Cyber Insurance & Insurable Topologies

Håvard Råmundal Halse
Jonas Hoemsnes

Title: Cyber Insurance & Insurable Topologies

Students: Håvard Råmundal Halse & Jonas Hoemsnes

Problem description:

Security breaches are increasingly prevalent in the Internet age causing huge financial losses for companies and their users. Cyber-insurance is a powerful economic concept that can help companies in the fight against such malicious behavior. Earlier research suggests that cyber- insurance has failed to reach its promising potential, although the concept of cyber-insurance has been around since the 1980s. The researchers claims that a functional model for cyber-insurance has to handle its unique problems regarding interdependent security, correlated-risk and asymmetrical-information. These challenges can be described and analyzed by network graphs, and positively some graphs will yield overall higher security (insurable topologies) than other graphs. In order to cater for cyber-insurance, it is essential to understand how to create new or transform existing networks to insurable topologies.

The students will:

– conduct a background study and a market survey to validate the current state of cyber- insurance

– study and characterize graphs describing insurable topologies

– build a model of network formation which gives rise to such insurable topologies

– apply the model to investigate a realistic ecosystem, e.g., cloud computing

Responsible professor: Jan A. Audestad, Professor II

Supervisor: Gergely Biczók, Postdoc

Abstract

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like "Huardest gefburn"? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

This is the second paragraph. Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like "Huardest gefburn"? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

And after the second paragraph follows the third paragraph. Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like "Huardest gefburn"? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

After this fourth paragraph, we start a new paragraph sequence. Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like "Huardest gefburn"? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of

the original language. There is no need for special content, but the length of words should match the language.

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like "Huardest gefburn"? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

Preface

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like "Huardest gefburn"? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

Contents

List of Figures

Chapter 1

Introduction to Cyber Insurance

1.1 Motivation

Security breaches are increasingly prevalent in the Internet age causing huge financial losses for companies and their users. Cyber-insurance is a powerful economic concept that can help companies in the fight against such malicious behavior. Earlier research suggests that cyber-insurance has failed to reach its promising potential, although the concept of cyber-insurance has been around since the 1980s. The researchers claims that a functional model for cyber-insurance has to handle its unique problems regarding interdependent security, correlated-risk and asymmetrical-information. These challenges can be described and analyzed by network graphs, and positively some graphs will be superior as cyber-insurance networks compared with other structures. In order to cater for cyber-insurance, it is essential to understand how to create new or transform existing networks to these beneficial structures.

1.2 Problem definition

Cyber-insurance is an insurance product used to transfer financial risk, associated with computer and network related incidents, over to a third party. In this project, the goal is to analyze the current state of the cyber-insurance market. Study and characterize network structures suited to be used as a cyber-insurance network. -A desired structure will possesses some characteristics that would be beneficial to reflect a cyber-insurance network. And to build a model, which can relate to different real world scenarios, using network formation to force the creation of these structures.

1.3 Readers guide

Readers guide

1.4   Insurance and cyber-insurance

Unfortunately it seems very unlikely that we will ever experience a flawless system, especially in our research area concerning networks. When facing a risk, there are typically four ways to handle it [BL08b].

1. Avoid the risk

2. Retain the risk

3. Self protect and mitigate the risk

4. Transfer the risk

In this project we will focus on risk management in the ICT-market. So far, the ICT-industry have tried to prevent risks with a mixture of option 2 and 3. This has lead to creation of systems and software trying to detect threats and anomalies and to protect the users and the structure. Anti-virus software is also a good example of a system which perform self-protection and hence mitigate the risk of becoming a victim of malicious attacks.

Unfortunately these types of systems does not eliminate the risk. Threats evolve over time, and there will always be accidents and security flaws. Cyber-insurance acts in the domain of the fourth option, and seeks to answer the question; -how can one handle this residual risk. The basic idea for cyber-insurance and insurance in general is to transfer the risk to a third party who willingly accept it in exchange for a predictable periodical fee, called premiums [BL08a]. Coverage's provided by cyber-insurance policies may include property loss and theft, data damage, cyber-extortion, loss of income due to denial of service attacks or computer failures [PD12]. Traditional coverage policies rarely cover these incidents, therefore is cyber-insurance seen as a huge potential market.

Although the concept of cyber-insurance has been around since the 1980s, it has failed to reach its promising potential. There might be several reasons for this slow development, however, it is believed that the main reason so far, is that no model deals with all the unique problems of cyber-insurance at once. In addition to the known difficulties of insurance, such as calculating risk, cyber-insurance has to deal with the problem of asymmetric information, correlated risk and interdependent security [GGJ$^+$10]. As we shall see cyber-insurance differs from traditional insurance, although there are many similarities.

Traditional Insurance.   The basic structure of cyber-insurance relates to traditional insurance, where an insurance contract (policy) binds the insurance

company to pay a specified amount to the insurance holder whenever an incidents occur. In return, the insurance holder has to pay a fixed monthly or annually fee (premium) to the insurance company [Rob12]. The contract includes a risk assessment of the company's vulnerability and clearly specifies the entitled amount of coverage for each of the different risks. These assessments are used to calculate the companies premium [Rob12]. Generally, this means that means to improve the security is negatively correlated with the premium costs. In cyber-insurance this means that better security will lower price on the insurance premium.

Generally, to ensure that their business is economically viable, the insurance company will require that an insurable risks possess seven distinct characteristics [MCR80]:

1. Large number of similar exposure units: Insurance is based on the principle of pooling resources, where insurance policies are offered to individual members of a large class. Meaning the more customers, the closer the predicted losses will get to the actual losses.

2. Definite loss: A loss should take place at a known time, in a known place and from a known cause. Incidents such as a fire or car crash, are examples where these terms are easy to verify.

3. Accidental loss: The event that triggers a claim should not be something the insurer has discretion or control over.

4. Large loss: The size of the loss must be meaningful from the perspective of the insured. Insurance premiums need to cover both the expected cost of the loss, in addition, cover all the expenses regarding issuing and administrating policies, adjusting losses and supplying the capital needed to be able to pay claims.

5. Affordable premium: The premium must be proportional to the security offered, otherwise no one will offer/buy the insurance. In the situation where the likelihood of the insured event is high, and the cost is large, it is unlikely that the insurance company will offer the insurance, or at least the premium would be too high for anyone to consider buying it.

6. Calculable loss: Both the probability and the cost of an insurable event, has to atleast be possible to estimate.

7. Limited risk of catastrophically large losses: If losses happen all at once the likelihood of the insurance company getting bankrupt is high. Therefore, losses are ideally independent and non-catastrophic.

This model will also apply to the risks covered by cyber-insurance. Unfortunately there are additional obstacles regarding cyber-insurance. As mentioned, the three major problems with cyber-insurance are related to; information asymmetry, interdependent security and correlated risk.

Information asymmetry. Information asymmetry arises when one side in a transaction or a decision has more or better information than the other party. There are two different cases of information asymmetry. The first one is called adverse selection, where one party simply has less information regarding the performance of the transaction. A good example is when buying health insurance, if a person with bad health purchases insurance, and the information about her health is not available to the insurer, we have a classical adverse selection scenario. We can observe a similar situation for the cyber-industry, where an insurer has no way of confirming whether your network is "healthy", i.e. not contaminated, or if it is infected. The other information asymmetry scenario is called moral hazard. It occurs after the signing of the contract, if one party deliberately takes some action that makes the possibility of loss higher, i.e. choosing not to lock your door, since you have insurance. Or in the computer setting, deliberately visiting hostile web-pages, or not using anti-virus software, firewalls or other self-protection software. [Pal12]

As we see, the information asymmetry problem is highly relevant regarding cyber-insurance. Measuring the level of security is very hard, and in order to lower the premiums people will have an incentive for hiding information about their security level. Another problem occurs on the customer side of the market. For a customer wanting to improve their defence mechanisms, the software security market often becomes a lemons market [1]. It is difficult for the buyer to distinguish the performance of different software products, and thus the reasonable thing to do, is to buy the cheapest. Thus, the good security products has to charge the same price as the bad. If the cost of producing good security software is too high, the problem can even result in abandoning the production of good software, because it would not be profitable.

Correlated risk. Another big concern regarding cyber-insurance, is the correlated risk. Among others, the problem occurs due to the need of standards. Standardization is an important part of computers and computer networks. Generally it enables computers to communicate, install and use different software. A good example is operative systems for personal computers, today we only have a small

---

[1]Lemon market, the problem of quality uncertainty, was first introduced in a paper [Ake97] by the economist George Akerlof in 1970,and used the market for used cars as an example.[Wik] The conclusion of the paper is that since the buyers lack information to distinguish a bad car(lemon) from a good one(cherry), the buyer will not pay the price the seller wants for a cherry, and the seller will not sell a cherry for the price of a lemon, and thus the lemons drives the cherries out of the market.

set of operative systems available, and these systems are standardized, so they can communicate over the same communication channels. The standards generates a lot of the value in the ICT-industry, but it also makes large extents of threats possible. All systems that uses the same standards, creates a large number of similar exposure units, they share common vulnerabilities, which could be exploited at the same time. As we see this violates the insurance characteristic of limited risk of catastrophically large losses. This creates a significant difficulty for the cyber-insurance industry, because when a security breach occurs there is a high probability that it will occur to a large number of people, i.e. catastrophic and extreme events occur with a higher probability than in the regular insurance business. To compensate, the logical thing to do would be to raise the premium cost, however this could violate the characteristics of affordable premiums and large losses. If the security breach is large, it could even potentially cause so much damage, that the insurers will not be able to pay all of the customers who suffered, and they could go bankrupt.[BS10]

Interdependent security.   Another problem in the ICT-industry is interdependent security. Meaning that you are not only dependent on your own investment in security, but also everyone else's. Investment in security generates positive externalities, and as public goods, this encourages to free riding. Why should I pay for security when I can just free ride on security invested by others? The problem is that the reward for a user investing in self-protection depends on the security in the rest of the network. i.e. The expected loss due to a security breach at one node, is not only dependent on this nodes level of investment in security, but also on the security investment done by adjacent nodes, and theirs adjacent nodes and so forth. A good example of this is the amount of spam sent every day, which is dependent on the number of compromised computers. Meaning if you have invested in security software of some kind, you still receive lots of spam because there are a variety of people who have not invested [Böh10].

Calculating losses   A problem in several areas of insurance is the calculation of risk. In cyber-insurance, the obstacles above contributes to make this particularly difficult. When facing a security breach there are two potential loss classes:[BMR09, MCR80]

– primary losses or first-degree losses: direct loss of information or data and operating loss. These arises from disuse, abuse or misuse of information. The cost of these arise from recovering, loss of revenue, PR and information sharing costs, hiring of IT-specialists etc.

– Secondary losses are indirectly triggered. These are the loss of reputation, goodwill, consumer confidence, competitive strength, credit rating and customer churning.

The value of the loss from both these classes can be difficult to determine, although the second one is probably the most difficult. Because it is challenging to put a value on i.e. how many potential customers did they loose due to the reputation loss, how many customers churned, and what was their value etc. It could also be difficult to determine when the loss happened, where and what caused it.

Cyber-insurance instead of security.   Another problem with cyber-insurance is actors seeing it as a solution to the problem of being secure. Instead of investing in security, they now have a way of buying their way out. However, as the paper [BL08a] shows, this problem might be solved with the right pricing options. Meaning that the insurance companies can create pricing models which makes it economical beneficial to invest in security and cyber-insurance. Cyber-insurance could also be used as an incentive for buying security. Such model will also make sense for the insurance company, since better security systems yields lower probability for incidents.

Despite that fact that other types of risks are insured, and that these risks have some characteristics which makes them more difficult to handle. Cyber-insurance are quite similar to regular insurance. The challenge is to find a way for the insurers to handle these special characteristics, in order to create a healthy cyber-insurance market. First, it would be useful to have a look at the current state of the market and what results related work have come up with, and look at how these results contributes.

1.5   The cyber-insurance market

The market for cyber-insurance emerged in the late 80's, when security software companies began collaborating with insurance companies to offer insurance policies together with their security products. From a marketing perspective, adding insurance helped highlighting the supposedly high quality of the security software. Regardless, the new product was a comprehensive solution, which dealt with both risk reduction and residual risk [BL08b]. Continuing into the beginning of the new millennium, several companies started offering standalone cyber-insurance, which sat the frame for the current insurance product. In Norway, startup-companies, such as Safensure AS where established with the goal to deliver cyber-insurance to the Norwegian and European market [dig]. In addition, already well-established insurance companies, such as Gjensidige Nor, started offering insurance products intended for the web-site market. These insurances where created to insure lost income due to malicious hackers, denial of service and other well know cyber-attacks at that time. In 2001 Gjensidige Nor, in cooperation with the German company Tela Versicherung, offered businesses insurance against financial losses due to hacker attacks and sabotage for up to 5 million NOK, given that the companies could provide proof that specified security measures were taken by the company [it].

Despite the fact that cyber-insurance has been around for a couple of decades, the market still struggles to gain a foothold. Safensure AS does not longer exist and Gjenside Nor does not advertise a cyber-insurance product anymore. It seems to be many challenges for both buyers and sellers. Buyers face tremendous confusion about cyber risks and their potential impacts on business. [PpD12] points out that people do not know or understand what kinds of risks the cyber-space involves, and how large the losses can be. Even when companies have decided to purchase a cyber-insurance, they are confused with what kind of insurance they should purchase, it is difficult to see what it cover, what is a reasonable price etc. Thus, the market for cyber-insurance tend to become a lemons market, where the buyer lacks knowledge, and struggles to see the differences between the different insurance contracts.

The UK and US market   We wanted to reveal the current status of the cyber-insurance market. We limited our survey to the UK and US-market, in addition to the Norwegian market. The first impression reveals that there are several different results and opinions regarding the health of the global cyber-insurance market. The paper [Ins11] studied a sample of 50 organizations in various industry sectors, located in the United States. They showed that in average every company suffered from more than one successful attack every week, and showed that successful cyber-attacks could result in serious financial consequences. They found that the median cost of cyber-crime in the U.S is $5.9 million per year, ranging from $1.5 million to $36.5 million per company, which is a 56 % increase from last year.

Another paper [Ris12] collected statistics about cyber-attacks in the UK, and the result claims that the costs is expected to be £27 billion a year, which makes it one of UK's biggest emerging threats. In addition, they pointed out that the victims is not only large companies like Google and PlayStation, but also small businesses. Despite these numbers only 35 % of the companies in the survey had purchased cyber-insurance. Which is surprisingly low since they found no shortage of providers, compared to the Norwegian market. -It was reviled that there are nine insurers with specialists in cyber-insurance in the UK, and in the US around 30-40 actors.

An article from CFC underwriting [New], a UK firm offering insurance to small and medium sized businesses, claims promising numbers for the US cyber-insurance market. On US soil, 20-50% of businesses purchased either standalone cyber-insurance or benefits from coverage provided in their already exciting insurance. However, despite recent years focus on the increasing cyber-crime activity and the catastrophic consequences of having weak security, only 1% of European businesses are enrolled in an insurance program covering cyber-threats. A more optimistic survey pointed out that more and more insurance companies offered cyber-insurance. Yet, of the 13000 companies, only 46 percent said they were insured against cyber-attacks [Pra].

The media coverage on corporate threats such as Stuxnet and the attacks on Playstation, which lead to a compromise of 77 million user accounts including credit card numbers [Chu], shows that the cyber-threats is growing, and one would assume that we were in need of cyber-insurance. However, the surveys shows, even when the number varies, that a large share of companies have chosen not to protect against the residual risk of cyber-attacks, by buying cyber-insurance.

The Norwegian market   In comparison, our survey of the Norwegian insurance market relieved that specialized cyber-insurance companies, such as Safensure AS, does not exist anymore. Only *one* out of the five biggest actors[2] offer something similar to a cyber-insurance. Gjensidige Nor offers something they call operation-loss-insurance which covers expenses due to reconstruction of files and reinstalling software and denial of service attacks. In addition, it is also possible to insure against hacking and sabotage [Nor]. From email correspondence with Gjensidige Nor it was clear that they needed lots of information regarding the company to be able to calculate the insurance premium. They required extensive information about the economic health of the company, and a model of what kind of software and hardware where used with estimated values on each component. Unfortunately, we were not able to obtain the cost of such an insurance.

Future market   The survey from [New] claimed that the US cyber-insurance market was much more mature compared to the European. A possible reason is the

---

[2]Gjensidige, If Skadeforsikring, DNB, TRYG, Storebrand

breach notification laws. In the US, 46 states have mandatory breach notification laws, combined with significant penalties for companies failing to protect sensitive data. This means that the US government are creating incentives for firms to buy cyber-insurance. In Europe, only Germany and Austria have similar laws, forcing companies to notify affected customers of data leakage. A recent proposal of the EU wants to introduce the notification law in Europe, and also include penalties for serious data breaches, these could be as high as 2 % of a companies global revenue [New]. It is proposed that the law should take effect in 2014, although this is highly unlikely regarding the complexity of the effects of this law. Undoubtedly this law would be a health injection to the rise of the cyber-insurance market, however, a market based on fear of the consequences of not being insured is not desirable. The ultimate goal for cyber-insurance, is to correlate the purchase of cyber-insurance with companies growing desire to invest in more security, and hence lower the risk of being a victim of cyber-crimes. The article claims that the way to meet this goal, is to the focus on the serious brand damage a company will experience and not just the financial loss.

In summary, the cyber-insurance market seems to have a huge potential, but need some new thinking to fully take advantage of it. We will focus on finding network structures that will help the insurers offer fair contracts, which is beneficial for both the customers and the suppliers. Which can help in the process of establishing a healthy cyber-insurance market.

Chapter 2

Relatedwork

2.1 Cyber-Insurance

While several authors have expressed doubts about the future of cyber-insurance, the authors of [BS10] still have faith in the prevalence of cyber-insurance. The paper describes the three main problems of cyber-insurance; information asymmetry, correlated risk and interdependent agents. They argue that a model for cyber-insurance has to encounter each of these obstacles. Instead of presenting a solution they propose a framework to classify models of cyber-insurance. The framework breaks the modeling down to five key components:

- network environment(nodes controlled by agents, who extract utility. Risk arises here.)
- demand side(agents)
- supply side(insurers)
- information structure, distribution of knowledge among the players.
- organizational environment. Public and private entities whose actions affect network security and agents security decisions.

The goal is that this unifying framework will help navigating the literature and stimulate research that results in a more formal basis for policy recommendations involving cyber-risk reallocation. They encourage to answer questions such as; under what conditions will a cyber-insurance market thrive? What is the effect of an insurance market, -will the Internet be more secure? Does it contribute to social welfare? They also analyze several other papers on cyber-insurance, and show how all of them are touching into the problems and key components showed above, but none handles all of them. The paper studies other existing models, and reveals a discrepancy between informal arguments in favor of cyber-insurance and analytic results questioning the viability of a cyber-insurance market.

