

CRETA

Centre for Research in Economic Theory and its Applications

Discussion Paper Series

A Game of Hide and Seek in Networks

Francis Bloch, Bhaskar Dutta & Marcin Dziubinski

*[\(This paper also appears as
Warwick Economics Research Papers series No: 1225\)](#)*

October 2019

[\(Updated 2020 & Published:
Journal of Economic Theory\)](#)

No: 53

CRETA

Centre for Research in Economic Theory and its Applications

Department of Economics
University of Warwick, Coventry,
CV4 7AL, United Kingdom

warwick.ac.uk/fac/soc/economics/research/centres/creta/papers

A Game of Hide and Seek in Networks*

Francis Bloch¹, Bhaskar Dutta², and Marcin Dziubiński^{†3}

¹Université Paris 1 and Paris School of Economics
48 Boulevard Jourdan
75014 Paris, France
`francis.bloch@univ-paris1.fr`

²University of Warwick and Ashoka University
CV4 7AL Coventry, UK
`b.dutta@warwick.ac.uk`

³Institute of Informatics, University of Warsaw
Banacha 2, 02-097
Warsaw, Poland
`m.dziubinski@mimuw.edu.pl`

June 2020.

Abstract

We propose and study a strategic model of hiding in a network, where the network designer chooses the links and his position in the network facing the seeker who inspects and disrupts the network. We characterize optimal networks for the hider, as well as equilibrium hiding and seeking strategies on these networks. We show that optimal networks are either equivalent to cycles or variants of a core-periphery networks where every node in the periphery is connected to a single node in the core.

Keywords: Network design; Hide and seek; Covert organizations; Networks
Declarations of interest: none

*Bloch's research was supported by Agence Nationale de la Recherche through grant ANR-18-CE26-0020-01. Dziubiński's work was supported by Polish National Science Centre through grants 2014/13/B/ST6/01807 and 2018/29/B/ST6/00174.

[†]Corresponding author

1 Introduction

In this paper, we consider the following network design problem involving two players. One player, H , is the “principal” or “leading” member of a covert or underground network with $(n - 1)$ members. H builds a network (set of links or arcs) on n nodes. This network is *observed* by an adversary (henceforth S). In a second stage, H chooses one node as her own hiding place, while S attacks one node. These actions are taken *simultaneously*. H is captured if she is in the neighbourhood of the node attacked by S , and then pays a penalty to S . Conditional on not being caught, H ’s payoff is increasing in the size of the component containing H if she is not caught – this is the set of network members with whom she can continue to communicate. The gain to H is also the loss of S and so the second-stage game is zero-sum.

This model has many potential applications, the leading one being the design of a covert organisation – a terrorist organisation such as Al Qaeda, a drug or criminal gang – where the leader H hides in a specific location from which he manages the organization. As is well known, leaders of Al Qaeda have been hiding in safe havens from which they have directed terror operations.¹ Criminal networks in Italy, Mexico and Colombia have also been led by fugitive bosses managing the organization from hiding places.² In most examples, the geographical locations where leaders hide are also the homes of some members of the network, so that we can identify the network of locations with the network of members of the organization. In these settings, S represents the enforcement agency.

As a historical example, the leaders of underground resistance movements in Europe during World War II hid under false identities to organize political and military actions against Nazi Germany.³

Hiding a leader while maintaining efficient communication among members of the organization involves a well-known trade-off between security (the ability to escape from the adversary) and efficiency (the ability to connect agents in the network). In the criminology literature, this trade-off has been highlighted by Morselli et al. (2007) who observe that it either results in long linear networks (when security matters most) or core-periphery networks (when efficiency and security both matter). This trade-off is also at the heart of our characterization of the optimal design of an underground network.

We characterise optimal network architectures chosen by the Hider. The optimal network can only take one of two forms: either it contains a Hamiltonian cycle (where all nodes are connected in a circle) with at least a third of the nodes only connected to two other agents, or is a special core-periphery network where half of the nodes form an interconnected core, and the other half are leaves, each

¹See, among many others, the book by Gunaratna (2002) for a very clear account of the early organization of Al Qaeda.

²See Allum et al. (2019) for a recent account of the Italian mafias and a discussion of the role of fugitives.

³There is an extensive literature on underground movements during the Second World War. As an example, the memoir of Egon Balas (Balas (2008)) contains a detailed account of his experience as an underground communist party member hiding in the city of Koloszar/Cluj in 1944. We are grateful to a referee for suggesting this reference.

connected to a single node in the core.⁴ In addition, a subset of the nodes will remain isolated. The number of isolated nodes, and the choice between the circle and the core-periphery network for connected nodes depends on the parameters of the game, and in particular the shape of the function mapping the size of the network into the benefit of the Hider. Moreover, in the cases where non-singleton nodes form a core-periphery network, the characterisation of an optimal network we obtain is complete.

To understand this characterisation of an optimal network, notice that any network which cannot be “disrupted” (in the sense that the network is not broken into different components if the Seeker fails to find the hidden object) must be 2-connected, and hence contain a cycle. Now, adding links to the cycle can only increase the sizes of the neighborhoods and hence the probability that the hidden object is discovered.⁵ Therefore, if the objective of the Hider is primarily to avoid disruption of the network, forming a cycle will be an optimal choice for the hider. Notice however that in a cycle, every agent has two neighbors, so the probability of discovery of the hidden object must be at least equal to $\frac{2}{n}$. In order to reduce this probability of discovery, while keeping the network connected, one has to allow for the possibility that some nodes only have degree one. In the core-periphery network where half of the nodes are leaves connected to one node in the core, the probability of discovery is reduced to the minimal value for a connected graph. In equilibrium, the Hider chooses to hide in any of the peripheral nodes, whereas the Seeker seeks in any of the core nodes. This uniform hide and seek strategy results in a probability of discovery equal to $\frac{2}{n}$, lower than in the cycle, but induces a larger disruption, as the size of the remaining component after the Seeker fails to find the object is equal to $n - 2$ rather than $n - 1$. In the main characterization Theorem, we show that no other network performs better than the cycle or the core-periphery network. The cycle is preferred when the Hider puts more weight on avoiding disruption and the core-periphery network is preferred when the Hider puts more weight on avoiding discovery of the hidden object.

While no real network has the exact architecture of a cycle or core-periphery network, our results echo some observations on underground networks. Balas (2008) describes his interactions with other communist party members while hiding in the spring and summer of 1944 in several safe houses in the city of Kolosvar/Cluj (then in Hungary and now in Romania). He managed to stay at the homes of sympathizers of the communist party, who knew very little of the underground organization. Balas only had contact with a small number of party members. He regularly met with the secretary of the regional committee, Sanyi Jakab, who was himself in contact with the party leadership in Budapest. When the leaders in Budapest were arrested in 1943, the communication links between the regional committee of the party in of Kolosvar/Cluj and the national committee of the party in Hungary were disrupted. The underground network of the communist party thus shares some characteristics with the core-periphery network: sympathizers offering

⁴If the number of nodes in the core-periphery network is odd, the architecture is slightly different.

⁵Notice however that adding links may not change the probability of capture, if the hider only hides in a subset of the nodes in the cycle.

hiding places are isolated, and only communicate with one or two other nodes in the network. However, the nodes that they connect too, like the regional committee secretary, belong to the core and are themselves connected to all other leaders of the party.

As an example of a circle network, consider the apartments which were used by French resistance fighters during the second world war in the city of Lyon. Lyon was the capital of the French resistance between 1940 and 1944. Historians claim that this is partly due to the existence of hidden passageways, the "traboules", some dating back from the Renaissance, which connect buildings and streets in the city. The traboules describe a circular network, allowing for easy communication through buildings and streets. This network was extensively used by the underground during the German occupation (Curvat et al. (2015)), as it allowed for secret meetings while guaranteeing easy escape and the possibility of keeping communication channels open if one of the buildings was raided by the German police.

Morselli et al. (2007) use data on terrorist networks (Krebs (2002)'s map of the 9/11WTC terrorist cells) and criminal networks (a drug-trafficking network in Canada) to illustrate the security/efficiency trade-off. They argue that terrorist networks are more sensitive to security, and have longer average distances and fewer connections than criminal networks with no node assuming a central position. In contrast, criminal networks are more geared towards efficiency, are clustered and exhibit a core of nodes with high centrality. In addition they note that support nodes (which are not direct perpetrators of criminal or terrorist activities) help connect distant nodes in terrorist networks but not in criminal networks, where each support agent is attached to a single agent in the core. The criminal networks thus resemble the core-periphery network we identify in our analysis, while the terrorist networks share one characteristic of the cycle: they have a large diameter and the average distance between agents is high and no agent is more central than any other agent. Figure 1 illustrates these network architectures, by reproducing the map of the 9/11 WTC terrorist network (Krebs (2002)) as well as the maps of two drug-trafficking mafia groups collected by Calderoni (2012).

2 Related literature

The related literature spans a variety of disciplines, with the earlier literature focusing more on the aspect of hiding and seeking. Perhaps, the first paper was by Von Neumann (1953) who discusses a zero-sum game where H chooses a cell of an exogenously given matrix, while S simultaneously chooses a column or row in the matrix. S "captures" H if the cell chosen by H lies in the row or column chosen by S . A related paper is Fisher (1991), who too analyses a similar zero-sum game, where H and S simultaneously choose vertices of an exogenously given graph. H is caught if S chooses the same node as him or a node connected to the node chosen by him. Interestingly, the value of this "hide and seek game" on a fixed arbitrary

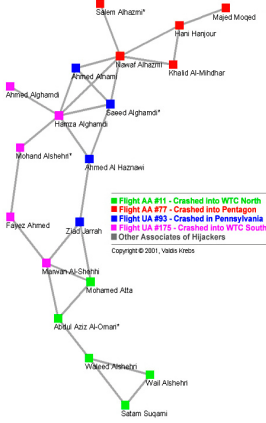
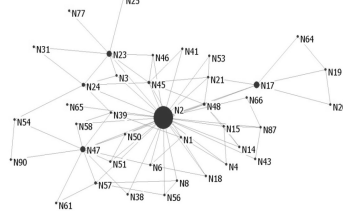
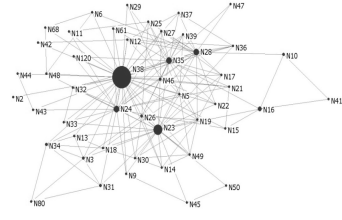


Figure 2: Trusted Prior Contacts

The 9/11WTCterrorist network



The N'Drangheta network of cocaine trafficking (operation Chalonero)



The N'Drangheta network of cocaine trafficking (operation Stupor Mundi)

Figure 1: Three examples of terrorist and criminal networks

network can be computed following Fisher (2002), using *fractional graph theory*.⁶

Computer scientists have also contributed to this literature with Waniek et al. (2017) and Waniek et al. (2018) studying a related, but different problem, of hiding in a network. They consider the leader of a terrorist or criminal organization, and ask the following question: How can a set of edges be added to the network in order to reduce the leader’s measure of centrality in order to avoid detection? Waniek et al. (2017) show that, both for degree and closeness centrality, the problem is NP-complete. However, they also propose a procedure to build a new network from scratch around the leader (the “captain network”) which achieves low levels of degree and closeness centrality but high values of diffusion centrality, where diffusion centrality is measured using the independent cascade and linear threshold diffusion models. Waniek et al. (2018) extend the analysis to betweenness centrality and to the detection of communities (rather than individuals) in the network. Notice, however, that these models are not fully strategic since S does not best respond to H ’s strategy.

