Network performance under attacks

I. Arribas\textsuperscript{a,b,c}, V. Luna\textsuperscript{a}, A. Urbano\textsuperscript{a,c}

\textsuperscript{a}Universitat de Valencia, Edificio Departamental Oriental, Campus del Tarongers, 46022 - Valencia, Spain
\textsuperscript{b}Ivie, Calle Daniel Balaciart, 3 - bajo, 456020 - Valencia, Spain
\textsuperscript{c}ERI-CES, Universitat de Valencia, c/Serpis 29, 46022 - Valencia, Spain

Abstract

The paper is a contribution to the study of robustness in economic and social networks. Unlike connectivity models, our robustness metric is based on network performance, which evaluates the system behavior and measures the flow or traffic among nodes. The paper develops a sequential model of network defense with two players, the Network Defender and the Network Attacker. Given a network, the Network Defender chooses a node communication path that maximizes the information transmission (the traffic flow) inside the network by means of a Gravity model subject to node capacity constraints. Then, a two-stage game between Network Defender and the Network attacker takes place. In the first stage, the Network Defender chooses a set of nodes to protect, where protecting a node is costly. In the second stage, the Network Attacker observes the defended network and decides whether to attack a set of nodes; attacking a node is costly. The subgame perfect equilibrium of this game, which is parameterized by the defense and attack costs, is obtained.

Keywords: Complex networks, network performance, network flow, gravity model, subgame perfect equilibrium.

JEL Classification: C72, C44.

\textsuperscript{*}Ivan Arribas and Amparo Urbano wish to thank the Ministry of Economics and Competitivity under projects ECO2016-75575-R, and the Generalitat Valenciana under the Excellence Programs PrometeoII/2014/054 and ISIC 2012/021 for their financial support

Email addresses: ivan.arribas@uv.es (I. Arribas), victor.luna@uv.es (V. Luna), amparo.urbano@uv.es (A. Urbano)
1. Introduction

Infrastructure, information transmission and traffic networks play an important role in current Economy. Communication networks, transports and interbank connections are only a few examples of this vital and crucial role. For this reason, there is nowadays much interest in the robustness of real-networks and the aim of this paper is to understand which topological features are desirable in communication networks in order to prevent node failures produced by targeted attacks.

This paper develops a sequential model of network defense with the following features: there are two players, the Network Defender and the Network Attacker. Given a network, the Network Defender chooses a node communication path that maximizes the performance (the traffic flow) inside the network. Then a two-stage game between the Network Defender and the Network Attacker takes place. In the first stage, the Network Defender chooses a set of nodes to protect; protecting a node is costly. Then, the Network Attacker observes the defended network and decides whether to attack a set of network nodes; attacking a node is costly. Namely, we analyze a model in which a complex network is given. The network consists of N nodes, each of them could be interpreted as an economic agent (for instance: a bank, a firm, a transport station, etc.). A link connecting a pair of nodes means the existence of a relationship between them. As the benchmark model, we consider perfect defense and perfect attack: a defended node is immune to attack and an undefended node is eliminated by attack. When an undefended node is attacked, this node and all its links are removed from the network. Then, we extend this model to consider imperfect defense and attack and compare its results with the benchmark model.

The value of the network is characterized by its performance. The network together with the choice of defense and attack define a residual network. The value of the residual network depends on the performance of the surviving network. The goal of the Network Defender is to maximize the value of the residual network less the cost of defense, while the objective of the Network Attacker is to minimize the value of the residual network plus the cost of attack. We study the subgame
perfect Nash equilibrium of this game.

There are two questions which deserve some clarification. First, as already said, the value of the network depends on the performance of its nodes. There are mainly two metrics to compare topologies with similar node degree distribution but different topological structure: Network connectivity and Network performance. \textit{Network performance evaluates the system behavior.} Performance is a measure of the maximum flow or traffic among nodes. \textit{The value of the network is the maximum flow of the surviving nodes.} In our model robustness is the ability of a network to maintain its total level of flow under removal of nodes and consequently links and where flows are the behavior occurring within a network. Therefore the performance considers flows within a giant components as well as flows within fragments components. This latter consideration is important because depending of the phenomenon under consideration, nodes with segmented components can interact and contribute to the robustness of the network. For instance, in the epidemic domain, virus propagation continues within subcomponents even though a giant component ceases to exist. The initial level of flow in a network determines its initial robustness. As nodes are removes the level of flow can change considerably and as a result, topologies which appear robust at the onset may potentially disintegrate as few nodes are removed.

Network performance is an important concept highly studied in other fields like Computer Science but it is just mentioned in a handful papers of Economic and Social Networks. One of the contributions of this paper is to introduce and use this metric in the study of Economic Networks. As an introductory example, in Figure 1, borrowed from Alderson \textit{et al.} (2005) we compare the performance and the physical distribution of several computer networks.

In this example we can see that identical networks from a node degree perspective could have completely different features. In the case that concern us, in figure 1 networks with the same node-degree distribution have different measure of performance. It highlights that the importance of finding a good design for the networks going beyond the simple study of the node degree, which is the usual
thing in the economic networks literature.

We use the London Underground Network\(^1\), for simplicity we use only stations from zone 1, as a simple but a real network to illustrate the surviving flow as a different useful metric to measure the importance of each node inside its network.

In this example, the network maximum performance is the maximum passengers flow that the network is able to maintain. Here, the maximum value is 31,235, which comes from maximizing the passengers flow which go into/out each node, as a kind of propensity to send/receive passengers of each node of the network, all of them subjected to some capacity constraints (see section 2), in this case we used the number of platforms of each station. In Figure 2, we use different colours to show the node degree of each station and its size to highlight the importance of

\(^1\)This data is available at github.com/jaron/railgraph/blob/master/graphs/tubeDLR.gephi
each node in this network using node performance (the loss of performance that
the network would have if this node were attacked and deleted). Figure 3 shows
that there does not exist a strong correlation between our metric and the node
degree. Interestingly, we can see that the most important station using our metric
is not the one with the biggest degree, is King Cross St.Pancrass, the station which
was attacked in July 2005.

![Figure 3: Correlation between Performance and node degree. Being $R^2 = 0.2964$ (Determination coefficient)](image)

We compare different metrics used by Jackson (2010) to describe the impor-
tance and centrality of each node with the loss of performance to verify that our
results are different and new, because we obtain a different rank of the importance
of each node inside the network. As an example, in figure 4 we can check the absence
of strong correlation between our metric and two of the most used metrics
in the literature, closeness and betweenness.

Our metric is related to other centrality measures which are more usual in
connectivity models (the node degree mainly), but, as our results show, the node
ranking is different. For this reason, the performance metric gives a new kind of
information that only the node degree. This is so because the former takes the
degree as a factor to calculate the capacity constraints of each node and analyzes
the maximum performance allowed by a network under the capacity of each node
to send/receive information. This results in a new and more realistic point of view
to study network performances. For instance, in our example, an attack to King Cross station implies a loss of the 28% of the traffic flow that this network could perform.

Second, irrespectively of the field of study, networks generally contain constraining components. For the case where a node is the constrained element, network performance is a suitable metric to evaluate such topologies. For instance, in the Internet network, where links capacities may be over provisioned, a metric for the constrained component of this network is the router and the constraints would be all router degree-bandwidths constrains.

In the context of network theory, a complex network is a graph with non-trivial topological features. These features do not occur in simple networks such as lattices or random graphs but often occur in real graphs. The study of complex networks is a young and active area of scientific research inspired largely by the empirical study of real-world networks such as computer networks and social networks. Most social, economic, biological, and technological networks display substantial non-trivial topological features, with patterns of connection between their elements that are neither purely regular nor purely random. Such features include a heavy tail in the degree (number of links) distribution of the nodes, a high clustering coefficient, assortativity or disassortativity among vertices, community structure, and hierarchical structure. The node degree distribution is very important to study social networks, such as the Internet, and more simple networks. A simple network model, for example, the (Bernoulli) random graph, in which each pair of nodes is connected (or not) with independent probability $p$ (or
1 − p), has a binomial degree distribution \( k \) or Poisson degree distribution for a large number of nodes. Most networks in the real world, however, have degree distributions very different from this. Most are highly right-skewed, meaning that a large majority of nodes have low degree but a small number, known as "hubs", have high degree. Some networks, notably the Internet, the world wide web, and some social networks are found to have degree distributions that approximately follow a power law: the probability to find a node with degree \( k \) is proportional to \( k^{-\gamma} \), where \( \gamma \) is a constant. Such networks are called scale-free networks and have attracted particular attention for their structural and dynamical properties. Complex networks may become significantly vulnerable to random failures and targeted attacks and exhibit cascading failures.

In our network model, which depends on the node degree probability distribution, the value of the residual network is the performance of the surviving nodes. Once we obtain the maximum value of this performance for any given network, we find the subgame Nash equilibrium for a general node capacity function, which can be a linear, a concave or a convex function of each node degree. The equilibrium is parameterized by the defense and attack costs, for a given node degree probability distribution.

Our paper contributes to the economic study of complex networks and their defense. The research of networks has been mainly concerned with their formation and structure of economic networks. For a survey of this work see Jackson (2010). Another interesting survey about different applications of networks in Economics is available in Allen and Babus (2009).

Dziubiski and Goyal (2013b) studies the problem of the defense of a simple given network focusing in the connectivity of this network with constant costs of attack and defense. Similar models which include network formation and contagion, but with simple networks and constant costs, could be found in Dziubiski and Goyal (2013) and Goyal and Vigier (2013). The importance of robustness in networks, following the previous model, is presented in Goyal and Vigier (2010).