The paper [PGP11] presents a cyber-insurance model which handles both risks due to security (e.g virus) and non-security related features such as power outage and hardware failure. Their model, Aegis, is a simple model in which the user accepts

a fraction of loss recovery to himself and the rest is transferred to the insurance company. They show that when it is mandatory to purchase insurance, risk averse agents would prefer Aegis contracts over traditionally cyber-insurance products. The model also give users incentive to take a greater responsibility in securing their own systems. Hence this answers one of the questions from [BS10]: The overall security of the Internet will increase if the Aegis is offered to the market. An interesting result from their analysis is the fact that a decrease/increase in the insurance premium may not always lead to increase/decrease in demand. From the insurers point of view, this features means that one can increase the margins without loosing possible customers. Hence it will be easier to create a market for cyber-insurance.

[PH12] adopts a topological perspective in proposing a mechanism that accounts for the positive externalities (due to purchase of security mechanisms)and network location of users. In addition they provide an appropriate way to proportionally allocate fines/rebates on user premiums. This feature relates to our model, where a central node in the network receives a bulk insurance discount, in order to facilitate creation of star topologies.

[PH] present the importance of discriminating network users in insurance contracts. This is done to prevent adverse selection, partly internalizing the negative externalities of interdependent security, achieving maximum social welfare, helping a risk-averse insurer to distribute costs of holding safety capital among its clients, and insurers sustaining a fixed amount of profit per contract. The paper proposes a mechanism to pertinently contract discriminate insured users when having complete network information. This is important since almost every node in the network is different from each other. Hence we need a way of distinguish good nodes from bad ones by the means of the premium price.

The paper [BL08a], presents how risk management on the internet only have involved methods to reduce the risks, such as firewalls, intrusion detection systems, anti virus etc. But none of these have managed to remove the risk completely. In general there are four possible ways of removing risk: avoid it, retain it, self protect and mitigate it or transfer the risk. Most entities on the internet have chosen a mix of of retaining and mitigate by self protecting.

Unfortunately, these solutions does not eliminate risk completely, and threats evolve over time. Thus, the only option for completely removing the risk, is to transfer it to a party who willingly accepts it, in exchange for a fee. The key-result of this paper is that they show that cyber-insurance will result in overall higher payoff. Because when the premiums discriminates users based on the investment in self protection, it will act as an strong incentive to acquire self protection.

The paper [DS06] describes an interesting network formation games. Although the paper tries to observe susceptibility to sybil attacks in peer-to-peer networks, their approach on network formation can be related to our thesis. In their game nodes are either friends or strangers, and the goal of the nodes is to selfishly try to fulfill their communication needs. Their needs is to communicate with as many as possible of their friends. This can be achieved by either direct or indirect connections. Every node has a link budget, i.e. a maximum number of links they can establish, and a set of friends they want to connect to. They proposes two random games where nodes might have to take the risk of connecting to non-insured nodes.

1. Random model: Every node in the network initiate a set for friendships with other nodes, denoted F. All nodes have the same link budget $L < F$.

2. Unbalanced Random Mode. The same friendship graph as in the random model is created. However one of the nodes have a significantly larger link budget ($L_0 > 2F$)

The first model does not result in any equilibrium, except the one where friends only connect to other friends. The other model shows some new insights, when the link budget is comparable with their number of friends, most still choose to only connect to friends. However, when the link budget is set to only one link, except for the rich node. Then the resulting equilibrium is a star topology.

2.1.1   Summary

There are many different papers that have described the problems of cyber-insurance, and proposed different models and solutions. However, as we revealed, the cyber-insurance market is yet far from established and still has lots of potential. Each of the presented models have a slightly different angel towards improving the cyber-insurance market. Although, promising results from the papers, no improvements have appeared in the market-state, and it seems like another approach is needed. -This is what we intend to do. In brief we will investigate whether there are any advantageous structures and use network formation to force nodes to end up in these structures, and stay there.

NOTES ... Til summary   As we can see from other related work, each and everyone of them are creating a model trying to solve the cyber-insurance market. Each model have a slightly different angel towards the problem, some of them tries to solve it and even make cyber-insurance better. As we have seen from the current market state, the cyber-insurance market is far from healthy. There are some promising numbers from the US. However, we believe that this market is built on fear from a having to pay high fees due the notification laws.

We want to take a step back and first determine if there are any network structures which would be preferred as a cyber-insurance market. What we are looking for is a structure that are stable and increases the utility for both the nodes and the insurer. More precisely we want to find a structure which minimizes the cost of h....

The next step will be to use network formation to find out how we from the insurers point of view can force nodes to end up in the preferred structure, and stay there (i.e. for a stable network).

Graphs and Network Formation

In nature and society there are lots of scenarios that can be described using graphs. From infrastructure, such as railroads, water pipelines and electricity grid, to societal relationships and disease epidemics, can all be visualized using graphs. Cyber-insurance is no exception, and can also be structured as a graph. This is of interest because, when one can describe a phenomenon with graphs, it is easier to analyze and possibly find some characteristics, the graph can be used as an analytic tool [Aud].

Several studies have been done on the characteristics of different graphs, such as E-R graphs and A-B graphs (scale-free graphs), these are thoroughly described in the methodology chapter. In addition, one have found special characteristics on star-shaped graphs and cliques. This chapter will highlight which characteristics are desirable to have in the cyber-insurance market, and which structures that possess these characteristics. These findings will serve as the foundation of our models, where we try to force these graph structures to emerge endogenously.

3.1   Real world graph structures

As a starting point lets have a look at a couple of real world examples of how complex systems with huge amount of data could be structured as graphs. We will see how complex structures becomes rather intuitive when presented as a graph. By looking at the graph structure, one can determine what type of graph that appears, and hence certain characteristics will apply.

Stock markets.   The research paper [Gar07], analyzes the correlation between different stocks in the Greek stock market in year 1997. They compared the daily closing price of stock i at day t, and compared the similarity of a pair of stocks i and j by using the correlation coefficient. The idea is that the correlation coefficient between a pair of stocks can be expressed using different distances in a graph structure.

A short distance means high correlation and long distance means low correlations between the stocks. Normally this network would be shown as a fully connected graph, which will consist of $\frac{n(n-1)}{2}$ edges, and would be difficult to analyze. However the approach taken in the paper presents a clear and understandable graph, consisting of $(n-1)$ edges showing the correlations between the stocks.

The resulting graph can be seen in Figure 3.1, and shows a network consisting of several clusters linked together. Instead of having to analyze a complex system with huge amount of data, the stock market can be analyzed by its topological properties, such as the high clustering coefficient, i.e a star-topology, which will among others point out which stocks have the most influence on others.

Figure 3.1: Network obtained by comparing two stocks correlation coefficient in the Greek stock market (Athens Stock Exchange, ASE) in year 1997. The different colors represent the different sectors of economic activity [Gar07].

Airline routes.   Another real world network which shows the same characteristics as scale-free graphs is the map of airline routes. Figure 3.2 shows the US route map of the American airline company, SkyWest. The characteristic clustering emerges in the figure, where a majority of the flights departs from either Denver, Chicago or San Francisco. Not surprisingly, these airports are all in the top 7 busiest

airports in the US [Faa], and serves as hubs for many of SkyWest flights. In the airline industry some airports are called hubs, because that's what they are, - a connection point for major parts of the network of flights. The network of flights, as depicted in Figure 3.2 follows the characteristics of A-B graphs. Hence, as we also can confirm from looking at the graph, the network are vulnerable against direct attacks. Meaning if a low edge degree airport is shut down, there will be little consequence for the rest of the network. However, if one of the hubs is forced to close, it will provoke huge delays through out the whole network of flights, because many of the destinations are interconnected via the hubs.

Figure 3.2: SkyWest Airline combined route map [CfAPA].

Here, both examples can be characterized as scale-free networks, and the work done by Albert and Barabási shows that a large part of natural systems is in fact scale-free graphs [Aud]. Since we are able to determine the graphs type, which in this case is scale-free graphs, we now know that the graph is vulnerable to attacks directed towards the hubs, i.e. the hubs need to be secured. For example if a delay occurs at a airline hub, these delays will probably cascade throughout the network. This shows the strength of being able to structure systems as graphs. When certain structures appears one can assume that the network will behave according to a set of rules. This is why we wish to determine whether there are any structures that possesses preferred characteristics to be associated with cyber-insurance. And then find a proper way to force these formations to evolve.

3.2   Network Structures

Just like stock markets and airline routes, the cyber-insurance market can be described using graphs. The structure that will evolve is dependent on all the nodes and how they connect with each other. The insurer can determine the cost of establishing link, and thus sort of determine which nodes will connect to each other. This is what we will try to achieve in our models. However, first we need to shield light on what kind of graph structures that would be desirable to force upon the cyber-insurance market.

To find the proper structure, many different scenarios needs to be covered. In the network a node's actions are influenced by their neighborhood structure, i.e. the network connections will affect each individual nodes payoff. Meaning that nodes are dependent on each other, and the probability of cascading failures are highly relevant. -If one or more fail, e.g. bankruptcy, failure to deliver at the expected time, system shut down, huge delays, higher cost etc. Then the whole network will be affected. In this case there are several types of networks to consider, all social and economic interactions where an agents well being is dependent on externalities as well as their own actions, is a network worth considering.

We found several interesting papers originated in evolutionary studies and disease epidemics, which described characteristics in different graph structures. The ones we found appropriate where those who described the benefits of star- and clique-shaped graphs. These graphs showed characteristics who could be used to make it feasible for both the insurer to offer - and the customer to acquire insurance. In addition papers describing network formation games was also interesting for our modelling.

The paper [LHN05] is about evolutionary dynamics and how some structures can amplify or sustain evolution and drift[1]. One aspect of cyber-insurance is risk, and knowledge of how, for example ,viruses spread in a network and how to use graph structures to prevent, both hackers from entering and virus from spreading is important. Evolutionary dynamics, and the research of how mutant genes spread through out a population, as described in the paper is analogous, to this issue. If we can determine some structures, where certain nodes are advantageous/disadvantageous, then these structures will have properties, such as sustaining viruses from spreading, or amplify the incentive for obtaining cyber-insurance.

The paper [LHN05], show that mutants inserted in to a circulation graph, will

---

[1]Drift is the opposite of selective evolution , it is when the network/structure evolve and change at random

have a fixation probability equal to

$$p_1 = \frac{(1 - \frac{1}{r})}{(1 - \frac{1}{r^N})}$$

(3.1)

Where r represents the relative fitness of the mutant, if it is advantageous it will have a certain chance of fixation, and disadvantageous mutants will have a chance of extinction. A circulation graph is a graph that satisfy these two properties:

1. The sum of all edges leaving a vertex is equal for all vertexes

2. The sum of all edges entering a vertex i equal for all vertexes

A clique is a good example of a circulation graph, and the probability of fixation is as in Eq. (3.1). The fixation probability determines how probable it is that the whole network will eventually be "infected" by the mutant. It determines the rate of evolution, which relies on both the size of the network and the evolution speed. If the relative fitness of the nodes are high, then the probability of fixation will be low. A probability equal to one means that every node in the network eventually will be affected by the mutant.

An essential part of cyber-insurance is for the insurer to be able to calculate the overall risk of the instance requesting to be insured. Since the probability of fixation can be calculated in circulation graphs, if the insurer knows that the instance is part of a circulation graph, it is possible for the insurer to calculate the probability of fixation in that network. If we can find graphs with fixation probability that exceeds Eq.(3.1) it is even better, because then the insurer are not only able to calculate the overall probability of fixation, but to also show that the probability of fixation are higher than the one for circulation graphs. The paper shows that there exists such graphs, one example is the star topology, (see Figure 3.3). In this topology the fixation probability is as shown in Eq.(3.2), or for more general see Eq.(3.3).

$$p_2 = \frac{(1 - \frac{1}{r^2})}{(1 - \frac{1}{r^{2N}})}$$

(3.2)

. or more generall:

$$p_k = \frac{(1 - \frac{1}{r^k})}{(1 - \frac{1}{r^{kN}})}$$

(3.3)

When comparing the Eq.(3.1) and Eq.(3.2), we see that the selective difference is amplified from r to r^2, i.e. a star act as an evolutionary amplifier, favoring advantageous mutants and inhibiting disadvantageous mutants.

There exists other graphs where the fixation probability is equal to 3.3, examples are super-stars, such as funnels and metafunnels. These are just more complex star

networks. This paper shows, that as N get large, the super-stars will have fixation probability, for an advantageous mutant, that converges to 1, and for disadvantageous converges to 0. As exemplified earlier in this chapter, we know that there are many topologies in our society that are so called scale-free graphs. These graphs have most of their connectivity clustered in a few verities, which are very similar to a star, and these networks can also be considered as potent selection amplifiers.

The paper [Blu11] present interesting results regarding network formation games. They set up a game where the nodes benefit from direct links, but these links also expose them for risk. Each node gains a payoff of a per link it establishes, but it can establish a maximum of δ links. A failure occur at a node with probability q, and propagates on a link with probability p. If a node fail, it will receive a negative payoff of b, no matter how many links it has established. The characteristics of this game is transferable to how we expect nodes in a cyber-insurance network will interact with each other. Therefore the results of how the overall payoff changes according to different collection of participants. The results from their model shows a situation where clustered graphs achieve a higher payoff when connected to trusted nodes, compared to when connecting with random nodes. Unlike in anonymous graphs, where nodes connect to each other at random, nodes in these graphs share some information with their neighbors, which is used when deciding whether to form a link or not. To further explain these results, they show that there exists a critical point, called *phase transition*, which occurs when nodes have a node degree of $\frac{1}{p}$. At this point a node gets a payoff of $\frac{a}{p}$, and to further increase the payoff the node needs to go into a region with significantly higher failure probability. Because once each node establish more than $\frac{1}{p}$ links, the contagious edges, will with high probability form a
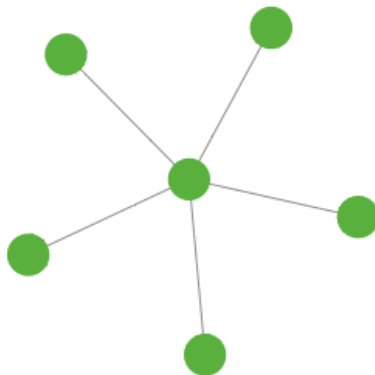
Figure 3.3: A star-topology.

large cluster. Which results in a rise in probability of node failure, and reduces the overall welfare. From this the paper say that when the minimum welfare exceeds $(1 + f(\delta) * \frac{a}{p})$ we have reached super critical payoff. Otherwise it is called sub-critical payoff. Further they show that the only possible way of ending up with super critical payoff, is by forming clustered networks consisting of cliques with slightly more than $\frac{1}{p}$ nodes. However, if the nodes form an anonymous market, by random linking, they can only get sub-critical payoff. In other words, if the nodes can choose who they connect with, and by doing so, creating trusted clustered markets, they can achieve a higher payoff, by exceeding the critical node degree point.

The paper [GGJ$^+$10] shows how network games evolve when the payoffs are determined not only by your own decisions, but also by your neighbors. This can be used to analyze the star network further. They analyze a game on public good, which is simple but highly relevant for our work. A good example of a public goods is security product. A security product suffers from strategic substitutes, i.e. if your neighbor acquire the security product, you have less incentive of also acquiring the security product. This is because when he acquire it, he gets more secure, and so do you, due to the positive externalities of the product.

The game is set up like this: We have an action space: $X = \{0, 1\}$, where 1 can be considered as acquiring information, take vaccine, buy security software etc. And 0 is not doing so. Each node i has a set of neighbors: N_i, and a payoff function $y_i = x_i + \bar{x} N_i$. The gross payoff to player i is 1 if $y_i >= 1$ and 0 otherwise. But each player also suffer from a cost of $0 < c < 1$ if they choose action 1. When looking at

(a)   Socially Optimal equilibrium, center node choose action 1

(b)   Non Socially Optimal equilibrium, leaf nodes choose action 1

Figure 3.4:   Figure 3.4a shows the socially optimal equilibrium, and Figure 3.4b shows the non optimal equilibrium.

Figure 3.4, we easily see that there is two equilibriums. One where the center node choose action 1 and the rest of the nodes choose action 0, and a second equilibrium

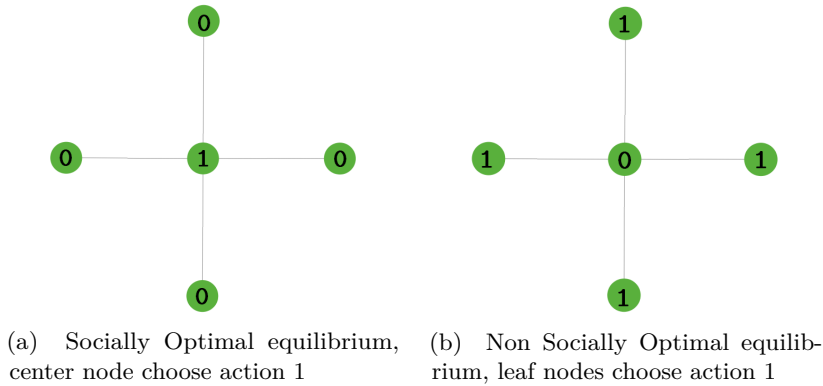where all the leaf nodes chooses 1 and the center choose 0. The overall payoff in these two differ from each other, the latter is not socially optimal because it suffers from a cost equal to: $\#leafnodes * c$, while the other equilibrium only have a total cost of c. It would have been beneficial if we where able to force the game to always end up in the social optimal equilibrium.

From a insurers point of view.   If a insurance company could identify these star-structures, and force them to end up in the social optimal equilibrium, i.e. minimize the overall cost of link establishment, it would have been very beneficial for both the insurer and the customers. First of all if the insurer could identify these structures, he could calculate the overall probability of fixation by a diseased mutant(virus, worm, trojan or other failures). If they could ensure that the center node is protected they could also calculate the probability of the diseased mutant being extinguished from the network, and possibly being able to almost ensure that the network is secure. One possibility of achieving this could be by offering very cheap insurance to the leaf nodes, and giving the center node an incentive to acquire security product, by informing the center node about the probability of failure unless he acquires security. And offer him a very good rebate if he acquires the security product, and a very expensive insurance if not. In this way the insurer could force a rational center node into getting both insurance and a security product, and thus securing the whole network.

