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

List of Algorithms

Chapter 1
Modeling Cyber-Insurance

1.1 Network Formation

In many scenarios agents 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 a balance between the expected earnings and the risk of the other party failing to complete the transaction. This is the reason why we seek to only download content from trusted peers and outlaw MC-gangs are consistently skeptical to enter into new agreements despite promising increased earnings, since the risk of undercover police are too high.

The 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.

1.1.1 Model of handling contagion risk

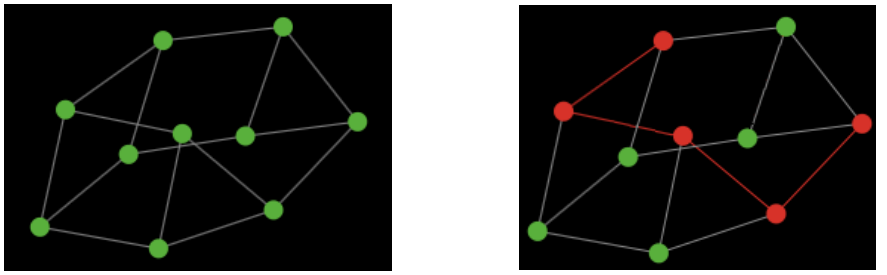
The model is simplified in order to show the concept of using cyber-insurance to encounter the problems with contagious risk. The model is formulated as follows. A set of n agents are randomly chosen to be insured or not. They all get their own income, and by connecting to other agents they will benefit from their income, i.e. when connected both agents will increase their income. However, when connecting to another agent naturally the cost of insurance increases due to aggregated risk. If and agent connects to someone without insurance a possible risk of severe losses due to cascading failure r has to be taken into account.

α - an agents income
β - income from direct links
I_o - cost of insurance.
I_l - increased insurance cost due to risk from a direct link.
r - cost of not having insurance, in case of failure.

Each agents payoff π is calculated with the following equation.

$$\pi = \alpha + \beta - I_o - Il - r \tag{1.1}$$

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 1.1 clustered networks of insured agents (red) are created, and according to [Blu11] the these agents achieves super-critical payoffs. Which demonstrates that



(a) Initial graph with 10 agents. (b) Insured agents (red) forms a network

Figure 1.1: shows how insured agents connects with each other to form a network to achieve super-critical payoffs.

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.

[BL08] 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.

[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.

[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.

[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.

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

[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.

[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.

[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.

[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.

[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.