Tjalling C. Koopmans Research Institute

Discussion Paper Series nr: 10-13

Strategic Network Disruption and Defense

Britta Hoyer
Kris De Jaegher

Universiteit Utrecht

Utrecht School of Economics

Tjalling C. Koopmans Research Institute
Utrecht School of Economics
Utrecht University

Kriekenpitplein 21-22
3584 EC Utrecht
The Netherlands
telephone +31 30 253 9800
fax +31 30 253 7373
website www.koopmansinstitute.uu.nl

The Tjalling C. Koopmans Institute is the research institute and research school of Utrecht School of Economics.
It was founded in 2003, and named after Professor Tjalling C. Koopmans, Dutch-born Nobel Prize laureate in economics of 1975.

In the discussion papers series the Koopmans Institute publishes results of ongoing research for early dissemination of research results, and to enhance discussion with colleagues.

Please send any comments and suggestions on the Koopmans institute, or this series to J.M.vanDort@uu.nl

ontwerp voorblad: WRIK Utrecht

How to reach the authors

Please direct all correspondence to the first author.

Britta Hoyer
Kris DeJeagher
Utrecht University
Utrecht School of Economics
Kriekenpitplein 21-22
3584 TC Utrecht
The Netherlands.
E-mail: b.hoyer@uu.nl

Utrecht School of Economics
Tjalling C. Koopmans Research Institute
Discussion Paper Series 10-13

Strategic Network Disruption and Defense

Britta Hoyer
Kris De Jaegher

Utrecht University School of Economics

update version March 2012

Abstract

We study a game between a network designer, who uses costly links to connect nodes in a network, and a network disruptor who tries to disrupt the resulting network as much as possible by deleting either nodes or links. For low linking costs networks with all nodes in symmetric positions are a best response of the designer under both link deletion and node deletion. For high linking costs the designer builds a star network under link deletion, but for node deletion excludes some nodes from the network to build a smaller but stronger network. For intermediate linking costs the designer again builds a symmetric network under node deletion but a star-like network with symmetric weak spots under link deletion.

Keywords: strategic network disruption, strategic network design, non-cooperative network games

JEL classification: C72, D85

1. Introduction

The rise of social networking sites such as Facebook, LinkedIn, MySpace and more recently Pinterest have made people more aware than ever that networks are a part of their daily lives. Consequently the study of networks in economics and sociology as well as in other disciplines has increased in both empirical as well as theoretical work. A large part of the recent economic literature regarding networks (for an overview, see Goyal (2009)[1]) has focused on strategic network formation and games being played on networks. Thus, one of the principal concerns of this literature is the cooperative side of networks. What has been generally ignored so far (at least in economics research) is that networks, once they are formed may be attacked from the outside. If the network itself is a commodity, such as is the case for military communications networks or terrorist networks, the network itself, or the players within the network, might become targets of an outside force attacking the network. Here an outsider's intention in attacking part of a network may be to cause damage to a particular person but by attacking a very central person or communications line, they might indirectly damage the network as a whole. Thus not only the individuals in the network are threatened by an attack but also the network as a whole is threatened. Arguilla and Ronfeldt (2000) refer to this concept of fighting against networked adversaries as "netwars". Dekker and Colbert (2004) find that two trends have recently emerged in military as well as civilian communications. The first is that the communications sector has become increasingly centered around networks and the second is that there is an "increasing threat to communications infrastructure. In the civilian sphere, the threat is from terrorist attacks, while in the military sphere this comes from the increasing tendency to view communications networks as high-value targets."(Dekker and Colbert, 2004, p.359).

If we are abstracting away from information decay, without taking into account such a threat of an attack, network structure does not matter a lot. For example, if there is no threat of an attack, it does not matter whether a military communications network looks like a star where all communication goes through one single player or whether it is structured as a line. However, if the nodes are under attack, taking out the central player completely destroys the star, whereas the line network the network is only cut in half. If the communication links themselves are under attack rather than the nodes, taking out one link in the star network does not make a lot of difference, whereas taking out the central link in the line network cuts the network in half. To counteract such impending attacks a number of measures can be taken. What we are looking at here is adding additional links to the network that would otherwise be redundant to keep the players within the network safe. The following examples illustrate the type of games we are looking at.

- Military units and the communication links between them can together be considered as military networks.[2] Particularly, if communication has to be achieved over larger distances these communications links are subject to interruptions that can be caused, for example, by the deliberate jamming of frequencies[3] (link deletion) or by deliberate elimination of units that enable communication (node deletion). Designers of such communications networks must therefore take such deliberate attacks into account and build networks that will still be functional in the event of such an attack. Thus, in the absence of a threat, using additional frequencies to communicate between two units is redundant and causes the network designer to incur unnecessary costs. If there is a threat, however, they can be used to make the network safe against the disruption of links.

- Criminal or terrorist organizations communicate through intricate networks.[4] Once such a network structure is known, the police or counter terrorist forces have the possibility to either attack the communication links between different members or the members themselves. The information and the

[1] For a good introduction on the literature and research on social and economic networks see Jackson (2008).

[2] For a comprehensive overview of military and security networks with references outside the field of game theory see Lipsey (2006).

[3] That such a threat actually exists can be seen from the efforts taken by homeland security and other government agencies to find a disruption tolerant network. Raytheon BBN Technologies reportedly "was awarded a $81 million contract to create a collaborative technology alliance in network science" (Baburajan, 2010) and in 2010 demonstrated a field experiment of a disruption tolerant military network (Baburajan, 2010).

[4] See for example the analysis of the terrorist cell networks after 9/11. For an interesting anthology on netwars as a whole, see for example Arguilla and Ronfeldt (2000) which interestingly enough has been published before 9/11.

possibilities of attack decide on which approach is feasible. However, depending on the structure of the network, either approach may lead to a complete breakdown in communication between some or all of the players.

While it is important how these networks are created, work together and what technologies they use, Arguilla and Ronfeldt (2000, p.xi) state that "the defining level of a netwar actor is its organizational design. (...) To cope with a network, analysts must first learn what *kind* of network it is and then draw on the best methods for analysis." Therefore, in this paper, we focus purely on the structure of the network and how to best defend it given a certain type of attack strategy. We are thus asking the following questions: What are the implications for the design and defense strategy of network designers when taking a possibility of disruption into account? Given the fact that additional links are used to keep the network safe, how does the cost of adding links affect network structure? Does it matter if the attack is targeting nodes or links in the network? And are there certain network structures that are inherently 'safe' against the disruption of a number of links or nodes?

To capture the influence that a threat of an attack has on the structure of the network, our paper models a sequential zero-sum game between a network designer and a network disruptor. We model network structure as being determined by a network designer, because in the first instance we want to gain insight into what is an efficient defense strategy for the network as a whole. Therefore, we can simply model the game as being played between a network designer and a network disruptor.

We begin by looking at the benchmark case in which there is no threat of a disruption. Since links are costly and we assume no decay in the network, all minimally connected networks are equally efficient.[5] Using any more links than those that are needed to build a network consisting of one component would include redundant links and since links are costly, this would not be efficient. We then proceed to look at cases where the network designer faces a network disruptor, where we first look at low linking costs, then at high linking costs and some intermediate levels of linking costs.

When linking costs are low, the network designer protects his network by constructing a regular network, where all nodes are equally well protected. Multiple architectures meet this requirement, but the designer should take care to avoid that the network includes small groups that are interconnected only by few links, as such networks are easy to disrupt(Proposition 1). This requirement is more restrictive for node deletion than for link deletion. Therefore, the set of best-response networks under node deletion is a subset of the set of best-response networks under link deletion. In general low levels of linking costs exists such that fully protected networks are the best response of the network designer to link deletion as well as node deletion (Proposition 2).

When linking costs are high, contrary to what is the case for low linking costs, the best-response architectures under link and node deletion look fundamentally different. Under link deletion, it is a best response to connect all nodes in a star network (Proposition 3). In such a network, the disruptor can only take out one node for each disrupted link. Intuitively, the star network keeps all nodes as close as possible to one another, in such a manner that the disruption of one link cannot disconnect several nodes. Under node deletion, the star network is on the contrary a very bad network, since deletion of the central node disconnects all nodes. In general, any minimal connected network is a bad response, as it can easily be cut up into components. Instead, it is a best response to leave some nodes out of the network, and build a smaller and stronger component (Proposition 6). Such components again should not involve local groups interconnected by few links.

For intermediate linking costs, the network designer finds it too expensive to fully protect all nodes. Our analysis suggests that, both under link and node deletion, the network designer constructs connected networks, i.e. does not leave nodes unconnected to construct smaller and stronger networks. But otherwise, the intuitions for high-linking costs are confirmed. Under link deletion, star-like networks should be constructed, consisting of low-degree - weak - nodes, and high-degree - strong - nodes. Just as in the star, there are multiple weak nodes, but only one can be disrupted. Also, the diameter of the network is kept

[5] A minimally connected network is a network connecting all n nodes into one component using $n-1$ links. For a definition see the graph theoretic appendix.

small so that deletion of links cannot cause large parts of the network do be disconnected. Under node deletion, whenever possible, all nodes get the same degree(Proposition 8). This is because high-degree nodes are not strong as is the case under link deletion, but would on the contrary be likely targets for disruption. This means again that the network designer does well by constructing a symmetric network

In the extensions we additionally look at the cases of imperfect information on the side of the network designer and the side of the network disruptor. We find that if the imperfect information is on the side of the network designer, his best response is to move away from the star network (Proposition 9), whereas the best response of the network designer if the imperfect information is on the side of the network disruptor, is to build a star network (Proposition 10).

The rest of the paper is organized as follows. After a short literature review in Section 2, Section 3 presents our model of design, defense and disruption of the network. Section 4 contains the analysis of cases of with low linking costs, section 5 deals with high linking costs and in section 6 we look at intermediate linking costs. In Section 7, we add some extensions to the model by looking at the case of imperfect information. Section 8 concludes. In the appendices, we give graph theoretic background in Appendix 1, while Appendices 2 and 3 contain some of the proofs.

2. Literature Review

While some aspects of network disruption have received a lot of attention in economics, we found that there is no simple model that focusses on the structural implications of adding a network disruptor to simple network formation model with homogeneous players.[6] We feel, however, that such a model is needed to provide accurate predictions of what effects network disruption will have on the structure of networks before looking at further extensions. Keeping linking costly and using only otherwise redundant links as a means of defense while at the same time allowing for an attack on either of the two building blocks of a network - namely links and nodes - allows us to make such predictions on the structure of robust network architectures, whereas the existing literature focusses on more special cases of network disruption. To give an overview, the existing work in the economics literature can broadly be grouped into two different categories according to the focus of the network disruptor.

In the first group of papers it is the network disruptor's purpose to learn as much of the information that is generated within a network as possible, whereas the network aims to keep this information secret. This group includes the work by Enders and Su (2007), Enders and Jindapon (2010), and Baccara and Bar-Isaac (2008) who take a game-theoretic approach similar to ours. In these models more links within a network allow more information to be produced. These papers then deal with the dual nature of links, which on the one hand enable information sharing but on the other hand allow the effect of an attack to spread through the network. However, since in our model the network disruptor wants to block information instead of learning it, the type of disruption modeled differs in our work. Larson (2011) also deals with the problem of the dual nature of links in a network. In his model good (e.g. news, stock tips,...) as well as bad items (e.g. viruses, biological as well as technological) can spread throughout a network. Players thus want to be as connected as possible to receive all the benefits. However, at the same time they want to not be connected at all to not receive any of the bad items. To protect themselves, players are then allowed to put effort into security, which is modeled as a screening device that will save them from receiving the bad items. A similar approach is found in Goyal and Vigier (2009), who focus on the protection of certain key nodes within the network. Here the device to protect these key nodes is modeled as a "firewall" which will keep the attack from spreading through them. Another paper that uses a similar approach is Hong (2008).[7]

[6] For a justification in terms of applications, see Arguilla and Ronfeldt (2000), who find that many networked groups are actually without leaders. Whereas this does not mean that all members of such a group are actually equal, it goes a long way in justifying the assumption of homogeneity of the nodes we use here.

[7] Kovenock and Roberson (2010) recently looked in a similar way at network defense yet their paper is less relevant to our model, as network structure is not taken into account. Instead, in their paper network vulnerability arises because of the production function generated by the nodes in the network, where in one extreme one node suffices to obtain full production and in the other case all nodes are necessary to produce.

The second group of papers centers around the topic of protecting certain key nodes on the side of the network designer and on the network disruptor's efforts to find such key players or key links to attack. In Bier et al. (2007) for example, the focus lies on defending certain nodes. In the model, a defender needs to decide how to allocate defensive efforts over two targets for attack. Just as is the case in our model, it may be optimal to defend the locations in an asymmetric way, leaving weak spots. Yet, whereas in their approach this is due to the fact that nodes have asymmetric values, in our model weak spots are simply a consequence of the network designer's modeling decisions as all nodes have equal values. In Ballester et al. (2006), the opposite approach is taken and therefore the focus lies on the disruption of the network. The "key player" in the network is defined as the node with the highest degree of Bonacich centrality (a centrality measure used in social network analysis). It is the disruptor's goal, then, to find this key player and attack it. An example of the game played is the coordination of criminal activity. As opposed to this in our model the centrality of any one player is not as important as the network can fight against a disruption by being re-organized by its designer. The focus in Hong (2009) lies on certain key links. In the model, terrorists try to carry an explosive through an exogenously given transport network, modeled as a directed flow network. By shutting down a minimal number of links, security services try to stop the explosive from reaching its destination. In contrast to that, our model focusses instead on undirected networks and network defense consists of adding links, not deleting them. McBride and Hewitt (2011) add imperfect information on the side of the network disruptor to such a model, and consider targeted as well as random attacks to the structure of the network.