In the present paper, we also assume that the Network Defender and the Net-
work. Attacker optimize the value of the residual network but, in contrast our network is complex; we focus on the network performance, the flow across the network, which depends on both the number of links and the capacity function of the nodes. We assume that defense and attack costs are a function of the node degree, a more realistic approximation because if a node has a bigger degree he will need more protection (e.g. if the train station A is bigger than train station B, A needs more security, so the defense costs of A will be bigger than that of B).

To maximize the flow traffic or performance among the nodes in the network we have adopted a gravity model. This model is perhaps one of the simplest models to such a goal: it assumes that the traffic between two nodes is proportional to the total traffic from the sender node to the receiver node. In network theory, the gravity model has been used in a handful paper of other disciplines like Computer Science and Physics. Hung et al. (2010) use the linear programming and the gravity model to optimize an objective function. Other papers, like Zhang et al. (2003) and Gunnar et al. (2004), present different approaches to the traffic matrix estimation, which are focused on Internet and Computer Networks. In our paper we maximize a network traffic matrix using nonlinear programming to get the network payoffs. This is a new point of view on the Social and Economic Networks. This new approach represents the functioning of real networks better than the connectivity approach\(^2\). Internet plays an important role in our society and in our economy, for this reason it is interesting to know the way in which this complex network is formed. Alderson et al. (2005) and Doyle et al. (2005) focus on this topic. In our paper, we use complex networks which follow scale free distributions too, like Internet does.

Other related papers on network games and financial networks are: Cabrales et al. (2014); Elliot et al. (2013); Montagna and Lux (2013) and Galleoti and Vega-Redondo (2011). These papers are focused on Complex Networks and defense and contagion in financial networks. To learn more about network games we recommend Galleoti et al. (2010).

\(^2\)For more information about optimization of robustness in complex networks, the lector can consult Paul et al. (2004)
The rest of the paper is organized as follows. Section 2 presents the benchmark model of defense and attack in networks with perfect and complete information, the network performance and the network gravity model are introduced as a subsection. In section 3 perfect equilibria with a linear node capacity function and perfect information are analyzed. In section 4, the model is modified to allow imperfect information and the Bayesian equilibria under imperfect information is discussed. Section 5 concludes the paper.

2. The benchmark model

We consider two players: a Network Defender (ND) and a Network Attacker (NA). They start with a given network with n nodes. The ND chooses a node communication path that maximizes the performance (the traffic flow) inside the network. Then a two-stage game takes place. In the first stage, the ND chooses a set of nodes to protect; protecting a node is costly. In the second stage, NA observes the defended network and decides whether to attack a set of nodes; attacking a node is costly. The network together with the choice of defense and attack define a residual network. The value of the residual network depends on the performance of the surviving nodes. The goal of ND is to maximize the value of the residual network less the cost of defense. For this reason he chooses a set of nodes of the given network to defend. The objective of the Network Attacker is to minimize the value of the residual network plus the cost of attack. We assume that NA chooses a single node to attack. For simplicity, we consider first perfect defense (a defended node always stays in the network) and perfect attack (an attacked node, which is undefended, is removed from the network). Then, we assume imperfect defense and attack and compare the corresponding equilibria.

Formally, let $N = \{1, 2, 3 \ldots n\}$, with $n \geq 2$, be a finite set of nodes (e.g. agents, companies, etc.). An edge is a link between a pair of nodes $\{i, j\}$ (or its abbreviation $ij$), we assume undirected links so $ij$ implies $ji$. Let $k_i$ be the degree of the node $i$, in other words, the number of links from $i$ to other nodes in $g$. The complex network is characterized by a degree distribution $P(k)$ (the probability of having a node with degree $k$ in our network).
Let $G$ be the set of all possible links combinations with a given $N$, being $g(P)$ an instance of $G$. Every network $g(P) \in G$ has a performance $\varphi(g(P)), \varphi : G \rightarrow R$, associated with it.

In the first stage of the game, the ND chooses his defense. A defense is a set of nodes $D \subseteq N$; a node $j \in N$ is defended under $D$ if and only if $j \in D$. Defense is costly, the cost of defending a node depends on its degree, so the defense cost of node $i$ is $c^D_i = \alpha \cdot k_i$. In the second stage, the NA chooses her attack. The attack is a set of nodes $A \subseteq N$. We assume that only one element is allowed in this set. Attack is also costly, the cost of attacking a node depends on its own degree, hence the cost attack of node $i$ is $c^A_i = \beta \cdot k_i$. We assume positive costs, so that $c^D_i, c^A_i \geq 0$.

Let $\varphi(g(P) - (A/D))$ be the value, in terms of performance, of the residual network, that is the network $g(P)$ without the set of nodes resulting from $(A/D)$. The payoff of ND when he chooses $D$, and NA chooses $A$, is:

$$\Pi_{ND}(g(P), D, A, \alpha) = \varphi(g(P) - (A/D)) - \alpha \cdot \sum_{i \in D} k_i$$

The payoff of NA is:

$$\Pi_{NA}(g(P), D, A, \beta) = -\varphi(g(P) - (A/D)) + \beta \cdot k_A$$

The goal of ND is to maximize the value or performance of the residual network at minimum cost. On the other hand, NA wants to minimize this value, taking into account her attack cost.

Before obtaining the subgame perfect Nash Equilibrium of this sequential NA-ND game, we have to analyze first the maximum performance of $g(P)$, where network performance has been defined as $\varphi(g(P)) : G \rightarrow R$.

2.1. Network performance

We start with the analysis of a model based on the performance problem: here the ND gains a payoff which depends on the information flows among the surviving
nodes. We have assumed that the network value function is the performance of $g(P)$ and thus we have to define next the meaning of network performance.

The measure of the network performance is assumed to be the information flow or volume of traffic flow between sets of nodes. Information flows or, in short, traffic, originate from a sender (or source) and is delivered to a receiver or several receivers (a destination or several destinations). The traffic traverses a set of links between some set of nodes. The links connecting nodes define the topology of the network, and the path chosen by traffic flows determine the routing. A traffic matrix is naturally represented by a matrix $X$, with $i-j$th matrix entry $x_{ij}$. Each entry represents the amount of information sent (the traffic volume) measured in terms of information units from source $i$ to destination $j$, i.e., a real number. Following Alderson et al. (2005), we define network performance as the maximum throughput on the network under heavy traffic conditions based on a gravity model.

Thus the network performance will be given by the traffic matrix which, in a nutshell, is an abstract representation of the traffic volume in the network. Each element of the matrix denotes the amount of traffic between a source and a destination pair. Amount here, in the networking context, is generally measured in the number of information units (i.e., bits) but could refer to other quantities such as messages, information amount, etc. The NDs goal is to maximize the traffic matrix or volume of traffic flow by organizing such a flow in the network subject to several constraints. For example, optimization includes finding the shortest paths for flows but also, importantly, load balancing to ensure that links remain uncongested.

Irrespective of the field of study, networks generally contain constraining components. For the case where a node is the constrained element, network performance is a suitable metric to evaluate such topologies. For instance, in the Internet network, where links capacities may be over provisioned, a metric for the constrained component of this network is the router and the constraints would be all router degree-bandwidths constrains. In our case, we assume that nodes have constraints and denote by $B_i$ the capacity of the node $i$. Then, capacity
constraints depend on the node degree, \( B_i = f(k_i) \) where \( f \), capacity function, is a general function of \( k \).

2.2. How to model an information flow matrix? The gravity model

We wish to focus on the properties of traffic between source and destination pairs, without regard to how the traffic changes in time. The gravity model is perhaps one of the simplest models to such a goal: it assumes that the traffic between two nodes is proportional to the total traffic from the source node to the destination node.

The name of the model derives from Newtons model of gravitation, where the gravitational force is proportional to the product of the mass of two objects divided by the distance between them squared. The general formulation of the gravity model is defined by two forces: the repulsive force (factor) \( R_i \), associated with leaving from \( i \) and the attractive force (factor) \( A_j \), associated with going into \( j \). Its general form is described by the following equation:

\[
x_{i,j} = \frac{R_i \cdot A_j}{f_{i,j}}
\]

where \( f_{i,j} \) represents the friction factor, which describes the weakening of the forces (akin to distance in Newtons model), depending on the physical structure of the modeled phenomenon. The model has been used extensively in various fields, for instance the modeling of street traffic. In the context of communication network, for instance Internet traffic matrix modeling, the friction factors have typically been taken to be constant. That is, distance is assumed to have little effect on information network traffic. Where distance is ignored, the above equation becomes

\[
x_{i,j} = \frac{x_{i}^{\text{in}} \cdot x_{j}^{\text{out}}}{x_{\text{total}}}
\]

where \( X^{\text{in}} \) is the total traffic entering the network through \( i \), \( X^{\text{out}} \) is the total traffic exiting the network through \( j \) and \( X^{\text{total}} \) is the total traffic across the network. The assumption that none of the nodes act as a source or sink of traffic (i.e., that
traffic is conserved in the network), implies that

\[ x^{total} = \sum_{i \in N} x^{{in}}_i = \sum_{j \in N} x^{{out}}_j \]

With this model at hand, maximizing the performance of \( g(P) \) subject to capacity constraints, means maximizing the flow of traffic information inside this network. Let \( x^{{in}}_i \) be the information flow which goes into the node \( i \), and \( x^{{out}}_i \) the information flow which goes out of this node. Then, the following problem has to be solved:

\[
\varphi^*(g) = \max_{x^{{in}}, x^{{out}}} \frac{\sum_{i=1}^{n} \sum_{j=1,j\neq i}^{n} r_{ij} \cdot x^{{in}}_i \cdot x^{{out}}_j}{\sum_{i=1}^{n} x^{{in}}_i} \tag{3}
\]

subject to

\[
R(g(P)) \cdot X \leq B \cdot \sum_{i=1}^{n} x^{{in}}_i \tag{4}
\]

\[
\sum_{i=1}^{n} x^{{in}}_i = \sum_{i=1}^{n} x^{{out}}_i \tag{5}
\]

\[ x^{{in}}, x^{{out}} \geq 0 \]

- \( R(g(P)) \) is the Routing Matrix (dimensions: \( n \times n \cdot (n - 1) \)), which depends on \( g(P) \), for simplicity \( R \). This matrix shows the set of nodes which are included in the shortest path between each pair of nodes in the network \( g \). Its elements could be 0 or 1. \( R_{i,kj} = 1 \) means that node \( i \) is part of the shortest path from \( k \) to \( j (k \neq j) \). The shortest path between two nodes, \( k \) and \( j \), is the most economical way to go from \( k \) to \( j \).

