Individual Security, Contagion, and Network Design*

Diego A. Cerdeiro†
Marcin Dziubiński‡
Sanjeev Goyal§

Abstract

Individuals derive benefits from their connections, but these may expose them to external threats. Agents therefore invest in security to protect themselves. What are the network architectures that maximize collective welfare? We propose a model to explore the tension between connectivity and exposure to an external threat when security choices are decentralized. We find that both over-investment and under-investment in security are possible, and that optimal network architectures depend on the prevailing source of inefficiencies. Social welfare may be maximized in sparse connected networks when under-investment pressures are present, and fragmented networks when over-investment pressures prevail.

Keywords: Network design; Individual security; Inefficiencies; Networks
JEL: D85; D62; C72

1 Introduction

Individuals derive benefits from being connected to others. These connections may, at the same time, transmit external threats. Online networks reflects this tension: connectivity facilitates communication but is also used by hackers, hostile governments, firms, and 'botnet' herders to spread viruses and worms which compromise user privacy and jeopardize the functioning of the entire system.[1] [2]

*This paper is based on a chapter in Diego Cerdeiro's doctoral thesis submitted to Cambridge University in June 2014, titled "Individual Security and Network Design".

†International Monetary Fund. E-mail: dcerdeiro@imf.org
‡Institute of Informatics, Warsaw University. E-mail: m.dziubinski@mimuw.edu.pl
§Faculty of Economics & Christ's College, University of Cambridge. E-mail: sg472@cam.ac.uk

[1]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."

[2]Moore et al. (2009) estimate that in 2009, roughly 10 million computers were infected with malware designed to steal online credentials. The annual damages caused by malware are very large: in the US

A prime example of networks that are subject to malicious intelligent and contagious attacks are overlay (logical) networks built on top of the Internet. These networks form the backbone for international trade and global capital flows, enable digital currencies, support production chains and research and development, and facilitate content sharing. We mention three leading examples to illustrate this point. SWIFT, the leading global router of private proprietary financial messages, is estimated to be responsible for over $6 trillion (about 8% of world GDP) in transfers every day (see e.g. Scott and Zachariadis (2013)). Bitcoin, the world's first decentralized digital currency, does not have a central monetary authority and relies instead on a peer-to-peer network to verify and process all transactions ("How does Bitcoin work?" The Economist, April 11, 2013). GitHub provides a suite of tools used not only to store and share documents, but also to organize workflow and manage business processes in (mostly, but not only) software development companies, from open-source projects to private businesses, and large organizations, such as NASA.

These networks help to generate a value that increases with their size but at the same time are the target of malicious attacks by hackers, hostile governments, and criminal organizations. There are four distinctive features of cyber risks: the presence of an active, persistent and sometimes sophisticated adversary, the broad range of entry points, the potential to cause significant disruptions to the broader financial system, and the ability to propagate rapidly within a network of systems BIS-IOSCO (2016).[3]

Security of these networks depends crucially on individual investments in security. Individual security requires using the right software (e.g. anti-virus, firewall), the right equipment (e.g. reliable Internet routers), and following the right security procedures (e.g. making software updates and backups, ensuring passwords updates, staying up to date with existing threats). All this entails costs and often requires employing specialized workforce. Individual incentives to invest in protection depend on exposure in the network and will generally depart from what is collectively desirable.[4]

---

the annual costs of identity theft are estimated at 2.8 billion USD. These large costs have led to the emergence of a large software security sector. As an example, we note that Intel bought McAfee in 2010, for 7.68 billion USD (bbc.co.uk; 19 August 2010).

[3] A recent prominent case is the February 2016 infiltration into Bangladesh central bank's servers to route fake payment orders via SWIFT, in an attempted $1bn heist involving (through a chain of correspondent banks) accounts in Philippines, Sri Lanka, and at the Federal Reserve Bank of New York (The Wall Street Journal, 15 August 2016). In 2014 Bitcoin was targeted in 22% of financial malware attacks CoinDesk (2014), with the objective of forging Bitcoins, jeopardizing transactions or stealing users' money. This was done by reducing access of "healthy" users to other "healthy" users (over the Bitcoin network) and, by restricting access to actual transaction logs. Content sharing networks like GitHub or Dropbox are also susceptible to attacks by adversaries who aim to jeopardize their functionality.

[4] As an example of how much individual protection decisions may depart from first best, it has been reported that the bank through which SWIFT was infiltrated in February 2016 "did not have a firewall, which is designed to block unauthorized access requests [and] used second-hand routers, which had cost $10, to connect to global financial networks" (BBC News, 13 May 2016).

The topology of networks such as those described above can be influenced by an external designer. Like other types of organizations, financial institutions and related infrastructures (including systemically important messaging systems) have the ability to influence online interactions between employees, services providers, and vendors.[5] Similarly, the underlying communications and production networks of organizations will influence the topology of connections in the GitHub network. In the case of peer-to-peer networks (like that underlying BitCoin), connections can be influenced by protocols designed to enforce a particular topology among peers. Designers can potentially use their ability to influence connections in a way that minimizes protection externalities.

Motivated by these considerations, we consider the following setting. There are $(n+2)$ 'players'. A designer first chooses the network over the n nodes. Given this network, each of the n nodes (simultaneously) chooses whether to protect or not, where protection carries a fixed cost. Finally, an adversary chooses a node to attack. If the attacked node is protected, then all nodes survive the attack. If the attacked node is not protected, then this node and all nodes with a path to the attacked node through unprotected nodes are eliminated. Central to the problem is that nodes are assumed to derive benefits from their connectivity. More specifically, node's payoff is increasing in the size of its surviving component. Node's net payoffs are equal to its connectivity payoffs less the amount spent on protection. To study the optimal design problem from a collective welfare point of view, we assume that the designer is utilitarian: he seeks to maximize the sum of nodes' payoffs. The adversary is intelligent, purposefully choosing the attacked node so as to minimize connectivity-related payoffs.

We start by analyzing the optimal design of a network when the the planner chooses the defence profile as well as the network structure. If protection is sufficiently cheap, all nodes are protected and any connected network is optimal. For intermediate costs of protection, the designer achieves first best payoffs with minimal defence outlays by choosing a star network and only protecting its centre. If protection costs are high, the designer splits the network into equal size components and leaves all nodes unprotected.

A number of problems arise when defence decisions are decentralized. Firstly, a node does not internalize the benefits accruing to others from its own protection. Thus, it is possible that the center-protected star is optimal and, at the same time, it is a strictly dominant strategy for the hub *not* to protect. Under-protection arises naturally as a result of positive externalities. Secondly, nodes may have incentives to protect to divert the adversary's attack to other parts of the network. In this case, protection decisions involve negative externalities: there are ranges of costs of protection for which a centre protected star is the first best while, at the same time, full protection is the unique equilibrium of the star network. How can the designer induce some nodes to be eliminated

[5]Acknowledging this, BIS-IOSCO (2016) states e.g. that "[c]yber considerations should be integral part of the [financial market infrastructures'] arrangements for managing vendors and vendor products in the areas of contracts, performance, relationships and risk."

in equilibrium? We show that the over-protection problem is pervasive: any optimal connected network has full protection as unique equilibrium. Thus, the designer must disconnect the network and sacrifice some nodes (as well as network connectivity) if he is to avoid the over-protection problem.

Thirdly, nodes may have incentives to protect only if sufficiently many other nodes protect as well. Thus it is possible that a fully protected clique is optimal but, at the same time, equilibria exist where no nodes protect. Protection has features of threshold public good and under-protection results from the strategic complementarity of defence decisions. We show that this problem can be solved by choosing the right network architecture. The idea is to create a cascade of incentives to protect in the network. That is, the network should be such that at least one node has incentives to protect in it. Then, for every such node, there should exist subsequent nodes that have incentives to protect, if one of the former nodes protects, etc. A network where such a cascade leads to full protection needs to have a *critical node* which has incentives to protect even if no other node protects.

Lastly, a more subtle under-protection problem arises due to interplay between nodes only reaping off benefits from their components and the strategic nature of the attack. More specifically, if one of the eliminated nodes protected, the adversary would disconnect the network and leave the deviating node in too small a component to make protection profitable. This is caused by component balancedness of nodes' gross utilities: even though choosing protection increases the overall value of the network, it may decrease the value of node's own component. The network architecture which is sufficiently "tight" prevents this problem.

The analysis summarized thus far focuses on networks that achieve maximum equilibrium welfare under *some* equilibrium. In general, however, some of these networks may feature multiple equilibria, each achieving vastly different welfare levels. How can the designer tackle potential coordination problems? To illustrate the issue at hand, suppose that the costs of protection are such that maximum equilibrium welfare is achieved via full protection on a connected network. The network where nodes are arranged on a cycle has a full protection equilibrium. However, there is another equilibrium on this network where no node protects and the adversary brings down the entire network. We provide a partial characterization of networks that induce full protection as the unique equilibrium. Such networks are *sparse* in the following sense: they must feature a node that can block the adversary's attack, thus saving a large part of the network.

The results summarized above show how to manipulate individual incentives through the network structure to maximize welfare. Our third result moves to the welfare implications of decentralization. We show that network design goes a long way in limiting the costs of decentralization: by appropriately choosing the network, the designer can put a limit on the potential negative effects of decentralization. It is important to note that our main results are robust to changes of the model. In the appendix we consider an extension where investments in protection are continuous. The main result there is that

it is still possible to mitigate the under-protection problem and enforce full protection by choosing a network which creates a cascade of incentives to protect. Like in the case of our main model, such networks must have a critical node that can block the adversary's attack and save sufficiently large fragment of the network. In a follow up that builds on our paper, Goyal et al. (2016) consider a model where both the protection decisions and the linking decisions are decentralized. They show that there is a pressure to create critical nodes, although the inefficiencies due to decentralization may become unbounded. They also show that there exist non-trivial equilibrium networks with very low cost of decentralization.

Our paper is a contribution to the theory of security in interconnected systems. The central tension here is that connections confer value but also bring with them the the threat of negative contagion. We study the extent to which appropriate network design can help resolve this tension. Earlier research on decentralized protection in environments has assumed that there is no value in being connected, i.e. nodes only care about their own survival (Kunreuther and Heal (2003),Varian (2004), Aspnes et al. (2006), Lelarge and Bolot (2008a,b), Acemoglu et al. (2016)). In particular, Aspnes et al. (2006) study a setting on a fixed network when nodes only care about their own survival, attack is random, protection is perfect and contagion is perfect: infection spreads to unprotected nodes with probability 1. The focus is on computing the Nash equilibria of the game. They show that the problem is NP-hard and provide approximation algorithms for finding the equilibria. Similarly, Lelarge and Bolot (2008a,b) use techniques based on local mean field analysis to study the problem of incentives and externalities in network security on random networks. More recently, Acemoglu et al. (2016) consider individual investments in a model of network attacks. Their focus is on the strategic structure of the security decisions across individuals and how the network shapes the choices under random versus targeted attacks. Our paper introduces two innovations: one, it assumes that there is a value to more connections, and two, it studies the optimal design of networks. In particular, the assumption that connectivity is valuable, helps us uncover a wealth of effects that influence the possible equilibrium outcomes.

Our paper builds on an earlier paper by Goyal and Vigier (2014): they consider the problem of security in a settings where security and network design are both chosen by a single planner. The results in the present paper highlight the large effects of decentralized defence for optimal design. In Goyal and Vigier (2014) the optimal design is a star network and optimal allocation of resources is exclusively on the central node. By contrast, when individual nodes choose security, the optimal design has to address problems of too much as well as too little protection. Such inefficiencies may lead the designer to disconnect the network and sacrifice some nodes (when over-protection pressures prevail), or create sparse connected networks to stave off coordination problems.[6]

[6]Baccara and Bar-Isaac (2008) study the optimal cross-holding of incriminating information in a

The rest of the paper is organized as follows. Section 2 presents the model. Section 3 presents the results and Section 4 provides discussion and highlights the key messages of the paper. We conclude in Section 5. Proofs not given in the main text are provided in the Appendix. In the second part of the Appendix, we consider an extension of the model where security investments are continuous.

2 The model

Players There are $(n+2)$ players: the designer (D), the nodes (V), and the adversary (A).

The timing There are three rounds of the game:

1. D chooses a network $G \in \mathcal{G}(V)$, where $\mathcal{G}(V)$ is the set of all undirected networks over V.

2. Nodes from V observe G and choose, simultaneously and independently, whether to protect (1) or not (0). This determines the set of protected nodes Δ.

3. A observes the protected network (G, Δ) and chooses a lottery over the set of nodes, $\xi \in \mathcal{L}(V)$, a *mixed attack strategy*. A realization of this lottery is the node to infect, $i \in V$. The infection spreads and eliminates all the unprotected nodes reachable from i in G via a path that does not contain a protected node from Δ. This leads to the residual network obtained from G by removing all the infected nodes. An attack strategy ξ infecting one node with probability 1 is called a *pure attack strategy*.

Payoffs Payoffs to the players are based on the residual network and costs of defence.

The returns from a network are measured by a *network value function*

$$\Phi : \bigcup_{U \subseteq V} \mathcal{G}(U) \to \mathbb{R}$$

that assigns numerical value to each of the networks that can be formed over a subset U of nodes from V.

A *component* of network G is a maximal set of nodes $C \subseteq V$ such that for all $i, j \in C$, $i \neq j$, i and j are connected (directly or indirectly) in G. The set of components of G is denoted by $\mathcal{C}(G)$. Given network G and node $i \in V$, $C_i(G)$ denotes the component $C \in \mathcal{C}(G)$ such that $i \in C$. Network G is *connected* if $|\mathcal{C}(G)| = 1$.

criminal organization, exploring the tradeoff between cooperation enforcement and potential detection by an external authority. However, no protection technology is available to agents; the choice of security is central to our study.

We consider the following family of network value functions:

$$\Phi(G) = \sum_{C \in \mathcal{C}(G)} f(|C|),$$

where $f : \mathbb{R} \to \mathbb{R}$ is increasing, strictly convex and $f(0) = 0$. In other words, the value of a connected network is an increasing and strictly convex function of its size. The value of a disconnected network is the sum of values of its components. This form of network value functions is in line with Metcalfe's law, where the value of a connected network over x nodes is equal to x^2, as well as with Reed's law, where the value of a connected network is of exponential order with respect to the number of nodes (e.g. $2^x - 1$). It reflects the idea that each node derives additional utility from every node it can reach in the network.

The *gross payoff* to node $j \in V$ in a network G is equal to $f(|C_j(G)|)/|C_j(G)|$, i.e. each node gets the equal share of the value of its component. Given the assumptions on f, this creates a tension between being connected and being exposed to contagious risk. The net payoff of a node is equal to the gross payoff minus protection spending. A removed node gets payoff 0. Defence has costs $c \in \mathbb{R}_{++}$.

Before defining payoff to a node from a given network, defence and attack, we need to define the residual network formally. A *network* is modelled by an undirected graph $G = (V, E)$, where V is a finite set of nodes, $|V| = n \geq 0$, and $E \subseteq \{ij : i, j \in V\}$ is a set of undirected edges. The set of all networks over the set of nodes V is denoted by $\mathcal{G}(V)$. A *path in* G *between nodes* $i, j \in V$ is a sequence of nodes $i_0, \ldots, i_m \in V$ such that $i = i_0$, $j = i_m$, $m \geq 2$, and $i_{k-1}i_k \in E$ for all $k = 1, \ldots, m$. Node j is *reachable* from node i in G if $i = j$ or there is a path between them in G.

Given network $G = (V, E)$ and a set of nodes $Z \subseteq V$, let $G - Z$ denote the network obtained from G by removing the nodes from Z and their connections from G. Thus $G - Z = (V \setminus Z, E[V \setminus Z])$, where $E[V \setminus Z] = \{ij \in E : i, j \in V \setminus Z\}$. Notice that infecting node $i \in V$ in network G with protected nodes Δ, the adversary removes the set of nodes $C_i(G - \Delta)$ from G. Hence the residual network after such an attack is $G - C_i(G - \Delta)$. Node j's payoff in network G with defended nodes, Δ, and infected node, i, is then equal to:

$$u^j(G, \Delta, i) = \begin{cases} \frac{f(|C_j(G - C_i(G-\Delta))|)}{|C_j(G - C_i(G-\Delta))|} - c, & \text{if } j \in \Delta \\ 0, & \text{if } j \in C_i(G - \Delta) \setminus \Delta \\ \frac{f(|C_j(G - C_i(G-\Delta))|)}{|C_j(G - C_i(G-\Delta))|}, & \text{otherwise.} \end{cases} \tag{1}$$

The expected net payoff of node j in network G with defended nodes, Δ, and mixed attack, ξ, is equal to:

$$U^j(G, \Delta, \xi) = \sum_{i \in V} \xi_i u^j(G, \Delta, i). \tag{2}$$

The designer aims to maximize social welfare, i.e. the sum of nodes' utilities, which is equal to the value of the residual network minus total costs of defence. Formally, the

designer's payoff from network G under defence Δ and infected node i is equal to:

$$u^{\mathsf{D}}(G,\Delta,i) = W(G,\Delta,i) = \sum_{j\in V} u^j(G,\Delta,i) = \left(\sum_{C\in\mathcal{C}(G-C_i(G-\Delta))} f(|C|)\right) - |\Delta|c. \tag{3}$$

The expected payoff of the designer from network G under defence Δ and mixed attack ξ is:

$$U^{\mathsf{D}}(G,\Delta,\xi) = \sum_{i\in V} \xi_i u^{\mathsf{D}}(G,\Delta,i). \tag{4}$$

The adversary is intelligent and aims to minimize gross welfare, i.e. the sum of nodes' gross payoffs, equal to the value of the residual network. Given G, Δ and i, payoff to the adversary is:

$$u^{\mathsf{A}}(G,\Delta,i) = -\sum_{C\in\mathcal{C}(G-C_i(G-\Delta))} f(|C|). \tag{5}$$

and the expected payoff to the adversary when mixed attack ξ is used is:

$$U^{\mathsf{A}}(G,\Delta,\xi) = \sum_{i\in V} \xi_v u^{\mathsf{A}}(G,\Delta,i). \tag{6}$$

To summarize, the set of players is $P = V \cup \{\mathsf{D},\mathsf{A}\}$. The set of strategies of player D is $S^{\mathsf{D}} = \mathcal{G}(V)$. A strategy of each node j is a function $\delta_j : \mathcal{G}(V) \to \{0,1\}$ which, given network $G \in \mathcal{G}(V)$, provides the defence decision $\delta_j(G)$ of the node. The individual strategies of the nodes determine a function $\Delta : \mathcal{G}(V) \to 2^V$ providing, given a network $G \in \mathcal{G}(V)$, the set of defended nodes $\Delta(G) = \{j \in V : \delta_j(G) = 1\}$. The set of strategies of each node $j \in V$ is $S^j = 2^{\mathcal{G}(V)}$.[7]

A strategy of player A is a function $\xi : \mathcal{G}(V) \times 2^V \to \mathcal{L}(V)$ which, given network $G \in \mathcal{G}(V)$ and set of protected nodes $\Delta \subseteq V$, provides the lottery over the set of nodes, $\xi(G,\Delta)$, determining the probability of infection for each node. The set of strategies of player A is $S^{\mathsf{A}} = \mathcal{L}(V)^{\mathcal{G}(V)\times 2^V}$.

Players D and A are expected utility maximisers. In the case of nodes we make an additional tie breaking assumption that in the case of expected utilities being equal, each node prefers to choose defence and stay uninfected. Similarly, we assume that in the case of expected utilities being equal, D prefers strategy profiles where less network value is lost. We are interested in subgame perfect equilibria of game Γ, called equilibria, for short. Pure strategy equilibria are equilibria in which the adversary uses a pure attack strategy in every subgame.

Throughout the paper we will also refer to the subgame ensuing after network G is chosen. We will denote this subgame by $\Gamma(G)$. We will abuse the notation by using the

[7] We will represent the strategies of the nodes with the function providing the set of defended nodes, for short.

same letters to denote the strategies in $\Gamma(G)$ and in Γ. The set of strategies of each node $i \in V$ in game $\Gamma(G)$ is $\{0,1\}$ and we will identify each strategy profile $(\delta_i)_{i\in V}$ of the nodes with the set of protected nodes $\Delta = \{i \in V : \delta_i = 1\}$. The set of strategies of A in $\Gamma(G)$ is $\mathcal{L}(V)^{2^V}$.