Our paper is also related to a recent strand of the economics literature analyzing network design and attack and defense on networks. Baccara and Bar-Isaac (2008) study network design by a criminal organization taking the detection strategy of the adversary as fixed. They highlight differences between two forms of detection, one which depends on the cooperation between criminals and the other which does not. In both situations, they characterize the optimal network archi-

⁶See also Theorem 1.4.1 in Scheinerman and Ullman (1997)

tecture of the criminal network, which either consists of isolated two-player cells (with independent detection) or an asymmetric structure with one agent serving as an information hub (with cooperation-based detection). Goyal and Vigier (2014) propose an alternative model of network design where the defender designs the network and chooses the distribution of defense across nodes before the attacker chooses to attack. Nodes are captured according to a Tullock contest function given the resources spent by the attacker and the defender. If a node is captured by the attacker, contagion occurs and the attacker starts attacking neighboring nodes while the defender loses his defense resources. The main message of Goyal and Vigier (2014) is that the defendant optimally forms a star and concentrates all the defenses at the hub. Dziubiński and Goyal (2013) analyze a related model, where the defender designs the network and chooses defense resources before the attacker attacks. As opposed to Goyal and Vigier (2014), contagion does not occur and the network structure only matters through the payoffs of the two-person zero-sum game between the defender and the attacker. The objective function of the defender is assumed to be increasing and convex in the size of components of the network, reflecting the fact that the defender wants to avoid disruption in the network. The analysis shows that the designer will either form a star and protect the hub, or not protect any node and choose to form a $(k + 1)$ -connected network when the attacker has k units, so that the attacker will not be able to disrupt the network. In the same model, Dziubiński and Goyal (2017) study equilibrium strategies of the defender and attacker for any arbitrary network structure while Cerdeiro et al. (2017) consider decentralized defense decisions by the different nodes in the network.

Thus, we see that the early (non-economics) literature focussed on the hide-and-seek issue, while the more recent literature from economists has focused on disruption. There is an important sense in which our model brings the two strands of the literature together. Our model incorporates the hide-and-seek aspect because the “leader” of the organisation, H , has a special significance and so seeking her is an objective of the adversary. At the same time, the payoff to H is increasing in the size of the residual network and so she wants to avoid disruption as far as possible. Like Baccara and Bar-Isaac (2008), our paper involves a trade-off between the optimal organisation of criminal organisation and the threat of disruption, though this trade-off emerges for quite different reasons. Notice also that unlike several of the previously cited papers, nodes cannot be defended in our model. Another difference between our model and related models comes from the timing of the game. We suppose that the hider and seeker *simultaneously* choose the nodes in which to hide and that they inspect, resulting in equilibria in mixed strategies as in Colonel Blotto games, whereas Goyal and Vigier (2014) and Dziubiński and Goyal (2013) assume that the defender and attacker move sequentially, allowing for pure strategy equilibria.

3 The Model

There are two players, a *Hider* (H) and a *Seeker* (S). The hider H constructs a network among n nodes and chooses a location in the network. For example, the Hider may be the leader of a covert terrorist or criminal organisation, which has $n - 1$ other members. The seeker is then interpreted as a law enforcement agency whose objective is to capture the leader of the organization or to disrupt the communication channels within the organisation. The interaction between H and S is modelled as a two-stage process, which is described below.

In the first stage, H chooses a network of interactions amongst the members of the organisation. Formally, H chooses a graph $G = \langle V, E \rangle$ where V is a set of n vertices, and E is a set of undirected edges $E \subseteq \binom{V}{2}$. A typical edge $e \in E$ will be denoted ij , where $i, j \in V$.

Both players observe the chosen network at the beginning of the second stage. After observing the network G , players H and S *simultaneously* choose *one* node each. The node chosen by the hider is his (hiding) position in the network. The node chosen by the seeker is the node she inspects (or attacks). Let k be the node chosen by S , and $N_G(k) = \{j \in V \mid kj \in E\}$. That is, $N_G(k)$ is the set of all neighbours of k in G . All nodes in $\{k\} \cup N_G(k)$ can be observed by the seeker. If the chosen position of H is in $\{k\} \cup N_G(k)$, then H is captured by S . In addition, node k is removed from the network, irrespective of whether H is captured or not.

The seeker uses his choice to capture the hider and to damage the network. Payoffs depend on whether or not the hider has been captured. If caught, the hider gets payoff $-\beta$, where $\beta \geq 0$.

If the hider is not captured, the covert network remains operational, but is damaged by the attack of the seeker. Then the hider's payoff is an increasing function of the *size* of the component where he is hiding in the residual network. The reason behind this specification is that communication is possible only within a connected component. Moreover, the larger the number of followers with whom H can communicate, the larger is the payoff to the organisation. Formally, his payoff is given by a function $f : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$ of the size of his component in the residual network. We assume f to be strictly increasing with $f(0) = 0$. An example of function f in line with these assumptions is the identity function, $f(x) = x$ for all $x \in \mathbb{R}_{\geq 0}$. The game is assumed to be a zero-sum game, so that the payoff to the seeker is equal to minus the payoff of the hider.

Given a set of nodes $U \subseteq V$, let $\mathcal{G}(U)$ be the set of all undirected graphs over U and let $\mathcal{G} = \bigcup_{U \subseteq V} \mathcal{G}(U)$ be the set of all undirected graphs that can be formed over V or any of its subsets. A strategy for the hider is a pair $(G, h) \in \mathcal{G}(V) \times V$, where G is the graph and h is the hiding place chosen by H in G . As the seeker chooses his inspected node after observing the network, a strategy for the seeker is a function $s : \mathcal{G}(V) \rightarrow V$.

Before defining the payoffs we introduce some auxiliary definitions on networks. Given a set of nodes $U \subseteq V$ and a graph $G = \langle U, E \rangle$ over U , a maximal set of nodes $C \subseteq U$ such that any two nodes $i, j \in C$ are connected in G is a *component* of G .⁷ The set of all components of G is denoted by $\mathcal{C}(G)$. In addition, given

⁷ Two nodes $i, j \in U$ are connected in $G = \langle U, E \rangle$ if there exists a sequence of nodes i_1, \dots, i_l

$i \in U$, let $C_i(G)$ be the component in G containing i . Given a set of nodes $U \subseteq V$, a graph $G = \langle U, E \rangle$ over U , and a set of nodes $U' \subseteq U$, let $G[U'] = \langle U', E[U'] \rangle$ with $E[U'] = \{ij \in E : \{i, j\} \subseteq U'\}$ be the *subgraph of G induced by U'* . Given a node $k \in V$ let $G - k = G[U \setminus \{k\}]$ be the *residual network* obtained from G by removing k and all its links from G .

Given the strategy profile $((G, h), s)$, the payoff to the hider is

$$\Pi^H(G, h, s) = \begin{cases} -\beta & \text{if } h \in \{s(G)\} \cup N_G(s(G)) \\ f(|C_i(G - s(G))|) & \text{otherwise.} \end{cases} \quad (1)$$

The payoff to the seeker is $\Pi^S((G, h), s) = -\Pi^H((G, h), s)$.

The cycle network and the core-periphery networks will be important in our analysis. The cycle network is a connected network where every node has exactly two neighbours.

A *core-periphery* network over a set $V = P \cup C$ of n nodes is defined as follows. There are $q \geq \lceil n/2 \rceil$ *core* nodes in set $C = \{c_1, \dots, c_q\}$ and $m \leq \lfloor n/2 \rfloor$ *periphery* nodes in set $P = \{p_1, \dots, p_m\}$. Nodes of the core form a connected graph, while each periphery node, p_i with $1 \leq i \leq m$, is connected to core node c_i . Nodes of the core which are not connected to a periphery node are called *orphaned*. Figure 2 illustrates a core-periphery network with orphaned nodes.

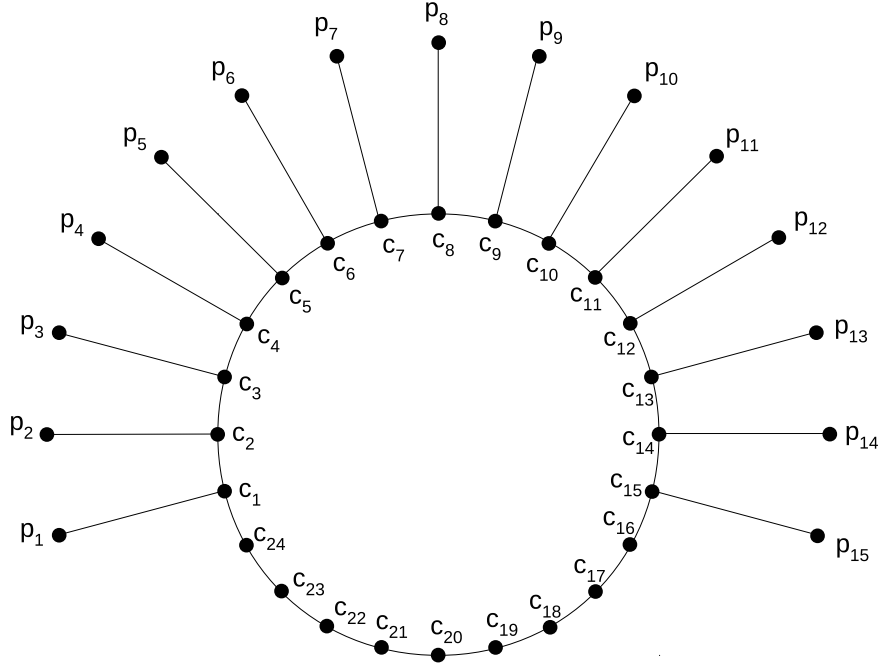


Figure 2: A core-periphery network over 39 nodes, with 15 periphery nodes and 9 orphaned core nodes.

