Available online at www.sciencedirect.com

ScienceDirect

Journal of Economic Theory 166 (2016) 536–585

JOURNAL OF Economic Theory

www.elsevier.com/locate/jet

Network security and contagion ☆

Daron Acemoglu [a,*], Azarakhsh Malekian [b], Asu Ozdaglar [c]

[a] *Department of Economics, Massachusetts Institute of Technology, Cambridge, MA, 02139, United States*
[b] *Rotman School of Management, University of Toronto, Toronto, ON, M5S 3E6, Canada*
[c] *Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA, 02139, United States*

Received 8 June 2015; final version received 21 September 2016; accepted 28 September 2016

Available online 6 October 2016

Abstract

We develop a theoretical model of security investments in a network of interconnected agents. Network connections introduce the possibility of cascading failures due to an exogenous or endogenous attack depending on the profile of security investments by the agents. We provide a tractable decomposition of individual payoffs into an own effect and an externality, which also enables us to characterize individual investment incentives recursively (by considering the network with one agent removed at a time). Using this decomposition, we provide characterization of equilibrium and socially optimal investment levels as a function of the structure of the network, highlighting the role of a new set of network centrality measures in shaping the levels of equilibrium and optimal investments. When the attack location is endogenized (by assuming that the attacker chooses a probability distribution over the location of the attack in order to maximize damage), similar forces still operate, but now because greater investment by an agent shifts the attack to other parts of the network, the equilibrium may involve too much investment relative to the social optimum.

JEL classification: D6; D62

☆ We thank various numerous seminar and conference participants for useful suggestions. We gratefully acknowledge financial support from the Toulouse Network with Information Technology and Army Research Office, ARO MURI W911NF-12-1-0509.

* Corresponding author.

E-mail addresses: daron@mit.edu (D. Acemoglu), azarakhsh.malekian@rotman.utoronto.ca (A. Malekian), asuman@mit.edu (A. Ozdaglar).

http://dx.doi.org/10.1016/j.jet.2016.09.009
0022-0531/

Keywords: Cascades; Contagion; Network security; Security investments; Network centrality

1. Introduction

Computer, communication, transport and economic networks all depend on some degree of security for their operation. For example, a virus that infects a set of connected computers or a malfunction in a router, domain or switch may influence the functioning of the entire system, and in the worst case scenario, will spread from one part to the rest of the network. Almost all networks are protected with security investments. For example, individual computers use virus scans and refrain from visiting websites that appear suspicious. Domains use firewalls and other security devices to prevent exposure to viruses and malware. Consequently, it has long been recognized, in Anderson and Moore's (2006, p. 610) words, that "security failure is caused at least as often by bad incentives as by bad design".

An emerging literature at the boundary of economics and computer science investigates how these incentives are determined and how they shape security investments and resilience of networks. A clear *positive externality* exists in security investments. An agent that fails to protect itself adequately not only increases the probability of its own infection but also increases the likelihood that infection will spread to other agents. Based on this intuition, the literature has so far presumed that there will be underinvestment in security (e.g., Anderson and Moore, 2006; Bachrach et al., 2012; Goyal and Vigier, 2011; Larson, 2011). These intuitions, however, are based on analysis of "symmetric networks". In symmetric networks, there is either no network and all agents (or individuals or nodes) interact with all others or, loosely speaking, all agents occupy the same position in the network as all others. Such symmetric networks are neither realistic nor conducive to an understanding of the role of the structure of the network on equilibrium (and optimal) security investments. The lack of realism is obvious: there is considerable heterogeneity across agents in all of the aforementioned networks; domains and routers differ in terms of their size and importance, and computer users are typically connected to very different numbers of users and occupy different positions in the overall network. The importance of analyzing the impact of network structure is also equally salient and has long been recognized as central for the study of network security as the following quote, again from Anderson and Moore (2006, p. 613), illustrates: "Network topology can strongly influence conflict dynamics... Different topologies have different robustness properties with respect to various attacks."

In this paper, we investigate the impact of the structure of the network on security investments and the likelihood of contagion in a general, asymmetric network. The key to our analysis is a characterization of infection probabilities of different agents, or nodes,[1] in terms of their position in the network when the levels of security investments are small. In our model, each agent i is connected to a subset of other agents and chooses a security investment q_i. An infection is probabilistically transmitted across connected agents. Conditional on transmission to agent i, the probability of infection of this agent is $1 - q_i$ (meaning that with probability q_i, this agent is immune to infection). This formulation is both tractable and makes the positive externality from network investments transparent. We distinguish two types of attacks: (1) *random attacks*, which are likely to hit each agent uniformly at random (and in particular independent of their security

[1] Throughout the paper we use the terms agents and nodes interchangeably. Similarly, we will use the terms network and graph interchangeably.

investments); (2) *strategic attacks*, where the location of the attack is determined by an adversary wishing to maximize expected infection (see also Bachrach et al., 2012; Goyal and Vigier, 2011).

We first provide a tractable decomposition of individual payoffs into an own effect and an externality, which underpins the rest of our analysis, applies in a very similar manner in both the random and the strategic attack models, and appears not to have been noticed so far in the literature. This decomposition enables us to write the payoff of an agent as a function of network effects of others and as a linear function of her own security investment, minus its own cost of investment. These network effects have a simple recursive structure and can be computed by considering the network with one agent removed at a time. Using these decompositions we establish the existence of a pure-strategy Nash equilibrium in the random attacks model.

Second, in the case where security investments are small (which will be the case when cost of investments are high or sufficiently convex), we provide a complete characterization of the relationship between the structure of the network and security investments. Our characterization highlights the importance of a new notion of network centrality, which we refer to as "protection centrality" and which conveniently summarizes the key strategic forces in our random attack model. It is related to how blocked (or protected) a node is by "gatekeepers".[2] Specifically, a node, say j, is a gatekeeper between two other nodes/agents, say i and k, if the infection traveling between i and k has to pass through node j (and has no other path). Loosely speaking, the protection centrality measure sums over the protection that all gatekeepers provides to an agent. Intuitively, when an agent has a high protection centrality (is well protected by gatekeepers), the infection is unlikely to reach her and she does not have incentives to choose a high level of security investment. This notion also highlights the role of *strategic substitutabilities* in our model: security investments are strategic substitutes, because the greater is the investment of its gatekeeper, the more protected is the agent and thus the more it can afford not to invest in its own security. As a result, in the example above, the more node j invests, the less nodes i and k are incentivized to invest themselves.

Under the same assumptions, we also provide a tight characterization of the relationship between socially optimal levels of investments (which maximize overall welfare in the network) and the structure of the network, and compare socially optimal and equilibrium levels of security investments. Socially optimal levels of investment depend on a different yet complementary notion of centrality, which we refer to as "gatekeeping centrality". While the protection centrality measure captures how protected a node is by gatekeepers, the gatekeeping centrality measure summarizes how much of a gatekeeper a node is to the rest of the network. It is intuitive that decentralized equilibrium investments depend on how protected an agent is while socially optimal investments depend on how much of a protection that agent offers to others.

We also show that these characterization results from our baseline model generalize under a variety of extensions. First, in our baseline model, we take the network as exogenously given, which we consider to be a good approximation to most modern communication networks where it is not the structure of the network itself but the level of precaution and security investments that respond to security considerations. Nevertheless, we show that our basic insights generalize to a setup in which the network is endogenous, except in cases where security concerns make agents drop almost all of their connections. Second, we generalize our characterization results to a setup in which infection travels through each link only probabilistically. Third, we also verify via simulations that our main characterization results, which are based on first-order Taylor

[2] We thank an anonymous referee for suggesting this terminology.

expansions for small levels of security investments, provide good approximations to the results when security investments are not small.

The second part of the paper turns to the strategic attack model and shows a robust force towards overinvestment in this case, which echoes an intuition going back to de Meza and Gould (1992): preventive activities can create negative instead of positive externalities when they shift attacks to other nodes. In this case, the game also has elements of *strategic complements*: the level of desired investment of a node is increasing in the investments of other nodes because such investments increase the likelihood that the strategic attacker will target the node in question. We provide a similar complete characterization of equilibrium investments under strategic attacks, and also present conditions under which symmetric networks (which always lead to underinvestment in the random attack model) generate under or overinvestment in this case. The possibility of overinvestment is a consequence of the strategic complementarities in investment decisions in this strategic attack model.

There is now a large literature on spreads of infections and epidemics over networks including, among others, Molloy and Reed (1998, 2000), Newman et al. (2001), and Chung and Lu (2002). Early works considering control of infections and epidemics include Sanders (1971) and Sethi (1974). Brito et al. (1991), Geoffard and Phillipson (1997), Goldman and Lightwood (1995), Toxvaerd (2009), and Galeotti and Rogers (2013) analyzed certain aspects of precautionary or vaccination behavior in related settings.

More closely related to our paper are Bachrach et al. (2012), Goyal and Vigier (2014) and Larson (2011), which analyze endogenous formation of networks (connections) together with security decisions in the presence of infections. In Larson's model, for example, network connections generate benefits for agents but also spread infection. Both of these papers focus on symmetric networks (e.g., Erdős–Rényi random graphs), and thus do not obtain any of our main results. Blume et al. (2011) also study network formation in the presence of negative contagion, but focus on providing bounds on the inefficiency of equilibrium.[3]

Also closely related are works related to "strategic attacks," where precautionary behavior shifts attacks from one agent to another. As mentioned above, an early paper showing this possibility is de Meza and Gould (1992). Related issues are studied in Baccara and Bar-Isaac (2008), Bachrach et al. (2012), Goyal and Vigier (2011), Kovenock and Roberson (2010), Bier et al. (2007) and Hoyer and Jaegher (2010), but once again without focusing on the effects of network structure.

Though focusing on different types of interactions, the literature on network games, and in particular the subbranch on the private provision of public goods over networks, is also closely related to our work. Papers such as Ballester et al. (2006), Bramoulle and Kranton (2007a, 2007b), Calvo-Armengol et al. (2009), Galeotti et al. (2010), Bramoullé et al. (2014) and Allouch (2015), show how equilibrium actions in such network games are often linked to simple network centrality measures. Given the nature of the interactions considered in these papers (e.g., linear-quadratic structures), the relevant statistics are typically standard eigenvector or Bonacich centrality measures. This contrasts with the rather different measures that emerge in

[3] Classic references on network formation include Jackson and Wolinsky (1996) and Bala and Goyal (2000). See also Jackson (2008) and Vega-Redondo (2007) for excellent book-length treatments of issues of contagion in networks and network formation.

our environment, which relate to how much of a gatekeeper a node is and how protected it is by other gatekeepers in the network.[4]

The rest of the paper is organized as follows. Section 2 presents our basic model. Section 3 focuses on the case in which attacks are random (undirected with respect to security investments), while Section 4 considers strategic attacks (directed with respect to the security investment profile of agents). Section 5 concludes, while the Appendix contains all the proofs and some additional examples.

2. Model

We study the spread of infection among a set $V = \{1, \ldots, n\}$ of agents over a network. Agent interactions are represented by an undirected network $G = (V, E)$, where E denotes the set of edges. An attacker exposes one of the agents to an infection (virus), which then spreads dynamically to the other agents. The attacker's decision of which agent to target is represented by the probability vector $\Phi = (\phi_1, \ldots, \phi_n)$, where ϕ_i denotes the probability of attacking agent i. We use the notation s to denote the selected target agent, also referred to as the *seed agent*. The infection is transmitted on the edges of the network.

Before the location of the attack is realized, each agent i invests in a security level $q_i \in [0, 1]$ to decrease the chance of getting infected. We use $\mathbf{q} = [q_j]_{j\in V}$ and $\mathbf{q}_{-K} = [q_j]_{j\in V,\ j\notin K}$ for an arbitrary set $K \subset \{1, \ldots, n\}$ to denote the security profiles (short for security investment profiles) of all agents and all agents other than agents in set K respectively.[5] Here, q_i can be interpreted as the probability that agent i is immune to the infection. Conversely, $1 - q_i$ is the probability that the agent is *susceptible*, meaning that if the infection reaches her, she gets infected with probability $1 - q_i$ (independent of all other events).[6] We use $\mathbb{X}_i$ to denote the indicator random variable which takes value 1 if agent i is susceptible and takes value 0, otherwise. Given network G, security profile $\mathbf{q}$ and attack decision Φ, we denote the probability of node i getting infected by $\mathbf{P}_i(G, \mathbf{q}, \Phi)$. The utility function of agent i, denoted by u_i is given by

$$u_i(G, \mathbf{q}, \Phi) = v_i\,(1 - \mathbf{P}_i(G, \mathbf{q}, \Phi)) - c_i(q_i),$$

where v_i is the value agent i derives from being uninfected and $c_i(q_i)$ is the cost agent i incurs for investing in security level q_i. We assume $v_i = 1$ in the rest of the paper, which is without loss of generality and we will also sometimes take the cost function to be the same to simplify the exposition. We adopt the following standard assumption on the investment cost function.

Assumption 1 *(Investment cost).* For each i, the function $c_i : [0, 1] \to \mathbb{R}^+$ is continuously differentiable, strictly increasing, strictly convex and satisfies the boundary conditions $c(0) = 0$, $c'(0) = 0$, and $\lim_{q\to 1} c'(q) = \infty$.[7]

We define (utilitarian) social welfare as the sum of the utilities of the agents in the network:

---

[4] See Acemoglu et al. (2015), Golub and Jackson (2012), and Goyal and Vigier (2013) for other models of the spread of shocks or information over networks.

[5] Unless otherwise stated, all vectors are taken to be column vectors.

[6] If we think of the spread of the infection dynamically over the network, this implies that if the agent is not infected the first time the infection reaches her, she will not be infected in any of the subsequent instances.

[7] The boundary conditions are imposed to simplify the exposition. All of our results can be generalized to the case in which these conditions are relaxed, though this would be at the expense of keeping track of whether an agent chooses positive investment.

$$W(G, \mathbf{q}, \Phi) = \sum_{i \in V} u_i(G, \mathbf{q}, \Phi).$$

We use G_{-K} for an arbitrary set $K \subset V$, to denote the network obtained from G after removing nodes in K from G. Given network G and security profile $\mathbf{q}$, we define susceptible agents $V_s \subseteq V$ as the set of all $i \in V$ for which $\mathbb{X}_i = 1$. We then define the *transmission network* as the subgraph of the network G induced over V_s and denote it by G^t. The infection is transmitted through the transmission network. In particular, given transmission network G^t and seed agent s, the set of infected agents consists of the set of agents that belong to the same connected component with agent s in G^t. We refer to a path in the transmission network as an *active path*.

We study two different attack models: a *random attack* model in which the attacker targets each agent with attack decision Φ, which is determined exogenously and independent of the security investments of the agents, and a *strategic attack* model in which the location of the attack is determined by an adversary who observes the security profiles of all agents and chooses one agent to attack with the goal of maximizing expected infections. The random attack model represents the scenario where the attack is an exogenous random event and one of the agents is selected at random according to Φ. The strategic attack model on the other hand represents a strategic adversary wishing to maximize the damage to the network.[8]

3. Random attack model

In this section, we focus on the random attack model, where the attacker's decision is an exogenously given probability vector $\Phi = (\phi_1, \ldots, \phi_n)$. We first present two useful characterization results, delineating the impact of an agent's security investments on the rest of the network. We use these characterizations to establish the existence of a pure-strategy Nash equilibrium for the resulting game and compare best response and welfare-maximizing strategies. Our most substantive results characterize equilibrium and socially optimal security investments in terms of the structure of the network for the case in which each agent's security investment is "small".

3.1. Key properties

Our first proposition provides a simple decomposition of individual utility functions into an own effect and network effects from other individuals.

Proposition 1 *(Network effect). Given network G, security profile $\mathbf{q}$, and attack decision Φ, the infection probability of agent i satisfies*

$$\mathbf{P}_i(G, \mathbf{q}, \Phi) = (1 - q_i)\tilde{P}_i(G, \mathbf{q}_{-i}, \Phi),$$

where $\tilde{P}_i(G, \mathbf{q}_{-i}, \Phi)$ is the probability of the infection reaching agent i (including the probability of agent i being the seed).

As with all the other results in the paper, unless stated otherwise, the proof of this proposition is provided in the Appendix.

[8] A hybrid model, where the attacker can target agents according to the characteristics but not their security investments, gives results very similar to the random attack model. We do not discuss this hybrid case to economize on space.

This result is intuitive in view of the fact that agent i is susceptible to infection with probability $1 - q_i$. If she is immune, then she will not get infected in any case. If she is susceptible, she will only get infected if the infection reaches her. In what follows, we refer to $\tilde{P}_i(G, \mathbf{q}_{-i}, \Phi)$ as the *network effect* of G on i. The network effect on an agent admits a simple decomposition and can be computed recursively by considering the network with one agent removed at a time.[9]

Proposition 2 *(Decomposition). Given network G, security profile $\mathbf{q}_{-j}$, and attack decision Φ, the probability of the infection reaching agent j, $\tilde{P}_j(G, \mathbf{q}_{-j}, \Phi)$, satisfies the following: For all $i \in V$, $i \neq j$,*

$$\tilde{P}_j(G, \mathbf{q}_{-j}, \Phi) = \tilde{P}_j(G_{-i}, \mathbf{q}_{-\{i,j\}}, \Phi) + (1 - q_i) Q_{ji}(G, \mathbf{q}_{-\{i,j\}}, \Phi),$$

where $Q_{ji}(G, \mathbf{q}_{-\{i,j\}}, \Phi)$ is the probability of infection reaching agent j only through a path that contains agent i conditional on i being susceptible.

We refer to $(1 - q_i) Q_{ji}(G, \mathbf{q}_{-\{i,j\}}, \Phi)$ as the *externality* of i on j.

This decomposition follows from considering the following mutually exclusive events under which infection reaches agent j: (A) there exists an active path from the seed agent s to j in the transmission network that does not include i, or (B) all possible paths from s to j in the transmission network go through i. The probability of the first event is equal to the probability of infection reaching agent j in the network G_{-i} and is independent of q_i (and q_j).[10] The probability of the second event can be written as the probability of infection reaching j through a path that contains i conditional on i being susceptible (which does not depend on q_i) times the probability of i being susceptible, which is $(1 - q_i)$. In Section 3.2, we use Proposition 1 to characterize best response and equilibrium investments, and then we compare them to welfare-maximizing investment levels which are obtained using Proposition 2. From Propositions 1 and 2, $\frac{\partial u_i}{\partial q_i \partial q_j} = -Q_{ji}(G, \mathbf{q}_{-\{i,j\}}, \phi) < 0$, which implies that our random attack model is a game of strategic substitutes, i.e., an agent will invest more when others are investing less.

3.2. Equilibrium investments

Using Proposition 1, we can write the utility function of agent i as

$$u_i(G, \mathbf{q}, \Phi) = \Big(1 - (1 - q_i)\tilde{P}_i(G, \mathbf{q}_{-i}, \Phi)\Big) - c_i(q_i).$$

Similarly, fixing any $i \in V$, from Propositions 1 and 2, social welfare takes the following form:

$$\begin{aligned} W(G, \mathbf{q}) &= \sum_{j \in V} u_j(G, \mathbf{q}, \Phi) \qquad (1) \\ &= \Big(1 - (1 - q_i)\tilde{P}_i(G, \mathbf{q}_{-i}, \Phi)\Big) - c_i(q_i) \\ &\quad + \sum_{j \in V\, j \neq i} \Big(1 - (1 - q_j)\Big(\tilde{P}_j(G_{-\{i\}}, \mathbf{q}_{-\{i,j\}}, \Phi) + (1 - q_i) Q_{ji}(G, \mathbf{q}_{-\{i,j\}}, \Phi)\Big)\Big) \\ &\quad - c_j(q_j). \end{aligned}$$

[9] In a graph $G = (V, E)$, a *path* between nodes u and v is a sequence of node and edges, $u = v_0, e_1, v_1, e_2, \ldots, e_k, v_k = v$ where $e_i = (v_{i-1}, v_i) \in E$, for all $1 \leq i \leq k$ with no repeated edges and nodes.

[10] This probability does not depend on Φ_i, nevertheless we keep the dependence on the entire vector Φ to simplify the notation.

A security profile $\mathbf{q}^e$ is a *(pure-strategy) Nash equilibrium* if for all $i \in V$ and all $q_i \in [0, 1]$,

$$u_i(G, \mathbf{q}^e, \Phi) \geq u_i(G, (q_i, \mathbf{q}^e_{-i}), \Phi).$$

Similarly, a security profile $\mathbf{q}^s$ is a *social optimum* if for all $\mathbf{q} \in [0, 1]^n$,

$$W(G, \mathbf{q}^s, \Phi) \geq W(G, \mathbf{q}, \Phi),$$

i.e., $\mathbf{q}^s$ is a global maximum of the social welfare function.

