Cambridge Working Papers in Economics

Attack, Defense and Contagion in Networks

Sanjeev Goyal and Adrien Vigier

CWPE 1327

Attack, Defense and Contagion in Networks

Sanjeev Goyal [*]   Adrien Vigier[†]

February 26, 2013

Abstract

Connections between individuals facilitate the exchange of goods, resources and information and create benefits. These connections may be exploited by adversaries to spread their attacks as well. What is the optimal way to design and defend networks in the face of attacks?

We develop a model with a Designer and an Adversary. The Designer moves first and chooses a network and an allocation of defense resources across nodes. The Adversary then allocates attack resources on nodes and determines how successful attacks should navigate the network.

Our main result is that, in a wide variety of circumstances, a star network with all defense resources allocated to the central hub node is optimal for the Designer. The Adversary targets undefended peripheral nodes; upon capture of these nodes the resources mount a concerted attack on the center.

[*] Faculty of Economics & Christ's College, University of Cambridge. Email: sg472@cam.ac.uk

[†] Department of Economics, University of Oslo. Email: a.h.vigier@gmail.com

We are grateful to the editor, Philipp Kircher, and three anonymous referees for many useful suggestions that have substantially improved the paper. We thank Marcin Dziubinksi for detailed and helpful comments. We also thank Nizar Allouch, Murali Agastya, Mariagiovanna Baccara, Oliver Bätz, Parimal Bag, Francis Bloch, Heski Bar-Isaac, Yann Bramoulle, Antonio Cabrales, Diego Cerdiero, Indranil Chakravarty, Matthew Elliot, Andrea Galeotti, Edoardo Gallo, Aditya Goenka, Britta Hoyer, Matthew Jackson, Daniel Kovenock, Gilat Levy, Margaret Meyer, Francesco Nava, Volcker Nocke, Romans Pancs, Rufus Pollock, Rony Razin, Bryony Reich, Pauline Rutsaert, Fernando Vega-Redondo, Rakesh Vohra, and participants at a number of seminars for comments. Sanjeev Goyal thanks the Keynes Fellowship and European Research Area Complexity-Net (grant 'Resilience and interaction of networks in ecology and economics') for financial support.

1 Introduction

Connections between individuals, cities, countries and computers facilitate the exchange of goods, resources and information and generate value. However, these connections may serve as a conduit for the spread of damaging attacks. The Internet reflects this tension clearly. Connectivity facilitates communication but is also used by hackers and 'botnet' herders to spread viruses and worms which compromise user privacy and jeopardize the functioning of the entire system.[1] As energy, communication, travel, consumer interaction increasingly adopt digital networks, cybersecurity has emerged as a major priority of national governments.[2] At the heart of these developments is the question of how to design and defend large scale networks that are robust to attacks.

In their influential paper on computer security, Staniford, Paxson and Weaver (2002) identify stealth worms and viruses as the main threats to security in large scale computer networks. Using data from actual attacks, they argue that adversaries scan the network to explore its topology and the vulnerabilities of nodes, prior to attack. In the first instance, the objective is to deploy a worm on selected hosts in the network. Deployed worms then exploit communication between nodes to progressively take control of neighboring hosts in the network. The likelihood of take over and spread in a network depends on the topology of connections and on vulnerabilities of individual hosts. These considerations motivate the following theoretical model.

We develop a model with a Designer and an Adversary. The Designer moves first and chooses a network and an allocation of defense resource. The Adversary then allocates attack resources on nodes and determines how successful attacks should navigate the network. Three ingredients of the model are key to the analysis: the value of the network, the contest between defense and attack resources, and the spread of attack through the network.

We assume that the value of a network is increasing and convex in the number of intercon-

[1] In 2009, roughly 10 million computers were infected with malware designed to steal online credentials. The annual damages caused by malware is of the order of 9.3 billion Euros in Europe, while in the US the annual costs of identity theft are estimated at 2.8 billion USD (Moore, Clayton and Anderson (2009)). One indicator of the economic magnitude of the problem is the valuation of security firms: Intel bought McAfee in 2010, for 7.68 billion USD (bbc.co.uk; 19 August 2010).

[2] For instance, in the United States, the Department of Homeland Security (DHS) is responsible for cybersecurity. Its mission statement reads,"Our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace. We rely on this vast array of networks to communicate and travel, power our homes, run our economy, and provide government services. DHS plays a key role in securing the federal government's civilian cyber networks and helping to secure the broader cyber ecosystem."

nected nodes.[3] We model the conflict between defense and attack resources on a network node as a Tullock *contest.*[4] The contest defines the probability of win for Designer and Adversary as a function of their respective resource allocation. The resources of the loser are eliminated, and a share of the winners resources may also be dissipated. In case the Adversary wins a contest on a node, he can relocate surviving attack resources to other defended nodes. The redeployed attack resources engage in contests with surviving defense resources. The dynamics of conflict continue as long as there remain both defense and attack resources. The initial network design and the conflict dynamics yield a probability distribution on surviving nodes. The Designer and Adversary are engaged in a zero sum game; so, given a defended network, we consider the minimum payoffs for the Designer, across all possible attack strategies. An *optimal defended network* maximizes these (minimum) payoffs.

Our main result is that, in a wide variety of circumstances, a star network with all defense resources allocated to the central hub node – the *CP-star* – is optimal for the Designer. The Adversary targets undefended peripheral nodes; upon capture of these nodes the resources mount a concerted attack on the center. We develop the argument in two parts: first, we establish that the result holds for the class of connected networks.[5] In the second step, we consider all networks and develop conditions on the network value function under which optimal networks are connected.

The intuition for the first step is as follows. The dynamics of conflict and contagion on the CP-star network yield extremal outcomes: either (almost) all nodes survive and remain connected or all nodes are eliminated. Consider next a network with two equally defended hub nodes and an equal number of other nodes linked to either hub. Faced with this defended network, the Adversary can allocate resources to peripheral nodes in line with the defense resources allocated to the corresponding hub node. The dynamics of conflict and contagion can generate extremal outcomes (as in the CP-star) but they also generate intermediate outcomes in which one hub is eliminated but the other hub (and its peripheral nodes) survives. Our analysis establishes that the expected number of surviving nodes is equal in the two scenarios,

[3] This is consistent with Metcalfe's Law (network value is proportional to the square of nodes) and Reed's Law (network value is exponentially increasing in nodes). For a discussion of alternative models of network values,, see Gueye and Marbukh (2012). Our assumption is also in line with the large theoretical literature on network externalities (Katz and Shapiro, 1985; Farrel and Saloner, 1986) and network economics (Bala and Goyal 2000a).

[4] Here we build on the rich literature on rent seeking and conflict, see Tullock (1980) and Hirshleifer (1995).

[5] Two nodes are connected if there is a path between them. A component is a maximal set of nodes that are connected. A network is connected if it contains only one component. Formal definitions are provided in Section 2.

but the two hub defended network yields a smoother distribution. More formally, the CP-star yields a mean preserving distribution on surviving nodes of the distribution obtained in the two defended hubs network. Since the network value function is convex in number of interconnected nodes, it follows that a CP-star generates greater expected payoffs for the Designer. Our proof of Theorems 1 and 2 shows that this idea can be generalized to cover all connected defended networks.

In the second step, we allow for networks with multiple components. So we study a situation where defense allocation, number of components and the architecture of individual components are all decision variables for the Designer. Theorem 4 characterizes network value functions for which optimal defended networks are connected. It says that, roughly speaking, if network value grows exponentially in the number of nodes then the CP-star is optimal, but if value grows at a slower rate (as in a polynomial function) then networks with multiple components may be optimal.

The optimality of CP-star is consistent with the practice of traffic monitoring at key nodes by security personnel, in the context of computer networks (Anderson, 2010). Financial contagion and liquidity freezes have been a major concern in the study of financial markets (Allen and Gale (2000)). The attractiveness of CP-star has also been highlighted in the context of financial networks. The complexity of bilateral deals among financial institutions makes it difficult for institutions to assess counter party risk. Haldane (2010) argues that a Centralized Counter Party Clearing House (CCP) would act as a resilient hub. The existence of such a hub would mitigate the uncertainty concerning the counter party. More generally, empirical work has highlighted the salience of hub-spoke structures (see e.g., Goyal, 2007; Newman, 2010) in a wide variety of contexts. Our results highlight the attractiveness of such an architecture from the point of view of defense.

Our framework of network design, defense and attack provides a useful way to think about a number of questions relating to networks that face threats. Section 4 shows that by varying our assumptions on network value functions, number of players, and the timing of moves we trace out an ensemble of models that can accommodate questions in economic epidemiology, terrorist networks, modern warfare, and criminal activity, in addition to Cybersecurity and financial networks. The exploratory analysis there suggests ways in which arguments developed in the proofs of Theorems 1-4 can be applied in other games and yields new insights that are consistent with empirical and applied work.

Our paper contributes to two rich strands of theoretical research in economics: the theory of networks and the theory of conflict.[6] The research on networks is concerned with the formation, structure and functioning of social and economic networks; for surveys of this work, see Goyal (2007), Jackson (2008), and Vega-Redondo (2007). To the best of our knowledge this is the first paper to study design and defense of networks that face an intelligent Adversary.[7]

In Baccara and Bar-Isaac (2008) information links between criminals facilitate cooperative play, but the detection of one criminal leads to the detection and punishment of connected others. This creates a trade-off between connections and vulnerability and suggests a similarity with the present paper. However, the models differ along a number of dimensions as they are motivated by very different applications. We highlight three differences. One, in our model the gains from large scale connectivity are key; by contrast, in their model the size of the network plays no essential role in defining network value.[8] Two, we study conflict between defense and attack; by contrast, there are no defense resources in their paper. Three, the Designer moves first in our model; the Adversary moves first in their model. Four, the nature of links is different. We assume undirected links, they assume directed links. A CP-star in our model and a hierarchy in their model are therefore very different objects. These these differences are substantive and together lead to different analysis and insights.

The theory of contests studies allocation of resources in situations of conflict; for overviews of this work, see Baye (1998), Konrad (2009), Sandler and Hartley (2007) and Garfinkel and Skaperdas (2012). There is also an extensive literature which studies conflict between two players across multiple battle fields with fixed budgets; Colonel Blotto games are a prominent example of such games (Hart, 2008; Bier, Oliveros and Samuelson, 2006; Powell 2008; and Roberson, 2006). The interest here is in understanding the equilibrium allocation of resources as conflict functions and budgets vary. Our paper extends this body of work along two dimensions: one, we locate individual battles within a network of interconnections and allow for successful resources to be moved from one battle to neighboring battles, and two, we study

[6] There is also a literature on network security spread across disciplines such as computer science, statistical physics, engineering and operations research (see Nagaraja and Anderson 2007; Newman 2010; Smith 2008). The strategic analysis of network design and defense in the face of an intelligent Adversary appears to be novel, in the context of these liteartures.

[7] Bala and Goyal (2000b) study network formation with exogenous probability of link failure. Hong (2008) studies the strategic complementarities between linking and protection. For a recent study of optimal network design in the face of random attacks, see Cabrales, Gottardi and Vega-Redondo (2011).

[8] For instance, in their model a network consisting of binary cells yields the same value as a connected network organized in a hierarchy with 2 agents at the the top. Section 4 analyzes a model in which the Adversary moves first. This is in line with the order of moves in Baccara and Bar-Isaac (2008). The discussion there clarifies the implications of difference in network value formulation.

the design of optimal interconnections across the ‘battlefields’.[9]

The rest of the paper is organized as follows. Section 2 presents our model and elaborates on the computer security application to illustrate the appropriateness of our assumptions. Section 3 studies optimal defended networks. Section 4 discusses open research questions. Section 5 concludes. The appendix contains proofs of some of the results.

2 Model and application

We study a zero-sum game between a Designer and an Adversary. The Designer has a collection of nodes and a given quantity of defense resources, while the Adversary has a given quantity of attack resources. The Designer moves first and chooses links between the nodes and allocates resources across the nodes to protect the network. The network and defense choices of the Designer are observed by the Adversary, who then chooses an attack strategy. The initial network design and the subsequent conflict together define a probability distribution on surviving networks. We next set out the notation and the concepts to formally describe this game. Then we elaborate on the computer security application and relate the assumptions of the model to features of the application.

2.1 The Designer-Adversary game

The Designer: The Designer, $\mathcal{D}$, has a collection of nodes $N = \{1, ..., n\}$, where $n \geq 2$; for expositional simplicity, assume that n is an even number. $\mathcal{D}$ chooses links between the nodes and allocates $d \in \mathbb{N}$ resource units across the nodes to protect the network. Let $\underline{d} = (d_1, d_2, ..., d_n)$ denote this allocation, where $d_i \in \mathbb{N}$ and $\sum_{i \in N} d_i \leq d$.[10]

A link between two nodes i and j is represented by g_{ij}: we set $g_{ij} = 1$ if there is a link between i and j, and $g_{ij} = 0$ otherwise. Links are undirected, i.e. $g_{ij} = g_{ji}$. The nodes and the links together define a network g.

There is a path between two nodes i and j in network g if there exists a sequence of nodes $i_1, .., i_k$ such that $i_1 = i$, $i_k = j$ and $g_{i_1 i_2} = ... = g_{i_{k-1} i_k} = 1$. Two nodes are said to be connected

[9] For a recent survey on conflict in fixed networks with no movement of resources, see Kovenock and Roberson (2012).

[10] In an earlier version of the paper, Goyal and Vigier (2010), the model and main results were established in a setting with continuous defense and attack resources; continuous defense and attack necessitate additional assumptions on the contest function and on the spread of attack resources. We felt these assumptions obscure the general arguments underlying our main results. So we work with integer valued defense and attack.

if there exists a path between them. A component of the network g is a maximally connected subset of nodes. $\mathcal{C}(g)$ is the set of components of g. We let $|C_k|$ indicate the cardinality (or size) of a component $C_k \in \mathcal{C}(g)$. A maximum component of g is a component with maximum cardinality in $\mathcal{C}(g)$. A network with a single component is said to be connected.[11] A network g' on N' is a sub-network of g if and only if $N' \subset N$, and $g'_{ij} = 1$ implies $g_{ij} = 1$. We let $G(g)$ denote the set of sub-networks of g.