- \( X \) is the Traffic Vector (Dimensions: \( n \cdot (n - 1) \times 1 \)). Its components are \( x^{{in}}_i \cdot x^{{out}}_j, i \neq j \), \( X = (x^{{in}}_1 \cdot x^{{out}}_2, x^{{in}}_1 \cdot x^{{out}}_3, \ldots, x^{{in}}_i \cdot x^{{out}}_j, \ldots, x^{{in}}_n \cdot x^{{out}}_{(n-1)}) \).

- \( B \) is the Capacity constraint vector (Dimensions: \( n \times 1 \)). \( B_i \) is the capacity of node \( i \). We will assume that capacity constraints depend on the node degree, \( B_i = f(k_i) \), where \( f \) is a general function of \( k_i \).

- \( r_{ij} \) is the same-component characteristic function, it could be 0 or 1, \( r_{ij} = 1 \)
meaning that node \( i \) and node \( j \) are in the same graph component. This parameter does not play any role when networks are connected.

This is a nonlinear programming problem, with a quadratic objective function and nonlinear constraints. Nevertheless a solution always exists, since the objective function is continuous and is maximized in a compact set.

3. Equilibrium analysis under perfect information

To calculate the subgame perfect equilibrium, we need to know the maximum network performance. The subgame perfect equilibrium will depend on the node capacity constraints, given that the budgets of NA and ND are exogenously given and that the defense and attack are perfect. First, we have to analyze the network maximum performance.

**Proposition 1.** Let \( g(P) \) be a network with node capacity constraints \( f(k_i) \), then the maximum network performance value has an upper bound equal to \( \varphi^*(g) \leq \sum_{i=1}^{n} f(k_i) \)

Proposition 1 shows that there exists an upper bound of network performance and it can be calculated, regardless of the type of capacity constraints that have been established. Having an upper bound allows us to have a simple way to compare different networks according the percentage of performance respect to the maximum possible. For some networks the upper bound is always reach as we show in Propositions 2 and 3.

**Proposition 2.** Let \( g \) be a complete network with node capacity constraints \( f(k_i) \), then the maximum network performance value is \( \varphi^*(g^{C}) = \sum_{i=1}^{n} f(k_i) = \frac{n \cdot f(n-1)}{2} \).

**Proposition 3.** Let \( g \) be a star network with node capacity constraints \( f(k_i) \) and with node 1 as the central node, then the maximum network performance value is \( \varphi^*(g^{S}) = \min(\sum_{i=2}^{n} f(k_i), f(k_1)) = \min((n - 1) \cdot f(1), f(n - 1)). \)
An important intuition of propositions 2 and 3 is that it suffices that nodes have a degree bigger than zero to have a positive network performance, and it does not matter whether the network gets the information flow through one or more components. Therefore, our model works even if the graph is not connected, which is a significant advantage over connectivity models mentioned in the introduction. Each component, with size bigger than 1, takes part in the performance of the whole network (i.e. any component in which its nodes have positive degree). Therefore, our model is compatible with epidemical models, e.g. virus propagation on the internet, which we mentioned in the introduction.

### 3.1. Linear capacity constraints

The simplest scenario is when capacity constraints depend linearly on the node degree: \( f(k_i) = m \cdot k_i \). In this case, the upper bound for the maximum network performance is always reached in complete and stars networks. A corollary of Propositions 1, 2 and 3 is:

**Corollary 1.** The maximum performance value under linear capacity constraints has an upper bound equal to \( \phi^*(g) \leq \frac{m \cdot \sum \limits_{i=1}^{N} k_i}{2} \). For the complete network is \( \phi^*(g) = \frac{m \cdot n \cdot (n-1)}{2} \) and for the star network is \( \phi^*(g) = \frac{m \cdot (n-1)}{2} \).

Corollary 1 is the direct implication of propositions 1 to 3 in the case of linear capacity constraints.

The next Proposition offers a characterization of the subgame perfect equilibrium of networks achieving the maximum performance value under linear capacity constraints. First:

**Lemma 1.** Let \( V(g) = \phi^*(g) \) be the network performance under linear capacity constraints of \( g(P) \). The maximum performance of the residual network, under a targeted attack of node \( i \) is \( \phi^*(g - i) \leq V(g) - m \cdot k_i \).

**Convention 1.** For simplicity, we assume that the nodes are decreasingly ordered by their degree. If \( i < j \rightarrow k_i \geq k_j, \forall i, j \in N \).
In the first stage, a strategy for ND is to choose his defense set: \( D \in S_D \), being \( S_D \) the set of \( 2^N \) feasible strategies that he has (all the possible combinations of sets with \( N \) nodes, including the empty set). It is easy to see that all of these actions are dominated by three strategies: not to defense \( D = \emptyset \); defense the \( i \) most important nodes, \( D = \{1 \ldots i\} \); and defense the whole network, \( D = N \). In the second stage, a strategy for NA is to choose his attack set: \( A \in S_A \), being \( S_A = N \cup \emptyset \) the set of feasible strategies that she has, all of them are dominated by two strategies, to attack the first undefended node, \( A = \{i + 1\} \) or not to attack, \( A = \emptyset \); as we show in the proof of Preposition 4.

Then, a combination of \((D^*, A^*)\) is a solution of this game if:

\[
\Pi_{ND}(g(P), D^*, A^*, \alpha) \geq \Pi_{ND}(g(P), D, A^*, \alpha) \forall D \in S_D
\]

and

\[
\Pi_{NA}(g(P), D^*, A^*, \beta) \geq \Pi_{NA}(g(P), D^*, A, \beta) \forall A \in S_A
\]

In proposition 4 we show the Nash equilibria depending on the attack and defense costs \( \alpha \) and \( \beta \):

**Proposition 4.** Consider the NA-ND game of network \( g \), where the network and all its subnetworks achieve the maximum performance value under linear capacity constraints of node degree, and with linear (on node degree) defense and attack costs \((\alpha, \beta)\). Then, at equilibrium:

- If \( \beta > m \), then \( D^* = \emptyset \) and \( A^* = \emptyset \).

- If \( \alpha > m \) and \( \beta < m \), then \( D^* = \emptyset \) and \( A^* = \{1\} \), i.e. the NA attacks the biggest node.

- If \( \alpha, \beta < m \), then \( D^* = \{1 \ldots i^*\} \) and \( A^* = \{i^* + 1\} \), where \( i^* \) is the node satisfying that: \( i^* \in \arg\min_i (\alpha \cdot \sum_{l=1}^i k_l + m \cdot k_{i+1}) \). The ND defends a set of nodes and the NA attacks the first unprotected node.

An important intuition of Propositions 2 and 3 is that the maximum value of the network performance (the upper bound) is achieved only if there are not
information flows between nodes which are not neighbors from each other. This is the case in star networks and complete networks, but also in some other irregular networks. Consider next the characterization of the subgame perfect equilibrium of networks which does not achieve the maximum performance value even under linear capacity constraints.

The NA will attack the undefended node \( i \) whenever \( \varphi^*(g) - \varphi^*(g - \{i\}) \geq \beta \cdot k_i \), this meaning that the loss of performance if NA attacks node \( i \) is bigger than the NA attacking cost. For this reason, to better understand the equilibrium of this game and study the most interesting scenarios, we suppose that the NA is interested in attacking any node:

**Assumption 1.** \( \frac{\varphi^*(g) - \varphi^*(g - \{i\})}{k_i} > \beta, \forall i \in N \)

To find the subgame perfect equilibrium, ND would like to protect some nodes but he cannot protect all of them. Let us assume the following condition:

**Assumption 2.**

\[
\frac{\varphi^*(g) - \varphi^*(g - \{i + 1\})}{\sum_{l=1}^{i+1} k_l} < \alpha < \frac{\varphi^*(g) - \varphi^*(g - \{i\})}{\sum_{l=1}^{i} k_l}
\]

Assumption 2 is easy to understand, if there is a value of parameter \( \alpha \) in which this condition is satisfied, then ND will be interested in defending a set of nodes \( C = \{1 \ldots i\}, 1 \leq i < n \). If he defends the next node \( i + 1 \), then the cost of this defense will be bigger than the value of performance saved, if NA will attack \( i + 1 \).

