,

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

List of Tables

Chapter 1
Introduction to Cyber Insurance

Cyber-insurance is an insurance product used to transfer financial risk associated with computer and network related incidents over to a third party. Coverages 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 cyber-insurance is 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, cyber-insurance has to deal with the problem of nodes asymmetric information, correlated risk and interdependent security [GGJ+10]. These three problem areas will be discussed in detail later in 1.2.1. First let's have a look at the similarities of normal insurances and cyber-insurance.

The basics principles of cyber-insurance relates to traditional insurance, where the insurance contract (policy) binds the insurance company to pay a specified amount to the insurance holder in case certain incidents occurs. In return, the insurance holder has to pay a fixed sum (premium) to the insurance company [Rob12]. As with other insurances, the cyber-insurance contract is signed between the insurance company and the insurer. The contract clearly specifies the type of coverage of the different risks, a risk assessment of the companies vulnerability and also an evaluation of the companies security systems. These assessments are used to calculate the companies premium [Rob12]. Generally, this means that the security is negatively correlated with the premium costs. Better security means lower price on the insurance premium.

1.1 General insurance

Generally, from the perceptive of the insurance company an insurable risks possesses seven distinct characteristics [MCR80]:

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

1.2 Cyber-insurance

When facing risk, there are typically four options available [A new perspective on internet security using insurance.. Bolot Lelarge]:

1. Avoid the risk

2. Retain the risk

3. Self protect and mitigate the risk

4. Transfer the risk

So far the risk management for computer networks have introduced methods to reduce the risks, 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 from these threats. 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 party who willingly accept it in exchange for a predictable periodical fee, namely premiums [BL08a].

1.2.1 Obstacles in cyber-insurance

As we have seen, cyber-insurance fit relatively well to the general insurance model, however there are some identifiable obstacles. These obstacles can be divided in to three categories, 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. A similar case for the security industry occur when buying insurance for your computer, and the insurance company has no way of confirming whether your computer is "healthy", i.e. not contaminated, or if it is infected. The other information asymmetry scenario is called moral hazard. It occurs when after the signing of the contract, 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 will see the information asymmetry problem is highly relevant regarding cyber insurance. Measuring the level of security is very hard, in addition will often people have an incentive for hiding information about their security strength. Because they might end up in a scenario where they describes what their weaknesses are, and thus the difficulty of successfully attacking them are lowered. Another problem

arising due to information asymmetry, is the so called lemons market [1]. It is difficult for a security software buyer to distinguish the performance(bad vs good) of different software products, and thus the reasonable thing to do, is to buy the cheapest. From this we see that every security software has to be sold at approximately the same price, and there is no way to distinguish good and bad software. If the cost of producing good security software is to 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, it enables computers to communicate, install and use different software. A good example is the operative systems for personal computers, today we only have a small set of operative systems available for use, and these systems have been standardized, such that they can communicate over the same communication channels, such as HTTP/IP. The standards are what makes the ICT-industry valuable, but also what makes the possible extent of the threats so large. All these systems that uses the same standards, creates a large number of similar exposure units, they share common vulnerabilities, which can be exploited at the same time.

A different scenario is natural disasters, If the backbone network is down for numerous reasons, every operator connected will loose the Internet connection, hence be entitled to receive compensation for the lost income.

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 occurs more likely, resulting in extremely high expenses. If the security breach is large, it could potentially cause so much damage, that the insurers will not be able to pay all of the customers who suffered, i.e. they go bankrupt.[BS10]

Interdependent security 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

[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(cherrie), the buyer will not pay the price the seller wants for a cherrie, and the seller will not sell a cherrie for the price of a lemon, and thus the lemons drives the cherries out of the market.

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 due to the fact that there are a variety of people who have not invested [Böh10].

Calculating loss Another concern regarding cyber-insurance relates to characteristic of calculating loss from [MCR80]. When facing a security breach there are to potential loss classes:[BMR09]

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

Cyber-insurance instead of security One 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, this problem might solve it self with the right pricing options. Meaning that the insurance companies can create pricing models which makes it economical beneficial to invest in security. Such model will also make sense for the insurance company, since better security systems yields lower probability for incidents. Similar pricing models are common through out the insurance industry, e.g. the bonuses a car driver might be offered due to no accidents for some time or being above a certain age etc. will lower the price the insurance premium.

1.3 Insurable topology

THIS IS WHAT WE MEAN BY AN INSURABLE TOPOLOGY

1.4 A small summary

Add a small summary here.. summary of related work

short presentation of what to come. "glidende overgang til current market".

Chapter 2
The cyber-insurance market

The market for cyber-insurance emerged in the late 90's when security software companies partnered with insurance companies and started offering insurance policies together with their security products. From a marketing perspective, adding the 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, starup companies, such as Safensure AS where established with respect to deliver cyber-insurance to the Norwegian and European market [dig]. Also established insurance companies such as Gjensidige Nor, started offering insurance products aimed for Internet web-sites. These insurances where created to insure lost income due to malicious hacker attacks, denial of service and other well know cyber-attacks at that time. E.g. 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 specified security measures were taken by the company [it].

2.1 Current market state

Despite the fact that cyber-insurance has been around for over a decade, the market still struggles to gain a foothold. Safensure AS does not exist anymore and Gjenside Nor does not advertise a cyber-insurance product. It seems to be lots of challenges for both buyers and sellers. Buyers face tremendous confusion about cyber risks and their potential impacts on business. In general, [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 especially due to network externalities. Even when companies have decided to purchase a cyber-insurance, they are confused with what kind of insurance they should purchase. The market of cyber-insurance tend to become a

lemons market, where the buyer have little knowledge to choose between the different insurances. Hence, people will buy the cheapest insurance, although it sometimes does not satisfies their requirement.

2.1.1 The UK and US market

The media coverage on corporate threats such as Stuxnet[1] 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. There are several different results and opinions regarding the health of the global cyber-insurance market. Companies studied in [Ins11] experienced successful attacks 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 an 56 percent 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, and that it is one of UKs 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. Although there is no shortage of providers,-they found that there are 9 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 where insured against cyber-attacks [Pra].

The numbers vary between the different surveys. However, all of them concludes that a large share of the companies are not protected against the residual risk of cyber attacks.

[1] Stuxnet, SKAL VI BESKRIVE HVA DET ER? ??

2.1.2 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. Additionally, 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 mail correspondence with Gjensidige Nor it was clear that they needed information 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. [Email from: Arild Hjelde, Gjennsidige Nor.] Unfortunately we were not able to obtain the cost of such insurance. However, a similar insurance is offered by RTM Insurance Brokers, a Danish company, with premiums ranging from DKK3400 for insuring a loss up to DKK2.5 million , to DKK12900 for insuring a loss valuated to DKK25 million [Bro]. This gives an indication of the cost of the current cyber-insurance in the Norwegian market.

2.2 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 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.

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

notes... One reason for why the number of insured companies are low could be the fact that a lot of companies are trusting their own IT-department to handle cyber risk. Hence they believe that they would not need a cyber-insurance [Wat11].

Part I

Prestudy

Chapter 3
Graph Theory

In nature and human societies there are lots of scenarios that can be described by using graphs and graph theory, from infrastructure, such as railroads, water pipelines and electricity grid, to societal relationships, disease epidemics and much more. Additionally computer networks, such as peer-to-peer networks, number of links to/from web-sites etc, is formed and evolves according to the laws of random graphs. When one can describe a phenomenon with graphs, it is much easier to analyze and find characteristics about the phenomenon, the graph serves as an analytical tool [Aud]. Our goal is to identify insurable graphs, such as graphs which yields higher security or graphs where the risk is calculable. This section will provide background information on how different graphs can be created and how they evolve.

There are some basic properties of graphs which is important to be familiar with. Figure 3.1 depicts the basics of an unweighted graph, 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 3.1).

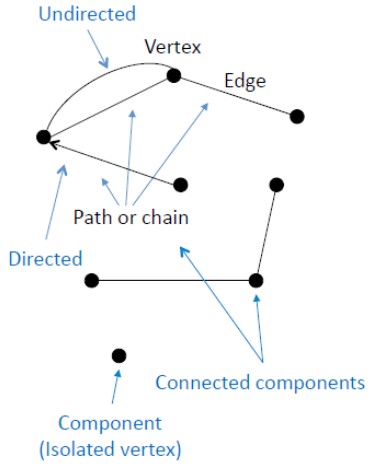


Figure 3.1: General graph [Aud].

3.1 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 $n(n-1)p/2 \approx n^2p/2$ 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 desrcription of 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. A 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 3.2 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.

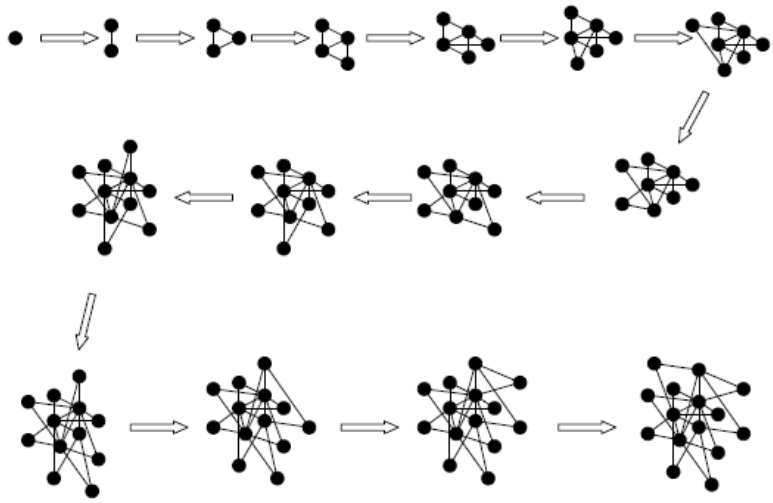


Figure 3.2: Forming a A-B graph in 15 generations [Aud].

In addition to the high clustering coefficient they showed that A-B-graphs have a fairly small diameter, which can be seen in Figure 3.2. A-B graphs are therefore comparable to the network formation of the Internet and other computer networks.

3.2 Real world graph structures

The internet, the World Wide Web, neural networks, scientific referencing and co-authorship, stock markets, airline routes, food webs, and modular software systems, all tend to evolve in a way similar to that described in the examples above. This section will provide some real world examples of how complex systems with huge amount of data can be described as network structures having the same characteristics as A-B graphs.

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 will present a clear understandable graph consisting of $(n-1)$ edges.

The resulting graph can be seen in Figure 3.3, and show a network consisting of several clusters linked together. Instead of having to analyze a complex system with huge amount of data, this 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.

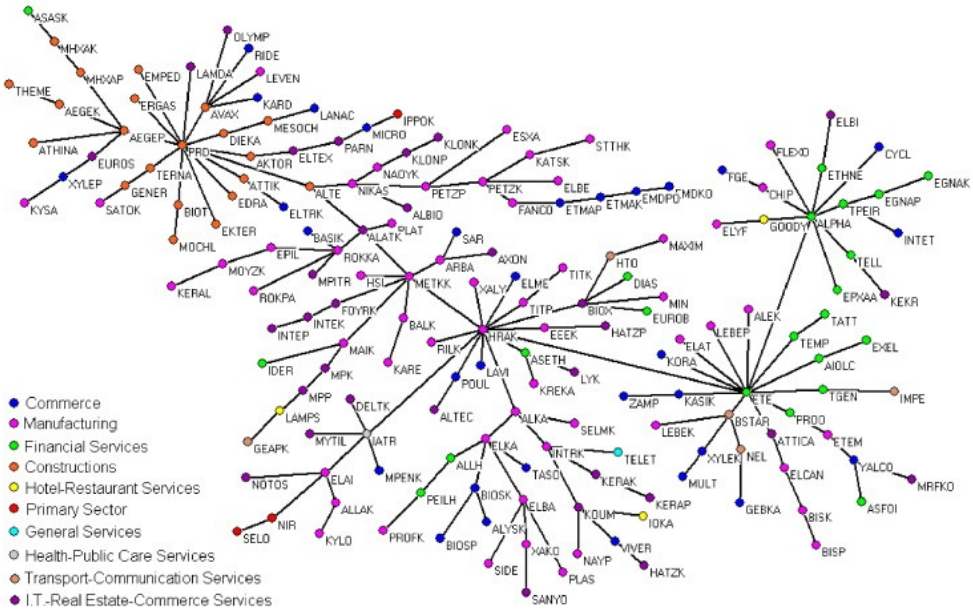


Figure 3.3: Network obtained by comparing two stocks correlation coefficient in the Greek stock market (Athens Stock Exchange, ASE) in year 1997. The different colors represent the different sectors of economic activity [Gar07].

Airline routes Another real world network which shows the same characteristics as scale-free graphs is the map of airline routes. Figure 3.4 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 3.4 follows the characteristics for A-B graphs. From the graph, we see that the network are vulnerable against direct attacks, meaning if an 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.

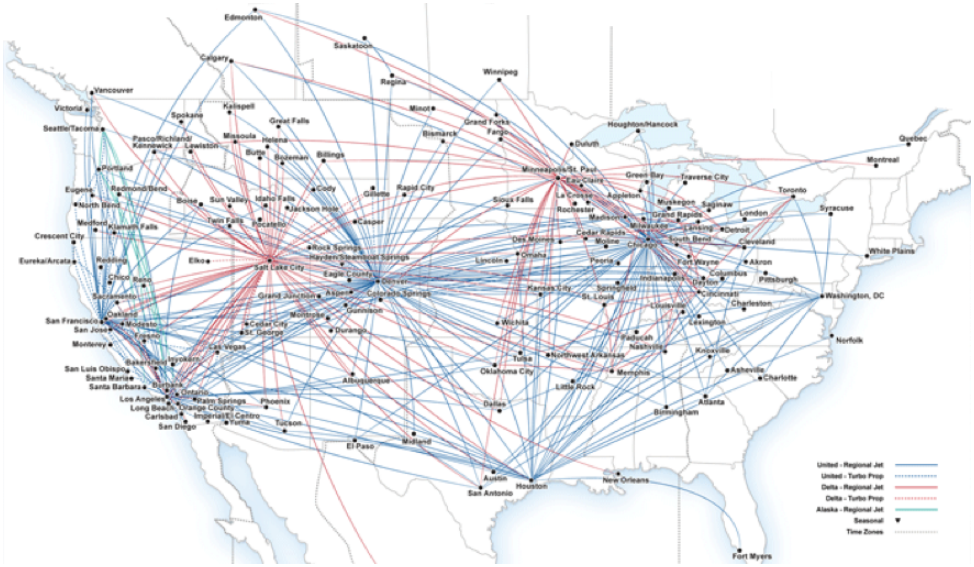


Figure 3.4: SkyWest Airline combined route map [CfAPA].