Following Myerson (1977), we assume that the value of a network is the sum of the value of the different components. We will assume, for simplicity, that the value from a component depends only on its size.[12] Let the twice continuously differentiable function $f : \mathbb{N} \to \mathbb{R}_+$ specify a value to component sizes. If f is decreasing, or increasing and concave, then a network with no links maximizes value. Our interest is in the tension between the pressure to connect nodes to create value and the threat of contagion of attack via connections; so, in the benchmark model, we assume increasing and convex returns to size of component.

Assumption A.1: *The value of network g is given by*

$$\Pi(g) = \sum_{C_k \in \mathcal{C}(g)} f(|C_k|). \tag{1}$$

where $f(0) = 0$, $f' > 0$, and $f'' > 0$.

Increasing and convex network value functions arise naturally in the large literature on network externalities (see e.g., Katz and Shapiro (1985); Farrell and Saloner (1986)). In that literature, the value to a consumer from buying a product is related to the number of other consumers who buy the same product, i.e., belong to the same network. In its simplest form this gives rise to the quadratic form, $f(n) = n^2$. Such a function also arises in the well known connections model in the literature on network economics (see e.g., Goyal (1993); Bala and Goyal (2000a); and Jackson and Wolinsky (1996)). The appendix derives this payoff from an example on communication networks.

[11] The complete network, g^c, has $g_{ij} = 1$, for all pairs (i, j). The empty network, g^e, has $g_{ij} = 0$ for all pairs (i, j). A core-periphery network has two types of nodes, N_1 and N_2. Nodes in N_1 constitute the periphery and have a single link each and this link is with a node in N_2; nodes in N_2 constitute the core and are fully linked with each other and with a subset of nodes in N_1. When the core contains a single node, we have a star network. For a general introduction to network terminology, see Goyal (2007).

[12] A natural way to enrich the model would be to suppose that value is increasing in 'proximity' of nodes to each other. Our results on the optimality of CP-star extend to this setting.

Given a network with defense $(g, \underline{d})$ we let K denote the subset of protected nodes and O the subset of unprotected nodes, so that

$$K = \{i \in N : d_i > 0\} \quad ; \qquad O = N - K \tag{2}$$

Let O_i denote the subset of nodes in O which can be reached from node i through a path such that each node on that path lies in O, so that:

$$O_i = \{j \in O : g_{ij} = 1 \text{ or } \exists\{j_1, ..., j_m\} \subseteq O \text{ s.t. } g_{ij_1}...g_{j_m j} = 1\} \tag{3}$$

Similarly, let K_i denote the subset of nodes in K which can be reached from node i through a path such that each node on that path lies in O, so that:

$$K_i = \{j \in K : g_{ij} = 1 \text{ or } \exists\{j_1, ..., j_m\} \subseteq O \text{ s.t. } g_{ij_1}...g_{j_m j} = 1\} \tag{4}$$

Adversary: The Adversary $\mathcal{A}$ has $a \in \mathbb{N}$ attack resources. He observes the defended network $(g, \underline{d})$ and makes two strategic choices: one, he allocates resources across the n nodes. We let $\underline{a} = (a_1, a_2, .., a_n)$ denote this allocation where $a_i \in \mathbb{N}$, and $\sum_{i \in N} a_i \leq a$. Here $a_i \in \mathbb{N}$ indicates resource units allocated to node $i \in N$ at the outset of the attack. Two, he chooses a matrix Δ specifying for each node $i \in N$ a 'pecking order' for the spread of successful attack resources located at node i (a detailed description of the way in which attacks spread through the network is provided at the end of this section). In particular, if $|K_i| = k'$ then for all $s \in \{1, ..., k'\}$ we can find $i_s \in K_i$ such that $\delta_{ii_s} = s$, while $\delta_{ij} = 0$ if $j \in N - K_i$.

Attack and defense resources allocated on a given node engage in conflict over control of the node. We model this conflict on a node as a *contest*. Suppose $\mathcal{D}$ allocates d_i and $\mathcal{A}$ allocates a_i to node i. If $a_i + d_i > 0$ then, following Tullock (1980), we set the the probability of successful attack to be

$$\frac{a_i^\gamma}{a_i^\gamma + d_i^\gamma} \tag{5}$$

where $\gamma > 0$. If $a_i, d_i = 0$, then the probability of successful attack is 0. Skaperdas (1996) provides axiomatic foundations for this contest function. The parameter γ is referred to as the technology of conflict in the literature on conflict (Hirshleifer (1995)). Observe that raising γ tends to favor the side with most resources. In particular, an all pay auction – where the side with most resources wins the contest for sure – is a special case of our model. Observe also that the contest function is homogenous of degree 0 in resources. Our proofs exploit this property of the contest function.

We assume that success of attack is independent across contested nodes. This assumption is made for expositional simplicity. Positive correlations across contests on different nodes would complicate the expressions but would not alter the results on the optimality of CP-star.

We turn next to the dynamics of the spread of attack. Time is discrete $t = 0, 1, 2, ...$ The rules of the dynamics specify how resources move across nodes and engage in conflict.

Note first that, at date $t = 0$, $\mathcal{D}$ chooses defended network $(g, \underline{d})$ and $\mathcal{A}$ chooses attack resource allocation and pecking order of subsequent movement of resources $(\underline{a}, \Delta)$. The Designer's resources are stationary: they remain on the nodes to which they are initially allocated.[13]

At time **<u>t=0</u>:** For all $i \in O$, if $a_i > 0$ then $\mathcal{A}$ (i) captures i, (ii) captures O_i, and (iii) reallocates a_i attack resources to $j \in K$ given by $\delta_{ij} = 1$.[14]

Let $(g^1, \underline{d}^1)$ denote the residual network (of non-captured nodes and links between them) and defense allocation, and $\underline{a}^1$ the allocation of attack resources at the end of period 0.[15]

At time **<u>t=1</u>**: Contests take place simultaneously at all i such that $a_i^1 > 0$.

1. If *attack succeeds at* i then $\mathcal{A}$ (i) captures i, (ii) captures O_i^1, (iii) eliminates all d_i^1 defense resources. In addition (iv) fraction α of all a_i^1 attack resources are dissipated. If $\alpha a_i^1 \in \mathbb{R} - \mathbb{N}$, then eliminate the integer part only.[16] Finally, if at the end of period 1 there remains any node from the set K_i then $\mathcal{A}$ relocates the remaining $(1 - \alpha)a_i^1$

[13] The asymmetry between Designer and Adversary is consistent with applications such as computer networks: security software is installed on computers while worms and viruses can attack individual computers and upon capture of a computer then may travel to other connected computers.
Our results do not hinge on the specifics of how attack resources are replicated: so, for instance, our results carry over in a model where successful attack resources multiply and spread to all defended neighbors (or neighbors of neighbors) instantly.

[14] So all attack resources at node i are moved to a single node j and they are moved at the same time. Splitting of the attack resources can be accommodated within our analysis in a straightforward way. The latter assumption - about simultaneous movement of resource – is exploited in our proofs: Tullock contests create an incentive for the Adversary to use attack resources in sequence rather than all at once. This alters the payoffs in different networks and is likely to modify the trade-offs with regard to design of networks. A general treatment of robust network defense and design with sequential moves of winning resources remains an open problem.

[15] We also define by a similar extension N^1, O^1, K^1, as well as O_i^1 and K_i^1 for all $i \in N^1$.

[16] This is to guarantee integer resources at all stages of the attack.

attack resources to node j given by $\delta_{ij} = \min\{\delta_{is} : s \in K_i \bigcap N^2\}$. If $K_i \bigcap N^2 = \emptyset$ then eliminate remaining attack resources on i.[17]

2. If *defense succeeds at i* then (i) eliminate a_i^1 attack resources, (ii) eliminate αd_i^1 defense resources (if $\alpha d_i^1 \in \mathbb{R} - \mathbb{N}$, then eliminate the integer part only).

Let $(g^2, \underline{d}^2)$ denote the residual network and defense resources, and $\underline{a}^2$ the allocation of attack resources at the end of period 1. If $\underline{a}^2 = \underline{0}$ then terminate the process. Otherwise, move to period 2.

For **$\underline{\mathbf{t>1}}$** the process now iterates following the rules laid out as in period $t = 1$.

Given a defended network $(g, \underline{d})$ and attack strategy $(\underline{a}, \Delta)$, the dynamics of conflict described above yield a probability distribution on the set of sub-networks of g. Let $\mathbb{P}(g'|g, \underline{d}, \underline{a}, \Delta)$ denote the probability that the sub-network g' is the residual network after all conflicts have ended. We let $\Pi^e(g, \underline{d}, \underline{a}, \Delta)$ denote the expected value to the Designer given defended network $(g, \underline{d})$ and attack strategy $(\underline{a}, \Delta)$, so that:

$$\Pi^e(g, \underline{d}, \underline{a}, \Delta) = \sum_{g' \in G(g)} \mathbb{P}(g'|g, \underline{d}, \underline{a}, \Delta)\Pi(g'). \tag{6}$$

Figures 1 and 2 illustrate the nature of dynamics and the expected value of defended networks. In Figure 1, $n = 12$, $a = d = 4$. The Designer allocates all 4 units to the central node, while the Adversary allocates 1 unit each to four undefended peripheral nodes. These attack units capture the 4 peripheral nodes and then attack the central node. The contest at the central node involves 4 units of attack and 4 units of defense. Under the contest function specification (5), there is an equal probability of Designer and Adversary winning. In case the Designer wins the contest, the attack resources are eliminated. The process ends with 8 surviving nodes that are connected. So the payoff to the Designer is $f(8)$. In case the Adversary wins, the central node is captured, the defense resources at the central node are eliminated, and the attack resources then capture the remaining 7 peripheral nodes instantly. The payoff to the Designer is $f(0)$. So the expected payoff to the Designer from this defended network (under this attack strategy) is $f(8)/2$.

[17] Different specifications are here possible that would not alter our main results. However, this particular specification seems to fit best the application we have in mind.

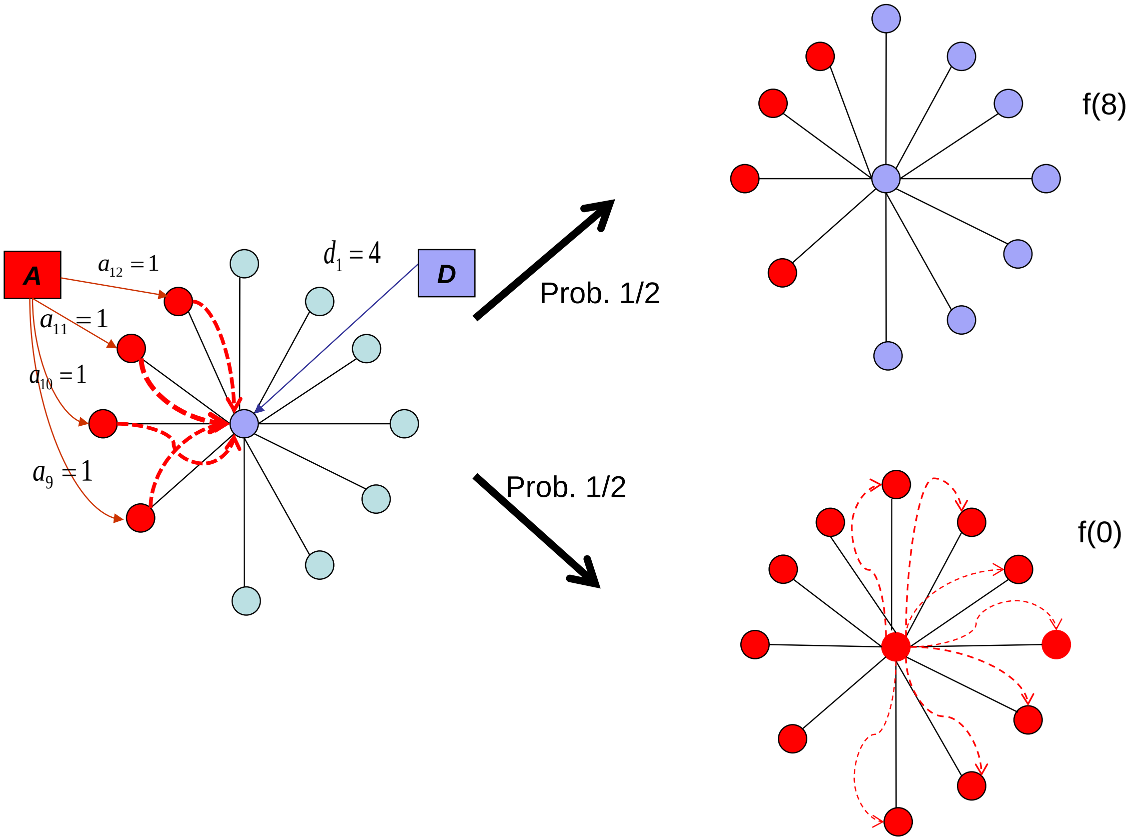


Figure 1: Attack and defense in star network: $n = 12$, $a = d = 4$.