If \( g(P) \) is quite homogeneous in the sense that all the nodes have a similar number of links (as in Poisson networks) the difference between the upper and lower bounds of Condition 1 will be small. Therefore, for low \( \alpha \) values a big set of nodes will be protected and for high \( \alpha \) values none will be protected. On the other hand, if \( g(P) \) has nodes with a huge number of links or hubs (as in a Scale Free network) and if nodes are decreasingly ordered by their degree (Convention 1), then there will be a node \( i \) with degree \( k_i \) followed by a node \( i + 1 \) with degree \( k_{i+1} \), with \( k_i >> k_{i+1} \), and a defense cost interval and an attack cost interval such that ND will defend \( \{1 \ldots i\} \) and NA will attack \( i + 1 \).
Proposition 5. Consider the NA-ND game of networks which does not achieve the maximum performance value even under linear capacity constraints of the node degree, with costs \((\alpha, \beta)\). Assume that convention 1 is satisfied and that attacking costs are low enough. Then, at equilibrium:

(i) If there is a nodes \(\{i^*\}\) that satisfies Assumption 2. Then \(D^* = \{1 \ldots i^*\}\) and \(A^* = \{i^* + 1\}\).

(ii) If there is a set of nodes \(C = \{i_1, i_2, \ldots, i_t\}\), \(t > 1\), such that all of them satisfy Assumption 2, then the solution \(\{i^*, j^*\}\) must satisfy

\[
i^* \in \arg \max_{(i,j) \in C} (\varphi^*(g - \{j\}) - \alpha \sum_{l=1}^{i} l)
\]

Then \(D^* = \{1 \ldots i^*\}\) and \(A^* = \{j^*\}\).

(iii) If no nodes satisfies Assumption 2. Then:

\(- D^* = \emptyset\) and \(A^* = \{1\}\) if \(\alpha > \frac{\varphi^*(g) - \varphi^*(g - \{1\})}{k_1}\),

\(- D^* = N\) and \(A^* = \emptyset\) if \(\alpha > \frac{\varphi^*(g) - \varphi^*(g - \{1\})}{k_1}\).

The intuition of Propositions 1-5 is as follows. First, if \(g(P)\) has nodes with a huge number of links (Scale Free networks), there should be an interval of defense costs such that the set of nodes protected by ND are those with the higher degree, the hubs, which are the most important nodes to maintain the network performance. On the other hand, if \(g(P)\) is a more homogeneous network (Poisson network), then this defense cost interval is either much smaller or does not exist. Second, for very low defense costs ND will defend the whole network, whatever the degree distribution of \(g(P)\).

For simplicity, we have assumed linear capacity constraints. Equivalent results can be found under convex or convex capacity constraints. In fact, propositions 1, 2 and 3 are obtained in a general context and they could be used for any kind of capacity constraint function.
4. The model under imperfect information

In the benchmark model, defense and attack were always successful, for this reason NA would never attack a defended node. In this section, we allow the attack and the defense to fail with some probability. Then, we add the following two parameters:

- $\delta_A \in [0, 1]$ Successful attack probability
- $\delta_B \in [0, 1]$ Successful defense probability

Let $J$ be the different combinations of successful/unsuccessful attack and defense, where

$$J = (1 - S_{A \cap D}) \cdot [\delta_A \cdot \varphi(g - A) + (1 - \delta_A) \cdot \varphi(g)] + (S_{A \cap D}) \cdot [(1 - \delta_A \cdot (1 - \delta_D)) \cdot \varphi(g) + \delta_A \cdot (1 - \delta_D) \cdot \varphi(g - A)]$$

$$S_{A \cap D} = \begin{cases} 0, & A \cap D = \phi \\ 1, & A \cap D \neq \phi \end{cases}$$

Then, the expected payoff of ND when he chooses $D$, and NA chooses $A$, is:

$$E[\Pi_{ND}(g(P), D, A, \alpha)] = J - \alpha \cdot \sum_{i \in D} k_i$$

On the other hand, the expected payoff of NA, when only one attack is allowed, is:

$$E[\Pi_{NA}(g(P), D, A, \beta)] = -J - \beta \cdot k_a$$

The goal of ND is to maximize the expected value or performance of the residual network at minimum cost. On the other hand, NA wants to minimize this value (considering her attack cost).

4.1. Equilibrium analysis under imperfect information

In this section we briefly consider the impact that a change on informational assumptions could have in our model. In section 2, the analysis is done under perfect and complete information. Now, we relax this assumption allowing complete but imperfect information, in other words, the NA and the ND have the same
information but there is unknown information for both of them, they dont know their ability to attack or defend successfully.

We study the Bayesian Equilibria of a complex network, under the benchmark model assumptions and the following ones:

- Imperfect attack and defense. Being $\delta_A \in [0, 1]$ Successful attack probability and $\delta_D \in [0, 1]$ Successful defense probability

- Let $V(g)$ be the network performance $\varphi(g(P))$, and $\varphi(g(P) - \{i\}) = V(g) - V_i(g)$. In other words, $V_i(g)$ is the loss of performance in the network $g(P)$ if the node $i$ is removed.

In the first stage of the game the ND choose a set of nodes to defense $D \in S_D$ (see subsection 3.1), being all the feasible actions dominated by: $D = \emptyset$; $D = \{1\ldots i\}$ and $D = N$. The ND does not know if he is a good defender or not, having $\delta_D$ of success.

In the second stage, the NA observes the defended network, she knows which nodes are defended but she does not know neither if the defense is successful or not, and decide whether attack or not. The NA has three information sets in which could be placed $\{I_N^{NA}, I_i^{NA}, I_N^{NA}\}$ (e.g: If the ND defens $D = \{1, 2\}$, then the NA will be in the information set $I_i^{NA}$ because she knows the defended nodes but not if the defense is successful or not). Then an attack strategy $A$ will be a 3-tupla of her possible actions in each information set. The feasible actions are dominated by: $\emptyset$; $\{1\}$ and $\{j\}$ (being $j$ the first non defended node). The NA does not know if she is a good attacker or not, having $\delta_A$ of success.

The three components of $A$ are the actions played by the NA if she were placed in the following decision nodes (information sets):

- Information set $\emptyset$ (attack strategy if ND plays $D = \emptyset$)

- Information set $i$ (attack strategy if ND plays $D = \{1\ldots i\}; 1 \leq i < N$),

- Information set $N$ (attack strategy if ND plays $D = N$)

20
We solve this game via backwards induction for given \((\alpha, \beta)\) and the successful defense and attack probabilities \((\delta_D, \delta_A)\), being the bayesian equilibria the set of the strategies \((D^*, A^*)\) which accomplishes:

\[
E[\Pi_{ND}(g(P), D^*, A^*, \alpha)] \geq E[\Pi_{ND}(g(P), D, A^*, \alpha)] \ \forall D \in S_D
\]

and

\[
E[\Pi_{NA}(g(P), D^*, A^*, \beta)] \geq E[\Pi_{NA}(g(P), D^*, A, \beta)] \ \forall A \in S_A
\]

In Proposition 6 we show a table with the bayesian equilibria under imperfect information depending on \(\alpha\) and \(\beta\) parameters \((\delta_D\) and \(\delta_A\) are given) with \(n\) nodes.

**Proposition 6.** Consider the NA-ND game with imperfect information, with linear (on node degree) costs \((\alpha, \beta)\). Then at equilibrium:

Insert Table 3 here

4.2. The case of the n-Complete Network

We analyze the Bayesian Equilibria of the n-Complete Network, under the same assumptions we have made in this section.

The ND has two dominant strategies: \(D = \emptyset\) and \(D = \{i\}\) (being \(i\) any node in the network). It is easy to prove that the only three possible performances in that case are:

- The maximum performance (no node is successfully attacked)

\[\varphi^*(g) = \frac{(n - 1) \cdot n}{2}\]

- A node is successfully attacked.

\[\varphi^*(g) = \frac{(n - 1) \cdot (n - 2)}{2}\]
In the first stage of the game ND chooses a set of nodes to defense among the above two possibilities: $D = \emptyset; D = N$. The ND knows that the defense has a probability $\delta_D$ of success. This information is also known by ND.

In the second stage, NA observes the defended network and decides whether to attack (only one type of attack is possible in a complete network). NA knows that her attack has a probability $\delta_A$ of success. This information is also common knowledge. When the NA attacks, she could do it in three decision nodes (depending on the ND strategy):

- Decision Node $\emptyset$ (attack strategy if ND plays $D = \emptyset$)
- Decision Node $N$ (attack strategy if ND plays $D = N$)

In the following tables we show a comparison between the equilibria under perfect and imperfect information (with imperfect information, the NAs strategy is a set with the three decisions that she would play in each decision node). In the first table the equilibria is obtained for any size of the network, in the second table we offer the results for big complete networks ($n \to +\infty$).

**Corollary 2.** Consider a ND-NA game in a n-complete network. Then at equilibrium:

---

Insert Table 4 here

---

### 4.3. The case of the n-Star Network

We analyze the Bayesian Equilibria of the n-Star Network, under the same assumptions we have made in this section.