In non-gametheoretic/non-economic literature related to our paper, the following papers providing related insights are worth mentioning. An influential paper is Albert et al. (2000), which treats a stochastic network generation process that yields networks with properties that are often observed in real-world networks (namely preferential attachment). It is shown that these networks are robust against random attacks, but vulnerable to targeted attacks.[8] Similarly, stars do badly in our analysis under node deletion. In the context of vulnerability of road networks, Taylor et al. (2006) treat the adding of links as a mechanism of network protection. They are interested, however, in the effect that this has on several vulnerability measures, whereas our focus is on network structure. Schwartz et al. (2011) also model a game between a network designer and disruptor. However, they focus on the connection between network reliability and security using a model of an undirected graph in which links may be unreliable. The non-gametheoretic paper most related to our work is Dekker and Colbert (2004), who study the node (link) connectivity of networks, which is the smallest number of nodes (links) which upon deletion results in a disconnected graph. Using certain graph theoretic properties that we also look at, they say that a graph is optimally connected if its node respectively link connectivity is equal to the minimal degree in the network. Finally, they show that networks that have certain symmetry properties are optimally connected. However, as is usually the case in graph theoretic literature, the authors do not consider linking to be costly and do not model strategic disruption.

3. The Model

At stage 1, for each pair of nodes (i, j) in the finite set of identical nodes N labeled $\{0, ..., (n-1)\}$,[9] the network designer decides whether or not to link i and j. The number of links any node i has, is defined as its degree of connectivity η_i. If the designer constructs a link between i and j, then we denote this as $g^1_{ij} = 1$. Links are undirected, so that $g^1_{ij} = g^1_{ji}$. If the designer does not construct a link between i and j, we denote this as $g^1_{ij} = 0$. The nodes are linked indirectly to one another 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 $g^1_{ii_1} = g^1_{i_1i_2} = ... = g^1_{i_{k-1}i_k} = g^1_{i_kj} = 1$. The set of all g^1_{ij} such that $g^1_{ij} = 1$ forms the pre-disruption network g^1.

[8] For a more strictly mathematical treatment of such models, see Bollobás and Riordan (2003).

[9] The usual labeling of nodes in the networks literature is $1, ..., n$. We diverge from this, as we later introduce a class of networks (Circulants), where the labeling needs to start from 0.

At stage 2, the network disruptor observes the pre-disruption network g^1. In the game of link deletion, he decides for every $g^1_{ij} = 1$ whether or not to remove the link between i and j. In the game of node deletion, the network disruptor decides for each node whether or not to remove it. The post-disruption network is denoted g^2 and it consists of all nodes i and j which were not directly targeted by the network disruptor in the case of node deletion and for which holds that $g^2_{ij} = 1$.

At stage 3, the players obtain their payoffs. The network designer and network disruptor each obtain a different value function from the post-disruption network g^2. The network disruptor incurs costs that are increasing in the number of links used in the pre-disruption network, the network designer incurs costs that are increasing in the number of nodes or links removed from the pre-disruption network.

Abstracting from any costs, the game between the network designer and the network disruptor is assumed to be a zero-sum game. The value of the post-disruption network to the designer is an increasing function of the value created in the network at each node. The network disruptor's payoff is a negative function of this value. The value of a node depends on the number of other nodes to which the node is connected (i.e. directly or indirectly linked). Define as $N_i(g)$ the set of nodes with whom node i is connected. 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 value to the network designer of a post-disruption network g^2 with x components is the sum of the values of each component, so $v(g^2) = v(C^1) + v(C^2) + ... + v(C^x)$. We assume $v(.)$ to be an exponential function for the following reason. In the simplest setting, the value of each node i equals the number of nodes $N_i(g)$ to which it is connected, so that in node i's component $N_i(g)$ nodes obtain a value of $N_i(g)$, showing that the value of a component may be exponential in the number of nodes it connects. If this value of a component is quite exponential in its order, then the network designer's payoff can be approximated by equating it to the order of the largest post-disruption component. Given the zero-sum structure of the payoffs, the network disruptor then minimizes the order of the largest component in g^2.

Additionally, we consciously assume away information decay (see Jackson and Wolinsky (1996)) and heterogeneous values of the nodes (see Galeotti et al. (2006)). In this way, in the absence of network disruption, any minimally connected pre-disruption architecture, [10] which uses $(n-1)$ links, is a best response of the designer. This means that, if there is a network disruptor, any restrictions that we obtain on the set of best-response architectures, or any non-minimal links in best-response architectures, are strictly there due to attempts to prevent disruption. Our model thus allows us to isolate the pure effect of defense against network disruption. Additionally, given that the nodes all have the same value, any asymmetries in network structure that we obtain are purely due to minimize the effect of disruption.

Rather than assuming an explicit cost function for the network designer and the network disruptor, we assume the following. For the network disruptor, we assume that there is a given budget of links (D_l) or nodes (D_v) that the disruptor can delete to minimize the order of the largest component in g^2. For the network designer we look at two different specifications of the model.

Approach 1:
In the first specification, we assume the designer targets a certain order[11] of the largest remaining component, and looks for the lowest number of links with which the designer can achieve this. In particular, we also consider at this point the case where the network designer keeps all nodes in his network in one connected component even after disruption.[12] We use the term *max*-proof networks to refer to such fully protected networks. Looking at such networks, it is obvious that while for link deletion a fully protected network includes as many nodes in one connected component before and after disruption, for node deletion any node that is attacked is also taken out. In order to make it easier to compare the results for link and node deletion, we thus define *max*-proof networks as follows:

[10] For definitions and proofs concerning the graph theoretic terms used in this paper see the Appendix.

[11] The order of the network is the size of the network in terms of the number of nodes it includes. This term is used rather than size so as to avoid confusion, as it is commonly used in graph theory.

[12] For node deletion this of course means only all nodes that were not specifically targeted by the network disruptor.

Definition 1. *A pre-disruption network g^1 is said to be* max-*proof against a link (node) deletion budget $D_l(D_v)$ if the largest remaining post-disruption component upon strategic link (node) deletion contains exactly n nodes (exactly $(n - D_v)$ nodes) for the case of link (node) deletion.*

Approach 2:
Alternatively, we assume in a similar fashion as we did for the disruptor, that in both the link and node deletion game, the network designer has a fixed budget B of links, that he can use to construct network g^1. The simplifying assumption about the cost function of the network designer is without loss of generality, as any network designer whose costs are increasing in the number of links used will seek to maximize payoff for any number of links used, and will always try to achieve any payoff level with a minimal number of links. The same holds for the assumption about the cost function of the network disruptor. Given this linking budget, the designer maximizes the order of the largest component in g^2.

While the two approaches that we use to model the decisions of the network designer (maximizing the size of the largest component for a fixed linking budget and minimizing the number of links used for achieving a post-disruption component of a fixed order) at first seem very different from one another, we will show that they are complementary to one another. In section 4, we assume low linking costs and take the assumption that the network designer has enough links to make his network completely proof against disruption as a starting point. We then look at the minimal amount of links needed to achieve such proofness (Approach 1). In section 5 on high linking costs, on the other hand, we take the number of links as given and look for the maximal degree of proofness we can reach with this (Approach 2). While we chose to take the different approaches for each section, because it makes the analysis more tractable, the results are complementary and can in both cases be interpreted as describing the network designer's best response. At the end of the respective sections, we shortly interpret the results given either one of the approaches.

The Network Disruptor's best response: For any given pre-disruption network, the disruptor's best response can be found by going through the following procedure. 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 disruptor chooses a best response in the form of an optimal network disruption strategy. Before we define the algorithm to find the network disruptor's best response, we need to introduce some graph theoretic concepts of connectivity that will be used in the algorithm. The formal definitions of these concepts can be found in the graph theoretic Appendix.

The connectivity of a graph can be considered in terms of nodes and links. The node connectivity κ of a graph, is defined as the smallest number of nodes whose removal from the graph will lead to a disconnected graph or a single node. The link connectivity λ of a graph, is defined as the smallest number of links whose removal from the graph will lead to a disconnected graph or a single node. From these definitions follow the definitions of node (link) cuts. A node (link) cut V (L) is a set of nodes (links) whose removal will lead to a disconnected graph or single node. Thus for any given graph, a node (link) cut has to be of at least cardinality κ (λ).[13]
The Algorithm:

1. Consider the degree of connectivity. If $D_l < \lambda$ ($D_v < \kappa$), no link cut L (node cut V) exists, thus no node can be disconnected. Stop. Otherwise move on to next step.
2. Consider the cardinality of all link cuts L (node cuts V) such that g_{-L} (g_{-V}) is the empty graph. If $L \leq D_l$ ($V \leq D_v$), it is a best response for the network disruptor to delete this link cut (node cut). Stop. Otherwise move on to the next step.
3. Consider the cardinality of all link cuts L (node cuts V) such that the smallest connected component in g_{-L} (g_{-V}) is or order 2. If $L \leq D_l$ ($V \leq D_v$), it is a best response for the network disruptor to delete this link cut (node cut). Stop. Otherwise move on to the next step.

[13] A well-known theorem in graph theory (Whitney's Theorem) then states that $\kappa \leq \lambda \leq \eta_i$. For a proof of this, see for example Diestel (2010) (p.12).

Continue until a link cut (node cut) is found. By step 1 we know that one has to be found, otherwise the disruptor should have already stopped after step 1.

We have also considered more standard economic concepts, such as betweeness centrality, Bonacich centrality, degree centrality or closeness centrality, to define which links (nodes) the disruptor will target. However, in our model, the network designer responds to a threat of disruption. He will therefore avoid central links (or nodes) as much as possible. This in turn then makes an analysis of the disruptor's strategy in terms of centrality futile.

4. Low Linking Costs

We begin our analysis by taking *Approach 1* as discussed in the modeling section. We consequently assume that the linking costs are so low that the network designer will always aim for full protection of his network - thus he will build a *max*-proof network. We denote the set of all networks that are *max*-proof against a link deletion budget of D_l as $\Gamma_{D_l}^{max}$ and those that are *max*-proof against a node deletion budget of D_v as $\Gamma_{D_v}^{max}$. As linking is costly, a network designer that aims at achieving *max*-proofness will do this with a minimal number of links. This leads us to the definition of minimal *max*-proofness.

Definition 2. *A network g is said to be **minimal** max-proof against a node (link) deletion budget D_v (D_l), if no network exists that achieves max-proofness using less links.*[14]

We denote the set of all networks that are minimal *max*-proof against a node (link) deletion budget of D_v (D_l) as $\Gamma_{D_v}^{max,min}$ ($\Gamma_{D_l}^{max,min}$). We know from the description of the network disruptor's best response algorithm above that a necessary condition for *max*-proofness under a disruption budget of $D_v = (r-1)$ or $D_l = (r-1)$ is that each node 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 3. *An r-regular network is a network in which each node is connected of exactly degree r.*

For any given n and r, any r-regular network has the same number of links. Thus, if there is an r-regular network that is *max*-proof, it is also necessarily minimal.[15] However, to achieve *max*-proofness, each *subset* of nodes also needs to have at least $(D_l + 1)$ links to other nodes for the case of link deletion and at least $(D_v + 1)$ direct neighbors for the case of node deletion.[16] Otherwise a subset of at least order one could be disconnected (for the case of node deletion this of course means one *additional* node next to the ones that are being attacked). This is illustrated in Figure 1, which shows five networks for the case where $n = 16$. Networks (a)-(d) are 3-regular, whereas network (e) is 4-regular. Only networks (d) and (e) can be checked to be *max*-proof under link deletion with $D_l = 2$ and under node deletion only network (d) is *max*-proof against a disruption budget of $D_v = 2$.

We will formalize the conditions that networks need to fulfill to be *max*-proof in Proposition 1. Moreover, Proposition 1 also shows that for the case $D_v = D_l$, the set of minimal *max*-proof networks under node deletion is a subset of the set of minimal *max*-proof networks under link deletion. This is illustrated in subfigure (e) of Figure 1, which is only *max*-proof against link deletion but not against node deletion.[17]

[14] This concept does not coincide with the graph theoretic concept of a minimally k-connected network, which denotes that each set of k links is critical (thus the network will be disconnected by taking out any set of k links). In contrast, our concept includes the economic perspective by looking a network that achieves graph theoretic minimality of a degree $(D_l + 1)$ (respectively $(D_V + 1)$) and at the same time uses the least number of links possible to achieve this.

[15] See Lemma A.6 in the appendix.

[16] As long as the subset under consideration is smaller than $(n - D_v)$ at least.

[17] One of the central results of graph theory, known as Menger's Theorem (see for example Menger (1927), shows that the robustness of a network to node or link deletion can be defined in terms of the number of node disjoint paths (or link disjoint paths respectively). The number of node disjoint paths (link disjoint paths), is given by the number of different paths between two nodes that do not share a node (link). In this sense, the reason that network (e) in Figure 1 is not *max*-proof under node deletion, is because the top node and the bottom node gives it too few node disjoint paths going though these two nodes. There are, however, a sufficient number of link disjoint paths.

For expositional simplicity we here focus on networks for which n and/or $(D_l + 1)$ is even since otherwise issues of divisibility will occur.[18]

Proposition 1. *Let n and/or $(D_v + 1)$ (respectively $(D_l + 1)$) be even. Then $\Gamma_{D_v}^{max,min}$ (and respectively $\Gamma_{D_l}^{max,min}$) 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 link cut sets (node cut sets) of order $\lambda \leq r$ ($\kappa \leq r$), where $r = (D_l + 1)$ ($r = (D_v + 1)$).*

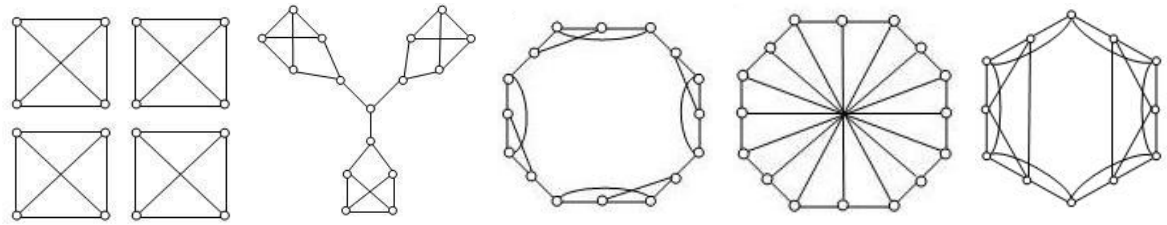
For $D_v = D_l$, it then holds that the set $\Gamma_{D_v}^{max,min}$ is a subset of the set $\Gamma_{D_l}^{max,min}$.

Proof We prove each part of the proposition separately.

(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, which is then already of an order smaller than n. The rest of the proof of this part follows by noting that all r-regular networks use exactly the same number of links and from Lemma A.6.

