# Cyber-insurance & endogenous network formation

Håvard Råmundal Halse[1], Jonas Hoemsnes[1] and Gergely Biczók[2]

[1] Dept. of Telematics
Norwegian University of Science and Technology
{havahals, jonashoe}@stud.ntnu.no
[2] Dept. of Telematics
Norwegian University of Science and Technology
gbiczok@item.ntnu.no

**Abstract.** Cyber-insurance is a powerful economic concept that can help companies in the fight against cybercrime. From the early 80s, several researchers claimed that cyber-insurance had a bright future, were it would become a huge economical tool for handling residual cyber-risks. However, both the European and US cyber-insurance market have failed to grasp its promising potential. To fully grasp this potential they need innovative approaches to handle the unique problems of cyber-insurance. This paper find and characterize network structures with properties that make them superior as cyber-insurance. And creates several models for forming these network structures. In every model, new properties that relate the model to the real-world and real-world insurance products are added. The results show that insurers can use the insurance premium as a tool for determining the resulting formation of the network, and if set to the right level, these superior structures will evolve. We believe our findings could help the cyber-insurance market evolve, by giving the insurers a proper tool to better analyze and control formation of cyber-insurance networks.

## 1 Introduction to cyber-insurance

Security breaches are increasingly prevalent in the Internet age causing huge financial losses for companies and their users. When facing security breaches and risk, there are typically four ways to act [BO1]:

1. Avoid the risk
2. Retain the risk
3. Self protect and mitigate the risk
4. Transfer the risk

The ICT industry have so far tried to prevent risks with a mixture of options two and three. This has lead to many different techniques and software trying to detect threats and anomalies, to protect the users and infrastructure. Firewalls, intrusion- detection and prevention systems, are some of the solutions. These will

reduce the risk, but do not eliminate the risk completely. Although they are all good and needed actions, it is impossible to achieve perfect cyber-security, due to many reasons: Threats are continuously evolving, there will always be accidents and security flaws, attackers have different intentions, network externalities and free-riding in security networks, the lemons-market in security products, misaligned incentives between users and product vendors, and many more. This is why we need cyber-insurance, as an fourth option, to handle the residual risk [BO2,RA1].

The market for cyber-insurance emerged in the late 80's, when security software companies began collaborating with insurance companies to offer insurance policies together with their security products. From a marketing perspective, adding insurance helped highlighting the supposedly high quality of the security software. Nevertheless, this new product was a comprehensive solution, which dealt with both risk reduction and residual risk [BO3]. Continuing into the beginning of the new millennium, several companies started offering standalone cyber-insurance, which sat the frame for the current insurance product. However, as found in the papers [PO1,ST1,GN1] both the US and the european market have not managed to reach its promising potential. Companies are weekly suffering from successful attacks, but most firms still have not acquired cyber-insurance. Researchers claim that the main reasons that cyber-insurance is struggling is the three unique problems, information asymmetry, correlated risk and interdependent agents [BS1].

*Information asymmetry.* Information asymmetry arises when one side of a transaction or 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 for the cyber-industry, where an insurer has trouble confirming whether your computer/network is "healthy". The other information asymmetry scenario is called moral hazard. It occurs after the signing of the contract, where one party deliberately takes some action that makes the possibility of loss higher, e.g. choosing not to lock your door. Or in the computer setting, deliberately visiting hostile web-pages, or not using anti-virus software, firewalls or other self-protection software, although you are required to do so.

*Correlated risk.* Another big concern regarding cyber-insurance, is the correlated risk. Among other things, the problem occurs due to the need for standards. Standardization is an important part of the business of computers and computer networks. Generally it enables computers to communicate, install and use different software. A good example is operative systems for personal computers, today we only have a small set of operative systems available, and these systems are standardized, so they can use the same communication channels. The standards generate a lot of the value in the ICT industry, but they also make many threats possible. All systems that use the same standards, create a large number of similar exposure units which could be exploited at the same time. Thus create 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.

*Interdependent security.* Another problem in the ICT industry is interdependent security, meaning that you are not only dependent on your own investment in security, but also on everyone else's. Investment in security generates positive externalities, and as public goods, this encourages free riding. 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 agent in the network, is not only dependent on this agent's level of investment in security, but also on the security investment done by adjacent agents, and their adjacent agents and so forth.

The cyber-insurance market seem to have a huge potential, but needs some new thinking to fully take advantage of it. We will take a new approach where we focus on finding network structures that will be beneficial for cyber-insurance, and see if it i possible for insurers to force these structures to evolve.

## 2 Cyber-insurance network structures

Like many phenomenons in our society, the cyber-insurance market can be described using graphs. Therefore we will see if there exists any graph structures that would be desirable for a cyber-insurance market.

The paper [LE1] is about evolutionary dynamics and how some structures can amplify or sustain evolution and drift[3]. One aspect of cyber-insurance is risk, and knowledge of how, for example, viruses spread in a network and how to use graph structures to prevent both hackers from entering and virus from spreading, is important. Evolutionary dynamics, and the research of how mutant genes spread throughout a population, as described in the paper, is analogous to this issue. If we can determine some structures where certain nodes are advantageous/disadvantageous, then these structures will have imporant properties, such as sustaining viruses from spreading.