The ND has three dominant strategies: $D = \emptyset; D = N$ and $D = \{1\}$ (being 1 the central node in the Star Network). It is easy to prove that the only three possible performances in that case are:

- The maximum performance (no node is successfully attacked)

$$\varphi^*(g) = n - 1$$
A peripheral node is successfully attacked.

\[ \varphi^*(g - \{i\}) = n - 2 \]

– The central node is successfully attacked

\[ \varphi^*(g - \{1\}) = 0 \]

In the first stage of the game ND chooses a set of nodes to defense among the above three possibilities: \( D = \emptyset; D = N \) and \( D = \{1\} \). The ND knows that the defense has a probability \( \delta_D \) of success. This information is also known by ND.

In the second stage, NA observes the defended network and decides whether to attack (only two attacks are possible in a star network, a peripheral node or the central one). NA knows that her attack has a probability \( \delta_A \) of success. This information is also common knowledge. When the NA attacks, she could do it in three decision nodes (depending on the ND strategy):

– Decision Node \( \emptyset \) (attack strategy if ND plays \( D = \emptyset \))

– Decision Node \( i \) (attack strategy if ND plays \( D = \{1\} \))

– Decision Node \( N \) (attack strategy if ND plays \( D = N \))

In the following tables we show a comparison between the equilibria under perfect and imperfect information (with imperfect information, the NAs strategy is a set with the three decisions that she would play in each decision node). In the first table the equilibria is obtained for any size of the network, in the second table we offer the results for big star networks \( (n \to +\infty) \).

**Corollary 3.** Consider a ND-NA game in a n-star network. Then at equilibrium:

---

Insert Table 5 here

---

23
The following example compares the different equilibria under perfect and imperfect information; it is easily seen that under imperfect information five new possible equilibriums appear.

**Example 1.** Equilibrium analysis: Star network with $n = 10$ with $\delta_A = \delta_D = 1$ (perfect information)

![Equilibrium analysis: star network with perfect information.](image)

![Table 1: Equilibria in Star Network with perfect information](image)

<table>
<thead>
<tr>
<th>Equilibrium</th>
<th>$e = {D,{A_0;A_i;A_N}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>${0,{0;0;0}}$</td>
</tr>
<tr>
<td>21</td>
<td>${0,{1;i;0}}$</td>
</tr>
<tr>
<td>22</td>
<td>${1,{1;i;0}}$</td>
</tr>
<tr>
<td>23</td>
<td>${N,{1;i;0}}$</td>
</tr>
</tbody>
</table>

D: The ND’s strategy (he could play $D = \emptyset; D = i$ and $D = N$)

A-$i$: The NAs strategy in the decision node $i$ (Being $A_0$ the strategy that NA follows if the ND plays $D = \emptyset$; $A_i$ the strategy that NA follows if the ND plays $D = 1$; $A_N$ the strategy that NA follows if the ND plays $D = N$)

**Example 2.** Equilibrium analysis: Star network with $n = 10$ with $\delta_A = 0.7$ and $\delta_D = 0.4$ (imperfect information)

D: The NDs strategy (he could play $D = \emptyset; D = i$ and $D = N$)

A-$i$: The NAs strategy in the decision node $i$ (Being $A_0$ the strategy that NA follows if the ND plays $D = \emptyset$; $A_i$ the strategy that NA follows if the ND plays $D = 1$; $A_N$ the strategy that NA follows if the ND plays $D = N$)
Figure 6: Equilibrium analysis: star network with imperfect information.

Equilibrium $e=\{D,\{A_0;A_i;A_N\}\}$

<table>
<thead>
<tr>
<th>Equilibrium</th>
<th>$e={D,{A_0;A_i;A_N}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>${0,{0;0;0}}$</td>
</tr>
<tr>
<td>21</td>
<td>${0,{1;i;0}}$</td>
</tr>
<tr>
<td>22</td>
<td>${1,{1;i;0}}$</td>
</tr>
<tr>
<td>23</td>
<td>${N,{1;i;0}}$</td>
</tr>
<tr>
<td>31</td>
<td>${0,{1;i;1}}$</td>
</tr>
<tr>
<td>32</td>
<td>${1,{1;i;1}}$</td>
</tr>
<tr>
<td>33</td>
<td>${N,{1;i;1}}$</td>
</tr>
<tr>
<td>41</td>
<td>${0,{1;1;1}}$</td>
</tr>
<tr>
<td>42</td>
<td>${1,{1;1;1}}$</td>
</tr>
</tbody>
</table>

Table 2: Equilibria in Star Network with imperfect information

$D = 1; A_N$ the strategy that NA follows if the ND plays $D = N$

5. Concluding remarks

Recently, there has been much interest in the robustness of real-world networks to intentional attack failures. This paper develops a model in which the robustness of a given complex network depends on the network performance obtained by solving a nonlinear programming problem subject to node capacity constraints.

Given a network, the Network Defender chooses a node communication path that maximizes the information transmission (the traffic flow) inside the network by means of a Gravity model subject to node capacity constraints, and a set of nodes to protect; protecting a node is costly. Then, the Network Attacker observes
the defended network and decides whether to attack a set of nodes; attacking a node is costly. The network together with the choice of defense and attack define a residual network. The value of the residual network depends on the performance of the surviving nodes. The goal of the Network Defender is to maximize the value of the residual network less the cost of defense, while the objective of the Network Attacker is to minimize the value of the residual network, less the cost of attack. We study the subgame perfect Nash equilibrium of this game.

Network performance is a measure of the maximum flow or traffic among nodes. In our model robustness is the ability of a network to maintain its total level of flow under removal of nodes and consequently links and where flows are the behavior occurring within a network. We have adapted the Gravity model to our purposes. The gravity model is perhaps one of the simplest models: it assumes that the traffic between two nodes is proportional to the total traffic from the source node to the destination node. The model can be interpreted as in terms of the principle of maximum entropy, in the sense of Shannons information Theory. The main critique to the model is its main assumption: the independence between each source $i$ and destination $j$. Most traffic between node pairs are determined by connections, so there could be dependences between pair connections.

Our main results are the characterization of the subgame perfect Nash equilibrium between the Network Defender and the Network Attacker for any capacity constraint function. The equilibrium is parameterized by the defense and attack costs, for a given node degree probability distribution. It is shown that there is an interval of defense costs such that the Network Defender will protect a set of nodes. This interval will depend on the degree probability distribution. Thus, when the network has nodes with a huge number of links, the set of nodes protected by the Network Defender are those with the higher degree, the hubs. When the network has a more homogeneous degree probability distribution, then this defense cost interval will be either much smaller or will not exist. Finally, for very low defense costs the Network Defender will defend the whole network, whatever the network degree distribution. In section 4, we extend our results to imperfect information,
finding the bayesian equilibria.

Our model contributes to the study of economic and social networks, and it could be the first step in a new field of study of the robustness based on the flow and network performance. The future research could be addresses in two directions. 1) To extend the present model letting the Network Attacker attack a set of nodes, i.e. not only one node; 2) another possible extension is to introduce a new model for traffic matrix that takes into consideration the bidirectional nature of many connections and apply it to financial markets.

References


nologies, architectures, and protocols for computer communications (pp. 301-312). ACM.

6. Appendix A

Proof of Proposition 1

Proof. General capacity means that \( B_i = f(k_i) \). We need to prove that the maximum performance always satisfies

\[
\frac{\sum_{i=1}^{n} \sum_{j=1, j \neq i}^{n} x_i^{in} \cdot x_j^{out}}{\sum_{i=1}^{n} x_i^{in}} \leq \frac{\sum_{i=1}^{n} B_i}{2}
\]  

Without loss of generality assume that the network is connected, then any node \( k \) is linked with any other node and hence \( R_{k,ij} = 1 \) if and only if \( i = k \) or \( j = k \) or \( k \) is participating in the shortest path between \( i \) and \( j \). Otherwise \( R_{k,ij} = 0 \). For a generic node \( k \), equation (4), consisting of \( N \) constraints, one for each node, can be rewritten as

\[
x_k^{in} \cdot \sum_{j=1, j \neq k}^{n} x_j^{out} + x_k^{out} \cdot \sum_{i=1, i \neq k}^{n} x_i^{in} + \sum_{i=1, i \neq k}^{n} \sum_{j=1, j \neq k}^{n} R_{k,ij} \cdot x_i^{in} \cdot x_j^{out} \leq f(k_k) \cdot \sum_{i=1}^{n} x_i^{in}
\]

Let \( e_k = \sum_{i=1, i \neq k}^{n} \sum_{j=1, j \neq k}^{n} R_{k,ij} \cdot x_i^{in} \cdot x_j^{out} \) and let \( h_k \) be the constraint slackness. Then,

\[
x_k^{in} \cdot \sum_{j=1, j \neq k}^{n} x_j^{out} + x_k^{out} \cdot \sum_{i=1, i \neq k}^{n} x_i^{in} + e_k + h_k = f(k_k) \cdot \sum_{i=1}^{n} x_i^{in}
\]

with \( e_k, h_k \geq 0 \). Since the network is connected, properly rewriting the right hand side of equation (3) shows that:
\[
\varphi^*(g) = \frac{\sum_{k=1}^n (x_k^m \cdot \sum_{j=1,j\neq k}^n x_j^o + x_k^o \cdot \sum_{i=1,i\neq k}^n x_i^m)}{2 \cdot \sum_{i=1}^n x_i^m} \leq \frac{\sum_{k=1}^n (x_k^m \cdot \sum_{j=1,j\neq k}^n x_j^o + x_k^o \cdot \sum_{i=1,i\neq k}^n x_i^m + e_k + h_k)}{2 \cdot \sum_{i=1}^n x_i^m} = \frac{\sum_{k=1}^n (f(k) \cdot \sum_{i=1}^n x_i^m)}{2} = \frac{\sum_{k=1}^n f(k)}{2} \tag{9}
\]