This is a simple scenario, analyzing an exogenous network formation [2], but it shows how a insurer can, force a star network to end up in the social optimal cost equilibrium. And how he can use this to provide better overall security for everyone. We also showed how the insurer can calculate the probabilities of failure in circulation-, star-, funnel-, meta-funnel- and super star,-graphs. And how nodes forming a trusted clique, can achieve a higher payoff than nodes in an untrusted clique. All this could contribute significantly to solving some of the problems with cyber-insurance. The problems with information asymmetry and interdependent risk problem has been reduced, since if the insurer knows the network structure, he can calculate the probabilities of failures and catastrophic events. If the network is a star and he can ensure that the center node is secure, the interdependent risk problem is limited to the security of the center node.

3.3   Research Question

So far, our thesis have introduced cyber-insurance, presented related work on the issues regarding cyber-insurance and this chapter have presented the properties

---

[2]Exogenous: The network formation is given. Endogenous: The structure originates from within the network, i.e. the opposite of exogenous

of different graph structures and briefly introduced the idea of network formation. Generally, the papers in the related work section have presented different models to try solving the problems with cyber-insurance. Nevertheless, as we have seen, the cyber-insurance market still fails to evolve completely, despite all the solutions presented in different papers. This is why we have chosen to take a different approach. In this chapter, we have shown some structures, especially the star and clique, which will generate benefit for both the insurer and customers in a cyber-insurance market. We will combine the knowledge of these structures and network formation to investigate whether it is possible for the insurer to force these structures to evolve endogenously. We will focus on how the insurer can determine the resulting formation by adjusting the parameter he can control, i.e. the insurance cost. We know that if the insurance premium is high, no one will buy it. On the other hand, if it is too low, everyone would benefit from having insurance, and insured nodes will make risky decisions, such as connecting to risky nodes. We will try to determine whether it is possible to find the intersections, where the desired structures will be create, and both the insurer and their customers will benefit from this.

NOTES. research question   All the other models to this... We will try a new approach... Combine knowledge of graphs, and network formation. We will investigate whether it is possible for the insurer to control the formation of the cyber-insurance network. So that we end up with a star or clique. Our approach will focus endogendous formation by controlling the cost parameters for the insurer. Hence if the insurance premium is high, no one will buy it. On the other hand, if it is free, everyone would benefit from having one, and clique formations will emerge. We are interested in finding the intersections, where both the insurer and their customers will benefit from cyber-insurances.

Chapter 4

Methodology

Our approach requires some basic understanding on graph theory, in addition game theory will be used to explain and prove our assumptions in our modeling work. To be able to visually confirm that our assumptions where correct, we created simulators using NetLogo.

4.1 Graph

As described earlier, graphs works as analytically tools when studying complex systems, and we will use graphs extensively throughout this thesis. Therefore it is important to establish a understanding of basic properties of graphs. Figure 4.1 depicts the basics of an unweighted graph, where the edges are not assigned any value. Weighted edges can be useful to e.g. reflect capacity constraints such as a link's maximum bandwidth, or the length of a road(edge). Other common definition used when describing graphs are listed below [Aud]:

- Edge degree: Number of edges connected with a node.

- Hub: Node with high edge degree.

- Cycle: A chain originating and terminating at the same node.

- Cluster: Subgraph of highly connected nodes.

- Cluster coefficient: Probability that two nodes that are adjacent to a third node are also adjacent.

- Clique: Subgraph where all nodes are adjacent (cluster coefficient = 1).

- Small world graph: Graph with small diameter and large cluster coefficient (e.g. the Internet and A-B graphs, described in section 4.2).

Figure 4.1: General graph [Aud].

4.2   Random Graphs

Cyber-insurance cover many fields, from financial transactions and outsourcing of tasks to computer networks, many of these fields share a common characteristic, they can all be described as a graph, and often a random graph. Therefore the study of random graphs are of special concern. The research on random graphs are fairly new compared to other mathematical discoveries. E-R graphs were first studied in 1959 by Erdös and Rényi, later and probably with more promising results was the graphs studied by Albert-Barabási in 1999 [Aud].

Erdös-Rényi Graphs.   E-R graphs is a network created between a fixed number of n-nodes, where each node connects to another of the $n-1$ nodes with probability p. The resulting graph will on average contain $\frac{n(n-1)p}{2} \approx \frac{n^2p}{2}$ edges [Bol85]. By analysing the graph, the authors found some interesting properties:

– If $p < n^{-2}$ then there is no edges in the graph.

– If $p = c/n$ where c is a constant between $1 < c < log\ n$, the graph will provoke a single large component to grow within the graph.

– If $p > (ln\ n)/n$ then the graph is completely connected.

– If $p = 1/n$ triangles start forming in the graph.

A fully connected E-R graph will have a short diameter similar to the Internet, and thus could be a very good description of structures similar to the internet. However, the edge degree follows a Poisson distribution, which means that the edge degrees are peaking around the average value [Aud]. Consequently E-R graphs does not capture the immense clustering coefficient which is present in networks such as the Internet. In other words, E-R graphs are not small world graphs, and another graph structure is needed to model computer networks. An interesting fact about these graphs are their vulnerability. These graphs are very vulnerable against random attacks, such as nature disasters, but robust against directed attacks. Due to the fact that if you remove all edges from one node, it does little damage, since the network is not dependent on single nodes. Every node has approximately the same node degree, and it is the sum of all the nodes connections that creates the network.

Albert-Barabási Graphs.   The structure which is believed to be most accurate regarding modeling computer networks are A-B graphs. A-B graphs are different from E-R graphs since they are scale-free, meaning that the vertices does not have an constant value throughout the entire graph. The formation of an A-B graph results in multiple hubs with a high edge degree. Albert and Barabási found that the edge degree of each vertex follows a power law distribution; meaning that the probability that the edge degree is g is proportional to $g^{-\gamma}$ where γ usually is a number between 2 and 3 This distribution is called a thick-tail distribution, because there is a significant probability that a node may have a very high degree. [Aud] These graphs are in contrast to E-R-graphs, very vulnerable to directed attacks, because if you take out a hub, you suddenly destroyed the whole graph. But the graph is very robust against random attacks, this is why most of the networks we observe in the nature can be depicted as A-B-graphs. A-B graphs can grow and become scale-free if every new vertex is connected to one or more already existing node with a probability proportional to the edge degree of that node . The paper presents an algorithm that creates A-B graphs and Figure 4.2 shows one graph that evolved from this algorithm:

– A new single vertex is added to the graph.

– This vertex is connected to exactly two other vertices in the graph.

– The probability that the new vertex connects to another vertex is dependent on the edge degree of the other vertex, higher edge degree meaning higher probability

– There is only one edge between two vertices.
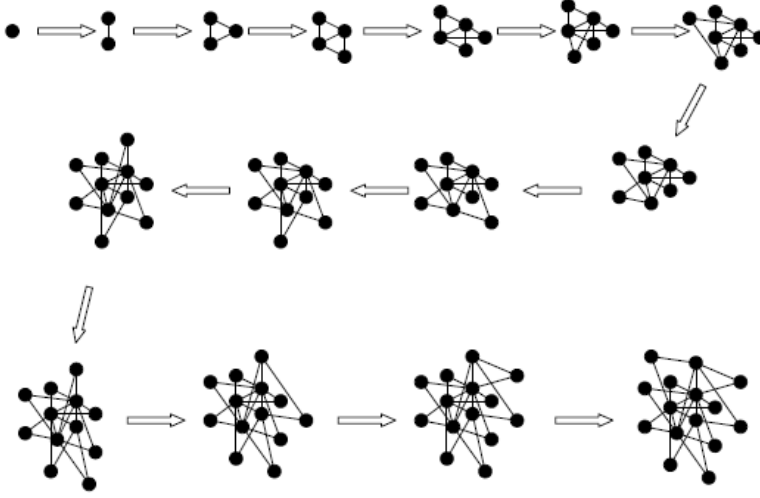
Figure 4.2: Forming a A-B graph in 15 generations [Aud].

In addition to the high clustering coefficient they showed that A-B-graphs have a fairly small diameter, which can be seen in Figure 4.2. A-B graphs are therefore comparable to the network formation of the Internet and other computer networks.

4.3   Game Theory

Here we will present some of the game theory concepts we use in our models, for more thoroughly explanation of game theory, see: [NRTV07, Wat08].

One shot game   This type of game assumes that players act at the same time instant, therefore there is no causality. A game in strategic (normal) form can be described by three elemetns:

- the set of players $i \in I$, which we take to be the finite set $1, 2, ..., I$.

- the pure-strategy space $s_i \in S_i$ for each player i, where s_i is a possible action of player i.

- and payoff functions U, which gives the players utility functions for each profile $s = (s_1, s_2, ..., s_I)$ of strategies.

A general solution concept for games of economic interest is the Nash Equlibrium solution. A Nash Equilibrium is a profile of strategies such that each players strategy is an best response to the other players strategies.

Nash Equilibrium   A pure strategy profile s^* is a Nash eqilibirum if, for all players i

$$U_i(s_i^*, s_{-i}^*) \geq U_i(s_i, s_{-i}^*) \in S_i \tag{4.1}$$

Stackelberg   Also known as a leader-follower game, it introduces multiple stages. The leader commits itself first, chooses its strategy, then the followers respond sequentially. The Stackelberg model can be solved to find the subgame perfect Nash Equilibrium, i.e. the strategy profile that serves each player best, given the strategies of the other players and that entails every player playing in a Nash Equilibrium in every subgame.

Subgame-perfect equilibrium   A strategy profile s is a subgame perfect equilibrium if it represents a Nash Equilibrium of every subgame of the original game.

Socially optimal   A socially optimal outcome is the set of choices that maximizes the sum of all players payoffs.

Price of stability   The price of stability (PoS) of a network game, is the ratio between the maximum sum of the players payoff, in a stable outcome, and the Socially optimal outcome.

Bayesian game   In Bayesian games, information about the other players characteristics is incomplete. In these types of games, there are one player(the agent) who knows both types, and another player (the principal) who does not know the type of the other player.

A pooling equilibrium, is a equilibrium where all both types of the agent chooses the same action, i.e. the principal is not able to distinguish the two types. A separating equilibrium is an equilibrium where the agents of different types, choose different actions, and thus the principal is able to determine the agents type by observing his actions.

4.4   Netlogo

In addition to analyzing the different models with game theory, we created a simulator for the models, in a program called Netlogo. Netlogo is a programmable modeling

environment for simulating natrual and social phenomena. It is well suited for modeling complex systems developing over time [Wil]. Netlogo where good to model our complex network formation games, and at the same time provided us with a good graphical user interface, that enabled us to see the result of the games, and also to easily adjust the different parameters. In Figure 4.3 we see the user interface, which are used to setup the parameters, start the modeling, and showing the resulting network formation. Figure 4.4 shows how the coding interface looked like. For detailed overview of the code used in our different models, see the appendix.
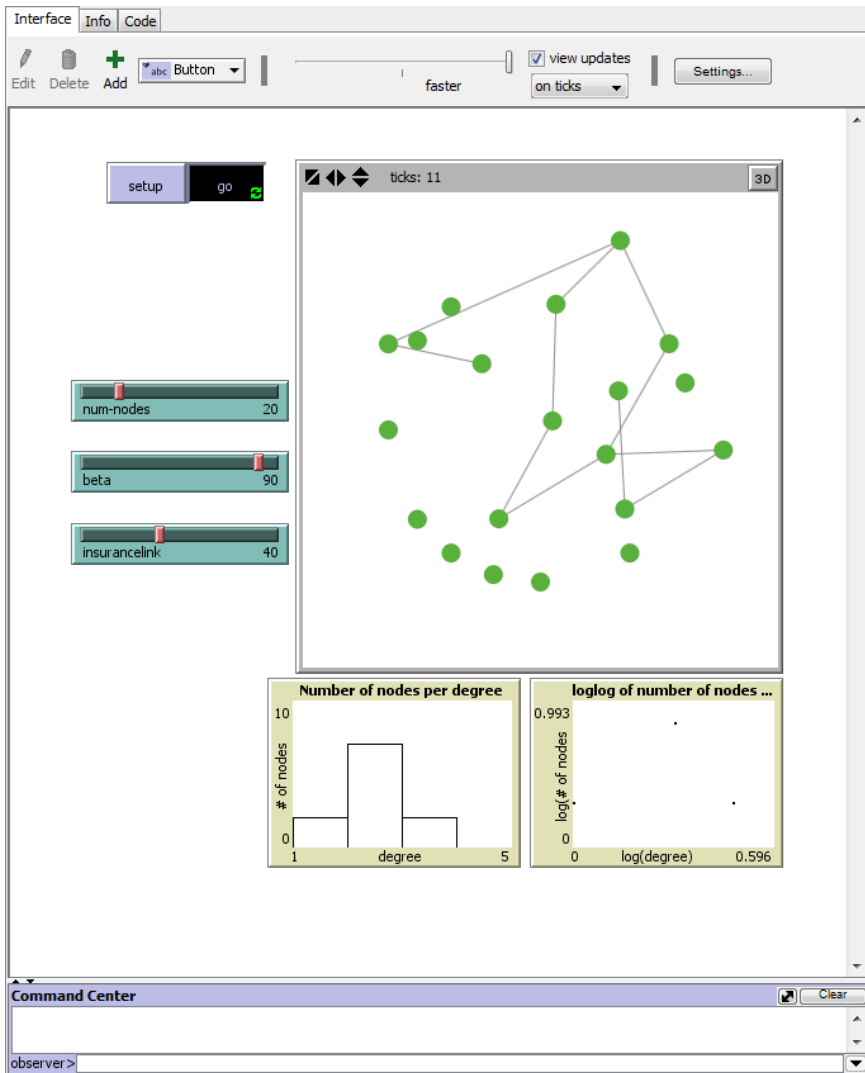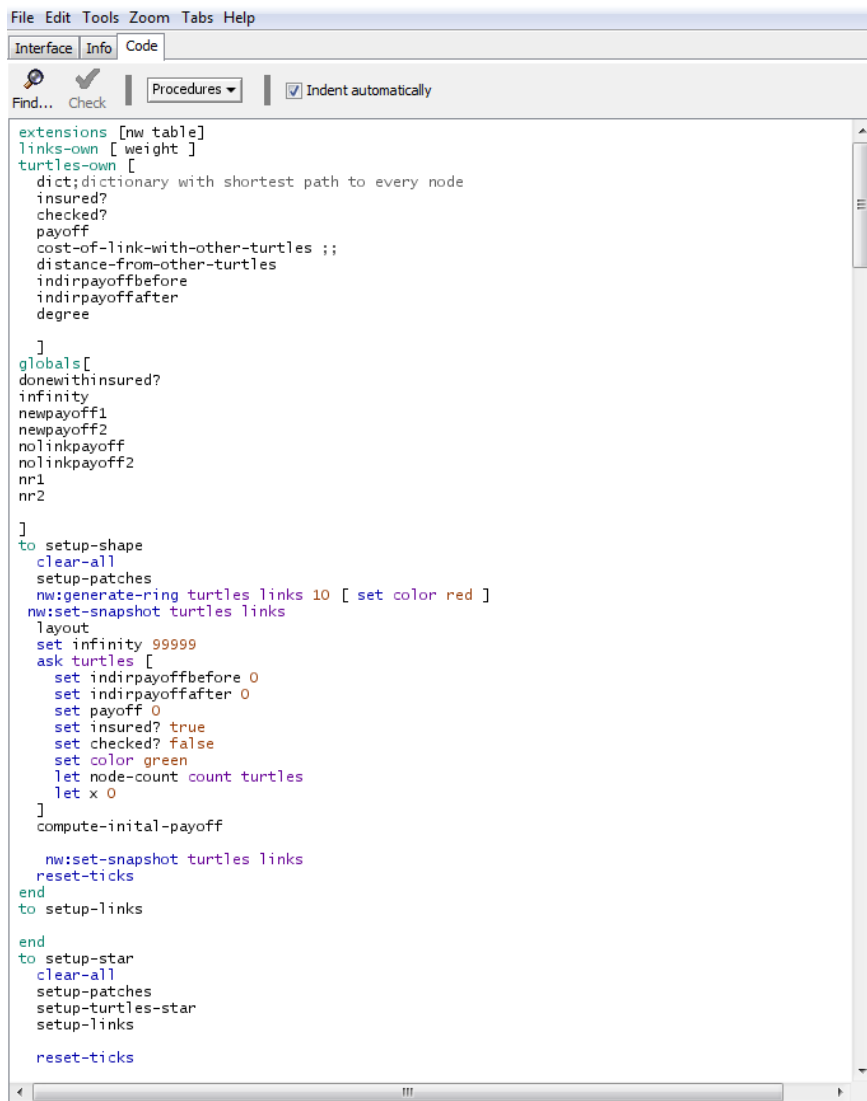
Figure 4.3: The figure shows a screen capture of netlogo, while we are running one of our simulations.

Figure 4.4:   The figure shows how the code interface in netlogo looks like.

Modeling Cyber-Insurance

In many scenarios nodes seeks to create networks in order to directly benefit from each other. The established links might represent companies out sourcing part of their manufacturing, or cooperative agreements in the development of new software products. In addition to increase the trade-off, each of the established links represents risk of being a victim of cascading failures. The intuitive example is the spread of epidemic diseases, also node failures of a power grid and financial contagion such as the one back in 2008 was a result of cascading failures. Strategic network formation using cyber-insurance can be used to prevent such situation in addition to increase the overall payoff of participants in a clustered network.

When deciding whether to establish connection to a neighbor agent, the payoff has to be higher in the balance between the expected earnings and the risk of the other party failing to complete the transaction. This is the reason why we seek to only download content from trusted peers and outlaw MC-gangs are consistently skeptical to enter into new agreements despite promising increased earnings, since the risk of undercover police are too high.

The model from [Blu11] described in the related work chapter introduces a model where each node benefit from direct links to other nodes. However establishing a link will expose them to a risk if the node is not protected. Information about other nodes status (in our case, insured or not) will help nodes to guarantee cliques consisting of only the insnured nodes. According to the paper, such cliques will result in super critical payoff for every node connected.

One of the problems with cyber-insurance is to define and calculate the risks, because the network structure is undefined. If an insurer where able to predict the network structure, the calculations of overall risk would be realizable, and even better if the insurer where able to force some more robust network structures to evolve. Examples of such structures are as described in the graph theory chapter, scale-free network, which have been proven to be very robust against random attacks.

Star-topologies, or star-like topologies, have a fixation probability that exceeds the fixation probability of circulation graphs. Star structures also have the nice property of minimizing the average path length, i.e. minimizing the cost spent on establishing links. In our thesis we want to find structures who can be analyzed by the insurer. The two main types of structures we will focus on are the clique and star-like structures. Since both of these have been identified to have calculable fixation probability. They also have other properties that are desirable for the insurer, such as the possibility of amplifying or suppress selection and drift. This is very desirable, because if the insurer is able to ensure that the nodes have a certain security level, especially the center node, then he can ensure that viruses does not spread. The clique has the nice property of being able to achieve super critical payoff, as showed in [Blu11].

