Mathematics and Financial Economics (2023) 17:247–283
https://doi.org/10.1007/s11579-023-00336-w

ORIGINAL PAPER

# Contagion risks and security investment in directed networks

**Hamed Amini**[1]

Received: 11 May 2022 / Accepted: 28 March 2023 / Published online: 17 May 2023


**Abstract**
We develop a model for contagion risks and optimal security investment in a directed network of interconnected agents with heterogeneous degrees, loss functions, and security profiles. Our model generalizes several contagion models in the literature, particularly the independent cascade model and the linear threshold model. We state various limit theorems on the final size of infected agents in the case of random networks with given vertex degrees for finite and infinite-variance degree distributions. The results allow us to derive a resilience condition for the network in response to the infection of a large group of agents and quantify how contagion amplifies small shocks to the network. We show that when the degree distribution has infinite variance and highly correlated in- and out-degrees, even when agents have high thresholds, a sub-linear fraction of initially infected agents is enough to trigger the infection of a positive fraction of nodes. We also demonstrate how these results are sensitive to vertex and edge percolation (intervention). We then study the asymptotic Nash equilibrium and socially optimal security investment. In the asymptotic limit, agents' risk depends on all other agents' investments through an aggregate quantity that we call network vulnerability. The limit theorems enable us to capture the impact of one class of agents' decisions on the overall network vulnerability. Based on our results, the vulnerability is semi-analytic, allowing for a tractable Nash equilibrium. We provide sufficient conditions for investment in equilibrium to be monotone in network vulnerability. When investment is monotone, we demonstrate that the (asymptotic) Nash equilibrium is unique. In the specific example of two types of core-periphery agents, we illustrate the strong effect of cost heterogeneity on network vulnerability and the non-monotonous investment as a function of costs.

**Keywords** Contagion · Security investment · Stochastic networks · Random graphs

**JEL Classification** C70 · D62 · G18

## 1 Introduction

Internet security is one of the major sources of concern in today's interconnected world. Fraud, cyber-attacks, and the influence of malicious software (or malware) on the World Wide Web

✉ Hamed Amini
aminil@ufl.edu

[1] Department of Industrial and Systems Engineering, University of Florida, Gainesville, FL, USA

and its plethora of overlying and underlying networks create significant economic, social, and political damages. In finance, security investment can be seen as a financial institution's decision to hold higher capital. Higher capital comes, of course, at a cost but has a benefit on the entire financial system because losses are absorbed. Otherwise, a firm's failure can translate into bankruptcy costs, and losses are imposed on other firms. As the financial crisis has highlighted, systemic risk is one of the most important risks in financial systems, with potential spillovers to the real economy. Investment in capital and liquidity has been mandated in various forms by financial regulators in the aftermath of the crisis.

Security investment is by no means specific to communication networks or to economic, information, or financial exchanges. In the current Covid-19 health emergency, the self-isolation decision played an important role in network vulnerability. Mitigating epidemic spreading and COVID-19 [1, 12, 26] can be seen as a variant of security investment when security investment is replaced by self-isolation decisions. However, the epidemic models in such applications are more realistically based on the Susceptible-Infected-Recovered (SIR) model for non-directed graphs.

In this paper, we propose a general framework in which a directed network of interconnected agents is subject to contagion risks and potential loss. We study the asymptotic Nash equilibrium and socially optimal security investments in a random directed network with fixed degrees. The structure of the networks plays an important role in the resilience of the network and impacts the decisions of different network players. We demonstrate how an agent's decision on their security level might depend on the decisions of other agents in the network. In particular, agents who decide not to invest in self-protection also put other network participants at contagion risk.

The independent threshold model with security profiles that we introduce generalizes several contagion models in the literature, particularly the independent cascade model and the linear threshold model. We state several limit theorems on the final size of infected agents in the case of random networks with fixed degrees, for finite and infinite variance degree distributions. The results allow us to derive resilience conditions for the network in response to small initial shocks.

We characterize the asymptotic Nash equilibrium and socially optimal security investment. In the asymptotic limit, agents' risk depends on all other agents' investments through an aggregate quantity, which we call network vulnerability, and which captures how risky an unknown counterparty is. Based on our results, the vulnerability is semi-analytic, allowing for a tractable Nash equilibrium.

We provide sufficient conditions for investment in equilibrium to be monotone in network vulnerability. When investment is monotone, we demonstrate that the asymptotic Nash equilibrium is unique. For the case of random regular graphs and core-periphery network models, the social optimum is explicit, and we theoretically guarantee that individual decisions will result in underinvestment compared to the social optimum. In the particular example of two types of agents, called core and periphery agents, we exhibit a strong effect of cost heterogeneity and, in particular, non-monotonous investment as a function of costs.

*Related literature*

Limiting contagion risk requires new analytical and computational tools. Extensive research in this area focuses on the spread of epidemics over different network structures. For example, see [14, 18, 21, 24, 32, 42] for SIR epidemics in random networks and [6, 37, 39, 41, 46] for threshold contagion models in random networks.

Another related strand of literature is on default cascades and systemic risk in random financial networks, see e.g., [5, 8, 11, 13, 17, 23, 25]. In particular, in [7], the authors study financial contagion on configuration model and derive a criterion for the resilience

of a financial network to insolvency contagion, based on connectivity and the structure of contagious links (i.e., those exposures of a bank larger than its capital).

There is an emerging literature on the economics of (information) security and the management of systemic cyber risk, see e.g., [2, 29, 40, 48]. In [29], the authors consider a simple one-period economic model for a single agent decision characterized by two parameters: $\ell \in \mathbb{R}_+$ for the monetary loss and $v \in [0, 1]$ called vulnerability, representing the probability that without additional security investment, the agent becomes infected and the loss $\ell$ occurs. The agent can invest the amount $x$ at time 0 to reduce the probability of infection (loss) to $p(x, v)$. Assuming the agent is risk-neutral, her optimal security investment would be the value $x_* = x_*(v, \ell)$ minimizing

$$x_*(v, \ell) = \arg\min\{x + \ell p(x, v) : x \geq 0\}.$$

Note that the fixed point solution(s) $x_(v, \ell)$ does not need to be non-decreasing in $(v, \ell)$. For instance, [29] consider the following example: $p(x, v) = v^{\alpha x+1}$, where $\alpha > 0$ is a productivity measure parameter for information security. A sufficient condition for monotone investment is given in [38]: Assume that $p(x, v)$ is twice continuously differentiable on $\mathbb{R}_+ \times [0, 1]$, non-increasing in $x$ and $\frac{\partial^2 p}{\partial x \partial v}(x, v) \leq 0$, then the function $(v, \ell) \to x_*(v, \ell)$ is non-decreasing in $(v, \ell)$. In this case, the security investment decision is simpler since there is an augmenting return on investment with vulnerability.

We extend the existing literature in several ways: we generalize the contagion model, allow for network heterogeneity and multiple security levels, and treat the directed network case. When investment is monotone, we show that the Nash equilibrium is unique. In the case of two types of core-periphery agents, we exhibit the strong effect of cost heterogeneity on network vulnerability and the non-monotonic investment as a function of costs.

*Outline* The paper is structured as follows. Section 2 provides two motivating examples for the optimal security investment game. In Sect. 3, we present our general framework for the study of contagion risks in random networks. We also state our main results on the asymptotic magnitude of contagion and resilience of large networks to small initial shocks in Sect. 3. In Sect. 4, we consider the network security game and provide a sufficient condition for the uniqueness of the equilibrium. In Sect. 5, we give a more detailed analysis of the particular case when there are two security classes, and investment in security provides strong protection. For the case of random regular graphs and core-periphery network modes, the social optimum is explicit, and we theoretically guarantee that the individual decision will be to underinvest compared to the social optimum. Section 6 concludes, and Appendix A contains all the proofs.

*Notations* We let $\mathbb{N}$ be the set of non-negative integers. For non-negative sequences $x_n$ and $y_n$, we write $x_n = O(y_n)$ if there exist $N \in \mathbb{N}$ and $c > 0$ such that $x_n \leq c y_n$ for all $n \geq N$, and $x_n = o(y_n)$ (or $x_n \ll y_n$), if $x_n/y_n \to 0$, as $n \to \infty$. Let $\{X_n\}_{n\in\mathbb{N}}$ be a sequence of real-valued random variables on a probability space $(\Omega, \mathbb{P})$. If $c \in \mathbb{R}$ is a constant, we write $X_n \xrightarrow{p} c$ to denote that $X_n$ converges in probability to $c$. That is, for any $\epsilon > 0$, we have $\mathbb{P}(|X_n - c| > \epsilon) \to 0$ as $n \to \infty$. Let $\{a_n\}_{n\in\mathbb{N}}$ be a sequence of real numbers that tends to infinity as $n \to \infty$. We write $X_n = o_p(a_n)$, if $|X_n|/a_n$ converges to 0 in probability. Additionally, we write $X_n = O_p(a_n)$, to denote that for any positive sequence $\omega(n) \to \infty$, we have $\mathbb{P}(|X_n|/a_n \geq \omega(n)) = o(1)$. If $\mathcal{E}_n$ is a measurable subset of $\Omega$, for any $n \in \mathbb{N}$, we say that the sequence $\{\mathcal{E}_n\}_{n\in\mathbb{N}}$ occurs with high probability (w.h.p.) if $\mathbb{P}(\mathcal{E}_n) = 1 - o(1)$, as $n \to \infty$. Also, we denote by $\mathsf{Bin}(k, p)$ a binomial distribution corresponding to the number of successes of a sequence of $k$ independent Bernoulli trials each having probability of success

**Table 1** Expected costs associated with investing and not investing in security

| | Agent 2<br>0 | 1 |
|---|---|---|
| Agent 1 | | |
| 0 | $\big(\alpha_1 + (1-\alpha_1)\alpha_2\beta_1\big)\ell_1, \big(\alpha_2 + (1-\alpha_2)\alpha_1\beta_2\big)\ell_2$ | $(\alpha_1\ell_1, C + \alpha_1\beta_2\ell_2)$ |
| 1 | $(C + \alpha_2\beta_1\ell_1, \alpha_2\ell_2)$ | $(C, C)$ |

$p$. We will suppress the dependence of parameters on the size of the network $n$, if it is clear from the context.

## 2 Preliminaries

To illustrate the basic intuition in a simpler framework, this section provides two motivating examples for the network security game. First, the case of two agents is considered, followed by a simplified contagion process in the form of a contact process on infinite regular trees.

### 2.1 Optimal security investment for two agents

We first look at the optimal security investment game in the case of two agents $\mathcal{A} = \{1, 2\}$ sharing two links ($1 \to 2$ and $2 \to 1$). Assume that each agent has two security choices $\mathcal{S} = \{0, 1\}$: $s_i = 1$ if the agent $i$ invests in strong security (in this case, she never gets infected) and $s_i = 0$ if the agent $i$ does not invest in security and is subject to epidemic risk.

Table 1 summarizes the expected costs to the agents for the four possible outcomes: $\ell_i$ is the loss in case agent $i$ becomes infected, and $C = C_1$ is the cost of investing in security (level 1). If agent $i$ does not invest in security, there is a probability $\alpha_i$ that they become infected directly. On the other hand, $\beta_i$ denotes the probability of indirect contagion from the other agent. Let us make the example even simpler and assume that only direct loss can be avoided by investing in security.

We observe that investing in security is a dominant strategy for agent 1 if $C < \alpha_1\ell_1$ and

$$C + \alpha_2\beta_1\ell_1 < (\alpha_1 + (1-\alpha_1)\alpha_2\beta_1)\ell_1 \Longrightarrow C < \alpha_1(1-\alpha_2\beta_1)\ell_1.$$

Similarly, investing in security is a dominant strategy for agent 2 if $C < \alpha_2\ell_2$ and

$$C + \alpha_1\beta_2\ell_2 < (\alpha_2 + (1-\alpha_2)\alpha_1\beta_2)\ell_2 \Longrightarrow C < \alpha_2(1-\alpha_1\beta_2)\ell_2.$$

We conclude that if

$$C < \min\left\{\alpha_1(1-\alpha_2\beta_1)\ell_1, \alpha_2(1-\alpha_1\beta_2)\ell_2\right\},$$

then both agents will invest in self-protection, while if

$$C > \max\left\{\alpha_1\ell_1, \alpha_2\ell_2\right\},$$

then neither agent will want to invest in self-protection. In the case

$$\max\left\{\alpha_1(1-\alpha_2\beta_1)\ell_1, \alpha_2(1-\alpha_1\beta_2)\ell_2\right\} < C < \min\{\alpha_1\ell_1, \alpha_2\ell_2\},$$

there are two Nash equilibria, (0,0) and (1,1), and the solution to this game is indeterminate. In other cases, the agent with higher loss will invest in security, while the agent with lower loss will prefer not to invest.

### 2.2 Contact process on infinite regular trees

We now consider a set of infinitely many agents placed over an infinite directed regular tree with the same in-degree (denoted by $d^+$) and out-degree (denoted by $d^-$) satisfying $d^+ = d^- = d$. Let $\mathcal{S} = \{0, 1, \ldots, K\}$ be a finite ensemble of all possible security strategies for each agent, and, $\beta_0 > \beta_1 > \cdots > \beta_K$ be the infection probabilities over each directed edge depending on the security investment of the host agent. Further, let $\alpha_0 \geq \alpha_1 \geq \cdots \geq \alpha_K$ denote the initial exogenous infection probabilities.

Let $\gamma_0, \gamma_1, \ldots, \gamma_K \in [0, 1]$ with $\gamma_0 + \gamma_1 + \cdots + \gamma_K = 1$ be the fraction (probability) of agents invested in each security class. A simple argument shows that

$$g_s(x) := 1 - (1 - \alpha_s)\,(1 - \beta_s x)^d$$

is the probability that an agent invested in security class $s \in \mathcal{S}$ ever gets infected assuming each of its incoming neighbors are infected with probability $x$.

Assume that each agent $i$ faces a fixed potential loss $\ell_i$ in case they become infected. Investing in a higher security class decreases the infection probability but increases the cost. Let $C_s$ denote the cost of investing in security level $s$. So we can write the loss function for agent $i$ investing in security class $s \in \mathcal{S}$ as

$$J_i(s, \gamma) = \ell_i g_s(x_*^\gamma) + C_s,$$

where (by a simple recursive argument) $x_*^\gamma$ is the solution in [0,1] to the fixed point equation

$$x = \Phi^\gamma(x) := \sum_{s \in \mathcal{S}} \gamma_s g_s(x).$$

Note that $\Phi^\gamma(0) \geq 0$, $\Phi^\gamma(1) \leq 1$ and $\Phi^\gamma(x)$ is a strictly increasing function of $x$. Hence, in this case the fixed point solution is unique.

We call $x_*^\gamma$ the *global network vulnerability parameter* as it represents the fraction of infected links in the network. Obviously, this parameter also depends on the agents security strategies through $\gamma_0, \gamma_1, \ldots, \gamma_K$. In order to find out these quantities in equilibrium, let us denote by $\delta_s(x)$ the infection probability variation between security level $s$ and $s - 1$, i.e.,

$$\delta_s(x) := g_{s-1}(x) - g_s(x) = (1 - \alpha_s)\,(1 - \beta_s x)^d - (1 - \alpha_{s-1})\,(1 - \beta_{s-1} x)^d > 0,$$

so that each agent $i$ prefers security class $s$ over $s - 1$ if and only if

$$\ell_i > \ell_s(x) := \frac{C_s - C_{s-1}}{\delta_s(x)}.$$

As we will see later in Sect. 4, we will assume that the cost function is such that

$$\ell_1(x) \leq \ell_2(x) \leq \cdots \leq \ell_K(x),$$

for all $x \in [0, 1]$. Indeed, if $\ell_{s+1}(x) < \ell_s(x)$, the agent who believes in vulnerability $x$ will never invest in security class $s$ for any loss $\ell$: If $\ell < \ell_s(x)$, the agent prefers $s - 1$ over $s$, and if $\ell \geq \ell_s(x) > \ell_{s+1}(x)$, the agent prefers security $s + 1$ over $s$. In particular, the condition will be satisfied if $g_s(x)$ and $C_s$ are both (discrete) convex functions of $s$:

$$C_{s+1} + C_{s-1} \geq 2C_s, \quad \text{and} \quad g_{s+1}(x) + g_{s-1}(x) \geq 2g_s(x),$$

since in this case $\delta_s(x) = g_{s-1}(x) - g_s(x)$ will be a decreasing function of $s$.

Consider now a strictly increasing continuous loss distribution function $F$. Consequently, it yields that the fraction $\gamma_e^{(s)}$ of agents investing in security $s$ in equilibrium satisfies

$$\gamma_e^{(s)} = F(\ell_{s+1}(x_*^{\gamma_e})) - F(\ell_s(x_*^{\gamma_e})),$$

where $x_*^{\gamma_e}$ is the unique solution to the fixed point equation $x = \Phi^{\gamma_e}(x)$:

$$x = \sum_{s \in \mathcal{S}} \gamma_e^{(s)} g_s(x),$$

and, we set $\ell_{K+1}(x) = \infty$, $F(\ell_{K+1}(x)) = 1$ and $F(\ell_0(x)) = 0$. We will come back to this example later in Sect. 5.2 and investigate how the social optimum security strategies differ from the individual decisions.