A particular class of core-periphery networks, which we call *maximal*, plays a crucial role in our characterisation. If n is even, a core-periphery network is

such that $i_0 = i$, $i_n = j$, and for all $k \in \{1, \dots, l\}$, $i_{k-1}i_k \in E$.

maximal if and only if it has $n/2$ periphery nodes and nodes of the core form a 2-connected graph.⁸ If n is odd, a core-periphery network is maximal if and only if it has $(n - 3)/2$ periphery nodes (and hence 3 orphaned nodes), nodes of the core form a 2-connected graph, and one orphaned node has exactly the two other orphaned nodes as its neighbours. Examples of maximal core-periphery networks are presented in Figure 3.

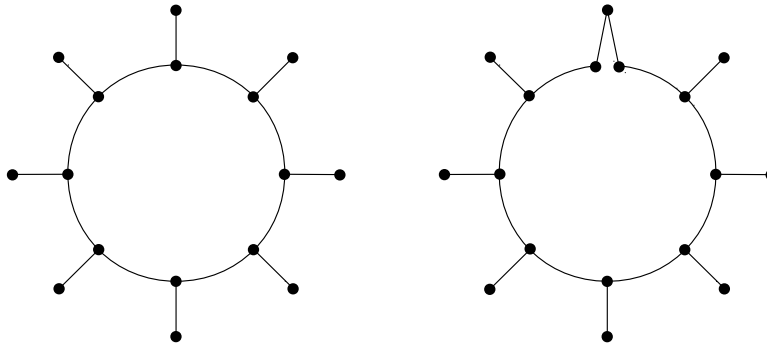


Figure 3: Maximal core-periphery networks over 16 nodes (left) and 17 nodes (right).

4 The Characterisation Results

Our objective in this section is to provide optimal networks for the hider as well as to characterise the hiding and the seeking strategies on these networks. We show in our main result (Theorem 1) that these networks consist of a number of singleton nodes and a connected component which either contains a *cycle* with at least a third of the nodes connected to only two agents or has a particular *core periphery* topology.

We state and prove a preliminary lemma that will be useful in proving the main result. The lemma asserts that in an optimal network there cannot be a component containing just two or three nodes.

Lemma 1. *Suppose G is an optimal network for H whose set of non-singleton components is \mathcal{X} . Then, each component $C \in \mathcal{X}$ contains at least 4 nodes.*

Proof. Suppose the lemma is not true and some $C \in \mathcal{X}$ has exactly three nodes, $C = \{n_1, n_2, n_3\}$. Following standard arguments, C must have a non-empty intersection with the support of H 's optimal hiding strategy as well as S 's optimal seeking strategy, given G . (If not, the hider or the seeker would have profitable deviations). Moreover, conditional on hiding in C , H is caught with probability ρ , where ρ is the total probability with which S seeks in C . This is true because S can always search one node in C that has two neighbours, and hence observe all nodes in the component.

⁸ A graph is 2-connected if and only if it does not get disconnected after removing a single node.

Let G' be another network which coincides with G everywhere except that C is broken up into singleton components $\{n_1\}$, $\{n_2\}$, $\{n_3\}$. Moreover, suppose H 's hiding strategy coincides with that in G everywhere on $V \setminus C$, while H distributes the earlier probability weight on C uniformly on the three nodes n_1, n_2, n_3 . It is straightforward to check that H 's expected payoff in G' is strictly higher than his expected payoff in inspecting a node in the component C , which must be equal to his expected payoff of using a mixed strategy in G , contradicting optimality of G .

A similar argument rules out an optimal network containing a component with only two nodes. \square

Remark 1. *An implication of this lemma is that the optimal network will either be completely disconnected with n singletons or will contain at most $n - 4$ singletons. This implication will be used throughout the proof of the theorem.*

At this stage, we describe the main result of the paper informally (the formal statement appears at the end of this Section). Whether a cycle or a core-periphery topology is better for H depends on the value of the expression.

$$T(n, s) = (n - s - 3)f(n - s - 1) - (n - s - 2)f(n - s - 2). \quad (2)$$

We will construct an equilibrium with the following features.

- The optimal network G has a fixed number of singleton nodes s (that will be determined) where $s \leq n - 4$ or $s = n$.
- If $T(n, s) \geq \beta$ and $s \neq n$, then G has a cycle component over $n - s$ nodes.
- If $T(n, s) < \beta$, $n - s \geq 4$, then G has a maximal core periphery component over $n - s$ nodes.
- The hider mixes between hiding in the singleton nodes and in the connected component with probabilities that will be determined. When hiding in the singleton nodes, he mixes uniformly across all these nodes. When hiding in the connected component, he mixes uniformly across all the nodes when it is a cycle, mixes uniformly across the periphery nodes when it is a maximal core-periphery network over even number of nodes, and mixes between hiding in periphery nodes, mixing uniformly across them, and the middle orphaned node, otherwise.
- The seeker mixes between seeking in the singleton nodes and in the connected component. When seeking in the singleton nodes, he mixes uniformly across all these nodes. When seeking in the connected component, he mixes uniformly across all the nodes when it is a cycle, mixes uniformly across the core nodes when it is a maximal core-periphery network over even number of nodes, and mixes between seeking in the neighbours of periphery nodes, mixing uniformly across them, and the middle orphaned node, otherwise.

To get some intuition behind this construction, notice that the hider faces a tradeoff between the cost of being caught and the value he gets in the residual

network. Adding links in the network increases connectivity and hence secures a larger value after the seeker's action *provided* he is not caught. However, a larger number of links also leads to higher exposure and a greater probability of being caught, as it increases the size of the neighbourhoods of the nodes in which the hider can hide.

Given a number of singleton nodes s , the choice between a cycle and a core-periphery network is influenced by the change in value of f , as measured by the quantity $T(n, s)$. The probability of being caught in a cycle of size $n - s$ is $3/(n - s)$, as each node has exactly two neighbours, while only one node is lost from the cycle component if H is not caught. The probability of being caught in a maximal core-periphery network (if $n - s$ is even) is $2/(n - s)$ since the hider hides mixing uniformly across the periphery nodes; in the event of H not being caught, two nodes are lost from the core periphery component since the seeker seeks mixing uniformly across the core nodes. If the change in f between $n - s - 2$ and $n - s - 1$ is sufficiently large, so that $T(n, s) > \beta$ then the marginal loss from an additional node being removed from a component is high, as compared to the penalty for being caught. In this case, a cycle is preferred over the core-periphery network. On the other hand, if the change in f is not sufficiently large, the marginal loss from an additional node being removed from a component is not sufficiently high and the hider prefers to opt for the safer core-periphery network.

The proof of the main theorem is rather long. We first give a brief sketch of the main steps of the proof. We start by constructing a feasible strategy of the seeker that, for each network over the set of nodes V , provides a (mixed) seeking strategy on that network. This strategy determines the payoffs the seeker can secure for each possible network over V . Since the game is zero-sum, minus these payoffs provide an upper bound on the payoff the hider can get for each network. Next, for each $s \in \{0, \dots, n - 4, n\}$, we construct a network that is optimal for the hider across all possible networks with exactly s singleton nodes. In the case of $T(n, s) \geq \beta$, as well as in the case of $n - s$ being even, these networks yield payoffs to the hider that meet the upper bound determined in the first part of the proof. In the case of $T(n, s) < \beta$ and odd $n - s$, the upper bound from the first part of the proof is not exact and we need additional computations to identify the optimal network. Finally, we show how the number of singleton nodes is determined to characterise the optimal network.

We now proceed to prove the theorem. We first introduce a partition of the nodes into different sets that will play a crucial role in the construction of a strategy for the seeker.

Given a (possibly disconnected) network G over the set of nodes V , node $i \in V$ is a *singleton node* if $|N_G(i)| = 0$. The set of singleton nodes of G is denoted by $S(G)$. Node $i \in V$ is a *leaf* if $|N_G(i)| = 1$. The set of leaves of G is denoted by $L(G)$. Given node $i \in V$, let $l_i(G) = |N_G(i) \cap L(G)|$ denote the number of leaf-neighbours of i . Let $D(G) = \{i \in L(G) : N_G(i) \subseteq L(G)\}$ be the set of leaves connected to a leaf only. Such leaves constitute two-node components in G . The set $D(G)$ can be partitioned into two equal-size subsets, $D_1(G)$ and $D_2(G)$, $D_1(G) \cup D_2(G) = D(G)$, such that for each $l \in \{1, 2\}$, and any two distinct nodes, i, j , in $D_l(G)$, nodes i

and j are not connected in G . In other words, for any 2-node component of G , one of its nodes is in $D_1(G)$ and the other one is in $D_2(G)$. We pick one such partition $D_1(G), D_2(G)$.

Let

$$M(G) = \{i \in V \setminus D_2(G) : l_i(G) = 1\}$$

be the set of nodes which are not in $D_2(G)$ and are connected to exactly one leaf in G and let

$$SL(G) = \{i \in L(G) : N_G(i) \cap M(G) \neq \emptyset\}$$

be the set of leaves connected to an element of $M(G)$ (clearly $D_2(G) \subseteq SL(G)$). Such leaves are called *singleton leaves*. Let $R(G) = V \setminus (S(G) \cup SL(G) \cup M(G))$ be the set of nodes in G which are neither a singleton, nor a singleton leaf, nor a neighbour of a singleton leaf.

We now construct step by step a strategy for the seeker which guarantees a fixed payoff for any network G . Take any network G over V and let $s = |S(G)|$ and $m = |M(G)|$. Moreover, let $GR = G[R(G)]$ be the subnetwork of G generated by the set of nodes $R(G)$. In particular, when $R(G) = \emptyset$, GR is the empty network with empty sets of nodes and links. Let $D(GR)$ be the set of nodes in $R(G)$ that belong to two-element subsets of $R(G)$.