Similar findings will appear in the different networks mentioned earlier in this chapter, and all of them will experience large consequences if a hub in the network stop functioning. This is important for cyber-insurance because many of the networks we are analyzing tends to look and behave like A-B graphs. For example, transactions between companies, big companies probably have more transactions than small companies, and thus creates a hub, this can be compared with how the correlation between stocks in a stock market works. I.e. we can say that small firms correlate highly with big-firms.

3.3 Evolutionary dynamics on graphs

When investigating cyber insurance and insurable topologies, it is important not to only focus on standard risk networks, such as the internet. Our goal is to investigate all kinds of networks, or especially networks where players actions are influenced by their neighbourhood structure, i.e. the network connections will affect each individual players payoff. 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 her own actions, is a network worth considering network.

As mentioned earlier, the internet is a very good example, because on the internet we are "all" connected, the benefit we get from the internet is strongly dependent on this, and so is the risk we face when using the internet. Other examples could be the networks that are formed when a company are developing a software product, this development process is often done by several different firms, and thus creates a development network, where everyone is dependent on the result of the others. If one or more fail in some way, bankruptcy, failure to deliver at the expected time, higher cost etc. Then the whole network will be affected. Or in a cloud computing network, there are many different users and internet service providers, and the overall security is dependent on all of them. As we see all these networks are different from each other, some face direct connections, other consist of social and economical connections. But they all share some main characteristics, they are all experiencing network effects, externalities, information asymmetry, correlated risk and interdependent security. [GGJ+10]

In our paper an insurable topology, is an network structure which makes it feasible for both the insurer(supply side) to offer and the customer(demand side) to acquire insurance. For this to be possible there are many difficulties to overcome, one example are the correlated risks, from the insurers point of view, the problem is to be able to calculate the overall probability of casualty/infection, which can be very difficult without graph theory.

The paper [LHN05] is about evolutionary dynamics and how certain structures can amplify or sustain evolution or drift[1]. To be able to find insurable topologies, an extensive study of different graphs and how they behave has to be conducted. Regarding security, knowledge of how viruses spread and how to use graph structures to prevent malicious hackers from entering your network is important. Evolutionary dynamics, and the research of how mutant genes spread though out a population is a very useful field when looking for an insurable topology. If one can determine some structures, where some nodes are advantageous/disadvantageous , then these structures will have certain properties, such as sustaining viruses from spreading, or amplify the incentive for obtaining cyber-insurance and protection software. If one could identify these nodes and networks, then this information could be used to determine if it is an insurable topology.

In the [LHN05] paper, they show that mutants inserted in to a circulation graph, will have a fixation probability equal to

$$p_1 = \frac{(1 - \frac{1}{r})}{(1 - \frac{1}{r^N})} \tag{3.1}$$

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

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

The fixation probability determines how probable it is that the whole network will eventually be "infected" by the mutant. I.e. it determines the rate of evolution, which relies on both the size of the network and the evolution speed. A probability equal to one means that every node in the network eventually will be affected by the mutant. A circulation graph is not necessarily an insurable topology, but if we can find graphs with fixation probability that exceeds Eq.(3.1) they could possibly be considered as insurable topologies, because if we can find these graphs, then it will be possible to suppress drift and amplify selection and visa versa. The paper shows that there exists such graphs, one example is the star topology, (see Figure 3.5). In this topology the fixation probability is as shown in Eq.(3.2), or for more general see Eq.(3.3).

$$p_2 = \frac{(1 - \frac{1}{r^2})}{(1 - \frac{1}{r^{2N}})} \tag{3.2}$$

. or more generall:

$$p_k = \frac{(1 - \frac{1}{r^k})}{(1 - \frac{1}{r^{kN}})} \tag{3.3}$$

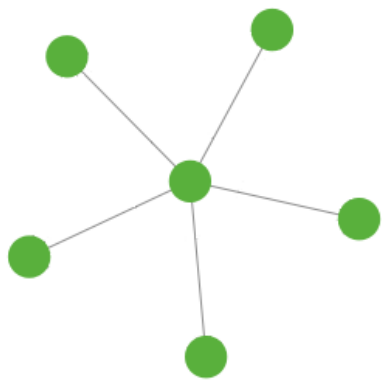


Figure 3.5: A star-topology.

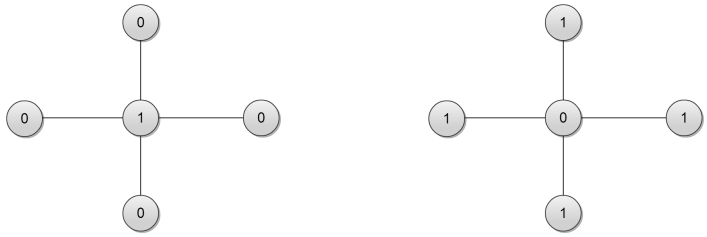
When comparing the Eq.(3.1) and Eq.(3.2), we see that the selective difference is amplified from r to r^2, i.e. a star act as an evolutionary amplifier, favouring advantageous mutants and inhibiting disadvantageous mutants.

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 the super-stars if N is large enough, the fixation probability for an advantageous mutant converges to 1, and for disadvantageous converges to 0. As we know from chapter 3, there are many topologies in our society that are so called scale-free. Scale-free networks have most of their connectivity clustered in a few verices, the star and the super-stars are all scale-free, and scale-free networks are potent selection amplifiers.

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

Lets consider a simple game shown in this paper, 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 neighbours: 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 Figure 3.6, 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: $\#leafnodes * c$, the first equilibrium have a total cost of only c. It would have been very good if we where able to force the game to 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 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) as shown earlier. And if they could ensure that the center node is protected they could also



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

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

Figure 3.6: Figure 3.6a shows the socially optimal equilibrium, and Figure 3.6b shows the non optimal equilibrium.

calculate the probability of the diseased mutant being extinguished from the network. 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 acquire the security product, and a very expensive insurance if not. In this way the insurer could force a rational center node to getting both insurance and 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, by using the results from [LHN05], force the game to end up in the social optimal equilibrium, and also how the insurer can calculate the probabilities of failure. The contributes 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, the most important information he needs is how secure the center node is. If he also can ensure that the center node is secure, the interdependent risk problem is limited to only one node, the center node. All this result in a simple but insurable network topology.

3.4 Notater og slikt

3.5 NOTES... random.. don't read

The game: The way this game works, is that we look at nodes that are mutated (A), and those who are not (B).

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

When we apply the game to a directed graph, there are four different outcomes, a,b,c and d, which represents the interaction between the nodes, as is depicted in Figure 3.7 below.

In the first figure (Positive symmetric) the fixation probability is related to r=b/c. If b is greater than c, the properties of mutant b will propagate in to all the other nodes, and the whole graph will eventually consists of only mutated nodes. The opposite will happen in the case where c is greater than b, leading to extinction of the mutation. The later scenario models the situation where proper protection against a mutant i.e. a security threat is installed. If the level of security, c is higher that the strength of the security threat it will be blocked from propagating further into the network.

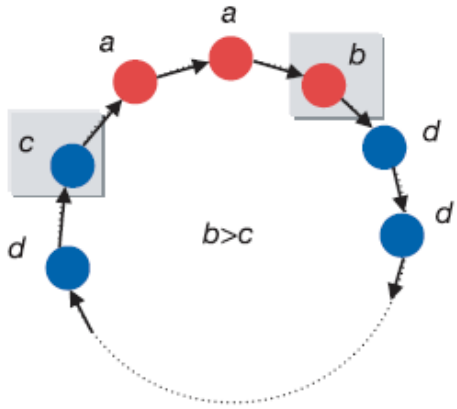


Figure 3.7: Mutant propagation game

More generalized, W does not need to be stochastic, $w_{ij} >= 0$. If the sum of all edges leaving a vertex is equal for all vertexes, then the graph will never suppress selection. If the sum of all edges entering a vertex is equal for all vertexes, the graph never suppress drift. If both then the graph is called a circulation.

Where the fixation probability determines the rate of evolution, which relies both on the size of the network and the evolution speed. A probability of 1 means that every node in the network eventually will be affected by the mutant. Isotherm graphs are a sub-graph of circulation.

If W is symmetric, or isotherm then the fixation probability is always Eq.(3.1) isotherm means doubly stochastic, all rows and cols sum to 1. If a graph is one rooted, it has a fixation prob of $1/N$ regardless of r. If a graph has more then one root, its fixation probability is zero. Is it possible to find graphs with fixation probability that

exceeds Eq.(3.1)? Is it possible to suppress drift and amplify selection?

NOTES!!! Geek stockmarket graph: http://www.sciencedirect.com/science/article/pii/S037843710

Hvorfor er slike strukturer viktige å forstå for oss? Som vi skal se senere oppfører hubene seg i A-B grafene som stjerne-topologier. Ved å ha oversikt over sitt eget nettverk vil man kunne identifisere hvor disse stjernene befinner seg, nettopp disse er det viktig at man sikrer for å ungå spredning av virus, samt fungere som en blokkade mot andre trusler e.g. hackers. (TROR DET er viktig at vi prøver å fokusere mot insurable og ikke spredning av virus.) så noe sånt: nettopp disse er viktige slik at man lettere kan kalkulere riskioen, og gi insentiver, ved hjelp av cyber insurance, til hubsa for å sikre seg eller no.

Chapter 4

Network formation: stability and efficiency

4.1 Survey of models of network formation: stability and efficiency

There is lots of economic situation where network structure plays an important role. It is very important to have information on how these structures form and matter. We can divide networks into two kinds, the ones where one central agent structures the whole network, such as airline network, or networks who are formed out of many different individuals decisions. This survey is about the second case, network connect a number of individuals.[Jac05] Three questions to focus on:

- How are such network relationships important in determining the outcome of economic interaction?
- How can we predict which networks are likely to form when individuals have the discretion to choose their connections?
- How efficient are the networks that form and how does that depend on the way that the value of a network is allocated among the individuals?

4.1.1 Defining Network Games

Players $N = 1, ...n$ set of players or individuals(organizations, firms, people, etc), modeled as nodes.

networks May take many forms, non-directed, directed networks. A network g is a list of which pairs of players are linked to each other. $N(g)$ is the set of players who have at least one link in the network g.

Paths and components Components of a network are the distinct connected subgraphs of a network, components of g are denoted $C(g)$.

Value functions

Network games

Allocation rules to know how much the total value of the network, we need to know how the value is allocated or distributed among players.

Chapter 5
Network Games

In the paper [Blu11], they come up with some 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 nodes fail, it will receive a negative payoff of b, no matter how many links it has established.

The results from their model shows a situation where clustered graphs achieve a higher payoff when connected to trusted agents, 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 neighbours, 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 $1/p$. At this point a node gets a payoff of a/p, 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 $1/p$ links, the edges which propagates risk, will with high probability form a large cluster. Which results in a rise in probability of node failure, and reduces the overall wellfare. From this the paper say that when the minimum welfare exceeds $(1 + f(\delta) * a/p)$ 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 supercritical payoff, is by forming clustered networks consisting of cliques with slightly more than $1/p$ nodes. If the nodes form an anonymous market, 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. But in random graphs, this is not possible.
notater The paper [Blu11] describes a model which seeks to capture the underlying trade-off between the benefits of adding new links and the problem with increased contagious risk. Results from the model describes a situation where clustered graphs

achieve a higher payoff when connected to trusted agents. This phenomena is called super-critical payoffs. Unlike in anonymous graphs, which are completely random, nodes in these graphs share some information with their neighbors, which is used when deciding whether to connect or not. The cliques, forms a clustered network of agents which trust each other, consequently the risk of cascading failures are lower. Inspired by this model, we created a model which shields light on how cyber-insurance can be used in network formation to prevent cascading failures and increase an agents payoff.

notater„, The notion of stable, is a relaxation of pairwise nash-stability, and is defined as:

- no node can improve their payoff by deleting all its links(removing itself from the network)
- There is no pair of nodes, i, j, who are not a part of the network G, who would have gained a higher payoff by joining the network.

This paper[GGJ+10] provide a framework for analyzing situations when a players actions is influenced by neghbourhood structure, modeled in terms of an underlying netwrok of connections that affect payoff. The players are partially informed about the structure.

There are many social and economic interactions where an agents well being depends on her own actions as well as on actions taken by others, i.e. externalities.

Chapter 6
Relatedwork

6.1 Cyber-Insurance

6.1.1 Paper from Bohme - SKAL FJERNES ETTERHVERT

While several authors have expressed doubts about the future of cyber-insurance, [EXAMPLES?] 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? 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.

6.1.2 A novel cyber-insurance Model - FJERNES ETTERHVERT

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 incentives users 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 its user 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.

6.1.3 Cyber-insurance for cyber-security, A Topological Take on Modulating Insurance Premiums - FJERNES ETTERHVERT

[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 insurable star topologies.

6.1.4 Differentiating Cyber-insurance Contracts, a topological Perspective - FJERNES ETTERHVERT

[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.

6.1.5 Towards Insurable Network Architectures

[BS10] A trusted component or system is one you can insure. Cyber insurance gives an incentive to better secure your network, and will thus reduce the overall threat for both first and third parties. It will also promote gathering and sharing of information related to security incidents. All in all this will increase the social welfare by decreasing the variance of losses. But even if cyber insurance seems very profitable for everyone, it has failed to evolve as much as expected. Some reasons for this, could be:

- lack of data to calculate premium.
- Underdeveloped demand due to missing awareness for cyber risks.
- legal and procedural hurdles in substaining claim.

A more economic model to describe why cyber insurance is still such a niche market.

Interdependent security Expected loss due to security breach at one agent is not only dependent on this agents lvl of security, but also by other agents security investment. A good example is spam, it is dependent of number of compromised computers. This also generates an externality and encourages to free riding. which then leads to underinvestment in security.

Correlated risks Many systems share common vulnerabilities, which can be exploited at the same time. This leads to a more likely occurrence of extreme and catastrophic events, which will result in uneconomical supply of cyber insurance.

information asymmetry Since measuring security strength is very hard, people have a high incentive for hiding info. This leads to information asymmetry. All these three form a triple obstacle, which eliminates the market in evolving. All these obstacles evolve from what makes ICT succeed, distribution, interconnection, universality and reuse. This is why Architecture matters. The obstacles does not arrive from properties of individual agents, but from integration and interaction in networking. Networking is not just physical, but a abstract structure mapping physical, logical and social interconnection. A good example is development tool chains. A web-browser is not just dependent of the security the developers have implemented, but also the security in the tools used, such as libraries. Topology determines to which extet a market for cyber-insurance is affected by interdependent security. Architecture of distributed systems is not given by nature, we can change it to the better. How to design a distributed system in an insurable way? These three problems have never been analysed together, this is what this paper contributes with.