Introduction to the modeling.   There are many examples of nodes needing to establish connections, one example is a company needing to out-source certain tasks to remain competitive. This outsourcing involves some risks, such as, will the company deliver at the reported time, to the reported costs, what happens if they fail to deliver, what if they go bankrupt etc. If the companies that are going to establish links(cooperative contracts), know that the other firms are insured, it will be more secure and reliable to enter into an cooperative agreement. In this way trusted cliques can evolve. The firms benefit from connecting to other insured firms, and the insurance company can offer fair prices to the insured companies, because the risk is calculable in a trusted clique.

So our goal with the models are to find out how and when different networks evolve, and how the insurer can ensure that this will happen, by adjusting the parameter he can control, the insurance cost.

In this chapter we will start out with a simple model, model 1: Initial Model, and adding new features to make the models more realistic and applicable to real world scenarios. An overview of the models we have created can be seen in Figure 5.1. For some of the models we created a simulator, to show and confirm the result of our calculations. This was done for model- 2,3 and 5.

5.1   Model 1: Initial Model

As a starting point the model is highly simplified in order to show the concept of how cyber-insurance can be used to separate insured and non-insured nodes into two cliques. We assume that every node has complete network information, i.e. it knows how many nodes that exists, and whether they are insured or not. The link establishment process is bidirectional, meaning both nodes must agree to establish the connection.
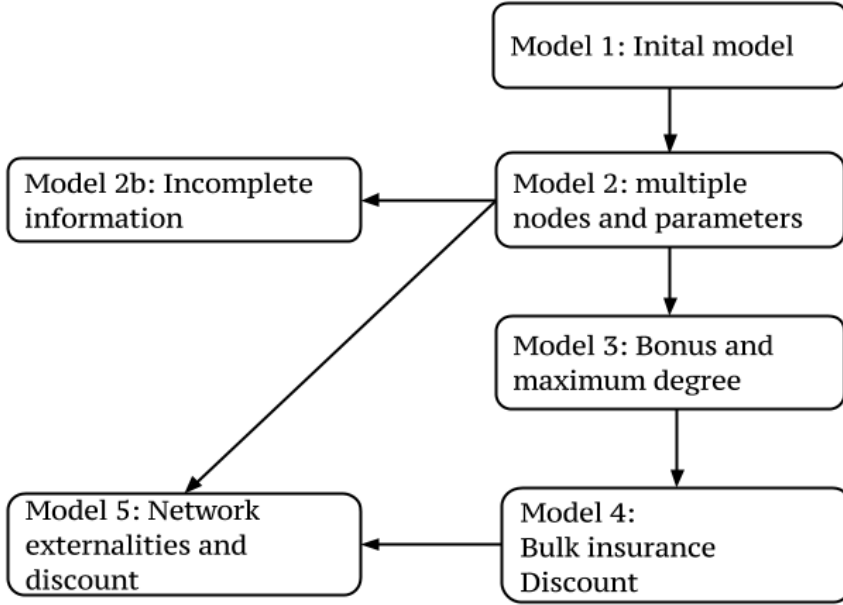
Figure 5.1: The figure show an overview of the different models we have created, and how they relate to each other. For every step, there are added some new features to the model.

For the first model, we assume a set of n nodes that are randomly chosen to be insured or not, as depicted in Figure 5.2a. They all get their own fixed income, and by connecting to other nodes they can increase their payoff. Non-insured nodes will have a risk of failure, which we model as an expected cost of failure. Therefore if an insured agents chooses to connect to a non-insured nodes they will also suffer from this expected cost of failure. To simplify the decision process, the model follows a rule that only allows insured to connect to other insured agents and non-insured agents can only connect with each other. The resulting graph will be two fully connected cliques, one consisting of insured agents and the other of non-insured agents, as shown in Figure 5.2b.

This dichotomy represents a trusted environment for the insured nodes, because they know that each node in the clique is insured against risk. These nodes will benefit from each connection without having to worry about contagious risks from the connected nodes. A node in the non-insured clique will also experience a change in payoff from the links it has established, however each of the links has a probability of failure. Hence this environment is not trusted, and a link establishment will always involve some risk.

The first model, although very simple, shows an topology where insured agents benefit from being insured, and are candidates to achieve super critical payoffs as described in [Blu11].

(a) 15 Agents randomly choosen to be either insured (green) or non-insured (red).

(b) Two clustered networks. One consisting of insured agents the other consists of non-insured.
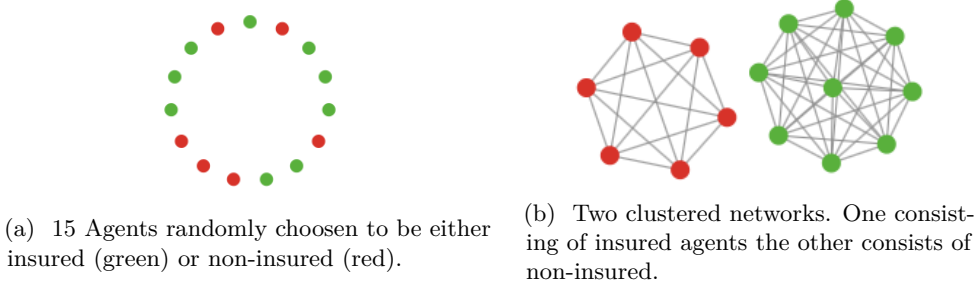
Figure 5.2: Shows how agents connects to eachother according to model described in section 5.1.

5.2   Model 2: Including Parameters

The first model is highly simplified and suffer from many limitations, among others it is too simple to reflect the dynamics of a real world scenario, where nodes will have different variables with different values. To improve this model we have to introduce parameters, that can be adjusted and reflects real world scenarios. It is fair to assume that the insured nodes must pay an insurance premium, and this premium should be dependent on the number of links the node establishes. When two insured nodes establish a link between each other, they both have to pay a premium, this is to make the game more fair, and more realistic. For example if the two nodes had different insurance companies, then both companies would charge them for insuring the link. When a node, insured or not, establish a link to a non-insured node, this involves a risk, and this risk will be represented as an expected risk cost. However, if the changes in payoff when establishing a link is only negative, then no node would want to establish links. Thus nodes will also receive a positive change in payoff when establishing different links.

5.2.1   Characteristics of the model

The process of establishing link is a bidirectional decision. The insurance premium is I_l, the expected risk cost is represented by r. β represents the benefit of establishing a link. Table 5.1 presents an overview of the parameters.

β - income from establishing a direct link
I_l - increased insurance cost per link the node establishes
r - expected risk cost

Table 5.1: Table showing the different parameters

Two nodes scenario

As a starting point lets look at the scenario involving only two nodes. In this game the strategy space of both players consist of four different strategies. A node can be insured or not, and choose whether to establish a link to the other node. I.e. the different strategies are: Be insured and establish link noted as: IL, be insured and not establish link: $I\overline{L}$. Not insured and establish link: $\overline{I}L$, and not insured and not establish link: $\overline{IL}$. It should be noted that since the decision to establish a connection is bidirectional, both have to choose a strategy where they want to establish a link, for the link establishment to be successful. Hence we end up with the game as shown in Figure 5.3.

As long as both I_l and r is less than β, the only nash equilibrium in Figure 5.3 is when both nodes chooses $\overline{I}L$. If we first look at node A, we see that when node B chooses IL, the best response is $\overline{I}L$, because $\beta > \beta - I_l$. And since the game is symmetric, the same holds for node B. When one of the nodes chooses $\overline{I}L$, the best response will be $\overline{I}L$, because $\beta - r > \beta - I_l - r$. And thus the only nash equilibrium is when both nodes play $\overline{I}L$.

This means that two nodes will end up in a classic prisoner's dilemma [1], where the best response is actually worse than the social optimal. In this case it is trivial to see that the social optimal scenario is for both nodes to choose IL, as long as $I_l < r$. However, the nodes will choose not to buy insurance. Or else they could risk ending up in a situation where only one of them pays the cost of insurance.

Introducing time.   One possibility for solving the problem where the two nodes end up choosing not to acquire insurance is to introduce a leader follower game. In this game the players does not act at the same time, but in a given order, and they can observe the other players action. If we consider a game with only two players, player one select strategy, insure or not, first. Then after observing this action player two chooses if he would like to insure or not. Then they choose if they would establish link or not, in the same order. In this type of game the leader, will benefit from a

---

[1]Prisoner's dilemma was originally framed by Merrill Flood and Melvin Dresher in 1950. The dilemma expresses a situation where two players each have two options whose output depends on the simultaneous choice made by the other. The original dilemma concerns two prisoners which separately decides whether to confess to a crime [Dic]. It is a paradox in decision analysis which shows why two individuals might not cooperate, even if it is in their best interest to do so.

Node A \ Node B	IL	$\overline{I}L$	$I\overline{L}$	$\overline{I}\,\overline{L}$
IL	$\beta - Il'$, $\beta - Il$	0 , 0	$\beta - Il - r$, β	0 , 0
$\overline{I}L$	0 , 0	0 , 0	0 , 0	0 , 0
$I\overline{L}$	β , $\beta - Il - r$	0 , 0	$\beta - r$, $\beta - r$	0 , 0
$\overline{I}\,\overline{L}$	0 , 0	0 , 0	0 , 0	0 , 0

Figure 5.3: Normal form game, showing the different strategies and the payoffs for the different outcomes. The payoff are written in this order, A then B's. An agent has a strategy space of size 4.

first mover advantage, because he can now force the game in the direction he prefers. We solve this by using backward induction on the extensiveform game, shown in Figure 5.4, and finding all the different subgame equilibrias. We assume that Eq. (5.1) holds. When we have worked our way back to player 1's first decision, Insure or not, we have this subgame equilibria:$(L_1, \overline{L_1^I}, \overline{L_1^{II}}, L_1^{III}), (I_2, \overline{I_2^I}, L_2 L_2^I, \overline{L_2^{II}}, L_2^{III})$ This means that player 1 now what will happen if he chooses to acquire insurance or not, if he acquires, he will get payoff: $\beta - I_l$, if does not acquire, he gets: $\beta - r$. And as long as $I_l < r$, he will chose to acquire insurance, and by doing this forcing the game to end up in an equilibrium where both players acquires insurance and would like to establish link.

$$I_l < \beta \text{ and } I_l > \beta - r \text{ and } r < \beta \qquad (5.1)$$

From this we see that if the insurance price are set to the right amount, the first player can force the outcome of the game to be the socially optimal outcome. The problem with this way of solving the problem is that it is very hard to solve for multiple nodes, because the extensive form game becomes extremely complicated. And that we are forcing the nodes to act in a given order. This is not done in the other models.

5.2.2   Multiple nodes

Assumptions

To make the modelling possible, we will from now on assume that the type of the nodes are given in advance, i.e. they are chosen to be insured or non-insured with a probability given in advance, and every node knows their own and others type. The reason for this is because, we are focusing on endogenous network formations, and by introducing this decision process it would only drastically increase the complexity of the models.

To make the model realistic we now introduce a multiple nodes. The objective of this model is to find characteristic network formations that will evolve endogenously when the parameters are within certain conditions. Examples of characteristic networks of interest are cliques, scale-free and star networks. We assume that every node has complete information of the network, i.e. every node knows the type of the other players. This is a very strong assumption, however in financial transactions and in cooperative software development networks, it is reasonable to assume that the parties can acquire this type of information prior to establishing a financial contract with each other. And as we will show in Section 5.3, when we introduce incomplete information between the nodes, it will not be possible to separate the two types, since they will have to act on beliefs.

Figure 5.4: Leader follower game, first player 1 chooses to insure or not, then player 2, and then they choose to establish link or not in the same order.

Analysis

As mentioned our goal is to find how and when certain network formations evolve. We know that if a node can increase his payoff by establishing a link, he will do so. Thus we can start analyzing the four possible link establishment scenarios, insured to insured, insured to non-insured, non-insured to insured, and non-insured to non-insured. Let U_i denote the payoff of a node with degree i, and let U_{i+1} be the payoff a node will receive if it establishes a new link.

Insured to insured. When two insured nodes are considering establishing a link, they will do so, if and only if both receive a higher payoff. In this scenario the the payoff function of adding a link is as shown in Eq.(5.2).

$$U_{i+1} = \begin{cases} \beta - I_l, & \text{if } i = 0 \\ U_i + \beta - I_l, & \text{if } i > 0 \end{cases} \tag{5.2}$$

For a link to be established between two insured nodes, Eq.(5.3) has to hold.

$$I_l < \beta \qquad (5.3)$$

Non-insured to insured. The payoff a non-insured receives by connecting to a insured is as described in Eq. (5.4). As we see this will always be a positive change in payoff, and thus an non-insured node will always choose to connect to an insured node.

$$U_{i+1} = \begin{cases} \beta, & \text{if } i = 0 \\ U_i + \beta, & \text{if } i > 0 \end{cases} \qquad (5.4)$$

Insured to non-insured. The payoff an insured node receives in this scenario is as follows:

$$U_{i+1} = \begin{cases} \beta - I_l - r, & \text{if } i = 0 \\ U_i + \beta - I_l - r, & \text{if } i > 0 \end{cases} \qquad (5.5)$$

For this to happen Eq.(5.6) has to hold, a non-insured node will always want to connect to an insured one, so this is the only condition that is needed for this to happen.

$$I_l + r < \beta \qquad (5.6)$$

Non-insured to Non-insured. The payoff a non-insured nodes receives when connecting to another non-insured node is as follows:

$$U_{i+1} = \begin{cases} \beta - r, & \text{if } i = 0 \\ U_i + \beta - r, & \text{if } i > 0 \end{cases} \qquad (5.7)$$

For this link-establishment scenario to happen Eq.(5.8) has to hold.

$$\beta > r \qquad (5.8)$$

Forming a trusted clique. We want to find the conditions for when different network structures will evolve, for example a clique of only insured nodes. For this to happen, all insured nodes must connect to each other, i.e. Eq.(5.3) has to hold. But we also need to ensure that insured nodes do not establish links with non-insured nodes. I.e. this has to hold:

$$I_l + r > \beta \qquad (5.9)$$

This gives us the limitation shown in Eq. (5.10) on the insurance link cost.

$$\beta - r < I_l < \beta \qquad (5.10)$$

As we see from the condition, if the link insurance cost is between the two boundaries all the insured nodes will connect with each other, and no other nodes. If the link insurance cost is greater than β, then no insured node will establish any links. And if it is below $\beta - r$, then the insured nodes will also connect to the non-insured ones. It should also be noticed that as long as $r < \beta$, then the non-insured nodes will connect to each other.

5.2.3 Result and findings

From the analysis we found different conditions on the link establishment process. If Eq.(5.10) is fulfilled, then the network will end up with one clique of only insured nodes. The non-insured nodes will end up in another clique if the risk of connecting to another non-insured node is less than the benefit of establishing link($r < \beta$). If the link insurance cost and risk of connecting to non-insured nodes is less than the benefit($I_l + r < \beta$), then insured nodes will also connect to non-insured nodes. And the network will end up in one giant clique.

These findings is independent of number of players, because we only consider one link at a time, and the change in payoffs is linear an independent of the nodes degree.

Stability and efficiency   When measuring stability in this model, it is easily seen that since the change in payoff when adding links is linear, and non-dependent on the nodes degree, the resulting network will be pairwise-stable. It also follows from the definition of a Nash equilibrium, that the resulting network is an equilibrium, since every player have best responded to the other players best responses, and no node can increase its payoff by single handedly changing a strategy. To calculate the efficiency we need to sum up the overall payoff, and compare it with the maximum possible payoff. I.e. we want to find the price of anarchy. The total payoff can be calculated as in Eq.(5.11), where $\sum I \times I$ represents the sum of payoffs achieved from links between insured nodes. $\sum I \times \bar{I}$ the sum of payoffs achieved from links between non-insured and insured, and $\sum \bar{I} \times \bar{I}$, the sum of payfoss achieved from links between non-insured and non-insured nodes.

$$U_{total} = \sum I \times I + \sum \bar{I} \times \bar{I} + \sum I \times \bar{I} \qquad (5.11)$$

When the parameters are inserted in Eq.(5.11), we get the Eq.(5.12), where N_I and $N_{\bar{I}}$, represents the number of insured and non-insured nodes in the network.

$$U_{total} = N_I(N_I - 1)(\beta - I_l) + N_{\bar{I}}(N_{\bar{I}} - 1)(\beta - r) + N_I N_{\bar{I}}(2\beta - r - I_l) \qquad (5.12)$$

If we calculate the overall payoff for a network with one-clique of insured and another with non-insured, i.e. Eq. (5.10) and $r < \beta$ has to hold. The total payoff is as shown in Eq. (5.13).

$$U_{total} = N_I(N_I - 1)(\beta - I_l) + N_{\bar{I}}(N_{\bar{I}} - 1)(\beta - r) \qquad (5.13)$$

However, this is not the socially best outcome, because there are no links between insured and non-insured, which would have contributed with $2\beta - r - I_l$ for every link, and since $2\beta > r + I_l$, will be true, as long as both the insurance cost and the expected risk cost is less than β. Thus the socially best outcome would have been one clique, with both insured and non-insured nodes. The formula for calculating the price of anarchy is shown in Eq. (5.14).

$$PoS = \frac{N_I(N_I - 1)(\beta - I_l) + N_{\bar{I}}(N_{\bar{I}} - 1)(\beta - r)}{N_I(N_I - 1)(\beta - I_l) + N_{\bar{I}}(N_{\bar{I}} - 1)(\beta - r) + N_I N_{\bar{I}}(2\beta - r - I_l)} \quad (5.14)$$

An interesting thing to notice is that the only scenario where the insurer are able to separate the two types of nodes, and at the same time ensuring an efficient and stable outcome, is when there are only links between insured, or between non-insured, or no links at all. This can only happen when $2\beta < I_l + r$, and $I_l > \beta + \beta - r$ or $r > \beta + \beta - I_l$ or if both I_l and r is larger than β.

Simulation of the results

To verify that our calculations of the network formation where consistent with the assumptions, we performed different simulations using NetLogo. The network formation is performed by selecting two random nodes, not neighboring each other, then both nodes checks whether they would prefer to establish a connection or not. The rules are as described earlier, when a node is considering establishing a link it chooses to do so if the payoff received is larger than the payoff he already poses, and the decision is bilateral. In the simulator a node is insured with a probability, p. This selection is repeated until the network are fully connected or no more nodes are willing to establish new connections. By selecting nodes at random and checking if both of them would like to connect to each other, we relax the assumption of full network information, because now nodes only get to know if another node is insured or not, when they ask each other.