The paper [LE1], shows that mutants inserted into a circulation graph, will have a fixation probability equal to

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

Where $r$ represents the relative fitness of the mutant i.e the agents security level, 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 satisfies these two properties:

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

---

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

2. The sum of all edges entering a vertex is equal for all vertices

A clique is a good example of a circulation graph, and the probability of fixation is as in Eq.(1). The fixation probability determines how probable it is that the whole network will eventually be "infected" by the mutant. Which means that it determines the rate of evolution, which relies on both the size of the network and the evolution speed. If the relative fitness of the nodes is high, then the probability of fixation will be low. A probability equal to one means that every node in the network will eventually be affected by the mutant.

An essential part of cyber-insurance is as mentioned earlier, for the insurer to be able to calculate the overall risk of the instance to be insured. Since the probability of fixation can be calculated in circulation graphs, if the insurer knows that the instance is part of a circulation graph, it is possible for the insurer to calculate the probability of fixation in that network. If we can find graphs with an fixation probability that exceeds Eq.(1) it is even better, because then the insurer is not only able to calculate the overall probability of fixation, but also to show that the probability of fixation is higher than the one for circulation graphs.

[LE1] shows that such graphs exist, and one example is the star topology. In this topology the fixation probability is as shown in Eq.(2), or more generally Eq.(3). $K$ is an amplifier parameter, the star-structure has an amplifier $K = 2$. The super-star, funnel and metafunnel can all be extendend to arbitrarily large K, thereby guaranteeing the fixation of any advantageous mutant. [LE1].

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

.

$$p_k = \frac{(1 - \frac{1}{r^k})}{(1 - \frac{1}{r^{kN}})} \tag{3}$$

When comparing Eq.(1) and Eq.(2), we see that the selective difference is amplified from $r$ to $r^2$, i.e. a star acts as an evolutionary amplifier, favoring advantageous mutants and inhibiting disadvantageous mutants.

The paper [**?**] present interesting results regarding network formation games. The authors set up a game where the nodes benefit from direct links, but these links also expose them to risk. Each node gains a payoff of $a$ per link it establishes, but it can establish a maximum of $\delta$ links. A failure occurs at a node with probability $q$, and propagates on a link with probability $p$. If a node fails, it will receive a negative payoff of $b$, no matter how many links it has established. The characteristics of this game is transferable to how we expect nodes in a cyber-insurance network to interact with eachother. Therefore, the results of the overall payoff change according to different collection of participants.

The results from the model presented by Blumen et.al. shows a situation where clustered graphs achieve a higher payoff when connected to trusted nodes, compared to when connecting with random nodes. Unlike in anonymous graphs, where nodes connect to each other at random, nodes in these graphs share some

information with their neighbors, which is used when deciding whether to form a link or not. To further explain these results, they show that there exists a critical point, called *phase transition*, which occurs when nodes have a node degree of $\frac{1}{p}$. At this point a node gets a payoff of $\frac{a}{p}$, and to further increase the payoff the node needs to go into a region with significantly higher failure probability. Because once each node establishes 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 states 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 Easley et.al, show that the only possible way of ending up with super critical payoff, is by forming clustered networks consisting of cliques with slightly more than $\frac{1}{p}$ nodes. However, if the nodes form an anonymous market, by random linking, they can only get sub-critical payoff. In other words, if the nodes can choose who they connect with, and by doing so, create trusted clustered markets, they can achieve a higher payoff by exceeding the critical node degree point.

*From an insurer's point of view.* Can the insurer force cyber-insurance networks to evolve into any of these structures, and at the same time separate the nodes into trusted and untrusted environments? If so, this could contribute significantly to solving the problems of cyber-insurance. The problems of information asymmetry and interdependent risk is reduced. Because, if the insurer knows the network structure, he can calculate the probabilities of failure and catastrophic events.

## 2.1 Research Question

Until now, our paper has introduced cyber-insurance, presented related work on the issues regarding cyber-insurance and this chapter has presented the properties of different graph structures and briefly introduced the idea of network formation. In this section, we have shown some structures, especially the star and clique, which could generate benefit for both the insurer and customers in a cyber-insurance market. We will combine the knowledge of these structures and network formation games to investigate networks consisting of nodes, insured or not, wanting to increase their payoff by establishing links with eachother. Is it possible for the insurer to force these networks to evolve endogenously into these structures? We will focus on how the insurer can determine the resulting formation by adjusting the parameter he can control, i.e. the insurance cost. We know that if the insurance premium is too high, no one will buy it. On the other hand, if it is too low, everyone would benefit from having insurance, and insured nodes will make risky decisions, such as connecting to risky nodes. We will try to determine whether it is possible to find the intersections, where the desired structures will evolve, and both the insurer and their customers will benefit from this.

## 3   Modeling Cyber-insurance

## 4   Models

There are many examples of nodes that need to establish connections with eachother. For example, when a firm is outsourcing tasks, cooperating or depending on other firms in some way. Such scenarios could be modeled, as networks where the nodes represents the firms and the links between them are their dependencies. However, the link between nodes involves some risks, such as: will the company deliver at the reported time, to the reported costs, what happens if it fails to deliver, what if the company goes bankrupt etc. To handle these risks, we need cyber-insurance.

