Journal of Mathematical Economics 68 (2017) 62–79

Contents lists available at ScienceDirect

Journal of Mathematical Economics

journal homepage: www.elsevier.com/locate/jmateco

Optimal design and defense of networks under link attacks☆

Christophe Bravard [a,b], Liza Charroin [c,*], Corinne Touati [d]

[a] Université Grenoble 2, UMR 1215 GAEL, F38000 Grenoble, France
[b] CNRS, France
[c] Univ Lyon, ENS de Lyon, GATE L-SE UMR 5824, F-69342 Lyon, France
[d] Inria, F38330 Montbonnot Saint-Martin, France

HIGHLIGHTS

- A two-player game with a Designer and an Adversary is studied.
- The Designer designs and defends the network to protect it from an intelligent attack on links. She can use non-protected or protected links, i.e. links that cannot be removed by an attack.
- The objective of the Adversary is to isolate a part of the network by attacking k links.
- In equilibrium, the Designer either builds a minimal 1-link-connected network which contains only protected links, or a minimal $(k+1)$-link-connected network which contains only non-protected links, or a network which contains one protected link and $(n-1)(k+1)/2$ non-protected links.
- If the number of protected links available for the Designer is bounded, then there exists an equilibrium network which contains several protected and non-protected links.

ARTICLE INFO

Article history:
Received 15 July 2015
Received in revised form
30 September 2016
Accepted 26 November 2016
Available online 6 December 2016

Keywords:
Attacks on links
Network defense
Network design

ABSTRACT

Networks facilitate the exchange of goods and information and create benefits. We consider a network with n complementary nodes, i.e. nodes that need to be connected to generate a positive payoff. This network may face intelligent attacks on links. To study how the network should be designed and protected, we develop a strategic model inspired by Dziubiński and Goyal (2013) with two players: a Designer and an Adversary. First, the Designer forms costly protected and non-protected links. Then, the Adversary attacks at most k links given that attacks are costly and that protected links cannot be removed by her attacks. The Adversary aims at disconnecting the network shaped by the Designer. The Designer builds a protected network that minimizes her costs given that it has to resist the attacks of the Adversary. We establish that in equilibrium the Designer forms a minimal 1-link-connected network which contains only protected links, or a minimal $(k+1,\, n)$-link-connected network which contains only non-protected links, or a network which contains one protected link and $\lceil (n-1)(k+1)/2 \rceil$ non-protected links. We also examine situations where the Designer can only create a limited number of protected links and situations where protected links are imperfect, that is, protected links can be removed by attacks with some probabilities. We show that if the available number of protected links is limited, then, in equilibrium, there exists a network which contains several protected and non-protected links. In the imperfect defense framework, we provide conditions under which the results of the benchmark model are preserved.

1. Introduction

Networks can be seen as communication structures. They are composed of nodes and links, where links represent the flow of information. Networks represent a crucial feature in our society, and are of particular interest in different fields such as military defense, telecommunication or computer networks. Some networks can be damaged by natural disasters or intelligent attacks. Attacks can affect nodes (agents, computers, telecommunication antennas, …) or links (roads, communications flows, …), and may disconnect a

☆ This research has been supported by a grant of the French National Research Agency (ANR, FELIS Grant, ANR-14-CE28-0010-01). It was performed within the framework of the LABEX CORTEX (ANR-11-LABX-0042) of Université de Lyon, within the program Investissements d'Avenir (ANR-11-IDEX-007) operated by the French National Research Agency (ANR). Funding for this project was provided by a grant from Région Rhône-Alpes (15.007742.01). The authors thank Pascal Billand, Hans Haller, Stéphan Sémirat, Jacques Durieu and an anonymous referee for their constructive comments and suggestions.

* Corresponding author.
E-mail addresses: christophe.bravard@univ-grenoble-alpes.fr (C. Bravard), charroin@gate.cnrs.fr (L. Charroin), corinne.touati@inria.fr (C. Touati).

http://dx.doi.org/10.1016/j.jmateco.2016.11.006
0304-4068/

network.[1] In this paper, we examine a model where attacks target links. To illustrate the type of situations we model, consider a firm which has several production units (nodes of the network). Each production unit produces a part of the product and the pieces are assembled by a given production unit. The links of the network allow the parts of the product to be transferred among the units. If one unit is not connected to the rest of the units, its production cannot be transferred and the production has no value. Recall that during the Second World War, the production units for the weapons (nodes) were buried, so they were impossible to target, and attacks had to target the roads (links) in order to destroy the production process of the enemy. Therefore, the issue was to design a communication network between the production units that the enemy could not disconnect.

Our goal is to examine how to design and protect the network in an optimal way, such that the network remains connected after an intelligent link attack.[2] We say that a network is designed and protected in an optimal way if the costs associated with the design and the protection of the network are minimized.

We consider a two-stage game with two players: a Designer (D) and an Adversary (A).