How can economic and actuarial risk models be used to guide the design of more resilient distributed systems?

How to estimate a coefficient of the strength of interdependent security?

Architecture of large distributed systems is the result of many individual agents decisions. Therefore it is hard impose a more resilient(insurable) architecture on the agents. What if we give the agents incentives to form this network instead? i.e. setting incentives for individual agents to influence their private decisions towards more resilient social outcome. (Field: endogenous network formation)

Uses GT to model incentives of the different agents.

6.1.6 Modeling cyber-insurance: towards a unifying Framework

[BS10] proposes a framework to classify models of cyber-insurance. Uses a common terminology, and deals with cyber-risk in a unified way.(combines the three risk properties, interdepenedent security , correlated risk, information asymmetri.) The paper studies other existing models, and reveals a discrepancy(AVIK) between informal arguments in favor of cyber-insurance and analytical results questioning the viability of a cyber-insurance market. Cyberinsurance, the transfer of financial risk associated with network and computers incidents to a third party, has been researched for several years. But reality continues to disappoint. Sets back by physical accidents such as 9/11 Y2K etc. Clients are for the most SMBs, limited market. Conservative forecast predicted cyber-insurance worth $2.5 billion in 2005. Jonas found a paper from 2012 that said the market was $800million.

All three obstacles has to be overcomed at the same time to fix the market, to do this we need a comprehensiv framework for modelling cyber-risk and cyber-insurance. many researchers have lost their optimism about cyberinsurance, but this paper has not. Goal is that this unifying framework will help navigating the literature and stimulates research that results in a more formal basis for policy recommendations involving cyber-risk reallocation. Framework can also be used to standardize tcyber-insurance papers.

Breaks the modeling down to five key components:
- network environment(nodes controlled by agents, who extract utility. The risk comes from here
- demand side(agents)
- supply side(insurers)
- information structure, distribution of knowledge among the players.
- organizational environment. public and private entities whose actions affect netwrok security and agents security decisions.

what can be answered with models of cyber insurance markets?

1. Breadth of the market:Looking at equilibrium we can determine under which conditions will a market for cyber-insurance thrive? or what are the reasons for failure, and how can we overcome this?

2. Network security: What is the effect of an insurance market on aggregate nework security? Will the internet become more secure?

3. Social welfare: What are the contributions to social welfare?

Network Environment: Connected nodes

Two properties distinguish cyber-insurance from regular insurance.

1. Interconnected devices in a network, this generates value, therefore risk and loss analysis must take this into account.

2. Dual nature. if operational: generate value, else loss sources. When abused generate threat to other nodes.

network is not necessarily a physical connection, also includes logical link or ties in social networks.

Defense function Defense function D describes how security investment affects the probability of loss p and the size of the loss l for individual nodes. In most general its a probability distribution. An agent i only chooses s_i and takes the the vector of all other nodes level of security as given. This is how we model interdependent security.

network topology G Describes the relation between elements of an ordered set of nodes.(connectivity)
- star-shaped
- tree shaped
- ER
- Structured clusters

There are no literature using scale-free graphs, even this topology is a good fit with real world networks. Network topology shapes the risk arrival process, or defines the information structure when asymmetric information is considered.

Layers of multiple topologies for different properties of cyber-risk ar conceivable, i.e to model the specific influence of social and physical connections. But this will complicate the model.

Risk arrival defined by the relation between network topology G and the value of the defense function D Two cases:

1. no risk propagation, easy to tract analytically.
2. risk propagation, this is harder, need recursive methods or approximations, and may lead to a dynamic equilibria. both interdependent and correlated risk is modelled.

Cyber risk is characterized by both interdependent security and correlated risk, which both have a common root cause: interconnected nodes. Interdependent risk is usually modeled on the demand side, in contrast correlated risk is just a supply-side problem.

Attacker model existing literature assume attacks are perfomed by "nature" rather than strategic players. But attackers react to agents and insurers decisions. this paper models attackers as players. but it might be hard to choose reasonable assumptions and parameters for their capability. They could be modeled as an additional class of players or a special type of agents.

Demand side agents

Make security decisions for one or more nodes. When buying full coverage of risks, permits the agent to exchange uncertain future costs with a predictable premium.

Node control Agents have node control, mapping one to one, or one to many. Agents choose security investments for the nodes.

Heterogenity Agents(and associated nodes) are either heterogen or homogeneous in:

- their size of the loss
- their wealth
- their defense function
- their risk aversion and this utility function.

agents are homogenous if all of the above statements are identical for them.

Risk Aversion They only seek insurance if they are risk averse(accept lower expected income if they can reduce uncertainty).

Action space Established models differ in the action space for agents purchasing insurance. Options are:

Full or partial. Full, the only choice is between full coverage of the potenital loss or no insurance at all, i.e. binary choice. A contract is called fair if the expected profit from it is zero(insurers point of view). If premiums are actuarially fair, risk averse agents strictly prefer full over partial coverage. If premium is above fair lvl, partial insurance are demanded.

Security investment: agents can self-protect by choosing $s_i > 0$, which result in less expected loss. Selfprotection creates an externality, ie interdependent security. Second kind of security investment, i.e selfinsurance, this does not generate externality, it only reduces your own size of potential loss.

Enogenous network formation: changes to the network topology as operable actions for agents is not yet explored by literature. For example, agents ccould destroy/create links to other nodes with the goal of reduce their expected loss. A simple first step would be to consider platform diversity and switching(f.eks mellom OS) as an endogenous network formation problem.

Time Simple models, single shot. i.e all choices are set only once by all agents(not necessarily at the same time.) This may not be enough when risk propagation is present. To avoid ambiguity the order should be specified in the model formulation, f.eks from the center of a star-shaped to its leaves.

Supply side, insurers

Modeling decisions: monopoly, oligopoly or competition? Homogenous or heterogenous? The dominant model used in literature is naive, homogenous and competitive insurer market. It is important to include these as players. Five attributes: market structure, risk aversion, markup, contract design and higherorder risk transfer.

Marketstructure , monopoly, oligopoly or competition. Homegenous or heterogenous? Competitions leads to low MC.

Risk aversion A simplification in economic textbooks is to use risk neutral insurers. But to avoid taking excessive risk and bankruptcy due to profit maximization, need a safety capital. Regulators decide a maximum residual risk.

Markup : insurers profit, admin-costs, cost of safety capital.

Contract design : fixed premium, premium differentiation, contract with fines.

Higher order risk transfer : Insurers need not be the last step in a chain of risk transfer.

Cyber-reinsurance, the usual way to do this is by generating pools of loosely correlated risks, i.e the loss events from the tail of the probability distribution. This is usually done by creating a pool from regional or international diversification. Cyber-reinsurance is virtually not existent, due to the global homogeneity of cyber risk.

catastrophe bonds, financial instrument which pay a decent yield as a risk premium in periods without catstrophic events, but lose their value when such an event occurs. These are inadequate for cyber-risk, because thei may generate an incentive for investors, to cause a cyber attack.

exploit derivatives. Links payout of financial instrument to the discovery of vulnerabilities in systems. This is better than cat-bonds.

Information structure

Symmetric and asymmetric. Leads to adverse selection if the insurer cant distinguish between the agents. Moral hazzard occurs if agents could undertake actions that affect the probability of loss ex post. Also information about security is hard to gather and evaluate,. . All this results in two types of contract scenario, pooling or separation(agents sort them self out).

- adverse selection, if the insurer cant distinguish agents before signing contract.
- moral hazzard, if agents can undertake actions that affect the probability of loss after signed contract. i.e. not locking the door.

From classical economics, insurers have to ways of creating the contract when they cannot distinguish the agents, pooling or seperating(agents sort them self out). there is practically understood and observable that strong disincentives keep information sharing below socially optiimal levels. Relevant information may not exist, but it is often the case that it exists but is not available to the decision maker.

Organizational Enviroment(stakeholders)

four relevant attributes: regulator, ICT manufacturers, network intermediaries and security service providers. How to include these into models of cyber-insurance markets?

Regulator Government/governmental authority, with power to impose regulation. Important for policy analysis.

- disclosure requirements, can improve information for agents and insurers.
- Taxes, fines and subsidies to alter agents and insurers cots.
- Mandatory security impositions.
- prudential supervision, the regulator defines the acceptable residual risk, the probability of insurer bankruptcy.

ICT manufacturers vendors of hardware and software equipment.

- system security: ICT manufacturers prioritization of security affects the defence function of nodes using their products.
- System diversity, market structure affects correlation in the risk arrival process.

Network intermediaries Provide network connectivity services, ISP, registrars, and application service providers. they can contribute to distributed defense by sharing info about threats or taking down compromised nodes, reducing risk propagation. They can also shape the network topology, generating a more safe topology. Problems: different incentives for different ISPs, such as large versus small ISP.

security service providers Contribute to network security, in helping to overcome information asymmetries through collection and aggregation of information as a trusted third party, or improve information efficiency in monitoring and enforcing contracts. (Forensic investigations certifying etc.)

6.1.7 Using this framework for a literature survey

This framework accounts for three factors, correlated risks, interdependent security and information asymmetries.

demand side some papers have homogenous agents, others have heterogenous. Contracts with deductibles are standard tools to deal with information asymmetries. These are introduced in 4 papers. All models featuring interdependent security must allow for some kind of security investment via self-protection(binary or continous choice). Partial insurance is common, or full for simplicity.

Supply side Homogenoues and perfectly competitive insurers, and premium markups. Several authors interpret the markup as a reflection of market power.

Organizational Environment Current formal models are not good at capturing parameters of the organizational environment. Do insurance need to be mandatory, or will a simple punnishing of agents underinvesting in self-protection be sufficient. Rebates and fines are also discussed in one paper.

Research Question No paper who capture all three obstacles theoretically and link them with social welfare. Only one study evaluates its model from the perspective of all three research questions: breadth of the market, network security, and social welfare. Literature inspured by interdependent security primarily investigates network security, the most natural variable of interest in this setting. By contrast, Correlated risk and information asymmetries are studied from the point of vie of explaining a missing market.

Discussion of models The results from the papers are very dissappointing, so one may ask what are they good for. They give intuition on specific aspects and help generate a general view.

Despite early optimism about positve effects of cyber-insurance on network security, the existing models find that insurance markets might fail. And if a market exists, it tends to have adverse effects on incentives to improve security. Future research: endogenize parameters that are exogenously given in the existing literature, information structure and or organizational environment. for instance network topology.(This is what we will try to grasp, let the topology be generated endogenizely. final observation: researchers write about how insurers will improve infomartion about security, but does not give any examples that reflects this. Affect agents choices of network products, but existing models of contracts do not reflect these choices. aggregate info about security(obtained from claims), but they do not model it parametrically. etc.....

6.1.8 A novel cyber-insurance Model

[PGP11] eliminate threats which cannot be tackled through traditional means, such as AV. Risks arrise due to both security attacks and non-security related failures. This paper analyzes cyber-insurance solutions when a user faces risks due to both of these. Propose a model called "Aegis", user accepts a fraction of loss recovery and transfers the rest.Mathematically show that only under conditoons when buying cyber-insurance is mandatory.

6.1.9 Cyber-insurance for cyber-security, A topological Take on Modulating Insurance Premiums

[PH12] Adopts a topological perspective in proposing a mechanism that accounts for the positive externalities, network location of users, and provide appropriate way to proportionally allocate fines/rebates on user premiums. Uses GT to prove. Consider a monopolistic cyber-insurer, prodividing full coverage. Each client is risk averse. A users investment and location in network determines his risk type. Each user has a utility function dependent on the rest of the users. Node centrality, maps to the externality effects a node has on other network nodes. Uses eigenvectors and bonacich papers. both these assign relative importance scores to all nodes, based on the concept of connections.

6.1.10 Differentiating Cyber-insurance Contracts, a topological Perspective

[PH] Important to discriminate network users on insurance contracts. prevent adverse selection, partly inernalizing 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. Important to find a way to properly discriminate. The paper propose a technique based on the topological location of users that allows cyber-insurers to appropriately contract discrimanate their clients. Consider single cyber-insurer providing full or partial coverage. Insurer have complete information about the topology. Discriminates on Bonacich/eigenvector centralities.

6.1.11 Cyber insurance as an Incentive for Internet Security

[BL08a] so far the risk management on the internet has involved methods to reduce the risks(firewalls, ids, prevention etc.) but not eliminate risk. Is it logical to buy insurance to protect the internet and its users. An important thing to notice when insuring internet, is that the entities on the internet are correlated, which means insurance claims will likely be correlated. Risks are interdependent, decision by an entity to invest in security affects the risks of others. Key result: using insurance would increase the overall security. Act as an powerful incentive, which pushes entities over the threshold where they invest in self-protection. Insurance should be an important component of risk management in the internet.

Four typical options available in the face of risks. 1. avoid the risk 2. retain 3. self protect and mitigate 4. transfer the risk. Most entities in the internet have choses a mix of 2 and 3. This has lead to lots of systems trying to detect threats and anomalies(both malicious and accidental) and to protect the users and the structure from these. but this does not eliminate risk, threats evolve over time and there is

allways accidents. How to handle this residual risk? Option 4, transfer the risk to another entity who willingly accept it(hedging), insure in exchange for a fee. Allows for predictable payouts for uncertain events. But does this makes sense for the internet, benefits, to whom? and to what extent?

How to model insurance and computing premiums. avoid ruin the insurer. Actuarial approach. Economic approach: premium should be negative correlated to the amount invested in security by the entity. Users can chose to invest c or not in security solutions. Shown that in the 2 user case in absence of insurance, there is a NE in a good state, if c is low enough. These result have been extended to a network setting. This paper starts out by adding insurance to the two person game, then the n-users network, where damages spread among the users. They show that if premium discriminates about investment in protection. Insurance is a strong incentive to invest in security. Also show how insurance can be a mechanism to facilitate the deployment of security investments by taking advantage network effects such as treshold or tipping point dynamics. Uses simple models.

Using cyber insurance as a way to handle residual risk started out early in the 90's. Software and insurance sold as packages. More recently insurance companies started offering standalone products. A challenging problem is the correlation between risks, interdependent risks(risk that depend on the behavior of others).

Classical model for insurance

agents try to maximize some kind of expected utility function, and are risk averse. $u[w_0 - \pi] = E[u[w_0 + X]]$

Investments for an agent is either self protect and or insurance. If insurance premium is not negatively correlated to the self protection, we get moral hazard. Because if not, insurance will disincourage self protection. In this way insurance can co-exist with selfprotection.

