networks are one of the essential building blocks of society. Not only do firms cooperate in R&D networks, but firms themselves may be seen as networks of information-exchanging workers. Social movements increasingly make use of networks to exchange information, just as on the negative side criminal and terrorist networks use them. However, the literature on networks has mainly focused on the cooperative side of networks and has so far neglected the competition side of networks. Networks themselves may face competition from actors with opposing interests to theirs. Several R&D networks may compete with one another. The firm as a network of employees obviously faces competition. Such network competition is what our paper is concerned with.

This paper investigates optimal network design when there are increasing benefits to linking nodes, while links are costly, and when the designer faces a strategic network disruptor, who is either able to delete a number of links or a number of nodes. A designer whose linking costs are low enough to fully protect the network builds a regular network that avoids local cliques connected by few links or few nodes, where a more narrow range of networks is optimal under node deletion. A designer whose linking costs are low enough such that he needs to sacrifice only one node, under link deletion builds a star-like network with a number of low-degree "weak" nodes, where the disruptor will be able to target one such weak spot. At the same time, there are high-degree "strong" nodes, which the disruptor can never delete. Under node deletion, the designer who is willing to sacrifice one node builds a regular network where each node is equally likely to be deleted. This is because under node deletion, high-degree nodes are a target for disruption. A designer whose linking costs are high under link deletion connects all nodes in a single network, namely the star. A designer whose linking costs are high under node deletion does not include all nodes, but instead excludes nodes to build a stronger, smaller component.

Key words: strategic network disruption, strategic network design, non-cooperative network games
JEL: C72, D85

[*] Corresponding author.
Email addresses: b.hoyer@uu.nl (B. Hoyer), K.Dejaegher@uu.nl (K. De Jaegher)

Preprint submitted to Singapore Multidisciplinary Decision Science Symposium *April 15, 2010*

1. Introduction

In the traditional economic model, the allocation of goods is based on competition on the market. Producers compete to sell goods, and consumers compete to buy them. Yet, when it comes to the allocation of information as a good, cooperation plays an important role. Through networks of friends and/or acquaintances, consumers exchang e information on e.g. the price and quality of goods (Goyal, 2009). Through e.g. R&D networks, firms exchange technological information (Bloch, 2002). Based on seminal papers by Jackson and Wolinsky (1996) and Bala and Goyal (2000)[1], this insight has lead to a large literature on network formation. With this literature has come the realization that networks are one of the essential building blocks of society. Not only do firms cooperate in R&D networks, but firms themselves may be seen as networks of information-exchanging workers. Social movements increasingly make use of networks to exchange information, just as on the negative side criminal and terrorist networks use them.
With a few exceptions, in its focus on cooperation, this literature has again paid too little attention to competition. Networks themselves may face competition from actors with opposing interests to theirs. Several R&D networks may compete with one another. The firm as a network of employees obviously faces competition. Politically opposed social movements compete with one another. Criminal and terrorist networks face security forces with interests diametrically opposed to theirs. Terrorists try to disrupt communication and transport networks.

All these examples may be referred to as *network competition*. This topic deserves special attention, because network competition has special features. Superficially, one could model the value of a network of information exchange depends strictly on the number of participants in the network. If one R&D network or network firm is able to lure a single participant away from a competing network, at first sight this would only seem to have a marginal effect. The same would seem to be true for the removal of single members from criminal and terrorist networks, or for the removal of single links from communication and transportation networks. Yet, it is a characteristic of networks that the removal of a single link or node from the network can have a vast impact on the value generated in the network. Clearly, if a network contains a single bridge node or bridge link that is the only means of one half of the network to talk to the other half, the removal of a single link or node will have a large rather than a marginal effect on the value of the network. It follows that the structure of a network matters for how severe the effect of network competition may be. Importantly then, networks that face competition will try to structure themselves in such a way that the effects of network formation are mitigated. Thus, the countering of the effects of network disruption may then become a driving force in network formation, and may have vastly different implications for the obtained network structures. For instance, if information decays the further it has to travel through the network, the star is an efficient network, as it brings all the players close to one another with a few links (Jackson and Wolinsky (1996) and Bala and Goyal (2000)). But with the minimal effort of removing a single node from the star, a disruptor can have maximal impact, in that there are no longer connections between nodes.

Network disruption so far has not received a lot of attention in the economics literature, but has been studied in other areas of research such as in crime network studies, internet security studies and studies on the reliability of road networks. Crime network studies have mostly focused on terrorist networks, such as for example, the paper by Enders and Su (2007). Here, however, the focus is specially on the secrecy that needs to be involved in the network, and the tradeoff between connectivity and security that evolves from that. Each terrorist cell should know as little as possible about any other, so that in case they are apprehended the security services can get as little information as possible. The interplay between a defense authority and an intelligent attacker in the context of terrorist attacks has also been studied by Bier et al. (2006). While their basic set up is similar to ours, their results are based on the assumptions that the network disruptor can only disrupt one target and that his goals and values are unknown. Internet networks have most often been studied as an example for so-called scale free networks. In an influential paper by Albert et al. (2000) it is shown that while these networks show a great tolerance towards random

[1] A critical appraisal of the theoretical literature on the economics of networks can be found in Jackson (2006).

errors, they are highly vulnerable to targeted attacks.[2] The literature on transportation- and road networks is mainly focused on random attacks and it deals in most parts with measures of accessibility of certain areas or towns and reliability of networks. A good, if a little outdated, review of what has been done can be found in Berdica (2002). A paper that is related to what we are doing here, in that it allows for extra links as a safety measure, is a study on rural Australian road networks by Taylor et al. (2006). They are, however, more interested in vulnerability measures of certain links and the effects on generalized costs of travel between two nodes, if a link should be disrupted.

Another paper that deals with network disruption, albeit in the field of engineering, is the work of Dekker and Colbert (2004). From a military perspective, and what they call Network Centric Warfare, they discuss the robustness of networks based on their graph topology. They reach similar conclusions about the topology of robust networks as we do, however, they do not consider the cost of linking, such that a large number of extra defensive links can be added, and that the network designer can assure that disruption is as small as it could possible be. This can be interpreted to correspond to one of the cases that we treat in this paper, namely the case of low linking costs. Still, even for low linking costs, in our paper the network designer does not want to waste any links. Further, Dekker and Colbert's focus is on showing that a particular set of graphs, namely graphs that have some of the different symmetry properties studied in graph theory, are robust to attacks. In particular, these are networks where nodes are similar, in that they have the same environment. Intuitively, there are no "weak spots" then in the network that are an easy target for attack. While our results for the case of low linking costs confirm this intuition, we also show that the set of robust graphs includes asymmetric graphs besides symmetric ones. The unifying characteristic of optimal graphs is that the network does not have local cliques with few links between them. Contrary to Dekker and Colbert, we further treat the case of high linking costs. In this case, the network designer finds it worth to put up with some disruption. If the network disruptor can delete links from the network, then the network designer will construct asymmetric networks with a star-like structure. Leaving many alternative weak spots for the disruptor means that he can only disrupt a few of them. If the network disruptor can instead delete nodes from the network, then the network designer will still construct networks that are roughly symmetric, and will not construct star-like networks. The designer may then even leave some nodes out of the network, to construct a smaller but more robust roughly symmetric network.

In economics, to the best of our knowledge, only few papers have dealt with the topic of network disruption by an intelligent adversary so far. One exception is the work by Baccara and Bar-Isaac (2008) in which they model a sequential move model between a legal authority and an organization in which links serve the purpose to transmit personal information about the members of the organization. Their model, however, deals with directed links and a repeated game and is therefore quite dissimilar to our work in terms of analysis and results. Instead of focussing on detection, in our model the network disruptor has already detected the network and we now focus on causing maximal damage to the network using minimal effort. Another paper in economics dealing with targeted network disruption is Ballester et al. (2006). Their network is a cooperation network, in that linked players play a game where their strategies are either strategic substitutes or strategic complements. We, on the other hand, deal with a communication network. Ballester et al. (2006) then define a *key player* in the network, whose disruption will cause maximal damage to the network. They also take into account a network planer's point of view, and therefore, just like we do, deal with optimality concerns of a collective outcome and not individual strategic considerations. However, they are more concerned with introducing a geometric characterization of this key player, which is based on a newly introduced intercentrality measure. This measure, unlike most other centrality measures, takes into account not only the player's centrality but also the way in which he contributes to the centrality of all other players.

A paper that is closer in terms of model set up is by Goyal and Vigier (2009). They consider a strategic interaction game between a network designer and an intelligent adversary. In the model, there is a group of homogeneous nodes that aims at performing a given task. Links between the nodes serve as a means of communication between the nodes. However, the group is facing an adversary that can detect nodes. Once detected, nodes are rendered unable to perform or communicate and also all nodes directly or indirectly

[2]For a more mathematical approach, resulting in the same conclusions, see Bollobás and Riordan (2003).

linked to the detected node are now detectable to the adversary. Goyal and Vigier show that when the designer has a possibility to defend certain nodes, highly connected hub-and-spoke networks are the most efficient solution. In their paper, protection is modeled very differently from our paper though. Whereas we use additional links to protect the network, that would be redundant when not facing an attack, they model protection as the network designer's ability to lessen the chances that a vulnerable node will be taken out. Thus while using a similar set up, we do not focus on the spread of infection but look for a robust network topology. Unlike them, we also do not limit ourselves to the deletion of nodes, but also deal with link deletion. We therefore reach different conclusions and also use different methods than they do.

To capture the basics of strategic network disruption, and strategic protection against network disruption, we set up the following simple game. At stage 1 of the game, a network designer constructs a pre-disruption network, with the purpose of achieving a high value of the network that will remain after the disruptor has deleted links or nodes, which takes place at stage 2. The designer structures the pre-disruption network in such a way to limit its vulnerability, where the designer may use any number of extra links over what is needed to connect all nodes, taking into account that linking is costly. The nodes in our game are therefore not individual players. Before one can think about the effects of network disruption on network formation by individual decision makers, one first needs to know as a benchmark case what is the best protective strategy for the network as a whole. This is the exercise undertaken in this paper.

The paper is structured as follows. In Section 2, we set up the formal model of this game. In Section 3, we then introduce a benchmark case without disruption, which is followed by dealing separately with two approaches to network disruption. First we investigate how to keep a certain size of a post-disruption network safe (Section 4) and then we turn to a fixed linking budget, for which we investigate the most robust network structures achievable (Section 5).

2. Model

We now turn to the concepts which formally describe this game. The two-player full information game is played by a network designer and a network disruptor. In stage 1, the network designer has a set of $N = \{1, ..., n\}$ homogeneous nodes available. The nodes are homogeneous in terms of value to the network as well as costs of linking them to each other. The network designer uses the nodes in N to build a pre-disruption network g^1. If two nodes i and j are directly linked, we say that $g^1_{ij} = 1$. If they are not linked to one another $g^1_{ij} = 0$.Given this notation, the pre-disruption network g^1 is the set of g^1_{ij} such that $g^1_{ij} = 1$ holds.[3] We denote the set of links by ℓ. Links are undirected so that $g^1_{ij} = g^1_{ji} = 1$ always holds. Nodes are indirectly linked to each other if a path exists between them. We assume that there exists a path between two nodes i and j if there exists a sequence of nodes $[i_1, ..., i_k]$ such that $g_{ii_1} = g_{i_1 i_2} = ... = g_{i_{k-1} i_k} = g_{i_k j} = 1$. We denote g^x_{-i} as network g^x with node i removed, and g^x_{-ij}, as network g with link ij removed.

At stage 2, the network disruptor observes the network and can then choose to disrupt it. We consider two models of network disruption, reflecting simply the constituting parts of any network. In the link deletion model, the disruptor can decide to delete a number of links from the pre-disruption network. This leads to a post-disruption network g^2 consisting of all the links for which $g^2_{ij} = 1$. In the node deletion model, the disruptor can decide to delete a subset v of nodes from the pre-disruption network, where $|v|$ denotes the cardinality of this set. The post-disruption network g^2 then consists of all links such that $g^2_{ij} = 1$, $i, j \notin v$. At stage 3, both players obtain their payoffs.