## 3 Independent threshold model with security profiles

In this section, we provide our general framework for the study of contagion risks in random networks and state our main results on the asymptotic magnitude of contagion. We will also provide a resilience condition for the large network to small initial shocks and show how the bailout and intervention by a planner (government) could change the results and make the network more resilient. These results are prerequisites for the analysis of the security game in the next section.

### 3.1 Contagion risk model

Consider a directed graph $G = (V, E)$ where $V = [n] := \{1, 2, \ldots, n\}$ is the set of $n$ vertices (agents). We study the independent threshold model with security investment, in which a vertex's threshold is drawn independently from a distribution which depends on the vertex's degrees and its security investment. More precisely, we consider a finite ensemble of security classes $\mathcal{S}$. We use the notations $\mathbf{s} = (s_1, s_2, \ldots, s_n)$ and $\mathbf{s}_{-i} = (s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_n)$ to denote the security profiles of all agents and all agents other than $i$ respectively.

The contagion process under the threshold model is a diffusion process that starts with a set $\mathcal{I}_0^{(\mathbf{s})} \subseteq V$ consisting of initially infected vertices, while every other vertex is uninfected. For each vertex $i \in V$ with security level $s \in \mathcal{S}$, we assign a (random) threshold $\Theta_i^{(s)} \in \mathbb{N}$ representing its capacity to resist infection from incoming neighbors. We denote by $p^{(s)}(d^+, d^-, \theta)$ the probability that a vertex with in-degree $d^+$, out-degree $d^-$ and investing in security class $s$ becomes infected after (exactly) $\theta$ of its incoming neighbors are infected:

$$p^{(s)}(d^+, d^-, \theta) := \mathbb{P}(\Theta_i^{(s)} = \theta),$$

for agent $i$ with degrees $(d^+, d^-)$ and investing in security class $s \in \mathcal{S}$.

The contagion process starts from $\mathcal{I}_0^{(\mathbf{s})}$ and continues progressively by rounds. In round $k \geq 1$, the contagion reaches a set

$$\mathcal{I}_k^{(\mathbf{s})} := \left\{ i \in V \mid \Theta_i^{(s_i)} \leq \#\{j \in \mathcal{I}_{k-1}^{(\mathbf{s})}, (j, i) \in E\} \right\}.$$

This is repeated until no more vertices become infected. Note that the set of final infected vertices depend on the security investment across all agents. The final infected set is denoted

by $\mathcal{I}_f^{(\mathbf{s})}$. We now provide few important classes of contagion models which can be seen as a special case of our general framework.

***Example 3.1*** (Independent cascade models) The cascade model has been extensively used for modeling the spread of infectious diseases, computer viruses, diffusion of innovation, and marketing. For example, consider the SIR (susceptible-infected-removed) epidemic model in which sites (vertices) begin as susceptible, and after being infected, they become removed, i.e., become immune to further infection. Let $\alpha_s$ denote the initial infection probability, and $\beta_s$ denote the probability of getting infected from each incoming neighbor if the host vertex invests in security (immunization) class $s$. It is easy to show that the above independent cascade model corresponds to the independent threshold model by setting

$$p^{(s)}(d^+, d^-, 0) = \alpha_s \quad \text{and} \quad p^{(s)}(d^+, d^-, \theta) = (1-\alpha_s)\beta_s(1-\beta_s)^{\theta-1},$$

for all $d^+, d^- \in \mathbb{N}$ and $\theta = 1, \ldots, d^+$.

***Example 3.2*** (Bootstrap percolation model) In the case where

$$p^{(s)}(d^+, d^-, 0) = \alpha_s, \quad p^{(s)}(d^+, d^-, \theta) = (1-\alpha_s)\mathbb{1}_{\{\theta=\theta_s\}},$$

our model is equivalent to the bootstrap percolation process for each security class $s$. This process (as well as numerous extensions and variations) has been used as a model to describe various complex phenomena in different areas. A short survey regarding its applications can be found in [3]. Several quantitative characteristics of bootstrap percolation, particularly the dependence of the initially infected set on the final infected set, have been studied on a variety of random graphs [6, 9, 10, 16, 33].

***Example 3.3*** (Linear threshold model) The linear threshold model has been extensively used in the literature, particularly to model neuronal activity [4, 22] and default contagion in financial networks [5, 7, 11, 27]. In this model, see e.g. [34], the edge weights $(L_{ij})$ denote the liability (influence) that agent $i$ has on agent $j$ and $C_i = C_i^{(s)}$ represents the capacity (capital or threshold) for agent $i$ to absorb the losses (influences) from incoming neighbors before becoming infected. At every time step, each agent $i$ computes the total incoming weight from all infected neighbors, and if the sum exceeds the threshold $C_i^{(s)}$, they become infected and remain so forever. For each $i \in \mathbb{N}$, let $\{L_{\ell,i}\}_{\ell=1}^{\infty}$ be a sequence of i.i.d. random variables. For a vertex $i$ with degree $(d^+, d^-)$, by setting

$$p^{(s)}(d^+, d^-, \theta) = \mathbb{P}(\Theta_i^{(s)} = \theta) = \mathbb{P}\left(\sum_{\ell=1}^{\theta-1} L_{\ell,i} \le C_i^{(s)} < \sum_{\ell=1}^{\theta} L_{\ell,i}\right), \tag{1}$$

all our results will be applicable to the linear threshold model with i.i.d. random weights.

### 3.2 The directed configuration model

We represent the underlying network as a set of vertices $[n] := \{1, 2, \ldots, n\}$, endowed with a sequence of in-degrees $\mathbf{d}^+ := \{d_i^+\}_{i\in[n]}$ and a sequence of out-degrees $\mathbf{d}^- := \{d_i^-\}_{i\in[n]}$. Naturally, the degrees should satisfy the condition that $\sum_{i=1}^n d_i^+ = \sum_{i=1}^n d_i^-$, in order for a graph with in- and out-degree sequence $(\mathbf{d}^+, \mathbf{d}^-)$ to exist. A vertex $i \in [n]$, with degree $(d_i^+, d_i^-)$ is assigned $d_i^+$ in-coming half edges and $d_i^-$ out-going half edges, and the condition above ensures that in total there are as many in-coming half edges as there are out-going half edges. The configuration model with given directed degree sequence $(\mathbf{d}^+, \mathbf{d}^-)$ is defined as

the multigraph resulting from the uniform random matching of the in-coming half edges and the out-going half edges [19, 43]. This graph is denoted by $\mathcal{G} = \mathcal{G}(\mathbf{d}^+, \mathbf{d}^-)$ and we write $(i, j) \in \mathcal{G}$ for the event that there is a directed link from $i$ to $j$. Although self-loops may occur, these become rare as $n \to \infty$. It is easy to see that, conditional on the multigraph being simple graph, we obtain a uniformly distributed random graph with these given degree sequences; see e.g., [43].

We now describe the regularity assumptions on vertex degrees under the security profile $\mathbf{s}_n = (s_1, s_2, \ldots, s_n)$. For each $n \in \mathbb{N}$ we have a degree sequence $(\mathbf{d}_n^+, \mathbf{d}_n^-)$ and security profile $\mathbf{s}_n = (s_1, s_2, \ldots, s_n)$, but (to lighten notation) this dependency on $n$ will not be carried in the notation. The empirical distribution of the degrees is denoted by $\mu_n$ which is given by

$$\mu_n^{(s)}(d^+, d^-) := \frac{1}{n} \sum_{i=1}^{n} \mathbb{1}_{\{d_i^+ = d^+, d_i^- = d^-, s_i = s\}}. \tag{2}$$

We assume that the sequence $(\mathbf{d}^+, \mathbf{d}^-, \mathbf{s})$ satisfies the following regularity conditions:

**Condition 3.4** (Degree regularity conditions) *We say that the sequence* $(\mathbf{d}^+, \mathbf{d}^-, \mathbf{s})$ *satisfies the regularity conditions if for some probability distribution* $\mu : \mathbb{N}^2 \times \mathcal{S} \to [0, 1]$*, independent of n, the following holds:*

*(C*$_1$*) for every* $d^+, d^- \in \mathbb{N}$ *and* $s \in \mathcal{S}$*, as* $n \to \infty$

$$\mu_n^{(s)}(d^+, d^-) \to \mu^{(s)}(d^+, d^-);$$

*(C*$_2$*) The average degree* $\lambda := \sum_{j=0}^{\infty} \sum_{k=0}^{\infty} \sum_{s \in \mathcal{S}} j \mu^{(s)}(j, k) \in (0, \infty)$ *and as* $n \to \infty$

$$\sum_{j=0}^{\infty} \sum_{k=0}^{\infty} \sum_{s \in \mathcal{S}} j \mu_n^{(s)}(j, k) \to \lambda.$$

We end this section by the following remark:

***Remark 3.5*** We state our results for the random multigraph $\mathcal{G}(\mathbf{d}^+, \mathbf{d}^-)$ constructed by configuration model. However, they could be transferred by conditioning on the multigraph being a simple graph (without loop and multiples edges). The resulting random graph, denoted by $\mathcal{G}^*(\mathbf{d}^+, \mathbf{d}^-)$, will be uniformly distributed among all directed graphs with the same degrees sequence. In order to transfer the results, we would need to assume that the degree distribution has a finite second moment, i.e.

$$\sum_{j=0}^{\infty} \sum_{k=0}^{\infty} \sum_{s \in \mathcal{S}} (j + k)^2 \mu^{(s)}(j, k) \in (0, \infty),$$

which from [30] implies that the probability that $\mathcal{G}(\mathbf{d}^+, \mathbf{d}^-)$ is simple being bounded away from zero as $n \to \infty$. However, as stated also in [32], we suspect that all results hold even without the second moment assumption for simple random graph $\mathcal{G}^*(\mathbf{d}^+, \mathbf{d}^-)$. In [20], the authors have recently shown results for the size of the giant component from the multigraph case without using the second moment assumption; they prove that even with the (exponentially) small probability that the multigraph is simple, the error probabilities are even smaller.

### 3.3 Limit theorems and the resilience conditions

We let $p^{(s)}(d^+, d^-, 0)$ the probability that agent $i \in [n]$ with degree $(d^+, d^-)$ and investing in security $s \in \mathcal{S}$ is initially infected:

$$p^{(s)}(d^+, d^-, 0) = \mathbb{P}(i \in \mathcal{I}_0^{(\mathbf{s})} \mid s_i = s, d_i^+ = d^+, d_i^- = d^-).$$

Let us denote by $\mathcal{I}_f^{(s)}(d^+, d^-)$ the set of finally infected agents with degrees $(d^+, d^-)$ and security level $s \in \mathcal{S}$.

We define the function $\Phi^{(\mathbf{s})} : [0, 1] \to [0, 1]$ as

$$\Phi^{(\mathbf{s})}(x) := \sum_{j=0}^{\infty} \sum_{k=0}^{\infty} \sum_{s \in \mathcal{S}} \frac{k\mu^{(s)}(j,k)}{\lambda} \sum_{\theta=0}^{j} p^{(s)}(j,k,\theta)\mathbb{P}(\mathsf{Bin}(j,x) \geq \theta), \tag{3}$$

and let $x_*^{(\mathbf{s})}$ be the smallest fixed point of $\Phi^{(\mathbf{s})}$ in $[0, 1]$. Note that $\Phi^{(\mathbf{s})}$ admits at least one fixed point since it is a continuous increasing function, $\Phi^{(\mathbf{s})}(1) \leq 1$ and $\Phi^{(\mathbf{s})}(0) \geq 0$.

We can interpret $x_*^{(\mathbf{s})}$ as the probability that an incoming neighbor of a randomly chosen agent gets infected during the contagion process. The intuition behind Eq. (3) is the as follows: The incoming neighbor of a randomly chosen agent has in-degree $j$, out-degree $k$, and security $s$ with the size-biased distribution $\frac{k\mu^{(s)}(j,k)}{\lambda}$. Moreover, they will have threshold $\theta$ with probability $p^{(s)}(j, k, \theta)$ and they will get infected if at least $\theta$ of their incoming neighbors are infected (each independently with probability $x_*^{(\mathbf{s})}$).

Our first theorem concerns the limit theorem for the final number of infected agents when the number of initially infected agents is macroscopic:

**Theorem 3.6** *Consider a sequence of random graphs $\mathcal{G}(\mathbf{d}^+, \mathbf{d}^-)$ and security profiles $\mathbf{s}$ satisfying Condition 3.4 and let $x_*^{(\mathbf{s})}$ be the smallest fixed point of $\Phi^{(\mathbf{s})}$ in $[0, 1]$. We have for all $\epsilon > 0$ w.h.p.*

$$\frac{|\mathcal{I}_f^{(\mathbf{s})}|}{n} \geq \sum_{j,k} \sum_{s \in \mathcal{S}} \mu^{(s)}(j,k) \sum_{\theta=0}^{j} p^{(s)}(j,k,\theta)\mathbb{P}(\mathsf{Bin}(j, x_*^{(\mathbf{s})}) \geq \theta) - \epsilon.$$

*Moreover,*

- *if $x_*^{(\mathbf{s})} = 1$ then w.h.p. almost all vertices become infected: $|\mathcal{I}_f| = n - o_p(n)$;*
- *if $x_*^{(\mathbf{s})} < 1$ and furthermore $x_*^{(\mathbf{s})}$ is a stable fixed point of $\Phi^{(\mathbf{s})}$ (i.e., $\Phi^{(\mathbf{s})}(x) < x$ for $x \in (x_*^{(\mathbf{s})}, x_*^{(\mathbf{s})} + \epsilon)$ and $\epsilon > 0$ small enough), then*

$$\frac{|\mathcal{I}_f^{(\mathbf{s})}|}{n} \xrightarrow{p} \psi(x_*^{(\mathbf{s})}) := \sum_{j,k} \sum_{s \in \mathcal{S}} \mu^{(s)}(j,k) \sum_{\theta=0}^{j} p^{(s)}(j,k,\theta)\mathbb{P}(\mathsf{Bin}(j, x_*^{(\mathbf{s})}) \geq \theta),$$

*and,*

$$\frac{|\mathcal{I}_f^{(s)}(d^+, d^-)|}{n\mu_n^{(s)}(d^+, d^-)} \xrightarrow{p} \psi^{(s)}(d^+, d^-, x_*^{(\mathbf{s})}) := \sum_{\theta=0}^{j} p^{(s)}(d^+, d^-, \theta)\mathbb{P}(\mathsf{Bin}(d^+, x_*^{(\mathbf{s})}) \geq \theta).$$

The theorem extends the result in [7] by allowing for different agent types (securities) distributions. The proof of the theorem is provided in Appendix A.3.

Our next theorem concerns the case with few initially infective agents, i.e. $|\mathcal{I}_0^{(\mathbf{s})}| = o(n)$. As a corollary of Theorem 3.6, we have:

**Theorem 3.7** *Consider a random graph* $\mathcal{G}(\mathbf{d}^+, \mathbf{d}^-)$ *and a security profile* $\mathbf{s}$ *satisfying Condition 3.4. If there exists* $x_0 > 0$ *such that for all* $0 < x < x_0$,

$$x > \sum_{j,k} \sum_{s\in\mathcal{S}} \frac{k\mu^{(s)}(j,k)}{\lambda} \sum_{\theta=1}^{j} p^{(s)}(j,k,\theta)\mathbb{P}(\mathsf{Bin}(j,x) \geq \theta),$$

*and we initially infect randomly* $|\mathcal{I}_0^{(\mathbf{s})}| = o(n)$ *vertices in* $[n]$, *then* $|\mathcal{I}_f^{(\mathbf{s})}| = o_p(n)$.

Further, as a corollary of the above theorem, we have the following result, which generalizes the resilience condition of [7] by allowing for different agent types.

Let us define

$$\mathcal{R}_0^{(\mathbf{s})} := \frac{1}{\lambda} \sum_{j,k\in\mathbb{N}} \sum_{s\in\mathcal{S}} jk\mu^{(s)}(j,k)p^{(s)}(j,k,1). \tag{4}$$

We denote by $\mathcal{S}_1$ to be the largest strongly connected component of the random graph $\mathcal{G}(\mathbf{d}^+, \mathbf{d}^-)$ on which we apply the site percolation process by removing all vertices with threshold $\Theta_i \geq 2$. Let $\mathcal{I}_f^{(\mathbf{s})}(i)$ denote the final infected set when the epidemic is initiated from vertex $i \in [n]$, under the security profile $\mathbf{s}$.

**Theorem 3.8** *Consider a random graph* $\mathcal{G}(\mathbf{d}^+, \mathbf{d}^-)$ *and a security profile* $\mathbf{s}$ *satisfying Condition 3.4.*

- *If* $\mathcal{R}_0^{(\mathbf{s})} < 1$,

$$\sum_{j,k} \sum_{s\in\mathcal{S}} jk\mu^{(s)}(j,k) < \infty$$

  *and we initially infect randomly* $|\mathcal{I}_0^{(\mathbf{s})}| = o(n)$ *vertices in* $[n]$, *then* $|\mathcal{I}_f^{(\mathbf{s})}| = o_p(n)$.
- *If* $\mathcal{R}_0^{(\mathbf{s})} > 1$ *then w.h.p. for any* $i \in \mathcal{S}_1$,

$$\liminf_n \frac{|\mathcal{I}_f^{(\mathbf{s})}(i)|}{n} \geq \liminf_n \frac{|\mathcal{S}_1|}{n} > 0.$$

The proof of the theorem is provided in Appendix A.6. It is worth noting that the above resilience condition requires $\sum_{j,k}\sum_{s\in\mathcal{S}} jk\mu^{(s)}(j,k) < \infty$. In [7], this is implied by the condition of finite second-order moment for the degree distribution. Thus, under the resilience condition and assuming that $\sum_{j,k} jk\mu(j,k) < \infty$, the infection amplification is finite. However, if

$$\sum_{j,k} \sum_{s\in\mathcal{S}} jk\mu^{(s)}(j,k) = \infty,$$

which is the case for many real-world networks, a small fraction of initially infected agents can still trigger a large cascade under certain conditions. This is the object of a new result in this paper, which we state below.

