Master Thesis Applied Mathematics
Faculty of Electrical Engineering, Mathematics and Computer Science (EEMCS)

Network games, information spread and endogenous security

Bram de Witte

April 13, 2015

Exam committee:

Prof. Dr. H.J. Zwart (UT)
Dr. P. Frasca (UT)
Dr. J.B. Timmer (UT)
Dr. B. Overvest (CPB)

UNIVERSITEIT TWENTE.

Centraal Planbureau

MASTER THESIS APPLIED MATHEMATICS

NETWORK GAMES, INFORMATION SPREAD AND ENDOGENOUS SECURITY

Student
Bram DE WITTE

Coordinators
Dr. P. Frasca
Dr. B. Overvest

April 13, 2015

UNIVERSITEIT TWENTE.

Centraal Planbureau

Abstract

A digital security breach where confidential information is being obtained often does not only influence the agent whose system is being infiltrated, also other agents socially or digitally connected to the damaged system can be affected. This leads to externalities in which the actual security of an agent does not only depend on his own investments in security, it also depends on investments by other agents. As no agent would invest to protect information of others, misaligned incentives may appear in this setting. It has been argued that these incentives provoke under-investments, which in turn make the network prone to fail. Recently this presumption is challenged however by the introduction of an intelligent adversary who chooses an optimal trade-off between expected damage and precision of the attack. In this research we build on the impact of an intelligent adversary by combing the strategic attack model with a new model for information spread. We show that agents tend to compete for security under the strategic attack as an increase in investments can cause the adversary to attack someone else. When dependencies among agents are low, because the network is not very dense or because the probability that information is shared is small, agents even invest more in security than they would in the social optimum. When dependencies increase these over-investments prevail due to a second order force originating from the adversary. In this situation the adversary chooses a more precise attack as the expected gain compensates the increased costs for a more precise attack. Nevertheless, when dependencies continue to increase and consequently it becomes meaningless to discourage an attack, at some point over-investments pass on to under-investments. We show that this point is reached earlier in a more dense network. However, when the network consists of several components where the intelligent adversary can strategically decide which component is attacked, investments are always higher in a more dense network.

Keywords: Network security, security investments, information protection

Preface

Thanks for taking interest in this paper. It contributes to the growing literature on the economics behind security investments. I hope this research may provide valuable knowledge to your research and I hope you enjoy reading this report.

The research in this paper has been conducted as a final project for my M.Sc. in Applied Mathematics at the University of Twente. For 5 years I studied at this small, but excellent university in the beautiful surroundings between Enschede and Hengelo. I hereby would like to thank all the teachers, professors and other staff members at the University of Twente who were involved in my study program. Special thanks go to Prof. Stoorvogel and Dr. Frasca who had a special role in my program. Prof. Stoorvogel lectured me in several courses and supervised me during my internship. Dr. Frasca supervised me in this final assignment. I am really grateful for their support.

Research in this paper has been conducted at the CPB Netherlands Bureau for Economic Policy Analysis (Dutch: Centraal Planbureau), a governmental but independent research center in The Hague. Research at the CPB is carried out on CPB's own initiative, or at the request of the government, parliament, national trade unions or employers federations. Much work is at the challenging crossroad of economic sciences and public policy and includes for instance economic forecasting and (quantitative) policy evaluations. I really enjoyed working at the CPB, not only because the CPB provided me with an excellent workplace and magnificent support, but also because I was able to learn a lot from all the other projects at the CPB. I really would like to thank all colleagues at the CPB who have showed interest in my research, provided valuable feedback and presented their own work. Special thanks is for Dr. Overvest who was my CPB supervisor during this research. I am really thankful for his valuable feedback, his contributions to this research and, last but not least for being a very nice colleague.

Bram de Witte
The Hague, April 2015

Contents

1 Introduction **1**
1.1 Motivation . . . 1
1.2 Summary of our contributions . . . 2
1.3 Outline of the report . . . 4

2 Background material and related literature **5**
2.1 Network games, strategic complements and strategic substitutes . . . 5
2.2 Diffusion through networks . . . 7
2.2.1 Compartment models and contact networks . . . 7
2.2.2 Percolation models . . . 9
2.3 Related literature on network security . . . 11
2.3.1 Exogenous network security . . . 11
2.3.2 Endogenous network security . . . 12

3 The model **15**
3.1 Notation and terminology . . . 15
3.2 Model description . . . 16
3.2.1 The security vector . . . 17
3.2.2 The attack vector . . . 18

4 Spreading of documents **21**
4.1 Basic definitions from graph theory . . . 21
4.2 Probability that documents are shared . . . 22
4.2.1 How to compute $D_{\mu,\nu}$? . . . 22
4.2.2 Exact probabilities in a complete network . . . 25
4.2.3 Comparing several networks . . . 27
4.3 Expected number of documents obtained . . . 28
4.3.1 How to compute D_ν? . . . 28
4.3.2 Vertex-transitive networks and circulant networks . . . 30
4.3.3 Growing networks and asymptotics . . . 32

5 The security game under a strategic attack **35**
5.1 The two-agent case . . . 35
5.2 Preliminaries to the security game . . . 38
5.2.1 Assumption on investment cost . . . 38
5.2.2 Maximum of strictly concave function . . . 38
5.2.3 Measure for expected damage . . . 38
5.3 Random attack as a benchmark . . . 39
5.4 Incentives of a malicious attacker . . . 40
5.4.1 General results . . . 41
5.4.2 Attacker's strategy in vertex-transitive networks . . . 46
5.5 Equilibrium investments in security . . . 47
5.5.1 Properties of the best response . . . 48
5.5.2 The symmetric pure strategy Nash equilibrium . . . 50
5.6 Optimal trade-off between security and costs . . . 55
5.7 Comparing the cooperative and the non-cooperative security game . . . 58
5.8 Dependency of investments on the network structure, cost functions and the number of agents . . . 60
5.8.1 Structure of the network . . . 60
5.8.2 Costs for agents . . . 63
5.8.3 Costs for the attacker . . . 64

5.8.4 Number of agents . . . 65

6 The security game with several components **69**
6.1 Extension to the model and assumptions . . . 69
6.2 The strategic-random attack . . . 70
6.2.1 Incentives of the strategic-random attacker . . . 70
6.2.2 Equilibrium of the non-cooperative game . . . 71
6.2.3 Optimal trade-off between security and costs . . . 72
6.3 Comparison of different attack forms . . . 74

7 Discussion **79**

A Appendices **81**
A Background material . . . 81
B Simulation of information spread . . . 82
C Nonexistence of Nash equilibrium without attacking cost . . . 83
D Investments in asymmetric networks . . . 84
E Metaphor for economic forces present in the security game . . . 85

References **89**

1 Introduction

1.1 Motivation

Our society and economy have become largely dependent on information networks. People communicate with others around the globe, students aggregate information from electric libraries and cloud computing services are widely used. Although in general these networks provide benefits, cyber attacks become more and more attractive and potentially disastrous as our dependence on these networks increase. Estimates of the total damage of cyber attacks vary as stakeholders generally conceal information to prevent reputational damage. Yet, security giant Symantec estimates that over 552 million identities were exposed via breaches and that 66% of email traffic was spam in 2013 (Symantec, 2014).

Security breaches come in many forms, such as spread of malware, social engineering compromises (e.g. phishing) and exploitations of a system's vulnerabilities. A special form of cyber-attack are attacks where hackers - without permission - obtain confidential information. Relevant information is diverse and includes for instance strategic decisions and intellectual properties (e.g. industrial espionage) but also includes identity information like passwords and (email) addresses. The impact of this stolen information can be destructive: bank accounts can be plundered, legitimate owners can be threatened that strategic decisions or sensitive information will be released or for instance identities can be stolen for criminal purposes. Recent examples are extensive. For instance on November 24, 2014, Sony Pictures Entertainment has been subject to a massive computer hack where attackers stole a huge number of confidential documents. Among the document are unreleased movies, internal e-mail contacts and personal information like medical information and salaries of employees and their families. Not only Sony, but also employees received threats that more sensitive data will be exposed unless certain demands are met. This attack on Sony is certainly not the first security breach where confidential information is obtained. On August 5, 2014, it was announced that hackers amassed over a billion passwords, names and e-mail addresses by breaching Internet websites. With this information, hackers accumulated money by hacking into e-mail and social accounts, posing as a trusted friend but sending malicious spam. Also smaller examples but potentially more destructive for individuals are known. For instance, fake social network accounts are notorious for, if accepted as 'friend', amassing sensitive information about their victims and - potentially - their victims friends.

These forms of cyber-attacks where confidential information is obtained are increasingly common and cybersecurity experts Jang-Jaccard and Nepal (2014) and security company Symantec (2014) worry that keeping personal information out of the hands of thieves is a losing battle. Although agents in information networks can protect against these attacks by using anti-virus programs, refraining from suspicious emails or by adopting prudently chosen passwords, it has been argued by Moore (2010), Dynes *et. al* (2007) and Anderson & Moore (2006) that security investments are not as high as they should be. These under-investments have been atrributed primary to *misaligned incentives* that arise from *externalities*. Externalities originate because confidential information can be leaked through other channels than one's own device. As a consequence, agents face risks whose magnitude depends not only on an agent's own security level, it also depends on the security level of others. In this setting investments in security act like strategic substitutes as benefits of security adoption are not exclusively for the one that invested in the security. Consequently, a negligent agent who does not adequately protect his system due to free-riding may cause considerable damage to other agents. This can lead to situations where benefits of security adoption fall significantly below the cost of adopting. This in turn provokes under-investments in security. Anderson and Moore (2006) recognize for instance that security failure is caused at least as often by bad incentives (not adopting security and incautious behavior) than by bad design (technical limitations to protect against security breaches). Lelarge and Bolot (2008) verify from a theoretical model that adopting new security features in the Internet has been an ongoing challenge due to externalities. Varian (2000) recognizes that a rational consumer might well spend effort to protect his own hard disk, he might not do so to prevent an attack on a wealthy company.

Recently this prediction of under-investments in information networks has been challenged. Acemoglu *et al.* (2013) and Bachrach *et al.* (2014) show that investments in security might as well be strategic complements when agents face an intelligent threat. As this intelligent threat endeavors to do as much

damage as possible, possibilities to free-ride are reduced as the attacker might target a negligent agent with a higher probability. This in turn forces agents to adopt security. This incentive may even lead to characteristics of an arms race where agents mutually compete who is targeted by the attacker. Acemoglu *et al.* show that agents indeed invest too much but stress that the exact magnitude depends on the network topology and on the specific cost functions. Bachrach *et al.* even propose that optimal policy requires taxing security, as opposed to subsidize security as recommended by models which do not include an intelligent adversary.

1.2 Summary of our contributions

Our model

This research builds on the growing literature on the economics behind security. We develop a theoretical model to investigate incentives to invest in security. The focus lies on comparing investment levels in a cooperative and a non-cooperative environment with the purpose to uncover the consequences of egoistic behavior. In line with Acemoglu *et al.* we adopt a model of an intelligent/strategic attacker. Although in potential a fruitful research direction with satisfying early results, the role of the attacker is not fully understood. To further understand this role, we combine the model of the strategic attack with a new spreading model fitted to spread of information[1].

Specifically, in our model every agent owns a unique document which for instance could be a credit card number, a strategic decision or a contract. It is assumed that documents are shared among agents in the network. Although the documents are confidential, it is beneficial (at least not detrimental) for an agent when this document is obtained by other agents. For instance, families might exchange credit card numbers, employees exchange strategic decisions and friends share personal information. It is assumed that the spreading of the documents happens independently of each other and in a way such that agents who are connected to the owner of the document, in a - so called- transmission network, obtain the document. This transmission network is formed from the original network by removing edges, independently of each other and with an *exogenous* probability $1-p$ (see figure 1). As we assume that this probability p is independent of security, agents do not limit spread facing the upcoming attack.

Before the spreading of documents is realized, we assume that agents had the opportunity to invest in security. These security investments reduce the chance that an attack is successful which would allow the malignant attacker to amass all the confidential documents obtained by the target agent. This attacker, who strives to obtain as many documents as possible, attacks one of the agents. This is modeled by drawing a random variable from a probability distribution over the agents. This distribution is set up *before* the documents diffuse through the network but *after* the precautionary security investments are made. Moreover it is assumed that a more precise attack, which requires more knowledge about the characteristics of the agents, is more costly. This set-up forces the attacker to determine an optimal trade-off between precision and cost.

We model the precautionary security investments as the outcome of a game between agents. In this game, rational agents simultaneously invest in security and in a way such that gains (reduced exposure risks) compensate investments costs. In the process of making this decision, agents have full information about the game, the network structure and choose their security investments *anticipating* the strategic decision of the attacker. Uncertainty lies in the probability that documents are shared, the location of the attack and the probability that this attack is successful. In order to fully characterize the role of a possible strategic attack, as opposed to a non-strategic (random) attack and the role of the level of cooperation among agents, we limit our attention to homogeneous agents. Such normalization guarantees that a change in investments is due to the attack form or to the cooperation level as opposed to heterogeneity across agents. Nevertheless, our simulation results indicate that forces present in homogeneous settings extend to broader, heterogeneous settings.

1. Although we focus on security investments to protect (digital) information, our model is easily extended to other situations where a successful 'attack' on one agent leads to damage to other agents. One can think of financial shocks, terrorist attacks and betraying criminals (in case law enforcement attacks/arrests one criminal who - in turn- betrays others).

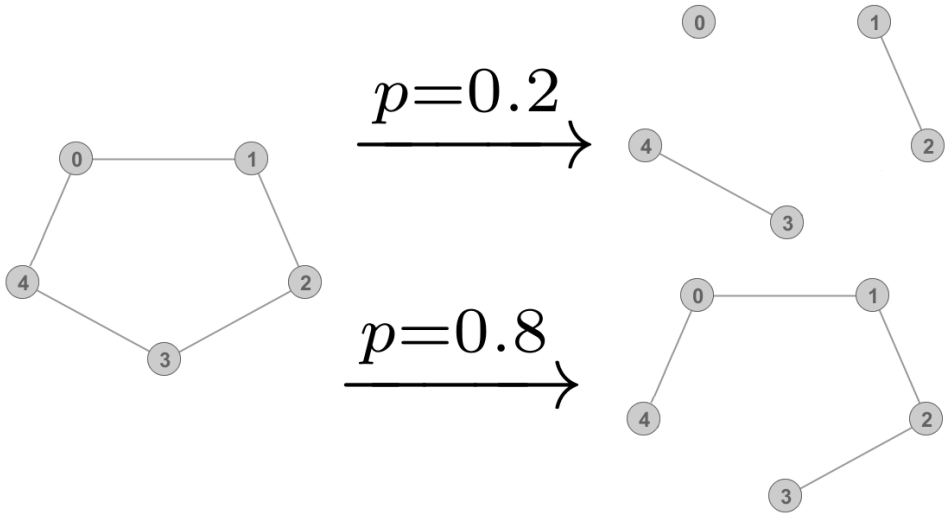

Figure 1 – *Our spread model: from the original interaction network (left network) edges are removed with probability $1-p$. This models the idea that agents may or may not communicate in some time period. Agents connected to each other in the remaining - so called - transmission network share their documents with each other. In the figure, the networks on the right are possible realizations of the transmission network for two different values of p. When $p = 0.2$ agent 1 obtains the document of agent 2 (and vice versa) and agent 3 obtains the document of agent 4 (and vice versa). When $p = 0.8$ an agent obtains all documents of others. The value of p is assumed to be exogenous and hence independent of security investments.*

Our results

The first set of results indicate that without a strategic attacker (random attack), agents invest less in equilibrium of a non-cooperative game than in social optimum (equilibrium of a full cooperative game). This result agrees with existing literature which presumes under-investments in security. However, the incentive structure is drastically changed when a strategic attacker is introduced. Although we base our conclusion on homogeneous agents and simulation results, we believe that our results point to a general theme: agents mutually compete for security when the attack is strategic. Specifically, we show that equilibrium investments under the strategic attack always exceed equilibrium investments under the random attack.

When we compare the investment levels in equilibrium with the social optimum our results challenge earlier results on the strategic attacker. In line with earlier research though, when dependencies between agents are low, because the network is not very dense or p is low, agents indeed invest too much and equilibrium investments exceed the social optimum. On the other side, when dependencies are large and therefore documents are shared with a high probability, agents tend to invest less than in social optimum. This result challenges existing literature on the strategic attacker which showed that under-investments (or over-investments) prevail independently of the level of dependencies between agents.

Furthermore we explore investment levels as function of dependencies between agents in more detail. We show that investments initially increase in p. This behavior originates from the strategic attacker whose strategy is an optimal trade-off between precision and cost. When p increases it becomes more and more optimal for the attacker to choose a more precise attack. As this leads to increased competition between agents, agents tend to invest more in security. On the other side, when p continues to rise, more agents obtain an agent's document. At some point this makes it meaningless for an agent to invest to cause the attacker to attack someone else. Specifically, we show that there is a unique transition point where over-investments pass on to under-investments. This point is reached earlier in a more dense network.

Lastly we extend our model to a situation where the network consists of several components. As information generally only spreads among members in a family, employees in a firm or in a specific operating system, the attacker can fit his attack to characteristics of the component. In this set-up we propose a new attack form: the *strategic-random* attack. Under this attack the malicious attacker strategically decides which component is attacked, but he or she can not decide which specific agent is attacked. Results indicate that equilibrium investments under this new attack form lie between equilibrium investments under the (full) random attack and the (full) strategic attack. Additionally we show that all investment levels increase in both the probability that information is shared (p) and the density of the network.

1.3 Outline of the report

This report is structured as follows. First we thoroughly discuss related literature and background material in chapter 2. The background material is focused on both diffusion models (e.g. epidemiology and gossip spread) and network games (strategic decision making in networks). In the discussion on related literature we primary focus on theoretic models that discuss incentives to adopt security. These models often combine diffusion models with network games. Next in chapter 3 we present our model more fundamentally and mathematically than in this introduction. The spread model is presented and analyzed in more detail in chapter 4. The core of our research is presented in chapter 5. Here we first endeavor to find characteristic equations for security investments in both a cooperative and in a non-cooperative environment. Later in this chapter we compare the outcomes and analyze the role of certain parameters. In chapter 6 we present an extension to our model where the attacker can focus his attack on one component in particular. Finally in chapter 7 we discuss limitations of our model and give an outlook on future research.

2 Background material and related literature

In this section we discuss several relevant models. First the focus lies on background material that combines network theory and game theory to models which are often called *network games*. The framework of network games is sketched and some examples are given. Next we focus on mathematical approaches to model diffusion in networks. After this discussion on background material we consider related literature in which security in networks is analyzed.

2.1 Network games, strategic complements and strategic substitutes

First of all, game theory studies strategical decision making of several involved agents. Often a formal mathematical model is set up in which every agent has a certain utility/payoff function which describes the 'well-being' of an agent. The process of strategical decision making, in a non-cooperative setting, is consequently modeled as optimizing this utility function given the anticipated/expected strategical decision of other agents. Peters (2008) more formally analyzes the theory and provides several results in the field.

The classic example in game theory is the prisoner's dilemma. In this dilemma two arrested suspects that collaborated in a crime each have the opportunity to betray the other criminal or to remain silent in a police interrogation. Each decision gives a different payoff for an agent depending on the decision made by the other criminal. A possible payoff structure is given in table 1. Because betraying the other

Player A / Player B	Betray	Silent
Betray	Player A serves 2 year/ Player B serves 2 year	Player A serves 0 year/ Player B serves 3 year
Silent	Player A serves 3 year/ Player B serves 0 year	Player A serves 1 year/ Player B serves 1 year

Table 1 – *Payoff structure in the prisoners' dilemma*

criminal offers a greater reward[2], all rational and self-interested criminals will betray each other. Note however that it is more (socially) optimal to remain silent for both agents.

In this research security adoptions are investigated in a similar way as behavior in the prisoners' dilemma is explored. Also in this research we compare the outcome in a non-cooperative and a cooperative (socially optimal) variant. Differently, in our research we consider a continuous game[3] with more than 2 agents. Additionally in our research the payoff of each agent depends on a network structure. This is the basic framework of a special class of game theory called network games.

Network games are thoroughly discussed by Jackson (2008) and Galeotti (2010). Networks itself allow to model dependencies and relations among objects like for instance people, cities and systems. In a network these objects, represented by nodes, are linked by edges, representing the relation between certain objects. This way a wide range of structures can be modeled varying from traffic architectures to social interactions to financial dependencies. In network games, an agent's well-being depends on his own action, as well on the actions taken by agents whom the agent is linked to in the network. Yet, in this setting an agent's well-being also depends on the actions taken by indirect neighbors, since the actions taken by an agent's neighbors - in turn - depend on their neighbors' actions (and so on). Formally in network games, the utility of an agent, say agent i, can be described by a function

$$\Pi_i(x_i, x_{\mathcal{N}_i(A)}), \tag{2.1}$$

where x_i is an agent's own action and $x_{\mathcal{N}_i(A)}$ is the profile of actions taken by agents whom agent i is linked to in the network.

2. This can be seen by noting that for each choice of player B, for player A it is optimal to betray. Parallel reasoning will show that B should also betray.
3. In a continuous game there are infinitely many strategies. In our research the strategy of each agent is a decision in $[0, 1]$.

Several forms for (2.1) exist. Note for instance that, as an extreme case, if the network is full (i.e. everybody is linked to each other), a network game is a standard (matrix) game like the prisoners' dilemma. If the network is not full, a network game adequately models situations where actions of other's are weighted differently: actions by neighbors have the largest impact whereas actions taken by agents 'further away' in the network have less impact. This corresponds for instance with changes in opinion: opinions of friends/eminent people have a greater influence on one's opinion than opinions of unknown people.

Another widely used form for (2.1) is as discussed by Jackson. In this model Π_i satisfies

$$\Pi_i(1, x_{\mathcal{N}_i(\mathcal{G})}) < \Pi_i(0, x_{\mathcal{N}_i(\mathcal{G})}) \text{ if and only if } \sum_{j \in \mathcal{N}_i(\mathcal{G})} x_j \geq t_i, \tag{2.2}$$

where $x_i \in \{0, 1\}$, t_i is some threshold and $\mathcal{N}_i(\mathcal{G})$ are the neighbors of agent i in network $\mathcal{G}$. In this model, taking action 1 is costly and therefore an agent would prefer that neighbors take action 1 rather than the agent himself. Actions are *strategic substitutes* here as actions mutually offset one another. Corresponding actions are for instance to buy a book (which can be borrowed from friends), to do the dishes or to invest in security/R&D, which - to some extent - provides benefits to others. In general, this model leads to incentives to *free-ride* on actions taken by others. This in turn might lead to under-provision of the good or under-investments. Figure 3 shows two possible equilibria for this game where the threshold, t_i in (2.2), is set to 1 for all agents. Here it is assumed that a profile of actions is in equilibrium if no agent would change his action under the current profile.

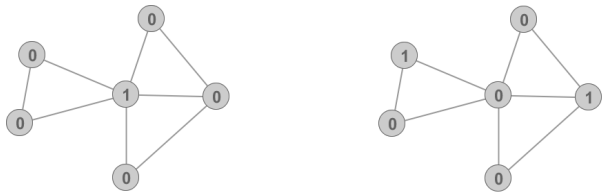

Figure 2 – *Two possible equilibrium situations in a game with utility as in (2.2) with $t_i = 1$. In the situations above no agent would change his behavior because either the agent himself, or an agent's neighbors takes action 1. Surely the left situation, where one agent takes action 1, is more (social) optimal than the right situation where two agents take action 1.*

Another case of interest has an opposite incentive structure. Now an agent does not tend to lower his action when neighbors increase their action profile, in this case, higher levels of actions by neighbors lead to incentives to take a higher action yourself. This corresponds for instance with investments in warfare material and changes in (social) behavior like pursuing higher education and adopting sustainable behavior. In this setting, actions are called *strategic complements* because they mutually reinforce one another. In this case, (2.1) is such that Π_i satisfies,

$$\Pi_i(1, x_{\mathcal{N}_i(\mathcal{G})}) > \Pi_i(0, x_{\mathcal{N}_i(\mathcal{G})}) \text{ if and only if } \sum_{j \in \mathcal{N}_i(\mathcal{G})} x_j \geq t_i. \tag{2.3}$$

Figure 3 shows two possible equilibrium action profiles for this game. In the figure the threshold t_i is set to 2 for each agent. Note that when actions are strategic complements, agents tend to invest more than when actions are strategic substitutes.

For wider strategy spaces, $x_i \in S_i$ for some set S_i, often the same framework as above is used. As an example, consider a game with three agents who are connected as in figure 4. Assume that the utility of each agent is

$$\Pi_i(x_i, x_{\mathcal{N}_i(\mathcal{G})}) = x_i(1 + \sum_{j \in \mathcal{N}_i((\mathcal{G})} x_j) - x_i^2, \tag{2.4}$$

where $x_i \in [0, \infty]$. One can show that actions are strategic complements[4] and that $x_1 = x_3 = 3/2$ and

4. One can prove that if Π_i is concave in the strategy of i and super-modular, then actions are strategic complements.

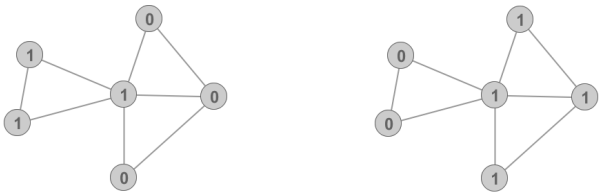

Figure 3 – *Two possible equilibrium situations in a game with utility as in (2.3) with $t_i = 2$. In the situations above no agent would change his behavior because either an agent takes action 1 and at least two neighbors take action 1, or an agent takes action 0 and less than two neighbors take action 1.*

$x_2 = 2$ is a (unique) equilibrium profile. This can be seen from figure 5, given the decision of others, no agent will change his action.

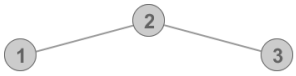

Figure 4 – *Network where the utility of each agent is given in (2.4). From figure 5 one can see that $\{3/2, 2, 3/2\}$ is an equilibrium action profile: given this action profile, no agent will change his behavior. One can also show that this equilibrium is unique.*

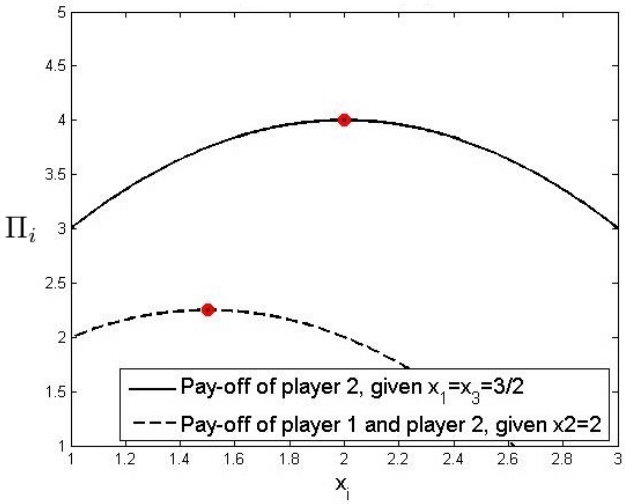

Figure 5 – *Pay-off function (2.4) given the decision of others. Note that the best response of player 2 is 2 and the best response of player 1 and player 3 is $3/2$.*

In this research, investments in security are modeled as a strategic decision in $S_i = [0, 1]$ for some utility function similar as in (2.4). In contrast with the models discussed above, in this research the utility function is such that investments/actions are in some cases strategic substitutes and in other cases strategic complements.

2.2 Diffusion through networks

In the network games discussed in the previous section, there is no element that spreads/diffuses through the network. However, when adopting security, often one protects against an element that spreads through the network. For instance, agents might adopt security to protect against infection of a virus or to protect against fires. In this review we discuss two diffusion models. First we give an overview of compartment models. Although traditionally applied to model spread of diseases, compartment models are also used to model spread of information and ideas. Next we discuss percolation models. Although percolation models are somewhat limited than compartments models, they are more tractable when combined with a network game.

2.2.1 Compartment models and contact networks

Jackson (2008) notes that the classic example in epidemiology of a model on diffusions is the Bass model. In this model, the number of agents in a compartment of infected/influenced agents is described

by a differential or a difference equation. In general the model (the continuous time variant) is described with

$$\frac{dA(t)}{dt} = f(A(t), \mathbf{p}),$$

where f is some function, $A(t)$ the number of influenced agents and $\mathbf{p}$ some set of parameters. Note that $A(t)$ is the compartment in this model. A widely used form for f is for instance $f = pA(t)(m - A(t))$ where p and m are some constants.

Since the Bass model several other, more complex models have been developed. Most prominent in epidemiology are the so called SIR and SIS models. In these models each individual is either: susceptible, meaning that the individual is susceptible to being infected or infected, meaning that the individual currently has the disease. Additionally in the SIR model an agent can be resistant; meaning that the individual does not have the disease, can not infect others and can not be infected. As agents interact with each other in a society, susceptible agents might be contaminated by infected agents. On the other hand, infected agents might heal and in the SIR model become resistant, or in the SIS model become susceptible again. These changes are often described by differential equations. For instance in the SIR model, for some functions f, g and h

$$\frac{dS}{dt} = f(S, I, R, \mathbf{p}), \qquad \frac{dI}{dt} = g(S, I, R, \mathbf{p}) \quad \text{and} \quad \frac{dR}{dt} = h(S, I, R, \mathbf{p}).$$

Although originally used to model spread of diseases, the SIR model is also used in other disciplines. For instance Xiang *et al.* (2014) model the propagation of worms in information networks with a SIR models.

Compartment models tend to overestimate the number of infected/influenced agents (Dimitrov and Meyers, 2006). An explanation of these overestimations is the fully mixed, homogeneous population assumption in compartment models: every individual equally likely catches the disease from any infected individual. This way, compartment models do not accurately model diverse interactions between individuals that underlie disease transmissions. For instance, in practice, agents in a cluster[5] in which the infection spreads face a higher contagion risk than agents outside this cluster. To overcome this limitation, recent literature proposed to combine SIR and SIS models with network models. Basic framework is as follows:

I. a contact network is constructed that describes interactions between agents,
II. diffusions are predicted in this contact network.

Several approaches are possible to predict diffusions in a contact network. Van Mieghem (2011) proposed the *N-intertwined model*: a SIS-model that incorporates a network structure. Instead of focusing on a compartment as a whole, in the N-intertwined model focus lies on each agent separately. When $x_i(t)$ is the event that agent i is infected at time t, it is assumed that

$$Pr\{x_i(t) = 1\} \;=\; v_i(t) \;=\; 1 - Pr\{x_i(t) = 0\}.$$

Here $v_i(t)$, the rate of change, is described by some differential equation

$$\frac{dv_i(t)}{dt} = f(v_i, v_{\mathcal{N}_i}), \tag{2.5}$$

where f is some function and $v_{\mathcal{N}_i}$ is the rate of change of neighboring agents. Generally, if an element in $v_{\mathcal{N}_i}$ increases (i.e. it is more likely that a neighbor is infected) also v_i will increase.

To build a contact network often a random graph model is considered. In this model the number of neighbors of each agent is a random variable drawn from some distribution. The classic example is the so called Poisson random graph (or Erdós-Rényi network) where this distribution is binomial with parameters $n - 1$ (there are n agent in the network) and p. Figure 6 shows a possible realization of

5. A cluster is a group of individuals who interact more often with each other than they would with individuals outside this cluster.

this procedure. Note that this realization features a unique largest component which is called the giant component in random graph theory. One can show that - if this giant component exists - it is unique with a probability going to one (in the number of nodes). Erdós and Rényi proved that there exist several thresholds for p so that the realized network attains some specific structure:

I. If $p > 1/n^2$ almost surely the first edges appear. The number of nodes in each component is at most $O(\log n)$.
II. If $p > 1/n$ almost surely a giant component exists. The expected fraction of nodes outside this giant component is the solution $0 < x < 1$ of

$$x = 1 - e^{-x(n-1)p}.$$

The size of all other component is at most $O(\log n)$.
III. If $p > log(n)/n$ almost surely the network is connected.

Alternatively the Poisson random graph can be constructed by removing edges in a full network, independently of each other and with probability $1-p$. Also when this network is not full, it can be proved that there exist several thresholds for p so that the realized network attains some specific structure. Frieze *et al.* (2004) provide thresholds for regular graphs and Chung *et al.* (2009) provide results for graphs that satisfy some mild conditions depending on its spectral gap[6] and higher moments of its degree sequence.

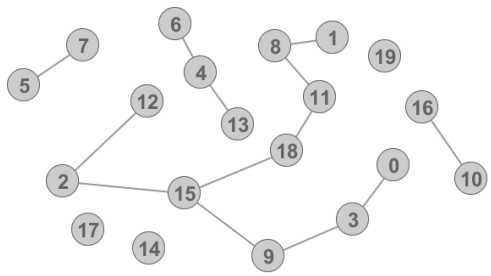

Figure 6 – *A possible realization of a Poisson random network. The network is formed by connecting each node with probability 0.055. Only 13 of the 190 edges are maintained. Note that there is a unique component which contains a nontrivial fraction of all nodes (the giant component).*

While the Poisson random graph exhibits some features observed in (disease/social) contact networks, some features are clearly lacked by the Poisson random graph (e.g. high clustering and preferential attachment[7]). Researchers (e.g. Newman, 2006) have focused on different models like small-world networks, (strategically) growing networks and random networks with different degree distributions. Alternative degree distributions are for instance an exponential distribution or a power-law distribution. Figure 7 shows a possible realization of a network created with a power-law distribution.

2.2.2 Percolation models

An alternative spread model is percolation theory. The theory originates from theoretical physics and models the spread of a liquid through some porous material. In this model, the porous material is modeled as a graph where nodes, called 'sites', are open with some probability and edges, called 'bonds', are open with some probability. The liquid will consequently flow only through open sites and open bonds. When all sites (nodes) are open, but not all bonds (edges) are, the model is denoted as bond percolation. The other way, when all bonds are open, but not all sites are, the model is denoted as site percolation. Also the spread of diseases and information can be modeled this way (Moore, 2000). In

6. For graphs, the spectral gap is the absolute value of the difference between the two largest eigenvalues of the adjacency matrix.
7. Preferential attachment is often found in growing networks. The more links a node has on some time instant; the more it will have later on. This corresponds for instance with a citation network or a friendship network.

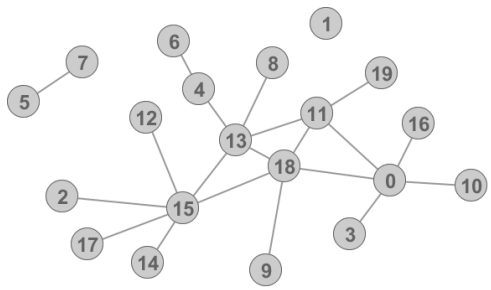

Figure 7 – *A network where the number of neighbors is drawn from a power-law distribution. Observe that the network features several nodes with a small number of neighbors and some nodes with a high number of neighbors (preferential attachment). Scale-free networks show to adequately model the structure of the Internet and the Word Wide Web (Newman, 2006).*

epidemiology, often two parameters are of interest: susceptibility and transmissibility. Susceptibility is the probability that an individual exposed to a disease/idea will contract it. Transmissibility is the probability that contact between an infected individual and a healthy individual will result in the healthy individual to become infected. When transmission takes place with less than 100% efficiency, but all individuals are susceptible, the spread of a disease can be modeled by bond percolation. Reversed, when transmission takes place with 100% efficiency, but not all individuals are susceptible, site percolation can be used. Basic framework of these diffusion models is as follows:

I. A contact network is constructed.
II. Nodes are removed (site percolation) or edges are removed (bond percolation) with some probability, leading to some transmission network $\mathcal{T}$.
III. All nodes connected - in this transmission network - to initially infected nodes are infected/influenced.

Bond percolation and site percolation often lead to totally different transmission networks. Figure 8 shows an example of site percolation and figure 9 shows an example of bond percolation. Generally bond percolation leads to larger transmission networks.

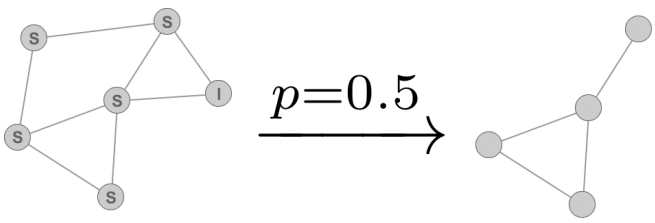

Figure 8 – *Site percolation: susceptible (S) nodes in a contact network (left network) are maintained in a transmission network (right network) with probability p. If one of the agents in the transmission network is initially infected, then all agents connected in the transmission network to this agent will become infected.*

Transmission networks can be seen as an extended contact network. Where contact networks model a *possible* contact between individuals, for instance friends might meet in some time period, the transmission network models if this contact *actually* occurred or not. This way spread of diseases or information can be modeled.

In this research, information spread is modeled as bond percolation opposed to site percolation. Reason for this choice is that we feel that an agent with a high number of contacts (i.e. neighbors), more likely becomes aware of information. When modeling information spread as site percolation, this probability is independent of the number of neighbors.

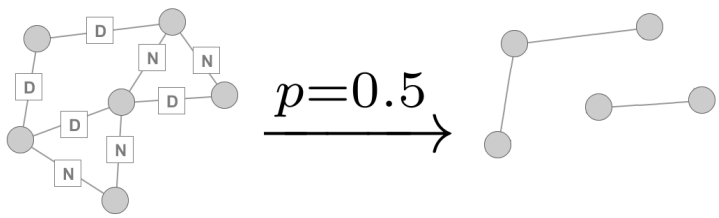

Figure 9 – *Bond percolation: diffusing (D) edges in a contact network (left) are maintained in a transmission network (right) with probability p. If one of the agents in the transmission network is initially infected, then all agents connected in the transmission network to this agent will become infected.*

2.3 Related literature on network security

In this section we give an overview of literature that models security in networks. Two different models are distinguished: models that cast security as exogenous and models that cast security as endogenous. When security is modeled as exogenous often an intelligent defender (like an authority) defends the network against an intelligent adversary. This form of security is often modeled as a (Colonel) Blotto game in the literature. Although there are many variants, in a Blotto game generally two players distribute resources over a network (like a battlefield). The player that allocates the highest level of resources to an object wins the object. In contrast, when security is modeled as endogenous, multiple intelligent and self-interested agents (modeled as nodes in a network) are responsible for security. In this research, network security is modeled as endogenous security where multiple agents secure against an intelligent attacker. For completeness we start with a prompt discussion on exogenous security.

