NetSciX2026: International School and Conference on Network Science
February 17^{th}-20^{th}, 2026 - Auckland, New Zealand

Network Security under Heterogeneous Cyber-Risk Profiles and Contagion

Keywords: Cyber-Risk, Network security, Game theory, Contagion, Optimal Investments.

As digital ecosystems become increasingly complex, the need to manage large amounts of data has led to infrastructures that are typically organized as networks of interconnected servers or units. While such interconnectivity enhances efficiency, scalability, and redundancy, it also introduces systemic vulnerabilities: a single breach can act as a gateway for contagion, allowing malicious activity to propagate and potentially compromise the entire system.

In this work, we propose a cyber risk management framework for digital networked systems, designed to identify an optimal investment strategy for allocating cybersecurity defenses across network nodes. The core components of our model include contagion across the network and the strategic behavior of cyber attacks. For the first, we draw inspiration from the extensive literature on complex networks [1, 2]. Typically, these models assume that the initial trigger—be it the zero-patient of an epidemic, a financial shock, or a rumor—is exogenous and random, reflecting events that are unintentional and difficult to predict or control.

However, this assumption does not hold in the context of cybersecurity, where attacks are often strategic and targeted. To address this, we adopt a game-theoretic framework, building on the literature of security games [3–6], which explicitly models the adversarial nature of cyber threats and the strategic allocation of defenses. Most of these models, still grounded in an epidemiological view of contagion, assume that the attacker's objective is simply to maximize the spread of infection across the network. However, in cybersecurity settings, the attacker may instead aim to reach specific nodes or regions considered strategic or of higher value. Similarly, the defender may prioritize the protection of critical nodes while allowing others to be sacrificed.

In our work, building on the contagion mechanism of [7, 8], we therefore consider a heterogeneous network in which both attacker and defender assign values to each node and a corresponding target risk. The attacker and defender may assign different value/risk profiles to the nodes, reflecting their asymmetric information and differing perspectives on the system's structure and strategic importance. Specifically, we consider a network $\mathscr{G}$ of n interconnected nodes represented by its adjacency matrix $\mathbf{A} = (A_{ij})_{i<j}^{n}$, $A_{ij} \in \{0,1\}$, $i, j = 1, \ldots, n$. Each node s can be the target of a cyber-threat with a probability $\phi_s \in [0,1]$, becoming the *seed* of a potential infection. Nodes can be either immune or susceptible to cyber-attacks. We introduce the susceptibility vector $\boldsymbol{X} = (X_i)_{i=1}^{n}$, where each $X_i \in \{0,1\}$ indicates whether node i is susceptible ($X_i = 1$) or immune ($X_i = 0$) to a cyber-threat. We model $\boldsymbol{X}$ as a random vector of independent Bernoulli variables, with $\mathbb{P}(X_i = 0) = q_i$ and $\mathbb{P}(X_i = 1) = 1 - q_i$, where $q_i \in [0,1]$. The vector $\boldsymbol{q}$ reflects how cybersecurity investments have been distributed across the network. We assuem that any susceptible node that is connected to the seed via a path consisting entirely of susceptible nodes will become infected.

On top of this environment, we consider a two players Stackelberg extensive game where the defender allocates cyber defenses across the network, by adjusting the system's security vector $\boldsymbol{q}$, and the attacker responds by optimizing the cyber-attack distribution vector $\boldsymbol{\phi}(\boldsymbol{q})$, strategically selecting the nodes where it is most advantageous to pose a threat.

The attacker's utility function $\mathscr{U}_a$ and the defender's loss function $\mathscr{L}_d$, which are to be

optimized, are defined with the following risk/cost structure:

$$\mathscr{U}_a(\boldsymbol{\phi};\boldsymbol{q}) = \sum_i^n \eta_i \mathscr{R}_i(\boldsymbol{q},\boldsymbol{\phi};\boldsymbol{A}) - \theta\, \mathscr{C}_a(\boldsymbol{\phi}), \quad \mathscr{L}_d(\boldsymbol{q};\boldsymbol{\phi}) = \sum_i^n z_i \mathscr{R}_i(\boldsymbol{q},\boldsymbol{\phi};\boldsymbol{A}) + \alpha\, \mathscr{C}_d(\boldsymbol{q}). \quad (1)$$

The strategy costs incurred by the attacker and the defender are denoted by $\mathscr{C}_a(\boldsymbol{\phi})$ and $\mathscr{C}_d(\boldsymbol{q})$. The vector $\mathscr{R} = (\mathscr{R}_i)_{i=1}^n$ measures the infection risk at each node, as a function of both the network structure $\boldsymbol{A}$ and the strategies adopted by the two players $(\boldsymbol{q},\boldsymbol{\phi})$, thereby defining the system's *risk profile*. We analyze two distinct risk measures: the first is based on the actual probability of a node being infected, while the second relies on the expected number of paths connecting the node to the infection seed. The *value profiles* $\boldsymbol{\eta} = (\eta_i)_{i=1}^n, \boldsymbol{z} = (z_i)_{i=1}^n \in \mathbb{R}^n$ model the perceived importance of different nodes or regions of the network for the attacker and the defender, respectively.

We provide a characterization of the Strong Stackelberg equilibrium (SSE) of the game $(q^*, \boldsymbol{\phi}^*(\cdot))$, in terms of naturally emerging network metrics. These metrics quantify the extent to which each node contributes to the overall protection of the system and are combined in a principled way according to the players' respective risk profiles. We compute the efficient frontier to analyze the overall system robustness to strategic attacks across different network topologies and risk profiles. Moreover, by analyzing the optimal allocation patterns, we show the emergence of *cyber-deception* effects, in which the attacker avoids a direct assault on the most valuable nodes to mislead the defender, who ends up dispersing investments away from the actual targets.

Finally, we examine the scenario where the risk is approximated by the expected number of paths to the attack seed. This choice enhances the scalability of the analysis for large networks. We show that the optimal strategy is optimally robust for real dynamic contagion. Moreover we show that there exists a dismantling phase transition in terms of the defender's budget.

References

[1] Mark Newman. *Networks*. Oxford university press, 2018.

[2] Steven H Strogatz. "Exploring complex networks". In: *nature* 410.6825 (2001), pp. 268–276.

[3] Milind Tambe. *Security and game theory: algorithms, deployed systems, lessons learned*. Cambridge university press, 2011.

[4] Sankardas Roy et al. "A survey of game theory as applied to network security". In: *2010 43rd Hawaii international conference on system sciences*. IEEE. 2010, pp. 1–10.

[5] Xiannuan Liang and Yang Xiao. "Game theory for network security". In: *IEEE Communications Surveys & Tutorials* 15.1 (2012), pp. 472–486.

[6] Mohammad Hossein Manshaei et al. "Game theory meets network security and privacy". In: *Acm Computing Surveys (Csur)* 45.3 (2013), pp. 1–39.

[7] James Aspnes, Kevin Chang, and Aleksandr Yampolskiy. "Inoculation strategies for victims of viruses and the sum-of-squares partition problem". In: *Journal of Computer and System Sciences* 72.6 (2006), pp. 1077–1093.

[8] Daron Acemoglu, Azarakhsh Malekian, and Asu Ozdaglar. "Network security and contagion". In: *Journal of Economic Theory* 166 (2016), pp. 536–585.