Define as $N_i(g)$ the set of nodes with whom node i maintains a (direct or indirect) link. Given a network g, a set $C \subset N$ is called a component of g if for every distinct pair of nodes i and j in C we have $j \in N_i(g)$, and there is no strict superset C′ of C for which this is true. The degree of connection of each node $\eta_i(g)$ is defined as the number of direct links the node has, so in effect the number of nodes it is directly linked with. The minimum degree of the graph, η_{min}, is the smallest degree of any of the individual nodes within

[3] We thereby exclude empty networks, however, empty networks are irrelevant for our analysis.

the network. The maximum degree of a graph, η_{max}, is the largest degree of any of the nodes within the network.

Contrary to what is the case in e.g. Jackson and Wolinsky (1996) and Bala and Goyal (2000), the nodes in our networks are not individual decision makers. Instead, there is a single decision maker, called the network designer, who benefits from the number of nodes connected into one network. The network designer's payoff is a function of the sum of the value of each node in the post-disruption network. Each node ex ante has one unit of information, but obtains information $|N_i(g^2)|$, i.e. obtains the total information of all nodes it is connected to. The value of a node i equals $u_i[|N_i(g^2)|]$, where $u'(.) > 0$, i.e. the value of node i is an increasing function of the amount of information obtained. The designer's payoff equals the sum of the values of all nodes, $\sum_i u_i[|N_i(g^2)|]$. The costs of the network designer are a function $c_{DES}(.)$, with $c_{DES'}(.) > 0$, of the number of links used in the pre-disruption network g^1. This number of links used is the sum of the degrees of each node divided by 2, or $[\sum_{i \in N} \eta_i(g^1)/2]$ and the costs therefore equal $[c_{DES}\left(\sum_{i \in N} \eta_i(g^1)/2\right)]$. The network designer plays in a zero-sum game against a network disruptor, therefore the disruptor's benefit equals $-\sum_i u_i[|N_i(g^2)|]$. The disruptor's cost function is an increasing function $c_{DIS}(.)$, with $c_{DIS'}(.) > 0$, of the number of links or nodes taken out from the pre-disruption network g^1. In case of link deletion, this is $[\sum_{g^2_{ij} \neq g^1_{ij}} g^2_{ij}]$. In case of node deletion, it is $|v|$.

As will become clear from the analysis, even with continuous function v, c_{DES} and c_{DIS}, the designer's and disruptor's maximands are discontinuous. It may be the case that a number of links added to g^1 does not increase the designer's payoff at all, in that the designer cannot protect the network in a better way by means of these links; but it may also be the case that one single link added has a huge effect on the designer's payoff, in making a huge difference for network protection. Similarly, it may be the case that a number of extra links or nodes deleted has little effect on the disruptor's payoff, in that they do not cause a substantial reduction in the designer's payoff; but it may also be that one extra link or node added has a huge effect, in enabling substantial disruption of the designer's network. In view of this, we cannot find the equilibria by means of maximization of continuous maximands.

Instead, first, we simplify the benefit functions of designer and disruptor, in assuming that the payoff of the designer (disruptor) is a positive (negative) function only of the size of the largest component in g^2.[4] This reflects the increasing marginal benefits of the information generated within a single component due to the non-excludable nature of information in our model. Let every node have one unit of information. Consider now a component of size x. The information generated by this component equals $(x)^2$. Everyone benefits from the information of an added node, and so the added benefit of increasing the size of a component are larger the more nodes this component already has. Second, we assume that the disruptor has a fixed link or node deletion budget, so has already decided on how many links or nodes to delete in g^1. This is without loss of generality. In any equilibrium, the disruptor decides on a certain number of links or nodes to be deleted. Given such a number of nodes or links, it must be the case that the designer chooses a best response in the form of an optimal network design strategy. Third, we either assume that the designer has a fixed defense budget, in the form of a fixed number of protective links that can be added to the minimal network with $(n-1)$ links; given such a budget, the designer then maximizes the value of the network, in maximizing the size of the largest component in the post-disruption network, after the disruptor has optimally deleted any links or nodes. Alternatively, we assume that the designer decides on achieving a fixed size for the largest component in g^2, and so a fixed benefit; given such a size, the designer aims to achieve this with a minimal number of links in g^1. Note that this reflects what takes place at an optimal solution:

[4] Of course there are extreme cases where $n_1^2 + (n - n_1) > n_2^2 + (n - n_2)^2, \forall n_1 > n_2$ does not hold. However, this is already an extreme comparison, as we take the worst case on the left-hand-side (one component, all other nodes are singlets) and the best scenario on the right hand side (2 components). Also we think that focussing solely on the largest component can be justified in terms of information flow. If there is no link between two groups, and a task has to be fulfilled by either one of them, chances are that the bigger one will succeed because there is more information within that group.

given the size of the largest component achieved there, this is achieved with a minimal number of links; given the number of links used, a maximal size for the largest component is aimed at. This is illustrated in Figure 1. On the X- and Y-axis are represented the two elements of the designer's payoff, namely the number of links used in the pre-disruption network, and the size of the largest remaining component in the post-disruption network. To each combination of these two measures corresponds a maximal payoff that can be achieved on the Z-axis, depending on an appropriate pre-disruption network structure. The payoff of the designer is represented in Figure 1 by means of a hill (even though the real payoff function is likely to be discontinuous). The curves represent the two approaches treated. In one approach, we look for the largest achievable remaining component for a given number of links. In the other approach, we look how a fixed size of the largest remaining component can be achieved with a minimal number of links.

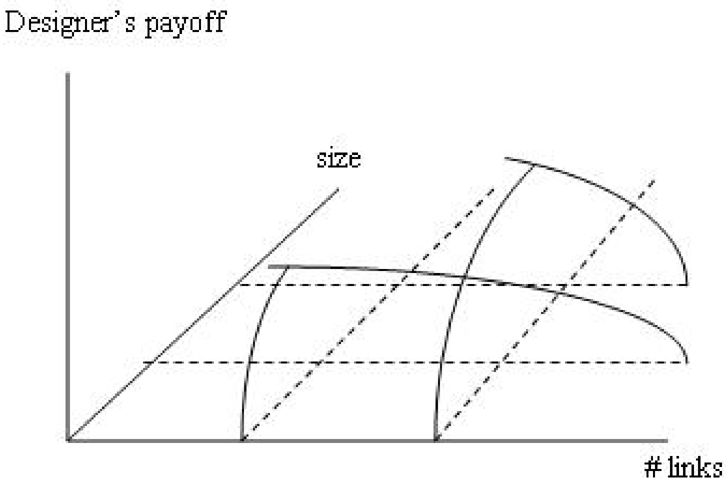


Figure 1: *Designer's Payoffs*

3. Benchmark Case

As long as there is no threat of attack on either the nodes or the links within a company, competition among firms will simply be based on prices. Therefore the structure of the within-firm network does not matter. As a benchmark case, we will therefore analyze the network, that the network designer will build in case that there is no threat of attack at all.

In this benchmark case, the network designer has a linking budget *B=(n-1)* and a defense budget of *Def=0*. He, therefore, can build a minimally connected network, as by definition, a minimally connected network uses exactly $(n-1)$ links. Since we assume that the network designer's net payoffs are convex in the size of the group that is connected, we can conclude that the network designer will always aim to form networks that consist out of one minimally connected component, as can be seen in figure 3 below. However, there are more than one way of building a minimally connected network, but in case of no attack they are all equally efficient.

Lemma 1. *Every minimally connected network is equally efficient if there is no threat of attack.*

Proof Every minimally connected network uses exactly $n-1$ links to connect n nodes. In case of no impending attack, it does not matter in which way the nodes are linked, as distance or decay does not play a role in the model. Therefore all minimally connected networks are equally efficient. □

The minimality of the efficient network is due to the assumption that no friction is involved in the network, so that the benefit of a connection does not depend on the length of the path between two agents. That the networks be minimally connected is, however, a very permissive requirement since it includes a range of network architectures even in the simplest cases with only a limited number of players. Networks (a) - (f) in figure 3 below are just examples of possible forms that a minimally connected network with 6 nodes can take. But in the case with no threat of an attack, these networks are all equally efficient. Thus, structure

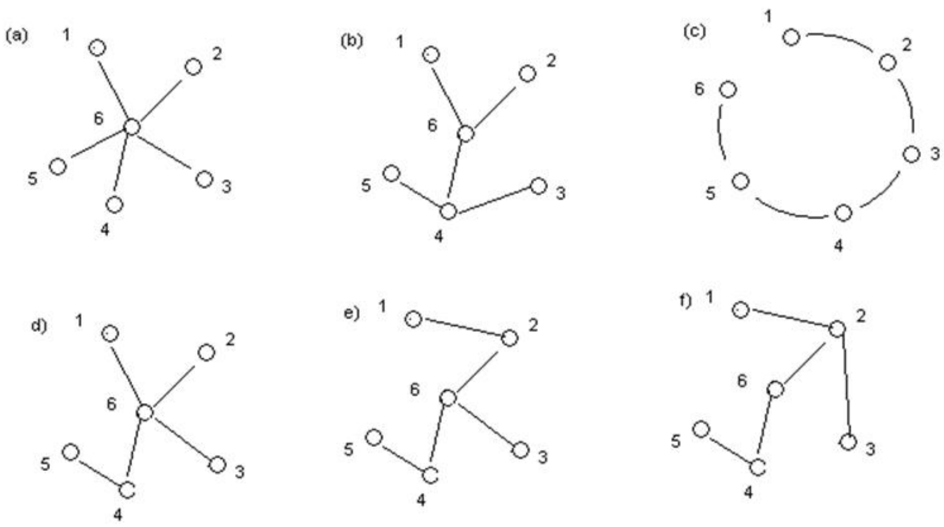


Figure 2: *Minimally Connected Networks*

does not matter if there is no threat of an attack. But if there is such a threat on either the nodes or the links, it does, as we will show in the following section.

4. Low Linking Costs

Introducing a network disruptor into the model, makes structure a decisive topic in the node deletion as well as in the link deletion case. Thus for firms that are facing an attack, the internal structure of the firm can be a decisive factor on how well they will deal with the attack. Since we are in a two-stage full information game, the network designer can anticipate a disruption of his network. An attack on the nodes of the network can be interpreted as the network disruptor trying to lure away crucial players from the network designer's network, towards his own. For the sake of simplicity, we abstract from the fact, that those players will be incorporated in the network disruptor's firm network somehow. To achieve this, the network disruptor has a disruption budget of D_v nodes, meaning that he can disrupt exactly D nodes. Link deletion in this context can be interpreted as an attack on the communication channels within a firm for example. Again we will abstract from the fact that the network disruptor might include the links he disrupts in his own network, and assume that he simply tries to cause maximal damage to the network designer's network. To achieve this, the network disruptor has a disruption budget of D_l nodes, meaning that he can disrupt exactly D links.

To start the discussion of network disruption , we will now start with the first approach introduced in figure 1. Therefore, we will focus on a certain fixed size of the post-disruption network. Hereby the network designer can use links to defend his network.

Definition A network g is said to be *(n-x)*proof against a link (node) deletion budget $D_l(D_v)$ if the largest remaining component upon strategic link (node) deletion contains at least $(n - x)$ nodes.

This definition leads to two observations, in the form of the following Lemmata.

Lemma 2. *For $x \geq 0$, a network is* (n-x) *proof against a link deletion budget D_l*

(i) if, for x>0, every set of x *nodes has at least D_l links to nodes outside the set* x*, and*

(ii) if every set of y *nodes, for y>x, has at least $(D_l + 1)$ links to nodes outside the set* y.

We then denote the set of all networks that are $(n-x)$-proof against a link deletion budget of D_l as $\Gamma_{l,D_l}^{(n-x)}$.

Lemma 3. *For $x \geq D_v$, a network is* (n-x) *proof against a node deletion budget D_v*

(i) if, for $x > D_v$, every set of $(x - D_v)$ nodes has at least D_v neighbors connecting it to nodes outside of the set of $(x - D_v)$ nodes, and

(ii) if every set of y *nodes, for y>x, has at least $(D_v + 1)$ links to neighbors connecting it to nodes outside the set* y.