Theorem 1 *(Equilibrium existence). Suppose Assumption 1 holds. Then, for any network G, a pure-strategy Nash equilibrium exists in the random attack model. Moreover, if $c''(x) \geq n$ for all $x \in [0, 1]$, the pure-strategy Nash equilibrium is unique.*

The existence of a pure-strategy Nash equilibrium follows readily from the concavity of the utility function $u_i(G, \mathbf{q}, \Phi)$ in q_i, its continuity in $\mathbf{q}$, and the fact that the strategy spaces are compact. Since the arguments are standard, we omit a formal proof. The uniqueness result builds on Rosen's (1965) proof of uniqueness of equilibrium based on diagonal strict concavity.

It is useful for what follows to define the *best response strategy* of an agent i, $B_i(\mathbf{q}_{-i})$, as the security level q_i that maximizes her utility given the security profile $\mathbf{q}_{-i}$ of other agents. Clearly:

$$c_i'(B_i(\mathbf{q}_{-i})) = \tilde{P}_i(G, \mathbf{q}_{-i}, \Phi). \tag{2}$$

Similarly, the *welfare maximizing strategy* of agent i, $S_i(\mathbf{q}_{-i})$, which maximizes social welfare given the security profile $\mathbf{q}_{-i}$ of other agents, satisfies

$$c_i'(S_i(\mathbf{q}_{-i})) = \tilde{P}_i(G, \mathbf{q}_{-i}, \Phi) + \sum_{j \neq i}(1 - q_j)Q_{ji}(G, \mathbf{q}_{-\{i,j\}}, \Phi). \tag{3}$$

A comparison of these two expressions immediately establishes that

$$B_i(\mathbf{q}_{-i}) \leq S_i(\mathbf{q}_{-i}), \tag{4}$$

or that an agent's best response to a strategy profile is always less than the welfare-maximizing investment in response to the same profile.[11] The network effect satisfies the following intuitive monotonicity properties.

Proposition 3. *Given network G and two security profiles $\mathbf{q}$ and $\hat{\mathbf{q}}$, the following properties hold for each agent $i \in V$:*

(a) If $\mathbf{q}_{-i} \geq \hat{\mathbf{q}}_{-i}$, then $\tilde{P}_i(G, \mathbf{q}_{-i}, \Phi) \leq \tilde{P}_i(G, \hat{\mathbf{q}}_{-i}, \Phi)$.
(b) For any $\hat{V} \subset V$, $\tilde{P}_i(G_{-\hat{V}}, \mathbf{q}_{-(\hat{V} \cup \{i\})}, \Phi) \leq \tilde{P}_i(G, \mathbf{q}_{-i}, \Phi)$.
(c) If $\tilde{P}_i(G, \mathbf{q}_{-i}, \Phi) \geq \tilde{P}_i(G, \hat{\mathbf{q}}_{-i}, \Phi)$, then $B_i(\mathbf{q}_{-i}) \geq B_i(\hat{\mathbf{q}}_{-i})$.

Part (a) of this proposition states the intuitive fact that probability of the infection reaching agent i is smaller when other agents select a higher security profile. Part (b) establishes that the

[11] This relationship does not establish that every agent will underinvest in equilibrium relative to the welfare-maximizing strategy profile. This is because investment levels are strategic substitutes, and the underinvestment of one agent may trigger a sufficiently large increase in the investments of others, which then ends up overinvesting relative to the welfare-maximizing profile.

probability of the infection reaching agent i is smaller in a subgraph (which is intuitive in view of the fact that there are more paths along which infection can reach agent i in the original graph). Finally, part (c) shows that the best response strategy of agent i is higher when the network effect of G on i is higher.

3.3. Symmetric networks

Before moving to our main focus, which is general networks, we briefly discuss *symmetric networks* (with symmetric agents in terms of their cost function c_i, which is denoted by c in this subsection). We use automorphism of a graph to define symmetric networks. An automorphism of a graph $G = (V, E)$ is defined as a permutation σ of the node set V, such that the pair of nodes $(u, v) \in E$ if and only if the pair $(\sigma(u), \sigma(v)) \in E$. Using this definition, we define symmetric networks as follows:

Definition 1 *(Symmetric network).* A network $G = (V, E)$ is symmetric if for any two pair of adjacent nodes $(u_1, v_1) \in E$ and $(u_2, v_2) \in E$, there exists an automorphism $f : V \to V$ such that $f(u_1) = u_2$ and $f(v_1) = v_2$.

Rings and complete graphs are examples of symmetric networks. Our next result shows that in symmetric networks, a unique symmetric equilibrium security profile exists and that investment levels in the symmetric equilibrium are always lower than the (unique) symmetric social optimum.

Theorem 2. *Suppose Assumption 1 holds and all agents have the same cost function. Then, for any symmetric network, there exists a unique symmetric pure-strategy Nash equilibrium (with investment q^e) and a unique symmetric social optimum (with investment q^s). Moreover, $q^e \le q^s$.*

The key result in Theorem 2 is the underinvestment in security in the symmetric equilibrium relative to the social optimum. This result, which confirms those in the existing literature, has a straightforward intuition, which can be seen from Eq. (4): given the security profile of all other agents, an individual always has weaker incentives to invest in security in the best response strategy than in the welfare maximizing strategy. In a symmetric equilibrium this implies that everybody will have weaker incentives to invest in security, leading to underinvestment.[12]

3.4. Network centrality and equilibrium investments

We now consider a situation in which equilibrium investments are all “small”, which will enable us to undertake a tractable first-order Taylor series expansion of best responses, and then express equilibrium investments in terms of the network position (centrality) of each agent.

Let us simplify the exposition in the rest of this section by assuming that all agents have the same cost function, and that $\Phi = (\frac{1}{n}, \dots \frac{1}{n})$, so that each agent is attacked with the same probability, $\frac{1}{n}$.[13] We also simplify the notation by suppressing Φ from $\mathbf{P}_i(G, \mathbf{q}, \Phi)$, writing it simply as $\mathbf{P}_i(G, \mathbf{q})$.

---

[12] Symmetric networks may have asymmetric equilibria, because the game is strategic substitute. See Bramoullé et al. (2014) for detailed discussion on multiplicity of equilibria in strategic substitute games.

[13] Both of these assumptions can be relaxed without any significant effect on our results.

Fig. 1. Examples of gatekeeper indicator variable.

We next characterize equilibrium investments in terms of the position of each agent within the network (and some implied network centrality measures). The key notion will turn out to be whether a node is a "gatekeeper" between two other agents, so that the infection traveling from one agent to the other has to pass through this node. In particular, let a^j_{ik} be an indicator variable that takes value 1 if node j is a *gatekeeper* between nodes i and k, meaning that j is included in all paths between i and k; in this case, if j were removed, the infection could not travel from agent i to agent k. We define $a^j_{ii} = 0$ for all $j \neq i$, and $a^j_{ij} = 1$ and $a^j_{ji} = 1$. For example in the network shown in Fig. 1a, node 1 is a gatekeeper between node 2 and node 4, i.e., $a^1_{24} = 1$, and in Fig. 1b, node 1 is not a gatekeeper between node 2 and node 4 since they still stay connected if node 1 is removed, thus $a^1_{24} = 0$, though 1 is a gatekeeper between 2 and 3. Based on this definition, we define the "protection" of node j for node i (meaning how much of a gatekeeper node j is in protecting agent i), denoted by a^j_i, as the fraction of nodes for which j is a gatekeeper to reach i.

Definition 2. The protection of node j for node i, a^j_i, is defined as $a^j_i \equiv \frac{1}{n}\sum_k a^j_{ik}$, with the convention that $a^i_i = 1$ for all i.[14]

In Fig. 1a, the protection of node 1 for 2 is 3/4, and in Fig. 1b, the protection of node 1 for 2 is 2/4. Intuitively, the protection of node j for node i designates how much of the infection can be blocked by node j on its way to i: the more protection node j provides for node i, the more the infection probability of node i depends on node j's security investment. Our first result provides a characterization of network effect of G on i, which we combine with Eq. (2) to characterize the equilibrium security investments.

Proposition 4. *Given a network G and the security investment* $\mathbf{q}$, *we have*[15]

$$\tilde{P}_i(G, \mathbf{q}_{-i}) = 1 - \sum_{j \neq i} a^j_i q_j + o(||\mathbf{q}||_\infty).$$

Because this proposition forms a foundation for many of our subsequent results and because it helps introduce several important notions we use in the rest of the analysis, we give a detailed sketch of the proof here. We start with the proof for tree networks. Note that we can express the network effect of G on i as

[14] For general $\Phi \neq (\frac{1}{n}, \dots, \frac{1}{n})$, we define $a^j_i \equiv \sum_k a^j_{ik}\phi_k$.

[15] We use the notation $o(x)$ to denote a function $h(x)$ that satisfies $\lim_{x\to 0} \frac{h(x)}{x} = 0$.

$$\tilde{P}_i(G, \mathbf{q}_{-i}) = \frac{1}{n} + \frac{1}{n}\sum_{k \neq i} Prob(\{i \leftrightarrow k\}|\mathbb{X}_i = 1) \tag{5}$$

The first term on the right hand side, is the probability that agent i is attacked and the second term is the sum over all agents $k \neq i$, the probability that agent k is attacked and there is an active path between i and k, denoted by the event $\{i \leftrightarrow k\}$, conditional on i being susceptible. The assumption of $\alpha = c''(0)$ sufficiently large ensures that the equilibrium security investments are small and we can express $Prob(\{i \leftrightarrow k\}|\mathbb{X}_i = 1)$ as

$$Prob(\{i \leftrightarrow k\}|\mathbb{X}_i = 1) = \prod_{j \in i \leftrightarrow k, j \neq i} (1 - q_j) = 1 - \sum_{j \in i \leftrightarrow k, j \neq i} q_j + o(||\mathbf{q}||_\infty), \tag{6}$$

where we used the notation $i \leftrightarrow k$ to denote the active path from i to k. Since G is a tree, there is a unique path between i and k, therefore, $j \in i \leftrightarrow k$ if and only if $a_{ik}^j = 1$, i.e., j is a gatekeeper between i and k. Therefore, we can rewrite Eq. (6) as

$$Prob(\{i \leftrightarrow k\}|\mathbb{X}_i = 1) = 1 - \sum_{j \neq i} a_{ik}^j q_j + o(||\mathbf{q}||_\infty).$$

Combining with Eq. (5), we obtain

$$\begin{aligned}\tilde{P}_i(G, \mathbf{q}_{-i}) &= \frac{1}{n} + \frac{1}{n}\sum_{k \neq i} Prob(\{i \leftrightarrow k\}|\mathbb{X}_i = 1) \\ &= \frac{1}{n} + \frac{1}{n}\sum_{k \neq i}(1 - \sum_{j \neq i} a_{ik}^j q_j) + o(||\mathbf{q}||_\infty) = 1 - \sum_{j \neq i} a_i^j q_j + o(||\mathbf{q}||_\infty).\end{aligned}$$

To extend the proof to general networks, we use a fundamental decomposition result from graph theory, referred to as *block tree decomposition of a graph* (Hopcroft and Tarjan, 1973). To state this result, we first define a connected graph to be *biconnected* if removal of any single node cannot make the graph disconnected (e.g. a ring network is biconnected). We also define a *cut vertex* to be a node whose removal makes the graph disconnected. Hence, a biconnected graph does not have a cut vertex. A tree network is not biconnected, and nodes except the leaves are cut vertices. The block-tree decomposition by Hopcroft and Tarjan (1973) states that any connected graph can be decomposed into a unique tree of maximal biconnected components.[16] We call each maximal biconnected component a *block* and the tree of blocks as the *block tree* of the graph. More formally, given a graph G, we define its block tree as a tree with its nodes consisting of all cut vertices of G and also all blocks of G (where a block is joined to all cut vertices of G contained in the block).

We use the block tree decomposition of graph G to analyze the probability that there is an active path between i and k, $Prob(\{i \leftrightarrow k\}|\mathbb{X}_i = 1)$. Consider the unique path from i to k in the block tree decomposition of G, defined in terms of the cut vertices shared between the blocks, denoted by $v_1, \ldots, v_t$, and let $i = v_0$ and $k = v_{t+1}$ (where v_1 and v_t are cut vertices in the blocks that i and k belong to). We characterize $Prob(\{i \leftrightarrow k\}|\mathbb{X}_i = 1)$ as

$$Prob(\{i \leftrightarrow k\}|\mathbb{X}_i = 1) \tag{7}$$

[16] Each biconnected component is maximal in a sense that the addition of any other node in the graph will make it non-biconnected. We will use this additional property of components in our proof.

$$= \prod_{j=1}^{t+1} Prob(v_j \text{ is susceptible }) \prod_{j=0}^{t} Prob(\{v_j \leftrightarrow v_{j+1}\}|v_j \& v_{j+1} \text{ are susceptible}).$$

Since v_j and v_{j+1} belong to the same block, which is a biconnected component, we have

$$Prob(\{v_j \leftrightarrow v_{j+1}\}|v_j \& v_{j+1} \text{ are susceptible }) = 1 - o(||\mathbf{q}||_\infty), \tag{8}$$

i.e., in order to have no active paths between v_j and v_{j+1}, we need to have at least two nodes on the paths between v_j and v_{j+1} to be immune, the probability of which is given by $o(||\mathbf{q}||_\infty)$. Combining Eqs. (7) and (8), we have

$$\begin{aligned} Prob(\{i \leftrightarrow k\}|\mathbb{X}_i = 1) &= \prod_{j=1}^{t+1} Prob(v_j \text{ is susceptible }) \cdot (1 - o(||\mathbf{q}||_\infty) \qquad (9) \\ &= 1 - \sum_{j=1}^{t+1} q_j + o(||\mathbf{q}||_\infty) = 1 - \sum_{j \neq i} a_{ik}^j q_j + o(||\mathbf{q}||_\infty). \end{aligned}$$

The third equality holds since only the cut vertices (and node k) on the unique path between i and k in the block tree are the gatekeepers between i and k in G, therefore, $a_{ik}^j = 1$ for all $j \in \{v_1, \ldots, v_{t+1}\}$ and $a_{ik}^j = 0$, otherwise. Combining Proposition 4 with the best response representation in Eq. (2), we obtain the full characterization of $\mathbf{q}^e$ in terms of protection values a_i^j. In the rest of the paper, we will use the notation $a \overset{\alpha}{\approx} b$ as a shorthand for $\|a - b\|_2 = o(\frac{1}{\alpha^2})$.

Theorem 3. *Suppose Assumption 1 holds. Then for $\alpha = c''(0)$ sufficiently large, the equilibrium security investments are given by*

$$\mathbf{q}^e \overset{\alpha}{\approx} (A + \alpha I)^{-1} e, \tag{10}$$

where A is the matrix with $A_{ij} = a_i^j$, for $j \neq i$, $A_{ii} = 0$, and e is the vector of all 1's.[17,18]

With a further approximation, we also have

$$\mathbf{q}^e \overset{\alpha}{\approx} \frac{1}{\alpha} e - \frac{1}{\alpha^2} Ae. \tag{11}$$

This theorem is stated under the assumption that $c''(0)$ is sufficiently large. Under this assumption, we show that the payoff functions are diagonally strictly concave, which implies that the equilibrium security investments are unique. Also, this assumption ensures that the last part of the theorem follows because, when α is large, we can also approximate Eq. (10) as

$$(A + \alpha I)^{-1} = \frac{1}{\alpha}\left(\frac{A}{\alpha} + I\right)^{-1} \overset{\alpha}{\approx} \frac{I}{\alpha} - \frac{A}{\alpha^2}.$$

[17] Directly imposing that these investments are small, we could have written Eq. (10) as $\mathbf{q}^e = (A + \alpha I)^{-1} e + \frac{1}{\alpha} o(||\mathbf{q}||_\infty)$. An alternative would have been to assume that the marginal cost of investment at zero, $c'(0)$, is sufficiently large, which would also rule out very high equilibrium security investment levels, though in this case we would have to keep track of the agents choosing zero investment, substantially complicating the analysis.

[18] It is also straightforward to generalize this theorem to the case of arbitrary Φ with $\sum_{j \in V} \phi_j < 1$, which would change Eq. (10) to $\mathbf{q}^e = (A + \alpha I)^{-1} e \sum_{j \in V} \phi_j + o(\frac{1}{\alpha^2})$.

It is also useful to remark that Eq. (10) holds even when $\alpha = c''(0)$ is not large, since we have included the residual term $o(\frac{1}{\alpha^2})$ explicitly, though in this case there may also be non-unique equilibrium investment levels.

We next introduce a new network centrality measure, called the *protection centrality*, measuring how much of a gatekeeper a particular node is to all agents in the network, and use this centrality measure to provide a ranking of the equilibrium security investments of all agents in the same or different networks, again focusing on the case where α is large (or equilibrium investments are small).

Definition 3. Given network G, we define the *protection centrality* of node i, a_i as the sum of the row i of A, i.e., $a_i \equiv \sum_j a_i^j$.

As can be seen from the definition, a_i measures how protected node i is by gatekeepers, i.e., a_i will be high if i is connected to the rest of the network through gatekeepers. Intuitively, when gatekeepers limit exposure of node i to infection or when node i is more blocked, the infection is less likely to reach it. Using Theorem 3, we have

$$q_i^e \overset{\alpha}{\approx} \frac{1}{\alpha}\left(1 - \frac{1}{\alpha}\sum_{j \neq i} a_i^j\right) = \frac{1}{\alpha}\left(1 - \frac{1}{\alpha}a_i\right). \tag{12}$$

As highlighted in Eq. (12), when a_i is high, i will choose a lower level of security investment. This expression is particularly simple since a_i is only a function of position of i in G. Based on this, we can also compare equilibrium investments of different nodes (in the same or different networks).

Corollary 1. *Suppose Assumption 1 holds and $\alpha = c''(0)$ is sufficiently large. Let G and $\hat{G}$ be two (arbitrary) networks. For agents i, j belonging to G and $\hat{G}$, respectively, if agent j has lower protection centrality (is less protected via gatekeepers) than agent i, then it has a greater equilibrium security investment.*

This corollary provides a sharp characterization (in particular because it applies to any two arbitrary networks), and shows that the ranking of the investments of any two nodes (in any two networks) is simply in terms of their protection centrality measures: the node with greater protection centrality will invest less. The next example illustrates one implication of this corollary.

Example 1. Consider two networks depicted in Fig. 2. The protection centrality of node x, a_x, is given by $a_x = \sum_{i=1}^6 a_x^i = 2 \times 3/7 + 4 \times 1/7 = 10/7$, because nodes 1 and 4 have protection of $3/7$ for x whereas all the other nodes are only gatekeepers for themselves and thus have protection of $1/7$. The protection centrality of node y, a_y, is, on the other hand, given by $a_y = \sum_{i=1}^6 a_y^i = 6 \times 1/7 = 6/7$. Thus, $a_x > a_y$, i.e., the protection centrality of x is higher than y. This is because node x is more "blocked" than node y as it is protected by two gatekeepers, nodes 1 and 4, which block the infection coming from nodes 2, 3, 5 and 6. Corollary 1 then implies that $q_x^e < q_y^e$, i.e., the more blocked node x invests less than node y.

The most substantive result of this corollary is that when security investments are small, the protection is the key structural feature of a network determining equilibrium security investments.

(a) $a_x = \frac{10}{7}$. (b) $a_y = \frac{6}{7}$.

Fig. 2. Node x invests less in the equilibrium compared to node y.

To understand the implications of this result, we first consider the case where the underlying network is a tree, and then explain the implications of this result for general networks.[19] For tree networks, a_i is just the average distance of the nodes to node i, and therefore, a_i has the same ordering as the "closeness centrality", i.e., for tree networks, nodes with higher closeness centrality have higher equilibrium security investments.[20] Moreover, rooting the tree at the node with the highest closeness centrality, as we move from the root toward the leaves, the closeness centrality decreases, which implies that the protection centrality increases, and the security investments decrease. In tree networks, the node with the highest closeness centrality also has the balancing property, i.e., the maximum size of the subtree rooted at his children is minimized. We will use this definition, to define balancing node for general networks, which also has the highest equilibrium security investment.