(ii) This follows directly from the conditions on building a *max*-proof network.

That $\Gamma_{D_v}^{max,min}$ is a subset of the set $\Gamma_{D_l}^{max,min}$ follows directly from the conditions on *max*-proofness that state that every subsets of nodes needs a certain number of links or neighbors. To ensure x neighbors, at least x links are needed. But since a subset of nodes can have links to the same node outside the set, having x links to the rest of the network does not ensure that a subset of nodes has x neighbors. □



(a) Segmented Network (b) Not *max*-proof (1) (c) Not *max*-proof (2) (d) Minimal *max*-proof (e) Proof only against link deletion

Figure 1: *Examples of Proposition 1*

From Proposition 1 and Figure 1, we can thus conclude that minimal *max*-proof networks are connected regular graphs that do not contain small node cuts or small link cuts. Intuitively, this means that networks that are *max*-proof should not contain clusters of highly connected local groups, with few links between them. Clearly, such networks are easy to disconnect. These results are also in line with the findings of Dekker and Colbert (2004) on robust network topologies. However, since they focus only on the robustness of networks and do not take into account linking costs, our class of optimal networks is considerably smaller than theirs, as we take linking costs into account.

[18]See Lemma A.8 for a proof that this is a necessary condition for the existence of r-regular networks.

As an example of a set of networks that fulfill the criteria stated in Proposition 1 and also provide a proof of existence of these networks, we can look at the set of networks that is known as circulant graphs.[19] In a subset of these graphs, each subset of nodes also has at least $(D_v + 1)$ neighbors in the network. For some examples of circulant graphs see Figure 2.

Definition 4. *A circulant graph $C_n(a_1, a_2, ..., a_k)$ or briefly $C_n(a_i)$, where $0 < a_1 < a_2 ... < a_k < \frac{n+1}{2}$, has node i adjacent to $i \pm a_1, i \pm a_2, ..., a \pm a_k$. The sequence (a_i) is called the jump sequence and the a_i are called the jumps. For expositional ease, we assume that the nodes of a graph are labeled $0, 1, 2, ..., n-1$.*

The circulant graph $C_n(1)$ gives the simple circle. In the Appendix (Lemma A.7), we show for the special case of $D_v = D_l = 1$ that the only 2-regular network is the circle containing all nodes and that this network is also *max*-proof. For any other degree of regularity there is a multitude of regular graphs which are not all necessarily circulant graphs, nor are they all minimal *max*-proof. We will therefore limit ourselves to the class of circulant graphs, showing their existence (see Appendix Lemma A.10) and that they are minimal *max*-proof for link deletion and under which conditions this also holds for node deletion.

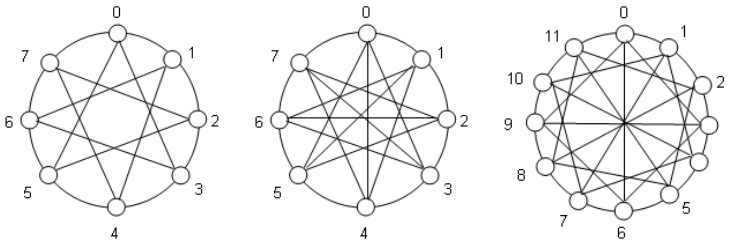
Circulant graphs, by definition, are all node-symmetric. We delegate the formal definition of node symmetry to the Appendix (X). Informally speaking, node symmetry means that every node has the same local environment so that nodes cannot be distinguished from one another based on their position in the network. To deduce that circulant graphs are *max*-proof under link deletion, we refer to some well-known graph theoretic results. In a translation of *Satz 6* in Mader (1971), Boesch and Tindell (1984) show that every connected r-regular node-symmetric graph has $\lambda = r$, where λ denotes the cardinality of the minimal link cut L of the graph, as defined in the modeling section. By the very definition of L, this then means that no subset of nodes can be disconnected from the network by a network disruptor with a disruption budget of $D_l = (r-1)$. The fact that this network is also minimal follows from the fact that a circulant network is also a regular network. Therefore we can deduce that any circulant network connected of degree r is minimal *max*-proof against a network disruptor with a disruption budget of $D_l = (r-1)$. While this may seem like a big restriction on the set of regular networks that is minimal *max*-proof, this is not the case. Gao (2010) shows that random r-regular graphs are asymptotically almost surely r-connected (thus that the link cut $\lambda = r$) for any even constant $r \geq 4$.

For the case of node deletion, we need to restrict the set of networks a bit further to find those networks that are minimal *max*-proof. This is due to the fact that the condition of having $(D_l + 1)$ links to the rest of the network for any subset of nodes is always met if these nodes have $(D_v + 1)$ neighbors but not the other way around, as the links could go to the same node. Indeed, it can be seen in circulant graphs such as $C_8(1, 3, 4)$ which is regular of degree $r = 5$, however, the cardinality of the node cut V is only 4, since it can be disconnected by taking out nodes $1, 3, 5$ and 7. For a depiction of this see Figure 2(b). However, Boesch and Felzer (1972) have shown that if the jumps in a circulant graphs are convex, i.e. $a_{i+1} - a_i \leq a_{i+2} - a_{i+1}$, where $1 \leq i \leq k-2$ and $a_1 = 1$,[20] then the cardinality of the node cut V fulfills $\kappa = r$. For a graph that fulfills this condition, see Figure 2(c). Thus, if this is fulfilled, circulant graphs or degree r are minimal *max*-proof against a network disruptor with a disruption budget of $D_v = (r-1)$. While convexity ensures that $V = \kappa = r$, it is not a necessary condition, as can be seen by the example of $C_{16}(1, 5, 7)$, which is not convex but has $V = \kappa = r$.

Looking at *Approach 2*, thus looking for the minimal number of links with which a certain level of proofness can be ensured, we have thus shown that the minimal number of links needed to ensure *max*-proofness against a disruption budget of size D is $n * \frac{D+1}{2}$. Starting from this linking budget, the highest level of proofness that can be achieved is obviously *max*-proofness. Consequently, given that the characterized networks both use a minimal number of links for the level of protection specified and do the best that can be done given the number of links, we can deduce that an explicit cost function must exist for which building a *max*-proof network is the network designer's best response. Particularly, what is required for this is that linking costs are low.

[19] The definition and notation given below follows the one given by Boesch and Tindell (1984).

[20] Here we follow the notation of Boesch and Tindell (1984).



(a) $C_8(1,3)$ (b) $C_8(1,3,4)$ (c) $C_{12}(1,3,6)$

Figure 2: Circulant graphs

Proposition 2. *Low levels of linking costs exist such that* max*-proof networks are the best response for the designer under both link deletion and node deletion.*

Proof Follows directly from the discussion above and Proposition 1. □

From the previous section it is straightforward to see that for a given number of nodes, n, and for $D_l = D_v$, the same amount of links is needed to build a network that is *max*-proof against node deletion or against link deletion and in principle the same structure is also needed, even though under node deletion more nodes will necessarily be taken out.[21] Thus if it is the designer's purpose to protect some absolute number of nodes, more links are needed in the case of node deletion than in the case of link deletion, but the structure of the best response network remains the same. In terms of the military communications application introduced earlier, this means that for low linking costs it need not matter for the structure of the best-response network if the attack is directed at the physical parts of the network (thus the nodes) or at the frequencies (the links). If additional links are used as a defense mechanism and those are relatively cheap to introduce, then constructing a rather highly connected symmetric network is always a best response. A number of alternative best responses to symmetric networks exist both under node deletion and under link deletion. These alternatives have in common that the designer does not construct local groups with few links between the groups. To conclude from this that when facing node deletion and link deletion the same structure will prove a best response in any network for any levels of linking costs, however, would be wrong. As we will presently show, for higher linking costs it is indeed no longer true that the same network structures can be used as best responses under node deletion and link deletion. We start in the next section by looking at the other end of the scale, where linking costs are very high.

5. High Linking Costs

In this part of the analysis we are looking at prohibitively high linking costs, which leads to a linking budget of only $B = (n-1)$ links. Adding additional links is thus prohibitively expensive. The network designer has to deal with the fact that some nodes will be disconnected from the network and prefers this to adding additional links, because such links are simply too expensive. As we have discussed in the modeling section, if there is no threat of an attack on the links of the network, all minimally connected networks are best responses as the network designer receives the same payoff irrespective of which minimally connected network he chooses to build. Given the fact that for any given n there is a whole range of minimally connected networks,[22] structure thus does not matter. As in the case of low linking costs, however, due to

[21] Of course the actual size of the largest remaining component is smaller for node deletion than for link deletion, but building a *max*-proof network is the best that the network designer can achieve in both cases and the way the network needs to be structured to reach *max*-proofness is the same.

[22] By Cayley's formula we know that there are exactly n^{n-2} different minimally connected networks for each n. For a proof of this, see for example Bondy and Murty (2008) Theorem 4.8.

the threat of disruption the structure of the network now becomes decisive again. While in the case of low linking costs, the same type of architectures are best responses (with the case of node deletion being more restrictive), here it quickly becomes apparent that fundamentally different architectures are best responses under link deletion compared to node deletion. This is obvious by simply looking at minimally connected networks. While under node deletion the network disruptor can completely disconnect the star network by taking out the central node, the maximum damage he can cause to the line network is to split the network into two separate components, thereby leaving a largest remaining component of $n/2$. For link deletion, however, the star network 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 line network can be cut in half. We will start by analyzing the link deletion case, and then turn to the node deletion case. For both cases, we also look at $B = (n - x)$ and $B = n$ as a sensitivity analysis.

5.1. Link Deletion - High Linking Costs

We will show in the following that the star network is the network structure that is the strict best response of the network designer who faces a network disruptor with a disruption budget of $D_l \geq 0$. In the star network, the maximal damage a network disruptor with any positive disruption budget can cause is to disconnect exactly D_l nodes.[23] To show that the star is the most robust network structure for a linking budget of $B = (n - 1)$ and a disruption budget of D_l, we need to prove that the minimal damage that can be caused in any minimally connected network that is not the star, is always larger than the damage that can be done to the star for the same disruption budget. Additionally, we need to show that in any segmented network where the connected component is smaller but stronger, in the sense that the network designer leaves out some nodes to use additional links to make his network more proof against attack, the largest remaining component will never be larger than the largest remaining component if g^1 is the star network (Lemma 2). Therefore, to show that the star network dominates all other network structures in this case, we need to prove that in every non-star network at least $(D_l + 1)$ nodes can be disconnected from the connected component (thus more than in the star network).

Lemma 1. *Under link deletion, a network disruptor with a disruption budget of D_l, can disconnect at least $(D_l + 1)$ nodes in every non-star minimally connected network.*

Proof Assume $n \geq 4$. We first show that every non-star, minimally connected network has a diameter of 3 or larger, where diameter is defined as the maximal distance between any two nodes in the network. There need to be at least 2 end-nodes in any minimally connected network, since by definition any minimally connected network does not contain a circle.[24] Take any minimally connected network and let node k be an end-node (thus connected of degree $\eta_k = 1$). By definition, node k must have a link to a node i in the network (otherwise the network would not be connected). Since the network is not a star, node i cannot receive another $(n - 2)$ links, next to link g_{ki}. Therefore there needs to be at least one more node h, which is only linked to i indirectly through node j. The distance between node k and h is then 3 and no matter how else the network looks, it has at least diameter 3. Consequently follows that if we delete link g_{ij}, at least 2 nodes are separated from the largest remaining component. This is because either nodes i and k are separated from the largest remaining component, or nodes j and h (possibly along with further nodes to which they are connected). The $(D_l - 1)$ remaining links that are deleted each time result in the separation of at least one node, as every link in a minimally connected network is a link cut.[25] □

Thus, the star network is strictly better than any other minimally connected network in the case of link deletion and high linking costs, since the largest remaining component after disruption in a star network

[23] See Lemma A.4 in the Appendix

[24] For proof see e.g. Bondy and Murty (2008) Proposition 4.2.

[25] See Bondy and Murty (2008) Proposition 4.1, which states that in a minimally connected network each two nodes are connected by exactly one path. Therefore, it holds that in a minimally connected network the k-connectivity is equal to one and each link is a link cut.

is of order $(n - D_l)$ (see Lemma A.4), whereas for any other minimally connected network it is maximally of order $(n - D_l - 1)$ as has been shown in Lemma 1.

Next to other minimally connected networks, the network designer could also decide to leave certain nodes isolated and make the connected component smaller but stronger. We know from the graph-theoretic Appendix that no minimally connected network contains a circle and in any network that is not minimally connected there is at least one circle. To build a circle of order m we know we need exactly m links. Since here, by assumption, we have a linking budget of $B = (n - 1)$, the network with a circle can therefore only maximally include $(n - 1)$ nodes. We also know that any end node can be disconnected by disrupting only one link. Thus, 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. This means that the network designer should include all $(n - 1)$ nodes in the circle. We have shown in the section on low linking costs that for $D_l = 1$ the circle is *max*-proof. Consequently, the connected component after disruption g^2 includes exactly $(n - 1)$ nodes, since irrespective of which link the network disruptor chooses to disrupt no additional node can be disconnected. Therefore, we can directly state that for $D_l = 1$ the largest remaining component after disruption in the circle and in the star are equally large. In both cases g^2 is of order $(n - D_l)$.

Lemma 2. *The best response strategy for a network designer with a linking budget of $B = (n - 1)$ when facing a network disruptor with a disruption budget of $D_l = 1$ is to build a star network including n nodes or a circle network including $(n - 1)$ nodes. In both cases g^2 is of order $(n - 1)$.*

For $D_l > 1$, however, we also know that the circle network is not *max*-proof. Therefore, we know that the network disruptor can directly disconnect at least one additional node from the network. Consequently the star network dominates that option. To make his network safer against disruption the network designer would thus have to add additional links to the network. However, since the linking budget is limited to $(n - 1)$, this would automatically entail that for every additional link the network designer wants to add to his network, he needs to leave one additional node unconnected. Theorem 1.3.3 in Cohn (2003) (p.19) states that any non minimally connected component can be seen as a minimally connected component plus added links. Given this, if the network designer leaves x nodes unconnected, he can construct a minimally connected component with exactly x additional links. In the following Proposition we will show that independent of how these links are added to the network the largest remaining component after disruption will never be as large as in the star network.