We then denote the set of all networks that are $(n-x)$-proof against a node deletion budget of D_v as $\Gamma_{v,D_v}^{(n-x)}$. If we then look at the two cases of link- and node deletion, we can see that it is straightforward to deduce how large the post-disruption network can maximally be in either case.

Lemma 4. *Under link deletion with a deletion budget of D_l, a network can be at most* n*-proof. Under node deletion with a deletion budget of D_v, a network can be at most $(n - D_v)$-proof.*

Proof The result for link deletion follows from the fact that it is not possible for a post-disruption network to contain more nodes than the pre-disruption network contained. The result for node deletion follows simply from the fact that at least D_n nodes will be removed from the network, due to the definition of node deletion.

Introducing different concepts that define the maximal proofness for the cases of link and node deletion makes it hard to compare the two cases. Therefore we define as a *max*-proof network a network that achieves the highest achievable proofness for a given node deletion or link deletion budget. As follows from Lemma 4, *max*-proofness than means *n*-proofness for the case of link deletion and $(n - D_v)$-proofness for the case of node deletion. In the same manner, we define as a $(max - x)$-proof network, a network where the largest remaining component after disruption has x less nodes than the max-proof network. We can also already see here that to achieve max-proofness, relatively many links need to be in the network designer's defense budget. Therefore, this situation can be understood as one with low linking costs.

A first result that we can then immediately state is that node deletion restricts network structure more so than link deletion. Thus when facing an attack on its nodes, the network designer is more restricted in the way he builds up his network than when the attack is directed on the links of his network.

Proposition 1. *Compare node and link deletion when $D_v = D_l$. Then any network that is (max-x)-proof under node deletion is also (max-x)-proof under link deletion. But not all networks that are (max-x)-proof under link deletion are also (max-x)-proof under node deletion. Put otherwise, for $D_v = D_l$, the set $\Gamma_{v,D_v}^{(max-x)}$ is a strict subset of the set $\Gamma_{l,D_l}^{(max-x)}$.*

Proof Any set of nodes x that has l neighbors connecting it to nodes outside of the set x necessarily has l links to nodes outside of the set x. Thus by taking out l links, no more than l nodes can be separated from the network. □

4.1. *Minimal* **max**-*proof Networks*

In case linking costs are low, the network designer can afford a large defense budget *Def*, to aim for a maximally robust network. However, since links are still costly, the network designer will still not want to waste any links. He will therefore try to build a max-proof network, while minimizing the number of links he needs to achieve this. Thus within a firm, extra links between single nodes may help to prevent the total disruption of the network due to the fact that a limited number of nodes has been taken out. However, even with low linking costs, the network designer will try to minimize the number of links used to achieve maximal proofness of the network. For this reason we add the following definition.

Definition A network g is said to be **minimal** $(max - x)$-proof against a node (link) deletion budget $D_v(D_l)$, if no network exists that achieves $(max - x)$-proofness using less links.

We denote the set of all networks that are minimal $(n - x)$-proof against a node (link) deletion budget of $D_v(D_l)$ as $\Gamma^{(n-x),min}_{v,D_v}$ and respectively $\Gamma^{(n-x),min}_{l,D_l}$. It should be noted that the fact that for $D_v = D_l$, the set $\Gamma^{(n-x)}_{v,D_v}$ is a strict subset of the set $\Gamma^{(n-x)}_{l,D_l}$ (see proposition 1) does not imply that the set $\Gamma^{(n-x),min}_{v,D_v}$ is a strict subset of the set $\Gamma^{(n-x),min}_{l,D_l}$.

To find such minimal max-proof networks, is a straightforward task. We know from Lemmata 2 and 3 that a necessary condition for *max*-proofness under a disruption budget of $D_v = (r - 1)$ or $D_l = (r - 1)$ is that each nodes receives at least r links. good candidates for minimal *max*-proof networks are therefore networks in which each node has exactly degree r, because then each link is crucial in assuring *max*-proofness. Such networks are known as r-regular networks.

Definition An r-regular network is a network in which each node is connected exactly of degree r.

For any given n and r, any r-regular network has the same number of links, which imposes the following necessary conditions on the existence of an r-regular network.

Lemma 5. *A necessary condition for existence of an r-regular network is that* n *and/or* r *is an even number, where the r-regular network then has exactly* $(n * r) \setminus 2$ *links.*

Proof As each node receives exactly r links, and since each link is shared by exactly two nodes, the total number of links in any r-regular network is $(n * r) \setminus 2$. It follows that an r-regular network only exists if n and /or r is even. □

Thus, if there is an r-regular network that is *max*-proof, it is necessarily also minimal.

Lemma 6. *If an r-regular network with* $r = (D_v + 1)$ *(respectively* $r = (D_l + 1)$*) exists that is* max*-proof given* $D_v(D_l)$*, then this network is also minimal* max*-proof. It is then the case that the sets* $\Gamma^{(n-x),min}_{v,D_v}$ *and respectively* $\Gamma^{(n-x),min}_{l,D_l}$ *only contain r-regular networks.*

Proof By Lemmata 2 and 3, any *max*-proof network must have nodes that each have at least r links. By Lemma 5, any network where each nodes has exactly r links has exactly the same number of links. It follows that any r-regular network that is *max*-proof is also minimal *max*-proof. □

This shows that there should not be any local cliques or clusters between nodes in a network, as this will make them easy targets to be separated from the rest of the network. In local clusters, links are wasted in the sense that would those links lead to the rest of the network, the topology of the whole network would be made safer.

Unfortunately not all regular networks are also *max*-proof, as can be seen from the example of the graphs in figure 3. While all three graphs contain 16 nodes and are 3 regular, only the last one is *max*-proof for

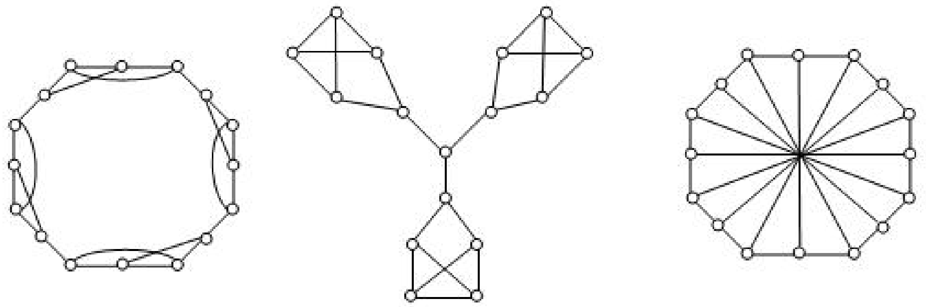


Figure 3: *3-regular Networks*

a disruption budget of $D_v = D_l = 2$. The first and the second one can be disrupted such that the post-disruption network would contain less than $(n-2)$ nodes. As can be seen here already, there are more than one ways to build r-regular networks. Therefore, it is also likely that there are more than one ways to build *max*-proof networks, which is indeed the case. However, we will now first show, that for the simple case where the disruption budget is 1, there is a unique minimal *max*-proof architecture and that this is the circle containing all nodes.

Proposition 2. *For $D_v = D_l = 1$, the unique minimal* max-*proof architecture is the circle containing all* n *nodes.*

Proof *Step 1.* We here show that any network with n nodes that uses $(n-1)$ links cannot contain a circle. A circle is a 2-regular network. Therefore by Lemma 5 we know that a circle contains $(n*2) \setminus 2$ links; thus exactly n links.
Step 2. Note that any network that does not contain a circle contains at least two end nodes, and is therefore not *max*-proof.
Step 3. Given that by Steps 1 and 2 no *max*-proof networks with $(n-1)$ links exist, if a network exists that is *max*-proof using n links, we know that the network using n links is minimal. The circle including n nodes is *max*-proof and therefore also minimal *max*-proof. Any other minimal *max*-proof network has then also exactly n links.
Step 4. Any network containing n nodes and links that contains a circle with $x < n$ nodes, has at least one end node and is therefore not *max*-proof. It follows that the circle containing n nodes is the unique minimal *max*-proof network architecture. □

The circle has several graph theoretic properties that are valuable to our further analysis and we will therefore define these properties here along the lines of standard graph theoretic literature, as can be found for example in Chartrand (1977) or Diestel (2005), before continuing with the actual analysis [5].

Definition A **hamiltonian** network is a network that contains a circle that contains all nodes.

Definition A network is **symmetric**, if no node can be distinguished from any other node in the network based on its position in the network.

[5]There are more graph theoretic concepts that we took into consideration, such as Menger's proposition (Menger, 1927) or the concept of *k-connectivity* (Frank, 1995), however, while they are close to what we are doing, we did not find them useful in further characterizing networks more stringently.

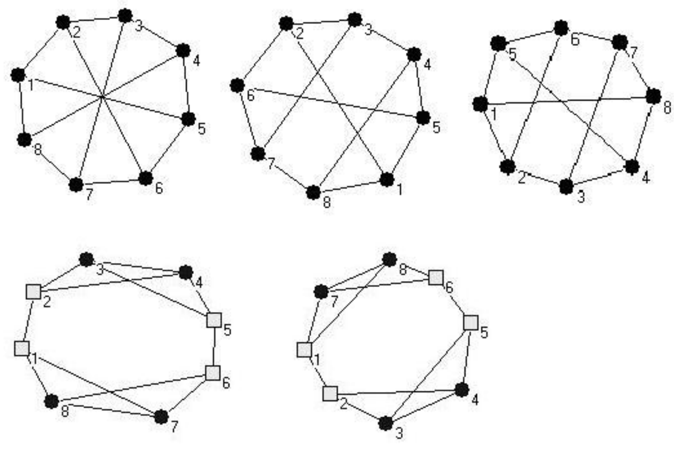


Figure 4: *Symmetric vs Non-Symmetric Networks*

This means that all node have exactly the same number of neighbors at distance 1,2,... . It is easy to see that then all nodes also need to receive the same number of links. Thus each symmetric network needs to be regular, however, the opposite is not the case. This can be seen from the networks in figure 4, where all networks contain 8 nodes and 12 links, however, only the top row of networks is symmetric. In the top row the nodes in the graphs all have the same number of neighbors at the same distance. Thus each node has 3 neighbors at distance 1, and 4 neighbors at distance 2, and this remains the same also in the different permutations of the graph. Therefore, you cannot distinguish the nodes from one another by means of their position in the network. In the bottom row this is not the case. Therefore the graphs are not symmetric.

Definition A **simple** network is an undirected network containing no multiple links between two nodes and no links beginning and ending at the same node (commonly referred to as loops).

Taking these definitions into account, we can define the minimal *max*-proof circle therefore as a simple, hamiltonian, symmetric, 2-regular network.

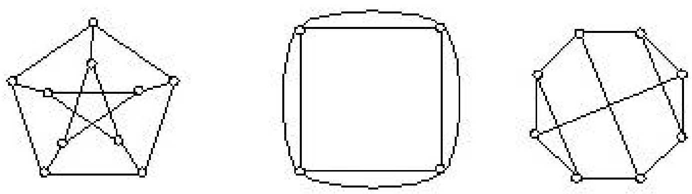
We now use a generalization of this idea to show the general existence of minimal *max*-proof networks. We construct simple, hamiltonian, symmetric, r-regular networks and show that these are indeed minimal *max*-proof under a deletion budget of $(r-1)$.