**Proof of Proposition 2**

**Proof.** Since we have a complete network any node \(k\) is linked directly with any other node in this network, for this reason \(R_{k,ij} = 1\) if and only if \(i = k\) or \(j = k\) (i.e. if \(j\) and \(i\) are not \(k\), there is a direct link between them and \(k\) is not participating on it). Hence, in expression (9), \(e_k = 0\) for any \(k \in N\), then:

\[
x_k^m \cdot \sum_{j=1,j\neq k}^n x_j^o + x_k^o \cdot \sum_{i=1,i\neq k}^n x_i^m \leq f(k) \cdot \sum_{i=1}^n x_i^m \tag{10}
\]

As each node has only direct links with any other node, we expect the same behavior for each \(x_j^o\) and each \(x_i^m\). Thus we can rewrite inequality (10) as:

\[
x^m \cdot (n-1) \cdot x^o + x^o \cdot (n-1) \cdot x^m \leq f(n-1) \cdot n \cdot x^m
\]

\[
2 \cdot x^o \cdot (n-1) \leq f(n-1) \cdot n
\]

\[
2 \cdot x^o \cdot (n-1) + h = f(n-1) \cdot n
\]

Since \(x^{OUT}\) depends only of \(n\), there is not loss of generality in assuming that \(h = 0\) in the above expression and then \(x^o = \frac{f(n-1) \cdot n}{2(n-1)} = x^m\) (by constraint 5).

This value of \(x^o\) and \(x^m\) implies \(e_k + h_k = 0\), and then inequality (7) in Prop. 1 is \(x_k^m \cdot \sum_{j=1}^n x_j^o + x_k^o \cdot \sum_{i=1}^n x_i^m = f(k) \cdot \sum_{i=1}^n x_i^m\) and \(\varphi^*(gC) = \frac{\sum_{k=1}^n f(k)}{2}\).

Since \(gC\) is a complete network \(k_k = n-1\) then \(\varphi^*(gC) = \frac{\sum_{k=1}^n f(k)}{2} = n \cdot f(n-1)\)

**Proof of Proposition 3**

**Proof.** In a star network \((gS)\) only one node \(k\) (for simplicity node 1) is linked
directly with any other node in the network, and the rest of the nodes are only linked to 1. For this reason \( R_{1,ij} = 1 \forall i, j \) and \( R_{k,ij} = 0, \forall k \neq 1 \) and \( \forall i, j \neq k \). Thus, equation (4) can be rewritten as:

\[
Node 1: \sum_{i=1}^{n} \sum_{j=1, j \neq i}^{n} x_{i}^{in} \cdot x_{j}^{out} \leq f(N - 1) \cdot \sum_{i=1}^{n} x_{i}^{in} \tag{11}
\]

\[
Node k \neq 1: x_{k}^{in} \cdot \sum_{j=1, j \neq k}^{n} x_{j}^{out} + x_{k}^{out} \cdot \sum_{i=1, i \neq k}^{n} x_{i}^{in} \leq f(1) \cdot \sum_{i=1}^{n} x_{i}^{in} \tag{12}
\]

It can also be assumed that the central node will have only input or output performance and the peripheral nodes the opposite performance. Let \( x_{k}^{in} = 0 \), when \( k \neq 1 \), then equation (12) is:

\[
x_{k}^{out} \cdot \sum_{i=1, i \neq k}^{n} x_{i}^{in} + x_{k}^{in} \cdot x_{k}^{out} \leq f(1) \cdot \sum_{i=1}^{n} x_{i}^{in} \cdot x_{k}^{out} \rightarrow
\]

\[
\rightarrow x_{k}^{out} \cdot \sum_{i=1}^{N} x_{i}^{in} \leq f(1) \cdot \sum_{i=1}^{n} x_{i}^{in} \rightarrow x_{k}^{out} \leq f(1)
\]

Then

\[
x_{k}^{out} = f(1) + h \text{ and } \sum_{i=1}^{n} x_{i}^{out} = (n - 1) \cdot (f(1) + h) \tag{13}
\]

where \( h \) is the slackness condition of these \((n - 1)\) constraints.

Using \( x_{k}^{in} = 0 \) and equation (5) in equation (11):

\[
x_{1}^{in} \cdot \sum_{j=2}^{n} x_{j}^{out} \leq f(N - 1) \cdot \sum_{i=1}^{n} x_{i}^{in} \rightarrow x_{1}^{in} \leq f(n - 1)
\]

Then

\[
x_{1}^{in} = f(n - 1) + h_1 \text{ and } \sum_{i=1}^{n} x_{i}^{in} = f(n - 1) + h_1 \tag{14}
\]
When $h_1$ is, similarly, the slackness condition.

By constraint [5] in equations (13) and (14) we have:

1. If $f(k)$ is a convex function, then $(n - 1) \cdot f(1) < f(n - 1)$, that implies $h = 0$ and $h_1 > 0$, then:

$$\sum_{i=1}^{n} x_{i}^{in} = \sum_{i=1}^{n} x_{i}^{out} = (n - 1) \cdot f(1)$$

Hence, $x_{1}^{in} = (n - 1) \cdot f(1)$; $x_{1}^{out} = 0$ and $x_{k}^{in} = 0$; $x_{k}^{out} = f(1)$, for any $k \neq 1$

$$\varphi^*(g^S) = \frac{\sum_{i=1}^{n} \sum_{j=1; j \neq i}^{n} x_{i}^{in} \cdot x_{i}^{out}}{\sum_{i=1}^{n} x_{i}^{in}} = \frac{(N - 1) \cdot ((N - 1) \cdot f(1) \cdot f(1))}{(N - 1) \cdot f(1)} = (n - 1) \cdot f(1) = \sum_{i=2}^{N} f(K_i)$$

2. If $f(k)$ is a concave function, then $(N - 1) \cdot f(1) > f(N - 1)$, that implies $h > 0$ and $h_1 = 0$, then

$$\sum_{i=1}^{n} x_{i}^{in} = \sum_{i=1}^{n} x_{i}^{out} = f(n - 1)$$

Hence, $x_{1}^{in} = f(n - 1)$; $x_{1}^{out} = 0$ and $x_{k}^{in} = 0$; $x_{k}^{out} = \frac{f(n-1)}{(n-1)}$, for any $k \neq 1$

$$\varphi^*(g^S) = \frac{\sum_{i=1}^{N} \sum_{j=1; j \neq i}^{n} x_{i}^{in} \cdot x_{i}^{out}}{\sum_{i=1}^{n} x_{i}^{in}} = \frac{(n - 1) \cdot ((n - 1) \cdot f(n - 1) \cdot f(n-1))}{f(n - 1)} = f(n - 1) = f(k_1)$$

3. If $f(k)$ is a linear function, then $(n - 1) \cdot f(1) = f(n - 1)$, that implies $h = h_1 = 0$, then:

$$\varphi^*(g^S) = (n - 1) \cdot f(1) = f(n - 1)$$

Proof of Lemma 1
Proof. We need to describe the different combinations of the $\varphi^*(g(P)) = V(g)$ and $\varphi^*(g(P) - \{i\})$ (whether they achieve the upper-bound).

First, if both $\varphi^*(g(P)) = V(g)$ and $\varphi^*(g(P) - \{i\})$ achieve the upper-bound, then $V(g) = \frac{m \cdot \sum_{j=1}^{N} k_j}{2}$, and if node $i$ is removed, then the degree all of its neighbors $t$ will be $k_i (g - \{i\}) = k_i(g) - 1, \forall t \in Neighbors(i)$ because all of them lose one connection. Then $\varphi^*(g(P) - \{i\}) = m \cdot \frac{\sum_{j=1; j \neq i}^{n} k_j - 2k_i}{2} = \frac{m \cdot \sum_{j=1}^{n} k_j}{2} - m \cdot k_i = V - m \cdot k_i$, with $\gamma = 0$

Proof of Proposition 4

Proof. It is easy to see that cost parameters $\alpha$ (defense) and $\beta$ (attack) must be included in the interval $[0, m]$. To show it, let $i \in N$ be a node with degree $k_i$ of a network $g(P)$ with $\varphi^*(g(P)) = V(g)$. By Lemma 1 if we delete $i$ from $g(P)$, the value of the network will be $\varphi^*(g(P) - \{i\}) = V(i) - m \cdot k_i$. ND will only defend a node if the decrease of the performance when node $i$ is deleted is bigger than the cost of protecting it. i.e., $m \cdot k_i > \alpha \cdot k_i$, so that $\alpha < m$. In the same way, NA will only attack if $m \cdot k_i > \beta \cdot k_i$, so that $\beta < m$. The lower bound is evident since costs are non-negative.

(i) $\beta > m$. $D = \emptyset$ and $A = \emptyset$. If $\beta > m$, NA will have more costs than profits if he attacks the network, so that $A = \emptyset$. In this case, if no node is attacked, ND can choose between defend a set of nodes or not to defend any of them: If he does not defend any node, then his payoff will be: $\Pi'_{ND}(g, D = \emptyset, A = \emptyset, \alpha) = \varphi^*(g)$

If he defends a non-empty set of nodes $C$, his payoff will be:

$$\Pi^r_{ND}(g, D = C, A = \emptyset, \alpha) = \varphi^*(g) - \alpha \cdot \sum_{i \in C} k_i$$

Since $\alpha > 0$, $\Pi'_{ND} > \Pi^r_{ND}$, and then $D = \emptyset$.