2.1 Remarks on the model

As far as we know, our work is the first attempt to study how inefficiencies due to defence decentralization can be mitigated by network design. To make progress, we make a number of simplifying assumptions that we now discuss. Firstly, we assume that protection decisions are binary and protection is perfect. This assumption is justified in scenarios where following good security practices provides full or nearly full protection against (most of) the attacks. The nodes then either follow the good practices or they do not (e.g. protect insufficiently well) in which case they are (nearly) certain to get infected in case of the attacks. It is possible that reliability of protection depends on the investment level or that protection is perfect, but users randomize when using it. We address this extension in the Appendix. Secondly, we assume that connection between nodes are chosen in a centralized way, by the designer. This is justifiable in some applications (like the examples mentioned in introduction), where the central planner can either directly decide on the connection between the nodes, or he can affect it indirectly by designing protocols that ensure desirable properties of the network topology. In other applications, however, the network is chosen in a decentralized way, by the nodes (examples include the network of e-mail contacts, Facebook contact, or Skype contacts). This extension is studied by Goyal et al. (2016) in a follow up that builds on our paper. Thirdly, we assume that all connections are equally important to every node and that all nodes contribute in the same way to the overall value of the network. This is a common assumption in the literature, but it is possible that some nodes (like servers in computer network or workers having different functions in organizations) are more important than others. Different values of nodes would affect the first best design, as there are more incentives to protect such nodes and, if protection is too costly, the network would be split in such a way that values of components are equalized. In particular, very high value nodes would be put in different components. Individual incentives of nodes to protect themselves would also be affected, because more important nodes contribute more to the value of a components and so choosing protection they are able to secure more value of the network. Thus to create a cascade of incentives to protect, in order to avoid underprotection, the designer should either make one of very high value nodes a critical node, or distribute the high value nodes appropriately across the subnetworks connected to the critical node. A more general intuition is that having more important nodes should (almost by definition) reduce inefficiencies, as the bigger a node is the more s/he internalizes externalities. In the limit, if instead of n nodes we have a single node with value $f(n)$, then inefficiencies van-

ish. In this sense, the model with equal values of nodes should bring out in the sharpest possible way the potential inefficiencies, which in turn makes the result on the bounds of decentralization costs even starker. Fourthly, we restrict attention to scenarios where the adversary attacks only one node in the network. This can be justified in situations where a coordinated attack on many nodes is very costly or hard to conduct (the attack on Bangladesh central bank using SWIFT network is an example), but in general coordinated attacks on several nodes in the network are possible. Lastly, the spread of infection in the network may decay stochastically so that nodes which are further from the initially infected node are less likely to get infected. Arguably, perfect spread of infection is a good abstraction of scenarios where infection spreading to subsequent nodes is very likely. This is the case for computer networks and was assumed by other authors as well (e.g. Aspnes et al. (2006)).

3 The analysis

We start the analysis with characterizing the optimal choice if the network and nodes' protection both are chosen by the designer. We then move to comparing thus obtained payoffs to the payoffs that can be obtained in the equilibria of the game.

Main difficulties in the analysis follow from a generality of the framework. We allow for a very general class of component value functions and do not restrict the considered topologies of networks. Technical results providing key properties of convex functions are Observations 1–3 and Lemma 6. These results might be useful for other problems involving the analysis of convex functions, as studied in this paper. Main difficulties when network topologies are concerned lied in providing the required constructions of graphs, particularly π-windmill graphs, as used in Proposition 3 for generating the cascade of incentives to protect and the network in Figure 1, used to demonstrate under-protection due to miscoordination.

3.1 First best

Before we state the proposition characterizing the first best, we need the following four quantities. Given $n \in \mathbb{N}$, let

$$Q^*(n) = \arg\max_{q \in \{1,\ldots,\lfloor \frac{n}{2} \rfloor\}} \left\lfloor \frac{n}{q} \right\rfloor f(q) + f(n \bmod q). \tag{7}$$

To understand the quantity $Q^*(n)$ consider the following problem. Find the optimal size of component, $q \in \{1, \ldots, \lfloor n/2 \rfloor\}$, such that partitioning the network over n nodes into components of size q with, possibly, one additional smaller component (in the case where q does not divide n) maximises the sum of values of all the components. Given $q \in \{1, \ldots, \lfloor n/2 \rfloor\}$ and n, there are $\lfloor n/q \rfloor$ components of size q and, possibly, one additional

component of size $n \bmod q$. Since the size of larger components varies from 1 to $\lfloor n/2 \rfloor$, the number of components varies from 2 (or 3 in the case of odd n) to n.

Moreover, let

$$c_1(n) = \frac{f(n) - f(n-1)}{n-1} \tag{8}$$

$$c_2(n) = c_2(n,q) = \frac{f(n) - \left(\left\lfloor \frac{n}{q} \right\rfloor - 1\right) f(q) - f(n \bmod q)}{n} \tag{9}$$

$$c_3(n) = c_3(n,q) = f(n-1) - \left(\left\lfloor \frac{n}{q} \right\rfloor - 1\right) f(q) - f(n \bmod q) \tag{10}$$

where $q \in Q^*(n)$.

Notice that for all $q \in \mathbb{N}$,

$$(n-1)(c_2(n,q) - c_1(n)) = c_3(n,q) - c_2(n,q) \tag{11}$$

and, consequently, we either have $c_1(n) \leq c_2(n) \leq c_3(n)$ or $c_3(n) \leq c_2(n) \leq c_1(n)$.

Quantity $c_1(n)$ is a threshold value for costs of protection below which fully protected connected network is better to D than centrally protected star. Quantity $c_2(n)$ is a threshold value for costs of protection below which fully protected connected network is better to D than optimal disconnected network without protection. Finally, $c_3(n)$ is a threshold value for costs of protection below which centrally protected star is better to D than optimal disconnected network without protection.

Proposition 1. *Let $c > 0$, $q \in Q^*(n)$, and let (G, Δ) be a first best protected network. Then*

1. *G is connected and $\Delta = V$, if $0 < c < \min(c_1(n), c_2(n))$.*
2. *G is a star and $\Delta = \{i\}$, where i is the centre of the star, if $c_1(n) < c < c_3(n)$.*
3. *G has $\lfloor \frac{n}{q} \rfloor$ components of size q and one component of size $n \bmod q$ (if $n \bmod q > 0$), and $\Delta = \varnothing$, if $\max(c_2(n), c_3(n)) < c$.*

The responses of the adversary to the first best protected networks are as follows: (1) A chooses any lottery $\xi \in \mathcal{L}(V)$, (2) A chooses any lottery over the set of spokes, $\xi \in \mathcal{L}(V \setminus \{i\})$, (3) A chooses any lottery over the set of nodes in maximal components, $\xi \in \mathcal{L}(\{i \in V : C_i(G) = q\})$.

Note that if f is such that for all integer $x \geq 2$,

$$f\left(\left\lfloor \frac{3x}{2} \right\rfloor\right) + f(x \bmod 2) > 2f(x), \tag{12}$$

then $Q^*(n) = \{\lfloor \frac{n}{2} \rfloor\}$ for any integer $n \geq 1$. In other words, the network in (1) consists of two components of size $\lfloor \frac{n}{2} \rfloor$ and, possibly, one of size 1. Condition (12) is satisfied,

for example, by $f(x) = x^a$ with $a > 2$, and $f(x) = a^x - 1$ for $a \geq 2$. In the case of $f(x) = x^2$, $Q^*(n) = \{3\}$ for any integer $n \notin \{9, 15\}$. In a sense, value functions that satisfy (12) entail sufficiently high connectivity payoffs so that a central planner is willing to compromise (roughly) half of the nodes for the remaining half to survive connected.

According to Proposition 1, when defence is sufficiently cheap, all nodes should be protected, and the maximum gross payoff of D, $f(n)$, is achieved through any connected network. For intermediate values of c, protecting all the nodes is too costly but the damage caused by the adversary can be brought to a minimum with a centre-protected star. When the costs of protection are large, no node is protected and a disconnected network is optimal.

Note that if f is such that marginal benefits from adding new nodes to the network grow very fast, it is possible that $c_1(n) > c_3(n)$,[8] in which case first best involves either full protection (when $c < c_2(n)$) or no protection (when $c > c_2(n)$).

3.2 Decentralized defence

To illustrate the inefficiencies that arise if protection decisions are decentralized, suppose that network $G \in \mathcal{G}(V)$ is a clique. Let $f(x) = x^2$ and $1 < c < c_1(n) = \frac{2n-1}{n-1}$. In this range of costs it is optimal to protect all the nodes. However, when the decision costs are decentralized, there are two equilibrium outcomes possible. One, where all nodes protect (attaining the social optimum), and another, where no node protects. The latter is due to the fact that it is not profitable for a node to protect if no other node survives in the network. Protection in this setting has features of threshold public goods: it is only profitable for the nodes to protect if there are sufficiently many other nodes protecting in the network. This is the under-protection problem due to strategic complementarities in protection.

Another source of inefficiencies are positive and negative externalities affecting the protection decisions. Suppose that $G \in \mathcal{G}(V)$ is a star. Let $f(x) = x^2$, $n - 1 < c < c_3(n) = \frac{n^2}{4} + n \bmod 2$, and $n \geq 16$. In this range of costs it is optimal to protect the centre of the star. However, in any equilibrium for this range of costs no node protects. This is the usual under-protection due to positive externalities: the centre of the star fails to internalize benefits accruing to others from its own protection and does not protect. On the other hand, suppose that $c_1(n) < c < n$. In this case it is optimal to protect the centre of the star, however, there are equilibria where all nodes protect. This is the over-protection problem due to negative externalities: nodes may have incentives to protect to divert the adversary's attack to other parts of the network.

Lastly, let us consider the network in Figure 1. Let $f(x) = x^4$ and $\frac{f(11)}{11} = 1,331 < c < c_1(23) \approx 2,072$. Since $c < c_1(23)$, full protection is the first best defence. However, a strategy profile where only nodes a and b protect, and the adversary attacks the nodes

[8] This is true for functions that grow faster than $x!$, e.g. $f(x) = (x+1)^x - 1$.

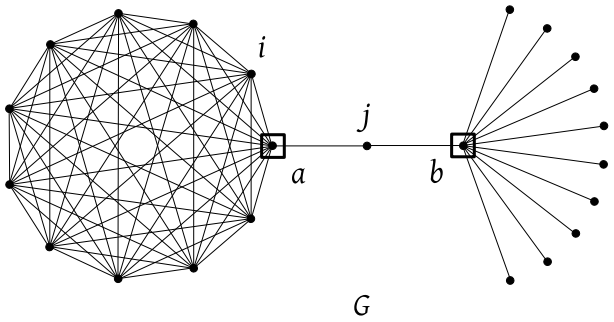

Figure 1: Network G, over 23 nodes, that features an equilibrium where only two nodes protect, while full protection is the first best.

to the left of a is an equilibrium. None of the protected nodes has incentives to deviate, because any of them would get eliminated by the adversary obtaining payoff 0 instead of $\frac{f(13)}{13} - c = 2,197 - c > 0$. None of the eliminated nodes has incentive to protect either. This is because if any one of them protected, say node i, then the adversary would deviate to attacking j, reducing the network value to $2 \cdot f(11) = 29,282$ instead of $f(14) = 38,416$. In effect, payoff to i is $\frac{f(11)}{11} - c < 0$. Thus i does not have an incentive to deviate. Under-protection here results from the fact that gross utilities of the nodes are component balanced (every node derives benefits from own component only). Notice that i's decision to protect has both positive and negative externalities: payoffs to all its unprotected neighbours (that would otherwise be eliminated) increase and payoffs to all the other nodes decrease.

Our interest is in analysing how the social welfare maximising designer can mitigate the decentralization problems by choosing the right topology of the network. We start by noting that for any network G and costs of protection c, there exists a pure strategy equilibrium in the subgame $\Gamma(G)$.

Lemma 1. *For any network $G \in \mathcal{G}(V)$ and costs of protection $c > 0$, $\Gamma(G)$ has a pure strategy equilibrium. Moreover, for any costs of protection $c > 0$, Γ has a pure strategy equilibrium.*

Proof. Let ξ be a strategy of A in $\Gamma(G)$ such that for all $\Delta \subseteq V$, $\xi(\Delta)$ is a best response to Δ and ξ is a pure attack strategy, infecting node $x(\Delta)$ with probability 1. Clearly such a strategy exists. network G and strategy ξ define game $\Gamma(G, x)$ with set of players V such that, given defence Δ induced by a strategy profile of the nodes $(\delta_1, \ldots, \delta_n)$, the utility of player i is $\tilde{u}^i(\Delta) = U^i(G, \Delta, x(\Delta))$.

We will show that $\Gamma(G, x)$ has a Nash equilibrium. To show that we will construct a set of defended nodes, Δ^*, such that the corresponding strategy profile of the nodes is Nash equilibrium of $\Gamma(G, x)$.

There are two cases possible. First, suppose that for all components $C \in \mathcal{C}(G)$,

$\frac{f(|C|)}{|C|} \geq c$. In this case $\Delta^* = V$ is an equilibrium protection of $\Gamma(G, x)$, as any node that would deviate and drop protection, would obtain payoff $0 \leq \frac{f(|C|)}{|C|} - c$.

Second, suppose that there exists $C \in \mathcal{C}(G)$ such that $\frac{f(|C|)}{|C|} < c$. Let $\mathcal{A}(G \mid c) = \{C \in \mathcal{C}(G) : f(|C|)/|C| < c\}$ be the set of all such components. We construct Δ^* using the following algorithm.

- $\Delta^* := V \setminus \bigcup \mathcal{A}(G \mid c)$, i.e. Δ^* protects all the nodes in components where protection yields non-negative payoffs to the protected nodes; For any $C \in \mathcal{A}(G \mid c)$, $C \cap \Delta^* = \varnothing$; note that $x(\Delta^*)$ removes $C \in \mathcal{A}(G \mid c)$ of maximal size.
- While there exists $i \in \Delta^*$ such that $x(\Delta^* \setminus \{i\}) \in \mathcal{A}(G \mid c)$ do
  - $\Delta^* := \Delta^* \setminus \{i\}$

Clearly the algorithm stops, as in every step at least one node is removed from Δ^*. Moreover, $x(\Delta^*)$ removes $C \in \mathcal{A}(G \mid c)$ of maximal size and no node in C has incentive to protect. The algorithm ensures that no node in Δ^* has incentive to drop protection either. Hence Δ^* is an equilibrium protection of $\Gamma(G, x)$ and (Δ^*, x) is an equilibrium of $\Gamma(G)$.

For pure strategy equilibrium existence in game Γ, let (G, Δ, ξ) be a strategy profile such that for any $G' \in \mathcal{G}(V)$, $(\Delta(G'), \xi(G'))$ is a welfare maximising equilibrium of $\Gamma(G')$ and $G \in \arg\max_{G' \in \mathcal{G}(V)}(\Delta(G'), \xi(G', \Delta(G'))$. Clearly (G, Δ, ξ) is a subgame perfect equilibrium of Γ. □

Given network $G \in \mathcal{G}(V)$, the set of all equilibria of $\Gamma(G)$ under costs of protection $c > 0$ is denoted by $\mathcal{E}(c \mid G)$. As the examples above show, depending on the network, $\Gamma(G)$ may feature multiple equilibria. Those of them that maximise social welfare, i.e. (Δ, ξ) such that

$$(\Delta, \xi) \in \arg\max_{(\Delta', \xi') \in \mathcal{E}(c|G)} W(G, \Delta, \xi(\Delta)), \tag{13}$$

are called *welfare maximising*. Those of them that minimise social welfare, i.e. (Δ, ξ) such that

$$(\Delta, \xi) \in \arg\min_{(\Delta', \xi') \in \mathcal{E}(c|G)} W(G, \Delta, \xi(\Delta)) \tag{14}$$

are called *welfare minimising*.

The set of all equilibria of Γ under costs of protection $c > 0$ is denoted by $\mathcal{E}(c)$. The equilibria of Γ that maximise social welfare, i.e. (G, Δ, ξ) such that

$$(G, \Delta, \xi) \in \arg\max_{(G, \Delta', \xi') \in \mathcal{E}(c)} W(G, \Delta(G), \xi(G, \Delta)), \tag{15}$$

are called welfare maximising. The equilibria of Γ that minimise social welfare, i.e. (G, Δ, ξ) such that

$$(G, \Delta, \xi) \in \arg\min_{(G, \Delta', \xi') \in \mathcal{E}(c)} W(G, \Delta(G), \xi(G, \Delta)), \tag{16}$$

are called welfare minimising.

To account for the inefficiencies resulting from defence decentralization, we will use two measures: the price of stability and the price of anarchy.

The price of stability is defined as the fraction of payoff to the designer in the first best over the maximal payoff to the designer that can be attained in equilibrium of Γ (for the given costs of protection c):

$$\text{PoS}(n,c) = \frac{W(G^{\text{fb}}, \Delta^{\text{fb}}, \xi^{\text{fb}})}{\max_{(G,\Delta,\xi)\in\mathcal{E}(c)} W(G, \Delta(G), \xi(G, \Delta(G)))}, \tag{17}$$

where $(G^{\text{fb}}, \Delta^{\text{fb}})$ is a first best protected network and ξ^{fb} is a best response to it by A.

The price of anarchy is defined as the fraction of payoff to the designer in the first best over the minimal payoff to the designer that can be attained in equilibrium of Γ (for the given costs of protection c):

$$\text{PoA}(n,c) = \frac{W(G^{\text{fb}}, \Delta^{\text{fb}}, \xi^{\text{fb}})}{\min_{(G,\Delta,\xi)\in\mathcal{E}(c)} W(G, \Delta(G), \xi(G, \Delta(G)))}. \tag{18}$$

3.2.1 Welfare maximising equilibria

The study of welfare maximising equilibria allows us to identify inefficiencies due to decentralization of protection decisions that cannot be mitigated through network design, even if nodes and the adversary coordinate on the best possible equilibrium outcome. The main departure from the first best in the case of these equilibria derives from the fact that centrally protected star may no longer be an equilibrium. As highlighted earlier, this is due to positive externalities. Depending on the costs of protection, either all or no nodes protect in equilibrium on a star network.

Let

$$d_2(n) = \frac{f(n-1)}{n-1} \tag{19}$$

$$d_3(n) = \frac{f(n)}{n}. \tag{20}$$

Notice that since f is strictly convex and strictly increasing, so $d_2(n) < d_3(n)$, for all $n \in \mathbb{N}$. As we show in the Appendix, when costs of protection are between $d_2(n)$ and $d_3(n)$, then the only equilibrium protection that can be obtained on any network is either full protection or no protection. When costs of protection are above $d_3(n)$ then no node finds it profitable to protect, on any network, and no protection is the only equilibrium outcome. The proposition below characterizes the optimal networks when nodes and the adversary choose welfare maximising equilibria.

Proposition 2. *Let $c > 0$. $q \in Q^*(n)$, and let (G, Δ, ξ) be a welfare maximising equilibrium. Then*

1. *G is connected and* $\Delta = V$*, if* $0 < c < \min(c_1(n), c_3(n))$ *or* $d_2(n) < c < c_2(n)$.

2. *G is a star and* $\Delta = \{i\}$*, where i is the centre of the star, if* $c_1(n) < c < d_2(n)$.

3. *G has* $\lfloor \frac{n}{q} \rfloor$ *components of size q and one component of size* $n \bmod q$ *(if* $n \bmod q > 0$*), where* $q \in Q^*(n)$*, and* $\Delta = \varnothing$*, if* $\max(d_2(n), c_2(n)) < c$ *or* $\max(c_2(n), c_3(n)) < c$.

By Proposition 2, first best defence can be attained in equilibrium on first best networks, if costs of protection are small, $c < \min(c_1(n), c_3(n))$ (so that full protection is the first best), low intermediate, $c \in (c_1(n), d_2(n))$ (so that centrally protected star is the first best),[9] or large $c > \max(c_2(n), c_3(n))$ (so that no protection is the first best).