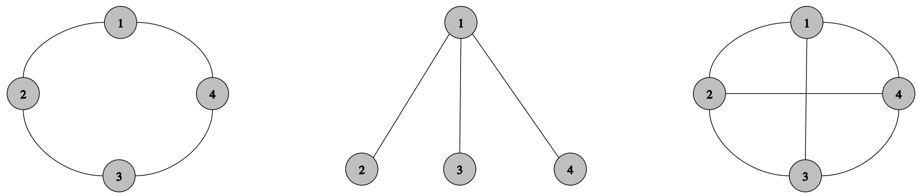
For general networks, we again consider the block tree decomposition of the network. In the block tree decomposition, we call two cut vertices *adjacent*, if they have a common neighbor (which is a block) in the decomposition. A cut vertex v is *balancing* if rooting the block tree at v, the maximum size of all subtrees rooted at his adjacent cut vertices, i.e., the size of the blocks in that subtree, is minimized among all cut vertices. We show that the balancing node i has the lowest a_i, which implies that the balancing node has the highest equilibrium security investment. Moreover, as we move down the block tree rooted at the balancing cut vertex toward the leaves, the protection centrality increase, and as a result the equilibrium security investments of cut vertices decrease. We next formally state these results.

Corollary 2. *Suppose Assumption 1 holds and $\alpha = c''(0)$ is sufficiently large. Consider the block tree decomposition of a given network. Then:*

(a) The balancing cut vertex has the highest equilibrium security investment in the network.
(b) Given two adjacent cut vertices i and j in the block tree, the node closer to the balancing cut vertex has higher equilibrium security investment.
(c) In each block, the equilibrium security investments of the cut vertices of the block are higher than the non-cut vertices belonging to that block. Moreover, the equilibrium security investments of all non-cut vertices in a block are the same up to $o(\frac{1}{\alpha^2})$ error.

[19] The theorem does not assume that the network is a tree. We are using the tree example to illustrate the idea.

[20] In connected graphs farness of a node s is defined as the sum of the length of their shortest paths to all other nodes, and its closeness is defined as the reciprocal of the farness (Bavelas, 1950).



(a) $b_{24}^{(1,3)} = 1$ (b) $b_{24}^{(1,3)} = 0$ (c) $b_{24}^{(1,3)} = 0$

Fig. 3. Examples of separating pairs.

This result implies that the node that balances the network has the highest security investment in the equilibrium, and as nodes get farther from this node, their security investments decrease.

3.5. Network centrality and socially optimal investments

We next provide a characterization of socially optimal security investments of agents as a function of their position in the network, and compare these to equilibrium investment. It will turn out that socially optimal investments depend not on the notion of protection centrality introduced in the previous subsection (in particular, recall Corollary 1), but a different notion related to gatekeeping centrality in the network: how much of a gatekeeper an agent is to the rest of the network. This is intuitive: as explained in subsection 3.4, in equilibrium an agent estimates the number of active paths from other agents to himself, i.e., the number of paths that are not blocked. However, in the socially optimal solution, an agent's investment should depend on the number of pairs of nodes that the node blocks.

Preparing for a formal derivation for these results, let us define, $b_{kt}^{(i,j)} \in \{0, 1\}$ as an indicator variable that takes value 1 if i and j is a separating pair defined as follows: (i, j) is a *separating pair* for nodes k and t if neither of these two nodes is a gatekeeper between nodes k and t (i.e., $a_{tk}^i = 0$ and $a_{tk}^j = 0$), but all paths between k and t includes either i or j. Put differently, (i, j) is a separating pair, if removing either one of them will not disconnect nodes k and t, but removing both will do so. For example in Fig. 3a, $(1, 3)$ is a separating pair for $2, 4$, i.e., $b_{24}^{(1,3)} = 1$, in Fig. 3b, even though after removing nodes 1 and 3, nodes 2 and 4 become disconnected, $(1, 3)$ is not a separating pair between them, since $a_{24}^1 = 1$, thus $b_{24}^{(1,3)} = 0$, and in Fig. 3c, nodes 2 and 4 stay connected even after removing both 1 and 3, thus $b_{24}^{(1,3)} = 0$. Based on this definition, we define *network separation* of node i and node j as the difference between the number of pairs for which both i and j are gatekeepers and the number of pairs for which (i, j) is a separating pair. More formally:

Definition 4. Given network G, network separation of i and j is defined as $b_i^j = \frac{1}{n} \sum_{k,t} \left(a_{kt}^j a_{kt}^i - b_{kt}^{(i,j)} \right)$, with the convention that $b_i^i = 0$.[21] We also define the gatekeeping centrality of node i, denoted by s_i, as $s_i = \sum_j a_j^i$.

[21] Note that $b_j^i = b_i^j$.

Intuitively, the gatekeeping centrality of node i measures the number of pairs of nodes for which i is a gatekeeper. In the example given in Fig. 3b, $b_3^1 = \frac{3}{2}$, in Fig. 3a, $b_3^1 = 0$, and in Fig. 3c, $b_3^1 = \frac{1}{2}$. We next provide a characterization of socially optimal investments in terms of b_i^j and s_i.

Theorem 4. *Suppose Assumption 1 holds. The socially optimal security investments are given by*

$$\mathbf{q}^s \overset{\alpha}{\approx} (B + \alpha I)^{-1} \mathbf{s}, \tag{13}$$

where B is the matrix with $B_{ij} = b_i^j$ for all j, and $\mathbf{s}$ is the vector of s_i's (as defined in Definition 4).

This theorem demonstrates that when security investments are small, the network separation property is the key structural feature that defines the socially optimal security investments. We provide a sketch of the proof here (see Appendix A for details). The proof relies on the characterization of social optimal security investments given in Eq. (3), i.e.,

$$c'(q_i^s) = \tilde{P}_i(G, \mathbf{q}_{-i}) + \sum_j (1 - q_j) Q_{ji}(G, \mathbf{q}), \tag{14}$$

which follows from the decomposition provided in Proposition 2. Note that the left hand side in this expression is the sum of the network effect of G on i and the externality of i on other agents. The proof proceeds by characterizing these two expressions using the gatekeeper and separating pair properties of nodes. In particular, using an argument similar to the one used for equilibrium investments (following Proposition 4), we obtain

$$\tilde{P}_i(G, \mathbf{q}_{-i}) = 1 - \sum_j a_i^j q_j + o(||\mathbf{q}||_\infty). \tag{15}$$

We next write, the externality of i on j, as

$$Q_{ji}(G, \mathbf{q})(1 - q_j) = a_j^i - \frac{1}{n} \sum_{k \neq i} \sum_t \left(a_{jt}^i a_{jt}^k - b_{jt}^{(i,k)} \right) q_k + o(||\mathbf{q}||_\infty) \tag{16}$$

The first term on the right hand side represents the fraction of nodes for which i is a gatekeeper to reach j, which is the same as the probability that infection falls on any of the nodes, $\frac{1}{n}$, times the number of such nodes. The second term, representing the fraction of nodes that are blocked from j by both i and k (conditioned on k being immune), corrects for the double-counting in the first term.[22] The third term represents the fraction of nodes that are blocked from j when both i and k are immune, i.e., (i, k) is a separating pair for j and all nodes in that set. Note that when (i, k) is a separating pair between j and t, if k is immune, which happens with probability q_k, all paths from t to j go through i, and should be counted in $Q_{ji}(G, \mathbf{q})$.[23] Combining Eqs. (15) and (16), we obtain

[22] Note that because of linearization, when computing the conditional probability Q_{ji}, we only need to consider double-counting due to another node k blocking infection paths to j, in addition to i. Double-counting due to three or more nodes blocking paths to j is second-order and neglected.

[23] To formalize the argument for general networks similar to Proposition 4, we use in the appendix a well-known unique decomposition of networks, first by their cut vertices and then by their separating pairs, by Hopcroft and Tarjan (1973).

$$\begin{aligned}
&\tilde{P}_i(G,\mathbf{q}_{-i}) + \sum_{j\neq i} Q_{ji}(G,\mathbf{q})(1-q_j) \\
&\quad = 1 - \sum_k a_i^k q_k + \sum_{j\neq i} a_j^i - \frac{1}{n}\sum_{k\neq i}\sum_t \left(a_{jt}^i a_{jt}^k - b_{jt}^{(i,k)}\right) q_k + o(||\mathbf{q}||_\infty) \\
&\quad = 1 + \sum_{j\neq i} a_i^j - \sum_{k\neq i} q_k \left(a_i^k + \frac{1}{n}\sum_{j\neq i}\sum_t a_{jt}^i a_{jt}^k + b_{jt}^{(i,k)}\right) + o(||\mathbf{q}||_\infty) \\
&\quad = s_i - \sum_{k\neq i} q_k b_i^k + o(||\mathbf{q}||_\infty).
\end{aligned}$$

The third equality here follows from the fact that for $j = i$, we have

$$\frac{1}{n}\sum_t \left(a_{jt}^i a_{jt}^k + b_{jt}^{(i,k)}\right) = \frac{1}{n}\sum_t a_{it}^k = a_i^k,$$

since $a_{it}^i = 1$ and $b_{it}^{(i,k)} = 0$ for all t. Combining this with Eq. (14), Theorem 4 follows.

Under the assumption that α is large, we can express the socially optimal investments as

$$q^s \overset{\alpha}{\approx} \frac{1}{\alpha}\left[\left(I - \frac{B}{\alpha}\right)\mathbf{s}\right].$$

This yields the following characterization for socially optimal security investments:

$$q_i^s \overset{\alpha}{\approx} \frac{1}{\alpha}\left(s_i - \frac{1}{\alpha}\sum_j B_{ij} s_j\right). \tag{17}$$

This expression highlights the role of the gatekeeping centrality of node i for its socially optimal level of investment.[24] The next corollary uses this characterization to provide a comparison of equilibrium and socially optimal levels of investment.

Corollary 3. *Suppose Assumption 1 holds and $\alpha = c''(0)$ is sufficiently large. Then:*

- *The equilibrium security investments are smaller than the socially optimal security investments.*
- *The node with the largest gatekeeping centrality increases its investment the most in the socially optimal solution compared to the equilibrium.*
- *For all nodes with the same gatekeeping centrality, the gap between socially optimal investment and equilibrium is proportional to $a_i - \sum_j B_{ij} s_j$.*

By combining Eqs. (12) and (17), we have

$$q_i^s - q_i^e \overset{\alpha}{\approx} \frac{1}{\alpha}\sum_{j\neq i} a_j^i - \frac{1}{\alpha^2}\left(\sum_{j\neq i} B_{ij} s_j - a_i^j\right). \tag{18}$$

[24] In tree networks, $b_{kt}^{(i,j)}$ terms are equal to zero, and thus the socially optimal investments can be expressed as a function of protections of nodes. In other networks, these terms are not zero due to the presence of separating pairs.

Also by definition $a^i_j \geq \frac{1}{n}$, since node i is a gatekeeper between himself and j, hence, $\sum_{j \neq i} a^i_j \geq 1 - \frac{1}{n}$. Therefore, the first term on the right hand side of Eq. (18) is strictly positive, and assuming α sufficiently large, it implies the first part of Corollary 3, i.e., $q^s_i > q^e_i$, for all nodes i. Moreover, for α sufficiently large, neglecting second order terms, this gap is proportional to $s_i - 1$, which implies the second part of the corollary. Finally, for two nodes i and k, if $s_i = s_k$, to compare the gap between the equilibrium and socially optimal investments in Eq. (18), one should consider the second term on the right hand side, i.e., in this scenario, if $a_i - \sum_j B_{ij} s_j > a_k - \sum_j B_{kj} s_j$, then $q^s_i - q^e_i < q^s_k - q^e_k$. To draw out the implications of this corollary, we can partition the nodes of a given graph into three classes:

(A) Nodes that are not cut vertices and also do not belong to any separating pair.
(B) Nodes that are not cut vertices but belong to at least one separating pair.
(C) Cut vertices.

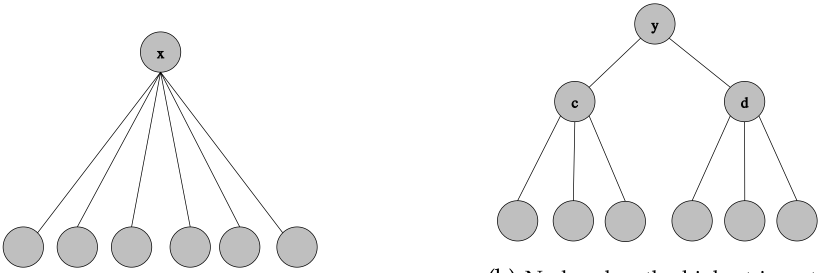
We show that the gap between socially optimal and equilibrium security investments, is ordered from lowest in class (A), to highest in class (C), using Corollary 3. Note that for node i in class (A), since i is not a cut vertex, $s_i - 1 = \sum_{j \neq i} a^i_j = 1 - \frac{1}{n}$, takes its smallest value and $B_{ij} = \frac{2}{n}$ for all j since i does not belong to any separating pair. For node i in class (B), $s_i - 1$ still takes its lowest value, however, compared to nodes in class (A), he has higher gap between socially optimal and equilibrium security investments. Note that for any node j that forms a separating pair with i, $\sum_j B_{ij} s_j < \frac{2}{n} \sum_j s_j$, and therefore Corollary 3 implies that nodes in class (B) have higher gaps between socially optimal and equilibrium investment levels than those in class (A). Finally, for a given node i in class (C), $s_i - 1 > 1 - \frac{1}{n}$, since $a^i_j > \frac{1}{n}$ for all j. Therefore, the gap in class (C) is strictly higher compared to the nodes in class (A) or (B).[25]

Intuitively, the social planner would like an agent to invest more when this agent is more of a gatekeeper, and thus her investment will protect a greater number of nodes in the network. Crucially, this is very different than the calculus that an agent engages in equilibrium, which, as we showed before, is related to how blocked the agent is by other nodes — her protection centrality. In general these two notions of centrality will not coincide, implying not only a gap between equilibrium and social optimum, but also that the ranking of nodes in terms of their investments in equilibrium and the socially optimal allocation will differ depending on the network positions of the nodes and the global properties of the network.

The next example illustrates some of these ideas by comparing equilibrium and social optimum investment level in different networks, and shows that even in tree networks, the node with the highest security investment in equilibrium could be different from the node with the highest security investment in the social optimum.

Example 2. Consider nodes x and y in the networks given in Fig. 4. In the star network, x has the lowest protection centrality and also has the highest gatekeeping centrality. Hence, x has the highest investment both in the equilibrium and the socially optimal investment. However, in the network given in Fig. 4b, y has the lowest protection centrality, but c and d have the highest gatekeeping centrality. This implies that $q^e_c < q^e_y$ while $q^s_c > q^s_y$.

[25] It is also useful to note that in tree networks, the ranking obtained by the gatekeeping centrality is the same as the betweenness centrality measure, though this is not generally the case for non-tree networks.



(a) Node x has the highest investment in both equilibrium and social optimum.

(b) Node y has the highest investment in equilibrium. Nodes c and d have highest investments in social optimum.

Fig. 4. The node with the highest security investment in the equilibrium may or may not coincide with the social optimum.

3.6. Equilibrium investment with probabilistic contagious links

In this and the next two sections, we consider various extensions of our baseline model and show that the main insights highlighted above continue to apply in these cases. To economize on space, we focus on equilibrium investments. We start with a generalization of the stochastic process by which an infection spreads over the network. In our baseline model, the infection is transmitted with probability 1 on any link (and is only prevented from further spreading when it encounters a node that is immune because of its security investments). Here we generalize this, assuming that each infected node transmits infection to any of his neighbors independently with probability $\beta \leq 1$, which defines a more general percolation process over the network (similar to the independent cascade model studied in Kempe et al., 2003). To study this, given a network $G = (V, E)$, we consider a random graph $G(\beta)$ constructed by including each edge of G with probability β, independent from every other edge. Equivalently, all graphs $G(V, \mathcal{E}')$ with $\mathcal{E}' \subseteq \mathcal{E}$, and $|\mathcal{E}'| = k$, have equal probability of $\beta^k(1-\beta)^{|E|-k}$.

Using this definition, let γ_{ij} denote the probability of j being connected to i in $G(\beta)$, so that $\gamma_i = \frac{1}{n}\sum_j \gamma_{ij}$ is the expected size of the component connected to i in $G(\beta)$. We also define σ^j_{ki}, as the probability of k being connected to i in $G_{-j}(\beta)$, where $G_{-j}(\beta)$ is the graph obtained from $G(\beta)$ after removing node j.

Based on these definitions, we define the *probabilistic gatekeeper* value of node j between node i and node k, as $z^j_{ik} = \gamma_{ik} - \sigma^j_{ik}$. Note that z^j_{ik} is similar to a^j_{ik}, and in fact if $\beta = 1$, we have $z^j_{ik} = a^j_{ik}$ since $\gamma_{ik} = 1$ and $\sigma^j_{ik} = 1 - a^j_{ik}$ (when $\beta = 1$, after removing j, i and k stay connected if and only if j is not a gatekeeper between them). Based on this definition, we define the *expected protection value* of node j for node i, denoted by z^j_i as the expected fraction of nodes for which j is a probabilistic gatekeeper to reach i.

Definition 5. The expected protection value of node j for node i, z^j_i is defined as $z^j_i \equiv \frac{1}{n}\sum_k z^j_{ik}$, with the convention that $z^i_i = 1$.

Intuitively the expected protection value of node j for node i defines how much of the infection can be blocked by j on its way to i. Similar to subsection 3.4, we first provide a characterization of network effect of G on i.

Proposition 5. *Given a random network $G(\beta)$ and security investments* $\mathbf{q}$*, we have*

$$\tilde{P}_i(G(\beta), \mathbf{q}) = \gamma_i - \sum_{j \neq i} q_j z_i^j + o\left(||\mathbf{q}||_\infty\right).$$

The first term on the right-hand side is the probability that the seed node is in the same connected component as i in $G(\beta)$, and the second term is the probability of i being protected by any other node j from i. Intuitively, z_i^j represents the expected protection of node j for node i, and when $\beta = 1$, this quantity is exactly a_i^j. We next characterize the equilibrium investments using Proposition 5.

Theorem 5. *Suppose Assumption 1 holds. For $\alpha = c''(0)$ sufficiently large, the equilibrium security investments satisfy*

$$\mathbf{q}^e = (\mathbf{Z} + \alpha \mathbf{I})^{-1} \gamma + o\left(\frac{1}{\alpha^2}\right), \tag{19}$$

where $\mathbf{Z}$ *is the matrix with $Z_{ij} = z_i^j$, and $Z_{ii} = 0$.*

This theorem provides a direct generalization of Theorem 3. To see the relationship between the two theorems more clearly, let us take another Taylor approximation, which gives

$$\mathbf{q}^e = \left(\frac{\mathbf{I}}{\alpha} - \frac{\mathbf{Z}}{\alpha^2}\right) \gamma + o\left(\frac{1}{\alpha^2}\right), \tag{20}$$

or

$$q_i^e = \frac{1}{\alpha}\left(\gamma_i - \frac{1}{\alpha} \sum_{k \neq i} z_i^k \gamma_k\right) + o\left(\frac{1}{\alpha^2}\right).$$

Eq. (20) can be directly compared to Eq. (11). In particular, when $\beta = 1$, Eq. (20) is the same as Eq. (11). More generally, when $\beta < 1$, the equilibrium investment of a node inherits the influences already highlighted in Theorem 3, but in addition, depends on the expected size of the component attached to that node in $G(\beta)$, given by γ_i. Moreover, the expected protection values of node j for node i is scaled by the expected size of the component of j, γ_j, which represents an approximation of the equilibrium security investment of j.