(ii) $\alpha > m$ and $\beta < m$. $D = \emptyset$ and $A = \{1\}$. ND will have more costs than profits if he defends any node in the network, so $D = \emptyset$. In this case, if no node is defended and $\beta < m^*$, then NA can choose to attack either the node with maximum degree, any other node or not to attack at all: If he does not attack any node, then his payoff will be:

$$\Pi'_{NA}(g, D = \emptyset, A = \emptyset, \beta) = -\varphi^*(g),$$

while if she attacks the node with maximum degree, any other node or not to attack at all: If he does not attack any node, then his payoff will be:

$$\Pi'_{ND}(g, D = \emptyset, A = \emptyset, \alpha) = \varphi^*(g) - \alpha \cdot \sum_{i \in C} k_i$$

Since $\alpha > 0$, $\Pi'_{ND} > \Pi^r_{ND}$, and then $D = \emptyset$. If he defends any node with maximum degree, any other node or not to attack at all: If he does not attack any node, then his payoff will be:

$$\Pi^r_{ND}(g, D = \emptyset, A = \emptyset, \alpha) = \varphi^*(g) - \alpha \cdot \sum_{i \in C} k_i$$

Since $\alpha > 0$, $\Pi'_{ND} > \Pi^r_{ND}$, and then $D = \emptyset$.
mum degree, by Lemma 1:

\[ \Pi''_{NA}(g, D = \emptyset, A = \{1\}, \beta) = -\varphi^*(g) + m \cdot k_1 - \beta \cdot k_1 = -\varphi^*(g) + (m - \beta) \cdot k_1. \]

Since \( \beta < m \), \( \Pi'_{NA} > \Pi''_{NA} \)

If he attacks any other different node \( i \):

\[ \Pi'''_{NA}(g, D = \emptyset, A = \{i\}, \beta) = -\varphi^*(g) + m \cdot k_i - \beta \cdot k_i = -\varphi^*(g) + (m - \beta) \cdot k_i. \]

Since \( k_i < k_1 \) and \( \beta < m \), \( \Pi'''_{NA} < \Pi''_{NA} \) then \( A = \{1\} \)

(iii) The interesting scenario is when \( \alpha, \beta < m \). Then \( D = \{1 \ldots i^*\} \) and \( A = j^* \). In this situation, NA will attack the undefended node with maximum degree, and ND will choose set \( D \). Since she wants to maximize the value of her residual network, then:

\[ \Pi_{ND}(g, D, A, \alpha) = \varphi^*(g - (A/D)) - \alpha \cdot \sum_{i \in D} k_i = \varphi^*(g) - m \cdot k_j - \alpha \cdot \sum_{i \in D} k_i \]

The maximum payoff is obtained when the expression \( (m \cdot k_j + \alpha \cdot \sum_{i \in D} k_i) \) takes the lowest value, with \( j = i + 1 \). Therefore \( D = \{1 \ldots i^*\} \) and \( A = \{j^*\} \). It is important to remark that if \( i = n \) then \( k_j = 0 \).

**Proof of Proposition 5**

**Proof.** We start by (iii). Since NA is always interested in attacking the undefended node with the maximum degree, there are two possible situations where condition 1 is not satisfied. The first one is when the cost of defending the first node is higher than the performance loss, when this node is removed, in other words, \( \alpha \cdot k_1 > \varphi^*(g) - \varphi^*(g - \{1\}) \). In this situation, as in the proof of proposition 4, \( A = \{1\} \). The second situation is the opposite one, when \( \alpha \cdot \sum_{i=1}^{N} k_i > \varphi^*(g) - \varphi^*(g - \{i\}) \), \( \forall i \in N \), then the ND wants to defend all the nodes, because the cost of defending any node \( i \in N \) is lower than the loss of performance, were \( i \) to be removed. For this reason \( D = N \), and \( A = \emptyset \).

(ii). Since NA can attack any undefended node, by Condition 1 ND will be
interested in defending a set of nodes \{1 \ldots i_p\} among the \(l\) possible sets in \(C\), \(1 \leq p \leq t\). At the following node \(j_p = i_p + 1\) the defense costs will be higher than the loss of performance if node \(j_p\) were removed. Therefore, it is easy to see that the last node i defended by ND must be included in \(C\). In this situation, NA could attack \(j_p\) or any other node \(j_s\), such that \(k_{j_p} > k_{j_s}\).

If NA attacks \(j_p\), then:

\[
\Pi'_{NA}(g, D = \{1 \ldots i_p\}, A = \{j_p\}, \beta) = -\varphi(g - (j_p)) - \beta \cdot k_{j_p}
\]

If NA attacks \(j_s\), then:

\[
\Pi''_{NA}(g, D = \{1 \ldots i_p\}, A = \{j_s\}, \beta) = -\varphi(g - (j_s)) - \beta \cdot k_{j_s}
\]

Since \(\varphi'(g) - \varphi'(g - \{i\}) > \beta, \Pi''_{NA} < \Pi'_{NA}\) so \(A = \{j_p\}\).

The remaining part of the proof consists of understanding that ND will choose the node \(i_p \in C\), the upper bound of \(D\), which satisfies the expression:

\[
\max_{i_p \in C}(\varphi^*(g - \{i_p\}) - \alpha \cdot \sum_{l=1}^{i_p} k_{l}), p \leq t
\]

The last expression is the value function of ND, so that he will choose the node \(i_p\) which maximizes his payoff (then NA will attack \(j_p\), as shown before). Then \(D = \{1 \ldots i_p\}\) and \(A = \{j_p\}\). The first part is obtained directly from the last point when \(|C| = 1\).

**Proof.** In the previous table we show the equilibria for different values of \(\alpha\) and \(\beta\). To prove these results we are going to solve the problem backwards, defining the values in which the NA would attack, and for these values what the ND is going to do depending of her costs.

1. The NA would prefer not to attack if:

\[
E[\Pi_{NA}(g(P), D = \emptyset, A = \{\emptyset, \ldots\}, \beta)] \geq E[\Pi_{NA}(g(P), D = \emptyset, A = \{\{j\}, \ldots\}, \beta)]
\]

35
\[-\varphi(g) > (1 - \delta_A) \cdot [-\varphi(g)] + \delta_A \cdot [-\varphi(g - \{j\})] - \beta \cdot k_j\]

\[-V > -V + \delta_A \cdot V - \delta_A \cdot V + \delta_A \cdot V_j - \beta \cdot k_j\]

\[\beta > \frac{V_j}{k_j} \cdot \delta_A; \forall j \in N\]

In that case, NA would not attack any node and, consequently the ND would not defend any node. Notice that \(\frac{V_j}{k_j} = 1\) for networks which accomplishes proposition 4.

2. The NA could attack any node (starting with node 1) if \(\beta < \frac{V_i}{k_i} \cdot \delta_A\) and the ND doesn’t defend, as we prove in step 1.

3. The NA would prefer to attack a defended node \(i\) than not to attack if:

\[\delta_A \cdot (1 - \delta_D) \cdot [-\varphi(g - \{i\})] + (1 - \delta_A \cdot (1 - \delta_B)) \cdot [-\varphi(g)] - \beta \cdot k_i > -\varphi(g)\]

\[\delta_A (1 - \delta_D) \cdot [-V + V_i] + (1 - \delta_A \cdot (1 - \delta_D)) \cdot [-V] - \beta \cdot k_i > -V\]

\[\beta < \frac{V_i}{k_i} \cdot \delta_A \cdot (1 - \delta_D)\]

4. The NA would prefer to attack a defended node \(i\) than an undefended node \(j\) \((i < j\) then \(V_j < V_i\) and \(\varphi(g - \{j\}) > \varphi(g - \{i\})\)) if:

\[\delta_A \cdot (1 - \delta_D) \cdot [-\varphi(g - \{j\})] + (1 - \delta_A \cdot (1 - \delta_D)) \cdot [-\varphi(g)] - \beta \cdot k_i\]

\[> (1 - \delta_A) \cdot [-\varphi(g)] + \delta_A \cdot [-\varphi(g - \{j\})] - \beta \cdot k_j\]

\[\delta_A \cdot (1 - \delta_D) \cdot [-V + V_i] + (1 - \delta_A \cdot (1 - \delta_D)) \cdot [-V] - \beta \cdot k_i\]

\[> -V + \delta_A \cdot V - \delta_A \cdot V + \delta_A V_j - \beta \cdot k_j\]

\[\beta < \frac{\delta_A[(1 - \delta_D) \cdot V_i - V_j]}{k_i - k_j}\]

It is important to highlight that the NA will always prefer to attack inside
the set of defended or undefended nodes, the first of them (following the order we made)

A. As we said before in 1, if the NA can not attack because of her costs, the ND will not defend any node.

B. If we are placed in situation 2 because of the values of $\beta$, in that situation the NA would attack the first undefended node. Then:

- The ND will prefer not to defend any node that defend a set $S$, which contains 1 to $i \in N$ defended nodes, if:

\[
(1 - \delta_A) \cdot [\varphi(g)] + \delta_A[\varphi(g - \{1\})] > \delta_D[\varphi(g - \{j\})] + (1 - \delta_D) \cdot \delta_A[\varphi(g)] - \alpha \sum_{l=1}^{i} k_l
\]

\[
\delta_A \cdot (V - V_j) + (1 - \delta_A) \cdot V > \delta_A(V - V_j) + (1 - \delta_A) \cdot V - \alpha \sum_{l=1}^{i} k_l
\]

\[
\alpha > \frac{\delta_A \cdot (V_i - V_j)}{\sum_{l=1}^{i} k_l}
\]

