# Thesis subject: Stochastic games over graphs: applications to cyber-insurance contracts

PhD Advisors: Nabil Kazi Tani, IECL
and Vineeth S Varma, CRAN

October 2021

## 1 Context of the PhD project

**Cyber-insurance.** Over the past ten years, the growing number of cyber related issues and incidents have made cybersecurity one of the main concerns in insurance. The COVID-19 pandemic has considerably increased the exposure of professionals and individuals to computer attacks. Cyber risk has thus been described as the second major risk of the decade to come in the Axa Future Risks report of 2021 [1]. It is even considered to be the main risk in France according to the Allianz Risk Barometer ranking of 2021 [2].

A cyber incident has various consequences, it can target the personal data of millions of connected people, as well as industrial secrets, often resulting in an interruption of production or service availability, generating significant financial losses. Cyber attacks can also damage reputation, threatening the trust of customers and business partners. As such, these incidents are sometimes overlooked to preserve the image of the company. This opacity contributes to reinforcing the lack of data related to cyber risk facing the insurance world.

**Cyber insurance contracts.** Thus, large companies are subject to large-scale claims amounting to tens of billions of euros, making reinsurers and insurers vulnerable to the risk of accumulation. Reinsurers saw their loss ratio (claim to premium ratio) jump from 84% in 2019 to 167% in 2020 (see [3]), which led to an increase in premiums and a decrease in coverage on most of the offered contracts. According to a study by the Amrae among eight large brokers [3], 87% of large companies are covered by a cyber insurance contract, compared to only 8% of mid-size companies. Likewise, small businesses and public authorities rarely subscribe to this type of coverage. Insurers face a contrast within the market, between large companies which are mostly protected by a cyber insurance contract but with less coverage than their needs and mid-size companies which have a large offer but underestimate their exposure to IT risk.

Cyber risk analysis and related insurance issues is a multidisciplinary subject, that has triggered an intensive research activity over the last 15-20 years [4, 5]. Cyber insurance and reinsurance is a promising tool of cyber risk management. However, despite the extensive research activity around cyber insurance (see for instance [6, 7, 8] and the references therein), its actuarial analysis is still at an early stage and many practical and theoretical problems remain open.

The main guarantees of cyber insurance contracts currently on the market are:

- identification of the problem and its extent,
- the implementation of corrective actions, additional protections and programs of prevention,
- the payment of certain costs associated with the claim.

The prices of this type of contract are very variable and depend on several macroeconomic factors such as the size of the company, its turnover as well as its exposure to IT risk (typically via the number of computers or servers). However, one aspect that is often ignored is the impact of the graph structure on the safety and robustness of the network.

**In this project, we aim to mathematically characterize the effect of the underlying network topology on prices, cyber risk assessment and management. To do so, we model the interactions between attackers and defenders as a stochastic game.**

# 2 Scientific challenge and state of the art

## 2.1 Task 1: Continuous-time optimal control of eigenvalues of matrix-valued stochastic processes.

The issue of the network's topology effect on risk management raised above is a wide and difficult question in general, for which a partial answer is given in the paper [9], in which the authors consider a loss accumulation scenario, in the sense that a computer attack on a given graph becomes endemic, for a standard compartmental epidemic model known as Susceptible-Infected-Susceptible (SIS). They consider an institution whose goal is to protect the network from communication interruption, by maintaining it as connected as possible in an endemic situation. This paper allows to determine where on a graph it is optimal to focus prevention measures or insurance protection, given a total protection budget. The obtained solution highly depends on the network topology, and thus provides an answer for the question above, when the focus is on optimal protection measures. The developed methodology relies on standard techniques from eigenvalues optimization theory [10], for which numerical techniques are available, that allow to solve the problem for large graphs. More precisely, it relies on results and numerical methods for the optimization of functions of the eigenvalues of matrix operators associated to finite graphs.

**Problem 1: Extending the results of [9] to a time dynamic framework.** This would have a broader theoretical interest, and a clear practical interest for dynamic cyber protection strategies adapted to the time evolution of an exterior attack. This can be a preliminary work done at the start of the PhD.