2.3.1 Exogenous network security

We define exogenous security as (theoretical) security models where not the nodes/agents in the network determine the security level, but instead an outsider (an authority or ISP) determines the security level. Often, for instance in Blotto games, this outsider chooses the security level anticipating an attack of a (malicious) attacker. The attacker, upon learning the 'defense resources', chooses an attack strategy. In this set-up security is modeled as a sequential game: a game where one player chooses his actions before others.

Blotto games can be used to model a wide range of situations. Possibilities include warfare battlefields, patrol schedules, terrorist attacks and firewall construction. In their recent paper, Goyal and Vigier (2014) build a model where a defender can both choose the security level and the network structure. They conclude that, in almost all situations, the star network with all defense resources allocated at the central node is optimal. In figure 10 an example is given from Goyal and Vigier. Bier (2007) builds a similar model: a defender allocates defensive resources to a collection of locations and an attacker, by observing these defensive resources, chooses a location of attack. Bier concludes that the defender sometimes prefers a higher vulnerability at a particular location even if a lower risk could be achieved at zero cost.

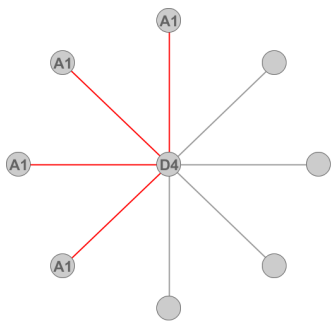

Figure 10 – *The attacker allocates 1 attack resource A at 4 periphery nodes while the defender allocates 4 defense resources D at the central node. In the figure the attack resources 'attack' the central node: an attack which is successful with probability (attack resources/total resources) $= 1/2$.*

2.3.2 Endogenous network security

Different than in exogenous security models, in endogenous security models (self-interested) agents are responsible for security. Often some specific elements (e.g. a virus, resource or information) spreads through a network and provide advantages or disadvantages to affected agents. The strategic decision of an agent often enhances or decreases the spread of these elements, providing benefits or disadvantages to the agent himself and, to some extent - dependent on the network structure - to other agents. Heal and Kunreather (2005) denote these models as interdependent security models (IDS). The central issue in these models is behavior in the face of risks whose magnitude depends on an agent's own risk-management strategies and those of others. In this section, we first discuss literature that cast the risk-management strategy as an *investment* in security. Next we discuss literature that includes an intelligent attacker in these models. Lastly, we discuss models that cast security as a network formation process. In this process, each agent determines his (expected) connectivity in the network.

IDS problems
In their widely referenced paper, Heal and Kunreuther set up an extensive interdependent security model (IDS). It is assumed that each agent has some direct loss, which depends on an agent's own strategy, and some indirect loss, which depends on the strategy of other agents. The authors show that security investments of an agent create positive externalities for others, which in turn may discourage the investments of others. In this case agents invest less than socially optimal. Interesting notion which is discussed is tipping: identifying a coalition of agents with the property that if they invest, others will follow.

Heal and Kunreather base their conclusions without explicitly including the network structure (adopting a complete network). Acemoglu *et al.* (2013) show in their recent paper that this network structure can be very relevant. In a model where spread of an infection is modeled as site percolation (see section 2.2.2) with a probability that depends on security investments, the authors give an example of an asymmetric network where agents invest more than socially optimal. Nevertheless, bulk of the research is based on showing that under-investments prevail in symmetric networks.

This approach of considering homogeneous agents in symmetric networks is more common. For instance Lelarge and Bolot (2008) model security investments in complete networks and tree networks where the infection spreads according to bond percolation. By using a local mean field method (LMF) based on estimating externalities by a tree structure, the authors compute the price of anarchy (PoA: measure of efficiency of the equilibrium due to selfish behavior) and conclude from this PoA that agents under-invest in security.

A similar approach as Lelarge and Bolot is applied by Amin *et al* (2013) and Yang and Lui (2014). Yang an Lui characterize a network game in which agents only have local information about the network structure and security investments. They show that under-investments in security prevail in this incomplete information model. Amin *et al.* model inter-connectivities between control systems where failures of one system influence the number of failures of other systems. The authors show that individual systems tend to invest less in a non-cooperative situation than in a cooperative situation (social optimum).

Although in previous literature contagion is modeled as percolation, also other possibilities are known. For instance Omic *et al.* (2009) model security investments in a compartment model (see section2.2.1). In their model the authors slightly adapt the N-intertwined model by including a 'curing rate'. Although a higher curing rate is more costly, agents with a higher curing rate recover more quickly from an infection. When agents choose their curing rate to minimize their cost function in a steady state environment, the authors show that the price of anarchy may be prohibitively high. This - once again - indicates under-investments in security.

IDS problems with an intelligent adversary
In this class of IDS problems the role of the adversary is explicitly modeled while maintaining the core component of the IDS problem: security investments of one agent affect other agents. Different than in the previous class, by including an intelligent adversary security adoptions might as well create negative externalities for others: greater investments by an agent pushes the attacker to attack someone else.

Acemoglu and others (2013) also analyze the effect of an intelligent adversary (strategic attack) in their paper. By allowing a mixed strategy for the attacker and obviate (by a cost function) a very precise location of the attack, the authors show that a Nash equilibrium exists. Additionally the authors derive several sufficient conditions for over-investment or under-investment in symmetric networks. They show that when the cost for the adversary is low, i.e. allowing a more precise attack, generally over-investments prevail.

Bachrach *et al.* (2013) set up a quite similar model as Acemoglu and others. Different however, they consider mixed strategies for agents and assume that the attacker does not incur any cost for attacking an agent. Their results (in complete networks) indicate a general theme: agents compete for security when the attacker is intelligent. In line with Acemoglu this competition results in over-investments in security. Additionally the authors show that an increase in the number of agents leads to a first order stochastic shift of the security investments.

Johnson *et al.* (2013) assume that the agent with the lowest protection is attacked by a strategic adversary. Although the authors do not incorporate contagion (empty network), they show that agents invest much more in a non-cooperative situation than in a cooperative situation.

Network formation as security measure
In previous literature security measures are *investments* in security which decrease the probability of infection or increase the recovery rate. An alternative security measure however is to adapt the network structure. In real world there are many situations in which self-interested agents form links with each other, producing an underlying network structure. Intuitively there is a trade-off between connectivity and contagion risk: while agents receive benefits by connecting to other agents, a higher connectivity results in more ways in which the infection can reach an agent.

Blume *et al.* (2013) construct a very basic model for this situation. Although an agent can not choose to whom he is connected, he receives some fixed payoff by choosing a higher connectivity. The authors show that that more welfare is obtained when agents cooperatively (socially) choose their connectivity.

Baccara and Bar-Isaac (2006) set up an extensive network formation model where criminals form connections with each other. Increased connectivity again provides an increased pay-off. Drawback of increased connectivity is an increased chance that the criminal is betrayed by other criminals who are 'detected' by an external authority. Baccara and Bar-Isaac provide characteristics of optimal networks. In most nontrivial situations (trivial situations lead to an empty or complete network) this is either a star network or a binary network in which every agent is connected to one (and only one) other agent.

Larson (2011) proposes a model in which agents can choose both their connectivity and their security investments. In this model, both (positive) tips and (negative) viruses spread through a large random network. Agents strategically decide, before the initial location of the virus/tip is known, their security level as well as their expected number of connections. For infinitely large random networks and under a symmetry assumption between agents, equilibria are derived and its properties are discussed for two cases of cost functions. The author shows for instance that connectivity in a cooperative game is lower than in the non-cooperative game. Also Larson derives conditions for over-connectivity and evaluates the effects of a change in likelihood that an outbreak is either a tip or a virus (resilience of the network). Although the model is exceptional in allowing individual agents to form links and to choose their security investments, the complexity of the model forces the author to work with infinitely large networks and a symmetry assumption between agents.

3 The model

In this chapter we first discuss the notation and terminology that we use in this research. Afterwards we present our model of endogenous security.

3.1 Notation and terminology

In this paper $\mathbf{x} = \{x_1, \ldots, x_n\}$ is viewed as a row vector where x_i is the ith element of $\mathbf{x}$. Define the subvector of $\mathbf{x}$ induced by some integer vector T as $\mathbf{x}_{-T} = \{x_i \in \mathbf{x} | i \notin T\}$. A vector $\mathbf{x}$ is said to be *symmetric* if all the elements are identical (i.e. $x_i = x_j \ \forall i, j$). In this case, the notation $\mathbf{x} = c$ indicates that all elements in $\mathbf{x}$ are equal to some scalar c. Similar, $c\mathbf{x}$ indicates that all elements in $\mathbf{x}$ are multiplied with c. A vector is said to feature *over-investments* relative to some equal length vector $\mathbf{y}$ if all elements in $\mathbf{x}$ are larger than the corresponding element in $\mathbf{y}$ (i.e. $x_i \geq \ y_i \ \forall i$). Similarly, $\mathbf{x}$ features *under-investments* relative to $\mathbf{y}$ if $x_i \leq \ y_i \ \forall i$. The 1-norm $|\mathbf{x}|$ is defined as the sum over all elements in $\mathbf{x}$.

In this research we consider twice differentiable functions f from $I^n = [0,1]^n$ to $I = [0,1]$. We say that f attains a *global maximum* in $f(\mathbf{x}^*)$ if $f(\mathbf{x}^*) \geq f(\mathbf{x})$ for all $\mathbf{x} \in I^n$. Note that by Weierstrass Theorem[8] f attains such global maximum in I^n. To find this global maximum some additional notions are required. We say that the function f attains a *local maximum* at $f(\mathbf{x}^*)$ if there exists an $\epsilon > 0$ such that $f(\mathbf{x}^*) \geq f(\mathbf{x})$ for all $\mathbf{x} \in B_\epsilon(\mathbf{x})$, where $B_\epsilon(\mathbf{x}^*) = \{\mathbf{x} \in I^n \mid |\mathbf{x} - \mathbf{x}^*| < \epsilon\}$. Surely any global maximum is a local maximum but the converse is not necessarily the case. We define the gradient of f at $\mathbf{x}^* \in I^n$ as

$$\nabla f(\mathbf{x}^*) = \{\frac{df}{dx_1}(\mathbf{x}^*), \ldots, \frac{df}{dx_n}(\mathbf{x}^*)\}$$

and say that f satisfies the *first order condition* (FOC) for optimality at $\mathbf{x}^*$ if

$$\nabla f(\mathbf{x}^*) = 0.$$

Although the local maxima of f necessarily satisfy the FOC, the global maximum may not do so. Specifically when the global maximum does not satisfy the FOC, then it is a *boundary maximum*. We say that f attains such boundary maximum at $\mathbf{x}^*$ if $f(\mathbf{x}^*)$ is a global maximum and either $0 \in \mathbf{x}^*$ or $1 \in \mathbf{x}^*$.

In this research we say that f is strictly concave when the Hessian of f,

$$H(f(x^*)) = \begin{bmatrix} \frac{d^2 f}{dx_1^2}(x^*) & \frac{d^2 f}{dx_1\, dx_2}(x^*) & \cdots & \frac{d^2 f}{dx_1\, dx_n}(x^*) \\ \frac{d^2 f}{dx_2\, dx_1}(x^*) & \frac{d^2 f}{dx_2^2}(x^*) & \cdots & \frac{d^2 f}{dx_2\, dx_n}(x^*) \\ \vdots & \vdots & \ddots & \vdots \\ \frac{d^2 f}{dx_n\, dx_1}(x^*) & \frac{d^2 f}{dx_n\, dx_2}(x^*) & \cdots & \frac{d^2 f}{dx_n^2}(x^*). \end{bmatrix}$$

is negative definite for every $\mathbf{x}^* \in I^n$. The function f is strictly convex when $-f$ is strictly concave. When a function is strictly concave it can not attain more than one local maxima.

To analyze the behavior of $f(\{x_i, \mathbf{x}_{-i}\})$, where $\mathbf{x}_{-i} \in I^n \backslash I$ is given, note that the same definitions as above apply to $f(\{x_i, \mathbf{x}_{-i}\})$ only with $f(\{x_i, \mathbf{x}_{-i}\})$ a 1-dimensional function. In this research we let $\varphi_i : I^n \backslash I \to B$ a set valued function[9] such that for all $x_i \in I$ and all $x_i^* \in \varphi_i(\mathbf{x}_{-i}^*)$:

$$f(\{x_i^*, \mathbf{x}_{-i}^*\}) \geq f(\{x_i, \mathbf{x}_{-i}^*\}).$$

This function $\varphi_i(\mathbf{x}_{-i}^*)$ is denoted as the *best response* in f and given $\mathbf{x}_{-i}^*$.

We say that $\mathbf{x}^*$ is a *fixed point* if $x_i^* \in \varphi_\nu(\mathbf{x}_{-\nu}^*)$ for every i. When $\varphi_i(\mathbf{x}^*) \in [0,1]$ we denote $\varphi = \{\varphi_1(\mathbf{x}_{-1}^*), \ldots, \varphi_n(\mathbf{x}_{-n}^*)\}$ as the vector of best responses. In this case $\mathbf{x}^*$ is a fixed point if $\varphi(\mathbf{x}^*) = \mathbf{x}^*$.

8. Let $D \subset \mathbb{R}^n$ be a compact set and $f : D \to (R)$ a continuous function, then f attains a maximum (and a minimum) on D.
9. Here a set valued function is a function that maps an element in $I^n \setminus I$ on some set in I, for instance an interval.

3.2 Model description

The strategic behavior of n interconnected agents is investigated in an undirected network $\mathcal{G} = (V(\mathcal{G}), A(\mathcal{G}))$ with some edge set $E(\mathcal{G})$[10]. Here $V = \{1, .., n\}$ is a finite set of agents and $A : V \times V \to \{0, 1\}$ is the adjacency matrix in which $A(\nu, \mu) = A(\mu, \nu) = 1$ if and only if ν and μ are linked.

Assume that every agent owns a unique document. We denote the document of agent ν as d_ν. Other agents in the network might obtain d_ν as the documents spread over the network. We assume that the spreading of the n distinct documents happens independently of each other. An agent ν might for instance share his own document with another agent, this agent in turn might not share his document with ν.

Spreading of the n documents happens according to the bond percolation model as described in section 2.2.2. From network $\mathcal{G}$ edges are removed, independently of each other and with some exogenous probability $1-p$. When we consider the spread of - say - document d_ν, we denote the emerging network as the *transmission network* $\mathcal{T}_\nu$. If an agent is still connected to ν in $\mathcal{T}_\nu$, then the agent receives d_ν. As the spreading of the n distinct documents happens independently, note that n transmission networks are formed when we consider the spreading of all documents.

By exploring the network structure one can compute the probability that a document spreads from the owner of a document to another agent. We set

$$D^{\mathcal{G}}_{\mu,\nu} = \Pr\{\text{Agent } \nu \text{ obtains } d_\mu \text{ in network } \mathcal{G}\}$$

and set $D^{\mathcal{G}}_{\nu,\nu} = 1$. Note that although $D^{\mathcal{G}}_{\mu,\nu}$ is a function of the network structure and p, we do not highlight this dependency as we assume the network structure and p to be exogenous. Also when there is no ambiguity we denote $D^{\mathcal{G}}_{\mu,\nu}$ as $D_{\mu,\nu}$ in this report. Note that in an undirected network, $D_{\mu,\nu} = D_{\nu,\mu}$ but also note that, as the documents spreads independently of each other

$$\Pr\{\text{Agent } \nu \text{ obtains } d_\mu \mid \text{Agent } \kappa \text{ obtains } d_\eta\ \} = Pr\{\text{Agent } \nu \text{ obtains } d_\mu\}$$

for every $\kappa \neq \nu$ and $\eta \neq \mu$.

We denote the *expected* number of documents obtained by agent ν in network $\mathcal{G}$ as $D^{\mathcal{G}}_{\nu}$. Again, when there is no ambiguity, we abbreviate $D^{\mathcal{G}}_{\nu}$ to D_ν. By noting that D_ν is the expectation of a sum of Bernoulli random variables, we establish that

$$D_\nu = \sum_{\mu \in V} D_{\mu,\nu}.$$

Now suppose that a malicious attacker attempts to hack one of the agents to acquire confidential documents. Although it is not harmful for an agent for other agents to possess his confidential document, it is detrimental if the attacker acquires his document. Assume that, if the attack is successful, the attacker obtains all the documents that are obtained by the target. This includes the target's own document but can additionally include documents of others which are obtained by the target. In expectation, if the attack on agent ν is successful, the attacker acquires D_ν documents. Let x_ν be the event that the document of agent ν is obtained by the attacker[11] and set $\mathbf{x} = \{x_1, \ldots, x_n\}$.

The decision of the attacker which agent to target can be represented by a random variable (r.v.) drawn from a probability space $\{\Omega, \mathcal{F}, a\}$, where $\Omega = \{1, \ldots, n\}$, $\mathcal{F} = \mathcal{P}(\Omega)$ the power set of Ω and $a : \mathcal{F} \to [0, 1]$ with $\sum_{\nu \in V} a(\{\nu\}) = 1$. This probability a can conveniently be represented by a probability vector[12] $\mathbf{a} = \{a_1, \ldots, a_n\}$, where a_ν is the probability that agent ν is attacked. Recognize that, as all a_ν add to one, the attacker will always attack an agent. The vector $\mathbf{a}$ is denoted as the *attack vector* in this

10. When there is no ambiguity these notions are abbreviated - respectively - to V, A and E.
11. Note that $x_\nu = 1$ if the attacker obtains d_ν and $x_\nu = 0$ if the attacker does not obtains d_ν.
12. The vector $\mathbf{a}$ is a probability vector if and only if all entries are non-negative and the entries add up to one.

research and, with a slight abuse of terminology, it is said that the decision of the attacker is a random variable drawn from $\mathbf{a}$.

To prevent that an attack is successful, agents precautionarily invest in security. Let $q_\nu \in [0,1]$ be the investment of agent ν and set $\mathbf{q} = \{q_1, \ldots, q_n\}$. The vector $\mathbf{q}$ is denoted as the *security vector* in this research. It is assumed that an attack on agent ν is successful with probability $(1-q_\nu)$ and not successful with probability q_ν. By conditioning we deduce that

$$\begin{aligned}
\Pr\{x_\nu = 1\} &= \Pr\{\text{ the attacker obtains } d_\nu \text{ }\} \\
&= \sum_{\mu \in V} a_\mu \Pr\{x_\nu = 1 | \mu \text{ is attacked }\} \\
&= \sum_{\mu \in V} a_\mu (1 - q_\mu) \Pr\{x_\nu = 1 | \mu \text{ is attacked, attack is successful }\} \\
&= \sum_{\mu \in V} a_\mu [1 - q_\mu] D_{\nu,\mu}. \qquad (3.1)
\end{aligned}$$

Recognize that $\mathbf{x}$ is a vector of Bernoulli random variables with probability of the ith element given in (3.1). Clearly this probability does not only depends on an agent's own security investment q_ν, but in fact depends on the whole security vector and, moreover, on the attack vector. In the next two sections we discuss how the security vector and the attack vector are established. First, table 2 gives a summary of all the relevant variables in our model.

Variable	Description
d_ν	Unique and confidential document of agent ν.
$\mathcal{G}$	Network where edges *may* transmit documents.
$\mathcal{T}_\nu$	Network where edges *do* transmit documents.
p	Probability that an edge transmits documents.
$\mathbf{q}$	Vector where q_ν are security investments of agent ν, $\mathbf{q} \in [0,1]^n$.
$\mathbf{a}$	Vector where a_ν is the probability that agent ν is attacked ($\lvert\mathbf{a}\rvert = 1$ and $a_\nu \geq 0$).
$\mathbf{x}$	Vector where x_ν is the event that d_ν is obtained by the attacker.
$D_{\nu,\mu}$	Probability that agent μ obtains d_ν.
D_ν	Expected number of documents obtained by agent ν.

Table 2 – *Summary of relevant variables in the model.*

3.2.1 The security vector

The security investments by each agent can be conveniently modeled as the outcome of a game between agents. This game can be represented by

$$\Gamma = \langle\ V,\ (q_\nu)_{\nu \in V},\ (\mathcal{H}_\nu)_{\nu \in V},\ (\Pi_\nu)_{\nu \in V}\ \rangle, \qquad (3.2)$$

where V is the set of agents in network $\mathcal{G}$, $q_\nu \in [0,1]$ is the strategy space (the investments in security) of agent ν, $\mathcal{H}_\nu$ is the information set and Π_ν is the utility function. The game Γ is called the *security game* between agents. In this game rational agents simultaneously choose their investments in security. This decision is made under $\mathcal{H}_\nu = \{\mathcal{G}, p, \mathbf{a}\}$: every agent has complete information about the network, is aware of the value of p and knows the attack vector $\mathbf{a}$.

We consider a *cooperative game* and a *non-cooperative game* in this research. If Γ is a non-cooperative game, every agent rationally chooses investments such that his utility is maximized given the expected strategic decision of other agents and under the information set. Formally every agent plays an element from his best response $\varphi_\nu(\mathbf{q}_{-\nu})$ in Π_ν and given $\mathbf{q}_{-\nu}$. We define a security profile $\mathbf{q}^N$ to be a (pure strategy) *Nash equilibrium* if the best response of each agent given $\mathbf{q}^N$ is the same security profile again (i.e. $\mathbf{q}^N$ is a fixed point of all best responses).

We assume that the utility $\Pi_\nu : [0,1]^n \to \mathbb{R}$ of agent ν is the probability that d_ν is not exposed to the attacker minus the investment cost:

$$\Pi_\nu = Pr\{x_\nu = 0\} - c(q_\nu). \tag{3.3}$$

Here $c(q_\nu)$ is the cost agent ν incurs for investing q_ν and $Pr\{x_\nu = 0\}$ is given in (3.1). As x_ν depends both on an agent's own strategy and on the strategy of other agents, we developed an interdependent security model as defined by Heal and Kunreuther (2004).

In a cooperative game, different than in a non-cooperative game, (two or more) agents cooperate to maximize their combined utility given the expected decisions of other agents. Let $T_1 \dots T_k$ be a partition of the vertex set V and assume that agents in each set cooperate. The combined utility S_{T_i} of agents in T_i is defined as

$$S_{T_i} = \sum_{\nu \in T_i} \Pi_\nu. \tag{3.4}$$

Again we assume that every agent plays a strategy such that S_{T_i} is maximized given the expected decision of other agents and under the information set. Specifically agent ν plays $q^*_\nu \in \varphi_\nu(\mathbf{q}_{-\nu})$, where φ_ν is the best response of ν in S_{T_i} given $\mathbf{q}_{-\nu}$. An equilibrium situation emerges when the best response of each agent given $\mathbf{q}^*$ is the same investment level again. Note that when T_i contains one agent for every i, the investment level $\mathbf{q}^* \equiv \mathbf{q}^N$, the Nash equilibrium of the security game. Differently when T_1 contains all agents, we define $\mathbf{q}^* \equiv \mathbf{q}^s$ to be the *social optimum* of the security game. In this case S_{T_1} is abbreviated to S. It can be showed that by combining (3.1) with (3.4), S can be written as

$$S = n - \mathbb{E}(\ |\mathbf{x}|\ ) - \sum_{\nu \in V} c(q_\nu), \tag{3.5}$$

where $\mathbb{E}(|\mathbf{x}|)$ is the expectation[13] of $|x|$.

Neither the Nash equilibrium nor the social optimum is always unique. Let $\{\mathbf{q}^N\}$ be the set of all pure Nash equilibria and similar $\{\mathbf{q}^s\}$ be the set of all social optima of Γ.

To measure the efficiently of the Nash equilibrium, the *price of anarchy* (PoA) can be used. In this paper, this PoA is defined as

$$PoA = \frac{\min_{\{\mathbf{q}^s\}} \mathbb{E}(\ |x| \mid \mathbf{q} = \mathbf{q}^s)}{\max_{\{\mathbf{q}^N\}} \mathbb{E}(\ |x|\ |\mathbf{q} = \mathbf{q}^N)}. \tag{3.6}$$

This PoA is the ratio between the expected damage in the best social optimum and the worst pure Nash equilibrium.

3.2.2 The attack vector

The probability that an agent is affected, as given in equation (3.1), does not only depends on the security vector, it also depends on the attack vector $\mathbf{a}$. In line with Acemoglu *et al.* (2013) we investigate two different strategies: a *random attack* and a *strategic attack*. Under the random attack $\mathbf{a}$ is a probability vector which is chosen independently of security investments and the network. In this situation the attacker targets agents according to for instance (non-modeled) characteristics or just randomly.

When the attack is strategic $\mathbf{a}$ does depend on the investments and the network. We assume that the attacker holds some utility function $\Pi_a : [0,1]^n \to \mathbb{R}$, where

$$\Pi_a = \mathbb{E}[\text{ number of documents obtained in an attack }] - \sum_{\nu \in V} \psi(a_\nu).$$

In this utility function $\psi(a_\nu)$ is the cost the attacker incurs for choosing a_ν. One can show that Π_a can be written as

$$\Pi_a = \mathbb{E}(\ |\mathbf{x}| \mid \mathbf{q}\ ) - \sum_{\nu \in V} \psi(a_\nu). \tag{3.7}$$

13. Note that $\mathbb{E}(\ |\mathbf{x}|\ ) = \mathbb{E}(\sum_\nu x_\nu) = \sum_\nu \mathbb{E}(x_\nu) = \sum_\nu Pr(x_\nu = 1)$ as in (3.1).

The attacker chooses $\mathbf{a}$ such that his utility is maximized. As this decision is under the constraint that the attack vector remains a probability vector, the strategy of the attacker is the solution of the program:

$$\begin{aligned} \textbf{max} \quad & \Pi_a \\ \text{subject to:} \quad & |\mathbf{a}| = 1 \text{ and } a_\nu \geq 0 \text{ for all } \nu \in V. \end{aligned} \tag{3.8}$$

Note that we assume that $\mathbf{q}$ is known to the attacker as $\mathbf{q}$ is given in (3.7). In this setting first agents play the security game, choosing their security investments. Next the attacker, by observing the security investments, chooses his strategy by solving (3.8). However, as **a** is included in the information set $\mathcal{H}_\nu$ of each agent, agents choose their security investments *anticipating* the decision of the attacker. Specifically, we assume that agents know the strategy of the attacker **a** as a function of **q**. This function (later we will show that it exists) is substituted in the utility of each agent[14].

Finally note the resemblance of the social utility (3.5) with (3.7). In this framework the attacker endeavors to find an optimal trade-off between damage and costs while the cooperating agents find an optimal trade-off between safety and costs[15].

To conclude this model description, figure 11 summarizes all the events and the corresponding timing.

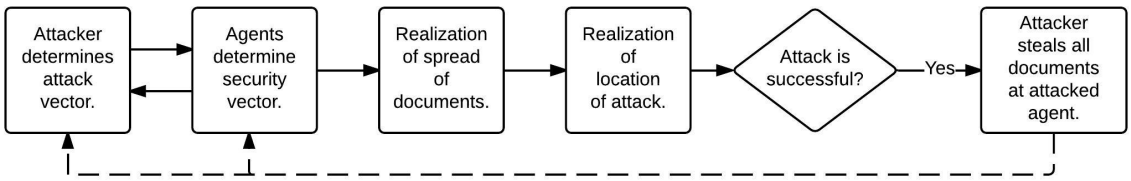

Figure 11 – *Summary of events and timing in the model. As decisions of the attacker and agents are based on stochastics of the last (right) event, the dashed line is included.*

14. This approach is common in sequential games where one player chooses his actions before others choose theirs (see Peters 2008). The strategy of the player who chooses last, is analyzed first and is substituted in the decision process of other agents.
15. In fact this setup is similar as seen in many Blotto games (see section 2.3.1 on page 11). For instance Goyal and Vigier (2014) adopt two utility functions that create opposite incentives: one player defends while the other attacks.

4 Spreading of documents

In this chapter we discuss the spreading of the documents in more detail. As our focus lies on the security game in this research the discussion in this chapter is not thorough. Yet, several results in this chapter are used later in the security game to analyze the role of the network structure.

First we present some basic definitions from graph theory to further specify the notations that we will use. Next we focus on the probability that documents are shared and afterwards we continue on the expected number of documents obtained by each agent.

4.1 Basic definitions from graph theory

Remind that the behavior of n interconnected agents[16] is investigated in a undirected network $\mathcal{G} = (V(\mathcal{G}), A(\mathcal{G}))$, with $E(\mathcal{G})$ the edge set of $\mathcal{G}$. In this research, $e = \{\nu, \mu\}$ is an edge in E if and only if $A(\nu, \mu) = 1$.

It is convenient to define several notions of connectivity of the network. For $l \in \mathbb{N}$, let $\mathcal{N}^l(\nu)$ be the l *order neighborhood* of ν. Formally define $\mathcal{N}^l(\nu)$ iteratively as

$$\mathcal{N}^l(\nu) = \{\mu \in V | A(\mu, \kappa) = 1, \text{ for some } \kappa \in \mathcal{N}^{l-1}(\nu)\},$$

with initial condition $\mathcal{N}^0(\nu) = \nu$.

Agent ν and agent μ are said to be *neighbors* if $\mu \in \mathcal{N}^1(\nu)$. We define the *degree* of agent ν as the number of neighbors of ν: degree$(\nu) = |\mathcal{N}^1(\nu)|$. Agent ν and agent μ are said to be *connected* if

$$\mu \in \bigcup_{l=0}^{\infty} \mathcal{N}^l(\nu),$$

which will be denoted as $\nu \sim \mu$. Note that as $\mathcal{G}$ is undirected, $\mu \in \bigcup_{l=0}^{\infty} \mathcal{N}^l(\nu)$ if and only if $\nu \in \bigcup_{l=1}^{\infty} \mathcal{N}^l(\mu)$. The *distance* between ν and μ is defined as dist$(\nu, \mu) = \min\{l | \mu \in \mathcal{N}^l(\nu)\}$. If ν and μ are not connected then dist$(\nu, \mu) = \infty$. We define the *component* C in which ν lies as

$$C(\nu) = \{\mu \mid \mu \in \cup_{l=0}^{\infty} \mathcal{N}^l(\nu)\}.$$

If all agents lie in the same component, then A is said to be *connected*.

Remind that our spread model is based on removing edges from a network. The process of removing edges (or nodes) leads to a *subgraph* of the original network. Formally $\mathcal{H}$ is said to be a subgraph of $\mathcal{G}$ (denoted as $\mathcal{H} \subset \mathcal{G}$) if $V(\mathcal{H}) \subset V(\mathcal{G})$ and the adjacency matrix of $\mathcal{H}$ is a subset of that of $\mathcal{G}$; restricted to the subset $V(\mathcal{H})$. The other way around, if $\mathcal{H}$ is a subgraph of $\mathcal{G}$, then we call $\mathcal{G}$ a *super-graph* of $\mathcal{H}$. Additionally we define a subgraph *induced* by $S \subset V$ as the graph $\mathcal{G}[S]$ with node-set S and $A_{\mathcal{G}[S]}(\nu, \mu) = 1$ if and only if $A_{\mathcal{G}}(\nu, \mu) = 1$ and $\nu, \mu \in S$.

A *path* in $\mathcal{G}$ is a sequence $u = \{\nu_1, e_1, \nu_2, \ldots, e_n, \nu_n\}$ such that all e_i are distinct and ν_1 and ν_n are connected by the path. We set $U_{\mu,\nu} = \{u_1, \ldots, u_n\}$ as the set of all paths between agent μ and agent ν. A *cycle* is a path from $U_{\nu,\nu}$, i.e. a path starting and ending at the same agent.

In figure 12 several concepts are illustrated. Additionally figure 13 features some networks that have a special interest in this research. Formally a *complete network* is a network which features a maximal number of edges. A network is a *ring network* if and only if there are two disjoint paths (i.e. no edge is in multiple paths) between any two nodes. Lastly in a *tree network* there is a unique path between any two agents.

16. In this research we use the terms agents, nodes and vertices (singular: vertex) interchangeable. Similarly the terms network and graph are used interchangeable.

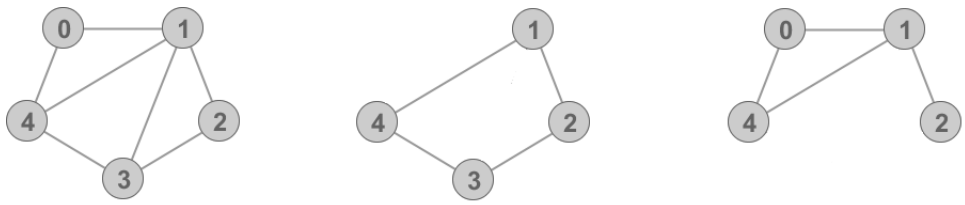

Figure 12 – *Denote the first (left network) as $\mathcal{G}$. Recognize that $\mathcal{N}^1(0) = \{1,4\}$, $\mathcal{N}^2(0) = \{2,3\}$ and $C(0) = V = \{0,1,2,3,4\}$. In the network $u_1 = \{0,(0,4),4,(4,1),1,(1,2),2\}$ is a path from agent 0 to agent 2. Note however that $u_2 = \{0,(0,1),1,(1,2),2\}$ is a shorter (in fact the shortest) path from agent 0 to agent 2. The other two networks in the figure are subgraphs of $\mathcal{G}$. Specifically, the last (right) network is a subgraph of $\mathcal{G}$ induced by $\{0,1,2,4\}$.*

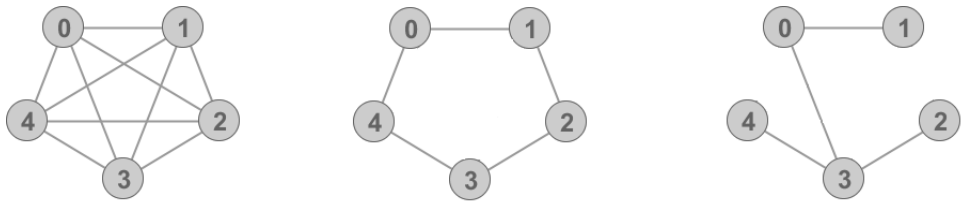

Figure 13 – *Several networks of interest. The first (left) network is the complete network K_5 while the middle network is the ring network R_5. The last (right) network is an example of a tree: there is a unique path between any two agents.*

4.2 Probability that documents are shared

Remind that the spreading of the documents happens independently of each other and according to bond percolation with probability p. Specifically, *for every* document a transmission network $\mathcal{T}$ is formed by removing edges in the original network, independently of each other and with some exogenous probability $1-p$. All the agents connected to the owner of a document in this transmission network obtain the document. Consequently, the probability that an agent obtains a document

$$\begin{aligned} D_{\mu,\nu} &= \Pr\{\text{Agent } \nu \text{ obtains } d_\mu\} \\ &= \Pr\{\nu \sim \mu \text{ in } \mathcal{T}_\mu\} = \Pr\{\nu \in C(\mu) \text{ in } \mathcal{T}_\mu\}, \end{aligned} \tag{4.1}$$

where $\mathcal{T}_\mu$ is the transmission network when considering document d_μ. When there is no ambiguity this is shortened to $\mathcal{T}$. In this section we present methods to compute $D_{\mu,\nu}$. As these methods require a lot of *ad hoc* reasoning we leave the computation of $D_{\mu,\nu}$ as an open problem for the practitioner. Yet we do compute $D_{\mu,\nu}$ in a ring and a complete network in this section.

4.2.1 How to compute $D_{\mu,\nu}$?

In this section we present two methods to compute $D_{\mu,\nu}$. The first method is based on removing edges from $\mathcal{G}$ while the second method is based on considering all paths between two agents in $\mathcal{G}$.

First method to compute $D_{\mu,\nu}$: decomposing the network.
One way to compute $D_{\mu,\nu}$ is to condition on the event that an edge is present, or not, in the transmission network. When an edge is not in $\mathcal{T}$, then it can be removed from the original network as this edge never transmits a document. The result is showed in the next proposition.

Proposition 4.1. *For all $e \in E(\mathcal{G})$*

$$\begin{aligned} D_{\mu,\nu} &= \Pr\{\nu \sim \mu \textit{ in } \mathcal{T}, e \in E(\mathcal{T})\} + \Pr\{\nu \sim \mu \textit{ in } \mathcal{T}, e \notin E(\mathcal{T})\} \\ &= Pr\{\nu \sim \mu \textit{ in } \mathcal{T} | e \in E(\mathcal{T})\}p + D_{\mu,\nu}^{E(\mathcal{G})\setminus e}(1-p), \end{aligned}$$

where $D_{\mu,\nu}^{E(\mathcal{G})\setminus e}$ is the probability that agent ν obtains d_μ in a network where e is removed.

The relation in the proposition provides some grasps on $D_{\mu,\nu}$. Note however that information between two arbitrary agents does not necessarily spread over e and hence ad hoc reasoning is required. Still, for some networks $D_{\mu,\nu}$ is readily computed by applying proposition 4.1. An example is a tree.

Proposition 4.2. *If $\mathcal{G}$ is a tree network, then $D_{\mu,\nu} = p^{dist(\mu,\nu)}$.*

Proof. Let $u = \{\nu, \ldots, \mu\}$ be the unique path from agent μ to agent ν. By applying proposition 4.1 to every edge in u and noting that $D_{\mu,\nu}^{E(\mathcal{G})\setminus e} = 0$, the result follows. □

Although quite sparse, there are some examples of information networks which themselves attain a tree structure. One can think of a hierarchy network in a company or a provider/user network. In the first example, information (a strategic decision) is told to a chef, who in turn might inform his chef about the decision. Note however that in reality the decision might first be told to a colleague who - in turn - informs the chef about the decision. This clearly touches the limitation of tree networks as in many real world information networks multiple cycles are present. Figure 14 shows for instance three (non exhausting) transmission networks in which agent 2 obtains d_0 in $\mathcal{G}$ as in figure 12. In the first two network the information is obtained through agent 1, while in the last network the information is obtained through agent 1 and agent 3[17].