Interdependent security and insurance

In presence of interdependent risks, the reward for a user investing in self-protection depends on the security in the rest of the network. Discrete choice, invest or not. loss occurs directly or indirectly. Cost of investing is c. This avoids the direct loss completely. In summary, insurance provides incentives for a small fraction of the population to invest in self-protection, which in turn induces the rest of the population to invest in self-protection as well, leading to the desirable state where all users in the network are self-protected. Furthermore, the parameter y provides a way to multiply the benefits of insurance, by lowering the initial fraction of the self-protected population needed to reach the desirable state. This paper shows that insurance

provides significant benefits to network of users facing correlated, interdependent risks. Insurance is a powerful mechanism to promote network-wide changes, i.e lead to self protection. How to estimate damage? This is very hard on the internet. This paper shows how it is economical rational for entities to prefer a relatively insecure system to a more secure, and that the adoption of security investments follows treshold/tipping point dynamics. And that insurance is a powerful incentive to push the users over the treshold.

6.1.12 A solution to the information Asymmetry Problem

REFERENCE??! AV and other security software reduces the risk, but does not remove it completely. Cyber-insurance, residueal risk elimination. But a problem with this is information asymmetry. This paper proposes three mechanisms to resolve this problem. Mechanisms based on the principal agent problem, difficulties in motivating one party(the agent) to act in the best interests of another (the principal) rather than in his or her own interests. Arises in almost every case where a party pays another party to do something. The agent has more information than the principal, asymmetric.

1 cyber insurance who only provide partial coverage to the insureds will ensure greater self defense efforts.

2 the lvl of deductible per network user contract increases in a concave manner with the topological degree of the user.

3 Cyber-insurance market can be made to exist in the presence of monopolistic insurers.

Security experts claim that it is impossible to achieve perfect internet security just via technological advancements.

1 there do not always exist fool-proof ways to detect and identify. Even the best software available have false-positive, false-negative. And threats evolve automatically in response to AV-software being deployed.

2 The internet is a distributed system, different security interests and incentives pr user. Might spend money to protect their own hard drive, but not on prevent its computer being used by an attacker for a DOS attack on a wealthy corporation.

3 Correlated and interdependent risks. As a result, a user who invest in security generates positive externality for others. Which will result in a free rider problem.

4 Network externalities due to lock-in and first mover effects of security software vendors affect the adoption of more advanced technology.

5 Security software suffer from lemons market.

Cyber-insurance and asymmetry insurers are unable to disttinguish high and low risk users, i.e adverse selection. users undertaking actions, i.e moral hazard.

Difficult for insurers to gather information about applications, software installed, security habbits etc. and users can hide inforamtion.

Users in general invest to little in self-defense relative to the socially efficient lvl due to the free-rider problem(externatlities). Thus the challenge to improving overall network security lies in incentivizing end users to invest in sufficient amount of self defense.

6.2 Networkformation

6.2.1 Model from Bohme

[DENNE SKAL SKRIVES OM OG TILPASSES RELATEDWORK]

Our model now includes a way of analyzing indirect connectivity among nodes. Inspired by the paper from [DS06] we are now expanding the model to look how network formation works when the nodes have a option to include uninsured nodes in their network. Although the paper tries to observe suseptibility to sybil attacks in peer-to-peer networks, their approach on network formation is related to our insurance network. They propose a network formation game consisting of "friends" and "strangers", which is similar to "insured" vs "non-insured" nodes. In a peer-to-peer network the peers selfishly tries to fulfill their communitaction needs, by establishing connections to friends or indirectly via strangers. This is similar to how companies selfishly choose to connect to other nodes with the goal of increasing their utility as much as possible.

In [DS06] the formation game shows how nodes routes messages between each other. The special case here is that a node does not have enough links to directly connect to everyone. We change the game variables to fit to our model, and the setup for the game is as follows:

1. There are a set of $Nnodes$ which are to be connected in a graph.
2. Each node, n has a set for friends (insured nodes) F_n which he want to connect to. The friendship is symmetric.

3. Each node also has a *link budget*, L_n which specifies the maximum number of links a node can establish directly to friends. It is also assumed that $L_n < F_n$. Additionally, if a link is established both nodes will decrease their link budget.

4. Given a graph of links between nodes the utility of each node is calculated using the negative sum of the length of the shortest path to all it friends. Negative sum yields higher utility as the different path lengths decreases.

The goal is obviously to increase the utility. To accomplish this one has to communicate with friends using a minimum number of hoops. If $L_n =< F_n$ the game would have been a straightforward dominant strategy, where insured nodes only chose to connect to other insured nodes. Hence every node would receive the maximum utility. In the scenario of peer-to-peer network it is easy to understand that one cannot have direct links to every friend on a scale free network, e.g. the Internet, hence $L_n < F_n$ makes perfect sense. It is also reasonable to take the same assumption for the insurance market, since one might not have the resources to insure every connection needed, i.e. the link budget $I_n < F_n$. Hence the nodes might take the risk of connection to non-insured nodes, since the cost of connecting to this node is free.

The graph is created by a pseudo-random selection of a possible link between two nodes. If the utility increases or is stable for both, the link is created and each node decreases their link budget by one.

[DS06] proposes two random games which interpret that 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 Nash equilibrium, it is believed that every node is eager to use their whole link budget in order to create direct connections to as many insured nodes as possible. In order to reach the rest of the insured nodes, they rely on indirect connectivity via the established connections.

The unbalanced model results in a scenario where the insured nodes still wishes to connect to other insured nodes. The reason for this is claimed to be that the average shortest path in a scale-free graph is $O(logN)$, and the probability that another node,

insured or not insured, is closer to to a node is roughly the same. Which means that on average an insured node will benefit from connecting to other insured nodes. However, if the link budget only allows each node to only establish 1 link (except the one with a large budget), it will emerge a Nash equilibrium which is star with the rich node in the center. If the rich node is a insured node, all the other insured nodes will connect to this node.

Maa tilpasse konklusjonene her bedre..

6.2.2 Related work 2

Virus and worm propagation on the Internet can be modeled as epidemic spreads. When we look a 2-agent model we can observe correlation between one agents choice of investing in protection. If agent 1 has a connection to agent 2, the probability of agent 2 being contagion is strongly correlated to the choice of agent 1. In the case where agent 1 invests in protection, agent 2 will not be infected. However, if chooses not to invest in protection, the probability of infection for agent 2 is p. After a number of equations the authors conclude that in presence of insurance, the optimal strategy for all users is to invest in self-protecting services as long as this cost is low enough.

Further the authors looks at the situation where the cost of selv-protection is different for different agents (heterogeneous users) in a complete graph (n-n). The conclusion states that insurance increase the adoption for a fraction of the users, which creates the cascading effect that the rest of the users also gains benefit from investing in insurance. We end up in a state where everyone in the network are self-protected.

In star shaped graphs (i.e. hubs), it is obvious that the network will decrease the probability contagion dramatically by investing in self-protection measures. The authors also assumes that it is likely that the other low connectivity nodes will follow the hub and adopt self-protection.

6.2.3 Contagion Paper

FLYTT DETTE TIL BACKGROUND og referer til det når vi viser at cliques er bra The paper [Blu11] come up with some 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 results from their model shows a situation where clustered graphs achieve a higher payoff when connected to trusted agents, 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 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 supercritical payoff, is by forming clustered networks consisting of cliques with slightly more than $\frac{1}{p}$ nodes. If the nodes form an anonymous market, 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. But in random graphs, this is not possible.

6.3 NOTES!!!!! This was previously placed in current market

When facing a security breach there are two potential loss classes: Primary losses, also called first-degree loss. Meaning a direct loss of information or data and operating loss. Which arises from unuse, disuse, abuse and misuse of information. The cost related to this losses comes from recovering, loss of revenue, PR and information sharing, hiring of IT-specialists etc. Secondary loss is indirectly triggered. Such as loss of reputation, goodwill, consumer confidence, competitive strength, credit rating and customer churn. These claims arise from loss of external parties, sensitive data, and generally contribute to an even higher cost [BMR09].

Both classes can be covered by cyber-insurance, and usually will these contracts based on the same two classes, i.e you have to get an insurance for both. Here is an example contract from [CoA].

6.3.1 Contract structure

Travelers cyber-insurance:

- Liability insurance.

1. Network and Information Security Liability
2. communications and Media Liability
3. Regulatory Defense Expenses

– First party insuring agreements:

1. Crisis managment event expenses
2. Security breach remediation and notification expenses
3. computer program and electronic data restoration expenses
4. computer fraud
5. fund transfer fraud
6. e-commerce extortion
7. business interruption and additional expenses

6.3.2 Economics

Traditional security is a public good and are usually provided by the government. The threats are also originating from a small number of actors. What about internet security, should it be handled by the government. We do not have anti-tank gear in every house, should we have anti virus software on every computer? there are strong externalities involved, if a unsecured computer joins the internet, it end up dumping costs on others, just like pollution. Lemons problem, antivirus software. because the customer cant see the difference. Asymmetric information explains many market failures, low prices in lemons-markets, why sick people struggle with getting to buy insurance. A good example of misaligned incentives is bank frauds in US and UK, in US the banks are the ones hold responsible, in UK it is the customers. One would think the banks in UK was better off, but they are not. Similar problems can be found in other systems, and the problem is security failing because the people guarding a system are not the poeple suffering the costs of failure.

6.3.3 Epidemics

[EK12] The social network within a population, has a big say in determining how diseases is likely to spread. it can only spread if there are contact between to persons(Nodes), the contact network. The contact network for to different diseases can differ radically, e.g java viruses versus worm propagating through another vulnerability. Or internet viruses versus viruses that spread through short-range wireless communication.

modeling contagion

branching processes first wave, a person carrying a new disease enters a network, and transmits to everyone he meets with a probability of p, he meets k-people. second wave, each person from the first wave now meets k new people, i.e a total of k times k and if infected passes the disease on with probability p. further waves are formed in the same way. With this simple modeling approach, we get a tree, with a root node which creates branches to new lvls of the tree. With low contagion probability, the infection is likely to die out quickly. If the disease in a branching process ever reaches a wave where it fails to infect anyone, then it has died out. It is only two possibilities for the disease in a branching model, either it dies out, or it continue to infect infinitely many waves. These two possibilities can be differentiaded by a quantity called the basic reproductive number. R_0, this is the expected number of new cases of the disease caused by one person/node. In this basic model this number is: $p * k$. If $R_0 < 1$ then with probability 1 the disease dies out after a finite number of waves, if $R_0 > 1$ then it continues to infect atleast one person each wave with a probability greater than 0. A interesting thing to notice about these statements, is if the R_0 is close to 1 in either way, then a small shift in the probability will change the disease status from terminating to widespread or visa versa. This suggests that around the critical value $R_0 = 1$ it can be worht investing large amounts of effort to produce small shifts in R.

SIR epidemic model Can be applied to any network structure, preserve the basics of the branching process at the level of individual nodes, but generalize the contact structure. A node goes through three potential stages:

1. Susceptible(S): Before the node has caught the disease.
2. Infectious(I): once the node has caught the disease, it is infectious and can infect other susceptible neighbors with probability p.
3. Removed(R): After a node has experienced the full infetious period, it is removed from consideration, since it no longer poses a threat.

Network with directed edges. The progress of the epidemic is ontrolled by the contact network structure, probability of contagion and t_I the length of infection. When a node enters the I state, it remains infectious for a fixed number of steps t_I. During each of these steps it has a probability of infecting its neighbours. After t_I it is removed(R). Good model for disease you can only catch once in a lifetime. Important to note that in networks that do not have tree structure, the claim made earlier about $1 > R_0 > 1$ does not necesarily hold anymore. The network structure is very important, it can decide if a disease will spread or not. Narrow channel example.

Extension to SIR The SIR model is simple, to make it more realistic we can add probability q of recovery, and also add different probabilities for contamination between nodes, due to stronger contact. We add periods to the infection time, early, middle and late and allow different probabilities for infecting in each of these states.

Model from dynamic to static(Percolation) assing a probability of infecting on every edge, calculate this at the beginning, and thus an infected node has to connected to another infected node by an open edge. Think of it as fluid running through open and closed pipes. Its only the open ones who can be affected.

SIS epidemic model Nodes can be reinfected. Only two states, susceptible and infectious. Researchers have proved "knife-edge" results on these networks as well. A SIS epidemic can be represented by a SIR model by using a "time-expanded" network. Duplicate the nodes to the next time-frame.

SIRS Epidemic model Remain removed(immune for a fixed period of time) t_R, this model fits good with many real world diseases. It can produce oscillations in very localized parts of the network, with patches of immunity following large numbers of infections in small areas.

6.3.4 Incentives and Information Security

People have realized that security failure is not only caused by technical mistakes but also misaligned incentives. When the person guarding them is not the one who suffers when the system fail, there are strong misaligned incentives. As the book [And10] states, the tools and concepts of game theory and microeconomic theory are becoming just as important as the mathematics of cryptography.

Informational asymmetries peer-to-peer network, these exploit network externalities to the fullest by having large member populations with a flat topology. Joining creates the possibility of collaboration with everyone. it is easy to cheat.One solution, change the network topology, create clubs of nodes, one need to establish trust with the club, then you can connect with outside groups through your group. Social networks can also be used to create better topologies, when honest players can select their friends as neghbors., they minimize the information asymmetry present during neighbor interactions. Another information asymmetry in security, is due to our inability to measure software security. Network science and information security, the network topology can strongly influence conflict dynamics. Externalities makes security problems reminiscent of environmental pollution, public goods.

.....End of the stuff from current market.....

Chapter 7
Methodology

7.1 Game Theory

7.1.1 Nash Equlibrium

7.1.2 Price of Anarchy

7.1.3 Social Optimal

7.1.4 Steckleberg game

7.2 Netlogo

Part II

Own Contribution

Chapter 8
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.

Inspired by the model in paper [Blu11] [SKRIV OM SÅ DET PASSER... DEN ER BESKREVET I RELATED WORK], we are step wise building a model which shields light on how cyber-insurance can be used in network formation games to prevent cascading failures and increase an agents payoff.

8.1 Model 1 - Initial Model

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

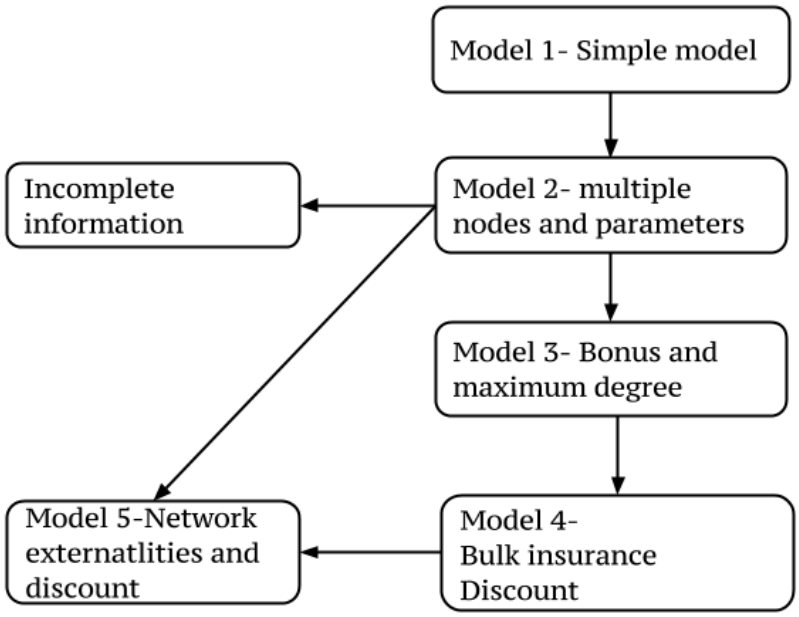


Figure 8.1: The figure show an overview of the different models we have created, and how they relate to each other. For every step, there are added some new features to the model.