Proposition 3. *When facing a network disruptor with a disruption budget of $1 < D_l < (n - 2)$ the strict best response of the network designer with a linking budget of $B = (n - 1)$ is to build a star network.*

Proof We prove this proposition in three parts. Part 1 shows that non-star minimally connected networks always do worse than the star. Part 2 and 3 show that the same holds for constructing a smaller connected component.

- *Part 1.* By Lemma 1, in every non-star minimally connected graph, at least $(D_l + 1)$ nodes can be removed. Further, we know from the the maximal damage caused to a star network is to disconnect D_l nodes. Consequently, the largest remaining component in the star network is strictly larger than that in any other minimally connected network.

- *Part 2.* We show that any connected component that is not *max*-proof can never be a best response of the network designer.

  1. Any non-minimally connected component, is a minimally connected component with added links. For a proof see Theorem 1.3.3. in Cohn (2003) (p.19).
  2. Leaving x nodes unconnected, allows the network designer to build a minimally connected component with x added links.
  3. Suppose $D_l < x$. x nodes remain unconnected. In the star network only D_l nodes can be disconnected. So g^2 in the star network is always of a larger order.

4. Suppose $D_l > x$. x nodes remain unconnected. The x added links can be disrupted by the network disruptor, leaving at best a minimally connected network (see (2)). Additionally the network disruptor can disconnect at least $(D_l - x)$ nodes from the connected component.
5. Suppose $D_l = x$. x nodes remain unconnected. Unless the network designer builds a *max*-proof network, at least one more node can be disconnected. We thus only need to look at *max*-proof networks.

- *Part 3.* Looking at building a *max*-proof component, given his linking budget of $B = (n-1)$, the network designer can use exactly $m = \frac{2(n-1)}{D_l+1}$ nodes. He therefore needs to leave $(n-m)$ nodes unconnected. Since no additional node can be disconnected, after the disruption $(n-m)$ nodes remain unconnected. Compared to that in the star network there are D_l nodes unconnected after disruption. Consequently, if $D_l < (n-m)$ holds, the star network is a strict best response. This holds if $1 < D_l < (n-2)$. Thus the star is a strict best response of the network designer if $1 < D_l < (n-2)$ and therefore in all relevant cases. □

It can be easily verified that this same analysis also holds, generally, for any case where $B = (n-x)$, with $x \geq 1$, i.e. for any case in which the linking budget is smaller than the number of nodes that can be used to build the network. The reasoning for the case of $B = (n-x)$ runs completely parallel to that for the case of $B = (n-1)$: the fact that there are only $(n-x)$ links can be treated as if there are only $(n-x+1)$ nodes, as at least $(x-1)$ nodes cannot be connected. These results suggests that even without the influence of information decay in the network, there are incentives to build networks with a limited diameter, such as the star network.

However, since the star network seems a very specific result, as a further sensitivity check we also look at the case of $B = n$. Here the case of $D_l = 1$ is a limit case, since in the limit high linking costs are approaching the case of low linking costs. For $D_l = 1$, the network designer is thus able to build a *max*-proof network (the circle) also for high linking costs. For disruption budgets larger than 1, however, we can show that the star network remains the best response architecture for the network designer. This of course means that we do not force the network designer to use up all his n links. Instead, although he could use n links, he will continue to use $(n-1)$ links and build a star network, as this is his best response.[26] To see this, we again need to compare the star network with all other minimally connected networks and networks consisting of a smaller but stronger connected component. To do this, Lemma 3 runs completely parallel to Proposition 3 for the case of $B = (n-1)$.

Lemma 3. *When facing a network disruptor with a disruption budget of* $1 < D_l < (n-6)$ *the weak best response of the network designer with a linking budget of* $B = n$ *is to build a star network.*

Proof We prove this Lemma in 3 parts. Part 1 shows that non-star minimally connected networks can never do better than the star. Parts 2 and 3 show that the same holds for constructing a smaller connected component.

- *Part 1.* Given that by Cohn (2003)(p.19) we know that any non-minimally connected component can be seen as a minimally connected component with added links, we can interpret $B = n$ as the network designer adding one link to any minimally connected network. By Lemma 1, in every non-star minimally connected graph, at least $(D_l + 1)$ nodes can be removed. Thus taking out the one additional link provided by the linking budget, still at least D_l nodes can be removed. Further, we know from the the maximal damage caused to a star network is to disconnect D_l nodes. Thus the largest remaining component in the star network is weakly larger than that in any other minimally connected network.

[26] While this at first does not seem to fit with Approach 1, it does if you consider that links are costly and the network designer is of course not forced to use up his budget.

- *Part 2.* We show that any connected component that is not *max*-proof can never be a best response of the network designer.
  1. Leaving x nodes unconnected, allows the network designer to build a minimally connected component with x added links.
  2. Suppose $D_l < x$. x nodes remain unconnected. In the star network only D_l nodes can be disconnected. So g^2 in the star network is always of a larger order.
  3. Suppose $D_l > x$. x nodes remain unconnected. The $x+1$ added links to any minimally connected network can be disrupted by the network disruptor, leaving at best a minimally connected network (see (Part 1)). Additionally the network disruptor can disconnect at least $(D_l - x - 1)$ nodes from the connected component, leaving a g^2 maximally of the same order as that of the star network.
  4. Suppose $D_l = x$. x nodes remain unconnected. Unless the network designer builds a *max*-proof network, at least one more node can be disconnected. We thus only need to look at *max*-proof networks.

- *Part 3.* Looking at building a *max*-proof component, given his linking budget of $B = n$, the network designer can use exactly $m = \frac{2n}{D_l+1}$ nodes. He therefore needs to leave $(n-m)$ nodes unconnected. Since no additional node can be disconnected, after the disruption $(n-m)$ nodes remain unconnected. Compared to that in the star network there are D_l nodes unconnected after disruption. Consequently, if $D_l \leq (n-m)$ holds, the star network is a weak best response. Comparing D_l and $(n-m)$ we find that this holds if $D_l(D_l+1) \leq n(D_l-1)$. In the limit this holds if $D_l \leq n$, however, for lower values of D_l such a general condition does not hold. However, if $D_l < (n-6)$, the inequality holds for any values of n and D_l. Thus the star is a weak best response of the network designer if $1 < D_l < (n-6)$ and therefore in all relevant cases. □

So while all minimally connected networks are equally good responses if there is no threat of an attack, the star is the only best-response minimally connected network in case of an impending attack for a linking budget of $B = (n-1)$. Additionally, we showed that the case of the star network as a best response is not a highly special case. In fact, it holds in its strict version for $B = (n-x)$ and it is a weak best response for the case of $B = n$ and $1 < D_l < (n-6)$. Considering again Approach 2, thus looking at a fixed size of the post-disruption component, minimizing the number of links used to achieve this, we can also state the main result as follows:

Proposition 4. *High levels of linking costs exist such that the designer's (weak) best response to an attack on the links of his network with a disruption budget of $D_l > 0$ is to build a star network.*

Proof This follows directly from Proposition 3. Additionally Lemma 3 shows that these levels of linking costs don't necessarily need to be so high that no additional link may be added to the network at all. □

5.2. Node Deletion - High Linking Costs

For node deletion we can immediately show that for the case of $D_v = 1$, the best the network designer with a linking budget of $B = (n-1)$ can do is to build a circle containing $(n-1)$ nodes. This suggests that in general, the network designer should build a smaller, stronger component, an intuition that we will indeed confirm in this section.

Proposition 5. *For $D_v = 1$, and a linking budget of $B = (n-1)$ nodes, the designer's best-response network architecture is the circle containing $(n-1)$ nodes.*

Proof *Step 1.*Every component that links $(n-1)$ nodes using $(n-1)$ links and is not a circle of $(n-1)$ nodes, has at least one end node. It follows that in this component, the disruptor can delete one extra node on top of the deleted node. Together with the node that was not connected in the pre-disruption network, this means that a largest post-disruption component of, at most, $(n-3)$ nodes remains. *Step 2.* Every

network that links less than $(n-1)$ nodes has a largest post-disruption component that is smaller than $(n-2)$ because one node can at least be taken out by definition. *Step 3.* In the circle that links $(n-1)$ nodes using $(n-1)$ links, if one node is deleted, a post-disruption component connecting $(n-2)$ nodes remains. □

For a larger disruption budget, we cannot give a full characterization of the designer's best response pre-disruption network. However, we can show that an essential feature of any best-response pre-disruption network is that the network does not connect all nodes to one another. In order to show that it is not a best response for the designer to construct a minimally connected pre-disruption network, we must first know the order of the largest remaining post-disruption component given a minimally connected pre-disruption network. We start by deriving this for the simple case of a deletion budget $D_v = 1$. We denote the smallest natural number larger than a number x as $\lceil x \rceil$.

Lemma 4. *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 order $\lceil \frac{(n-1)}{2} \rceil$.*

Proof We show this in 3 steps.

- *Step 1.* By Lemma A.5, in any minimally connected network, every node is a node cut, so that any minimally connected network can always be separated into at least two components by removing one node.
- *Step 2.* A disruptor can always do better than to take out a node such that the largest remaining component is of an order larger than $\lceil \frac{(n-1)}{2} \rceil$. Let the disruptor take out node x with degree $\eta_i(g) = d$, which has links to nodes $y_1, y_2, \ldots, y_d$. Given that by Lemma A.5, each node in a minimally connected graph is a node cut, taking out node x leads to d separated components, which we can denote as $C_1, C_2, \ldots, C_d$. Let the component C_d contain s nodes, with $s > \lceil \frac{(n-1)}{2} \rceil$. Then it follows that $g - C_d$, meaning the network obtained when component C_d is removed from the network, is of an order smaller than $\lceil \frac{(n-1)}{2} \rceil$. By removing y_d in C_d instead, the disruptor can assure that the component g_{z_d} which includes nodes connected to a neighbor z_d of y_d is of an order of at most $(s-1)$, so that the order of this component is smaller than the order of C_d. At the same time, we have already seen that the order of component $g - C_d$ is smaller than $\lceil \frac{(n-1)}{2} \rceil$. It follows that the disruptor is better off by disrupting y_d. Therefore, a disruption strategy where a largest component larger than $\lceil \frac{(n-1)}{2} \rceil$ is left can never be optimal for the disruptor.
- *Step 3.* Given that by Step 1, a network disruptor never leaves a largest component of an order larger than $\lceil \frac{(n-1)}{2} \rceil$, the best that the designer can possibly do is to leave a largest component of an order of exactly $\lceil \frac{(n-1)}{2} \rceil$. □

The *line* architecture shows that the network designer can actually achieve the maximal order of the post-disruption network suggested by Lemma 4. For a generalization of Lemma 4 to generic disruption budgets, see Lemma A.11 in the Appendix.

As we will presently demonstrate, the network designer can fare better by constructing a circle of $(n-1)$ nodes, than with a minimally connected network . By Proposition 5, we already know that this result holds for $D_v = 1$, where in fact the circle of order $(n-1)$ is the unique best-response architecture. We now move to prove that, for any relevant disruption budget, the circle including $(n-1)$ nodes is a (weak) best response. We start by deriving the order of the largest component that can remain after disruption in a circle of order $(n-1)$.

Lemma 5. *In a circle network of order $(n-1)$, the network disruptor with a disruption budget of D_v will cause maximal damage by cutting the network into D_v separate components, each maximally of order $\lceil \frac{(n-1-D_v)}{D_v} \rceil$.*

Proof As the circle is completely symmetric, any disruption strategy by the disruptor can be seen as the deletion of one random node in the circle and $(D_v - 1)$ further nodes. After the deletion of this random node, the remaining network takes the form of a line, i.e. a minimal connected component of order $(n-1)$, in which the disruptor can delete $(D_v - 1)$ nodes. It follows directly from Lemma A.11 that the largest remaining post-disruption component has an order of $\frac{[(n-2)-(D_v-1)]}{[(D_v-1)+1]} \simeq \lceil \frac{(n-1-D_v)}{D_v} \rceil$. □

We are now ready to show that the minimally connected network is never better than the circle that excludes one node.

Proposition 6. *When facing a network disruptor with a node disruption budget D_v the line architecture with order n is never better than the circle architecture with order $(n-1)$. For $D_v > \lceil \frac{n-1}{2} \rceil$ they are equally good responses.*

Proof From Lemma A.11 we know that the largest remaining post-disruption component with a pre-disruption line of n nodes has order $\lceil \frac{(n-D_v)}{(D_v+1)} \rceil$. By Lemma 5 we know that the largest remaining post-disruption component in a circle of order $(n-1)$ has order $\lceil \frac{(n-D_v-1)}{D_v} \rceil$. It is straightforward to calculate that $\frac{(n-D_v)}{(D_v+1)} < \frac{(n-D_v-1)}{D_v} \iff D_v < \frac{(n-1)}{2}$. Thus for $D_v < \frac{(n-1)}{2}$ the circle is strictly better than the line. However, as the terms need to be natural numbers, this inequality does not always hold. What does hold however, is that if $D_v < \frac{(n-1)}{2}$ then $\lceil \frac{(n-D_v)}{(D_v+1)} \rceil \leq \lceil \frac{(n-D_v-1)}{D_v} \rceil$, since it holds that if $x < y$, then $\lceil x \rceil \leq \lceil y \rceil$. That this holds strictly in some cases, thus that the circle strictly dominates the line architecture can easily be verified by using n and D_v in such a way that the fractions are natural numbers (e.g. $n = 11$ and $D_v = 2$). It then easy to see that $\frac{(n-D_v-1)}{D_v} - \frac{(n-D_v)}{(D_v+1)}$ is an increasing function of n and is larger than 1 for a range of n above a certain threshold.