Inefficiencies due to defence decentralization cannot be avoided when costs of protection are high intermediate, $c \in (\max(d_2(n), c_1(n)), c_3(n))$. Due to positive externalities, a centrally protected star cannot be obtained as an equilibrium outcome. The designer can mitigate the inefficiencies in two different ways, depending on the costs, the number of nodes, n, and function f. If $c \in (d_2(n), c_2(n))$ (so that a connected network with full protection is better than any network with no protection), then choosing a connected network with full protection in equilibrium is optimal. On the other hand, if $c \in (c_2(n), c_3(n))$, then choosing the first best disconnected network with no protection in equilibrium is optimal.[10]

3.2.2 Welfare minimising equilibria

The study of welfare minimising equilibria allows us to identify optimal network topologies that are, in an equilibrium sense, robust to coordination failures by the nodes and the adversary (from the point of view of the designer). Departures from the first best arise under welfare minimizing equilibria at various ranges of costs of defence. Firstly, if costs of defence are small, so that connected and fully protected network is the first best, there is a potential under-protection problem due to negative externalities: there are connected networks where full protection is not the only equilibrium outcome. Secondly, if costs of defence are intermediate, so that a centrally protected star is the first best, apart from under-protection problem due to negative externalities, identified already under welfare maximising equilibria, there is also an over-protection problem due to negative externalities. Finally, if costs of defence are high, so that a disconnected network with

[9] Note that the range $(c_1(n), d_2(n))$ may be empty if marginal benefits from adding the last node to the network are sufficiently large (e.g. when $f(n) - f(n-1) > f(n-1)$). This is true, for example, when f is exponential, e.g. $f(x) = a^x - 1$, with $a > 2$.

[10] Note that range $(d_2(n), c_2(n))$ may be empty when marginal benefits from new nodes in the network are not high enough (e.g. if $f(x) = x^2$). It is non empty for faster growing f, e.g. $f(x) = x^a$, $a \geq 3$ (when x is not too large) as well as $f(x) = 2^x - 1$ (for any $x \geq 2$). For such functions there is range of costs where the designer would rather have all nodes protected than loose a component of an optimal disconnected network.

no protection is the first best, over-protection problem due to negative externalities is possible: all nodes protect in equilibrium, even if the network is fully disconnected.[11]

Let us begin by discussing the limits to what network design can achieve when all possible equilibria are considered. Let

$$d_0 = f(1). \tag{21}$$

Since f is strictly convex and increasing, $d_0 < d_2(n)$, for all $n \in \mathbb{N}$. When costs of defence are below d_0, an equilibrium with full protection exists on any network. Thus if $\max(c_2(n), c_3(n)) < d_0$ or $c_1(n) < d_0$, the over-protection problem cannot be avoided under welfare minimizing equilibria by choosing the network topology. As we show in the Appendix, the interval $(\max(c_2(n), c_3(n)), d_0)$ is empty for any f, if n is sufficiently large. However, the interval $(c_1(n), d_0)$ may be non-empty for any (sufficiently large) n if marginal benefits from adding new nodes to the network are small (e.g. when $f(x) = x^a$ with $a < 2$).

When costs of defence are below $d_3(n)$, then every connected network has an equilibrium where all nodes protect. This suggests that the over-protection problem in the range $(c_1(n), d_3(n))$ can only be addressed by disconnecting the network. Observe that this interval is non-empty, as long as the interval $(c_1(n), c_2(n))$ is non-empty. Thus sacrificing some nodes to avoid excessive protection is necessary in the intermediate range of costs, where centrally protected star is the first best.

When costs of protection are above $d_2(n)$, it is not profitable for any node to protect if all other nodes do not protect. Thus if $c > d_2(n)$, any network has an equilibrium where no nodes protect. When $d_2(n) < c < c_3(n)$, in which case at least one node is protected in the first best, we face under-protection problem due to positive externalities that cannot be eliminated by network design. Thus if $d_2(n) < c < c_3(n)$ (in which case at least one node is protected in the first best) there is always an equilibrium where no nodes protect, regardless of what network is chosen by the designer.

We divide the study of how inefficiencies under welfare minimizing equilibria can be addressed by network design into three cases corresponding to three different types of first best outcomes.

Low costs of defence: securing full protection. When costs of defence are low, $c < \min(c_1(n), c_2(n))$, a fully protected connected network is the first best. The most important result of this section is that full protection in equilibrium can be enforced by network design, when costs of protection are sufficiently low. When the costs are low-intermediate, then full protection cannot be enforced and the best we can do is to choose a star where the centre protect in equilibrium. Lastly, when the costs are in the upper

[11] This last problem requires the marginal benefits from adding new nodes to the network to be sufficiently small. Due to convexity of function f, there is always a size of network, n, where this ceases to be the case.

range of the considered interval, then no protection cannot be avoided and the first best unprotected network is the best choice.

Suppose that $c < \min(c_1(n), c_2(n), d_2(n))$. If costs of protection are very low: $c < \frac{f(1)}{n}$, then any attacked node is better off by protecting, independent of the protection decisions of other nodes. Therefore in any equilibrium outcome full protection is secured, regardless of the network. Thus D can attain the first best by choosing any connected network.

What if costs of protection are low but not very low: $\frac{f(1)}{n} < c < \min(c_1(n), c_2(n), d_2(n))$? As we discussed already, there are connected networks were inefficient equilibrium outcomes are possible, as nodes may fail to coordinate on the efficient equilibria (e.g. no protection on the clique, when full protection is the first best, or a more subtle underprotection illustrated in Figure 1). However, this problem can be solved by choosing the right topology of the network. The idea is to create a *cascade of incentives to protect* in the network. That is, the network should be such that at least one node has incentives to protect in it. Then, for every such node, there should exist subsequent nodes that have incentives to protect, if one of the former nodes protects, etc. A network where such a cascade leads to full protection needs to have a *critical node* which has incentives to protect even if no other node protects. Critical node is defined as follows.

Definition 1 (k-critical node)**.** Node $i \in V$ is *k-critical* in a connected network $G \in \mathcal{G}(V)$ if $\min_{C \in \mathcal{C}(G-\{i\})} |V \setminus C| = k$.

Loosely speaking, the importance of a node as a barrier against contagion is increasing in its criticality. For example, any node in a d-connected network, $d \geq 2$, is 1-critical.[12] When protected, it secures one node from being infected. On the other hand, the centre of a star is $(n-1)$-critical. When protected, it secures $n-1$ nodes from being infected.

Let $h(x) = \frac{f(x)}{x}$ denote the gross payoff of a node in a component of size x. Since f is increasing and strictly convex, h is increasing and has well defined inverse, $h^{-1}(x)$, which is also increasing. As we show in the Appendix, existence of k-critical node with $k \geq h^{-1}(c)$ in a connected network $G \in \mathcal{G}(V)$ is a necessary condition for having full protection in any equilibrium outcome of $\Gamma(G)$. In essence, the presence of a k-critical node, with $k > h^{-1}(c)$, rules out equilibrium outcomes where no node protects: each such k-critical node has incentive to protect, regardless of what other nodes choose. However, it is not sufficient for having full defence in any equilibrium outcome. Consider the following example.

Example 1. Let $f(x) = x^2$, $V = \{1, \ldots, 6\}$, and suppose that $1 < c \leq \frac{11}{5} = \min(c_1(6), d_2(6), c_2(6))$. Let G be a star network with centre 1. Consider the strategy profile (Δ, ξ) of $\Gamma(G)$ such that $\Delta = \{1\}$, i.e. only the centre protects, and $\xi(\Delta)$ mixes uniformly on all the spokes. Payoff to a spoke j from this strategy profile is $\left(\frac{4}{5}\right) \cdot 5 = 4$. If j protects,

[12] A network is d-connected if there is no set of $l < d$ nodes whose removal disconnects the network and the network can be disconnected by removing a set of d nodes (see Bollobás (1998), for example).

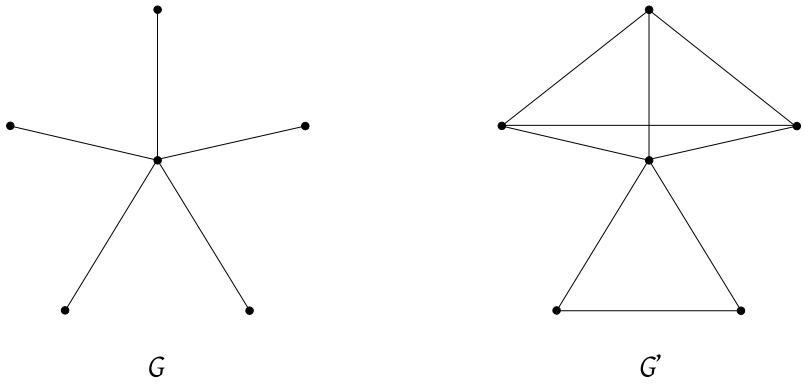

Figure 2: Networks G, a star over 6 nodes, and G', obtained by fully connecting three of the spokes in one group and the remaining two in another group.

the payoff is $5 - c$, which is less than 4 for any $c \in (1, \frac{11}{5})$. Hence there is an equilibrium where only one node protects in $\Gamma(G)$. When the centre protects, player A chooses a maximal component of $G - \{i\}$ to eliminate. In the case of the star network the number of the maximal components is large and if A mixes across them with equal probability, each spoke prefers not to protect, as the probability of being eliminated is relatively low. To trigger a cascade of incentives to protect, the designer has to create imbalance in the sizes of components of $G - \{i\}$. This increases the chances for the nodes to be eliminated and gives them more incentives to protect.

In the example above, let G' be network obtained from G by forming a clique over the spokes $\{2, 3, 4\}$ and a clique over the spokes $\{5, 6\}$ (c.f. Figure 2). Node 1 is 3-critical and since $3 > c$, so it protects even if no other node protects. When 1 protects, the adversary attacks the group of three interconnected spokes, $\{2, 3, 4\}$, with probability 1. Because of that any of the spokes from the group has incentive to protect when 1 protects. Suppose that 1 and 2 protects. Then the adversary is indifferent between attacking the group $\{3, 4\}$ and $\{5, 6\}$. If A chooses one of the groups uniformly, payoff from protecting for any of the unprotected nodes is $4 - c$ while payoff from not protecting is $\left(\frac{1}{2}\right) \cdot 4$. Thus it is profitable for the node to protect if $1 < c \leq 2$ and it is not if $2 < c < \frac{11}{5}$. Suppose that nodes $\{1, 2, 3\}$ protect. It is straightforward to verify that then all other nodes find it profitable to protect as well. Hence full protection is the only equilibrium outcome on G' when $1 < c \leq 2$. In the case of $2 < c \leq \frac{11}{5}$, full protection cannot be secured and the optimal network is a star where, in the worst equilibrium, the centre protects and one of the spokes is destroyed by the adversary.

The example above illustrates that along with a critical node i in network G, it is also necessary to have the right sizes of components in $\mathcal{C}(G - \{i\})$. It is related to existence of properly balanced partition of $n - 1$ nodes. Given quantity $q \in \mathbb{N}_{++}$, a *partition* of q is a sequence $\pi(q) = (s_1, \ldots, s_m)$ such that $s_j \in \mathbb{N}_{++}$, for all $j \in \{1, \ldots, m\}$, $\sum_{j=1}^{m} s_j = q$, and $s_1 \geq \ldots \geq s_m$. Given partition $\pi(q)$ and number $j \in \mathbb{N}$, let $L_j(\pi(q)) = \max\{r \in$

$\{1,\ldots,m\} : s_r \geq j\}$ be the number of parts of size at least j.

Definition 2 ((h,c)-partition)**.** A partition $\pi(q) = (s_1,\ldots,s_m)$ of q is a (h,c)-*partition* if for all $j \in \{1,\ldots,m\}$ it holds

$$L_j(\pi(q)) \leq \frac{h(q-j)}{c} \tag{22}$$

Existence of (h,c)-partition of $n-1$ nodes depends on the cost, c, function f, and the number of nodes. Let

$$d_1(n) = \max\left\{c \in \mathbb{R}_{++} : \sum_{j=1}^{n-1}\left\lfloor \frac{h(j)}{c}\right\rfloor \geq n-1\right\} \tag{23}$$

Notice that $d_0 \leq d_1(n) \leq d_2(n)$. To see that observe that $\sum_{j=1}^{n-1}\lfloor\frac{h(j)}{c}\rfloor$ is (weakly) decreasing in c. Since $h(j) \geq f(1) = d_0$, for all $j \geq 1$ with strict inequality for $j > 1$, so $\sum_{j=1}^{n-1}\lfloor\frac{h(j)}{f(1)}\rfloor \geq n-1$ (with strict inequality for $n \geq 3$) and, consequently, $d_0 \leq d_1(n)$. Since $\sum_{j=1}^{n-1}\lfloor\frac{h(j)}{c}\rfloor$ is less than $n-1$, for all $c > d_2(n)$, so $d_1(n) \leq d_2(n)$. As we show in the Appendix, an (h,c)-partition of $n-1$ exists if and only if $c < d_1(n)$.

Lastly, to prevent under-protection due to component balancedness of nodes' gross payoffs, the network topology should be "tight" enough to avoid equilibria such as the one illustrated in Figure 1. In further analysis, the following networks, defined for a given non-empty sequence of positive integers, π, will be important.

Definition 3 (π-windmill networks)**.** Given a sequence of positive integers, $\pi = (s_1,\ldots,s_m)$, let G be a network over $n = 1 + \sum_{j=1}^{m} s_j$ nodes defined as follows. Put one node, say i, aside and partition the remaining nodes into groups of sizes $s_1,\ldots,s_m$. Connect the nodes within each group to form m cliques. Lastly, connect all the nodes in the cliques to node i

As we show in the Appendix, if π is an (h,c)-partition of $n-1$ then any π-windmill network has full protection as the unique equilibrium outcome if $c < d_1(n)$.

Definition 4 (Family $\mathcal{G}^f(n,c)$)**.** Given function f, the number of nodes n, and cost of protection c, let $\mathcal{G}^f(n,c)$ denote the set of networks over n nodes such that in every equilibrium (Δ,ξ) of $\Gamma(G)$, all nodes protect, i.e. $\Delta = V$.

Notice that if $0 < c < \frac{f(1)}{n}$ then $\mathcal{G}^f(n,c)$ is the set of all connected networks over n nodes. Moreover, if $\frac{f(1)}{n} < c < d_1(n)$, then $\mathcal{G}^f(n,c)$ is non-empty and contains π-windmill networks with π being an (h,c)-partition of $n-1$.

If costs of protection are in the upper range of the considered interval, $d_2(n) < c < \min(c_1(n), c_2(n))$ then every network has an equilibrium where no node protects. As we observed above, this cannot be addressed by network design. The optimal choice of the designer is the first best unprotected network. The following proposition characterizes welfare minimising equilibria for low costs of defence.

Proposition 3. *Let* $0 < c < c_1(n)$.

1. *If* $0 < c < d_1(n)$ *then* $\mathcal{G}^f(n,c) \neq \varnothing$ *and* (G, Δ, ξ) *such that* $G \in \mathcal{G}^f(n,c)$ *and* $\Delta = V$ *is a welfare minimising equilibrium.*

2. *If* $d_1(n) < c < \min(c_1(n), c_2(n), d_2(n))$ *then* (G, Δ, ξ) *such that* G *is a star network with centre* i, $\Delta = \{i\}$, *and* ξ *is a probability distribution on* $V \setminus \{i\}$, *is a welfare minimising equilibrium.*

3. *If* $d_2(n) < c < \min(c_1(n), c_2(n))$ *then* (G, Δ, ξ) *such that* G *has* $\lfloor \frac{n}{q} \rfloor$ *components of size* q *and one component of size* $n \bmod q$ *(if* $n \bmod q > 0$*), where* $q \in Q^*(n)$, *and* $\Delta = \varnothing$, *is a welfare minimising equilibrium.*

Intermediate costs of defence: addressing over-protection and under-protection. When costs of defence are intermediate, $c_1(n) < c < c_3(n)$, a centrally protected star is the first best. As we discussed above, two types of inefficiencies appear when defence is decentralized and costs of defence are intermediate, $c_1(n) < c < c_3(n)$. In the upper range of the interval, when $d_2(n) < c < c_3(n)$, there is an under-protection problem due to positive externalities. When $c_1(n) < c < d_2(n)$, there is an over-protection problem due to negative externalities.

The most important result of this section is that the only way to mitigate over-protection by network design is by splitting the network, while under-protection is unavoidable. The optimal topology of the network that mitigates over-protection is closely tied to the shape of function f. We end the section by an example of optimal design for Metcalf's law, $f(x) = x^2$.

Consider the upper range of costs of protection, $d_2(n) < c < c_3(n)$. When $d_3(n) < c_3(n)$, then no node protects in any equilibrium on any network. Thus in this range of costs of defence, the only thing the designer can do is choosing the first best disconnected network with no protection. If $d_2(n) < c < \min(d_3(n), c_3(n))$, then the centre of the star finds it unprofitable to protect, unless all the nodes in the network protect. Thus the designer could address the problem in two ways: enforce excessive protection, by choosing a network where all nodes protect in the welfare minimising equilibrium, or enforce no protection, by choosing a network where no nodes protect in welfare minimising equilibrium. When $c_2(n) < c < \min(d_3(n), c_3(n))$, first best disconnected network is better for the designer than any fully protected network, and no protection is the only equilibrium outcome on the first best disconnected network. Hence it is optimal for the designer to choose the first best disconnected network with no protection. When $d_2(n) < c < c_2(n)$, full protection is the preferred equilibrium outcome. However, with $c > d_2(n)$, any network has an equilibrium where no nodes protect. Hence full protection cannot be secured by network design. Therefore the best choice of the designer is again a first best disconnected network, which has no protection in any equilibrium when $c > d_2(n)$.

Second, consider the lower range of costs of protection, $c_1(n) < c < \min(d_2(n), c_3(n))$. When $c_1(n) < c < d_2(n)$, a star network has two possible equilibrium outcomes: only the centre protects, or all nodes protect. Thus under-protection is no longer an issue and a new problem arises: over-protection due to negative externalities. If $c_1(n) < c < d_0$, full protection is an equilibrium outcome on any network. Therefore this range of costs the over-protection problem cannot be avoided and an optimal choice is a connected network where full protection is the worse equilibrium outcome. This motivates the definition of the following family of networks.

Definition 5 (Family $\mathcal{G}^w(n,c)$)**.** Given function f, the number of nodes n, and cost of protection c, let $\mathcal{G}^w(n,c)$ denote the set of connected networks over n nodes such that in the worse equilibrium (Δ, ξ) of $\Gamma(G)$, all nodes protect, i.e. $\Delta = V$.

Notice that if $0 < c < \frac{f(1)}{n}$ then $\mathcal{G}^w(n,c)$ is the set of all connected networks over n nodes. Moreover, if $\frac{f(1)}{n} < c < d_0$, then $\mathcal{G}^w(n,c)$ is non-empty and contains star networks over n nodes.

If $\max(c_1(n), d_0) < c < d_2(n)$ then any connected network has an equilibrium with full protection. Therefore over-protection cannot be avoided on the connected network and the inefficiencies due to over-protection can only be mitigated by splitting the network and sacrificing some nodes. In particular, any such network must have a component small enough so that no node in it finds it profitable to protect. The discussion above is summarized in the following proposition.

Proposition 4. *Let $c_1(n) < c < c_3(n)$.*

1. *If $c_1(n) < c < d_0$ then (G, Δ, ξ) with $G \in \mathcal{G}^w(n,c)$ and $\Delta = V$ is a welfare minimising equilibrium.*

2. *If $\max(c_1(n), d_0) < c < d_2(n)$ and (G, Δ, ξ) is a welfare minimising equilibrium with $\Delta(G) \subsetneq V$, then either G is a disconnected network and contains a component of size m such that $\frac{f(m)}{m} < c$ or $G \in \mathcal{G}^w(n,c)$ and $\Delta = V$.*

3. *If $d_2(n) < c < c_3(n)$ then (G, Δ, ξ) such that G has $\lfloor \frac{n}{q} \rfloor$ components of size q and one component of size $n \bmod q$ (if $n \bmod q > 0$), where $q \in Q^*(n)$, and $\Delta = \varnothing$, is a welfare minimising equilibrium.*

Notice that the second bullet of the proposition does not specify the number of components and their topology, in the case were over-protection can be mitigated by splitting the network. It only states that splitting the network is the only thing we can do to address over-protection in this case and that it requires separating at least one components from the network which is sufficiently small to make individual protection unprofitable for any node. These small components can have any topology. The number of components and the topology of the larger components depends on the shape of function f. An example

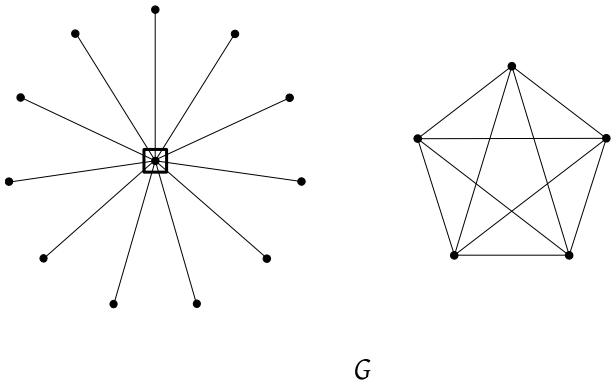

Figure 3: Network G consisting of a star over 12 nodes, and a clique over 5 nodes.

below illustrates how splitting the network can be used to mitigate the over-protection problem in the case of $f(x) = x^2$, i.e. in the case of network value function consistent with Metcalfe's law.