Consider a mixed strategy of player S , $\sigma = (\sigma_1, \dots, \sigma_n)$, with the following probabilities:

$$\sigma = \lambda_S \sigma^S + (1 - \lambda_S) (\lambda_R \sigma^R + (1 - \lambda_R) \sigma^M) \quad (3)$$

where $\lambda_R, \lambda_S \in [0, 1]$, and

$$\begin{aligned} \sigma_i^S &= \begin{cases} \frac{1}{s}, & \text{if } i \in S(G), \\ 0, & \text{otherwise,} \end{cases} \\ \sigma_i^M &= \begin{cases} \frac{1}{m}, & \text{if } i \in M(G), \\ 0, & \text{otherwise,} \end{cases} \\ \sigma_i^R &= \begin{cases} \frac{l_i(GR)+1}{n-s-2m}, & \text{if } i \in R(G) \setminus (L(GR)), \\ 0, & \text{otherwise,} \end{cases} \end{aligned}$$

We first show that these probabilities are well-defined.

Lemma 2. σ is a feasible strategy for the seeker S .

Proof. Clearly, σ^S is a valid probability distribution as long as $S(G) \neq \emptyset$, that is $s > 0$. Similarly, σ^M is a valid probability distribution as long as $M(G) \neq \emptyset$, that is $m \geq 1$. We also claim that σ^R is a valid probability distribution as long as $R(G) \neq \emptyset$. To see this, notice that $R(G)$ contains exactly $n - s - 2m$ nodes and σ^R can be obtained from a uniform distribution on $R(G)$ by moving the probability mass assigned to leaves in GR to their neighbours. Lastly, notice that if $S(G) \neq \emptyset$, then either all the non-singleton nodes in G have degree 1, in which case $M(G) \neq \emptyset$, or there exists a node in G of degree 2 or more, in which case either $M(G) \neq \emptyset$ or $R(G) \neq \emptyset$. Hence if $S(G) \neq \emptyset$, then either σ^M or σ^R is a valid probability distribution. By these observations, σ is a valid probability distribution as long as

$\lambda_S = 1$, if $s = n$, $\lambda_S = 0$, if $s = 0$, $\lambda_R = 0$, if $R(G) = \emptyset$, and $\lambda_R = 1$, if $m = 0$. So, the lemma is true. \square

The idea behind the construction of strategy σ is as follows. With probability λ_S , player S seeks in the set of singleton nodes, $S(G)$, and with probability $(1 - \lambda_S)$ he seeks outside this set. Conditional on seeking outside $S(G)$, with probability λ_R player S seeks in the set of nodes $R(G)$ and with probability $(1 - \lambda_R)$ he seeks in the set $SL(G) \cup M(G)$. When seeking in $S(G)$, S mixes uniformly across all the singleton nodes. When seeking in $SL(G) \cup M(G)$, S mixes uniformly across all the nodes neighbouring a singleton leaf, that is all the nodes in $M(G)$. Lastly, when seeking in the set of nodes $R(G)$, S mixes using strategy σ^R .

In the next two lemmas, we compute lower bounds on the probability of capture of the hider in different regions of the network.

Lemma 3. *The probability of capture of player H is at least $\frac{3(1-\lambda_S)\lambda_R}{(n-s-2m)}$, if H hides in $R(G) \setminus (S(GR) \cup SL(GR))$.*

Proof. Take any node $i \in R(G) \setminus (S(GR) \cup SL(GR) \cup D(GR))$. Suppose, first, that i is not a leaf in GR , i.e. $i \in R(G) \setminus L(GR)$. Then i has at least two neighbours in $R(G)$ and the probability that seeker seeks at i or at one of i 's neighbours is at least $(1 - \lambda_S)\lambda_R 3/(n - s - 2m)$. Suppose, next, that $i \in L(GR) \setminus (SL(GR) \cup D(GR))$. Then i has a neighbour $j \in R(G)$ that has at least one more leaf neighbour in GR . Since $\sigma_j = (1 - \lambda_S)\lambda_R 3/(n - s - 2m)$, the lemma is true. \square

We now narrow down the possible strategies, σ , by setting the value of λ_R . This is done under the assumption that $S(G) \neq V$, that is $s \leq n - 4$ and there exist non-singleton nodes in G . Let

$$\begin{aligned} \rho &= \frac{(n - s - 2m)(f(n - s - 2) + \beta)}{3m(f(n - s - 1) + \beta) + (n - s - 2m)(f(n - s - 2) + \beta)} \\ &= 1 - \frac{3m(f(n - s - 1) + \beta)}{3m(f(n - s - 1) + \beta) + (n - s - 2m)(f(n - s - 2) + \beta)} \end{aligned}$$

and

$$\lambda_R = \begin{cases} 0, & \text{if } R(G) = \emptyset, \\ \rho, & \text{otherwise.} \end{cases} \quad (4)$$

Clearly $\rho \in [0, 1]$ and $\lambda_R \in [0, 1]$.

Lemma 4. *The probability of capture of player H is at least $\frac{3(1-\lambda_S)\lambda_R}{(n-s-2m)}$, if H hides in $S(GR) \cup SL(GR)$.*

Proof. In this case, i must have a neighbour, j , in $M(G)$. For otherwise i would be a singleton node in H or a singleton leaf in H and so i would belong to $S(G) \cup M(G)$

and not to $R(G)$. Now, the probability of S putting a seeking resource in j is

$$\begin{aligned}
\sigma_j &= (1 - \lambda_S)(1 - \lambda_R) \left(\frac{1}{m} \right) \\
&\geq (1 - \lambda_S) \min \left(1, \frac{3m(f(n-s-1) + \beta)}{3m(f(n-s-1) + \beta) + (n-s-2m)(f(n-s-2) + \beta)} \right) \left(\frac{1}{m} \right) \\
&= (1 - \lambda_S) \left(\frac{3(f(n-s-1) + \beta)}{3m(f(n-s-1) + \beta) + (n-s-2m)(f(n-s-2) + \beta)} \right) \\
&> (1 - \lambda_S) \left(\frac{3(f(n-s-2) + \beta)}{3m(f(n-s-1) + \beta) + (n-s-2m)(f(n-s-2) + \beta)} \right) \\
&= (1 - \lambda_S) \lambda_R \left(\frac{3}{n-s-2m} \right).
\end{aligned}$$

Thus i is caught with probability at least $(1 - \lambda_S) \lambda_R 3 / (n - s - 2m)$. \square

We now use these characterisations to compute lower bounds on the expected payoff of the seeker when the hider hides in different parts of the network.

Lemma 5. *Conditional on H hiding in a node of $R(G)$ and S using σ , the expected payoff of S is at least*

$$\begin{aligned}
L^R(n, m, s) &= (1 - \lambda_S) \left(\lambda_R \left(\left(\frac{3}{n-s-2m} \right) \beta - \left(1 - \frac{3}{n-s-2m} \right) f(n-s-1) \right) \right. \\
&\quad \left. - (1 - \lambda_R) f(n-s-2) \right) - \lambda_S f(n-s) \quad (5)
\end{aligned}$$

Proof. Suppose that H hides in $R(G)$. From Lemmas 3 and 4, H is captured with probability at least $(1 - \lambda_S) \lambda_R 3 / (n - s - 2m)$ when S chooses σ . If not captured, only one node is removed when S searches in $R(G)$. With probability $(1 - \lambda_S)((1 - \lambda_R))$, S searches in $M(G)$ and removes two nodes, but does not capture H . Finally, with probability λ_S , S searches in $S(G)$, and does not catch H . Then, her payoff is at least $-f(n-s)$ – this happens if G is connected over $n-s$ nodes. \square

Similarly, we compute a lower bound on the expected payoff of the seeker when the hider hides in $M(G)$ or $SL(G)$:

Lemma 6. *Conditional on H hiding in a node of $M(G) \cup SL(G)$, player S by choosing σ obtains a payoff of at least*

$$\begin{aligned}
L^M(n, m, s) &= (1 - \lambda_S) \left((1 - \lambda_R) \left(\left(\frac{1}{m} \right) \beta - \right. \right. \\
&\quad \left. \left. \left(1 - \frac{1}{m} \right) f(n-s-2) \right) - \lambda_R f(n-s-1) \right) - \lambda_S f(n-s), \quad (6)
\end{aligned}$$

Proof. The probability of capture of H is at least $(1 - \lambda_S)(1 - \lambda_R)1/m$. If H is not captured, S guarantees that the component of the hider has size at most $n-s-2$ with probability $(1 - \lambda_S)(1 - \lambda_R)$ when the attack is in $M(G)$. Furthermore, at least one node is removed with probability $(1 - \lambda_S) \lambda_R$ when the attack is in $R(G)$. Finally, the component containing H has size at most $n-s$ when the attack is in $S(G)$, and this happens with probability λ_S . \square

We show in the Appendix that the chosen value of λ_R ensures that for any $s \in \{0, \dots, n-4\}$,

$$L(n, m, s) = L^R(n, m, s) = L^M(n, m, s) = (1 - \lambda_S)A(n, m, s) - \lambda_S f(n - s) \quad (7)$$

where $A(n, m, s)$ is a complex function whose exact functional form is derived in the Appendix.

Remark 2. $A(n, m, s)$ is strictly decreasing in m if $T(n, s) > \beta$ and strictly increasing in m if $T(n, s) < \beta$.

To complete the definition of strategy σ we compute the value of the probability of seeking in singleton nodes, λ_S . Conditional on H hiding in a node of $S(G)$, using any of the strategies σ defined above, player S obtains payoff of at least $L^S(n, m, s) = \lambda_S B(s) - (1 - \lambda_S) f(1)$, where

$$B(s) = \left(\frac{1}{s}\right) \beta - \left(1 - \frac{1}{s}\right) f(1),$$

regardless of the strategy of the hider, as the probability of capture is λ_S/s and, in the case of not capturing the hider, S gets payoff $-f(1)$. Let

$$\lambda_S = \begin{cases} 1, & \text{if } s = n, \\ \frac{A(n, m, s) + f(1)}{A(n, m, s) + B(s) + f(1) + f(n-s)}, & \text{if } s \neq n \text{ and } A(n, m, s) > -f(1), \\ 0, & \text{otherwise.} \end{cases}$$

To see that $\lambda_S \in [0, 1]$, notice that $B(s) > -f(1) \geq -f(n-s)$, for any $\beta \geq 0$ and $0 \leq s \leq n-4$.

It is straightforward to verify the following for any $s \in \{0, \dots, n-4\}$:

- (i) if $A(n, m, s) > -f(1)$, then $L^S(n, m, s) = L(n, m, s)$.
- (ii) if $A(n, m, s) \leq -f(1)$ then $L^S(n, m, s) \geq L(n, m, s)$.