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.

As a starting point the model is highly simplified in order to show the concept of how cyber-insurance can be used to create an insurable topology. We assume that every node has complete network information, i.e. it knows how many nodes that exists, if they are insured or not. The link establishment process is bidirectional, meaning both nodes must agree to establish the connection. Through out this chapter new features will be added to the model to make it more realistic and applicable, an overview of the different models can be seen in Figure 8.1.

A set of n nodes are randomly chosen to be insured or not, as depicted in Figure 8.2a. 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 i.e. 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

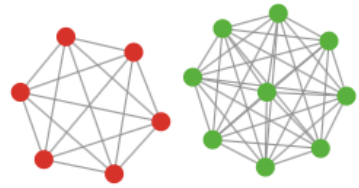
agents and non-insured agents can only connect with each other.

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 8.2b.

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.

Hence this model, although very simple, shows an insurable topology where insured agents benefit from being insured.

(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 8.2: Shows how agents connects to eachother according to model described in section 8.1.

fjern dette? This model is very simplified and suffer from many limitations, among others it is too simple to reflect the dynamics of a real world scenario, where each node will have different variables with different values. Although it tries to deal with the problem of correlated risks and preventing free riders from entering the trusted clique (interdependent security problem), each node have a complete network information i.e. the problem with information asymmetry is not taken into account. **slutt paa fjern dette**

8.2 Model 2 - Including Parameters

To make the simple model more realistic, we have to introduce some parameters, that 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 a 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 the nodes will also receive a positive change in payoff when establishing different links.

8.2.1 Characteristics of the model

The type of the nodes are given in advance, i.e. they are chosen to be insured or non-insured. The process of establishing link is a bidirectional decision. The insured nodes have to pay an insurance cost I_0, which represents the cost of signing a contract with an insurance company. I.e this could be an actual fee or a cost reflecting the work a player has to do to get a contract. The insurance premium is I_l, the expected risk cost is represented by r. β represents the benefit of establishing a link. Table **??** presents an overview of the parameters.

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

8.2.2 Two nodes scenario

To begin analyzing the model, lets start with a simple 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 or not. 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. Figure 8.3 shows the different outcomes of this game.

As long as both I_l and r is less than β, the only nash equilibrium in Figure 8.3 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

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

Figure 8.3: 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. Maa ENDRES, FIKS NAVN IKKE FIRM, MEN NODE

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 case where they pay I_l without receiving any other benefit.

8.3 Solving the prisonersdilemma

One possibility for solving the problem that 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 order, and they can observe the other players action. If we consider a game with only two players, player one are the first to select an action. He chooses to insure or not. 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 first mover advantage, because he can now force the game in a direction he prefers.

$$I_l < \beta \text{ and } I_l > \beta - r \text{ and } r < \beta \tag{8.1}$$

By finding all subgame equilibria in Figure 8.4 except the last one, i.e. the subgame where player one chooses to Insure or not, we get this subgame equilibria: $(L, \overline{L_1^I}, \overline{L_1^{II}}, L_1^{III}), (I_2, \overline{I_2^I}, L_2 L_2^I, \overline{L_2^{II}}, L_2^{III})$ We have now analyzed the two different outcomes of player 1 choosing insure or not, thus he can now see what find his best response. The two options he can choose between are: Insure and get payoff $\beta - I_l$ or not insure and get payoff $\beta - r$. I.e. if $I_l < r$ player one will chose to insure, and thus forcing the game to end up in a equilibrium where both players insure and establish link. If the cost of insuring is higher than the expected risk cost r, then obviously there is no reason to choose insurance. From this we see that if the insurance price are set to the right amount, one 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.

[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. In 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.

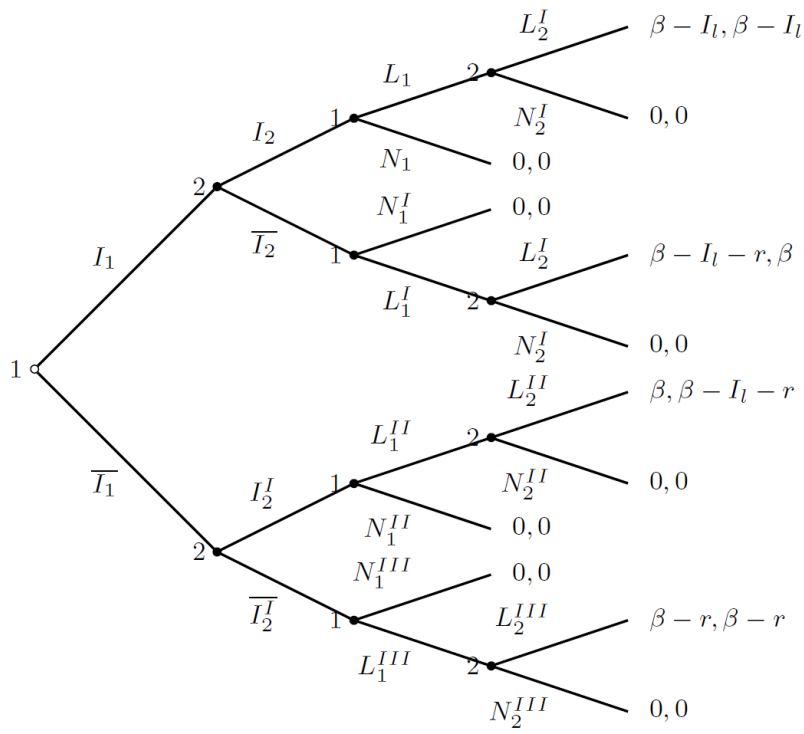


Figure 8.4: Leader follower game, first player 1 chooses to insure or not, then player 2, and then they choose to establish link or not in the same order.

8.3.1 Multiple nodes

Assumptions

In this model we introduce multiple nodes, the type of the node is as before given in advance. 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 software development networks, it is reasonable to assume that the parties can acquire this type of information regarding their transactional partners. For example by requiring proof of insurance prior to establishing a financial contract.

Analyzis

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. And thus we start by 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, only if both receive a higher payoff. In this scenario the the payoff function of adding a link is as shown in Eq.(8.2).

$$U_{i+1} = \begin{cases} \beta - I_l, & \text{if } i = 0 \\ U_i + \beta - I_l, & \text{if } i > 0 \end{cases} \tag{8.2}$$

For insured node to connect to another insured node, the condition shown in Eq.(8.3) has to hold.

$$I_l < \beta \tag{8.3}$$

Non-insured to insured The payoff a non-insured receives by connecting to a insured is as described in Eq. (8.4). As we see this will allways be a positive change in payoff, and thus an non-insured node will allways, if possible, want to connect to an insured node.

$$U_{i+1} = \begin{cases} \beta, & \text{if } i = 0 \\ U_i + \beta, & \text{if } i > 0 \end{cases} \tag{8.4}$$

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

$$U_{i+1} = \begin{cases} \beta - I_l - r, & \text{if } i = 0 \\ U_i + \beta - I_l - r, & \text{if } i > 0 \end{cases} \tag{8.5}$$

For this to happen Eq.(8.6) has to hold, a non-insured node will allways want to connect to a insured one, so this is the only condition that is needed for this to happen.

$$I_l + r < \beta \tag{8.6}$$

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

$$U_{i+1} = \begin{cases} \beta - r, & \text{if } i = 0 \\ U_i + \beta - r, & \text{if } i > 0 \end{cases} \tag{8.7}$$

And for this link-establishment scenario to happen Eq.(8.8 has to hold.

$$\beta > r \tag{8.8}$$

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.(8.3) 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:

$$I_l + r > \beta \tag{8.9}$$

This gives us the limitation shown in Eq. (8.10) on the insurance link cost.

$$\beta - r < I_l < \beta \tag{8.10}$$

As we see from the condition, if the link insurance cost is between the two boundaries all 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.

8.3.2 Result and findings

From the analyzis we found different conditions on the link establishment process. If Eq. (8.10) 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 versus 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 defintion of a nash equilibrium, that the resulting network is a 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. The total payoff can be calculated as in Eq. (8.11), where $\sum I \times I$

represents the sum of payoffs achieved from links between insured nodes. $\sum I \times \overline{I}$ the sum of payoffs achieved from links between non-insured and insured, and $\sum \overline{I} \times \overline{I}$, the sum of payfoss achieved from links between non-insured and non-insured nodes.

$$U_{total} = \sum I \times I + \sum \overline{I} \times \overline{I} + \sum I \times \overline{I} \tag{8.11}$$

When the parameters are inserted in Eq. (8.11), we get the Eq. (**??**), where N_I and $N_{\overline{I}}$, represents the number of insured and non-insured nodes in the network.

$$U_{total} = N_I(N_I - 1)(\beta - I_l) + N_{\overline{I}}(N_{\overline{I}} - 1)(\beta - r) + N_I N_{\overline{I}}(2\beta - r - I_l) \tag{8.12}$$

If we calculate the overall payoff for a network with one-clique of insured and another with non-insured, i.e. Eq. (8.10) has to hold and $r < \beta$. The total payoff is as shown in Eq. (8.13).

$$U_{total} = N_I(N_I - 1)(\beta - I_l) + N_{\overline{I}}(N_{\overline{I}} - 1)(\beta - r) \tag{8.13}$$

However, this is not the socially best outcome, because in this scenario, $2\beta > r + I_l$, will always be true. Thus the socially best outcome would have been one clique, with both insured and non-insured nodes. The price of stability is shown in Eq. (8.14).

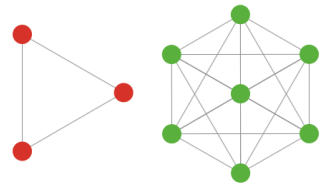
$$PoS = \frac{N_I(N_I - 1)(\beta - I_l) + N_{\overline{I}}(N_{\overline{I}} - 1)(\beta - r)}{N_I(N_I - 1)(\beta - I_l) + N_{\overline{I}}(N_{\overline{I}} - 1)(\beta - r) + N_I N_{\overline{I}}(2\beta - r - I_l)} \tag{8.14}$$

From this we see that the only scenario where the insurer are able to seperate the two types of nodes, and have 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 the result of this network formation game with multiple nodes, we performed different simulations. The network formation is performed by selecting two random nodes, not neighbouring 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, by asking them.

(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

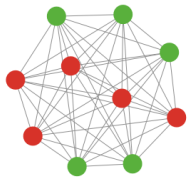
Figure 8.5: The figure shows the resulting network from a simulation with parameters: $\beta = 0.9$, $I_l = r = 0.5$.

In Figure 8.5 we see the result of a simulation with the parameters: $\beta = 0.9$, $I_l = r = 0.5$. With these parameters the Eq.(8.10) 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 8.5b, and confirms our calculations. In this figure there are only included $n = 10$ nodes, this is done to make the figure readable and easy to understand. The same results where obtained when performing the simulation with larger values of n, however the resulting printouts was very complex and chaotic.

In the next simulations, the parameters where chosen to violate the Eq.(8.10). The result can be seen in Figure 8.6. In figure 8.6a we see the result when $I_l < \beta - r$, the result is one clique of both insured and non-insured nodes. In figure 8.6b the insurance cost is $I_l > \beta$, and as we see only non-insured nodes connect to each other, because the insurance cost per link cost more than the benefit given from connecting to a new node, i.e. the insured ones choose not to establish any connections.

8.4 Forcing non-insured nodes to buy insurance(FIX!!!!!!!!)

In this section we try to find a condition which gives all nodes incentive to buy insurance. The basic idea is to create a scenario where it is beneficial for a node to be insured, i.e the non-insured nodes wants to to purchase insurance. This scenario will also benefit the insurer, obviously because more nodes purchases insurance. In addition, the insurer now have incentive to handle the problem with asymmetry. In previous models, the insurer would have difficulty obtaining sufficient information to calculate a node's risk. Because the nodes would did not have incentive to provide information to the insurance company. Hence the insurance company could enter



(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.(8.10), 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 8.6: The figure shows the two possible scenarios that violates the Eq.(8.10), 8.6a shows the result when $I_l < \beta - r$ and 8.6b shows the result when $I_l > \beta$.

into risky contracts. Now, we have a different scenario. Since non-insured nodes want to be insured, they can be forced to give up information about their current condition, both financial and list possible risks. From the market survey, we found that companies offering cyber-insurance actually required this information. The information received can be analyzed in different ways. If the nodes provide enough information, the insurer are able to calculate the risk, and offer a premium. On the other hand, if a node acts suspiciously and tries to hide information from the insurer, the insurer have reasonable cause to not chose to insure the node. Either way, it is a seller's market, where the insurance company can dictate the outcome of the network by pricing the insurance according to equations provided in this section.

Initial conditions are equal to the previous, where every node are randomly chosen to be either insured or not. Hence we could use the same payoff matrix as shown in Figure 8.3 to analyze how we could force the non-insured nodes to purchase insurance. In order to give incentive for a non-insured node to purchase insurance, the payoff has to always be higher, i.e.

$$\textit{Utility insured node} > \textit{Utility non-insured node} \tag{8.15}$$

This means that we need to make sure that a non-insured node in any circumstances will benefit from purchasing insurance. From the payoff matrix, Figure 8.3 we find the different conditions. When a connection is established, we need the payoff for insured nodes to be higher than non-insured nodes:

$$\begin{aligned} & \beta - I_0 - I_l > \beta - r \\ \rightarrow \quad & I_0 + I_l < r \end{aligned} \tag{8.16}$$

For the other case, when the nodes have not established any connections the following has to hold:

$$\begin{aligned} & -I_0 > -r \\ \rightarrow \quad & I_0 < r \end{aligned} \tag{8.17}$$

In addition we need to make sure that it is not beneficial for insured nodes to connect to non-insured nodes:

$$I_l + r < \beta \tag{8.18}$$

If these conditions are met, we are guaranteed to get a network consisting of only insured nodes. Because in any case, the non-insured nodes will get a higher payoff from purchasing insurance. It is interesting to see that both conditions are completely dependent upon how the insurance company chooses to price their products. If the insurer collects enough information to calculate an accurate risk, he could price both I_0 and I_l to meet the conditions. Hence he forces the network to end up with every node having incentive to purchase insurance.