To see the difference that $\beta < 1$ makes, consider two different biconnected networks with four nodes, a ring network and a complete network. Let q_r^e denote the symmetric equilibrium investment of nodes in ring network, and q_c^e denote the symmetric equilibrium investment of nodes in complete network. For $\beta = 1$, using Eq. (11), we have

$$q_r^e \overset{\alpha}{\approx} q_c^e \overset{\alpha}{\approx} \frac{1}{\alpha}(1 - \frac{3}{4\alpha}).$$

When $\beta < 1$, Eq. (20) implies that the security investment of a node depends on γ_i, on whether it is blocked by other nodes, and how well connected those nodes are. Let γ_i^c and γ_i^r denote the expected size of the component attached to node i in the complete network and the ring network, respectively. Using Eq. (20), we calculate q_i^c and q_i^r for $\alpha = 2.5$ and for various values of β, as given in Fig. 5. It can be seen from this figure that when $\beta < 1$, the approximate equilibrium investments may be different in biconnected networks. In fact, when α is sufficiently large (where we can ignore terms of $o(\frac{1}{\alpha})$), equilibrium investment of node i is proportional to γ_i, and as the

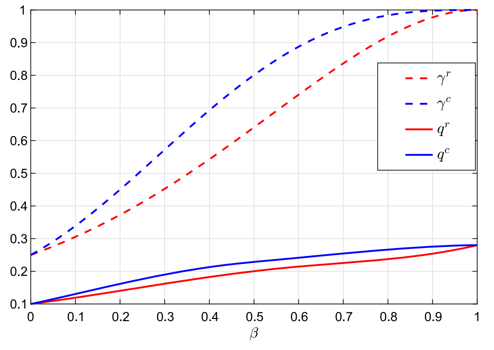


Fig. 5. Equilibrium security investments for various values of β, for a complete network and a ring network of size 4. (For interpretation of the references to color in this figure, the reader is referred to the web version of this article.)

network becomes denser, the equilibrium investment of all nodes increase. Moreover, in a given network, nodes with larger γ_i have higher equilibrium security investments.

3.7. Numerical results

Our results on the relationship of network and equilibrium investments were derived under the assumption that $\alpha = c''(0)$ is large (or equilibrium investment levels are small). A natural question is whether the relationships highlighted by our characterization in Theorem 3 also apply when this assumption does not hold. In this section, we shed some light on this question by comparing equilibrium investment levels in general to those obtained in Theorem 3, and show a close correspondence.

For illustration purposes, we focus on a star network (of 21 nodes), a ring network of 11 nodes, two attached rings of 4 nodes (7 nodes in total) and also a barbell network of 20 and 40 nodes. Throughout we take $\beta = 1$. The figures that follow plot, for $5 \leq \alpha \leq 100$, the approximation q_i^e calculated from Theorem 3 and the approximation from Eq. (12) as well as the exact equilibrium investment levels (see Figs. 6, 7, 8, 9). Note that for a complete network of any size, when $\beta = 1$, Eq. (12) and the exact solution are the same. For the other networks, as shown in these figures, the gap between either approximation and the exact solution is low and goes to zero as α increases.

3.8. Network formation and equilibrium investments

In our baseline model, the network of connections is taken as exogenous. Though this is a good starting point, it is natural to wonder whether endogenous changes in network would fundamentally alter the insights highlighted so far. To provide an answer to this question, in this section we consider a more general setting, where agents obtain utility from their connections and can decide to sever these links in order to protect themselves against infection. For simplicity, throughout this section we take $\beta = 1$.

Formally, we assume that, before the location of the attack is realized, each agent i decides which subset $\tilde{\mathcal{E}}_i \subset E$ of his initial connections to maintain as well as his security investment level, $q_i \in [0, 1]$, as before. A connection between two agents will be maintained only if both agents decide to maintain the connection, i.e., an edge (i, j) will be maintained, if and only if $(i, j) \in \tilde{\mathcal{E}}_i \cap \tilde{\mathcal{E}}_j$. We denote the set of maintained edges by $\hat{\mathcal{E}}$, and the induced network over these edges by $\hat{G}$, i.e.,

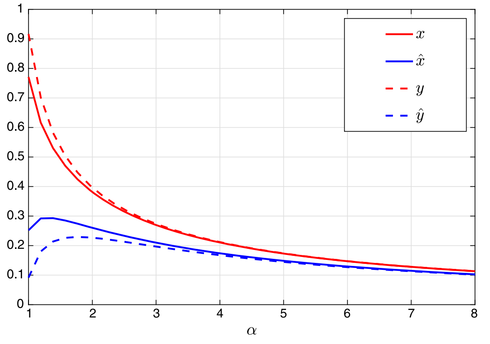


Fig. 6. Star network of size 21: the solid and dashed lines represent the exact and approximate equilibrium investments, respectively. (For interpretation of the references to color in this figure, the reader is referred to the web version of this article.)

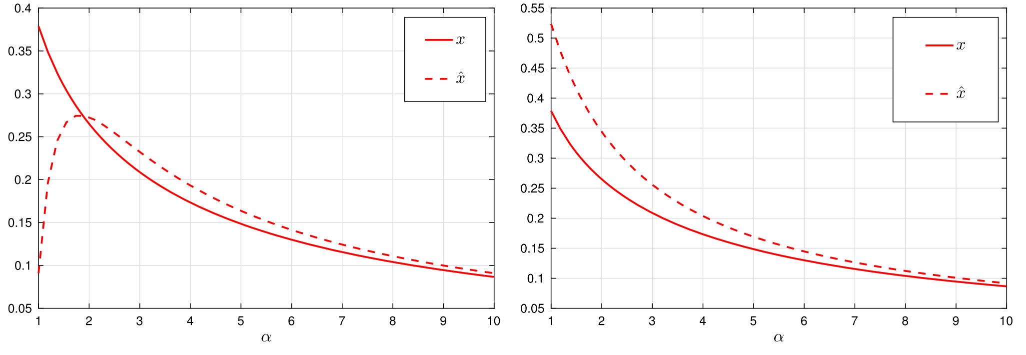


Fig. 7. Equilibrium security investment levels as a function of α for a ring network of size 11. The solid line plots the exact equilibrium investment. The dashed line in (a) plots the approximation from Eq. (12) and the dashed line in (b) plots the approximation from Theorem 3.

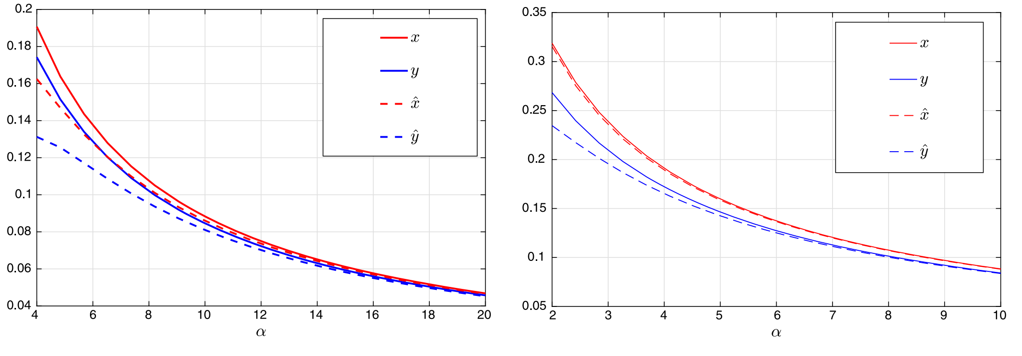


Fig. 8. Equilibrium security investment levels as a function of α for a barbell network of size 20. The solid line plots the exact equilibrium investment. The dashed line in (a) plots the approximation from Eq. (12) and the dashed line in (b) plots the approximation from Theorem 3. (For interpretation of the references to color in this figure, the reader is referred to the web version of this article.)

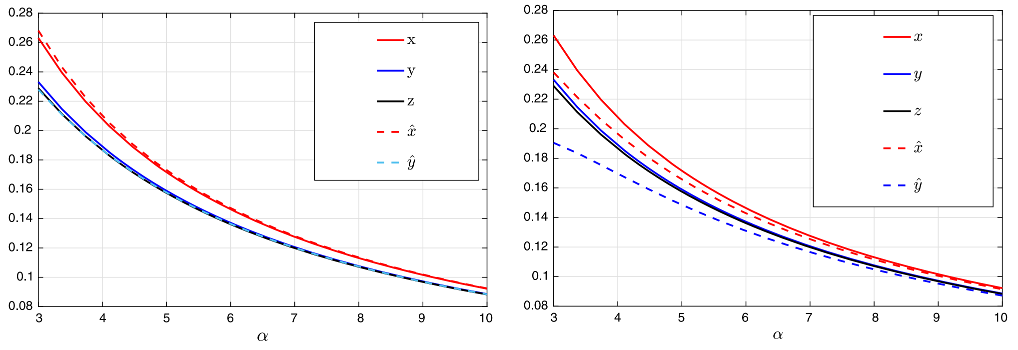


Fig. 9. Equilibrium security investment levels as a function of α for a connection of two rings of overall size 7. The solid line plots the exact equilibrium investment. The dashed line in (a) plots the approximation from Eq. (12) and the dashed line in (b) plots the approximation from Theorem 3. (For interpretation of the references to color in this figure, the reader is referred to the web version of this article.)

$$\hat{G} = (V, \hat{\mathcal{E}}), \quad \hat{\mathcal{E}} = \left\{(i, j) \in \mathcal{E} \ : \ (i, j) \in \tilde{\mathcal{E}}_i \cap \tilde{\mathcal{E}}_j\right\}.$$

Given $\hat{G}$ and security investments $\mathbf{q}$, the utility function of agent i is given by

$$u_i(\hat{G}, \mathbf{q}) = v_i|\hat{\mathcal{E}}_i|\left(1 - \mathbf{P}_i(\hat{G}, \mathbf{q})\right) - c_i(q_i), \tag{21}$$

where v_i is the value agent i derives from each connection conditional on being uninfected, and $\hat{\mathcal{E}}_i = \tilde{\mathcal{E}}_i \cap \hat{\mathcal{E}}$ (i.e., neighbors of agent i in $\hat{G}$). Similar to the rest of the paper, in this section, we assume $v_i = 1$. We further focus on a quadratic cost function $c(q) = \frac{\alpha}{2}q^2$ for simplicity.

Let $C_i(\hat{G})$ denote the size of the connected component attached to i in $\hat{G}$, and the component size vector of $\hat{G}$ is then defined as $\mathbf{C}(\hat{G}) = [C_i(\hat{G})]_{i \in V}$. Using a similar argument to that of Theorem 3, we first generalize the equilibrium investments characterization, removing the assumption that $\hat{G}$ is connected, and also allowing various agents to obtain different values when they are not infected. Note that in this setting Eq. (2) no longer holds. Instead, for a given network $\hat{G}$, we have

$$c'(B_i(\mathbf{q}_{-i})) = |\mathcal{E}_i|\tilde{P}_i(\hat{G}, \mathbf{q}_{-i}), \tag{22}$$

where $B_i(\mathbf{q}_{-i})$ denotes the security level that maximizes the utility of agent i. Furthermore, in this setting since $\hat{G}$ can be disconnected, we use an extension of Proposition 4 for a general (possibly disconnected) graph, i.e.,[26]

$$\tilde{P}_i(\hat{G}, \mathbf{q}) = \frac{C_i(\hat{G})}{n} - \sum_{j \neq i} a_i^j(\hat{G})q_j + o(||\mathbf{q}||_\infty).$$

We next provide a characterization of equilibrium investments $\mathbf{q}^e$ in terms of component size vector, degrees of the nodes and the protection values in $\hat{G}$.

Proposition 6. *Suppose Assumption 1 holds. Given a network $\hat{G}$ (not necessarily connected), for $\alpha = c''(0)$ sufficiently large, the equilibrium security investments are unique and satisfy*

[26] For a general network (possibly disconnected), we use the same definition for a_i^j, i.e., $a_i^j(\hat{G}) = \frac{1}{n}\sum_k a_{ki}^j(\hat{G})$. Note that if i and k are not connected in $\hat{G}$, $a_{ik}^j(\hat{G}) = 0$ for all j.

$$\mathbf{q}^e = \frac{1}{n}\left(\alpha\mathbf{I} + \mathbf{K}\hat{A}\right)^{-1}\mathbf{K}\mathbf{C}(\hat{G}) + o\left(\frac{1}{\alpha^2}\right),$$

where $\hat{A}$ is the matrix with $\hat{A}_{ij} = a_i^j(\hat{G})$, and $\mathbf{K} = Diag(|\mathcal{E}_1|, \cdots, |\mathcal{E}_n|)$.

For large α we can approximate the matrix inverse using Taylor's series approximation, i.e.,

$$\left(I + \frac{1}{\alpha}KA\right)^{-1} \overset{\alpha}{\approx} I - \frac{1}{\alpha}KA,$$

which yields the following characterization for equilibrium investments:

$$q_i^e \overset{\alpha}{\approx} \left[\frac{1}{n\alpha}\left(I - \frac{K\hat{A}}{\alpha}\right)K\mathbf{C}(\hat{\mathbf{G}})\right]_i = \frac{|\mathcal{E}_i(\hat{G})|}{\alpha}\left(\frac{C_i(\hat{G})}{n} - \frac{1}{\alpha}\sum_{j\neq i} a_i^j(\hat{G})|\mathcal{E}_j(\hat{G})|\frac{C_j(\hat{G})}{n}\right). \tag{23}$$

Note that $a_i^j(\hat{G}) \neq 0$ if and only if j and i reside on the same connected component. Therefore, we can rewrite Eq. (23) as

$$q_i^e \overset{\alpha}{\approx} (\frac{|\mathcal{E}_i(\hat{G})|C_i(\hat{G})}{n})\frac{1}{\alpha}\left(1 - \frac{1}{\alpha}\sum_{j\neq i} a_i^j(\hat{G})|\mathcal{E}_j(\hat{G})|\right). \tag{24}$$

When $\hat{G}$ is connected, $\frac{C_i(\hat{G})}{n} = 1$, for all i, therefore, for α sufficiently large, q_i^e is proportional to $|\mathcal{E}_i|$, which implies that nodes with higher degree invest in more security. For an agent i with a given degree, the equilibrium investments also depend on $\sum_{j\neq i} a_i^j(\hat{G})|\mathcal{E}_j(\hat{G})|$, which means how protected node i is by other nodes of high degree. We next characterize the equilibrium network, once again under the assumption of $c''(0) = \alpha$ sufficiently large. Using Eq. (22), we have

$$u_i(\hat{G}, \mathbf{q}^e) = |\mathcal{E}_i|\left((1 - (1 - q_i^e)\tilde{P}_i(\hat{G}, \mathbf{q}_{-i}^e)\right) - c(q_i^e) = |\mathcal{E}_i| - (1 - q_i^e)c'(q_i^e) - c(q_i^e)$$

Since $c(q) = \frac{\alpha}{2}q^2$, using Eq. (24), the utility of agent i in the equilibrium can be expressed as

$$u_i(\hat{G}, \mathbf{q}^e) = |\mathcal{E}_i|(1 - \frac{C_i(\hat{G})}{n}) - \frac{1}{\alpha}\left(\frac{|\mathcal{E}_i|C_i(\hat{G})}{n}(\sum_{j\neq i} a_i^j|\mathcal{E}_j| - \frac{1}{2})\right) + o(\frac{1}{\alpha}).$$

This expression allows us to decompose the optimization problem of agent i: she first decides on the connections she maintains to maximize the number of connections times the probability of infection not being present in this component, then she selects her security investment according to Eq. (24).

Proposition 7. *Suppose $c(q) = \frac{\alpha}{2}q^2$. For α sufficiently large, in the network formation equilibrium, agents maintain connections to maximize $|\hat{\mathcal{E}}_i|\left(1 - \frac{C_i(\hat{G})}{n}\right)$ in the equilibrium, where $\hat{\mathcal{E}}_i = \tilde{\mathcal{E}}_i \cap \tilde{\mathcal{E}}_{-i}$, and $\hat{G} = (V, \hat{\mathcal{E}})$ with $\hat{\mathcal{E}} = \cup_{j\in V}\tilde{\mathcal{E}}_j \cap \tilde{\mathcal{E}}_{-j}$.*

Intuitively, agents try to decrease the size of the connected component they belong to by dropping some of their connections, while maintaining as many edges as possible. When an agent decreases her degree, there are two forces affecting her utility: (i) the size of her connected component (i.e., $C_i(\hat{G})$) decreases, resulting in larger utility (because with a smaller connected component, the risk of infection goes down); (ii) the size of her neighborhood (i.e., $|\hat{\mathcal{E}}_i|$) decreases, resulting in smaller utility.[27]

Overall, this characterization implies that the same forces as in Theorem 3 continue to apply when agents decide on their equilibrium security investments. However, we also obtain additional insights in this case as both security investments and individuals' connection decisions depend on others' connection decisions, which determine the size of the connected component in the graph.

4. Strategic attack model

We have so far focused on the random attack model where the attack decision Φ is determined randomly and independently from the security investments of the agents. In many applications, however, the attack is not a random event, but the act of a strategic adversary, intended on causing maximum damage. This, in particular, implies that the location of the attack will in general depend on network positions and security investments. In this section, we focus on this latter case. The main insight is that strategic attack generates a clear, new force towards overinvestment in security relative to the socially optimal security investments.

We consider a strategic attacker which, after observing the security profile of agents, selects an attack decision $\Phi = (\phi_1, \ldots, \phi_n)$ (where ϕ_i is the probability of attacking agent i) to maximize his utility given by expected infections minus the cost of the attack decision. We assume that the cost of an attack decision Φ is given by $\sum_{i=1}^{n} \zeta(\phi_i)$ where ζ is a convex function. We introduce a convex cost function for the attacker both for substantive and technical reasons. Substantively, targeting attacks according to the investment vector would require very precise knowledge about each agent's investments. A convex cost function enables us to capture the idea that the closer the attacker would like to come to precisely targeting one agent over all others, the greater the cost it has to incur. Most importantly, the convexity of this cost function will also contribute to the existence of a pure-strategy equilibrium as we explain next.

Because in our model the attacker observes the security level of all the agents, the relevant equilibrium concept is that of the *Stackelberg equilibrium* of the resulting two stage game: the agents first select their security levels anticipating the decision of the attacker and the attacker optimizes his attack strategy given the security choices. We refer to it simply as "equilibrium" to simplify terminology.

The next example shows that, without the convexity of ζ, a pure-strategy equilibria may fail to exist for reasons similar to the non-existence of pure-strategy equilibria in Bertrand competition with capacity constraints, as the next example illustrates.

Example 3. Consider the network G with 2 singleton agents. We show that attacking a single agent without cost may lead to non-existence of a pure-strategy equilibrium. For any security profile $\mathbf{q}$, the attacker selects the agent with minimum security level to attack. We next consider all possible candidates for a pure-strategy equilibrium and present a profitable deviation for each candidate, establishing non-existence:

[27] Note however that the equilibrium solution may not be unique; see Appendix A for details.

Finally, though most of the results in this section can be derived for general convex cost functions for the attacker, in the remainder we simplify the analysis by assuming a quadratic form:

Assumption 2 *(Attack cost).* $\zeta(\phi) = \frac{\theta}{2}\phi^2$.

4.1. Equilibrium in the strategic attack model

In this section, we study the equilibrium in the strategic attack model with convex cost. In the rest of this section, we will use the following notation. We use 1_n to denote the vector of dimension n with each entry equal to $\frac{1}{n}$, e_i to denote the vector of all 0's except the ith entry which is 1, e to denote the vector of all 1's, and $I(G, \mathbf{q}, \Phi)$ to denote the expected number of infected people given the security profile $\mathbf{q}$ and attack decision Φ. The utility function of the attacker, given network G, security profile $\mathbf{q}$, and an attack decision $\Phi = (\phi_1, \ldots, \phi_n)$, $u_a(G, \mathbf{q}, \Phi)$ is defined as follows:

$$u_a(G, \mathbf{q}, \Phi) = \sum_{i=1}^{n} \phi_i \frac{I(G, \mathbf{q}, e_i)}{n} - \zeta(\phi_i).$$

In this model, since the security choices of agents impact the location of the attack, the network effect on an agent is no longer independent of his security level, i.e., Proposition 1 does not hold for this model. This implies that security investments will no longer satisfy the characterization we used so far, cf. Eq. (2).

Nevertheless, expected infections when agent i is targeted (in the strategic attack model) are closely linked to the infection probability of agent i under random attack model (where, recall each agent is attacked with equal probability independent of their security investments). This property enables us to use the decomposition similar to that in Proposition 1 to write the utility function of the attacker in closed form.

Lemma 6. *Given network G and security profile $\mathbf{q}$, expected infections when agent i is attacked is $I(G, \mathbf{q}, e_i) = n\mathbf{P}_i(G, \mathbf{q}, 1_n) = n(1 - q_i)\tilde{P}_i(G, \mathbf{q}_{-i}, 1_n)$.*

Intuitively, the infection probability of agent i under the random attack model is the probability of having a path between i and a randomly selected agent. Conveniently, expected infections when i is attacked are given by the sum (over all j) of the probability of having a path between i and j, and thus the two quantities are closely linked as shown in the lemma. Using this result, we next prove:

Theorem 7. *In the strategic attack model, suppose that $c''(q)\theta \geq 2n$ and $\theta \geq n$. Then there exists a pure-strategy equilibrium.*

The condition in this theorem is sufficient to ensure concavity of each agent's utility in their own investment. This theorem clarifies the role of the parameter θ. When $\theta = 0$, so that the attacker can target any node without cost, Example 3 showed the possibility that a pure-strategy equilibrium may fail to exist. The condition in this theorem prevents this possibility. In the next subsection, we show that for symmetric networks equilibria in the strategic attack model may involve overinvestment.