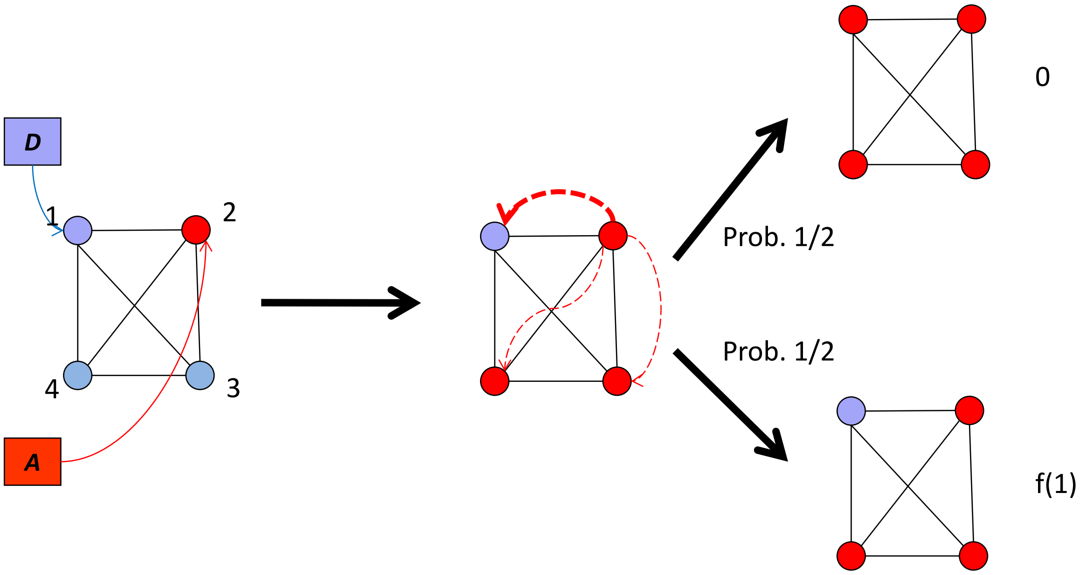


Figure 2: Attack and defense in complete network: $n = 4$, $a = d = 1$.

Figure 2 illustrates the dynamics in the complete network, with $n = 4$ and $a = d = 1$. Suppose that $\mathcal{D}$ allocates his resource to node 1, while $\mathcal{A}$ allocates his resource to node 2. Then at time $t = 0$, node 2 is captured and attack also spreads and captures $O_2 = \{3, 4\}$ (indicated by light dashed arrows). At time 1, attack resource target the single defended node 1 (indicated by heavy dashed arrows). As defense and attack resources are equal, given the contest function (5), the conflict on node 1 leads to capture and survival with equal probability. In case of survival the payoff to the Designer is $f(1)$, and in case of capture the payoff to the Designer is 0.

Our aim is to characterize optimal network design and defense for the Designer. Recall, Designer and Adversary are engaged in a zero sum game. Let $\overline{\Pi}^e(g, \underline{d})$ denote the minimum expected value given defended network $(g, \underline{d})$:

$$\overline{\Pi}^e(g, \underline{d}) = \min_{\underline{a}, \Delta} \Pi^e(g, \underline{d}, \underline{a}, \Delta) \tag{7}$$

We may now define optimal defended networks:

Definition 1 *A defended network $(g, \underline{d})$ is optimal if $\overline{\Pi}^e(g, \underline{d}) \geq \overline{\Pi}^e(g', \underline{d}')$ for all defended* *networks* $(g', \underline{d}')$.

Let $\epsilon > 0$. A defended network $(g, \underline{d})$ is ϵ-optimal if $\overline{\Pi}^e(g, \underline{d}) \geq (1 - \epsilon)\overline{\Pi}^e(g', \underline{d}')$ for all defended networks $(g', \underline{d}')$.

2.2 Application: computer network security

We discuss security in Peer-to-Peer (P2P) networks. This is an overlay computer network built on top of the physical computer network topology (other examples include the World Wide Web and e-mail networks). The most popular use of such networks is file sharing; examples include BitTorrent, Kazaa or eMule. The returns from joining the network are increasing in the number of users (as more users means more resources). This is in line with our assumption (A.1), the total social value of a component is increasing and convex in its size.

Online criminals, such as hackers and 'botnet' herders take the topology and security of a P2P network as given when they attack hosts taking part in the network. These adversaries generally prepare their attack, after scanning the network to assess its topology and security; in their well known paper, Staniford, Paxson and Weaver (2002) elaborate on the different mechanisms available for such scanning and highlight the growing efficacy of scanning. This is in line with our assumption that the Adversary is aware of the topology and the defense allocations, prior to choosing the attack. Adversary knowledge of the network and vulnerabilities of nodes is assumed in the computer science and electrical engineering literature; see e.g., Saia et al (2002) and Suto et al. (2012). A theoretical reason for this assumption is that sometimes the interest is in understanding the behavior of the system in the worst possible case; assuming complete knowledge of the network enables the most effective attack. So a network that survives such an attack is especially attractive.

One of the most dangerous threats to P2P networks are forms of self propagating malicious software called contagious (or stealth) worms. Worms are typically deployed by an external attack with viruses or other forms of malware; their objective is to deploy a worm on selected hosts in the network. The likelihood of successful infection of a host is lower the more sophisticated is the security installation and specialized personnel assigned to it. This feature of security is intuitive and is reflected in our contest function formulation (5).

Deployed worms propagate through the network by progressively taking control of neighboring hosts in the network. This is done by exploiting the communication mechanisms within the network. The worm attaches itself to packages of data sent between connected hosts and infects the neighbors of the hosts that are already infected; see Staniford, Paxson and Weaver

(2002) for a detailed discussion of worm contagion through exploitation of neighbors. The probability that the worm succeeds in infecting neighboring computers varies with the level of security installations on those computers. This transmission of a worm via communication links and subsequent conflict between the virus and the security installed on neighboring hosts is consistent with our rules on dynamics.

3 Optimal defended networks

The Designer has two instruments at his disposal to sustain network value: strategic deployment of defense resources and creation of links. In particular, the Designer chooses the number and architecture of components and the allocation of defense resources across these components. This optimization problem is complicated and for expositional simplicity it is convenient to proceed in steps. We start by solving the problem of optimal architecture and defense at the level of a single component. This problem is of independent interest in situations where attacks are rare. The convexity of the network value function implies that the network is connected: defense resources are then primarily used to maximize operational capability in the rare event of attack.[18]

We then consider the pure problem of number of components, in the absence of any defense resources. Finally, we combine the insights and present a result on optimal defended network where defense allocation, architecture of individual components and the number of components are all decision variables for the Designer.

We shall assume that $a > 0$: the case of $a = 0$ is uninteresting as any connected network is then optimal. If g is a star network and all defense resources are allocated to the central node we will refer to the resulting defended network as a *CP-star*, and denote it by $(g^s, \underline{d}^s)$.

3.1 Connected networks

Discrete optimization problems are marked by divisibility issues. We circumvent these difficulties by assuming throughout that $\frac{a}{d} \in \mathbb{N}$ and $n > a + 1$. Given defended network $(g, \underline{d})$ we will say that attack $(\underline{a}, \Delta)$ *mimics* defense if and only if for each defended node i_s in $K = \{i_1, ..., i_k\}$ one resource unit is allocated to exactly $\frac{a}{d} d_{i_s}$ distinct nodes in O_{i_s}, and all $\frac{a}{d} d_{i_s}$ attack resources thereafter mount a concerted attack on node i_s.

[18] We thank the editor for this suggestion.

Definition 2 *Given defended network* $(g, \underline{d})$*, we say that* $(\underline{a}, \Delta)$ mimics defense *if and only if there exists a set of a distinct nodes,* $\{j_1, ..., j_a\}$*, such that:*

1. $\{j_1, ..., j_{\frac{a}{d}d_{i_1}}\} \in O_{i_1}$, $\{j_{\frac{a}{d}d_{i_1}+1}, ..., j_{\frac{a}{d}d_{i_1}+\frac{a}{d}d_{i_2}}\} \in O_{i_2}$, ..., $\{j_{\frac{a}{d}d_{i_{k-1}}+1}, ..., j_{\frac{a}{d}d_{i_{k-1}}+\frac{a}{d}d_{i_k}}\} \in O_{i_k}$

2. $\delta_{j_s i_1} = 1$, $\forall s$ *s.t.* $s \leq \frac{a}{d}d_1$, $\delta_{j_s i_2} = 1$, $\forall s$ *s.t.* $\frac{a}{d}d_1 + 1 \leq s \leq \frac{a}{d}d_1 + \frac{a}{d}d_2$, ..., $\delta_{j_s i_k} = 1$, $\forall s$ *s.t.* $\frac{a}{d}d_{k-1} + 1 \leq s \leq \frac{a}{d}d_{k-1} + \frac{a}{d}d_k$

Figure 1 provides a simple example of an attack strategy that mimics defense: there is one defended node, and the two requirements are satisfied so long as $n > a + 1$. Consider next a slightly more complicated example of 2 hubs and suppose that $a = d = 4$. Suppose the Designer allocates 2 units of defense to each hub. Figure 3 illustrates an attack that mimics defense. The Adversary allocates 1 unit of resource to two peripheral nodes connected to each hub. These 2 units then move to attack their respective hubs. So the attack resources engage in contests on two hubs; the resource proportions are exactly in line with the proportion of the aggregate resources of a versus d.

We must also consider the possibility that, for some defended networks, the set of attacks which mimic defense may be empty. This happens if and only if $(g, \underline{d})$ satisfies property P.

Property P: *A defended network satisfies property P if we can find a subset of defended nodes,* $\{i_1, i_2, ..., i_{k'}\} \subset K$*, such that:*

$$|\bigcup_{s=1}^{k'} O_{i_s}| < \frac{a}{d}\sum_{s=1}^{k'} d_{i_s} \tag{8}$$

A simple example of a defended network which satisfies property P is the complete network in which every node is protected by 1 unit of defense. Another example of a defended network that satisfies property P is the following: fix $n = 12$ and $a = d = 4$, the network has two hubs, with the first hub being linked to 9 peripheral nodes and the second hub being linked to one peripheral node. If Designer allocates 2 units to each hub, then there is no attack that can mimic defense in this defended network.

Our first result shows that, in the class of connected networks, an optimal defended network is either the CP-star or satisfies property P.

Theorem 1 *Assume that (A.1) holds, $a, d > 0$, $\frac{a}{d} \in \mathbb{N}$ and $n > a+1$. Within the class of connected networks, either (i) a defended network satisfying property P is optimal, or (ii) the CP-star is uniquely optimal.*

Proof: Given a CP-star the optimal attack consists in allocating 1 resource unit to a unprotected nodes, thereafter targeting the center, so that:

$$\overline{\Pi}^e(g^s, \underline{d}^s) = \frac{d^\gamma}{d^\gamma + a^\gamma} f(n-a) \tag{9}$$

Here we apply the rules of the dynamic: capture of undefended nodes and spread of attack resources on these nodes precedes conflict on nodes with positive defense and attack resources. So it is strictly better for the Adversary to allocate all its resources to peripheral nodes.

Let $(g, \underline{d}) \neq (g^s, \underline{d}^s)$ denote an arbitrary (connected) defended network which does not satisfy property P. We will show that there exists an attack $(\underline{a}, \Delta)$ such that $\Pi^e(g, \underline{d}, \underline{a}, \Delta) < \frac{d^\gamma}{d^\gamma + a^\gamma} f(n-a)$. Define $K = \{i_1, ..., i_k\}$ to be the subset of protected nodes in $(g, \underline{d})$.

Case 1: $k = 1$

Note that since $(g, \underline{d}) \neq (g^s, \underline{d}^s)$ we can find two nodes in O with a link between them. By allocating one resource unit to one of these nodes we can then find an attack $(\underline{a}, \Delta)$ such that $\Pi^e(g, \underline{d}, \underline{a}, \Delta) \leq \frac{d^\gamma}{d^\gamma + a^\gamma} f(n-a-1)$.

Case 2: $k > 1$

Construct the sequence of sets $\left(N_{i_s}\right)_{1 \leq s \leq k}$ recursively as follows:

$$N_{i_1} = O_{i_1} \ , \ N_{i_2} = O_{i_2} - N_{i_1} \ , \ ... \ , \ N_{i_k} = O_{i_k} - \bigcup_{s=1}^{k-1} N_{i_s}$$

Let $n_{i_s} = |N_{i_s}|$, $s = 1, ..., k$. Note that by connectedness of g, $\bigcup_{s=1}^{k} N_{i_s} = O$.

Suppose first that $n_{i_s} \geq \frac{a}{d} d_{i_s}$, $\forall s$, and attack mimics defense in such a way that one resource unit is allocated to exactly $\frac{a}{d} d_{i_s}$ nodes in N_{i_s}, each of these resource units thereafter spreading to node i_s. Let Π^e denote the resulting expected network value.

Observe that, since $N_{i_s} \subset O_{i_s}$, a necessary condition for nodes in N_{i_s} to survive the attack is that i_s itself survives the attack. So the distribution of the total number of surviving nodes is first order stochastically dominated by that of $(n_{i_1} + 1 - a_{i_1})I_1 + .. + (n_{i_k} + 1 - a_{i_k})I_k$, where $\{I_1, .., I_k\}$ denotes a set of independent Bernoulli random variables such that $P(I_s = 1) =$

$\frac{d^\gamma}{d^\gamma+a^\gamma}$, $\forall s \in \{1,..,k\}$. Now since f is increasing and convex this implies that:

$$\Pi^e \leq \mathbb{E}[f\big(\sum_{s=1}^{k}(n_{i_s}+1-a_{i_s})I_t\big)] \tag{10}$$

But by Lemma 1 (in the appendix):

$$\mathbb{E}[f\big(\sum_{s=1}^{k}(n_{i_s}+1-a_{i_s})I_s\big)] < \mathbb{E}[f\big((\sum_{s=1}^{k}n_{i_s}+1-a_{i_s})I_1\big)] = \mathbb{E}[f\big((n-a)I_1\big)] \tag{11}$$

Hence:

$$\Pi^e < \frac{d^\gamma}{d^\gamma+a^\gamma}f(n-a) \tag{12}$$

Finally, since $(g,\underline{d})$ does not satisfy property P, we can always find a sequence of a nodes such that the first $\frac{a}{d}d_{i_1}$ of these nodes belong to O_{i_1}, the next $\frac{a}{d}d_{i_2}$ of these nodes belong to O_{i_2}, and so on up to k. So, by relabeling appropriately, the previous steps can be repeated in the case where $n_{i_s} < \frac{a}{d}d_{i_s}$ for some s.