Lemma 7. *For* n *and/or* r *even, the sets* $\Gamma^{(n-x),min}_{v,D_v}$ *and respectively* $\Gamma^{(n-x),min}_{l,D_l}$*, are non-empty. In particular, we show that for each appropriate pair* (n,r) *with* $r > 2$*, a simple, hamiltonian, symmetric r-regular network exists that is minimal* max*-proof.*

Proof Step 1 shows that an r-regular network can be constructed whenever n and/or r is even. Step 2 shows that the constructed networks are max-proof under a disruption budget *(r - 1)*.
Step 1. Label each node i with a label $l_i \in \{1,2,...,n\}$. For each $\delta \leq r \setminus 2$, define a network $g^{\delta} = \left\{ ij : l_i = l_j + \delta, i_x j_x \not\equiv i_y j_y (\text{mod} n) \right\}$. For n odd, and for n even and $\delta \neq r \setminus 2$, all such networks take the form of a circle, or if $(n \setminus \delta)$ is an integer, take the form of a set of δ circle components of size $(n \setminus \delta)$. For n even and $\delta = r \setminus 2$, $g^{r \setminus 2}$ consists of *(n/2)* components consisting of a single link. An r- regular symmetric network when n is odd, or when n is even and r is even, can be constructed as follows: $g^1 \cup g^2 \cup ... \cup g^{(r/2)-1}$. An r-regular symmetric network when n is even and r is odd can be constructed as follows: $g^{r/2} g^1 \cup g^2 \cup ... \cup g^{(r-1)/2-1}$. Note that each of these networks is a Hamiltonian network, as g^1 is an n circle.
Step 2. We know that in an r-regular network, the disruptor cannot cause the post-disruption network to

contain any isolated single node component. We still need to show that the disruptor cannot cause the post-disruption network to contain isolated components of more than one node. Consider the case where r is even, and consider any component of x adjacent nodes, with $x \leq n \setminus 2$, in g^1. For $1 \leq x \leq r \setminus 2$, such a component has $x(r - x + 1)$ outlinks to the rest of the nodes. For $x \geq r/2$, such a component has $r/2(r/2 + 1)$ outlinks to the rest of the nodes. As $r/2(r/2 + 1) > x(r - x + 1)$, it suffices to check that $r/2(r/2 + 1) > (r - 1)$ to show that the disruptor cannot isolate components larger than 1. In fact, $r/2(r/2 + 1) > r \Leftrightarrow r > 2$. It follows that the disruptor is also not able to take out x adjacent nodes in g^1 when a new r'-regular network is constructed, with $r' = (r + 1)$, obtained by adding network $g^{r' \setminus 2}$.
Note next that components of x adjacent nodes on the g^1 have the largest possible number of links with each other in $g^1 \cup g^2 \cup ... \cup g^{(r/2)-1}$. It follows that, given that they have a sufficient number of outlinks, so will any other component of x adjacent nodes. Additionally, we need to consider the case where $(n \setminus \delta)$ is an integer, in which case the constructed network contains circle components of size $(n \setminus \delta)$. Any such circle has a sufficient number of outlinks. It follows as well that any larger circle contained in the network has a sufficient number of outlinks. □

While we thus showed that the set of networks is non-empty, there is unfortunately not a one-to-one correspondence between the set of simple, hamiltonian, symmetric r-regular networks and the set of minimal *max*-proof networks. *First* we can find graphs that do not fulfill one or all of these specifications but are still minimal *max*-proof. A well-known example of such a graph is the so-called Petersen graph, which is the graph on the left in figure 5. This can be checked to be minimal *max*-proof for $D_v = 2$ or $D_l = 2$, but is non-Hamiltonian. The second graph in the figure is also 5 is also minimal *max*-proof, however, not a simple network. The third graph, while being minimal *max*-proof, is non-symmetric.



(a) Non-Hamiltonian (b) Non-Simple (c) Non-Symmetric

Figure 5: Minimal Max-proof Networks

The second case can be illustrated by graph in figure 6. It is a simple, hamiltonian, however, it is not *max*-proof. If we look at the second graph in figure 4, we find a symmetric graph that is not *max*-proof. We conclude from these examples that there are no readily available graph-theoretic characteristics that

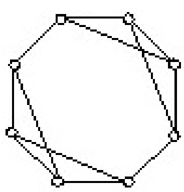


Figure 6: *Non-Max-proof Graphs*

characterize which r- regular networks are minimal *max*-proof. Still, we can simply note that minimal *max*-proof networks do not contain any bridge link sets, or bridge node sets, where these terms are defined as follows.

Definition A set of links $ij, kl, \ldots$ in a connected graph g, is called a bridge link set, if $g_{-ij,-kl,\ldots}$ is disconnected.

Definition A set of x nodes $i, j, k, \ldots$ in a connected graph g, is called a bridge node set , if $g_{-i,-j,-k,\ldots}$ contains a largest remaining component with size smaller than (n - x).

In effect, this means that in networks that do not contain any bridge link sets or bridge node sets, not only all single nodes need to be linked of a certain degree to the rest of the network, but also all sets of nodes are linked to the rest of the network with a certain number of links. Thus, we can come to the following proposition.

Proposition 3. *Let* n *and/or* $(D_l + 1)$ *be even. Then* $\Gamma^{max,min}_{v,D_v}$ *(and respectively* $\Gamma^{max,min}_{l,D_l}$*) is the set of all networks* g *with the following characteristics:*

(i) g *is a connected* $(D_v + 1)$ *(respectively* $(D_l + 1)$*) regular network;*

(ii) g *does not contain any bridge link sets (bridge node sets) of size* $x \leq r$*.*

Proof We proof each part of the proposition independently.

(i) Under link deletion, any minimal *max*-proof pre-disruption network must be connected, since otherwise the post-disruption network is not connected no matter which links are deleted. Under node deletion, any minimal *max*-proof pre-disruption network must be connected, since otherwise the disruptor can remove at least D_v nodes in the largest pre-disruption component. The rest of the proof of this part follows from Lemmata 5 and 6.

(ii) This follows directly from Lemmata 2 and 3. □

An illustration of proposition 3 is given in figure 7, for the case where $n = 16$ and $r = 3$. It can be checked that all represented graphs in the figure use exactly 24 links. We will investigate what happens when they are facing a network disruptor with a disruption budget of $D_v = D_l = 2$ The largest remaining connected component in the non-connected network (a) in the graph, consists of only 4 nodes. The network (b), which has been taken from Dekker and Colbert (2004), contains a bridge node as well a bridge link. Under node deletion the largest remaining component contains only 5 nodes and 6 nodes under link deletion. The network (c), also contains a bridge node and a bridge link. However, under node deletion the largest remaining component includes 8 nodes and 10 nodes under link deletion. The network (d) contains a 2 bridge link set and a 2 node bridge set. Therefore the largest remaining component under node deletion contains only 7 nodes and under link deletion 8 nodes. The graphs (e), (f), and (g) are *max*-proof. As can be seen here, there are different ways of constructing *max*-proof networks for the same n and r using the same number of links. It should also be noted here, that there are more than one ways to represent one and the same network, and the ones introduced here are merely examples.

We can thus conclude, that minimal *max*-proof networks are connected regular graphs that do not contain small bridge node sets or small bridge link sets. Intuitively, this means that networks that are not *max*-proof contain clusters of highly connected local cliques, with few links between the cliques. This is a waste of links, in the sense that cliques can be separated from one another quite easily.

We have already shown in proposition 1 that network structure is more restrictive for node deletion than for link deletion, when building *max*-proof networks. We now extend this to show that this also holds for *minimal max*-proof networks.

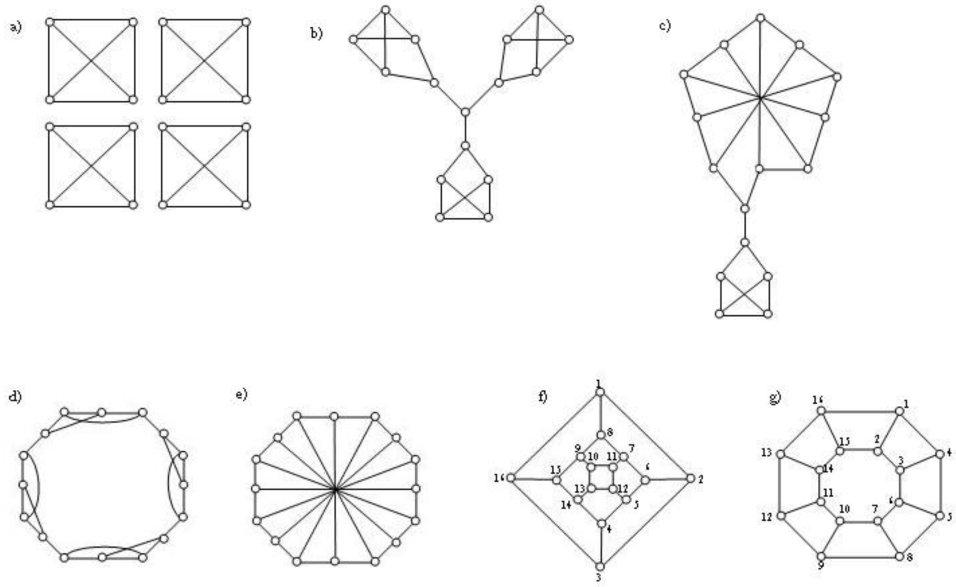


Figure 7: *Max- and Non-Max-proof 3-regular Networks*

Proposition 4. *The set* $\Gamma_{v,D_v}^{(n-x),min}$ *is a strict subset of the set* $\Gamma_{l,D_l}^{(n-x),min}$.

Proof *Step 1.* The set $\Gamma_{v,D_v}^{(n-x),min}$ contains only simple graphs. When there are multiple links between two nodes, removing one of these links does not make any difference for the proofness of the network under node deletion.
Step 2. Consider a non-simple graph of the following form. For $r \geq 4$ and being an even number, construct a circle, and double $(r = 4)$, triple $(r = 6)$, etc. each link. Such a graph is r-regular and minimal *max*-proof under link deletion, however, by step 1, not under node deletion. □

An illustration of proposition 4 is in figure 8, representing the case for $n = 16$ and $r = 4$, which is minimal *max*-proof under link deletion but not *max*-proof under node deletion.

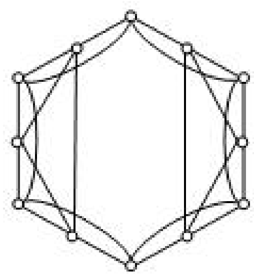


Figure 8: *Max*-proof under Link Deletion but not under Node Deletion

4.2. *Minimal* (max-1)*-proof Networks*

For node deletion, as well as link deletion, we can treat the concept of *max*-proofness in a somewhat more general way. If the network designer does not focus on keeping the whole network safe, but instead, is willing to sacrifice a small part of his network, he might be able to use a lot less links, than when trying to keep his network safe from disruption. We will therefore, in this section, treat networks that are minimal (*max-1*)-proof against disruption. We start by considering a fixed linking budget $B = (n-1)$ of the network designer. This is a good starting point, as we can easily compare it to our benchmark case, since $B = (n-1)$ is exactly the linking budget needed to build a minimally connected network.

While in the benchmark case, the structure of the minimally connected network did not matter, it does matter if there is an impending attack. We show that the minimal (*max-1*)-proof network for the case of link deletion, when facing a network disruptor with a disruption budget of $D_l = 1$, is the star network, which is defined as follows.

Definition A star network has a central node i, such that $g_{ij} = 1$ for all $j \in N \setminus i$ and no other links.

Proposition 5. *For $D_l = 1$, the two unique minimal (*max-1*)-proof network architectures are the star including all* nodes *and the circle including* n-1 *nodes.*

Proof *Step 1.* To achieve (*max-1*)-proofness, the pre-disruption architecture must include a component with at least $(n-1)$ nodes. As soon as this is not the case, the post-disruption largest component has automatically less than $(n-1)$ nodes. By arguments identical to those in proposition 2, one can show that, in the set of pre-disruption networks linking exactly $(n-1)$ nodes, the unique *max*-proof network that uses a minimal number of links is the circle made up of (n-1) nodes. The rest of the proof shows that one can do equally well with a star made up of n nodes.
Step 2. Here we show by contradiction that any network made up of n nodes using $(n-1)$ links does not contain a circle. Suppose such a network would contain a circle. Not that any circle of x nodes by definition contains x links. There are now *n-x* remaining nodes that need to be linked to build a network including all n nodes and *(n-x-1)* remaining links. This would require a minimum of *n-x* additional links. Thus no network including n nodes using *(n-1)* links can contain a circle.
Step 3. Consider thee case where the pre-disruption network is a connected network. Any such network uses at least $(n-1)$ links. The star uses exactly $(n-1)$ links and is (*max-1*)-proof under $D_l = 1$. Among the pre-disruption networks including all n nodes, the star thus achieves (*max-1*)-proofness with a minimal number of links. Any network including n nodes using *(n-1)* links that is not the star, ist not *(max-1)*-proof. To see why note that any such network ocntains at least one path wx, xy, yz. by Step 2, it must be the case that $x \neq y \neq z$. Since the network does not contain any circles, deleting link xy means that there is no connection between nodes wx and yz. It follows that ay non-star network in this setting is not *(max-1)*-proof.
Step 4. By Step 1, a *(max-1)*-proof pre-disruption network contains either a component with n nodes or a component with $(n-1)$ nodes. In both cases, the minimal number of links needed to achieve *(max-1)*-proofness is $(n-1)$. It follows that the star with n nodes and the circle with $(n-1)$ nodes are the unique minimal *(max-1)*-proof architectures. □

Obviously it is not a good idea to build a star network under node deletion, as the deletion of a single node, namely the central node, will lead to a post-disruption network of all single unconnected nodes. We next show that the unique minimal *(max-1)*-proof network under node deletion is the circle containing $(n-1)$ nodes.