Example 2. Let $f(x) = x^2$ and $n = 17$. Suppose that $c \in (10, 16) \subseteq (\frac{33}{16}, 16) = (\min(c_1(n), d_0), d_2(n))$. In this range of costs, centrally protected star is the first best and yields payoff $256 - c \in (240, 246)$ to player D. An equilibrium outcome from welfare minimising equilibrium on the star network is full protection, which results in payoff $289 - 17c \in (17, 119)$ to D. The first best disconnected network with no protection consists of two components of size 8 and one component of size 1, and yields payoff 65 to D.

Consider network G consisting of two components: one a star over 12 nodes and another one, a clique, over 5 nodes (c.f. Figure 3). It is easy to verify that in the unique equilibrium outcome in $\Gamma(G)$ in the range of costs under consideration, the centre of the star protects and the adversary removes the clique. This yields payoff $144 - c > 289 - 17c$, if $c \geq 10$. Thus G is better to D than the star network. It is also better than the first best disconnected network, as $144 - c > 65$ if $c < 16$.

High level of costs: no inefficiencies for large networks. No node has incentive to protect in components of size $q \in Q^*(n)$ if $c > \max(c_2(n), c_3(n))$, as long as $q \geq 2$. Thus if $d_0 < \max(c_2(n), c_3(n))$, then first best equilibrium outcome is attained in every equilibrium for high level of costs of defence. Since $d_0 < c_3(n)$, for sufficiently high n, so the first best equilibrium for high costs of protection can be attained if the number of nodes is large enough. In the case of $c \in (\max(c_2(n), c_3(n)), d_0)$ there is a problem of over-protection. In this case it is optimal for the designer to choose a connected network which features full protection in the worst equilibrium outcome, i.e. a network in $\mathcal{G}^w(n, c)$. The following proposition characterizes optimal networks under welfare minimising equilibria.

Proposition 5. *Let $c > \max(c_2(n), c_3(n))$. Let (G, Δ, ξ) be a welfare minimising equilibrium of Γ. Then*

1. *If* $c < d_0$ *then* $G \in \mathcal{G}^w(n,c)$ *and* $\Delta = V$.

2. *If* $c > d_0$ *then* G *has* $\lfloor \frac{n}{q} \rfloor$ *components of size* q *and one component of size* $n \bmod q$ *(if* $n \bmod q > 0$*), where* $q \in Q^*(n)$*, and* $\Delta = \varnothing$.

Moreover, for sufficiently high n, $d_0 < c_3(n)$ *and only point 2 applies.*

3.3 The price of decentralization

The analysis in Section 3.2 allows us to measure the costs of decentralization in terms of the price of anarchy (PoA) and the price of stability (PoS). Notice first that, by Proposition 2, $\text{PoS}(n,c) = 1$, unless $c \in (d_2(n), c_3(n))$. In this case the centrally protected star is the first best, but, due to positive externalities, this outcome cannot be obtained in any equilibrium on any network. It is easy to see that the threshold cost $d_2(n)$ is increasing. If it is unbounded, then for any fixed c, if the network is sufficiently large, $c < d_2(n)$ and $\text{PoS}(n,c) = 1$. That is, the first best can be attained as an equilibrium outcome if the number of nodes is sufficiently large. However, if $d_2(n)$ is bounded, there might exists levels of costs of protection c for which $\text{PoS}(n,c) > 1$ even if the network is very large. Take for example $f(x) = x - \ln(x+1)$. This function is strictly increasing and convex, but the marginal benefits from subsequent nodes in the network, although increasing, are bounded from above by 1. Because of that, utility of a node, $\frac{f(m)}{m}$, converges to 1 when its component grows.

Consider now the worst case scenario, where nodes and the adversary coordinate on welfare minimising equilibria. Firstly, we note that if costs of protection are sufficiently low, $c < \min(c_1(n), c_2(n), d_1(n))$, or sufficiently high, $c > \max(c_2(n), c_3(n), d_0)$ then, by Propositions 3 and 5 the designer can fully prevent the inefficiencies due to decentralization by the right network design. Hence $\text{PoA}(n,c) = \text{PoS}(n,c) = 1$ in this case.

We show in the Appendix that

$$\lim_{n\to+\infty} d_1(n) = \lim_{n\to+\infty} d_2(n) = \lim_{n\to+\infty} d_3(n) = \lim_{n\to+\infty} \frac{f(n)}{n}. \tag{24}$$

Thus, given fixed costs of protection, c, when n is sufficiently large then either the gross payoff to a node in a connected network is higher than c (in which case, by Proposition 3, full protection can be secured by network design) or it is lower than c (in which case no node protects in every equilibrium, on any network). In the former case the relative loss from possible over-protection converges to a constant value when the number of the nodes increases. In particular, it vanishes if the gross payoff is unbounded and the number of the nodes grows. The latter case implies the $f(n) < nc$ in which case choosing a first best unprotected network to mitigate the effects of under-protection leads to small relative loss from defence decentralization. The theorem below summarizes the asymptotic behaviour of the inefficiencies due to decentralization.

Theorem 1. *Let $c > 0$ be costs of protection and $|V| = n$ be the number of nodes.*

1. *If $c < \min(c_1(n), c_2(n), d_1(n))$ or $c > \max(c_2(n), c_3(n), d_0)$, then $\mathrm{PoA}(n, c) = \mathrm{PoS}(n, c) = 1$.*
2. *If $\lim_{n\to+\infty} \frac{f(n)}{n} = p \leq c$, then $\mathrm{PoS}(n, c), \mathrm{PoA}(n, c) \lesssim \frac{p}{f(1)}$ when $n \to +\infty$.*
3. *If $\lim_{n\to+\infty} \frac{f(n)}{n} = p < +\infty$ with $p > c$, then $\lim_{n\to+\infty} \mathrm{PoS}(n, c), \lim_{n\to+\infty} \mathrm{PoA}(n, c) \lesssim \frac{p}{p-c}$ when $n \to +\infty$.*
4. *If $\lim_{n\to+\infty} \frac{f(n)}{n} = +\infty$ then $\lim_{n\to+\infty} \mathrm{PoS}(n, c) = \lim_{n\to+\infty} \mathrm{PoA}(n, c) = 1$.*

As a corollary from Theorem 1, note that if $f(x) = x^a$, with $a > 1$, or $f(x) = a^x - 1$, with $a > 1$, then $\lim_{n\to+\infty} f(n)/n = +\infty$ and

$$\lim_{n\to+\infty} \mathrm{PoA}(n, c) = \lim_{n\to+\infty} \mathrm{PoS}(n, c) = 1. \tag{25}$$

In particular, in the case of Metcalfe's law and Reed's law inefficiencies due to decentralization can be mitigated arbitrarily well by network design for sufficiently large number of nodes.

4 Discussion

In this section we summarize the results from Section 3 and highlight the main messages of the paper. We focus on welfare minimizing equilibria. To make the presentation clearer we distinguish two cases: (1) one where f does not grow extremely fast, so that $c_1(n) < c_3(n)$, and (2) one where f grows extremely fast, so that $c_1(n) > c_3(n)$.

We start with case (1). This is the richer case and it covers all functions of the form $f(x) = x^a$ with $a > 1$ as well as all functions of the form $f(x) = a^x - 1$ with $a > 1$. As the analysis in Section 3 shows, we have two sets of thresholds for costs of protection: one set for the first best and one for the decentralized protection. For the first best we have two key thresholds, $c_1(n) < c_3(n)$, and

(i). if $c < c_1(n)$ then connected fully protected network is the first best outcome,

(ii). if $c_1(n) < c < c_3(n)$ then centrally protected star is the first best outcome, and

(iii). if $c > c_3(n)$ then first best outcome is disconnected unprotected network,

For the decentralized protection we have three key thresholds, $d_0 \leq d_1(n) \leq d_2(n)$, and

(i). if $c < d_0$ then any network has an equilibrium outcome where all nodes protect,

(ii). if $c < d_1(n)$ then there exist connected networks which have full protection as the unique equilibrium outcome,

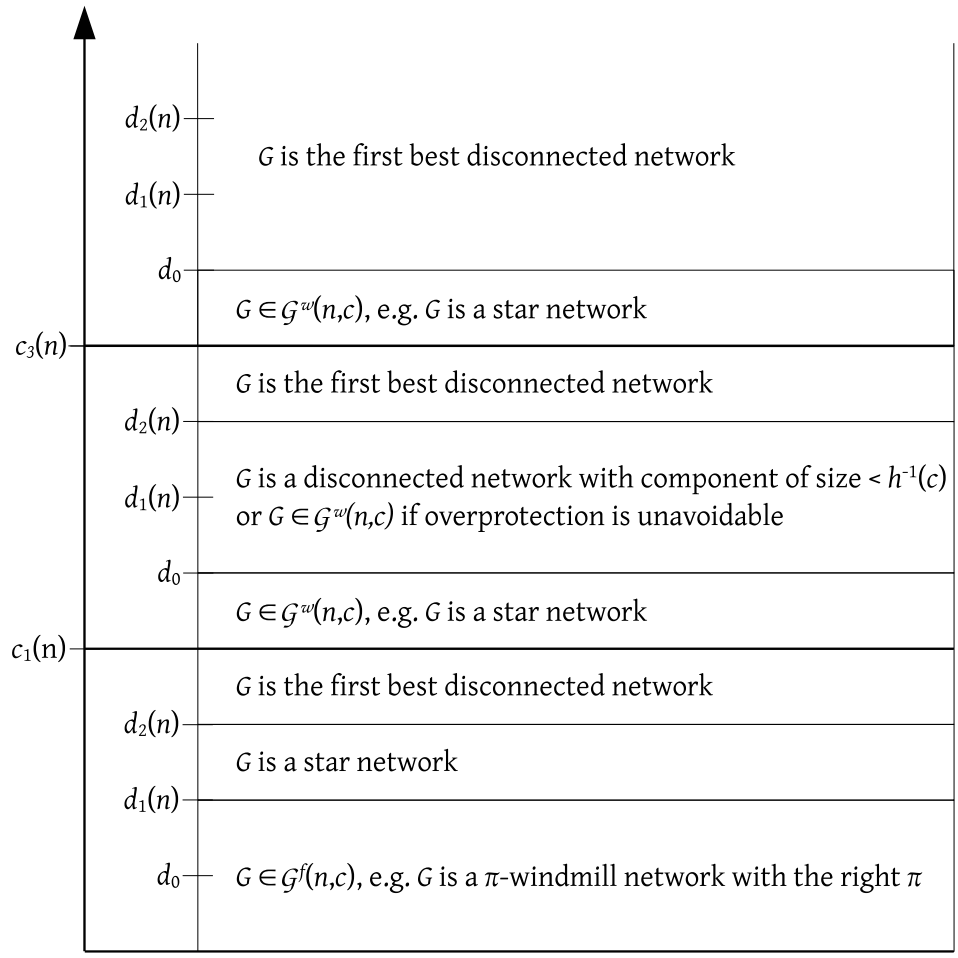

Figure 4: Welfare minimizing equilibria for different values of costs and f not growing extremely fast.

(iii). if $d_1(n) < c < d_2(n)$ then any connected network has an equilibrium outcome where at least one node does not protect,

(iv). if $c > d_2(n)$ then two equilibrium outcomes are possible: no node protects (this is an equilibrium outcome on any network), or all nodes protect (this equilibrium outcome is possible on connected networks only, and it exists on any connected network).

Depending on how the above sets of thresholds interleave (which depends on function f), we have different problems and different design choices. Let us analyse the design decisions, as c changes (which is summarized in Figure 4).

Consider first $c < c_1(n)$. In this case full protection in a connected network is the first best equilibrium outcome and the only inefficiencies that may appear when protection decisions are decentralized is the under-protection problem. If $c < d_1(n)$ then, by point 1 of Proposition 3, first best outcome can be attained as a unique equilibrium outcome if the network topology is properly chosen: given c, n, and f, we can get a partition of nodes

in n, π, and choose a π-windmill network to enforce full protection in every equilibrium. If $c > d_1(n)$, then any network features an equilibrium where at least one node does not protect and so the under-protection problem cannot be avoided by network design. In the case of $c \in (d_1(n), d_2(n))$, cost of protection is not very high and the best choice is a star network, where the centre protects in the welfare minimising equilibrium and the attack removes only one node (Proposition 3, point 2). When $c > d_2(n)$, every network features an equilibrium where no nodes protect and the first best disconnected network features only such equilibria. Therefore first best disconnected network is a welfare minimizing equilibrium choice in this case (Proposition 3, point 2).

Second, consider $c \in (c_1(n), c_3(n))$. In this case centrally protected star the first best equilibrium outcome and both, the over-protection and the under-protection problems may appear. If $c < d_0$ then every network features an equilibrium where all nodes protect. Hence we have an over-protection problem which cannot be avoided by network design. Note that although there is an equilibrium with full protection on any network, there can be networks where there are equilibria which are even worse. Also, an equilibrium with full protection is best on connected networks. For these reasons the designer chooses a connected network where full protection is the worse equilibrium outcome (Proposition 4, point 1). An example of such a network is a star network. If $c \in (d_0, d_2(n))$, then every connected network features an equilibrium with full protection, while there may exist disconnected networks where at least one node does not protect in equilibrium. Thus over-protection can be mitigated only by disconnecting the network and the designer chooses between a connected network with full protection in the welfare minimising equilibrium and a the best disconnected network with partial protection in the worst equilibrium (Proposition 4, point 2). If $c > d_2(n)$, then every network features an equilibrium where no nodes protect and the first best unprotected network is chosen by the designer (Proposition 4, point 3).

Third, consider $c > c_3(n)$. In this case an optimal disconnected network with no protection is the first best equilibrium outcome. This outcome can be attained as long as $c > d_0$, because in this case the first best disconnected network features equilibria with no protection only (Proposition 5, point 2). If $c < d_0$, then there is an equilibrium with full protection on any network and so we have an unavoidable over-protection problem. In this case the designer chooses a connected network where full protection is the welfare minimising equilibrium, e.g. a star network ((Proposition 5, point 1)).

We now switch to case (2), where f grows extremely fast. This covers functions f that grow at least as fast as $x!$, for example $f(x) = (x+1)^x - 1$. For first best we have one key threshold, $c_2(n)$. If $c < c_2(n)$, then connected fully protected network is the first best equilibrium outcome, and if $c > c_2(n)$, then the first best outcome is disconnected unprotected network. The thresholds for decentralized protection are like in the case above. Again, depending on function f, $c_2(n)$ may be in different intervals determined by $d_0 < d_1(n) < d_2(n)$, which leads to different problems. Figure 5 summarizes the design

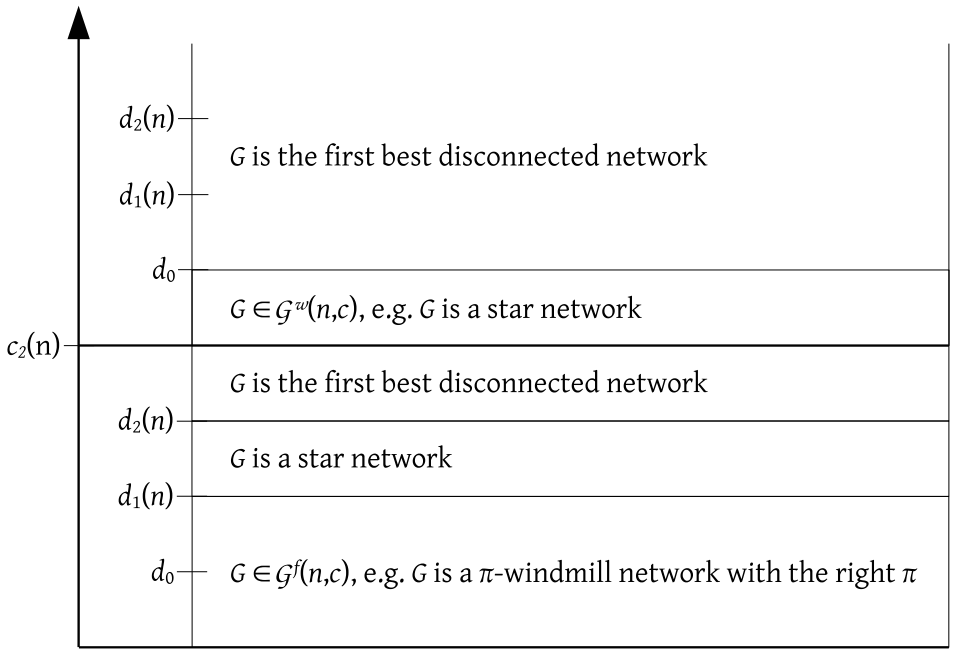

Figure 5: Welfare minimizing equilibria for different values of costs and f growing extremely fast.

decisions as c changes. The analysis of the case $c < c_2(n)$ is analogous to the case of $c < c_1(n)$, discussed above, and the analysis of the case $c > c_2(n)$ is analogous to the case of $c > c_3(n)$, discussed above (and we do not repeat it here).

There are two key messages from Section 3. First, there are ranges of costs where inefficiencies due to decentralization can be fully addressed or at least mitigated. In the low range of costs, network design can be used to create cascade of incentives to secure full protection as a unique equilibrium outcome on a connected network. In the intermediate range of costs network design can be used to mitigate the inefficiencies, but it requires splitting the network (and so giving up some value due to connectivity and sacrificing some nodes). Second, there is a range of costs where network design is ineffective. When $\max(c_1(n), d_2(n)) < c < c_3(n)$ then inefficiencies due to decentralization are unavoidable and present in any equilibrium outcome. Therefore different means must be used to address the inefficiencies (e.g. subsidising some nodes or allocating more network value to them, to motivate protection).

An important result in terms of asymptotics (Equation 24) is that thresholds $d_1(n)$, $d_2(n)$ and $d_3(n)$ all converge to the same value, $\frac{f(n)}{n}$, which is the share a node gets from a connected network of size n (i.e. it is the gross utility of a single node). Thus the range $(d_1(n), d_3(n))$ shrinks and the most important construction for large networks in terms of network design is that of enforcing full protection by creating a cascade of incentives to protect by network design.

5 Conclusions

In this paper we studied the problem of using network design to address inefficiencies resulting from decentralized protection. We showed that if costs of protection are either sufficiently high or sufficiently low, the first best defence can be enforced by choosing the right network topology. If costs of protection are intermediate, over- and under-protection problems arise. The best way to tackle the over-protection problem is by disconnecting the network and sacrificing some nodes. The under-protection problem cannot be removed by network design and can only be mitigated by disconnecting the network and reducing the number of nodes infected by the adversary. Although the first best cannot be attained in this case, for some network value functions (including those following from Metcalfe's law and Reed's law) the inefficiency ratio, as measured by price of anarchy and price of stability, converges to 1 when the number of nodes grows. That is, network design can prove a powerful tool to mitigate protection inefficiencies.

As discussed in Section 2.1, we made a number of simplifying assumptions and relaxing them opens avenues for further research. One extension that seems particularly interesting is heterogenous importance of the nodes in the network. It would be interesting to study whether trying to protect more important nodes and ensuring connections to them would result in significantly higher inefficiencies.

Acknowledgements Sanjeev Goyal and Diego Cerdeiro were supported by European Research Area Complexity-Net (`http://www.complexitynet.eu`) through grant, Resilience and interaction of networks in ecology and economics (RESINEE). Diego Cerdeiro acknowledges financial support from Queens' College and the Cambridge Overseas Trust Marcin Dziubiński was supported by the Strategic Resilience of Networks project realized within the Homing Plus programme of the Foundation for Polish Science, co-financed by the European Union from the Regional Development Fund within Operational Programme Innovative Economy ("Grants for Innovation"). Sanjeev Goyal acknowledges financial support from a Keynes Fellowship and the Cambridge-INET Institute.