Consider the case when $\sum_{j,k}\sum_{s\in\mathcal{S}} jk\mu^{(s)}(j,k) = \infty$. Suppose that there is a positive fraction of vertices with a finite threshold and at the same time with a large number of in- and out-degrees. These vertices will amplify the initial infections: their large number of incoming links will likely be connected to multiple initially infected vertices, and thus these vertices will reach their infection threshold. Moreover, these vertices have a large out-degree, and thus they will increase the rate of the epidemic's spread. The following theorem is another corollary of Theorem 3.6.

**Theorem 3.9** *Consider a random graph $\mathcal{G}(\mathbf{d}^+, \mathbf{d}^-)$ and a security profile* **s** *satisfying Condition 3.4. Assume that a small fraction $\epsilon > 0$ of all vertices represent the initial seed, i.e.,*

$$\sum_{j,k}\sum_{s\in\mathcal{S}} \mu^{(s)}(j,k)p^{(s)}(j,k,0) = \epsilon.$$

*If there exists $x_0 > 0$ such that for all $0 < x < x_0$,*

$$x < \sum_{j,k}\sum_{s\in\mathcal{S}} \frac{k\mu^{(s)}(j,k)}{\lambda} \sum_{\theta=1}^{j} p^{(s)}(j,k,\theta)\mathbb{P}(\mathsf{Bin}(j,x) \geq \theta),$$

*then with high probability (for all $\epsilon > 0$)*

$$\frac{|\mathcal{I}_f^{(s)}|}{n} > \psi(x_0) > 0.$$

The following corollary shows a discontinuity at 0 for the final size of the infected agents when the degree distribution is heavy-tailed, such as in scale-free networks.

**Corollary 3.10** *Assume that for some $K \in \mathbb{N}$, $c \in \mathbb{R}^+$ and $\chi \in (2,3)$:*

$$\sum_{k\in\mathbb{N}}\sum_{s\in\mathcal{S}}\sum_{\theta=1}^{K} k\mu^{(s)}(j,k)p^{(s)}(j,k,\theta) \geq cj^{-\chi+1}$$

*for all $j \in \mathbb{N}$. Consider a small fraction $\epsilon > 0$ of all vertices represent the initial seed, i.e.,*

$$\sum_{j,k}\sum_{s\in\mathcal{S}} \mu^{(s)}(j,k)p^{(s)}(j,k,0) = \epsilon.$$

*Then there exists $\hat{x} > 0$ the smallest positive solution of*

$$x = \sum_{j,k}\sum_{s\in\mathcal{S}}\sum_{\theta\geq 1} \frac{k\mu^{(s)}(j,k)}{\lambda} p(j,k,\theta)\mathbb{P}(\mathsf{Bin}(j,x) \geq \theta) \tag{5}$$

*such that for all $\epsilon > 0$, with high probability*

$$0 < \psi(\hat{x}) < \frac{|\mathcal{I}_f^{(s)}|}{n} < \psi(\hat{x}) + 2\epsilon.$$

The proof of above corollary is provided in Appendix A.4. This shows that the final size of the cascade has a jump discontinuity at 0 when the degree distribution is heavy-tailed and the condition

$$\sum_{k\in\mathbb{N}}\sum_{s\in\mathcal{S}}\sum_{\theta=1}^{K} k\mu^{(s)}(j,k)p^{(s)}(j,k,\theta) \geq cj^{-\chi+1}$$

holds for all $j \in \mathbb{N}$. In particular, this condition implies that (since $\chi \in (2,3)$),

$$\sum_{j,k}\sum_{s\in\mathcal{S}} jk\mu^{(s)}(j,k) \geq c\sum_{j} j^{-\chi+2} = \infty.$$

The interest of this result lies in the case $K > 1$, since when $K = 1$, we already know from Theorem 3.8 that with this condition $\mathcal{R}_0^{(\mathbf{s})} > 1$, and the network is not resilient. Note that

in the fixed-point equation (5), the threshold runs over $\theta \geq 1$, contrary to the fixed point of the function $\Phi^{(\mathbf{s})}$ in Theorem 3.6. Corollary 3.10 states that as the fraction of vertices with $\theta = 0$ tends to zero, the number of vertices that become infected (which have a threshold $\theta > 0$) represents a positive fraction of the system. We also give a precise value for this final fraction of infected vertices.

### 3.4 Targeting interventions

In this section, we consider a social planner (lender of last resort or government) who seeks to intervene and make the network (which is initially subject to an exogenous shock) resilient, by targeting the most central players. Note that the interventions are based on the partial information of the network (based on the degrees and security class of each agent). The complete information setup has been studied in various papers, see e.g., [15, 28, 34–36].

We assume that the planner's intervention could be either saving (vulnerable) links in the network or saving (defaulting/infected) agents based on their degrees and security classes. We denote by $(1 - \pi_e) \in [0, 1]$ the fraction of links saved by the planner, i.e., $\pi_e$ denotes the fraction of remaining links in the network. Further, for a given function $\pi_v : \mathbb{N}^2 \times \mathcal{S} \to [0, 1]$, we denote by $(1 - \pi_v^{(s)}(d^+, d^-))$ the fraction of agents with degree $(d^+, d^-)$ and invested in security class $s \in \mathcal{S}$ saved (bailed out) by the planner.

The above intervention model is equivalent to considering contagion in the percolated random graph, where we first generate the random graph $\mathcal{G}(\mathbf{d}^+, \mathbf{d}^-)$ using the configuration model and then randomly delete either vertices or edges based on the given intervention policy (since saved links and agents will not play any role in the contagion process). We denote this percolated random graph by $\mathcal{G}_{\pi_v,\pi_e}(\mathbf{d}^+, \mathbf{d}^-)$. Specifically, each edge of $\mathcal{G}(\mathbf{d}^+, \mathbf{d}^-)$ is deleted with probability $1 - \pi_e$ and each agent with degree $(d^+, d^-)$ and invested in security $s$ is removed from the network with probability $1 - \pi_v^{(s)}(j, k)$. Consider now the independent threshold model on the percolated random graph $\mathcal{G}_{\pi_v,\pi_e}(\mathbf{d}^+, \mathbf{d}^-)$.

**Theorem 3.11** *Consider $\mathcal{G}_{\pi_v,\pi_e}(\mathbf{d}^+, \mathbf{d}^-)$ and suppose that Condition 3.4 holds. Let $x_*^{(\mathbf{s})}$ be the smallest fixed point in [0,1] of*

$$\Phi^{(\mathbf{s})}_{\pi_v,\pi_e}(x) := \sum_{j,k} \sum_{s\in\mathcal{S}} \frac{k\mu^{(s)}(j,k)\pi_v^{(s)}(j,k)}{\lambda} \sum_{\theta=0}^{j} p^{(s)}(j,k,\theta)\mathbb{P}(\mathsf{Bin}(j, x\pi_e) \geq \theta).$$

*If $x_*^{(\mathbf{s})} < 1$ and furthermore $x_*^{(\mathbf{s})}$ is a stable fixed point of $\Phi^{(\mathbf{s})}_{\pi_v,\pi_e}$, then*

$$\frac{|\mathcal{I}_f^{(\mathbf{s})}|}{n} \xrightarrow{p} \sum_{j,k} \sum_{s\in\mathcal{S}} \mu^{(s)}(j,k)\pi_v^{(s)}(j,k) \sum_{\theta=0}^{j} p^{(s)}(j,k,\theta)\mathbb{P}(\mathsf{Bin}(j, x_*^{(\mathbf{s})}\pi_e) \geq \theta),$$

*and,*

$$\frac{|\mathcal{I}_f^{(s)}(d^+,d^-)|}{n\mu_n^{(s)}(d^+,d^-)\pi_v^{(s)}(d^+,d^-)} \xrightarrow{p} \sum_{\theta=0}^{j} p^{(s)}(d^+,d^-,\theta)\mathbb{P}(\mathsf{Bin}(d^+, x_*^{(\mathbf{s})}\pi_e) \geq \theta).$$

The proof of theorem is provided in Appendix A.5

We now investigate how the interventions could make the network resilient. Let us denote by $\tilde{\mathcal{S}}_1$ the largest strongly connected component of the percolated random graph $\mathcal{G}_{\pi_v,\pi_e}(\mathbf{d}^+, \mathbf{d}^-)$ (network after interventions) on which we apply (another) site percolation by removing all vertices with threshold $\Theta_i \geq 2$.

**Theorem 3.12** *Consider $\mathcal{G}_{\pi_v,\pi_e}(\mathbf{d}^+,\mathbf{d}^-)$ and suppose that Condition 3.4 holds. We have:*

*(i) If $\sum_{j,k,s} jk\mu^{(s)}(j,k) < \infty$ and*

$$\pi_e < \pi_e^* := \frac{\lambda}{\sum_{j,k,s} jk\mu^{(s)}(j,k)\pi_v^{(s)}(j,k)p^{(s)}(j,k,1)},$$

*then the network is resilient, i.e., if we we start by initially infecting (randomly) $|\mathcal{I}_0^{(\mathbf{s})}| = o(n)$ vertices in $[n]$, then $|\mathcal{I}_f^{(\mathbf{s})}| = o_p(n)$.*

*(ii) If $\pi_e > \pi_e^*$, then w.h.p. for any $i \in \tilde{\mathcal{S}}_1$,*

$$\liminf_n \frac{|\mathcal{I}_f^{(\mathbf{s})}(i)|}{n} \geq \liminf_n \frac{|\tilde{\mathcal{S}}_1|}{n} > 0.$$

The proof of theorem is provided in Appendix A.6. The theorem characterizes the critical value of the bond percolation parameter (fraction of vulnerable links saved by the planner) required to make the network resilient. Note that if $\pi_e^* > 1$, then the network is already resilient under the site percolation (agents bailout by the planner).

## 4 Network security games

In this section, we study the network security game and provide sufficient conditions for the uniqueness of an (asymptotic) Nash equilibrium.

***Remark 4.1*** For the financial applications, considering the linear threshold model of Example 3.3, the threshold represents the liquidity or capital to absorb incoming losses from the defaulted neighbors (creditors). In this case, the security class could represent the quality of a firms' assets in terms of liquidity and capital charges. A firm with more liquid assets will then have higher Tier 1 capital. In this case, instead of security classes, we can introduce different asset liquidity classes, so that agents (banks) choose optimally their asset liquidity classes. Our results could be easily transferred to this case.

### 4.1 Contagion risks model

We consider a network security game introduced and motivated in Sect. 2. We assume that agent $i$ can obtain a security level $s \in \mathcal{S} := \{0, 1, \ldots, K\}$ for a cost $C_i^{(s)} = C^{(s)}(d_i^+, d_i^-)$, and faces a potential loss $\ell_i$ in case it becomes infected. It is natural to assume that:

($C_3$) For all vertices the threshold is stochastically increasing with the security investment i.e., for any agent with degrees $(d^+, d^-)$ and for $s < s'$ we have for all $k \in \mathbb{N}$,

$$\sum_{\theta=0}^{k} p^{(s)}(d^+, d^-, \theta) > \sum_{\theta=0}^{k} p^{(s')}(d^+, d^-, \theta). \tag{6}$$

On the other hand, we assume that investing in a higher security class increases the cost and thus $C_i^{(s)}$ is strictly increasing in $s$.

The timeline is as follows: agents learn their potential loss in case they become infected. This is their private information, but the distribution of losses, denoted by $F$, is common knowledge. Agents then decide on their security level. They draw a threshold $\theta$ from a

distribution that increases stochastically with their security investment and depends on their degree. Agents that have a threshold of zero are initially infected and trigger a cascade of infections. This is equivalent to the random attack model, in which the attacker targets and infects each agent based on their degree and security level (see, e.g., [2]).

We assume that agents are risk neutral, so in the network of size $n$, we can write the payoff of vertex $i$ as

$$J_i(\boldsymbol{\ell}, \mathbf{s}) = J_i(\ell_1, \ldots, \ell_n, s_1, \ldots, s_n) := \ell_i \mathbb{P}_n(i \in \mathcal{I}_f^{(\mathbf{s})}) + C_i^{(s_i)},$$

where $\mathbb{P}_n(i \in \mathcal{I}_f^{(\mathbf{s})})$ is over the distribution of the random graph $\mathcal{G}(\mathbf{d}^+, \mathbf{d}^-)$ of size $n$ and random thresholds, given all vertices' degrees, losses and investment security vector $\mathbf{s}$.

We say that a security investment across agents $\mathbf{s}^* = (s_1^*, s_2^*, \ldots, s_n^*)$ is a (pure-strategy) *Nash equilibrium* if

$$s_i^* \in \arg\min_{s \in \mathcal{S}} J_i(\ell_1, \ldots, \ell_n, s_1^*, \ldots, s_{i-1}^*, s, s_{i+1}^*, \ldots, s_n^*),$$

for all $i \in [n]$.

Similarly, a security profile $\mathbf{s}^* = (s_1^*, s_2^*, \ldots, s_n^*)$ is a *social optimum* if for all $\mathbf{s} \in \mathcal{S}^n$,

$$\sum_{i=1}^{n} J_i(\boldsymbol{\ell}, \mathbf{s}^*) \leq \sum_{i=1}^{n} J_i(\boldsymbol{\ell}, \mathbf{s}).$$

### 4.2 Conditions for monotone investment

Consider a sequence of random graphs $\mathcal{G}(\mathbf{d}^+, \mathbf{d}^-)$ and security profiles $\mathbf{s}$ satisfying Condition 3.4. According to Theorem 3.6, see also the proof in Appendix A.3, we know that $x_*^{(\mathbf{s})}$ is the ratio of infected edges among all the edges. We call this parameter the global vulnerability of the network and securities. Then, for a given random network with vulnerability $x$, a representative agent with degrees $(d^+, d^-)$ and security $s$ will become infected and faces losses $\ell$ with (asymptotic) probability

$$\psi^{(s)}(d^+, d^-, x) := \sum_{\theta=0}^{d^+} p^{(s)}(d^+, d^-, \theta) \mathbb{P}(\mathsf{Bin}(d^+, x) \geq \theta).$$

Consequently, under the network vulnerability parameter $x \in [0, 1]$, the agent's optimal security investment shall be the value $s^*(x)$ satisfying

$$s^*(x) \in \arg\min_{s \in \mathcal{S}} \left\{ \ell \psi^{(s)}(d^+, d^-, x) + C^{(s)}(d^+, d^-) \right\}.$$

This can be interpreted as an *asymptotic Nash equilibrium* with respect to the representative agent's optimal security investment when the global network vulnerability $x$ summarizes the impact of all individuals' optimal security strategies and degrees distribution. This is a fixed point problem that will be described in the following.

In particular, the representative agent prefers the security class $s$ over a lower security class $s-1$ if and only if

$$\ell \left( \psi^{(s-1)}(d^+, d^-, x) - \psi^{(s)}(d^+, d^-, x) \right) > C^{(s)}(d^+, d^-) - C^{(s-1)}(d^+, d^-).$$

Note also that

$$\delta_s(d^+, d^-, x) := \psi^{(s-1)}(d^+, d^-, x) - \psi^{(s)}(d^+, d^-, x)$$

$$= \sum_{\theta=0}^{d^+} \left( p^{(s-1)}(d^+, d^-, \theta) - p^{(s)}(d^+, d^-, \theta) \right) \mathbb{P}(\mathsf{Bin}(d^+, x) \geq \theta)$$
$$= \sum_{\theta=0}^{d^+} q_s(d^+, d^-, \theta) \mathbb{P}(\mathsf{Bin}(d^+, x) = \theta) > 0,$$

since by Condition $(C_3)$,

$$q_s(d^+, d^-, \theta) := \sum_{j=0}^{\theta} \left( p^{(s-1)}(d^+, d^-, j) - p^{(s)}(d^+, d^-, j) \right) > 0.$$

In order to restrict ourselves to threshold-type strategies, we need a stronger assumption. Specifically, let us define for $k = 1, 2, \ldots, K$:

$$\ell_s(d^+, d^-, x) := \frac{C^{(s)}(d^+, d^-) - C^{(s-1)}(d^+, d^-)}{\delta_s(d^+, d^-, x)}, \tag{7}$$

so that the representative agent with degrees $(d^+, d^-)$ would prefer the security class $s$ over $s-1$ if and only if $\ell > \ell_s(d^+, d^-, x)$.

$(C_4)$ We assume in the following that for all $d^+, d^- \in \mathbb{N}$ and $x \in [0, 1]$,

$$\ell_1(d^+, d^-, x) < \ell_2(d^+, d^-, x) < \cdots < \ell_K(d^+, d^-, x).$$

Under this condition, the optimal agent's security investment is threshold-type: invest in security class $k$ if and only if $\ell \in (\ell_k, \ell_{k+1}]$ (we set $\ell_{K+1} = \infty$). Note that the above condition is automatically verified for the case with only two security strategies, i.e., $\mathcal{S} = \{0, 1\}$.