■

In the proof, the arguments focus on networks which violate property P. First, we show that in a CP-star network the expected payoff of the Designer is given by (9). The second step constitutes the heart of the proof: any defended network which does not satisfy property P has defended nodes surrounded by sufficient number of unprotected nodes. This opens the way to attacks which *mimic* defense. But attacks which mimic defense have a remarkable property: the probability distribution on surviving nodes induced in the CP-star is a mean preserving spread of the (best possible) distribution on surviving nodes induced by a mimic defense. Since f is convex, the expected network value achieved under the mimic defense is less than that achieved with a CP-star.

We illustrate this point with the help of Figure 3. In this Figure, $n = 12$, $a = d = 4$. The network has a core-periphery structure in which two hubs are linked to each other and to 5 other peripheral nodes each. The Designer allocates 2 resource units to each hub and the Adversary employs a mimic attack strategy: he allocates 2 resources to peripheral nodes connected to one hub and 2 resource units to peripheral nodes connected to the other hub. In the first instance, the Adversary captures 4 peripheral nodes. The resources then target their respective hub nodes. This is illustrated in the network on the left.

There are four possible outcomes of the two contests on the hubs: either both hubs survive, both hubs are captured or one hub survives and the other is captured. Given the equal resources engaged in contests, it follows that the first two outcomes each arise with probability 1/4. The two outcomes define terminal states of the dynamics, represented at the top and the bottom end of the Figure. There is a probability 1/2 that one of the hubs survives and the other is captured. This is represented in the middle network of the Figure. Moreover, the captured hub triggers the capture of the peripheral nodes while attack resources then target the surviving hub. This leads to a second contest at the surviving hub. With probability 1/2 the hub survives the attack, and with probability 1/2 it is captured. In case of capture the attack resources then instantly also capture the remaining 3 peripheral nodes. This dynamic process yields probability density $\mathbb{P}_m$ on surviving nodes: with probability 1/2 all nodes are captured, with probability 1/4 eight nodes survive and with probability 1/4 four nodes survive. Observe that the probability distribution is first order stochastically dominated by the distribution $\mathbb{P}'$: with probability 1/4 all nodes are captured, with probability 1/2 eight nodes survive and with probability 1/4 four nodes survive.

Finally, an inspection of Figure 1 reveals that the probability density $\mathbb{P}_s$ of surviving nodes is as follows: with probability 1/2 all nodes are captured, with probability 1/2 all nodes survive. It is easy to verify that $\mathbb{P}_s$ is a mean preserving spread of $\mathbb{P}'$. Since f is convex, the expected payoff to the Designer from the CP-star is higher than the expected payoff from the core-periphery network with 2 hubs.

Theorem 1 tells us that optimal defended networks either satisfy property P or must be the CP-star network. We now explore the circumstances under which property P may be attractive for the Designer. Consider a setting where $n = 3$, $f(n) = n^2$, and $a = d = 2$. The CP-star network yields the Designer an expected payoff of 1/2. By contrast, the complete network with two protected nodes yields at least 1. So the complete network dominates the CP-star. Observe that the complete network satisfies property P. This raises the question: how attractive are defended networks with property P, more generally?

The key to the problem is the number of nodes, n: to see this note that, in this example, the expected payoff of the Designer under the complete network is bounded above by 4 (for all n), while the minimum expected payoff from the CP-star is given by $1/2(n-2)^2$. So for $n \geq 5$, the CP-star dominates the complete network. Our next result, Theorem 2, shows that this is a more general point: for large n, the CP-star dominates *all* defended networks which satisfy property P.

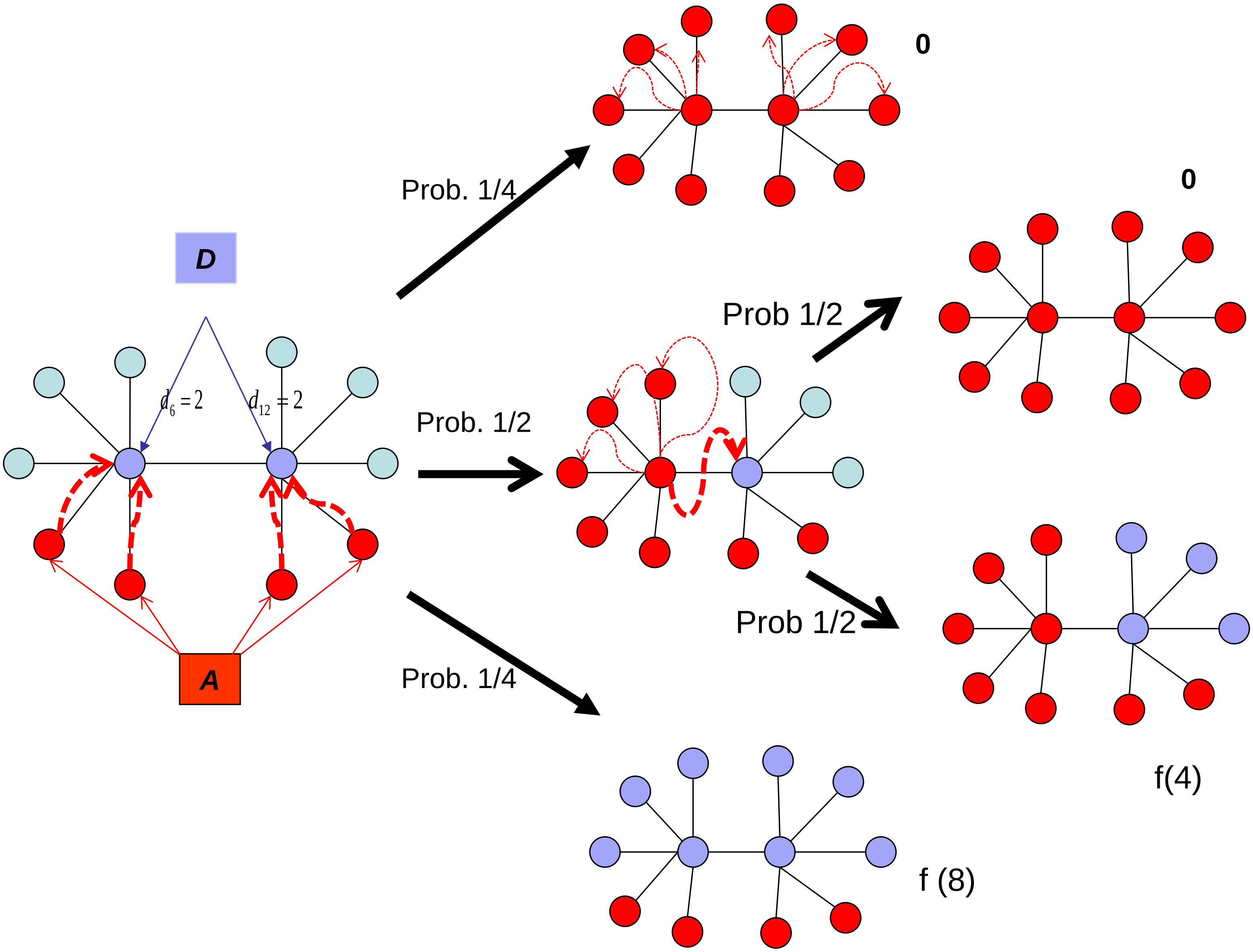


Figure 3: Mimic attack in core-periphery network: $n = 12$, $a = d = 4$.

To formally state and prove the result, we proceed by assuming that $\frac{f(n-1)}{f(n)}$ converges as $n \to \infty$. Define

$$\ell = \lim_{n\to\infty} \frac{f(n-1)}{f(n)} \tag{13}$$

In the communication networks example, $f(n) = n^2$, and the limit $\ell = 1$. By contrast, for the function $f(n) = 2^n$, the limit $\ell = 1/2$.

Theorem 2 *Assume that (A.1) holds, $a, d > 0$, $\frac{a}{d} \in \mathbb{N}$ and $n > a + 1$. Let $\epsilon > 0$ and consider connected networks. There exists n_0 such that, for all $n > n_0$:*

1. *If $\ell < 1$ the CP-star is uniquely optimal.*

2. *If $\ell = 1$ the CP-star is ϵ-optimal.*

There are two parts to the result. The first part pertains to the case where $\ell < 1$. Consider a defended network which satisfies property P: suppose there are k defended nodes. If $k = 1$ and the network is not a star, then it is easy to see that the Adversary can eliminate strictly more than a nodes before mounting an attack on the single protected node. Thus expected payoff to the Designer is strictly lower than in the CP-star. If $k > 1$, then there is at least one defended node i such that $O_i \geq (n-k)/k$. For large n, $(n-k)/k > a$. Consider the attack strategy in which $\mathcal{A}$ allocates all resources to O_i. Then the probability that node i survives attack is $d_i^\gamma/(d_i^\gamma + a^\gamma)$ and in this event the payoff to Designer is $f(n-a)$. In case the attack succeeds the maximum payoff to the Designer is bounded above by $f(n-(n-k)/k)$. If $\ell < 1$, this last term becomes very small, as n grows. So in the event that the attack succeeds, the Designer earns very little. On the other hand, the probability of survival $d_i^\gamma/(d_i^\gamma + a^\gamma)$ is smaller than the probability of survival in the CP-star, $d^\gamma/(d^\gamma + a^\gamma)$, since $d_i < d$. So it is this latter effect that prevails, as n gets large.

The second part pertains to the case where $\ell = 1$. In this case, for any $\epsilon > 0$, $f(n-a) \geq (1-\epsilon)f(n)$ for large enough n. Consider a direct attack strategy which targets the k protected nodes in proportion to the defense resources allocated to them. Lemma 1 and Theorem 1 tell us that $\Pi^e \leq d^\gamma/(d^\gamma + a^\gamma)f(n)$. Putting together these inequalities yields us the inequality $(1-\epsilon)\Pi^e \leq d^\gamma/(d^\gamma + a^\gamma)f(n-a)$: so the CP-star is ϵ-optimal.

Theorem 2 is a powerful result: in the class of connected networks, the CP-star is optimal, when n is large. In particular, it holds for all payoff functions which satisfy (A.1): so the result does not depend on the curvature of f. The result holds for all γ in the Tullock contest function: so the conclusion is robust with respect to the technology of conflict. It holds for all resource configurations between the Designer and the Adversary which respect the property $a/d \in \mathbb{N}$. Finally, the result holds for all values of α, the parameter of resource dissipation.[19]

In an influential paper, Albert, Jeong and Barabasi (2000) have argued that hub-spoke architectures are robust to random attacks but vulnerable to strategic attacks since the Adversary can significantly reduce a hub-spoke network's functionality by removing only a few hub nodes. Our result, on the other hand, highlights the attractiveness of hub-spoke architectures when attacks can spread in networks and there are limited defense resources.

Theorems 1 and 2 complete our analysis of optimal defended networks within the class of connected networks. We now turn to the study of networks with multiple components.

3.2 Number of components

When the Designer has 0 defense, the only way to sustain network value is to separate the nodes into distinct components. Any component which is attacked will be completely captured, irrespective of its architecture. This allows us to focus on the pure problem of number of components in optimal networks. The following result provides a characterization of the optimal number of components.

Theorem 3 *Assume that (A.1) holds, $a > 0$ and $d = 0$. (i) If $a < n/2$ then the optimal network contains at least $a + 1$ maximal components and at most one component which is smaller; the Adversary targets at most one node in each component. (ii) If $n/2 \leq a < n - 1$, then the empty network is the optimal network; the Adversary eliminates a nodes. (iii) If $a \geq n$ then every network is optimal as the Adversary eliminates all n nodes.*

The proof is given in the appendix. If $a \geq n$ then the Adversary can always eliminate all nodes, irrespective of the structure of the network. So, it follows that the Designer earns a payoff of 0 irrespective of the network. Similarly, if $a \geq n/2$ then the Adversary can always eliminate any component with two nodes or more. So the interesting case really is when $a < n/2$.

Observe that there must be at least $a + 1$ components: else the payoff is 0. And a network with $a + 1$ components on the other hand, guarantees $\mathcal{D}$ strictly positive payoff. Next, we

[19] We note that the Designer is assumed to be risk-neutral in our model. If the Designer is significantly risk-averse then this may make his objective function concave, in spite of convex network value function. In that case, optimal networks will be empty.

show that there are at least $a+1$ maximum components. If there are a or fewer maximum components then all of them will be eliminated. However, the Designer can do strictly better by simply taking one node i out of a maximum component, say, C_1. As part of his best response the Adversary must eliminate C_1 less i. But then $\mathcal{D}$ does strictly better by this deviation. We then show that at most, one component has size strictly smaller than the maximum size. If there were two such components, then the Designer could take one node from the smaller to the larger of the two components. As this new larger component still remains (weakly) smaller than the maximum component, the Adversary will not attack it. It now follows from the convexity of f that payoffs to $\mathcal{D}$ are strictly increased by this move.

In case $a < n/2$, Theorem 3 sets lower bounds on the number of components; the precise number of components depend on the convexity of the payoffs function. To develop this idea further, we work with a class of network value functions $f(n) = n^{\beta}$, where $\beta > 1$. We interpret β as a measure of the convexity of the network value function. Define $x(a, \beta) = \frac{\beta a}{\beta - 1}$.