References

D. Acemoglu, A. Malekian, and A. Ozdaglar. Network security and contagion. *Journal of Economic Theory*, 166:536– 585, 2016.

J. Aspnes, K. Chang, and A. Yampolskiy. Inoculation strategies for victims of viruses and the sum-of-squares partition problem. *Journal of Computer and System Sciences*, 72(6):1077–1093, 2006.

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

BIS-IOSCO. Guidance on cyber resilience for financial market infrastructures. Report, Bank for International Settlements and International Organization of Securities Commissions, June 2016.

B. Bollobás. *Modern Graph Theory*. Springer, July 1998.

CoinDesk. Report: Bitcoin targeted in 22% of financial malware attacks. `http://www.coindesk.com/report-bitcoin-targeted-22-financial-malware-attacks/`, August 2014.

S. Goyal and A. Vigier. Attack, defence, and contagion in networks. *The Review of Economic Studies*, 81(4):1518–1542, 2014.

S. Goyal, S. Jabbari, M. Kearns, S. Khanna, and J. Morgenstern. *Strategic Network Formation with Attack and Immunization*, pages 429–443. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016.

H. Kunreuther and G. Heal. Interdependent Security. *The Journal of Risk and Uncertainty*, 26:231–249, 2003.

M. Lelarge and J. Bolot. Network externalities and the deployment of security features and protocols in the internet. *ACM SIGMETRICS Performance Evaluation Review - SIGMETRICS*, 36(1):37–48, 2008a.

M. Lelarge and J. Bolot. A local mean field analysis of security investments in networks. In J. Feigenbaum and Y. R. Yang, editors, *NetEcon*, pages 25–30. ACM, 2008b.

T. Moore, R. Clayton, and A. R. The economics of online crime. *Journal of Economic Perspectives*, 23(3):3–20, 2009.

S. Scott and M. Zachariadis. *The Society for Worldwide Interbank Financial Telecommunication (SWIFT): Cooperative governance for network innovation, standards, and community*. Global Institutions. Routledge, 2013.

H. Varian. *System Reliability and Free Riding*, pages 1–15. Springer US, Boston, MA, 2004.

A Proofs

A.1 First best

Proof of Proposition 1. Let (G, Δ) be a first best protected network. Three cases are possible.

Case (i): $\Delta = N$ Clearly in this case G must be a connected network.

Case (ii): $\varnothing \subsetneq \Delta \subsetneq N$ In this case A removes at least one node from G and so gross welfare is bounded from above by $f(n-1)$. Star network is the unique network that attains this upper bound by using only one unit of protection. This is the lowest possible number of protected nodes possible in Case (ii). This G is a star and $\Delta = \{i\}$, where is is the centre of G.

Case (iii): $\Delta = \varnothing$ As long as $n > 1$, any disconnected G yields higher welfare than a connected network in this case. Moreover, there are at most two sizes of components in $\mathcal{C}(G)$. For assume otherwise and let $C_1, C_2, C_3 \in \mathcal{C}(G)$ be such that $|C_1| > |C_2| > |C_3|$. Then, since f is strictly increasing and strictly convex, D is better of by moving a node from C_3 to C_2. Lastly, if C_1 is the component of maximal size in $\mathcal{C}(G)$, then there is at most one component $C \in \mathcal{C}(G)$ with $|C| < |C_1|$. If there was another component $C' \in \mathcal{C}(G)$ with $|C'| = |C|$, then, since f is strictly increasing and strictly convex, D would be better off by moving a anode from C' to C. It is straightforward to see that the number and the sizes of the components are as stated in the proposition. □

A.2 Welfare maximising equilibria

Before we provide the proof of the main result for welfare maximising equilibria, Proposition 2, we prove two auxiliary results: Observation 1 and Lemma 2.

Observation 1 implies that if the size of the larger components in the first best networks with no protection is at least two, then no node has incentive to protect in equilibrium. Consequently, in this case the first best outcomes can be attained in any equilibrium for sufficiently large costs of defence: $c > c_3(n)$.

Observation 1. *For all* $2 \leq q \leq n-1$,

$$\frac{f(q)}{q} < f(n-1) - \left(\left\lfloor \frac{n}{q} \right\rfloor - 1 \right) f(q) - f(n \bmod q) \tag{26}$$

Proof. Let $2 \leq q \leq n-1$. Since f is strictly increasing and strictly convex and $q \leq n-1$, so

$$qf(n-1) \geq (n-1)f(q), \tag{27}$$

and since $q \geq 2$ so

$$qf(n-1) \geq (n-q+1)f(q). \tag{28}$$

Let $r = n \bmod q$. Since $r < q$ and f is strictly increasing and strictly convex, so $rf(q) > qf(r)$ and

$$qf(n-1) > (n-r-q+1)f(q) + qf(r). \tag{29}$$

Dividing both sides by q we get

$$f(n-1) > \left(\frac{n-r}{q} - 1\right) f(q) + f(r) + \frac{f(q)}{q}. \tag{30}$$

Noticing that $\frac{n-r}{q} = \lfloor \frac{n}{q} \rfloor$ and reorganizing, we get

$$f(n-1) - \left(\left\lfloor \frac{n}{q} \right\rfloor - 1\right) f(q) - f(r) > \frac{f(q)}{q}, \tag{31}$$

which completes the proof. □

Lemma 2 establishes a range of costs of protection for which the effects of network design are very limited. By the lemma, if costs of protection are between $d_2(n)$ and $d_3(n)$, then the only equilibrium protection that can be obtained on any network is either full protection or no protection. Depending on the value of connections (as captured by f) and the number of nodes, n, the range of costs where a centrally protected star is the first best, $(c_1(n), c_3(n))$, and the range of costs where equilibrium protection is either empty or full, $(d_2(n), d_3(n))$, may overlap, in which case we face either under or over-protection.

Lemma 2. *Let (G, Δ, ξ) be an equilibrium of Γ.*

(i). If $d_2(n) < c < d_3(n)$ then either $\Delta = V$ and G is connected, or $\Delta = \varnothing$.

(ii). If $c > d_3(n)$ then $\Delta = \varnothing$.

Proof. Let (G, Δ, ξ) be an equilibrium of Γ.

We proceed in two steps. First, we show that if $d_2(n) < c$ then it must be that either $\Delta = \varnothing$ or $\Delta = V$ and G is connected.

Suppose that $d_2(n) < c$. Assume, to the contrary, that $\varnothing \subsetneq \Delta \subsetneq V$ or $\Delta = V$ and G is not connected. Thus there exists a protected node, $j \in \Delta$ such that the largest component of j in the residual network, after the attack of A is executed, has size $m \leq n-1$. Hence the expected payoff to j satisfies

$$U^j(G, \Delta, \xi) \leq \frac{f(m)}{m} - c \leq \frac{f(n-1)}{n-1} - c, \tag{32}$$

as $\frac{f(x)}{x}$ is increasing, by the fact that f is increasing and strictly convex. Since $U^j(G, \Delta, \xi) < 0$ so j is better off by deviating to no protection and getting payoff 0 or more. Thus (G, Δ, ξ) cannot be an equilibrium, a contradiction.

Second, we show that if $c > d_3(n)$, then $\Delta \neq V$. Assume to the contrary that $\Delta = V$. Expected payoff to any node $j \in V$ is

$$U^j(G, \Delta, \xi) \leq \frac{f(n)}{n} - c < 0, \tag{33}$$

as $c > d_3(n)$. Hence j is better off by deviating to no protection. A contradiction with the assumption that (G, Δ, ξ) is an equilibrium.

By the two steps above, if $c > d_3(n)$ then $\Delta = \varnothing$ (point 2), and if $d_2(n) < c < d_3(n)$ then either $\Delta = \varnothing$, or $\Delta = V$ and G is connected (point 1). This completes the proof. □

Now we are ready to prove Proposition 2.

Proof of Proposition 2. For point 1, suppose that $0 < c < \min(c_1(n), c_3(n))$ or $d_2(n) < c < c_2(n)$. Let G be a connected network and let (G, Δ, ξ) be a strategy profile such that $\Delta = V$ and $\xi(G', \Delta')$ is a best response to (G', Δ'), for any $G' \in \mathcal{G}(N)$ and $\Delta' \subseteq V$. Expected payoff to any node j from (G, Δ, ξ) is

$$U^j(G, \Delta, \xi) = \frac{f(n)}{n} - c > 0, \tag{34}$$

as $c < f(n)/n$. Deviation by j to no protection results in j being eliminated and yields payoff equal to 0. Hence (Δ, ξ) is an equilibrium of $\Gamma(G)$.

If $0 < c < \min(c_1(n), c_3(n))$ then, by Proposition 1, (G, Δ) is the first best, and so it is a welfare maximising equilibrium of Γ. If $d_2(n) < c < c_2(n)$ then, by Lemma 2, in any other equilibrium outcome no node protects. By Proposition 1 connected network with full protection is better than optimal disconnected network with no protection when $c < c_2(n)$.

For point 2, suppose that $c_1(n) < c < d_2(n)$. Let G be a star over V with centre $j \in V$. Let (G, Δ, ξ) be a strategy profile with $\Delta = \{j\}$ and ξ such that $\xi(G, \Delta)$ is a uniform distribution on $V \setminus \{j\}$, and $\xi(G', \Delta')$ is a best response to (G', Δ'), for any $G' \in \mathcal{G}(N) \setminus \{G\}$ and $\Delta' \in 2^V \setminus \{\Delta\}$. Expected payoff to node j from (G, Δ, ξ) is

$$U^j(G, \Delta, \xi) = \frac{f(n-1)}{n-1} - c. \tag{35}$$

Deviating to no protection yields payoff 0 to j. Since $c < d_2(n)$, the deviation is not profitable. Expected payoff to any node $k \neq j$ is

$$U^k(G, \Delta, \xi) = \left(\frac{n-2}{n-1}\right)\left(\frac{f(n-1)}{n-1}\right). \tag{36}$$

Deviating to protection is profitable for k if

$$c < \left(\frac{1}{n-1}\right)\left(\frac{f(n-1)}{n-1}\right). \tag{37}$$

Since

$$\left(\frac{1}{n-1}\right)\left(\frac{f(n-1)}{n-1}\right) < \frac{f(n) - f(n-1)}{n-1} < c, \tag{38}$$

as $\frac{f(n)}{n} > \frac{f(n-1)}{n-1}$, so the deviation is not profitable. Hence (Δ, ξ) is an equilibrium of $\Gamma(G)$. By Proposition 1, (G, Δ) is the first best, and so it is a welfare maximising equilibrium of Γ.

For point 3, suppose that $\max(d_2(n), c_2(n)) < c$ or $\max(c_2(n), c_3(n)) < c$. Let G be a disconnected network with sizes of components as stated in the proposition. Let (G, Δ, ξ) be a strategy profile such that $\Delta = \varnothing$ and $\xi(G, \Delta)$ is a uniform distribution on the nodes in components of size q, and $\xi(G', \Delta')$ is a best response to (G', Δ'), for any $G' \in \mathcal{G}(N)$ and $\Delta' \subseteq V$. Clearly no node has incentive to protect in the component of size $n \bmod q$ (if such component exists), as it is never attacked. Take any $j \in V$ such that j is in a component of size q. If unprotected, j is removed with probability $1/\lfloor \frac{n}{q} \rfloor$. Expected payoff to j from (G, Δ, ξ) is

$$U^j(G, \Delta, \xi) = \left(1 - \frac{1}{\left\lfloor \frac{n}{q} \right\rfloor}\right) \frac{f(q)}{q}, \tag{39}$$

Deviation by j to protection results in diverting attacks of the adversary to other components and yields j expected payoff

$$U^j(G, \Delta \cup \{j\}, \xi) = \frac{f(q)}{q} - c \leq \frac{f(n-1)}{n-1} - c, \tag{40}$$

as $q \leq \lfloor \frac{n}{2} \rfloor \leq n-1$. If $c > \max(d_2(n), c_2(n))$, then the expected payoff after the deviation is negative and so j does not have incentive to deviate. Suppose that $c > \max(c_2(n), c_3(n))$. We will show that, for all $1 \leq q \leq \lfloor \frac{n}{2} \rfloor$,

$$\max(c_2(n,q), c_3(n,q)) > \left(\frac{1}{\left\lfloor \frac{n}{q} \right\rfloor}\right) \frac{f(q)}{q} = \left(\frac{q}{n-r}\right) \frac{f(q)}{q}, \tag{41}$$

where $r = n \bmod q$. This, together with $c > \max(c_2(n), c_3(n))$, implies that $U^j(G, \Delta, \xi) > U^j(G, \Delta \cup \{j\}, \xi)$, so deviation to protection is not profitable. If $q = 1$ then $c_2(n, q) > RHS$, as

$$\frac{f(n) - (n-1)f(1)}{n} > \frac{f(1)}{n}. \tag{42}$$

If $q \geq 2$ then $c_3(n, q) > LHS$, by Observation 1 and the fact that $q < n - r$, as $q \leq \lfloor \frac{n}{2} \rfloor$. Hence no node has incentive to deviate to protection and (Δ, ξ) is an equilibrium of $\Gamma(G)$. □

A.3 Welfare minimising equilibria

In this part of the Appendix we provide proofs of the main results on welfare minimising equilibri. We start with a lemma that identifies the limits to what network design can achieve when all possible equilibria are considered.

Lemma 3. *(i). If $c < d_0$ then for any network G the game $\Gamma(G)$ has an equilibrium (Δ, ξ) where $\Delta = V$.*

(ii). If $c < d_3(n)$ then for any connected network G the game $\Gamma(G)$ has an equilibrium (Δ, ξ) where $\Delta = V$.

(iii). If $c > d_2(n)$ then for any network G the game $\Gamma(G)$ has a n equilibrium (Δ, ξ) where $\Delta = \varnothing$.

Proof. For point (i), let $c < d_0$ and let $G \in \mathcal{G}(V)$ be any network. Assume, to the contrary, that in any equilibrium (Δ, ξ) of $\Gamma(G)$, $\Delta \subsetneq V$. Pick any equilibrium (Δ, ξ) of $\Gamma(G)$ with pure attack strategy ξ (by Lemma 1 such an equilibrium exists). Let $j \in V \setminus \Delta$ be the unprotected node attacked by $\xi(\Delta)$ with probability 1. Deviating to protection, j would obtain payoff at least $f(1) - c > 0$ instead of 0. A contradiction with the assumption that (Δ, ξ) is an equilibrium. This shows point (i).

For point (ii), let $c < d_3(n)$ and let $G \in \mathcal{G}(V)$ be a connected network over V. Consider a strategy profile (Δ, ξ) such that $\Delta = V$ and for any Δ', $\xi(\Delta')$ is a best response to Δ'. Take any node $j \in V$. Deviation to no protection by j results in getting attacked and obtaining payoff $0 < \frac{f(n)}{n} - c$. Hence no node has incentive to deviate and (Δ, ξ) is an equilibrium of $\Gamma(G)$. This shows point (ii).

For point (iii), let $c > d_2(n)$ and let $G \in \mathcal{G}(V)$ be any network. By Lemma 2, if G is not connected, then in every equilibrium outcome there are no protected nodes in this range of costs. Suppose that G is connected and consider a strategy profile (Δ, ξ) such that $\Delta = \varnothing$ and $\xi(\Delta')$ maximises the damage to the network, for all $\Delta' \subseteq V$. Pick any node $j \in V$ and suppose that j deviates to protection. The adversary attacks an unprotected node and the value of the residual network is at most $\frac{f(n-1)}{n-1} = d_2(n) > c$. Hence such a deviation is not profitable and (Δ, ξ) is an equilibrium. □

Now we are ready to prove the results for the three ranges of costs of defence: low, intermediate and high.

A.3.1 Low costs of defence

Before proving the main result for this section (Proposition 3), we prove three auxiliary lemmata. Lemma 4 states that existence of k-critical node with $k \geq h^{-1}(c)$ in a connected network $G \in \mathcal{G}(V)$ is a necessary condition for having full protection in any equilibrium outcome of $\Gamma(G)$.

Lemma 4. *Let $G \in \mathcal{G}(V)$ be a connected network and $c > 0$. If $\Delta = V$ for any equilibrium (Δ, x) of $\Gamma(G)$, then there exists a k-critical node in G with $k \geq h^{-1}(c)$.*

Proof. Let $G \in \mathcal{G}(V)$ be a connected network over V. For a contradiction, suppose there is no k-critical node with $k \geq h^{-1}(c)$ in G. Consider the strategy profile (Δ, ξ) in which no node protects. Pick any node $i \in V$. If i does not protect, it gets an expected payoff 0. If i protects, it gets an expected payoff of $U^i(G, \Delta, \xi(\Delta)) < \frac{f(k_i)}{k_i} - c$, where k_i is the

size of the largest component in $G - \{i\}$. Since there is no k-critical node with $\frac{f(k)}{k} \geq c$ so $U^i(G, \Delta, x(\Delta)) < 0$. Therefore (Δ, ξ) is an equilibrium of $\Gamma(G)$. □

Lemma 5 below provides a sufficient condition on the network topology that guarantees full protection as the unique equilibrium outcome.

Lemma 5. *Let $G \in \mathcal{G}(V)$ be a connected network and $c > 0$. If there exists $i \in V$ such that sizes of components in $\mathcal{C}(G - \{i\})$ are an (h, c)-partition of $n - 1$ and for all $j \in V \setminus \{i\}$, j has a link to i, then in any equilibrium (Δ, ξ) of $\Gamma(G)$, $\Delta = V$.*

Proof. Let G be a network over V and let $i \in V$ be a node such that sizes of components in $\mathcal{C}(G - \{i\})$ are an (h, c)-partition of $n - 1$, and for all $j \in V \setminus \{i\}$, j has a link to i. Let s be the maximal size of a component in $\mathcal{C}(G - \{i\})$.

Let (Δ, ξ) be an equilibrium of $\Gamma(G)$. Assume, to the contrary, that $\Delta \subsetneq V$. Notice first that $i \in \Delta$. This is because if i does not protect, then it gets eliminated with probability 1 by any best response to Δ, as it is connected to all other nodes in the network. If i protects, then any attack by the adversary leaves the network connected. In any best response to Δ, the adversary mixes across the nodes in maximal size components of $G - \Delta$. The value of residual network after the attack is at least $f(n - s)$. Hence payoff to i from protections is $h(n - s) - c$. Since the sizes of components in $\mathcal{C}(G - \{i\})$ are (h, c)-partition of $n - 1$ and there are $m \geq 1$ components of sizes at least s so $m \leq \frac{h(n-s)}{c}$. Hence $h(n - s) \geq c$ and i prefers to protect (in the case of equality, the tie breaking assumption applies).

Thus we know that $i \in \Delta$. Now we will show that there exist nodes in $V \setminus \Delta$ that are better off by protecting. Let s' be the maximal size of component in $\mathcal{C}(G - \Delta)$ and let m' be the number of such components. Any component of size s' in $\mathcal{C}(G - \Delta)$ must be a subset of a component of size at least s' in $\mathcal{C}(G - \{i\})$. Since sizes of components in $\mathcal{C}(G - \{i\})$ are (h, c)-partition of $n - 1$, so

$$m' \leq \frac{h(n - s')}{c}. \tag{43}$$

On the other hand, there exists node j in a component of size s' that is eliminated with probability at least $\frac{1}{m'}$ by $\xi(\Delta)$. If j is not eliminated, the adversary removes s' nodes from the network without disconnecting it and j obtains payoff $h(n - s')$. Expected payoff to j is then

$$\left(1 - \frac{1}{m'}\right) h(n - s'). \tag{44}$$

If j protects, s/he is not eliminated and the adversary removes at most s' nodes from G without disconnecting it. Expected payoff to j is at least $h(n - s') - c$. Since being unprotected is preferred so

$$m' > \frac{h(n - s')}{c} \tag{45}$$

This contradicts (43) and so it must be that $\Delta = V$. □

The construction in Lemma 5 depends on the value of connections given by f, as it requires using a (h, c)-partition of the set of $n-1$ nodes. The lemma below provides sufficient and necessary condition on function f that allows existence of connected networks where full protection is unique equilibrium defence. Moreover, if such a network exists, then the construction from Lemma 5 is feasible.