For $D_v \geq \lceil \frac{(n-1)}{2} \rceil$, in both the mentioned circle and line, the disruptor can reduce the post-disruption network to a set of isolated components, so that both architectures are equivalent in this extreme case. □

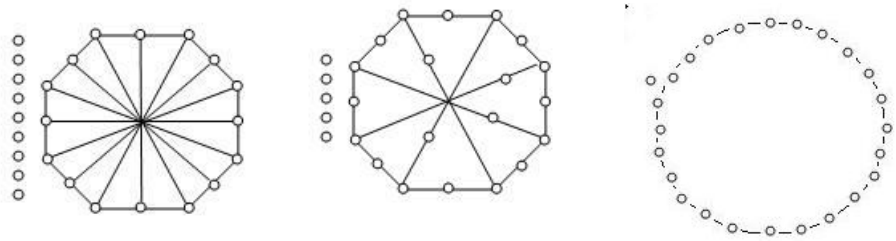
With Proposition 6 we do not mean to imply that the circle network is the best possible network for a network designer to build in the case of node deletion under high linking costs. We merely use Proposition 6 to show that it is never a (strict) best response to build a network including all nodes for the case of high linking costs. This suggests that instead of building a large connected pre-disruption component, a network designer should rather build a smaller but more highly connected pre-disruption component, even though this means that he will have to leave a number of nodes unconnected. This is caused by the fact that due to the limited number of available links, building large connected pre-disruption components always implies that they are very vulnerable to disruption. While in the analysis so far we have only studied this for the case of leaving one node unconnected, this implies that there may be still better architectures where more nodes are left out, enabling the designer to construct a stronger component. For these more general cases, the main insight, namely that the network designer will leave nodes unconnected to build a smaller but stronger connected component, however, not the strongest one possible because he would have to leave out too many nodes to do so, remains the same. However, since these cases are hard to characterize, we will show what such networks can possibly look like only by means of an example.

We have already shown in the section on low linking costs, that in order to make his network maximally robust against any attack, the network designer would have to build an r-regular network that meets the conditions of Proposition 2. However, as discussed in Section 5.1 building such a network is very expensive. Given the number of links we know the network designer needs to build an r-regular component and the size of his linking budget $B = (n-1)$, we can calculate the number of nodes he can use in the component to be $\frac{2}{r} * (n-1)$. Thus, $\frac{r-2}{r} * (n-1) + 1$ nodes will have to be left out of the component. The following example will clarify this.

Take a network disruptor with a disruption budget of $D_v = 2$. We know that the *max*-proof component will have to be a symmetric 3-regular component. Therefore the network designer can only use $\frac{2}{3} * (n-1)$ nodes to build the component and is forced to leave $\frac{1}{3} * (n-1) + 1$ nodes unconnected.[27] For a linking

[27] Assuming that (n-1) is divisible by 3 and a 3-regular network exists.

budget of $B = 24$ links and $n = 25$, the network that results can be depicted as in Figure 3(a). In this network 9 nodes remain unconnected. And since the connected component is *max*-proof, this network is the one with the smallest possible connected component in the pre-disruption network g^1 of the class of networks that might be best responses of the network designer.



(a) 3-regular (b) bipartite (c) cycle

Figure 3: Different 25 node networks

The circle network in Figure 3(c), on the other hand, leaves out only 1 node. As we have seen in the previous Lemmata and Proposition, the circle network will lead to a larger connected component in the post-disruption network g^2 than any minimally connected network. Thus the circle network is the network that includes most nodes in the connected component in the pre-disruption network g^1, of the class of networks that might be best responses of the network designer.

The network in Figure 3(b) is an intermediate case leaving 5 nodes unconnected in the pre-disruption network g^1. In the connected component there is one node in between every 2 highly connected nodes. Thus this network has some 'weak' spots built into the connected component.

However, the size of the connected component in the pre-disruption network g^1 is only one of the two deciding factors we need to look at when discussing which of these networks will be the best option for the network designer. The possible damage the network disruptor can cause with his disruption budget of $D_v = 2$, is the other. In the network in Figure 3(a), the connected component is *max*-proof. Thus, the network disruptor cannot disconnect any additional nodes. Consequently, the largest remaining connected component in the post-disruption network g^2 will be of order 14. In the circle network in Figure 3(c), the network disruptor can cut the connected component in half by taking out 2 nodes. Therefore, the largest remaining connected component in g^2 will be of order 11. In the bipartite network in Figure 3(b), the maximum damage the network disruptor can cause is to disconnect one additional node from the connected component leaving a largest connected component in g^2 of order 17. Thus, the best option of the network designer in this case is to build the bipartite network.

Even in this short example with a limited number of nodes, we can see that there is a definite trade-off between building a larger but weaker network and building a smaller but stronger network. While building a network with a *max*-proof component dominates the option of building a cycle network, as has been seen in the example above (and is proven for a general case in Lemma A.12 in the Appendix), what we have also seen in the example above is that both extreme cases (the cycle and the *max*-proof component) are dominated by a middle option. Appendix 3 shows that for a general disruption budget, the cycle and the *max*-proof network are not best responses of the network designer. Instead it is shown that networks that are neither fully robust against disruption and do not include all nodes in the pre-disruption component will be the best response of the network disruptor. This has been moved to the appendix, as some concepts that are only introduced in Section 5 will be employed in the proof.

Just as in the section on high linking costs and link deletion, we here also look at $B = n$ and $B < (n-1)$ as a sensitivity analysis. For $B < (n-1)$ it is straightforward to see that nothing changes in the analysis. Building a *max*-proof network gets even more expensive and the payoff for a pre-disruption component including as many nodes as possible decreases, because due to the smaller linking budget it is no longer

viable to include all nodes in one connected component, which means that the network designer would have to leave even more nodes unconnected to build a *max*-proof component. Therefore, the best response of the network designer is also in this case, to build a network that is neither fully robust nor includes all nodes in the pre-disruption component. For $B = n$, the analysis is not completely tractable, however, we can easily see that for any positive disruption budget D_v, a circle does not fare worse than a minimally connected network. Given the result in Proposition 6, if a circle including $(n-1)$ nodes is a (weakly) better response than any minimally connected network, a circle including n nodes will definitely be as well. Thus, the network designer will use all n links to build his network. Again deducing from the previous analysis, adding one link will not enable the network designer to build a *max*-proof network, except for the case of $D_v = 1$. This however, as has been explained for the case of link deletion, is a limit case. For $D_v > 1$ the best response of the network designer remains to build a network that is neither fully robust nor includes all nodes in the pre-disruption component, also for the case of $B = n$.

As in the previous sections, here we will also look at the two approaches to finding robust network topologies. In this section, we took the budget as a given and looked for the best response strategy of the network designer. Parallel to Proposition 4, this result can thus be stated as a general proposition as follows:

Proposition 7. *For the case of node deletion, high levels of linking costs exist such that the designer's best response will never be to build a* max*-proof network nor a network which includes all nodes in the connected pre-disruption component.*

Proof This follows directly from Proposition 3 and Lemma A.12. □

We have seen in this section that while for node deletion there is a trade-off for the network designer between building a large but weak connected component in the pre-disruption network and a small but very strong one, no such trade-off takes place in the case of link deletion. Therefore, unlike the case of low linking costs, 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 than links, not only because in the node deletion case nodes will be disrupted by definition, but also because all links attached to a node may be removed from the network once the node has been deleted. Therefore, it is much harder to keep nodes safe from disruption than to keep links safe.

In terms of our military communications network application, this means that first of all, for high linking costs, it is important to know whether the attack will be directed at the links or the nodes of the network. If the links are being targeted, building a star network, taking into account that in case of an attack some communication facilities will be lost, is the best option. Should, on the other hand, the nodes be under attack, the only viable option is to build a smaller network that is more highly connected. Otherwise, even when taking out just a couple of nodes, the network as a whole can be disconnected into a number of small, scattered groups.

6. Intermediate Linking Costs

We have so far treated the extreme cases where either linking is cheap enough for the network designer to build a completely proof network, or where linking is so expensive that the network designer does not want to add any links above the minimum needed to connect all nodes. In this section, we explore the in-between cases, where linking costs are intermediate, so that the designer is willing to add defensive links, but not to the extent that the network is protected to the highest level achievable. We limit ourselves to the case where the network designer builds a $(max-1)$-proof network,[28] meaning that the designer tolerates

[28] $(max-1)$-proofness is directly related to the graph theoretic concept of *restricted connectivity* as introduced by Harary (1983). This concept refers to the smallest link cut (node cut) in a graph, which disruption will lead to a disconnected graph where each component is of at least order 2. This is thus equivalent to the definition of $(max-1)$-proofness. However, since graph theory is not interested in minimality in the economic sense (thus using as few links as possible) we cannot actively use the results obtained in our analysis.

that the largest component in the post-disruption network has one node less than is possible with maximal network defense. We approach the matter in this manner not only because it is analytically tractable but also because, at least for the case of link deletion, the difference between the largest remaining component in a star network and in a $(max-1)$-proof network, especially for cases where the ratio between D_l and n is large, usually only consists of a couple of nodes, thereby implying that the network designer either chooses to almost completely protect his network or not protect it at all beyond connecting all nodes in one component.

The case of $(max-1)$-proofness is analytically tractable for the following reason. We know from Section 4 which linking budget B is minimally needed to achieve *max*-proofness. Suppose that we take a linking budget smaller than B. Then we know that *max*-proofness is not achievable for this linking budget, so that the best that can be achieved is $(max-1)$-proofness. Thus, if we find networks for such linking budgets smaller than B that achieve $(max-1)$-proofness, then these networks do the best possible with this linking budget.

From the previous section, we already know that for a linking budget $B=(n-1)$, if $D_l=1$, the network designer achieves $(max-1)$-proofness in the star architecture; if $D_v=1$, the network designer achieves $(max-1)$-proofness in the circle of order $(n-1)$. These results suggest, in general, that under link deletion the network designer should construct a star or star-like architecture in which the network has a set of one or more strong (i.e. high-degree) nodes which the disruptor cannot remove and a set of weak (i.e. low-degree) nodes where the disruptor is able to remove only one of the weak nodes. Under node deletion the basic results suggest that in general the network designer should avoid having nodes with higher degree as these then become targets to the disruptor. Instead, the disruptor should ensure that all nodes have the same degree. Our analysis below indeed confirms this line or reasoning.

A network structure that is $(max-1)$-proof needs to fulfill certain requirements, very similar to those for *max*-proof networks described in Proposition 1. For *max*-proof networks, the basic requirement was that every node had to be connected of at least degree $\eta=(D_l+1)$ (respectively $\eta=(D_v+1)$). To minimize the amount of links used, a further requirement was for every node to be connected of exactly degree $\eta=(D_l+1)$ ($\eta=(D_v+1)$ respectively). The class of networks fulfilling this requirement was *r*-regular networks. Following from this, here the basic requirement is that every pair of nodes is jointly connected of at least degree $\eta=(D_l+1)$ (respectively $\eta=(D_v+1)$) - thus every pair of nodes needs to have at least (D_l+1) (respectively (D_v+1)) links to the rest of the network, no matter if the nodes are directly connected or not.[29] Again to minimize the number of links used, we here use a generalization of the concept of regular networks to define the class of networks that is a good candidate for $(max-1)$-proofness. We term this generalization pair *r*-regularity and it is defined below. For examples of pair *r*-regular networks, see Figure 4.

Definition 5. *In any pair r-regular network, each pair of directly linked nodes has exactly r links to the rest of the nodes.*

Using the concept of pair *r*-regularity we can thus ensure that no directly linked pair of nodes can be disconnected from the network. Of course, as was the case for regular networks, not all pair *r*-regular networks will be $(max-1)$-proof against network disruption. For example, this condition does not take into account how many links each single node has. Looking at Figure 4, it is straight forward to see that in networks (a) and (b) multiple single nodes can be disconnected, although each pair receives 6 links. Thus, those networks that ensure the robustness of the network have to fulfill certain additional criteria, as was the case for *max*-proofness as well. The first criterion is that not only no pair of nodes can be disconnected but also no smaller or larger subset of nodes. To ensure this, in pair *r*-regular networks every subset of nodes needs to have at least D_l+1 links to the rest of the network (or respectively D_v+1 neighbors). As for the case of low linking costs we can therefore directly state that the set of $(max-1)$-proof networks for node deletion will be a subset of the set of $(max-1)$-proof networks for link deletion.

[29] For connected pairs, this concept coincides with the graph theoretic concept of *edge degree*, as defined for example in Esfahanian and Hakimi (1988).

Lemma 6. *The set of $(max-1)$-proof networks under node deletion $\Gamma_{D_v}^{(max-1)}$, is a subset of the set of $(max-1)$-proof networks under link deletion $\Gamma_{D_l}^{(max-1)}$.*

Proof By definition, having r direct neighbors in the network implies that a pair (or larger subset) of nodes needs to have r links. However, a pair (or larger subset) of nodes having r links does not imply that they have r neighbors as the two players in the pair (or larger subset) could have links to the same neighbor. □

Unfortunately, unlike in the case of regular networks, we do not need the same number of links for any pair r-regular network for any given n and r. Therefore to find networks that at least fulfill a local minimality condition, we first need to analyze how many links are needed to build such networks. To do so, we first show that in any pair r-regular network each node has one out of a set of at most two degrees, where high-degree nodes can be interpreted as strong spots, and low-degree nodes as weak spots. We therefore label the two groups of nodes as n_1 and n_2. 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 *high-degree nodes*, and the type-2 nodes *low-degree nodes*. In the following Lemma, where the main characteristics of pair r-regular networks are described, we show that we can now exactly calculate how many high-degree and low-degree nodes there are in a pair r-regular network and how many links are used to build it. How many links are needed to build such a network then depends on how these links are split up over the high- and low-degree nodes and how many high- and low-degree nodes there are in the network (for an example see Figure 4). How the distribution of degrees over pairs of nodes influences the number of links needed is also shown in Lemma 7. Intuitively, by making the distribution of degrees over any pair of nodes more unequal, so that r_2 becomes smaller and r_1 larger, we will have fewer high-degree nodes and more low-degree 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 $r_1 = (n-1)$. For expositional simplicity we here focus on networks for which n is divisible in such a way that $(r_1 + r_2 - 2) = r$ and $r \geq 2$ holds, since otherwise issues of divisibility will occur. The last characteristic of pair r-regular networks described in Lemma 7 focusses on the best response quality of pair r-regular networks. They are best-responses, as the budgets described above, which are just sufficient to build pair r-regular networks, do not allow *max*-proofness to be achieved for the case where $D_l = (r-1)$, respectively $D_v = (r-1)$. It follows that if we can show that a pair r-regular network is $(max-1)$-proof, then for the number of links that is used in the given network, the network is the best that the network designer can do. The simple case where $r = 2$ and $D_l = 1$, respectively $D_v = 1$ is an exception, as the pair 2-regular network (namely the circle) is also *max*-proof in this case - this is why we exclude it. Further, we show that for sufficiently large n, the network designer cannot build an r-regular component connecting $(n-1)$ nodes. It follows then that any best response pre-disruption network for these linking budgets must be connected.