From the insurer's point of view, a problem with cyber-insurance is to define and calculate risk, because the network structure is undefined. If an insurer were able to predict the network structure, the calculations of overall risk would be realizable. The situation could be even better if the insurer could force the structures found earlier to evolve, hence, ensuring a higher total payoff for the network. In summary, star topologies, or star-like topologies, have a fixation probability that exceeds the fixation probability of circulation graphs. Star structures also have a desirable property of minimizing the average path length, i.e. minimizing the cost spent on establishing links. Finally, the clique has a nice property of being able to achieve super-critical payoff, as showed in [Blu11]–fix. Both the clique and star have the possibility of amplifying or suppressing selection and drift. This is favorable, because if the insurer is able to ensure that the nodes have a certain security level, one can prevent viruses from spreading.

In our models a node is an agent who is either insured or not, and the nodes' goal is to maximize its payoff, by establishing links with other nodes. Our goal for the models is to find out if and how an insurer can force these cyber-insurance networks to evolve into the desirable structures mentioned in previous sections. The different parameters used to model the formation games are denoted as follows: The insurance premium is $I_l$, the expected risk cost is represented by $r$. $\beta$ represents the benefit of establishing a link. When establishing a link, the decision is a bidirectional decision.

## 5   Model 1: Including maximum node degree and bonus

In real world networks, such as in the manufacturing industry, software development firms and many other types of business, in some scenarios a product can usually not be completed without outsourcing some of the work needed. For the manufacturer, it could be beneficial to buy certain parts from others instead of producing them on his own. A software product might need the combined knowledge from different firms. Thus the firm that outsources tasks is dependent on the other firms, and will not reach its goal before the other firms deliver their contribution. When the product is finished the company gets paid. To model

this scenario we introduce a maximum node degree, $m$, per node, which represents the number of partners needed to complete a task. Additionally a bonus $\gamma$ represents the payoff a node receives when $m$ links are established.

When establishing a link between two insured nodes, the payoff the nodes will receive is as described in Eq.(5). 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.

$$U_{i+1} = \begin{cases} \beta - I_l, & \text{if } i = 0 \\ U_i + \beta - I_l, & \text{if } i > 0 \\ U_i + \beta - I_l + \gamma, & \text{if } i = m - 1 \end{cases} \tag{4}$$

### 5.1 Analysis

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$(\frac{\gamma}{m-i})$ in the decision process every time a node is considering to establish a link. In this way, nodes with higher degree will be more risk willing than nodes with low degree. For example, an insured node is more likely to accept a risky link when it only needs one more link to reach the goal, compared to when it need several more links to reach the goal.

We start our analysis by analyzing the four possible link establishment scenarios, insured to insured, insured to non-insured, non-insured to insured, and non-insured to noninsured. When establishing a link between two insured nodes, the payoff the nodes will receive is as described in Eq.(5).

$$U_{i+1} = \begin{cases} \beta - I_l, & \text{if } i = 0 \\ U_i + \beta - I_l, & \text{if } i > 0 \\ U_i + \beta - I_l + \gamma, & \text{if } i = m - 1 \end{cases} \tag{5}$$

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.(6) has to hold.

$$U_i + \beta - I_l + \frac{\gamma}{m - i} > U_i$$
$$\beta - I_l + \frac{\gamma}{m - i} > 0$$
$$\rightarrow \qquad \beta + \frac{\gamma}{m - i} > I_l \tag{6}$$

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

$$U_{i+1} = \begin{cases} \beta - I_l - r, & \text{if } i = 0 \\ U_i + \beta - I_l - r, & \text{if } i > 0 \\ U_i + \beta - I_l - r + \gamma, & \text{if } i = m - 1 \end{cases} \tag{7}$$

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

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

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

$$\rightarrow \qquad \beta + \frac{\gamma}{m-i} - r > I_l \qquad (8)$$

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

$$U_{i+1} = \begin{cases} \beta - r, & \text{if } i = 0 \\ U_i + \beta - r, & \text{if } i > 0 \\ U_i + \beta - r + \gamma, & \text{if } i = m - 1 \end{cases} \qquad (9)$$

To establish the connection, the following equation has to hold:

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

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

$$\rightarrow \qquad \beta + \frac{\gamma}{m-i} > r \qquad (10)$$

In the case of a non-insured node wanting to establish a link with an insured node, the payoff is a strictly increasing function, see Eq.(11), and thus a non-insured node will always connect to an insured node if possible.

$$U_{i+1} = \begin{cases} \beta, & \text{if } i = 0 \\ U_i + \beta, & \text{if } i > 0 \\ U_i + \beta + \gamma, & \text{if } i = m - 1 \end{cases} \qquad (11)$$

### 5.2   Result and findings

If we want a clique of only insured nodes, we have to ensure that insured nodes connect to each other, and that they do not establish connections to non-insured nodes. We know that an insured node would want to connect to another insured node if Eq.(6) is satisfied. In the equation we see that the expected bonus per established link is increasing. Thus, if an insured node of degree zero is willing to connect to another insured node, then every insured node with a degree higher than zero would also like to connect to another insured node. To ensure that insured nodes connect to eachother this equation has to hold:

$$\beta + \frac{\gamma}{m} > I_l \qquad (12)$$

We also want to ensure that insured nodes never establish links with non-insured nodes, from Eq.7 we see that this has to hold:

$$\beta + \frac{\gamma}{m-i} - r < I_l \tag{13}$$

This can be simplified, if one can ensure that the most risk willing insured node, i.e. the node with degree $m-1$, does not establish links with non-insured nodes. Then we know that no insured node with degree less than $m-1$ will establish links with non-insured nodes. From this we get equation Eq.(14).