On the other hand, we will also need to assume that such thresholds are (strictly) decreasing with the network vulnerability level $x$:

$(C_5)$ For all $d^+, d^- \in \mathbb{N}$, $s \in \mathcal{S}$ and $x \in [0, 1]$, the threshold function $\ell_s(d^+, d^-, x)$ is a decreasing function of $x$.

The above monotone investment condition states that the level of loss where agents choose to invest in higher security class is lower when the network vulnerability is higher. The higher the global network vulnerability, the more agents invest in security.

**Lemma 4.2** *The monotone investment condition* $(C_5)$ *holds if and only if for all* $d^+, d^- \in \mathbb{N}$, $s \in \mathcal{S}$ *and* $x \in [0, 1]$,

$$\sum_{\theta=1}^{d^+} \left( p^{(s-1)}(d^+, d^-, \theta) - p^{(s)}(d^+, d^-, \theta) \right) \mathbb{P}(\mathsf{Bin}(d^+ - 1, x) = \theta - 1) > 0.$$

The proof of lemma is provided in Appendix A.7. Consequently, the above lemma implies that if

$$p^{(s-1)}(d^+, d^-, \theta) > p^{(s)}(d^+, d^-, \theta)$$

for all $\theta < d^+$, then the monotone investment condition will be held. In particular, when we consider the strong versus weak protection setting in Sect. 5.1, the above condition will be held since $\mathcal{S} = \{0, 1\}$ and the agent investing in security will never get infected, i.e., $p^{(1)}(d^+, d^-, \theta) = 0$. Therefore, the condition in the lemma will be satisfied.

### 4.3 Asymptotic Nash equilibrium analysis

We are now ready to describe the asymptotic Nash equilibrium as a fixed point problem. In the previous section we described the agents' strategy given the global network vulnerability. Let $x_e$ denote the expected network vulnerability (expected ratio of infected links among all the links) of the random network under expected security investments across all agents.

The representative agent with degrees $(d^+, d^-)$ would invest in the security class $s \in \mathcal{S}$ if and only if

$$\ell_s(d^+, d^-, x_e) < \ell \leq \ell_{s+1}(d^+, d^-, x_e).$$

Hence, the fraction of agents with degrees $(d^+, d^-)$ investing in security class $s = 0, 1, \ldots, K$ will be (set $F(\ell_{K+1}) = 1$)

$$\gamma_e^{(s)}(d^+, d^-) = F(\ell_{s+1}(d^+, d^-, x_e)) - F(\ell_s(d^+, d^-, x_e)),$$

and we have

$$\mu_e^{(s)}(d^+, d^-) = \mu(d^+, d^-)\gamma_e^{(s)}(d^+, d^-).$$

On the other hand, given the probability distributions $\gamma_e : \mathbb{N}^2 \to \mathcal{P}(\mathcal{S})$, following Theorem 3.6, a vertex $i$ with degrees $(d^+, d^-)$ will invest in security class $s \in \mathcal{S}$ as long as

$$\ell_s(d^+, d^-, x_*^{\gamma_e}) < \ell_i \leq \ell_{s+1}(d^+, d^-, x_*^{\gamma_e}),$$

where $x_*^{\gamma_e}$ is the smallest fixed point of

$$\Phi^{\gamma_e}(x) := \sum_{j,k} \sum_{s \in \mathcal{S}} \frac{k\mu(j,k)\gamma_e^{(s)}(j,k)}{\lambda} \sum_{\theta=0}^{j} p^{(s)}(j,k,\theta)\mathbb{P}(\mathsf{Bin}(j,x) \geq \theta), \tag{8}$$

in $[0, 1]$. Hence, the actual fraction of vertices with degree $(d^+, d^-)$ investing in security class $s \in \mathcal{S}$ is given by

$$\gamma^{(s)}(d^+, d^-) = F(\ell_{s+1}(d^+, d^-, x_*^{\gamma_e})) - F(\ell_s(d^+, d^-, x_*^{\gamma_e})). \tag{9}$$

Then for $s = K$, we have

$$\ell_K(d^+, d^-, x_*^{\gamma_e}) = F^{-1}\Big(1 - \gamma^{(K)}(d^+, d^-)\Big),$$

and, by backward induction, we obtain for $s = 1, \ldots, K$:

$$\ell_s(d^+, d^-, x_*^{\gamma_e}) = F^{-1}\left(1 - \gamma^{(K)}(d^+, d^-) - \cdots - \gamma^{(s)}(d^+, d^-)\right) = F^{-1}\left(\sum_{k=0}^{s-1} \gamma^{(k)}(d^+, d^-)\right).$$

The willingness to pay to move from security class $s-1$ to $s$ for the last vertex with degrees $(d^+, d^-)$ in a network with fraction investing in security $\gamma$ and with expectation $\gamma_e$ can be defined as

$$W_{\gamma,\gamma_e}^{(s)}(d^+, d^-) := \delta_s(d^+, d^-, x_*^{\gamma_e})F^{-1}\left(\sum_{k=0}^{s-1} \gamma^{(k)}(d^+, d^-)\right). \tag{10}$$

For a fixed cost function $C : \mathcal{S} \times \mathbb{N}^2 \to \mathbb{R}^+$, in equilibrium, the expected fraction $\gamma_e$ and the actual one $\gamma$ must satisfy (for all $d^+, d^-$ with $\mu(d^+, d^-) > 0$):

$$C^{(s)}(d^+, d^-) - C^{(s-1)}(d^+, d^-) = \delta_s(d^+, d^-, x_*^{\gamma_e}))F^{-1}\left(\sum_{k=0}^{s-1} \gamma^{(k)}(d^+, d^-)\right).$$

Hence in equilibrium, when expectations are fulfilled, the possible equilibria are given by the fixed point equations (for all $d^+, d^-$ with $\mu(d^+, d^-) > 0$)

$$\ell_s(d^+, d^-, x_*^{\gamma}) = F^{-1}\left(\sum_{k=0}^{s-1} \gamma^{(k)}(d^+, d^-)\right), \tag{11}$$

where $x_*^{\gamma}$ is the smallest fixed point in $[0, 1]$ of equation

$$\Phi^{\gamma}(x) := \sum_{j,k}\sum_{s\in\mathcal{S}} \frac{k\mu(j,k)\gamma^{(s)}(j,k)}{\lambda} \sum_{\theta=0}^{j} p^{(s)}(j,k,\theta)\mathbb{P}(\mathsf{Bin}(j,x) \geq \theta). \tag{12}$$

### 4.4 Uniqueness of equilibrium

For any $z \in [0, 1]$, $(d^+, d^-) \in \mathbb{N}^2$ and $s \in \mathcal{S}$, following Eq. (11), we define

$$\gamma^{(s)}(d^+, d^-, z) = F(\ell_{s+1}(d^+, d^-, z)) - F(\ell_s(d^+, d^-, z)),$$

and we set

$$\Phi^{\gamma(z)}(x) := \sum_{j,k}\sum_{s\in\mathcal{S}} \frac{k\mu(j,k)\gamma^{(s)}(j,k,z)}{\lambda} \sum_{\theta=0}^{j} p^{(s)}(j,k,\theta)\mathbb{P}(\mathsf{Bin}(j,x) \geq \theta).$$

In the following theorem, we show the uniqueness of the (asymptotic) Nash equilibrium for the security mean-field game under monotone investment conditions.

**Theorem 4.3** *Consider the network security game in a random graph $\mathcal{G}(\mathbf{d}^+, \mathbf{d}^-)$. Assume that $(C_1)$–$(C_5)$ hold. We have at most one mean-field equilibrium, which is given by the solution of the following equation:*

$$z = \inf_{x\in[0,1]}\{x : \Phi^{\gamma(z)}(x) = x\}. \tag{13}$$

The proof of theorem is provided in Appendix A.8.

### 4.5 Algorithms to find the fixed point

In this section, we present an iterative algorithm to compute the mean-field equilibrium in Theorem 4.3 for our baseline model. We assume that the degrees are bounded from above by $\Delta$. Note that, by Condition 3.4, one can always choose $\Delta = \Delta_\epsilon$ such that

$$\sum_{j=0}^{\infty}\sum_{k=\Delta_\epsilon}^{\infty}\sum_{s\in\mathcal{S}} j\mu^{(s)}(j,k) + \sum_{j=\Delta_\epsilon}^{\infty}\sum_{k=0}^{\infty}\sum_{s\in\mathcal{S}} j\mu^{(s)}(j,k) < \epsilon.$$

.

Under the assumptions of Theorem 4.3, the following algorithm is guaranteed to converge to the unique fixed point of the mapping $\Phi^{\gamma}$.

**Step 0:** For initialization set $t = 0$, the error tolerance $\epsilon > 0$ and $\gamma_0^{(s)}(j,k) = \mathbf{1}_{\{s=0\}}$ for all $0 \le j,k \le \Delta$. Let $x_0$ be the smallest solution $x \in [0,1]$ of the fixed-point iteration algorithm with error tolerance $\epsilon$ given by

$$\Phi_0(x) := \sum_{j=0}^{\Delta}\sum_{k=0}^{\Delta}\sum_{s\in\mathcal{S}} \frac{k\mu(j,k)\gamma_0^{(s)}(j,k)}{\lambda} \sum_{\theta=0}^{j} p^{(s)}(j,k,\theta)\mathbb{P}(\mathsf{Bin}(j,x) \ge \theta)$$
$$= \sum_{j=0}^{\Delta}\sum_{k=0}^{\Delta} \frac{k\mu(j,k)}{\lambda} \sum_{\theta=0}^{j} p^{(0)}(j,k,\theta)\mathbb{P}(\mathsf{Bin}(j,x) \ge \theta).$$

This is the fixed-point equilibrium under no security investment.

**Step 1:** Set $t \leftarrow t+1$. For all $0 \le j,k \le \Delta$, we set the fraction of agents with degrees $(j,k)$ investing in security $s \in \mathcal{S}$ at step $t$ to

$$\gamma_t^{(s)}(j,k) := F(\ell_{s+1}(j,k,x_{t-1})) - F(\ell_s(j,k,x_{t-1})),$$

and let $x_t$ be the smallest fixed-point $x \in [0,1]$ of

$$\Phi_t(x) := \sum_{j=0}^{\Delta}\sum_{k=0}^{\Delta}\sum_{s\in\mathcal{S}} \frac{k\mu(j,k)\gamma_t^{(s)}(j,k)}{\lambda} \sum_{\theta=0}^{j} p^{(s)}(j,k,\theta)\mathbb{P}(\mathsf{Bin}(j,x) \ge \theta).$$

**Step 2:** If $x_{t-1} - x_t < \epsilon$, terminate the algorithm. Otherwise, return to Step 1.

Note that due to the monotone investment conditions and the strictly increasing cdf function $F$, $\Phi_t(x)$ is strictly increasing in $x$ and strictly decreasing in $t$ (see Appendix A.8). Hence, the fixed-point sequence $x_t$ will be decreasing, converging to $x_*^{(\mathbf{s})}$, which is unique by Theorem 4.3. Since $x_t$ is non-increasing and the algorithm terminates when $x_{t-1} - x_t < \epsilon$, the algorithm converges in at most $\lfloor x_0/\epsilon \rfloor$ steps.

## 5 Examples and applications

In this section, we provide a more detailed analysis of the particular case where there are two security classes, and investment in security provides strong protection. For the case of random regular graphs and core-periphery network models, the social optimum is explicit, and we can theoretically guarantee that the individual decision will result in underinvestment compared to the social optimum.

### 5.1 Equilibrium analysis in the case of strong protection

We assume $\mathcal{S} = \{0,1\}$ and consider the (extreme) case where a vertex invested in security cannot be infected at all, i.e. $p^{(1)}(j,k,\theta) = 0$ and $p^{(0)}(j,k,\theta) = p(j,k,\theta)$ for all $j,k,\theta$. Namely, $s_i = 0$ if vertex $i$ does not invest in security (i.e. $C_i^{(0)} = 0$) and $s_i = 1$ if vertex $i$ invests in security. An agent $i$ with degrees $(d^+,d^-)$ can obtain a security level 1 for a cost $C_i = C(d^+,d^-)$. Let $\gamma(d^+,d^-)$ denotes the fraction of vertices (in equilibrium) with degrees $(d^+,d^-)$ invested in security. Hence, all vertices investing in security can be removed from the network and contagion goes through all non secured vertices. This is similar to site percolation model by setting $\pi_v^{(s)}(d^+,d^-) = 1 - \gamma(d^+,d^-)$.

Note that in this setting, the conditions $(C_3) - (C_5)$ are automatically satisfied (see the remark after Lemma 4.2). Hence, the optimal decision for a vertex $i$ with degrees $(d^+, d^-)$ and expected vulnerability belief for the network $x_e$ is

$$\ell_i \sum_{\theta} p(d^+, d^-, \theta)\mathbb{P}(\mathsf{Bin}(d^+, x_e) \geq \theta) > C(d^+, d^-) \iff \text{agent} i \text{invests in security.}$$

The equilibrium fixed point equations can be simplified to

$$\gamma(d^+, d^-) = 1 - F\left(\frac{C(d^+, d^-)}{\sum_{\theta} p(d^+, d^-, \theta)\mathbb{P}(\mathsf{Bin}(d^+, x_*^{\gamma}) \geq \theta)}\right),$$

where $x_*^{\gamma}$ is the smallest fixed point in $[0, 1]$ of equation

$$\Phi^{\gamma}(x) := \sum_{j,k} \frac{k\mu(j,k)(1-\gamma(j,k))}{\lambda} \sum_{\theta=0}^{j} p(j,k,\theta)\mathbb{P}(\mathsf{Bin}(j,x) \geq \theta).$$

### 5.2 Equilibrium analysis in the case of random regular graphs

We next consider the previous strong protection setting in the case of random regular graphs, where $d_i^+ = d_i^- = d$ for all vertices $i \in [n]$. Hence, $\mu(d,d) = 1, \lambda = d$, and we simplify the notations to

$$p(\theta) = p^{(0)}(d,d,\theta), \gamma = \gamma(d,d), C = c(d,d),$$

and

$$\delta(x) = \delta_1(d,d,x) = \sum_{\theta=0}^{d} p(\theta)\mathbb{P}(\mathsf{Bin}(d,x) \geq \theta).$$

Consequently in this case the optimal decision for agent $i$ and expected global network vulnerability belief $x_e$ is

$$\ell_i > \frac{C}{\delta(x_e)} \iff \text{agent} i \text{invests in security.}$$

The equilibrium fixed point equations can be simplified as follows:

$$1 - \gamma = F\left(\frac{C}{\delta(x_*^{\gamma})}\right) = F\left(\frac{C}{x_*^{\gamma}(1-\gamma)}\right) \Longrightarrow C = x_*^{\gamma}(1-\gamma)F^{-1}(1-\gamma),$$

where $x_*^{\gamma}$ is the smallest fixed point in $[0, 1]$ of equation

$$\Phi^{\gamma}(x) := (1-\gamma)\sum_{\theta=0}^{d} p(\theta)\mathbb{P}(\mathsf{Bin}(d,x) \geq \theta) = F\left(\frac{C}{\delta(x)}\right)\delta(x).$$

In this case, the social utility averaged over all agents converges to

$$\frac{1}{n}\sum_{i=1}^{n} J_i(\boldsymbol{\ell}, \mathbf{s}) \xrightarrow{p} \bar{J}_{\text{social}}(\gamma) = \delta(x_*^{\gamma}) \int_{\gamma}^{1} F^{-1}(1-u)du + C\gamma,$$

where $\delta(x_*^{\gamma}) \int_0^{\gamma} F^{-1}(1-u)du$ is the (expected) gross cost imposed by the $(1-\gamma)$-fraction of agents not investing in security and $C\gamma$ is the total cost of security.

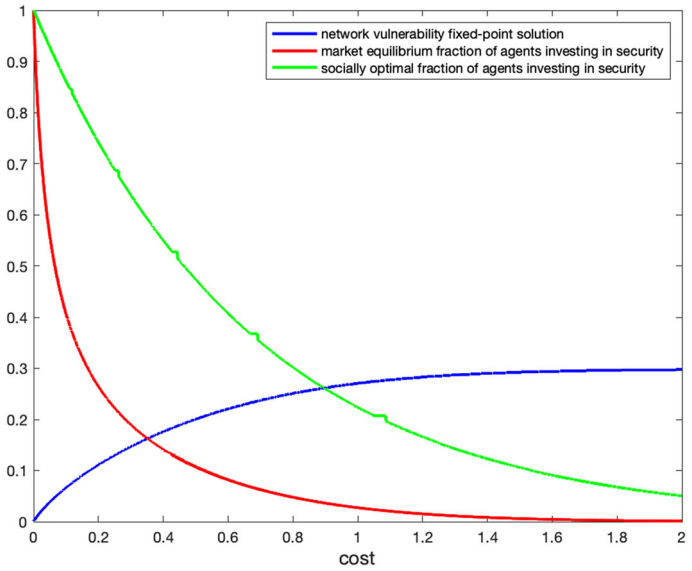


**Fig. 1** Equilibrium solutions for contact process on random regular graphs: Here $d = 10$, $p(0) = \alpha$, $p(\theta) = (1-\alpha)\beta(1-\beta)^{\theta-1}$ for $\theta = 1, \ldots, d$, with $\alpha = 0.05$, $\beta = 0.1$ and $L$ follows an exponential distribution with mean one, i.e. $F(\ell) = 1 - e^{-\ell}$

**Proposition 5.1** *The social planner will choose a larger fraction $\gamma$ of agents to invest in security than the market equilibrium for any fixed cost $C$.*

The proof of proposition is provided in Appendix A.9.