4.2. Strategic attacks in symmetric networks

In this subsection, we consider the strategic attack model over symmetric networks. As explained in subsection 3.3, in the random attack model the security investments create positive externalities on others. Our results so far have shown that, under our baseline assumptions, this force ensures that expected equilibrium infections are greater than expected infections in the social optimum (see in particular Corollary 3). In the strategic attack model, however, security investments also create negative externalities on others because they divert the attacker to other agents. The next example shows the possibility of overinvestment with strategic attacks.

Example 4. Consider the line network with two agents and suppose the investment cost function is $c'(q) = \frac{q}{2(1-q)}$ for both agents, and attacker cost function is $\zeta(\phi) = \frac{\phi^2}{24}$. It can be verified that the unique (pure-strategy) Nash equilibrium is $\mathbf{q}^e = (0.66, 0.66)$ while the socially optimal security profile is $\mathbf{q}^s = (0.63, 0.63)$.

The force towards overinvestment is intuitive: by investing more, an agent not only reduces the probability of infection conditional on attack, but also discourages attacks. The strategic attacker would prefer to target a low-investment node from where a successful attack can spread. A high level of investment, on the other hand, increases the likelihood that the attack will be dead in its tracks. This implies that, in addition to the positive externality identified so far (that security investments reduce infection probability for the rest of the network), there is a negative externality (that high security investments increase the probability that the attacker will target another agent). The example provides an instance where the negative externality dominates the positive externality, leading to overinvestment relative to the socially optimal investment levels. In fact, in contrast to our random attack model, our strategic attack model has elements of both strategic substitutes and complements. The latter element arises from the response of the strategic attacker who becomes more likely to target a node when others are investing more, thus inducing the node in question to also increase its investment. It is through this channel that there is an "arms race" between different nodes in this model, whereby each invests more in order to discourage the attack, in the process potentially amplifying the negative externalities they impose on others. This arms race was at the root of the non-existence problem in Example 3, and even though it does lead to non-existence of pure-strategy equilibria here, it does undergird overinvestment.

The next theorem provides a characterization of over- and underinvestment relative to the socially optimal investment levels in strongly symmetric networks. We first define strongly symmetric networks before stating the result.

Definition 6 *(Strongly symmetric network).* A network G is strongly symmetric if any permutation $\pi : V \to V$ is an automorphism. Similarly, a random network G drawn from a probability space $(\Omega, \mathbb{F}, \mathbb{P})$ is strongly symmetric if by applying any permutation $\pi : V \to V$ the probability space of the random graph stays unchanged.

Note that rings are symmetric but not strongly symmetric. Examples of strongly symmetric networks include complete networks, Erdős–Rényi random graphs and random graphs with arbitrary degree distributions. Note also that for random networks, the interaction network need not be symmetric; rather, agent locations within the network are identical in expectation.

Theorem 8. *Suppose Assumptions 1 and 2 hold and the network G is strongly symmetric. Then a pure-strategy symmetric Nash equilibrium always exists. Furthermore, if $\theta \geq 1$ underinvestment always happens and if for all $q \in [0, 1]$, $c''(q)\theta > n$ and $\theta \leq \frac{n-1}{n^2} c'^{-1}(\frac{1}{n})$ then overinvestment will happen.*

The conditions for under/overinvestment in the theorem are intuitive and are related to the degree of convexity of the attacker's cost function. Overinvestment requires this cost function not to be "too convex" (θ not too high), whereas underinvestment results when the cost function is highly convex (θ high). To understand this, recall the discussion of negative externalities in the strategic attack model provided above. If the attacker's cost function were very convex, then the attacker would end up choosing probabilities of attack very close to those in the random attack model (uniform across all agents), thus muting the negative externalities resulting from the agents' responses to a strategic attack.

4.3. Network centrality and strategic attack equilibrium investments

In this subsection, we provide a characterization of equilibrium security investments for strategic attack model for a general network. This characterization highlights how the presence of strategic attacks changes investments relative to the random attack model and determines how equilibrium investments vary by network position. Let us first define d^j_{ik} as the difference of the protection value of j for i when k is targeted and the protection value of j for i in the random attack model. Note that the gatekeeper indicator variable a^j_{ik} specifies whether j can block the infection reaching i when k is attacked. With this interpretation, we can express d^j_{ik} as

$$d^j_{ik} = a^j_{ik} - \frac{1}{n}\sum_k a^j_{ik} = a^j_{ik} - a^j_i .$$

This quantity captures whether node j becomes more of a gatekeeper when node k is attacked compared to the random attack profile. Based on this definition, we define inverse scaled protection of node k for node i, denoted by d^j_i, as follows:

Definition 7. Given network G, for two nodes i, j, the scaled protection of j for i is $d^j_i = \sum_k a^i_k d^j_{ik} = \sum_k a^i_k (a^j_{ik} - a^j_i)$ We also define the inverse scaled protection of node i, d_i, as the negative of the sum of scaled protection of all nodes for node i, i.e., $d_i = -\sum_{j \neq i} d^j_i$.

Note that a^i_k is proportional to the number of people infected through i when k is attacked, which reflects the probability of agent k being attacked, and d^j_{ik} denotes how much the protection of the node j for node i increases when k is attacked instead of having a random attack. Hence, scaled protection of j for i, d^j_i, represents the expected increase in the protection value of j for i in the strategic attack model compared to the random attack model and d_i represents the change in the expected protection of i in the strategic attack compared to the random attack model. We next provide a characterization of strategic attack equilibrium investments in terms of scaled protection measures.

Theorem 9. *Suppose Assumptions 1 and 2 hold and $\alpha = c''(0)$ and θ are sufficiently large. In the strategic attack model the equilibrium investments are given by*

$$\mathbf{q}^{stattack} \overset{\alpha}{\approx} (D + \alpha I)^{-1} e,$$

where $D_{ij} = a_i^j + \frac{d_i^j}{\theta}$ *for* $j \neq i$, $D_{ii} = 0$.

This characterization shows how security investments in the strategic attack model compare to the random attack model. Note that if $d_i^j = 0$, then $D_{ij} = A_{ij}$.

We next present an alternative characterization of equilibrium security investments in the strategic attack model in terms of the inverse scaled protection of each agent, d_i. In particular, under the assumption that α is large, equilibrium investments can be expressed as

$$\mathbf{q}^{stattack} \overset{\alpha}{\approx} \frac{1}{\alpha}\left(I - \frac{D}{\alpha}\right) e.$$

Expanding the right hand side, we have

$$q_i^{stattack} \overset{\alpha}{\approx} \frac{1}{\alpha}\left(1 - \frac{1}{\alpha}\sum_j D_{ij}\right) = q_i^e + \frac{1}{\alpha^2\theta} d_i,$$

or

$$q_i^{stattack} - q_e^i \overset{\alpha}{\approx} \frac{1}{\alpha^2\theta} d_i,$$

where q_i^e denotes the equilibrium investment of node i in the random attack model. It reflects the fact that some nodes will voluntarily increase their investment to decrease the probability of attack on nodes that they are not well protected against. Using this inverse scaled protection measure, we obtain the following characterization of strategic attack equilibrium investments relative to the random attack equilibrium investments.

Corollary 4. *Suppose Assumptions 1 and 2 hold. For $\alpha = c''(0)$ and θ sufficiently large, for a given network, the node with the greatest inverse scaled protection measure, d_i, has the greatest gap between random attack equilibrium security investment and the strategic attack equilibrium security investment.*

To relate the inverse scaled protection measure to underlying network properties, we first consider tree networks. We first provide a characterization of d_i for tree networks based on average distance of nodes to i and the size of subtrees of i. We also show that d_i can take both positive and negative values, which implies that depending on the position of an agent in the graph, the equilibrium security investment in the strategic attack model might be lower or higher compared to the random attack model. In particular, for node i, let $C_1, \ldots, C_k$ denote the size of the subtrees obtained after removing i, and let Δ_j denote the average distance of the nodes in the subtree j to node i. For a tree network, we have

$$d_i = \frac{\sum_{j=1}^k C_j^2}{n}\left(\frac{\sum_{j=1}^k \Delta_j C_j^2}{\sum_{j=1}^k C_j^2} - \frac{\sum_{j=1}^k \Delta_j C_j}{\sum_{j=1}^k C_j}\right) \tag{25}$$

(see the appendix for the proof). This is equivalent to comparing the weighted average of distances with two different weights. For larger components, the weights of the first term are higher than the weights of the second term. Using Holders inequality, one can further show that if the larger subtrees have greater average distance, then this value is always positive, and thus the

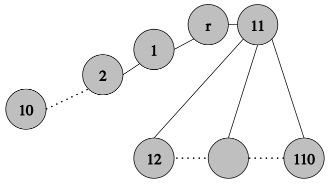


Fig. 10. The security investment of node r in the equilibrium is lower in the strategic attack model compared to the random attack model.

agent in question will choose a greater security investment in the strategic attack model than in the random attack model. Note that in this scenario, an agent would like to shift the attack away from low average distance subtrees and towards a higher average distance component. This would enable her to have a larger distance from the source of the infection, which would increase her security.

On the other hand, if larger subtrees have smaller average distances, then this value is negative, inducing the agent to choose a lower level of investment in the strategic attack model than in the random attack model. Intuitively, agents are now taking into account the differential attack probability they will be subject to (relative to the random attack model). Some agents, because they are a convenient pathway to other nodes in the network, will particularly act strategically to direct the attacker to one or another part of the network. Recognizing this, they will choose greater or lower security investments. These considerations are captured by the inverse scaled protection measure, d_i, which approximates the scale with which i can direct the attacker toward another agent times the effect of this manipulation on i's protection.

In general networks, in a biconnected component, any non-cut vertex i has $d_i > 0$, since

$$d_i = \sum_{j \neq i} a_i^j \sum_k a_k^i - \sum_k a_k^i \sum_{j \neq i} a_{ik}^j = \frac{2n-1}{n} \sum_{j \neq i} a_i^j - \sum_k \frac{1}{n} \sum_{j \neq i} a_{ik}^j = \frac{n-1}{n} \sum_{j \neq i} a_i^j > 0$$

This implies that these nodes have greater security investments in the strategic attack model compared to the random attack model. The next example illustrates these considerations.

Example 5. Consider Fig. 10. The inverse scaled protection measure of node r, d_r, is given by

$$d_r = \frac{1}{111}(20450 - 23111.71) = -23.979,$$

which implies that $q_r^{stattack} < q_r^e$. In general, node r invests less in the strategic attack model than in the random attack model when the "large" subtrees connected to r have "small" average distances to r while small subtrees connected to r have high average distances to r.

5. Conclusion

In this paper, we developed a theoretical model of security investments in a network of interconnected agents. An infection spreads over a network of agents depending on the profile of security investments by the agents. We provided a tractable decomposition of individual payoffs into an own effect and an externality, and use this decomposition to show how individual investments can be characterized recursively (by considering the network with one agent removed at a time). This enables us to establish a tight characterization of equilibrium and socially optimal investment levels and link those to the structure of the network. We showed that two new measures of network centrality, one related to how protected an individual is by gatekeepers in the network and the other to how much of a gatekeeper the agent is to the rest of the network, shape equilibrium and socially optimal levels of security investments.

We then extended this framework to allow for the case of strategic attack where an attacker chooses a probability distribution over the location of the attack in order to maximize damage. We showed that the same decomposition applies in this case and enables a similar characterization of equilibrium (and its relationship to certain network centrality measures). But a new economic force now changes the nature of incentives: greater investment by an agent shifts the attack to other parts of the network. This implies that the equilibrium may now involve too much investment relative to the social optimum.

We believe that our paper points to several interesting directions for research. First, our sharpest results focus on the case in which high costs lead to relatively low levels of security investments. Identifying the more general relationship between the structure of the network and equilibrium and socially optimal levels of investments is more challenging and may require different mathematical approaches. Second, an interesting extension would consider the case where some agents control or influence the security investments of several nodes in the network (e.g., domains or software providers in computer networks). Third, an interesting direction is to allow real-time defense against the spread of infections, for example, in the form of dynamic responses as agents or a centralized domain observe the spread of the infection over time.

Appendix A

Proof of Proposition 1 (Network effect). Agent i gets infected only if i is susceptible. Let (X_i) denote the event that agent i is susceptible. The infection probability of i can be stated as

$$\mathbf{P}_i(G, \mathbf{q}, \Phi) = \mathbf{P}_i(G, \mathbf{q}, \Phi|(X_i))(1 - q_i). \tag{A.1}$$

We next show that $\mathbf{P}_i(G, \mathbf{q}, \Phi|(X_i))$ does not depend on q_i. Let $i \xrightarrow{G^t} j$ denote the event that i is connected to j in the transmission network G^t. By definition, i gets infected if $i \xrightarrow{G^t} s$. The infection probability of i conditional on (X_i) can be written as

$$\begin{aligned}\mathbf{P}_i(G, \mathbf{q}, \Phi|(X_i)) &= \sum_{\{G^t | s \in G^t \,\&\, i \xrightarrow{G^t} s\}} P_{(G,\mathbf{q})}(G^t|(X_i)) \\ &= \sum_{\{G^t | s \in G^t \,\&\, i \xrightarrow{G^t} s\}} \sum_{\{V_s \subseteq V | G^t = G[V_s]\}} \prod_{j \in V_s\, j \neq i} (1 - q_j) \prod_{j \notin V_s} q_j.\end{aligned}$$

Second equality follows from the definition of the probability of the transmission network and the fact that conditional on (X_i), $i \in V_s$. This shows that $\mathbf{P}_i(G, \mathbf{q}, \Phi|(X_i))$ is independent of q_i. Substituting $\mathbf{P}_i(G, \mathbf{q}, \Phi|(X_i))$ with $\tilde{P}_i(G, \mathbf{q}_{-i}, \Phi)$ in Eq. (A.1) we have $\mathbf{P}_i(G, \mathbf{q}, \Phi) = (1 - q_i)\tilde{P}_i(G, \mathbf{q}_{-i}, \Phi)$. □

Proof of Proposition 2 (Decomposition). Let (X_i) denote the event that agent i is susceptible, $i \xrightarrow{G^t} j$ denote the event that i is connected to j in G^t, and let s denote the seed node. In the transmission network $G^t \sim (G, \mathbf{q})$, for two agents j and i with $i \neq j$, one of the following mutually exclusive events will happen: (A) s is connected to j in G^t_{-i}, (B) s is not connected to j in $G^t{}_{-i}$, but is connected to j in G^t, or (C) s is not connected to j in G^t. Agent j gets infected if event (A) or (B) happens. We next express infection probability of agent j as the sum of probabilities of events (A) and (B). Let $i \xrightarrow{G} j$ denote the event that i is connected to j in G. Also, let $\mathbb{G}^j$ denote the collection of transmission networks in which j is connected to s, i.e., $\mathbb{G}^j = \{G^t \sim (G, \mathbf{q}) | j \xrightarrow{G^t} s\}$. The infection probability of agent j can be written as

$$\mathbf{P}_j(G, \mathbf{q}, \Phi) = \sum_{G^t \in \mathbb{G}^j} P_{(G,\mathbf{q})}(G^t)$$
$$= \sum_{\{G_t | G^t_{-i} \in \mathbb{G}^j_{-i}\}} P_{(G,\mathbf{q})}(G^t) + \sum_{\{G^t | G^t_{-i} \notin \mathbb{G}^j_{-i} \bigwedge G^t \in \mathbb{G}^j\}} P_{(G,\mathbf{q})}(G^t), \tag{A.2}$$

where the first and the second term in the last equation are the probabilities of event (A) and (B), respectively. We show that the first term can be written as $\mathbf{P}_j(G_{-i}, \mathbf{q}_{-i}, \Phi)$. By definition,

$$\mathbf{P}_j(G_{-i}, \mathbf{q}_{-i}, \Phi) = \sum_{\{\bar{G}^t | \bar{G}^t \in \mathbb{G}^j_{-i}\}} P_{(G_{-i}, \mathbf{q}_{-i})}(\bar{G}^t). \tag{A.3}$$

The probability of the transmission network $\bar{G}^t$ generated from $(G_{-i}, \mathbf{q}_{-i})$ is the marginal probability of G^t that satisfies $G^t_{-i} = \bar{G}^t$, i.e., $P_{(G_{-i},\mathbf{q}_{-i})}(\bar{G}^t) = \sum_{\{G^t | G^t_{-i} = \bar{G}^t\}} P_{(G,\mathbf{q})}(G^t)$. Combining the preceding relation with Eq. (A.3), we obtain

$$\mathbf{P}_j(G_{-i}, \mathbf{q}_{-i}, \Phi) = \sum_{\{\bar{G}^t | \bar{G}^t \in \mathbb{G}^j_{-i}\}} \sum_{\{G^t | G^t_{-i} = \bar{G}^t\}} P_{(G,\mathbf{q})}(G^t) = \sum_{\{G^t | G^t_{-i} \in G^j_{-i}\}} P_{(G,\mathbf{q})}(G^t),$$

which shows the desired result. We next rewrite the second term in Eq. (A.2), i.e., probability of event (B) by conditioning it on the event that i and j are susceptible.

$$\sum_{\{G^t | G^t_{-i} \notin \mathbb{G}^j_{-i} \bigwedge G^t \in \mathbb{G}^j\}} P_{(G,\mathbf{q})}(G^t)$$
$$= (1 - q_i)(1 - q_j) \sum_{\{G^t | G^t_{-i} \notin \mathbb{G}^j_{-i} \bigwedge G^t \in \mathbb{G}^j\}} P_{(G,\mathbf{q})}(G^t | (X_i) \cap (X_j)). \tag{A.4}$$

Let $Q_{j,i}$ be the function that represents the probability of event (B) conditional on the event $(X_i) \cap (X_j)$. Clearly, $\sum_{\{G^t | G^t_{-i} \notin \mathbb{G}^j_{-i} \bigwedge G^t \in \mathbb{G}^j\}} P_{(G,\mathbf{q})}(G^t | (X_i) \cap (X_j))$ only depends on $\mathbf{q}_{-\{i,j\}}$ and G and is independent of q_i and q_j. Hence, $Q_{j,i}$ is a function of G, $\mathbf{q}_{-\{i,j\}}$, and Φ. Hence, it can be expressed as $Q_{j,i}(G, \mathbf{q}_{-\{i,j\}}, \Phi)$. Combining the preceding relation with Eqs. (A.2), (A.3), and (A.4) and using Proposition 1, we obtain

$$\mathbf{P}_j(G, \mathbf{q}, \Phi) = \mathbf{P}_j(G_{-i}, \mathbf{q}_{-i}, \Phi) + (1 - q_i)(1 - q_j) Q_{j,i}(G, \mathbf{q}_{-\{i,j\}}, \Phi)$$
$$= (1 - q_j)\left(\tilde{P}_j(G_{-i}, \mathbf{q}_{-i}, \Phi) + (1 - q_i) Q_{j,i}(G, \mathbf{q}_{-\{i,j\}}, \Phi)\right).$$

By applying Proposition 1 to the preceding equation, we obtain

$$\tilde{P}_j(G, \mathbf{q}_{-j}, \Phi) = \frac{\mathbf{P}_j(G, \mathbf{q}, \Phi)}{1 - q_j} = \tilde{P}_j(G_{-i}, \mathbf{q}_{-\{i,j\}}, \Phi) + (1 - q_i) Q_{j,i}(G, \mathbf{q}_{-\{i,j\}}, \Phi),$$

which shows the desired result. □

Proof of Theorem 1 (Equilibrium existence). We show the uniqueness of equilibrium when $c''(x) \geq n$, using the result by Rosen (1965). The strategy space of each agent in this problem is $q_i \in [0, 1]$ which is a compact set and can be defined as all q for which $h(q) = q - q^2$ is greater or equal 0. We next show that the utility of each agent is diagonally strictly concave. A set of payoff functions $(u_1, ..., u_I)$ are diagonally strictly concave, if for every $x^*, \bar{x} \in S$, we have $(\bar{x} - x^*)^T \nabla u(x^*) + (x^* - \bar{x})^T \nabla u(\bar{x}) > 0$. Rosen (1965) showed that given a strategic form game, if the strategy space S_i of each agent can be represented by $S_i = \{x_i \in R^{m_i} | h_i(x_i) \geq 0\}$, where $h_i(\cdot)$ is a concave function, if there exists some $\bar{x}_i \in R^{m_i}$ such that $h_i(\bar{x}_i) > 0$, and if the payoff functions $(u_1, \ldots, u_I)$ are diagonally strictly concave for $x \in S$, then the game has a unique pure-strategy Nash equilibrium. Furthermore, Rosen showed that a sufficient condition for diagonal concavity is to have the symmetric matrix $(U(x) + U^T(x))$ being negative definite for all $x \in S$, where $U(x)$ is the Jacobian of $\nabla u(x)$. i.e., if for all $x \in S$, we have $y^T(U(x) + U^T(x))y < 0 \; \forall y \neq 0$, then the payoff functions $(u_1, ..., u_I)$ are diagonally strictly concave for $x \in S$. Let us define matrix U as follows:

$$U = \begin{pmatrix} \frac{\partial^2 u_1(\mathbf{q})}{(\partial q_1)^2} & \frac{\partial^2 u_1(\mathbf{q})}{\partial q_1 \partial q_2} & \cdots \\ \frac{\partial^2 u_2(\mathbf{q})}{\partial q_2 \partial q_1} & \ddots & \\ \vdots & & \end{pmatrix} = \begin{pmatrix} -c''(q) & -Q_{12}(G, q) & \cdots \\ -Q_{21}(G, q) & \ddots & \\ \vdots & & \end{pmatrix}$$

From Rosen (1965), it is sufficient for the uniqueness of pure-strategy Nash equilibrium to show that $U + U^T$ is negative definite. Since $Q_{ji}(G, q) \leq 1$, from Gershgorin's Theorem we obtain $c''(q) \geq n \geq \sum_j Q_{ji}(G, q)$ as a sufficient condition. □

Proof of Proposition 3.