$$\beta + \frac{\gamma}{m-(m-1)} - r < I_l$$
$$\rightarrow \qquad \beta + \gamma - r < I_l \tag{14}$$

To summarize, Eq.(12) and Eq.(14) give the final limitation on the link insurance cost, Eq.(15). If this equation is satisfied, the resulting network will contain a clique of only insured nodes.

$$\beta + \gamma - r < I_l < \beta + \frac{\gamma}{m} \tag{15}$$

For this to even be possible, $\beta + \gamma - r < \beta + \frac{\gamma}{m}$, i.e. Eq.(16) has to hold. This equation reflects that as the risk to bonus ratio gets smaller, it gets more and more difficult to ensure a clique of only insured nodes.

$$\gamma - r < \frac{\gamma}{m}$$
$$1 - \frac{r}{\gamma} < \frac{1}{m}$$
$$\rightarrow \qquad 1 - \frac{1}{m} < \frac{r}{\gamma} \tag{16}$$

It is also useful to know when non-insured nodes connect to each other. This happens when Eq.(9) 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 too high, then the non-insured node must establish links with insured nodes before it could be willing to establish risky links.

With these findings, an insurer can determine the outcome of the network formation game by adjusting the insurance cost parameter. If he wants a clique of only insured nodes Eq.(15) has to hold. However, it is easy to relax the condition, so that insured nodes only connect to, $j = 1, 2, 3..m$ non-insured nodes. This is done by changing Eq.(14) to $\beta + \frac{\gamma}{m-(m-j)} - r < I_l$, which gives us Eq.(17).
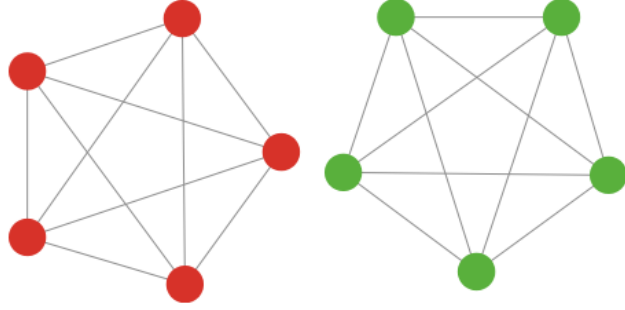
$$\beta + \frac{\gamma}{j} - r < I_l \tag{17}$$

**Fig. 1.** Two cliques, one consisting of insured agents the other consists of non-insured. All nodes have reached their goal.

### 5.3 Simulation of the results

For the first simulation the parameters are set to the following: $\beta = 0.9, I_l = 0.7, r = 0.5, \gamma = 0.2$ and $m = 4$, in order to satisfy condition Eq.(15), and enable all nodes to reach their maximum degree.

As we see in Figure 1, the results were as expected, the cost of insuring a link satisfied the conditions found earlier, and thus the result was two cliques, one consisting of only insured nodes and the other of non-insured nodes. The price of anarchy in this scenario is 1, i.e. the socially optimal outcome.

In the second simulation we set the parameter $m = 5$, and kept the other variables unchanged. The resulting network was as expected the same as in the last simulation, but since the nodes did not reach their maximum degree, the price of anarchy is less than one. The price of anarchy can be seen in Eq.(18).

$$PoA = \frac{\text{Sum of payoffs}}{\text{Sum of Socially optimal payoffs}}$$
$$PoA = \frac{5\times4\times(0.9-0.7)+5\times4\times(0.9-0.5)}{5\times4\times(0.9-0.7)+5\times4\times(0.9-0.5)+5\times(2\times0.9-0.7-0.5+2\times0.2)}$$
$$PoA = \frac{12}{17} \tag{18}$$

When we changed the link insurance cost to $I_l = 0.5$, the resulting networks change. Now we found that the insured nodes are willing to establish risky links to reach their maximum degree. Some of the resulting networks can be seen in the figures 2 and 3. In figure 2 the price of anarchy is 0.95, and in figure 3 the price of anarchy is 1, i.e. it has reached the socially optimal outcome.

## 6 Model 2: Including bulk insurance discount

It seems to be common for insurance companies to offer discount to their customers if the customers choose to combine some or all of their insurances with them. We would like to introduce a discount rate dependent on the degree of the
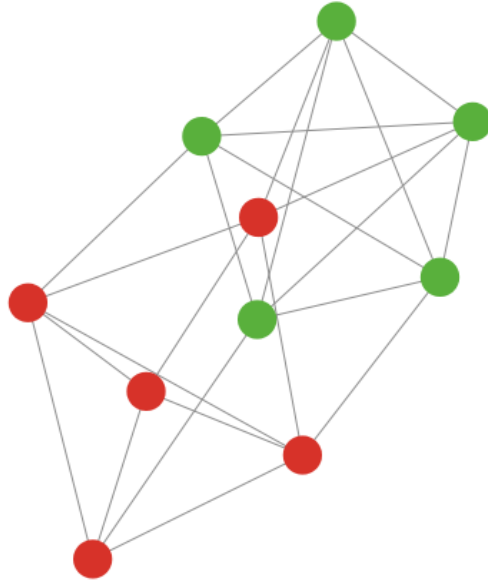
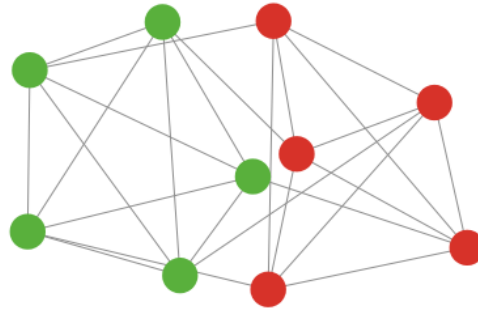**Fig. 2.** One non-insured node has connected to two insured nodes.