## 2.2 Task 2: Dynamic game models of attack and defense.

Assuming that both the attacker and the defender behave in a rational manner, we can characterize their interactions under a dynamic game framework. While we can assume that the structure of the network is known to the defender, the attacker may not have this information or may possess an imperfect knowledge of the graph. An important issue for both of these entities is to identify and order the nodes in terms of their strategic importance. For example, in a star graph, defending the central node is much more important than other nodes. A study of the resulting game will help predict the likelihood that a network gets compromised when under attack, with a given (and known) budget of defense and attack. For an example of a competitive game in which the strategy depends on the graph structure, we refer to [11].

Let us describe in more details a particular game framework that could be studied by a PhD candidate.

The network is described by nodes that belong to a set $\mathcal{V} := \{1, 2, \ldots, N\}$ and are connected by a graph $G = (\mathcal{V}, \mathcal{E})$ where $\mathcal{E} \subset \mathcal{V}^2$ is the set of undirected edges. We use $X_n(t) \in \{0, 1\}$ to denote the state of node $n \in \mathcal{V}$ at time $t \in \mathbb{Z}$ with 0 indicating a susceptible node and 1 indicating a compromised (infected) node.

The attacker can try to spread a virus or hack a subset of $\mathcal{V}$ nodes through the internet or another external network, at any given time instant with a certain budget $B_a$. The intensity of the attack on node $n \in \mathcal{V}$ at time $t$ is given by $c_n(t)$ with $\sum_{n\in\mathcal{V}} c_n(t) \leq B_a$. Since this attack comes from outside the network, it is easier to detect and protect against.

On the other hand, the defender can allocate its cyber-security budget $B_d$ to stop external cyber-attacks, with a protection rate $p_n(t)$ or to recover a compromised node at rate $r_n(t)$ with $\sum_{n\in\mathcal{V}} p_n(t) + \gamma r_n(t) \leq B_d$. Here $\gamma >> 1$ as recovery costs a lot more than protection.

A compromised or infected node will attack its neighbors over the network, which is harder to defend against as it comes from within the network and this can be modelled via an SIS process for example. At each time instant $t$, any node may get infected from an external source through cyber-attacks or a neighbor, with a probability depending on the protection rate $p_n(t)$ and the attack intensity $c_n(t)$, and we have

$$\Pr(X_n(t+1) = 1 | X(t), X_n(t) = 0) = \frac{c_n(t) + |N_n|^{-1} \sum_{j\in N_n} X_j(t)}{1 + p_n(t) + c_n(t)} \tag{1}$$

where $N_n$ is the set of neighbors of node $n$ with cardinality $|N_n| \geq 1$ for all $n \in \mathcal{V}$. This equation is an example model of the cyber-attack scenarios we plan to study.

The objective of the attacker is to maximize the number of compromised nodes, and the defender naturally tries to minimize the number of compromised nodes. When a critical number of nodes are compromised, the insurance contract is applied, and the final goal of this project will be to evaluate the probability of this scenario for a given $B_a, B_d$ and graph structure.

**Problem 2: the resulting interaction can be described by a zero-sum stochastic game, which we plan to study during the course of a PhD.**

For certain graph structures, we may use the mean-field approximation to simplify the interactions and formulate a mean-field game. In the continuous time framework, probabilistic techniques, based on backward stochastic differential equations (BSDEs for short) are well developed to solve control and game problems for $\mathbb{R}^d$-valued stochastic processes. These can be seen as dynamic programming equations in a non Markovian framework.

**Problem 3: relate the value function of stochastic games on graphs to the solution of a well chosen BSDE.**

# 3 Complementary expertise of the advisors

**Initiative:** This collaboration started at the "journées scientifiques de la Fédération Charles Hermite" titled "Science des Réseaux" on 7th of October, 2021. For CRAN, this project is in accordance with its scientific strategy and priorities, namely Network Science and Complex systems an is also an opportunity of enlarging the investigation area of the CID department on these topics. For IECL, this PhD subject falls within the specialties of the Probability and Statistics team, and widens the domains of applications to actuarial models of cyber risk management.