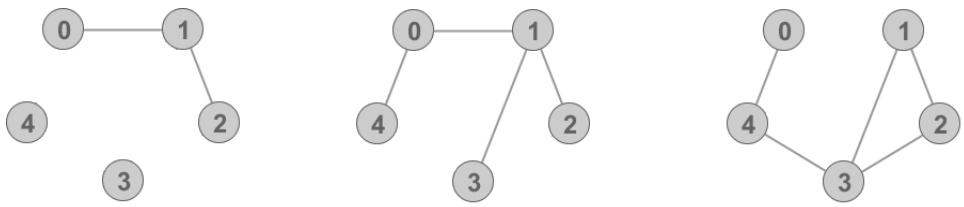

Figure 14 – *Transmission networks of $\mathcal{G}$ as in figure 12. In these transmission networks agent 2 obtains d_0. The networks emerge with a probability of (from left to right) $p^2(1-p)^5$, $p^4(1-p)^5$ and $p^4(1-p)^5$. Note however that the probability that (for instance) the path $\{0,(0,1),1,(1,2),2\}$ emerges in $\mathcal{T}$ is p^2.*

Figure 14 highlights that a document can spread over several paths. To compute $D_{\mu,\nu}$ in these networks, the practitioner should apply proposition 4.1 in a way such that the number of cycles are reduced. When repeating this procedure, eventually all cycles are removed and a tree network emerges. Consequently proposition 4.2 can be used to compute $D_{\mu,\nu}$ in this tree network. For instance in K_3, as showed in figure 15, $D_{0,2}$ can be computed by removing $(0,2)$:

$$\begin{aligned} D_{0,2} &= \Pr\{0 \sim 2 \text{ in } \mathcal{T} | (0,2) \notin E(\mathcal{T})\}(1-p) + \Pr\{0 \sim 2 \text{ in } \mathcal{T} | (0,2) \in E(\mathcal{T})\}p \\ &= p^2(1-p) + p \\ &= p + p^2 - p^3. \end{aligned}$$

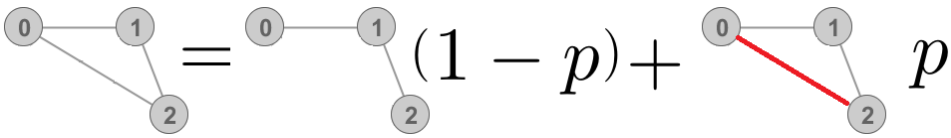

Figure 15 – *Computing $D_{0,2}$ in a network with a cycle by applying proposition 4.1.*

Like every network can be decomposed to a network without cycles (a tree), also every network can be decomposed to a network in which every edge is in at least one cycle. Specifically, every network can

17. Note that as our spread model is time independent, one can not deduce from who - agent 1 or agent 3 - agent 2 obtains d_0 first. Also note that in our model it does not make any difference if a document is obtained once or multiple times.

be decomposed to a network that does not feature any cut-edges[18]. As a cut edge is either in every path between two agents, or not in any path between these agents, the following result is established.

Proposition 4.3. *Let e be a cut-edge. If e is in every path between agent ν and μ,*

$$D_{\mu,\nu} = \Pr\{\textit{Agent } \nu \textit{ obtains } d_\mu \textit{ in } \mathcal{G}\ \} = p\Pr\{\textit{Agent } \nu \textit{ obtains } d_\mu \textit{ in } \mathcal{G}\cdot e\ \},$$

where $\mathcal{G}\cdot e$ is the network where e is contracted[19]*. If e is not in any path between agent ν and μ,*

$$D_{\mu,\nu} = \Pr\{\textit{Agent } \nu \textit{ obtains } d_\mu \textit{ in } \mathcal{G}\ \} = \Pr\{\textit{Agent } \nu \textit{ obtains } d_\mu \textit{ in } \mathcal{G}\cdot e\ \}.$$

The next example will shed some light on the proposition above.

Example 4.1. In this example we compute $D_{0,2}$ in the first (left) network in figure 16. As $(0,4)$ is a cut-edge and in every path between agent 0 and agent 2 we are allowed to apply proposition 4.3 to $(0,4)$. It follows that $D_{0,2} = pD^M_{0,2}$, where M is the middle network in figure 16. The network can be further decomposed by applying proposition 4.3 to $(0,3)$. It follows that $D_{0,2} = pD^M_{0,2} = p^2D^L_{0,2}$, where L is the last (right) network. Consequently by using the earlier result in K_3, it follows that $D_{0,2} = p^2(p+p^2-p^3) = p^3+p^4-p^5$.

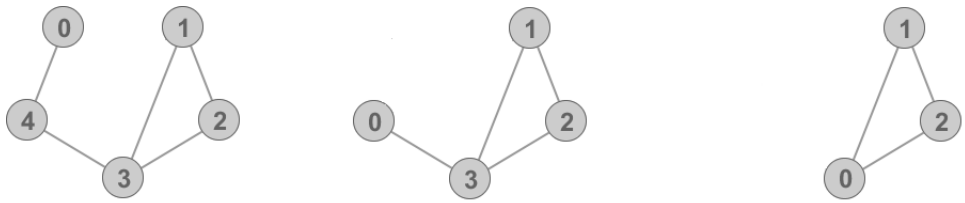

Figure 16 – *Networks in which $D_{0,2}$ is computed by contracting edges.*

Second method to compute $D_{\mu,\nu}$: probability that a path exists in $\mathcal{T}$.

An alternative method to compute $D_{\mu,\nu}$ is to consider all paths between agent μ and agent ν. Clearly, agent ν obtains d_μ when at least one path between the two agents is (still) present in the transmission network, that is

$$\Pr\{\nu \sim \mu \text{ in } \mathcal{T}\} = \Pr\{\bigcup_{i=1}^{n}\Big[\ \mathcal{G}[u_i^*] \subset \mathcal{T}\ \Big]\},$$

where u_i^* is the set of all agents in a path between agent ν and agent μ[20]. Note that, as paths may overlap (an edge may be present in several paths), $\mathcal{G}[u_i^*] \subset \mathcal{T}$ and $\mathcal{G}[u_j^*] \subset \mathcal{T}$ are not always independent events. By using the inclusion-exclusion principle[21]

$$\begin{aligned} D_{\mu,\nu} &= \Pr\{\nu \sim \mu \text{ in } \mathcal{T}\} \\ &= \sum_{i=1}^{n}\Pr\{\mathcal{G}[u_i^*] \subset \mathcal{T}\} - \sum_{i<j}^{n}\Pr\{\bigcap_{s=\{i,j\}}\mathcal{G}[u_s^*] \subset \mathcal{T}\} + \sum_{i<j<k}^{n}\Pr\{\bigcap_{s=\{i,j,k\}}\mathcal{G}[u_s^*] \subset \mathcal{T}\} - \dots, \end{aligned} \tag{4.2}$$

continuing till $s = V$. In the next proposition we extend (4.2) to an alternative method to compute $D_{\mu,\nu}$.

Proposition 4.4. *Let $\{u_1,\dots,u_n\}$ be all the paths between agent ν and μ. When $|u_iu_ju_k\dots|$ are the number of edges in $u_i \cup u_j \cup u_k \dots$, then*

$$D_{\mu,\nu} = \sum_{i=1}^{n} p^{|u_i|} - \sum_{i<j}^{n} p^{|u_iu_j|} + \sum_{i<j<k}^{n} p^{|u_iu_ju_k|} - \dots + (-1)^{n+1}\sum_{1<\dots<n} p^{|u_1u_2\dots u_n|}$$

18. An edge e is a cut edge if and only if $\mathcal{G}$ with $E \setminus e$ is disconnected.
19. Edge contraction is an operation that removes an edge from a network while merging the two nodes that were joined by the edge.
20. To clarify the expression, first note that $\mathcal{G}[u_i^*]$ is the subgraph induced by u_i^*, which simply is the path itself. If this path is a subgraph of $\mathcal{T}$, i.e. the path is present in $\mathcal{T}$, then ν obtains d_μ. As there possibly are several paths, we use the $\cup$ operator.
21. Note that $\sum_{i<j<k\dots}$ is a contraction of $\sum_{i=1}^{n}\sum_{j=i+1}^{n}\sum_{k=j+1}^{n}\cdots$.

Proof. First note that the probability that a particular graph emerges as subgraph of $\mathcal{T}$ is p^x, where x are the number of edges in the graph. When applying this to (4.2), the result follows. □

To apply proposition 4.4 still a lot of *ad hoc* reasoning is required as it is unclear how many edges are included in each combination of paths. Still, proposition 4.4 can be an useful tool to compute $D_{\mu,\nu}$, for instance in the next example.

Example 4.2. Consider the first network in figure 17. We like to compute $D_{0,2}$ by applying proposition 4.4. Note that (with help of the 4 paths highlighted in figure 17)

$$\sum_{i=1}^{n} p^{|u_i|} = p^{|u_1|} + p^{|u_2|} + p^{|u_3|} + p^{|u_4|} = p^2 + p^2 + p^3 + p^3.$$

By repeating this procedure:

$$\sum_{i=1}^{n}\sum_{j>i}^{n} p^{|u_i u_j|} = 5p^4 + p^5, \quad \sum_{i=1}^{n}\sum_{j>i}^{n}\sum_{k>j}^{n} p^{|u_i u_j u_k|} = 4p^5 \text{ and lastly } \sum_{i=1}^{n}\sum_{j>i}^{n}\sum_{k>j}^{n}\sum_{l>k}^{n} p^{|u_i u_j u_k u_l|} = p^5.$$

By combining the results it follows that

$$D_{0,2} = [2p^2 + 2p^3] - [5p^4 + p^5] + [4p^5] - p^5 = 2p^2 + 2p^3 + 2p^5 - 5p^4.$$

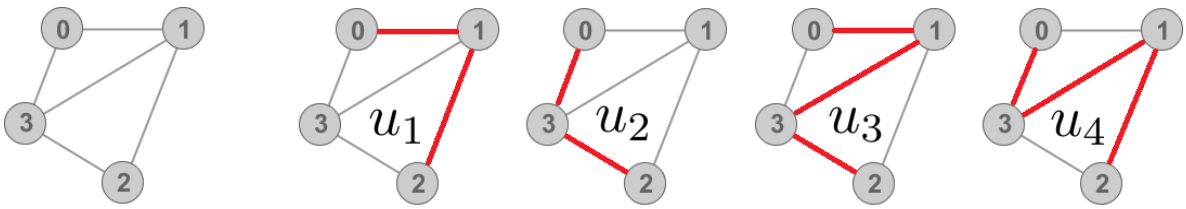

Figure 17 – *The network K_4 with all the paths between agent 0 and agent 2.*

Also more general results can be derived by using proposition 4.4. For instance in a ring network, $D_{\mu,\nu}$ is readily computed as there are only two paths between any two nodes.

Proposition 4.5. *In a ring network on n nodes, $D_{\mu,\nu} = p^{dist(\mu,\nu)} + p^{n-dist(\mu,\nu)} - p^n$.*

Proof. Let u_1 and u_2 be the two - disjoint - paths between agent μ and agent ν. Note that the number of edges in the shortest path is equal to the distance between ν and μ, while the number of edges in the longest path is equal to $n - \text{dist}(\mu, \nu)$. By applying proposition 4.4 the results follows. □

4.2.2 Exact probabilities in a complete network

Proposition 4.4 is not easily applied to networks with multiple paths between two nodes. To give an indication that the number of paths may be very large, in K_{10} there are 109,601 distinct paths between two arbitrary nodes[22]. Clearly another method is required to compute $D_{\mu,\nu}$ in a complete network. Proposition 4.7 provides such method. The method is based on the following result[23].

22. In K_n, the number of paths between any two nodes can be computed by the recursive relation, $p(n) = 1 + (n-2)p(n-1)$, where $p(n)$ are the number of paths between any two nodes in K_n and $p(2) = 1$.
23. The result in proposition 4.6 - without proof - is found at slide 4 in: 'http://keithbriggs.info/documents/connectivity-Manchester2004Nov19.pdf'

Proposition 4.6. *Let $\mathcal{T}_n$ be the transmission network of K_n, the complete network on n nodes. Then, for any p*

$$\Pr\{\mathcal{T}_n \textit{ is connected}\} = 1 - \sum_{i=1}^{n-1} \binom{n-1}{i-1} (1-p)^{i(n-i)} \Pr\{\mathcal{T}_i \textit{ is connected}\}, \tag{4.3}$$

with $\Pr\{\mathcal{T}_1 \textit{ is connected}\} = 1$.

Proof. Define $C_n(\nu)$ as the component in which ν lies in the transmission network T_n. Definitely the event that T_n is connected is equivalent with the event that all nodes lie in the component in which ν lies. Consequently,

$$\begin{aligned}\Pr\{\mathcal{T}_n \text{ is connected }\} &= \Pr\{|C_n(\nu)| = n\} \\ &= 1 - \sum_{i=1}^{n-1} \Pr\{|C_n(\nu)| = i\},\end{aligned}$$

where $|C_n(\nu)|$ is the number of nodes in $C_n(\nu)$. Next we will show that

$$\Pr\{|C_n(\nu)| = i\} = \binom{n-1}{i-1} (1-p)^{i(n-i)} \Pr\{|C_i(\nu)| = i\}, \tag{4.4}$$

completing the proof. For this, let $\mathcal{V}_i \subset V$ be all the subsets of size i of V that include node ν. Recognize that there are $\binom{n-1}{i-1}$ elements in $\mathcal{V}_i$. Next, by conditioning on all $\tilde{V} \in \mathcal{V}_i$,

$$\Pr\{|C_n(\nu)| = i\} = \sum_{\tilde{V} \in \mathcal{V}_i} \Pr\{C_n(\nu) = \{\nu\} \cup \tilde{V}\}.$$

As each edge is included independently in $\mathcal{T}_i$

$$\begin{aligned}&\sum_{\tilde{V} \in \mathcal{V}_i} \Pr\{C_n(\nu) = \{\nu\} \cup \tilde{V}\} \\ &\quad = \sum_{\tilde{V} \in \mathcal{V}_i} \Pr\{\ \{\nu\} \cup \tilde{V} \text{ is connected }\} \Pr\{\text{ no edge between } (\{\nu\} \cup \tilde{V}) \text{ and } (V \setminus (\{\nu\} \cup \tilde{V}))\ \} \\ &\quad = \sum_{\tilde{V} \in \mathcal{V}_i} \Pr\{|C_i(\nu) = i|\} \Pr\{\text{ no edge between } (\{\nu\} \cup \tilde{V}) \text{ and } (V \setminus (\{\nu\} \cup \tilde{V}))\ \} \\ &\quad = \sum_{\tilde{V} \in \mathcal{V}_i} \Pr\{|C_i(\nu) = i|\}(1-p)^{i(n-i)} = \binom{n-1}{i-1} (1-p)^{i(n-i)} \Pr\{|C_i(\nu) = i|\}.\end{aligned}$$

In this derivation the second equality follows because - in a complete network - the probability that $\nu \cup \tilde{V}$ is connected is independent of the nodes in $\tilde{V}$. The third equality follows because there are $i(n-i)$ edges between $(\{\nu\} \cup \tilde{V})$ and $(V \setminus (\{\nu\} \cup \tilde{V}))$, all included with probability p. □

The probability that the transmission network of a complete network is connected can be linked to $D_{\mu,\nu}$. The next proposition presents a method.

Proposition 4.7. *In a complete network on n nodes, for every p and all $\mu \neq \nu$*

$$D_{\mu,\nu} = \sum_{i=2}^{n} \binom{n-2}{i-2} (1-p)^{i(n-i)} \Pr\{\mathcal{T}_i \textit{ is connected}\}, \tag{4.5}$$

where $\Pr\{\mathcal{T}_i$ is connected$\}$ is given in (4.3).

Proof. By conditioning on the size of the component in which ν lies

$$\begin{aligned} D_{\mu,\nu} &= \Pr\{\nu \sim \mu \text{ in } \mathcal{T}\} \\ &= \sum_{i=1}^{n} \Pr\{\nu \sim \mu \text{ in } \mathcal{T} \mid |C_n(\nu)| = i\} \Pr\{|C_n(\nu)| = i\} \;=\; \sum_{i=1}^{n} \frac{i-1}{n-1} \Pr\{|C_n(\nu)| = i\}, \end{aligned}$$

where the second equality follows because every node - in the transmission network of a complete network - equally likely is in $C_n(\nu)$. By using (4.4) in proposition 4.6, the result follows. □

The following example helps to elucidate the result.

Example 4.3. When $x_i = \Pr\{\mathcal{T}_i \text{ is connected }\}$, by equation (4.3):

$$\begin{aligned} &x_1 = 1, \\ &x_2 = 1 - (1-p)x_1 = p \text{ and} \\ &x_3 = 1 - (1-p)^2 x_1 - 2(1-p)^2 x_2 = 1 - (1-p)^2 - 2(1-p)^2 p = 3p^2 - 2p^3. \end{aligned}$$

Consequently by using (4.5):

$$\begin{aligned} &D_{1,2}^{K_2} = x_2 = p \text{ and} \\ &D_{1,2}^{K_2} = x_2(1-p)^2 + x_3 = p(1-p)^2 + 3p^2 - 2p^3 = p + p^2 - p^3. \end{aligned}$$

This result agrees with the result derived in figure 15.

As a final comment, recognize that $D_{\mu,\nu}$ is independent of μ and ν in a complete network.

4.2.3 Comparing several networks

Proposition 4.1, proposition 4.4 and the exact results in a complete and a ring network are the tools used in this research to compute $D_{\mu,\nu}$ for arbitrary networks. As the focus lies on the security game, this probability is not further explored in this chapter. Nevertheless, the following proposition provides some grasp on this value.

Proposition 4.8. *Let $\mathcal{H}$ be a subgraph of $\mathcal{G}$, then for any ν and μ, $D_{\mu,\nu}^{\mathcal{H}} \leq D_{\mu,\nu}^{\mathcal{G}}$. Moreover, for any network in which μ and ν are connected, $D_{\mu,\nu}$ is strictly increasing in p.*

Proof. Surely, all paths between μ and ν in $\mathcal{H}$ also exist in $\mathcal{G}$. Consequently the result follows by noting that

$$D_{\mu,\nu}^{\mathcal{H}} = \Pr\{\bigcup_{i=1}^{n} \Big[\, \mathcal{H}[u_i^*] \subset \mathcal{T} \,\Big]\} = \Pr\{\bigcup_{i=1}^{n} \Big[\, \mathcal{G}[u_i^*] \subset \mathcal{T} \,\Big]\} \leq \Pr\{\bigcup_{i=1}^{m} \Big[\, \mathcal{G}[u_i^*] \subset \mathcal{T} \,\Big]\} = D_{\mu,\nu}^{\mathcal{G}},$$

where $u_1^*, \ldots, u_n^*$ are the paths between μ and ν in $\mathcal{H}$ and $u_{n+1}^*, \ldots, u_m^*$ the paths between μ and ν in $\mathcal{G}$.

Next, when p is increasing, the probability that any path u_i^* in particular is still present in $\mathcal{T}$ is strictly increasing. Consequently it can not be the case that $D_{\mu,\nu} = \Pr\{\bigcup_{i=1}^{n} \mathcal{G}[u_i] \subset \mathcal{T}\}$ is decreasing. □

Proposition 4.8 has an intuitive motivation, when dependencies grow between agents, in the form of more connections or a higher value of p, information is shared with a higher probability. This property can be used to find bounds on $D_{\mu,\nu}$. For instance, in any network $\mathcal{G}$ on n nodes, $D_{\mu,\nu}^{\mathcal{G}}$ is bounded above by $D_{\mu,\nu}^{K_n}$ in a complete network. The following example further demonstrates the result in proposition 4.8 and shows - in some simple networks - the effects of adding an edge to the network.

Example 4.4. In this example we compute and compare the probability that agent 2 obtains d_0 in the networks showed in figure 18. First $D_{0,2}^{\mathcal{G}_1}$ and $D_{0,2}^{\mathcal{G}_4}$ are computed by applying - respectively - proposition 4.7 and proposition 4.5. Next note that $D_{0,2}^{\mathcal{G}_3}$ and $D_{0,2}^{\mathcal{G}_4}$ can be computed from

$$D_{0,2}^{\mathcal{G}_3} = p + (1-p) D_{0,2}^{\mathcal{G}_4} \text{ and } D_{0,2}^{\mathcal{G}_1} = p + (1-p) D_{0,2}^{\mathcal{G}_2};$$

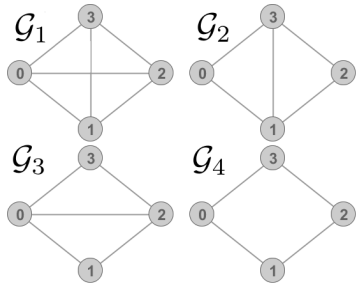

Figure 18 – *Several networks on 4 nodes.*

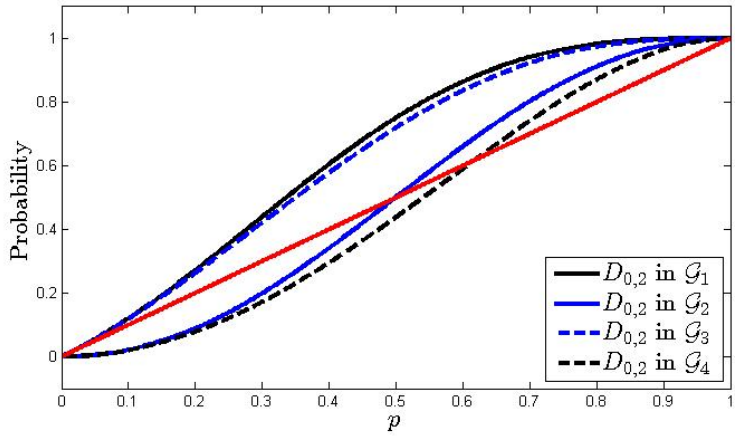

Figure 19 – *Probability that agent 2 obtains d_0 for the networks showed in figure 18.*

two expressions that follow from proposition 4.1 when deleting, in both cases, $(0, 2)$. The results are plotted in figure 19.

Several characteristics are noticeable in figure 19. First observe that, as stated in proposition 4.8, $D_{0,2}$ is strictly increasing in p and in the number of edges. Not every edge has the same impact though. For instance, the impact of removing $(1, 3)$ in a full graph is negligible as the plots of $D_{0,2}^{\mathcal{G}_1}$ and $D_{0,2}^{\mathcal{G}_3}$ are quite similar. This shows that by increasing the number of edges, the probability that information is shared does not necessarily increase significantly.

Another noticeable feature in figure 19 is that - for small p - the probability that agent 2 obtains d_0 in network $\mathcal{G}_2$ and network $\mathcal{G}_4$ is lower than in a two agent network with agent 0 and agent 2 (solid red line is above solid blue and dashed black). As a network with two agents is neither a subgraph of $\mathcal{G}_2$ or $\mathcal{G}_4$, this confirms that proposition 4.8 only holds if one graph is a subgraph of the other. In fact, $\mathcal{G}_1$ and $\mathcal{G}_3$ are super-graphs of a two agent network with agent 0 and agent 2 and hence it follows indeed that $D_{0,2}^{\mathcal{G}_1}$ and $D_{0,2}^{\mathcal{G}_3}$ are larger than the solid red line in figure 19.

4.3 Expected number of documents obtained

In our model we assume that every agent will store his own document and the documents obtained by other agents. In this section we focus on the *expected* number of documents stored at an agent. This stochastic variable - denoted by D_ν for agent ν - depends on p and the network structure. Remind that the attacker, if his attack on an agent is successful, will steal - in expectation - this quantity of documents.

4.3.1 How to compute D_ν?

When $D_{\mu,\nu}$ is known for all μ, then also D_ν can be computed. This follows because

$$\begin{aligned} D_\nu &= \mathbb{E}(\text{ documents obtained by agent } \nu) \\ &= \sum_{\mu \in V} \mathbb{E}(\alpha_{\mu,\nu}) = \sum_{\mu \in V} \Pr\{\alpha_{\mu,\nu} = 1\} = \sum_{\mu \in V} D_{\mu,\nu}, \end{aligned} \tag{4.6}$$

where $\alpha_{\mu,\nu}$ is the event that agent ν obtains d_μ. The third equality in (4.6) follows because $\alpha_{\mu,\nu}$ is a Bernoulli random variable[24].

24. Note that D_ν is not equivalent with the expected size of the (random)-component in which ν lies in the transmission network (as used often in random graph theory). This follows because in our model the n documents spread independently of each other and hence n transmission networks are formed.

Note that the dependency on $D_{\mu,\nu}$ allows to extend properties of $D_{\mu,\nu}$ to D_ν. For instance proposition 4.8 can be extended.

Proposition 4.9. *Let $\mathcal{H}$ be a subgraph of $\mathcal{G}$, then for all $\nu \in V(\mathcal{H})$, $D_\nu^{\mathcal{H}} \leq D_\nu^{\mathcal{G}}$. Moreover, for any network in which degree$(\nu) > 0$, D_ν is strictly increasing in p.*

The result follows easily by combining (4.6) with the results in proposition 4.8.

The dependency of D_ν on $D_{\mu,\nu}$ additionally allows to compute D_ν in specific networks. For instance in a ring and a complete network the following results hold.

Proposition 4.10. *In a ring network on n nodes, if $p < 1$*

$$D_\nu = \frac{1 + p - p^n(1+n) + p^{n+1}(n-1)}{1-p}, \tag{4.7}$$

and if $p = 1$ then $D_\nu = n$. In a complete network on n nodes for every μ,

$$D_\nu = 1 + (n-1)D_{\mu,\nu}, \tag{4.8}$$

where $D_{\mu,\nu}$ follows from (4.5).

Proof. From proposition 4.5, in a ring network $D_\nu = 1+2\sum_{i=1}^{n} p^i - (n-1)p^n$. By observing the geometric series, this expression can be written to the result in the proposition. The result in a complete network follows by the earlier observation that $D_{\mu,\nu}$ is identical for every choice of ν and $\mu \neq \nu$. □

Figure 20 shows D_ν as function of p for a complete and a ring network for several values of n. Observe for instance that D_ν is increasing in p and in n. Additionally observe that $D_\nu^{K_n}$ much faster touches n than $D_\nu^{R_n}$. Surely this follows because a document can spread over way more paths in the complete network.

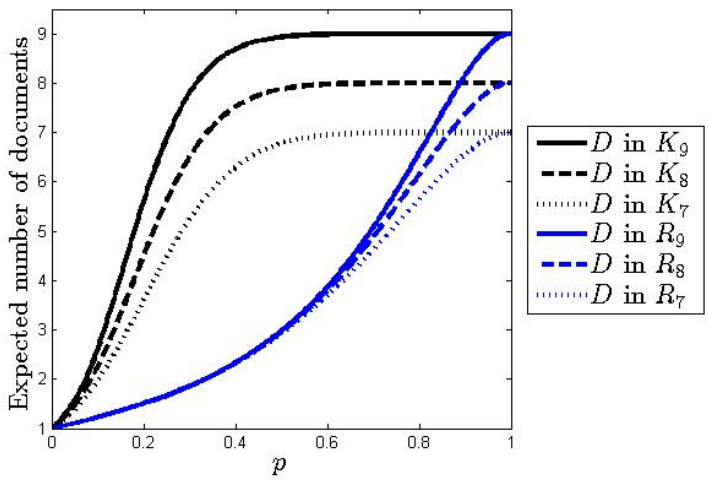

Figure 20 – *Expected number of documents D obtained by each agent in a complete network K and a ring network R. Note that D is both increasing in p and in the density of the network.*

Also note that D_ν is independent of ν in both a complete network and a ring network. Apparently every agent obtains as much documents - in expectation and for every value of p - as every other agent. This property, present in several networks, is highly used in this research and allows to compute security investments more efficiently. In the sequel of this section, if D_ν is identical for every ν, D_ν is shortened[25] to D. In the next section we define a class of networks for which this is the case.

25. To recapitulate, $D_\nu^{\mathcal{G}}$ are the expected number of documents obtained by agent ν in network $\mathcal{G}$. When there is no ambiguity this expression is shortened to D_ν and even further shortened to D when D_ν is identical for every ν.

4.3.2 Vertex-transitive networks and circulant networks

In this section we first define vertex-transitive (VT) networks. For this class of networks D_ν shows to be identical for every ν. Additionally we specify a subclass of VT-networks: circulant networks. We prove that D_ν in circulant network can be bounded below and bounded above by respectively a ring and a complete network.

Vertex-transitivity is related to automorphisms. An automorphism is a mapping from a graph to itself (a permutation) while preserving the edge-vertex connectivity. Formally, an automorphism is a permutation ϕ of the vertex set V, such that if and only if ν and μ are neighbors then $\phi(\nu)$ and $\phi(\mu)$ are neighbors. One can define a set of all such permutations.

Definition 1. The automorphism group is the group $Aut(\mathcal{G})$ such that

$$Aut(\mathcal{G}) = \{\phi : V \to V \mid \forall \nu, \mu \in V \; A(\nu, \mu) = A_\phi(\phi(\nu), \phi(\mu))\}, .$$

where A_ϕ is the adjacency matrix of the image of ϕ.

One can prove that $Aut(\mathcal{G})$ satisfies the group axioms: closure, associativity and an identity and inverse exist in $Aut(\mathcal{G})$. Moreover note that because the structure of the network is unchanged under an automorphism, also A - the adjacency matrix - is unchanged under an automorphism (i.e. $A \equiv A_\phi$).

Vertex-transitivity is closely related to $Aut(\mathcal{G})$ as the following definition shows.

Definition 2. A network $\mathcal{G}$ is vertex-transitive if and only if for all $\nu, \mu \in V$ there is a $\phi^* \in Aut(\mathcal{G})$ such that $\phi^*(\nu) = \mu$.

In other words, a network is vertex-transitive if for every two nodes, there exists an automorphism that maps one of these nodes on the other node while the structure of the network is preserved. Informally stated, a VT-network is one that 'looks the same' at every vertex, such as a cube, tori or complete graph.

Vertex-transitivity is a stronger requirement than regularity of a graph as it can be proved that every VT-network is regular but, on the other side, not every regular graph is vertex-transitive.

Figure 21 shows some examples of regular graphs. The first (left) and the middle graph are both vertex-transitive as - informally - the network looks the same at every node. For the last (right) network this is much harder to see. In fact, although the graph is regular, it is not vertex-transitive[26].

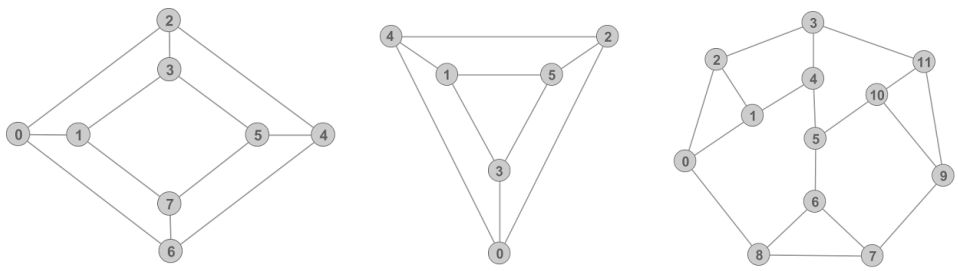

Figure 21 – *Several regular networks. The first two (from the left) are VT-networks while the last network is not.*

When two identical VT-network are combined, the result is still a VT-network as the following proposition shows.

Proposition 4.11. *If $\mathcal{G} = \mathcal{G}_1 \cup \mathcal{G}_2$ is the union of two identical networks which are both vertex-transitive, then $\mathcal{G}$ is also vertex-transitive.*

26. This follows because not every node is part of a clique of three nodes. A clique is a subgraph induced by a set $B \subseteq V(A)$ such that $A[B]$ is fully connected. For instance $S = \{0, 1, 2\}$ is a clique on three nodes. Observe that node 3 is not part of a clique of three node and hence a mapping such that (for instance) $\phi^*(2) = 3$ can never be in $Aut(\mathcal{G})$.

Proof. Label the vertices in $\mathcal{G}$ as $V(\mathcal{G}) = \{1^{\mathcal{G}_1}, .., n^{\mathcal{G}_1}, 1^{\mathcal{G}_2}, .., n^{\mathcal{G}_2}\}$. To prove the first statement, first note that when mapping $\nu^{\mathcal{G}_i}$ on $\mu^{\mathcal{G}_i}$, then there clearly exists (by vertex-transitivity of both networks) a $\phi_1 \in Aut(\mathcal{G}_1) \times Aut(\mathcal{G}_2)$ such that $\phi_1(\nu^{\mathcal{G}_i}) = \mu^{\mathcal{G}_i}$. Second, when mapping $\nu^{\mathcal{G}_i}$ on $\nu^{\mathcal{G}_j}$, there exists a $\phi_2 \in Aut(\mathcal{G})$ such that $\phi^*(\nu^{\mathcal{G}_1}) = \nu^{\mathcal{G}_2}$ and $\phi^*(\nu^{\mathcal{G}_2}) = \nu^{\mathcal{G}_1}$ for all $\nu = 1, 2, ..n$. The result follows by noting that $\phi_2(\phi_1) \in Aut(\mathcal{G})$ because $Aut(\mathcal{G})$ is a group. □

The results in the proposition shows to be useful when an extension of the security game is considered in chapter 6. In this extension the attacker can (strategically) choose which network to attack.

As already stated, in vertex transitive networks D_ν is independent of ν. As the network seen from every agent is identical in a VT-network, the result is intuitive. In the following proposition we prove this mathematically.

Proposition 4.12. *In a vertex-transitive network $\mathcal{G}$, $D_\nu \equiv D_\mu$ for every $\nu, \mu \in V$.*

Proof. In this proof we show that $\sum_\kappa D_{\kappa,\nu} = \sum_\kappa D_{\kappa,\mu}$ in VT-networks. For this let $\phi^* \in Aut(\mathcal{G})$ such that $\phi^*(\nu) = \mu$ and denote the network $\mathcal{G}$ after this automorphism as $\mathcal{G}_\phi$. It follows that

$$\sum_{\kappa \in V(\mathcal{G})} D_{\kappa,\nu} = \sum_{\phi^*(\kappa) \in V(\mathcal{G}_{\phi^*})} D_{\phi^*(\kappa),\nu}.$$

By noting that $V(\mathcal{G})$ and $V(\mathcal{G}_{\phi^*})$ are the same sets, the result follows. □

Although the proposition above allows to conclude that D_ν is independent of ν in VT-networks, it does not say anything about the exact value of D. As the practitioner can compute D by earlier tools and using equation (4.6), we continue by finding bounds on D; other than (by definition) the lower bound of 1 and the upper bound of n.

First note for instance that D is clearly bounded above by D in a complete network by proposition 4.9. To find a (more strict) lower-bound, we first define a special class of networks.

Definition 3. A network $\mathcal{G}_n$ is said to be a circulant network on n nodes with structure $S \subset V$ if and only if for all $\nu, \mu \in V$ for which $(\nu - \mu) \mod (n) \in \mathcal{S}$ it holds that $A(\mu, \nu) = A(\nu, \mu) = 1$.

For instance, when $\mathcal{S} = \{1\}$ (or $\mathcal{S} = \{n-1\}$), the circulant graph is a ring network and if $\mathcal{S} = V$ (or $\mathcal{S} = \{1, \ldots, \lfloor \frac{n}{2} \rfloor\}$), the circulant graph is a complete network. Figure 22 shows three circulant networks with $\mathcal{S} = \{1, 2\}$.

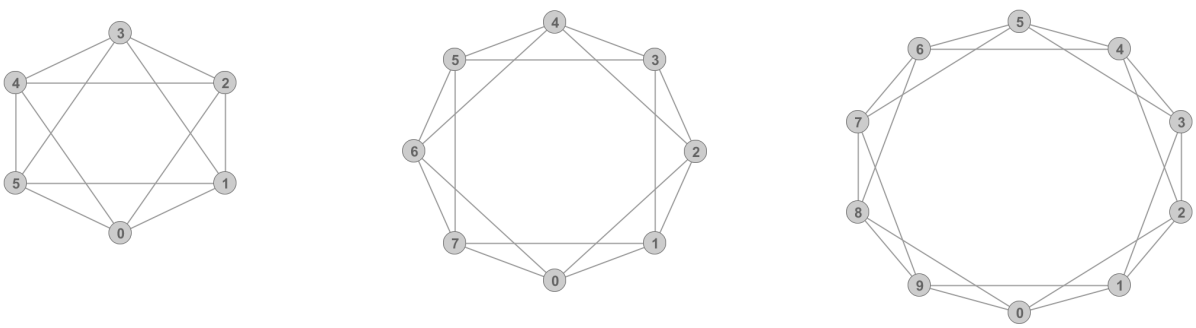

Figure 22 – *Circulant networks with structure $\mathcal{S} = \{1, 2\}$ on 6, 8 and 10 nodes.*

Although one easily observes that the networks in figure 22 are circulant, it is not always easy to conclude that a network is circulant. For instance the first network in figure 21 is not circulant (as shown by Leighton, 1982), while the middle network is circulant (with structure $\mathcal{S} = \{2, 3, 4\}$).

One can prove that all circulant networks are vertex-transitive[27]. Indeed the networks in figure 22 and the middle network in figure 21 are vertex-transitive. Note however that the first network in figure 21 is vertex-transitive but not circulant and hence not all VT-networks are circulant.

The expected number of documents obtained in a circulant network can be bounded by D in a larger circulant network. This property is showed in the next proposition.

Proposition 4.13. *Let $\mathcal{H}$ and $\mathcal{G}$ be two circulant networks; both with n nodes and respectively with structure $\mathcal{S}_{\mathcal{H}} \subset \mathcal{S}_{\mathcal{G}}$. It holds that $D^H \leq D^G$.*

Proof. The results is a corollary of proposition 4.9. As $\mathcal{S}_{\mathcal{H}} \subset \mathcal{S}_{\mathcal{G}}$, $\mathcal{H}$ is a subgraph of $\mathcal{G}$ and the result follows. □

Specifically the proposition allows to conclude that D in circulant network with structure $\mathcal{S} \supset \{1\}$ on n nodes always lies between D^{R_n} and D^{K_n} (D always lies between the black and the blue lines in figure 20). Circulant networks with structure $\mathcal{S} \supset \{1\}$ can be 'build' from a ring network by adding edges such that the lth order neighborhood in the ring becomes the first order neighborhood if and only if $l \in \mathcal{S}$. Hence any circulant network with structure $\mathcal{S} \supset \{1\}$ is a super-graph of the ring network.