To summarize, the lower bound on the payoff of S in G , secured by the strategy σ , is given by

$$Q(n, m, s) = \begin{cases} B(n), & s = n \\ \frac{A(n, m, s)B(s) - f(1)f(n-s)}{A(n, m, s) + B(s) + f(1) + f(n-s)}, & \text{if } s \leq n-4 \text{ and } A(n, m, s) > -f(1), \\ A(n, m, s), & \text{otherwise,} \end{cases} \quad (8)$$

This, together with Remark 2 and Claim 1 in the Appendix, yields the following crucial fact.

Remark 3. For all $s \leq n-4$, $Q(n, m, s)$ is minimised at $m = (n-s)/2$, when $T(n, s) < \beta$, and is minimised at $m = 0$, when $T(n, s) > \beta$.

Why is Remark 3 important? Since the game is zero-sum, the lower bound on the payoff of S is also the upper bound on the payoff of H . Since the upper bound on H 's payoff will be when $Q(n, m, s)$ is minimised, Remark 3 indicates the nature of the optimal network for H .

Fix the number of singleton nodes, $s \leq n - 4$. Define a new function $\bar{Q}(n, s)$ as follows

$$\bar{Q}(n, s) = \begin{cases} Q(n, 0, s), & \text{if } s \leq n - 4 \text{ and } T(n, s) \geq \beta, \\ Q(n, (n - s)/2, s), & \text{if } 0 \leq s \leq n - 4, T(n, s) < \beta \text{ and } n - s \text{ is even,} \\ Q(n, (n - s - 3)/2, s), & \text{if } 0 \leq s \leq n - 4, T(n, s) < \beta \text{ and } n - s \text{ is odd.} \end{cases}$$

Consider first the case where $n - s$ is even.

Lemma 7. *Suppose H builds a network with s singleton nodes such that $n - s$ is even. Then, an optimal strategy for H provides H with payoff $-\bar{Q}(n, s)$. If $T(n, s) < \beta$, G is optimal if the subnetwork over $n - s$ nodes is a maximal core-periphery network. If $T(n, s) > \beta$, G is optimal if the subnetwork over $n - s$ nodes is a cycle.*

Proof. Fix s such that $n - s$ is even. Let

$$\bar{A}(n, s) = \begin{cases} A(n, (n - s)/2, s), & \text{if } T(n, s) < \beta, \\ A(n, 0, s), & \text{if } T(n, s) \geq \beta. \end{cases}$$

and let

$$\kappa = \begin{cases} \frac{B(s) + f(1)}{\bar{A}(n, s) + B(s) + f(n - s) + f(1)} & \text{if } \bar{A}(n, s) > -f(1), \\ 1, & \text{otherwise.} \end{cases} \quad (9)$$

Let H choose a network G such that :

- (i) G has exactly s singletons.
- (ii) G is a maximal core periphery on $n - s$ nodes if $T(n, s) < \beta$.
- (iii) G is a cycle on $n - s$ nodes if $T(n, s) \geq \beta$.

Moreover, suppose that the hider hides in the component of size $n - s$ with probability κ , mixing uniformly on the periphery nodes in the case of the component being a core-periphery network, and mixing uniformly over all its nodes in the case of the component being a cycle. Also, she hides in the singleton nodes with probability $1 - \kappa$, mixing uniformly on them. By similar arguments to those used for λ_S above, $\kappa \in [0, 1]$ and so the strategy is valid.

If the seeker seeks in the singleton nodes, this yields payoff of at least $\kappa f(n - s) - (1 - \kappa)B(s)$ to the hider. Similarly, if the seeker seeks in the core-periphery component, this yields payoff of at least $-\kappa \bar{A}(n, s) + (1 - \kappa)f(1)$ to the hider. With the value of κ , above, both values are equal in the case of $\bar{A}(n, s) > -f(1)$, and the latter is greater, otherwise.

Hence, the strategy guarantees a payoff $-\kappa \bar{A}(n, s) + (1 - \kappa)f(1)$ to the hider. Note that

$$-\kappa \bar{A}(n, s) + (1 - \kappa)f(1) = -\bar{Q}(n, s)$$

As we have mentioned before, $-\bar{Q}(n, s)$ is the maximal payoff the hider can get on any network with exactly s singleton nodes and hence the network constructed above as well as the hiding strategy must be optimal for the hider. \square

Next, consider the case of $n - s$ being odd. The proof of the following lemma is in the Appendix.

Lemma 8. *Suppose that $n - s$ is odd. Then, an optimal strategy for H gives him a payoff of $-Q(n, (n - s - 3)/2, s)$. If $T(n, s) < \beta$, G is optimal if the subnetwork over $n - s$ nodes is a maximal core-periphery network. If $T(n, s) > \beta$, G is optimal if it the subnetwork over $n - s$ nodes is a cycle.*

Since the game is zero-sum, the hider maximises his payoff when the seeker's payoff is minimised. Therefore, an optimal network has $s \in S^*(n)$ singleton nodes, where

$$S^*(n) = \arg \min_{s \in \{0, \dots, n\}} \bar{Q}(n, s).$$

Lemmas 7 and 8 have therefore proved the characterization result that we summarize in the following Theorem.

Theorem 1. *For any number of nodes, $n \geq 1$, and any $\beta \geq 0$ there exists an equilibrium of the game, $((G, h), s)$ such that*

- G has exactly $s \in S^*(n)$ singleton nodes and either $s \leq n - 4$ or $s = n$.
- If $T(n, s) \geq \beta$ and $n - s \geq 4$ then G has a cycle component over the remaining $n - s$ nodes.
- If $T(n, s) < \beta$, $n - s \geq 4$ then G has a maximal core-periphery component over $n - s$ nodes.
- The hider mixes between hiding in the singleton nodes and in the connected component. When hiding in the singleton nodes, he mixes uniformly across all these nodes. When hiding in the connected component, he mixes uniformly across all the nodes (when it is a cycle), mixes uniformly across the periphery nodes (when it is a maximal core-periphery network and $n - s$ is even), and mixes between hiding in periphery nodes, mixing uniformly across them, and the middle orphaned node (otherwise).
- The seeker mixes between seeking in the singleton nodes and in the connected component. When seeking in the singleton nodes, he mixes uniformly across all these nodes. When seeking in the connected component, he mixes uniformly across all the nodes (when it is a cycle), mixes uniformly across the core nodes (when it is a maximal core-periphery network and $n - s$ is even), and mixes between seeking in the neighbours of periphery nodes, mixing uniformly across them, and the middle orphaned node (otherwise).

Equilibrium payoff to the hider is $-\bar{Q}(n, s)$.

We have shown in the proof of Theorem 1, that the equilibrium payoff to the seeker in an optimal network with at least one singleton node is a convex combination of $B(s)$ which is greater than $-f(1)$ and $-f(1)$ and so it is at least $-f(1)$. Hence the payoff that the hider can secure in such a network is at most $f(1)$. Thus if the payoff the seeker can secure in a connected component of size n , $\bar{A}(n, 0)$ is smaller than $-f(1)$, then the payoff the hider can secure in such a component is $-\bar{A}(n, 0) > f(1)$. If that inequality holds, it is optimal for the hider to choose a connected network without singleton nodes.

If, on the other hand, the cost of being caught, β , is sufficiently high then $\bar{A}(n, 0) > -f(1)$ and the payoff the hider can secure in a connected network, $-\bar{A}(n, 0)$, is less than the payoff he gets if he is not caught in a singleton node. This leads the hider to construct a network with a smaller component and $s \geq 1$ singleton nodes. If the cost of being caught is sufficiently high, it is optimal for the hider to choose a disconnected network with $s = n$ singleton nodes.

The characterisation of equilibrium networks provided in Theorem 1 is not complete. This Theorem displays network architectures which achieve the highest possible payoff for the hider, but does not show that these network topologies are unique. As we prove below, if $T(n, s) < \beta$ the connected component must be a maximal core-periphery network. So in this case we obtain a complete characterization of equilibrium networks. If $T(n, s) > \beta$ there exist network topologies other than the cycle which are optimal. We establish necessary properties that the optimal network topologies must possess.

Theorem 2. *For any number of nodes, $n \geq 1$, and any $\beta \geq 0$, if $((G, h), s)$ is an equilibrium of the game then*

- *G has exactly $s \in S^*(n)$ singleton nodes.*
- *If $T(n, s) < \beta$, $n - s \geq 4$, then G has a maximal core-periphery component over $n - s$ nodes.*
- *If $T(n, s) > \beta$, then G has a 2-connected component over $n - s$ non-singleton nodes with at least $\lceil (n - s)/3 \rceil$ nodes of degree 2 and the hider never hides in nodes of degree greater than 2 in equilibrium.*

Proof. The fact that G must have exactly $s \in S^*(n)$ singleton leaves is already established in proof of Theorem 1. For the properties of the remaining part of equilibrium network, we consider the cases of $T(n, s) < \beta$ and $T(n, s) > \beta$ separately.

Suppose that $T(n, s) < \beta$. Suppose first that $n - s$ is even. Since $Q(n, m, s)$ is decreasing in m and the maximum feasible value for m , when $n - s$ is even, is $(n - s)/2$, the subnetwork over $n - s$ non-singleton nodes in any optimal network must have $(n - s)/2$ singleton leaves. If the network is optimal, the neighbours of the singleton leaves must form a 2-connected network. Otherwise, the seeker would obtain a payoff that is strictly higher than $\bar{Q}(n, s)$ by mixing uniformly on the neighbours of non-singleton leaves when seeking outside singleton nodes. This is because in the case of not capturing the hider, he will leave the subnetwork over

$n - s$ nodes disconnected with non-zero probability. Hence the optimal subnetwork over $n - s$ non-singleton nodes must be a maximal core-periphery network.

Second, suppose that $n - s$ is odd. We have shown in proof of Lemma 8 that the optimal number of singleton leaves in the subnetwork over $n - s$ non-singleton nodes is $(n - s - 3)/2$. Moreover, as we argued above, nodes which are not singleton leaves must form a 2-connected network. Thus this subnetwork must be a core-periphery network with 2-connected core and three orphaned nodes.

What remains to be shown is that one of the orphaned nodes must have exactly the other two orphaned nodes as its neighbours in this subnetwork. Since the subnetwork formed by the nodes of the core must be 2-connected, any node of the core must have at least two neighbours. Suppose, to the contrary, that each of the orphaned nodes has at least one neighbour that is not an orphaned node. Then, mixing uniformly on non-orphaned core nodes, the seeker captures the hider with higher probability than in a maximal core-periphery network (regardless of the strategy of the hider) and causes the same damage in the case of not capturing the hider. This results in strictly lower payoff to H than $-\bar{Q}(n, s)$ and so the network is not optimal. Therefore the neighbours of one of the orphaned nodes must be exactly the two other orphaned nodes.