**Nabil Kazi-Tani.** Nabil specializes in probability theory, in the study of stochastic differential equations, risk measures and optimization, with applications in financial and actuarial models. He is a certified member of the French institute of actuaries.

He will bring his expertise on continuous time stochastic control and stochastic differential games, and in particular on the probabilistic approach based on backward stochastic differential equations to solve these problems. His experience/collaboration with cyber-insurance companies could be useful for this project. Indeed, discussions with professionals from the private sector could be a valuable source of information on the practical scientific needs in cyber risk management. Independently of this PhD project, we plan to organize an open working group, involving people from the cyber insurance industry to come discuss with computer scientists, mathematicians and automatic control specialists. Risk managers from the two companies SCOR and Sia Partners already agreed to come to Metz/Nancy and participate in such a working group. Such discussions could lead to broader collaborations with these companies. In particular, it could be a source for funding half of a PhD cost.

**Vineeth S Varma.** Vineeth specializes in optimization, control and games over networked systems with application to telecommunication, opinion dynamics and epidemics. In this project, he will bring his expertise on applying game theoretical and control tools on multi-agent systems interacting over graphs. In stochastic games theory, every player can interact with all the other players. This induces an implicit symmetry in the game, that can be used to solve it. The fact that the interactions that we consider are on a graph (which is not necessarily the complete graph!) breaks this symmetry and complicates the problem. Vineeth's expertise on these systems is thus crucial for this PhD project.

**PhD.** The multi-disciplinary nature of such a subject requires several skills from a PhD student. She/he should have a strong background in probability, optimization, and she/he would be expected to manipulate scientific software such as Python, R or Matlab for simulation and numerical implementation of optimal control strategies. The PhD student would need to quickly assimilate the needed notions of graph theory. Knowledge in computer science, in particular on cyber security, and/or some knowledge of actuarial models would be a plus. The student will be hosted by IECL (Metz) and will make frequent visits to CRAN (Nancy).

# References

[1] Axa. Axa future risks report 2021. `https://www.axa.com/fr/presse/publications/future-risks-report-2021`. Accessed: 2021-10-14.

[2] Allianz. Allianz risk barometer 2021. `https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2021.html`. Accessed: 2021-10-14.

[3] Amrae. Lumière sur la cyberassurance. `https://www.amrae.fr/bibliotheque-de-amrae?ref_id=3214&ref_type=publication`. Accessed: 2021-10-14.

[4] Lawrence A Gordon and Martin P Loeb. The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, 5(4):438–457, 2002.

[5] Lawrence A Gordon, Martin P Loeb, Lei Zhou, et al. Investing in cybersecurity: insights from the gordon-loeb model. *Journal of Information Security*, 7(02):49, 2016.

[6] Matthias A Fahrenwaldt, Stefan Weber, and Kerstin Weske. Pricing of cyber insurance contracts in a network model. *ASTIN Bulletin: The Journal of the IAA*, 48(3):1175–1218, 2018.

[7] Yannick Bessy-Roland, Alexandre Boumezoued, and Caroline Hillairet. Multivariate hawkes process for cyber insurance. *Annals of Actuarial Science*, 15(1):14–39, 2021.

[8] Caroline Hillairet and Olivier Lopez. Propagation of cyber incidents in an insurance portfolio: counting processes combined with compartmental epidemiological models. *Scandinavian Actuarial Journal*, pages 1–24, 2021.

[9] Thierry Cohignac and Nabil Kazi-Tani. Laplacian spectra of graphs and cyber-insurance protection. 2020.

[10] Stephen Boyd. Convex optimization of graph laplacian eigenvalues. In *Proceedings of the International Congress of Mathematicians*, volume 3, pages 1311–1319, 2006.

[11] Vineeth S Varma, Irinel-Constantin Morărescu, Samson Lasaulce, and Samuel Martin. Marketing resource allocation in duopolies over social networks. *IEEE control systems letters*, 2(4):593–598, 2018.