Figure 1 varies the cost $C$. As the cost function increases, the network vulnerability fixed point solution increases, while the final fraction of individuals investing in security decreases. The figure also shows the gap between the fraction of individuals who self-protect in equilibrium and the social optimum.

### 5.3 Analysis of agents heterogeneity: Core-periphery setup

Financial networks often involve significant asymmetries, such as the presence of a core-periphery structure. In order to provide more insights on the impact of network heterogeneity and how agents influence each other, we consider a special case where there are two types of agents: core agents with high degrees $d_H^+ = d_H^- = d_H$ and periphery agents with low degrees $d_L^+ = d_L^- = d_L < d_H$. We denote by $\mu_H$ and $\mu_L$ (respectively) the fraction of core agents and periphery agents in the (large) network. We assume that the cost of (strong) self-protection for core agents is $C_H$ and the loss due to being infected follows distribution $F_H$. Similarly, for a periphery agent, the cost is $C_L < C_H$ and the loss follows distribution $F_L$. We also set

$$p_H(\theta) = p^{(0)}(d_H, d_H, \theta) \quad \text{and} \quad p_L(\theta) = p^{(0)}(d_L, d_L, \theta).$$

A core agent $i$ will invest in security (with expected network vulnerability $x_e$) if

$$\ell_i > \frac{C_H}{\delta_H(x_e)}, \ \delta_H(x) = \sum_{\theta=0}^{d_H} p_H(\theta)\mathbb{P}(\mathsf{Bin}(d_H, x) \geq \theta),$$

while a periphery agent $i$ will invest in security in the case

$$\ell_i > \frac{C_L}{\delta_L(x_e)},\ \delta_L(x) = \sum_{\theta=0}^{d_L} p_L(\theta)\mathbb{P}(\mathsf{Bin}(d_L, x) \geq \theta).$$

Hence, the (asymptotic) fraction of core agents $\gamma_H$ and periphery agents $\gamma_L$ investing in security satisfies the equilibrium fixed point equations

$$\gamma_H = 1 - F_H\left(\frac{C_H}{\delta_H(x_*^\gamma)}\right),\ \ \gamma_L = 1 - F_L\left(\frac{C_L}{\delta_L(x_*^\gamma)}\right),$$

where $x_*^\gamma$ is the smallest fixed point in $[0, 1]$ of equation

$$\Phi^\gamma(x) := \frac{d_H\mu_H(1-\gamma_H)\delta_H(x) + d_L\mu_L(1-\gamma_L)\delta_L(x)}{d_H\mu_H + d_L\mu_L}.$$

In this case, the average social cost function $\frac{1}{n}\sum_{i=1}^n J_i(\boldsymbol{\ell}, \mathbf{s})$ converges to

$$\bar{J}_{\text{social}}(\gamma_H, \gamma_L) = \delta_H(x_*^\gamma)\int_{\gamma_H}^1 F_H^{-1}(1-u)du + \delta_H(x_*^\gamma)\int_{\gamma_L}^1 F_L^{-1}(1-u)du + C_H\gamma_H + C_L\gamma_L.$$

Similarly to Proposition 5.1, we have:

**Proposition 5.2** *The social planner will choose a larger fraction $\gamma$ of core and periphery agents investing in security than the market equilibrium for any fixed costs $C_H$ and $C_L$.*

The proof of proposition is provided in Appendix A.9.

Figure 2varies the cost for core $C_H$ and periphery $C_L$ agents and plots the fraction of core agents who invest in security against the fraction of peripheral agents who invest. The game's equilibrium decisions are symmetric for agents of the same type based on the loss function. As the cost for periphery agents increases, we note that their investment decreases and this decreases is most pronounced close to zero. This means, as soon as the cost becomes positive, the fraction of peripheral agents investing quickly decreases. For core agents, the slope at zero is much more pronounced. When the cost for both agents is low, both have large fractions investing in security. When the cost for peripheral is low and for core it is high, we see that peripheral agents invest even more. Essentially, because they anticipate underinvestment from the cores they protect themselves to the highest degree possible. Otherwise, the contagion risk from the highly connected cores is too high. It is the cores who are the free riders, and this is based on the implicit threat of the systemic risk they impose. When the cost is high for the peripherals and low for the cores, a high proportion of cores chooses to invest. Note that peripheral agents do not immediately become free riders even when their costs become high and all cores are invested. When the cost for peripheral agents is low and fixed, the fraction of cores investing in protection is not monotone in cost. This is because of the discontinuity of the fixed point solution as a function of initially self protected cores.

The above core-periphery example clearly shows that, in a general non-symmetric network, the security investment decisions of agents not only create positive externalities but are also strategic substitutes. This means that greater investment by one type of agent typically reduces the willingness for investment of other agents. Similarly, underinvestment by some agents will encourage over-investment by others.

In the case of introducing insurance to the model, as studied in e.g. [48], the combination of security investment and insurance raises the problem of moral hazard, in which agents covered by insurance may take fewer secure measures, or even falsify their loss.

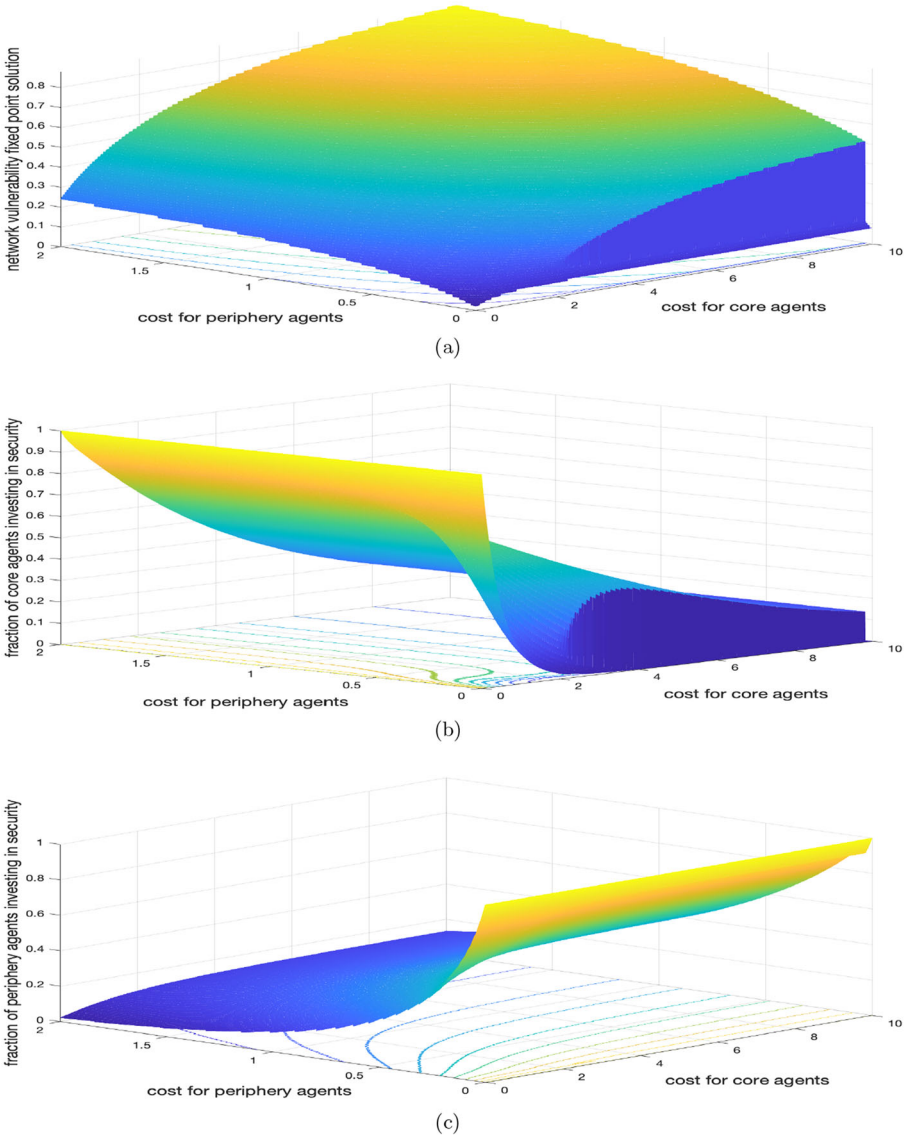


**Fig. 2** Equilibrium solutions for security investment in core-periphery networks: Here $\mu_H = 0.2, d_H = 20, p_H(0) = 0.1, p_H(5) = 0.9$ and $d_L = 4, \mu_L = 0.8, p_L(0) = 0.2, p_L(1) = 0.3, p_L(2) = 0.5$. Further, we set $F_L(\ell) = F_H(5\ell) = 1 - e^{-\ell}$; the (potential) infection loss for periphery and core agents follow exponential distributions with mean 1 and 5, respectively

## 6 Concluding remarks

In this paper, we propose a general framework for security investment in a directed network of interconnected agents subject to contagion risks and potential loss. We state various limit theorems and resilience conditions depending on network structure and agent security profile. We show how these results are sensitive to edge and vertex percolation. We study the

asymptotic Nash equilibrium and socially optimal security investments in a random directed network with fixed degrees. Our results allow us to understand how the structure of networks affects the resilience of the network and impacts the decisions of different network players. We show how an agent's decision on their security level might depend on the decision of other agents in the network. In particular, we quantify how agents who decide not to invest in security protection would put the other network participants at contagion risks.

When the agents' costs vary, the impact of the security choice on the overall system is ambiguous. When peripheral agents anticipate investment by cores, they do not completely decrease investment even when their costs increase. In contrast, cores can quickly become free-riders when their costs increase and when they anticipate investment by the periphery agents (for example because those agents have low costs). There are also non-monotonicities in the investment choices of the cores as a function of their costs. Our results point to a strong effect of the cost heterogeneity across classes of agents.

The model can be extended along the following directions.

Consider a strategic attacker which, after observing the degree and security profile of agents, selects an attack decision $\boldsymbol{\alpha}$, with

$$\alpha^{(s)}(d^+, d^-) = p^{(s)}(d^+, d^-, 0),$$

that represents the fraction of agents which are attacked and thus act as initial seed of the contagion. His objective is to maximize his utility given by the expected infections minus the cost of the attack decision. The cost of an attack can be captured in a simple way, for example

$$\zeta(\boldsymbol{\alpha}) = \sum_{d^+,d^-} \sum_{s\in\mathcal{S}} \mu^{(s)}(d^+, d^-)\zeta_s(\alpha^{(s)}(d^+, d^-)),$$

where $\zeta_s$ denotes the cost of initially infecting (attack) the fraction of individual with security $s \in \mathcal{S}$. This can turn into a attacker-defender game, if individuals take into account the possibility of strategic attack.

The model could also be applied to the insurance industry, where security investments can represent fraud detection capabilities. This means that firms with better security have a greater risk-bearing capacity than those with lower security.

Another area of interest is the cyber-insurance market. One can investigate how the presence of competitive insurers can affect security adoption. One problem with the combination of insurance and self-protection is moral hazard, which occurs when the insurance provider cannot observe the protection level of each agent [48]. The reward for a user investing in security depends on the general level of security in the network, leading to the following feedback loop situation [40]: self-protection $\longrightarrow$ state of the network $\longrightarrow$ pricing of the premium $\longrightarrow$ strategy of the agent $\longrightarrow$ self-protection. Note that if insurance providers cannot observe the security levels of the agents, there may be agents who choose not to invest in self-protection if the insurance covers part of their losses. Hence, insurance might provide a negative incentive for self-protection.

**Acknowledgements** I would like to thank Erhan Bayraktar and Andreea Minca for helpful discussions and the two anonymous reviewers for their useful comments and suggestions.

## Appendix A: Proofs

This appendix contains the proofs of all lemmas and theorems in the main text.

We start by describing the dynamics of the contagion on $\mathcal{G}_n = \mathcal{G}(\mathbf{d}_n^+, \mathbf{d}_n^-)$ as a Markov chain, which is perfectly tailored for asymptotic study. Let

$$m_n := \sum_{j,k} \sum_{s\in\mathcal{S}} j\mu_n^{(s)}(j,k) = \sum_{j,k} \sum_{s\in\mathcal{S}} k\mu_n^{(s)}(j,k)$$

denote the number of incoming (outgoing) edges in the graph.

### A.1. Markov chain transitions

Consider the configuration model algorithm described in Sect. 3.2. One can observe that the uniform matching which constructs the graph can be obtained sequentially: choose an outgoing half edge according to any rule (random or deterministic) and then choose the corresponding incoming half edge uniformly over the unmatched incoming half edges.

At time 0 the threshold of each agent is distributed randomly. For $\theta \in \mathbb{N}$, let $p_n^{(s)}(j,k,\theta)$ denotes the fraction of agents with in-degree $j$, out-degree $k$ and security profile $s$ which are given threshold $\theta$. Hence, $p_n^{(s)}(j,k,\theta) \to p^{(s)}(j,k,\theta)$ as $n \to \infty$. At a given time step $t$ agents (vertices) are partitioned into infected $\mathbb{I}(t)$ and uninfected $\mathbb{U}(t)$. We further partition the class of uninfected vertices according to their in-degree, out-degree, security profile and threshold $\mathbb{U}(t) = \bigcup_{j,k,s,\theta} \mathbb{U}^{jks\theta}(t)$.

At time zero, $\mathbb{I}(0)$ contains the initial set of infected agents. At each step we have one interaction only between two agents, yielding at least one infected. Our processes at each step is as follows:

- Choose an outgoing edge of an infected agent $i$;
- Identify its partner $j$ (i.e. by construction of the random graph in the configuration model, the partner is given by choosing an incoming edge randomly among all available incoming edges);
- Delete both edges. If $j$ is currently uninfected with threshold $\theta$ and it is the $\theta$-th deleted incoming edge from $j$, then $j$ fires.

Let us define $U_n^{jks\theta,\ell}(t)$, $0 \le \ell \le \theta$, the number of uninfected agents with in-degree $j$, out-degree $k$, security $s$, threshold $\theta$ and $\ell$ incoming edges from the infected agents at time $t$. We introduce the additional variables of interest:

- $I_n^{jks\theta}(t)$: the number of infected agents with in-degree $j$, out-degree $k$, security $s$ and threshold $\theta$ at time $t$,
- $I_n^-(t)$: the number of outgoing edges belonging to infected agents at time $t$,
- $I_n(t)$: the number of infected agents at time $t$.

Because at each step we delete one incoming edge and the number of incoming edges at time 0 is $m_n$, the number of existing incoming edges at time $t$ will be $m_n - t$. It is easy to see that the following identities hold:

$$\begin{aligned}
I_n^{jks\theta}(t) &= \mu_n^{(s)}(j,k)p_n^{(s)}(j,k,\theta) - \sum_{\ell=0}^{\theta-1} U_n^{jks\theta,\ell}(t),\\
I_n^-(t) &= \sum_{j,k} \sum_{s\in\mathcal{S}} \sum_{\theta=0}^{j} k I_n^{jks\theta}(t) - t,\\
I_n(t) &= \sum_{j,k} \sum_{s\in\mathcal{S}} \sum_{\theta=0}^{j} I_n^{jks\theta}(t).
\end{aligned}$$

The contagion process will finish at the stopping time $T_n$ which is the first time $t \in \mathbb{N}$ where $I_n^-(t) = 0$. The final number of infected agents will be $I_n(T_n)$. By definition of our process $\mathbf{U}_n(t) = \left\{U_n^{jks\theta,\ell}(t)\right\}_{j,k,s,\theta,\ell}$ represents a Markov chain. We write the transition probabilities of the Markov chain. There are three possibilities for the $B$, the partner of an outgoing edge of an infected agent $A$.

1. $B$ is infected, the next state is $\mathbf{U}_n(t+1) = \mathbf{U}_n(t)$.
2. $B$ is uninfected of in-degree $j$, out-degree $k$, security $s$, threshold $\theta$ and this is the $(\ell+1)$-th deleted incoming edge and $\ell + 1 < \theta$. The probability of this event is $\frac{(j-\ell)U_n^{jks\theta,\ell}(t)}{m_n - t}$. The changes for the next state will be
$$U_n^{jks\theta,\ell}(t+1) = U_n^{jks\theta,\ell}(t) - 1,$$
$$U_n^{jks\theta,\ell+1}(t+1) = U_n^{jks\theta,\ell+1}(t) + 1.$$
3. $B$ is uninfected of in-degree $j$, out-degree $k$, security $s$, threshold $\theta$ and this is the $\theta$-th deleted incoming edge. The probability of this event is $\frac{(j-\theta+1)U_n^{jks\theta,\theta-1}(t)}{m_n - t}$. The changes for the next state will be
$$U_n^{jks\theta,\theta-1}(t+1) = U_n^{jks\theta,\theta-1}(t) - 1.$$

Let $\Delta_t$ be the difference operator: $\Delta_t X := X(t+1) - X(t)$. We obtain the following equations for the expectation of $\mathbf{U}_n(t+1)$, conditional on $\mathcal{F}_{n,t}$ (the pairing generated by time $t$), by averaging over the possible transitions:

$$\begin{aligned}
\mathbb{E}\left[\Delta_t U_n^{jks\theta,0} | \mathcal{F}_{n,t}\right] &= -\frac{jU_n^{jks\theta,0}(t)}{m_n - t}, \\
\mathbb{E}\left[\Delta_t U_n^{jks\theta,\ell} | \mathcal{F}_{n,t}\right] &= \frac{(j-\ell+1)U_n^{jks\theta,\ell-1}(t)}{m_n - t} - \frac{(j-\ell)U_n^{jks\theta,\ell}(t)}{m_n - t}.
\end{aligned} \tag{14}$$

The initial condition is

$$U_n^{jks\theta,\ell}(0) = n\mu_n^{(s)}(j,k)p_n^{(s)}(j,k,\theta)\mathbb{1}(\ell = 0)\mathbb{1}(0 < \theta \leq j).$$

Remark that we are interested in the value of $I_n(T_n)$, where $T_n$ is the first time that $I_n(t) = 0$. In case $T_n < m_n$, the Markov chain can still be well defined for $t \in [T_n, m_n)$ by the same transition probabilities. However, after $T_n$ it will no longer be related to the contagion process and the value $I_n^-(t)$, representing for $t \leq T_n$ the number of in-coming half-edges belonging to infected agents, becomes negative. We consider from now on that the above transition probabilities hold for $t < m_n$.