8.4.1 Violating the conditions

Since the risk are difficult to calculate, there is a possibility of ending up in states where a node would actually benefit from doing the opposite. If the actual scenario ends up with the following conditions:

$$\begin{aligned} I_0 &< r \\ I_l &> r \end{aligned} \tag{8.19}$$

Now we will have a situation where it first looks beneficial to be purchase insurance. However, as the nodes adds more connections, and pays I_l pr connection, the node would actually be better of with not being insured. This demonstrates the importance of being able to accurately calculate the risk.

8.5 Model 3 - Including maximum node degree and bonus

In real world networks, such as in software development, consultant firms and many other types of business, a goal can not be completed without outsourcing some of the task needed for reaching the goal. This could be because the firm lack knowledge, the task can only be performed by specialists etc. 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 a bonus γ, which represents the payoff when a node reach their desired number off established connections, i.e. their maximum node degree(m). Except from this the game is as before.

8.5.1 Analyzis

This model is very similar to the earlier model, for nodes to connect to each other, the change in payoff 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($\frac{\gamma}{m-i}$), every time a node is considering a link establishment. 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 the already established connections.

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

Insured to insured When establishing a link between two insured nodes, the payoff the nodes will receive is as described in Eq. (8.20).

$$U_{i+1} = \begin{cases} \alpha + \beta - I_0 - I_l, & \text{if } i = 0 \\ U_i + \beta - I_l, & \text{if } i > 0 \\ U_i + \beta - I_l + \gamma, & \text{if } i = m \end{cases} \tag{8.20}$$

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. (8.21) has to hold.

$$\begin{aligned} U_i + \beta - I_l + \frac{\gamma}{m-i} &> U_i \\ \beta - I_l + \frac{\gamma}{m-i} &> 0 \\ \rightarrow \quad \beta + \frac{\gamma}{m-i} &> I_l \end{aligned} \tag{8.21}$$

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

$$U_{i+1} = \begin{cases} \alpha + \beta - I_0 - I_l - r, & \text{if } i = 0 \\ U_i + \beta - I_l - r, & \text{if } i > 0 \\ U_i + \beta - I_l - r + \gamma, & \text{if } i = m \end{cases} \tag{8.22}$$

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

$$\begin{aligned} U_i + \beta - I_l - r + \frac{\gamma}{m-i} &> U_i \\ \beta - I_l - r + \frac{\gamma}{m-i} &> 0 \\ \rightarrow \quad \beta + \frac{\gamma}{m-i} - r &> I_l \end{aligned} \tag{8.23}$$

Non-insured to non-insured When a non-insured node connect to another not-insured node this is the payoff they receive:

$$U_{i+1} = \begin{cases} \alpha + \beta - r, & \text{if } i = 0 \\ U_i + \beta - r, & \text{if } i > 0 \\ U_i + \beta - r + \gamma, & \text{if } i = m \end{cases} \tag{8.24}$$

To establish the connection the following equation has to hold:

$$\begin{aligned} U_i + \beta - r + \frac{\gamma}{m-i} &> U_i \\ \beta - r + \frac{\gamma}{m-i} &> 0 \\ \rightarrow \quad \beta + \frac{\gamma}{m-i} &> r \end{aligned} \tag{8.25}$$

Non-insured to insured

$$U_{i+1} = \begin{cases} \alpha + \beta, & \text{if } i = 0 \\ U_i + \beta, & \text{if } i > 0 \\ U_i + \beta + \gamma, & \text{if } i = m \end{cases} \tag{8.26}$$

As we see, this is a strictly increasing function, and thus a non-insured will always connect to an insured node if possible.

8.5.2 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 establishes connections to non-insured nodes. We know that an insured node would want to connect to another insured node if Eq.(8.21) is satisfied. In the equation we see that the expected bonus per established link is increasing, i.e. if an insured node of degree zero is willing to connect to another insured node, then every 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:

$$\beta + \frac{\gamma}{m} > I_l \tag{8.27}$$

We also want to ensure that insured nodes never establishes links with non-insured nodes, from 8.22 we see that this has to hold:

$$\beta + \frac{\gamma}{m - i} - r < I_l \tag{8.28}$$

This can be simplified, if 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 link with non-insured nodes. From this we get the equation Eq. (8.29).

$$\begin{aligned} \beta + \frac{\gamma}{m - (m-1)} - r &< I_l \\ \rightarrow \qquad \beta + \gamma - r &< I_l \end{aligned} \tag{8.29}$$

To summarize, Eq.(8.27) and Eq.(8.29) gives the final limitation on the link insurance cost, Eq. (8.30). If this equation is satisfied the resulting network will contain a clique of only insured nodes.

$$\beta + \gamma - r < I_l < \beta + \frac{\gamma}{m} \tag{8.30}$$

For this to even be possible $\beta + \gamma - r < \beta + \frac{\gamma}{m}$, i.e. Eq. (8.32) 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. And when the risk to bonus ratio is less than $1-\frac{1}{m}$, such a clique will never occur. If we think about a real world scenario where you get a bonus for establishing a fixed number of equations, you would be more willing to take a risk if the possible reward of doing so is large, this is what this equation express. It is also useful to know when non-insured nodes connect to each other, this happens when Eq. (8.24) 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 wait for one or more insured node who are willing to establish links with non-insured nodes. With these findings, an insurer can easily determine the outcome of the network formation game, by adjusting the insurance cost parameter. If he want a clique of only insured nodes Eq. (8.30) has to hold. However, it is easy to relax the condition, such that a insured node only connect to, $j = 1, 2, 3..m$ nodes, this is done by changing Eq. (8.29) to $\beta + \frac{\gamma}{m-(m-j)} - r < I_l$, which gives us Eq. (8.31). 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 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. Hence the node might end up not reaching the desired goal. This can happen if there is not enough nodes willing to establish links. If the bonus to risk ratio is very high, or nodes need lots of links, then this is a likely scenario. And nodes who do not reach their goal can end up with a payoff less than U_0.

$$\beta + \frac{\gamma}{j} - r < I_l \tag{8.31}$$

$$\begin{aligned} & \gamma - r && < \tfrac{\gamma}{m} \\ & 1 - \frac{r}{\gamma} && < \tfrac{1}{m} \\ \rightarrow \quad & 1 - \frac{1}{m} && < \tfrac{r}{\gamma} \end{aligned} \tag{8.32}$$

Efficiency and Stability(SKRIVE NOE OM DETTE, selvom det er vanskelig å analysere In this model, the incentive for establishing links has been increased. And thus to maintain a stable network with two cliques, the cost of link establishment has to be increased, compared to model 2. This increased incentive may result in a higher price of stability.

Simulation of the results

In our first simulation we have set the variables such that Eq.(8.30) are satisfied. The parameters are set to the following: $\beta = 0.9, I_l = 0.7, r = 0.5, \gamma = 0.2$ and $m = 5$.

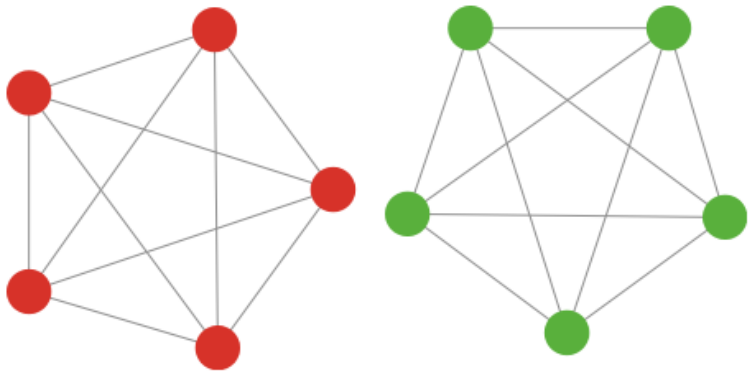


Figure 8.7: Two cliques, one consisting of insured agents the other consists of non-insured. All nodes have reached their goal.

As we see in Figure 8.7 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.

If we change the link insurance cost to the same value as in model 2, $I_l = 0.5$, the result is as depicted in Figure 8.8. Here we see that allmost every insured node has taken the risk of connecting to a non-insured node in order to achieve their goal. By inserting the numbers in to Eq. (8.31) we see that the insured nodes are willing to connect to up to two non-insured nodes to reach their goal.

8.6 Model 4 - Including bulk insurance discount

Putte det som starter her i background? 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].

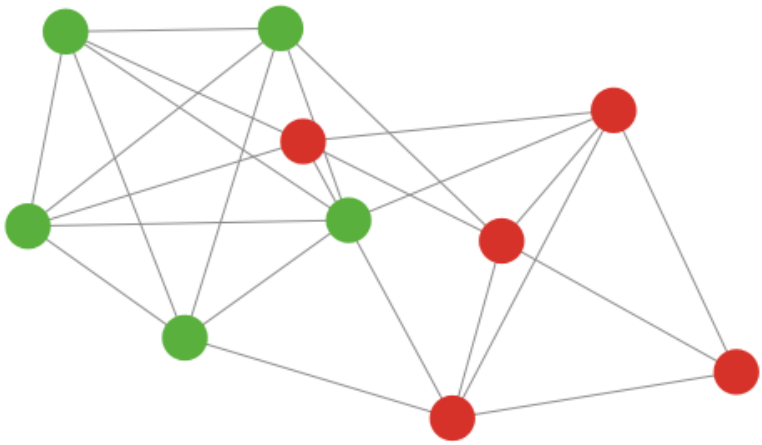


Figure 8.8: Simulation when the cost of insuring a link is just below the limits.

- 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. **til hit!!**

So far our model reflects that a company have to insure each of the links to other nodes, inspired by other insurance products, we would like to introduce a discount rate following the degree of the nodes. 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 good 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(REFERER TIL CHAPTER BACKGROUND), or let the discount follow a power law. However, we choose to follow a discount rule which directly reflects the number of links the node has established.

8.6.1 Analyzis

The price for adding a new link follows the equation:

$$\frac{I_l}{i+1} \tag{8.33}$$

Here, i is the current number of established connections. This means that the more connections a node acquire the cheaper the links will be.

Discount model

We start our analyzis by considering a model where only the discount are included, not the bonus, and 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.

Insured to insured When we add the discount to the conditions found in model 2 we find the condition shown in Eq. (8.34).

$$\frac{I_l}{i+1} < \beta \tag{8.34}$$

Insured to non-insured For this scenario to be possible Eq. (8.35) has to hold.

$$\frac{I_l}{i+1} + r < \beta \tag{8.35}$$

Result and findings For a 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 does not connect to non-insured, thus we get the final condition in Eq. (8.36), where N_I is the number of insured nodes in the network.

$$(N_I - 1)(\beta - r) < I_l < \beta \tag{8.36}$$

This is condition is very strong, because it says that $\beta - r < \frac{1}{N_I - 1}$, 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.

Price of Stability versus efficiency If we compare the total payoff equation in this model, see Eq. (8.37), with the one in model 2(Eq. (8.12)). We see that what has changed is the cost for insured nodes, and thus the payoff generated from

links between insured nodes has increased, and so have the payoff received from 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: $(N_I N_{\overline{I}}\beta + N_I(-\sum_{i=N_I}^{N_{\overline{I}}-1} \frac{I_l}{i}))$, and as long as $(N_I N_{\overline{I}}\beta > N_I(-\sum_{i=N_I}^{N_{\overline{I}}-1} \frac{I_l}{i}))$ 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 stability will increase compared to the price of stability 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.

$$U_{total} = (N_I(N_I-1)\beta - N_I \sum_{i=1}^{N_I-1} \frac{I_l}{i}) + (N_{\overline{I}}(N_{\overline{I}}-1)(\beta - r)) + (N_I N_{\overline{I}}\beta + N_I(-\sum_{i=N_I}^{N_{\overline{I}}-1} \frac{I_l}{i})) \tag{8.37}$$

Discount and Bonus model

We also need to apply the discount to the model where the bonus is included, and we start out 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.

Insured to insured If we add the new rule to the Eq.(8.20) which shows the connection between two insured nodes, we get the following equations:

$$U_{i+1} = \begin{cases} \beta - I_l, & \text{if } i = 0 \\ U_i + \beta - \frac{I_l}{i+1}, & \text{if } i > 0 \\ U_i + \beta - \frac{I_l}{i+1} + \gamma, & \text{if } i = m \end{cases} \tag{8.38}$$

For insured to connect to each other Eq. (8.39) has to hold.

$$\begin{aligned} U_i + \beta - \frac{I_l}{i+1} + \frac{\gamma}{m-i} &> U_i \\ \beta - \frac{I_l}{i+1} + \frac{\gamma}{m-i} &> 0 \\ \rightarrow \quad \beta + \frac{\gamma}{m-i} &> \frac{I_l}{i+1} \end{aligned} \tag{8.39}$$

insured to non-insured When insured are considering connecting to non-insured, they payoff they will receive are shown in Eq. (8.40).

$$U_{i+1} = \begin{cases} \beta - I_l - r, & \text{if } i = 0 \\ U_i + \beta - \frac{I_l}{i+1} - r, & \text{if } i > 0 \\ U_i + \beta - \frac{I_l}{i+1} - r + \gamma, & \text{if } i = m \end{cases} \tag{8.40}$$

For this scenario to be able to happen Eq. (8.41) has to hold.

$$\begin{aligned} U_i + \beta - \frac{I_l}{i+1} + \frac{\gamma}{m-i} - r \quad &> U_i \\ \rightarrow \qquad \beta + \frac{\gamma}{m-i} \quad &> r + \tfrac{I_l}{i+1} \end{aligned} \tag{8.41}$$

8.6.2 Result and findings

If we analyze the same scenario as in the other models, a clique of only insured nodes. The first step is to ensure that insured nodes connect to each other when the expected payoff is lowest, 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. (**??**) from model 3 holds, insured nodes will connect to other insured nodes.

But the condition for ensuring that insured 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 do so either. From this we find the condition, see Eq. (8.42)

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

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. (8.42).

$$m(\beta + \gamma - r) < I_l < \beta + \frac{\gamma}{m} \tag{8.42}$$

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 seperate insured and non-insured nodes.

8.7 Model with incomplete information

An interesting scenario to model is when the nodes are missing some 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. What we want to find is if it possible for the nodes with incomplete information to distinguish a insured node from a non-insured one.

8.7.1 Analyzis

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

Node 2 is insured Since every node knows their own type, 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.