In Figure 5.5 we see the result of a simulation with the parameters: $\beta = 0.9$, $I_l = r = 0.5$. With these parameters the Eq.(5.10) holds, and $r < \beta$. Thus the network formation game ends up in two cliques, one with insured nodes and another with non-insured. The result are shown in Figure 5.5b, and confirms our calculations. The price of anarchy in this scenario is: $PoA = \frac{8}{15}$. In this figure there are only included $n = 10$ nodes, this is done to make the figure readable and easy to understand. Similar results where obtained when performing the simulation with larger values of n, however the resulting printouts included to many nodes and links to be included.

In the next simulations, the parameters were chosen to violate the Eq.(5.10). The result can be seen in Figure 5.6. In figure 5.6a we see the result when $I_l < \beta - r$, the result is one clique of both insured and non-insured nodes, and the price of anarchy is 1, i.e. this is the socially optimal outcome. In figure 5.6b the insurance cost is $I_l > \beta$,

(a) Ten nodes randomly, with probability 0.5, chosen to be either insured (green) or non-insured (red).

(b) Two clustered fully connected networks. One consisting of insured agents the other consists of non-insured. The link establishment is done by following the rules described above
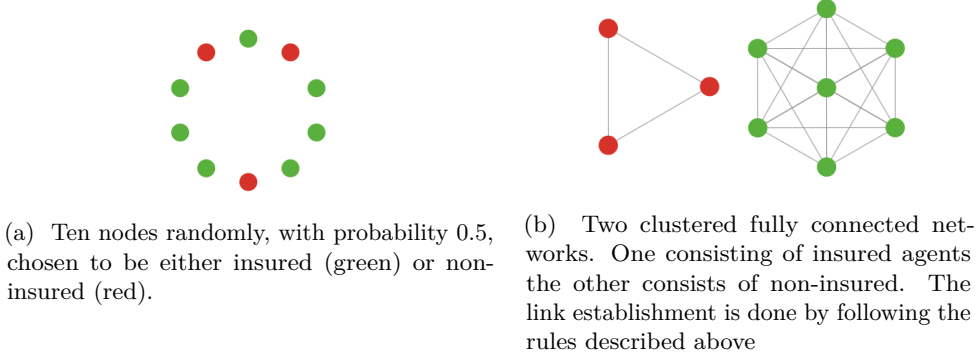
Figure 5.5: The figure shows the resulting network from a simulation with parameters: $\beta = 0.9$, $I_l = r = 0.5$.

and as we see only non-insured nodes connect to each other, because the insurance cost per link is higher than the benefit given from connecting to a new node, i.e. the insured ones choose not to establish any connections. The price of anarchy in this scenario is: $PoA = \frac{32}{35}$, and is thus close to the socially optimal outcome.

(a) Ten nodes insured with probability 0.5, the parameters where: $\beta = 0.9$, $I_l = 0.3$ and $r = 0.5$. I.e. the link insurance cost, I_l, is violating the condition in Eq.(5.10), and the resulting network is one clique of both insured and non-insured nodes.

(b) Ten nodes insured with probability 0.5, with parameters as before, except for the link insurance cost:$I_l = 0.95$. This resulted in a clique of only non-insured nodes.

Figure 5.6: The figure shows the two possible scenarios that violates the Eq.(5.10), 5.6a shows the result when $I_l < \beta - r$ and 5.6b shows the result when $I_l > \beta$.

5.3   Model 2b: Model with incomplete information

An interesting scenario to model is when the nodes lack information about the other nodes type. The way we model this is by letting nature selecting whether a player is insured or not, a node is insured with probability p, and not insured with probability

$1 - p$. All nodes know their own type, but in the link establishment process there are only one node who knows the type of the other. The other node only know the probability of the other node being insured or not. We want to see if it is possible for the nodes with incomplete information to distinguish an insured node from a non-insured one.

5.3.1   Analysis

When facing a game like this, there exists two types of equilibriums, one where node 2 is able to seperate node 1's type, called separating equilibrium. And another where he is not able to separate them, called pooling equilibrium. We have two types of node, type 1 ($t1$): insured and type 2 ($t2$): not insured.

Node 2 is insured.   There are two different games to model, one where node 2 is insured, and the other where he is not insured. We start with the one where he is insured. Node 1's type is chosen randomly by nature, with probability p of being type 1 and $1 - p$ of being type 2.
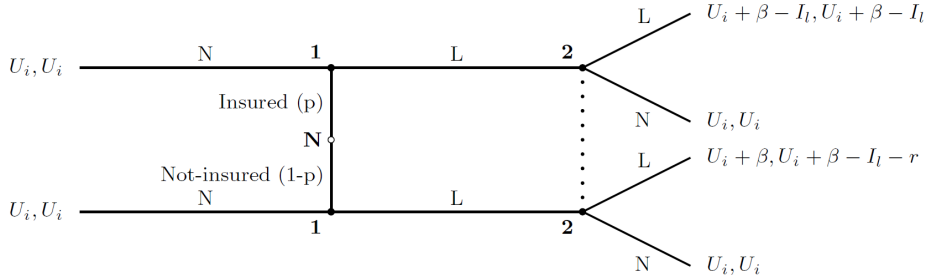
Figure 5.7: Signalling game with two nodes, node 1's type choosen by nature, node 2 is insured. Node 1 have complete information, node 2 suffer from incomplete information, and act on best response functions based on beliefs.

In the extensive-form shown in Figure 5.7, we see that $t2's$ strategy L dominates N, and thus $t2$ will never play N.

Separating equilibrium.   Since node 1 will never play N as type 2, there are only one possible separating equlibrium, type 1 plays L and type 2 plays N. Hence node 2's beliefs are as in Eq.(5.15).

$$\sigma_1(t_i) = \begin{cases} N, & \text{if } t1 \\ L, & \text{if } t2 \end{cases} \tag{5.15}$$

Let $\mu_1(t_i|N)$, denote the probability that node 1 is of type t_i. By using bayes rule we get this equation:

$$\mu_1(t_1|N) = \frac{P(N|t_1)P(t_1)}{P(N)} = \frac{P(N|t_1)P(t_1)}{P(N|t_1)P(t_1) + P(N|t_2)P(t_2)} \qquad (5.16)$$

With node 2's belief, we get that $\mu_1(t_1|N) = 1$ and $\mu_1(t_2|L) = 1$. We can now calculate node 2's expected utility from playing L and N:

$$EU_2(L, L) = \mu_1(t_1|L)U_2(L, L; t_1) + \mu_1(t_2|L)U_2(L, L; t_2)$$
$$\rightarrow \qquad EU_2(L, L) = U_i + \beta - I_l - r \qquad (5.17)$$
$$EU_2(N, L) = \mu_1(t_1|L)U_2(N, L; t_1) + \mu_1(t_2|L)U_2(N, L; t_2)$$
$$\rightarrow \qquad EU_2(N, L) = U_i \qquad (5.18)$$

From these two equations we see that the best response of node $2(BR_2)$ when he observes the other node choosing action L is:

$$BR_2(L) = \begin{cases} L, & \text{if } \beta - r \geq I_l \\ N, & \text{if } \beta - r < I_l \end{cases} \qquad (5.19)$$

Node 2's expected utility when type 1 chooses N, is easily seen to be U_i. To confirm if this is a separating equilibrium we must see if node 1 has any incentive to deviate from the strategies in node 2's belief. Type 2 will never deviate, so lets investigate type 1. In order to get node 1 to be willing to play N when he knows node 2's best response function, the following must hold: $\beta < I_l$. If this is true, then node 2's best response is to play N. I.e. the only separating equilibrium is the following:

$$\beta < I_l \qquad (5.20)$$
$$\sigma_1 = \begin{cases} N, & \text{if } t1 \\ L, & \text{if } t2 \end{cases} \qquad (5.21)$$
$$BR_2(\sigma_1) = N \qquad (5.22)$$

This means that in a separating equilibrium, the game will end up with no link establishment.

Pooling equilibrium. In a pooling equilibrium node 2 will not be able to distinguish the two types, and since $t1$'s strategy L dominates N, i.e. there is only one possible equilibrium, the one where both types of node 1 plays L.

$$\sigma_1(t_i) = \begin{cases} L, & \text{if } t1 \\ L, & \text{if } t2 \end{cases} \qquad (5.23)$$

By using bayes rule we get that $\mu(t_1|L) = p$ and $\mu(t_2|L) = 1 - p$. Node 2's expected utility is then:

$$EU_2(L, L) = p(U_i + \beta - I_l) + (1 - p)(U_i + \beta - I_l - r)$$
$$\rightarrow \qquad EU_2(L, L) = U_i + \beta - I_l - r + pr \qquad (5.24)$$
$$EU_2(N, L) = U_i \qquad (5.25)$$

From this we get node2's best response:

$$BR_2(L) = \begin{cases} L, & \text{if } \beta + rp - r \geq I_l \\ N, & \text{if } \beta + rp - r < I_l \end{cases} \qquad (5.26)$$

By using this best response function, node 1 sees that as long as $\beta > I_l$ he will never deviate from node 2's beliefs. And it is a pooling equilibrium where both nodes choose L, as long as $\beta > I_l$ and $\beta + rp - r > I_l$. We also know that: $rp - r \leq 0$ is allways true, and thus there also exists a pooling equilibrium where node 1, plays L, and node 2, plays N. This equilibrium will occur when $\beta > I_l$ and $\beta + rp - r < I_l$.

Node 2 not insured. Here we will analyze the game when node 2 is not insured. The rules of the game are as before, the only thing that has changed is the type of node 2, and thus the payoffs are different and we need to see if there exists separating and pooling equilibrium in this game as well.
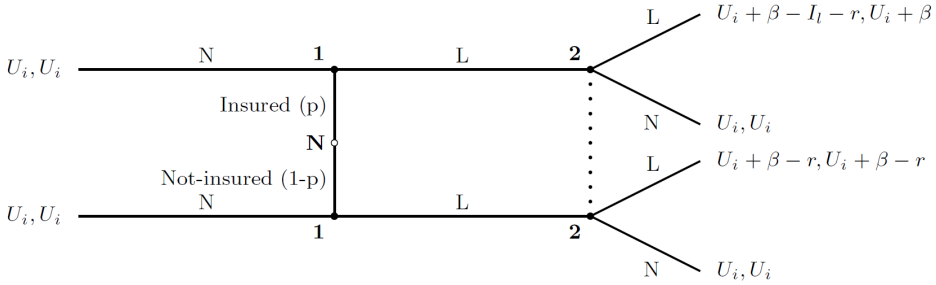
Figure 5.8: Signalling game with two nodes, node 1's type choosen by nature, node2 is not insured. Node 1 have complete information, node 2 suffer from incomplete information, and act on best response functions based on beliefs.

Separating equilibrium. In this game there is no dominant strategy for node 1, thus we have to check for the two possible separating equilibriums. We start with the separating equilibrium with the beliefs shown in Eq.(5.27).

$$\sigma_1(t_i) = \begin{cases} L, & \text{if } t1 \\ N, & \text{if } t2 \end{cases} \qquad (5.27)$$

With the beliefs in Eq.(5.27), this is node 2's expected payoffs:

$$EU_2(L, L) = (U_i + \beta) \tag{5.28}$$
$$EU_2(N, L) = (U_i) \tag{5.29}$$

From this we see that his best response when node 1's action is L, is to allways play L:

$$BR_2(L) = L \tag{5.30}$$

To see if this is an equilibrium, we have to see if node 1 has any incentive to deviate. We need to check for the two types of node 1: If $\beta > r$ then type 2 would deviate, because he could achieve a higher payoff by playing L, given the beliefs of node 2 in Eq.(5.27). So we know that for this to be an equilibrium,

$$\beta < r \tag{5.31}$$

When analyzing from node 1 type 1's perspective, for him to play L, this has to hold: $U_i + \beta - I_l - r > U_i$. The only way this can hold is if $\beta > I_l + r$. We see that Eq.(5.31) is violating this condition, and thus we have no separating equilibrium with the beliefs in Eq.(5.27).

Now lets look at the other possible separating equilibrium, see Eq.(5.32).

$$\sigma_1(t_i) = \begin{cases} N, & \text{if } t1 \\ L, & \text{if } t2 \end{cases} \tag{5.32}$$

Node 2's expected payoffs are as follows:

$$EU_2(L, L) = U_i + \beta - r \tag{5.33}$$
$$EU_2(N, L) = U_i \tag{5.34}$$

From this we get the best response function:

$$BR_2(L) = \begin{cases} L, & \text{if } \beta \geq r \\ N, & \text{if } \beta < r \end{cases} \tag{5.35}$$

For this to be a separating equilibrium, we need to see if node 1 would deviate from node 2's beliefs. Type $t1$ will not deviate as long as $\beta < I_l + r$. Type $t2$ will not deviate if $\beta \geq r$, if this condition is true, we see that node 2 will play L. I.e. the only separating equilibrium that exists is when node 2 plays L, node 1 of type $t1$ plays N and node 1 of type $t2$ plays L. For this to happen we get this condition on β.

$$I_l + r > \beta > r \tag{5.36}$$

Pooling equilibrium.   Two possible, one where both types of node 1 plays L, and one where both types plays N. Lets first analyze the one where both types of node 1 plays L.

$$\sigma_1(t_i) = \begin{cases} L, & \text{if } t1 \\ L, & \text{if } t2 \end{cases} \tag{5.37}$$

With the beliefs shown above, node 2's expected payoffs are:

$$EU_2(L) = p(U_i + \beta) + (1-p)(U_i + \beta - r)$$
$$EU_2(L) = U_i + \beta - r + pr \tag{5.38}$$
$$EU_2(N) = U_i \tag{5.39}$$

From this we get the best response function :

$$BR_2(L) = \begin{cases} L, & \text{if } \beta \geq r - pr \\ N, & \text{if } \beta < r - pr \end{cases} \tag{5.40}$$

Will node 1 deviate knowing this? Type $t1$ will not deviate as long as: $\beta - I_l \geq r$, and type $t2$ will not deviate as long as $\beta > r$. From this we get this final condition, if $\beta - I_l \geq r$ then there exists a pooling equilibrium where both types of node 1 plays L and node 2 also play L. From this we see that the other pooling equilibrium where both types of node 1, plays N, will only occur when $\beta < r$ and $\beta < I_l + r$.

Result and findings.   When one player lack knowledge about the other player, we were only able to find two scenarios where he could separate the two types of the other node. This is possible when player 2 is insured and $\beta < I_l$. He can then separate the insured and non-insured types of the other node, because it is only the non-insured node who would want to establish link. Since $\beta < I_l$ his best response is to not establish any link.

The other scenario where the node with incomplete information are able to separate is when he is not insured, and $r < \beta < I_l + r$. In this scenario it is only the non-insured node who would want to establish a link. Thus in this scenario the game will end up with a link between two non-insured nodes.

We where also able to find some pooling equilibriums, if the node with incomplete information is insured, a link will be established if $\beta + rp - r > I_l$. However, if $I_l < \beta$ but $I_l > \beta + rp - r$, then the pooling equilibrium will be that node 1 wants to establish link, but node 2 rejects. A pooling equilibrium where both nodes want to establish a link, occur when node 2 is not insured and $\beta - I_l > r$. If $\beta < r$ there will be a pooling equilibrium where both players choose not to establish link.

What this shows us is that when one player suffer from incomplete information, it is no longer possible for the insurer to force a network to evolve into a clique of

only insured nodes. It will also be harder to establish links, because one player must act on beliefs.

5.4   Model 3: Including maximum node degree and bonus

In real world networks, such as in the manufacturing industry, software development firms and many other types of business, a product can not be completed without outsourcing some of the task needed. For the manufacturer, it could be beneficial to buy certain parts from others instead of producing them on their own. A software product might need the combined knowledge from different firms. Thus the firm that outsource tasks are dependent on the other firms, and will not reach their goal before the other firms deliver their contribution. For example, lets consider a software company who want to develop a new product. However, they do not have the required resources or knowledge to complete the product, and will therefore need help from other companies with the desired knowledge or resources. When the product is finished the company get paid, but not before, to finish the product they need to cooperate with others. This process of outsourcing introduces a risk of failure due to other parties. To model this scenario we introduce a maximum node degree per node, and a bonus γ, which represents the payoff when a node reach their maximum degree, i.e. their maximum node degree(m). Except from this the game is as before.

5.4.1   Analysis

This model is very similar to the earlier model, for nodes to connect to each other, the change in payoff still has to be positive: $U_{i+1} > U_i$. However, we also need to consider the bonus received when reaching the maximum node degree, m. To model this we add the possible bonus divided on the number of links required to reach the bonus($\frac{\gamma}{m-i}$) in the decision process every time a node is considering establishing a link. In this way the model will change from the former models, because now the nodes have more incentive to connect to other nodes, and for every step closer to the goal, the nodes are more willing to accept risk than before. For example, an insured node is more likely to accept a risky link when it only need one more link to reach the goal. Compared to when it needs many more links to reach the goal.

The model now introduces a risk factor, because it is not certain that the nodes will obtain enough links, and if not, they will not receive their bonus, and they are stuck with their already established connections.

To analyze this model, lets take a closer look on the four different scenarios of the game.