We will show in the next section that the trajectory of these variables throughout the algorithm is a.a.s. (asymptotically almost surely, as $n \to \infty$ ) close to the solution of the deterministic differential equations suggested by these equations.

### A.2. Fluid limit of contagion process

Let (DE) be the following system of differential equations:

$$(u^{jks\theta,0})'(\tau) = -\frac{ju^{jks\theta,0}(\tau)}{\lambda - \tau},$$

$$(u^{jks\theta,\ell})'(\tau) = \frac{(j-\ell+1)u^{jks\theta,\ell-1}(\tau)}{\lambda-\tau} - \frac{(j-\ell)u^{jks\theta,\ell}(\tau)}{\lambda-\tau}, \qquad \text{(DE)},$$

with initial conditions

$$u^{jks\theta,\ell}(0) = \mu^{(s)}(j,k)p^{(s)}(j,k,\theta)\mathbb{1}(\ell=0)\mathbb{1}(0<\theta\le j).$$

**Lemma A.1** *The system of ordinary differential equations* (DE) *admits the unique solution*

$$\mathbf{u}(\tau) := \left\{u^{jks\theta,\ell}(\tau)\right\}_{j,k,s,0\le\ell<\theta\le j},$$

*in the interval* $0 \le \tau < \lambda$, *with*

$$u^{jks\theta,\ell}(\tau) := \mu^{(s)}(j,k)p^{(s)}(j,k,\theta)\binom{j}{\ell}(1-\frac{\tau}{\lambda})^{j-\ell}(\frac{\tau}{\lambda})^{\ell}. \tag{15}$$

***Proof*** We denote by $\mathrm{DE}_K$ the set of differential equations defined above, restricted to $j \wedge k < K$ and by $b_K$ the dimension of the restricted system. (The operator $\wedge$ is defined as $x \wedge y = \max(x, y)$.) Since the derivatives of the functions $\left\{u^{jks\theta,\ell}(\tau)\right\}_{j\wedge k<K,s,0\le\ell<\theta\le j}$ depend only on $\tau$ and the same functions, by a standard result in the theory of ordinary differential equations, there is an unique solution of $\mathrm{DE}_K$ in any domain of the type $(-\epsilon,\lambda)\times R$, with $R$ a bounded subdomain of $\mathbb{R}^{b_K}$ and $\epsilon > 0$. The solution of (DE) is defined to be the set of functions solving all the finite systems ($\mathrm{DE}_K$, $K \ge 1$). We solve now the system DE. Let $\gamma = \gamma(\tau) = -\ln(\lambda-\tau)$. Then $\gamma(0) = -\ln(\lambda)$, $\gamma$ is strictly monotone and so is the inverse function $\tau = \tau(\gamma)$. We write the system of differential equations (DE) with respect to $\gamma$:

$$\begin{aligned}(u^{jks\theta,0})'(\gamma) &= -ju^{jks\theta,0}(\gamma),\\ (u^{jks\theta,\ell})'(\gamma) &= (j-\ell+1)u^{jks\theta,\ell-1}(\gamma) - (j-\ell)u^{jks\theta,\ell}(\gamma).\end{aligned}$$

Then we have

$$\frac{d}{d\gamma}(u^{jks\theta,\ell+1}e^{(j-\ell-1)(\gamma-\gamma(0))}) = (j-\ell)u^{jks\theta,\ell}(\gamma)e^{(j-\ell-1)(\gamma-\gamma(0))},$$

and by induction, we find

$$u^{jks\theta,\ell}(\gamma) = e^{-(j-\ell)(\gamma-\gamma(0))}\sum_{r=0}^{\ell}\binom{j-r}{\ell-r}\left(1-e^{-(\gamma-\gamma(0))}\right)^{\ell-r}u^{jks\theta,r}(\gamma(0)).$$

By going back to $\tau$, we have

$$u^{jks\theta,\ell}(\tau) = (1-\frac{\tau}{\lambda})^{j-\ell}\sum_{r=0}^{\ell}u^{jks\theta,r}(0)\binom{j-r}{\ell-r}(\frac{\tau}{\lambda})^{\ell-r}.$$

Then, by using the initial conditions, we find (for $\theta > 0$)

$$u^{jks\theta,\ell}(\tau) = \mu^{(s)}(j,k)p^{(s)}(j,k,\theta)\binom{j}{\ell}(1-\frac{\tau}{\lambda})^{j-\ell}(\frac{\tau}{\lambda})^{\ell}.$$

□

A key idea to prove Theorem 3.6 is to approximate, following [47], the Markov chain by the solution of a system of differential equations in the large network limit. We summarize here the main result of [47].

For a set of variables $Y^1, \ldots, Y^b$ and for $\mathcal{D} \subseteq \mathbb{R}^{b+1}$, define the stopping time

$$T_{\mathcal{D}} = T_{\mathcal{D}}(Y^1, \ldots, Y^b) = \inf\{t \geq 1, (t/n; Y^1(t)/n, \ldots, Y^b(t)/n) \notin \mathcal{D}\}.$$

**Lemma A.2** [45, 47] *Given integers $b, n \geq 1$, a bounded domain $\mathcal{D} \subseteq \mathbb{R}^{b+1}$, functions $(f_\ell)_{1\leq\ell\leq b}$ with $f_\ell : \mathcal{D} \to \mathbb{R}$, and $\sigma$-fields $\mathcal{F}_{n,0} \subseteq \mathcal{F}_{n,1} \subseteq \ldots$, suppose that the random variables $\left(Y_n^\ell(t)\right)_{1\leq\ell\leq b}$ are $\mathcal{F}_{n,t}$-measurable for $t \geq 0$. Furthermore, assume that, for all $0 \leq t < T_{\mathcal{D}}$ and $1 \leq \ell \leq b$, the following conditions hold*

*(i)* (Boundedness). $\max_{1\leq\ell\leq b} |Y_n^\ell(t+1) - Y_n^\ell(t)| \leq \beta$,

*(ii)* (Trend-Lipschitz). $|\mathbb{E}[Y_n^\ell(t+1) - Y_n^\ell(t)|\mathcal{F}_{n,t}] - f_\ell(t/n, Y_n^1(t)/n, \ldots, Y_n^\ell(t)/n)| \leq \delta$, *where the function $(f_\ell)$ is L-Lipschitz-continuous on $\mathcal{D}$,*

*and that the following condition holds initially:*

*(iii)* (Initial condition). $\max_{1\leq\ell\leq b} |Y_n^\ell(0) - \hat{y}^\ell n| \leq \alpha n$, *for some $\left(0, \hat{y}^1, \ldots, \hat{y}^b\right) \in \mathcal{D}$.*

*Then there are $R = R(\mathcal{D}, L) \in [1, \infty)$ and $C = C(\mathcal{D}) \in (0, \infty)$ such that, whenever $\alpha \geq \delta \min\{C, L^{-1}\} + R/n$, with probability at least $1 - 2be^{-n\alpha^2/(8C\beta^2)}$ we have*

$$\max_{0\leq t\leq\sigma n} \max_{1\leq\ell\leq b} |Y_n^\ell(t) - y^\ell(t/n)n| < 3e^{CL}\alpha n,$$

*where $\left(y^\ell(t)\right)_{1\leq\ell\leq b}$ is the unique solution to the system of differential equations*

$$\frac{dy^\ell(t)}{dt} = f_\ell(t, y^1, \ldots, y^b) \text{ with } y^\ell(0) = \hat{y}^\ell, \text{ for } \ell = 1, \ldots, b,$$

*and $\sigma = \sigma(\hat{y}^1, \ldots, \hat{y}^b) \in [0, C]$ is any choice of $\sigma \geq 0$ with the property that $(t, y^1(t), \ldots, y^b(t))$ has $\ell^\infty$-distance at least $3e^{LC}\alpha$ from the boundary of $\mathcal{D}$ for all $t \in [0, \sigma)$.*

### A.3. Proof of Theorem 3.6

We apply Lemma A.2 to the contagion model described in Sect. A.1. Let us define, for $0 \leq \tau \leq \lambda$,

$$\eta^{jks\theta}(\tau) := \mu^{(s)}(j,k)p^{(s)}(j,k,\theta) - \sum_{\ell=0}^{\theta-1} u^{jks\theta,\ell}(\tau),$$

$$\eta^{-}(\tau) := \sum_{j,k}\sum_{s\in\mathcal{S}}\sum_{\theta=0}^{j} k\eta^{jks\theta}(\tau) - \tau, \text{ and}$$

$$\eta(\tau) := \sum_{j,k}\sum_{s\in\mathcal{S}}\sum_{\theta=0}^{j} \eta^{jks\theta}(\tau),$$

with $u^{jks\theta,\ell}$ given in Lemma A.1. With $\mathsf{Bin}(j, \pi)$ denoting a binomial variable with parameters $j$ and $\pi$, we have

$$\eta^{jks\theta}(\tau) = \mu^{(s)}(j,k)p^{(s)}(j,k,\theta)\mathbb{P}\left(\mathsf{Bin}(j, \frac{\tau}{\lambda}) \geq \theta\right), \tag{16}$$

$$\eta^{-}(\tau) = \sum_{j,k}\sum_{s\in\mathcal{S}} k\mu^{(s)}(j,k)\sum_{\theta=0}^{j} p^{(s)}(j,k,\theta)\mathbb{P}\left(\mathsf{Bin}(j, \frac{\tau}{\lambda}) \geq \theta\right) - \tau = \lambda\left(\Phi^{(\mathbf{s})}(\frac{\tau}{\lambda}) - \frac{\tau}{\lambda}\right),$$

(17)

and

$$\eta(\tau) = \sum_{j,k} \sum_{s\in\mathcal{S}} \mu^{(s)}(j,k) \sum_{\theta=0}^{j} p^{(s)}(j,k,\theta)\mathbb{P}\left(\mathsf{Bin}(j, \frac{\tau}{\lambda}) \geq \theta\right) = \psi(\frac{\tau}{\lambda}). \tag{18}$$

We now proceed to the proof of Theorem 3.6 whose aim is to approximate the value $I_n(T_n)/n$ as $n \to \infty$. We base the proof on Lemma A.2. We first need to bound the contribution of higher order terms in the infinite sums (17) and (18). Fix $\epsilon > 0$. By Condition 3.4,

$$\lambda := \sum_{j,k\in\mathbb{N}} \sum_{s\in\mathcal{S}} j\mu^{(s)}(j,k) = \sum_{j,k\in\mathbb{N}} \sum_{s\in\mathcal{S}} k\mu^{(s)}(j,k) < \infty$$

Then, there exists an integer $K_\epsilon$, such that

$$\sum_{k\geq K_\epsilon} \sum_{j,s} k\mu^{(s)}(j,k) + \sum_{j\geq K_\epsilon} \sum_{k} j\mu^{(s)}(j,k) < \epsilon,$$

which implies that

$$\sum_{j\wedge k\geq K_\epsilon} \sum_{s\in\mathcal{S}} k\mu^{(s)}(j,k) < \epsilon.$$

It follows that for all $0 \leq \tau \leq \lambda$,

$$\sum_{j\wedge k\geq K_\epsilon} \sum_{\theta=0}^{j} \sum_{s\in\mathcal{S}} k\mu^{(s)}(j,k)p^{(s)}(j,k,\theta)\mathbb{P}\left(\mathsf{Bin}(j, \frac{\tau}{\lambda}) \geq \theta\right) < \epsilon. \tag{19}$$

The number of vertices with degree $(j,k)$ and security $s$ is $n\mu_n^{(s)}(j,k)$. Again, by Condition 3.4,

$$\sum_{j,k} \sum_{s\in\mathcal{S}} k\mu_n^{(s)}(j,k) = \sum_{j,k} j\mu_n^{(s)}(j,k) \to \lambda \in (0,\infty).$$

Therefore, for $n$ large enough, $\sum_{j\wedge k\geq K_\epsilon} \sum_{s\in\mathcal{S}} k\mu_n^{(s)}(j,k) < \epsilon$, and for all $0 \leq t \leq m_n$,

$$\sum_{j\wedge k\geq K_\epsilon} \sum_{\theta=0}^{j} \sum_{s\in\mathcal{S}} kU_n^{jks\theta}(t)/n < \epsilon. \tag{20}$$

For $K \geq 1$, we denote

$$\mathbf{y}^K := \left(u^{jks\theta,\ell}(\tau)\right)_{j\wedge k<K,\ s\in\mathcal{S},\ 0\leq\ell<\theta\leq j} \text{ and}$$
$$Y_n^K := \left(U_n^{jks\theta,\ell}(\tau)\right)_{j\wedge k<K,\ s\in\mathcal{S},\ 0\leq\ell<\theta\leq j},$$

both of dimension $b(K)$, and $\eta^{jks\theta}(\tau)$, $u^{jks\theta,\ell}(\tau)$ are solutions to a system (DE) of ordinary differential equations. Let

$$x_*^{(\mathbf{s})} = \min\{x \in [0,1] : \Phi^{(\mathbf{s})}(x) = x\}.$$

For the arbitrary constant $\epsilon > 0$ fixed above, we define the domain $\mathcal{D}_\epsilon$ as

$$D_\epsilon = \{\left(\tau, y^{K_\epsilon}\right) \in \mathbb{R}^{b(K_\epsilon)+1} \ : \ -\epsilon < \tau < \lambda - \epsilon \ , \ -\epsilon < u^{jks\theta,\ell} < 1\}. \tag{21}$$

The domain $\mathcal{D}_\epsilon$ is a bounded open set which contains the support of all initial values of the variables. Each variable is bounded by a constant times $n$ ($C_0 = 1$). By the definition of our process, the Boundedness condition is satisfied with $\beta = 1$. The second condition of the theorem is satisfied by some $\delta_n = O(1/n)$. Finally the Lipschitz property is also satisfied since $\lambda - \tau$ is bounded away from zero. Then by Lemma A.2 and by convergence of initial conditions, we have:

**Lemma A.3** *For a sufficiently large constant C, we have*

$$\mathbb{P}(\forall t \le n\sigma_H(n), \mathbf{Y}_n^{K_\epsilon}(t) = n\mathbf{y}^{K_\epsilon}(t/n) + O(n^{3/4})) = 1 - O(b(K_\epsilon)n^{-1/4}\exp(-n^{-1/4})) \tag{22}$$

*uniformly for all $t \le n\sigma_H(n)$ where*

$$\sigma_H(n) = \sup\{\tau \ge 0, d(\mathbf{y}^{K_\epsilon}(\tau), \partial D_\epsilon) \ge Cn^{-1/4}\}.$$

When the solution reaches the boundary of $\mathcal{D}_\epsilon$, it violates the first constraint, determined by $\hat{\tau} = \lambda - \epsilon$. By convergence of $\frac{m_n}{n}$ to $\lambda$, there is a value $n_0$ such that $\forall n \ge n_0$, $\frac{m_n}{n} > \lambda - \epsilon$, which ensures that $\hat{\tau}n \le m_n$. Using (19) and (20), we have, for $0 \le t \le n\hat{\tau}$ and $n \ge n_0$:

$$\begin{aligned}
\left|I_n^-(t)/n - \eta^-(t/n)\right| &= \left|\sum_{j,k}\sum_{s\in\mathcal{S}}\sum_{\theta=0}^{j} k(I_n^{jks\theta}(t)/n - \eta^{jks\theta}(t/n))\right| \\
&\le \sum_{j,k}\sum_{s\in\mathcal{S}}\sum_{\theta=0}^{j} k\left|I_n^{jks\theta}(t)/n - \eta^{jks\theta}(t/n)\right| \\
&\le \sum_{j\wedge k\le K_\epsilon}\sum_{s\in\mathcal{S}}\sum_{\theta=0}^{j} k\left|I_n^{jks\theta}(t)/n - \eta^{jks\theta}(t/n)\right| + 2\epsilon,
\end{aligned} \tag{23}$$

and

$$|I_n(t)/n - \eta(t/n)| \le \sum_{j\wedge k\le K_\epsilon}\sum_{s\in\mathcal{S}}\sum_{\theta=0}^{j}\left|I_n^{jks\theta}(t)/n - \delta^{jks\theta}(t/n)\right| + 2\epsilon. \tag{24}$$

We obtain by Lemma A.3 that

$$\sup_{t\le\hat{\tau}n}\left|I_n^-(t)/n - \eta^-(t/n)\right| \le 2\epsilon + o_p(1), \text{ and} \tag{25}$$

$$\sup_{t\le\hat{\tau}n}|I_n(t)/n - \eta(t/n)| \le 2\epsilon + o_p(1). \tag{26}$$

We now study the stopping time $T_n$ and the size of the contagion $I_n(T_n)$. First assume $I(x) > x$ for all $x \in [0, 1)$, i.e., $x_*^{(\mathbf{s})} = 1$. Then we have for all $\tau < \hat{\tau}$

$$\eta^-(\tau) = \sum_{j,k}\sum_{s\in\mathcal{S}}\sum_{\theta=0}^{j} k\eta^{jks\theta}(\tau) - \tau > 0.$$

Then we have that $T_n/n = \hat{\tau} + O(\epsilon) + o_p(1)$ and from convergence (26), since $\delta(\hat{\tau}) = 1 - O(\epsilon)$, we obtain by tending $\epsilon$ to 0 that

$$|D_n(T_n)| = n - o_p(n).$$

This proves the first part of the theorem.