Suppose next that $T(n, s) > \beta$. In this case, $Q(n, m, s)$ is increasing in m and so the optimal network has no singleton leaves in the subnetwork over the $n - s$ non-singleton nodes.

Let U be the set of $n - s$ non-singleton nodes in the network and let F be the subnetwork over this set of nodes. As argued above, the seeker has a seeking strategy that guarantees him a probability of capture at least $3/(n - s)$ in F . If F is not 2-connected, the seeker will leave the subnetwork disconnected in the event of not capturing H . This gives strictly lower payoff to H than in the cycle. Hence F must be 2-connected. Hence all the nodes in F have degree at least 2.

Suppose that F has $t < \lceil (n - s)/3 \rceil$ nodes of degree 2. Note that since F is 2-connected, only one node is removed if H is not captured. So, the expected payoff of H (and hence S) only depends on the probability of capture. Consider any strategy η of H and let T be its support on U . Let σ'_T be a mixed strategy of the seeker that mixes uniformly on $N_F[T]$.⁹ Let $\sigma_T = \lambda \sigma'_T + (1 - \lambda) \sigma^S$ be a strategy of the seeker that mixes uniformly on the singleton nodes with probability $1 - \lambda$ and uses σ'_T with probability λ , where λ is such that the lower bound on the expected payoff to the seeker when the hider hides in T is equal to the lower bound on the expected payoff to the seeker when the hider hides in singleton nodes.

Notice that the lower bound on the expected payoff to the seeker from using σ'_T when the hider hides in T is strictly higher than $3/(n - s)$. For if T contains a node of degree at least 3 then the seeker captures the hider with probability strictly greater than $3/|N_F[T]| \geq 3/(n - s)$, and if T does not contain a node of degree 3 then $|N_F[T]| \leq 3|T| < n - s$ and the seeker captures the hider with probability $3/|N_F[T]| > 3/(n - s)$. Hence there exists $p_T > \bar{Q}(n, s)$ such that the expected payoff to the seeker from using σ_T against any strategy of the hider, η , with support T on U is at least p_T . Taking $\varepsilon = \min_{T \subseteq U} (\bar{Q}(n, s) - p_T)$ shows that

⁹ Given graph $G = \langle V, E \rangle$ and a set of nodes $U \subseteq V$, set $N_G[U] = U \cup \{v \in V : uv \in E \text{ for some } u \in U\}$ is the *closed neighbourhood* of U in G .

F cannot be optimal for H .

Notice also that if the support of H 's strategy in a network with 2-connected component F contains nodes of degree greater than 3 then strategy σ guarantees the seeker payoff strictly greater than $\bar{Q}(n, s)$. Therefore, in equilibrium, the hider never hides in nodes of degree greater than 2 in the 2-connected component of an optimal network. \square

We next provide examples of topologies of the connected component other than the cycle in equilibrium networks for the case of $T(n, s) > \beta$. Suppose that $n - s = 3t$ where $t \geq 2$ is an integer. Let U be the set of nodes of the component. Suppose that the nodes in U are connected, forming a cycle, and let $T \subseteq U$, $|T| = t$, be a subset of the nodes such that any two nodes in T are separated by two nodes from $U \setminus T$. Any network obtained from the cycle by adding links between the nodes in $U \setminus T$ is optimal (an example is presented in Figure 4). Both players mixing uniformly on U is an equilibrium on any such network.

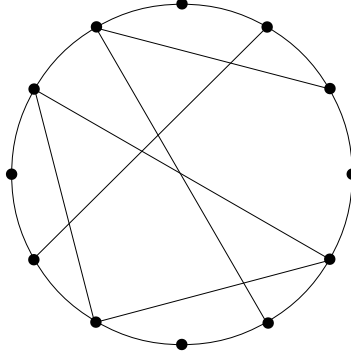


Figure 4: An optimal component for $n - s = 12$.

Theorems 1 and 2 provide a characterization of optimal networks for the hider in terms of the quantity $T(n, s)$. As this expression is not transparent, we provide sufficient conditions on the utility function $f(\cdot)$ which guarantee that the connected component of an optimal network is a maximal core-periphery network.

Theorem 3. *Suppose that either*

- (i) *f is concave, or*
- (ii) *f is convex and for all $x \geq 2$*

$$f(x + 1) < \frac{x}{x - 1} f(x)$$

Then, for all $n \geq 1$, and any $\beta \geq 0$, G is an equilibrium network if and only if G has $s \in S^(n)$ singleton nodes and a maximal core-periphery component over $n - s$ nodes. In addition, if f is linear then $S^*(n) = \{0, 1, n\}$.*

Proof. Notice that

$$T(n, s) = (n - s - 3)\Delta f(n - s - 2) - f(n - s - 2)$$

and

$$T(n, s + 1) = (n - s - 3)\Delta f(n - s - 3) - f(n - s - 2)$$

Hence,

$$\begin{aligned} T(n, s + 1) - T(n, s) &= -(n - s - 3)(\Delta f(n - s - 2) - \Delta f(n - s - 3)) \\ &= -(n - s - 3)\Delta^2 f(n - s - 3). \end{aligned}$$

where $\Delta f(x) = f(x + 1) - f(x)$ is the first-order (forward) difference of f at x and $\Delta^2 f(x) = \Delta f(x + 1) - \Delta f(x)$ is the second-order (forward) difference of f at x . Hence, if f is concave, then $\Delta^2 f(n - s - 3) \leq 0$, and so

$$T(n, s + 1) - T(n, s) \geq 0 \text{ for all } s \leq n - 4$$

In addition $T(n, n - 4) = f(3) - 2f(2)$ which is negative if f is concave and strictly increasing. Thus for all $n \geq 4$ and $s \leq n - 4$, $T(n, s) < 0 \leq \beta$.

From Theorems 1 and 2, G is an equilibrium network if and only if its connected component is a maximal core-periphery network over $n - s$ nodes.

If f is convex then $\Delta^2 f(n - s - 3) \geq 0$ and $T(n, s + 1) - T(n, s) \leq 0$, for all $s \leq n - 4$. Thus $T(n, s)$ is decreasing in s on $[0, n - 4]$, for all $n \geq 4$.

Suppose that $f(x + 1) < x/(x - 1)f(x)$ for all $x \geq 2$.¹⁰ Then $T(n, 0) = (n - 3)f(n - 1) - (n - 2)f(n - 2) < 0$ and so

$$T(n, s) \leq T(n, 0) < \beta, \text{ for all } s \in [0, n - 4].$$

Again, by Theorems 1 and 2, G is an equilibrium network if and only if its connected component is a maximal core-periphery network over $n - s$ nodes.

Next, note that if $n \leq 5$, then Lemma 1 shows that $s^* \leq 1$. Suppose that f is linear and that $n \geq 6$. We show in the Appendix (Lemma 10) that if $n \geq 6$, then $Q(n, (n - s)/2, s)$ is minimised either at $s = 0$ or at $s = 1$ or at $s = n$. This shows that $s^* \in \{0, 1, n\}$ and completes the proof of the theorem. \square

Remark 4. *The theorem establishes a full characterisation of equilibrium networks when f is concave or convex but growing slowly.*

5 Conclusions

We propose and study a strategic model network design and hiding in the network facing a hostile authority that attempts to disrupt the network and capture the hider. We characterise optimal networks for the hider as well as optimal hiding and seeking strategies in these networks. Our results suggests that the hider chooses

¹⁰ An example of a family of strictly increasing convex functions that satisfy this property are the functions $f(x) = x^\gamma/(x + 1)^{\gamma-1}$ with $\gamma > 1$.

networks that allow him to be anonymous and peripheral in the network. We also develop a technique for solving such models in the setup of zero-sum games.

There are at least two avenues for future research. Firstly, different forms of benefits from the network could be considered. For example, the utility of the hider could depend not only on the size of his component but also on his distance to the nodes in the component. Given our results, we conjecture that this would make the core periphery components with better connected core more attractive. But answering this problem precisely requires formal analysis. Secondly, the seeker could be endowed with more than one seeking unit and the units could be used either simultaneously or sequentially. Our initial investigation suggests that solving such an extension might be an ambitious task.

References

- Felia Allum, Isabella Clough Marinaro, and Rocco Sciarrone. *Italian Mafias Today: Territory, Business and Politics*. Edward Elgar Publishing, 2019.
- M. Baccara and H. Bar-Isaac. How to organize crime. *The Review of Economic Studies*, 75(4):1039–1067, 2008.
- Egon Balas. *Will to freedom: a perilous journey through fascism and communism*. Syracuse University Press, 2008.
- Francesco Calderoni. The structure of drug trafficking mafias: the ‘Ndrangheta and cocaine. *Crime, law and social change*, 58(3):321–349, 2012.
- Diego A Cerdeiro, Marcin Dziubiński, and Sanjeev Goyal. Individual security, contagion, and network design. *Journal of Economic Theory*, 170:182–226, 2017.
- Serge Curvat, Denise Domenach-Lallich, Chantal Duprat-Odet, François-Yves Guillin, and Henri Hours. *Lieux Secrets de la Resistance: Lyon 1940-1044*. Editions Lyonnaises d’Art et d’Histoire, 2015.
- Marcin Dziubiński and Sanjeev Goyal. Network design and defence. *Games and Economic Behavior*, 79:30–43, 2013.
- Marcin Dziubiński and Sanjeev Goyal. How do you defend a network? *Theoretical Economics*, 12(1):331–376, 2017.
- D. Fisher. Two person zero-sum games and fractional graph parameters. *Congressus Numerantium*, 85:9–14, 1991.
- D. Fisher. Fractional dominations and fractional total dominations of graph complements. *Discrete Applied Mathematics*, 122:283–291, 2002.
- S. Goyal and A. Vigier. Attack, defence, and contagion in networks. *The Review of Economic Studies*, 81(4):1518–1542, 2014.
- Rohan Gunaratna. *Inside Al Qaeda: global network of terror*. Columbia University Press, 2002.
- Valdis E Krebs. Mapping networks of terrorist cells. *Connections*, 24(3):43–52, 2002.
- Carlo Morselli, Cynthia Giguère, and Katia Petit. The efficiency/security trade-off in criminal networks. *Social Networks*, 29(1):143–153, 2007.
- E. Scheinerman and D. Ullman. *Fractional Graph Theory*. Wiley, New York, 1997.
- John Von Neumann. A certain zero-sum two-person game equivalent to the optimal assignment problem. *Contributions to the Theory of Games*, 2(0):5–12, 1953.