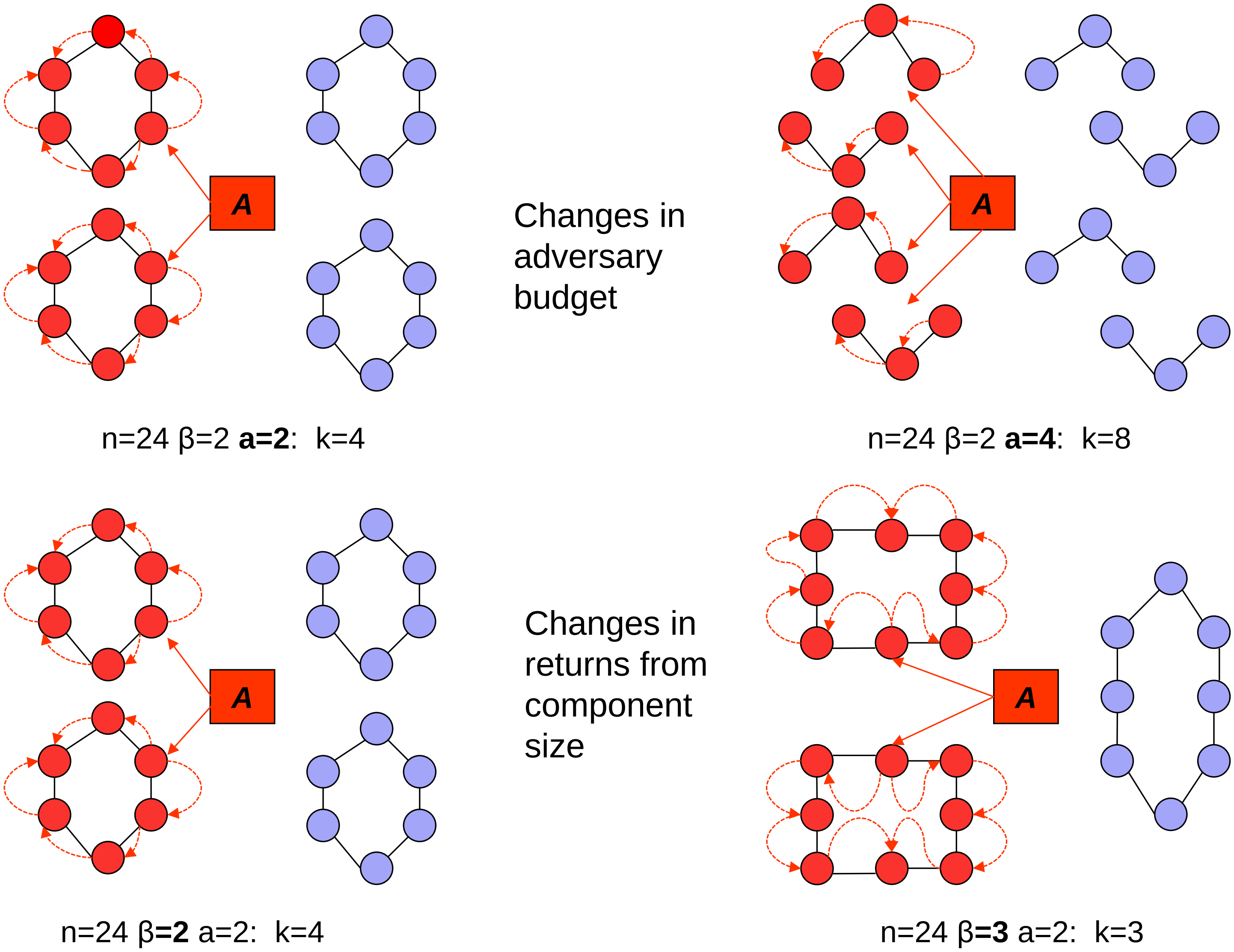
Proposition 1 *Assume that (A.1) holds and suppose $f(n) = n^{\beta}$* for $\beta > 1$. *If $x(a, \beta) \in \{a+1, .., n\}$ and divides n, then the unique equilibrium network consists of $x(a, \beta)$ equal size components.*

The proof is provided in the appendix. Observe that $x(a, \beta)$ is increasing in Adversary budget, a, and falling in the parameter of convexity, β.[20]

Figure 4 illustrates the comparative statics for Adversary budget and the convexity of the network value function. We take $n = 24$. First, consider the effects of budgets: here we suppose that $\beta = 2$. The optimal number of components increases from 4 to 8, as we increase the Adversary budget from 2 to 4. Second, consider the effects of convexity: here we suppose the budget to be $a = 2$, the optimal number of components falls from 4 to 3 as we raise the convexity from $\beta = 2$ to $\beta = 3$.

The analysis so far shows that, within the class of connected networks, the optimal network is either a CP-star or satisfies property P. Moreover, if n is large, then the CP-star is optimal or almost optimal. When $\mathcal{D}$ has no defense resources, his choice of optimal networks revolves around the number of components. Optimal networks contain equal sized components whose

[20] These findings on the relation between adversary budgets, on the one hand, and network size and success of the network, on the other hand, echo discussions in the popular press with regard to terrorist networks. For instance, the editor of Newsweek magazine, Mr. Zakaria (2008) wrote, " ...... the world's governments have effectively put them on the run ... the Jihadists have had to scatter, work in small local cells... Terrorists have not been able to hit big, symbolic targets.... So they blow up bombs in cafes, marketplaces, and subway stations" (Zakaria (2008, p. 3)).


A
A
Changes in adversary budget
A
Changes in returns from component size
A

n=24 β=2 **a=2**: k=4

n=24 β=2 **a=4**: k=8

n=24 β**=2** a=2: k=4

n=24 β**=3** a=2: k=3

Figure 4: Optimal networks: $f(m) = (m)^{\alpha}$, $n = 24$, β=2,3 and $a = 2, 4$

number is falling in the convexity of the value function and increasing in the Adversary's budget. We now combine these insights and study optimal defended networks in a setting where defense allocation, architecture of individual components and the number of components are all decision variables for the Designer.

3.3 The general optimization problem of Designer

A remarkable feature of Theorems 1 and 2 is that they make no assumptions on the extent of f's convexity. However, Proposition 1 shows that the curvature of f will affect the number of components. It is, after all, the convexity of f which creates the tension between the pressure to connect nodes to create value and the threat of spread of attack via connections. Insufficient gains from connecting nodes will naturally induce optimal networks with multiple components. Similarly, a sufficient amount of convexity will restrict optimal networks to the set of connected networks. Our next proposition builds on these remarks to characterize network value functions for which optimal defended networks will be connected.

Theorem 4 *Assume that (A.1) holds, $a, d > 0$, $\frac{a}{d} \in \mathbb{N}$, $n > a + 1$, and let $\epsilon > 0$.*

1. *If $\ell < 1$ there exists n_0 such that, for all $n > n_0$, the CP-star is ϵ-optimal among all defended networks.*

2. *If $\ell = 1$ then optimal defended networks may contain multiple components.*

Proof. For the first part, it follows from Theorem 2 that, for large n, we only need to compare the performance of the CP-star with that of unconnected defended networks.

Consider therefore defended network $(g, \underline{d})$, with g unconnected. Let C denote the largest component in g, $n_C = |C|$, and d_C the total amount of resources allocated to nodes in C. Note in particular that $d_C \leq d$, while $n_C < n$.

Suppose first $n_C \leq \frac{n}{2}$. As in Theorem 2, choose $\ell' < 1$ and n_0' such that $f(m) < (\ell')^{n-m} f(n)$, $\forall n \geq m \geq n_0'$. For $n > 2n_0$ and irrespective of attack the network value is then bounded above by $2(\ell')^{\frac{n}{2}} f(n)$. Now, again as in Theorem 2 choose $\ell'' > 0$ and n_0'' such that $f(n-a) > (l'')^a f(n)$, $\forall n \geq n_0''$. Then for n large enough and irrespective of attack the network value is bounded above by $2(\ell')^{\frac{n}{2}} (\ell'')^{-a} f(n-a)$. A comparison with (9) establishes that the CP-star dominates $(g, \underline{d})$, for large enough n.

Assume henceforth $n_C > \frac{n}{2}$. By Theorem 2 we can find an attack on g with resulting expected network value Π^e such that

$$\Pi^e \leq \frac{d_C^\gamma}{d_C^\gamma + a^\gamma} f(n_C - a) + f(n - n_C) \tag{14}$$

But for $n \geq n_0' + n_C$ we have $f(n - n_C) \leq (\ell')^{n_C} f(n)$. Since $\ell' < 1$ and $n_C > \frac{n}{2}$ we obtain

$$\Pi^e < \frac{d_C^\gamma}{d_C^\gamma + a^\gamma} f(n_C - a) + (\ell')^{\frac{n}{2}} f(n) \tag{15}$$

Using the fact that $f(n) < (\ell'')^{-a} f(n-a)$ for $n \geq n_0''$ we then have, for n large enough:

$$\Pi^e < \frac{d_C^\gamma}{d_C^\gamma + a^\gamma} f(n_C - a) + (\ell')^{\frac{n}{2}} (\ell'')^{-a} f(n - a) \tag{16}$$

Finally, $n_C < n$,

$$\Pi^e < \left(\frac{d_C^\gamma}{d_C^\gamma + a^\gamma} + (\ell')^{\frac{n}{2}} (\ell'')^{-a} \right) f(n - a) \tag{17}$$

The first bracketed term in (17) is at most $\frac{d^\gamma}{d^\gamma + a^\gamma}$, since $d_C \leq d$, while the second term tends to 0 as n becomes large. This completes the proof of the first part of the proposition.

For the second part, suppose $f(n) = n^2$, $d = 1$, $a = 2$. In the class of connected networks, Theorem 2 tells us that CP-star is optimal. In the CP-star network, the expected payoff is:

$$\overline{\Pi}^e(g^s, \underline{d}^s) = \frac{1}{1 + 2^\gamma}(n-2)^2 \tag{18}$$

Now let $(g, \underline{d})$ denote a defended network consisting of two components of equal size; suppose one component is a star with defended central node. We then have

$$\overline{\Pi}^e(g, \underline{d}) = \frac{1}{2}(\frac{n}{2} - 1)^2 \tag{19}$$

If $n \geq 4$, then $\overline{\Pi}^e(g, \underline{d}) > \overline{\Pi}^e(g^s, \underline{d}^s)$, for all $\gamma > 5$.

■

Observe that $\ell < 1$ implies that network value grows exponentially in the number of nodes: so the loss in value from splitting the network into multiple components can be made very large, by suitably raising n. This is most easily seen in the case when the maximum component comprises less than one half of the nodes. In that case the expected payoffs to the

Designer are bounded above by $2(x)^{\frac{n}{2}}(y)^{-a}f(n-a)$, where $y < \ell < x < 1$. Recall that the expected payoffs from the CP-star network are given by (9). For large n, a comparison of the expressions yields the desired result. Observe that if $\ell < 1$ then for large enough n, optimal defended networks are connected for all $\gamma > 0$ and for all $a, d > 0$ satisfying $a/d \in \mathbb{N}$. By contrast, when $\ell = 1$, network value is reflected in polynomial functions and optimal networks may consist of multiple components. Moreover, our construction in the proof of Theorem 4 suggests that the number of components in a optimal defended network will generally depend on the resources of Designer and Adversary and the technology of conflict (parameterized by γ). In a situation where attack resources exceed defense resources ($a > d$), an increase in γ makes the defense in a CP-star less effective and therefore renders the alternative of separation of nodes into distinct components more attractive.

4 Discussion

Our framework of network design, defense and attack provides a useful way to think about a number of questions relating to networks that face threats. In particular, variations on network value functions, number of players, and the timing of moves enable us to trace out an ensemble of models that can accommodate a wide range of other applications. A complete analysis of these alternative models is outside the scope of the present paper; the exploratory analysis undertaken here suggests that arguments developed in the proofs of Theorems 1-4 can be applied to other games and also serves to bring out new insights that are consistent with empirical and applied work.

4.1 Decentralized linking and defense

In the benchmark model there is one Designer and one Adversary. In large scale computer networks, there are typically many players who can choose links and security.[21] Similarly, in social contexts, the spread of diseases depend on interaction and vaccination choices of individuals (Geoffard and Philipson (1997), Kremer (1996), Pongou and Serrano (2009)). And in financial networks, banks make choices on linkages with other banks and also choose investments and level of reserves (Allen and Gale (2000)).

There are two natural variants within the decentralized decision making context. The first scenario involves a single Designer who chooses links but many players/nodes that choose

[21] For a discussion of issues in the theory of decentralized information networks, see van Zandt (1999).

security. This may correspond to the case where a central authority chooses an infrastructure while individual nodes choose defense or security levels. Individual security choices will generally create externalities on others (as in models of vaccination and epidemics). So the problem is to design a network in which the negative effects of these externalities are mitigated. The second scenario involves many players choosing links as well as security; here coordination problems arise in addition to the externalities present in the first scenario.

Our results, Theorems 1-4, are useful for the study of the decentralized problem as they may be interpreted as the first best (or the planner) solution. They alow us to ask questions such as what is the the price of decentralization of links and of security (i.e., the difference between the social welfare attained in the first best and the expected welfare attained in the decentralized equilibrium).

4.2 Richer network value models

In the benchmark model, network value is strictly increasing and convex in number of nodes in a component. It is clear that, in our framework, a network value function that is concave would render the problem of optimal network design uninteresting. But there is a range of possible alternatives between concave and convex network value functions. In particular, in some settings the marginal value of connections is initially increasing but then dissipates sharply. The aim of the example below is to draw out an implication of such network value functions for the structure of our argument in Theorems 1-2.

Suppose that $n = 12$, $a = d = 2$, and the network value function is as follows:

$$f(n) = \begin{cases} n^2 & \text{for } 0 < n \leq 6 \\ 36 + 0.2(n-6) & \text{for } 6 < n \leq 12. \end{cases} \tag{20}$$

For expositional simplicity, we also assume that $\alpha = 1$.

The expected payoff from a two hub core-periphery network depends on the attack strategy of the Adversary. It may be checked that the Adversary prefers to attack periphery nodes attached to distinct hub nodes. So the probability distribution of the surviving nodes under CP-star is: probability 1/2 of 10 surviving nodes, and probability 1/2 for 0 surviving nodes. The probability distribution of surviving nodes under the two hubs network is: probability 1/4 of 10 surviving nodes, probability 1/2 for 5 surviving nodes and probability 1/4 for 0 surviving nodes. The former is a mean preserving spread of the latter.