Proposition 6. *For $D_v = 1$, the unique minimal* (max-1)*-proof architecture is the circle containing $(n-1)$ nodes.*

Proof *Step 1.* Every connected network that uses $(n-1)$ links has at least two end nodes, and is therefore not *(max-1)*-proof. It follows that if a connected network exists that is *(max-1)*-proof and uses n links, it is also minimal $(max-1)$-proof.

Step 2. Every network using $(n-1)$ nodes that is not a circle has at least one end node and is thus not *(max-1)*-proof (see Step 4 of proposition 2). □

The specific case of a disruption budget of 1 suggests a basic principle, namely that under *link deletion*, if the designer is willing to sacrifice one node to save on links, he should build a star or star-like network. The central node cannot be removed, because it has too many links. The peripheral nodes form symmetric weak spots, only one of which the disruptor is able to disconnect from the network. Under *node deletion*, central nodes should on the contrary be avoided, because their deletion can cause great damage to the network. A circle, or circle-like network avoids the existence of central nodes. We now treat *(max-1)*-proofness when $D_l > 1$ or $D_v > 1$, and show that these intuitions are indeed general. That this might indeed be reasonable can be seen from the immense amount of links needed to make a network *max*-proof, especially if the disruption budget of the network disruptor increases.

By Lemmata 2 and 3, we know that a condition for a network to be *(max-1)*-proof is that each connected and unconnected pair of nodes needs to have at least $(D_l + 1)$ links to other nodes in the network under link deletion and at least $(D_v + 1)$ neighbors in the rest of the network under node deletion. A good starting point to look for minimal *(max-1)*-proof networks are the cases where each connected pair of nodes exactly achieves the restrictions that it should have a certain number of r outlinks. That all unconnected pairs fulfill this restriction, is obvious, due to the degree of connectivity of the network. We call such networks pair r-regular networks.

Definition In any pair r-regular network, each pair of neighboring nodes has *exactly r* links to the rest of the nodes.

We next show that in any pair regular network, there are exactly two types of nodes, and that nodes of the same type are not linked. In graph-theoretic terms, this means that pair r-regular networks are *bipartite* networks. Just like r-regular networks, pair r-regular networks can be depicted in a number of different ways. We give some examples in figure 9. We can also see, that due to this multiple possibilities of building the network not all pair r-regular networks are necessarily minimal or *(max-1)*-proof. The network on the left and in the middle are both *(max-1)*-proof under a link deletion budget of $D_l = 3$, however, while the network on the left uses 18 links, the one in the middle only uses 16 links. The network on the right, is also minimal, in that it only uses 16 links, however it is not *(max-1)*-proof.

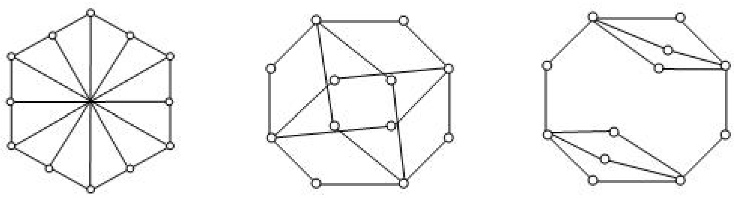


Figure 9: *Pair 4-regular Networks with n=12*

Proposition 7. *In any pair r-regular network, each node has either degree r_1, or degree r_2, where $r_1 + r_2 - 2 = r$, and nodes with degree r_1 are not linked to nodes with degree r_2.*

Proof Consider a pair r-regular network where in a single connected pair (x_1x_2), node x_1 has degree r_1 and node x_2 has degree r_2, such that $r_1 + r_2 - 2 = r$. Note that the 2 in the latter expression accounts for the direct link of the two nodes, so that r is indeed their number of links to the rest of the nodes. The $(r_1 - 1)$ links of node x_1 to nodes other than x_2 each form a pair. Take one such node y_1 connected to x_1. In the pair x_1y_1, x_1 has degree r_1, so that y_1 must necessarily have degree r_2. In the same manner, every node connected to y_1 must again have degree r_1. And so on. Similarly, each neighbor of x_2 must have degree r_1, the neighbors of this neighbor must again have degree r_2, and so on. □

Knowing that any pair r-regular network is bipartite, we can label the two groups of nodes. By n_1 we denote the number of nodes with degree r_1, and by n_2 the number of nodes with degree r_2, where we label the type-1 and type-2 nodes such that $r_1 \geq r_2$, where $r_2 \geq 1$ (note that for $r_2 = 1$, the only pair r-regular network is the star, which is pair (n - 2) regular). We then call the type-1 nodes *core nodes*, and the type-2 nodes *peripheral nodes*. Note that if you look at figure 9, you can see that the core nodes need not necessarily be in the *core* of the depiction of the graph, but that is simply a matter of how the graphs are being drawn.

Proposition 8. *In any pair r-regular network, we have* $n_1 = n * [r_2/(r_1 + r_2)] = n * [r_2/(r + 2)]$ *and* $n_2 = n * [r_1/(r_1 + r_2)] = n * [r_1/(r + 2)]$*, and the network has exactly* $n * [r_1 r_2/(r_1 + r_2)] = n * [r_1(r + 2 - r_1)/(r + 2)]$ *links.*

Proof By proposition 7, any pair r-regular network is a bipartite graph, with nodes with only two kinds of degrees. It follows that for L, the number of links used in the network, it is the case that $L = n_1 r_1 = n_2 r_2$. Combining this with the fact that $n_1 + n_2 = n$, and using the fact that $r_1 + r_2 - 2 = r$, the given expressions for n_1 and n_2 are obtained. These expressions, and the fact that $L = n_1 r_1 = n_2 r_2$ again allow us to calculate that $L = n * [r_1 r_2/(r1 + r2)] = n * [r_2(r + 2 - r_2)/(r + 2)]$. □

The intuition behind proposition 8 is of course, that by making the distribution of degrees over any pair of nodes more unequal, so that r_2 becomes smaller and r_1 bigger, we will have fewer core nodes and more peripheral nodes. This can be seen in the extreme case of the star network, where we have only one core node and $(n - 1)$ peripheral nodes with $r_2 + 1$ and $r_1 = (n - 1)$.

That the set of pair r-regular networks is not empty, follows from proposition 9.

Proposition 9. *For* $r < (n - 2)$*, and for* $r_1 + r_2 - 2 = r$ *with* $r_1 \geq r_2$*, let* $n_1 = n * [r_2/(r_1 + r_2)]$ *and* $n_2 = n * [r_1/(r_1 + r_2)]$ *be integer numbers. Then the set of pair r-regular networks is not empty.*

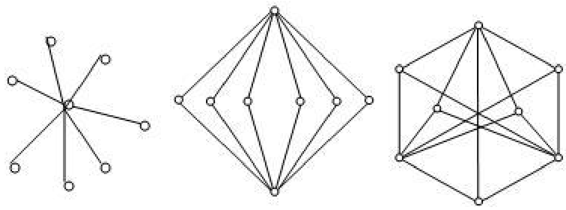
Proof Construct a circle of $2 * n_1$ nodes, namely n_1 type 1 nodes and n_2 type 2 nodes. In the circle every type 1 node is connected to type 2 nodes, and vice versa. Next, add the appropriate number of links to each pair on the circle, namely $(r_1 - 2)$ links for each of the type 1s, and $(r_2 - 2)$ for each of the type 2 nodes. These nodes added to the circle make a total of $n_1(r_1 + r_2 - 4)$ links connected to nodes on the circle on the one side, and that still need to be connected to other nodes, on or off the circle. Also, $(n_1 + n_2 - 2n_1) = (n_2 - n_1)$ nodes still need to be connected to the network. These remaining nodes are all type 2 nodes. All the $n_1(r_2 - 2)$ links of the type 2 nodes on the circle need to be to a type 1 node on the circle, as type 1 nodes by assumption only lie on the circle. We can let each of the n_1 nodes on the circle receive $n_1 * [(r_2 - 2)/n_1] = (r_2 - 2)$ such links from type 2 nodes on the circle. For $r_1 > r_2$, all of the remaining $[n_1 * (r_1 - 2) - n_1 * (r_2 - 2)] = n_1(r_1 - r_2)$ links of the type 1 nodes on the circle need to be to type 2 nodes not on the circle; each such type 2 node not on the circle needs to receive links from exactly r_2 of the type 1 nodes, each type 1 node needs to have $(r_1 - r_2)$ such links. This means that there must be exactly $n_1(r_1 - r_2)/r_2$ type 2 nodes that do not lie on the circle. We therefore have $n_2 = n_1 + n_1 * [(r_1 - r_2)/r_2] = n_1 r_1/r_2$ type 2 nodes, and n_1 type 1 nodes. Also, $n_2 = n_1 r_1/r_2 \Leftrightarrow n = n_1(r_1 + r_2)/r_2 \Leftrightarrow n_1 = n * [r_2/(r_1 + r_2)]$. □

Thus knowing that the set of pair r-regular networks is not empty, the next question is, are all pair r-regular networks minimal. We have already seen that there are different ways to build such networks, and therefore, the answer, unfortunately, is no. However, there is a clear rule, on how the number of links needed to make a pair r-regular network can be determined, as will be seen in proposition 10.

Proposition 10. *For given* n *with* $r < (n - 2)$*, consider the set of pair r-regular networks, where n is assumed such that for all* $r_1 \geq r_2$ *(with* $r_1 + r_2 - 2 = r$*), it is the case that* $n * [r_2/(r_1 + r_2)]$ *and* $n * [r_1/(r_1 + r_2)]$ *are integer numbers. Then in this set, pair r-regular networks have less links the smaller their* r_2*, and the pair r- regular networks with* $r_2 = 2$ *have the smallest number of links in this set.*

Proof A pair r-regular network with $r_2 = 1, r_1 = (r+1)$ is only possible with the star architecture, and is pair (n - 2)- regular. This case is here excluded given that $r < (n-2)$. The smallest possible r_2 is then $r_2 = 2$. In the expression $L = n * [r_2(r+2-r_2)/(r+2)]$ derived in the proof of Proposition 2, the number of links used is smaller the smaller r_2. The result follows. □

The intuition behind proposition 10 is that as we use more periphery and less core nodes, we need less links to build the network. However, this also means that we use more *weak* and less *strong* nodes, therefore the network won't be very well protected. To see this, consider the graphs in figure 10. Graph 10(a) is the star, using least links, however, it is also only *(max-1)*-proof against a disruption budget of $D_l = 1$. This is the most extreme case, since it only has one node of group n_1 and $(n-1)$ nodes of group $n-2$. Graph 10(b) uses more links, however, it is *(max-1)*-proof against a disruption budget of $D_l = 2$ and it includes 2 nodes of group n_1 and 6 nodes of group n_2. Graph 10(c) uses most links and has most core nodes (5), it is also most proof though. It is *(max-1)*-proof for $D_l = 3$.