- M. Waniek, T. Michalak, T. Rahwan, and M. Wooldridge. On the construction of covert networks. In *Proceedings of the 16th Conference on Autonomous Agents and MultiAgent Systems*, AAMAS'17, pages 1341–1349, Richland, SC, 2017. International Foundation for Autonomous Agents and Multiagent Systems.
- M. Waniek, T. Michalak, M. Wooldridge, and T. Rahwan. Hiding individuals and communities in a social network. *Nature Human Behaviour*, 2:139–147, 2018.

Appendix

Derivation of $A(n, ms)$

Using value of λ_R , the lower bound on the payoff of player S in G when H hides outside singleton nodes is

$$L(n, m, s) = L^R(n, m, s) = L^M(n, m, s) = (1 - \lambda_S) A(n, m, s) - \lambda_S f(n - s) \quad (10)$$

where

$$A(n, m, s) = \begin{cases} \frac{\beta}{m} - \left(\frac{m-1}{m}\right) f(n - s - 2), & \text{if } R(G) = \emptyset, \\ \left(\frac{D(n, s)D(n-1, s)}{3D(n, s) - 2D(n-1, s)}\right) \left(\frac{3(\beta - T(n, s))}{m(3D(n, s) - 2D(n-1, s)) + (n-s)D(n-1, s)} - 1\right) + \beta, & \\ \text{otherwise} \end{cases}$$

with

$$D(n, s) = f(n - s - 1) + \beta$$

and

$$T(n, s) = (n - s - 3)D(n, s) - (n - s - 2)D(n - 1, s) + \beta$$

In particular, the derivation above is valid for the extreme cases of $m = 0$ and $m = (n - s)/2$. Notice that $A(n, m, s)$ is strictly increasing in m if $T(n, s) > \beta$, is strictly decreasing in m if $T(n, s) < \beta$, and is constant if $T(n, s) = \beta$.

We now derive the formula for $A(n, m, s)$. By Equations (6) and (7)

$$A(n, m, s) = (1 - \lambda_R) \left(\left(\frac{1}{m}\right) \beta - \left(1 - \frac{1}{m}\right) f(n - s - 2) \right) - \lambda_R f(n - s - 1)$$

If $R(G) = \emptyset$ then, by (4), $\lambda_R = 0$ and so

$$A(n, m, s) = \left(\frac{1}{m}\right) \beta - \left(1 - \frac{1}{m}\right) f(n - s - 2).$$

If $R(G) \neq \emptyset$ then, by (4), $\lambda_R = \rho$ and

$$A(n, m, s) = (1 - \rho) \left(\left(\frac{1}{m}\right) \beta - \left(1 - \frac{1}{m}\right) f(n - s - 2) \right) - \rho f(n - s - 1), \quad (11)$$

where

$$\begin{aligned} \rho &= 1 - \frac{3m(f(n - s - 1) + \beta)}{3m(f(n - s - 1) + \beta) + (n - s - 2m)(f(n - s - 2) + \beta)} \\ &= 1 - \frac{3mD(n, s)}{3mD(n, s) + (n - s - 2m)D(n - 1, s)} \\ &= 1 - \frac{3mD(n, s)}{Z(n, m, s)} = \frac{(n - s - 2m)D(n - 1, s)}{Z(n, m, s)} \end{aligned}$$

where

$$Z(n, m, s) = m(3D(n, s) - 2D(n - 1, s)) + (n - s)D(n - 1, s).$$

Equation (11) can be rewritten as

$$\begin{aligned}
A(n, m, s) &= -(1 - \rho) \left(\frac{(m - 1)(f(n - s - 2) + \beta)}{m} \right) - \rho \left(\frac{m(f(n - s - 1) + \beta)}{m} \right) + \beta \\
&= -(1 - \rho) \left(\frac{(m - 1)D(n - 1, s)}{m} \right) - \rho \left(\frac{mD(n, s)}{m} \right) + \beta \\
&= \frac{-3(m - 1)D(n, s)D(n - 1, s) - (n - s - 2m)D(n, s)D(n - 1, s)}{Z(n, m, s)} + \beta \\
&= X(n, s)Y(n, m, s) + \beta
\end{aligned}$$

where

$$X(n, s) = \frac{D(n, s)D(n - 1, s)}{3D(n, s) - 2D(n - 1, s)}$$

and

$$\begin{aligned}
Y(n, m, s) &= \frac{(3D(n, s) - 2D(n - 1, s))(-3(m - 1) - (n - s - 2m))}{Z(n, m, s)} \\
&= \frac{(3D(n, s) - 2D(n - 1, s))(-m - (n - s - 3))}{Z(n, m, s)} \\
&= \frac{3(\beta - T(n, s)) - Z(n, m, s)}{Z(n, m, s)} \\
&= \frac{3(\beta - T(n, s))}{Z(n, m, s)} - 1.
\end{aligned}$$

This complete the derivation of $A(n, m, s)$.

Proofs

Proof of Lemma 8

Suppose that $n - s$ is odd. Then, an optimal strategy for H gives him a payoff of $-Q(n, (n - s - 3)/2, s)$. If $T(n, s) < \beta$, G is optimal if the subnetwork over $n - s$ nodes is a maximal core-periphery network. If $T(n, s) > \beta$, G is optimal if it the subnetwork over $n - s$ nodes is a cycle.

Proof. Let

$$\bar{A}(n, s) = \begin{cases} A(n, (n - s - 3)/2, s), & \text{if } T(n, s) < \beta, \\ A(n, 0, s), & \text{if } T(n, s) \geq \beta. \end{cases}$$

and let κ be defined as in (9). If $T(n, s) \geq \beta$ then choosing a cycle over $n - s$ nodes and using the same hiding strategy as in the case of $n - s$ being even, the hider secures the highest possible payoff on a network with exactly s singleton nodes.

Suppose that $T(n, s) < \beta$. Since $(n - s)/2$ is not an integer, the hider cannot attain the upper bound on his payoff determined by the lower bound on the payoff to the seeker, $\bar{Q}(n, s)$. Recall that if $T(n, s) < \beta$ then for any $0 \leq s \leq n - 4$, $Q(n, m, s)$ is decreasing in m . We show below for any $0 \leq s \leq n - 4$, the hider can

attain payoff $-Q(n, (n-s-3)/2, s)$, and that this is the maximal payoff he can secure when $n-s$ is odd.

Suppose that the hider chooses a maximal core-periphery network (with three orphaned nodes) over $n-s$ nodes (c.f. Figure 5).

Consider a strategy of the hider

$$\boldsymbol{\eta} = \kappa(\mu\boldsymbol{\eta}^M + (1-\mu)\boldsymbol{\eta}^R) + (1-\kappa)\boldsymbol{\eta}^S,$$

where

$$\eta_i^M = \begin{cases} \frac{1}{m}, & \text{if } i \in SL(G), \\ 0, & \text{otherwise,} \end{cases}$$

(i.e. $\boldsymbol{\eta}^M$ mixes uniformly on the periphery nodes of G),

$$\eta_i^R = \begin{cases} 1, & \text{if } i \text{ is the middle orphaned node in } G, \\ 0, & \text{otherwise,} \end{cases}$$

$$\eta_i^S = \begin{cases} \frac{1}{s}, & \text{if } i \in S(G), \\ 0, & \text{otherwise.} \end{cases}$$

(i.e. $\boldsymbol{\eta}^S$ mixes uniformly on the singleton nodes of G), and

$$\mu = \frac{(n-s-3)f(n-s-2) + (n-s-3)\beta}{(n-s-3)f(n-s-1) + 2f(n-s-2) + (n-s-1)\beta}.$$

It is immediate to see that $\mu \in [0, 1]$ and so the hiding strategy is valid. If the seeker seeks in the orphaned nodes of the core-periphery component, this yields payoff of at least $\kappa(\mu f(n-s-1) - (1-\mu)\beta) + (1-\kappa)f(1)$ to the hider and, since the game is zero-sum, of at most minus this value to the seeker. Similarly, if the seeker seeks in periphery nodes or their neighbours in the core-periphery component, this yields payoff of at least $\kappa(\mu(-2\beta/(n-s-3) + (1-2/(n-s-3))f(n-s-2)) + (1-\mu)f(n-s-2)) + (1-\kappa)f(1)$ to the hider and of at most minus this value to the seeker. With the value of μ , above, both these guarantees are equal.

It is straightforward to verify that

$$\begin{aligned} \kappa(\mu f(n-s-1) - (1-\mu)\beta) + (1-\kappa)f(1) &= -\kappa A(n, (n-s-3)/2, s) + (1-\kappa)f(1) \\ &= -Q(n, (n-s-3)/2, s). \end{aligned}$$

Since $Q(n, (n-s-3)/2, s)$ is a lower bound on the payoff that the seeker can secure in a network with exactly s singleton nodes and at most $(n-s-3)/2$ singleton leaves, the negative of this value is the highest payoff that the hider can secure in a network with exactly s singleton nodes and at most $(n-s-3)/2$ singleton leaves. The only networks that could yield a higher payoff to the seeker are networks with exactly s singleton nodes and $(n-s-1)/2$ singleton leaves. But we show in Lemma 9 that these networks have a lower value for the hider. \square

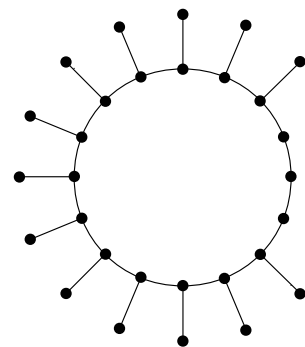


Figure 5: A core-periphery network over 23 nodes with 3 orphaned nodes.

Lemma 9. *If $n - s$ is odd and $T(n, s) < \beta$, the hider obtains a higher expected payoff in a core-periphery network with $(n - s - 3)/2$ singleton leaves than in a core-periphery network with $(n - s - 1)/2$ singleton leaves.*

Proof. In a core-periphery network with $(n - s - 1)/2$ singleton leaves, the set $R(G)$ consist of exactly one node and this node is connected to at least two nodes in $M(G)$. It cannot be connected to one node in $M(G)$, because in this case its neighbour would have two leaf-neighbours and could not be a member of $M(G)$.