- Stage 1. The Designer moves first and chooses both a set of protected, and a set of non-protected links. Protected links cannot be removed by the attacks of the Adversary.
- Stage 2. After observing the protected network (strategy) formed by the Designer, the Adversary attacks the network by allocating attacks to specific links. Since the attacks are costly, the Adversary has an incentive to attack at most k links.

Creating protected and non-protected links is costly for the Designer. The benefits obtained by the Designer at the end of the game depend on the connectivity of the residual network, that is, the network obtained after the attack of the Adversary. If the residual network is connected, then the Designer wins the game: her benefits are equal to 1 and the benefits of the Adversary are 0. If the residual network is not connected, then the Adversary wins the game: her benefits are equal to 1 and the benefits of the Designer are 0. The payoffs obtained by the players are equal to the difference between their benefits and the costs associated with their strategies.[3]

We are interested in the Sub-game Perfect Equilibrium (SPE) of the two-stage game. We assume that the cost of protected links and non-protected links are sufficiently low so that the Designer has some profitable strategies which allow the residual network to be connected. First, we provide for each number of protected links, the minimal number of non-protected links that the Designer has to form in order to prevent the Adversary from disconnecting the network as well as a method to construct a solution network. Second, we establish that only three polar non-empty networks may arise in equilibrium in the benchmark model.

1. A minimal $(k+1, n)$-link-connected network which contains no protected links.[4]
2. A minimal $(1, n)$-link-connected network which contains $n-1$ protected links.
3. A network which contains one protected link and $\lceil (n-1)(k+1)/2 \rceil$ non-protected links.

The first family of networks constitutes the optimal strategy of the Designer when the cost of forming non-protected links is sufficiently low relative to that of forming protected links. The second one is the optimal strategy when the cost of forming non-protected links is sufficiently high relative to that of forming protected links. The third one is optimal for intermediate relative costs (cost of a protected link/cost of a non-protected link) when the number of nodes is odd and the number of attacks is even.

Additionally to the benchmark model described above, we study some variations of the game to develop a larger understanding of optimal design of protected networks. We take into account two types of limitations concerning protections. First, we consider that D cannot create as many protected links as in the benchmark model.[5] Then, we consider a framework where each protected link has a probability π to be removed when it is attacked by A.[6]

In the framework where the number of protected links available for D is limited, we show that for intermediate relative costs, the optimal strategy of D consists in designing a network which contains both protected links and non-protected links. In the framework where protected links are removed by attacks with some probabilities, we provide conditions under which the results obtained in our benchmark model are preserved.

We now relate our paper to the existing literature on networks. This literature has become broader in the recent years (Jackson, 2008; Goyal, 2012; Vega-Redondo, 2007). The two seminal papers on the formation of social and economic networks are the paper of Jackson and Wolinsky (1996) and the paper of Bala and Goyal (2000a). Bala and Goyal (2000b) and Haller and Sarangi (2005) introduce imperfectly reliable links in the Bala and Goyal (2000a) model. Bala and Goyal (2000b) show that, for certain ranges of linking cost and probability of failure, the equilibrium network is at least $(2, n)$-link-connected, i.e. any two nodes are connected by at least two paths. Haller and Sarangi (2005) extend the model of Bala and Goyal (2000b) by allowing heterogeneity in probabilities of link failure. These authors model random link failure but not an intelligent attack that seeks to interrupt the communication flow. In the present paper, we study the robustness of a network that must be designed and protected to resist an intelligent attack on links.

A growing literature on attacked networks studies the optimal strategy of a Designer whose network is under node attack. Dziubiński and Goyal (2013) (DG) study the optimal design and defense of networks under an intelligent attack. In their framework, there are two players: the Designer and the Adversary; the Designer can form links between n nodes, and protect these nodes to ensure their survival. The model we propose is close to the model of DG, with the following major differences:

- The Adversary attacks nodes in the DG's framework while she attacks links in our framework;
- In our framework, the Designer wins the game if every node is able to communicate with any other node in the residual network. In the DG's framework, the Designer wins the game if the residual network is connected regardless of the number of nodes removed by the Adversary. Thus, our setting is based on the complementarity of nodes while DG assume that nodes are substitutable.

---

1 A network is connected if no set of nodes is isolated from the others.

2 Note that an intelligent attack can also be seen as the worst case scenario.

3 If we take again our military example, and assume that node $i-1$ is the supplier of node i, then the Designer has to maintain a path between each pair of nodes $i-1$ and i to obtain some end products. In other words, the residual network has to be connected to allow some production.

4 A network g, which contains n nodes, is a minimal $(k+1, n)$-link-connected network, if it is not possible to disconnect it by removing k links, and such that there is no network which cannot be disconnected by removing k links and contains a smaller number of links.

5 If we take again our military example, the Designer may not have enough resources to protect the whole network.

6 Despite the effort of the Designer (of the army) to protect the communication flow, the Adversary (the enemy) may still be able to succeed in destroying protected links with some probabilities.