Lemma 6. *Let $c > 0$ and f be an increasing and strictly convex function with $f(0) = 0$. $\mathcal{G}^f(n, c) \neq \varnothing$ if and only if*

$$\sum_{j=1}^{n-1} \left\lfloor \frac{h(j)}{c} \right\rfloor \geq n-1. \tag{46}$$

Moreover, if (46) is satisfied, then there exists a (h, c)-partition of $n-1$.

Proof. For the left to right implication, assume that there exists a network $G \in \mathcal{G}(V)$ such that for any equilibrium (Δ, ξ) of $\Gamma(G)$, $\Delta = V$. By Lemma 4, there exists a z-critical node in G with $z \geq h^{-1}(c)$. Take any such node and call it i. Consider a sequence of nodes, $i_1, \ldots, i_n$ and a corresponding sequence of defence profiles, $\Delta^1, \ldots, \Delta^n$, such that $i_1 = i$, $\Delta^k = \{i_1, \ldots, i_k\}$, for all $k \in \{1, \ldots, n\}$, and i_{k+1} belongs to a maximal size component of $G - \Delta^k$ and is a neighbour of a node in Δ^k. Notice that, by this construction, $\Delta^n = V$. Given $k \in \{1, \ldots, n-1\}$, let s_k be the size of maximal component in $\mathcal{C}(G - \Delta^j)$, and m_k be the number of components of size s_k in $\mathcal{C}(G - \Delta^k)$. By the construction above, $G[\Delta^k]$ is a connected subgraph of G and best response to Δ^k removes s_k nodes from G without disconnecting it. The value of residual network after such attack is $f(n - s_k)$.

We will first show that

$$m_k \leq \left\lfloor \frac{h(n - s_k)}{c} \right\rfloor, \tag{47}$$

for all $k \in \{1, \ldots, n-1\}$. Take any $k \in \{1, \ldots, n-1\}$. Since full protection is the only equilibrium defence on G so Δ^k cannot be an equilibrium defence. Thus either there exists $j \in \Delta^k$ such that j is strictly better off by dropping protection or there exists $j \in V \setminus \Delta^k$ such that j is better off by choosing protection. We will argue that only the latter is possible. For assume otherwise, i.e. that there exists $j \in \Delta^k$ such that j is strictly better off by dropping protection. Let $Z \subseteq \Delta^k$ be a maximal set of nodes such that for all $j' \in Z$, $\Phi(G - C_{j'}(G - (\Delta^k \setminus Z))) \leq f(n - s_k)$ (i.e. the adversary is weakly better off by attacking a maximal component in $G - \Delta^k$ rather than attacking j'). There exists a non-empty such Z that contains j. Moreover, by the construction of Z, there exists an equilibrium of $\Gamma(G)$, (Δ', ξ') such that $\Delta' = \Delta^k \setminus Z$ and $\xi'(\Delta')$ attacks a maximal component in $G - \Delta^k$ with probability 1 (and so does not attack any node in Z). A contradiction with the assumption that full protection is the only equilibrium defence in $\Gamma(G)$. This shows that there must exist $j \in V \setminus \Delta^k$ such that j is better off by choosing protection. Node j must be an element of a maximal component in $G - \Delta^k$ (the nodes in other components of Δ^k are not attacked in any best response to Δ^k). Suppose that $m_k \geq 2$, so that there are at least two components in $G - \Delta^k$ of maximal size. Then j protecting diverts the adversary

to attacking another maximal component in $G - \Delta^k$ and payoff to j is $h(n - s_k) - c$. This is strictly better to no protection if

$$\left(\frac{m_k - 1}{m_k}\right) h(n - s_k) \leq h(n - s_k) - c \tag{48}$$

from which we get

$$m_k \leq \frac{h(n - s_k)}{c} \tag{49}$$

and, sine $m_k \in \mathbb{N}$, (47) follows (for $m_k \geq 2$). The inequality holds for $m_k = 1$ as well, by the following argument. Since $i_1 = i$ is a z-critical node with $z \geq h^{-1}(c)$ so $h(n - s_1) \geq c$ and, further, $\lfloor \frac{h(n-s_1)}{c} \rfloor \geq 1$. Since h is strictly increasing and $s_k \leq s_1$, for all $k \in \{1, \ldots, n-1\}$, so $\lfloor \frac{h(n-s_k)}{c} \rfloor \geq 1$.

With Inequality (47) in hand, we are ready to establish Inequality (46). Let $M : \mathbb{N} \to \mathbb{N}$ be a function such that

$$M(x) = \begin{cases} \max_{\substack{j \in \{1,\ldots,n-1\} \\ s_j = x}} m_j & \text{if } x = s_j \text{ for some } j \in \{1, \ldots, n-1\} \\ 0, & \text{otherwise.} \end{cases} \tag{50}$$

By the definition of M, $\sum_{x=1}^{n-1} M(x) = n - 1$. This is because for every node i_k in the sequence $i_1, \ldots, i_{n-1}$, either a new maximal size s_k appears or the maximal size $s_k = s_{k-1}$ and the same maximal size s_k stays for m_k nodes in the sequence. Moreover, for all $x \in \{1, \ldots, n-1\}$, $M(x) \leq \lfloor \frac{h(n-x)}{c} \rfloor$. This is because it is either $M(x) = 0 \leq \lfloor \frac{h(n-x)}{c} \rfloor$ or there exists $k \in \{1, \ldots, n-1\}$ such that $s_k = x$ and Inequality (47) applies.

Since for all $x \in \{1, \ldots, n-1\}$, $M(x) \leq \lfloor \frac{h(n-x)}{c} \rfloor$, so

$$\sum_{j=1}^{n-1} \left\lfloor \frac{h(j)}{c} \right\rfloor = \sum_{j=1}^{n-1} \left\lfloor \frac{h(n-j)}{c} \right\rfloor \geq \sum_{j=1}^{n-1} M(j) = n - 1. \tag{51}$$

This shows the left to right implication.

For the right to left implication it is enough to show that if Inequality (46) holds, then there exists a (h, c)-partition of $n - 1$. This, together with Lemma 5 implies the result. So suppose that Inequality (46) holds. As we observed above, it can be rewritten as

$$\sum_{j=1}^{n-1} \left\lfloor \frac{h(n-j)}{c} \right\rfloor \geq n - 1. \tag{52}$$

It follow that there exists $m \in \{1, \ldots, n-1\}$ such that

$$s^* = \min \left\{ s \in \{1, \ldots, n-1\} : \sum_{j=1}^{s} \left\lfloor \frac{h(n-j)}{c} \right\rfloor \geq n - 1 \right\} \tag{53}$$

and

$$r = \left(\sum_{j=1}^{s^*} \left\lfloor \frac{h(n-j)}{c} \right\rfloor \right) - n + 1. \tag{54}$$

Consider function $p : \mathbb{N} \to \mathbb{N}$ defined as follows:

$$p(j) = \begin{cases} \left\lfloor \frac{h(n-j)}{c} \right\rfloor - \left\lfloor \frac{h(n-j-1)}{c} \right\rfloor, & \text{if } j \leq s^* - 2 \\ \left\lfloor \frac{h(n-j)}{c} \right\rfloor - r, & \text{if } j = s^* - 1 \\ r & \text{if } j = s^* \\ 0 & \text{otherwise.} \end{cases} \tag{55}$$

Function p defines a partition of $n-1$ in the following way: for each $j \in \mathbb{N}$, there are $p(j)$ parts of size j (if $p(j) > 0$) or there are not such parts (otherwise). In particular, the largest part has size at most s^*. To see that thus defined partition is indeed a partition of $n-1$ notice that

$$\begin{aligned} \sum_{j=1}^{s^*} j \cdot p(j) = &\sum_{j=1}^{s^*-2} j \cdot \left(\left\lfloor \frac{h(n-j)}{c} \right\rfloor - \left\lfloor \frac{h(n-j-1)}{c} \right\rfloor \right) + \\ &(s^* - 1) \cdot \left(\left\lfloor \frac{h(n-s^*+1)}{c} \right\rfloor - r \right) + s^* \cdot r \\ = &\sum_{j=1}^{s^*-1} \left\lfloor \frac{h(n-j)}{c} \right\rfloor + r = n - 1. \end{aligned} \tag{56}$$

Moreover, the partition is also a (h, c)-partition, because for any $s \in 1, \ldots, s$, the number of parts of size at least s is

$$\begin{aligned} \sum_{j=1}^{s^*} p(j) = &\sum_{j=1}^{s^*-2} \left(\left\lfloor \frac{h(n-j)}{c} \right\rfloor - \left\lfloor \frac{h(n-j-1)}{c} \right\rfloor \right) + \left(\left\lfloor \frac{h(n-s^*+1)}{c} \right\rfloor - r \right) + r \\ = &\left\lfloor \frac{h(n-s)}{c} \right\rfloor. \end{aligned} \tag{57}$$

This completes the proof. □

Now we are ready to prove Proposition 3.

Proof of Proposition 3. Points 2 and 3 follow directly from the discussion at the beginning of the paragraph on securing full protection (in the case of point 3, $\Delta = \varnothing$ follows from Lemma 2). Point 1 follows from Lemmata 5 and 6. □

A.3.2 Intermediate costs of defence

Proof of Proposition 4. We show point 2 only. All the remaining points are direct corollaries from Lemmata 2 and 3 and Proposition 1.

Let $\max(c_1(n), d_0) < c < d_2(n)$ and let (G, Δ, ξ) be a welfare minimizing equilibrium with $\Delta(G) \subsetneq V$. Notice that since $c < d_2(n) = \frac{f(n-1)}{n-1}$ and $\frac{f(x)}{x}$ is increasing (as f is increasing and strictly convex), so if G contains a component of size m such that

$\frac{f(m)}{m} < c$ then G must be disconnected. Thus it is enough to show that G contains such a component.

Suppose, to the contrary, that for all $C \in \mathcal{C}(G)$, $\frac{f(|C|)}{|C|} \geq c$. Let G' be a star network over V. We will show that G' is a better response to (Δ, ξ) than G.

Let $U^* = U^{\mathsf{D}}(G, \Gamma(G), \xi(G, \Gamma(G)))$ denote the expected payoff to D on the equilibrium path. Let (Δ', ξ') be a strategy profile of $\Gamma(G)$ where $\Delta' = V$ and $\xi'(\Delta)$ maximises the utility of A, for all $\Delta \subseteq V$. Since $\frac{f(|C|)}{|C|} \geq c$, for all $C \in \mathcal{C}(G^*)$, so no node has incentive to deviate to no protection and (Δ', ξ') is an equilibrium of $\Gamma(G)$. Since (G, Δ, ξ) is welfare minimising equilibrium, (Δ', ξ') yields at least as high payoff to the designer as $(\Delta(G), \xi(G, \cdot))$ in $\Gamma(G)$. Thus $U^* < f(n) - nc$. Switching to G' yields payoff $f(n) - nc$ (in the worst equilibrium, for the range of costs under consideration). This is strictly better then G, a contradiction. Thus G must have a component $C \in \mathcal{C}(G)$ with $\frac{f(|C|)}{|C|} < c$. □

A.3.3 High costs of defence

We start with the observation that $d_0 < c_3(n)$ for every strictly increasing and strictly convex f and sufficiently large n.

Observation 2. *Let f be a strictly increasing and strictly convex function with $f(0) = 0$. There exists $n^* \geq 0$ such that for all $n \geq n^*$, $c_3(n) > d_0$.*

Proof. Let f be a function satisfying the assumption of the observation. We start by showing that

$$f(x) > (x+1)f(1) \tag{58}$$

for sufficiently large x. Let $l(x) = (f(2) - f(1))x + 2f(1) - f(2)$. It is easy to verify that $l(1) = f(1)$ and $l(2) = f(2)$. Since f is strictly strictly convex, so

$$\left(\frac{1}{x-1}\right) f(x) + \left(\frac{x-2}{x-1}\right) f(1) > f\left(\left(\frac{x}{x-1}\right) + \left(\frac{x-2}{x-1}\right)\right) = f(2) \tag{59}$$

for all $x \geq 2$. Reorganizing we get $f(x) > l(x)$, for all $x \geq 2$. Since $l(x) \geq (x+1)f(1)$ for all $x \geq \frac{f(2)-f(1)}{f(2)-2f(1)}$ so

$$f(x) > (x+1)f(1) \tag{60}$$

for all $x \geq \max(x, \frac{f(2)-f(1)}{f(2)-2f(1)})$. Taking $x := n-1$ and $q := 1$ this is equivalent to

$$qf(n-1) > (n-q+1)f(1), \tag{61}$$

which is Equation (28) in proof of Observation 1 and the remaining argument there yields the result. □

Now we are ready to prove Proposition 5.

Proof of Proposition 5. Point 1 follows from point 2 of Proposition 4. For point 2 let G be the first best network for high costs of protection, as stated in the proposition. If $q \geq 2$ then, by Observation 1, no node has incentive to protect in a component of size q. If $q = 1$ then no node has incentive to protect by the fact that $c > d_0$. □

A.4 The price of decentralization

We start with the observation that that thresholds values for costs of protection, $d_1(n)$, $d_2(n)$, and $d_3(n)$, all converge to $\frac{f(n)}{n}$ – the utility a single node gets from a connected network over n nodes.

Observation 3. $\lim_{n\to+\infty} d_1(n) = \lim_{n\to+\infty} d_2(n) = \lim_{n\to+\infty} d_3(n) = \lim_{n\to+\infty} \frac{f(n)}{n}$.

Proof. Seeing that $\lim_{n\to+\infty} d_2(n) = \lim_{n\to+\infty} d_3(n) = \lim_{n\to+\infty} \frac{f(n)}{n}$ is immediate. In the remaining part of the proof we show that $lim_{n\to+\infty} d_1(n) = \lim_{n\to+\infty} \frac{f(n)}{n}$.

Let $h(n) = \frac{f(n)}{n}$. Notice first that since $h(n)$ is increasing and non-negative, so there exists $p \in \mathbb{R}_{++} \cup \{+\infty\}$ such that $\lim_{n\to+\infty} h(n) = p$. To show the claim, we show first that $d_1(n) \leq h(n)$, for all $n \geq 1$. Let $H(n,c) = \sum_{j=1}^{n-1} \lfloor \frac{h(j)}{c} \rfloor$. Notice that $H(n, h(n)) = 0 \leq n-1$, for all $n \geq 1$. Hence $d_1(n) \leq h(n)$.

Second, we show that for all $c < p$, there exists $n^*(c)$ such that for all $n > n^*(c)$, $d_1(n) > c$. This, together with the fact that $d_1(n)$ is bounded from above by $h(n)$ and $\lim_{n\to+\infty} h(n) = p$ proofs the claim. Since $p > c$ so there exists $\underline{n}(c)$ such that for all $n > \underline{n}(c)$, $h(n) > c$. We will show that in this case there exists $n^*(c)$ such that $d_1(n) > c$ for $n > n^*(c)$. Notice that $H(n+1,c) - H(n,c) = \lfloor \frac{h(n)}{c} \rfloor > 1$ if $n > \underline{n}(c)$. Thus if $n > \underline{n}(c)$ then $H(n,c)$ grows faster than $n-1$ and so there exists $n^*(c)$ such that for all $n > n^*(c)$, $H(n,c) > n-1$. Consequently, $d_1(n) > c$ for all $n > n^*(c)$. This completes the proof. □

Now we are ready to prove Theorem 1.

Proof of Theorem 1. Point 1 follows directly from the discussion at the beginning of Section 3.3.

For point 2, suppose that $\lim_{n\to+\infty} \frac{f(n)}{n} = p \leq c$. Since $\frac{f(n)}{n}$ is increasing, so $\frac{f(n)}{n} < c$ for all $n \geq 0$. Moreover, $\lim_{n\to+\infty} \frac{f(n)-f(n-1)}{n-1} = 0$. Thus $c_1(n) < c$ (for sufficiently large n). and $c_2(n) < d_3(n) < c$. Hence either $c \in (c_2(n), c_3(n))$, in which case centrally protected star is the first best, or $c > c_3(n)$, in which case a disconnected network with full protection is the first best. Moreover, since $d_2(n) < c$ so no node protects in every equilibrium on the first best disconnected network. Thus choosing the first best disconnected network we either obtain $\mathrm{PoS}(n,c) = \mathrm{PoA}(n,c) = 1$, if $c > c_3(n)$, or centrally protected star is the first best and the first best disconnected network yields payoff at least as high as fully disconnected network. Thus

$$\mathrm{PoS}(c,n), \mathrm{PoA}(c,n) \lesssim \lim_{n\to+\infty} \frac{f(n-1)-c}{(n-1)f(1)} = \frac{p}{f(1)}, \text{ when } n \to +\infty. \tag{62}$$

For point 3, suppose that $\lim_{n\to+\infty} \frac{f(n)}{n} = p < +\infty$ and $p > c$. Like for point 2 above, we start by observing that $\frac{f(n)}{n} < p$ for all $n \geq 0$ and $\lim_{n\to+\infty} \frac{f(n)-f(n-1)}{n-1} = 0$. Thus $c > c_1(n)$. If $c > \max(c_2(n), c_3(n))$ then, by Observation 2, for sufficiently large n, choosing the first best disconnected network we obtain no protection in every equilibrium

and so $\text{PoS}(n,c) = \text{PoA}(n,c) = 1$. If $c_1(n) < \max(c_2(n), c_3(n))$ then centrally protected star is the first best. By Observation 3, for sufficiently large n, $d_1(n) > c$ so D can secure full protection in every equilibrium by choosing a network from $\mathcal{G}^f(n,c)$. Thus

$$\begin{aligned}\text{PoS}(c,n), \text{PoA}(c,n) \lesssim & \lim_{n\to+\infty} \frac{f(n-1)-c}{f(n)-nc} = \lim_{n\to+\infty} \frac{1-\left(\frac{n-1}{f(n)}\right)\left(\frac{f(n)-f(n-1)}{n-1}\right)-\frac{c}{f(n)}}{1-\left(\frac{n}{f(n)}\right)c} \\ = & \frac{p}{p-c}, \text{ when } n \to +\infty. \end{aligned} \tag{63}$$

For point 4, suppose that $\lim_{n\to+\infty} \frac{f(n)}{n} = +\infty$. We will show that in this case, either $\text{PoS}(n,c) = \text{PoA}(n,c) = 1$ or they get arbitrarily close to 1 when $n \to +\infty$.

If $c < \min(c_1(n), c_2(n), d_1(n))$ then, by Proposition 3, full protection can be secured on a connected network, and so first best outcome can be secured when defence is decentralized. Thus in this case $\text{PoS}(n,c) = \text{PoA}(n,c) = 1$. Similarly, if $c > \max(c_2(n), c_3(n))$ then, by Observation 2 and Proposition 5, first best outcome can be secured when defence is decentralized. Thus $\text{PoS}(n,c) = \text{PoA}(n,c) = 1$ in this case. Suppose that $\min(c_1(n), c_2(n), d_1(n)) < c < \max(c_2(n), c_3(n))$. By Observation 3, $\lim_{n\to+\infty} d_1(n) = \lim_{n\to+\infty} \frac{f(n)}{n} = +\infty$. Hence, for sufficiently large n and fixed c, $\min(c_1(n), c_2(n), d_1(n)) < c < \max(c_2(n), c_3(n))$ implies $\min(c_1(n), c_2(n)) < c < \max(c_2(n), c_3(n))$. Moreover, since either $c_1(n) < c_2(n) < c_3(n)$ or $c_3(n) < c_2(n) < c_1(n)$ so $\min(c_1(n), c_2(n)) < c < \max(c_2(n), c_3(n))$ implies $c_1(n) < c < c_3(n)$. Lastly, since $\lim_{n\to+\infty} d_2(n) = \lim_{n\to+\infty} \frac{f(n-1)}{n-1} = +\infty$ so, for sufficiently large n, $c_1(n) < c < \min(c_3(n), d_2(n))$. Hence we are in a range where centrally protected star is the first best and in any equilibrium on a star network either all nodes protect or the centre protects. Since the ratio of payoffs from fully protected star to payoffs from centrally protected star satisfies

$$\lim_{n\to+\infty} \frac{f(n-1)-c}{f(n)-nc} = \lim_{n\to+\infty} \frac{1-\left(\frac{n-1}{f(n)}\right)\left(\frac{f(n)-f(n-1)}{n-1}\right)-\frac{c}{f(n)}}{1-\left(\frac{n}{f(n)}\right)c} = 1. \tag{64}$$

(as $\frac{f(n)-f(n-1)}{n-1} = c_1(n) < c$) so

$$\lim_{n\to+\infty} \text{PoS}(c,n) = \lim_{n\to+\infty} \text{PoA}(c,n) = 1. \tag{65}$$

This completes the proof. □

B Continuous protection decisions

Consider an extension of our model where protection decisions are continuous: every node $i \in V$ chooses protection level $\delta_i \in [0,1]$ at cost $\delta_i c$. The protection level corresponds to

its robustness. An attacked node i with protection level δ_i gets removed with probability $(1-\delta_i)$ and stays intact with probability δ_i. In particular, protection level $\delta = 1$ means perfect protection and protection level $\delta = 0$ means no protection. We will use $\mathbf{1}$ to denote the full protection profile $(1,\ldots,1)$, where all nodes choose perfect protection, and $\mathbf{0}$ to denote the no protection profile $(0,\ldots,0)$, where all nodes choose no protection.