**Fig. 3.** Every non-insured node is connected to one insured node, this is the optimal outcome with these parameters.

node. In a real-world scenario where nodes have an option of acquiring insurance or not, this will make it more attractive for nodes with high degree to acquire insurance, and the discount could act as an incentive for nodes to also acquire insurance.

How insurance companies choose to formulate their discount rate might vary. One solution might be to follow a strict 5% discount per new connection, or let the discount follow a power law, or a log-function etc. We choose to follow a discount rule which directly reflects the node's degree.

## 6.1 Analysis

The price for adding a new link follows the equation:

$$\frac{I_l}{i+1} \tag{19}$$

Here, $i$ is the node's current degree. This means that the more links a node establishes the cheaper the link insurance will be.

**Discount and Bonus model** When the discount is applied to model 1, the only connection scenarios that is worth considering in this model is the ones where insured nodes connects to other insured nodes or when insured nodes connects to non-insured nodes.

When insured nodes are considering to establish links with eachother, their payoff functions are as shown in Eq.(20).

$$U_{i+1} = \begin{cases} \beta - I_l, & \text{if } i = 0 \\ U_i + \beta - \frac{I_l}{i+1}, & \text{if } i > 0 \\ U_i + \beta - \frac{I_l}{i+1} + \gamma, & \text{if } i = m - 1 \end{cases} \tag{20}$$

For insured nodes to connect to eachother Eq.(21) has to hold.

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

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

$$\rightarrow \qquad \beta + \frac{\gamma}{m-i} > \frac{I_l}{i+1} \tag{21}$$

When insured nodes are considering to connect to non-insured nodes, their payoff functions are as shown in Eq. (22).

$$U_{i+1} = \begin{cases} \beta - I_l - r, & \text{if } i = 0 \\ U_i + \beta - \frac{I_l}{i+1} - r, & \text{if } i > 0 \\ U_i + \beta - \frac{I_l}{i+1} - r + \gamma, & \text{if } i = m - 1 \end{cases} \tag{22}$$

For this to happen Eq.(23) has to hold.

$$U_i + \beta - \frac{I_l}{i+1} + \frac{\gamma}{m-i} - r \quad > U_i$$
$$\rightarrow \qquad \beta + \frac{\gamma}{m-i} > r + \frac{I_l}{i+1} \qquad (23)$$

## 6.2   Result and findings

We want to find the condition for separating insured and non-insured nodes. The first step is to guarantee that insured nodes connect to eachother. To ensure that this happens, we need to find the condition for the lowest expected increase in payoff, i.e. at node degree zero. If nodes are willing to establish links 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.(12) from model 1 holds, insured nodes will connect to other insured nodes.

The condition for guaranteeing that insured nodes do not connect to non-insured nodes has changed, we know that if an insured node does not want to establish a link with a non-insured node at degree $m-1$, then neither will any insured node with degree lower than $m-1$ do so. From this we find the condition in Eq.(24)

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

This is a very strong condition, because the only way this can happen is if $\beta + \gamma - r < \frac{1}{m}$. This shows us that when the incentives for establishing links increase, it gets more and more difficult for the insurer to guarantee a clique of only insured nodes. The final condition for ensuring a clique of only insured nodes is shown in Eq.(24).

$$m(\beta + \gamma - r) < I_l < \beta + \frac{\gamma}{m} \qquad (24)$$

The quantum discount results in an overall higher payoff for the insured nodes, since the cost of insuring a new link becomes cheaper. This means that the insured nodes will have a higher incentive to create links, making it harder for the insurer to separate insured and non-insured nodes.

We see that the problem of separating the two node types have increased compared to the previous model, meaning that if we have a network where the insurer has managed to separate them, the price of anarchy is also higher compared to a similar scenario in the first model.

# 7   Model 3: Network externalities

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

We apply the results from the paper from Jackson and Wolinsky [**?**] and use a network formation game found in [**?**] to study indirect network 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 "friends of the friend", and "friends of the friends of the friend" etc. This is achieved by letting the payoff be calculated relative to the distance between the nodes. $\beta$ now depends on the minimum number of hops to the node. We want the benefit to decrease with distance, therefore we need the limitation: $0 < \beta < 1$. The total payoff for a node is:

$$\sum_{j \neq i} \beta_{ij}^{d(ij)} - \sum_{j:ij \in g} c_{ij}, \tag{25}$$

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.