4.3.3 Growing networks and asymptotics

Recognize from figure 20 that the expected number of documents obtained by agents in both a ring and a complete network are increasing in n. In this section we define what is meant with 'D is increasing in n' and (promptly) discuss some asymptotics. To highlight the dependency of D on n, the notation $D(n)$ is used in this section.

A network is growing in n when nodes are added to the network. To say something about the emerging network, we assume that the same 'structure' is maintained when nodes are added. This leads to the following definition.

Definition 4. The set $G = \{\mathcal{G}_i, \mathcal{G}_{i+1}, \ldots, \mathcal{G}_n\}$ is sequence of growing networks when $\mathcal{G}_j$ is a circulant network with structure $\mathcal{S}$ for all $i \leq j \leq n$.

As an example: R_5, R_6, R_7 is a sequence of growing ring networks and figure 22 shows a (part of the) sequence of growing networks with structure $\mathcal{S} = \{1, 2\}$. When $D(n)$ is increasing in n, we mean that $D^{\mathcal{G}_n} \leq D^{\mathcal{G}_{n+1}}$ where both $\mathcal{G}_n$ and $\mathcal{G}_{n+1}$ are from a sequence of growing networks.

We expect $D(n)$ to be strictly increasing in a ring and a complete network. For a ring network this result is not so trivial because $D_{\nu,\mu}$ is decreasing in n. This is showed in the next example.

Example 4.5. Consider two ring networks; one on 4 and one on 5 nodes. In both networks let agent 1 and agent 2 be two neighboring agents. Note that $D^{R_4}_{1,2} = p + p^3 - p^4$ and $D^{R_5}_{1,2} = p + p^4 - p^5$. It follows that $D^{R_4}_{1,2} > D^{R_5}_{1,2}$ for $0 < p < 1$. Also note that (from proposition 4.10)

$$D(4) = \frac{1 + p - 5p^4 + 3p^5}{1 - p} \quad \text{and} \quad D(5) = \frac{1 + p - 6p^5 + 4p^6}{1 - p}.$$

As $-5p^4 + 3p^5 < -6p^5 + 4p^6$ for $0 < p < 1$, it follows that $D(5) > D(4)$. So while the probability that agent 2 obtains d_0 is decreasing in n, the expected number of documents obtained by agent 2 is increasing in n.

Next we formally prove that $D(n)$ is strictly increasing in a complete and a ring network.

Proposition 4.14. *The expected number of documents obtained by each agent in a ring and in a complete network is strictly increasing in the number of agents when $p > 0$.*

27. To prove this, we show that there always exists a $\phi \in Aut(\mathcal{G})$ such that $\phi(\nu) = \mu$ for two arbitrary nodes ν and μ. Specifically, define $\phi(\nu)$ as $\nu + k \mod (n)$ where k is such that $\nu + k \mod (n) = \mu$. Next, if (κ_1, κ_2) is an edge, then clearly $(\phi(\kappa_1), \phi(\kappa_2)) = (\kappa_1 + k, \kappa_2 + k)$ is an edge because $(\kappa_1 + k) - (\kappa_2 + k) = \kappa_1 - \kappa_2$.

Proof. To show that $D(n)$ is strictly increasing in a ring network (for $0 < p < 1$), the derivative of (4.7) to n can be computed. This leads to

$$\frac{dD}{dn} = \frac{-\ln(p)p^n(1+n) - p^n + \ln(p)p^{n+1}(n-1) + p^{n+1}}{1-p}.$$

Note that the denominator is always strictly larger than 0 for $p < 1$. As the numerator is also strictly larger than 0 for $p > 0$[28], it follows that $D(n)$ is strictly increasing in n when $0 < p < 1$. When $p = 1$ then $D(n) = n$ and D is definitely increasing in n.

For a complete network the result is trivial as $D = 1+(n-1)D_{\nu,\mu}$ for every $\mu \neq \nu$. As a complete network on n nodes is a super-graph of a complete network on $n-1$ nodes, $D_{\nu,\mu}$ is increasing by proposition 4.8. Consequently, as $D(n+1) = 1 + nD_{\nu,\mu}^{K_{n+1}} > 1 + (n-1)D_{\nu,\mu}^{K_{n+1}} \geq 1 + (n-1)D_{\nu,\mu}^{K_n} = D(n)$, $D(n)$ is indeed strictly increasing in n. □

In fact one can prove that $D(n) \to \frac{1+p}{1-p}$ when $n \to \infty$ in a ring network. In a complete network $D(n)$ is a divergent series as $D(n) \to \infty$.

Although simulation results in appendix section B conjecture that $D(n)$ is increasing in n for a wide range of circulant networks, it is hard to prove this formally. We leave this conjecture as an open problem in this research.

Another open problem is whether or not $D(n)$ converges. Simulation results lead to the presumption that $D(n)$ converges when $\mathcal{S}$ is independent of n (e.g. a ring). Contrary, when $\mathcal{S}$ depends on n, different behavior is observed. Specifically, when $\mathcal{S}$ increases 'significantly' (e.g. in a complete network) we feel that $D(n)$ diverges. On the other side, when $\mathcal{S}$ does not increase significantly then $D(n)$ might as well converge. We do not further explore these surmises in this research as the focus lies on the security game.

Asymptotic behavior of $D(n)/n$.
Also the asymptotic behavior of $D(n)/n$, the expected fraction of documents obtained by an agent is of interest in this research. In a ring the following result holds.

Proposition 4.15. *In a ring network, for all $p < 1$*

$$\lim_{n\to\infty} \frac{D(n)}{n} = 0.$$

Proof. For a ring network $D(n)$ is given in (4.7). As $D_\nu \to 1+p/1-p$ when $n \to \infty$, the result follows. □

The following proposition shows that different behavior is observed in a complete network.

Proposition 4.16. *In a complete network, for all $p > 0$*

$$\lim_{n\to\infty} \frac{D(n)}{n} = 1.$$

Proof. The proof is based on showing that a Poisson-random graph, in which the number of agents is asymptotically large and $p > 0$ fixed, is almost surely connected. More formally and in the notation of proposition 4.6, we would like to show that $\Pr\{\mathcal{T}_n \text{ is connected }\} \to 1$. This would imply that $D_{\nu,\mu} \to 1$ (by proposition 4.5) and hence $D/n = [1 + (n-1)D_{\mu,\nu}]/n] \to 1$.

To show that $\Pr\{\mathcal{T}_n \text{ is connected }\} \to 1$, let x_n be the probability that the transmission network of a complete network on n nodes is connected and take $p > 0$ fixed. From proposition 4.6, x_n is iteratively

28. This follows because the numerator can be written as $p^n[\ln(p)[p(n-1) - (n+1)] + p - 1]$. This expression is strictly larger than 0 for $p > 0$ because $p(n-1) - (1+n) < 0 < \frac{p-1}{ln(p)}$.

computed with (4.3). Note that

$$0 \;\leq\; \sum_{i=1}^{n-1} \binom{n-1}{i-1} (1-p)^{i(n-i)}\, x_i \;\leq\; \sum_{i=1}^{n-1} \binom{n-1}{i-1} (1-p)^{i(n-i)}$$
$$\leq \sum_{i=1}^{n-1} \binom{n-1}{i-1} (1-p)^{i-1} \;=\; (1-p)^{n-1} - (n-1)(1-p)^{n-2} \xrightarrow{n\to\infty} 0.$$

The second inequality follows because $0 \leq x_i \leq 1$ by definition. The third inequality is correct because $i(n-i) = in - i^2 \geq i(i+1) - i^2 = i > i-1$, where the second equality follows because $i \leq n-1$. The third inequality follows from the binomial theorem. By inspection of (4.3) we conclude that $x_n \to 1$. □

Again it is hard to say what the asymptotic behavior of $D(n)/n$ is in other circulant networks. In appendix section B some simulation results are given. The results conjecture that $D(n)/n$ converges to zero when we consider circulant networks where $\mathcal{S}$ is independent of n. When $\mathcal{S}$ depends on n different behavior is observed. Overall we conjecture that $D(n)/n$ converges to one when the structure increases 'significantly' with n (e.g. in a complete network). Similar as for $D(n)$, we do not fully explore the behavior of $D(n)/n$ in circulant networks and leave the conjectures as open problems.

5 The security game under a strategic attack

In this chapter we analyze the security game. Main focus lies on finding the pure strategy Nash equilibrium and the social optimum as function of the network structure and p. First an extensive example is given in section 5.1 to elucidate the model and to give a preview of some results. Next in section 5.3, after some preliminaries in section 5.2, the focus lies on the random attack. Results are used as benchmark in subsequent sections on the strategic attack. This analysis is started in section 5.4 where the strategy of the attacker is uncovered. Next in section 5.5 and in section 5.6 the security game is analyzed in respectively a non-cooperative environment and in a cooperative environment. Lastly, we compare results in section 5.7 and analyze the role of certain parameters in section 5.8.

5.1 The two-agent case

Suppose two agents - agent 1 and agent 2 - play the security game. We assume that the cost to adopt security is $(1/2)q_\nu^2$. Consequently, the utility of each agent is reduced to

$$\Pi_\nu = 1 - a_\nu(\mathbf{q})[1 - q_\nu] - a_{-\nu}(\mathbf{q})[1 - q_{-\nu}]p - \frac{1}{2}q_\nu^2. \tag{5.1}$$

Figure 23 shows the network and highlights how certain parameters relate to each other.

When considering a random attack in which $a_1 = a_2 \equiv 1/2$, an agent's best response is independent of the strategy of the other agent. This can be seen by noting that the external effect on an agent's utility, $a_\nu[1 - q_{-\nu}]p$, is independent of an agent's own strategy. Consequently, although the security investments of the other agent impacts an agent's utility, the best response is independent of this investment.

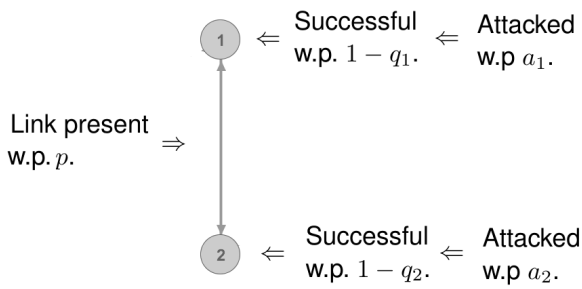

Figure 23 – *Two interconnected agents who play the security game. In this figure p is the probability that the link between 1 and 2 is present in the transmission network. Every agent is attacked with probability a_ν, an attack which is successful with probability $1 - q_\nu$. If an attack is successful the attacker will steal all the documents stored at an agent. This is necessarily the target's own document and, with probability p, the document of the other agent.*

The best response of each agent can be found by maximizing the utility function when $q_{-\nu}$ is given. Later we show that this best response under the random attack is such that $c'(q_\nu) = 1/n$. Under the current assumption on investment costs, a fixed point of the best responses of agent 1 and agent 2 is

$$\mathbf{q}^N = \{\frac{1}{2}\ ,\ \frac{1}{2}\}. \tag{5.2}$$

A fixed point of the best responses is a pure strategy Nash equilibrium of the game.

Differently, the social optimum can be found by maximizing $S = \Pi_1 + \Pi_2$ in $[0, 1]^2$. It can be showed that

$$\mathbf{q}^s = \{\frac{1}{2} + \frac{p}{2}\ ,\ \frac{1}{2} + \frac{p}{2}\} \tag{5.3}$$

is the unique social optimum. Observe that (for each p) q^N features under-investments relative to q^s.

The random attack is used as a benchmark for the strategic attack. In this strategic attack $\mathbf{a}$ is chosen such that the utility of the attacker,

$$\Pi_a = a_1(1 - q_1)(1 + p) + a_2(1 - q_2)(1 + p) - \psi(a_1) - \psi(a_2)$$

is maximized, subject to $a_1 + a_2 = 1$, $a_1 \geq 0$ and $a_2 \geq 0$. One can show that when $\psi = a^2$ and $p = 0.5$, the strategy of the attacker is uniquely described with

$$a_1(\mathbf{q}) = \frac{3}{8}q_2 - \frac{3}{8}q_1 + \frac{1}{2} \text{ and (surely) } a_2(\mathbf{q}) = 1 - a_1(\mathbf{q}). \tag{5.4}$$

Note for instance that if $q_1 = q_2$ then $a_1 = a_2 = 1/2$. Also observe that a_1 is decreasing in q_1 (i.e. an agent can discourage an attack by increasing investments).

Remind that in the security game agents choose their strategy *anticipating* the strategy of the attacker. This is modeled by substituting (5.4) in an agent's utility in (5.1). This procedure leads to

$$\Pi_\nu = \frac{11}{16}q_\nu + \frac{1}{16}q_{-\nu} + \frac{9}{16}q_\nu q_{-\nu} - \frac{7}{8}q_\nu^2 - \frac{3}{16}q_{-\nu}^2 + \frac{1}{4}. \tag{5.5}$$

This function is plotted for both agents in figure 24. Observe that Π_ν is strictly concave in $\mathbf{q}$, a property which greatly simplifies the optimization process. By finding the first order condition for optimality (and checking that the solution is indeed the global maximum of (5.5)), one finds that the best response is $\varphi_\nu(q_{-\nu}) = (9/28)q_{-\nu} + (11/28)$. Figure 24 also features the utility at this best response for both agents. Note that there is a unique intersection of both lines: the utility at the Nash equilibrium. The exact location of this intersection can be found by solving the system of best responses:

$$\varphi_1(q_2) = \frac{9}{28}\varphi_2(q_1) + \frac{11}{28} \quad \text{and} \quad \varphi_2(q_1) = \frac{9}{28}\varphi_1(q_2) + \frac{11}{28}.$$

One can prove that

$$\mathbf{q}^N = \{\frac{11}{19}\ ,\ \frac{11}{19}\} \tag{5.6}$$

is the unique solution.

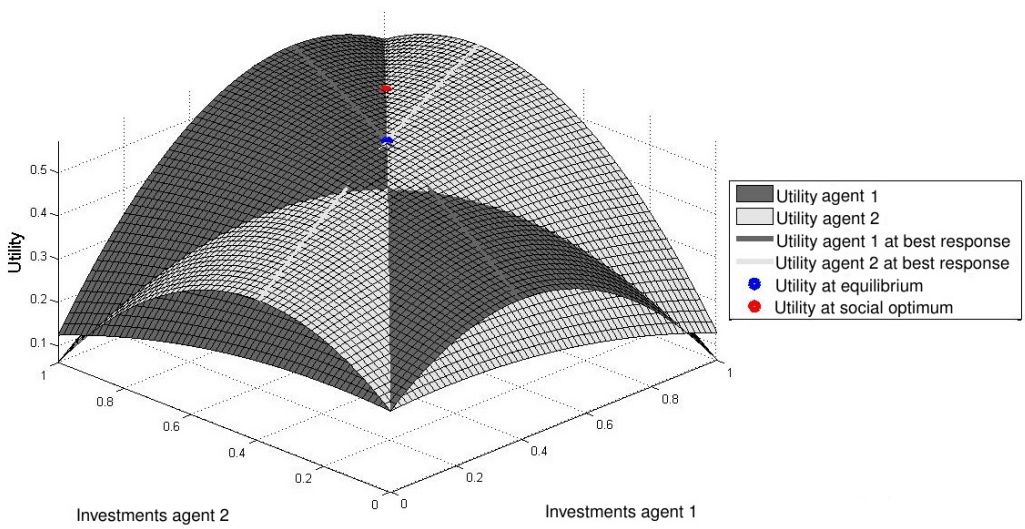

Figure 24 – *Plot of utility functions in (5.5) together with the utility when each agent plays his best response. The intersection of these lines is the utility at the Nash equilibrium (blue point). One can show that the red point is the utility at the social optimum. Note that under-investments prevail in equilibrium relative to social optimum.*

Note that the equilibrium investment level under the strategic attack, in (5.6), is larger than the investment level in the random attack in (5.2). Apparently an agent indeed uses the opportunity to discourage an attack by increasing investments. Unfortunately, as also other agents use this opportunity, still $a_\nu = 1/n$ and each agent is attacked with the same probability.

Yet, the increase of investments under the strategic attack makes the Nash equilibrium more socially optimal. This can be showed by first proving that the social optimum under the strategic attack is equivalent with the social optimum under the random attack. This indicates that by substituting $p = 0.5$ in (5.3), $\mathbf{q}^s = \{3/4\ ,\ 3/4\}$ under both the random and the strategic attack. Next the price of anarchy can be computed:

$$PoA_{\text{strategic attack}} = \frac{(1+p)(1-\frac{3}{4})}{(1+p)(1-\frac{11}{19})} = \frac{1/4}{9/19} = \frac{19}{36}$$

and

$$PoA_{\text{random attack}} = \frac{(1+p)(1-\frac{3}{4})}{(1+p)(1-\frac{1}{2})} = \frac{1}{2} = \frac{18}{36}.$$

As $PoA_{\text{random attack}} < PoA_{\text{strategic attack}} < 1$ we conclude that the outcome under the strategic attack is more social optimal.

Note however that although the investments in equilibrium are more socially optimal, still under-investments prevail when $p = 0.5$ because $\mathbf{q}^N = 11/19 < 3/4 = \mathbf{q}^s$. This can be different when p is changed. For instance when $p = 0.1$, the utility of each agent and the corresponding utility at the best response is showed in figure 25. Note that the Nash equilibrium features over-investments relative to the social optimum in this case.

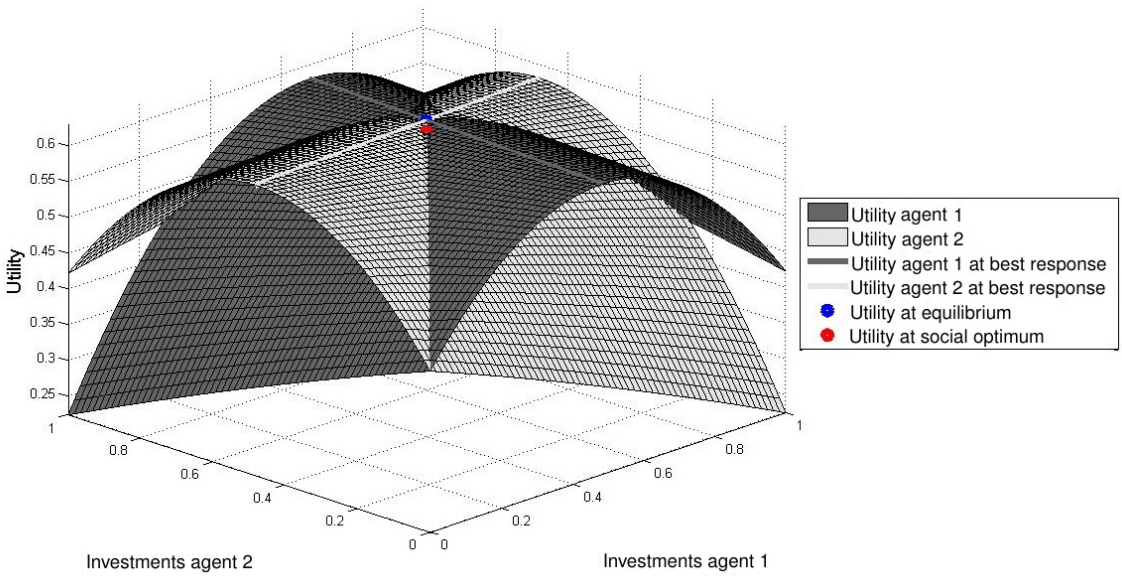

Figure 25 – *Plot of the utility of each agent when $p = 0.1$. Similar as in figure 24, again the blue point is the utility at the Nash equilibrium and the red point is the utility at the social optimum. Note that in this case over-investments prevail in equilibrium relative to social optimum.*

In this research - similar as in the example - the outcomes of the security game in a cooperative (social optimum) and a non-cooperative environment (Nash equilibrium) are compared. Differently, this is done for a much wider space of possible cost functions, values of p and network topologies.

5.2 Preliminaries to the security game

5.2.1 Assumption on investment cost

Throughout this research the following basic assumption on the security cost is adopted.

Assumption 1. (**Security cost**) The cost function $c : [0,1] \to \mathbb{R}^+$ is assumed to be two times continuously differentiable in $[0,1]$, to be strictly convex in $(0,1]$, strictly increasing in $(0,1]$ and to satisfy the boundary conditions $c(0) = 0$, $c'(0) = 0$, $c(1) \geq 1$ and $c'(1) \geq 1$.

The convexity assumption implies that marginal costs will increase when security investments are higher, which is a standard assumption in economic literature. The boundary assumptions are technical restrictions and generally make sure that solutions fall inside the interior of the strategy space.

5.2.2 Maximum of strictly concave function

The following result is highly used in this research. It formally shows that the first order condition for optimality of a strictly concave function - without a boundary maximum - has a unique solution. At this solution the function is globally maximized.

Proposition 5.1. *Let $f(\mathbf{q})$ be a twice differentiable function from $[0,1]^n$ to $\mathbb{R}$. If for every $\mathbf{q} \in [0,1]^n$ the Hessian $H(f(\mathbf{q})) < 0$ and $\nabla(f(\mathbf{q}))$ does not point outward I^n at the boundary, then there is a unique solution $\mathbf{q}^* \in I^n$ of $\nabla(f(\mathbf{q})) = 0$. Necessarily $f(\mathbf{q}^*)$ is the unique global maximum.*

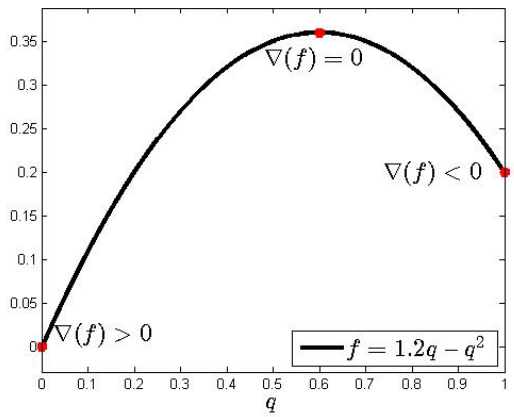

Figure 26 – *Illustration of the result in proposition 5.1.*

The results allows to conclude that a function attains his unique global maximum at the unique solution of the first order condition (FOC). This observation is showed in figure 26. Note that the function is strictly concave with $\nabla(f(0)) > 0$ and $\nabla(f(1)) < 0$. By using proposition 5.1 we conclude that there is a unique solution to the FOC and that f attains the global maximum at this solution.

5.2.3 Measure for expected damage

The variable $\mathbb{E}(\ |x|\ )$ is an important random variable in this research as this expectation is not only included in the social utility in (3.5), also the utility of the attacker in (3.7) features this variable. This is no surprise because informally $\mathbb{E}(\ |x|\ )$ can be seen as a measure of the (expected) damage done by an attack. Of course the attacker would like to maximize this quantity while cooperating agents (or some security planner/authority) would like to minimize this quantity. Formally $\mathbb{E}(\ |x|\ )$ can be written as

$$\begin{aligned}
\mathbb{E}(\ |x|\ ) = \sum_{\nu} x_\nu &= \sum_{\nu} \Pr\{x_\nu = 1\} \\
&= \sum_{\nu} \sum_{\mu} a_\mu (1 - q_\mu) D_{\nu,\mu} \\
&= \sum_{\mu} a_\mu (1 - q_\mu) \sum_{\nu} D_{\nu,\mu} \\
&= \sum_{\mu} a_\mu (1 - q_\mu) D_\mu .
\end{aligned}$$

In this derivation the second equality follows because x_ν is a Bernoulli random variable, the fourth equality- switching of summation sign - is allowed because there are a finite amount of agents and - lastly - the fifth equality follows because $D_{\nu,\mu} = D_{\mu,\nu}$ as the network is undirected.

5.3 Random attack as a benchmark

In this section we analyze the security game under the random attack. Remind that under this attack every agent is attacked with an exogenous probability. This models a situation where agents can not discourage an attack by increasing investments. In this case the adversary attacks according to non-modeled characteristics or just randomly. We normalize the probability that every agent is attack to $1/n$ for every agent. This allows to use the derivations in this section as a benchmark for results later in this report.

Under the random attack an agent's utility is reduced to

$$\Pi_\nu = 1 - \frac{1}{n}\sum_\mu (1-q_\mu)D_{\nu,\mu} - c(q_\nu).$$

An agent cannot control the external effect in his utility as this external effect ($\sum_{\mu\neq\nu}(1-q_\mu)D_{\nu,\mu}$) is independent of an agent's own strategy. So although this external effect alters an agent's well-being, a rational agent will not change his strategy due to this. The pure strategy Nash equilibrium takes a very comprehensive form when the investment cost satisfies assumption 1.

Proposition 5.2. *Under the random attack and under assumption 1, the unique Nash equilibrium level solves*

$$c'(q_\nu^N) = \frac{1}{n} \tag{5.7}$$

for each agent.

Proof. To find the best response of each agent, first note that

$$\frac{d\Pi_\nu}{dq_\nu} = \frac{1}{n} - c'(q_\nu).$$

Clearly the solution of (5.7) solves this FOC above. Uniqueness and existence of the solution follows from lemma A.1 on page 81. To prove that the solution is indeed an agent's best response (i.e. a maximum) note that

$$\frac{d^2\Pi_\nu}{dq_\nu^2} = -c''(q_\nu) < 0,$$

and that

$$\frac{d\Pi_\nu}{dq_\nu}(0, q_{-\nu}) = \frac{1}{n} \geq 0 \text{ and } \frac{d\Pi_\nu}{dq_\nu}(1, q_{-\nu}) = \frac{1}{n} - c'(1) \leq 0.$$

By combining these observations with proposition 5.1, it follows that (5.7) is the unique Nash equilibrium. □

As an agent cannot control the external risk that his document is lost through another agent, every rational agent will act accordingly and only protects against a direct loss. Many real world cases can be modeled this way; in particular in situations where the attack is not too involved. One can think of a Facebook identity theft (which may simply consist of sending - randomly - a friend request) or a hacker sending malware to randomly guessed email-addresses.

In a cooperative environment agent's agree that they also invest to protect documents of others. We assume that agents adopt a security investment such that

$$\begin{aligned} S = \sum_\nu \Pi_\nu &= n - \mathbb{E}(\,|x|\,) - \sum_\nu c(q_\nu) \\ &= n - \frac{1}{n}\sum_\mu [1-q_\mu]D_\mu - c(q_\mu) \end{aligned}$$

is maximized in $[0,1]^n$. Remind that the investment level for which S is maximized is denoted as the social optimum. By analyzing if S is strictly concave and $\nabla(S)$ does not point outward at the boundary, the next result can be proved.

Proposition 5.3. *Under the random attack, the unique social optimal investment level of agent ν solves*

$$c'(q_\nu^s) = \frac{D_\nu}{n} \tag{5.8}$$

for each agent.

Proof. The social optimum $\mathbf{q}^s$ is the argument of the global maximum of S. This value can be found by solving the FOC and verifying that this solution indeed is the global maximum. For this, first note that the derivative of S to q_ν is given by

$$\frac{dS}{dq_\nu} = \frac{1}{n}D_\nu - c'(q_\nu).$$

Clearly the solution of (5.8) solves this FOC. Uniqueness and existence of $\mathbf{q}^s$ follow again from lemma A.1. To prove that the solution of 5.8 indeed is the global maximum, we next prove that S is strictly concave in $\mathbf{q}$ and does not feature any boundary maximums. Note that

$$\frac{dS}{dq_\nu}(\{0, \mathbf{q}_{-\nu}\}) = \frac{1}{n}D_\nu \geq 0 \text{ and } \frac{dS}{dq_\nu}(\{1, \mathbf{q}_{-\nu}\}) = \frac{1}{n}D_\nu - c'(1) \leq 0,$$

from which it follows that ∇S does not point outward $[0,1]^n$ at the boundary. This - in turn - implies that there cannot be a boundary global maximum. Finally, note that

$$\frac{d^2S}{dq_\nu^2} = -c''(q_\nu) < 0 \text{ and } \frac{d^2S}{dq_\nu dq_\mu} = 0,$$

which implies that the Hessian $H(S)$ features negative entries on the diagonal while other entries are zero. As this means that $H(S)$ is negative definite, we conclude that S is strictly concave. By using proposition 5.1 we indeed prove that S attains it's global maximum at the unique solution of (5.8). □

By comparing proposition 5.2 and proposition 5.3 one immediately sees that - when c is strictly convex (and hence c' is strictly increasing) - the Nash equilibrium features under-investments relative to the social optimum for every value of p. Economic motivation for this result is intuitive. As an agent can not control a possible external loss in a random attack, an increase in investments does not lead to a reduced risk that his document is stolen through another agent. This forces an agent - in non-cooperative setting - to ignore the external risk and to find the optimal trade-off between investment costs and protection against a direct loss. Contrary, in the cooperative game an agent invests as well to protect documents of others. This leads to the higher investments in security in a cooperative setting. The following example shows this observation in a star network.

Example 5.1. Consider a star network on four nodes as showed in figure 27. Recognize that $D_1 = 1+3p$ and $D_2 = D_3 = D_4 = 1 + p + 2p^2$. When we assume that the cost to adopt security is $(1/2)q_\nu^2$, it follows that $\mathbf{q}^N = 1/4$, $q_1^s = 1/4 + 3p/4$ and $q_2^s = q_3^s = q_4^s = 1/4 + p/4 + 2p^2/4$. These investment levels are plotted in figure 28 as function of p. Observe that the Nash equilibrium indeed features under-investments relative to the social optimum in figure 28. Also observe that the social optimal investment level of agent 1, the central agent, is higher than investments of other agents. Of course this is in line with expectation as the central agent obtains more documents in expectation.

5.4 Incentives of a malicious attacker

Now that we have established characteristic equations to find the Nash equilibrium and the social optimum under the random attack, we shift the focus to the strategic attack. Remind that under this attack the attacker observes the security investments made by the agents (the outcome of the security game)

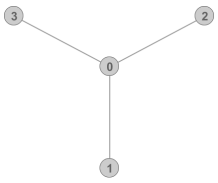

Figure 27 – *The star network on four nodes.*

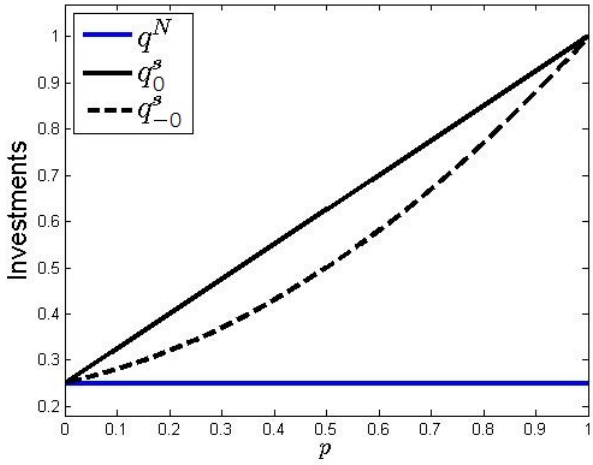

Figure 28 – *Equilibrium investments q^N under the random attack. In this figure the network of figure 27 is adopted. Note that q^N features under-investments relative to social optimum $\mathbf{q}^s = \{q_0^s, q_{-0}^s, q_{-0}^s, q_{-0}^s\}$.*

and consequently chooses an optimal probability distribution over all agents. Nevertheless, as we assume that agent's choose their investments *anticipating* the decision of the attacker, agents know the strategy of the attacker as function of their investments. Consequently, to adequately analyze the behavior of agents, the strategy of the attacker is analyzed first in this report.

First some basic results like uniqueness of the attack vector are deduced for arbitrary networks. These results are derived from Kuhn-Tucker conditions which are conditions to solve maximization problems with both equality and inequality constraints. Next the strategy of the attacker is analyzed in vertex-transitive networks. Remind that in these networks the expected number of documents stored at each agent (D_ν) is identical for every agent ν (and therefore shortened to D). This makes the attacker indifferent if investments are identical among agents.

5.4.1 General results

Remind that the utility of the attacker are the expected number of documents obtained in an attack minus the attack costs. The expected number of documents obtained in an attack is equivalent with $\mathbb{E}(|x|)$ as the following derivation shows:

$$\begin{aligned}
&\mathbb{E}[\text{ \# of documents obtained }] \\
&\quad = \sum_\nu \Pr\{\text{agent } \nu \text{ is attacked}\}\mathbb{E}[\text{ \# of documents obtained } |\text{agent } \nu \text{ is attacked }] \\
&\quad = \sum_\nu a_\nu \Pr\{\text{attack is successful}\}\mathbb{E}[\text{ \# of documents obtained } |\text{agent } \nu \text{ is attacked successfully }] \\
&\quad = \sum_\nu a_\nu (1-q_\nu) D_\nu \;=\; \mathbb{E}(\;|x|\;).
\end{aligned}$$

In this derivation, the third equality follows because both a_ν and $1-q_\nu$ are Bernoulli random variables.

The utility of the attacker is subsequently described with

$$\Pi_a = \sum_\nu a_\nu [1-q_\nu] D_\nu - \psi(a_\nu). \tag{5.9}$$

In this research we adopt the following assumption assumption on ψ.

Assumption 2. (**Attacking cost**) The cost function $\psi : [0,1] \to \mathbb{R}^+$ is assumed to be a two times continuously differentiable in $[0,1]$, strictly convex in $(0,1]$, strictly increasing in $(0,1]$ and to satisfy the boundary conditions $\psi(0) = 0$, $\psi'(0) = 0$ and $\psi'(1) \geq 1$.

Similar as the investment costs, the attacking costs are assumed to be strictly convex and strictly increasing. This set-up presumes the attacker to incur more costs when he or she chooses a more precise attack. Motivation follows because, by choosing a more precise attack, the attacker requires more detailed knowledge about the network structure and characteristics of agents. Nevertheless, the assumption also has a technical motivation as a Nash equilibrium does not always exists when the assumption is violated. In appendix section C an example is showed where, in a network with two agents, a pure strategy Nash equilibrium and even a mixed strategy Nash equilibrium does not exists when $\psi \equiv 0$.

We continue to discuss the strategy of the attacker. Remind that this strategy (globally) maximizes (5.9) subject to this strategy to remain a probability distribution (see (3.8) in the model description). Kuhn-Tucker (KT) conditions can be used to solve these optimization problems as they provide first order necessary conditions for optimization problems with both equality and inequality constraints. In this problem however, because the objective function in the optimization problem (Π_a) is strictly concave[29] in $\mathbf{a}$ and each constraint is linear, the Kuhn-Tucker conditions are not only necessary conditions, they also are sufficient for solving (3.8).

To apply Kuhn-Tucker first define

$$L(\mathbf{q}, p) = \Pi_a + \lambda[\sum_{\nu \in V} a_\nu - 1] + \sum_{\nu \in V(A)} \kappa_\nu a_\nu, \tag{5.10}$$

where $\lambda \in \mathbb{R}$, $\kappa_\nu \in \mathbb{R}^+$ for each ν and Π_a as in (5.9). Consequently, the KT-conditions are

$$\begin{aligned} &\forall \nu \in \mathcal{G}(V), \\ &\quad 1.\ \frac{\partial L}{\partial a_\nu} = [1 - q_\nu]D_\nu - \psi'(a_\nu) + \lambda + \kappa_\nu = 0, \\ &\quad 2.\ \kappa_\nu a_\nu = 0, \\ &\quad 3.\ a_\nu \geq 0, \\ &\quad 4.\ \sum_{\nu \in V} a_\nu = 1. \end{aligned} \tag{5.11}$$

Surely, the solution of these KT-conditions ($3n+1$ in total) depend on both $\mathbf{q}, p$ and the network structure. By noting that either a_ν or κ_ν is larger than zero for every ν, the following result is established.

Proposition 5.4. *The solution $\mathbf{a}$ of the KT-conditions in (5.11) uniquely describes the strategy of the attacker. When $\mathbf{q}$ and D_ν are given and ψ satisfies assumption 2, for every $\nu \in V$ the strategy of the attacker solves*

$$a_\nu = \psi'^{-1}(\ \max\{0,\ [1 - q_\nu]D_\nu + \lambda\ \}). \tag{5.12}$$

In (5.12), $(\psi')^{-1} : [0, \psi'(1)] \to [0,1]$ is the inverse[30] of ψ' and $\lambda \in \mathbb{R}$ solves

$$\sum_\nu \psi'^{-1}(\ \max\{0,\ [1 - q_\nu]D_\nu + \lambda\ \}) = 1. \tag{5.13}$$

Proof. First remind that the KT-conditions are both sufficient and necessary for optimization as Π_a is strictly concave and the constraints linear. Next, equation (5.12) follows from the KT-conditions given in

29. This can be seen by noting that the Hessian of Π_a only features $-\psi''(a_\nu)$ on its diagonal. By using assumption 2, $H(\Pi_a)$ is negative definite and consequently Π_a strictly concave in $\mathbf{a}$.
30. A function $g : B \to A$ is said to be the inverse of $f : A \to B$ if for all $a \in A$, $g(f(a)) = a$.

(5.11). First observe that λ is bounded as for all ν, KT-condition *1.* can be written to

$$\begin{aligned}\lambda &= \psi'(a_\nu) - (1-q_\nu)D_\nu - \kappa_\nu \\ &\leq \max_\nu[\psi'(a_\nu) - (1-q_\nu)D_\nu - \kappa_\nu] \leq \psi'(1).\end{aligned}$$

Next recognize that if $a_\nu > 0$ then necessarily $\kappa_\nu = 0$ from the second KT-condition. From this it follows, by rewriting *1.*, that for all ν with $a_\nu > 0$:

$$a_\nu = \psi'^{-1}([1-q_\nu]D_\nu + \lambda), \tag{5.14}$$

where $(\psi')^{-1}$ is the inverse of ψ'. By boundedness of λ, input of ψ'^{-1} in (5.14) is necessarily a subset of the co-domain of ψ'. By combining this with the result that the inverse of a strictly increasing function necessarily exists (see lemma A.4 on page 81), it follows that ψ'^{-1} is well-defined.

As $\psi'^{-1}(0) = 0$ by assumption 2, equation (5.14) can be easily extended to all agents with $a_\nu = 0$. This leads to (5.12) in the proposition. Next, to prove that λ solves (5.13), simply observe that by summing (5.12) over all agents, KT-condition *4.* has to be satisfied. □

The following example will shed some light on how to compute the attack vector by using proposition 5.4. Also some insights are obtained on the role of p and ψ on this attack vector.