Lemma 7. *All pair r-regular networks fulfill the following basic characteristics:*

- *In any connected 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*
- *Pair r-regular networks have less links the smaller their r_2, and the pair r-regular networks with $r_2 = 1$ have the smallest number of links in this set.*
- *Let it not be the case that both $r_1 = 2$ and $r_2 = 2$. Then with any number of links $B = n * [r_1 r_2/(r_1+r_2)]$ that exactly allows one to build a pair r-regular network, one cannot build a connected r-regular network. Moreover, a critical n_C exists such that, for all $n > n_C$, the linking budget B is also too small to construct an r-regular component connecting $(n-1)$ nodes.*

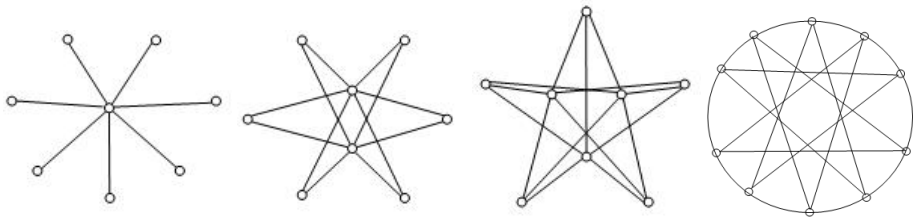
Proof We proof each of these statements independently:

- Any pair r-regular network has nodes with only two different degrees. It follows that for B, the number of links used in the network, it is the case that $B = n_1 r_1 = n_2 r_2$. 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 $B = n_1 r_1 = n_2 r_2$ again allow us to calculate that $B = n * [r_1 r_2/(r_1 + r_2)] = n * [r_2(r + 2 - r_2)/(r + 2)]$.

- 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. The smallest possible r_2 is then $r_2 = 1$. In the expression $B = n * [r_2(r + 2 - r_2)/(r + 2)]$ derived in the proof of the previous statement, the number of links used is smaller the smaller r_2. The result follows.

- The r-regular connected network uses more links than the pair r-regular network iff $n * r/2 > n * [r_1 r_2/(r_1 + r_2)] \Leftrightarrow (r_1 + r_2 - 2)(r_1 + r_2) > 2 * r_1 r_2 \Leftrightarrow {r_1}^2 + {r_2}^2 > 2(r_1 + r_2)$. The latter is true for the specified r. The r-regular component connecting $(n - 1)$ nodes uses more links than the pair r-regular network iff $(n - 1) * r/2 > n * [r_1 r_2/(r_1 + r_2)]$. For large n, this is true by the same calculations. □

The last part of Lemma 7 suggests that the network designer who decides to construct a pair r-regular network with the purpose of achieving $(max - 1)$-proofness, in order to save as much as possible on links, should distribute links across pairs as unequally as possible. In Figure 4 (case where $n = 8$ for subfigures (a)-(c) and $n = 10$ for subfigure (d), $r = 6$), network (a) uses 7 links, network (b) 12 links and network (c) 15 links, while all achieving pair 6-regularity.[30] However, as we now show, a distribution that is too unequal makes it possible for the disruptor to remove multiple low-degree nodes from the network. This puts a cap on how unequal the distribution may be. This is illustrated in network (b) in Figure 4, if either $D_l = 5$ or $D_v = 5$, the disruptor is able to take out at least two low-degree nodes. Moreover, for node deletion, an additional danger of an unequal link distribution is that the disruptor can do a lot of damage by targeting the high-degree nodes. By the same line of reasoning, when the linking budget is equal to $(n - 1)$, the star fares poorly under node deletion.[31] Also the network (c) in Figure 4 still has a division that is too unequal for node deletion. By deleting the three high-degree nodes, the disruptor can make sure that all nodes are isolated. The network in subfigure (d) on the other hand, which next to being pair 6-regular is also a 4-regular graph, is $(max - 1)$-proof against a disruption budget of $D_v = 5$. Here we have exactly the same number of nodes in group n_1 as in group n_2 and the nodes in both groups receive the same amount of links.



(a) 1 core node (b) 2 core nodes (c) 3 core nodes (d) 4 regular

Figure 4: Pair 6-regular Networks

We are now ready to summarize our results about pair r-regular networks that achieve $(max - 1)$-proofness, and do so with a minimal number of links. Our main idea is that under link deletion, links can to a limited extent be unequally distributed over the two sides of any connected pair, saving links. Under

[30] Note that for the case introduced in Figure 4, the network designer would need to use 24 links to build a *max*-proof network including all 8 nodes (or 30 links for all 10 nodes). To build a *max*-proof network connecting only 7 nodes, thus having a largest remaining component after disruption of the same order as when building a $(max - 1)$-proof network, he would need to use 21 links.

[31] The case of the star network and link deletion was analyzed already in the section on high linking costs.

node deletion, links should be equally distributed. For this reason, we focus on the case where r is even; for r is odd, there is a divisibility problem in that links simply cannot be equally distributed over the two sides of a connected pair.

Proposition 8. *Let* r *be even and* ≥ 4 *and let* n_1 *and* n_2 *be natural numbers. Then in the set* $\Gamma_{D_l}^{(max-1)}$ *(and respectively* $\Gamma_{D_v}^{(max-1)}$*)as defined in Lemma 6, all pair r-regular networks* g *fulfill the following conditions:*

1. $r_2 > (r-1)/2 \Leftrightarrow r_2 > (r_1 - 3)$ *for* $D_l = (r-1)$ *(respectively* $D_v = (r-1)$*)*
2. $r_2 > (r_1 - 2)$ *for* $D_v = (r-1)$

$\Gamma_{D_l}^{(max-1)}$ *(and respectively* $\Gamma_{D_v}^{(max-1)}$*) uses a minimal number of links if:*

- $r_1 = r/2 + 2, r_2 = r/2$*, so that the type-1 nodes have two extra links compared to type-1 nodes for the case of link deletion*
- $r_1 = r_2 = (r+2)/2$*, so that all nodes have the same degree, meaning that we have a* $(r+2)/2$*-regular network for the case of node deletion*

Proof We prove statements (1) and (2) independently.

1. If $r_2 \leq (r-1)/2$, the disruptor is able to delete several nodes with degree r_2, by either deleting all their links in the case of link deletion, or all their neighbors in case of node deletion.
2. 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.

The minimality condition follows directly from statements (1) and (2) and Lemma 7. □

Now while this sounds abstract, finding networks that fulfill these conditions is straightforward. For the case of node deletion, Proposition 8 states that in a minimal $(max-1)$-proof network all nodes receive the same amount of links. Consequently such a network is a regular network. To determine the degree of regularity we need to look for, we can use the relationship between regularity and pair regularity. If a network is regular of degree r, then the degree of pair regularity is given by $2r - 2$, as every node in a pair has exactly r links but one of these links is to one another. From the class of regular networks we here focus on circulant networks as introduced in Section 4. To fulfill the conditions of Lemma 6 it is straightforward to see that a jump of size $a_2 = 2$ cannot be part of the network, as otherwise a pair of nodes was linked to the same neighbor and therefore would not have $D_v + 1$ neighbors. That no larger subset has too few neighbors, can then be regulated via the jumps within any circulant network. Looking at such networks (e.g. subfigure (d) in Figure 4), we can also see that Lemma 6 holds, as this network is not only $(max-1)$-proof against node deletion but also against link deletion. However, for link deletion, we can also build $(max-1)$-proof networks using less links.

To show that such networks exist and that they are indeed $(max-1)$-proof against link deletion, we can look at a subclass of pair r-regular networks, namely complete bipartite networks. In complete bipartite networks each node in n_1 is directly linked to each node in n_2 but to no other node in n_1.[32] It is straightforward that in such complete bipartite networks, if no pair of nodes can be disconnected also no larger subset of nodes can be disconnected. To make this obvious, we will use the example of a complete bipartite network using $n = 8$ nodes. Networks (a)-(c) in Figure 4, show 3 of the 4 possibilities of building such a network. The fourth would be $n_1 = n_2 = 2$, which then uses 16 links. All complete bipartite networks for $n = 8$ are pair 6-regular, however, using different amounts of links. Since by disconnecting a single node nothing changes about the connectivity of the other low degree nodes, we can find the complete bipartite

[32]For a formal definition of complete bipartite networks see see Definition VIII in the graph theoretic appendix.

network that fulfills the requirements of $(max-1)$-proofness using the least links easily. We need to ensure that no two low degree nodes can be disconnected and no single high degree node can be disconnected. Due to the definition of complete bipartite networks, this is ensured if each pair of low degree nodes receives at least $(\frac{D_l}{2}+1)$ nodes. As soon as no pair of nodes can be disconnected also no larger subset can be disconnected. Thus it needs to hold that $n_1 > \frac{D_l}{2}$. In our example of $n = 8$ this is given for the networks with $n_1 = 3$ and $n_1 = 4$. While the network with $n_1 = 3$ uses 16 links only, the network with $n_1 = 4$ uses 16 links. Thus the network that is minimal $(max-1)$-proof is the network with $n_1 = 3$.

We have thus shown that while for link deletion the network designer should build star-like structures with a number of central nodes that are highly connected and a number of weak spots, for node deletion the network designer should build a circle-like structure where all nodes receive the same amount of links. In terms of the military application introduced earlier, this means that for the case of a possible attack on the links of the network, the network designer should basically keep a star-like architecture of his network. This star can be complemented with additional links in such a way that we may have more than one central node but there will be no links between the spokes. Building a network in such a way means that at most one of the spokes can be disconnected, but due to this no other line of communication will be completely closed down. Since the central nodes are not connected amongst each other, there is an added security in the network that even if one central node should be disconnected, the rest of the network remains connected. For the case of targeting the actual physical communication bases, this means that a circular component should be the basis for any such network. Thereby, the network will not have any weak spots which would be obvious targets. Since the structures that are optimal for node deletion and link deletion are fundamentally different, it is thus important to first find out if a possible attack will be targeting the physical means of communication or the lines of communication.

7. Extensions

Finally, we will turn to looking at some extensions to the model we have analyzed so far. In most applications of a network disruption model, there will neither be perfect information on the side of the network designer nor on the side of the network disruptor. Therefore, we will look at the case of imperfect information and how robust our results are to this. In the first instance, we look at the case of imperfect information on the side of the network designer by keeping the information on what type of disruption budget the network disruptor has private. Thus, while the network designer knows the size of the network disruption budget, he does not know if the disruptor will attack links or nodes within the network. In a second extension we consider imperfect information on the side of the network disruptor. Here we assume that the network disruptor does not know the structure of the network, but only knows the number of nodes within the network for the case of node deletion or the number of links for the case of link deletion. He thus randomly attacks the network.

7.1. Imperfect Information - Network Designer

Imperfect information on the side of the network designer can either be about the size of the disruption budget or about the type of disruption budget. Within our model, it is not possible to look at imperfect information considering the size of the disruption budget, however, analyzing the case of imperfect information about the type of disruption budget is a possible extension to the model. Therefore, we will now include uncertainty into our model by allowing the disruptor to keep the type of his disruption budget quiet. Consequently, the network designer only knows the size of the disruption budget but not its type.

For low linking costs, we have seen in Section 4 that the same network structure is a best response irrespective of the type of attack. Thus, with or without uncertainty over the type of attack, the network designer's best-response is going to be to build a *max*-proof network structure for low linking costs.

For high linking costs we have seen in Sections 5.1 and 5.2 that the most robust network structures for link deletion and node deletion differ greatly. Whereas for link deletion the most robust network structure for any disruption budget is the star network, for node deletion we cannot make such a precise prediction. What we did show in Section 5.2 is that the best response network will be a network that does not include all

nodes within one connected component and within the connected component has some symmetric weak spots. Since the optimal network therefore highly depends on the number of nodes and the size of the disruption budget, we cannot compare it to the star network. However, we have shown that the *max*-proof network is in any case a better response by the network designer than the minimally connected network or the cycle. Since the *max*-proof network has clear properties, we can compare it to the star network and in this way find a lower boundary on the belief of the network designer that the form of the attack will indeed be link deletion, for him to find the star network a best reply.

We have shown that under link deletion the largest remaining component in a star network will be of size $(n - D_l)$. Under node deletion, it is straight forward to see that the largest remaining component will be of size 1 as the network disruptor can simply disrupt the central node. For the *max*-proof network, we have shown that given a linking budget of $B = (n-1)$ exactly $m = \frac{2(n-1)}{D+1}$ nodes can be used to build a *max*-proof component. The size of the largest remaining component for link deletion will then be $\frac{2(n-1)}{D_l+1}$ and for node deletion it will be $\frac{2(n-1)}{D_v+1} - D_v$. Comparing these two payoffs we find that the lower limit on the belief that the attack will be directed towards the links of the networks has to be at least 0.75 for the star network to be a better response than the *max*-proof network.

Proposition 9. *The belief of the network designer that he faces an attack on the links of the network has to exceed* 0.75 *for the star network to be a best-response structure if there is uncertainty about the type of the network disruptor's disruption budget.*

Proof Assume α is the belief of the network designer that he faces link deletion and β is the belief on node deletion and that it holds that $\alpha + \beta = 1$.

$$\alpha * (n - D) + \beta * 1 > \alpha * m + \beta * (m - D) \Leftrightarrow \frac{\alpha}{\beta} > \frac{2n - 3 - D^2 - 2D}{nD - n - D^2 - D + 2} \tag{1}$$

Given the claim that the belief in link deletion, α, has to be at least 0.75, this needs to hold as long as $\frac{\alpha}{\beta} > 3$. Thus:

$$\frac{\alpha}{\beta} > \frac{2n - 3 - D^2 - 2D}{nd - n - D^2 - D + 2} > 3 \Leftrightarrow n > \frac{9 - 2D^2 - D}{5 - 3D} \tag{2}$$

To see that this holds in all relevant cases, we can check the extreme case of $D = (n-2)$.

$$n > \frac{9 - 2(n-2)^2 - (n-2)}{5 - 3(n-2)} \tag{3}$$

This holds for all $n \geq 4$, and thus in all relevant cases. Thus for all $n > 4$, the star may only be a best response network structure, if the believe of the network designer that the attack will indeed be directed towards the links of the network exceeds 0.75. For all cases where the believe that he deals with link deletion is below 0.75, the star is never a best response network architecture. □

This result can of course be explained by the fact that while *max*-proof networks do well for node deletion as well as link deletion, the star network is an extremely poor option for the case of node deletion. What we have shown here is that while the *max*-proof network is not necessarily the best network for node deletion under high linking costs, taking it as a point of reference we at least get a lower boundary on the feasibility of the star network under uncertainty. Given the linking budget and the size of the disruption budget, we can then calculate for every case singularly if the star remains a best response structure or not.