In the paper [**?**], the authors analyze the networks created with these rules with two different approaches, one with focus on efficiency and the other on stability. The optimal network is of course both efficient and stable, but as we shall see there are some conflicts between efficiency and stability. Matthew, et.al. showed that an efficient network is:

1. *a complete graph $g^N$ if $c < \beta - \beta^2$,*
2. *a star encompassing every node if $\beta - \beta^2 < c < \beta + \frac{(N-2)}{2}\beta^2$,*
3. *an empty network (no links) if $\beta + \frac{(N-2)}{2}\beta^2 < c$.*

The most efficient structure is a star structure which encompasses every node. A star structure has the characteristics of minimizing the average path length and uses the minimum number of links $(N-1)$ required for including every node. However, it is not preferable to be the center node, due to the cost of all the direct links. This structure provides the highest overall payoff for the network, but this network is not necessarily stable.

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

1. *a pairwise stable network consists of at most one (non-empty) component,*
2. *if $c < \beta - \beta^2$, the unique pairwise stable network will be a complete graph $g^N$,*

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

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

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

It should be noticed that it is more beneficial for a node to operate as a leaf node compared to being a center node, due to the cost of direct connections.

## 7.1 Insurance and connection game

The findings about efficiency and stability are very useful for our model, because if one has knowledge of the different variables it is possible to determine how the network will evolve. Additionally, if you are able to control the variables, you can actually determine the resulting network structure.

From this point on, the game we will consider is a homogeneous network setting, where every node is considered to be insured, and the benefit, $\beta$ and cost $I_l$ is the same for all nodes. This is done because it will simplify an otherwise very complex model.

In the paper [?] the authors came up with the following proposition: Consider the symmetric connections model in the case where $\beta - \beta^2 < c < \beta$. As the number of nodes grows, the probability that a stable state (under the process where each link has an equal probability of being identified) is reached with the efficient network structure of a star goes to zero. But if a network reaches the efficient star structure, it is also pairwise stable, and will remain a star.

Using the discount formula from the previous model, we end up with Eq.(26) to achieve an efficient and stable star topology. $i$ represents the node degree.

$$\beta - \beta^2 < \frac{i_l}{i+1} < \beta \tag{26}$$

An interesting property of the discount model is that the conditions for efficient and stable networks will change. Because when the node degree increases, the insurance cost might reach the critical degree $g$, and the best strategy for a node with degree $g$ or higher, is to connect to every node, as shown in Eq.(27). The critical degree occurs when a node's optimal strategy changes from relaying on indirect connections to connecting to every node.

$$\frac{I_l}{g} < \beta - \beta^2 \tag{27}$$

This is possible when $g < n$, where $n$ represents the number of nodes in the network. The stability condition has changed for a node with a critical degree.

The stable and efficient condition for this node is, as shown earlier, to have a direct connection to every other node. Thus if we have a star topology, both the leaf nodes and the center node are stable, and the center node has been compensated for its role in the network. This could be used to increase the probability of reaching a star formation.

When a node $i$ reaches the critical degree $g$ its optimal strategy is to connect to every node, since the payoff generated from direct connections is larger than any indirect connection. In general, nodes prefer to connect to nodes with high connectivity[4], 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 has a degree greater than or equal to $g$, and remove the links to their low-degree nodes which they can instead reach through the node with high connectivity.

From this we get the conjectures:

**Conjecture 1** *If the critical degree ratio is low, i.e. the ratio between critical degree and number of nodes in the network, the resulting network will with high probability be a clique.*

**Conjecture 2** *If the critical degree ratio is at a medium level, the resulting network will with high probability be a star.*

**Conjecture 3** *If the critical degree ratio is high, the resulting network will with high probability be a star-like/scale-free structure.*

A numerical example of the boundaries between the different structures, we found from our simulation (described in the next section) with 20 nodes is the following: As seen in Figure 4 a critical degree of 1-5 applies to conjecture 1, 6-12 applies to conjecture 2 and 13-20 applies to conjecture 3.

**Results and findings** To prove the conjectures above, we created a simulator. The rules of the simulator are as following: Every round of the game,two random nodes, not neighbors, are selected, and asked if they would want to establish a link. The link establishment is a symmetric decision, i.e. the link is established if it result in an increased payoff for both nodes. If the link is added, we check if either of the nodes would prefer to delete some of their already existing links, this decision is asymmetric. A link will be deleted if the node will achieve a higher payoff without it. Then we ask the rest of the nodes if they would like to delete any links. This procedure is repeated as long as it is possible to add new links. The payoff function of each node is as described earlier (see Eq.(25)), except that the cost is now dependent on the degree of the node. For the simulations to be realizable, we had to set the number of nodes to 20, or else the computational time would be to high. For every critical degree, from three to nineteen, we ran 50 simulations, and noted the resulting network formation. We chose to start from critical degree equal three, since any number below would result in a clique, because it would be more beneficial to be directly connected to every node.