The network attack scenario involves stochastic spread of infection. A node gets attacked if either it is attacked directly by the adversary or one of its neighbours gets attacked and its protection fails. A node that is attacked and survives becomes immune to any subsequent indirect attacks. We denote the game with continuous protection decisions by Γ'.

Continuous protection decisions increase the set of choices of the defender in the centralized protection model and they also increase the set of strategy profiles in decentralized protection model. In the case of centralized protection model, this enriches the set of first best networks and makes the characterization of them a much more difficult problem. In particular, there are parameters f and c of the centralized protection game for which a network with partial protection is a better choice than any of the first best networks under binary protection decisions. Nevertheless, when costs of protection are sufficiently low or sufficiently high, the set of first best protected networks is the same as in the binary protection model. In the case of the model with decentralized protection decisions, continuous protection allows the nodes finer grained responses to defence decisions of other nodes. In effect, the over-protection problem becomes starker than in the case of binary protection model. In particular, unlike in the model with binary protection decisions, no protection defence profile is not an equilibrium defence profile on first best disconnected networks. On the other hand, the under-protection problem can be solved by similar means as in the case of the binary protection model: that is by choosing a network with a critical node and creating a cascade of incentives to protect. We elaborate on these observations below.

Consider the model with centralized protection first. Continuous protection decisions enrich the set of possible first best networks. In particular, it is possible that the first best protection levels involve protecting some of the nodes partially. Consider the following example. Let $f(x) = x^2$, $n = 4$, and $c > 2.25$. In this case $c < c_1(n) = 7/3$, hence in the model with binary protection decisions, first best is a fully protected connected network and the first best designer's payoff is 7. In the model with continuous protection, a star network where the centre receives protection 0.94 and each of the spokes receives protection 0.89 yields payoff ≈ 7.05 to the designer and dominates fully protected connected networks. Obtaining a full characterization of all the first best protected networks is beyond the scope of this paper and seems a hard problem. Still, if costs of protection are sufficiently low, a first best is a fully protected connected network and if costs of protection are sufficiently how, the first best disconnected networks with no protection from the binary protection model are exactly the first best protected networks in the continuous

protection model. This is stated in the observation below.

Observation 4. *Let $c > 0$, $q \in Q^*(n)$, and let $(G, \boldsymbol{\delta})$ be a first best protected network in the model with continuous protection. Then*

(i). G is connected and $\boldsymbol{\delta} = \mathbf{1}$, if $0 < c < \left(\frac{n-1}{n}\right) c_1(n)$.

(ii). G has $\lfloor \frac{n}{q} \rfloor$ components of size q and one component of size $n \bmod q$ (if $n \bmod q > 0$), and $\boldsymbol{\delta} = \mathbf{0}$, if $c > \frac{f(n)+(n-2)f(n-2)}{n} + f(n-1)$.

Proof. Given a strategy profile $\boldsymbol{\delta}$, let $\hat{\delta} = \min_{i \in V} \delta_i$ and $\bar{\delta} = \sum_{i \in V} \delta_i$. Suppose that $\hat{\delta} < 1$. Notice that given defence profile $\boldsymbol{\delta}$, the value of the residual network after the attack of the adversary is at most

$$U^{\mathsf{D}}(G, \boldsymbol{\delta}) < \hat{\delta} f(n) + (1 - \hat{\delta}) f(n-1) - n\hat{\delta} c. \tag{66}$$

Thus if

$$f(n) - nc > \hat{\delta} f(n) + (1 - \hat{\delta}) f(n-1) - n\hat{\delta} c) \tag{67}$$

then a fully protected connected network is better than a partially protected network $(G, \boldsymbol{\delta})$. From this and by the fact that $1 - \hat{\delta} > 0$ we get

$$c < \frac{f(n) - f(n-1)}{n}. \tag{68}$$

Since this is less than $\min(c_1(n), c_2(n))$, the first point of the observation follows.

For the second point of the observation, we consider two cases separately: (a) $\bar{\delta} \geq 1$ and (b) $\bar{\delta} < 1$. For case (a), notice that if

$$c > \left(\frac{\hat{\delta}}{\bar{\delta}}\right) f(n) + \left(\frac{1 - \hat{\delta}}{\bar{\delta}}\right) f(n-1) \tag{69}$$

then

$$U^{\mathsf{D}}(G, \boldsymbol{\delta}) < \hat{\delta} f(n) + (1 - \hat{\delta}) f(n-1) - n\bar{\delta} c < 0 \tag{70}$$

and so the first best network with no protection from the binary protection model dominates $(G, \boldsymbol{\delta})$ in this case. Since $\bar{\delta} \geq n\hat{\delta}$, $\bar{\delta} \geq 1$ and $f(n) > f(n-1)$ so

$$\begin{aligned}\left(\frac{\hat{\delta}}{\bar{\delta}}\right) f(n) + \left(\frac{1 - \hat{\delta}}{\bar{\delta}}\right) f(n-1) &\leq \left(\frac{1}{n}\right) f(n) + \left(\frac{n-1}{n}\right) f(n-1) \\ &< \left(\frac{f(n) + (n-2) f(n-2)}{n}\right) + f(n-1)\end{aligned}$$

and so if $c > \left(\frac{f(n)+(n-2)f(n-2)}{n}\right) + f(n-1)$, the second point of the observation follows. For case (b) notice that

$$U^{\mathsf{D}}(G, \boldsymbol{\delta}) < \hat{\delta} f(n) + (1 - \hat{\delta}) \left(\check{\delta} f(n-1) + (1 - \check{\delta}) \sum_{j=1}^{n-2} f(j) \delta^{(j)} \prod_{k=j+1}^{n-2} (1 - \delta^{(k)}) \right) - n\bar{\delta} c, \tag{71}$$

where $\delta^{(n-2)} \geq \ldots \geq \delta^{(1)}$. Furthermore, since $f(n-2) > \ldots > f(1)$ so

$$U^{\mathsf{D}}(G,\boldsymbol{\delta}) < \hat{\delta} f(n) + (1-\hat{\delta}) \left(\tilde{\delta} f(n-1) + (1-\tilde{\delta}) \sum_{j=1}^{n-2} f(j) \hat{\delta} \prod_{k=j+1}^{n-2} (1-\hat{\delta}) \right) - n\bar{\delta}c, \quad (72)$$

where $\tilde{\delta} = \bar{\delta} - (n-1)\hat{\delta}$. Thus if

$$c > \left(\frac{\hat{\delta}}{\bar{\delta}} \right) f(n) + (1-\hat{\delta}) \left(\left(\frac{\tilde{\delta}}{\bar{\delta}} \right) f(n-1) + (1-\tilde{\delta}) \left(\frac{\hat{\delta}}{\bar{\delta}} \right) \sum_{j=1}^{n-2} f(j)(1-\hat{\delta})^{n-j-2} \right), \quad (73)$$

then $U^{\mathsf{D}}(G,\boldsymbol{\delta}) < 0$ and the first best network with no protection from the binary protection model dominates $(G,\boldsymbol{\delta})$. Since $n\hat{\delta} \leq \bar{\delta}$, $\tilde{\delta} \leq \bar{\delta}$, $\hat{\delta} < 1$, and $\tilde{\delta} < 1$ so if

$$c > \left(\frac{1}{n} \right) f(n) + f(n-1) + \left(\frac{n-2}{n} \right) f(n-2), \quad (74)$$

then $U^{\mathsf{D}}(G,\boldsymbol{\delta}) < 0$ and the second point of the observation follows. □

When protection decisions are decentralized, part of the results from the model with binary protection model continue to hold in the model with continuous protection decisions. The main difficulty here comes from the lack of full characterization of the first best defended networks. Not knowing them, we do not know the optimal choices for different ranges of intermediate costs of defence. Nevertheless, by Observation 4, we know that if costs of defence are sufficiently low or sufficiently high, the same defended networks are first best in the binary and continuous model and we can check whether continuous protection decisions in the decentralized model affect the result.

The key fact here is that keeping the protection choices of other nodes and the attack choice of the adversary fixed, it is optimal for a node to either choose full protection or no protection.

Fact 1. *Let G be a network over a set of nodes V, $j \in V$ be a node, $\xi \in \mathcal{L}(V)$ be a mixed attack, and $\boldsymbol{\delta}_{-j}$ be a profile of protection decisions of the nodes different to j. If protection $\delta_j \in [0,1]$ maximises j's expected payoff, $U^j(G,(\delta_j,\boldsymbol{\delta}_{-j}),\xi)$, then, generically, $\delta_j \in \{0,1\}$.*

Proof. Let $\Psi_j(G \mid \xi, \boldsymbol{\delta}_{-j})$ denote the expected payoff to player j in G under ξ and $\boldsymbol{\delta}_{-j}$, conditioned on j being attacked (directly or not) and surviving. Let $\overline{\Psi}_j(G \mid \xi, \boldsymbol{\delta}_{-j})$ denote the expected payoff to player j in G under ξ and $\boldsymbol{\delta}_{-j}$, conditioned on j not being attacked (neither directly nor indirectly). Let $P_j(G \mid \xi, \boldsymbol{\delta}_{-j})$ be the probability that j is attacked (either directly or indirectly) in G under ξ and $\boldsymbol{\delta}_{-j}$. Expected payoff to node j from defence profile $\boldsymbol{\delta}$ and mixed attack ξ in G can be written as

$$U^j(G,\boldsymbol{\delta},\xi) = \delta_j P_j(G \mid \xi, \boldsymbol{\delta}_{-j}) \Psi_j(G \mid \xi, \boldsymbol{\delta}_{-j}) + (1 - P_j(G \mid \xi, \boldsymbol{\delta}_{-j}))\, \overline{\Psi}_j(G \mid \xi, \boldsymbol{\delta}_{-j}) - c\delta_j. \quad (75)$$

Clearly, keeping $\boldsymbol{\delta}_{-i}$ and ξ fixed, $U^j(G,\delta_i,\boldsymbol{\delta}_{-i},\xi)$ is maximised when either $\delta_j = 1$, in the case of $P_j(G \mid \xi, \boldsymbol{\delta}_{-j}) \Psi_j(G \mid \xi, \boldsymbol{\delta}_{-j}) > c$, or $\delta_j = 0$, otherwise. □

Consider welfare maximising equilibria first. Notice that when $c < f(n)/n = d_3(n)$ then any connected network has an equilibrium where all nodes protect. This is because any node j with protection level $\delta_j < 0$ and with other nodes having protection level 1, gets attacked and, by Fact 1, has an incentive to increase his protection to full protection. Thus if c is sufficiently low, the first best equilibrium protection can be attained in the best equilibrium and so there is no under-protection problem in this case, assuming that nodes and the adversary coordinate on the best equilibrium. Note however, that when $c > f(n)/n$ then, unlike in the binary model, there may be networks where in every equilibrium there are nodes that choose some positive level of protection. In particular, no protection is not an equilibrium defence outcome on the first best disconnected networks. This is because a node in a component attacked by the adversary with positive probability has an incentive to increase protection from 0 to an arbitrarily low $\varepsilon > 0$, which would divert the attack to a different component. Thus the possibility of choosing continuous protection by the nodes requires more care in design decisions. In particular, choosing a first best disconnected network for $n-1$ nodes and then adding one node to a maximal size component and making that increased component 2-connected, results in no protection being a unique equilibrium defence. This is because the adversary would attack the unique maximal size component and would continue to do so even if a single node chose a positive protection level.

Consider welfare minimising equilibria. Notice first that, by Fact 1, if $c < f(1) = \delta_0$ then, like in the model with binary protection decisions, every network has an equilibrium where all nodes protect. Hence the over-protection problem is unavoidable if full protection is not the first best for some cost $c < f(1)$. Notice that the range of such costs may be higher in the continuous model, because a network with partial protection may be better than a fully protected network for lower costs than in the case of the binary protection model. As we argued for the case of welfare maximising equilibria, if $c < d_3(n)$ then any connected network has an equilibrium where all nodes protect. This implies, like in the case of the binary protection model, that the only way to mitigate the over-protection problem, when $d_3(n)$ falls in the range of cost with partial protection in the first best, is by splitting the network. As we observed above, even if $c < f(n-1)/(n-1) = d_2(n)$, there may be networks where no protection is not an equilibrium. In particular, as we observed for the case of welfare maximising equilibrium, this is the case for the first best disconnected networks. This leads to an over-protection problem that requires more care in choosing the network than in the case of the model with discrete defence. Choosing disconnected networks as described above, for the welfare maximising equilibria, guarantees uniqueness of the no protection equilibrium but requires the designer to sacrifice some value of the network, when compared to the centralized defence case.

The under-protection problem for low costs of defence can be mitigated by network design in a similar way as in the case of the model with binary protection choices: by creating a cascade of incentives to protect. This can be done by constructing a π-windmill

network where partition π is such that the network has a k-critical node with $k \geq h^{-1}(c)$. Any such network has full protection as the unique equilibrium outcome if $c < d_1(n)$. Notice that this construction puts less constraints on the the partition π than in the case of the binary protection model. This is because continuous protection decisions allow the nodes to divert attacks to other nodes by increasing their protection slightly and this makes it easier to trigger the cascade of incentives to protect. The key results for this construction to work, in the case of binary protection decisions, are Lemmata 4 and 5. A straightforward adjustment to the proof of Lemma 4 shows that it holds for the case of continuous protection decisions as well. An analogue of Lemma 5 holds in the continuous protection model and we state and prove it below. The general idea of the proof is similar but it requires a considerable extension due to much larger space of possible defence profiles that continuous protection decisions allow.

Lemma 7. *Let $G \in \mathcal{G}(V)$ be a connected network and $c > 0$. If G is a π-windmill network with a k-critical node i where $k \geq h^{-1}(c)$, then in any equilibrium $(\boldsymbol{\delta}, \xi)$ of $\Gamma'(G)$, $\boldsymbol{\delta} = \mathbf{1}$.*

Proof. Let G be a π-windmill network with a k-critical node, i, where $k \geq h^{-1}(c)$. Thus the maximal size, s, of a component in $\mathcal{C}(G - \{i\})$ is such that $f(n-s)/(n-s) \geq c$, all nodes in $V \setminus \{i\}$ are connected to i and nodes in each component of $\mathcal{C}(G - \{i\})$ form a clique.

By Fact 1, the full protection profile $\boldsymbol{\delta} = \mathbf{1}$ is an equilibrium defence profile. This is because, given that all other nodes fully protect, any node with partial protection would be attacked by the adversary and would have an incentive to increase protection (because $c < f(n)/n$). We show that any other defence profile cannot be an equilibrium defence profile. We do it by showing that for partial defence profile there exists a node with an incentive to increase protection (clearly any such attacked node must have protection strictly below 1).

Before we proceed with the main part of the proof, we need to establish some properties of defence profile $\boldsymbol{\delta}$ when the adversary is indifferent between attacking the critical node i and some other node $j \neq i$. Given a natural number $m \geq 2$ and a defence profile $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_m)$, let $Z(m, \boldsymbol{\sigma})$ be a random variable whose realizations are the numbers of infected nodes in a clique of size m with protection $\boldsymbol{\sigma}$, after all the nodes are attacked directly with probability 1. The expected payoff to the adversary from attacking i is given by

$$\begin{aligned} U^{\mathsf{A}}(G, \boldsymbol{\delta}, i) = &- \delta_i f(n) - (1-\delta_i)\Bigg(\delta_j \mathbf{E}\left[f\left(|C_j| - Z\left(|C_j|-1, \boldsymbol{\delta}\right)\right)\right] + \\ &(1-\delta_j)\mathbf{E}\left[f\left(|C_j| - 1 - Z\left(|C_j|-1, \boldsymbol{\delta}\right)\right)\right] + \\ &\sum_{\substack{C \in \mathcal{C}(G-\{i\}) \\ C \neq C_j}} \mathbf{E}\left[f(|C| - Z(|C|, \boldsymbol{\delta}))\right]\Bigg) \end{aligned} \tag{76}$$

Similarly, the expected payoff to the adversary from attacking j is given by

$$U^{\mathsf{A}}(G,\boldsymbol{\delta},j) = -\delta_j f(n) - (1-\delta_j)\delta_i \mathbf{E}\left[f\left(n-1-Z\left(|C_j|-1,\boldsymbol{\delta}\right)\right)\right] - (1-\delta_j)\left(1-\delta_i\right)\left(\mathbf{E}\left[f\left(|C_j|-1-Z\left(|C_j|-1,\boldsymbol{\delta}\right)\right)\right] + \sum_{\substack{C\in\mathcal{C}(G-\{i\})\\ C\neq C_j}} \mathbf{E}\left[f(|C|-Z(|C|,\boldsymbol{\delta}))\right]\right). \tag{77}$$

where $C_j = C_j(G-\{i\})$ is the component of $G-\{i\}$ containing j. Equalizing the two payoffs and reorganizing, we get

$$\delta_j f(n) + (1-\delta_j)\delta_i \mathbf{E}\left[f\left(n-1-Z\left(|C_j|-1,\boldsymbol{\delta}\right)\right)\right] = \delta_i f(n) + \left(1-\delta_i\right)\delta_j\left(\mathbf{E}\left[f\left(|C_j|-Z\left(|C_j|-1,\boldsymbol{\delta}\right)\right)\right] + \sum_{\substack{C\in\mathcal{C}(G-\{i\})\\ C\neq C_j}} \mathbf{E}\left[f(|C|-Z(|C|,\boldsymbol{\delta}))\right]\right). \tag{78}$$

Two consequence of Equation (78) are key for further part of the proof. Firstly, dividing both sides of the equation by n and reorganizing, we get

$$\left(\delta_i-\delta_j\right)\left(\frac{f(n)}{n}\right) \leq (1-\delta_j)\delta_i \mathbf{E}\left[\frac{f\left(n-1-Z\left(|C_j|-1,\boldsymbol{\delta}\right)\right)}{n}\right]. \tag{79}$$

Secondly, Equation (78) implies that either $\delta_i=\delta_j=0$ or $\delta_i=\delta_j=1$ or $0<\delta_j<\delta_i<1$. For assume otherwise. Then either $\delta_j>\delta_i$ and $0<\delta_j=\delta_j<1$. If $\delta_j=\delta_i$ then LHS $>$ RHS because, by strict convexity of f and $f(0)=0$,

$$\mathbf{E}\left[f\left(n-1-Z\left(|C_j|-1,\boldsymbol{\delta}\right)\right)\right] > \mathbf{E}\left[f\left(|C_j|-Z\left(|C_j|-1,\boldsymbol{\delta}\right)\right)\right] + \sum_{\substack{C\in\mathcal{C}(G-\{i\})\\ C\neq C_j}} \mathbf{E}\left[f(|C|-Z(|C|-1,\boldsymbol{\delta}))\right] > \mathbf{E}\left[f\left(|C_j|-Z\left(|C_j|-1,\boldsymbol{\delta}\right)\right)\right] + \sum_{\substack{C\in\mathcal{C}(G-\{i\})\\ C\neq C_j}} \mathbf{E}\left[f(|C|-Z(|C|,\boldsymbol{\delta}))\right].$$

and $(1-\delta_j)\delta_i = (1-\delta_i)\delta_j > 0$, as $0<\delta_j<1$. In addition, $\partial\text{LHS}/\partial\delta_j > \partial\text{RHS}/\partial\delta_j$, because

$$f(n) > \mathbf{E}\left[f\left(n-1-Z\left(|C_j|-1,\boldsymbol{\delta}\right)\right)\right] > \delta_i \mathbf{E}\left[f\left(n-1-Z\left(|C_j|-1,\boldsymbol{\delta}\right)\right)\right] + \left(1-\delta_i\right)\left(\mathbf{E}\left[f\left(|C_j|-Z\left(|C_j|-1,\boldsymbol{\delta}\right)\right)\right] + \sum_{\substack{C\in\mathcal{C}(G-\{i\})\\ C\neq C_j}} \mathbf{E}\left[f(|C|-Z(|C|,\boldsymbol{\delta}))\right]\right).$$

and both LHS and RHS are continuous in δ_j. Hence LHS > RHS for $\delta_j > \delta_i$ as well. In both cases we get contradiction with (78). Thus it must be that

$$U^{\mathsf{A}}(G, \boldsymbol{\delta}, i) = U^{\mathsf{A}}(G, \boldsymbol{\delta}, i) \text{ implies } \delta_i = \delta_j = 0 \text{ or } \delta_i = \delta_j = 1 \text{ or } 0 < \delta_j < \delta_i < 1. \quad (80)$$