Now consider the case $x_*^{(\mathbf{s})} < 1$, and furthermore $x_*^{(\mathbf{s})}$ is a stable fixed point of $\Phi^{(\mathbf{s})}(x)$. Then by definition of $x_*^{(\mathbf{s})}$ and by using the fact that $\Phi^{(\mathbf{s})}(1) \leq 1$, we have $\Phi^{(\mathbf{s})}(x) < x$ for some interval $(x_*^{(\mathbf{s})}, x_*^{(\mathbf{s})} + \tilde{x})$. Then $\eta^-(\tau)$ is negative in an interval $(\tau_*, \tau_* + \tilde{\tau})$, with $\tau_* = \lambda x_*^{(\mathbf{s})}$. Let $\epsilon$ such that $2\epsilon < -\inf_{\tau \in (\tau_*, \tau_* + \tilde{\tau})} \eta^-(\tau)$ and denote $\hat{\sigma}$ the first iteration at which it reaches the minimum. Since $\eta^-(\hat{\sigma}) < -2\epsilon$ it follows that with high probability $I^-(\hat{\sigma}n)/n < 0$, so $T_n/n = \tau_* + O(\epsilon) + o_p(1)$. The Theorem 3.6 thus follows by taking the limit $\epsilon \to 0$.

### A.4. Proof of Corollary 3.10

Let $x_*^{(\mathbf{s})}(\epsilon)$ be the smallest fixed point of $\Phi^{(\mathbf{s})}$ in $[0, 1]$, when a fraction $\epsilon$ of all vertices represent fundamental defaults, i.e., this is the smallest solution in $[0, 1]$ to the fixed point equation

$$x = \Phi_\epsilon^{(\mathbf{s})}(x) := \epsilon + \sum_{j,k} \sum_{s \in \mathcal{S}} \sum_{\theta \geq 1} \frac{k\mu^{(s)}(j,k)}{\lambda} p^{(s)}(j,k,\theta) \mathbb{P}(\mathsf{Bin}(j,x) \geq \theta).$$

Further, let $\hat{x} > 0$ be the smallest positive solution of

$$x = \Phi_0^{(\mathbf{s})}(x) := \sum_{j,k} \sum_{s \in \mathcal{S}} \sum_{\theta \geq 1} \frac{k\mu^{(s)}(j,k)}{\lambda} p^{(s)}(j,k,\theta) \mathbb{P}(\mathsf{Bin}(j,x) \geq \theta).$$

We first show that such a solution exists in $(0, 1)$. Note that $\Phi_0^{(\mathbf{s})}(0) = 0$, $\Phi_0^{(\mathbf{s})}(1) \leq 1$ and $\Phi_0^{(\mathbf{s})}$ is an increasing function of $x$. Then in order to prove the existence of such a positive $\hat{x}$ it suffices to show that $\Phi_0'(x) > 1$ for $x$ close to zero.

**Claim A.4** *Assume that for some $\Theta \in \mathbb{N}$, $\gamma \in \mathbb{R}^+$ and $\beta \in (2, 3)$:*

$$\sum_{k} \sum_{s \in \mathcal{S}} \sum_{\theta=1}^{\Theta} k\mu^{(s)}(j,k) p^{(s)}(j,k,\theta) \geq \gamma j^{-\beta+1}$$

*for all $j \in \mathbb{N}$. Then there exists $x_0 \in (0, 1)$ such that we have $\Phi_0'(x) > 1$ for all $x \in (0, x_0]$.*

***Proof*** We have for $x \in (0, 1)$ and $\Delta \in \mathbb{N}$

$$\begin{aligned}
\Phi_0'(x) &= \sum_{j,k} \sum_{s \in \mathcal{S}} \sum_{\theta \geq 1} \frac{jk\mu^{(s)}(j,k)}{\lambda} p^{(s)}(j,k,\theta) \mathbb{P}(\mathsf{Bin}(j-1,x) = \theta - 1) \\
&\geq \frac{1}{\lambda} \sum_{j=\Delta+1}^{2\Delta} \sum_{k} \sum_{\theta=1}^{\Theta} jk\mu^{(s)}(j,k) p^{(s)}(j,k,\theta) \mathbb{P}(\mathsf{Bin}(j-1,x) = \theta - 1).
\end{aligned}$$

We now set $x_0 = \frac{1}{\Delta}$ so that we have for $x \leq x_0$ and $\Delta$ large enough

$$\Phi_0'(x) \geq \frac{1}{\lambda} \sum_{j=\Delta+1}^{2\Delta} \sum_{k} \sum_{s \in \mathcal{S}} \sum_{\theta=1}^{\Theta} jk\mu^{(s)}(j,k) p^{(s)}(j,k,\theta) e^{-(j-1)x} \frac{((j-1)x)^{\theta-1}}{(\theta-1)!}$$

$$\geq \frac{e^{-2}}{\lambda(\Theta-1)!}\sum_{j=\Delta+1}^{2\Delta} j\sum_{k}\sum_{s\in\mathcal{S}}\sum_{\theta=1}^{\Theta} k\mu^{(s)}(j,k)p^{(s)}(j,k,\theta)$$

$$\geq \frac{\gamma e^{-2}}{\lambda(\Theta-1)!}\sum_{j=\Delta+1}^{2\Delta} j^{-\beta+2} > \frac{\gamma e^{-2}}{\lambda(\Theta-1)!}\Delta^{-\beta+3}.$$

Hence by choosing $\Delta$ large enough, e.g.,

$$\Delta \geq \left(\frac{\gamma e^{-2}}{\lambda(\Theta-1)!}\right)^{\frac{1}{3-\beta}},$$

and setting $x_0 = 1/\Delta$ we have $I_0'(x) > 1$ for all $x \leq x_0$ and the claim thus follows. □

Since $\Phi_\epsilon^{(\mathbf{s})}$ is continuous we have $\lim_{\epsilon\to 0^+} x_*^{(\mathbf{s})}(\epsilon) = \hat{x}$. The corollary now follows by Theorem 3.6.

### A.5. Proof of Theorem 3.11

Consider the percolated random graph $\mathcal{G}_{\pi_v,\pi_e}(\mathbf{d}^+,\mathbf{d}^-)$ and suppose that Condition 3.4 holds. Our proof of Theorem 3.11 is based on ideas applied in [31] to study the conditions for existence of giant component in the percolated random non directed graph with given vertex degrees; see also [44]. The site percolation model for directed random graphs has also been investigated in [7] in the context of skeleton of contagious links in financial networks.

We fist consider the site percolation model where we remove (delete) each vertex with degrees $(d^+,d^-)$ with probability $1-\pi_v^{(s)}(d^+,d^-)$, independently. This would be equivalent to changing the initial infection probability (for all $d^+,d^-\in\mathbb{N}$ and $s\in\mathcal{S}$) to

$$\widetilde{p}^{(s)}(d^+,d^-,\theta) = \pi_v^{(s)}(d^+,d^-)p^{(s)}(d^+,d^-,\theta) \text{ for } \theta = 0,1,\ldots,d^+, \tag{27}$$

and $\widetilde{p}^{(s)}(d^+,d^-,d^++1) = 1-\pi_v^{(s)}(d^+,d^-)$. Note that the removed vertices in site percolation model are the vertices with threshold $d^++1$ in our new contagion process. Hence, they will never get infected and the final infected set would have the same distribution in both contagion models.

We now consider the bond percolation model, where we remove each link with probability $(1-\pi_e)$. For all $i\in[n]$, let $D_i^+(\pi_e)\sim \mathsf{Bin}(d_i^+,\pi_e)$ be binomial random variables independent over all vertices. We then split a vertex with degree $(d^+,d^-)$ into a single vertex with degree $\left(D^+(\pi_e),d^-\right)$ plus $d^+-D^+(\pi_e)$ red (artificial) vertices with in-degree 1 and out-degree 0. We call this the explosion of a vertex. Note that the red vertices may be considered as being artificial as they will later need to be removed. After all explosions, a directed edge is retained when its incoming half-edge is retained, which occurs with probability $\pi_e$ as it should be. Let

$$N^+(\pi_e) = \sum_{i=1}^{n}\left(d_i^+ - D_i^+(\pi_e)\right),$$

so that $N(\pi_e) = n + N^+(\pi_e)$ denotes the (new) total number of vertices after explosions. Then $[N(\pi_e)]/[n]$ will be the set of all artificial (red) vertices.

Further, instead of removing the $N^+(\pi_e)$ red vertices with degrees (1,0), we will give threshold 2 to these artificial vertices so that they will never get infected and hence they will not play any role in the contagion process.

Note that as $n \to \infty$, since $m_n/n \to \lambda$,

$$\frac{N(\pi_e)}{n} = 1 + \frac{\sum_{i=1}^{n}\left(d_i^+ - D_i^+(\pi_e)\right)}{n} = 1 + \frac{m_n - \mathsf{Bin}(m_n, \pi_e)}{n} \xrightarrow{p} 1 + \lambda(1-\pi_e)$$

and then

$$\frac{N^+(\pi_e)}{N(\pi_e)} \xrightarrow{p} \frac{\lambda(1-\pi_e)}{1+\lambda(1-\pi_e)}.$$

Consequently, it would be quite easy to show that the set of final infected vertices in the initial contagion process on percolated random graph $\mathcal{G}_{\pi_v,\pi_e}(\mathbf{d}^+, \mathbf{d}^-)$ will have the same distribution as the contagion process in configuration model with $N(\pi_e)$ vertices where the degrees converges (in probability) to the new distribution

$$\widehat{\mu}^{(s)}(1,0) = \frac{\mu^{(s)}(1,0)}{1+\lambda(1-\pi_e)} + \frac{\lambda(1-\pi_e)}{1+\lambda(1-\pi_e)} \text{ and } \widehat{\mu}^{(s)}(d^+,d^-) = \frac{\mu^{(s)}(d^+,d^-)}{1+\lambda(1-\pi_e)} \quad (28)$$

for $(d^+, d^-) \neq (1, 0)$. Further, the new threshold distribution function satisfies

$$\widehat{p}^{(s)}(d^+,d^-,\theta) = \pi_v^{(s)}(d^+,d^-)p^{(s)}(d^+,d^-,\theta) \text{ for } \theta = 0,1,\ldots,d^+. \quad (29)$$

Note that $\widetilde{p}$ (threshold distribution after site percolation model) and $\widehat{p}$ (threshold distribution after site and bond percolation) only doesn't agree each other for $\theta > d^+$; in particular for $d^+ = 1, d^- = 0$ and $\theta = 2$. However, this difference will not play any role on the final infected set in the contagion process and the changes will be due to the new degree distribution.

We conclude by applying Theorem 3.6 to the new degree distribution that

$$\frac{|\mathcal{I}_f^{(\mathbf{s})}|}{N(\pi_e)} \xrightarrow{p} \sum_{j,k}\sum_{s\in\mathcal{S}} \widehat{\mu}^{(s)}(j,k) \sum_{\theta=0}^{j} \widehat{p}^{(s)}(j,k,\theta)\mathbb{P}(\mathsf{Bin}(j, \widehat{x}_*^{(\mathbf{s})}) \geq \theta),$$

and then, using $N(\pi_e)/n \to 1+\lambda(1-\pi_e)$, Eqs. (28), (29) and $\widehat{x}_*^{(\mathbf{s})} = x_*^{(\mathbf{s})}\pi_e$ we have

$$\frac{|\mathcal{I}_f^{(\mathbf{s})}|}{n} \xrightarrow{p} \sum_{j,k}\sum_{s\in\mathcal{S}} \mu^{(s)}(j,k)\pi_v^{(s)}(j,k) \sum_{\theta=0}^{j} p^{(s)}(j,k,\theta)\mathbb{P}(\mathsf{Bin}(j, x_*^{(\mathbf{s})}\pi_e) \geq \theta).$$

Note that $x_*^{(\mathbf{s})}$ by Theorem 3.6 is the smallest fixed point in [0,1] of

$$\begin{aligned}\Phi^{(\mathbf{s})}_{\pi_v,\pi_e}(x) &:= \sum_{j,k}\sum_{s\in\mathcal{S}} \frac{k\widehat{\mu}^{(s)}(j,k)}{\lambda} \sum_{\theta=0}^{j} \widehat{p}^{(s)}(j,k,\theta)\mathbb{P}(\mathsf{Bin}(j, x\pi_e) \geq \theta).\\ &= \sum_{j,k}\sum_{s\in\mathcal{S}} \frac{k\mu^{(s)}(j,k)\pi_v^{(s)}(j,k)}{\lambda} \sum_{\theta=0}^{j} p^{(s)}(j,k,\theta)\mathbb{P}(\mathsf{Bin}(j, x\pi_e) \geq \theta).\end{aligned}$$

Similarly, by applying Theorem 3.6, we obtain

$$\frac{|\mathcal{I}_f^{(s)}(d^+,d^-)|}{n\mu_n^{(s)}(d^+,d^-)} \xrightarrow{p} \pi_v^{(s)}(d^+,d^-) \sum_{\theta=0}^{j} p^{(s)}(d^+,d^-,\theta)\mathbb{P}(\mathsf{Bin}(d^+, x_*^{(\mathbf{s})}\pi_e) \geq \theta),$$

and the theorem follows.

### A.6. Proof of Theorems 3.8 and 3.12

We first use Theorem 3.6 to prove that if $\mathcal{R}_0^{(\mathbf{s})} < 1$,

$$\sum_{j,k}\sum_{s\in\mathcal{S}} jk\mu^{(s)}(j,k) < \infty$$

and we initially infect randomly $|\mathcal{I}_0^{(\mathbf{s})}| = o(n)$ vertices in $[n]$, then $|\mathcal{I}_f^{(\mathbf{s})}| = o_p(n)$. Let us assume that $p^{(s)}(d^+, d^-, 0) = \epsilon$ for all $d^+, d^- \in \mathbb{N}$ and $s \in \mathcal{S}$. We show that as $\epsilon \to 0$ then $x_*^{(s)}(\epsilon) \to 0$ which implies the claim. Note that by Theorem 3.6, $x_*^{(s)}(\epsilon)$ is the smallest fixed point of $\Phi_\epsilon^{(\mathbf{s})}$ in $[0, 1]$, where

$$\Phi_\epsilon^{(\mathbf{s})}(x) := \epsilon + \sum_{j=0}^{\infty}\sum_{k=0}^{\infty}\sum_{s\in\mathcal{S}} \frac{k\mu^{(s)}(j,k)}{\lambda}\sum_{\theta=1}^{j} p^{(s)}(j,k,\theta)\mathbb{P}(\mathsf{Bin}(j,x)\geq\theta). \tag{30}$$

Hence $\Phi_\epsilon^{(\mathbf{s})}(0) > 0$ and, for $\sum_{j,k}\sum_{s\in\mathcal{S}} jk\mu^{(s)}(j,k) < \infty$ and $x \approx 0$,

$$\frac{d\big(\Phi_\epsilon^{(\mathbf{s})}(x) - x\big)}{dx} = \frac{1}{\lambda}\sum_{j,k\in\mathbb{N}}\sum_{s\in\mathcal{S}} jk\mu^{(s)}(j,k)p^{(s)}(j,k,1) - 1 = \mathcal{R}_0^{(\mathbf{s})} - 1 < 0.$$

This implies that the smallest fixed point $x_*(\epsilon) \to 0$ as $\epsilon \to 0$.

We now consider the supercritical case when $\mathcal{R}_0^{(\mathbf{s})} > 1$. From [7, 43], we know if

$$\sum_{s\in\mathcal{S}} jk\mu^{(s)}(j,k) > \lambda,$$

there exists a giant strongly connected component in the random graph $\mathcal{G}(\mathbf{d}^+, \mathbf{d}^-)$. Let $\mathcal{S}_1$ be the largest strongly connected component of the random graph $\mathcal{G}(\mathbf{d}^+, \mathbf{d}^-)$ on which we apply site percolation by removing all vertices with degrees $(d^+, d^-)$ and security level $s$ with probability $1 - p^{(s)}(d^+, d^-, 1)$ (we remove all vertices with threshold greater than or equal to 2).