Example 5.2. Continuing on example 5.1 where $p = 0.5$. In this situation $D_0 = 2.5$ and $D_1 = D_2 = D_3 = 2$. Also set $\psi = a^2$ and assume the investment level is $\mathbf{q} = \{\frac{5}{8}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\}$. By noting that $\psi'^{-1}(y) = (1/2)y$, the value of λ can be found by solving

$$\frac{1}{2}\max\{0,\ 2.5\,\frac{3}{8} + \lambda\ \}) + \frac{3}{2}\max\{0,\ 2\,\frac{1}{2} + \lambda\ \}) = 1.$$

A good approach to find λ is to first consider the case where both $\max$ operators are excessive. This leads to the solution $\lambda = -0.7334$. As we later show that λ is unique, it is consequently unnecessary to consider other cases. By substituting $\lambda = -0.7334$ in (5.12) it follows that

$$a_0 = 0.2266 \ \text{ and } \ a_1 = a_2 = a_3 = 0.2578.$$

Note that the central agent in figure 27 is attacked with a lower probability under the strategic attack than in the random attack. This follows of course because $q_0 > q_{-0}$, but is not trivial because also $D_0 > D_1$; the middle agent obtains in expectation more documents.

When costs to make a more precise attack are reduced, for instance by setting $\psi = \frac{1}{3}a^3$, it turns out that the attacker prefers a more precise attack on the periphery agents:

$$a_0 = 0.1402 \ \text{ and } \ a_1 = a_2 = a_3 = 0.2866.$$

This also turns out to be the case when p is increased to 0.8 (and ψ is reset to a^2):

$$a_0 = 0.1506 \ \text{ and } \ a_1 = a_2 = a_3 = 0.2831.$$

This result is no surprise because when $p = 0.8$, opposed to $p = 0.5$, the difference between D_0 and D_1 is reduced; making it more attractive to attack the periphery agents (under the current investment level).

Figure 29 gives a more in-depth view of the probability that agent 1 is attacked. Observe that - intuitively correct - when q_0 is high and q_{-0} is low, a_0 is low (and vice versa). Also observe that the derivative of a_0 to $\mathbf{q}$ is constant (or does not exists). This shows to be characteristic for quadratic ψ. Lastly note that when $\mathbf{q}_{-0} = 0$, it is more optimal for agent 0 to invest 0.6 than to invest 0.8 as a_0 remains 0 is both cases. This optimization process made by every agent is considered in the security game in the next section.

Although proposition 5.4 provides a way to find the strategy of the attacker, it can be arduous to solve (5.13) and we cannot give a closed-form solution. Yet, some properties of $\mathbf{a}$ can be found by using proposition 5.4 though. For instance one can deduce that a_ν is non-increasing in q_ν and non-decreasing in every element in $q_{-\nu}$. First however we show that the attack vector is unique for every $\mathbf{q}$.

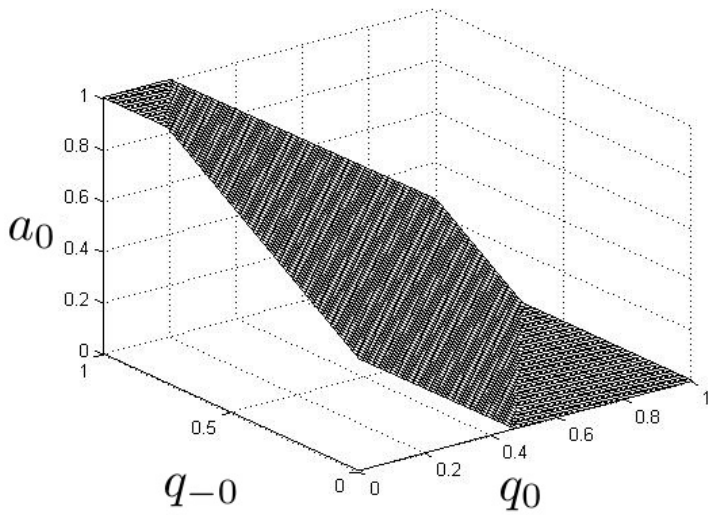

Figure 29 – *Probability a_0 that agent 0 in figure 27 is attacked as function of q_0 and $q_{-0} \equiv q_1 = q_2 = q_3$. In this figure $p = 0.5$ and the cost for the attacker is set to $\psi = a^2$. Note that a_0 is bounded below by zero and bounded above by one.*

Proposition 5.5. *The attack vector is unique for every given security vector.*

Proof. Uniqueness of a_ν - for every ν - follows from uniqueness of λ. This can be seen from (5.12) as ψ'^{-1} and the $\max$ operator are both well-defined and continuous under assumption 2.

Remains to show that λ - implicitly defined in (5.13) - is unique for every choice of the security vector. First observe that ψ'^{-1} can be ignored as it is strictly increasing and continuous in its argument. Next by setting $0 \leq y_\nu \equiv (1 - q_\nu)D_\nu \leq n$, uniqueness of λ in (5.13) follows from uniqueness of λ implicitly defined in

$$\sum_\nu \max\{0, y_\nu + \lambda\} = 1 \tag{5.15}$$

where $y_\nu \in \mathbb{R}^+$.

Assume next that for some security vector $\mathbf{q}^*$ there is more than one solution λ of (5.15). Let λ_1 and λ_2 be two of these solutions. It follows that

$$\sum_\nu \max\{0, y_\nu + \lambda_1\} - \sum_\nu \max\{0, y_\nu + \lambda_2\} = 0.$$

Now let $V_1, V_2 \subset V$ be two subsets for which, for all $\nu \in V_1$: $y_\nu + \lambda_1 > 0$ and, for all $\nu \in V_2$: $y_\nu + \lambda_2 > 0$. W.lo.g. assume that $\lambda_1 < \lambda_2$ and note that due to this necessarily $V_1 \subset V_2$. Now by rewriting the expression above:

$$\sum_{\nu \in V_1} y_\nu - \sum_{\nu \in V_2} y_\nu = \lambda_2 |V_2| - \lambda_1 |V_1|.$$

Observe that the LHS of this expression is smaller than zero, while conversely the RHS is larger than zero. As this leads to a contradiction our assumption that there are several solutions of (5.15)shows to be false. □

Although the attack vector is unique for every choice of $\mathbf{q}$, continuity of $\mathbf{a}$ in $\mathbf{q}$ is hard to prove. Note that the implicit function theorem (see lemma A.5) can not be used as (5.15) is not differentiable when $y_\nu + \lambda = 0$ for some ν. Though, later in this research in proposition 5.9, we show that $\mathbf{a}$ is continuous in a vertex-transitive network where all agents - other than one agent - play the same strategy.

Despite continuity of the attack vector remains - for now - an open question, one can show that the attack vector may not be differentiable to $\mathbf{q}$ in some cases. Specifically, a_ν is not differentiable when both $a_\nu = 0$ and $\kappa_\nu = 0$ as in the KT-conditions in (5.11). In this situation, inspection of KT-condition *1.* reveals that $\lambda = -[1 - q_\nu]D_\nu$. When combining this observation with (5.12) one finds that a_ν is indeed not differentiable.

Contrary to the cases where $a_\nu = 0$, when a_ν is larger than zero then it is differentiable to q_ν. Additionally it is differentiable to q_μ when $a_\mu > 0$. The specific rate of change can be found from the KT-conditions as showed in the next proposition.

Proposition 5.6. *The derivative of $a_\nu > 0$ to q_ν and the derivative of a_ν to q_μ for which $a_\mu > 0$ are given by*

$$\frac{da_\nu}{dq_\nu} = \frac{-D_\nu}{\psi''(a_\nu)} + \frac{D_\nu}{\psi''(a_\nu)^2\Phi} \quad \textit{and} \quad \frac{da_\nu}{dq_\mu} = \frac{D_\mu}{\psi''(a_\nu)\psi''(a_\mu)\Phi}. \tag{5.16}$$

In this expression

$$\Phi = \sum_{\kappa|a_\kappa>0} \frac{1}{\psi''(a_\kappa)}. \tag{5.17}$$

Proof. The results follow again from the KT-conditions in (5.11). When $a_\nu > 0$, and therefore $\kappa_\nu = 0$, by differentiating *1.* to q_ν:

$$\frac{da_\nu}{dq_\nu}\psi''(a_\nu) = -D_\nu + \frac{d\lambda}{q_\nu}. \tag{5.18}$$

Similar, for all $\mu \neq \nu$ for which $a_\mu > 0$:

$$\frac{da_\mu}{dq_\nu}\psi''(a_\mu) = \frac{d\lambda}{dq_\nu}. \tag{5.19}$$

By combining the observation that

$$\sum_{\mu\in V} \frac{da_\mu}{dq_\nu} = \sum_{\mu|a_\mu>0} \frac{da_\mu}{dq_\nu} = 0,$$

by differentiating KT-condition *4.* to q_ν, with (5.18) and (5.19) and noting that division by $\psi''(a_\mu) > 0$ is allowed:

$$\frac{-D_\nu}{\psi''(a_\nu)} + \frac{d\lambda}{dq_\nu} \sum_{\mu|a_\mu>0} \frac{1}{\psi''(a_\mu)} = 0.$$

When using Φ as in (5.17), it follows that

$$\frac{d\lambda}{dq_\nu} = \frac{D_\nu}{\psi''(a_\nu)\Phi}.$$

By substituting this result in (5.18) and (5.19) the results in the proposition follow. □

Recognize that the equations in (5.16) in fact are differential equations which can be used to set up a system of differential equations from which $\mathbf{a}$ can be solved. Yet, the complexity of these differential equations do not allow to easily find a solution. This limits the use of (5.16) to find the rate of change of $\mathbf{a}$ when the current level of $\mathbf{a}$ is known. The following example applies the proposition to the star network.

Example 5.3. Continuing on example 5.1 and example 5.2. Recognize that $\psi''(a) = 2$ when $\psi(a) = a^2$ and remind that $D_0 = 2.5$ and $D_1 = D_2 = D_3 = 2$ when $p = 0.5$. In example 5.2 we computed that $a_0 = 0.226 > 0$ and $a_{-0} = 0.2578 > 0$. Consequently, by substituting values in (5.16) one finds for instance that

$$\frac{da_0}{dq_0} = \frac{-2.5}{2} + \frac{2.5}{4(\frac{1}{2} + \cdots + \frac{1}{2})} = \frac{-2.5}{2} + \frac{2.5}{8} = -\frac{15}{16} \quad \text{and} \quad \frac{da_0}{dq_2} = \frac{2}{4(\frac{1}{2} + \cdots + \frac{1}{2})} = \frac{1}{4}.$$

As exact results indicate that

$$a_0 = [-\frac{15}{16}q_0 + \frac{1}{4}q_1 + \frac{1}{4}q_2 + \frac{1}{4}q_3 + \frac{7}{8}]^{+/-},$$

where $[\cdot]^{+/-}$ is $\max\{0, \min\{1, \cdot\}\}$, the result is verified[31].

Note from the example above that the derivatives in (5.16) are independent of $\mathbf{a}$ when ψ is quadratic. In this situation derivatives can be significantly simplified. By noting that there is some scalar α for which $\psi''(a) = \alpha$, it follows by rewriting derivatives in (5.16) that

$$\frac{da_\nu}{dq_\nu} = \frac{1 - n^*}{\alpha n^*} D_\nu \quad \text{and} \quad \frac{da_\nu}{dq_\mu} = \frac{1}{\alpha n^*} D_\mu, \tag{5.20}$$

where $1 \leq n^* \leq n$ are the number of agents that have strict positive chance of being attacked. Note that these expressions imply that a_ν is non-increasing in q_ν and a_ν is non-decreasing in every element in $\mathbf{q}_{-\nu}$ (as $n^* \geq 1$). This observation is generally true as the following proposition shows.

Proposition 5.7. *The probability that an agent is attacked is non-increasing in an agent's own security investments, while it is is non-decreasing in the security investments of other agents.*

Proof. Specifically, we proved that $a_\nu(\{q_\nu, q_{-\nu}\})$ is non-increasing in q_ν and non-decreasing in any element in $q_{-\nu}$.

First suppose that $a_\nu > 0$. By using (5.16), da_ν/dq_ν is smaller or equal than zero when

$$\frac{D_\nu}{\psi''(a_\nu)}(-1 + \frac{1}{\psi''(a_\nu)\Phi}) \leq 0.$$

By rewriting this expression and noting that $D_\nu/\psi''(a_\nu) > 0$ and hence can be removed, da_ν/dq_ν is smaller than zero when

$$\frac{1}{\psi''(a_\nu)} \leq \Phi.$$

As $a_\nu > 0$ this expression always hold. We conclude that - indeed - a_ν is non-increasing in q_ν. By using a similar line of argument it follows that a_ν is non-decreasing in q_μ ($\mu \neq \nu$) when $a_\mu > 0$.

When $a_\nu = 0$ we have to consider two cases: $\kappa_\nu = 0$ and $\kappa_\nu > 0$. First, when $\kappa_\nu = 0$ the derivative of a_ν to q_μ does not exists by earlier analysis. When $\kappa_\nu > 0$, differentiating of KT-condition *2.* reveals that

$$\frac{da_\nu}{dq_\mu}\kappa_\nu = -\frac{d\kappa_\nu}{dq_\mu}a_\nu. \tag{5.21}$$

Surely when $a_\nu = 0$ and $\kappa_\nu > 0$, $da_\nu/dq_\mu = 0$ for all μ. This completes the proof of the proposition. □

5.4.2 Attacker's strategy in vertex-transitive networks

In vertex transitive networks the expected number of documents obtained by each agent is identical, i.e. $D_\nu \equiv D$ for every ν. Earlier results are significantly eased by this observation as diversity in the argument of (5.12) only arise from diversity in $\mathbf{q}$ (and no longer from D_ν). Note for instance that if all security investments are identical in a VT-network, then $\mathbf{a} = 1/n$ and the attacker is indifferent[32].The next proposition shows some results which hold in VT-networks.

31. As we focus on the security game in *vertex-transitive networks* in subsequent sections, this example on the star is finished. Nevertheless in appendix section D on page 84 simulation results are presented which conjecture that results in VT-networks expand to asymmetric networks like the star.
32. Although $\mathbf{a} = 1/n$, da_ν/q_μ might not be zero and consequently $\mathbf{a} \not\equiv 1/n$ as in the random attack.

Proposition 5.8. *If the network $\mathcal{G}$ is vertex-transitive and ψ satisfies assumption 2,*

1. *the attacker is indifferent under an automorphism of nodes and the corresponding investment levels, that is for every $\phi \in Aut(\mathcal{G})$, $a_\nu(q_1, ..., q_n) = a_{\phi(\nu)}(q_{\phi(1)}, ..., q_{\phi(n)})$,*
2. *if and only if $q_\nu > q_\mu$ or $q_\nu = q_\mu$ for some $\nu \neq \mu \in V$, then respectively $a_\nu < a_\mu$ or $a_\nu = a_\mu$,*
3. *if and only if $q_\nu = q_\mu$ then $\frac{da_\nu}{dq_\nu} = \frac{da_\mu}{dq_\mu}$.*

Proof. Result *1.* and *2.* follow easily from (5.12) and (5.13) as λ is unique and ψ'^{-1} is strictly increasing. Result *3.* follows by combining (5.16) with *2.* in the proposition. □

The results in the proposition allow to compute a wide range of characteristics of $\mathbf{a}$. For instance, by using result *1*. one can focus the analysis on one agent and consequently extend properties to all agents. Also, despite the simplicity of *3.*, more results can be deduced from it. For instance, if all elements in $\mathbf{a}_{-\nu}$ are identical it follows that[33]

$$\frac{da_\nu}{dq_\nu} = \frac{-1}{n-1}\frac{da_\mu}{dq_\nu} \tag{5.22}$$

for some $\mu \neq \nu$.

Later in the security game we use (5.22) to show that a symmetric Nash equilibrium exists. To do this, we additionally need that $\mathbf{a}$ is continuous. This is showed in the following proposition.

Proposition 5.9. *In a vertex-transitive network every element in $\mathbf{a}$ is continuous at every $\mathbf{q} = \{q_\nu, \mathbf{q}_{-\nu}\}$ where $q_{-\nu}$ is symmetric.*

Proof. Continuing on the proof of proposition 5.5, every element in $\mathbf{a}$ is continuous at $\mathbf{q}$ when λ implicitly defined in (5.15) is continuous at $\mathbf{q}$. Now when $\mathbf{q} = \{q_\nu, \mathbf{q}_{-\nu}\}$ where $\mathbf{q}_{-\nu} = q_{-\nu}$ is symmetric (i.e. identical elements), the exact value of λ can be computed by considering three exclusive events: **a)** $y_\nu + \lambda \leq 0$, **b)** $y_{-\nu} + \lambda \leq 0$ and **c)** both $y_\nu + \lambda \geq 0$ and $y_{-\nu} + \lambda \geq 0$. This leads to expressions for λ as showed in figure 30. Clearly only concern regarding continuity of λ is at the transition lines. However at the (upper) solid transition line: from above

$$\lambda = \frac{1}{n-1} - y_{-\nu} = \frac{1}{n-1} - (y_\nu + \frac{1}{n-1}) = -y_\nu$$

and from below

$$\lambda = \frac{1 - y_\nu - (n-1)y_{-\nu}}{n} = \frac{1 - y_\nu - (n-1)(y_\nu + \frac{1}{n-1})}{n} = -y_\nu.$$

This proofs that λ is continuous at the upper transition line. In a similar way we can show that λ is continuous at the lower transition line. □

5.5 Equilibrium investments in security

In this section the security game is analyzed when agents do not cooperate and the attack is strategic. Different than under the random attack, under this attack agents can discourage a direct attack by increasing investments. Intuitively, when dependencies between agents are low and therefore the chance that an agent's document is lost through another agent is small, the impact of a direct attack is large. In this scenario an agent has incentives to invest more in security, forcing the attacker to attack someone else. Contrary, when dependencies are large it might be less beneficial to increase investments. This follows because the chance that a document is obtained by another agent is much larger; reducing the stimulus to force the attacker to attack another agent. In this section we analyze this and other incentives present in the security game.

33. By differentiating both sides of the constraining assumption $\sum_\nu a_\nu = 1$ to q_ν, it follows that $\frac{da_\nu}{dq_\nu} + \sum_{\mu \neq \nu} \frac{da_\mu}{dq_\nu} = 0$. Consequently by using *3.* the result follows.

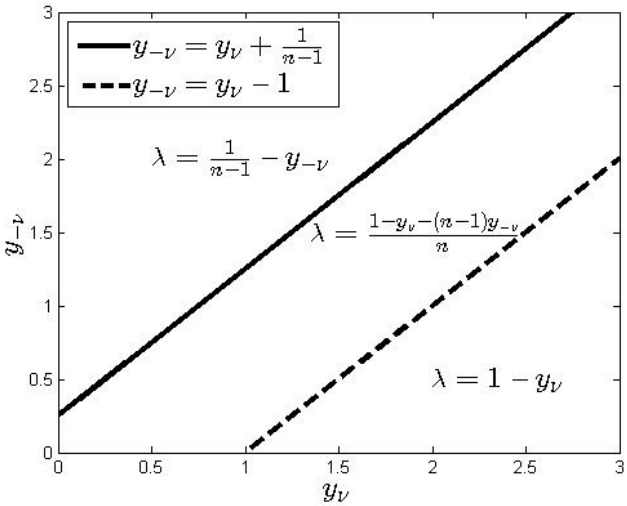

Figure 30 – *Expressions for λ as function of y_ν and $y_{-\nu}$. In the figure n is set equal to 5.*

Specifically, in this section we focus on proving that a pure strategy Nash equilibrium exists and finding the corresponding investment level. To make the analysis tractable, we assume that dependencies among agents adopt a vertex-transitive structure. Note that this assumption removes all heterogeneity between agents[34]. Although this assumption quite limits the impact of the results, there is some evidence that forces present in vertex-transitive networks also subsist to a wider scope of network structures (see simulation results in appendix section D on page 84).

In this section first some technical results are given that allow to compute the best response of an agent in vertex-transitive networks. We show that this best response is always interior of an agent's strategy space and show that the best response is never such that either $a_\nu = 0$ or $a_\nu = 1$. Next we show that a symmetric pure strategy Nash equilibrium exists when certain conditions on the cost for the attacker are satisfied. Moreover characteristic equations are given that allow to find the investment level in this symmetric Nash equilibrium.

5.5.1 Properties of the best response

First remind that the utility of each agent is given by

$$\Pi_\nu = 1 - \sum_\mu a_\mu [1 - q_\mu] D_{\nu,\mu} - c(q_\nu); \tag{5.23}$$

a function which an agent would like to make as large as possible. As Π_ν is a function of both q_ν and $\mathbf{q}_{-\nu}$, an agent adopts his best response $\varphi_\nu(\mathbf{q}_{-\nu})$. This best response is an investment level which maximizes (5.23), given $\mathbf{q}_{-\nu}$.

Several properties of $\varphi_\nu(\mathbf{q}_{-\nu})$ can be deduced. For instance, by the boundary presumptions on c in assumption 1, $\varphi_\nu(\mathbf{q}_{-\nu})$ is necessarily interior of $[0, 1]$. This is showed in the following proposition.

Proposition 5.10. *When c satisfies assumption 1 and the network is vertex-transitive, the best response of each agent is in $(0, q^*)$ where $q^* \leq 1$ solves $c(q^*) = 1$.*

Proof. First note that q^* exists because $c(0) = 0$ and $c(1) \leq 1$ by assumption 1. The proof is consequently split in two parts. First we show that it is always optimal for an agent to slightly invest more than

34. In fact the security game is symmetric in vertex-transitive networks as the utility functions are permutation-invariance. Formally, following Dasgupta and Maskin (1986), a game Γ is symmetric if and only if for every automorphism ϕ between agents and their strategic decisions, $\Pi_\nu((q_1, \ldots, q_n)) = \Pi_{\phi(\nu)}((q_{\phi(1)}, \ldots, q_{\phi(n)}))$.

zero. Next we show that the utility of an agent who plays q^* or more is not higher than his utility when he or she plays zero. This implies that there must be a $0 < q < q^*$ such that $U(\{q, q_{-\nu}\}) > U(\{0, q_{-\nu}\}) \geq U(\{q^*, q_{-\nu}\})$.

Note that the derivative of (5.23) to q_ν is

$$\frac{d\Pi_\nu}{dq_\nu} = a_\nu - \sum_\mu \frac{da_\mu}{dq_\nu}[1 - q_\mu]D_{\nu,\mu} - c'(q_\nu). \tag{5.24}$$

When agent ν does not invest in security, i.e. $q_\nu = 0$, it is always optimal to (slightly) increase investments:

$$\begin{aligned}\frac{d\Pi_\nu}{dq_\nu}(\{0, q_{-\nu}\}) &= a_\nu - \sum_{\mu\neq\nu} \frac{da_\mu}{dq_\nu}[1 - q_\mu]D_{\nu,\mu} - \frac{da_\nu}{dq_\nu} \\ &> a_\nu - \sum_{\mu\neq\nu} \frac{da_\mu}{dq_\nu} - \frac{da_\nu}{dq_\nu} \\ &= a_\nu - \sum_{\mu\neq\nu} \frac{da_\mu}{dq_\nu} = a_\nu \geq 0.\end{aligned}$$

The first inequality is strict because when it is an equality then necessarily $\mathbf{q} = 0$. In this situation every agent adopts an identical strategy and $\mathbf{a} = 1/n > 0$ by *2.* in proposition 5.8 (note that the vertex-transitivity assumption is used here). When $\mathbf{a} = 1/n$ this would in turn force the last inequality to be strict. The third equality follows because

$$\sum_\mu \frac{da_\mu}{dq_\nu} = 0$$

as the elements in $\mathbf{a}$ sum to 1.

Next we show that $U(\{0, q_{-\nu}\}) \geq U(\{q^*, q_{-\nu}\})$. By substituting values

$$\Pi(\{0, q_{-\nu}\}) = 1 - a_\nu - \sum_{\mu\neq\nu} a_\mu[1 - q_\nu]D_{\nu,\mu} \geq 0$$

as elements in $\mathbf{a}$ sum to one and both $1 - q_\mu \leq 1$ and $D_{\nu,\mu} \leq 1$. Also for all $q_\nu \geq q^*$:

$$\begin{aligned}\Pi(\{q_\nu, q_{-\nu}\}) &= 1 - \sum_\mu a_\mu[1 - q_\nu]D_{\nu,\mu} - c(q_\nu) \\ &\leq -\sum_\mu a_\mu[1 - q_\nu]D_{\nu,\mu} \leq 0,\end{aligned}$$

and the result follows. □

The proposition above allows to conclude that an agent's best response is not at the boundary of the strategy space. This in turn implies that the best response necessarily solves the FOC of (5.23) given $\mathbf{q}_{-\nu}$. The FOC is showed in the following proposition.

Proposition 5.11. *In a vertex-transitive network where c satisfies assumption 1 and where $\mathbf{q}_{-\nu} \in [0, 1]^{n-1}$ is given, if $q_\nu = \varphi_\nu(\mathbf{q}_{-\nu})$ is an agent's best response then q_ν solves*

$$c'(q_\nu) = a_\nu - \sum_\mu \frac{da_\mu}{dq_\nu}[1 - q_\mu]D_{\nu,\mu}. \tag{5.25}$$

Proof. By proposition 5.10, $\varphi_\nu(\mathbf{q}_{-\nu}) \in (0, 1)$. This necessarily means that $\varphi_\nu(\mathbf{q}_{-\nu})$ solves the FOC of Π_ν as showed in (5.25). □

The use of proposition 5.11 is quite small for the moment. First of all the proposition only provides a necessary condition for optimality and therefore solutions of (5.25) can also be local maxima or minima. Second, although there necessarily is one solution (because there is not a boundary maximum), (5.25) can have more than one solution.

Note however that we can further expose the best response by analyzing the da_μ/dq_ν term inside. For this derivatives in (5.16) can be used. As the next proposition ensures that an agent's best response is always such that neither $a_\nu = 0$ nor $a_\nu = 1$, the use of these derivatives is allowed.

Proposition 5.12. *When c satisfies assumption 1 and the network is vertex-transitive, an agent's best response is not such that $a_\nu = 0$ or $a_\nu = 1$.*

Proof. Note that when $\varphi_\nu(\mathbf{q}_{-\nu})$ is such that $a_\nu = 0$ for some agent ν, the utility in (5.23) is reduced to

$$\Pi_\nu(\{\varphi_\nu(\mathbf{q}_{-\nu}), \mathbf{q}_{-\nu}\}) = 1 - \sum_{\mu \neq \nu} a_\mu [1 - q_\nu] D_{\nu,\mu} - c(\varphi_\nu(\mathbf{q}_{-\nu})).$$

As $\varphi_\nu(\mathbf{q}_{-\nu})$ necessarily maximizes Π_ν and - as a consequence - also the expression above, it follows that $\varphi_\nu(\mathbf{q}_{-\nu}) = 0$. This contradicts the result in proposition 5.10 in which we showed that $\varphi_\nu(\mathbf{q}_{-\nu}) \neq 0$.

Similarly, when $\varphi_\nu(\mathbf{q}_{-\nu})$ is such that $a_\nu = 1$ then $a_{-\nu} = 0$. This in turn makes

$$\Pi_\nu(\{\varphi_\nu(\mathbf{q}_{-\nu}), \mathbf{q}_{-\nu}\}) = \varphi_\nu(\mathbf{q}_{-\nu}) - c(\varphi_\nu(\mathbf{q}_{-\nu})).$$

Consequently the optimal $\varphi_\nu(\mathbf{q}_{-\nu})$ is q^* such that $c'(q^*) = 1$. Again this contradicts the result in proposition 5.10. □

5.5.2 The symmetric pure strategy Nash equilibrium

Although derivatives of $\mathbf{a}$ further exposes characteristics of (5.25), the equation is still difficult analyzed due to the a_ν terms. A bright approach however is to use proposition 5.8 2. in which we showed that $a_\nu = a_\mu$ when $q_\nu = q_\mu$ in a VT-network. By using this observation, we can prove that a symmetric Nash equilibrium exists when the cost for the attacker satisfies certain conditions. This result is showed and proved in the following proposition.

Proposition 5.13. *In the security game assume that dependencies between agents adopt a vertex-transitive structure. If the cost to invest in security satisfies assumption 1, the cost to attack an agent satisfies assumption 2 and for every a the following condition hold:*

$$B \leq \frac{2A^2}{D} + \inf\{c''(q) | q \in [0,1]\} \frac{A^3}{D^2}, \tag{5.26}$$

where

$$A = \psi''(a_\nu) + \frac{1}{n-1}\psi''(\frac{1-a_\nu}{n-1}), \tag{5.27}$$

and

$$B = \psi'''(a_\nu) - \frac{1}{(n-1)^2}\psi'''(\frac{1-a_\nu}{n-1}), \tag{5.28}$$

then there exists a symmetric pure strategy Nash equilibrium.

Proof. By applying the result of Debreu *et al.* - as stated in lemma A.2 on page 81 - a pure strategy Nash equilibrium exists when Π_ν is quasi-concave in q_ν and continuous in $\mathbf{q}_{-\nu}$. As it is troublesome to show that Π_ν is quasi-concave in q_ν, in this proposition we prove that a *symmetric* pure strategy Nash equilibrium exists. For this, assume that all agents other than agent ν are playing q^*, i.e. $\mathbf{q}_{-\nu} = q^*$. First note that Π_ν is continuous when $\mathbf{q} = \{q_\nu, q^*\}$ because $\mathbf{a}$ is by proposition 5.9. Consequently, our main focus in this proof lies on showing that $\Pi(\{q_\nu, q^*\})$ is quasi-concave in q_ν for every choice of $q^* \in [0,1]$.

First note that because every agent $\mu \neq \nu$ plays q^*, from *3.* in proposition 5.8:

$$\frac{da_\nu}{dq_\nu} = -(n-1)\frac{da_\mu}{dq_\nu}. \tag{5.29}$$

When we substitute this result in (5.24):

$$\frac{d\Pi_\nu}{dq_\nu} = a_\nu - \frac{da_\nu}{dq_\nu}(1-q_\nu) + \frac{da_\nu}{dq_\nu}\frac{1}{n-1}(1-q^*)(D-1) - c'(q_\nu). \tag{5.30}$$

Consequently the second derivative of Π_ν to q_ν can be found by differentiating (5.30). This procedure leads to

$$\frac{d^2\Pi_\nu}{dq_\nu^2} = 2\frac{da_\nu}{dq_\nu} - \frac{d^2a_\nu}{dq_\nu^2}(1-q_\nu) + \frac{d^2a_\nu}{dq_\nu^2}\frac{1}{n-1}(1-q^*)(D-1) - c''(q_\nu). \tag{5.31}$$

To establish that Π_ν is quasi-concave in q_ν, we continue by proving that (5.31) is non-positive. For this, derivatives in (5.16) can be used. This is allowed because by proposition 5.12 an agent's best response is always such that $a_\nu > 0$.

Now, as every agent other than agent ν hold the same strategy, equation (5.16) is reduced to

$$\frac{da_\nu}{dq_\nu} = D[-\frac{1}{\psi''(a_\nu)} + \frac{1}{\psi''(a_\nu) + \frac{(n-1)\psi''(a_\nu)^2}{\psi''(\frac{1-a_\nu}{n-1})}}].$$

This in turn can be written as

$$\frac{da_\nu}{dq_\nu} = -D[\frac{1}{\psi''(a_\nu) + \frac{1}{n-1}\psi''(\frac{1-a_\nu}{n-1})}] \tag{5.32}$$

and consequently as $da_\nu/dq_\nu = -D/A$, with A as in (5.27).

The second derivative of a_ν to q_ν can be found by differentiating $-D/A$ to q_ν. It follows that $d^2a_\nu/dq_\nu^2 = DA'/A^2$ where

$$A' = \frac{da_\nu}{dq_\nu}[\psi'''(a_\nu) - \frac{1}{(n-1)^2}\psi'''(\frac{1-a_\nu}{n-1})].$$

By substituting (5.32) and B as in (5.28):

$$\frac{d^2a_\nu}{dq_\nu^2} = -\frac{D^2B}{A^3}. \tag{5.33}$$

Now we have a full characterization of the derivatives of a_ν and (5.32) and (5.33) can be substituted in (5.31). This leads to

$$\begin{aligned}\frac{d^2\Pi_\nu}{dq_\nu^2} &= -2\frac{D}{A} + \frac{D^2B}{A^3}(1-q_\nu) - \frac{D^2B}{A^3}\frac{1}{n-1}(1-q^*)(D-1) - c''(q_\nu)\\ &= -2\frac{D}{A} + \frac{D^2B}{A^3}[1-q_\nu - \frac{D-1}{n-1}[1-q^*]] - c''(q_\nu).\end{aligned}$$

Consequently Π_ν is quasi-concave in q_ν when for all $q_\nu \in [0,1]$ and all $q^* \in [0,1]$,

$$\frac{D^2B}{A^3}(1-q_\nu - \frac{D-1}{n-1}(1-q^*)) \leq 2\frac{D}{A} + c''(q_\nu).$$

By noting that $(1-q_\nu - \frac{D-1}{n-1}(1-q^*)) \leq 1$, the inequality above is satisfied when

$$\frac{D^2B}{A^3} \leq 2\frac{D}{A} + c''(q_\nu)$$

is satisfied. Additinally, because both $A \geq 0$ and $D \geq 1$, Π_ν is quasi-concave if

$$B \leq \frac{2A^2}{D} + c''(q_\nu)\frac{A^3}{D^2},$$

As this must hold for all $q_\nu \in [0,1]$, we establish (5.26) in the proposition. □

Although the proposition above makes sure that a symmetric Nash equilibrium exists, it does not say anything about possible asymmetric equilibria[35]. The impact of an asymmetric equilibrium can be large as properties which hold in a symmetric equilibrium may not extend to asymmetric equilibria. Making things worse, the symmetric equilibrium might be unstable when there is an asymmetric equilibrium: a small permutation in $\mathbf{q}$ can lead to a shift from the symmetric equilibrium to the asymmetric equilibrium. When this is the case the impact of the symmetric equilibrium is small. Yet - in the sequel of this research - the focus lies on the symmetric equilibrium of the security game. This is motivated because simulation results in VT-networks conjecture that no asymmetric equilibria exist in a wide range of games[36]. Moreover, when ψ is quadratic we are able to prove that no asymmetric equilibrium exists (see proposition 5.14). Nevertheless one has to keep in mind the possibility of an asymmetric equilibrium in the sequel of this report.

Another noticeable feature in proposition 5.13 is the baffling condition (5.26) on the cost for the attacker. Beforehand it is hard to say which functions satisfy (5.26) other than quadratic cost functions. Figure 31 shows that (5.26) is satisfied when $c = 5q^2$ and $\psi = a^4$, whereas it is not satisfied when $c = 2q^2$ and $\psi = (1/2)a^4$.

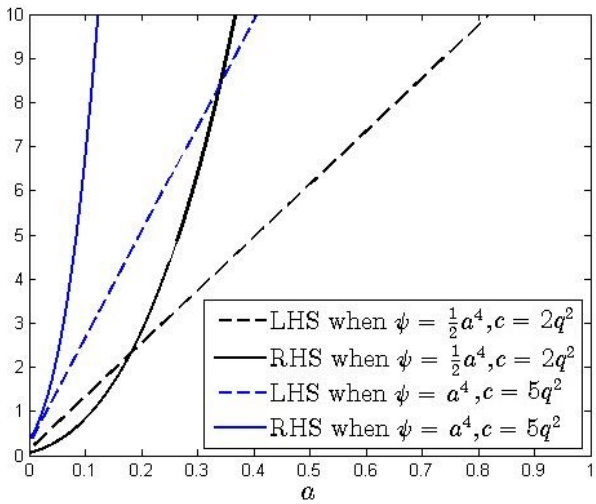

Figure 31 – *The LHS and RHS of (5.26) for several combinations of cost functions. For a symmetric Nash equilibrium to exists, we require that the LHS is larger than the RHS for all* $a \in [0, 1]$.

To make sure that (at least) a symmetric Nash equilibrium exists in the security game, condition (5.26) is added to assumption 2. This leads to an extended version of the assumption.

Assumption 2^+. **(Attacking cost)** In addition to assumption *2.*, presume ψ to satisfy (5.26) for each $a \in [0, 1]$.

A motivation for condition (5.26) can be found in (5.33): if B is 'large' (relative to A) also d^2a_ν/dq_ν^2 is. When this is the case, $\mathbf{a}$ is changed quite drastically when an element in $\mathbf{q}$ is changed. As this means that the attacker easily focuses his attack on other agents, agents may have incentives to incessantly (slightly) increase investments to push the attacker to attack someone else (similar as in appendix section C on page 83). In this situation no Nash equilibrium exists.

To halt possible incessantly increasing of investments, condition (5.26) can be used as it prevents that B is large. It is no surprise that the second derivative of both c and ψ are included in this condition.

35. One might argue that a symmetric game - like the security game in this research - can not have a asymmetric equilibria as all agents should behave identically. Literature indicates however that this is not the case. Two examples are given in Fey (2011).
36. These simulation results are based on iteratively determining the best response of each agent in a DISCRETE variant of the security game. When the procedure converges a Nash equilibrium is found. A sketch of the algorithm is showed in algorithm 2 on page 84.

When the cost to invest is sufficiently convex (i.e. $c'' >> 0$) then it is too costly for an agent to slightly increase investments at some point. On the other side, when $\psi'' >> 0$ it is too costly for the attacker to choose d^2a_ν/dq_ν^2 to be very high. Note that this is confirmed in figure 31 as, in the first case when $\psi = (1/2)a^4$ and $c = 2q^2$, both c''' and ψ'' are smaller than in the second case.

The exact investment level in the symmetric Nash equilibrium can be found by considering (5.25) when all agents hold the same security investment. This procedure leads to the following proposition.

Theorem 5.1. *In the security game in a vertex-transitive network where ψ satisfies assumption 2$^+$ and c satisfies assumption 1, the symmetric pure strategy Nash equilibrium q^N solves*

$$c'(q^N) = \frac{1}{n} + \frac{[n-D]D}{n\psi''(\frac{1}{n})}[1-q^N]. \tag{5.34}$$

This solution q^N of (5.34) is unique and continuous in D (and thus in p). Moreover q^N is initially increasing in p, till the point where $D = n/2$ after which q^N is decreasing in p.