---

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

We know that if Eq.(26) is satisfied for all $i$, then the efficient and stable state is a star. But a more interesting scenario occurs when we have a graph where one or more of the nodes reaches the critical degree. -Will the final structure be scale-free, a star or simply just unstructured? The results from the simulation can be seen in Figure 4, 5 and 6. As we see from Figure 4, 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 confirm our conjectures, and show that the discount can drastically increase the probability of the network ending up in a star.
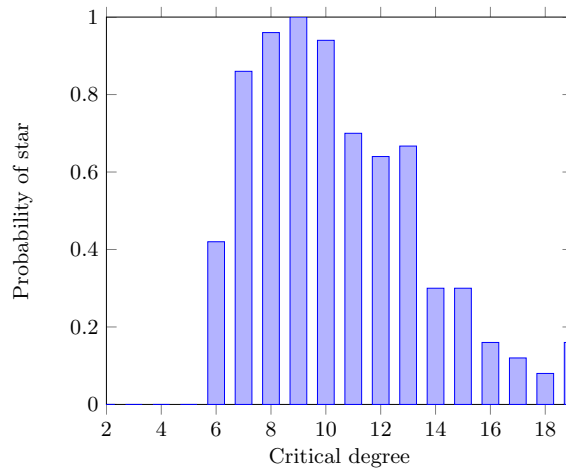


**Fig. 4.** Shows the probability of the network ending up in a star, given different critical degrees.

From Figure 5 we can observe that the opposite is happening when the critical degree is increased; the probability of the resulting network being a clique drastically decreases. As we can see with a critical degree of seven or higher, it is very unlikely that we end up with a clique. These findings support our conjectures.

In Figure 4 when the critical degree gets closer to the number of nodes in the network, the probability of the network evolving into a star decreases. However, in Figure 6, we have plotted the probability of the network evolving into a network where only a few(2-4) nodes end up with a high degree, but not necessarily a critical degree. As we see, this occurs with high probability from critical degree six and up. These networks are so called scale-free networks (A-B graphs, described in the methodology chapter), because there are a few hubs, that account for most of the connectivity in the network. The reason why we end up with a scale-free network is because nodes prefer to be connected with nodes with high connectivity, and thus will delete links to nodes with low connectivity.
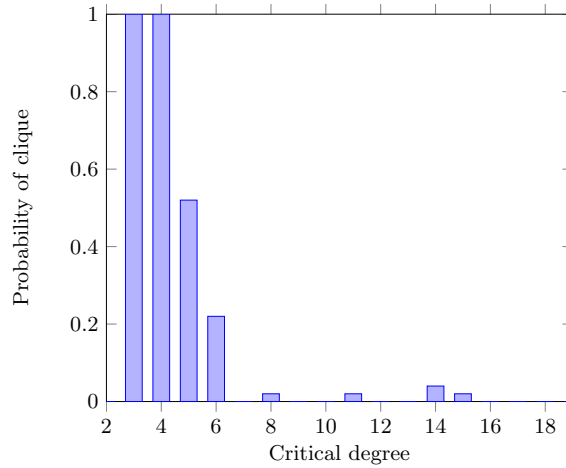
**Fig. 5.** Shows the probability of the network ending up in a clique, given different critical degrees.

This is very similar to the simple model that creates scale-free networks, where the probability of connecting to a node is proportional to the degree of the node.

*Price of Anarchy.* Another interesting thing is the average price of anarchy as function of the critical degree. The price of anarchy was calculated by taking the average total payoffs and dividing on the optimal payoff. The result can be seen in Figure 7.

We see that the price of anarchy for the first critical degrees is 1, and then decreases until degree six, and at seven it increases again. This is because at degree one to five, the socially optimal structure is a clique. At degree six, a clique and a star, are almost equally good, and at degree seven and up, a star structure is the socially optimal outcome. In other words, when the cost is low, a clique is the optimal structure, and when the cost is high a star is the optimal structure.

This further improves our findings, because we have now shown how an insurer can determine the resulting network formation by changing the cost. In addition, the formation that evolves has a price of anarchy close to 1.

## 8   Discussion

In this paper we have introduced tree different models, model 1: Bonus, model 2: Bonus and discount, model 3: Symmetric connection game with discount.

Model 1 can be applied to certain real-world scenarios, such as software development firms/chains, or other networks where the final product is dependent on the collaboration of multiple participants. This was done by including a bonus, which is first received when a node reaches the desired number of links (called
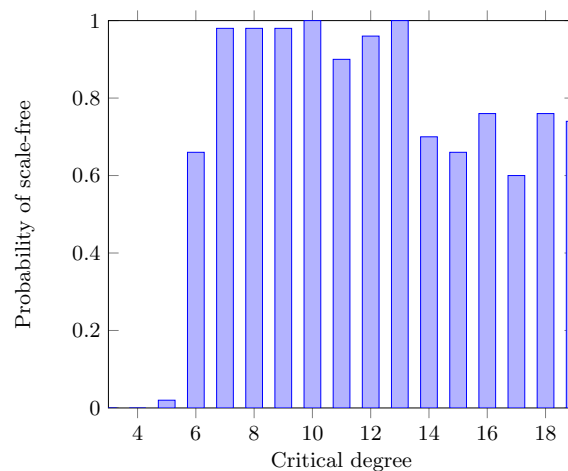
**Fig. 6.** Shows the probability of the network ending up in a scale-free structure, given different critical degrees.
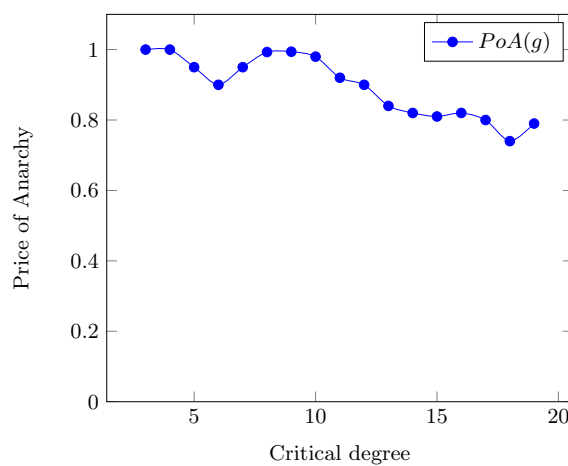