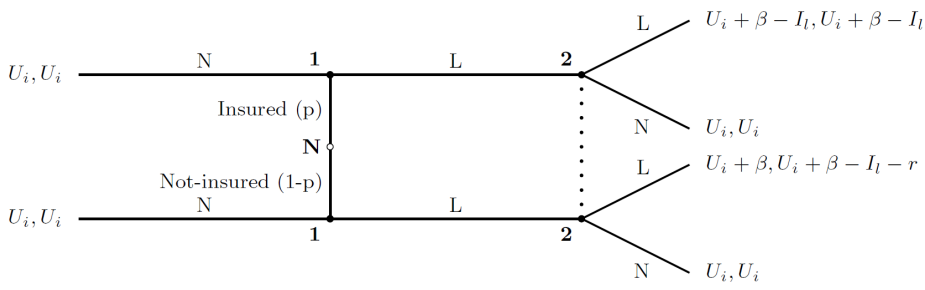


Figure 8.9: Signalling game with two nodes, node 1's type choosen by nature, node 2 is insured. node 1 have complete information, node 2 suffer from incomplete information, and act on best response functions based on beliefs.

In the extensive-form shown in Figure 8.9, 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.(8.43).

$$\sigma_1(t_i) = \begin{cases} N, & \text{if } t1 \\ L, & \text{if } t2 \end{cases} \tag{8.43}$$

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

$$\mu_1(t_1|N) = \frac{P(N|t_1)P(t_1)}{P(N)} = \frac{P(N|t_1)P(t_1)}{P(N|t_1)P(t_1) + P(N|t_2)P(t_2)} \tag{8.44}$$

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

$$\begin{aligned} EU_2(L,L) &= \mu_1(t_1|L)U_2(L,L;t_1) + \mu_1(t_2|L)U_2(L,L;t_2) \\ &\rightarrow \qquad EU_2(L,L) = U_i + \beta - I_l - r \qquad (8.45) \\ EU_2(N,L) &= \mu_1(t_1|L)U_2(N,L;t_1) + \mu_1(t_2|L)U_2(N,L;t_2) \\ &\rightarrow \qquad EU_2(N,L) = U_i \qquad (8.46) \end{aligned}$$

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:

$$BR_2(L) = \begin{cases} L, & \text{if } \beta - r \geq I_l \\ N, & \text{if } \beta - r < I_l \end{cases} \tag{8.47}$$

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. For node 1 to be willing to play N when he knows node 2's best response function, this 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:

$$\beta < I_l \tag{8.48}$$

$$\sigma_1 = \begin{cases} N, & \text{if } t1 \\ L, & \text{if } t2 \end{cases} \tag{8.49}$$

$$BR_2(\sigma_1) = N \tag{8.50}$$

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.

$$\sigma_1(t_i) = \begin{cases} L, & \text{if } t1 \\ L, & \text{if } t2 \end{cases} \tag{8.51}$$

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:

$$\begin{aligned} EU_2(L, L) &= p(U_i + \beta - I_l) + (1 - p)(U_i + \beta - I_l - r) \\ \rightarrow \quad EU_2(L, L) &= U_i + \beta - I_l - r + pr \qquad (8.52) \\ EU_2(N, L) &= U_i \qquad (8.53) \end{aligned}$$

From this we get node2's best response:

$$BR_2(L) = \begin{cases} L, & \text{if } \beta + rp - r \geq I_l \\ N, & \text{if } \beta + rp - r < I_l \end{cases} \tag{8.54}$$

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 node 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.

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.(8.55).

$$\sigma_1(t_i) = \begin{cases} L, & \text{if } t1 \\ N, & \text{if } t2 \end{cases} \tag{8.55}$$

With the beliefs in Eq.(8.55), this is node 2's expected payoffs:

$$EU_2(L, L) = (U_i + \beta) \tag{8.56}$$

$$EU_2(N, L) = (U_i) \tag{8.57}$$

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

$$BR_2(L) = L \tag{8.58}$$

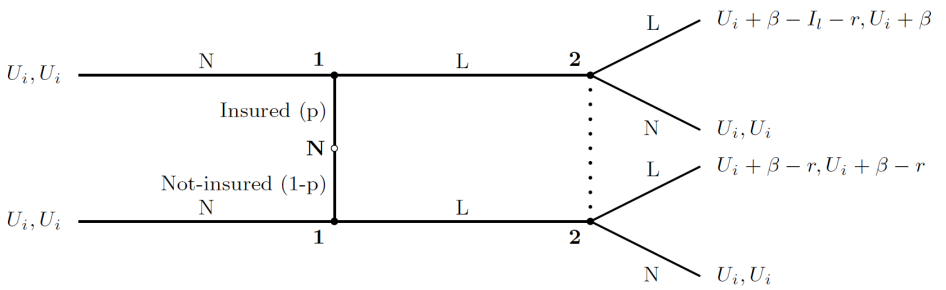


Figure 8.10: Signalling game with two nodes, node 1's type choosen by nature, node2 is not insured. Node 1 have complete information, node 2 suffer from incomplete information, and act on best response functions based on beliefs.

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.(8.55). So we know that for this to be an equilibrium,

$$\beta < r \tag{8.59}$$

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.(8.59) is violating this condition, and thus we have no separating equilibrium with the beliefs in Eq.(8.55). Now lets look at the other possible separating equilibrium, see Eq.(8.60).

$$\sigma_1(t_i) = \begin{cases} N, & \text{if } t1 \\ L, & \text{if } t2 \end{cases} \tag{8.60}$$

Node 2's expected payoffs are as follows:

$$EU_2(L, L) = U_i + \beta - r \tag{8.61}$$

$$EU_2(N, L) = U_i \tag{8.62}$$

From this we get the best response function:

$$BR_2(L) = \begin{cases} L, & \text{if } \beta \geq r \\ N, & \text{if } \beta < r \end{cases} \tag{8.63}$$

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. And for this to happen we get this condition on β.

$$I_l + r > \beta > r \tag{8.64}$$

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.

$$\sigma_1(t_i) = \begin{cases} L, & \text{if } t1 \\ L, & \text{if } t2 \end{cases} \tag{8.65}$$

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

$$EU_2(L) = p(U_i + \beta) + (1-p)(U_i + \beta - r)$$

$$EU_2(L) = U_i + \beta - r + pr \tag{8.66}$$

$$EU_2(N) = U_i \tag{8.67}$$

From this we get the best response function :

$$BR_2(L) = \begin{cases} L, & \text{if } \beta \geq r - pr \\ N, & \text{if } \beta < r - pr \end{cases} \tag{8.68}$$

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 only found 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. And 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 seperate 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, and this is beneficial for both. 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.

8.8 Model 5-The connection game

In the earlier model, the experienced network effects only arose from their neighbours. I.e. when a node established a connection the change in utility where only dependent on fixed variables, and non dependent of the rest of the network. In some real world scenarios there is more realistic that a node will be strongly affected by the indirect connections to other nodes as well, social connection networks are good examples of such networks.

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: $0 < \beta < 1$.

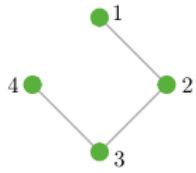


Figure 8.11: Four nodes interconnected with each other.

Example Lets consider the network shown in 8.11. 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:

$$\sum_{j \neq i} \beta_{ij}^{d(ij)} - \sum_{j:ij \in g} c_{ij}, \tag{8.69}$$

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 two different networks outcomes, one with the focus on efficiency and the other on pairwise stability. An efficient network means ending up with a network where the sum of every nodes payoff is maximized. The optimal network is of course both efficient and stable, but as we shall see there are some conflicts between efficiency and stability. In the paper they found 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 created in the intermediate cost of insuring links, and ends up in 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. Indisputable this structure provides the highest overall payoff for the network, but this network is not necessarily stable, as we will show later on.

Pairwise stability:(HVERTFALL ISH) A graph is pairwise stable if:

1. *No node wishes to delete a link he is involved in.*
2. *If there exists a node who want to add a link, then the node on the other end of the link do not want to establish this link.*

The limitations of pairwise stability is that we only consider one link and one pair of nodes at a time.

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 thus be 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 connection. 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.

8.9 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 one are able to determine the variables one can actually determine the network structure. From the papers we know that there exists different boundaries on the cost of establishing a new link, and how the resulting stable and efficient network will be. From our earlier models we know that the cost of establish a link is the insurance cost and 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. And of course 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.

One important thing to notice is that even if 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 in this game we only consider a link at a time, and not the whole network.

8.9.1 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 greatly simplify an otherwise very complex model, and because what we are analyzing is the resulting network structure, this 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 8.12.

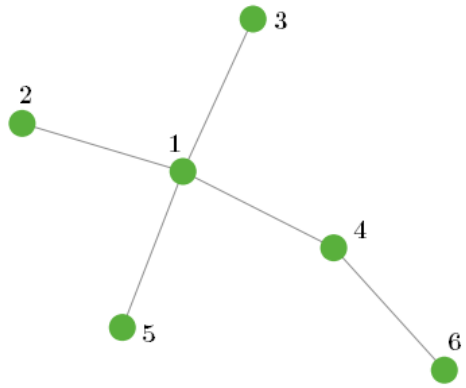


Figure 8.12: The resulting network after a simulation with the parameters $\beta = 0.9, I_l = 0.5$.

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.(8.73).

$$U_1 = 4\beta + \beta^2 - 4c \tag{8.70}$$
$$U_2 = U_3 = U_5 = \beta + 3\beta^2 + \beta^3 - c \tag{8.71}$$
$$U_4 = 2\beta + 3\beta^2 - 2c \tag{8.72}$$
$$U_6 = \beta + \beta^2 + 3\beta^3 - c \tag{8.73}$$

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.

Star not possible with high n In the paper [Jac05] they come up with this 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 0. 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 rarely was a star.

However, the structure of the networks 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 8.13, 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.

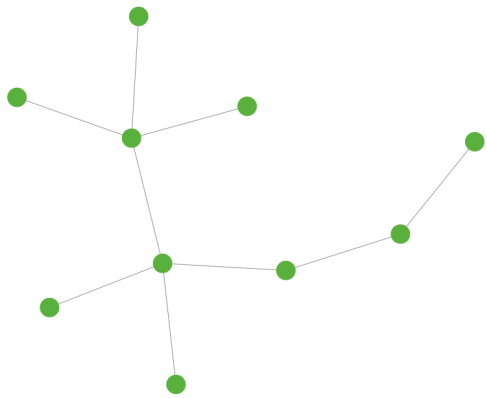


Figure 8.13: The resulting network after a simulation with the parameters from table **??** and ten nodes.

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 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.(8.74) to achieve a efficient and stable star topology. i represents the node degree.

$$\beta - \beta^2 < \frac{i_l}{i+1} < \beta \tag{8.74}$$

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, see Eq.(8.75).

$$\frac{I_l}{g} < \beta - \beta^2 \tag{8.75}$$

For this to be possible $g < n$, 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 nodes 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.(8.76). γ is the power law parameter, as described in Chapter 3.

$$P(g) = g^{-\gamma} \tag{8.76}$$

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

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 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.

Conjecture 2. If the probability that there exists a node with critical degree, is such that only a few nodes will reach this degree, then the resulting network will be a star-topology or other similar network structures.

8.9.2 Simulation

To see if the conjectures above where true, we created a simulator. 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. If the link is added, we check if either of the nodes would

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

prefer to delete some of their already existing links, this decision is asymmetric. This procedure is repeated as long as there are possible to add new links. The payoff function of each node is as described earlier(see Eq.(8.69)), except that the cost is now dependent on the degree of the node. We know that if Eq.(8.74) is satisfied for all i, then the efficient and stable state is a star. But whats of interest is when some nodes reaches the critical degree.

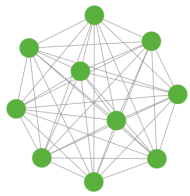
For the simulations to be realizable, we had to set the number of nodes to 20, or else the computational time was to high. For every critical degree, from three to nineteen, we ran 50 simulations, and noted the resulting network formation. The results can be seen in XXXX. And as we see from the figure, 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 the simulations we also observed that as the critical degree is increased, the probability of the resulting network being a clique, drastically decreases. From degree seven and up, the network ended up being a scale-free or some variant of a star, with 99 % probability.

Low critical node degree, KANSKJE FJERNE DETTE HER OG neste subpara To explain why a network where the critical node degree is set to a low degree, ends up in a clique, lets consider the variables and their values shown in (table 8.1), $n-$ is the number of nodes. We see that Eq.(8.74) is satisfied until a node is considering establish its third direct link. At this point the node has reached the critical degree, and will strictly prefer to establish direct links. This will lead to even more nodes reaching the critical degree level, and the result is that almost every node connects to every one else. Two of the resulting simulating networks with these parameters can be seen in Figure 8.14. As we can see from the parameters in table 8.1, the critical degree is reached when a node gets a degree of two. From degree two and up, $c < \beta - \beta^2$. The expected number of nodes with degree of two are $E(g = 2) = 10 * 2^{-2} = 2.5$. This is when we assume that the network follow a power-law with $\gamma = 2$.

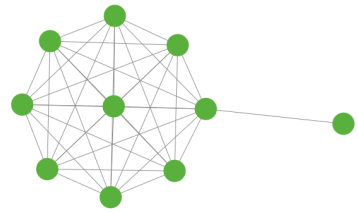
$n = 10, \beta = 0.7, \beta - \beta^2 = 0.21, I_l = 0.6$

Table 8.1: The parameters used in the simulation in 8.12

High critical node degree To ensure that the network will form a star, we have to find parameters such that, Eq.(8.74) is satisfied, and the probability of a node having a critical degree has to be relative low. In a network with ten nodes, the expected number of nodes with degree five in a network with ten nodes, is



(a) A clique consisting of ten nodes.



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

Figure 8.14: Two different outcomes of the simulations with parameters from table 8.1.

$E(g = 5) = 10 * 5^{-2} = 0.4$. With the parameters from table 8.2, these conditions are satisfied and the resulting network can be seen in Figure 8.15a.

$n = 10, \beta = 0.8, \beta - \beta^2 = 0.16, I_l = 0.7$

Table 8.2: The parameters used in the simulation in 8.15a

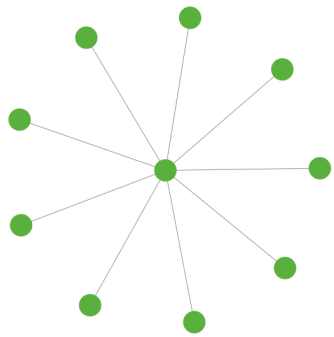
Another possibility for solving the problem with unfair costs, could be to use a shared-network cost instead. i.e. every node pays a cost equal to the total cost of the network divided on the number of nodes. Similar value distribution has been analyzed by Jackson and Wolinsky in [JW96], and is called an egalitarian allocation rule, this rule guarantees that any efficient network is also pairwise stable. But this is unfortunately a very extreme rule.