Proof. First note that by proposition 5.13 a symmetric Nash equilibrium exists. Denote this symmetric equilibrium as q^N. As every agent holds the same security investment in a symmetric investment level, $\mathbf{a} = 1/n$ by *3.* in proposition 5.8. By substituting this observation in (5.16)

$$\frac{da_\nu}{dq_\nu} = -D\frac{n-1}{n\psi''(\frac{1}{n})}. \tag{5.35}$$

As each agent by definition plays his best response in a symmetric Nash equilibrium, equation (5.25) has to be satisfied. By substituting values and rewriting

$$\begin{aligned}
c'(q^N) &= a_\nu - \sum_\mu \frac{da_\mu}{dq_\nu}[1-q_\mu]D_{\nu,\mu} \\
&= \frac{1}{n} - [1-q^N]\sum_{\mu\neq\nu}\frac{da_\mu}{dq_\nu}D_{\nu,\mu} - \frac{da_\nu}{dq_\nu}[1-q^N] \\
&= \frac{1}{n} + \frac{1-q^N}{n-1}\frac{da_\nu}{dq_\nu}\sum_{\mu\neq\nu}D_{\nu,\mu} - \frac{da_\nu}{dq_\nu}[1-q^N] \\
&= \frac{1}{n} - [1-q^N]\frac{D}{n\psi''(\frac{1}{n})}\sum_{\mu\neq\nu}D_{\nu,\mu} + D\frac{n-1}{n\psi''(\frac{1}{n})}[1-q^N] \\
&= \frac{1}{n} - [1-q^N]\frac{D}{n\psi''(\frac{1}{n})}[[D-1]-[n-1]], \\
&= \frac{1}{n} - [1-q^N]\frac{[D-n]D}{n\psi''(\frac{1}{n})},
\end{aligned}$$

and the result follows. In this derivation the third equality follows from (5.29).

To prove uniqueness of the symmetric Nash equilibrium, note that the LHS of (5.34) is strictly increasing in q^N by strict convexity of c. By combining this with the observation that the RHS is decreasing in q^N, there either is one or no solution. To prove that there indeed is one solution, observe that

$$LHS(0) = c'(0) = 0 \leq \frac{1}{n} + \frac{[D-n]n}{n\psi''(\frac{1}{n})} = RHS(0) \quad \text{and} \quad LHS(1) = c'(1) \geq 1 > \frac{1}{n} = RHS(1),$$

where $LHS(x)$ and $RHS(x)$ are respectively the LHS and RHS of (5.34) at x. Note that there must be an intersection of the LHS and the RHS (see lemma A.1 on page 81) and hence (5.34) has a unique solution.

To prove continuity of q^N in p and to find the global maximum of q^N, we subsequently compute the derivative of q^N to p by differentiating both sides of (5.34) to p:

$$\frac{dq^N}{dp}c''(q^N)\psi''(\frac{1}{n})n = (\frac{dD}{dp}n - 2\frac{dD}{dp}D)(1-q^N) - \frac{dq^N}{dp}(nD - D^2).$$

By rewriting and combining terms it follows that

$$\frac{dq^N}{dp}[c''(q^N)\psi''(\frac{1}{n})n + nD - D^2] = \frac{dD}{dp}(n-2D)(1-q^N).$$

Note that $c''(q^N) > 0$ (remind that $q^N \neq 0$ by proposition 5.12), $\psi''(\frac{1}{n}) > 0$ and $nD - D^2 \geq 0$. From this we conclude that dq^N/dp exists for every p. This in turn implies that q^N is continuous in p.

Finally note that $dq^N/dp = 0$ for $n - 2D = 0$, $q^N = 1$ and/or $dD/dp = 0$. These last two possibilities are excluded however because respectively $q^N \neq 1$ (again by proposition 5.12) and D is strictly increasing in p (by proposition 4.9 on 29). Consequently by observe that $dq^N/dp(0) \geq 0$ and $dq^N/dp(1) \leq 1$, we establish that q^N attains a global maximum at $D = n/2$. When $D < n/2$ or $D > n/2$ one can easily show that respectively $dq^N/dp > 0$ and $dq^N/dp < 0$. □

Expression (5.34) uniquely determines the symmetric Nash equilibrium of the security game. Several economic forces present in the security game - under the strategic attack - manifest themselves in the expression. For instance, since it is pointless for an agent to discourage an attack when p is large, it is no surprise that q^N (as function of p) decreases at some point.

The increase in q^N when p is smaller than $D/2$ is hard to predict *a priori* from the model. Reason behind this increase can be found in a second order effect originating from the attacker. When p increases also the potential gain of an attack increases (as more documents - in expectation - are stored at each agent). This increase in potential gain causes the attacker to choose a more precise attack (the increase in costs is compensated by the increased expected gain). As agents are aware of this strategic behavior of the attacker, they in turn have incentives to invest more as they can more easily ward off an attack. These forces lead to the initial increase of q^N when p increases. Note however that when p continues to grow it become less and less beneficial to discourage an attack (as it is very likely that an agent's document is stored at another agent). This in turn leads to the eventual decrease in q^N.

Note however that the exact magnitude of several forces depend on p, the network structure and the cost functions c and ψ. Later - in section 5.8 - the role of these parameters on q^N is analyzed. In appendix section E a metaphor is given which lightens all the forces present under the strategic attack. From this metaphor it becomes more clear why q^N first increases in p.

Remind that the results in this section - and the discussion above - are based on the symmetric Nash equilibrium. As it is hard to formally prove that no asymmetric Nash equilibrium exists, we cannot extend results to the complete security game. Yet, when ψ is quadratic we are able to prove that no asymmetric Nash equilibrium exists. This results is showed in the next proposition.

Proposition 5.14. *When $\psi = \alpha a^2$ with $\alpha > 0$ and when c satisfies assumption 1, then the symmetric Nash equilibrium of the security game is the unique Nash equilibrium.*

Proof. The result is based on a result by Hefti (2011) stated in lemma A.3 on page 81. When all principal minors in the negated Jacobian of $(\frac{d\Pi_1}{dq_1}, \ldots, \frac{d\Pi_n}{dq_n})$ are positive, then the Nash equilibrium in symmetric games is unique.

To start with, note that when ψ is quadratic, the derivatives of $\mathbf{a}$ are showed in (5.20). In these derivatives $n^* = n$ as no agent holds a strategy such that $a_\nu = 0$ by proposition 5.12.

We continue by finding the second order derivatives of Π_ν when $\psi = \alpha a^2$. By differentiating (5.24) to q_ν,

$$\begin{aligned}\frac{d^2\Pi_\nu}{dq_\nu^2} &= 2\frac{da_\nu}{dq_\nu} - c''(q_\nu)\\ &= \frac{2-2n}{\alpha n}D - c''(q_\nu),\end{aligned}$$

where the first equality follows because second order derivatives of a_ν are zero by (5.20). Next, by differentiating (5.24) to q_μ:

$$\begin{aligned}\frac{d^2\Pi_\nu}{dq_\nu dq_\mu} &= \frac{da_\nu}{dq_\mu} + \frac{da_\mu}{dq_\nu} D_{\nu,\mu} \\ &= \frac{D}{\alpha n}(1 + D_{\nu,\mu}).\end{aligned}$$

Consequently the negated Jacobian becomes

$$-J = \begin{bmatrix} \frac{2n-2}{\alpha n} D + c''(q_1) & -\frac{D}{\alpha n}(1 + D_{1,2}) & \cdots & -\frac{D}{\alpha n}(1 + D_{1,n}) \\ -\frac{D}{\alpha n}(1 + D_{2,1}) & \frac{2n-2}{\alpha n} D + c''(q_2) & \cdots & -\frac{D}{\alpha n}(1 + D_{2,n}) \\ \vdots & \vdots & \ddots & \vdots \\ -\frac{D}{\alpha n}(1 + D_{n,1}) & -\frac{D}{\alpha n}(1 + D_{n,2}) & \cdots & \frac{2n-2}{cn} D + c''(q_n). \end{bmatrix}$$

Note that

$$\begin{aligned}\sum_{j \neq i} |-J_{i,j}| &= \sum_{j \neq i} \frac{D}{\alpha n}(1 + D_{i,j}) \\ &= \frac{D(n-1)}{\alpha n} + \frac{D(D-1)}{\alpha n} \\ &< \frac{D(n-1)}{\alpha n} + \frac{D(n-1)}{\alpha n} \\ &= D\frac{2n-1}{\alpha n} \;=\; J_{i,i},\end{aligned}$$

From which it follows that $-J$ is diagonally dominant. As $-J$ additionally features positive entries on its diagonal, we conclude that $-J$ is positive definite and all principal minors are positive. Now that Hefti's condition is satisfied we are able to conclude that there is a unique pure strategy Nash equilibrium. □

5.6 Optimal trade-off between security and costs

Perfect security is a delusion. Even if it was technically realizable, it would not be desirable as costs may outweigh security. This trade-off between security and costs is analyzed in this section.

We assume that an optimal trade-off between security and costs is social and such that agents cooperate to maximize their combined utility. Environments in which agents cooperate are quite common and can include an internal (company/family) network or a network in which an authority is responsible for security. In these examples an agent does not only invest to protect his own information (or document) but also invest to protect information of others. Specifically we assume that agents invest such that their combined utility, given by

$$\begin{aligned}S &= \sum_{\nu \in V} \Pi_\nu \\ &= n - \sum_{\nu} a_\nu [1 - q_\nu] D_\nu - c(q_\nu),\end{aligned} \tag{5.36}$$

is (globally) maximized in $[0,1] \times \cdots \times [0,1] = [0,1]^n$. Remind that the investment level $\mathbf{q}^s$ for which $S(\mathbf{q}^s)$ is maximized is denoted as the *social optimum*. Although existence of $\mathbf{q}^s$ follows easily by continuity of S and compactness of $[0,1]^n$, in this section focus lies on finding the exact value of $\mathbf{q}^s$ and proving that this social optimum is unique.

Specifically, first we show that no element in $\mathbf{q}^s$ is either 0 or 1. Informally this means that the social optimum is never such that an agent either invest maximally or invest nothing. This in turn implies that

the social optimum solves the first order condition for optimality (FOC), which makes it more tractable to find the social optimum. Next we show that there does not exists an asymmetric investment level which solves this FOC. Consequently, with this observation in mind, we find a symmetric social optimum and prove that this (symmetric) optimum is unique.

To start with, the next proposition makes sure that $\mathbf{q}^s$ solves the FOC.

Proposition 5.15. *In a vertex-transitive network where c satisfies assumption 1, the social optimum $\mathbf{q}^s$ solves for each agent ν*

$$c'(q_\nu^s) = a_\nu D - D \sum_\mu \frac{da_\mu}{dq_\nu}[1 - q_\mu^s]. \tag{5.37}$$

Proof. First we prove that no boundary maxima exist of S by showing that $\nabla(S)$ does not point outward at the boundary of $[0,1]^n$. More specific, we show that $\nabla(S(\{0, \mathbf{q}_{-\nu})) > 0$ and $\nabla(S(\{1, \mathbf{q}_{-\nu})) < 1$ independently of $\mathbf{q}_{-\nu}$. This result would indicate that the maximum (or maxima) of S necessarily solve the FOC of (5.36). This FOC is easily found by differentiating (5.36) and finding it's roots. This procedure leads to (5.37). In this derivation, remind that in a vertex-transitive network $D_\nu \equiv D$ for all ν.

To show that no boundary maxima exist, observe that when $0 \in \mathbf{q}$:

$$\begin{aligned}
\frac{dS}{dq_\nu}(\{0, \mathbf{q}_{-\nu}\}) &= a_\nu D - \frac{da_\nu}{dq_\nu} D - D \sum_{\mu \neq \nu} \frac{da_\mu}{dq_\nu}[1 - q_\mu] - c'(0) \\
&\geq a_\nu D - \frac{da_\nu}{dq_\nu} D - D \sum_{\mu \neq \nu} \frac{da_\mu}{dq_\nu} \\
&= a_\nu D - D \sum_\mu \frac{da_\mu}{dq_\nu} = a_\nu D \geq 0.
\end{aligned}$$

Alternatively when $1 \in \mathbf{q}$:

$$\begin{aligned}
\frac{dS}{dq_\nu}(\{1, \mathbf{q}_{-\nu}\}) &= a_\nu D - \sum_{\mu \neq \nu} \frac{da_\mu}{dq_\nu}[1 - q_\mu] D - c'(1) \\
&\leq - \sum_{\mu \neq \nu} \frac{da_\mu}{dq_\nu}[1 - q_\mu] D \leq 0,
\end{aligned}$$

where the first inequality follows because $a_\nu D - c'(1) \leq 0$. This inequality follows as $c'(1) \geq 1$ by assumption 1 and $a_\nu \leq 1/n$ because $q_\nu = 1$ is larger (or equal) than every element in $\mathbf{q}_{-\nu}$ and $2.$ in proposition 5.8 on page 47. □

Although proposition 5.15 provides some grasp on the social optimum, the terms relating to the strategy of the attacker ($\mathbf{a}$) make the solution (or solutions) of (5.37) hard to find. Nevertheless one can prove that the social optimum is not asymmetric by showing that (5.37) cannot be satisfied when $\mathbf{q}^s$ is asymmetric. The following proposition formally proofs this.

Proposition 5.16. *In the security game in a vertex-transitive network, under assumption 1 and assumption 2, there does not exists an asymmetric social optimum.*

Proof. Let $\mathbf{q}^s$ be an investment level which maximizes (5.36). Without loss of generality let $q_1 = \max \mathbf{q}^s$ and $q_2 = \min \mathbf{q}^s$ and assume that $q_1 > q_2$. Agree subsequently that $c'(q_1) > c'(q_2)$ by strict convexity of c and that, by using *2.* in proposition 5.8, $a_2 > a_1$. Next, as $\mathbf{q}^s$ solves (5.37) by proposition 5.15:

$$\begin{aligned}
c'(q_1) &= a_1 D - D \frac{da_1}{dq_1}(1 - q_1) - D \sum_{\nu \neq 1} \frac{da_\nu}{dq_1}(1 - q_\nu) \\
&= a_1 D + D \sum_{\nu \neq 1} \frac{da_\nu}{dq_1}(1 - q_1) - D \sum_{\nu \neq 1} \frac{da_\nu}{dq_1}(1 - q_\nu)
\end{aligned} \tag{5.38}$$

and similarly

$$c'(q_2) = a_2 D - D\frac{da_2}{dq_2}(1-q_2) - D\sum_{\nu\neq 2}\frac{da_\nu}{dq_2}(1-q_n u)$$
$$= a_2 D + D\sum_{\nu\neq 2}\frac{da_\nu}{dq_2}(1-q_2) - D\sum_{\nu\neq 2}\frac{da_\nu}{dq_2}(1-q_\nu). \tag{5.39}$$

Next we show that the RHS of (5.39) is larger than the RHS of (5.38). This would contradict the observation that $c'(q_1) > c'(q_2)$. Consequently $q_1 \not> q_2$ and hence $\min \mathbf{q}^s = \max \mathbf{q}^s$.

To prove that the RHS of (5.39) is larger than the RHS of (5.38), first note that $a_1 D < a_2 D$. Second, observe that as $0 \leq 1 - q_1 < 1 - q_\nu$ and $da_\nu/dq_1 \geq 0$ for all $\nu \neq 1$:

$$D\sum_{\nu\neq 1}\frac{da_\nu}{dq_1}(1-q_1) - D\sum_{\nu\neq 1}\frac{da_\nu}{dq_1}(1-q_\nu) < 0.$$

By a similar line of argument

$$D\sum_{\nu\neq 2}\frac{da_\nu}{dq_2}(1-q_2) - D\sum_{\nu\neq 2}\frac{da_\nu}{dq_2}(1-q_\nu) > 0.$$

□

The proposition above indicates that it is never socially optimal for an agent to invest more or less than others. Although this result is not completely unexpected in a vertex-transitive network where all agents are homogeneous, the result is not intuitive. For instance Bier *et al.* (2007) and Johnson *et al.* (2012) suggest that it might be optimal to leave some agents unprotected; making them sacrificing lambs. Beforehand one could argue that also in our setting this strategy can be optimal when p is low. This claim proves to be false however because of the increasing and convex costs for the attacker. Due to this it is not optimal for the attacker to focus the attack - with high probability - on the sacrificed lamb.

As no asymmetric social optimum exists, this section continues by exploring possible symmetric social optima. The next result shows that such symmetric social optimum exists and proves that the corresponding investment level is unique.

Theorem 5.2. *In a vertex-transitive network where c satisfies assumption 1 and ψ satisfies assumption 2, the social optimum q^s solves*

$$c(q^s) = \frac{D}{n}. \tag{5.40}$$

The solution $\mathbf{q}^s$ is the unique social optimum. Moreover $\mathbf{q}^s$ is continuous and increasing in p.

Proof. Suppose q^s is a symmetric social optimal investment level. Note that q^s necessarily solves the FOC in (5.37). Consequently, by substituting values, (5.40) is easily established:

$$c'(q^s_\nu) \;=\; \frac{D}{n} - D[1-q^s]\sum_\mu \frac{da_\mu}{dq_\nu} \;=\; \frac{D}{n}.$$

The second equation follows because the elements in $\mathbf{a}$ sum to one. Uniqueness of q^s follows easily by recognizing that the conditions in lemma A.1 on page 81 are satisfied.

To prove that S attains a maximum at $\mathbf{q}^s$ opposed to a minimum, remind that ∇S does not point outward at the boundary. When we combine this observation with uniqueness of the solution of the FOC, we are forced to conclude that S attains a maximum. That is, if S would attain a minimum at $\mathbf{q}^s$ then either ∇S points outward at the boundary or there are multiple solutions of the FOC.

Continuity in p follows easily by the implicit function theorem. Finally, as D is increasing in p by proposition 4.9 on page 29 also $\mathbf{q}^s$ is. □

The theorem above gives a very strong result. Independently of characteristics of the attacker, there is a unique social optimum which necessarily solves (5.40). Also note the resemblance with the result in proposition 5.3 on page 40 for the random attack. Apparently the social optimum under the random attack and under the strategic attack are equivalent.

5.7 Comparing the cooperative and the non-cooperative security game

Earlier results allow to compare security investments in a cooperative and a non-cooperative environment. In this section we focus on this comparison. We intent to determine if under-investments or over-investments prevail in equilibrium (non-cooperative game) relative to social optimum (cooperative game). Also benchmarking results under the random attack are included in the analysis. Table 3 gives a summary of characteristic equations which uniquely determine security investments.

Case	Necessary assumptions	Security investment solves
Random attack, Nash equilibrium **in proposition 5.2**	Assumption 1	$q_\nu^N = c'^{-1}(\frac{1}{n})$
Random attack, social optimum **in proposition 5.3**	Assumption 1	$q_\nu^s = c'^{-1}(\frac{D_\nu}{n})$
Strategic attack, Nash equilibrium, Symmetric investments **in theorem 5.1**	Assumption 1, assumption 2^+ and network is vertex-transitive	$q^N = c'^{-1}(\frac{1}{n} + \frac{[n-D]D}{n\psi''(\frac{1}{n})}[1-q^N])$
Strategic attack, social optimum **in theorem 5.2**	Assumption 1, assumption 2 and network is vertex-transitive.	$q^s = c'^{-1}(\frac{D}{n})$

Table 3 – *Summary of characteristic equations and necessary assumptions.*

We propose the following definition to adequately compare investment levels.

Definition 5. In the security game in a vertex transitive network where c satisfies assumption 1 and ψ satisfies assumption 2^+. Define q_r^N as the Nash equilibrium under the random attack. Similarly let q_s^N be the *symmetric* Nash equilibrium under the strategic attack. Also set q_s as the social optimum investment level[37].

The next proposition gives a complete classification of investment levels as introduced in definition 5.

Theorem 5.3. *The security investments outlined in definition 5 satisfy:*

1. *for all* $p \in [0,1]$
   (a) $q_r^N \leq q^s$,
   (b) $q_r^N \leq q_s^N$,
2. *there exists a unique* p^* *such that*
   (a) *if* $p = p^*$ *then* $q_s^N = q^s$,
   (b) *if* $p < p^*$ *then* $q_s^N > q^s$,

37. Note that neither q_r^N or q_s^N is a vector and consequently notation is slightly abused when saying that q_r^N or q_s^N is a Nash investment level, which has to be a vector. The notation is allowed here however because the Nash equilibrium is symmetric. Similarly, this notation is also applied to q^s as opposed to the formally correct $\mathbf{q}^s$. Lastly note that the notation q_r^s and q_s^s are unnecessary as the social optimum investment levels are equivalent under the random and the strategic attack

(c) if $p > p^*$ then $q_s^N < q^s$.
The value of p^* is the unique solution inside $[0, 1]$ of

$$\psi''(\frac{1}{n})\frac{D-1}{D} = [n-D][1-c'^{-1}(\frac{D}{n})]. \tag{5.41}$$

Proof. The results under *1.* follow directly by comparing characteristic equations in table 3 and using that c and ψ are strictly convex and $1 \leq D \leq n$. The results under *2.* require more explanation. However when $p = 0$:

$$c'(q^s) = \frac{D}{n} = \frac{1}{n} < \frac{1}{n} + \frac{n-1}{n\psi''(\frac{1}{n})}(1-q^N) = c'(q_s^N),$$

from which we conclude that $q_s^N > q^s$. Differently when $p = 1$, then $D = n$ and therefore

$$c'(q^s) = \frac{D}{n} = 1 > \frac{1}{n} = c'(q_s^N),$$

in turn proving that $q_s^N < q^s$. By continuity of both q^s and q_s^N in p it follows that there necessarily exists an intersection of q_s^N and q^s. To prove that this intersection is unique, note that in the intersection p^* is such that

$$\frac{D}{n} = \frac{1}{n} + \frac{[n-D]D}{n\psi''(\frac{1}{n})}[1-c'^{-1}(\frac{D}{n})].$$

This expression can subsequently be written as (5.41). Note that the LHS of (5.41) is strictly increasing in p, while - on the other side - the RHS is strictly decreasing in p. By applying lemma A.1 we conclude that p^* is unique. □

Theorem 5.3 can be seen as the main result in our research as it allows to compare several situations[38]. Most striking observation are the over-investments in Nash equilibrium relative to social optimum when p is low (see *2.(b)*). As discussed earlier, when p is low, investments in security are strategic complementaries; if one agent invests others will follow (to discourage an attack). Although this may lead to a more social optimal situation in some situations (e.g. following education), in this situation agents invest too much, leading to a less social optimal situation (e.g. an arms race).

The expression in (5.41) characterizes the point where over-investments turn into under-investments. The solution p^* is denoted as the *transition point* of the security game in this research. Note that this transition point is a function of the number of agents n, the expected number of documents obtained by each agent D (which in turn depends on p and the network structure) and the cost functions for both the agents and the attacker. In the next section the role of each parameter is analyzed rigorously. First however the following example illustrates the statements in theorem 5.3.

Example 5.4. Suppose an information network is complete and holds 5 agents who mutually share their documents. When agents incur a cost of $c = (1/2)q^2$ to hold investment level q and when the attacker incurs a cost of $\psi = (1/2)a_\nu^2$ for attacking agent ν with probability a_ν, figure 32 shows certain investment levels.

Observe that all statements in theorem 5.3 are illustrated in figure 32. Clearly the presence of a strategic attacker makes agents to invest more in security. Although this makes the network more secure, when p is low the network is too secure and benefits of risk-reduction do not compensate the increased costs.

Several things strike from the figure which are not mentioned in theorem 5.3 and in earlier results. First of all, when $p = 0$ the social optimum is the same as the equilibrium investments under the random

38. Prudence is called when applying theorem 5.3 to real world cases. As the utility of both agents and the attacker are independent of characteristics of the document, p or the network, investment levels can only be compared when the SAME document is considered. For instance one can cannot (directly) conclude from theorem 5.3 that PIN-codes are better secured than postal codes as p is lower in the first case.

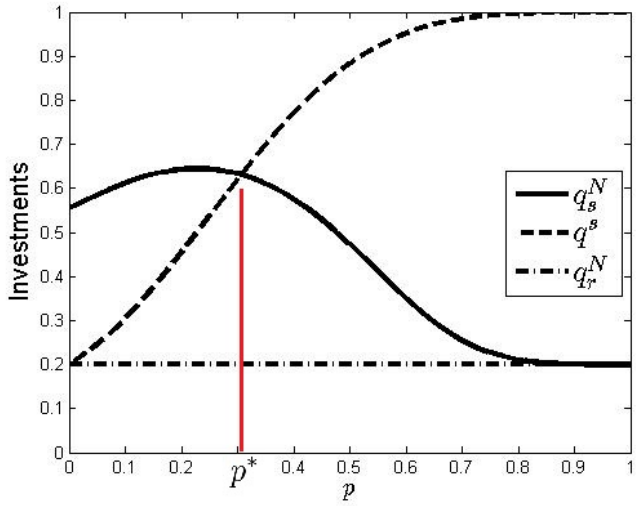

Figure 32 – *Security investments in K_5 where $\psi = a^2/2$ and $c = q^2/2$. As equilibrium investments q_s^N under the strategic attack are above equilibrium investments q_r^N under the random attack, a strategic attacker forces agents to invest more in security. Agents may even invest too much in security. Specifically, if $p < p^*$ then q_s^N features over-investments relative to the social optimum q^s. If $p > p^*$ then q_s^N features under-investments relative to q^s.*

attack. This of course follows mathematically but also economically as there is no external effect for an agent when $p = 0$. Consequently it is socially optimal to only protect one's own document against a direct attack; a similar incentive as in the random attack. Second observe that when $p = 1$, equilibrium investments under the random attack and the strategic attack are identical. This observation is motivated because when $p = 1$ an agent shares his document with everybody in the network. This in turn makes it pointless to discourage an attack, which in turn makes incentives under the strategic and the random attack equivalent.

Lastly note that also the statements in theorem 5.1 are visible in the figure. For instance q_s^N initially increases in p and consequently decreases in p. Also remind that q_s^N attains its global maximum when $D = n/2 = 2.5$. One can show that $p \approx 0.22$ in this case. Additionally, by working out (5.41) one can show that q_s^N and q^s intersect when $D \approx 3.15$. The value of p is approximately 0.3 in this case.

5.8 Dependency of investments on the network structure, cost functions and the number of agents

In this section we analyze the role of certain parameters on investments in security. The analysis combines earlier results in the security game (as summarized in table 3) but also includes results derived in chapter 4. First we analyze the role of the network structure and prove for instance that the transition point p^* in a circulant network always lies between p^* in a ring and p^* in a complete network. Next we analyze the role of certain costs functions on investment levels. Generally, when costs (both for agents and the attacker) increases, investments will decrease. Nevertheless, different than when the costs for the attacker increases, when the costs for agents increase the transition point will increase. Finally we analyze the role of the number of agents n on investments. We show for instance that the social optimum investment level converges to 0 in a ring and to $c'^{-1}(1)$ is a complete network.

5.8.1 Structure of the network

Investment levels highly depend on D; the expected number of documents obtained by each agent. In chapter 4 we derived several properties of D and provided a method to determine D exactly for a

complete and a ring network. When we combine these exact results with characteristic equations in table 3, investment levels can be derived for a ring and for a complete network. For instance when there are 6 agents in the security game, investment levels are as in figure 33.

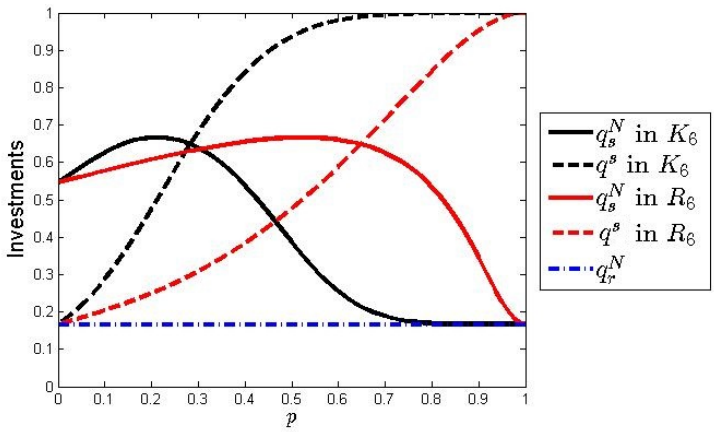

Figure 33 – *Security investments in a complete network on 6 nodes K_6 and in a ring network on 6 nodes R_6. Note that over-investments in equilibrium q_s^N relative to social optimum q^s prevail for a much wider space of p in a ring network than in a complete network. In the figure $c = (1/2)q^2$ and $\psi = (1/2)a^2$.*

Observe that earlier results derived on investment levels manifest themselves in figure 33. While over-investments prevail for a low value of p, for larger values of p under-investments prevail in equilibrium. Additionally observe that when p is low, equilibrium investments under the strategic attack are increasing in p. Earlier we motivated that this behavior originates because the attacker can do more damage when p is increasing.

When we compare investment levels in a complete and a ring network, we see that over-investments prevail for a much wider space of p in the ring network. This is no surprise as dependencies between agents are much lower in a ring network opposed to a complete network. When dependencies are low, there is more competition between agents as it is more beneficial to discourage an attack.

Also observe from figure 33 that equilibrium investments in a complete network can be larger than equilibrium investments in a ring network (solid black line is larger than solid red line when p is low). This may come as a surprise because one can argue that because dependencies are larger in a complete network, investments will be lower. Note however that because a strategic attacker can do more damage in a complete network, it is more beneficial for the attacker to choose a more precise attack vector. Consequently, as agents anticipate a more precise attack, investments will increase[39].

More generally it holds that in any circulant network with structure $\mathcal{S} \supset \{1\}$ (see definition 3 on page 31) there exists a value p where agents invest more than they would in any other circulant network with a similar number of agents and structure $\mathcal{S}^* \supset \{1\}$. This is showed, among two other results, in the next proposition.

Proposition 5.17. *Define $\mathcal{C}_n$ as the set of all (excluding isomorphisms) circulant networks on n nodes with structure $\mathcal{S} \supset \{1\}$. For some $\mathcal{G} \in \mathcal{C}_n$:*

1. *there exists an interval in p for which q_s^N in $\mathcal{G}$ is strictly larger than q_s^N in $\mathcal{H}$ for every $\mathcal{H} \in \mathcal{C}_n \setminus \mathcal{G}$,*
2. *for $\mathcal{H} \in \mathcal{C}_n \setminus \mathcal{G}$, if and only if $\mathcal{H} \subset \mathcal{G}$ then q^s in $\mathcal{G}$ is strictly larger than q^s in $\mathcal{H}$.*
3. *for $\mathcal{H} \in \mathcal{C}_n \setminus \mathcal{G}$, if and only if $\mathcal{H} \subset \mathcal{G}$ then the transition point p^* in $\mathcal{G}$ is strictly smaller then the transition point p^* in $\mathcal{H}$.*

39. Note that this is a similar argument which was used to motivate the initial increase of equilibrium investments q_s^N in p.

Proof. To prove result *1.* let $\overline{p}$ be such that $D^{\mathcal{G}} = n/2$. By theorem 5.1 it follows that q_s^N is globally maximized for this value of p. Next coordinates of this maximum can be found by substituting $D = n/2$ in (5.35) on page 53. It follows that these coordinates are $\{\overline{p}, \beta\}$ where β solves

$$c'(\beta) = \frac{1}{n} + \frac{n}{4\psi''(\frac{1}{n})}(1-\beta). \tag{5.42}$$

Note that β is independent of network structure[40].

Now suppose that there is some network $\mathcal{H} \in \mathcal{C} \setminus \mathcal{G}$ for which equilibrium investments are **a)** larger or **b)** equal than in $\mathcal{G}$ when $p = \overline{p}$. The case **a)** is excluded because the global maximum of equilibrium investment in $\mathcal{H}$ is also β. Additionally **b)** is excluded because it is not possible that equilibrium investments in $\mathcal{H}$ are globally maximized at $\overline{p}$. This follows because $\mathcal{H}$ is either a supergraph or a subgraph of $\mathcal{G}$, which implies that D is respectively more or less than $n/2$ by proposition 4.9 on page 29. Finally the existence of $\overline{p}$ can be extended to the existence of an interval $(\overline{p} - \epsilon_1, \overline{p} + \epsilon_2)$ by continuity of q_s^N.

Result *2.* follows easily by combining proposition 4.9 with the characteristic equation for q^s. As D is larger in $\mathcal{G}$ than in $\mathcal{H}$, the result follows by convexity of c.

Finally *3.* follows from inspection of (5.41). Remind that the unique solution of this equation is the transition point p^*. Note that the LHS of this expression is increasing in D, while the RHS is decreasing in D. Consequently, when D is higher in some network then necessarily the LHS and the RHS intersect each other for a smaller value of p. □

The first result in the proposition confirms earlier observations in the complete and the full network. Figure 33 indeed shows that there is some interval where equilibrium investment in the complete network are higher than in a ring network (and vice versa). The result indicates that this holds more generally for circulant networks (which are a supergraph of a ring). Hereby the result contradicts the initiative hypothesis that there always exists a network in which equilibrium investments are always (for every p) higher than in some other network. Apparently investments can not be bounded by investments in some other network[41].

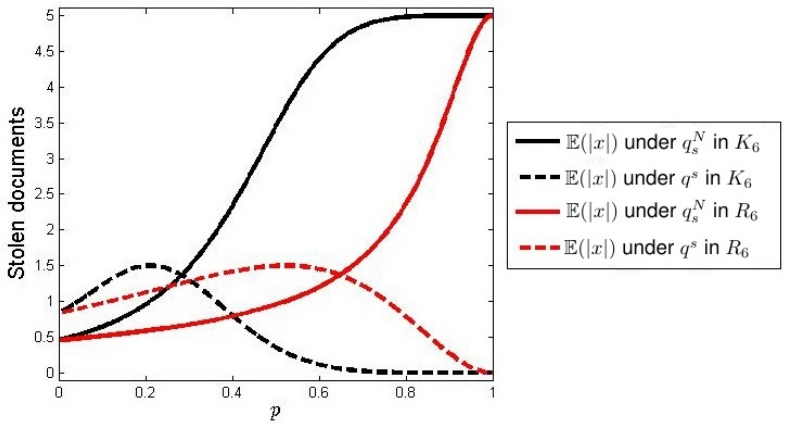

Figure 34 – *Expected number of documents $\mathbb{E}(|x|)$ stolen in a complete network on 6 nodes K_6 and in a ring network on 6 nodes R_6 under different investment levels. Note that $\mathbb{E}(|x|)$ is always lower in a ring than in a complete network in equilibrium q_s^N. Nevertheless $\mathbb{E}(|x|)$ can be higher in a ring than in a complete network in social optimum q^s.*

40. One can see this for instance in figure 33. Note that the maxima of the solid lines are equal. By solving (5.42) one can show that $\beta = 2/3$.
41. Yet one can show that investments are bounded above by β and bounded below by the *minimum*of 1) investments in a ring and 2) investments in a complete network.

Mind however that result *1.* does not imply that there always exists an interval for which a more dense network is *safer*[42] than a less dense network. One can see this in figure 34: there does not exists an interval in which the complete network is safer than the ring network in equilibrium (solid black line upper-bounds the solid red line).

Nevertheless figure 34 also indicates that the expected damage in a complete network can be lower than in a ring network when agents cooperate (dashed red line upper-bounds black dashed line for high p). The existence of such interval is hard to prove though and therefore we do not further explore this property.

Results *2.* and *3.* in proposition 5.17 may come 'unannounced' but are not difficult motivated. Result *2.* implies that the social optimum is always lower than the social optimum in a supergraph. In other words, if dependencies between agents are stronger then a higher social optimum is required. This implies for instance that the social optimum of a circulant network (with structure $\mathcal{S} \subset \{1\}$) always lies between the social optimum in the complete and in the ring network.

Result *3.* in proposition 5.17 shows that over-investments prevail for a wider space of p when dependencies are *lower*. This is in line with the idea that agents in particular compete for security when dependencies are low. Specifically result *3.* implies that the transition point of a circulant network (with structure $\mathcal{S} \subset \{1\}$) always lies between the transition point in a ring and the transition point in a complete network.

Summarizing the analysis above. For two circulant networks $\mathcal{C}_1$ and $\mathcal{C}_2$ which are supergraph of a ring network, if $D^{\mathcal{C}_1} > D^{\mathcal{C}_2}$ then,

- over-investments relative to social optimum prevail for a smaller space of p in $\mathcal{C}_1$ opposed to $\mathcal{C}_2$.
- Nevertheless, there exists an interval in which investments in $\mathcal{C}_1$ are larger than in $\mathcal{C}_2$.
- Yet, this does not imply that there always exists an interval in which $\mathcal{C}_1$ is more secure than $\mathcal{C}_2$.

5.8.2 Costs for agents

Also the cost functions play a role on investment in security. In this section we analyze the role of c, the cost agents incur for adopting security. In the next section we analyze the role of ψ, the cost the attacker incurs.

Intuitively, when costs to adopt security are higher, agents will invest less in security. This indeed shows to be the case in the security game.

Proposition 5.18. *When costs to invest are lower, investments in equilibrium and in the social optimum are higher.*

Proof. We say that costs to invest are lower when $c''(a)$ is lower for every a. When using this definition, c'^{-1} increases faster when costs are lower. In turn one can easily observe from the characteristic equations in table 3 that all investment levels will consequently decrease. □

Figure 35 confirms the proposition above in a complete network where costs to invest are respectively $(1/2)q^2$, q^2 and $2q^2$. Note that the solid black line upper-bounds the solid red line, which in turn upper-bounds the solid blue line. Investments indeed decrease when costs increase.

Another striking observation can be made from figure 35. When costs increase, the transition point seems to shift to the right (i.e. over-investments prevail for a wider range of p). Although this observation is easily confirmed by inspection of (5.41), the result does not come intuitively though. When costs are higher one would expect that over-investments prevail for a smaller space as it is less beneficial to invest. Yet the result follows because not only equilibrium investments q_s^N are decreasing when cost increase, also the social optimum q^s is decreasing. As the relative decrease of q^s is larger than the decrease of q_s^N for large values of p (observe this from figure 35), the intersection p^* will shift to the right.