(a) 7 links (b) 12 links (c) 15 links

Figure 10: Minimal Max-proof Networks

Additionally not even all pair r-regular networks are necessarily *(max-1)*-proof, as will be seen from the following Lemmata. However, we will as a first step now show that for all relevant cases, any linking budget that allows one to build exactly a pair r-regular network, is insufficient to build an r-regular network. The consequence of this is that, if the network designer has a linking budget that exactly allows him to build a pair (D_l+1)-regular network, and if this network is $(n-1)$-proof under link deletion with a disruption budget of D_l, then this is the maximal proofness that can be achieved with this budget, as n-proofness cannot be achieved.

Lemma 8. *Let $r_1 \geq 3, r_2 \geq 2$. Then with any number of links $L = n * [r_1 r_2/(r_1+r_2)]$ that exactly allows one to build a **pair r-regular** network, one cannot build an **r-regular** network.*

Proof $n * r/2 > n * [r_1 r_2/(r_1+r_2)] \Leftrightarrow (r_1+r_2-2)(r_1+r_2) > 2 * r_1 r_2 \Leftrightarrow r_1^2 + r_2^2 > 2(r_1+r_2)$ □

Thus Lemma 8 shows that for a given budget, the best the network designer can achieve is *(max-1)*-proofness. He will achieve this by then building a pair r-regular network.However, as we have pointed out above, not all pair r-regular networks are *(max-1)*-proof.

Lemma 9. *A necessary condition for a pair r-regular network to be*

(i) (n - 1)-proof under link deletion with $D_l = (r-1)$

(ii) $(n - D_v - 1)$-proof under node deletion with $D_v = (r-1)$

is that $r_2 > (r-1)/2 \Leftrightarrow r_2 > (r_1-3)$.

Proof If $r_2 \leq (r-1) \setminus 2$, the disruptor is able to delete several nodes with degree r_2, by either deleting all their links, or all their neighbors. □

For the case of node deletion, this means specifically, if the nodes with degree r_1 are given too many links, the network may not be *(max-1)*-proof, because the disruption of the core nodes then disconnects the network.

Lemma 10. *A necessary condition for a pair r-regular network to be $(n - D_v - 1)$-proof under node deletion with $D_v = (r-1)$ is that $r_2 > (r_1 - 2)$.*

Proof Consider two neighbors of a type-1 node x_1. By definition, these two neighbors are type-2 nodes. Each of them have $(r_2 - 1)$ type-1 neighbors other than x_1. If $[2 * (r_2 - 1) + 1] \leq D_v = (r-1)$, then by taking all the $[2(r_2 - 1) + 1]$ type-1 neighbors of the two mentioned type-2 nodes out, the disruptor can take out two extra nodes. □

For link deletion, giving too many links to a few core nodes, is also not a good idea, since then too many peripheral nodes can be disconnected by disconnecting just a few links. These two observations already speak for the fact that there is a tradeoff between using a minimal amount of links and making the network *(max-1)*-proof when building a pair r-regular network. These observations also lead us to the conclusion, that while distributing links as unevenly as possible between core and periphery nodes, leads to using the least amount of links, these networks won't be proof. Therefore, in the following propositions, we suggest, that for the case of node deletion as well as link deletion, it is most sensible to distribute the links as evenly as possible over the two groups of nodes. Thus given the necessary conditions provided by these Lemmata 9 and 10, we now derive necessary conditions for the minimal number of links needed to construct a *(max - 1)*-proof pair r-regular network, both under link deletion and node deletion.

Proposition 11. *For odd* r*, under link deletion with $D_l = (r-1)$, the candidate* (max - 1)*-proof pair r-regular network that uses a minimal number of links, has $r_1 = (r+3)/2, r_2 = (r+1)/2$, so that the type-1 nodes have only one link extra. For even* r*, we have $r_1 = r/2 + 2, r_2 = r/2$, so that the type-1 nodes have two links extra.*

Proof This follows directly from proposition 10 and Lemma 9. □

Proposition 12. *For odd* r*, under node deletion, if $n_1 > D_v$, the candidate $(n - D_v - 1)$-proof pair r-regular network that uses a minimal number of links has $r_1 = (r+3)/2, r_2 = (r+1)/2$, so that the type-1 nodes have only one link extra. For even* r*, we have $r_1 = r_2 = (r+2)/2$, meaning that the network is $(r+2)/2$-regular.*

Proof Note that with $n_1 \leq D_v$, as each type-2 node has only type-1 neighbor, by deleting all type-1 nodes, the disruptor can reduce the network to at most a set of n_2 one-node components. The rest of the proof follows directly from proposition 10 and Lemma 10. □

proposition 11 suggests that leaving weak spots in the network is a good idea under link deletion, though the weak spots should not be too weak. proposition 12 shows that leaving weak spots under node deletion is a bad idea. This generalizes the idea that stars are bad under node deletion. The fact that for odd *r*, it is still the case that not every node has the same degree is because there simply does not exist a way to divide the r outlinks equally over the two nodes of the pair. An example is given in Figure 11 for the case n = 12, r = 4, $D_l = D_v = 3$. The left graph is pair 4-regular where each connected pair has two outlinks on each side, and is at the same time 3-regular. It uses 18 links. The right graph is pair 4-regular, where each time one node of each connected pair has three outlinks, and the other node has one outlink. It uses only 16 links. In both graphs the largest remaining component under link deletion includes 11 nodes. Under node deletion, the largest remaining component in the left graph includes 11 nodes as well, however, only 8 nodes in the right graph.

Unfortunately here there is no straightforward extension of this concept to more than $(max - 1)$-proofness. While the basic definition and intuition still holds, it becomes increasingly difficult to find conditions that all networks need to fulfill to be $(max - x)$-proof for any given x and D_v or respectively D_l. However, based on the insides gained from this first discussion, we see that what follows from this is that pair-regular networks still tend towards symmetry. We cannot use the very rigorous graph theoretic

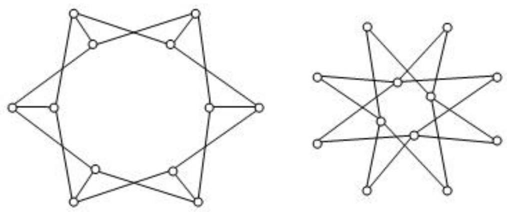


Figure 11: Pair 4-regular Networks

concept of symmetry introduced earlier in the paper here, as we have different kinds of nodes. However, these nodes are kept as similar to one another as possible. There are only two different groups of nodes in the network. Looking at each group of nodes individually, you cannot distinguish one node from another in the same group just by means of their location within the network. This indicates that while we are certainly leaving weak spots within the network, we are leaving symmetric weak spots, which again shows that building local cliques or clusters is not a sensible technique when facing an attack by a network disruptor. Thus in terms of internal firm organization this means that there should still be a very little hierarchical and more symmetrical structure within the firm. Employees should be directly linked to more than one of their superiors, so in case communication is disturbed between any of them, there will still be other means of communication throughout the firm. This will ensure the robustness of the internal firm network against attack. It will also ensure that by symmetrically leaving weak spots within the network, the network designer has some measure of control about which subsections will be disrupted from his network.

5. Fixed Linking Budget

Now looking at the second approach introduced in figure 1, we investigate what happens if the network designer has a fixed linking budget. In this case here, we are looking at permissively high linking costs, which leads to a defense budget of $Def = 0$. Thus adding additional links next to the original linking budget of $B = (n - 1)$, is permissively expensive; Leaving the network designer to structure his network as robustly as possible with this limited amount of links. As in the previous case, the structure within the firm now becomes decisive again. However, while in the case of low linking costs, there was no difference in structure needed between the cases of link deletion and node deletion, here it becomes quickly apparent that link deletion and node deletion do not lead to the same results. This is obvious by simply looking at the minimally connected networks introduced in figure 2. While the network disruptor can completely separate the star network (a), by taking out the central node, the maximum damage he can cause to the chain network (c) is to separate two additional nodes from the network, thus leaving a largest remaining component of $n/2$. For link deletion, however, the star network (a) seems like a good option, since the maximal damage the network disruptor can cause by taking out a single link, is to disconnect one node from the network, whereas the chain network (c) can be cut in half. Thus, here again, we will start by analyzing the link deletion case, and then turning to the node deletion case.

5.1. Link Deletion - High Linking Costs

We have shown in the benchmark case, that if there is no threat of an attack on the links of the network, all minimally connected networks are equally efficient. However, now taking into account that there is a network disruptor with a disruption budget $D_l > 0$, not all minimally connected networks are equally efficient any longer. We will show in the following that the star network is the only efficient network in case the network designer faces a network disruptor with a disruption budget of $D_l \geq 1$. Using a linking budget of only $B = (n - 1)$ links and no defense budget, can be interpreted as very high linking costs. In this case the network designer rather takes into account that some nodes will be disconnected from the network than add additional links to the pre-disruption network, because additional links are simply too expensive.

We have shown in proposition 5 that the unique minimal *(max-1)*-proof networks for $D_l = 1$ are the star and the circle with $(n-1)$ nodes. Thus we know that the maximal damage a network disruptor with a disruption budget of $D_l = 1$ can do a star network is disconnect exactly one node from the rest of the network. Now if we generalize the argument, we see that no matter how large the disruption budget is, as long as there is no defense budget of the network designer, the star network is the most robust network topology against attack in the case of link deletion.

Lemma 11. *The maximal damage a network disruptor with a disruption budget of D_l can cause in a star network is to disconnect exactly D nodes.*

Proof By proposition 5 we know that with a disruption budget of 1, only 1 node can be separated from the network. The same argument applies to any disruption budget. With each link that the network disruptor can delete, he can only separate one node from the network and therefore, with a disruption budget of D, he can separate exactly D nodes. □

To show that the star is the most robust network topology for a linking budget of $B = (n-1)$ and a disruption budget of D_l, we need to consider then what happens to other minimally connected networks.

Lemma 12. *Any minimally connected network that is not the star contains at least two nodes that are connected of a degree larger than one.*

Proof In a star network, by definition, there is one central node i and $(n-1)$ end-players $j \, \forall j = \{j_1, j_2, ..., j_{n-1}\}$. Therefore there are $(n-1)$ nodes connected of degree one and one node connected of degree $(n-1)$. In any minimally connected network that is not a strict star, there will be no direct link from i to j_1, so that $g_{i,j_1} = g_{j_1,i} = 0$. For node j_1 to still be connected to the network, it must be connected to any node $j = \{j_2, ..., j_{n-1}\}$. Since all of these nodes are also connected to i, there will be at least one node except for i that is connected of a degree larger than one, so in total at least two nodes that are connected of a degree larger than 2. □

The fact that the star is the only minimally connected network that consists of $(n-1)$ nodes that are end-players is important as it shows that the star is the only efficient minimally connected network in case of an impending attack, since in all other cases the damage that can be done by a network disruptor is greater, as can be seen from the following Lemma.

Lemma 13. *The minimal damage a network disruptor with a linking budget D_l can do in any minimally connected network is to disconnect D_l nodes.*

Proof Every link in a minimally connected network is a bridge. It follows that every link removed removes at least one node. □

Thus the minimal damage that can be done in any minimally connected network is equal to the damage that is done in the star network, as can be seen from Lemma 11. Therefore the star network needs to at least weakly dominate all other minimally connected networks in this case.

What we have not considered so far is, however, the case when the network designer might build a smaller but stronger network by not including all nodes in the component, but using links instead to make the network more robust against attack. Therefore we will now turn to these cases. We know that in any minimally connected network there is no circle and in any network that is not minimally connected there is at least one circle. To build a cycle we know we need exactly n links. Since we have a linking budget of $B = (n-1)$, the network with a circle can therefore only include $(n-1)$ nodes. We also know that any end node can be disconnected by disrupting one link only. Therefore, if we do build a network including less nodes, we should not leave any end nodes in the network because they are natural weak spots. Therefore the network designer, should include all $(n-1)$ nodes in the circle. For any additional link the network designer might want to add to the circle, he has to leave one additional node out of the connected component. Therefore, we can calculate exactly how large the network in question will be, depending on the number of links added to the basic cycle.