.....FROM HERE, it's only notes.....

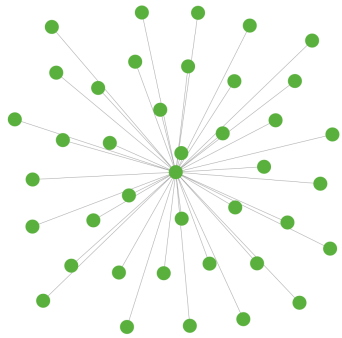
8.10 DETTE ET ANNET STED KANSKJE? BLIR LITT RART Å HOPPE INN I DET HER

By adjusting the parameter one can assure that only insured agents connects to other insured agents, and the opposite, that only uninsured agents connects to each other. Hence as we can see from the Figure 8.16 clustered networks of insured agents (red) are created, and as the paper [Blu11] showed, these clustered trusted networks, can achieve higher, super-critical, payoff by increasing their node degree past the critical point.

, because the nodes can thus receive a super-critical payoff, and they are also insured against contagious risk.



(a) The result of simulating with the parameters in table 8.2, a star with ten nodes



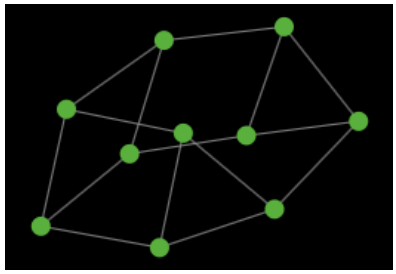
(b) A star network formed when running a simulation with forty-nodes, and parameters satisfying proposition 2

Figure 8.15: Two star-network, ten- and forty-nodes, both are the result of simulations with parameters satisfying proposition 2.

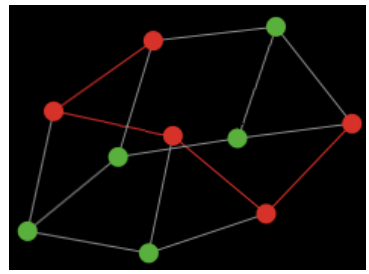
Figure 8.17 presents the individual payoffs in a formation game between two agents in the described model. It is assumed that both agents has to have a desire to establish a connection in order to create a link between them. This is reasonable since a company would not prefer to enter into an agreement with negative expected payoff. As in this case would be the result when an insured agent is requested a connection with someone without insurance.

If we give value to the variables in Figure 8.17 one can observe the model's different equilibrium's. It is difficult to know exactly how the variables are set and this would vary considerably between different markets. In a real worlds scenario the variables would also be different for each agent. However in Figure 8.18 we decided to set a fixed value (which is assumed to be corresponding to the real values) for each

[3] A link will only be created if both agents wishes to establish a connection.



(a) Initial graph with 10 agents.



(b) Insured agents (red) forms a network

Figure 8.16: shows how insured agents connects with each other to form a network to achieve super-critical payoffs.

		Firm B			
		IL	$I\overline{L}$	$\overline{I}L$	$\overline{IL}$
Firm A	IL	$\alpha+\beta-I_o-Il$ $\alpha+\beta-I_o-Il$	$\alpha-I_o$ $\alpha-I_o$	$\alpha+\beta-I_o-Il-r*q$ $\alpha+\beta-r*q$	$\alpha-I_o$ $\alpha-r*q$
	$I\overline{L}$	$\alpha-I_o$ $\alpha-I_o$	$\alpha-I_o$ $\alpha-I_o$	$\alpha-I_o$ $\alpha-r*q$	$\alpha-I_o$ $\alpha-r*q$
	$\overline{I}L$	$\alpha+\beta-r*q$ $\alpha+\beta-I_o-Il-r*q$	$\alpha-r*q$ $\alpha-I_o$	$\alpha+\beta-2*r*q$ $\alpha+\beta-2*r*q$	$\alpha-r*q$ $\alpha-r*q$
	$\overline{IL}$	$\alpha-r*q$ $\alpha-I_o$	$\alpha-r*q$ $\alpha-I_o$	$\alpha-r*q$ $\alpha-r*q$	$\alpha-r*q$ $\alpha-r*q$

Figure 8.17: Normal form game between two agents individually choosing to purchase insurance and express desire to connect to the other [3]

variable in order to show a concept of how cyber-insurance can be used to create beneficial payoffs. The following values where used: $\alpha = 10$, $\beta = 10$, $I_o = 5$, $I_l = 2$, $r = 20$, $q = 0.5$.

		Agent B			
		IL	$I\overline{L}$	$\overline{I}L$	$\overline{IL}$
Agent A	IL	12 ,12	5,5	4,12	5,2
	$I\overline{L}$	5,5	5,5	5, 2	5,2
	$\overline{I}L$	12,4	2,5	4,4	2,2
	$\overline{IL}$	2,5	2,5	2,2	2,2

Figure 8.18: Shows equilibrium's in the resulting payoff matrix.

From the payoff matrix 8.18 we observe two different Nash equilibrium's: One when both agents are insured and wants to connect to the other agent, and one when both are insured but does not want to establish a connection. These are the possible outcomes between the two agents, however as we can see it the social optimal solution would be for two insured agents to connect with each other, i.e they would both receive a significantly higher payoff. This demonstrates that a cluster of insured nodes would achieve higher payoffs.

Chapter 9
Summary of results/conclusion

Model-1: Showed a very simple and naive way for the insurer to separate between insured and non-insured nodes.

Model-2: Made model-1 realizable, by including parameters and making it apply for multiple nodes. 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. We also showed that when the insurer sets the cost such that the network ends up in two cliques, then this has a cost compared to the most efficient network. The cost of stability, this is because in overall the network will suffer from the lost benefits of connections between insured and non-insured nodes.

Model-3: In this model we tried to apply 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 parts. This was done by including a bonus, which where received when you reached the desired number of links(called max-degree). This made the separation process of insured and non-insured nodes, more difficult for the insurer. Because the nodes now have more incentive to establish links, and are thus more acceptable towards risk. We found the conditions for the different network structures to evolve, and showed that these where very strongly dependent on the max-degree. And when the max-degree increases, it gets harder and harder to guarantee two separate cliques.

Model-4: In this model we tried to make the model more comparable to other insurance products, by including a bulk-discount. We did this on both model 2 and 3. This resulted in even more incentive, or less disincentive, for insured node to establish links with non-insured nodes, since the cost of doing so decreases linearly with the nodes degree. We found the different conditions for when the different networks would evolved, and showed that when applying the discount to model 3, it is very

hard for the insurer to ensure two seperate cliques. 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 the potential payoff that are missing, when we have two separate cliques, are increasing.

Model-5: In this model we used the findings from a well know game called the symmetric connection game, and applied these to our scenario with insurance. Since the game is well known in network formation research, this game have allready been analyzed thoroughly, some of these findings are very interesting. They show how a star, under cost-conditions, is the most efficient, and can also be stable. But they also show that as the number of nodes increases, the probability of reaching a star approaches zero. By applying our insurance discount to this model, we found a conjecture that says, by setting the cost to the right level, one can most certainly ensure that a star will evolve.

9.1 Game including max node degree

FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF So far the model describes a scenario where the goal is to get all the insured nodes to connect with each other. As we have seen this creates a strong trusted environment for the insured nodes when the parameters are adjusted to certain values. However, in many scenarios the goal might not be to be connected to everyone. Sometimes a company wishes to reach a specific number of connections in order to receive a significant profit, which is denoted γ. Such scenario might create incentives for insured nodes to connect with non-insured, in order to reach the desired number of connections. As an example consider a software company wanting to implement a new software program, however they do not have the capacity or resources to do it alone. Their goal is to establish enough partnerships to be able to create the new program. In this game we might end up in a situation where insured agents are willing to connect with non-insured, to reach the desired number of partners. Table 9.1 summarizes the added parameters.

m - an agents desired number of connections
n - an agents number of established connections L_i - connections with insured agents
L_{ni} - connections with non-insured agents
γ - an agents profit from reaching m

Table 9.1: Table showing the parameters added to the model

Building on the already existing model this model adds the property of a significant bonus γ if a desired number of links m are established. From here we can describe two different models, one where the insured agent first tries to connect with other insured agents, however if there are not enough insured agents it will try to establish connections with non-insured agents. The other model shows a game where the insured agent is less strict on whether the other node is insured or not. The insured agent makes a decision with regards to the Eq.(9.2). Here $\frac{\gamma}{L_{ni}}$ will increase as more connections are established. I.e. the more established connections the higher probability for the insured agent to connect to a non-insured agent.

9.1.1 Game random connection

As described we now have possibility that insured and non-insured agents will establish a connection. This means that γ has to be reflected in the equation relating to whether nodes, insured or not will connect. To simplify the scenario we assume that each new connection contribute with an extra $\frac{\gamma}{m-\#l}$, which reflects an expectation of reaching m connections, hence we end up with the following equations for the new game:

Insured connects to insured:

$$U_{i+1} = U_i - I_l + \beta + \frac{\gamma}{m - \#l} \tag{9.1}$$

Insured connects to not insured

$$U_{i+1} = U_i - I_l - r + \beta + \frac{\gamma}{m - \#l} \tag{9.2}$$

not insured connects to insured

$$U_i = U_i + \beta + \frac{\gamma}{m - \#l} \tag{9.3}$$

Not insured connects to not insured

$$U_i = U_i - r + \beta + \frac{\gamma}{m - \#l} \tag{9.4}$$

Each agent now has to evaluate whether it is beneficial to connect to a non-insured agent or not. Our goal is to be able to force that only insured nodes will connect to other insured nodes. The problem in this game is how to handle the γvaiable. The equation $\frac{\gamma}{m-\#l}$ reflects that the likelihood of reaching m connections, and the bonus profit increases linearly with the nodes number of own connections, $\#l$. If we evaluate the game we will end up with the following scenario:

A insured node will not connect to a noninsured node if the equation is met:

$$I_l > \beta - r + \frac{\gamma}{m - (m-1)} = I_l > \beta - r + \gamma \tag{9.5}$$

In addition the cost of establishing the new link, also has to be low enough for the transaction to the profitable. This means that I_l also has to be:

$$I_l < \beta + \frac{\gamma}{m)} \tag{9.6}$$

This means to ensure that only insured nodes connects to other insured nodes, and still have a profitable result I_l has to follow this equation:

$$\beta + \frac{\gamma}{m} < I_l < \beta - r + \gamma \tag{9.7}$$

9.1.2 Game connecting to insured first

Insured agents still prefer to connect to other insured agents, however, if it is not possible they will consider connecting to non-insured. As we see from Eq.(9.8) insured agents will have to establish L_{ni} connections to non-insured agents in order to receive γ.

$$L_{ni} = m - L_i \tag{9.8}$$

An insured agent will only connect with an non-insured agent if the following is fulfilled:

$$\frac{\gamma}{L_{ni}} > r + I_l \tag{9.9}$$

In addition the agent has to ensure that $non{-}insured\ agents\ willing\ to\ connect \geq L_{ni}$, else one will end up in a scenario where the agent takes unnecessary risk without being able to receive γ at the end. This means that the insured agent only consider connecting to other non-insured nodes if and only if it is guaranteed that the desired number of connections will be met.

Chapter 10
Future work

10.1 Risk

In our model we used an additive risk parameter, meaning that each connection to a non-insured node adds a fixed negative value r to the node's utility. It is reasonable to assume that the probability of failure increases if a node accepts more and more non-insured nodes. However, whether the risk parameter increases according to an additive distribution is difficult to confirm. Hence 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. The probability might as well be multiplicative, exponential or logarithmic. Although it is highly uncertain, we believe that the risk parameter will follow an exponential distribution similar to the one in Eq.(10.1).

$$F(x;\lambda) = \begin{cases} 1 - e^{-\lambda x}, & \text{if } x \geq 0 \\ 0, & \text{if } x < 0 \end{cases} \tag{10.1}$$

When λ have a value around 0.5, we get a curve 10.1 which captures how we believe the risk in a network will increase as more non-insured nodes are added. We believe that if one have a growing network consisting of insured nodes only, the first non-insured node added will contribute more risk than the consecutive non-insured nodes. When the 2.nd and 3.rd and so on, node are added there are already a probability that the network will be infected. It reasonable to believe that the overall risk wont increase additive, but at a lower rate. The risk added for each new non-insured node will decrease. Hence we believe that the accentual risk parameter will follow a exponential distribution.

read more in the paper: Uncertainty in Interdependent Security Games

From this paper presents a description of how to measure risk within a local

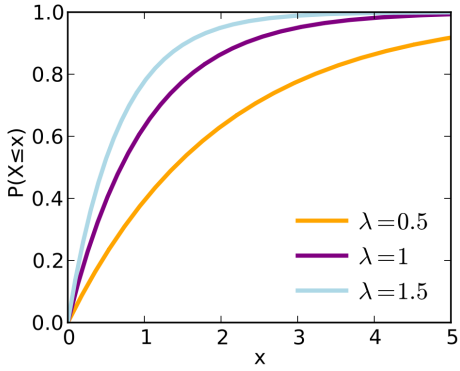


Figure 10.1: Figure showing the distribution of Eq.(10.1).

network. The idea is that for a cost c, you can protect yourself from threats outside your own LAN or corporation. This is analogous to purchase a firewall and anti-virus software. However, you can still be affected by threats from non-insured nodes inside your own local network. This means that as long as not every node is insured, the non-insured node will introduce a risk q to the local network. p reflects the probability of getting affected by a risk, and q represents the likelihood of spreading it to others in the local network. The paper presents a swift model for measuring the risk in you local network.

$$U_i = \begin{cases} -c + (1-q)^k, & \text{if not buying insurance} \\ (1-p)(1-q)^k, & \text{ifbuying insurance} \end{cases} \tag{10.2}$$

This model can be used to look at a the decision process of single node on whether to buy insurance or not. The paper presents certain conditions which creates scenarios where we end up with a network where either every node chooses to buy or every one chooses not to buy insured.

If $c < p$ then everyone will buy insurance, since this is cheaper than the expected loss. The other equilibrium where no one buys insurance, occurs when the cost of insurance is higher that the likelihood that a player fails to protect him selves, assuming that also fails to protect. i.e. $c > p(1-q)^{1-n}$

Our model's ultimate goal is to end up with insurable topologies which are able to measure risk in networks with a mix of insured and non-insured nodes. Therefore we will not take the same approach towards handling the problem with internal risk, i.e always forcing the network to either consist of insured nodes or not not-insured nodes. Instead we want to transfer this risk to the insurance company. Each node

will have the opportunity to purchase a link insurance, which compensate from any financial loss from a specific node.

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.cfcunderwriting.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. Accessed: 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 Directorate. 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.

[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.