When establishing a link between two insured nodes, the payoff the nodes will receive is as described in Eq. (5.41).

$$U_{i+1} = \begin{cases} \alpha + \beta - I_0 - I_l, & \text{if } i = 0 \\ U_i + \beta - I_l, & \text{if } i > 0 \\ U_i + \beta - I_l + \gamma, & \text{if } i = m \end{cases} \tag{5.41}$$

As described earlier we need to include the possibility of reaching the goal in the decision, and thus for insured nodes to connect to each other, Eq. (5.42) has to hold.

$$U_i + \beta - I_l + \frac{\gamma}{m-i} > U_i$$

$$\beta - I_l + \frac{\gamma}{m-i} > 0$$

$$\rightarrow \qquad \beta + \frac{\gamma}{m-i} > I_l \tag{5.42}$$

The payoff an insured node receives when connecting to a non-insured is as follows:

$$U_{i+1} = \begin{cases} \alpha + \beta - I_0 - I_l - r, & \text{if } i = 0 \\ U_i + \beta - I_l - r, & \text{if } i > 0 \\ U_i + \beta - I_l - r + \gamma, & \text{if } i = m \end{cases} \tag{5.43}$$

To establish a connection from an insured node to a non-insured one, the following has to hold:

$$U_i + \beta - I_l - r + \frac{\gamma}{m-i} > U_i$$

$$\beta - I_l - r + \frac{\gamma}{m-i} > 0$$

$$\rightarrow \qquad \beta + \frac{\gamma}{m-i} - r > I_l \tag{5.44}$$

When a non-insured node connect to another non-insured node this is the payoff they both will receive:

$$U_{i+1} = \begin{cases} \alpha + \beta - r, & \text{if } i = 0 \\ U_i + \beta - r, & \text{if } i > 0 \\ U_i + \beta - r + \gamma, & \text{if } i = m \end{cases} \tag{5.45}$$

To establish the connection the following equation has to hold:

$$U_i + \beta - r + \frac{\gamma}{m-i} > U_i$$

$$\beta - r + \frac{\gamma}{m-i} > 0$$

$$\rightarrow \qquad \beta + \frac{\gamma}{m-i} > r \tag{5.46}$$

In the case of non-insured node wanting to establish a link with an insured node, the payoff is a strictly increasing function, see Eq. (5.47), and thus a non-insured will always connect to an insured node if possible.

$$U_{i+1} = \begin{cases} \alpha + \beta, & \text{if } i = 0 \\ U_i + \beta, & \text{if } i > 0 \\ U_i + \beta + \gamma, & \text{if } i = m \end{cases} \tag{5.47}$$

5.4.2   Result and findings

If we want an clique of only insured nodes, we have to ensure that insured nodes connect to each other, and that they do not establish connections to non-insured nodes. We know that an insured node would want to connect to another insured node if Eq.(5.42) is satisfied. In the equation we see that the expected bonus per established link is increasing. Thus if an insured node of degree zero is willing to connect to another insured node, then every insured node with a degree higher than zero also would like to connect to another insured node. Thus to ensure that insured nodes connect to each other this equation has to hold:

$$\beta + \frac{\gamma}{m} > I_l \tag{5.48}$$

We also want to ensure that insured nodes never establishes links with non-insured nodes, from 5.43 we see that this has to hold:

$$\beta + \frac{\gamma}{m-i} - r < I_l \tag{5.49}$$

This can be simplified, if one can ensure that the least risk averse insured node, i.e. the node with degree $m - 1$, do not establish links with non-insured nodes. Then we know that no insured node with degree less than $m - 1$ will establish links with non-insured nodes. From this we get the equation Eq. (5.50).

$$\begin{aligned} \beta + \frac{\gamma}{m - (m-1)} - r &< I_l \\ \rightarrow \qquad \beta + \gamma - r &< I_l \end{aligned} \tag{5.50}$$

To summarize, Eq.(5.48) and Eq.(5.50) gives the final limitation on the link insurance cost, Eq.(5.51). If this equation is satisfied the resulting network will contain a clique of only insured nodes.

$$\beta + \gamma - r < I_l < \beta + \frac{\gamma}{m} \tag{5.51}$$

For this to even be possible $\beta + \gamma - r < \beta + \frac{\gamma}{m}$, i.e. Eq.(5.53) has to hold. This equation reflects that as the risk to bonus ratio gets smaller, it gets more and more

unlikely to ensure a clique of only insured nodes. When the risk to bonus ratio is less than $1 - \frac{1}{m}$, such a clique will never occur. The equation shows that a node would be more and more willing to take a risk, as the reward of doing so increases.

It is also useful to know when non-insured nodes connect to each other, this happens when Eq.(5.45) is satisfied. This equation is dependent on the node degree, and thus for the first link to be established from a non-insured node, the expected payoff has to be higher than the risk($\beta + \frac{gamma}{m} > r$). If the risk is to high, then the non-insured node must establish links with insured nodes before it is willing to establish risky links.

With these findings, an insurer can by adjusting the insurance cost parameter, determine the outcome of the network formation game. If he want a clique of only insured nodes Eq.(5.51) has to hold. However, it is easy to relax the condition, such that insured nodes only connect to, $j = 1, 2, 3..m$ nodes, this is done by changing Eq.(5.50) to $\beta + \frac{\gamma}{m-(m-j)} - r < I_l$, which gives us Eq. (5.52). An interesting result in this model is that due to the risk willingness among the nodes, the lower boundary on the link insurance cost has increased compared to the one found in model 2.

Consequences of not reaching required number of edges.   When a node establishes a link, it does not know whether it will reach the maximum node degree, unless the current node degree is $m - 1$. Hence the node might end up not reaching the desired goal. This can happen if there is not enough nodes willing to establish links. Nodes who do not reach their goal could end up with a payoff less than U_0.

$$\beta + \frac{\gamma}{j} - r < I_l \tag{5.52}$$

$$
\begin{aligned}
\gamma - r &< \frac{\gamma}{m} \\
1 - \frac{r}{\gamma} &< \frac{1}{m} \\
\rightarrow \qquad 1 - \frac{1}{m} &< \frac{r}{\gamma}
\end{aligned}
\tag{5.53}
$$

Efficiency and Stability.   In this model, the incentive for establishing links is increased. Thus to maintain a stable network with two cliques the cost of link establishment, in comparison with model 2, has to be increased. This increased incentive may result in a higher price of stability, however if every node has received their bonus, then the price of anarchy is one. The price of anarchy is dependent on the number of nodes in both cliques, and if it is enough nodes for everyone to reach their maximum degree or not. If there exists nodes that have not reached their maximum degree in both cliques, then the resulting network is not necessarily the most efficient, and we could be missing a potential payoff due to the cost constraint.

By introducing the maximum degree, m, we are limiting the problem of price of anarchy, because as long as m is less than the number of insured and number of non-insured nodes, it will be less links established compared to model 2, and overall fever possible links between insured and non-insured. However, the bonus the nodes receives, will contribute to inefficiency, because when nodes do not reach their maximum degree, the potential payoff that could be generated by allowing insured and non-insured to connect, is greater than in model 2.

Simulation of the results

For the first simulation the parameters are set to the following: $\beta = 0.9, I_l = 0.7, r = 0.5, \gamma = 0.2$ and $m = 4$, in order to satisfy the condition Eq.(5.51), and enable all nodes to reach their maximum degree.
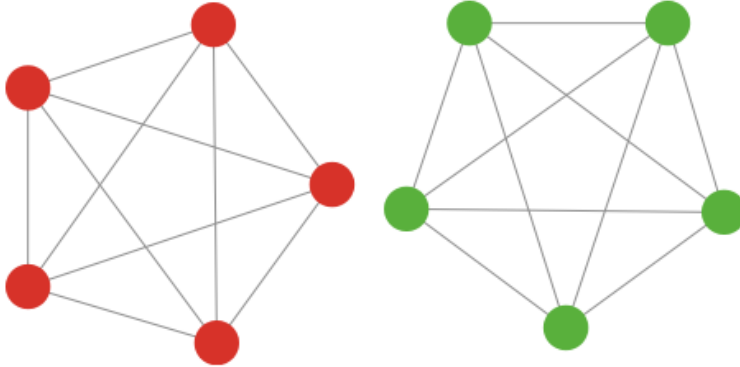

Figure 5.9:   Two cliques, one consisting of insured agents the other consists of non-insured. All nodes have reached their goal.

As we see in Figure 5.9 the results where as expected, the cost of insuring a link satisfied the conditions found earlier and thus the result where two cliques, one consisting of only insured and the other of non-insured nodes. An interesting thing to notice is that β and r is the same as in model 2, but to ensure that only insured connect to each other, the link insurance cost needs to be higher. This is to compensate for the risk the nodes now are willing to take. The price of anarchy in this scenario is one, i.e. the socially optimal outcome. In the second simulation we set the parameter $m = 5$, and kept the other variables as they where. The resulting network were as expected the same as in the last simulation, but since the nodes did not reach their maximum degree, the price of anarchy is less than one. The price of

anarchy can be seen in Eq. (5.54).

$$PoA \qquad = \frac{Sum of payoffs}{Sum of Socially optimal payoffs}$$
$$PoA \quad = \frac{5\times4\times(0.9-0.7)+5\times4\times(0.9-0.5)}{5\times4\times(0.9-0.7)+5\times4\times(0.9-0.5)+5\times(2\times0.9-0.7-0.5+2\times0.2)}$$
$$PoA \qquad\qquad = \frac{12}{17} \tag{5.54}$$

When we changed the link insurance cost, and set it to the same value as in model 2, $I_l = 0.5$, the resulting networks changes.Now we the insured nodes are willing to establish risky links to reach their maximum degree. Some of the resulting network can be seen in Figure 5.10. In figure 5.10a the price of anarchy is 0.95, and in figure 5.10b the price of anarchy is 1, i.e. it has reached the socially optimal outcome.

## 5.5   Model 4: Including bulk insurance discount

Insurance companies often interpret a quantum discount when purchasing multiple products. From convenience stores we are used to the slogan "buy one get one for free". It seems to be common for insurance companies to offer discount to their customers if they choose to collect some or all of their insurances with them. Several insurance companies in Norway, such as Sparebank 1 offers customers up to 25 % discount according to the following rules [Spa].

- 10% discount if the person has signed three different insurances

- 15% discount if the person has signed four different insurances

- 20% discount if the person has signed five or more different insurances

- Plus additional 5% discount if the person is a customer of the bank.

The insurance offered is intended to the individual market and includes among others: travel insurance, household insurance, car insurance, house insurance, insurance of valuable items and yacht insurance.

Inspired by other insurance products, we would like to introduce a discount rate dependent on the degree of the node. This will make it more attractive for nodes with high degree to acquire insurance, and this could act as a incentive for other nodes to also acquire insurance. Thus this seems like a reasonable model to include.

How insurance companies choose to formulate their discount rate might vary. One solution might be to follow a strict 5% discount per new connection, similar to the one from Sparebank 1, or let the discount follow a power law, or a log-function etc. We choose to follow a discount rule which directly reflects the nodes degree.
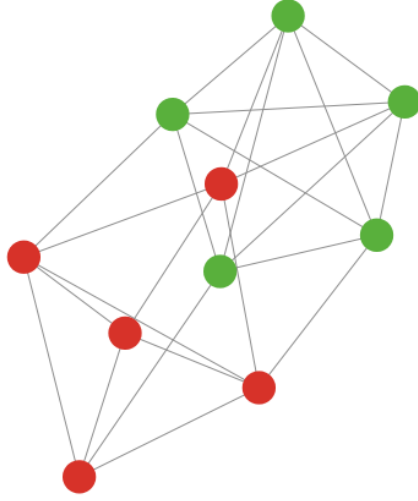
(a) One non-insured node has connected to two insured nodes.
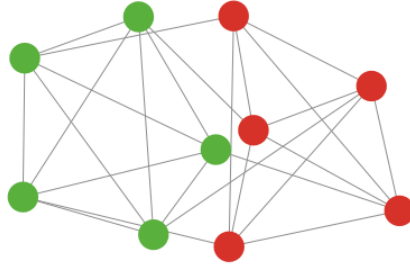
(b) Every non-insured node is connected to one insured node, this is the optimal outcome with these parameters.

Figure 5.10: To possible outcomes, when insured nodes are willing to take a risk of connecting to non-insured nodes, to receive their bonus. Figure a shows a scenario where one non-insured node has connected to more than one insured node, thus not a socially optimal outcome. Figure b shows the optimal outcome.

5.5.1   Analysis

The price for adding a new link follows the equation:

$$\frac{I_l}{i + 1} \tag{5.55}$$

Here, i is the nodes current degree. This means that the more link a node establish the cheaper the link insurance will be.

Discount model

We start our analysis by applying the discount to model 2. As before we analyze the four different connection scenarios. However, it is only the scenario where insured connects to other insured nodes and insured to non-insured nodes, that has changed compared to model 2.

When we consider links between insured and insured nodes, we need to add the discount to the conditions found in model 2. The condition for establishing links between two insured nodes is shown in Eq. (5.56).

$$\frac{I_l}{i+1} < \beta \qquad (5.56)$$

For a link between insured and non-insured to be established, Eq. (5.57) has to hold.

$$\frac{I_l}{i+1} + r < \beta \qquad (5.57)$$

Result and findings   For an insurer to be able to ensure that the network ends up in a clique with only insured nodes, we must ensure that the most expensive link establishment, i.e. the first, to another insured node can be achieved. This gives us the same condition as in model 2, i.e. $I_l < \beta$. We also need to ensure that insured nodes does not connect to non-insured, thus we get the final condition in Eq. (5.58), where N_I is the number of insured nodes in the network.

$$(N_I)(\beta - r) < I_l < \beta \qquad (5.58)$$

This is condition is very strong, because it says that $\beta - r < \frac{\beta}{N_I}$, and as the number of insured nodes gets higher this get more and more unlikely. Thus by including bulk-discount, the insurer are making it harder for himself to constrain the network formation. This is because the incentive for establishing links are higher than without discount, and thus more links will be established.

Stability and efficiency   If we compare the total payoff equation in this model, see Eq.(5.59), with the one in model 2 (Eq.(5.12)). We see that the cost for insured nodes has changed, and therefore the payoff achieved from links between insured nodes has increased, and so has the payoff received from potential links between insured and non-insured nodes. As we know, in a scenario where the insurer sets the cost, such that the network will end up in two cliques, the payoff received from links between insured and non-insured are zero. This potential payoff, in a scenario where there are two cliques, can be described like this: $(N_I N_{\bar{I}}\beta + N_I(-\sum_{i=N_I}^{N_{\bar{I}}-1}\frac{I_l}{i}))$, and as long as $(N_I N_{\bar{I}}\beta > N_I(-\sum_{i=N_I}^{N_{\bar{I}}-1}\frac{I_l}{i}))$ it would have been socially optimal to have one-clique of both insured and non-insured nodes. When the cost of establishing

links decreases and the insurer forces the network formation to end up in two cliques, the price of anarchy will be higher compared to the price of anarchy in model 2. This is because the incentive for establishing links has increased, and thus for the insurer to be able to constrain the network formation, the cost of establishing links has to be higher.

$$U_{total} = (N_I(N_I-1)\beta - N_I \sum_{i=1}^{N_I-1} \frac{I_l}{i}) + (N_{\bar{I}}(N_{\bar{I}}-1)(\beta - r)) + (N_I N_{\bar{I}}\beta + N_I(- \sum_{i=N_I}^{N_{\bar{I}}-1} \frac{I_l}{i}))$$

$$(5.59)$$

Discount and Bonus model

We also need to apply the discount to model-3. The only scenarios that has changed in this model is the one where insured nodes connects to either other insured nodes or non-insured nodes are affected.

When insured nodes are considering establishing links with each other, their payoff functions are as shown in Eq. (5.60).

$$U_{i+1} = \begin{cases} \beta - I_l, & \text{if } i = 0 \\ U_i + \beta - \frac{I_l}{i+1}, & \text{if } i > 0 \\ U_i + \beta - \frac{I_l}{i+1} + \gamma, & \text{if } i = m \end{cases} \qquad (5.60)$$

For insured to connect to each other Eq.(5.61) has to hold.

$$U_i + \beta - \frac{I_l}{i+1} + \frac{\gamma}{m-i} \quad > U_i$$

$$\beta - \frac{I_l}{i+1} + \frac{\gamma}{m-i} \quad > 0$$

$$\rightarrow \qquad \beta + \frac{\gamma}{m-i} \quad > \frac{I_l}{i+1} \qquad (5.61)$$

When insured nodes are considering connecting to non-insured, their payoff functions are as show in Eq. (5.62).

$$U_{i+1} = \begin{cases} \beta - I_l - r, & \text{if } i = 0 \\ U_i + \beta - \frac{I_l}{i+1} - r, & \text{if } i > 0 \\ U_i + \beta - \frac{I_l}{i+1} - r + \gamma, & \text{if } i = m \end{cases} \qquad (5.62)$$

For this to happen Eq.(5.63) has to hold.

$$U_i + \beta - \frac{I_l}{i+1} + \frac{\gamma}{m-i} - r \quad > U_i$$
$$\rightarrow \quad \beta + \frac{\gamma}{m-i} \quad > r + \frac{I_l}{i+1} \tag{5.63}$$

5.5.2   Result and findings

If we analyze the same scenario as in the other models, namely a clique of only insured nodes. The first step is to ensure that insured nodes connect to each other. To ensure that this happen, we need to find the condition for the lowest expected increase in payoff, i.e. at node degree zero. If they are willing to establish link at this point, then they will also be willing at all degrees higher than zero. At degree zero there is no discount on the insurance link cost, and thus if Eq.(5.48) from model 3 holds, insured nodes will connect to other insured nodes.

The condition for ensuring that insured nodes do not connect to non-insured has changed, we know if an insured node do not want to establish a link with a non-insured at degree $m - 1$, then no insured node with degree lower than $m - 1$ will either do so. From this we find the condition, see Eq.(5.64)

$$U_i + \beta - \frac{I_l}{m} + \frac{\gamma}{m - (m-1)} - r \quad < U_i$$
$$\beta + \gamma - r \quad < \frac{I_l}{m}$$
$$\rightarrow \quad m(\beta + \gamma - r) \quad < I_l$$

This is a very strong condition, because the only way this can happen is if $\beta + \gamma - r < \frac{1}{m}$. This shows us that when the incentives for establishing links increases, it gets more and more difficult for the insurer to ensure a clique of only insured nodes. The final condition for ensuring a clique of only insured nodes is shown in Eq. (5.64).

$$m(\beta + \gamma - r) < I_l < \beta + \frac{\gamma}{m} \tag{5.64}$$

Similar calculation can be done for the other three scenarios in the game, and they all show the same. The quantum discount results in a overall higher payoff for the nodes, since the cost of insuring a new link becomes cheaper. This means that the nodes will have a higher incentive to create links to each other. Which makes it harder for the insurer to separate insured and non-insured nodes.

Since this is just model 3 with discount, we see that in this model, problem of separating the two node types have increased. And if we have a network where the insurer have managed to separate them, then this has a cost, compared to the most efficient network, i.e. the price of anarchy has increased.

5.6   Model 5: Network externalities

In the earlier models, the experienced network effects only arose from their neighbours. I.e. when a node established a connection the change in utility were only dependent on fixed variables, and not dependent of the rest of the network. In many real world scenarios it is more realistic that a node will also be strongly affected by the indirect connections to other nodes. Social relationships between nodes are good examples of such networks, where they offer benefits in terms of favors, information etc.

We apply the results from the paper from Jackson and Wolinsky [JW96] and uses a network formation game in [Jac05], to study indirect networks effects in our model.

The benefits a player receives in this game are calculated as follows. In addition to the benefit from the direct connection, a node will also benefit from "the friends of the friend", and "the friends of the friends of the friend" etc. This is achieved by letting the payoff be calculated relative to the distance between the nodes. β is now dependent on the minimum number of hops to the node e.g. the benefit of a direct connection is β, the benefit of a friend of a friend is β^2 etc. We want the benefit to decrease with the distance, therefore we need the limitation: $0 < \beta < 1$.
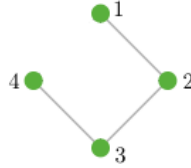

Figure 5.11:   Four nodes interconnected with each other.