7.2. Imperfect Information - Network Disruptor

Imperfect information on the side of the network disruptor can be modeled by giving him no (or only limited) knowledge of the network structure. Thus for the case of node deletion this means that the network disruptor knows how many nodes there are in the network, but not how they are linked to one another. For the case of link deletion this means that he knows how many links there are but not how many nodes.

Consequently, he randomly chooses which links or nodes to disrupt within this setting as he does not know the structure of the network at all.

Looking first at the case of low linking costs, it is straightforward to see that the network designer will still build a *max*-proof network in the case of link deletion as well as node deletion. For both types of disruption, irrespective of the network disruptor's knowledge of the network structure he will not be able to disconnect any additional node from the connected component. Thus, the *max*-proof network remains a best response. For the case of high linking costs, we first look at the case of link deletion.

For link deletion it is easy to see that nothing is going to change concerning the best response structure of the network designer. Building a star network is a best reply in the case of perfect information and it also holds for imperfect information. This is due to the fact that in the star network, the deletion of links is random to begin with, as it does not matter which links the network disruptor targets, he will always cause the exact same amount of damage - namely, disconnecting one node per targeted link. Therefore, in the case of imperfect information regarding the network structure, there is no incentive for the network designer to change anything, since already all n nodes are included in the connected component, so he cannot build some structure that include more nodes in the belief that chances of the disruptor to hit specific important links are too low.

For node deletion we have shown above that for the case of high linking costs we cannot strictly define the best response architecture of the network designer. Thus for the same reasons as in the previous section we use the *max*-proof network here as a benchmark case. For $B = (n-1)$, the network designer can then use $\frac{2(n-1)}{D_v+1}$ nodes in the connected component, leaving $1 - \frac{2(n-1)}{D_v+1}$ nodes unconnected. Facing a random attack from a network disruptor, the size of the largest remaining component depends on the exact nodes the network disruptor disconnects - thus, if he disconnects nodes that are within the connected component or outside of it. Consider the case of $D_v = 1$. The *max*-proof network is then the circle network and the largest remaining component will be given by $\frac{n-1}{n} * (n-2) + (1 - \frac{n-1}{n}) * (n-1)$. Comparing this with the largest remaining component in a star network which is given by $\frac{1}{n} * 1 + (1 - \frac{1}{n}) * (n-1)$, we find that even for this case where only one node needs to be left out to build a *max*-proof network, it holds that the largest remaining component in the star network is larger than that in the cycle network for any n. Since for an increase in the disruption budget, even more nodes need to be left out of the pre-disruption connected component to make it *max*-proof, it is clear that the star will then also be a better reply strategy than the *max*-proof component. Thus, it follows that for node deletion for the case of high linking costs with imperfect information on the side of the network disruptor the star network is a better response than the *max*-proof network for any n.

Proposition 10. *If there is imperfect information on the side of the network disruptor about the structure of the network, the best reply structure for low linking costs is the* max*-proof network for both link deletion and node deletion. For high linking cost the best reply structure for link deletion is the star network, and for node deletion the star network is a better reply structure than the* max*-proof network.*

Proof For low linking costs the network designer is able to build a *max*-proof network. Thus, with or without imperfect information the network disruptor cannot cause any additional damage and can therefore randomly delete links (nodes). The same holds for high linking costs and link deletion where in the star network the deletion of links is random for perfect information as well as imperfect information.

For the case of high linking costs and node deletion, comparing the expected payoff of the star network with that of the *max*-proof network for the case of $D_v = 1$, it holds that the payoff for the star network is larger than that of the *max*-proof network if it holds that $1 > \frac{n-1}{n}$. This is always given. For $D_v > 1$, the network designer needs to leave even more nodes unconnected to build a *max*-proof component, while the expected payoff of the star network decreases only marginally. □

We have, thus, seen in these robustness checks that for the case of low linking costs, our model is robust to introducing imperfect information on the side of the network designer as well as on the side of the network disruptor.However, for the case of node deletion the star network becomes a better response structure than the *max*-proof network in many cases, whereas the *max*-proof network was a better response in our original model.

8. Conclusion

In this paper we looked at the purely structural implications of network design. Abstracting from different value of players or links between them, we looked at what happens when a network is under attack by a network disruptor either attacking the links or the nodes of the network. We analyzed the implications of different linking costs on such a network structure and which network structures were safe against attack.

Summarizing our results, when linking costs are low, the network designer protects his network by constructing a regular network, where all nodes are equally well protected. When linking costs are high, contrary to what is the case for low linking costs, the best-response architectures under link and node deletion look fundamentally different. Under link deletion, it is a best response to connect all nodes in a star network. Under node deletion, it is a best response to leave some nodes out of the network, and build a smaller and stronger component. For intermediate linking costs, our analysis suggests that, under link deletion, star-like networks should be constructed, while under node deletion, whenever possible, all nodes get the same degree.

Thus comparing link deletion and node deletion, it can be said that while the optimal network structures start of completely different for high linking costs, they move to the same network structure if linking costs are low. Additionally, for the case of intermediate linking costs, it can be seen that while the optimal structures are more similar than for high linking costs there are still decisive differences between best-response structures for node deletion and link deletion. In cases where linking is extremely expensive, the knowledge about whether nodes or links are a potential target for disruption is vitally important when forming a network that is to be as proof as possible against disruption. Thus our analysis suggests that by increasing linking costs, the knowledge about which part of the network is being targeted becomes more vital for the network designer.

We end by exploring possibilities for future research, where the key question is to extend our present approach of a network designer to a multi-player game, where the nodes in the network are actual players. Let us start by looking at agents' incentives to form links, independently from the presence of a disruptor. In a more realistic model, there may be information decay, where information is worth less the larger the distance it traveled in the network (Jackson and Wolinsky (1996) and Bala and Goyal (2000)). From the perspective of information sharing, it is efficient for nodes to be as close to one another as possible, as is the case in the star; in equilibrium, players also have the tendency to connect to a central node, such that the star is likely to arise. As our analysis shows, at least for high linking costs, the star is also efficient under link deletion. However, it is a bad network under node deletion. Further, players' incentives to link to certain nodes may not only depend on the information obtained from those nodes, but may also depend on players' preferences. A well-known phenomenon in sociology is homophily, where in networks, birds of a feather flock together (McPherson et al., 2001). As shown in our analysis, such preferences are in direct conflict with efficient defense against network disruption, as a deletion of a few links or nodes may then cause great damage to the network.

Further, players may also directly take into account network defense and network disruption when deciding on which links to form. In one type of network formation extension of our model, we could assume that players dislike being removed from a network. An example would be a member of in an illegal network who does not want to be arrested. In some of our results, it is efficient to leave weak spots in the network, which are then more likely to be removed from the network. But individual players may not want to be at such weak spots then. In another type of network extension of our model, players may on the contrary like to be at vulnerable positions in a network. If a firm defects to a competing alliance, then this need not make the firm worse off. In its present network, each firm may try to manoeuvre itself in a crucial position, in order to have larger bargaining power in its network. This follows Burt (1992)'s argument that an individual may gain advantage by bridging structural holes in networks, thus assuring that information exchange takes place between different groups (for recent game-theoretic translations of this argument, see Goyal and Vega-Redondo (2007) and Kleinberg et al. (2008)). In our argument, this strong position as such does not relate to the bridging function, but to the fact that a disruptor is willing to give the such a bridge player a large payment for defecting, creating a very viable outside option for the

player, and increasing his bargaining power in his present network. This does not mean, however, that in equilibrium such bridging positions may ever arise, as every players seeks to obtain them.

Bibliography

Albert, R., Jeong, H., Barabasi, A.L., 2000. Error and attack tolerance of complex networks. Nature 406 (6794), 378–382. URL http://dx.doi.org/10.1038/35019019, m3: 10.1038/35019019; 10.1038/35019019.

Arguilla, J., Ronfeldt, D. (Eds.), 2000. Networks and Netwars: The Future of Terror, Crime, and Militancy. RAND Corporation.

Baburajan, R., 2010. Raytheon bbn technologies demos disruption-tolerant network. TMCnet.com 05 Feb 2010, 04 June 2010. URL http://election-2008.tmcnet.com/topics/technology-impact/articles/74686-raytheon-bbn-technologies-demos-disruption-tolerant-network.htm.

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

Bala, V., Goyal, S., 2000. A noncooperative model of network formation. Econometrica 68 (5), 1181–1229. URL http://www.jstor.org/stable/2999447.

Ballester, C., Calvo-Armengol, A., Zenou, Y., 2006. Who's who in networks. wanted: The key player. Econometrica 74 (5), 1403–1417. URL http://www.jstor.org/stable/3805930.

Bier, V.M., Oliveros, S., Samuelson, L., 2007. Choosing what to protect: strategic defensive allocation against an unknown attacker. Jounal of Public Economic Theory 9, 563–587.

Boesch, F., Tindell, R., 1984. Circulants and their connectivities. Journal of Graph Theory 8 (4), 487–499.

Boesch, F., Felzer, A., 1972. A general class of invulnerable graphs. Networks 2 (3), 261–283.

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

Bondy, J.A., Murty, U.S.R., 2008. Graph Theory. Springer, London, 2 edn.

Burt, R.S., 1992. Structural Holes. Harvard University Press, Cambridge.

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

Chiang, W., Chen, R., 1995. The (n, k)-star graph: a generalized star graph. Information Processing Letters 56 (5), 259–264.

Cohn, P., 2003. Basic algebra: groups, rings, and fields. Springer. URL http://books.google.nl/books?id=VESm0MJ0iDQC.

Dekker, A., Colbert, B., 2004. Network robustness and graph topology. In: Estivill-Castro, V. (Ed.), 27th Australasian Computer Science Conference. pp. 359–368. URL http://crpit.com/confpapers/CRPITV26Dekker.pdf.

Diestel, R., 2010. Graph Theory. Springer Verlag, Heidelberg, 4th edn. URL http://diestel-graph-theory.com/GrTh.html.

Enders, W., Jindapon, P., 2010. Network externalities and the structure of terror networks. Journal of Conflict Resolution 54 (2), 262–280.

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

Esfahanian, A.H., Hakimi, S., 1988. On computing a conditional edge-connectivity of a graph. Information Processing Letters 27 (4), 195 – 199. URL http://www.sciencedirect.com/science/article/pii/0020019088900257.

Galeotti, A., Goyal, S., Kamphorst, J., 2006. Network formation with heterogeneous players. Games and Economic Behavior 54 (2), 353–372.

Gao, P., 2010. Connectivity of random regular graphs generated by the pegging algorithm. Journal of Graph Theory 65 (3), 185–197. URL http://dx.doi.org/10.1002/jgt.20472.

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

Goyal, S., Vega-Redondo, F., 2007. Structural holes in social networks. Journal of Economic Theory 137 (1), 460–492.

Goyal, S., Vigier, A., 2009. Robust networks. Working Paper, Cambridge University URL http://www.econ.cam.ac.uk/faculty/goyal/wp09/robustnetwork2.pdf.

Harary, F., 1983. Conditional connectivity. Networks 13 (3), 347–357. URL http://dx.doi.org/10.1002/net.3230130303.

Hong, S., 2008. Hacking-proofness and stability in a model of information security networks. Working Paper, Vanderbilt University .

Hong, S., 2009. Enhancing transportation security against terrorist attacks. Working Paper, Vanderbilt University URL http://www.gtcenter.org/Archive/Conf09/Conf/Hong778.pdf.

Jackson, M.O., 2008. Social and Economic Networks. Princeton University Press, Princeton.

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

Kleinberg, J., Suri, S., Tardos, E., Wexler, T., 2008. Strategic network formation with structural holes. In: Proceedings of the 9th ACM Conference on Electronic Commerce. pp. 284–293. URL http://portal.acm.org/citation.cfm?id=1386835.

Kovenock, D., Roberson, B., 2010. The optimal defense of networks of targets. Purdue University, Working Paper p. 14. Oct. 2010.

Larson, N., 2011. Network security .

Lipsey, R.A., 2006. Network warfare operations: Unleashing the potential. Mimeo Center for Strategy and Technology, Air War College, Air University URL http://www.au.af.mil/au/awc/awcgate/cst/bugs_ch01.pdf.

Mader, W., 1971. Minimalen-fach kantenzusammenhängende graphen. Mathematische Annalen 191 (1), 21–28.

McBride, M., Hewitt, D., 2011. The enemy you canŠt see: An investigation of the disruption of dark networks .

McPherson, M., Smith-Lovin, L., Cook, J.M., 2001. Birds of a feather: Homophily in social networks. Annual Review of Sociology 27, 415–444. URL http://www.jstor.org/stable/2678628.

Menger, K., 1927. Zur allgemeinen kurventheorie. Fundamenta Mathematicae 10, 96–115. URL http://matwbn.icm.edu.pl/ksiazki/fm/fm10/fm1012.pdf.

Schwartz, G., Amin, S., Gueye, A., Walrand, J., 2011. Network design game with both reliability and security failures. In: Communication, Control, and Computing (Allerton), 2011 49th Annual Allerton Conference on. IEEE, pp. 675–681.

Taylor, M., Sekhar, S., D'Este, G., 2006. Application of accessibility based methods for vulnerability analysis of strategic road networks. Networks and Spatial Economics 6 (3), 267–291. URL http://dx.doi.org/10.1007/s11067-006-9284-9, m3: 10.1007/s11067-006-9284-9.