(a) Network effect monotonicity in security profile: We first show that given network G and two security profiles $\mathbf{q}_{-i}$ and $\hat{\mathbf{q}}_{-i}$ with $\mathbf{q}_{-i} \geq \hat{\mathbf{q}}_{-i}$, we have $\tilde{P}_i(G, \mathbf{q}_{-i}, \Phi) \leq \tilde{P}_i(G, \hat{\mathbf{q}}_{-i}, \Phi)$. Let $\hat{V}$ denote the set of agents with strictly higher security levels in the security profile $\mathbf{q}$ compared to $\hat{\mathbf{q}}$, i.e., $\hat{V} = \{v \in V_{-i} \mid q_v > \hat{q}_v\}$. We prove the claim by induction on $|\hat{V}|$. The base case is immediate: If $|\hat{V}| = 0$, then $q_v = \hat{q}_v$ for all $v \in V_{-i}$. Hence, $\tilde{P}_i(G, \mathbf{q}_{-i}, \Phi) = \tilde{P}_i(G, \hat{\mathbf{q}}_{-i}, \Phi)$. We next assume that for an integer $m > 0$, if $|\hat{V}| = m$, the claim holds, i.e., $\tilde{P}_i(G, \mathbf{q}_{-i}, \Phi) \leq \tilde{P}_i(G, \hat{\mathbf{q}}_{-i}, \Phi)$ (Induction Hypothesis). We will next prove that the claim still holds if $|\hat{V}| = m + 1$. Consider an arbitrary agent $1 \in \hat{V}$. Define a new security profile $\tilde{\mathbf{q}}$ such that $\tilde{q}_v = q_v$ for all $v \neq 1$, and $\tilde{q}_1 = \hat{q}_1$. Note that $\mathbf{q}_{-i}$ and $\tilde{\mathbf{q}}_{-i}$ only differ in the security level of agent 1. We first show that $\tilde{P}_i(G, \mathbf{q}_{-i}, \Phi) \leq \tilde{P}_i(G, \tilde{\mathbf{q}}_{-i}, \Phi)$. Using Proposition 2 (with the identification $j = i$ and $i = 1$), we can rewrite $\tilde{P}_i(G, \mathbf{q}_{-i}, \Phi)$ as

$$\begin{aligned} \tilde{P}_i(G, \mathbf{q}_{-i}, \Phi) &= \tilde{P}_i(G_{-1}, \mathbf{q}_{-\{1,i\}}, \Phi) + Q_{i,1}(G, \mathbf{q}_{-\{i,1\}}, \Phi)(1 - q_1) \\ &\leq \tilde{P}_i(G_{-1}, \mathbf{q}_{-\{1,i\}}, \Phi) + Q_{i,1}(G, \mathbf{q}_{-\{i,1\}}, \Phi)(1 - \tilde{q}_1) \\ &= \tilde{P}_i(G_{-1}, \tilde{\mathbf{q}}_{-\{1,i\}}, \Phi) + Q_{i,1}(G, \tilde{\mathbf{q}}_{-\{i,1\}}, \Phi)(1 - \tilde{q}_1) = \tilde{P}_i(G, \tilde{\mathbf{q}}_{-i}, \Phi). \end{aligned} \tag{A.5}$$

The inequality follows from $\tilde{q}_1 = \hat{q}_1 < q_1$ and the last equality follows from $\tilde{q}_j = q_j$ for all $j \neq 1$. We next compare $\tilde{P}_i(G, \tilde{\mathbf{q}}_{-i}, \Phi)$ with $\tilde{P}_i(G, \hat{\mathbf{q}}_{-i}, \Phi)$. First note that $\tilde{\mathbf{q}} \geq \hat{\mathbf{q}}$. Moreover, we have $|\{j \in V_{-i} \mid \tilde{q}_j > \hat{q}_j\}| = m$. Induction hypothesis implies that $\tilde{P}_i(G, \tilde{\mathbf{q}}_{-i}, \Phi) \leq \tilde{P}_i(G, \hat{\mathbf{q}}_{-i}, \Phi)$. Combining with Eq. (A.5), we obtain $\tilde{P}_i(G, \mathbf{q}_{-i}, \Phi) \leq \tilde{P}_i(G, \hat{\mathbf{q}}_{-i}, \Phi)$.

(b) Network effect monotonicity in network density: We show that given $\hat{V} \subset V$ and agent $i \in V - \hat{V}$, $\tilde{P}_i(G_{-\hat{V}}, \mathbf{q}_{-\hat{V}\cup\{i\}}, \Phi) \leq \tilde{P}_i(G, \mathbf{q}_{-i}, \Phi)$. Using Proposition 1, we have $\mathbf{P}_i(G_{-\hat{V}}, \mathbf{q}_{-\hat{V}}, \Phi) = (1 - q_i)\tilde{P}_i(G_{-\hat{V}}, \mathbf{q}_{-(\hat{V}\cup\{i\})}, \Phi)$. By definition, $\tilde{P}_i(G_{-\hat{V}}, \mathbf{q}_{-(\hat{V}\cup\{i\})}, \Phi)$ is the probability of infection reaching agent i in $G_{-\hat{V}}$. Consider a transmission network $\bar{G}^t$ generated from $(G_{-\hat{V}}, \mathbf{q}_{-\hat{V}})$ in which infection can reach agent i. The probability of the transmission network $\bar{G}^t$ can be written as the marginal probability of the transmission networks G^t generated from $(G, \mathbf{q})$ that satisfies $G^t_{-\hat{V}} = \bar{G}^t$. Furthermore, in any transmission network G^t that satisfies $G^t_{-\hat{V}} = \bar{G}^t$, infection can reach agent i. Hence, the probability of infection reaching agent i in a transmission network generated from $(G, \mathbf{q})$ is at least $\tilde{P}_i(G_{-\hat{V}}, \mathbf{q}_{-(\hat{V}\cup\{i\})}, \Phi)$. In other words, $\tilde{P}_i(G_{-\hat{V}}, \mathbf{q}_{-\hat{V}\cup\{i\}}, \Phi) \leq \tilde{P}_i(G, \mathbf{q}_{-i}, \Phi)$.

(c) Best response monotonicity in network effect: Given network G and security profiles $\mathbf{q}_{-i}$ and $\hat{\mathbf{q}}_{-i}$, if $\tilde{P}_i(G, \mathbf{q}_{-i}, \Phi) \geq \tilde{P}_i(G, \hat{\mathbf{q}}_{-i}, \Phi)$, then $B_i(\mathbf{q}_{-i}) \geq B_i(\hat{\mathbf{q}}_{-i})$. Using Eq. (2), we have $c_i'(B_i(\mathbf{q}_{-i})) = \tilde{P}_i(G, \mathbf{q}_{-i}, \Phi) \geq \tilde{P}_i(G, \hat{\mathbf{q}}_{-i}, \Phi) = c_i'(B_i(\hat{\mathbf{q}}_{-i}))$. Combining with Assumption 1, we obtain $B_i(\mathbf{q}_{-i}) \geq B_i(\hat{\mathbf{q}}_{-i})$ which shows the desired result. □

Proof of Eq. (4). Let $B_i(\mathbf{q}_{-i})$ and $S_i(\mathbf{q}_{-i})$ denote the best response strategy and welfare maximizing strategy of agent i. Using Eq. (3) we have $c_i'(S_i(\mathbf{q}_{-i})) = \tilde{P}_i(G, \mathbf{q}_{-i}, \Phi) + \sum_{j\neq i} Q_{j,i}(G, \mathbf{q}_{-\{i,j\}}, \Phi)(1 - q_j)$. By definition, $Q_{j,i}(G, \mathbf{q}_{-\{i,j\}}, \Phi)(1 - q_j)$ is a probability. Therefore, we have

$$c_i'(S_i(\mathbf{q}_{-i})) = \tilde{P}_i(G, \mathbf{q}_{-i}, \Phi) + \sum_{j\neq i} Q_{j,i}(G, \mathbf{q}_{-\{i,j\}}, \Phi)(1 - q_j) \geq \tilde{P}_i(G, \mathbf{q}_{-i}, \Phi)$$
$$= c_i'(B_i(\mathbf{q}_{-i})),$$

where the last equation follows from Eq. (2). The claim follows by the assumption that $c_i(\cdot)$ is strictly convex (cf. Assumption 1), and therefore $c_i'(\cdot)$ is a strictly increasing function. □

Proof of Theorem 2.

Existence of the symmetric pure-strategy Nash equilibrium. We show that there exists a $q^e \in [0, 1]$ such that $u(G, \mathbf{q}, \Phi)$ achieves its maximum at $\mathbf{q} = \mathbf{q}_n^e$. Due to symmetry, we have

$$\frac{\partial}{\partial q_i} u(G, \mathbf{q}, \Phi)|_{\mathbf{q}=\mathbf{q}_n} = \frac{\partial}{\partial q_j} u(G, \mathbf{q}, \Phi)|_{\mathbf{q}=\mathbf{q}_n} \ \forall\, i, j \in V. \tag{A.6}$$

Let $f(x) = \frac{\partial}{\partial q_j} u(G, \mathbf{q}, \Phi)|_{\mathbf{q}=\mathbf{x}_n}$. We show that, $f(x)$ is decreasing in x. The continuity and differentiability of $u(G, \mathbf{q}_n, \Phi)$ follows from Propositions 1, 2 and Assumption 1. By definition, $u(G, \mathbf{q}_n, \Phi) = 1 - (1 - q)\tilde{P}(G, \mathbf{q}_{n-1}, \Phi) - c(q)$. Hence, $f(q) = \tilde{P}(G, \mathbf{q}_{n-1}, \Phi) - c'(q)$. Using Proposition 3(a), we have $\tilde{P}(G, \mathbf{q}_{n-1}, \Phi)$ is a decreasing function in q. Also by Assumption 1, $c'(q)$ is continuous and strictly increasing, which shows that $f(q)$ is strictly decreasing in q. We next show that, there exists a unique $q^e \in (0, 1)$ such that $f(q^e) = 0$. Using Assumption 1 and the inequality $0 \leq \tilde{P}(G, \mathbf{q}_{n-1}, \Phi) \leq 1$, it is guaranteed that $f(0) \geq 0$ and $f(1) < 0$. Therefore, there exists a unique q^e such that $f(q^e) = 0$. As a result, using Eq. (A.6), $\mathbf{q}_n^e$ is the unique symmetric equilibrium.

Underinvestment in the symmetric equilibrium. For the sake of contradiction, assume $q^e > q^s$. We next show that under this assumption, we have $c'(q^s) \geq c'(q^e)$. Using Eqs. (2), (3), and the fact that $\tilde{P}(G, \mathbf{q}_{n-1}, \Phi)$ is decreasing in q, the following relations hold.

$$c'(q^s) = \tilde{P}(G, \mathbf{q}^s_{n-1}, \Phi) - (1-q^s)\frac{\partial}{\partial q^s}\tilde{P}(G, \mathbf{q}^s_{n-1}, \Phi) \geq \tilde{P}(G, \mathbf{q}^s_{n-1}, \Phi)$$
$$\geq \tilde{P}(G, \mathbf{q}^e_{n-1}, \Phi) = c'(q^e),$$

where the second inequality follows from Proposition 3(a). Assumption 1 implies that $c'(q^e) > c'(q^s)$ assuming $q^e > q^s$. This contradicts the preceding inequality, completing the proof. □

Proof of Theorem 3. The uniqueness of equilibrium security investments follows from Theorem 1. Let $\mathbf{q}^e$ denote the equilibrium security investment obtained from Eq. (2), i.e., $c'(q_i^e) = \tilde{P}_i(G, \mathbf{q}^e_{-i})$, and let $\tilde{\mathbf{q}}$ denote the solution to $\tilde{\mathbf{q}} = (\alpha I + A)^{-1}e$, i.e.,

$$\alpha \tilde{q}_i = 1 - \sum_{j\neq i} a_i^j \tilde{q}_j. \tag{A.7}$$

We next show that $||\mathbf{q}^e - \tilde{\mathbf{q}}||_\infty = o(\frac{1}{\alpha^2})$. By Proposition 4, we have $\tilde{P}_i(G, \mathbf{q}) = 1 - \sum_{j\neq i} a_i^j q_j + o(||\mathbf{q}||_\infty)$, for all $\mathbf{q} \in [0, 1]^n$. Moreover, writing the Taylor series expansion for function $c'(q)$ around 0, we have $c'(q) = c'(0) + c''(0)q + o(q) = \alpha q + o(q)$. Combining with Eq. (2) we obtain

$$\alpha \mathbf{q}^e = e - A\mathbf{q}^e + \Delta, \tag{A.8}$$

where for all i we have $|\Delta_i| = o(||\mathbf{q}^e||_\infty)$. Note that using Eq. (2), we have for all i, $c'(q_i^e) = \tilde{P}_i(G, \mathbf{q}^e) \leq 1$. Moreover, from the Taylor approximation, assuming $c''(0) \geq \alpha$, we have $c'(q_i^e) = c'(0) + c''(0)q_i^e + o(||\mathbf{q}^e||_\infty) \geq \alpha q_i^e + o(||\mathbf{q}^e||_\infty)$. Therefore, $q_i^e \leq \frac{b}{\alpha}$ for some constant b.

Combining Eqs. (A.7) and (A.8) we have $\alpha(\mathbf{q}^e - \tilde{\mathbf{q}}) = A(\tilde{\mathbf{q}} - \mathbf{q}^e) + \Delta$, which leads to

$$\|\mathbf{q}^e - \tilde{\mathbf{q}}\| = \|(A+\alpha I)^{-1}\Delta\| \leq \|(A+\alpha I)^{-1}\|\|\Delta\|$$
$$= \frac{1}{\alpha}\left\|\left(\frac{1}{\alpha}A + I\right)^{-1}\right\|\|\Delta\| \leq \frac{1}{\alpha}\left\|\left(\frac{1}{\alpha}A + I\right)^{-1}\right\|\frac{b}{\alpha^2} = o\left(\frac{1}{\alpha^2}\right),$$

where we used $|\Delta_i| = o(||\mathbf{q}^e||_\infty)$ along with $q_i^e \leq \frac{b}{\alpha}$ for all i, and $\lim_{\alpha\to\infty}\left\|\left(\frac{1}{\alpha}A + I\right)^{-1}\right\| = 1$. □

Proof of Corollary 2.

(a) We first show that for two non-cut vertices i, j belonging to the same block, $a_{it}^k = a_{jt}^k$, for all $k \neq i, j$. Suppose to the contrary that for some k, $a_{it}^k = 1$ and $a_{jt}^k = 0$. This implies that by removing k from the network, nodes j and t are still connected, but node i and t become disconnected. Since both nodes i and j belong to the same bi-connected component, by removing only one node, they still stay connected, which implies that i and t are also connected, which shows the contradiction. With a similar argument, we have for all $k, t \neq \{i, j\}$, $a_{kt}^i = a_{kt}^j = 0$. Using Definition (2), we have $a_i^k = \frac{1}{n}\sum_t a_{it}^k = \frac{1}{n}\sum_t a_{jt}^k = a_j^k$, and $a_i^j = a_j^i = \frac{1}{n}$. Using Proposition 4 we have

$$\alpha q_i^e + \frac{1}{n}q_j^e = 1 - \sum_{k\neq i,j} a_i^k q_k^e + o\left(\frac{1}{\alpha}\right), \alpha q_j^e + \frac{1}{n}q_i^e = 1 - \sum_{k\neq i,j} a_j^k q_k^e + o\left(\frac{1}{\alpha}\right).$$

This implies that $(\alpha - \frac{1}{n})(q_i^e - q_j^e) = 1 - \sum_{k \neq i,j} a_i^k q_k^e - (1 - \sum_{k \neq i,j} a_j^k q_k^e) + o\left(\frac{1}{\alpha}\right) \overset{\alpha}{\approx} 0$, completing the proof. Note that we only used Theorem 3, and did not need to use the second Taylor series approximation given in Eq. (12). With a similar argument, one can show that for a cut vertex k and a non-cut vertex i in the same bi-connected component, $a_i^k > a_k^i$, which implies that $q_e^k > q_e^i$.

(b) and (c) We first show part (c). Consider two cut vertices i and j that are adjacent in the block tree decomposition, i.e., there exists a block which is the neighbor of both i and j in the block tree decomposition. First note that $a_{it}^k = a_{jt}^k$ for all $k, t \neq \{i, j\}$, since i and j are connected via a block. We define the size of a subtree in the block tree as the number of nodes from G, that belong to that subtree. Let x and y denote the size of subtrees attached to j and i after removing the common block between i and j in the block tree decomposition. One can verify that $a_i^j = \frac{x}{n}$ and $a_j^i = \frac{y}{n}$ and $x + y \leq n$. Using Proposition 4 and assuming $x < y$, with a similar argument given in part (a), we obtain $q_i^e > q_j^e$, completing the proof of part (c).