**Being j the first undefended node**

- The ND will prefer to defend a set $S$ (nodes $1 \ldots i \in N$) if $\alpha < \frac{\delta_A \cdot (V_i - V_j)}{\sum_{l=1}^{i} k_l}$ being the node $i$, the node which accomplishes the following expression:

\[
\max_{i \in N}[(V - V_i) + \delta_A \cdot (V_i - V_{i+1}) - \alpha \cdot \sum_{l=1}^{i} k_l]
\]

C. If we are placed in situation 4, the NA will attack the most important node for her, defended or not, for this reason the ND has to decide if this node is defended or not. Then ND will defend node 1 if:

\[
\delta_A \cdot (1 - \delta_D) \cdot [\varphi(g - \{1\})] + (1 - \delta_A \cdot (1 - \delta_D)) \cdot [\varphi(g)] - \alpha \cdot k_1 \\
> (1 - \delta_A) \cdot [\varphi(g)] + \delta_A \cdot [\varphi(g - \{1\})]
\]

37
\[ \delta_A \cdot (1 - \delta_D) \cdot [V - V_1] + (1 - \delta_A \cdot (1 - \delta_D)) \cdot V - \alpha \cdot k_1 \]

\[ > \delta_A \cdot (V - V_1) + (1 - \delta_A) \cdot V \]

\[ \alpha < \delta_A \cdot \delta_B \cdot \frac{V_1}{k_1} \]
TABLE 3: GENERAL NETWORKS

<table>
<thead>
<tr>
<th>Imperfect defense and attack ($\delta_A$ probability of succesful attack / $\delta_D$ probability of succesful defense)</th>
<th>$\beta &gt; \frac{V_j}{k_j} \cdot \delta_A$</th>
<th>$\frac{V_j}{k_j} \cdot \delta_A \cdot (1 - \delta_D) &lt; \beta &lt; \frac{V_j}{k_j} \cdot \delta_A$</th>
<th>$\delta_A \cdot \frac{(1 - \delta_D) \cdot V_i - V_j}{k_i - k_j} &lt; \beta &lt; \frac{V_j}{k_j} \cdot \delta_A \cdot (1 - \delta_D)$</th>
<th>$\beta &lt; \frac{\delta_A \cdot [(1 - \delta_D) \cdot V_i - V_j]}{k_i - k_j}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A = {\emptyset, \emptyset, \emptyset}$</td>
<td>$A = {1, j, \emptyset}$</td>
<td>$A = {1, j, 1}$</td>
<td>$A = {1, 1, 1}$</td>
<td></td>
</tr>
<tr>
<td>$D = \emptyset$</td>
<td>- If $\alpha &gt; \delta_A \frac{V_i - V_j}{\sum_{l=1}^i k_l}$ $D = \emptyset$</td>
<td>- If $\alpha &gt; \delta_A \frac{V_i - V_j}{\sum_{l=1}^i k_l}$ and $\alpha &gt; \delta_A \frac{V_i}{\sum_{l=1}^i k_l}$ $D = \emptyset$</td>
<td>- If $\alpha &gt; \frac{V_i}{k_1} \cdot \delta_D \cdot \delta_A$ $D = \emptyset$</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- If $\alpha &lt; \delta_A \frac{V_i - V_j}{\sum_{l=1}^i k_l}$ $D = S$</td>
<td>- $\alpha &lt; \delta_A \frac{(V_i - (1 - \delta_D) \cdot V_{i-1})}{\sum_{l=1}^i k_l}$ and $\alpha &lt; \delta_A \frac{V_i}{\sum_{l=1}^i k_l}$ $D = N$</td>
<td>- If $\alpha &lt; \frac{V_i}{k_1} \cdot \delta_D \cdot \delta_A$ $D = {1}$</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Other cases: $D = S$</td>
<td>- Other cases: $D = S$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The ND will defend the set $S = \{1\ldots i\}$, being $i$ the node which accomplishes the following condition:

$$\max_{i \in N} [(V_i - V_i) + \delta_A \cdot (V_i - V_{i+1}) - \alpha \sum_{l=1}^i k_l]$$

Notice that $\frac{V_i}{k_i} = 1$ for networks which accomplish Proposition 4 (for instance: star networks and complete networks).
### TABLE 4: n-COMPLETE NETWORK

<table>
<thead>
<tr>
<th>Perfect defense and attack</th>
<th>Imperfect defense and attack (δ&lt;sub&gt;A&lt;/sub&gt; probability of successful attack / δ&lt;sub&gt;D&lt;/sub&gt; probability of successful defense)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>β &gt; 1</strong></td>
<td><strong>β &lt; 1</strong></td>
</tr>
</tbody>
</table>
| **A = ∅**                 | **A = {∅, ∅}**  

1. If α > $\frac{1}{n}$  

1. If $α > \frac{1}{n} \cdot δ_A$  

1. If $α > \frac{1}{n} \cdot δ_D \cdot δ_A$  

D = ∅  

D = ∅  

D = ∅  

| D = ∅                     | **A = {i, ∅}**  

2. If α < $\frac{1}{N}$  

2. If $α < \frac{1}{n} \cdot δ_A$  

2. If $α < \frac{1}{n} \cdot δ_D \cdot δ_A$  

D = N  

D = N  

D = N  

<table>
<thead>
<tr>
<th><strong>A = Φ and D = N</strong></th>
<th><strong>A = Φ and D = N</strong></th>
<th><strong>A = Φ and D = N</strong></th>
<th><strong>A = Φ and D = N</strong></th>
<th><strong>A = Φ and D = N</strong></th>
</tr>
</thead>
</table>

**n → +∞**

| **β > 1**                 | **β < 1**                                                              | **β > δ<sub>A</sub>**                                      | **δ<sub>A</sub> · (1 − δ<sub>D</sub>) < β < δ<sub>A</sub>** | **β < δ<sub>A</sub> · (1 − δ<sub>D</sub>)** |
|---------------------------|---------------------------------------------------------------------------------------------------------------------|
| **A = ∅**                 | **A = {∅, ∅}**  

1. If α > 0  

1. If $α > 0$  

D = ∅  

D = ∅  

| D = ∅                     | **A = {i, ∅}**  

1. If α > 0  

1. If $α > 0$  

D = ∅  

D = ∅  

A = {i, i}  

A = {i, i}  

<table>
<thead>
<tr>
<th><strong>A = {i} and D = ∅</strong></th>
<th><strong>A = {i} and D = ∅</strong></th>
<th><strong>A = {i} and D = ∅</strong></th>
<th><strong>A = {i} and D = ∅</strong></th>
<th><strong>A = {i} and D = ∅</strong></th>
</tr>
</thead>
</table>
### TABLE 5: n-STAR NETWORK

<table>
<thead>
<tr>
<th>Perfect defense and attack</th>
<th>Imperfect defense and attack (δ_A probability of successful attack / δ_D probability of successful defense)</th>
</tr>
</thead>
<tbody>
<tr>
<td>β &gt; 1</td>
<td>β &lt; 1</td>
</tr>
<tr>
<td>A = \emptyset</td>
<td>β &lt; 1</td>
</tr>
<tr>
<td>D = \emptyset</td>
<td></td>
</tr>
<tr>
<td>1. If α &gt; \frac{n-2}{n-1}</td>
<td>A = {∅, ∅, ∅}</td>
</tr>
<tr>
<td></td>
<td>D = ∅</td>
</tr>
<tr>
<td>2. If \frac{1}{n-1} &lt; α &lt; \frac{n-2}{n-1}</td>
<td>A = {i} and D = ∅</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>3. If α &lt; \frac{1}{n-1}</td>
<td>A = ∅ and D = N</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### n → +∞

<table>
<thead>
<tr>
<th>β &gt; 1</th>
<th>β &lt; 1</th>
<th>β &gt; δ_A · (1 – δ_D) &lt; β &lt; δ_A</th>
<th>β &lt; δ_A · (1 – δ_D)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A = \emptyset</td>
<td>β &lt; 1</td>
<td>β &gt; δ_A · (1 – δ_D) &lt; β &lt; δ_A</td>
<td>β &lt; δ_A · (1 – δ_D)</td>
</tr>
<tr>
<td>D = \emptyset</td>
<td></td>
<td>β &lt; δ_A · (1 – δ_D) &lt; β &lt; δ_A</td>
<td>β &lt; δ_A · (1 – δ_D)</td>
</tr>
<tr>
<td>1. If α &gt; 1</td>
<td>A = {∅, ∅, ∅}</td>
<td>A = {1, i, ∅}</td>
<td>A = {1, 1, 1}</td>
</tr>
<tr>
<td></td>
<td>D = ∅</td>
<td>D = ∅</td>
<td>D = ∅</td>
</tr>
<tr>
<td>2. If α &lt; 1</td>
<td>A = {i} and D = {1}</td>
<td>1. If α &gt; δ_A</td>
<td>D = ∅</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. If α &lt; δ_A</td>
<td>D = {1}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. If α &lt; δ_D \cdot δ_A</td>
<td>D = {1}</td>
</tr>
</tbody>
</table>