Let $\tilde{\sigma} = \lambda\sigma^S + (1 - \lambda)\sigma^M$, where σ^M and σ^S are the mixed strategies of the seeker, defined earlier in the proof,

$$\lambda = \begin{cases} \frac{X(n, s) + f(1)}{B(s) + X(n, s) + f(1) + f(n - s)}, & \text{if } X(n, s) > -f(1), \\ 0, & \text{otherwise,} \end{cases}$$

and

$$X(n, s) = \frac{2\beta}{n - s - 1} - \left(1 - \frac{2}{n - s - 1}\right) f(n - s - 2).$$

Using this strategy, with probability λ , S mixes uniformly on the nodes in $M(G)$ and with probability $(1 - \lambda)$, S mixes uniformly on the singleton nodes of G . The payoff to S conditional on H hiding in a singleton node is at least $\lambda B(s) - (1 - \lambda)f(1)$ and the payoff to S conditional on H hiding outside singleton nodes is at least $(1 - \lambda)X(n, s) - \lambda f(n - s)$. It is easy to verify that the value of λ is such that both these payoffs are equal (in the case of $X(n, s) > -f(1)$) or the latter is higher, for any value of λ . Therefore the payoff to S from using $\tilde{\sigma}$ against any strategy of H is at least

$$Y(n, s) = \begin{cases} \frac{B(s)X(n, s) - f(1)f(n - s)}{B(s) + X(n, s) + f(1) + f(n - s)}, & \text{if } X(n, s) > -f(1), \\ X(n, s), & \text{otherwise,} \end{cases}$$

and so the upper bound on the payoff to the hider on any network with s singleton nodes and $(n - s - 1)/2$ singleton leaves is at most $-Y(n, s)$. To see that $-Q(n, (n - s - 3)/s, s) > -Y(n, s)$ notice that

$$X(n, s) - A(n, (n - s - 3)/2, s) = \frac{2(f(n - s - 1) - f(n - s - 2))(f(n - s - 2) + \beta)(n - s - 3)}{(n - s - 1)(f(n - s - 1)(n - s - 3) + 2f(n - s - 2) + \beta(n - s - 1))} > 0$$

and so $X(n, s) > A(n, (n - s - 3)/2, s)$.

Next consider the following Claim:

Claim 1. *The function*

$$\varphi(Z) = \begin{cases} \frac{B(s)Z - f(1)f(n - s)}{Z + B(s) + f(n - s) + f(1)}, & \text{if } Z > -f(1), \\ Z, & \text{otherwise,} \end{cases}$$

is strictly increasing in Z .

Proof. Notice that $\varphi(-f(1)) = -f(1)$ when $Z = -f(1)$. Moreover, φ is increasing in Z if $Z < -f(1)$. Let $Z > -f(1)$. Taking the derivative of φ with respect to Z we get

$$\varphi'(Z) = \frac{(B(s) + f(1))(B(s) + f(n-s))}{(Z + B(s) + f(n-s) + f(1))^2}$$

and it is immediate to see that $\varphi'(Z) > 0$ and φ increases in Z when $B(s) > -f(1)$ and $B(s) \geq -f(n-s)$. Notice that $B(s) = (\beta + f(1))/s - f(1) > -f(1)$ for any $\beta \geq 0$ and $s > 0$. Also $f(n-s) \geq f(1)$ for all $s \in [0, n-1]$. Thus, by the observation on function φ , above, $\varphi(Z)$ increases when Z increases. \square

Claim 1, together with $X(n, s) > A(n, (n-s-3)/2, s)$, implies that $Y(n, s) > Q(n, (n-s-3)/2, s)$, completing the proof of the Lemma. \square

Lemma 10. *Let $\lambda > 0$ and let $f(x) = \lambda x$, for all $x \in \mathbb{R}_{\geq 0}$. For any natural $n \geq 6$, $t \in \{0, 1\}$ and any $s \in \{t+1, \dots, n\}$, $Q(n, (n-s)/2, s) > \min(Q(n, 0, n), Q(n, (n-t)/2, t))$*

Proof. Let $f(x) = \lambda x$, with $\lambda > 0$, and let $\tilde{\beta} = \beta/\lambda$. Let

$$\tilde{A}(n, s) = A(n, (n-s)/2, s) = \lambda \left(2 \left(\frac{\tilde{\beta} - 2}{n-s} \right) + 4 - (n-s) \right), \text{ for } 0 \leq s \leq n-2,$$

$$B(s) = \lambda \left(\frac{\tilde{\beta} + 1}{s} - 1 \right),$$

and

$$\tilde{Q}(n, s) = Q(n, (n-s)/2, s) = \begin{cases} \tilde{A}(n, s), & \text{if } \tilde{A}(n, s) \leq -\lambda \text{ or } s = 0, \\ AB(n, s), & \text{if } 1 \leq s \leq n-2 \text{ and } \tilde{A}(n, s) > -\lambda \\ B(n), & \text{otherwise,} \end{cases}$$

with

$$AB(n, s) = (1 - \rho)\tilde{A}(n, s) - \rho\lambda(n-s) \tag{12}$$

where ρ solves

$$(1 - \rho)\tilde{A}(n, s) + \rho\lambda(s-n) = \rho B(s) - (1 - \rho)\lambda. \tag{13}$$

Solving (13) we get

$$\rho = \frac{s(2(\tilde{\beta} - 2) - (n-s)(n-s-5))}{s(2(\tilde{\beta} - 2) - (n-s)(n-s-5)) + (n-s)(s(n-s-1) + \tilde{\beta} + 1)}.$$

Notice that $2(\tilde{\beta} - 2) - (n-s)(n-s-5) > 0$ if and only if $\tilde{A}(n, s) > -\lambda$, and $(n-s)(s(n-s-1) + \tilde{\beta} + 1) > 0$ for $s \leq n-1$. Thus if $\tilde{A}(n, s) > -\lambda$ then $\rho \in (0, 1)$. In addition $B(s) > -\lambda$, for all $s > 0$, so if $\rho \in (0, 1)$ then $AB(n, s) > -\lambda$. Moreover, $\tilde{A}(n, s)$ is increasing in s on $[0, n-2]$ and it is equal to β at $s = n-2$. By the

observations above, if $\tilde{A}(n, 1) \leq -\lambda$ then $\bar{Q}(n, 0) = \tilde{A}(n, 0) < \tilde{A}(n, 1) = \tilde{Q}(n, 1) \leq -\lambda < \bar{Q}(n, s)$, for all $s \in \{2, \dots, n\}$, and the claim of the lemma holds.

For the remaining part of the proof suppose that $\tilde{A}(n, 1) > -\lambda$. This implies $2(\tilde{\beta} - 2) > (n - 1)(n - 6)$ and, consequently, $\tilde{\beta} > 2$ if $n \geq 6$. We will show that $\tilde{Q}(n, s)$ is either decreasing or first increasing and then decreasing on $[0, n - 1]$. Let $\tilde{s} = \inf\{s \in [0, n - 2) : \tilde{A}(n, s) \geq -\lambda\}$. Since $\tilde{A}(n, s)$ is increasing in s and equal to $\beta \geq 0$ at $s = n - 2$ so the infimum exists and \tilde{s} is well defined. On $[0, \tilde{s}]$, $\tilde{Q}(n, s) = \tilde{A}(n, s)$ and, as we argued above, $\tilde{Q}(n, s)$ is increasing. Consider the interval $[\tilde{s}, n - 1]$. Notice that since $B(s) > -\lambda \geq -\lambda(n - s)$, for all $0 < s \leq n - 1$, and $\tilde{A}(n, \tilde{s}) = -\lambda$ so $AB(n, \tilde{s}) = -\lambda$. In addition, $AB(n, n) = B(n)$. We will show that $AB(n, s)$ is either decreasing or first increasing and then decreasing on $[0, n]$. Inserting ρ into (12) we get

$$AB(n, s) = \frac{(n^2(\tilde{\beta} + 1) - 2n(s(\beta/\lambda - 1) + 2(\tilde{\beta} + 1)) + s^2(\tilde{\beta} - 3) + 6s\tilde{\beta} - 2(\tilde{\beta} + 1)(\tilde{\beta} - 2))}{s(4s - \tilde{\beta} + 5) - n(4s + \tilde{\beta} + 1)}.$$

Taking the derivative of $AB(n, s)$ with respect to s we get

$$\frac{\partial AB(n, s)}{\partial s} = \frac{(\tilde{\beta} + 1)W(s)}{(s(4s - \tilde{\beta} + 5) - n(4s + \tilde{\beta} + 1))^2},$$

where

$$W(s) = Xs^2 - 2Ys + \left(n + \frac{\tilde{\beta} - 2}{2}\right)Y - \left(\frac{\tilde{\beta} - 2}{2}\right)(n - 4)(\tilde{\beta} + 1),$$

with $X = 4n - \tilde{\beta} - 15$ and $Y = 4n^2 + n(\tilde{\beta} - 19) - 8(\tilde{\beta} - 2)$.

The sign of $\partial AB/\partial s$ is the same as the sign of $W(s)$. Notice that $W(n) = -2(\tilde{\beta} - 2)(n + \tilde{\beta} - 5) < 0$, as $n \geq 6$ and $\tilde{\beta} > 2$. When $X > 0$, then $W(s)$ is an \cup -shaped parabola and, since $W(n) \leq 0$, either W is negative or W is first positive and then negative on $[0, n]$. Thus in this case AB is either increasing or first increasing and then decreasing on $[0, n]$. Similar observation holds when $X = 0$. Suppose that $X < 0$. In this case $W(s)$ is an \cap -shaped parabola and it has a maximum at $s^* = Y/X$. Suppose that $s^* \in (0, n - 2)$. Since $X < 0$ so $Y < 0$. Moreover, for $n \geq 6$, $X < 0$ implies $\beta > 5$ and, consequently,

$$\begin{aligned} W(s^*) &= -Ys^* + \left(n + \frac{\tilde{\beta} - 2}{2}\right)Y - \left(\frac{\tilde{\beta} - 2}{2}\right)(n - 4)(\tilde{\beta} + 1) \\ &= \left(n - s^* + \frac{\tilde{\beta} - 2}{2}\right)Y - \left(\frac{\tilde{\beta} - 2}{2}\right)(n - 4)(\tilde{\beta} + 1) < 0. \end{aligned}$$

Thus W is either negative or first positive then negative on $[0, n]$, for any natural $n \geq 5$. Hence ABQ is either decreasing or first increasing and then decreasing on $[0, n]$, for any natural $n \geq 6$.

By the analysis above, when $\tilde{A}(n, 1) > -\lambda$ then $AB(n, s)$ is either decreasing or first increasing and then decreasing in s on $[0, n]$ and $AB(n, n) = B(n)$. Hence, by the definition of $\tilde{Q}(n, s)$, the claim of the lemma follows immediately. \square