Lemma 14. *The network designer with a linking budget of $B = (n-1)$, needs to leave one additional node out of the connected component, as compared to a minimally connected network, for each additional link he wants to add to the connected component.*

Proof For a circle this is trivially true, as we know that any cycle needs exactly n links. Thus for a linking budget of $B = (n-1)$ we can build a circle only with $(n-1)$ nodes. For any additional link that we want to add to the circle, we need to leave one additional node out of the circle to enable us to do so, since then we have a linking budget of $(n-1)$ links, but can use only $(n-2)$ links in the circle, thus the circle can only include $(n-2)$ nodes. □

Knowing this, the question is, how many nodes remain in the post-disruption network g^2 then, because the component does not only get smaller but also stronger. We have seen this already for the case of a disruption budget of 1 and the star and the circle network. The circle network is smaller but therefore stronger and has thus an equally large post-disruption network as the star. We know for certain values of n and D_l exactly what will happen, namely for the regular networks. For r-regular networks we know by Lemma 5 that we need exactly $(n * r)/2$ links. Thus if we rearrange this equation, we get that for a linking budget of $(n-1)$, we can build a r-regular network with exactly $(n-1) * 2/r$ nodes. Then if the network is r-regular, we know that for $D_l < r$ no additional nodes can be removed from the network. Therefore, whenever $(n-1) * 2/r < n - (r-1)$, the star network is a better choice than the r-regular network. Solving this inequality, we get that this is indeed the case when $r + 1 < n$.[6] However, that still leaves the possibility of not including all nodes, and not building a r-regular network but some in-between case. Here we can use, that we do know that in any network that is not r-regular for $D_l \geq r$, we can remove at least one node from the network.[7]Thus, to show that a star network is indeed the optimal strategy of the network designer, we need to show that the post-disruption network for the star network will be always at least as good as for any other possible network with the same linking budget.

Proposition 13. *When facing a network disruptor with a disruption budget of D_l, the network designer's weakly dominating strategy is to build a star network, $\forall D_l = 0 < D_l \leq \ell - 1$.*[8]

Proof We proof this proposition in two steps. First we show that the star network is always better than any other minimally connected network.
Step 1. By Lemma 12, we know that the network disruptor with a disruption budget of 1 will be able to disconnect at least one node from any minimally connected network. By Proposition 5, we know that in a star the maximal damage that can be caused is disconnecting exactly one node. Therefore the star is efficient as well as the circle with $(n-1)$ nodes. By Lemma 11 we know that in any other minimally connected network, at least one more node is connected of a degree larger than one, and therefore more than one node can be separated from the network by deleting one link. So there is always the possibility to disconnect at least one more node from any other minimally connected network than from the star.
We now turn to proofing the proposition for any not minimally connected network.
Step 2. Assume that $D_l \leq x$, where x denotes the number of links left out of the pre-disruption network. In that case, we know that in the network, because it is not r-regular, and thus $\eta_{min} \leq D_l$, at least one additional node can be separated from the network. Thus the largest remaining post-disruption network

[6]Thus in all interesting cases because since $D_l = r - 1$, otherwise we end up with only one link in the post disruption network in any case.

[7]Usually more nodes can be disconnected but starting from this "worst case scenario" we can already show that the star network is always at least as good as any other possible network.

[8]For a disruption budget of $D_l > \ell - 1$,it does not matter with which minimally connected network we start as only 1 link will remain.

that could be obtained would consist of $n - x - 1$ nodes. For the star network, the largest remaining post-disruption network would be of size $n - D_l$. Since by assumption $D_l \leq x$, we know that $n - D_l > n - x - 1$ always holds. *Step 3.* Assume that $D_l > x$. Leaving x nodes out of the component allows the network designer to build any minimally connected network of the $(n - x)$ nodes and add an additional x links to it, as can be seem from Lemma 14. For $D_l > x$, let's assume that $D_l > x + y$. The network disruptor can then disrupt all x links added to the network, as can be seen from Lemma 13 as well as y additional ones. Disrupting the x nodes that had been added to some form of a minimally connected network, will leave a minimally connected network. Therefore we know by Lemma 11 and Lemma 1 that depending on the minimally connected network we remain with, we can minimally still disconnect y additional nodes with a disruption budget of y. Therefore, the maximally remaining largest component will be $n - x - y$ which equals $n - D_l$. As has been shown in Lemma 11 this is the same size as the post-disruption star network. □

So while all minimally connected networks are equally efficient if there is no threat of an attack, the star is the only efficient minimally connected network in case of an impending attack for a linking budget of $B = (n - 1)$. The star network is also always at least as good as any other possible network made up of $(n - 1)$ links. Only in few, very special cases, such as the circle, are there networks that are as good as the star network.

5.2. Node Deletion - High Linking Costs

For node deletion we know from proposition 6 that for the case of $D_v = 1$ the best the network designer can do is to build a circle containing $(n - 1)$ nodes, if he has a linking budget of $B = (n - 1)$ links. Unfortunately the case is not as clear cut for larger disruption budgets. We can show, however, the general form of networks that we expect to hold for larger disruption budgets and show that there is a tradeoff between building smaller and stronger networks or larger and weaker networks.

Lemma 15. *In any minimally connected network, the largest remaining component after an attack by a network disruptor with a disruption budget of $D_v = 1$, will be maximally of size $(n - 1)/2$* [9].

Proof Since, by definition there is no cycle in any minimally connected network, it can always be cut into at least two separate components by disrupting a single node.
Step 1. A disruptor can always do better than to take out a node such that the largest remaining component has size larger than $(n - 1)/2$. Let the disruptor take out node x with degree $\eta_i(g) = d$, which has links to nodes $y_1, y_2, , y_d$. Given that only $(n - 1)$ links are used, taking out node x leads to d separated components, which we can denote as $g_1, g_2, , g_d$. Let the node labeled y_d and the corresponding component g_d have size s, with $s > (n - 1)/2$. Then it follows that $g - g_d$, meaning the network obtained when component g_d is removed, has size smaller than $(n - 1)/2$. By instead disconnecting y_d in g_d, the disruptor can assure that the componentg_{z_d} of nodes connected to a neighbor z_d of y_d has a size of at most $(s - 1)$, so that the size of this component is at most $(n - 1)/2$. At the same time, we have already seen that the size of component $g - g_d$ is smaller than $(n - 1)/2$. It follows that the disruptor is better of by disrupting y_d. It follows that a disruption strategy where a largest component larger than $(n - 1)/2$ is left can never be optimal for the disruptor.
Step 2. Given that by Step 1 a network disruptor never leaves a largest component larger than $(n - 1)/2$, the best that the designer can possible do is to leave a largest component of exactly size $(n - 1)/2$. □

The intuition behind this proof can be seen in figure 12. That such networks exist for which the most harm a network designer can cause is actually leaving a largest remaining component of $n/2$ nodes, can be seen from the example of the *line* network. While the line network certainly is not the only minimally connected network for which this lemma holds, it shows in a very straight forward way, that this kind of networks do exist. The node that will be deleted in any such network is the most central node in terms of

[9] This holds for an odd number of nodes. For an even number of nodes the size will maximally be n/2.

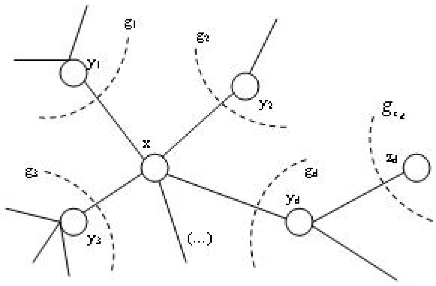


Figure 12: Minimally Connected Network

closeness of the network. Thus it is the node which has the shortest path to all other nodes in the network. Unfortunately, it is not so straightforward to extend to cases where the disruption budget is larger than 1. You cannot simply disrupt the two most central nodes. However, we can generalize what we have found for a disruption budget of 1, into a general formula. Then in general, no largest remaining component in a network will be larger than $(n - D_v)/(D_v + 1)$, as that is a general expression for $(n-1)/2$ we have found in the case of a disruption budget of 1.

Lemma 16. *In any minimally connected network, the largest remaining component after an attack by a network disruptor on the nodes of the network with a disruption budget D_v, will be maximally of size $(n - D_v)/[(D_v) + 1]$* [10]*.*

Proof We prove this by induction. Step 1 is the base step, step 2 the inductive step.
Step 1. The largest remaining component for $D_v = 1$ has size $(n-1)/2$, as can be seen from Lemma 15.
Step 2. Consider the subclass of all networks in which there is at least one node i such that $N_j(g_{-ij}) = (n - D_v)/(D_v + 1)$. We show in this step that, if the largest remaining component for $D'_v = (D_v - 1)$ is $(n - D'_v)/(D'_v + 1)$, then the largest remaining component for D_v is $(n - D_v)/(D_v + 1)$. The fact that a node j exists as specified above means that, after deleting j, a connected component remains with exactly the following number of nodes: $n - (n - D_v)/(D_v + 1) - 1 = n(D_v + 1)/(D_v + 1) - (n - D_v)/(D_v + 1) - (D_v + 1)/(D_v + 1) = (n * D_v - 1)/(D_v + 1)$. By assumption, for $D'_v = (D_v - 1)$, the largest remaining component after deletion of D'_v nodes from the component with size $(n * D_v - 1)/(D_v + 1)$ has size $[(n * D_v - 1)/(D_v + 1) - (D_v - 1)]/D_v$. By means of some simple steps of calculations this is simply equal to $(n - D_v)/)D_v + 1)$, which completes the proof of this step.
Step 3. Steps 1 and 2 show that the proposition holds for the subclass of networks in which there is at least one node i such that $N_j(g_{-ij}) = (n - D_v)/(D_v + 1) + 1$.
Step 4. Consider now the subclass of networks that do not contain any node i such that $N_j(g_{-ij}) = (n - D_v)/(D_v + 1)$. Then there must be nodes j such that $N_j(g_{-ij}) > (n - D_v)/(D_v + 1)$; at the same time, for each neighbor k of j other than i, removal of this node k results in disconnection of a component smaller than $(n - D_v)/(D_v + 1)$. But it follows simply then that if j is removed, the removed nodes do not form a component that is larger than $(n - D_v)/(D_v + 1)$ nodes. The remaining, non-removed nodes are now in a component smaller than $[n - (n - D_v)/(D_v + 1) - 1]$. Using induction, in the same way as in Steps 1 through 3, it follows that the largest remaining component after disruption also has size at most $(n - D_v)/(D_v + 1)$ for this subclass of networks. □

However, if we do not include all nodes into the connected component, the network designer can build a stronger network, by leaving one node out of the connected component, and building a circle network

[10] Again this holds for odd numbers of nodes.

of the remaining $(n-1)$ nodes. By proposition 6, we know that the network is then *(max - 1)*-proof. Thus the largest remaining component in the post-disruption network will contain $(n-2)$ nodes. We can now generalize this for a larger disruption budget.

Lemma 17. *In a circle network, the network disruptor with a disruption budget of D_v will cause maximal damage by cutting the network into* D *separate components, each maximally of size $(n-D)/D$* [11].