The expected payoff from the CP-star is given by

$$\frac{1}{2}f(10) = \frac{1}{2}(36 + 0.8) = 18.4. \tag{21}$$

The expected payoffs to the Designer under two hubs network are given by:

$$\frac{1}{4}f(10) + \frac{1}{2}f(5) = 21.7. \tag{22}$$

Thus the two hub network dominates the CP-star. The move from the CP-star network to the two hub defended network creates the following trade-off: the probability of 10 nodes surviving goes down from 1/2 to 1/4, but the probability of 5 nodes surviving goes up from 0 to 1/2. As the network value function is eventually linear, most of the potential network value is attained with the few initial nodes. So the increase in probability of 5 hubs surviving is more attractive for the Designer. This example illustrates the role of convex network value function in the analysis of Section 3. If a significant part of the network value is attainable with a subset of the resources then multi-hub networks may be optimal.

An implicit assumption in the benchmark model is that there are no congestion effects; so traffic flows equally well through a single hub as through multiple hubs. In actual practice, both in computer networks as well as other infrastructure networks, it is likely that congestion effects are important. Large congestion costs will create a pressure toward multiple paths and the creation of multiple hubs. A general analysis of optimal networks in the presence of significant congestion costs remains an open problem for future research.

4.3 Alternative timing of moves

In the benchmark model, we studied a sequential move game in which the Designer moves first, followed by the Adversary. In this section we show that by varying the order of moves, we can accommodate a variety of new applications.

Adversary moves first, followed by Designer: In some settings the Adversary is constrained to commit itself to a policy which is publicly observable. This may be due to political, legal or organizational reasons; a prominent instance is public policy with regard to crime. The state and the police may have to commit themselves to a course of action in advance.[22]

[22] See Baccara and Bar-Isaac (2008) for a detailed discussion of the reasons for such commitment.

So suppose the Adversary moves first and chooses to allocate his budget $a \in \mathbb{N}$ across N nodes. The Designer observes this allocation and then chooses a network. To fix ideas suppose that $\ell = 1$. The Designer can then isolate all the nodes which are being attacked and constitute a component with the remaining nodes. A maximum of a nodes can be targeted: so the minimal payoff of the Designer is $f(n-a)$. As $\ell = 1$, it follows that for any $\epsilon > 0$, there is a $\bar{n}$, such that $f(n'-a) \geq (1-\epsilon)f(n)$, for all $n' \geq \bar{n}$. In other words, the Designer can ensure himself an expected payoff which is arbitrarily close to what he could attain in the absence of any Adversary.

This timing of moves allows us to relate our paper to Baccara and Bar-Isaac (2008) more closely. In their paper, attack resources are continuous variables and they suppose that $a_i \in [0,1]$. Fix $a = 1$ and suppose that $f(n) = n^2$. Consider the case of symmetric allocation $a_i = 1/n$. The payoff from a connected network is then simply the probability that it is not successfully attacked, which is $(1-1/n)^n f(n)$. It is possible to verify that as n gets large, the connected network dominates networks with multiple equal components. On the other hand, Baccara and Bar-Isaac (2008) show that, for small a_i, a network with binary cells is optimal. Clearly, in our setting a collection of binary cells is very unattractive.

This discussion abstracts from defense allocation: a more complicated design would involve protecting a subset of the attacked nodes and possibly linking these nodes. But this is a second order problem, given the high payoffs already attained.

The Simultaneous Game: In some contexts it may be possible to conceal the network structure and defense allocations: leading examples are terrorist networks or civil and political protest movements. In addition to the government, the Adversary often includes intelligence agencies and secret services. These organizations (as their name suggests) are allowed (by law) to keep their actions covert. These considerations motivate a game in which the Designer and Adversary make all choices simultaneously.[23]

Our analysis shows that the Designer and the Adversary will seek to exploit simultaneity: both of them will mix their choices in a bid to gain strategic advantage. Moreover, this

[23] A referee has drawn our attention to a paper by Gueye and Marbukh (2012) in which players move simultaneously; we note that this paper appeared after the first preprint of our paper which dates from 2010 (see Goyal and Vigier, 2010). Gueye and Marbukh (2012) study a game in which the Designer picks a spanning tree from a network while an Adversary picks a link to delete. The aim of the Adversary is to maximize the loss to the Designer. They show the existence of mixed strategy equilibrium and their analysis highlights the role of link between-ness in understanding strategic behavior. The simultaneous game being considered in this section shares the same order of moves but there are crucial differences between the papers: we study optimal network defense and design and contagion plays a key role in our model. By contrast, in their work the Designer chooses only the spanning tree from a given network and there is no threat of contagion.

opportunity for disguising the network will enable the Designer to earn higher payoffs as compared to the benchmark sequential model analyzed in Section 3. Our finding with regard to mixing by the Adversary echoes recent research on the practical value of mixed strategies as highlighted in the recent work of Tambe (2011) with the Los Angeles Police Department. On the other hand, our finding on the mixing by the Designer suggests that flexible networks are attractive for criminal and terrorist organizations. This is consistent with the prominent role of flexible networks – that permit quick reconfiguration of connections – in modern insurgencies (Arquilla and Ronfeldt, (1996, 2001)).

A mixed strategy of the Designer is a probability distribution, σ, on the set of networks and defense allocations. The mixed strategy of the Adversary, ρ, is a probability distribution on the set of attack allocations.[24] The expected payoffs to $\mathcal{D}$ from strategy σ when $\mathcal{A}$ chooses ρ are:

$$\sum_{(g,\underline{d})\in\text{supp }\sigma;\underline{a}\in\text{supp }\rho} \sigma(g,\underline{d})\rho(\underline{a}) \sum_{g'\in G(g)} P(g'|\underline{a},\underline{d},g)\left[\sum_{C_k\in\mathcal{C}(g')} f(|C_k(g')|)\right] \tag{23}$$

Consider a network with large n and two hubs who are each linked to $(n-2)/2$ nodes. Suppose for simplicity that $a = d = 2$ and that Designer allocates 1 resource unit to each hub. Suppose the Adversary targets one peripheral node each attached to different hubs. Then the probability distribution of surviving nodes is $\bar{P}$: probability 1/2 for 0 surviving nodes, probability 1/4 for $(n-2)$ surviving nodes and probability 1/4 for $(n/2-1)$ surviving nodes. Figure 3 illustrates the dynamics and this distribution. Next suppose that the Adversary targets 2 peripheral nodes attached to the same hub node. Then the probability distribution of surviving nodes is given by $\tilde{P}$: probability 4/9 for 0 surviving nodes probability 3/9 for $(n-2)$ surviving nodes and probability 2/9 for $n/2-1)$ surviving nodes. Figure 5 illustrates this distribution.

It is easy to verify that $\tilde{P}$ first order stochastically dominates $\bar{P}$. Since network value f is increasing, it follows that $\mathcal{D}$ favors the latter attack strategy. The Designer can enforce his favored distribution by mixing across the allocation of peripheral nodes to hubs. In the face of this mixing, the Adversary is indifferent between mixing and not mixing his attack allocation. This advantage of the Designer in the simultaneous game has a general implication: in equilibrium he must earn (weakly) more in the simultaneous game as compared to the

[24] We abstract from the issue of routing of winning attacks by the Adversary here; for simplicity we assume that winner's resource captures neighboring undefended nodes but does not travel to other defended nodes.

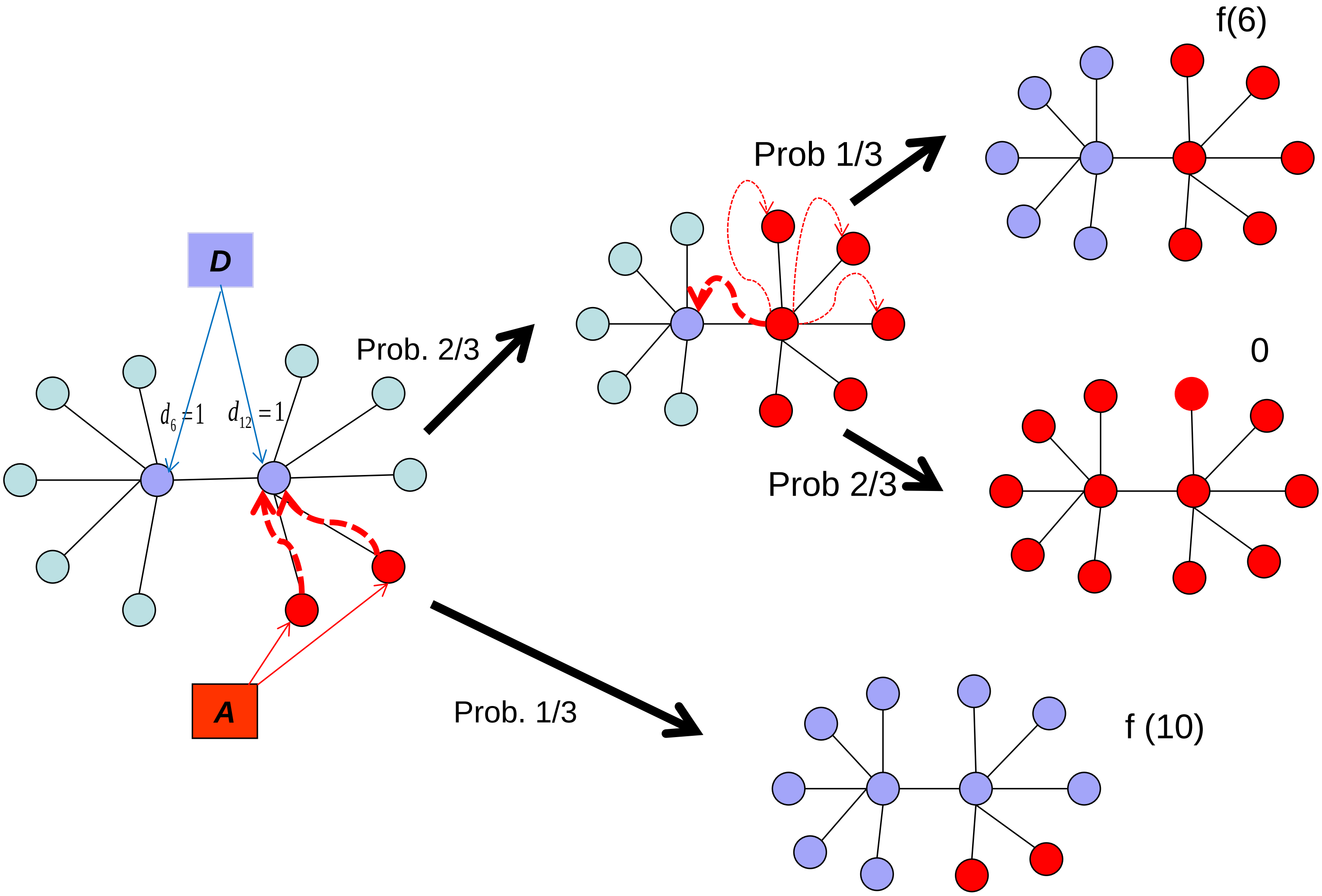


Figure 5: Mimic attack in core-periphery network: $n = 12$, $a = d = 4$.

benchmark sequential game analyzed in Section 3. This is because, given a CP-star, it is optimal for the Adversary to target a peripheral nodes. This means that there is a strategy which ensures the Designer expected payoffs (9) in the simultaneous game.

Consider next the case of 0 defense. The Designer chooses a network and the Adversary allocates a units of resources. Networks with equal size components provide a useful analytical benchmark. Suppose the Adversary allocates one unit of resource to a nodes chosen uniformly at random from the set of nodes. The probability that a component of size m survives is:

$$\begin{pmatrix} n-m \\ a \end{pmatrix} \Big/ \begin{pmatrix} n \\ a \end{pmatrix} = \frac{(n-m)!}{(n)!} \frac{(n-a)!}{(n-m-a)!} \tag{24}$$

The total payoffs of the Designer from a network with all components having equal size s is then:

$$\frac{n}{s} \frac{(n-s)!}{(n)!} \frac{(n-a)!}{(n-s-a)!} f(s) \tag{25}$$

For n large this becomes, approximately:

$$\frac{n}{s} n^{-s} (n-a)^s f(s) = \frac{n}{s} f(s) (1 - \frac{a}{n})^s \tag{26}$$

Abstracting from integer constraints, the optimal size, s^*, solves the following equation:

$$s^* \left[f'(s^*) + f(s^*) \ln(1 - \frac{a}{n}) \right] - f(s^*) = 0. \tag{27}$$

For this to be a maximum, the second order condition must be satisfied: $f''(s) + s f'(s) \ln(1 - a/n) + f(s) \ln(1 - a/n) < 0$. So there exists an equilibrium in which the Designer randomizes uniformly over all networks with equal size components s^*, while the attacker allocates one unit of resource to a nodes chosen uniformly at random.[25]

We conclude by noting that the expected payoffs to the Designer must be strictly larger in the simultaneous game as compared to the sequential game. Suppose the Designer chooses the size and number of components as in the sequential game but randomizes the allocation of the nodes to components. Then from the above construction we know that it is optimal for the Adversary to attack a nodes at random. But this mixing creates a positive probability that

[25] Observe that:

$$\frac{\mathrm{ds}^*}{\mathrm{da}} = \frac{s^* f(s^*) n^{-1} (1 - a/n)^{-1}}{f''(s^*) + s^* f'(s^*) \ln(1 - a/n) + f(s^*) \ln(1 - a/n)} \tag{28}$$

The numerator is positive while the denominator is negative (from the second order condition). So a growth in Adversary budget leads to a fall in component size.

two or more nodes are attacked in the same component. This is an entirely wasteful outcome for the Adversary and implies that the Designer has a feasible strategy which ensures strictly higher expected payoffs (than in the sequential game). This must also be true in equilibrium then.