Example: Lets consider the network shown in 5.11. Node 1 and node 4, in the network will receive a benefit of $\beta + \beta^2 + \beta^3$ by being connected with node 2 and 3. $\beta^2 + \beta^3$ represents the indirect benefits from node 3 and 4. Node 2 and 3 receives a benefit of $\beta + \beta + \beta^2$. For this network to make sense, it is important to also include some cost of having direct connections, or else the rational thing would be to establish a link with everyone. This is done as in earlier models, every node pay a cost for direct connections, but no cost for indirect connections. Thus the total payoff for a node is:

$$\sum_{j \neq i} \beta_{ij}^{d(ij)} - \sum_{j:ij \in g} c_{ij}, \tag{5.65}$$

where $d(ij)$ represents the shortest path between node i and node j, and c_{ij} represents node i's cost of establishing a link between the two nodes. To simplify the model we choose a symmetric connection process where β and c is set to a fixed global value.

In the paper [JW96], they analyze the networks with two differen approaches, one with focus on efficiency and the other on stability. The optimal network is of course both efficient and stable, but as we shall see there are some conflicts between efficiency and stability. They showed that an efficient network is:

1. *a complete graph g^N if $c < \beta - \beta^2$,*

2. *a star encompassing every node if $\beta - \beta^2 < c < \beta + \frac{(N-2)}{2}\beta^2$,*

3. *an empty network(no links) if $\beta + \frac{(N-2)}{2}\beta^2 < c$.*

The most efficient structure is a star structure which encompasses every node. A star structure have the characteristics of minimizing the average path length and uses the minimum number of links($N-1$) required for including every node. This structure provides the highest overall payoff for the network, but this network is not necessarily stable.

When analyzing the stability of the network, by using the definition of pairwise stability, Jackson and Wolinsky found four different stability conditions:

1. *a pairwise stable network consists of at most one (non-empty) component,*

2. *if $c < \beta - \beta^2$, the unique pairwise stable network will be a complete graph g^N,*

3. *if $\beta - \beta^2 < c < \beta$, a star encompassing every node will be pairwise stable, although not necessarily the unique pairwise stable graph,*

4. *if $\beta < c$, any pairwise stable network which is nonempty is such that each player has at least two links and is thus inefficient.*

We see that the stability condition 2, is the same as the efficiency condition 1, and thus if this condition is fulfilled, the network is both stable and efficient. Condition 3 shows us why the efficient star network is not necessarily stable. If $\beta \leq c < \beta + \frac{(N-2)}{2}\beta^2$ then the efficient network will be a star, but it is not stable.

It should be noticed that it is more beneficial for a node to operate as a leaf node compared to being a center node, due to the cost of direct connections. In a star structure, a leaf node will only have to pay the cost of the link to the center node,

and will benefit indirectly for each node connected to the center node. The center node will benefit from each new connection, however, the payoff will only be $\beta - c$ for each connection.

5.6.1   Insurance and connection game

The findings about efficiency and stability are very useful for our model, because if one has knowledge of the different variables it is possible to determine how the network will evolve. And if you are able to control the variables, you can actually determine the resulting network structure. From the papers, we know that there exists different boundaries on the link cost, and how the resulting stable and efficient network will be. Our earlier models shows that the cost of establish a link is the insurance cost and/or the risk cost. From this we can show that if $\beta - \beta^2 < I_l < \beta$ and $r > \beta$ a star with only insured nodes, and no connections between non-insured nodes, are both a stable and an efficient network. If $\beta - \beta^2 < I_l + r < \beta$ and $\beta - \beta^2 < I_l$ and $\beta - \beta^2 < r$ the stable and efficient network is a star consisting of both insured and non-insured nodes. If $I_l < \beta - \beta^2$ all insured nodes will connect to every other insured node, and if $r < \beta - \beta^2$ all non-insured nodes will connect to every other non-insured node. In addition if $r + I_l < \beta - \beta^2$ the resulting network will be a clique of both insured and non-insured nodes. The insurer can thus determine the formation of the network by adjusting the cost parameters.

5.6.2   Homogenous symmetric connection game

From this point and on, the game we will consider is a homogenous network setting where every node is considered to be insured. This is done because it will simplify an otherwise very complex model. We are analyzing the resulting network structure, which is easier when only considering one homogenous cost for every node. Lets look at an example, where the parameters are set to: $\beta = 0.9, I_l = 0.5$, the resulting network are shown in Figure 5.12.

As we see this is not an efficient star, but the network is stable. The efficient network would be to delete the link $4, 6$ and adding the link $1, 6$. But since we only consider a link at a time this can not be done. To show this let U_i denote the payoff of node i, the payoffs of the nodes are as described in Eq.(5.69).

$$U_1 = 4\beta + \beta^2 - 4c \tag{5.66}$$

$$U_2 = U_3 = U_5 = \beta + 3\beta^2 + \beta^3 - c \tag{5.67}$$

$$U_4 = 2\beta + 3\beta^2 - 2c \tag{5.68}$$

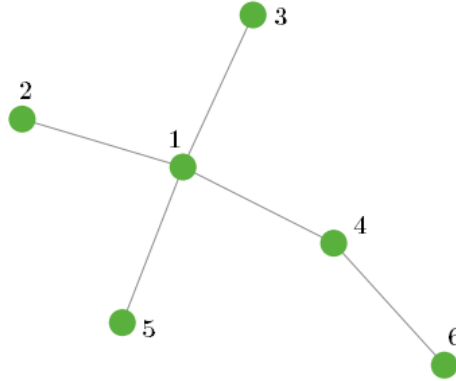$$U_6 = \beta + \beta^2 + 3\beta^3 - c \tag{5.69}$$

Figure 5.12:   The resulting network after a simulation with the parameters $\beta = 0.9, I_l = 0.5$.

Node 6 would benefit from adding the link $1, 6$, but node 1 is not willing to do so because then he must pay an extra cost, and since $\beta^2 > \beta - c$. Thus the network is stable but not efficient.

From this we see that, even when the most efficient and the stable network is a star, we can not guarantee that the network formation game will end up in a star. This is because we only consider one link at a time, and not the whole network.

Star not possible with high n.   In the paper [Jac05] they came up with the following proposition: Consider the symmetric connections model in the case where $\beta - \beta^2 < c < \beta$. As the number of nodes grows, the probability that a stable state (under the process where each link has an equal probability of being identified) is reached with the efficient network structure of a star goes to zero. But if a network reaches the efficient star structure, it is also pairwise stable, and will remain a star. We confirmed this when running multiple simulations, when we used few nodes the resulting network often became a star, but as the number of nodes increased the network seldom became a star.

However, the structure of the networks that evolve are very similar to a scale-free network. There are many nodes with low node degree, and few with a high node degree. One example of this is shown in Figure 5.13, there are only ten nodes, but the network have the properties of a scale-free. Two nodes with degree of 4, and the rest have a degree of one or two.

Bulk insurance.   As noted before it is not preferable to be the center node, due to the cost of all the direct links. If we consider the model with bulk insurance
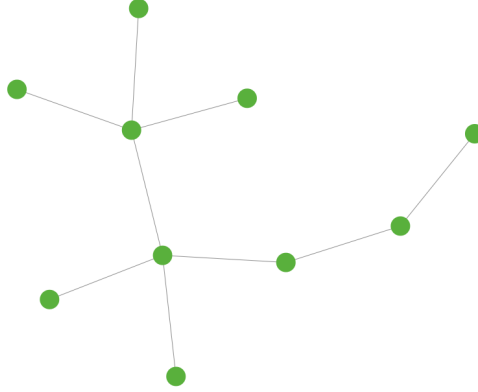
Figure 5.13: The resulting network after a simulation with the parameters described earlier and ten nodes.

discount, this would lower the extra cost for the center node significantly. This could be used to increase the probability of reaching a star formation.

Using the discount formula from the previous model, we end up with Eq.(5.70) to achieve a efficient and stable star topology. i represents the node degree.

$$\beta - \beta^2 < \frac{i_l}{i+1} < \beta \qquad (5.70)$$

An interesting property of the discount model is that the conditions for a efficient networks will change. Because when the node degree increases, the insurance cost might reach the critical degree g, the best strategy for a node with degree g or higher, is to connect to every node, as shown in Eq.(5.71).

$$\frac{I_l}{g} < \beta - \beta^2 \qquad (5.71)$$

This is possible when $g < n$, where n-represents the number of nodes in the network. The stability condition have changed for a node with a critical degree, the stable and efficient condition for this node is, as shown earlier, to have a direct connection to every other node. Thus if we have a star-topology both the leaf nodes and the center node are stable, and the center node has been compensated for its role in the network.

Since the networks formed are similar to scale-free networks, we can calculate the probability of a node having degree g, see Eq.(5.72). γ is the power law parameter, as described in Chapter 3.

$$P(g) = g^{-\gamma} \qquad (5.72)$$

When a node i reaches the critical degree g its optimal strategy is to connect to every node, since the payoff generated from direct connections is larger than any indirect

connection. And in general nodes prefer to connect to nodes with high connectivity [2], and will thus prefer to connect to this node compared to nodes with a degree lower than g. In this way nodes will connect to the node who have a degree greater or equal to g, and remove the links to their low-degree nodes which they can instead reach through the node with high connectivity.

Lets consider a case with $n-$nodes, and two of these nodes, i and j, have an equal degree larger than g. The rest of the nodes has a degree of one or zero. If there exists a node with degree zero, it would prefer to be connected to i or j, and so will i and j, so this will eventually happen. If a node connected to i are considering connecting to j, or visa versa, it will do so because j can offer a higher connectivity than i. Now j has a higher degree than i, and thus every node would prefer to connect to j over i. This will eventually result in a star formation, with j as the center node. From this we get the propositions:

Conjecture 1. If the probability that there exists a node with critical degree, is such that the expected number of nodes with critical degree($E(Nodes with degree g) = g^{-}2$) is less than 0.8. Then the resulting network will with high probability be a star-like structure.

Conjecture 2. If the probability that there exists a node with a critical degree is high, the resulting network will with high probability end up in a network where the average degree is close to the max-degree, i.e. a clique or almost a clique.

Results and findings

To prove the conjectures above, we created a simulator [REFERENCE TO APPENDIX?]. The rules of the simulator are as follows. Every round two random nodes, not neighbors, are selected, and asked if they would want to establish a link. The link establishment is a symmetric decision, i.e. the link is established if it result in an increased payoff for both nodes. If the link is added, we check if either of the nodes would prefer to delete some of their already existing links, this decision is asymmetric. A link will be deleted if the node will achieve a higher payoff without it. And then we the rest of the nodes if they would like to delete any links. This procedure is repeated as long as there is possible to add new links. The payoff function of each node is as described earlier(see Eq.(5.65)), except that the cost is now dependent on the degree of the node. For the simulations to be realizable, we had to set the number of nodes to 20, or else the computational time was to high. For every critical degree, from three to nineteen, we ran 50 simulations, and noted the resulting network formation. We chose to start from critical degree equal three, since any number below would result in a clique, because it would be more beneficial to be directly connected to every node.

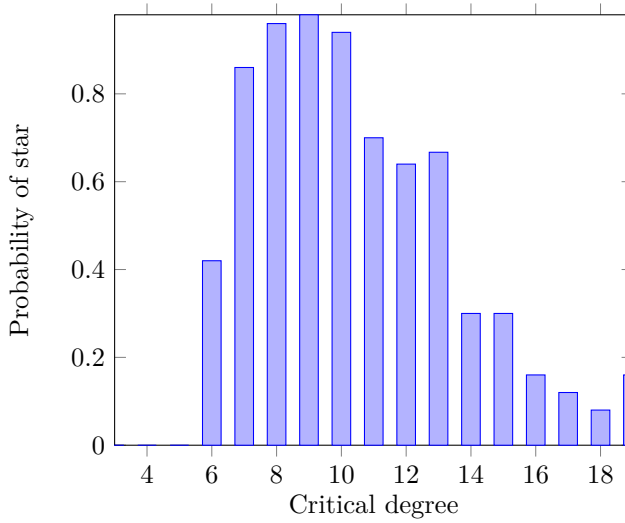[2]A node with high degree implies a node with high connectivity.

Figure 5.14: Shows the probability of the network ending up in a star given different critical degrees.

We know that if Eq.(5.70) is satisfied for all i, then the efficient and stable state is a star. But a more interesting scenario occurs when we have a graph where one or more of the nodes reaches the critical degree. -Will the final structure become a scale-free, a star or simply just unstructured? The results from the simulation can be seen in Figure 5.14, 5.17 and 5.15. As we see from the figure 5.14, the probability of the resulting network being a star, suddenly increases from zero to 42% at critical degree five to six, and then jumps from 42 to 70-, 86-,96-, 98% at critical degree six to nine. These results confirms our conjectures, and show that the discount can drastically increase the probability of the network ending up in a star.

From Figure 5.15 we can observe that the opposite is happening, as the critical degree is increased, the probability of the resulting network being a clique, drastically decreases. As we can see with a critical degree of seven or higher, it is very unlikely that we end up with a clique. These findings also supports our conjectures.

An interesting comparison can be made between the emergence of a star versus a clique. In Figure 5.16, shows a plot of the network resulting in a star and another plot of the probability the resulting network being a clique. As we can see, from a critical degree of five to seven, the resulting network structure, changes from almost certain ending up in a clique, to almost certain ending up in a star structure. The reason is as mentioned before that when the critical degree is low, the likelihood of many nodes reaching it is high. And none of these would like to delete any links. Hence we end up with a clique. The reason why we end up with star structures is because it is
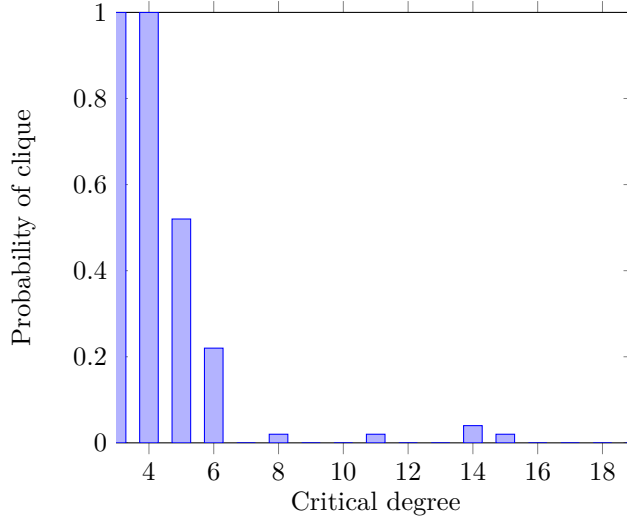
Figure 5.15:   Shows the probability of the network ending up in a clique, given different critical degrees.

less likely that many nodes end up reaching the critical degree, hence it most of the nodes still prefer to rely on indirect links, but the ones who reach the critical degree prefer to connect to every one. And since the nodes with critical degree, have high connectivity, nodes will prefer to be connected with these, compared to other nodes. Nodes prefer to be connect to the ones with critical degree, the nodes with critical degree would like to connect to every one, and thus the structure evolves into a star, with the critical degree node in the center.

In Figure 5.14, when the critical degree gets closer to the number of nodes in the network, the probability of the network evolving into a star decreases. However, in Figure 5.17, we have plotted the probability of the network evolving into a network where only a few($two to four$) nodes end up with a high degree, but not necessarily a critical degree. And as we see, this occurs with high probability from critical degree six and up. These networks are so called scale-free networks, because there are a few hubs, that account for most of the connectivity in the network. The reason why we end up with scale-free network is because nodes prefer to be connected with nodes with high connectivity, and thus will delete links to nodes with low connectivity. This is very similar to the simple model that creates scale-free networks, where the probability of connecting to a node is proportional to the degree of the node.

Price of Anarchy.   Another interesting thing is the average price of anarchy as function of the critical degree. The price of anarchy where calculated by taking
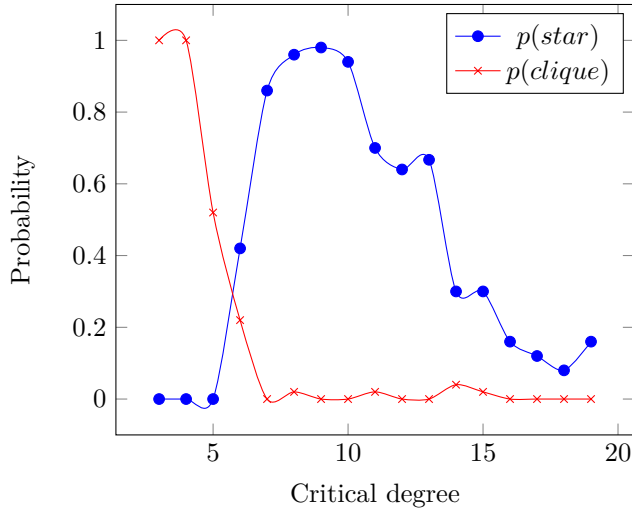
Figure 5.16: Shows the comparison between the probability of the network ending up in a star (blue) or clique (red), given different critical degrees.
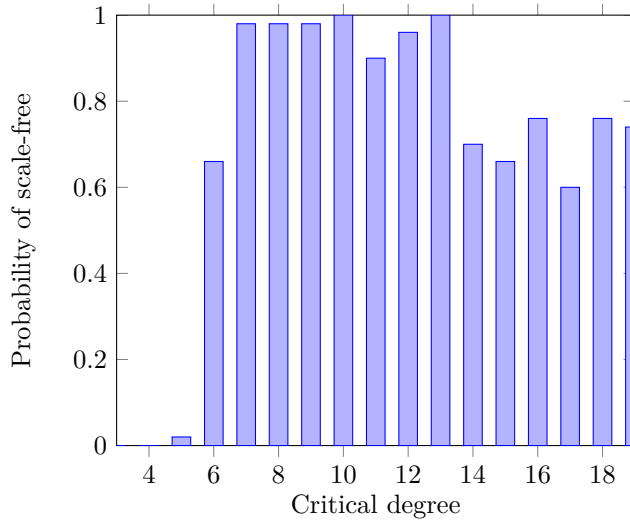

Figure 5.17: Shows the probability of the network ending up in a scale-free structure, given different critical degrees.
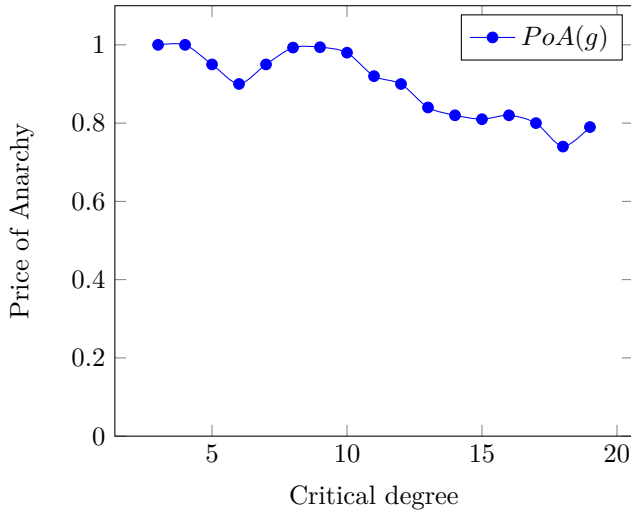
Figure 5.18: Shows the price of anarchy as a function of critical degree

the average total payoffs and dividing on the optimal payoff. The result can be seen in Figure 5.18.