42. In safer network the expected number of stolen documents, formally: $\mathbb{E}(|x|) = (1-q)D$, is lower.

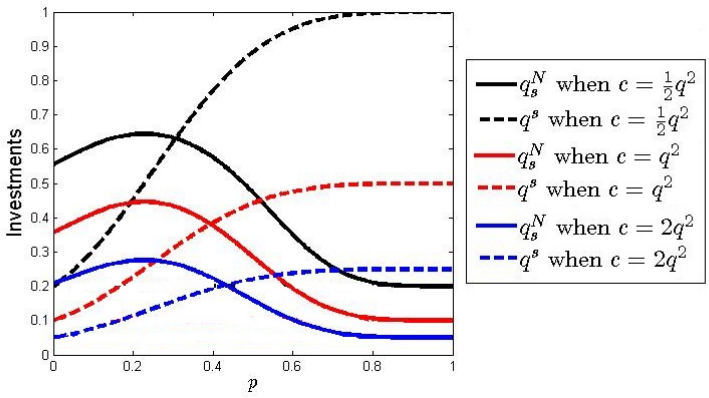

Figure 35 – *Investments in equilibrium q_s^N and social optimum q^s under different cost functions for agents in a complete network on 5 nodes. Observe that while investments decrease in c'', the transition point (intersection of solid and dashed lines) increases in c''. In the figure $\psi = \frac{1}{2}a^2$.*

Summarizing the analysis above:

- When costs to invest in security increase, investment levels decrease.
- Nevertheless, when costs increase, agents invest too much in equilibrium relative to the social optimum for a wider space of p.

5.8.3 Costs for the attacker

Also the costs for the attacker ψ influences behavior of agents. For instance when these costs are *lower*, the attacker has more resources to perform a more precise attack. As agents in turn anticipate a more precise attack, equilibrium investments under the strategic attack will increase. This result is formally presented in the next proposition.

Proposition 5.19. *When costs to attack are lower, equilibrium investments under the strategic attack are higher.*

Proof. Denote q_1 as the equilibrium investments when the cost to attack is ψ_1 and similarly q_2 as the equilibrium investments when the cost to attack is ψ_2. W.l.o.g. assume $\psi_1'' > \psi_2''$. Now suppose that $q_1 \geq q_2$ for some p. We will show that this assumption leads to a contradiction.

By theorem 5.1 on page 53 both q_1 and q_2 satisfy (5.34). Consequently by convexity of c is must hold that

$$\frac{1}{n} + \frac{(D-n)D}{n\psi_2''(\frac{1}{n})}(1-q_2) = c'(q_2) \leq c'(q_1) = \frac{1}{n} + \frac{(D-n)D}{n\psi_1''(\frac{1}{n})}(1-q_1).$$

By deleting identical terms it must hold that

$$\frac{1}{\psi_2''(\frac{1}{n})}(1-q_1+x) \leq \frac{1}{\psi_1''(\frac{1}{n})}(1-q_1),$$

where $x \geq 0$ is such that $q_2 = q_1 - x$. By rewriting it follows that it must hold that

$$\psi_1''(\frac{1}{n})(1-q_1+x) \leq \psi_2''(\frac{1}{n})(1-q_1),$$

and finally by rewriting once more

$$\psi_1''(\frac{1}{n}) - \psi_2''(\frac{1}{n}) \leq [\psi_1''(\frac{1}{n}) - \psi_2''(\frac{1}{n})]q_1 - \psi_1''(\frac{1}{n})x.$$

The expression above can only hold when $q_1 = 1$ (remind that $q_1 \in [0,1]$) and $x = 0$. Nevertheless by proposition 5.10 on page 48, q_1 can not be 1. This completes the proof (by contradiction). □

The result above is confirmed in figure 36. Note that equilibrium investments under the strategic attack indeed increase when costs to attack decrease. Additionally observe that the social optimum and the equilibrium investments under the random attack are unchanged. This follows because characteristic equations in these cases do not depend on ψ (see table 3). Also note that the black, red and blue lines attain there maximum at the same value of p. Surely, this necessarily holds as q_s^N attains its maximum at a value p^* where $D = n/2$. These parameters are unchanged in this situation.

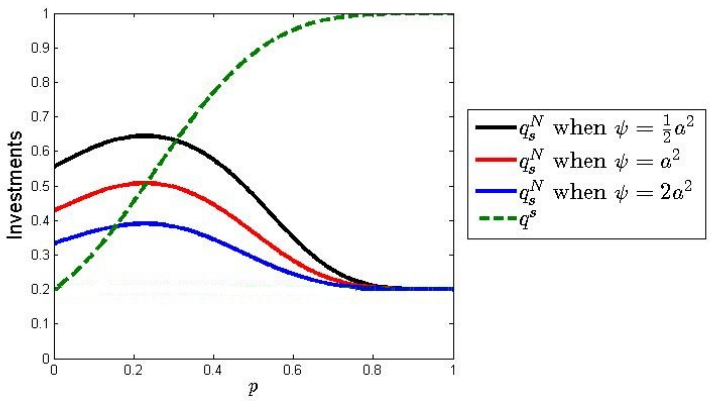

Figure 36 – *Investments in equilibrium q_s^N and social optimum q^s in a complete network on 5 nodes under different costs functions for the attacker. Observe that q_s^N increases when ψ decreases. Additionally, the transition point (intersection of solid lines and dashed line) increases when ψ decreases. In the figure $c = (1/2)q^2$.*

Finally, also observe from figure 36 that over-investments prevail for a wider space of p when costs for the attacker decrease (the transition point p^* moves to the right). This follows as q_s^N is increasing while the social optimum is unchanged when costs for the attacker decrease.

Summarizing, in this section we showed:

- when costs for the attacker increase, equilibrium investments under the strategic attack decrease while other investment levels remain unchanged.
- Additionally, when costs to attack increase, over-investments prevail for a smaller space of p.

5.8.4 Number of agents

Forces present in the security game can be reduced or enlarged when more agents are added to the network. One way, when there are more agents, the chance that documents are lost through other agents is generally increased. This leads to reduced incentives to invest in security. The other way, as it is usually more beneficial for the attacker to perform a more precise attack when there are more agents, competition increases and hence incentives to invest may also increase.

The exact change of incentive when more agents play the security game is difficult analyzed. Not only n in the characteristic equations in table 3 and equation (5.41) is changed, also D - as function of n - is changed. Consequently, to analyze the effect of a change in the number of agents, also knowledge about the evolution of D, D/n and $D(n-D)$ (as function of n) is required. Although we derived some exact results for the complete and the ring network in section 4.3.3 on page 32, the complexity forced us to base the analysis in other (circulant) network on simulation results. We therefore focus on the complete and the ring network in this section and leave the analysis for other networks as an open problem.

For a ring and a complete network we are capable of analyzing the (changed) incentives when agents are added to the network (while the structure remains the same). For the ring network this is showed in figure 37. Observe from the figure that the social optimum is decreasing in the number of agents. This

observation, which may come as a surprise as D is strictly increasing in n, follows from proposition 4.15 on page 33. As D/n is converging to 0 when n goes to infinity (the network becomes asymptotically large), also q^s is converging to 0 when n goes to infinity. Additionally observe from the figure that the transition point p^* moves to the right; i.e. over-investments prevail for a wider interval of p. As more agents are competing for security when n increases, this result comes naturally[43].

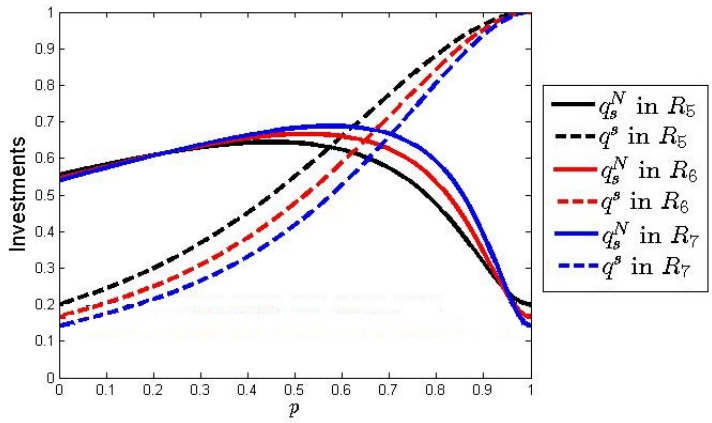

Figure 37 – *Social optimum q^s and equilibrium q_s^N investments in ring networks with 5, 6 and 7 agents. Recognize that while q^s decreases in n, q_s^N might as well increase in n. Additionally note that the transition point where over-investments of q_s^N relative to q^s pass on to under-investments is also increasing in n. In the figure $c = (1/2)q^2$ and $\psi = (1/2)a^2$.*

Figure 38 features investments in a complete network for $n = 5$, $n = 6$ and $n = 7$. Observe that, opposed to a ring network, the transition point in a complete network moves to the left when n is increasing. Apparently a complete network becomes 'too dense' when agents are added, which makes it less and less beneficial to discourage an attack. Note that the behavior in a ring is opposite. A ring becomes 'too sparsely' connected when agents are added, which in turn makes it more and more beneficial to discourage an attack.

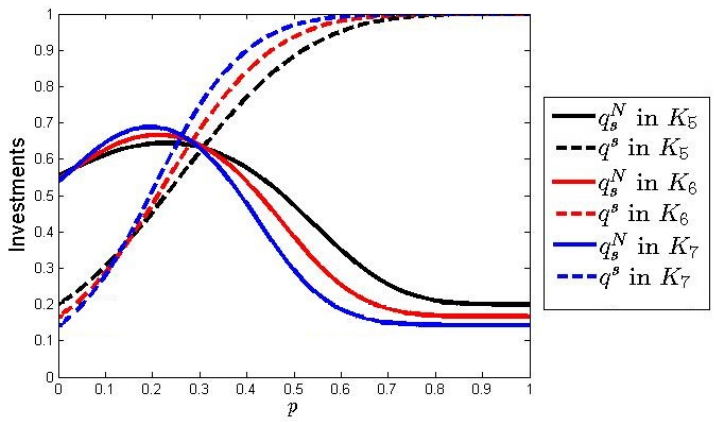

Figure 38 – *Social optimum q^s and equilibrium q_s^N investments in complete networks with 5, 6 and 7 agents. Note that the transition point where q^s and q_s^N intersect is decreasing in n. This behavior is opposite to the behavior in a ring as showed in figure 37. In this figure $c = (1/2)q^2$ and $\psi = (1/2)a^2$.*

Additionally remind from section 5.8.1 that the transition point in a circulant network always lies between

43. Yet mathematically it is hard to prove that p^* increases in n from equation (5.41). When we solve (5.41) for D when ψ and c are quadratic, the solution behaves like $n - \log(n)$. This implies for instance that p^*, although close to 1, does not converge to 1.

the transition point in a ring and a complete network. As these transition points in a complete and a ring are moving 'away' from each other, the space in which the transition point of a circulant network lies is strictly increasing in n. More research is required to explore the effects of an increase in n on the transition point in a circulant network.

Finally also observe from figure 38 that the social optimum converges to 1. In fact one can formally show that q^s is converging to 1 in this case; a result which follows easily from from proposition 4.16 on page 33. As D/n converges to 1, q^s necessarily converges to $c^{-1}(1) \leq 1$.

In this section we highlighted that

- the effect of a change in the number of agents is hard to analyze as more properties of D are required.
- However we were able to show that the social optimum converges to 0 in a ring network and converges to $c'^{-1}(1)$ in a complete network,
- and we conjectured that the transition point in a ring is strictly increasing, while the transition point in a ring is strictly decreasing.

6 The security game with several components

In many real world situations the information network consists of several individual networks. For instance a strategic decision often only spreads under employees of a firm or for instance bank-account information generally only spreads in the network of the specific bank. An attacker can focus his attack on one network in particular as he or she can write malicious software for a specific platform or can focus a phishing attack on employees of one bank in particular. In this section we consider this situation where the attacker can choose between several networks. We will call these individual networks *components*.

We focus once more on endogenous security where agents invest in security. Additionally, we introduce a new attack form: the *strategic-random attack*. Under this attack, the attacker strategically determines which component is attacked, but cannot specify which agent inside this component is attacked. In this chapter we first extend our model to allow such strategic-random attack. Next we establish characteristic equations from which we can find the Nash equilibrium and the social optimum. Subsequently we compare these outcomes with result of the (full) strategic and the (full) random attack as derived in the previous chapter.

6.1 Extension to the model and assumptions

Some small changes are required to the model in chapter 3 to investigate the behavior of agents inside a component. In this chapter we will investigate the behavior of nm agents in network $\mathcal{G}$. We assume that the set of agents is partitioned[44] in m *components* such that $V(\mathcal{G}) = \{V_1 \cup \cdots \cup V_m\}$. A component is defined as $C_i = (V_i, A_i)$ where A_i is the adjacency matrix of $\mathcal{G}$ restricted to the subset V_i. We assume that each component contains a same number of agents n. Agents inside each component share information with each other, but do not share information with agents outside the components (i.e. no edges exist which link two agents who are not in the same component). In this section we assume that each component attain the same vertex-transitive structure. By a slight extension of proposition 4.11 on page 30, we conclude that network $\mathcal{G}$ is vertex-transitive.

An example of a network with 3 components in showed in figure 39. In this figure each component holds 5 agents and attains a complete structure. Note that information never spreads among agents in different components.

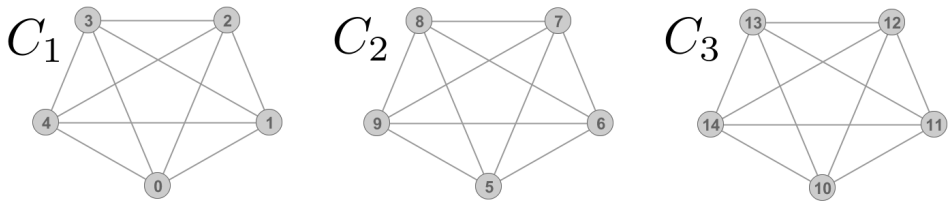

Figure 39 – *A network $\mathcal{G} = \{C_1, C_2, C_3\}$ with 3 components. In this chapter we consider cases where each component attains the same vertex-transitive structure and holds an identical number of agents. This implies that network $\mathcal{G}$ is vertex-transitive.*

Spreading happens - similarly as before - according to bond percolation with probability p. We assume that this probability p is exogenous and identical in each component. Consequently, as no heterogeneity exists between agents in different components:

$$D^{\mathcal{G}} \equiv D^{C_i} \text{ for every } i.$$

Remind that D are the expected number of documents obtained by each agent. As each C_i is vertex-transitive we - once more - adopt the notation D for D^{C_i}.

44. A partition of a set X are sets $X_1, \ldots X_n$ such that $X_1 \cup \cdots \cup X_n = X$ and $X_i \cap X_j = \emptyset$ for all combinations of i and j.

Note that we are still allowed to use the characteristic equations in table 3 on page 58 as the network is vertex-transitive. Later in this chapter we will use these equations to compare the (full) strategic attack and the (full) random attack with the strategic-random attack.

Next we present some new notations which we will use. We denote the probability that component i is attacked by the attacker as b_i. Again $\mathbf{b} = \{b_1, \ldots, b_m\}$ is a probability vector and the realization of the attack is modeled as a random variable drawn from $\mathbf{b}$. We adopt the notation $\overline{q}_i$ to denote the average security investments in component i. When an agent ν lies in component i, we might as well denote the component as $C(\nu)$.

Through this section we adopt assumption 1 on the cost function c. Remind that agents incur a cost of $c(q)$ for investing q in security. The attacker, on the other side, will incur a cost of $\psi(b_i)$ for attacking component i with probability b_i. In this section we consider quadratic costs for the attacker:

$$\psi' = \alpha b,$$

for some $\alpha > 0$. Note that ψ satisfies assumption 2$^+$ as in the previous chapter.

6.2 The strategic-random attack

In this section we discuss the strategic-random attack and derive characteristic equations from which the Nash equilibrium and the social optimum can be solved. As these derivations are generally in line with those in the previous chapter, the reasoning in this section is not always thorough and we often refer to similar proofs in chapter 5.

6.2.1 Incentives of the strategic-random attacker

We start the discussion on the attacker who performs a strategic-random attack. Following (3.7), the utility of the attacker under this attack form becomes:

$$\begin{aligned} U_a &= \mathbb{E}(|x| \; |\mathbf{q}) - \sum_i \psi(b_i) \\ &= \sum_i^m b_i \mathbb{E}(\text{expected number of documents obtained} \mid \text{attack on component } i) - \sum_i \psi(b_i) \\ &= \sum_{i=1}^m b_i [\sum_{\nu \in C_i} \frac{D}{n}(1 - q_\nu)] - \psi(b_i) \\ &= \sum_{i=1}^m b_i (1 - \overline{q}_i) D - \psi(b_i), \end{aligned} \tag{6.1}$$

where $\overline{q}_i$ is known to the attacker[45] for all i. Note that the strategy of the attacker follows from the average investment level in each component.

A clear similarity exists between (5.9), the utility of the attacker in the original security game and (6.1). Only difference is the diluted effect of an individual action of an agent. Yet, this difference does not impede that properties of the strategic attacker can be extended to the strategic-random attacker. Most relevant properties are stated in the next proposition.

Proposition 6.1. *Under the strategic-random attack the probability that component i is attacked is*

$$b_i = \max\{0, \; \frac{D}{\alpha n}(1 - \overline{q}_i) + \frac{\lambda}{\alpha} \}, \tag{6.2}$$

where $\lambda \in \mathbb{R}$ is the unique solution of

$$\sum_i \max\{0, \; \frac{D}{\alpha n}(1 - \overline{q}_i) + \frac{\lambda}{\alpha} \} = 1.$$

45. Also in this chapter we consider a sequential game where the attacker determines his strategy after agents choose theirs.

The derivative of b_i to q_ν for $\nu \in C_i$ and to q_μ for $\mu \notin C_i$ is given respectively by

$$\frac{db_i}{dq_\nu} = \frac{1-m^*}{\alpha n m^*} D \quad \text{and} \quad \frac{db_i}{dq_\mu} = \frac{D}{\alpha n m^*}, \tag{6.3}$$

where m^* are the number of components that have strict positive probability of being attacked.

Proof. Both (6.2) and (6.3) follow from Kuhn-Tucker conditions. As the required steps are similar as in proposition 5.4 on page 42 and proposition 5.6 on page 45, we omit a formal proof to economize on space. □

6.2.2 Equilibrium of the non-cooperative game

Now that we have established the strategy of the attacker, we can focus our analysis on the strategy of agents. Note that the utility of - say agent ν - is given by

$$\Pi_\nu = 1 - b_{C(\nu)}[\sum_{\mu \in C(\nu)} \frac{1}{n}(1-q_\mu)D_{\nu,\mu}] - c(q_\nu), \tag{6.4}$$

where $C(\nu)$ is the component in which ν lies. We assume that each agent plays the best response of Π_ν given $\mathbf{q}_{-\nu}$. As each agent determines this best response anticipating the strategy of the attacker, we substitute the solution b_i of (6.2) in (6.4). Consequently, a similar approach as in section 5.5 leads us to the following proposition.

Proposition 6.2. *In the security game in network $\mathcal{G} = \{C_1 \cup \cdots \cup C_m\}$ where all C_i attain the same vertex-transitive structure and each C_i holds n agents. If c satisfies assumption 1 and $\psi = \alpha b^2$, under the strategic-random attack the symmetric pure strategy Nash equilibrium $\mathbf{q}^\mathbf{N}$ solves*

$$c'(q^N) = \frac{1}{nm} + \frac{m-1}{\alpha m n^2} D^2 (1-q^N). \tag{6.5}$$

The solution $\mathbf{q}^\mathbf{N}$ is unique, continuous and strictly increasing in D (and thus in p).

Proof. The result is established in several steps. These steps are identical as in chapter 5.5 and therefore somewhat shortened in this proof. First we prove that a symmetric pure strategy Nash equilibrium exists by showing that the conditions of Debreu in lemma A.2 on page 81 are satisfied. Next we prove that this symmetric pure strategy Nash equilibrium solves the FOC of (6.4). This FOC consequently leads to the characteristic equation in (6.5). Finally we promptly discuss the steps required to show that $\mathbf{q}^N$ is unique, continuous and strictly increasing.

We start by proving that a symmetric pure strategy Nash equilibrium exists. For this, suppose that all agents other than agent ν play strategy $\mathbf{q}^*$. Continuity of Π_ν in $\mathbf{q}^*$ follows by a similar line of argument as in proposition 5.9 on page 47. We omit this proof to economize on space. To prove that Π_ν is quasi-concave in q_ν, note that the derivative of (6.4) is given by

$$\frac{d\Pi_\nu}{dq_\nu} = \frac{b_{C(\nu)}}{n} - \frac{db_{C(\nu)}}{dq_\nu}[\sum_{\mu \in C(\nu)} \frac{1}{n}(1-q_\mu)D_{\nu,\mu}] - c'(q_\nu). \tag{6.6}$$

By differentiating this expression once more, it follows that

$$\frac{d^2\Pi_\nu}{dq_\nu^2} = \frac{2}{n}\frac{db_{C(\nu)}}{dq_\nu} - \frac{d^2 b_{C(\nu)}}{dq_\nu^2}[\sum_{\mu \in C(\nu)} \frac{1}{n}(1-q_\mu)D_{\nu,\mu}] - c''(q_\nu). \tag{6.7}$$

By noting from (6.3) that $db_{C(\nu)}/dq_\nu \leq 0$ and $db^2_{C(\nu)}/dq_\nu^2 = 0$, it easily follows that $\frac{d^2\Pi_\nu}{dq_\nu^2} \leq 0$. We conclude that a symmetric pure strategy Nash equilibrium exists.

Next we prove that an agent's best response $\varphi(\mathbf{q}_{-\nu})$ always solves the FOC of (6.4) given $\mathbf{q}_{-\nu}$. By noting that independently of the strategy of other agents,

$$\frac{d\Pi_\nu}{dq_\nu}(0) > 0$$

and that $\Pi_\nu(1) < \Pi_\nu(0)$, we conclude that the global maximum of Π_ν necessarily solves the FOC. Additionally it is easy to show that an agent's best response is never such that $b_i = 0$ or $b_i = 1$. The proof is similar as proposition 5.12 on page 50.

Finally we establish equation (6.5). For this, suppose that $\mathbf{q}^N$ is the *symmetric* pure strategy Nash equilibrium. As $\mathbf{q}^N$ is symmetric it follows from (6.2) that every component is attacked with an identical probability of $1/m$. Consequently by substituting (6.3) in (6.6), the FOC becomes

$$c'(q^N) = \frac{1}{nm} + [\frac{m-1}{\alpha nm}D][\frac{1}{n}(1-q^N)D].$$

The RHS of this expression is readily written as the RHS of (6.5) in the proposition.

By noting that the LHS of (6.5) is strictly increasing while the RHS is strictly decreasing in q^N, it follows that there is a unique solution of (6.5). This in turn implies that $\mathbf{q}^N$ is the global maximum and that $\mathbf{q}^N$ is the unique symmetric Nash equilibrium. Continuity follows from the implicit function theorem and $\mathbf{q}^N$ is strictly increasing because one easily checks that the derivative of $\mathbf{q}^N$ to D is strictly positive. □

Note that the proposition above does not say anything about the uniqueness of the Nash equilibrium. Although the symmetric equilibrium is unique, the equilibrium itself might not be unique. In line with proposition 5.14 on page 54 we tried to use Hefti (2011) to show that the equilibrium is unique. From these derivations (not showed in this report) we conclude that the Nash equilibrium under the strategic-random attack is unique when c'' is sufficiently large.

6.2.3 Optimal trade-off between security and costs

Next we focus on the social optimum under the strategic-random attack. Remind that the social optimum is the optimal trade-off between security and costs from a social perspective. Specifically, the social optimum is an investment level such that the social utility

$$S = \sum_\nu \Pi_\nu,$$

is maximized in $[0,1]^{nm}$. By substituting (6.4), this social utility can be written as

$$\begin{aligned}
S &= \sum_\nu [1 - b_{C(\nu)}[\sum_{\mu \in C(\nu)} \frac{1}{n}(1-q_\mu)D_{\nu,\mu}] - c(q_\nu)] \\
&= nm - \sum_\nu \sum_{\mu \in C(\nu)} \frac{b_{C(\nu)}}{n}(1-q_\mu)D_{\nu,\mu} - c(q_\nu) \\
&= nm - \sum_\nu \sum_\mu \frac{b_{C(\mu)}}{n}(1-q_\mu)D_{\nu,\mu} - c(q_\nu) \\
&= nm - D\sum_\mu \frac{b_{C(\mu)}}{n}(1-q_\mu) - c(q_\mu) \\
&= nm - D\sum_i b_i(1-\overline{q}_i) - \sum_\mu c(q_\mu) \qquad (6.8)
\end{aligned}$$

where the third equality follows because $D_{\nu,\mu} = 0$ for $\mu \notin C(\nu)$. The fourth equality follows by a change in the order of the summation signs and because $D_{\nu,\mu} = D_{\mu,\nu}$ as our network is undirected.

The next proposition shows that the social optimum is unique, symmetric and solves (6.9).

Proposition 6.3. *In the security game in network $\mathcal{G} = \{C_1 \cup \cdots \cup C_m\}$ where all C_i attain the same vertex-transitive structure and each C_i holds n agents, suppose that c satisfies assumption 1 and $\psi = \alpha b^2$. When the social optimum under the strategic-random attack solves the first order condition of (6.8) then it is the unique solution of*

$$c'(q^s) = \frac{D}{nm}. \tag{6.9}$$

When the conditions are satisfied, the solution $\mathbf{q}^s$ is the unique social optimum which is strictly increasing and continuous in D (and thus in p).

Proof. First note that we require that the social optimum solves the FOC of (6.8). This technical requirement excludes the possibility that a boundary social optimum exists. Although we tried to present this proposition without this extra assumption, we were unable to do so in a limited amount of time[46].

In this proof we first show that the social optimum is not asymmetric, provided that it is not on the boundary of $[0,1]^{nm}$. Next we show that there is a unique symmetric social optimum.

First note that the derivative of S in (6.8) is given by

$$\begin{aligned}\frac{dS}{dq_\nu} &= \frac{Db_{C(\nu)}}{n} - D\sum_\mu \frac{db_{C(\mu)}}{dq_\nu}\frac{1}{n}(1-q_\mu) - c'(q_\nu) \\ &= \frac{Db_{C(\nu)}}{n} - D^2\frac{1-m*}{\alpha n m^*}(1-\overline{q}_i) - \sum_{j\neq C(\nu)} D^2\frac{1}{\alpha n m^*}(1-\overline{q}_j) - c'(q_\nu),\end{aligned} \tag{6.10}$$

where m^* are the number of components that have strict positive probability of being attacked.

Next we easily establish that all agents inside the same component hold an identical strategy. This follows because all terms in (6.10) are the same for agents inside the same component. Consequently, agents inside the same component hold an identical strategy equal to $\overline{q}_i^s$.

Consequently we show that $\overline{\mathbf{q}}^s = \{\overline{q}_1^s, \ldots, \overline{q}_n^s\}$ is symmetric. For this, w.l.o.g. suppose that $\overline{q}_1^s = \min\{\overline{\mathbf{q}}^s\}$ and $\overline{q}_2^s = \max\{\overline{\mathbf{q}}^s\}$. We show that the assumption $\overline{q}_1^s < \overline{q}_2^s$ leads to a contradiction. As both $\overline{q}_1^s$ and $\overline{q}_2^s$ solve the root of (6.10), necessarily

$$c'(\overline{q}_1^s) = \frac{Db_1}{n} - D^2\frac{1-m*}{\alpha n m^*}(1-\overline{q}_1) - D^2\frac{1}{\alpha n m^*}(1-\overline{q}_2) - \sum_{j\neq\{1,2\}} D^2\frac{1}{\alpha n m^*}(1-\overline{q}_j) \tag{6.11}$$

and

$$c'(\overline{q}_2^s) = \frac{Db_2}{n} - D^2\frac{1-m*}{\alpha n m^*}(1-\overline{q}_2) - D^2\frac{1}{\alpha n m^*}(1-\overline{q}_1) - \sum_{j\neq\{1,2\}} D^2\frac{1}{\alpha n m^*}(1-\overline{q}_j). \tag{6.12}$$

Next note that our assumption $\overline{q}_1^s < \overline{q}_2^s$ implies that $(1-\overline{q}_1) > (1-\overline{q}_2)$ and that $b_1 > b_2$ by (6.2). When comparing similar terms in (6.11) and (6.12) it follows that the RHS of (6.11) is larger than the RHS of (6.12). As this contradicts convexity of c, we conclude that $\overline{q}_1^s = \overline{q}_2^s$.

Now that we have established that all agents play the same strategy, we focus on finding a symmetric root of (6.10). When all agents play the same strategy q^s, expression (6.10) is reduced to

$$\begin{aligned}\frac{dS}{dq_\nu} &= \frac{D}{mn} - D(1-q^s)\sum_i \frac{db_i}{dq_\nu} - c'(q^s) \\ &= \frac{D}{mn} - c'(q^s),\end{aligned} \tag{6.13}$$

46. We tried two approaches. First, similar as in proposition 5.15, we tried to show that $dS/dq_\nu(0) \geq 0$ and $dS/dq_\nu(1) \leq 0$. This approach failed however as the effect of $q_\nu = 0$ on $\overline{q}_{C(\nu)} = 0$ is unclear. Second, we tried to show that the Hessian is negative definite for all values in $[0,1]^{nm}$. This showed to be the case if $m^* = m$ (remind that m^* are the number of components with strict positive probability of being attacked). Currently we are unable to show this.

as one easily shows that $\sum_i db_i/dq_\nu = 0$.

Clearly the root of (6.13) above is the solution of (6.9). As the LHS of (6.9) is increasing in q^s while the RHS is constant, there is in fact a unique solution of (6.9). Continuity of the solution of (6.9) follows easily by the implicit function theorem. Finally, q^s is strictly increasing in p because D is by proposition 4.9 on page 29. □

As a final comment, note that the social optimum under the strategic-random attack is - once more - equivalent with the social optimum under the strategic and the random attack (see table 3 on page 58).

6.3 Comparison of different attack forms

In this section we compare investment levels under the strategic-random attack with investment under the strategic and under the random attack. Additionally we present some examples of investment levels under these different attack forms.

To adequately compare our results, first note that we are (still) allowed to use the characteristic equations in table 3 on page 58 for the strategic and the random attack. As these equations are in the same form as (6.5) and (6.9) investment levels are readily compared. Yet, for an efficient comparison we first propose some small (notational) adjustments.

Definition 6. In the security game in network $\mathcal{G} = \{C_1 \cup \cdots \cup C_m\}$ where all C_i attain the same vertex-transitive structure and each C_i holds n agents. If c satisfies assumption 1 and $\psi = \alpha b^2$ for $\alpha > 0$, define q_{sr}^N as the symmetric investment level under the strategic-random attack that is a pure strategy Nash equilibrium. The investment levels q_s^N, q_r^N and q^s are similarly defined as in definition 5 on page 58 only with network $\mathcal{G} = \{C_1 \cup \cdots \cup C_m\}$.

Also remind that we consider behavior of a total of nm agents in this chapter. Consequently n in table 3 is changed to nm in this chapter and D is changed to the expected number of documents obtained by each agent when there are n agents (remind that there are n agents inside a component).

By comparing all investment levels we derive the following results[47].

Proposition 6.4. *Under investment levels defined in definition 6:*

- *for all $p \in [0,1]$, $q_r^N \leq q_{sr}^N < q_s^N$,*
- *q_{sr}^N, q_s^N and q^s are all increasing in p and increasing in the density of the network.*

Proof. The property $q_r^N \leq q_{sr}^N$ follows easily by comparing (6.5) with the characteristic equation for q_r^N in table 3. To prove that $q_{sr}^N < q_s^N$, suppose that there is a p^* for which $q_{sr}^N = q_s^N$. From the characteristic equations it follows that p^* is such that

$$\frac{m-1}{\alpha m n^2} D^2 = \frac{(nm - D)D}{\alpha n m}$$

By removing terms, p^* is such that

$$\frac{m-1}{n} D = nm - D,$$

which consequently implies that p^* is such that

$$D = \frac{n^2 m}{n + m - 1}.$$

Next we show that such p^* does not exists because $\max_{p \in [0,1]} D = n$. For this we have to show that

$$\frac{nm}{n + m - 1} > 1.$$

47. This comparison is not exhaustive and several other interesting comparisons would be possible. Especially a comparison between equilibrium investments and the social optimum and an investigation on their possible intersections would be interesting.

As $nm \geq n + m$ for all $n \geq 2$ and $m \geq 2$ this expression above clearly holds. Nonexistence of a p^* for which $q_{sr}^N = q_s^N$ implies that either $q_{sr}^N > q_s^N$ or $q_{sr}^N < q_s^N$. As we easily prove that $q_{sr}^N < q_s^N$ when $p = 0$, we are consequently allowed to extend this property for all values of p.

To prove the second result in the theorem we start with q_s^N; the Nash equilibrium under the strategic attack. Remind that q_s^N is increasing in p till the (unique) point where $D = nm/2$ by theorem 5.1 on page 53. As $\max_{p\in[0,1]} D = n$ and $m \geq 2$ in this chapter, we conclude that q_s^N is increasing in p. Consequently as D is a strictly increasing function of p, this immediately implies that q_s^N is increasing in D. Finally because D in a more dense network is larger for all p then D in a less dense network by proposition 4.9 on page 29, the result follows.

To establish that q_{sr}^N is increasing in D, Let $\mathcal{G}_1$ and $\mathcal{G}_2$ be two networks for which respectively $D_1 > D_2$ for all p (other parameters are similar in both networks). We will show that equilibrium investments in $\mathcal{G}_1$ are larger than in $\mathcal{G}_2$. For this, assume the contrary that there is a p^* for which $\overline{q}_{sr}^N > q_{sr}^N$ where $\overline{q}_{sr}^N$ is the investment level in $\mathcal{G}_2$. By convexity of c is must hold that

$$\frac{m-1}{\alpha mn^2} D_2^2 (1 - \overline{q}_{sr}^N) > \frac{m-1}{\alpha mn^2} D_1^2 (1 - q_{sr}^N).$$

This expression clearly does not hold as $D_2^2 < D_1^2$ and $(1 - \overline{q}_{sr}^N) < (1 - q_{sr}^N)$. Consequently, by contradiction, we proved that equilibrium investments in a denser network are higher for all values of p. Moreover, as D is a strictly in p, we are allowed to extend the result to p.

The result for q^s follows easily by considering equation (6.9). By convexity of c the social optimum necessarily increases when D does. □

The first result in the proposition above is no surprise. The level of competition created under the strategic-random attack clearly falls between the level of competition created under the random attack and the strategic attack. Hence also investments under the strategic-random attack fall between the other two attack forms. This result once again confirms that the introduction of a strategic component in the attack leads to more investments in security. Yet, note that the exact investment level depends on the parameters α, c'', n and m. We do not explore the role of these parameters in this research.

Different than the first result in proposition 6.4, the second result does come as a surprise. Remind that we derived in the previous chapter that equilibrium investments eventually decrease in p when there is one component (see figure 32 for instance). This decrease was motivated by the observation that when p increases - with high probability - all agents obtain the document of an agent. This in turn makes it pointless to invest to cause the attacker to attack someone else. Contrary, when there is more than one component there are always agents who do not obtain the document of an agent (remind that D converges to n opposed to nm when p goes to 1). In this case, agents always have incentives to discourage an attack.

We end the analysis in this chapter with some examples of investment levels. In the examples $\mathcal{G}_{n,m}$ represents a network with m components where each component attains the structure of $\mathcal{G}$ and holds n agents.

First, figure 40 shows investments in a network with four complete components all with four agents (solid lines), and investments in a network with four ring components also with four agents (dashed lines). Note that investment indeed increase in p and in the density of the network as proved in proposition 6.4. The increase in p seems to be faster under the random-strategic attack than under the strategic attack[48]. Finally also observe from figure 40 that for all values of p over-investments exist under the strategic and under the strategic-random attack relative to the social optimum. We do not further explore this property due to a limited amount of time.

48. This is no surprise because under the strategic-random attack the attack inside a component is random and therefore no competition inside a component exists. If there would be any competition inside a component, then equilibrium investments eventually decrease in p as it becomes more and more likely that other agents obtain your document.

Figure 41 shows a possible effect when the number of agents inside a component are reduced. Although equilibrium investments under the strategic attack decrease, the effect under the strategic-random attack is not so clear: for small and high values of p equilibrium investments increase. This effect is also observed on the equilibrium investments in figure 42 when we decrease the number of components. Once more we do not further explore these observations.