We next provide the proof for part (b). Let v denote the balancing cut vertex in the block tree decomposition, i.e., the maximum size of the subtrees rooted at his adjacent cut vertices is minimized. Using part (c), one can show that v has a higher security investment compared to any cut vertex u adjacent to v (in the block tree decomposition), since the size of the subtree attached to v is higher that the size of the subtree attached to u, after removing the common block between u and v. Using similar argument, considering v as the root, as the nodes get farther from v, their security investments decrease. □

Lemma A.1. *The total expected infection passing through agent i in a network is equal to*

$$\tilde{P}_i(G, \mathbf{q}) + \sum_j (1 - q_j) Q_{ji}(G, \mathbf{q}) = s_i - \sum_j b_i^j q_j + o(||\mathbf{q}||_\infty).$$

Proof of Lemma A.1. We start by providing the proof for tree network structures. Using Proposition 4, we have $\tilde{P}_i(G, \mathbf{q}) = 1 - \sum_{j \neq i} a_i^j q_j + o(||\mathbf{q}||_\infty)$. We next characterize $Q_{ji}(G, \mathbf{q})$. The probability of infection reaching agent j through i (conditioning on i being susceptible) can be written as

$$Q_{ji}(G, \mathbf{q})(1 - q_j) = \frac{1}{n} \sum_t Prob(j \overset{i}{\leftrightarrow} t | \mathbb{X}_i = 1). \tag{A.9}$$

The term on the right hand side is sum over all agents t, the probability that agent t is attacked and all active paths between t and j go through i, denoted by the event $Prob(j \overset{i}{\leftrightarrow} t | \mathbb{X}_i = 1)$. Assuming $\alpha = c''(0)$ is sufficiently large ensures that the equilibrium security investments are small and we can express $Prob(j \overset{i}{\leftrightarrow} t | \mathbb{X}_i = 1)$ as

$$Prob(j \overset{i}{\leftrightarrow} t | \mathbb{X}_i = 1) = a_{jt}^i \prod_{k \in j \leftrightarrow t, k \neq i} (1 - q_k) \approx a_{jt}^i (1 - \sum_{k \in j \leftrightarrow t, k \neq i} q_k) + o(||\mathbf{q}||_\infty). \tag{A.10}$$

Since G is a tree, there is a unique path between j and k, therefore $i \in j \leftrightarrow t$ only if $a_{jt}^i = 1$, and also $k \in j \leftrightarrow t$ if and only if $a_{jt}^k = 1$. Therefore, we can rewrite Eq. (A.10) as $Prob(j \overset{i}{\leftrightarrow} t | \mathbb{X}_i = 1) = a_{jt}^i - \sum_{k \neq i} a_{jt}^i a_{jt}^k q_k + o(||\mathbf{q}||_\infty)$. Combining with Eq. (A.9), we have

$$Q_{ji}(G,\mathbf{q})(1-q_j) = \frac{1}{n}\sum_t Prob(j \overset{i}{\leftrightarrow} t|\mathbb{X}_i = 1) \tag{A.11}$$
$$= \frac{1}{n}\sum_t (a^i_{jt} - \sum_{k\neq i} a^i_{jt}a^k_{jt}q_k) + o(||\mathbf{q}||_\infty)$$
$$= a^i_j - \frac{1}{n}\sum_{k\neq i,t} a^i_{jt}a^k_{jt}q_k + o(||\mathbf{q}||_\infty).$$

Combining Proposition 4, and Eq. (A.11), we have

$$\tilde{P}_i(G,\mathbf{q}) + \sum_{j\neq i}(1-q_j)Q_{ji}(G,\mathbf{q}) \tag{A.12}$$
$$= 1 - \sum_{k\neq i} a^k_i q_k + \sum_{j\neq i}(a^i_j - \frac{1}{n}\sum_{k\neq i,t} a^i_{jt}a^k_{jt}q_k) + o(||\mathbf{q}||_\infty)$$
$$= 1 + \sum_{k\neq i} a^i_k - \sum_{k\neq i} a^k_i q_k + \sum_{j\neq i}\sum_{k\neq i}\frac{1}{n}a^i_{jt}a^k_{jt}q_k + o(||\mathbf{q}||_\infty)$$
$$= s_i - \sum_{k\neq i} q_k\left(a^k_i + \frac{1}{n}\sum_{j\neq i}\sum_t a^i_{jt}a^k_{jt}\right) + o(||\mathbf{q}||_\infty).$$

Also note that

$$a^k_i + \frac{1}{n}\sum_{j\neq i}\sum_t a^i_{jt}a^k_{jt} = a^i_k + \frac{1}{n}\sum_j\sum_t a^i_{jt}a^k_{jt} - \frac{1}{n}\sum_t a^i_{it}a^k_{it} \tag{A.13}$$
$$= a^i_k + \frac{1}{n}\sum_j\sum_t a^i_{jt}a^k_{jt} - a^k_i = \frac{1}{n}\sum_j\sum_t a^i_{jt}a^k_{jt},$$

where the second equation follows from $\sum_t a^i_{it}a^k_{it} = \sum_t 1 \times a^k_{it} = na^k_i$. Combining Eqs. (A.12) and (A.13), we obtain

$$\tilde{P}_i(G,\mathbf{q}) + \sum_{j\neq i}(1-q_j)Q_{ji}(G,\mathbf{q}) = s_i - \sum_{k\neq i} q_k\frac{1}{n}\sum_j\sum_t a^i_{jt}a^k_{it} + o(||\mathbf{q}||_\infty)$$
$$= s_i - \sum_{k\neq i} b^k_i q_k + o(||\mathbf{q}||_\infty),$$

completing the proof for the tree networks, since in tree network structures $b^{(i,j)}_{kt} = 0$. The proof extends to general networks using similar arguments to those we used for Theorem 3. We use again a decomposition result from graph theory, referred to as the *SPQR tree decomposition* of a biconnected graph. To state the result, we first define a connected network to be tri-connected if removal of any pair of nodes, or any single node, cannot make the graph disconnected (e.g., a ring network is not tri-connected, but a complete network is tri-connected). Hopcroft and Tarjan (1973) present a *series-parallel rigid (SPQR) tree decomposition* of a graph, which states that any bi-connected network can be decomposed into a unique tree of (maximal) tri-connected components connected to each other via separating pair nodes. Furthermore, the set of maximal tri-connected components are unique. We next show that $Prob(j \overset{i}{\leftrightarrow} t) = a^i_{jt} + \sum_{k\neq i} b^{(i,k)}_{jt} q_k - \sum_{k\neq i} a^i_{jt}a^k_{jt}q_k + o(||\mathbf{q}||_\infty)$. Consider the unique path from j to t in the block tree decomposition, given by $j = v_0, \cdots, v_m, v_{m+1} = t$, where v_1 and v_m are the cut vertices in the blocks that j and t belong to. Let $\mathcal{V}_{jt} = \{v_1, \cdots, v_{m+1}\}$. Event $j \overset{i}{\leftrightarrow} t$ happens if either $i \in \mathcal{V}_{jt}$, or $i \notin \mathcal{V}_{jt} \& \exists p, v_p \overset{i}{\leftrightarrow} v_{p+1}$. Without loss of generality, conditioning on i being susceptible, we have $Prob(j \overset{i}{\leftrightarrow} t|\mathbb{X}_i = 1) = \beta_0 - \sum_{k\neq i} \beta_k q_k + +o(||\mathbf{q}||_\infty)$. We first show that $\beta_0 = a^i_{jt}$ and $\beta_k = a^i_{jt}a^k_{jt} - b^{ik}_{jt}$. Tree decomposition results guarantee that the paths in the block tree decomposition, and also SPQR tree are unique, therefore simplifying the arguments. There are two possible scenarios, **(a)** either $i \in \mathcal{V}_{jt}$. In this scenario, $a^i_{jt} = 1$, and all paths between j and t should go through i. The probability of having a path between j and t has been calculated in subsection 3.4. Also, note that by definition, $b^{(i,k)}_{jt} = 0$ for all k, since $i \in \mathcal{V}_{jt}$. Therefore, we have $\beta_0 = 1 = a^i_{jt}$ and $\beta_k = a^k_{jt} = a^i_{jt}a^k_{jt} - b^{(i,k)}_{jt}$, or **(b)** $i \notin \mathcal{V}_{jk}$, which implies that there exists a block p, such that $v_p \overset{i}{\leftrightarrow} v_{p+1}$. Since all blocks are biconnected, assuming i is susceptible, assuming all paths between v_p and v_{p+1} pass through i, we have $Prob(v_p \overset{i}{\leftrightarrow} v_{p+1}) = \sum_k b^{(i,k)}_{v_p v_{p+1}} q_k - o(||\mathbf{q}||_\infty)$. Therefore, in this scenario, we have

$$
\begin{aligned}
& Prob(j \overset{i}{\leftrightarrow} k|\mathbb{X}_i = 1) \\
&= \prod_{j=0}^{t+1} Prob(v_j \text{ is susceptible }) \prod_{j=0, j\neq m}^{t} Prob(\{v_j \leftrightarrow v_{j+1}\}|v_j \& v_{j+1} \text{ are susceptible}) \\
&\qquad \times Prob(\{v_m \overset{i}{\leftrightarrow} v_{m+1}\}|v_m \& v_{m+1} \& i \text{ are susceptible}) \\
&= \prod_{j=0}^{t+1} Prob(v_j \text{ is susceptible }) \left(\sum_k b^{(i,k)}_{v_p v_{p+1}} q_k + o(||\mathbf{q}||_\infty) \right) (1 - o(||\mathbf{q}||_\infty)) \\
&= \sum_k b^{(i,k)}_{v_p v_{p+1}} q_k + o(||\mathbf{q}||_\infty) = \sum_t b^{(i,k)}_{jt} q_k + o(||\mathbf{q}||_\infty).
\end{aligned}
$$

In this scenario $\beta_0 = 0 = a^i_{jt}$, and $\beta_k = -b^{(i,k)}_{jt} = a^i_{jt}a^k_{jt} - b^{(i,k)}_{jt}$. Therefore, we have

$$
\begin{aligned}
\tilde{P}_i(G, \mathbf{q}) + \sum_j (1 - q_j) Q_{i,j}(G, \mathbf{q}_{-\{i,j\}}) &= \frac{1}{n} \sum_j \sum_{\{t|i \in j \leftrightarrow t\}} Prob(\{j \overset{i}{\leftrightarrow} t|\mathbb{X}_i = 1\}) \\
&= \frac{1}{n} \sum_j \sum_t a^i_{jt} - \frac{1}{n} \sum_j \sum_t \sum_{k\neq i} \left(a^i_{jt}a^k_{jt} - b^{(i,k)}_{jt} \right) q_k + o(||\mathbf{q}||_\infty) \\
&= (1 + \sum_{j\neq i} a^i_j) - \frac{1}{n} \sum_j \sum_t \sum_{k\neq i} \left(a^i_{jt}a^k_{jt} - b^{(i,k)}_{jt} \right) q_k + o(||\mathbf{q}||_\infty) \\
&= (1 + \sum_{j\neq i} a^i_j) - \frac{1}{n} \sum_{k\neq i} \sum_j \sum_t \left(a^i_{jt}a^k_{jt} - b^{(i,k)}_{jt} \right) q_k + o(||\mathbf{q}||_\infty) \\
&= s_i - \sum_{k\neq i} b^k_i q_k + o(||\mathbf{q}||_\infty),
\end{aligned}
$$

completing the proof. □

Proof of Theorem 4. Using the optimality conditions for socially optimal investments, we have

$$c'(q_i^s) = \tilde{P}_i(G, \mathbf{q}_{-i}^s) + \sum_j (1 - q_j^s) Q_{ij}(G, \mathbf{q}_{-\{i,j\}}^s). \tag{A.14}$$

Using similar argument as given for Theorem 3, we can show that when Assumption 1 holds, for α sufficiently large, we can approximate $P_i(G, \mathbf{q}^s) + (1 - q_i^s)\sum_j (1 - q_j^s) Q_{i,j}(G, \mathbf{q}_{-\{i,j\}})$ with first order terms. Combining Lemma A.1 and Eq. (A.14), we have $\alpha q_i^s \overset{\alpha}{\approx} s_i - \sum_{j \neq i} b_i^j q_j$. Rewriting the preceding equation in terms of matrix B, we have $\alpha \mathbf{q}^s \overset{\alpha}{\approx} \mathbf{s} - B\mathbf{q}^s$, which implies

$$\mathbf{q}^s \overset{\alpha}{\approx} (B + \alpha I)^{-1} \mathbf{s} = \frac{1}{\alpha}\left(\frac{B}{\alpha} + I\right)^{-1} \mathbf{s},$$

completing the proof. □

Proof of Corollary 3. Using Eqs. (12) and (17), we have

$$\begin{aligned} q_i^s - q_i^e &= \frac{1}{\alpha}(s_i - 1) - \frac{1}{\alpha^2}\left(\sum_{j \neq i} B_{ij} s_j - a_i^j\right) + o\left(\frac{1}{\alpha^2}\right) \\ &= \frac{1}{\alpha}\left(1 + \sum_{j \neq i} a_j^i - 1\right) - \frac{1}{\alpha^2}\left(\sum_{j \neq i} B_{ij} s_j - a_i^j\right) + o\left(\frac{1}{\alpha^2}\right) \\ &= \frac{1}{\alpha}\sum_{j \neq i} a_j^i - \frac{1}{\alpha^2}\left(\sum_{j \neq i} B_{ij} s_j - a_i^j\right) + o\left(\frac{1}{\alpha^2}\right). \end{aligned}$$

One can show that for any graph G, there exists α_0, such that for all $\alpha > \alpha_0$, $\frac{1}{\alpha}\sum_{j \neq i} a_j^i - \frac{1}{\alpha^2}\left(\sum_{j \neq i} B_{ij} s_j - a_i^j\right) + o\left(\frac{1}{\alpha^2}\right) > 0$, since $\sum_j a_j^i > 0$. For α sufficiently large, we have

$$q_i^s - q_i^e \overset{\alpha}{\approx} \frac{1}{\alpha}\sum_{j \neq i} a_j^i - \frac{1}{\alpha^2}\left(\sum_{j \neq i} B_{ij} s_j - a_i^j\right),$$

which shows the second part of the corollary. Finally for two nodes i, j with the same gatekeeping centrality, we have

$$\begin{aligned} (q_i^s - q_i^e) - (q_j^s - q_j^e) &= \left(\frac{1}{\alpha}\sum_{k \neq i} a_k^i - \frac{1}{\alpha^2}\sum_{k \neq i}(B_{ik} s_k - a_i^k)\right) \\ &\quad - \left(\frac{1}{\alpha}\sum_{k \neq i} a_k^j - \frac{1}{\alpha^2}\sum_{k \neq i}(B_{jk} s_k - a_j^k)\right) + o\left(\frac{1}{\alpha^2}\right) \\ &= \frac{1}{\alpha^2}\left(\sum_{k \neq i}(B_{jk} s_k - a_j^k) - \sum_{k \neq i}(B_{ik} s_k - a_i^k)\right) + o\left(\frac{1}{\alpha^2}\right) \\ &\overset{\alpha}{\approx} \frac{1}{\alpha^2}\left(\sum_{k \neq i}(B_{jk} s_k - a_j^k) - \sum_{k \neq i}(B_{ik} s_k - a_i^k)\right), \end{aligned}$$

completing the proof. □

Proof of Proposition 5. For a given network G (deterministic) let $x_{ik}(\hat{G})$ denote the indicator variable for i being connected to k in $\hat{G}$. Also, we define $Prob(i \overset{\hat{G}}{\leftrightarrow} k)$ as the probability of i being connected to k in $\hat{G}$, which is a function of $\mathbf{q}$ (again $\hat{G}$ is a deterministic network), and finally $a_{ik}^j(\hat{G})$ denotes the indicator variable of j being a gatekeeper between i and k in $\hat{G}$. Note that if i is not connected to k, $a_{ik}^j(\hat{G}) = 0$. By definition we have

$$\tilde{P}_i(G(\beta), \mathbf{q}) = \sum_{\hat{G} \sim G(\beta)} P(\hat{G}) \tilde{P}_i(\hat{G}, \mathbf{q}) = \sum_{\hat{G} \sim G(\beta)} P(\hat{G}) \frac{1}{n} \sum_k Prob(i \overset{\hat{G}}{\leftrightarrow} k | \mathbb{X}_i = 1) \quad \text{(A.15)}$$

Combining with Eq. (9), we have

$$\begin{aligned} \tilde{P}_i(G(\beta), \mathbf{q}) &= \frac{1}{n} \sum_{\hat{G} \sim G(\beta)} P(\hat{G}) \sum_k Prob(i \overset{\hat{G}}{\leftrightarrow} k | \mathbb{X}_i = 1) \quad \text{(A.16)} \\ &= \frac{1}{n} \left(\sum_{\hat{G} \sim G(\beta)} P(\hat{G}) \sum_k \left(x_{ik}(\hat{G}) - \sum_{j \neq i} a_{ik}^j(\hat{G}) q_j \right) \right) + o(||\mathbf{q}||_\infty) \\ &= \frac{1}{n} \sum_k \sum_{\hat{G} \sim G(\beta)} P(\hat{G}) x_{ik}(\hat{G}) - \frac{1}{n} \sum_{j \neq i} q_j \sum_k \sum_{\hat{G} \sim G(\beta)} P(\hat{G}) a_{ik}^j(\hat{G}) + o(||\mathbf{q}||_\infty) \end{aligned}$$

Note that if i is connected to k in $\hat{G}$, $x_{ik}(\hat{G}) = 1$, and the second equation is the same as Eq. (9), and if i is not connected to k, $x_{ik}(\hat{G})$ as well as all $a_{ik}^j = 0$ for all j. Furthermore, by definition, we have

$$\gamma_i = \frac{1}{n} \sum_k \gamma_{ik} = \frac{1}{n} \sum_k \sum_{\hat{G} \sim G(\beta)} P(\hat{G}) x_{ik}(\hat{G}), \quad \text{(A.17)}$$

$$\begin{aligned} z_i^j &= \frac{1}{n} \sum_k z_{ik}^j = \frac{1}{n} \sum_k (\gamma_{ik} - \sigma_{ik}^j) = \frac{1}{n} \sum_k \sum_{\hat{G} \sim G(\beta)} P(\hat{G}) \left(x_{ik}(\hat{G}) - x_{ik}(\hat{G}_{-j}) \right) \quad \text{(A.18)} \\ &= \frac{1}{n} \sum_k \sum_{\hat{G} \sim G(\beta)} P(\hat{G}) a_{ik}^j(\hat{G}). \end{aligned}$$

Combining Eqs. (A.16), (A.17), and (A.18), we obtain $\tilde{P}_i(G(\beta), \mathbf{q}) = \gamma_i - \sum_{j \neq i} q_j z_i^j + o(||\mathbf{q}||_\infty)$, completing the proof. □

Proof of Theorem 5. Using Eq. (2), equilibrium investments satisfy $c'(q_i^e) = \tilde{P}_i(G, \mathbf{q}_{-i}^e)$. Using Proposition 5 we have $c'(q_i^e) = \tilde{P}_i(G, \mathbf{q}_{-i}^e) = \gamma_i - \sum_{j \neq i} q_j z_i^j + o(||\mathbf{q}||_\infty)$. For α sufficiently large, and knowing that $q^e < \frac{1}{\alpha}$, we obtain $\alpha \mathbf{q}^e = \gamma - \mathbf{Z} \mathbf{q}^e + o(||\mathbf{q}||_\infty)$. Therefore, we have $(\alpha \mathbf{I} + \mathbf{Z}) \mathbf{q}^e = \gamma + (||\mathbf{q}||_\infty)$. Note that under Assumption 1, $(\alpha \mathbf{I} + \mathbf{Z})$ is non-singular, completing the proof. □