We see that the price of anarchy for the first critical degrees is one, and then decreases until degree six, and at seven it increases again. This is because at degree one to five, the socially optimal structure is a clique, at degree six, a clique and a star, are almost equally good, and at degree seven and up a star-structure is the socially optimal outcome. In other words, when the cost is low, then a clique is the optimal structure, and when the cost is high a star is the optimal structure.

This is further improves our findings, because now we have shown how an insurer can determine the resulting network formation by changing the cost, and also the formation that evolves also has a price of anarchy close to one.

Example structures from the simulation.   In Figure 5.19 we see two of the many possible outcomes when the critical degree is achieved at a low node degree. And as we see most of the nodes have reached the critical degree, and thus connected to every other node. In Figure 5.20 we see one example of a scalefree network, and the standard star network, both with twenty nodes and results from the simulations when the critical degree were set to a value above six.

(a) A clique consisting of twenty nodes.

(b) A network with high average node degree, but not a clique.

Figure 5.19: Two different outcomes of the simulations where the critical degree is low

(a) A star consisting of twenty nodes

(b) A scalefree network with twenty nodes, where three nodes account for most of the connectivity.

Figure 5.20: Two different outcomes from running simulations with a high critical degree.

6.1 Discussion

From our background study it was relieved that the current market for cyber-insurance is far from healthy, and many people are skeptical about the future of cyber-insurance. We believe that there is a need for cyber-insurance, since it is impossible to ensure 100 percent security. As described in the introduction, there are certain obstacles unique for cyber-insurance, and arguably these are the reasons why cyber-insurance have not emerged as expected. In light of earlier failed attempts to establish a cyber-insurance market, such as those we found here in Norway, we wanted to take a new approach towards analyzing the cyber-insurance market.

First we studied a variety of different network formation games, in order to find out if there where any superior network topologies that would fit as a cyber-insurance network. -Where ideally both the insurer and customers gets a higher payoff from purchasing cyber-insurance. As described in the background study, we found that star and clique structures had appropriate characteristics, not only do they have calculable fixation probability, but they could also generate better security and overall higher payoff for the nodes. With these structures in mind, we wanted to find a way of forcing networks to evolve into these structures. We found that insurers could use the insurance premium in order to control the formation of networks. If the price is set to the right level, networks with calculable risk will evolve, and if the insurer are able to separate the nodes into two different network, one consisting of trusted, insured nodes, the other of non-insured nodes, the trusted nodes can even further increase their payoff. The insurer now posses a tool for setting the insurance premium properly, resulting in possible better products for both the customer and the insurer.

We created several different models, where the first model, showed a very simple and naive way for the insurer to separate insured and non-insured nodes, into two cliques. In the other models we added more and more features, to make them more

applicable to real world scenarios. To get an overview of the models we created, we refer to the Figure 5.1.

In model-2 we made model-1 realizable, by including the parameters: expected risk cost,insurance cost and the benefit per link. We then analyzed the parameters and found out when and how different network structures would evolve. By adjusting the insurance cost to the right level, the insurer can make the network formation game end up in one clique of both insured and non-insured nodes, or a clique of only insured and another of only non-insured. The condition for separating insured from non-insured are: $\beta - r < I_l < \beta$, and if also $\beta > r$, then the resulting network will be two cliques. The solution is also stable, since the resulting network consist of one or two cliques, there is not possible to add any more links. And because the change in payoff is linear and non-dependent on the rest of the network, when a link is added, there is no reason to remove it later. This holds for model 1,2,3 and 4. We also showed that when the insurer sets the cost such that the network ends up in two cliques, it is not the socially optimal. Because the network will suffer from the lost benefits of connections between insured and non-insured nodes.

In model-3 we applied the model to certain real world scenarios, such as software development firms/chains, or other networks where the final product is dependent on the collaboration of several partners. This was done by including a bonus, which is received when a node reach the desired number of links(called max-degree). This made the separation process of insured and non-insured nodes more difficult for the insurer. Due to the possibility of reaching the bonus, a node will have more incentive to establish links, and are thus more acceptable towards establishing connections to risky nodes. The condition for separating insured and non-insured nodes are: $\beta + \gamma - r < I_l < \beta + \frac{\gamma}{m}$. For the separation to be possible, $1 - \frac{1}{m} < \frac{r}{m}$, and as we see as γ and/or m increases, this gets more and more difficult to achieve. The condition are strongly dependent on the max-degree. When the max-degree and bonus increases , it gets harder and harder to guarantee separation of insured and non-insured nodes.

In Model-4 we tried to implement a common feature used by insurance companies, bulk-discount, in order to see how this affected the network formation. The cost of insuring a link are now dependent on the nodes degree. We implemented this feature on both model 2 and 3, which resulted in even more incentive, or less disincentive, for an insured node to establish links with non-insured nodes. The reason is intuitive since the cost of doing so decreases as the nodes degree increases. When we applied the discount on model 2, the condition for ensuring separation of insured and non-insured nodes were: $N_I(\beta - r) < I_l < \beta$, where N_I represents the number of insured nodes in the network. This is a very strong condition, because we for the separation to be possible this has to hold: $N_I(\beta - r) < \beta$. For this to be true for a large number

of insured nodes, we see that β need to be just slightly bigger than r. And as we see, it is now more difficult for the insurer to separate insured and non-insured, compared to model 2.

When applying the discount to model 3, this is the condition to ensure separation: $m(\beta + \gamma - r) < I_l < \beta + \frac{\gamma}{m}$, and as in the other models, this further complicates the separation process for the insurer.

We also showed that the price of stability is even higher when applying discount to model 2. This is because the costs are decreasing, and thus when we have two separate cliques the potential lost payoff between them will increase. We where not able to calculate the price of stability in model 3, because the calculation of the optimal solution is to complex when the bonus and max degree is introduced. However, we can see that since the incentive for establishing links have increased, and thus the insurer has to set a higher price to compensate for this, the price of stability will be present. The same holds when we apply the discount to model 3, because this only further increases the incentive of establishing links, i.e. it gets harder to ensure separation of the nodes.

In our last model we applied our model-4(discount) to an already existing model, "the symmetric connection game". In this old game it has been shown that there exists three different efficient and stable networks, clique, star and an empty network, that arise under certain cost conditions. If $I_l < \beta - \beta^2$, the efficient and stable network is a clique. If $\beta - \beta^2 < I_l < \beta$ a star is both stable and efficient. If $\beta + \frac{N-2}{2}\beta^2$ an empty network is both stable and efficient. In general a clique is the most efficient if the cost of establishing links, is less than the benefit gained from indirect connections. A star is the most efficient if the cost is higher than the benefit from indirect connections, but less than the benefit of direct connections. However, it is proved that as the number of nodes in the networks increase, the probability of the network ending up in star goes to zero. But when we applied our insurance discount to this model, we found a conjecture that says, by setting the cost to the right level, one can with high probability ensure that a star will evolve. This changes the connection game drastically for the insurer, because he is now able to force the network into two possible network formations. Where the star has a fixation probability that exceeds the cliques. The insurer can use these findings to ensure that a star or a clique evolves. If the insurer are able to force a star to evolve, this can be used to drastically increase the overall security, and at the same time minimizing the overall link-cost.

Limitations and future work   One limitation to our work, and a suggestion for future work, is mapping our models and simulations to real world networks in a more convincing way. Real world network are not random, nodes may prefer to talk to nodes with high degree or low degree, i.e. the payoff function has to be changed.

Another limitation and suggestion for future work, is that we have assumed additive risk. It is reasonable to assume that the probability of failure increases if a node accepts more and more links to non-trusted nodes. However, whether the risk parameter increases according to an additive distribution, exponential, logarithmic or something completely different we where not able to determine. And by introducing a complex risk function, we would only have distorted the goal of the models. The decision of using additive risk was take due to the simplicity of the function and the fact that we do not know for sure how the distribution actually looks like. So suggestions for future work is to introduce different risk parameter, that are more applicable to the real world.

Another interesting thing to research, is the game of choosing insurance or not, in future work this could be applied to our models, however this could possibly be too complex, and only disrupt the models.

6.2   Conclusion

One of the many problems with cyber-insurance is to define the risk and calculate premiums, we think that by being able to both identify and force certain network structures to evolve, this could be easier to achieve. We surveyed different literature on networks and risk, and found recent literature who showed how graphs like cliques, star, super-star, funnel and meta-funnel, all have a calculable fixation probability, and that stars and funnels fixation probability exceeds the one of a clique. With these structures in mind, we created and analyzed different network formation games, and tried to find link-cost constraints, that enabled these structures to evolve. The analyzis where performed mathematically by using game-theory and confirming the results with a simulator created in NetLogo.

We created and analyzed five different models, starting with a very simple model, and step wise made it more complex and realistic.

In model one to four, we found cost constraints to separate insured and non-insured nodes into two cliques. In every model we added some new features that made the model more applicable to real world scenarios, and for every feature added it became more difficult for the insurer to separate the two types of nodes. This is due to the increased incentive for establishing links, and thus the nodes became more and more acceptable towards risk. We also showed that to be able to separate the networks into two cliques, the nodes must know the other nodes types. Or else, the nodes will have incentive to pretend to be an insured node, regardless of type, which will result in a untrusted network.

In the last model we introduced the concept of bulk-insurance into an already

existing network formation game, the connection game, and showed that this enabled the insurer to determine, with high probability, when and how, cliques, stars or scale-free network would evolve with. We showed that at a point, called critical degree, a nodes optimal strategy will change from relaying on indirect connections, to suddenly wanting to connect to everyone. If the critical degree is set to the right level, one can ensure that the different structures evolve. If the critical degree is set to a low degree, a clique will most certainly evolve, at a medium level a star will evolve, and at a high level a scale-free network will evolve. We proved this by performing multiple simulations, 50 simulations for every critical degree. What makes this an even more interesting finding, is that it is earlier proven that in the connection game, the probability of the network reaching a star goes towards zero as the number of nodes increases. However by introducing a discount, that will subsidize the center node, one can drastically increase the probability of the network ending up in a star.

In summary we have shown how insurers can, by adjusting the insurance cost, determine the resulting networks for different network formation games. And at the same time helping the insurer calculating the overall probability of fixation. We found these conditions for several models, with different aspects that relate them to real world and other insurance products. We believe our findings can help the cyber-insurance market evolve into the state everyone thought it would reach.

AVOID this in conclsuion   Avoid claiming findings that you have not proven-throughout your thesis • Avoid introducing new data • Avoid hiding weaknesses or limitations in your thesis(make a virtue of showing strong analytical skills and self-critique by discussing the limitations–but don't gooverboard on this!) • Avoid making practical recommendations (e.g. for policy).If you must include them put them in an appendix. • Avoid being too long (repetitive) or too short (sayingnothing of importance)

References

[Ake97]   George A Akerlof. The market for" lemons": Quality uncertainty and the market mechanism. *Readings in Microeconomic Theory*, page 285, 1997.

[And10]   R.J. Anderson. *Security Engineering: A guide to building dependable distributed systems.* Wiley, 2010.

[Aud]   Jan A. Audestand. Some aspects concerning the vulnearbility of the computerized society. http://www.item.ntnu.no/_media/academics/courses/ttm6/vulnerability.pdf. Accessed: 20/02/2013.

[BL08a]   Jean Bolot and Marc Lelarge. Cyber insurance as an incentive for internet security. *Managing information risk and the economics of security*, pages 269–290, 2008.

[BL08b]   Jean C Bolot and Marc Lelarge. A new perspective on internet security using insurance. In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, pages 1948–1956. IEEE, 2008.

[Blu11]   Easley D. Kleinber J. Kleinberg R. anad Tardon E. Blumen, L. Network formation in the presence of contagious risk. 2011.

[BMR09]   T. Bandyopadhyay, V.S. Mookerjee, and R.C. Rao. Why it managers don't go for cyber-insurance products. *Communications of the ACM*, 52(11):68–73, 2009.

[Böh10]   Rainer Böhme. Towards insurable network architectures. *Information Technology*, 2010, 2010.

[Bol85]   B. Bollobás. Random graphs. *Academic Press*, 1985.

[Bro]   RTM Insurance Brokers. Rtm's hackersforsikring. http://www.hackerforsikring.dk/index.html. Accessed: 13/02/2013.

[BS10]   R. Böhme and G. Schwartz. Modeling cyber-insurance: Towards a unifying framework. *Proceedings of GameSec*, 2010, 2010.

[CfAPA]   CAPA Centre for Asia Pacific Aviation. Skywest airlines. http://centreforaviation.com/profiles/airlines/skywest-airlines-oo. Accessed: 08/04/2013.

[Chu]   Emily Chung. Playstation data breach deemed in 'top 5 ever'. http://www.cbc.ca/news/business/story/2011/04/27/technology-playstation-data-breach.html. Accessed: 2/05/2013.

[CoA]   Travelers Casualty and Surety Company of America. Cyberrisk. https://www.travelers.com/business-insurance/management-professional-liability/Cyber-Risk.aspx. Accessed: 31/01/2013.

[Dic]   Oxford Dictionaries. Prisoner's dilemma. http://oxforddictionaries.com/definition/english/prisoner's%2Bdilemma. Accessed: 25/04/2013.

[dig]   digi.no. Vil forsikre alt og alle på nett. http://www.digi.no/39107/vil-forsikre-alt-og-alle-paa-nett. Accessed: 18/02/2013.

[DS06]   George Danezis and Stefan Schiffner. On network formation,(sybil attacks and reputation systems). In *DIMACS Workshop on Information Security Economics*, pages 18–19, 2006.

[EK12]   D. Easley and J. Kleinberg. Networks, crowds, and markets: Reasoning about a highly connected world, 2012.

[Faa]   faa Federal aviation administration. Calendar year 2011 primary airports. http://www.faa.gov/airports/planning_capacity/passenger_allcargo_stats/passenger/media/cy11_primary_enplanements.pdf. Accessed: 08/04/2013.

[Gar07]   Argyrakis P. Garas, A. Correlation study of the athens stock exchange. 2007.

[GGJ$^+$10] A. Galeotti, S. Goyal, M.O. Jackson, F. Vega-Redondo, and L. Yariv. Network games. *The review of economic studies*, 77(1):218–244, 2010.

[Ins11]   Ponemon Institute. Second annual cost of cyber crime study, benchmark study of u.s: Companies. Technical report, Ponemon Institute, Aug 2011.

[it]   Dagens it. Forsikring mot hackere. http://www.dagensit.no/arkiv/article1345297.ece. Accessed: 14/02/2013.

[Jac05]   M.O. Jackson. A survey of network formation models: Stability and efficiency. *Group Formation in Economics: Networks, Clubs and Coalitions, ed. G. Demange and M. Wooders*, pages 11–57, 2005.

[JW96]   Matthew O Jackson and Asher Wolinsky. A strategic model of social and economic networks. *Journal of economic theory*, 71(1):44–74, 1996.

[LHN05]   Erez Lieberman, Christoph Hauert, and Martin A Nowak. Evolutionary dynamics on graphs. *Nature*, 433(7023):312–316, 2005.

[MCR80]   R.I. Mehr, E. Cammack, and T. Rose. *Principles of insurance.* RD Irwin, 1980.

[New]   Graeme Newman. Cyber liability in europe: What insurers should knowl. http://www.cfunderwriting.com/media/news-articles/european-cyber.aspx. Accessed: 14/02/2013.

[Nor]   Gjensidige Nor. Medlemsfordeler hos gjensidige 2012 - nal. http://www.arkitektur.
            no/gjensidige?iid=372345&pid=NAL-Article-Files.Native-InnerFile-File.   Ac-
            cessed: 14/02/2013.

[NRTV07]   Noam Nisan, Tim Roughgarden, Eva Tardos, and Vijay V Vazirani. *Algorithmic
            game theory*. Cambridge University Press, 2007.

[Pal12]   Ranjan Pal. Cyber-insurance for cyber-security a solution to the information
            asymmetry problem. May 2012.

[PD12]   National Protection and Programs Directorate. Cybersecurity insurance workshop
            readout report. *U.S. Department of Homeland Security*, 2012.

[PGP11]   Ranjan Pal, Leana Golubchik, and Konstantinos Psounis. Aegis a novel cyber-
            insurance model. In *Decision and Game Theory for Security*, pages 131–150.
            Springer, 2011.

[PH]   Ranjan Pal and Pan Hui. On differentiating cyber-insurance contracts a topological
            perspective.

[PH12]   Ranjan Pal and Pan Hui. Cyberinsurance for cybersecurity a topological take on
            modulating insurance premiums. *ACM SIGMETRICS Performance Evaluation
            Review*, 40(3):86–88, 2012.

[PpD12]   National Protection and U.S. Department of Homeland Security programs Direc-
            torate. Cybersecurity insurance workshop readout report, Nov 2012.

[Pra]   Mary K. Pratt.   Cyber insurance offers it peace of mind – or maybe
            not.   http://www.computerworld.com/s/article/9223366/Cyber_insurance_
            offers_IT_peace_of_mind_or_maybe_not?taxonomyId=17&pageNumber=1.
            Accessed: 31/01/2013.

[Ris12]   Stratic Risk. Evolving cyber cover. http://www.strategic-risk.eu/Journals/2012/
            02/22/i/j/w/RiskFinancing_Mar12.pdf, March 2012. Accessed: 31/01/2013.

[Rob12]   N. Robinson. Incentives and barriers of the cyber insurance market in europe.
            2012.

[Spa]   Sparebank1. Spar inntil 25 https://www2.sparebank1.no/sr-bank/forsikring/
            skadeforsikring/fa-rabatt-pa-forsikringer/. Accessed: 09/04/2013.

[Wat08]   Joel Watson. *Strategy: An introduction to game theory*. WW Norton, 2008.

[Wat11]   Tower Watson. Despinte increasing cyber threats, most companies are not buying
            network liability policies. http://www.towerswatson.com/press/4482, May 2011.
            Accessed: 31/01/2013.

[Wik]   Wikipedia. The market for lemons. http://en.wikipedia.org/wiki/The_Market_
            for_Lemons. Accessed: 13/02/2013.

[Wil]   Uri Wilensky.   Netlogo, programmable modeling enviroment.   Accessed:
            15/02/2013.