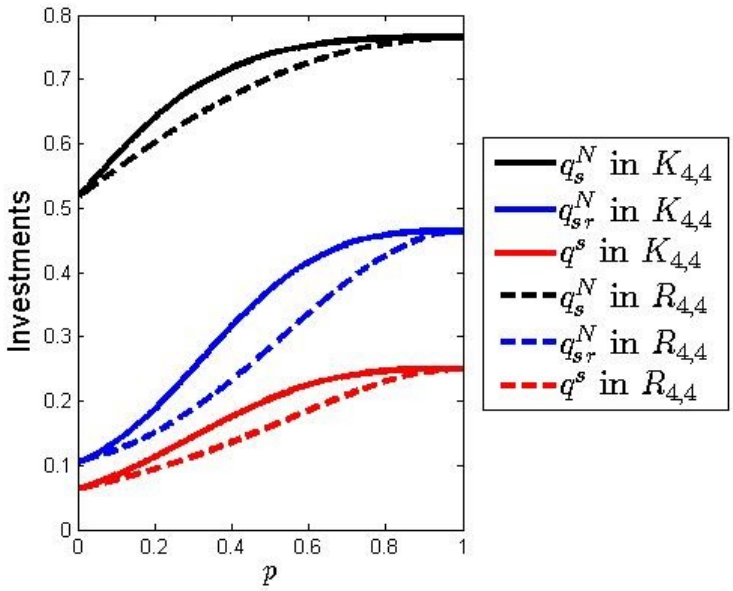

Figure 40 – *Equilibrium investment levels q_s^N and q_{sr}^N and the social optimum q^s as function of p. The investment levels are defined in definition 6. Note that investments increase in the density of the network as the complete network K is more dense than the ring network R. Also note that under both the strategic and the strategic-random attack over-investments prevail relative to the social optimum. In the figure $\psi = a^2$ and $c = q^2$.*

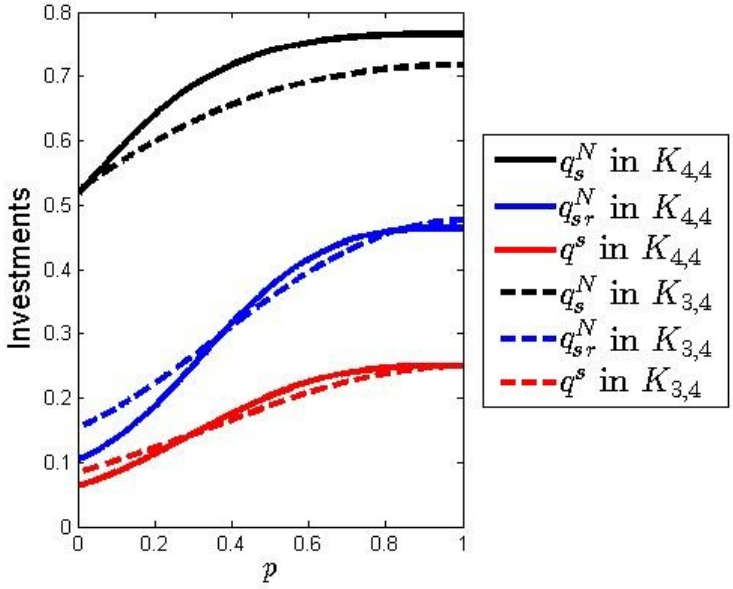

Figure 41 – *Equilibrium investment levels q_s^N and q_{sr}^N and the social optimum q^s as function of p. The investment levels are defined in definition 6. Note that while investments increase in n under the (full) strategic attack, under the strategic-random attack investments decrease for low and high values of p. In the figure $\psi = a^2$ and $c = q^2$.*

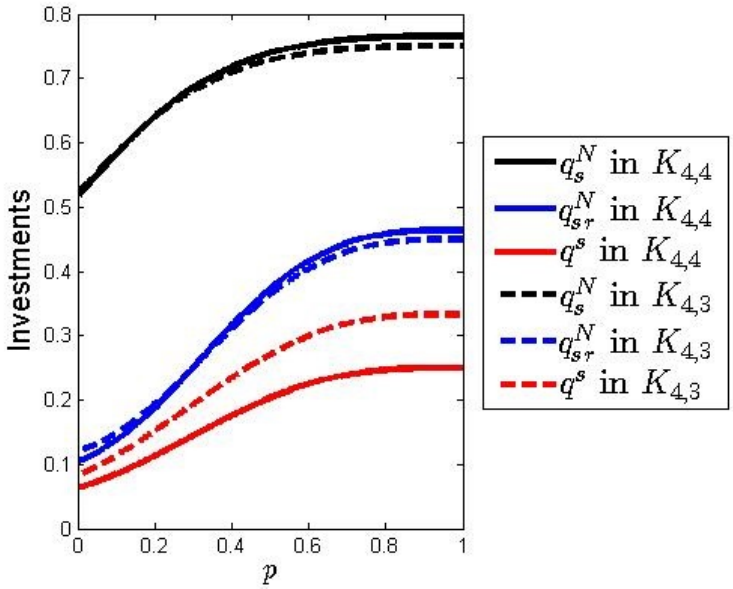

Figure 42 – *Equilibrium investment levels q_s^N and q_{sr}^N and the social optimum q^s as function of p. The investment levels are defined in definition 6. Observe that investments increase in m under the (full) strategic attack. However, under the strategic-random attack investments might as well decrease for small values of p. In the figure once more $\psi = a^2$ and $c = q^2$.*

7 Discussion

Network connections introduce externalities in adopting security. Although it is generally presumed that these externalities result in under-investment in security, it has been showed that the introduction of an intelligent attacker can as well lead to over-investments. In this research we further explored the role of the intelligent attacker in a new spread model. Although we relied on several assumptions we feel that our results point to a general theme: agents invest too much in security when they face an intelligent threat. Yet, these over-investments do not prevail when the network is dense and/or information is shared with a high probability. However, if the network consists of several components and if the attacker is able to strategically decide which component is attacked, agents still invest too much in security.

As our research has pioneered in systematically analyzing incentives to invest in security, several issues remain for discussion. First, because we have built a game theoretical model upon a spread model, we considered spreading of information which is independent of security investments. Although this is a good model for situations where agents do not limit (or enhance) spread facing the upcoming attack, in reality alternative security measures are available in which spreading and security decisions are intertwined. One can think of situations where agents choose their network connections (*network formation model*), choose the probability that they diffuse information (endogenous and local values of p) or adjust behavior when confronted with the actual realization of information spread (*dynamic model*). The avid researcher who adopts this research is confronted with a challenging direction. Not only because the literature on network games that intertwine spreading and decisions is sparse, also because in our - not too involved - spreading model already several open problems remain.

Second, we challenge researchers to fit decision making of agents and the attacker to more realistic situations. One can think of a game where several parameters are unknown to the attacker or to agents (*Bayesian game*). In reality the attacker might not be completely aware of the (precise) security level and agents might not have full information about the network structure. Interesting question is if ignorant agents with incomplete information tend to invest more in security (and follow worst-case scenario's) or invest less (when also the attacker has incomplete information we expect the attack to be more random). Another interesting question is if heterogeneity across agents (e.g. an asymmetric network and/or varying utility/costs) will provoke investments. In reality the systems of large companies are for instance attacked with higher probabilities than systems of individuals (Symantec, 2014). Does this lead to incentives for the large company to increase security investments? Additionally further research can include the possibility of several (strategic) attacks, include the possibility for the attacker to refrain from attacking, include the possibility of semi-cooperation among agents (only subsets of agent cooperate) or allow the attacker to weight documents differently.

Third, as our research contributes to a more general discussion on the economics behind cyber-security, it is appealing to include additional parameters in the model. Our model can for instance be extended to a competition model where companies do not only compete for security but also compete for market share. Do companies have enough incentives to invest in security or will they use their resources to improve market share till they obtain a dominant position (which provokes more cyber attacks)? Additionally policy evaluations can be included in the analysis. Should governments obligate shareholders to invest in security or should they subsidize (or tax) security? To increase investments in network with small dependencies and to decrease investments in networks with high dependencies, the main policy recommendation from our results - ignoring all the practical objections - is to subsidize security in the first case and tax security in the latter case.

Fourth question is if security strategies are changed when agents are faced with the consequences of past behavior. An agent whose information is exposed multiple times in earlier attacks would for instance have incentives to increase investments. We consider this *evolutionary game* as a very promising research direction in the field of security adoptions. Specifically the role of the network structure and the role of an (intelligent) attacker is worth knowing. Information asymmetries which are generally present in security decisions (Moore, 2010) can also be adequately modeled in an evolutionary game. The recent paper of Zhang *et al.* (2014) would provide a good starting point of this research. We challenge

researchers to extend the model of Zhang to an endogenous security model where multiple agents are responsible for security. Optionally the role of the strategic attacker can be included in this model.

Finally we would like to highlight some open problems resulting from our model. The most prominent open question is if the behavior in vertex-transitive networks can be extended to general, asymmetric networks. Although our simulation results do conjecture this hypothesis, we did not provide a formal proof. Additionally the distribution of investments over the set of agents in asymmetric networks is of interest. From simulation results we have the feeling that agents who obtain more documents will invest more in security. Nevertheless the exact magnitude is unknown. Another open question is if results still hold when we relax assumptions on cost functions. We for instance did not investigate the effects when cost functions do not satisfy the boundary conditions in assumption 1 and assumption 2. Finally we challenge future researchers to further explore our spread model. Several open questions remain regarding the probability that information is shared. As exact computation is problematic, simulation results (as in appendix section B) or estimates from random graph theory can be used (like Chung *et al.*, 2009 and Frieze *et al.*, 2004).

A Appendices

A Background material

Lemma A.1. *Let $f : [0,1] \to \mathbb{R}$ and $g : [0,1] \to \mathbb{R}$ ($f \not\equiv g$) be two continuous functions for which $f - g$ is strictly increasing (decreasing). If $f(0) \leq g(0)$ ($f(0) \geq g(0)$) and $f(1) \geq g(1)$ ($f(1) \leq g(1)$) then there exists a unique $c \in [0,1]$ such that $f(c) = g(c)$.*

Proof. Existence of a solution follows easily by the intermediate value theorem. To prove uniqueness assume that there are two intersections of f and g: c_1 and c_2 and assume w.lo.g that $c_1 < c_2$. Also assume w.l.o.g. that $f(0) \leq g(0)$ and $f(1) \geq g(1)$ and $f - g$ is strictly increasing. However as $0 = f(c_1) - g(c_1) < f(c_2) - g(c_2) = 0$ we found a contradictions and hence $c_1 = c_2$. □

Lemma A.2. ***(Debreu, Glicksberg, Fan)***[49] *Consider a strategic form game $\langle \mathcal{I}, (S_i)_{i\in\mathcal{I}}, (\Pi_i)_{i\in\mathcal{I}} \rangle$ where $\mathcal{I}$ is the set of agents, S_i is the space of possible strategies of agent i and Π_i is the pay-off function of agent i. If for each $i \in \mathcal{I}$:*

- *S_i is compact and convex;*
- *$\Pi_i(s_i, s_{-i})$ is continuous in s_{-i};*
- *$\Pi_i(s_i, s_{-i})$ is continuous and quasi-concave in s_i,*

then a pure Nash equilibrium exists.

Proof. Sketch: the proof is based on applying Kakutani's fixed point theorem to the best response of an agent $B_i(s_{-i})$. The conditions in the lemma make sure that $S = \prod_i S_i$ is compact, convex and non-empty and B_i is non-empty, convex and a closed graph[50]. □

Lemma A.3. ***(Hefti)*** *Suppose that in a strategic form game $\langle \mathcal{I}, (S_i)_{i\in\mathcal{I}}, (\Pi_i)_{i\in\mathcal{I}} \rangle$, $\frac{d^2\Pi_i}{dq_{ij}^2}$ exists for every i, j. Consequently let J be the Jacobian of $F = (\frac{d\Pi_1}{dq_1}, \ldots, \frac{d\Pi_n}{dq_n})$. If all principal minors $-J(\mathbf{q})$ are positive for every $\mathbf{q} \in [0,1]^n$, then at most one interior equilibrium exists.*

Lemma A.4. *Let $f : [0,1] \to [0,A]$ be a continuous and strictly increasing function with $f(0) = 0$ and $f(1) = A$. Then there exists a continuous and strictly increasing function $g : [0,A] \to [0,1]$ such that for all $x \in [0,1]$, $g(f(x)) = x$.*

Proof. Notice that the inverse function g clearly exists as f is bijective. Also g is continuous because f is continuous. To prove this, notice that for every sequence in the domain, $x_n \to a$ we have that $f(x_n) \to f(a)$. Consequently, for every sequence $f(x_n) \to f(a)$ in the codomain, we have $g(f(x_n)) = x_n \to a = g(f(a))$. Hence g is continuous at $f(a)$.

To prove that g is strictly increasing, assume the contrary, then there exist $y_1 < y_2$ such that $x_1 = g(y_1) \geq g(y_2) = x_2$. As f is strictly increasing, $y_1 = f(x_1) \geq f(x_2) = y_2$, contradicting the assumption. □

Lemma A.5. ***(Implicit Function Theorem)*** *Let X be a subset of $\mathbb{R}^n$, let P be a metric space and let $U : X \times P \to \mathbb{R}^n$ be continuous. Suppose that the derivative D_xU of U with respect to x exists at a point $(\overline{x}, \overline{q})$ and that $D_xf(\overline{x}, \overline{q})$ is invertible. Set $\overline{y} = f(\overline{x}, \overline{q})$. Then for any neighborhood U of $\overline{x}$, there is a neighborhood W of $\overline{q}$ and a function $g : W \to U$ such that:*

- *$g(\overline{q}) = \overline{x}$*
- *$f(g(q), q) = \overline{y}$ for all $q \in W$*
- *g is continuous at the point $\overline{q}$*

49. The theorem is often called the Debreu, Glicksberg, Fan existance theorem and is based on merged work of the authors. A proof can be found on page 20 in Osborne and Rubinstein (1994).
50. A set-valued function $\varphi : X \to 2^Y$ is said to have closed graph if the set $\{(x,y) | y \in \varphi(x)\}$ is a closed subset of $X \times Y$.

B Simulation of information spread

In this section we estimate D, the expected number of documents obtained by each agent. The focus lies on the relation between D and the number of agents n in the network. In section 4.3.3 we have showed that $D(n)$ converges in growing ring networks, while $D(n)$ diverges in growing complete networks. Without any closed form formula for $D(n)$ in general circulant networks with structure $\mathcal{S}$, we are forced to simulate spreading of information and estimate $D(n)$. In algorithm 1 we present a procedure to estimate D in circulant networks. The procedure is easily extended to other networks.

```
Result: D
Input: S,n,p,k1
A = Construct_adjacency_matrix(S,n);
c(k1) =Max_Iterations;
for k2 ≠ k1 do
    while r < Max_Iterations do
        r=r++;
        Ar = Remove_edges(A,p);
        Check_if_connected(Ar, k1,k2);
        if k1 ∼ k2 then
            c(k2) =c(k2)+1;
        end
    end
end
D = sum(c)/Max_Iterations;
```

Algorithm 1: *Algorithm to estimate D. In the algorithm S is the structure $\mathcal{S}$ of the network and $k1$ is an (arbitrary) agent.*

The evolution of D as function of n can be investigated by repeating the procedure in algorithm 1 for different values of n. In figure 43 on page 86 this evolution is plotted for several circulant networks with fixed structures (independent of n). Observe that D is higher in networks where k is higher in $\mathcal{S} = \{1, k\}$. This is no surprise as these networks are stronger connected. Also observe from the figure that D is strictly increasing in n for all networks. As this property is also observed in other simulation results (not showed here), we hold the conjecture that for all circulant networks with $\mathcal{S} \subset \{1\}$, D is strictly increase in n.

Additionally observe in figure 43 that D seems to converge when $\mathcal{S}$ is independent of n. Different behavior is observed in figure 44. Here the evolution is plotted for circulant networks with an increasing structure (i.e. increasing in n). Apparently D might even diverge when $\mathcal{S}$ increases 'significantly'. As a full investigation of behavior of D as function of $\mathcal{S}$ is outside the scope of this research, we do not further investigate the relation between D and $\mathcal{S}$. Yet we conjecture that D converges when $\mathcal{S}$ is independent of n and diverges when $\mathcal{S}$ increases 'significantly'.

Alternatively we are able to estimate D/n by algorithm 1. This leads to the results in figure 45. Note that D/n can converge to 0 (like the ring network), converge to 1 (like the complete network) or does not converge[51]. The behavior of D/n when $\mathcal{S} = \{1, \ldots, \sqrt{n}\}$ and $\mathcal{S} = \{1, 2, 3\}$ is no surprise when consid-

51. Our range of n is somewhat limited to make any presumptions. When we increase n though, computation time of algorithm 1 increases significantly. We encourage to make algorithm 1 more efficient by using for instance the symmetry property of circulant networks.

ering the behavior of D for these structures in respectively figure 43 and figure 44. Yet the behavior of D/n in other (circulant) network remains an open question.

C Nonexistence of Nash equilibrium without attacking cost

Remind that the attacker incurs some cost when choosing the attack vector $\mathbf{a}$. In this section it is showed that no pure and no mixed Nash equilibrium exist in a two agent network where the attacker does not incur any cost.

Consider a network with two interconnected agents. Remind that the attacker will maximize (5.9) under the constraint that the elements in $\mathbf{a}$ are non-negative an add up to 1. When $\psi \equiv 0$, the strategy of the attacker is easily determined: the attacker will attack the agent with the lowest investments in security. Hence

$$a_1 = 1 - a_2 = \begin{cases} 1 & \text{if } q_1 < q_2, \\ 1/2 & \text{if } q_1 = q_2, \\ 0 & \text{if } q_1 > q_2. \end{cases} \tag{A.1}$$

The utility of the two agents can be expressed as

$$\Pi_1 = 1 - a_1(1-q_1) - (1-a_1)(1-q_2)p - c(q_1),$$

$$\Pi_2 = 1 - (1-a_1)(1-q_2) - a_1(1-q_1)p - c(q_2),$$

where c satisfies assumption 1. In the following proposition we prove that no pure strategy Nash equilibrium exists in this situation.

Proposition A.1. *In a network with two interconnected agents and under a strategic attack, if $\psi \equiv 0$ then no pure strategy Nash equilibrium exists.*

Proof. Let q^N be a pure strategy Nash equilibrium. When $q_1^N = q_2^N$ an agent always gains by raising investments slightly. It follows for instance that $\varphi_1(q_2^N) \neq q_1^N$, where φ is the best response of agent 1.

Next assume that $q_1^N < q_2^N$. From proposition 5.11, q^N solves the first order condition for optimality. For agent 1, as $a_1 = 1$ this FOC becomes

$$c'(q_1) = 1 - \frac{da_1}{dq_1}(1-q_1) + \frac{da_1}{dq_1}(1-q_2)p, \tag{A.2}$$

and for agent 2,

$$\begin{aligned} c'(q_2) &= \frac{da_1}{dq_2}(1-q_2) - \frac{da_1}{dq_2}(1-q_1)p \\ &= -\frac{da_1}{dq_1}(1-q_2) + \frac{da_1}{dq_1}(1-q_1)p. \end{aligned} \tag{A.3}$$

Consequently note that our assumption $q_1^N < q_2^N$ implies that the RHS of (A.2) is larger than the RHS of (A.3). This in turn contradicts convexity of c as it must hold that $c(q_1^N) < c(q_2^N)$. We conclude that no pure strategy Nash equilibrium exists. □

One can even prove that no mixed strategy Nash equilibrium exists.

Proposition A.2. *In a network with two interconnected agents, then under the strategic attack where $\psi \equiv 0$, no symmetric mixed strategy Nash equilibrium exists.*

Proof. Suppose that both agents play a random response. Now let q_2 be a random variable drawn from some probability space F with support $[0, 1]$. As the strategy of the attacker is given by (A.1), the

expected utility of agent 1 becomes

$$\begin{aligned}\mathbb{E}(\Pi_1) &= \int_0^{q_1} 1-(1-q_2)p - c(q_1)\, dF(q_2) + \int_{q_1}^1 q_1 - c(q_1)\, dF(q_2) \\ &= \int_0^{q_1} dF(q_2) - \int_0^{q_1} p\, dF(q_2) + p\int_0^{q_1} q_2\, dF(q_2) + q_1(1-F(q_1)) - c(q_1). \end{aligned} \tag{A.4}$$

Note that agent 1 has to be indifferent under every outcome of $F(q_2)$ because if not, then agent 1 holds a pure response. So it must hold that

$$\frac{d\mathbb{E}(\Pi_1)}{dq_1} = F'(q_1) - pF'(q_1) + pq_1F'(q_1) + 1 - F(q_1) - F'(q_1)q_1 - c'(q_1) = 0.$$

By rewriting it follows that

$$\begin{aligned} F(q_1) &= F'(q_1)[1-p+pq_1-q_1] + 1 - c'(q_1) \\ &= F'(q_1)(1-p)(1-q_1) + 1 - c'(q_1), \end{aligned} \tag{A.5}$$

a differential equation which solution F must satisfy the properties of a cumulative distribution function. Yet one can show that by substituting $q_1 = 1$ in (A.5):

$$1 = F(1) = 1 - c'(1) < 1,$$

a contradiction. We conclude that no solution F of (A.5) exists. □

D Investments in asymmetric networks

Remind that the results in this report are limited to situations where dependencies between agents adopt a vertex-transitive structure. This homogeneity assumption is quite restrictive as real world communication structures may not be symmetric. For instance a hierarchy structure, often seen in companies or in provider/user relations, may attain a tree structure. In this section some simulation results are presented that conjecture that several forces present under the strategic attack in a vertex-transitive network extend to a wider range of (asymmetric) networks.

The simulations in this section are based on the following algorithm.

```
Result: Best_response
Input: Dp, IC, precision1,precision2
Bestres = IC;
while Change_of_Bestres < precision1 do
    for ν=1:n do
        for i=0:precision2:1 do
            a = Strategy_Attacker(i,Bestres,Dp);
            U(i) = Compute_utility(i,Bestres,a,Dp);
        end
        Bestres(ν) = argmax(U);
    end
end
```

Algorithm 2: *Algorithm to estimate investments in security. In the algorithm 'Bestres' is a vector of best responses, Dp is a matrix of $D_{\nu,\mu}$ probabilities and IC is the initial conditions of the best responses. Optionally Dp can be estimated by a small adaption to the procedure in algorithm 1.*

Now suppose that the network is a star on 4 nodes (this continues on example 5.3). The results of the procedure in algorithm 2 are showed in figure 46. Observe that, similarly as in vertex-transitive networks, investments in Nash equilibrium are first increasing in p and later decreasing in p. Also note that the central agent holds a higher security investment than the periphery agents. This follows because the attacker has a larger stimulus to attack the central agent as this agent - in expectation - obtains more documents than the periphery agents. This forces the central agent to invest more in security to cause the attacker to attack someone else.

We observe similar behavior as in the star in other asymmetric networks. For instance in figure 47 simulation results are showed when dependencies adopt network $\mathcal{G}_3$ in figure 18 on page 28. In this network it holds that $D_0 = D_2 \geq D_1 = D_3$ for small p. The simulation results in figure 47 indicate that agent 0 and agent 2 invest more in security than agent 1 and agent 3 when p is low.

The results in figure 46 and figure 47 as well as other simulation results lead to the conjecture that forces present in vertex-transitive networks extend to a wider range of networks. Specifically we conjecture that **a)** investments initially increase in p and later decrease in p and that **b)** agents who obtain more documents invest more in security than other agents.

E Metaphor for economic forces present in the security game

In proposition 5.1 on page 53 we showed that equilibrium investments first increase in p and later decrease in p. Although the eventual decrease in p follows intuitively, the increase in p is not directly clear from the model. In this section we present a metaphor which makes it more clear why investments initially increase in p.

Consider a pyromaniac who tries to burn down as much (rundown) houses as possible (see figure 48). When a house is ablaze the fire may spread to surrounding houses. This happens with a probability that depends on the distance between the houses. For instance when the distance is very large (1 kilometer) this probability is very small, whereas this probability is very large when the distance is small (1 meter). The pyromaniac can only attempt to ignite one house (a day). Also the pyromaniac (rationally) finds an optimal balance between effort (e.g. spying on houses to optimize the attack) and damage.

Now suppose that the owners of the houses can protect against an initial ignition by adopting security measures like for instance an alarm, fences, cameras or by hiring a guard. When the distance between houses is large (1 kilometer or 100 meters), an owner has a strong incentive to invest in security to discourage an attack and push the attacker to attack the other house. Note however that the expected damage done by an attack is higher when houses are closer to each other. In this situation a pyromaniac might spend closer. Nevertheless, when houses are too close to each other and the fire spreads with a high probability, it becomes pointless to invest to push the pyromaniac to attack the other house. In this situation, investments in security decrease.

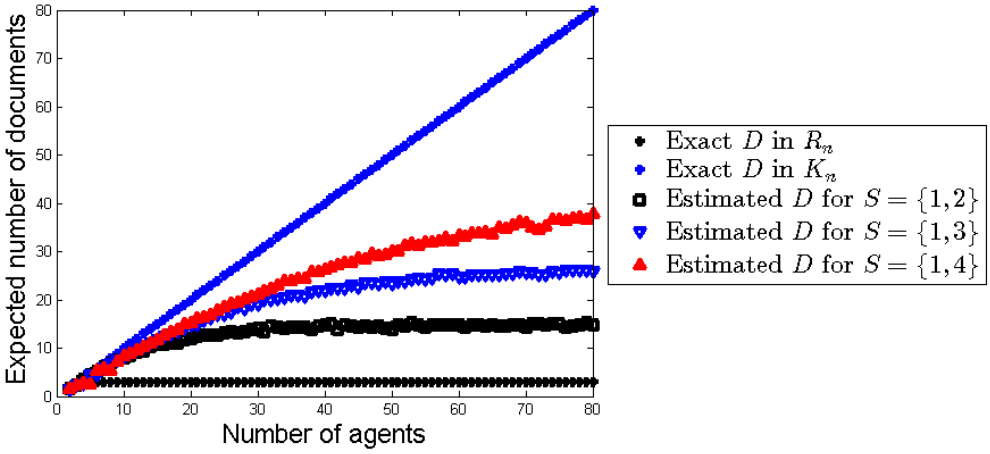

Figure 43 – $D(n)$ *plotted for several networks with* $p = 0.5$*. Note that* $D(n)$ *seems to converge when* $\mathcal{S}$ *is independent of* n*.*

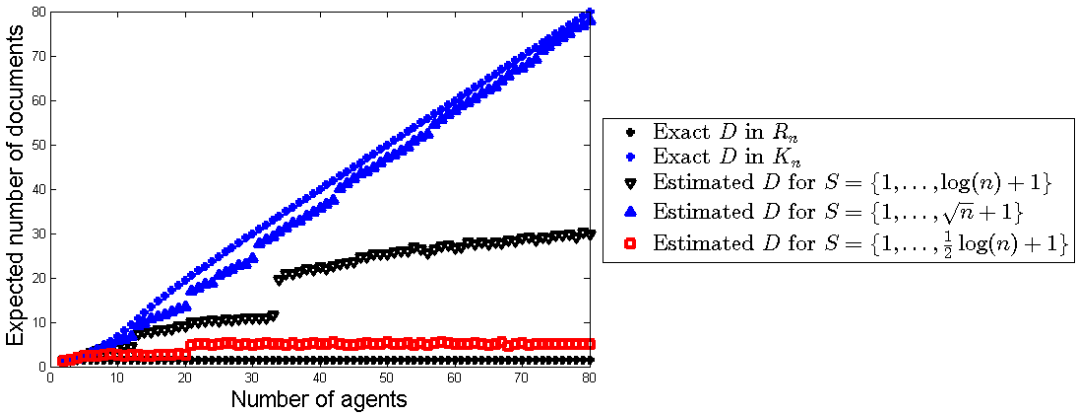

Figure 44 – $D(n)$ *plotted for several networks with* $p = 0.2$*. Different than in figure 43,* $D(n)$ *seems to diverge when* $\mathcal{S}$ *increases significantly.*

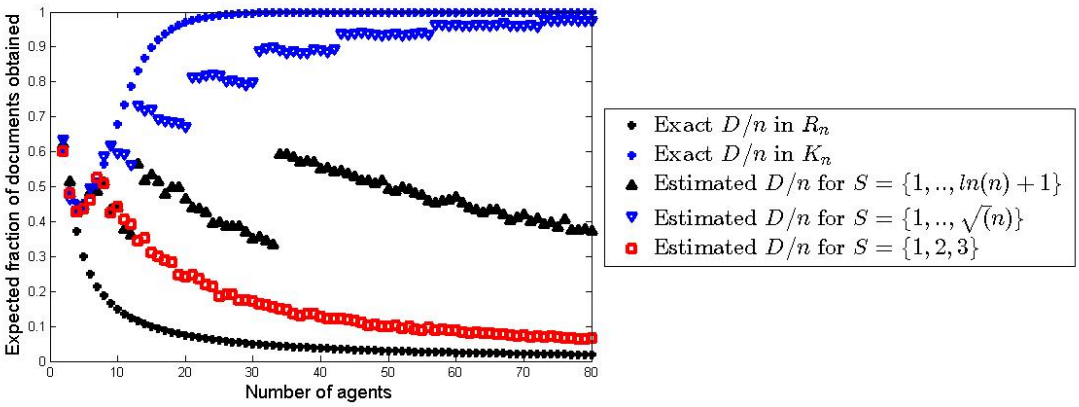

Figure 45 – *Expected fraction of documents obtained when* $p = 0.2$*. Observe that* $D(n)/n$ *seems to converge to 0 when* $\mathcal{S}$ *is independent of* n *and seems to converge to 1 when* $\mathcal{S}$ *increases significantly.*

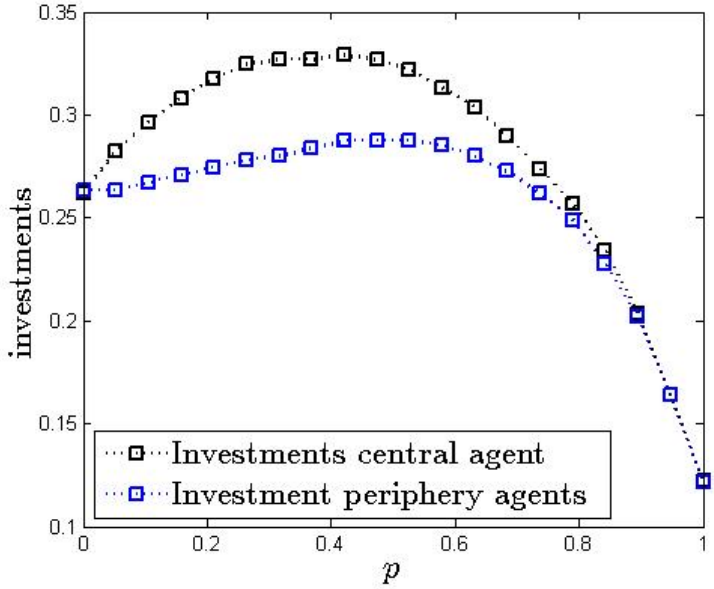

Figure 46 – *Simulation results in a non-cooperative game, under the strategic attack where dependencies attain a star structure with 4 agents. In this figure $c = q^2$ and $\psi = a^2$. Note that investments first increase in p and later decrease in p. Additionally note that the central agent invests more in security.*

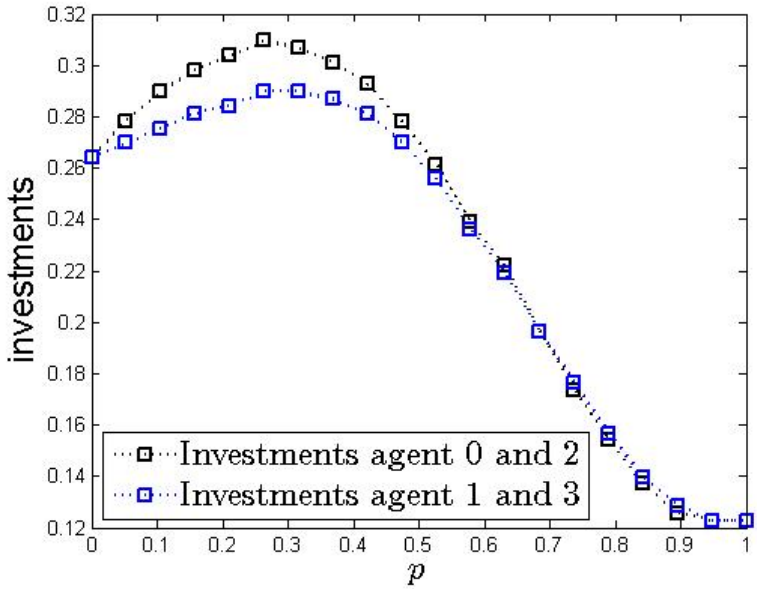

Figure 47 – *Simulation results in network A_3 in figure 18 on page 28. In this figure $c = q^2$ and $\psi = a^2$. Note that investments - once more - first increase in p and later decrease in p.*

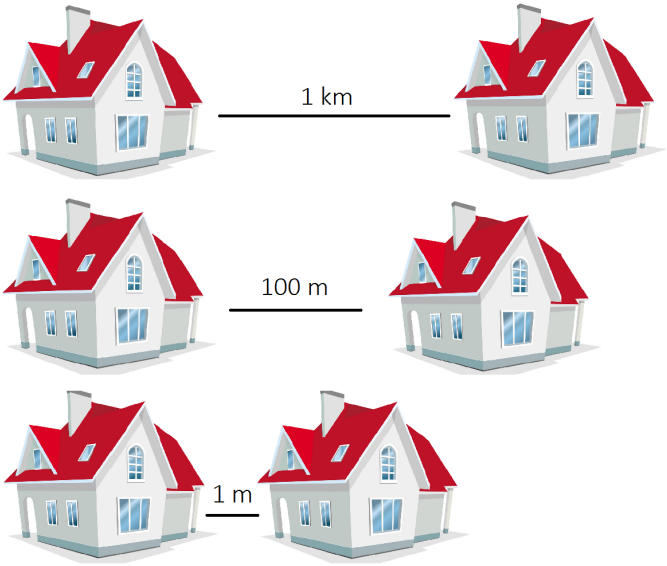

Figure 48 – *Incentives of a pyromaniac and householders who adopt security. Householders spend the most in security when the houses are 100 meters from each other.*

References

[1] D. Acemoglu, A. Malekian, and A. Ozdaglar. “Network Security and Contagion”. *MIT Mimeo* (2013).

[2] S. Amin, G.A. Schwartz, and S.S. Sastry. “Security of interdependent and identical networked control systems”. *Automatica* 49 (2013), pp. 186–192.

[3] R. Anderson and T. Moore. “The Economics of Information Security: A survey and Open Questions”. *Science* 314.5799 (2006), pp. 610–613.

[4] M. Baccara and H. Bar-Isaac. “How to Organize Crime”. *Review of Economic Studies* 75.4 (2008), pp. 1039–1067.

[5] Y. Bachrach, M. Draief, and S. Goyal. “Contagion and Observability in Security Domains”. *Proceedings of 51th Allerton Conference* (2013), pp. 1364–1371.

[6] V.M. Bier. “Choosing What to Protect”. *Risk Analysis* 27 (2007), pp. 607–620.

[7] L. Blume et al. “Network Formation in the Presence of Contagious Risk”. *ACM Transactions on Economics and Computation* 1.2 (2013), pp. 1–20.

[8] F. Chung, P. Horn, and L. Lu. “The giant component in a random subgraph of a given graph”. *Algorithms and Models for the Web-Graph* (2009), pp. 38–49.

[9] Symantec Corporation. “Internet Security Threat Report” (2014).

[10] P. Dasgupta and E. Maskin. “The existence of equilibrium in discontinuous economic games, I: Theory”. *The Review of Economic Studies* 53.1 (1986), pp. 1–26.

[11] N.B. Dimitrov and L.A. Meyers. “Mathematical Approaches to Infectious Disease Prediction and Control”. *Bull. Amer. Math. Soc.* 44.1 (2006), pp. 63–86.

[12] S. Dynes, E. Goetz, and M. Freeman. “Cybersecurity: Are Economic Intentives Adequate?” *Critical Infrastructure Protection, Springer* (2007), pp. 15–27.

[13] M. Fey. “Symmetric games with only asymmetric equilibria”. *Games and Economic Behavior* 75.1 (2012), pp. 424–427.

[14] A. Frieze, M. Krivelevich, and R. Martin. “The emergence of a giant component in random subgraph of pseudo-random graphs”. *Structure and Algorithms* 24 (2004), pp. 42–50.

[15] ”A. Galeotti, S. Goyal, M.O. Jackson, and F. Vega-Redondo”. “Network Games”. *Review of Economic Studies* 77 (2010), pp. 218–214.

[16] S. Goyal and A. Vigier. “Attack, Defense and Contagion in Networks”. *Cambridge Working Papers in Economics* 1327 (2014).

[17] G. Heal and H. Kunreuther. “Interdependent Security”. *The Journal of Risk and Uncertainty* 26.2/3 (2003), pp. 231–249.

[18] A. M. Hefti. “On uniqueness and stability of symmetric equilibria in differential symmetric games”. *ECON - Working papers* 018 (2011).

[19] M.O. Jackson. *Social and Economic Networks*. Princeton University Press, 2008.

[20] J. Jang-Jaccard and S. Nepal. “A survey of emerging threats in cybersecurity”. *Computer and System Sciences* 80.5 (2014), pp. 973–993.

[21] B. Johnson, J. Grossklags, N. Christin, and J. Chuang. “Nash Equilibria for Weakest Target Security Games with Heterogeneous Agents”. *Springer LNICST* 75 (2012), pp. 444–458.

[22] N. Larson. “Network Security”. *MPRA paper* (2011).

[23] F.T. Leighton. “Circulants and the Characterization of Vertex-Transitive Graphs”. *Journal of Research of the National Bureau of Standards* 88.6 (1983).

[24] M. Lelarge and J. Bolot. “Network Externalities and the Deployment of Security Features and Protocols in the Internet”. *Sigmetrics Performance Evaluation Review* 36.1 (2008), pp. 37–48.

[25] P. van Mieghem. “The N-interwined SIS epidemic network model”. *Computing* 93 (2011), pp. 147–169.

[26] C. Moore and M.E.J. Newman. “Epidemics and percolation in small-world networks”. *Phys. Rev.* 61 (2000), pp. 5678 –5682.

[27] T. Moore. “Introducing the Economics of Cybersecurity: Principles and Policy Options”. *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy Available at: http://www.nap.edu/catalog/12997.html* (2010).

[28] M.E.J. Newman. “The structure and function of complex networks”. *SIAM Rev.,* 45.2 (2006), pp. 167 –256.
[29] J. Omic, A. Orda, and P. van Mieghem. “Protecting Against network Infections: A Game Theoretic Perspective”. *INFOCOM* (2009), pp. 1485–1493.
[30] M.J. Osborne and A. Rubinstein. *A Course in Game Theory*. Mit Press Ltd, 1994.
[31] H. Peters. *Game Theory, A Multi-Leveled Approach*. Springer, 2008.
[32] H. Varian. “Managing Online Security Risks”. *Economic Science Column, The New York Times* (June 1, 2000).
[33] Y. Xiang, X. Fan, and W.T. Zhu. “Propagation of Active Worms: A Survey”. *IEEE Communications Surveys and Tutorials* 16.2 (2014), pp. 942–960.
[34] Z. Yang and C.S. Lui. “Security Adoption in Heterogeneous Networks: the Influence of Cyber-insurance Market”. *Performance Evaluation* 74 (2014), pp. 1–17.
[35] C. Zhang, R. Pan, A. Chaudhury, and C. Xu. “Effect of Security Investment on Evolutionary Games”. *Journal of Information Science and Engineering* 30 (2014), pp. 1695–1718.