We denote by $\mathcal{S}_1$ the largest strongly connected component of the random graph $\mathcal{G}(\mathbf{d}^+, \mathbf{d}^-)$ on which we apply site percolation by removing all vertices with threshold $\Theta_i \geq 2$. Let $\mathcal{I}_f^{(\mathbf{s})}(i)$ denotes the final infected set is when we initiate the epidemic from $\mathcal{I}_0^{(\mathbf{s})} = \{i\}$ for all $i \in [n]$. Using the coupling argument on the site percolation model used in the last section, we obtain if $\mathcal{R}_o^{(\mathbf{s})} > 1$, i.e.,

$$\sum_{s\in\mathcal{S}} jk\mu^{(s)}(j,k)p(j,k,1) > \lambda,$$

there exists a giant strongly connected component in the percolated random graph and we have

$$\liminf_n \frac{|\mathcal{I}_f^{(\mathbf{s})}(i)|}{n} \geq \liminf_n \frac{|\mathcal{S}_1|}{n} > 0,$$

which concludes the proof of Theorem 3.8.

Moreover, using the distribution $\widehat{\mu}$ and $\widehat{p}$ obtained from last section for the percolated random graph $\mathcal{G}_{\pi_v,\pi_e}(\mathbf{d}^+, \mathbf{d}^-)$, gives us the new contagion reproduction number

$$\mathcal{R}_0^{(\mathbf{s})}(\pi_v,\pi_e) := \frac{1}{\bar{\lambda}} \sum_{j,k\in\mathbb{N}} \sum_{s\in\mathcal{S}} jk\widehat{\mu}^{(s)}(j,k)\widehat{p}^{(s)}(j,k,1)$$
$$= \frac{1}{\lambda\pi_e} \sum_{j,k\in\mathbb{N}} \sum_{s\in\mathcal{S}} jk\mu^{(s)}(j,k)\pi_v^{(s)}(j,k)p^{(s)}(j,k,1).$$

Hence, if $\sum_{j,k,s} jk\mu^{(s)}(j,k) < \infty$ and $\mathcal{R}_0^{(\mathbf{s})}(\pi_v,\pi_e) < 1$, i.e.,

$$\pi_e < \pi_e^* := \frac{\lambda}{\sum_{j,k,s} jk\mu^{(s)}(j,k)\pi_v^{(s)}(j,k)p^{(s)}(j,k,1)},$$

then initially infecting randomly $|\mathcal{I}_0^{(\mathbf{s})}| = o(n)$ vertices in $[n]$ implies that $|\mathcal{I}_f^{(\mathbf{s})}| = o_p(n)$.

Further, if $\pi_e > \pi_e^*$ then $\mathcal{R}_0^{(\mathbf{s})}(\pi_v,\pi_e) > 1$ and w.h.p. for any $i \in \tilde{\mathcal{S}}_1$,

$$\liminf_n \frac{|\mathcal{I}_f^{(\mathbf{s})}(i)|}{n} \geq \liminf_n \frac{|\tilde{\mathcal{S}}_1|}{n} > 0,$$

which concludes the proof of Theorem 3.12.

### A.7. Proof of Lemma 4.2

We show that under the lemma condition, $\delta_k(d^+,d^-,x)$ will be strictly increasing function of vulnerability parameter $x$. This is equivalent to

$$\frac{\partial\delta_k(d^+,d^-,x)}{\partial x} = \sum_{\theta=0}^{d^+} q_k(d^+,d^-,\theta)\frac{\partial\mathbb{P}(\mathsf{Bin}(d^+,x)=\theta)}{\partial x}$$
$$= d^+\sum_{\theta=0}^{d^+} q_k(d^+,d^-,\theta)\left(\mathbb{P}(\mathsf{Bin}(d^+-1,x)=\theta-1)-\mathbb{P}(\mathsf{Bin}(d^+-1,x)=\theta)\right)$$
$$= d^+\sum_{\theta=1}^{d^+}\left(q_k(d^+,d^-,\theta)-q_k(d^+,d^-,\theta-1)\right)\mathbb{P}(\mathsf{Bin}(d^+-1,x)=\theta-1)$$
$$= d^+\sum_{\theta=1}^{d^+}\left(p^{(k-1)}(d^+,d^-,\theta)-p^{(k)}(d^+,d^-,\theta)\right)\mathbb{P}(\mathsf{Bin}(d^+-1,x)=\theta-1) > 0$$

for all $d^+,d^-,k=1,2,\ldots,K$. Consequently, $\delta_k(d^+,d^-,x)$ is strictly increasing function of $x$ and so

$$\ell_k(d^+,d^-,x) := \frac{C^{(k)}(d^+,d^-)-C^{(k-1)}(d^+,d^-)}{\delta_k(d^+,d^-,x)}$$

is a strictly increasing function of global network vulnerability $x$, as desired.

### A.8. Proof of Theorem 4.3

Define a function $\psi:[0,1]\to[0,1]$ via the following,

$$\psi(z) := \inf_{x\in[0,1]}\{x : \Phi^{\gamma(z)}(x) = x\}.$$

It can be easily seen that $\Phi^{\gamma(z)}(0) > 0$, $\Phi^{\gamma(z)}(1) < 1$. In conjugation with the continuity of $x \mapsto \Phi^{\gamma(z)}(x)$, we conclude that for any $z \in [0, 1]$, the set $\{x : \Phi^{\gamma(z)}(x) = x\}$ is nonempty and closed, and hence $\psi(z) \in (0, 1)$ is well-defined.

Now we show that $z \mapsto \psi(z)$ is decreasing in $z$, which implies that (13) has at most one solution. Suppose we have $0 < z_1 < z_2 < 1$.

It can be easily seen that (note that $F(\ell_{K+1}(j, k, z)) = 1$)

$$\begin{aligned}
\Phi^{\gamma(z)}(x) &= \sum_{j,k} \sum_{s\in\mathcal{S}} \frac{k\mu(j,k)\gamma^{(s)}(j,k,z)}{\lambda} \sum_{\theta=0}^{j} p^{(s)}(j,k,\theta)\mathbb{P}(\mathsf{Bin}(j,x) \geq \theta) \\
&= \sum_{j,k} \frac{k\mu(j,k)}{\lambda} \sum_{s\in\mathcal{S}} (F(\ell_{s+1}(j,k,z)) - F(\ell_s(j,k,z))) \sum_{\theta=0}^{j} p^{(s)}(j,k,\theta)\mathbb{P}(\mathsf{Bin}(j,x) \geq \theta) \\
&= \sum_{j,k} \frac{k\mu(j,k)}{\lambda} \sum_{s=1}^{K+1} F(\ell_s(j,k,z)) \sum_{\theta=0}^{j} \left(p^{(s-1)}(j,k,\theta) - p^{(s)}(j,k,\theta)\right) \mathbb{P}(\mathsf{Bin}(j,x) \geq \theta) \\
&= \sum_{j,k} \frac{k\mu(j,k)}{\lambda} \sum_{s=1}^{K+1} F(\ell_s(j,k,z))\delta_s(j,k,x).
\end{aligned}$$

Hence, by monotone investment conditions and since $F$ is strictly increasing cdf function, $\Phi^{\gamma(z)}(x)$ is strictly increasing in $x$ and strictly decreasing function of $z$. So that we have $\Phi^{\gamma(z_1)}(x) > \Phi^{\gamma(z_2)}(x)$ for any $x \in [0, 1]$, and

$$\Phi^{\gamma(z_2)}(\psi(z_1)) - \psi(z_1) < \Phi^{\gamma(z_1)}(\psi(z_1)) - \psi(z_1) = 0.$$

Combining with the fact that $\Phi^{\gamma(z_2)}(0) \geq 0$ and the continuity of $x \mapsto \Phi^{\gamma(z_2)}(x)$, there exists an $x < \psi(z_1)$ such that $\Phi^{\gamma(z_2)}(x) = x$, which implies that $\psi(z_2) < \psi(z_1)$.

### A.9. Proof of Propositions 5.1 and 5.2

We will prove Proposition 5.2, which implies Proposition 5.1 by setting $\mu_H = 1, d_H = d, C_H = C$, and $\mu_L = C_L = 0$. Note that $\gamma_e = (\gamma_{eH}, \gamma_{eL})$ is such that

$$\delta_H(x_*^{\gamma_e})F_H^{-1}(1 - \gamma_{eH}) = C_H, \quad \delta_L(x_*^{\gamma_e})F_L^{-1}(1 - \gamma_{eL}) = C_L,$$

while the social planner chooses $\gamma_s = (\gamma_{sH}, \gamma_{sL})$ which minimizes $\bar{C}_{\text{social}}(\gamma)$:

$$\gamma_s = \underset{\gamma_H,\gamma_L\in[0,1]}{\arg\min} \left\{ \delta_H(x_*^{\gamma}) \int_{\gamma_H}^{1} F_H^{-1}(1-u)du + \delta_H(x_*^{\gamma}) \int_{\gamma_L}^{1} F_L^{-1}(1-u)du + C_H\gamma_H + C_L\gamma_L \right\}.$$

Since $x_*^{\gamma}$ is decreasing in $\gamma_H$, $\gamma_L$ and $\delta_H(.)$, $\delta_L(.)$ are increasing functions, $\delta_H(x_*^{\gamma})$, $\delta_L(x_*^{\gamma})$ are decreasing functions of $\gamma_H$ and $\gamma_L$. Moreover, we have

$$\begin{aligned}
\frac{\partial J_{\text{social}}(\gamma_{eH}, \gamma_{eL})}{\partial \gamma_H} &\leq -\delta_H(x_*^{\gamma_e})F_H^{-1}(1 - \gamma_e) + C_H = 0, \\
\frac{\partial J_{\text{social}}(\gamma_{eL}, \gamma_{eL})}{\partial \gamma_H} &\leq -\delta_L(x_*^{\gamma_e})F_L^{-1}(1 - \gamma_e) + C_L = 0,
\end{aligned}$$

and the proposition follows.

## References


1. Acemoglu,, D., Chernozhukov, V., Werning, I., Whinston, M.D.: A multi-risk SIR model with optimally targeted lockdown. Working Paper 27102, National Bureau of Economic Research (2020)
2. Acemoglu, D., Malekian, A., Ozdaglar, A.: Network security and contagion. J. Econ. Theory **166**, 536–585 (2016)
3. Adler, J., Lev, U.: Bootstrap percolation: visualizations and applications. Braz. J. Phys. **33**(3), 641–644 (2003)
4. Albert, R., Barabási, A.: Statistical mechanics of complex networks. Rev. Mod. Phys. **74**(1), 47–97 (2002)
5. Allen, F., Gale, D.: Financial contagion. J. Polit. Econ. **108**(1), 1–33 (2000)
6. Amini, H.: Bootstrap percolation and diffusion in random graphs with given vertex degrees. Electron. J. Combin. **17**, R25 (2010)
7. Amini, H., Cont, R., Minca, A.: Resilience to contagion in financial networks. Math. Financ. **26**(2), 329–365 (2016)
8. Amini, H., Feinstein, Z.: Optimal network compression. Eur. J. Oper. Res. **306**(3), 1439–1455 (2023)
9. Amini, H., Fountoulakis, N.: Bootstrap percolation in power-law random graphs. J. Stat. Phys. **155**(1), 72–92 (2014)
10. Amini, H., Fountoulakis, N., Panagiotou, K.: Bootstrap percolation in inhomogeneous random graphs. Adv. Appl. Probab. (2023)
11. Amini, H., Minca, A.: Inhomogeneous financial networks and contagious links. Oper. Res. **64**(5), 1109–1120 (2016)
12. Amini, H., Minca, A.: Epidemic spreading and equilibrium social distancing in heterogeneous networks. Dyn. Games Appl. **12**(1), 258–287 (2022)
13. Amini, H., Minca, A., Sulem, A.: A dynamic contagion risk model with recovery features. Math. Oper. Res. **47**(2), 1412–1442 (2022)
14. Ball, F.G., Sirl, D.J., Trapman, P., et al.: Epidemics on random intersection graphs. Ann. Appl. Probab. **24**(3), 1081–1128 (2014)
15. Ballester, C., Calvó-Armengol, A., Zenou, Y.: Who's who in networks. wanted: the key player. Econometrica, **74**(5):1403–1417 (2006)
16. Balogh, J., Pittel, B.G.: Bootstrap percolation on the random regular graph. Random Struct. Algorithms **30**(1–2), 257–286 (2007)
17. Battiston, S., Gatti, D.D., Gallegati, M., Greenwald, B., Stiglitz, J.E.: Liaisons dangereuses: increasing connectivity, risk sharing, and systemic risk. J. Econ. Dyn. Control **36**(8), 1121–1141 (2012)
18. Bhamidi, S., Van Der Hofstad, R., Komjáthy, J.: The front of the epidemic spread and first passage percolation. J. Appl. Probab., **51**(A), 101–121 (2014)
19. Bollobas, B.: Random Graphs. Cambridge University Press (2001)
20. Bollobás, B., Riordan, O.: An old approach to the giant component problem. J. Combin. Theory Ser. B **113**, 236–260 (2015)
21. Britton, T., Janson, S., Martin-Löf, A.: Graphs with specified degree distributions, simple epidemics, and local vaccination strategies. Adv. Appl. Probab. **39**(4), 922–948 (2007)
22. Cheng, B., Titterington, D.M.: Neural Networks: A Review from a Statistical Perspective. Stat. Sci., pp. 2–30 (1994)
23. Detering, N., Meyer-Brandis, T., Panagiotou, K., Ritter, D.: Managing default contagion in inhomogeneous financial networks. SIAM J. Financ. Math. **10**(2), 578–614 (2019)
24. Draief, M., Ganesh, A., Massoulié, L.: Threshold of virus spread on networks. Ann. Appl. Probab. **18**, 359–378 (2008)
25. Elliott, M., Golub, B., Jackson, M.O.: Financial networks and contagion. Am. Econ. Rev. **104**(10), 3115–53 (2014)
26. Farboodi, M., Jarosch, G., Shimer, R.: Internal and external effects of social distancing in a pandemic. In: Working Paper 27059, National Bureau of Economic Research (2020)
27. Gai, P., Kapadia, S.: Contagion in financial networks. Proc. R. Soc. A: Math. Phys. Eng. Sci. **466**(2120), 2401–2423 (2010)
28. Galeotti, A., Golub, B., Goyal, S.: Targeting interventions in networks. Econometrica **88**(6), 2445–2471 (2020)
29. Gordon, L.A., Loeb, M.P.: The economics of information security investment. ACM Trans. Inf. Syst. Secur. **5**(4), 438–457 (2002)
30. Janson, S.: The probability that a random multigraph is simple. Combin. Probab. Comput. **18**(1–2), 205–225 (2009)
31. Janson, S., et al.: On percolation in random graphs with given vertex degrees. Electron. J. Probab. **14**, 86–118 (2009)

32. Janson, S., Luczak, M.J., Windridge, P.: Law of large numbers for the SIR epidemic on a random graph with given degrees. Random Struct. Algorithms **45**(4), 726–763 (2014)
33. Janson, S., Łuczak, T., Turova, T., Vallier, T.: Bootstrap percolation on the random graph $G_{n,p}$. Ann. Appl. Probab. **22**(5), 1989–2047 (2012)
34. Kempe, D., Kleinberg, J., Tardos, É.: Maximizing the spread of influence through a social network. In: Proceedings of the Ninth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 137–146 (2003)
35. Kempe, D., Kleinberg, J., Tardos, É.: Influential nodes in a diffusion model for social networks. In: International Colloquium on Automata, Languages, and Programming, pp. 1127–1138. Springer (2005)
36. Klages-Mundt, A., Minca, A.: Optimal intervention in economic networks using influence maximization methods. Eur. J. Oper. Res. **300**(3), 1136–1148 (2022)
37. Kleinberg, J.: Cascading behavior in networks: algorithmic and economic issues. Algorithmic Game Theory **24**, 613–632 (2007)
38. Lelarge, M.: Coordination in network security games: a monotone comparative statics approach. IEEE J. Sel. Areas Commun. **30**(11), 2210–2219 (2012)
39. Lelarge, M.: Diffusion and cascading behavior in random networks. Games Econom. Behav. **75**(2), 752–775 (2012)
40. Lelarge, M., Bolot, J.: Economic incentives to increase security in the internet: the case for insurance. IEEE INFOCOM **2009**, 1494–1502 (2009)
41. Morris, S.: Contagion. Rev. Econ. Stud. **67**(1), 57–78 (2000)
42. Pastor-Satorras, R., Castellano, C., Van Mieghem, P., Vespignani, A.: Epidemic processes in complex networks. Rev. Mod. Phys. **87**, 925–979 (2015)
43. van der Hofstad, R.: Random Graphs and Complex Networks. Cambridge University Press (2016)
44. van der Hofstad, R.: Stochastic Processes on Random Graphs. Lecture Notes for the 47th Summer School in Probability Saint-Flour (2017)
45. Warnke, L.: On wormald's differential equation method. Available at arXiv:1905.08928 (2019)
46. Watts, D.J.: A simple model of global cascades on random networks. Proc. Natl. Acad. Sci. **99**(9), 5766–5771 (2002)
47. Wormald, N.: Differential equations for random processes and random graphs. Ann. Appl. Probab. **5**(4), 1217–1235 (1995)
48. Yang, Z., Lui, J.C.: Security adoption and influence of cyber-insurance markets in heterogeneous networks. Perform. Eval. **74** (2013)