**Fig. 7.** Shows the price of anarchy as a function of critical degree

max-degree). This made the separation process of insured and non-insured nodes more difficult for the insurer. Due to the possibility of achieving the bonus, a node will have more incentive to establish links, and is thus more accepting towards establishing links with risky nodes. The conditions for separating insured and non-insured nodes in this model are: $\beta + \gamma - r < I_l < \beta + \frac{\gamma}{m}$. For the separation of insured and non-insured nodes to be possible, the following has to hold: $1 - \frac{1}{m} < \frac{r}{m}$. As we see, as $\gamma$ and/or $m$ increases, this gets more and more difficult to achieve.

In Model 2 we tried to implement a common feature used by insurance companies, bulk discount, in order to see how this affected the network formation. The cost of insuring a link is now dependent on the node's degree. The discount resulted in even higher incentive for insured nodes to establish links with non-insured nodes. The reason is intuitive, since the cost of doing so decreases as the node degree increases. The condition to ensure separation becomes: $m(\beta + \gamma - r) < I_l < \beta + \frac{\gamma}{m}$, and as in the other models, this further complicates the separation process for the insurer.

Since the incentive for establishing links has increased, the insurer has to set a higher price to compensate for this, therefore the potential price of anarchy is higher than in model 1 i.e. the more incentive for link establishment you have, the harder it gets to ensure separation of the nodes.

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

## 9   Conclusion

From our background study, it was revealed that the current market for cyber-insurance is far from healthy, and many have failed in attempts to establish

a cyber-insurance market. As described in the introduction, there are certain obstacles that are unique for cyber-insurance, and arguably these are the reasons why cyber-insurance has not emerged as expected. However, we believe that there is a need for cyber-insurance, and that our new approach of analyzing the cyber-insurance market through graphs and network formation games could help establishing and improving the market.

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

*Limitations and future work* One limitation to our work, and a suggestion for future work, is to map our models and simulations to real-world networks in a more convincing way. Real-world networks are not random. Nodes may prefer to talk to nodes with high degree or low degree. In addition, the decision to use additive risk were taken due to the simplicity of the function and the fact that we do not know how a real-world risk distribution actually looks like. By introducing a complex risk function, we would only have distorted the goal of our models. i.e. suggestions for improving our models is to introduce more realistic payoff functions.

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

# References

[BO1]  Bolot, Jean and Lelarge, Marc: Cyber insurance as an incentive for Internet security Managing information risk and the economics of security (2008) 269–290

[BO2]  Lelarge, Mark, and Jean Bolot: Economic incentives to increase security in the internet: The case for insurance. INFOCOM (2009), IEEE.

[BO3]  Bolot, Jean C and Lelarge, Marc A new perspective on internet security using insurance INFOCOM The 27th Conference on Computer Communications. IEEE (2008) 1948–1956

[RA1]    Pal, Ranjan and Hui, Pan On Differentiating Cyber-Insurance Contracts A Topological Perspective Internet Management Conference (2013), IEEE.

[PO1]    Ponemon Institute Second Annual Cost of Cyber Crime Study, Benchmark Study of U.S: Companies Ponemon Institute (2011)

[ST1]    Evolving cyber cover `http://www.strategic-risk.eu/Journals/2012/02/22/i/j/w/RiskFinancing_Mar12.pdf` Accessed: 31/01/2013

[GN1]    Graeme Newman Cyber liability in Europe: What insurers should knowL CFC Underwriter `http://www.cfcunderwriting.com/media/news-articles/european-cyber.aspx` Accessed: 14/02/2013

[BS1]    Böhme, R. and Schwartz, G. Modeling cyber-insurance: Towards a unifying framework Proceedings of GameSec (2010)

[LE1]    Lieberman, Erez and Hauert, Christoph and Nowak, Martin A Evolutionary dynamics on graphs Nature Publishing Group 433-7023 (2005) 312–316

[CE1]    Clarke, F., Ekeland, I.: Nonlinear oscillations and boundary-value problems for Hamiltonian systems. Arch. Rat. Mech. Anal. **78** (1982) 315–333

[CE2]    Clarke, F., Ekeland, I.: Solutions périodiques, du période donnée, des équations hamiltoniennes. Note CRAS Paris **287** (1978) 1013–1015

[MT1]    Michalek, R., Tarantello, G.: Subharmonic solutions with prescribed minimal period for nonautonomous Hamiltonian systems. J. Diff. Eq. **72** (1988) 28–55

[Ta1]    Tarantello, G.: Subharmonic solutions for Hamiltonian systems via a $\mathbb{Z}_p$ pseudoindex theory. Annali di Matematica Pura (to appear)

[Ra1]    Rabinowitz, P.: On subharmonic solutions of a Hamiltonian system. Comm. Pure Appl. Math. **33** (1980) 609–633