Notice also that increasing defence at a node decreases the utility of the adversary from attacking that node the most: for all $k, k' \in V$ such that $k \neq k'$,

$$\frac{\partial U^{\mathsf{A}}(G, \boldsymbol{\delta}, k)}{\partial \delta_k} < \frac{\partial U^{\mathsf{A}}(G, \boldsymbol{\delta}, k')}{\partial \delta_k}. \quad (81)$$

We show the inequality for the cases of $k = i$ and $k' = i$, the cases of $k, k' \neq i$ can be shown by similar arguments. By strict convexity of f:

$$\begin{aligned}
\frac{\partial U^{\mathsf{A}}(G, \boldsymbol{\delta}, i)}{\partial \delta_i} &= \sum_{\substack{C \in \mathcal{C}(G - \{i\}) \\ C \neq C_j}} \mathbf{E}\left[f(|C| - Z(|C|, \boldsymbol{\delta}))\right] + \delta_j \mathbf{E}\left[f\left(|C_j| - Z\left(|C_j| - 1, \boldsymbol{\delta}\right)\right)\right] + \\
&\qquad (1 - \delta_j)\mathbf{E}\left[f\left(|C_j| - 1 - Z\left(|C_j| - 1, \boldsymbol{\delta}\right)\right)\right] - f(n) \\
&< \sum_{\substack{C \in \mathcal{C}(G - \{i\}) \\ C \neq C_j}} \mathbf{E}\left[f(|C| - Z(|C|, \boldsymbol{\delta}))\right] + \mathbf{E}\left[f\left(|C_j| - Z\left(|C_j| - 1, \boldsymbol{\delta}\right)\right)\right] - f(n) \\
&< \sum_{\substack{C \in \mathcal{C}(G - \{i\}) \\ C \neq C_j}} \mathbf{E}\left[f(|C| - Z(|C|, \boldsymbol{\delta}))\right] + \mathbf{E}\left[f\left(|C_j| - 1 - Z\left(|C_j| - 1, \boldsymbol{\delta}\right)\right)\right] - f(n-1) \\
&< (1 - \delta_j)\Bigg(\sum_{\substack{C \in \mathcal{C}(G - \{i\}) \\ C \neq C_j}} \mathbf{E}\left[f(|C| - Z(|C|, \boldsymbol{\delta}))\right] + \mathbf{E}\left[f\left(|C_j| - 1 - Z\left(|C_j| - 1, \boldsymbol{\delta}\right)\right)\right] - \\
&\qquad \mathbf{E}\left[f\left(n - 1 - Z\left(|C_j| - 1, \boldsymbol{\delta}\right)\right)\right] \Bigg) = \frac{\partial U^{\mathsf{A}}(G, \boldsymbol{\delta}, j)}{\partial \delta_i}
\end{aligned}$$

$$\frac{\partial U^{\mathsf{A}}(G,\boldsymbol{\delta},j)}{\partial \delta_j} = \delta_i \mathbf{E}\left[f\left(n-1-Z\left(|C_j|-1,\boldsymbol{\delta}\right)\right)\right] + (1-\delta_i)\Bigg(\sum_{\substack{C\in\mathcal{C}(G-\{i\})\\ C\neq C_j}} \mathbf{E}\left[f(|C|-Z(|C|,\boldsymbol{\delta}))\right] +$$

$$\mathbf{E}\left[f\left(|C_j|-1-Z\left(|C_j|-1,\boldsymbol{\delta}\right)\right)\right]\Bigg) - f(n) = \delta_i\left(\mathbf{E}\left[f\left(n-1-Z\left(|C_j|-1,\boldsymbol{\delta}\right)\right)\right] - f(n)\right) +$$

$$(1-\delta_i)\left(\sum_{\substack{C\in\mathcal{C}(G-\{i\})\\ C\neq C_j}} \mathbf{E}\left[f(|C|-Z(|C|,\boldsymbol{\delta}))\right] + \mathbf{E}\left[f\left(|C_j|-1-Z\left(|C_j|-1,\boldsymbol{\delta}\right)\right)\right] - f(n)\right)$$

$$< (1-\delta_i)\Bigg(\sum_{\substack{C\in\mathcal{C}(G-\{i\})\\ C\neq C_j}} \mathbf{E}\left[f(|C|-Z(|C|,\boldsymbol{\delta}))\right] + \mathbf{E}\left[f\left(|C_j|-1-Z\left(|C_j|-1,\boldsymbol{\delta}\right)\right)\right] -$$

$$\mathbf{E}\left[f\left(|C_j|-Z\left(|C_j|-1,\boldsymbol{\delta}\right)\right)\right]\Bigg) = \frac{\partial U^{\mathsf{A}}(G,\boldsymbol{\delta},i)}{\partial \delta_j}$$

Now we are ready to proceed with the main part of the proof. Take some strategy profile $(\boldsymbol{\delta},\xi)$ with partial protection profile, $\boldsymbol{\delta}$, and suppose to the contrary, that it is an equilibrium of the subgame $\Gamma'(G)$. Given node $j \in V$, let $E(j) = \{k \in V \setminus \{j\} : U^{\mathsf{A}}(G,\boldsymbol{\delta},j) = U^{\mathsf{A}}(G,\boldsymbol{\delta},k)\}$ be the set of nodes that are equally good targets to the adversary as j. Let $j \in V$ be a node attacked with probability $\xi_j > 0$ under ξ. We consider a number of cases separately.

Suppose that $E(j) = \varnothing$. In this case, $\xi_j = 1$ and the expected payoff to j from being attacked with probability 1 is $U^j(G,\boldsymbol{\delta},j) = \delta_j\left(\frac{f(n)}{n}\right) - \delta_j c$. By continuity of the utility of the adversary in protection of nodes, there exists $\varepsilon > 0$ such that the adversary keeps attacking j after δ_j is increased by an amount smaller than ε. Since $f(n)/n > c$, node j has an incentive to increase his protection and so $\boldsymbol{\delta}$ cannot be an equilibrium protection in this case.

From now on we assume that $E(j) \neq \varnothing$, which means that the adversary has some targets as good as j to attack.

Suppose that for all $k \in E(j)$, $\delta_k = 0$, and that $\delta_i < 1$. This means that the adversary attacks nodes with no protection only and the central node is not fully protected. By continuity of the utility of the adversary in protection of nodes, there exists $\varepsilon > 0$ such that the adversary keeps attacking one of the nodes with no protection after δ_i is increased by an amount smaller than ε. Hence for all $\delta_i' \in [\delta_i, \delta_i + \varepsilon)$, node i is attacked (either directly or indirectly) with probability 1 under defence profile $(\delta_i', \boldsymbol{\delta}_{-i})$ and the expected payoff to i from a defence δ_i' is

$$U^i(G,(\delta_i',\boldsymbol{\delta}_{-i}),i) \geq \delta_i'\left(\frac{f(n-s)}{n-s}\right) - \delta_i' c, \tag{82}$$

where s is the maximal size of a component in $\mathcal{C}(G-\{i\})$. Since $f(n-s)/(n-s) \geq c$ so increasing protection to $\delta_i' \in (\delta_i, \delta_i + \varepsilon)$ is profitable to i (in the case of equality the tie breaking assumption applies). Hence $\boldsymbol{\delta}$ cannot be an equilibrium protection in this case.

Suppose that $\delta_i = 1$, for all $k \in E(j)$, $\delta_k = 0$ and $k \in C_j(G-\{i\})$. This means that the central node is fully protected and that the adversary attacks nodes with no protection that belong to the same component in $G-\{i\}$ only. Using an analogous argument to that given for the case above, j has incentive to increase his protection: When j increases δ_j by a sufficiently small amount, the adversary continues attacking unprotected nodes in the neighbourhood of j and so j continues being attacked with probability 1. In addition, in case of surviving the attack, j secures sufficiently large value of the network with probability 1, because $\delta_i = 1$. Hence $\boldsymbol{\delta}$ cannot be an equilibrium protection in this case.

From now on we assume that either there exists $k \in E(j)$ with $\delta_k > 0$, or $\delta_i = 1$ and there exists $k \in E(j)$ such that $k \notin C_j(G-\{i\})$. Notice that by (80), this implies that $\delta_i > 0$, which means that the critical node has some positive protection level.

Suppose that $j = i$, that is that the critical node, i, is attacked with positive probability under ξ. It must be that $\delta_i < 1$. Take any $j \in E(i)$. By (80) we have $\delta_j < 1$, because $\delta_i < 1$. The expected payoff to i from the adversary attacking j is

$$U^i(G, \boldsymbol{\delta}, j) = \delta_j \left(\frac{f(n)}{n} \right) + (1-\delta_j)\delta_i \mathbf{E}\left[\frac{f\left(n-1-Z\left(|C_j|-1, \boldsymbol{\delta}\right)\right)}{n-1-Z\left(|C_j|-1, \boldsymbol{\delta}\right)} \right] - \delta_i c. \tag{83}$$

By (79) and $\delta_j < 1$ we have

$$(\delta_i - \delta_j)\left(\frac{f(n)}{n} \right) < (1-\delta_j)\delta_i \mathbf{E}\left[\frac{f\left(n-1-Z\left(|C_j|-1, \boldsymbol{\delta}\right)\right)}{n-1-Z\left(|C_j|-1, \boldsymbol{\delta}\right)} \right], \tag{84}$$

where the strict inequality follows from the facts that $\delta_i > 0$, $\delta_j < 1$, and $|C_j| \leq n-1$. The inequality is equivalent to $U^i(G, \boldsymbol{\delta}, i) < U^i(G, \boldsymbol{\delta}, j)$. Thus for all $j \in E(i)$ we have $U^i(G, \boldsymbol{\delta}, i) < U^i(G, \boldsymbol{\delta}, j)$. By (81), an increase in δ_i by sufficiently small $\varepsilon > 0$ diverts the attack to a subset of nodes in $E(i)$ and, by what was shown above, this increases the utility of i (for any $\xi_i > 0$). Hence $\boldsymbol{\delta}$ cannot be an equilibrium protection in this case as well.

Suppose that $j \neq i$. It must be that $\delta_j < 1$. Take any such j with minimal δ_j. Take any $k \in E(j)$. There are three cases possible: (i) $k = i$, (ii) $k \neq i$ and $k \notin C_j(G-\{i\})$, and (iii) $k \in C_j(G-\{i\})$. Expected payoffs to j from the adversary attacking k with

probability 1 in each of these cases are given by, respectively,

$$U^j(G,\boldsymbol{\delta},i)=\delta_i\left(\frac{f(n)}{n}\right)+(1-\delta_i)\delta_j\mathbf{E}\left[\frac{f\left(|C_j|-Z\left(|C_j|,\boldsymbol{\delta}\right)\right)}{|C_j|-Z\left(|C_j|,\boldsymbol{\delta}\right)}\right]-\delta_j c \tag{85}$$

$$U^j(G,\boldsymbol{\delta},k)=\delta_k\left(\frac{f(n)}{n}\right)+(1-\delta_k)\delta_i\mathbf{E}\left[\frac{f\left(n-1-Z\left(|C_k|-1,\boldsymbol{\delta}\right)\right)}{n-1-Z\left(|C_k|-1,\boldsymbol{\delta}\right)}\right]+$$
$$(1-\delta_k)(1-\delta_i)\delta_j\mathbf{E}\left[\frac{f\left(|C_j|-Z\left(|C_j|,\boldsymbol{\delta}\right)\right)}{|C_j|-Z\left(|C_j|,\boldsymbol{\delta}\right)}\right]-\delta_j c \tag{86}$$

$$U^j(G,\boldsymbol{\delta},k)=\delta_k\left(\frac{f(n)}{n}\right)+(1-\delta_k)\delta_j\Bigg(\delta_i\mathbf{E}\left[\frac{f\left(n-1-Z\left(|C_j|-2,\boldsymbol{\delta}\right)\right)}{n-1-Z\left(|C_j|-2,\boldsymbol{\delta}\right)}\right]+$$
$$(1-\delta_i)\mathbf{E}\left[\frac{f\left(|C_j|-1-Z\left(|C_j|-2,\boldsymbol{\delta}\right)\right)}{|C_j|-1-Z\left(|C_j|-2,\boldsymbol{\delta}\right)}\right]\Bigg)-\delta_j c. \tag{87}$$

In case (i) we have $\delta_i>\delta_j$, as $\delta_i>0$, $\delta_j<1$, and (80) applies. Consequently, $U^j(G,\boldsymbol{\delta},i)>U^j(G,\boldsymbol{\delta},j)$. In case (ii), $U^j(G,\boldsymbol{\delta},k)>U^j(G,\boldsymbol{\delta},j)$, because $\delta_i>0$, $|C_k|\leq n-1$, and, by the assumption of minimality of δ_j, $\delta_k\geq\delta_j$. In case (iii), it must be $\delta_k=\delta_j$ as the adversary is indifferent between attacking k and j and they are both in the same component of $G-\{i\}$. If $\delta_j>0$, then $U^j(G,\boldsymbol{\delta},k)>U^j(G,\boldsymbol{\delta},j)$. Suppose that $\delta_j=0$, in which case $\delta_k=0$ as well. By the earlier analysis, in this part of the proof we are restricting attention to the situation where either there exists $l\in E(j)$ with $\delta_l>0$, or $\delta_i=1$ and there exists $l\in E(j)$ such that $l\notin C_j(G-\{i\})$. In the case of $\delta_l>0$, it cannot be that $l\in C_j(G-\{i\})$ and, by (80), it cannot be that $l=i$. As we have shown for point (ii), $U^j(G,\boldsymbol{\delta},l)>U^j(G,\boldsymbol{\delta},j)$. We will show that when j increases δ_j to $\delta_j'=\delta_j+\varepsilon$, where $\varepsilon>0$ is sufficiently small, then $U^{\mathsf{A}}(G,(\delta_j',\boldsymbol{\delta}_{-j}),l)>U^{\mathsf{A}}(G,(\delta_j',\boldsymbol{\delta}_{-j}),k)$ and so a best responding adversary attacks nodes from $E(j)$ that are in a different component of $G-\{i\}$ than j. The utility of the adversary from attacking l is

$$U^{\mathsf{A}}(G,\boldsymbol{\delta},l)=-\delta_l f(n)-(1-\delta_l)\delta_i\mathbf{E}\left[f\left(n-1-Z\left(|C_l|-1,\boldsymbol{\delta}\right)\right)\right]-$$
$$(1-\delta_l)\left(1-\delta_i\right)\Bigg(\mathbf{E}\left[f\left(|C_l|-1-Z\left(|C_l|-1,\boldsymbol{\delta}\right)\right)\right]+\delta_j\mathbf{E}\left[f\left(|C_j|-1-Z\left(|C_j|-2,\boldsymbol{\delta}\right)\right)\right]+$$
$$(1-\delta_j)\,\mathbf{E}\left[f\left(|C_j|-2-Z\left(|C_j|-2,\boldsymbol{\delta}\right)\right)\right]+\sum_{\substack{C\in\mathcal{C}(G-\{i\})\\ C\neq C_j,\ C\neq C_l}}\mathbf{E}\left[f(|C|-Z(|C|,\boldsymbol{\delta}))\right]\Bigg). \tag{88}$$

and the utility of the adversary from attacking k is

$$U^{\mathsf{A}}(G,\boldsymbol{\delta},k) = -\delta_i\Big(\delta_j\mathbf{E}\left[f\left(n-1-Z\left(|C_j|-2,\boldsymbol{\delta}\right)\right)\right] + (1-\delta_j)\,\mathbf{E}\left[f\left(n-2-Z\left(|C_j|-2,\boldsymbol{\delta}\right)\right)\right]\Big) -$$
$$(1-\delta_i)\left(\mathbf{E}\left[f\left(|C_l|-Z\left(|C_l|,\boldsymbol{\delta}\right)\right)\right] + \delta_j\mathbf{E}\left[f\left(|C_j|-1-Z\left(|C_j|-2,\boldsymbol{\delta}\right)\right)\right] + (1-\delta_j)\,\mathbf{E}\left[f\left(|C_j|-2-Z\left(|C_j|-2,\boldsymbol{\delta}\right)\right)\right] + \sum_{\substack{C\in\mathcal{C}(G-\{i\})\\ C\neq C_j,\ C\neq C_l}}\mathbf{E}\left[f(|C|-Z(|C|,\boldsymbol{\delta}))\right]\right). \quad (89)$$

Taking derivatives with respect to δ_j we get

$$\frac{\partial U^{\mathsf{A}}(G,\boldsymbol{\delta},l)}{\partial\delta_j} =$$
$$-(1-\delta_l)(1-\delta_i)\left(\mathbf{E}\left[f\left(|C_j|-1-Z\left(|C_j|-2,\boldsymbol{\delta}\right)\right)\right]-\mathbf{E}\left[f\left(|C_j|-2-Z\left(|C_j|-2,\boldsymbol{\delta}\right)\right)\right]\right) >$$
$$-\delta_i\Big(\mathbf{E}\left[f\left(n-1-Z\left(|C_j|-2,\boldsymbol{\delta}\right)\right)\right]-\mathbf{E}\left[f\left(n-2-Z\left(|C_j|-2,\boldsymbol{\delta}\right)\right)\right]\Big) -$$
$$(1-\delta_i)\left(\mathbf{E}\left[f\left(|C_j|-1-Z\left(|C_j|-2,\boldsymbol{\delta}\right)\right)\right]-\mathbf{E}\left[f\left(|C_j|-2-Z\left(|C_j|-2,\boldsymbol{\delta}\right)\right)\right]\right)$$
$$= \frac{\partial U^{\mathsf{A}}(G,\boldsymbol{\delta},k)}{\partial\delta_j}.$$

Since $U^{\mathsf{A}}(G,\boldsymbol{\delta},l) = U^{\mathsf{A}}(G,\boldsymbol{\delta},k)$, $\partial U^{\mathsf{A}}(G,\boldsymbol{\delta},l)/\partial\delta_j > \partial U^{\mathsf{A}}(G,\boldsymbol{\delta},k)/\partial\delta_j$, and the utilities are continuous in protection levels, so $U^{\mathsf{A}}(G,(\delta_j',\boldsymbol{\delta}_{-j}),l) > U^{\mathsf{A}}(G,(\delta_j',\boldsymbol{\delta}_{-j}),k)$ in the neighbourhood of δ_j. Thus if j raises δ_j by positive and a sufficiently small amount, the adversary switches to attacking nodes in a different component of $G-\{i\}$ than j and for any such node l, $U^j(G,\boldsymbol{\delta},l) > U^j(G,\boldsymbol{\delta},j)$.

In each of the cases above an increase in δ_j by sufficiently small $\varepsilon > 0$ diverts the attack to a subset of nodes in $E(j)$ and, by what was shown above, this increases the utility of j (for any $\xi_j > 0$). This shows that $\boldsymbol{\delta} = \mathbf{1}$ is the unique equilibrium defence profile in G. □

We conclude this section by noting that the first part of point 1 and point 4 of Theorem 1 hold in the model with continuous protection: when cost of defence small enough so that full protection is the first best or when $f(x)/x$ is unbounded so that full protection is the first best for sufficiently large n, the construction above allows us to ensure full protection as a unique equilibrium by network design and to fully mitigate inefficiencies due to defence decisions decentralization.