Proof *Step1*. Suppose we have a circle network of size n. Then we know that it is a 2-regular network with exactly n links. For a disruption budget of $D_v = 1$, we know that the network disruptor can disconnect only the node he disrupts, leaving a post-disruption network of $n-1$ nodes connected in one component.
Step 2. For a disruption budget of $D_v = 2$, the network disruptor can disconnect all nodes that are in between the two nodes he disturbs, because as we have shown that all nodes are on a circle. Thus taking out 2 nodes that are not directly linked leads to the separation of the network. Knowing this, the network disruptor will cause maximal damage by making the separated part as large as possible, however, not larger than $n/2-1$ because then the remaining component would be smaller than that, and we are only interested in the largest remaining component. Thus the network disruptor will separate $n/2-1$ nodes from the network, leaving a post disruption network of two separate components of size $n/2-1$.
Step 3. Taking any positive disruption budget D_v, the network disruptor can separate any nodes from the network that lie between any two of the nodes he disrupts, thus separating the network into D parts. Since we are only concerned with the largest remaining component, making all parts equally large is the best option because otherwise, by making one part smaller, he would automatically make another one bigger, since the pre-disruption network was a circle. Thus, to cause maximal damage, he will cut the network into D equally sized parts.
Step4. The size of the parts is then determined by the number of nodes that are disrupted. Since if D nodes are disrupted, only $(n-D)$ nodes are left in the network, the parts will be of size $(n-D)/D$. □

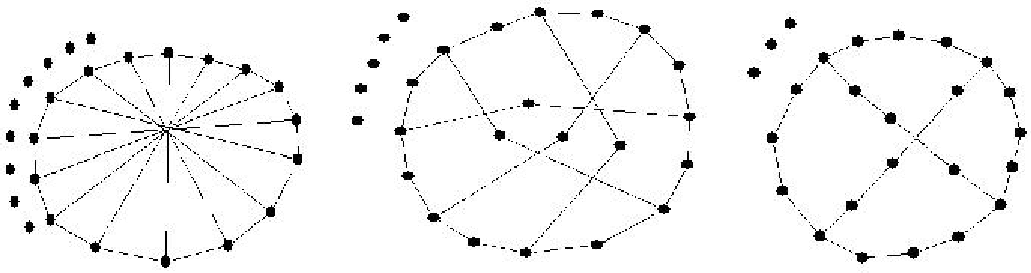
As we can already see for the case of a disruption budget of 1, this implies that there is a tradeoff for the network designer between building a large but weak component, and building a smaller, stronger component. If we increase the complexity of the model more and allow for the network disruptor to have a positive disruption budget up to the size of $D_v = B/2$, we see this trade off even more explicitly. Thus to see that it is never a good idea, to build a network encompassing all nodes, given a linking budget of $B = (n-1)$, we need to show that $(n-D)/(D+1) < (n-D-1)/D$. Here it is $(n-D-1)$ and not simply $(n-D)$ because in a circle network for a linking budget of $n-1$, we can only use $n-1$ nodes and not all n nodes. If we solve this inequality for D, we receive that for any D smaller $(n-1)/2 = B/2$, building a circle network is the better solution. This means that it is a better solution to build a circle network than a minimally connected network if facing a network disruptor, for all interesting cases, because any disruption budget larger or equal to $B/2$, will lead to a complete disruption of the network into all single nodes.

Proposition 14. *When facing a network disruptor with a positive disruption budget smaller $B/2$, a network designer with a linking budget of $B = (n-1)$, will never build a network encompassing all* n *nodes.*

Proof By Lemma 15 we know that the largest remaining component in a minimally connected network after the disruption by a network disruptor with a disruption budget of D_v, will be maximally of size $(n-D)/(D+1)$. By Lemma 17 we know that the largest remaining component in a circle network after the disruption by a network disruptor with a disruption budget of D_v, will be $(n-D-1)/D$ for a network using a linking budget of $B = (n-1)$. Solving this inequality, it can be shown that for any $D < B/2$, the post-disruption network in a circle network will always be larger than the post-disruption budget in a minimally connected network. □

[11] Abstracting from issues of divisibility.

This of course does not imply that the circle network is the best possible network for the network designer to build. What it does show, however, is that it is never good to build a network including all nodes, if you have a limited linking budget. It also implies, though, that there is a tradeoff between building a larger and a stronger network. Here the tradeoff only deals with one single node, however, this result hints that better networks may exist, where even less nodes are used, but that are more highly connected and therefore stronger. However, this leads to multiple different pre-disruption networks that are all equally good. Since these cases are hard to characterize, we will only hint at what such networks can possibly look like by means of an example.
We have already shown in the case of the low cost links, that to make his network maximally robust against any attack, the network designer would have to build an optimally connected symmetric r-regular network with $r = D_v + 1$. However, due to the limited linking budget this would lead to leaving out already a considerable amount of nodes. For a disruption budget of $D_v = 2$, this would then lead to building a connected, symmetric 3-regular network. Thus knowing the linking budget of $B = (n-1)$, and that the network designer needs exactly $3/2 * n$ links to make a network 3-regular, leads to the conclusion that the network designer is forced to leave $1/3 * (n-1)$ nodes out of the connected network to build a symmetric 3-regular network. Now taking as an example a network with n=25 nodes and a linking budget of B=24 links that is build in 3 different ways in figure 13.



(a) 3-regular (b) bipartite (c) 3 nodes left out

Figure 13: Different 25 node networks

The 3-regular network in graphic a, only uses $2/3 * B$ nodes, as has been calculated above. In network b, there is exactly one node between any two highly connected nodes. Thus we know that the post-disruption network will consist of 3 nodes less than the pre-disruption network. In network c, there are 3 nodes between any two highly connected ones. Therefore we know that any post disruption network will consist of 5 nodes less than the pre-disruption network. However, the second factor that we need to take into account is the size of the pre-disruption network. Network c, uses 22 nodes, network b uses 20 nodes and network a uses only 16 nodes. Therefore, although less damage in terms of disconnected nodes can be done to network a, as compared to b and c, the post-disruption network might still turn out to be smaller than in the larger networks. In this particular example, we can see, that networks b and c have the largest post-disruption network, since they contains a connected component of 17 nodes, as compared to 14 in network a. Even in this small example with a limited number of nodes only, we can see that there is a definite trade-off between including more nodes in the pre-disruption network and making a stronger network. It can be seen that the 3-regular network has a smaller post-disruption network than the larger and less strong networks b and c. However, when comparing this to the cycle network, we have shown in Lemma 10 above that the largest remaining component will only consist of 11 nodes, which is even smaller than the post-disruption network in the 3-regular network. Thus, a circle network seems to be a too weak pre-disruption network.

We have seen in this section that while there is a tradeoff between larger and stronger networks for the case of node deletion, no such tradeoff takes place in the case of link deletion. Therefore, the most robust network topology is quite different for the two cases. In the link deletion case, it is always optimal to include all nodes in the pre-disruption component, whereas in the node deletion case, the network designer is better off leaving out a number of nodes to build a smaller but stronger pre-disruption network. In general it seems that nodes are harder to protect in a network then links, not only because in the node deletion case nodes will be disrupted by definition in the node disruption case but also because all links attached to a node are disrupted once the node is disrupted. Therefore it is much harder to keep nodes safe from disruption than to keep links safe.

6. Conclusion

So far the literature on networks has mainly focused on the cooperative side of networks. In contrast to this, in this paper we investigated optimal network design when there are increasing benefits to linking nodes, while links are costly, and when the designer faces a strategic network disruptor, who is either able to delete a number of links or a number of nodes.

By treating two approaches, focusing separately on having a fixed size for a post-disruption network trying to use minimal links to achieve this on the one hand and, on the other hand having a fixed linking budget, looking for a maximally robust network given this constraint, we could show that the optimal structure of a firm network does not solely depend on the size of the network and the size of the expected attack, but also on the price of the links between nodes. If these links are not very costly, it is easy for the network designer to focus on building a maximally proof network, thus starting from the first approach we introduced. If links, on the other hand, are very costly, it is more reasonable to fix a linking budget and do the best he possibly can, given this budget.

We have shown that structure becomes increasingly important if links between nodes are very costly. Then the topology of the network does not only depend on the size of the disruption budget that the network disruptor has but also on the network designer's expectation on whether the attack is directed on the nodes or links of his network. If it is directed on the links, he will include all nodes in the pre-disruption network and arrange then in form of a star network, thus a hierarchical network with one key player. If the attack, however, is directed on the nodes of the network, the network designer faces a trade-off between the size of the pre-disruption network and the strength of that network, since it is always better to not include all nodes within the network. In both cases it is clear that forming clusters or local cliques is not a good mechanism, since these clusters are likely to become targets of attack.

Our results are in line with some of the research that has been done on this topic however, due to our difference in focus from most other work, other results are contrary to previous findings. The findings by Albert et al. (2000) on scale-free networks, are basically that there are a few nodes with a lot of links and lots of nodes with few links. Therefore the network is safe against a random attack on nodes because the chance that one of the highly connected nodes will be hit is very low. Against targeted attacks, however, this network is not safe. This can be found in our results as well, since we show that the star network, while being optimal for link deletion is the worst case scenario for node deletion. The work by Dekker and Colbert (2004) can be interpreted as our case of low linking costs. They find that a symmetric network is the most robust to attack. Our result is broader in the sense that is also allows for non-symmetric networks as long as they fulfill some specifications. As they are not concerned with linking costs, they do not have results about the minimality of these networks though, which is where we add to their results. A third paper that we can compare our results directly with, is by Goyal and Vigier (2009). Their focus on the spread of detection, which they share with most of the crime network literature, as well as their defense mechanism of defending one vulnerable node, leads them to optimal networks that completely differ in shape from optimal networks in our model, as they find that for node deletion the robust network is a star. This can be explained by their protection mechanism, which will protect the central node and thereby considerably lessen the chances of a successful attack on the network that will cause any considerable damage. Our method of defense, adding additional links, on the other hand, makes a star network the most hard to protect network, and therewith the network whose protection is the most expensive.

Of course this work is exploratory work and there is still a lot of room for further research. The first step being to research how exactly networks should be structured in the case of node deletion, what happens once the network designer has any positive defense budget and in what relation the size of the network stands to the post-disruption network. For this it will be necessary to deal more with the mathematical discipline of graph theory, which, if used properly can be enormously helpful. However, since they have a different goal-setting it needs to be carefully reflected which results can be used in economic theory.

Bibliography

References

Albert, R., Jeong, H., and Barabasi, A.-L. (2000). Error and attack tolerance of complex networks. *Nature*, 406(6794):378–382. M3: 10.1038/35019019; 10.1038/35019019.

Baccara, M. and Bar-Isaac, H. (2008). How to organize crime. *The Review of Economic Studies*, 75(4):1039–1067.

Bala, V. and Goyal, S. (2000). A noncooperative model of network formation. *Econometrica*, 68(5):1181–1229.

Ballester, C., Calvo-Armengol, A., and Zenou, Y. (2006). Who's who in networks. wanted: The key player. *Econometrica*, 74(5):1403–1417.

Berdica, K. (2002). An introduction to road vulnerability: what has been done, is done and should be done. *Transport Policy*, 9(2):117–127.

Bier, V., Oliveros, S., and Samuelson, L. (2006). Choosing what to protect: Strategic defensive allocation against an unknown attacker. *Journal of Public Economic Theory*, 9:1–25.

Bloch, F. (2002). Coalitions and networks in industrial organization. *The Manchester School*, 70(1):36–55.

Bollobás, B. and Riordan, O. (2003). Robustness and vulnerability of scale-free random graphs. *Internet Mathematics*, 1(1):1–35.

Chartrand, G. (1977). *Introductory Graph Theory*. Dover Publication, New York.

Dekker, A. and Colbert, B. (2004). Network robustness and graph topology. In Estivill-Castro, V., editor, *27th Australasian Computer Science Conference*, volume 26, pages 359–368.

Diestel, R. (2005). *Graph Theory*. Springer Verlag, Heidelberg.

Enders, W. and Su, X. (2007). Rational terrorists and optimal network structure. *Journal of Conflict Resolution*, 51(1):33–57.

Frank, A. (1995). *Connectivity and Network Flows*, pages 111–178. Handbook of Combinatorics. Elsevier Science B.V., Amsterdam, 1 edition.

Goyal, S. (2009). *Connections: An Introduction to the Economics of Networks*. Princeton University Press, Princeton.

Goyal, S. and Vigier, A. (2009). Robust networks.

Jackson, M. O. (2006). *The Economics of Social Networks*, pages 1–56. Advances in Economics and Econometrics, Theory and Applications: Ninth World Congress of the Econometric Society (Volume 1). Cambridge University Press, Cambridge, 1 edition.

Jackson, M. O. and Wolinsky, A. (1996). A strategic model of social and economic networks. *Journal of Economic Theory*, 71(1):44–74.

Menger, K. (1927). Zur allgemeinen kurventheorie. *Fundamenta Mathematicae*, 10:96–115.

Taylor, M., Sekhar, S., and D'Este, G. (2006). Application of accessibility based methods for vulnerability analysis of strategic road networks. *Networks and Spatial Economics*, 6(3):267–291. M3: 10.1007/s11067-006-9284-9.