Graph-Theoretic Appendix

Graph Theoretic Lemmata and Definitions:

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

Definition II. *A* line graph *is an alternating sequence of nodes and links, which begins and ends with a node and each link connects exactly two nodes.*

Definition III. *A graph where each node is connected exactly of degree 2, is called a* circle graph.

Definition IV. *An* end node *is a node that is connected exactly of degree $\eta_i(g) = 1$.*

Definition V. *A link (or set of links) (ij) in a connected graph g, is called a* link cut *L, if g_{-L} is disconnected.*

Definition VI. *A node (or set of nodes) i in a connected graph g, is called a* node cut *V, if g_{-V} is disconnected.*

Lemma A.1. *Every connected graph contains at least $(n-1)$ links.*

Proof Build up a network step by step. Start with one node. Connect another node to it, and so on (note that any network can be constructed in such a manner). For each node you connect, you need at least one link. □

Definition VII. *Each graph that uses exactly $(n-1)$ links to connect n nodes, is called* minimally connected.

Lemma A.2. *Every minimally connected graph that is not a star has at least two nodes with degree larger than 1.*

Proof Any star has $(n-1)$ nodes with degree 1. In every minimally connected graph, each node has degree at least 1. It follows that in every non-star minimally connected network, at least two nodes have degree 1. It follows that at least two nodes have degree larger than 1. □

Lemma A.3. *Minimally connected graphs do not contain any circles.*

Proof This follows from Definition VII and from Chartrand (1977) Chapter 4. □

Definition VIII. *A graph G is called* bipartite, *if it is possible to divide the node set into two sets, N_1 and N_2, where each link connects a node of subset N_1 with a node of subset N_2 and no two nodes of the same set are directly linked.*

Lemma A.4. *The maximal damage a network disruptor with a disruption budget of D_l can cause in a star network is to disconnect exactly D_l nodes.*

Proof The star consists of exactly $(n-1)$ links, which connect one node with degree $(n-1)$ with $(n-1)$ nodes with degree 1. With each link that the network disruptor can delete, he can therefore only separate one of these nodes with degree 1 from the central node. Therefore, with a disruption budget of D_l, he can separate exactly D_l nodes. □

Lemma A.5. *Every connected, finite, 2-regular network architecture is isomorphic to the circle.*

Proof A 2-regular network cannot contain any end nodes, as these have degree 1. Alternatively, construct a 2-regular network step by step. Start with one node. This node should have two neighbors. These two neighbors should each have an extra neighbor. Continue this procedure until one node remains to be added, this leads to the construction of a line of $(n-1)$ nodes. The network can only be made 2-regular by connecting the 2 extreme nodes of this line (since n is finite), resulting in a circle. □

Lemma A.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 $\Gamma_{D_v}^{(max),min}$ and respectively $\Gamma_{D_l}^{(max),min}$ only contain r-regular networks.*

Proof Let $D_l = (r-1)(D_v = (r-1))$ and assume there exists a node i that is incident with less than r links. Then with a disruption budget of $D_l(D_v)$ we can delete all links incident with i (delete all nodes neighboring i) so that the largest component in g^2 has at most $n-1$ nodes ($n - D_v - 1$ nodes). Hence a network containing a node of degree less than r is not max-proof.[33]

Appendix 2 - Existence of circulant networks

Lemma A.7. *For $D_v = D_l = 1$, the unique minimal* max*-proof architecture is the circle containing all n nodes.*

Proof Graph-theoretically, the only connected 2-regular network is the circle (see Lemma A.5). In the circle, every set of connected nodes has two links and two neighbors connecting the set to the other nodes.[34] Every set of nodes including nodes unconnected to one another has more than two links and more than two neighbors connecting it to the rest of the nodes. Given Lemma A.6 the circle is minimal *max*-proof. □

The circle is a node-symmetric, simple network (see definitions below) that is minimal *max*-proof for the smallest deletion budget. This suggests that a network with these properties is minimal *max*-proof for general disruption budgets. To show existence of minimal *max*-proof networks, we here show the existence of circulant networks, which are node-symmetric and simple. We have shown in the main part of the paper that any circulant network is minimal *max*-proof.

Definition IX. *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).*

Definition X. *A graph is* node-symmetric *if and only if for any pair of nodes i and j it holds that there exists an automorphism*[35] *of the graph that maps i to j.*[36]

Necessary conditions on the existence of circulant networks are:

Lemma A.8. *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 $(n * r)/2$ 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 $(n * r)/2$. It follows that an r-regular network only exists if n and/or r is even. □

Lemma A.9. *For $D_l = (r-1)$ any r-regular circulant graph is minimal* max*-proof. For $D_v = (r-1)$ any r-regular circulant graph for which the jumps are convex is minimal* max*-proof. The set of minimal* max*-proof networks for node deletion is thus a subset of the set of minimal* max*-proof networks for link deletion.*

Proof We proof this in two steps.

- According to Mader (1971), every connected r-regular node-symmetric graph has $\lambda = r$ and, by definition, every circulant graph is node-symmetric. By definition for $D_l < \lambda$ the network disruptor cannot disconnect any node from the connected pre-disruption network. Consequently, for $D_l = (r-1)$ any r-regular circulant graph is minimal *max*-proof.

[33] For the formulation of this proof we would like to thank Kirby Fears.

[34] For a proof see Lemma A.5 in the Appendix.

[35] An automorphism of a simple graph is just a permutation α of its vertex set which preserves adjacency: if uv is an edge then so is $\alpha(u)\alpha(v)$ (see e.g. Bondy and Murty (2008) p.15).

[36] In this definition we follow Chiang and Chen (1995).

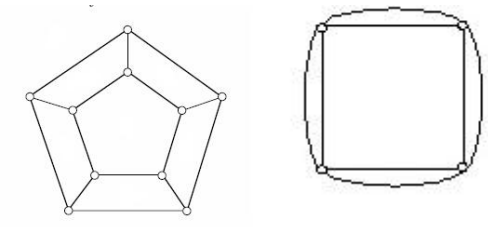
- According to Boesch and Felzer (1972) circulant graphs with convex jumps, i.e. for which $a_{i+1} - a_i \leq a_{i+2} - a_{i+1}$ and $1 \leq i \leq k-2$ have $\kappa = r$. By definition for $D_v < \kappa$ the network disruptor cannot disconnect any additional node from the connected pre-disruption network. Consequently, for $D_v = (r-1)$ any r-regular circulant graph with convex jumps is minimal *max*-proof. □

Lemma A.10. *For n and/or r even (where $r \geq 2$), a circulant network exists that is minimal* max*-proof both under a link deletion budget $D_l = (r-1)$ and a node deletion budget $D_v = (r-1)$.*

Proof That a circulant network with convex jumps where $a_1 = 1$ is minimal *max*-proof for node deletion follows directly from Lemma A.9. Since the set of minimal *max* proof networks for node deletion is a subset of that for link deletion, proving that the set for node deletion exists is sufficient. We prove the existence of such networks by constructions.

- Label the nodes of a graph $0, 1, 2, ..., n-1$.
- To build a circulant network with convex jumps that is minimal *max*-proof against node deletion it needs to hold that $a_1 = 1$. Thus the basic network is a circle spanning all n nodes.
- Since by definition in a circulant network node i is adjacent to any node $i \pm a_i$, each jump increases the degree of node i by 2 with the exception for even n of a jump going to node labeled $\frac{n}{2}$ which increases the degree of node i by 1, as $i + a_{\frac{n}{2}} = i - a_{\frac{n}{2}}$.
- For even n we only need to consider jumps up to node $\frac{n}{2}$ and for odd n up to $\frac{n-1}{2}$, as every jump above that can be described by the $i - a_i$ part of a smaller jump.
- Assume n is even and r is odd. By the previous step, to achieve an odd r the largest jump needs to go to node $\frac{n}{2}$. Every other jump needs to be in between $a_i = 1$ and $a_i = \frac{n}{2}$. To fulfill convexity the sequence $1, 2, 3, ..., \frac{n}{2}$ is enough. Thus the network exists.
- Assume r is even. To achieve even r the largest jump is of size $\frac{n-1}{2}$ for odd n and of size $\frac{n-2}{2}$ for even n. Every other jump needs to be in between $a_i = 1$ and $a_i = \frac{n-1}{2}$ ($\frac{n-2}{2}$ respectively). To fulfill convexity the sequence $1, 2, 3, ..., \frac{n-1}{2}$ ($1, 2, 3, ..., \frac{n-2}{2}$ respectively) is enough. Thus the network exists. □

Lemma A.10 does not imply, however, that every minimal *max*-proof network is circulant. This can be illustrated by the so-called Petersen graph, a well-known graph in graph theory. Here it 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 it is not a circulant. The right graph in Figure 5 is also minimal *max*-proof but is not not a simple network.



(a) Petersen Graph (b) Non-Simple

Figure 5: Minimal Max-proof Networks

Appendix 3 - Addition to Section on Node Deletion with High Linking Costs

Lemma A.11. *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 an order $\lceil (n - D_v)/[D_v + 1] \rceil$.*

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 order $\lceil (n-1)/2 \rceil$, as is shown by Lemma 4.
Step 2. We show in this step that, if it is true that the largest remaining post-disruption component in a pre-disruption minimal connected network of order γ, given $D'_v = (D_v - 1)$, is $\lceil (\gamma - D'_v)/(D'_v + 1) \rceil$, then it follows that the largest remaining component for a minimal connect network, given D_v, is $\lceil (n - D_v)/(D_v + 1) \rceil$.

Consider a link ij in a minimal connected g^1, where node j has the following properties. Among the components in g^1_{-j} not connected to i, the largest component has an order of at most $\lceil (n - D_v)/[D_v + 1] \rceil$; in g^1_{-i}, the component connected to j has an order larger than $\lceil (n - D_v)/[D_v + 1] \rceil$. Every minimal connected network contains at least one link ij where node j has these properties. This is because in a minimal connected network, every node lies on a path between two end nodes. Every deleted node cuts the network in at least two components. As one deletes consecutive nodes along this path, the maximal order of one component becomes smaller, while the maximal order of the other component gets larger. By continuity, one must meet a node j with the properties above.

Suppose that the disruptor deletes node j. Then i is part of a connected component C of an order of at most $[n - \lceil (n - D_v)/(D_v + 1) \rceil - 1]$ remains, in which the disruptor can delete a further $D'_v = (D_v - 1)$ nodes. By the assumption at the start of this step, the largest remaining component in C after the disruptor has taken out a further D'_v nodes from C has an order of at most $\lceil (n - D_v)/[D_v + 1] \rceil$. It follows that this is also the largest component that the designer can keep when the disruptor deletes D_v nodes from the entire network. □

The difference between the circle network and the *max*-proof network, is quite extreme. In Section 6, it is shown how a *(max* - 1)-proof network can be constructed in the form of a pair *r*-regular network. Such an architecture can also be used to make a smaller but stronger component in the case of node deletion and high linking costs. For a number of nodes γ, a pair *r*-regular network $B = \gamma * [r_1 r_2/(r_1 + r_2)]$ links, where by Proposition 8, $r_1 = r_2 = (r + 2)/2$. It follows that $L = (\gamma * (r + 2))/4$. Given that the linking budget is $(n - 1)$, it follows that the pair *r*-regular network has a number of nodes $\gamma = [4 * (n - 1)]/(r + 2) = [4 * (n - 1)]/(Dv + 3)$. We can now show that building a *max*-proof network is never the best option, and is either dominated by the circle network or by the *(max* - 1)-proof network.

Lemma A.12. *For any linking budget $B = (n - 1)$ links, and any disruption budget $D_v > 1$, a max-proof network weakly dominates the circle network for all $(n - 1) \geq D_v(D_v + 1)$.*

Proof The largest remaining component in a circle network after an attack by a network disruptor with a disruption budget of D_v is $\lceil [(n - 1) - D_v]/D_v \rceil$. The largest remaining component in a *max*-proof network after disruption with a disruption budget of D_v is $\lceil 2 * (n - 1)/(D_v + 1) - D_v \rceil$. To show that the *max*-proof network weakly dominates the cycle, we do not need to use the formulation to make both natural numbers as it holds that if $x \geq y$ then $\lceil x \rceil \geq \lceil y \rceil$.
$[2 * (n - 1)/(D_v + 1)] - D_v \geq [(n - 1) - D_v]/D_v$
$\Leftrightarrow [2 * (n - 1)/(D_v + 1)] - [(n - 1)]/D_v \geq D_v - 1$
$\Leftrightarrow [(n - 1)(D_v - 1)]/[D_v(D_v + 1)] \geq D_v - 1$
$\Leftrightarrow (n - 1) \geq D_v(D_v + 1)$ □

Lemma A.13. *For a linking budget of $B = (n - 1)$ links, where $(n - 1) \geq D_v(D_v + 1)$ and a disruption budget of D_v, the $(max - 1)$-proof network weakly dominates the max-proof network.*

Proof The largest remaining component in a *max*-proof network, after an attack by a network disruptor with a disruption budget of D_v will be $\lceil 2 * (n-1)/(D_v+1) - D_v \rceil$. The largest remaining component in a *max-1*-proof network, after an attack by a network disruptor with a disruption budget of D_v will be $\lceil 4 * (n-1)/(D_v+3) - (D_v+1) \rceil$ [37]. Again we do not need to use the formulation to make both natural numbers as it holds that if $x \geq y$ then $\lceil x \rceil \geq \lceil y \rceil$.
$4 * (n-1)/(D_v+3) - (D_v+1) \geq 2 * (n-1)/(D_v+1) - D_v$
$\Leftrightarrow 4 * (n-1)/(D_v+3) - 2 * (n-1)/(D_v+1) \geq 1$
$\Leftrightarrow (n-1) \geq (D_v+3)(D_v+1)/2(D_v-1)$
Thus what remains to be shown is that this is indeed larger than $D_v(D_v+1)$.
$(D_v+3)(D_v+1)/2(D_v-1) > D_v(D_v+1)$
$\Leftrightarrow (D_v+3)/2(D_v-1) > D_v$
$\Leftrightarrow (D_v+3)/2 > D_v^2 - D_v$
$\Leftrightarrow (D_v+1)/D_v^2 > 2/3$ This holds for all $D_v > 0$, since D_v by definition is a natural number. □

[37] We show this here explicitly for an even r, however, the same holds for odd r