We have brought out some interesting implications of simultaneity in moves and related them to applications. These observations should help in developing a characterization of optimal defended networks, a problem which we leave for future research.

Design followed by conflict: In some applications, the network is a physical object, e.g., transport or telecommunication infrastructure. Such a network takes time to build, is not easy to modify in the short run and is very visible. The resources of Designer and the Adversary may represent personnel or equipment. These considerations motivate a model in which the Designer sets up a network; this network is observed by the Adversary and the two players then simultaneously choose the allocation of resources on this network.

Our analysis proceeds by way of an example about core-periphery networks: it shows that the Adversary and Designer have an incentive to mimic their resource allocations. This mimic behavior allows us then to exploit the mean preserving spread arguments developed in Theorem 1 and 2 to demonstrate that the star is optimal. This result illustrates how the techniques we develop there are of more general interest.

Define a k-regular core-periphery network as a core-periphery network in which there are k core nodes and each core node is connected to $(n-k)/k$ peripheral nodes. Figure 6 illustrates core-periphery networks with $n = 12$.

Proposition 2 *Assume that (A.1) holds. Let $a, d > 0$, $a/d \in \mathbb{N}$ and $\alpha = 1$. Suppose $\ell = 1$. Then for large enough n, the star is optimal in the class of regular core-periphery networks.*

The proof is presented in the appendix. In the star network, given that $\ell = 1$ and n is large, there is a (Nash) equilibrium in which $\mathcal{D}$ allocates all resources to the central node and the Adversary allocates all resources to peripheral nodes. The key step in the proof shows that in case of multiple hubs, it is optimal for $\mathcal{D}$ to allocate equal resources to each hub and for the Adversary to adopt a mimic strategy. The optimality of the mimic strategy lies in the nature of the conflict technology: it exhibits decreasing returns. The best response to equal allocations by the opponent is a mimic allocation. Given this equilibrium it then follows from arguments in Theorem 1-2 that the probability distribution of surviving nodes in the star is a

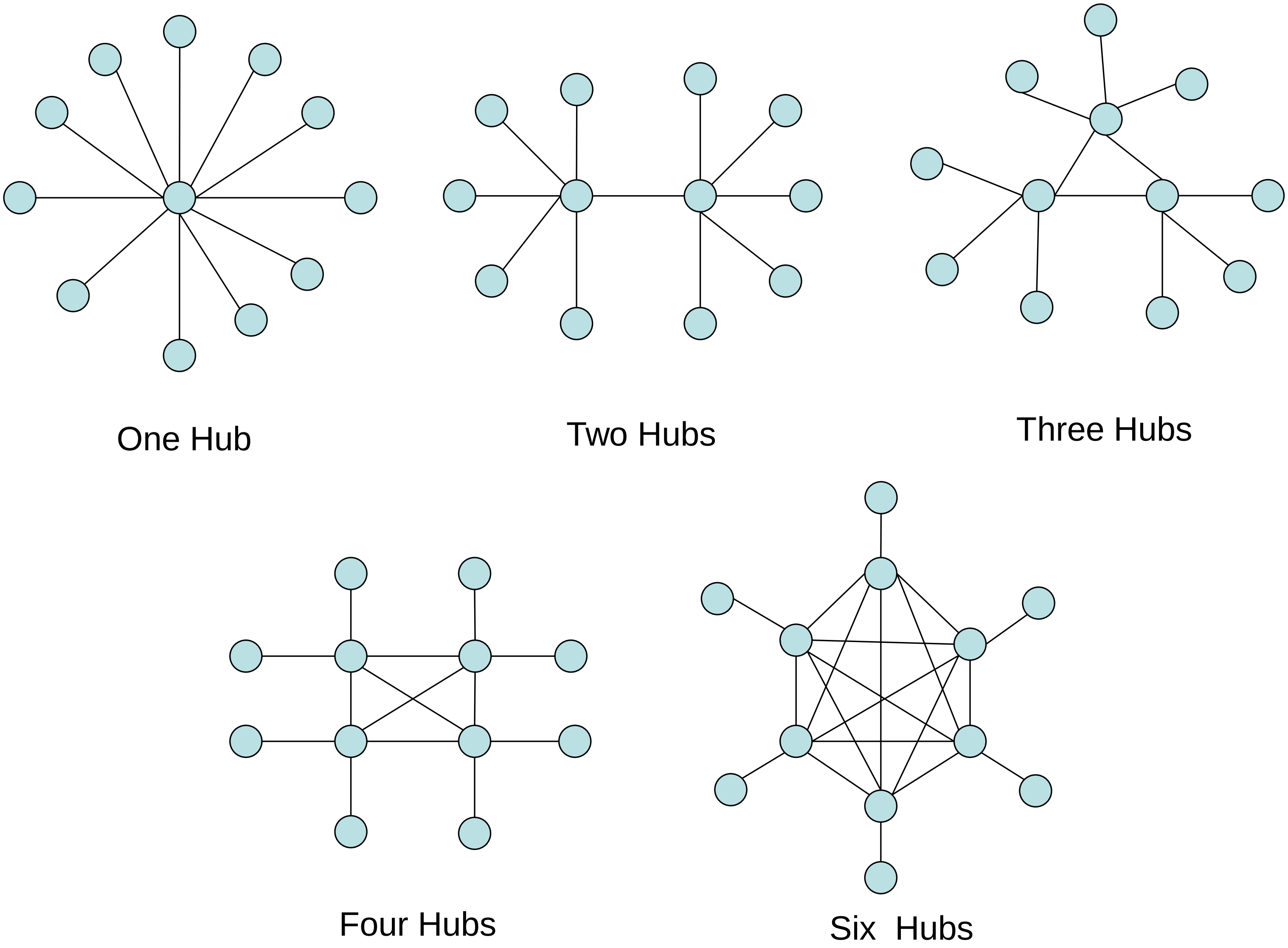


Figure 6: Regular core-periphery networks: $n = 12$.

mean preserving spread of the distribution obtained under a multiple core-periphery network. The result then follows from the assumption that f is convex.

This result suggests that the star with protected center is an attractive configuration for the Designer in settings beyond the benchmark model; a general characterization of optimal networks and defense remains an open problem.

5 Conclusion

Connections between individuals facilitate the exchange of goods, resources and information and create benefits. These connections may serve as a conduit for the spread of attacks and negative shocks as well. This paper asks: What is the optimal way to design and defend networks in the face of attacks?

We developed a model with a Designer and an Adversary. The Designer moves first and chooses a network and an allocation of defense resource. The Adversary then allocates attack resources on nodes and determines how successful attacks should navigate the network.

Our main result is that, in a wide variety of circumstances, a star network with all defense resources allocated to the central hub node is optimal for the Designer. The Adversary targets undefended peripheral nodes; upon capture of these nodes the resources mount a concerted attack on the center.

Our framework of network design, defense and attack offers a useful way to think about a number of questions relating to inter-connected social and economic systems that face threats. The baseline model was motivated by the application of computer security. We have outlined how, by varying the payoff function, the number of players, and the timing of their moves, we trace out an ensemble of models that can address questions in economic epidemiology, the organization of terrorist networks, financial networks, modern warfare, transport and telecommunications infrastructure, and criminal activity. We argued that our methods of analysis and our results are useful in the study of these other models.

6 Appendix

Example 1 *Communication networks (Goyal (1993); Bala and Goyal (2000a))*

Suppose every individual has one piece of information with value 1, to everyone. A link between X and Y allows X to access Y's information as well as information which Y may have accessed via his links with others. In a network g, X has access to all others in his component C_k; his payoff is $|C_k|$. As there are $|C_k|$ nodes in the component, the total payoff in component C_k is $|C_k|^2$. The aggregate social payoff in a network is the sum of the payoffs from the different components:

$$\sum_{C_k \in \mathcal{C}(g)} |C_k|^2. \tag{29}$$

The payoffs given in (29) satisfy (*A.1*). $\triangle$

Lemma 1 *Let* $\{I_1, .., I_k\}$*,* $k \geq 2$*, denote a set of i.i.d. Bernoulli random variables with mean in* $(0,1)$*. A realization of 1 for* I_i *yields a value* n_i*. If* $f : \mathbb{R} \to \mathbb{R}$ *is convex then*

$$\mathbb{E}[f\big(\sum_{t=1}^{k} n_t I_t\big)] < \mathbb{E}[f\big((\sum_{t=1}^{k} n_t) I_1\big)] \tag{30}$$

Proof. Note first that it is enough to show that $(n_1 + .. + n_k)I_1$ is a mean-preserving spread of $n_1 I_1 + .. + n_k I_k$ (see e.g. Rothschild and Stiglitz (1970)).

Let $\delta = \mathbb{P}(I_i = 1)$.

Suppose, without loss generality, that $n_1 \leq .. \leq n_k$. We prove the result by induction on k.

Suppose $k = 2$. Let F and G denote the cumulative distribution functions of $(n_1 + n_2)I_1$ and $n_1 I_1 + n_2 I_2$, respectively. Define $1 - \delta = \alpha$. Then

$$F(x) = \begin{cases} \alpha & \text{if } 0 \leq x < n \\ 1 & \text{if } x = n \end{cases} \tag{31}$$

and

$$G(x) = \begin{cases} \alpha^2 & \text{if } 0 \leq x < n_1 \\ \alpha & \text{if } n_1 \leq x < n_2 \\ 1 - \delta^2 & \text{if } n_2 \leq x < n \\ 1 & \text{if } x = n \end{cases} \tag{32}$$

So, using Theorem 1 in Rothschild and Stiglitz (1970), $(n_1 + n_2)I_1$ is a mean-preserving spread (MPS) of $n_1 I_1 + n_2 I_2$ if and only if

$$\alpha - \alpha^2 = 1 - \delta^2 - \alpha \tag{33}$$

or, substituting for δ

$$\alpha - \alpha^2 = 2\alpha - \alpha^2 - \alpha \tag{34}$$

So the result holds for $k = 2$. Next, suppose the result holds up to $k \geq 2$. We want to show that it also holds for $k + 1$.

Observe that that if Y is a MPS of X then, for any random variable Q independent of X and Y, $Y + Q$ is a MPS of $X + Q$.

But then setting $X = n_1 I_1 + n_2 I_2 + ... + n_k I_k$, $Y = (n_1 + n_2 ... + n_k) I_1$, $Q = n_{k+1} I_{k+1}$, using the result for $k = 2$ and the induction step, it follows that $(n_1 + n_2 + .. + n_{k+1}) I_1$ is a MPS of $n_1 I_1 + n_2 I_2 + n_3 I_3 .. + n_{k+1} I_{k+1}$.

■

Proof of Theorem2: By Theorem 1: $\overline{\Pi}^e(g^s, \underline{d}^s) > \overline{\Pi}^e(g, \underline{d})$ for any defended network not satisfying property P. So we are only left to compare the performance of the CP-star with that of a network satisfying property P.

Case 1: $l < 1$

We will show that for any (connected) defended network $(g, \underline{d})$ satisfying property P and for n large enough: $\overline{\Pi}^e(g, \underline{d}) < \frac{d^\gamma}{d^\gamma + a^\gamma} f(n - a)$.

Let $\epsilon' > 0$ such that $\ell' = \ell + \epsilon' < 1$. We can find n_0' such that $\frac{f(n-1)}{f(n)} < \ell'$, $\forall n \geq n_0'$. Then by induction $f(m) < (\ell')^{n-m} f(n)$, $\forall n \geq m \geq n_0'$.

Consider next a (connected) defended network $(g, \underline{d})$ satisfying property P. Let $i \in K$ such that $|O_i| \geq \frac{n-k}{k}$. Since $k \geq 2$, note that $d_i < d$. Suppose all attack resources are allocated in O_i, thereafter spreading to node i. Let Π^e denote the resulting expected network value. We have $\Pi^e \leq \frac{d_i^\gamma}{d_i^\gamma + a^\gamma} f(n - a) + \Gamma$, where $\Gamma \leq f(n - \frac{n-k}{k}) = f(1 + \frac{k-1}{k} n)$. Note from the remark above that for n large enough $f(1 + \frac{k-1}{k} n) < (\ell')^{\frac{n}{k} - 1} f(n)$. Thus, for n large enough, $\Gamma < (\ell')^{\frac{n}{k} - 1} f(n)$ and, finally:

$$\Pi^e < \frac{d_i^\gamma}{d_i^\gamma + a^\gamma} f(n - a) + (\ell')^{\frac{n}{k} - 1} f(n) \tag{35}$$

Now let $\epsilon'' > 0$ such that $\ell'' = l - \epsilon'' > 0$. We can find n_0'' such that $\frac{f(n-1)}{f(n)} > \ell''$, $\forall n \geq n_0''$. Then by induction $f(n - a) > (\ell'')^a f(n)$, $\forall n \geq n_0'' + a$. For n large enough (35) now yields

$$\Pi^e < \left(\frac{d_i^\gamma}{d_i^\gamma + a^\gamma} + (\ell')^{\frac{n}{k} - 1} (\ell'')^{-a} \right) f(n - a) \tag{36}$$

The first bracketed term in (36) is less than $\frac{d^\gamma}{d^\gamma + a^\gamma}$, since $d_i < d$, while the second term tends to 0 as n becomes large. We thus obtain $\Pi^e < \frac{d^\gamma}{d^\gamma + a^\gamma} f(n-a)$ for n large enough.

Case 2: $l = 1$

Let $(g, \underline{d})$ denote a defended network satisfying property P. Notice first that we can find n_0 such that $f(n-a) \geq (1-\epsilon) f(n)$ for all $n > n_0$. Consider attack such that $a_i = \frac{a}{d} d_i$, $\forall i \in K$. Observe that the assumption $a \geq d$ and $a/d \in \mathbb{N}$ ensure that such a strategy is feasible. Let Π^e denote the resulting expected network value. It follows from the proof of Theorem 1 that $\Pi^e < \frac{d^\gamma}{d^\gamma + a^\gamma} f(n)$. So for $n > n_0$: $\frac{d^\gamma}{d^\gamma + a^\gamma} f(n-a) \geq (1-\epsilon) \frac{d^\gamma}{d^\gamma + a^\gamma} f(n) > (1-\epsilon)\Pi^e$. But this implies $\frac{d^\gamma}{d^\gamma + a^\gamma} f(n-a) > (1-\epsilon)\overline{\Pi}^e(g, \underline{d})$.

■

Proof of Theorem 3: If $a \geq n$ then the Adversary can always eliminate all nodes, irrespective of the structure of the network. So, it follows that the Designer earns a payoffs of 0 irrespective of the network. Hence, any network can be sustained in equilibrium. Now let us take up the case of $a \leq n - 1$.

First, we note that there must be at least $a + 1$ components: if the number of components is fewer than $a + 1$, then $\mathcal{A}$ can set $a_i = 1$ for one node in each component and thereby ensure that $\mathcal{D}$ earns zero payoff. A network with $a + 1$ components on the other hand, guarantees $\mathcal{D}$ strictly positive payoff as at least one component survives any attack of $\mathcal{A}$ with some probability.

Second, we show that there are at least $a + 1$ maximum components. Suppose this is not the case and let component C_1 denote a maximum component. As part of his response, $\mathcal{A}$ must eliminate C_1. Next, form a new network g' from g in which C_1' is obtained from C_1 by isolating a single node, leaving the rest of the network unchanged. In g', either C_1' is maximal, or at most $a - 1$ components have size strictly greater than it. Hence, without loss of generality, we may assume that C_1' is eliminated as part of the best response by $\mathcal{A}$. But then $\mathcal{D}$ does strictly better with g' as compared to g, since by doing so she saves the node which has been isolated. This contradicts the hypothesis that g is optimal.

Third, we show that, at most, one component has size strictly smaller than the maximum size $\overline{s}$. Suppose we can find two such components. $\mathcal{D}$ can then take a node from the smaller of the two components and place it in the larger component. The larger component still remains (weakly) smaller than the maximal components, and it now follows from the convexity of $f_n(.)$ that payoffs to $\mathcal{D}$ are strictly increased by this move.

Fourth, at most one node is attacked in a component. Observe there are always more components than Adversary budget. So each component is assigned at most one unit of attack resource. If $\mathcal{A}$ attacks two nodes, there is positive probability of a state in which both nodes are eliminated and a corresponding state in which neither is eliminated: this is wasteful as elimination of one node is sufficient to remove the entire component.

Finally, observe that if $a \geq n/2$ then $\mathcal{A}$ can always eliminate every component with 2 or more nodes. Hence, the empty network is the unique equilibrium outcome. ■

Proof of Proposition 1: Consider a network g consisting of equal size components, and let m denote this size. Using arguments from Theorem 3 we find

$$\overline{\Pi}^e(g) = f(m)(\frac{n}{m} - a). \tag{37}$$

By simple algebra, (37) is maximized at $m = \frac{n(\beta-1)}{a\beta}$.

Next, consider a network g' with all but one component having maximum size m', and one component of size s, $0 < s < m'$. Let $b = \frac{n-s}{m'}$ denote the number of maximum components in g'. It follows from optimality of Adversary strategy that

$$\overline{\Pi}^e(g') = f(m')(b - a) + f(s). \tag{38}$$

Observe then that by convexity of f

$$\overline{\Pi}^e(g') < f(m')(b - a) + \frac{s}{m'}f(m'). \tag{39}$$

Substituting for b and simplifying, we then obtain

$$\overline{\Pi}^e(g') < f(m')(\frac{n}{m'} - a). \tag{40}$$

So, by the first step, a network with $\frac{\beta a}{\beta-1}$ equal size components dominates any network in which one component has less than maximum size. By Theorem 3, it then follows that a network with $\frac{\beta a}{\beta-1}$ equal size components is in fact optimal.

■

Proof of Proposition 2: We note that in the CP-star network, it is an equilibrium for for the Designer to allocate d to the central node and Adversary allocates a to a peripheral nodes. This follows from standard considerations, as in Theorem 1.

Fix number of hubs to $k = 2$. Then there is an equilibrium (in the set of pure strategies) in which Designer allocates $d/2$ to each core-node and Adversary allocates a nodes to peripheral nodes, an equal number corresponding to each hub. Label the core nodes 1 and 2.

Suppose the Adversary does choose the mimic strategy. Consider a defense allocation $d_1 = d/2 + x$, $d_2 = d/2 - x$. We show that it is optimal for the Designer to set $x = 0$.

Given that $\ell = 1$, it is optimal to allocate No resource to the peripheral nodes. Next, consider allocations on the two core nodes. Observe that there are four states of the world: both core nodes are defended, both are attacked successfully, and two states corresponding to the case where only one of them is attacked successfully. The payoff to the Designer from this strategy is given by:

$$f(\frac{n}{2} - 1)\left[\frac{2da}{(d + 2x + a)(d - 2x + a)}\right] + f(n - 2)\frac{d^2 - 4x^2}{(d + 2x + a)(d - 2x + a)} \tag{41}$$

Differentiating with respect to x, we get:

$$f(\frac{n}{2}-1)\left[\frac{-8x}{(d + 2x + a)^2(d - 2x + a)^2}\right]+f(n-2)\left[\frac{(-8x)((d + 2x + a)(d - 2x + a) - (d^2 - 4x^2))}{(d + 2x + a)^2(d - 2x + a)^2}\right]. \tag{42}$$

Simplifying, we get

$$\left[\frac{-8x}{(d + 2x + a)^2(d - 2x + a)^2}\right]\left[-f(\frac{n}{2} - 1) + f(n - 2)(a^2 + 2ad)\right]. \tag{43}$$

This expression in negative if

$$\frac{f(n - 2)}{f(n/2 - 1)} > \frac{1}{a^2 + 2ad}. \tag{44}$$

So the Designer allocates resources equally to the two core nodes if this inequality is satisfied. This inequality is satisfied for all functions $f(.)$ which satisfy $(A.1)$.

Now consider optimality of the Adversary's strategy in the face of an equal split of defense resources $d/2$ between the two hub nodes. The payoff to an attack strategy $a/2 + x, a/2 - x$ is given by:

$$f(\frac{n}{2} - 1)\left[\frac{2da}{(d + 2x + a)(d - 2x + a)}\right] + f(n - 2)\frac{d^2}{(d + 2x + a)(d - 2x + a)}. \tag{45}$$

It is easily checked that the denominator is falling in x. So it follows that the Designer's payoff is increasing in x and is minimized at $x = 0$. This completes the argument for the case of 2 core nodes.

This argument can be generalized to cover $k \geq 2$ nodes: fix equal allocations for the protected nodes for the Designer and Adversary some allocation of $k-2$ nodes. Now use the $k=2$ arguments to show show that the Adversary gains by equalizing the allocations on the remaining two nodes. Then repeat the exercise for the Designer.

■

7 References

1. Albert R, Jeong H, Barabási, A-L (2000), Error and attack tolerance of complex networks, *Nature*, 406: 378-82.

2. Allen, F. and D. Gale (2000), Financial Contagion, *Journal of Political Economy*, 108, 1, 1-33.

3. Anderson, R. (2008), *Security Engineering.* Second Edition. Wiley.

4. Arquilla, J. and D. Ronfeldt (1996), *The Advent of Netwar* (RAND: Santa Monica, CA).

5. Arquilla, J. and D. Ronfeldt (2001), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (RAND: Santa Monica, CA).

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

7. Bala, V. and S. Goyal. (2000a), A non-cooperative model of network formation, *Econometrica*, 68, 5, 1181-1229.

8. Bala, V. and Goyal, S. (2000b), An analysis of strategic reliability, *Review of Economic Design*, 5, 205-28.

9. Baye, M. (1998), *Recent Developments in the Theory of Contests: Advances in Applied Microeconomics.* JAI Press.

10. Bier, V., S. Oliveros and L. Samuelson (2006), Choosing what to Protect: Strategic Defensive Allocation against an Unknown Attacker, *Journal of Public Economic Theory*, 9, 1-25.

11. Cabrales, A., P. Gottardi and F. Vega-Redondo (2011), Risk-sharing and contagion in networks. Mimeo, EUI Florence.

12. Farrell, F. and G. Saloner (1986), Installed base and compatibility: Innovation, product preannouncements, and predation *American Economic Review*, 76, 940-955.

13. Garfinkel, M. and Skaperdas, S. (2012), *The Oxford Handbook of the Economics of Peace and Conflict.* Oxford University Press.

14. Garicano, L. (2000), Hierarchies and the Organization of Knowledge in Production, *Journal of Political Economy*, 108, 874-904.

15. Geoffard, P-Y., and Philipson, T. (1997), Disease eradication: private versus public vaccination, *American Economic Review*, 87(1):222-230.

16. Goyal, S. (1993), Sustainable communication networks, *Tinbergen Institute Discussion Paper, TI 93-250*, Rotterdam-Amsterdam.

17. Goyal, S. (2007), *Connections: an introduction to the economics of networks.* Princeton University Press.

18. Goyal, S. and A. Vigier (2010), Robust Networks. *mimeo* Cambridge University.

19. Garicano, L. (2000), Hierarchies and the Organization of Knowledge in Production, *Journal of Political Economy*, 108, 874-904.

20. Grotschel, M., C.L. Monma and M. Stoer (1995), Design of survivable communication networks, in M.O. Ball, TL. Magnanti, C.L. Monma and G.L. Nemhauser (eds) *Handbooks of Operations Research and management science: Network Models.* North Holland. Amsterdam, 617-672.

21. Gueye, A. and V. Marbukh (2012), Toward a network of communication network vulnerability to attack: a game theoretic approach. *mimeo*, National Institute of Standards and Technology.

22. Haldane, A (2009), Rethinking the financial network, *www.bankofengland.co.uk/publications.speeches/*

23. Hart, S. (2008), Discrete Colonel Blotto and General Lotto games, *International Journal of Game Theory*, 36, 3, 441-460.

24. Hirshleifer, D. (1995), Theorizing about conflict. *Mimeo*, UCLA.

25. Hong, S. (2008), Hacking-proofness and Stability in a Model of Information Security Networks, working paper.

26. Jackson, M. O. (2008), *Social and economic networks.* Princeton University Press. Princeton. New Jersey.

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

28. Katz, M. and C. Shapiro, (1985), Network Externalities, Competition and Compatibility, *American Economic Review*, 75, 3, 424-440.

29. Konrad, K. (2009), *Strategy and Dynamics in Contests.* Oxford University Press.

30. Kovenock, D. and B. Roberson (2012), Conflicts with multiple battle fields, in Garfinkel, M. and Skaperdas, S. (eds), *The Oxford Handbook of the Economics of Peace and Conflict.* Oxford University Press.

31. Kremer, M. (1996), Integrating Behavioral Choice into Epidemiological Models of AIDS, *The Quarterly Journal of Economics*, MIT Press, vol. 111(2), pages 549-73.

32. Moore, T., R. Clayton and R. Anderson (2009), The economics of online crime, *Journal of Economic Perspectives*, 23, 3, 3-20.

33. Myerson, R. (1977), Graphs and cooperation in games, *Mathematics of Operations Research*, 2, 225-229.

34. Nagaraja, S., Anderson, R. (2007) The topology of covert conflict, *Cambridge Computer Laboratory Technical Report 637.*

35. Newman, M. (2010), *Networks: an introduction.* Oxford University Press.

36. Pongou, R., and R. Serrano (2009) A Dynamic Theory of Fidelity Networks with an Application to the Spread of HIV/AIDS, *Working Paper 2009-02*, Department of Economics, Brown University.

37. Powell, R. (2009), Sequential non-zero sum Blotto: allocating defense resources prior to attack, *Games and Economic Behavior*, 67 2, 611-615.

38. Roberson, B. (2006), The Colonel Blotto Game, *Economic Theory*, 29, 1?24.

39. Rothschild, M. and J. E. Stiglitz (1970), Increasing risk: I. A definition, *Journal of Economic Theory*, 2, 3, 225-243.

40. Saia, J., A.Fiat, S.Gribble, A.R.Karlin, and S.Saroiu (2002), Dynamically fault-tolerant content addressable networks, in *Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS '02).*

41. Sandler, T. and K. Hartley (2007), *The Handbook of defense Economics, Volume 2: defense in a Globalized World*. Elsevier. Amsterdam.

42. Smith, C. J (2008), Preface to special issue on *Networks: Games, Interdiction, and human interaction problems on networks*, Volume 52, 3, 109-110.

43. Skaperdas, S. (1996), Contest success functions, *Economic Theory*, 7, 2, 283-290.

44. Staniford, S., V. Paxson and N. Weaver (2002), How to own the Internet in your spare time, *Proceedings of the 11th USENIX Security Symposium*, 149-167.

45. Suto, K., H. Nishiyama, X. Shen, N. Kato (2012), Designing P2P Networks Tolerant to Attacks and Faults Based on Bimodal Degree Distribution, *Journal of Communications* 7, 8, 587-595,

46. Tambe, M. (2011), *Security and Game Theory.* Cambridge University Press.

47. Tullock, G. (1980), Efficient rent seeking, *Towards a theory of the rent-seeking society*, edited by Buchanan, J., Tollison, R., and Tullock, G., Texas A&M University Press.

48. Van Zandt, T. (1999), Decentralized information processing in the theory of organizations, *Contemporary Economic Issues Volume 4: economic design and behavior*, edited by Murat Sertel. MacMillan Press. London.

49. Vega-Redondo, F. (2007), *Complex social networks.* Cambridge University Press. Cambridge, England.

50. Zakaria, F. (2008), The Rise of the Rest, *Newsweek*, May 12.