Proof of Proposition 6. Applying first order condition on Eq. (21), and using Proposition 1, we obtain $c'(q_i^e) = |\mathcal{E}_i| \tilde{P}_i(\hat{G}, \mathbf{q}_{-i}^e)$. Also, using similar argument as in Proposition 4, we have

$$\tilde{P}_i(\hat{G}, \mathbf{q}) = \frac{C_i(\hat{G})}{n} - \sum_j a_i^j(\hat{G}) q_j + o(||\mathbf{q}||_\infty), \quad 1 \leq i \leq n,$$

where $a_i^j(\hat{G})$ denotes the fraction of nodes blocked from i by j in $\hat{G}$. Combining the preceding equations and assuming $c(q) = \frac{\alpha}{2}q^2$, we obtain $\alpha q_i^e = |\mathcal{E}_i|\left(\frac{C_i(\hat{G})}{n} - \sum_j a_i^j(\hat{G})q_j\right) + o(||\mathbf{q}||_\infty)$, $1 \le i \le n$. Rewriting in vector form, we have $\alpha \mathbf{K}^{-1}\mathbf{q}^e = \frac{\mathbf{C}(\hat{G})}{n} - \hat{A}\mathbf{q}^e + o(||\mathbf{q}||_\infty)$, which implies that

$$\mathbf{q}^e \overset{\alpha}{\approx} \left(\alpha \mathbf{K}^{-1} + \hat{A}\right)^{-1} \frac{\mathbf{C}(\hat{G})}{n} = \frac{1}{\alpha}\left(\mathbf{K}^{-1}(I + \frac{1}{\alpha}\mathbf{K}\hat{A})\right)^{-1} \frac{\mathbf{C}(\hat{G})}{n}$$
$$= \frac{1}{\alpha}\left(I + \frac{1}{\alpha}\mathbf{K}\hat{A}\right)^{-1} \mathbf{K}\frac{\mathbf{C}(\hat{G})}{n},$$

completing the proof. □

Proof of Proposition 7. We use Proposition 6, and calculate the utility of agents in $\hat{G}$, when agents invest in $\mathbf{q}^e$. Using Eq. (21), we have

$$\begin{aligned}
u_i(\hat{G}, \mathbf{q}^e) &= |\hat{\mathcal{E}}_i|\left(1 - \mathbf{P}_i(\hat{G}, \mathbf{q}^e)\right) - c_i(q_i^e) \qquad \text{(A.19)}\\
&= |\hat{\mathcal{E}}_i|\left(1 - \tilde{P}_i(\hat{G}, \mathbf{q}_{-i}^e)(1 - q_i^e)\right) - c_i(q_i^e)\\
&\overset{(1)}{=} |\hat{\mathcal{E}}_i|\left(1 - \frac{c'(q_i^e)}{|\mathcal{E}_i|}(1 - q_i^e)\right) - c_i(q_i^e)\\
&= |\hat{\mathcal{E}}_i|\left(1 - \frac{\alpha q_i^e}{|\mathcal{E}_i|}(1 - q_i^e)\right) - \frac{\alpha q_i^{e^2}}{2} = |\hat{\mathcal{E}}_i| - \alpha q_i^e + \frac{\alpha q_i^{e^2}}{2}\\
&= |\mathcal{E}_i| - |\mathcal{E}_i|\frac{C_i(\hat{G})}{n}(1 - \frac{1}{\alpha}\sum_{j \ne i} a_i^j(\hat{G})|\mathcal{E}_i|)\\
&\quad \times (1 - \frac{1}{2\alpha}|\mathcal{E}_i|\frac{C_i(\hat{G})}{n}(1 - \frac{1}{\alpha}\sum_{j \ne i} a_i^j(\hat{G})|\mathcal{E}_j|)) + o(\frac{1}{\alpha})\\
&= |\mathcal{E}_i|(1 - \frac{C_i(\hat{G})}{n}) - \frac{1}{\alpha}\left(\frac{|\mathcal{E}_i|C_i(\hat{G})}{n}(\sum_{j \ne i} a_i^j|\mathcal{E}_j| - \frac{1}{2})\right) + o(\frac{1}{\alpha}),
\end{aligned}$$

where (1) follows from $\mathbf{P}_i(\hat{G}, \mathbf{q}^e) = (1 - q_i^e)\tilde{\mathbf{P}}_i(\hat{G}, \mathbf{q}^e) = (1 - q_i^e)\frac{c'(q_i^e)}{|\mathcal{E}_i|}$. Assuming α sufficiently large, we then have $u_i(\hat{G}, \mathbf{q}^e) = |\hat{\mathcal{E}}_i|\left(1 - \frac{C_i(\hat{G})}{n}\right) + O\left(\frac{1}{\alpha}\right)$. Hence, to maximize her utility, an agent maintains connections, maximizing $|\hat{\mathcal{E}}_i|\left(1 - \frac{C_i(\hat{G})}{n}\right)$, where $\hat{\mathcal{E}}_i = \tilde{\mathcal{E}}_i \cap \tilde{\mathcal{E}}_{-i}$, and $\hat{G}$ with node set V has edge set $\hat{\mathcal{E}} = \cup_{j \in V}\tilde{\mathcal{E}}_j \cap \tilde{\mathcal{E}}_{-j}$. Note that the solution might not be unique, as explained next. □

Example 6. Consider a path of length $n - 1$ with n nodes. We next show that the formed equilibrium network may not be unique. Suppose n is divisible by 4. For α sufficiently large, one equilibrium is having agent $n/2$ not maintaining her connection to agent $n/2 + 1$, and all other nodes keeping their connections. Note that for agent $n/2$, if she keeps both his edges, $|\mathcal{E}|\left(1 - \frac{C(G)}{n}\right) = 2(1 - 1)$ which is less than $1(1 - 1/2)$, her utility after dropping her link to the next node. For any other agent j, the dominant term of utility is $2(1-1/2)=1 \geq 1(1-C_j)$. Another equilibrium of the path is obtained by breaking the link between agent $n/4$ and $n/4+1$, and the link between agent $3n/4$ and $3n/4+1$, while maintaining the rest of the edges. If agent $n/4$ (or agent $3n/4$) keeps both her edges, the dominant term of his utility would be $2(1-3/4)=1/2$ which is lower than $1(1-1/4)$. Any other agent obtains at least $2(1-1/2)$ which is higher than only maintaining one edge.

Proof of Lemma 6. Let (X_i) denote the event that agent i is susceptible. In the random attack model, the probability of a susceptible agent i getting infected is $\mathbf{P}_i(G,\mathbf{q},\Phi) = \mathbf{P}_i(G,\mathbf{q},\Phi|(X_i))(1-q_i)$. Put differently, the probability of a susceptible agent i getting infected is equal to the probability of having a path between agent i and a randomly selected seed node s in the transmission network $G^t \sim (G,\mathbf{q})$, i.e., $\mathbf{P}_i(G,\mathbf{q},1_n|(X_i)) = \frac{1}{n}\sum_{s\in V}\sum_{\{G^t|(s\in G^t)\bigwedge i \xrightarrow{G^t} s\}} \mathbf{P}_{(G,\mathbf{q})}(G^t|(X_i))$. Moreover, to compute the expected infections after attacking agent i, we can restate it as the sum over all agents j, the probability of agent i being connected to agent j. Using this interpretation it is clear that $I(G,\mathbf{q},e_i) = n\mathbf{P}_i(G,\mathbf{q},1_n)$. Using Proposition 2, we have $I(G,\mathbf{q},e_i) = \tilde{P}_i(G,\mathbf{q}_{-i},1_n)(1-q_i)n$. □

Proof of Theorem 7. For a given security profile $\mathbf{q}$ let $\bar{P}_i = \mathbf{P}_i(G,\mathbf{q},1_n)$ and $P_i(e_j) = \mathbf{P}_i(G,\mathbf{q},e_j)$, where e_j is the vector of 0's except the jth element which is 1. The utility of an agent in the strategic attack model can be written as follows:

$$u_i^s(G,\mathbf{q}) = 1 - \mathbf{P}_i(G,\mathbf{q},\phi) - c(q_i) = 1 - \sum_j \phi_j P_i(e_j) - c(q_i),$$

where ϕ denotes the strategic attack decision and it is the solution to the following optimization problem:

$$\text{maximize} \quad \sum_i \phi_i \frac{I(G,\mathbf{q},e_i)}{n} - \zeta(\phi_i), \qquad \text{s.t.} \quad \sum_i \phi_i = 1,\ \phi_i \geq 0$$

Using Lemma 6 and Assumption 2, the preceding optimization can be written as

$$\text{maximize} \quad \sum_i \phi_i \bar{P}_i - \frac{\theta}{2}\phi_i^2, \qquad \text{s.t.} \quad \sum_i \phi_i = 1, \quad \phi_i \geq 0.$$

Define $L(\Phi,\lambda,\mu) = \sum_{i=1}^n \phi_i \bar{P}_i - \frac{\theta}{2}\phi_i^2 + \lambda\left(\sum_{i=1}^n \phi_i - 1\right) + \sum_{i=1}^n \mu_i\phi_i$, where $\lambda \in \mathbb{R}$ and $\mu_i \in \mathbb{R}_+$. By the first order necessary conditions for the optimality of the solution of a nonlinear program, we have $\frac{\partial}{\partial\phi_i}L = \bar{P}_i - \theta\phi_i + \lambda + \mu_i = 0$, and $\mu_i\phi_i = 0$ (for all $i \in [n]$), which implies that $\phi_i = \max\left\{0, \frac{\bar{P}_i+\lambda}{\theta}\right\}$. We first assume that θ is chosen such that $\phi_i > 0$. Since $\sum_i \phi_i = 1$, we have $\sum_i \phi_i = \sum_i \frac{\bar{P}_i+\lambda}{\theta} = 1$. Thus if for all i, $\phi_i > 0$, we have

$$\lambda = \frac{\theta - \sum_j \bar{P}_j}{n}, \qquad \phi_i = \frac{1}{n} + \frac{1}{\theta}\left(\bar{P}_i - \frac{\sum_j \bar{P}_j}{n}\right). \tag{A.20}$$

To ease the notation, let $\text{avg}(\bar{P}) = \frac{\sum_i \bar{P}_i}{n}$ and $Q_{ji} = Q_{ji}(G,\mathbf{q}^e,[\frac{1}{n}])(1-q_j)$. We then have

$$u_i(G,\mathbf{q},\phi) = 1 - \sum_j \phi_j P_i(e_j) - c(q_i) = 1 - \sum_j \left(\frac{1}{n} + \frac{1}{\theta}\left(\bar{P}_j - \text{avg}(\bar{P})\right)\right) P_i(e_j) - c(q_i)$$

$$= 1 - \frac{1}{n}\sum_j P_i(e_j) - \frac{1}{\theta}\sum_j \left(\bar{P}_j - \operatorname{avg}(\bar{P})\right) P_i(e_j) - c(q_i)$$
$$= 1 - \bar{P}_i + \frac{1}{\theta}\sum_j \bar{P}_j(\bar{P}_i - P_i(e_j)) - c(q_i).$$

Assuming $c''(q) \geq (2n)/\theta$ we then have

$$\frac{\partial^2 u_i(G, \mathbf{q}, \phi)}{\partial {q_i}^2} = \frac{\partial^2}{\partial {q_i}^2}\left(1 - \bar{P}_i + \frac{1}{\theta}\sum_j \bar{P}_j(\bar{P}_i - P_i(e_j)) - c(q_i)\right)$$
$$= \frac{\partial}{\partial q_i}\left(\tilde{P}_i - \frac{1}{\theta}\sum_j Q_{ji}(\bar{P}_i - P_i(e_j)\right) - \frac{1}{\theta}\sum_j \bar{P}_j(\tilde{P}_i - \tilde{P}_i(e_j)) - c'(q_i)$$
$$= \frac{2}{\theta}\sum_j Q_{ji}(\tilde{P}_i - \tilde{P}_i(e_j)) - c''(q_i) \overset{(1)}{\leq} \frac{2}{\theta}\sum_j Q_{ji} - c''(q_i)$$
$$\leq \frac{2n}{\theta} - c''(q_i) \leq 0,$$

where (1) follows from having $\tilde{P}_i - \tilde{P}_i(e_j) \leq 1$. Moreover, assuming $\theta > n$ is a sufficient condition for the solution of ϕ_i to be interior. □

Proof of Theorem 8. Consider a security profile in which the security level of all agents except agent i is equal to q^e and the security level of agent i is q'. In the rest of this section, we define $\mathbf{q}^e = [q^e]_n$. Assuming that the attack cost function is convex, for a strongly symmetric network, the attack decision of the strategic attacker can be stated as, $\Phi = (\phi_1, \ldots, \phi_n)$, where $\phi_i = \phi$, and for all $j \neq i$, $\phi_j = (1-\phi)/(n-1)$. Let $\hat{P}(n, q) = \tilde{P}(G, \mathbf{q}_n, 1_n)$ and $\hat{P}(n-1, q) = \mathbb{E}_{v \in V}\left[\tilde{P}(G_{-v}, \mathbf{q}_{-v}, \hat{1}_{n-1})\right]$. The optimal value of ϕ is obtained from the following program:

$$\begin{aligned}
&\text{maximize} \\
&\quad \phi(1-q')\hat{P}(n, q^e) + (1-\phi)(1-q^e)\left(\hat{P}(n-1, q^e) + (1-q')\frac{\hat{P}(n, q^e) - \hat{P}(n-1, q^e)}{1-q^e}\right) \\
&\qquad - \frac{\theta\phi^2}{2} - \frac{\theta(1-\phi)^2}{2(n-1)}, \\
&\text{subject to} \quad 0 \leq \phi \leq 1.
\end{aligned} \tag{A.21}$$

We first show under what condition the utility of agent i with respect to q' is always concave in the symmetric setting. Using Proposition 1, we can rewrite the utility of agent i as follows:

$$u_i(G, (q', \mathbf{q}^e_{n-1}), \Phi)$$
$$= 1 - (1-q')\left(\phi\frac{n}{n-1}(1 - \hat{P}(n, q^e)) + \frac{1}{n-1}(n\hat{P}(n, q^e) - 1)\right) - c(q'). \tag{A.22}$$

Hence, we have

$$\frac{\partial^2}{\partial q'^2} u_i(G, (q', \mathbf{q}^e_{n-1}), \Phi) = -c''(q') + \frac{n}{n-1}(\hat{P}(n, q^e) - 1)\left(-2\frac{\partial\phi}{\partial q'} + \frac{\partial^2\phi}{\partial q'^2}(1-q')\right). \tag{A.23}$$

We next show that under Assumptions 1 and 2, $\frac{\partial \phi}{\partial q'} < 0$ and $\frac{\partial^2 \phi}{\partial q'^2} > 0$. Assuming the existence of an interior solution for ϕ, the optimality condition of ϕ in Eq. (A.21) implies

$$\phi = \frac{1}{n} + \frac{n-1}{\theta n}\hat{P}(n-1, q^e)(q^e - q'), \quad \frac{\partial \phi}{\partial q'} = \frac{-(n-1)\hat{P}(n-1, q^e)}{n\theta} \leq 0, \quad \frac{\partial^2 \phi}{\partial q'^2} = 0. \tag{A.24}$$

Combining Eqs. (A.23) and (A.24) with the fact that $\tilde{P}(G, q, \Phi) \leq 1$ implies that given a strongly symmetric network, if Assumptions 1 and 2 hold, then $\frac{\partial}{\partial^2 q'} u(G, (q', q^e), \Phi) \leq 0$. Also, when ϕ hits the boundary conditions, it will not change, and utility stays concave. We next show that if $q^e = 0$, $q' > 0$, and if $q^e = 1$, assuming $c'(1) > \frac{1}{n}$, $q' < 1$. Assuming $q^e = 0$, we have $u_i(G, (q', 0_{n-1}), \Phi) = 1 - (1 - q')(\phi + (1 - \phi)) - c(q') = q' - c(q')$, and optimality implies that $q' > 0$. Moreover, for $q^e = 1$ we have $u_i(G, (q', e), \Phi) = 1 - (1 - q')\phi - c(q')$, where $\phi = \min\{1, \frac{1}{n} + \frac{n-1}{n\theta}(1 - q')\}$. Note that if $q' = 1$, then $\phi = \frac{1}{n}$ and is interior, therefore it should satisfy $\phi = \frac{1}{n} + \frac{n-1}{n\theta}(1 - q')$, and in the utility function of i, we should have $\frac{\partial}{\partial q'} u_i(G, (q', e), \Phi)|_{q'=1} = \frac{2(n-1)}{n\theta}(1 - q') + \frac{1}{n} - c'(q') \geq 0$, which under the assumption of $c'(1) > \frac{1}{n}$ does not hold. Therefore, the best response strategy when $q^e = 1$ is $q' < 1$. Furthermore, using Eq. (A.24), one can show that ϕ is continuous in $(q', \mathbf{q}^e)$, therefore $u(G, (q', \mathbf{q}^e), \Phi)$ is continuous in $(q', \mathbf{q}^e)$ (when hitting the boundary conditions ϕ stays unchanged and as a result maintains continuity). Combined with Kakutani's fixed point theorem, this implies the existence of symmetric pure strategy Nash equilibrium, completing the proof of the first part. We next study the conditions under which we have under or overinvestment in strongly symmetric networks for the strategic attack model. We first study the symmetric socially optimal solution. Let us denote the symmetric socially optimal security level by q^s and the symmetric equilibrium security level, q^e. Note that in symmetric equilibrium $\phi = \frac{1}{n}$. We then have

$$\begin{aligned}
c'(q^s) = g(q^s) &= \tilde{P}(G, \mathbf{q}^s_{n-1}, 1_n) - (1 - q^s)\frac{\partial}{\partial q^s}\tilde{P}(G, \mathbf{q}^s_{n-1}, 1_n) \\
&= \hat{P}(n, q^s) - (1 - q^s)\frac{\partial}{\partial q^s}\hat{P}(n, q^s), \\
c'(q^e) = f(q^e) &= \hat{P}(n, q^e) - (1 - q^e)\left(\frac{n}{n-1}\left(1 - \hat{P}(n, q^e)\right)\frac{\partial \phi}{\partial q'}|_{q'=q^e}\right) \\
&= \hat{P}(n, q^e) + (1 - q)\frac{\hat{P}(n-1, q^e)(1 - \hat{P}(n, q^e))}{\theta},
\end{aligned} \tag{A.25}$$

where the first order condition in the equilibrium follows from Eq. (A.22), and Eq. (A.24) is used to obtain the last equation. We show that if $\theta > 1$ or $c''(q)\theta > n$, then the derivative of the utility with respect to the symmetric security investment is monotonically decreasing, i.e., $d/dq(f(q) - c'(q)) \leq 0$.

$$\begin{aligned}
&\frac{d}{dq}(f(q) - c'(q)) = \frac{d}{dq}(\hat{P}(n, q) + (1 - q)\frac{\hat{P}(n-1, q)(1 - \hat{P}(n, q))}{\theta} - c'(q)) \\
&= \frac{d}{dq}\hat{P}(n, q)\left(1 - \frac{(1 - q)}{\theta}\hat{P}(n-1, q)\right) + \frac{d}{dq}\hat{P}(n-1, q)\left(\frac{(1 - \hat{P}(n, q))(1 - q)}{\theta}\right) \\
&\quad - \frac{\hat{P}(n-1, q)(1 - \hat{P}(n, q))}{\theta} - c''(q)
\end{aligned}$$

$$\leq \frac{d}{dq}\hat{P}(n,q)\left(1-\frac{(1-q)\hat{P}(n-1,q)}{\theta}\right)-c''(q)\leq 0, \tag{A.26}$$

where the first inequality follows from Proposition 3 which implies that $\frac{d}{dq}\hat{P}(n,q)$, $\frac{d}{dq}\hat{P}(n-1,q)<0$. If $\theta>1$, then $1-\frac{(1-q)\hat{P}(n-1,q)}{\theta}>1$, implying the last inequality. If $\theta<1$, using the assumption we have $c''(q)\theta>n$. Also note that

$$\frac{d}{dq}\hat{P}(n,q)\left(1-\frac{(1-q)\hat{P}(n-1,q)}{\theta}\right)-c''(q)\leq \frac{d}{dq}\hat{P}(n,q)\frac{-(1-q)}{\theta}-c''(q), \tag{A.27}$$

where the inequality follows from $\frac{d}{dq}\hat{P}(n,q)<0$, and $\hat{P}(n-1,q)<1$. We next show that $\frac{d}{dq}\hat{P}(n,q)>\frac{-n\hat{P}(n,q)}{1-q}$. For a given symmetric security profile $\mathbf{q}_n$ we can rewrite $\hat{P}(n,q)$ as $\hat{P}(n,q)=\sum_{i=0}^{n-1}b_iq^i(1-q)^{n-i-1}$, which implies that

$$\begin{aligned}\frac{\partial}{\partial q}\hat{P}(n,q)&=\sum_{i=1}^{n-1}ib_iq^{i-1}(1-q)^{n-i-1}-\sum_{i=0}^{n-2}(n-i-1)b_iq^i(1-q)^{n-i-2}\\&\geq-\sum_{i=0}^{n-2}(n-i-1)b_iq^i(1-q)^{n-i-2}\\&\geq-n\sum_{i=0}^{n-2}b_iq^i(1-q)^{n-i-2}\geq\frac{-n}{1-q}\sum_{i=0}^{n-2}b_iq^i(1-q)^{n-i-1}\geq\frac{-n}{1-q}\hat{P}(n,q).\end{aligned} \tag{A.28}$$

Combining Eqs. (A.27) and (A.28) with the assumption of $c''(q)\theta>n$, completes the proof of Eq. (A.26). We next show that under this assumption, at $q=q^s$, we have $c'(q^s)=g(q^s)<\hat{P}(n,q^s)+\frac{n(1-q^s)}{1-q^s}\hat{P}(n,q^s)<f(q^s)$. Combining this with the observation that $f(q)-c'(q)$ is monotonically decreasing, it implies that $q^e>q^s$. Using Eq. (A.25), to show the preceding inequality, it suffices to show that

$$\frac{\hat{P}(n-1,q)(1-\hat{P}(n,q))}{\theta}\geq\frac{n\hat{P}(n,q)}{(1-q)},\qquad\text{or}$$

$$n\theta\leq(1-q)\frac{\hat{P}(n-1,q)(1-\hat{P}(n,q))}{\hat{P}(n)}=R,\qquad\text{for } q=q^s.$$

We next find a lower bound for the right hand side of the preceding relation, which is denoted by R. By definition, we have

$$\frac{1}{n}\leq\hat{P}(n,q^s)\leq\frac{1}{n}+\frac{n-1}{n}(1-q^s),\qquad\frac{1}{n}\leq\hat{P}(n-1,q^s)\leq\frac{1}{n}+\frac{n-2}{n}(1-q^s).$$

Using the preceding inequalities, it is easy to show that

$$R\geq\frac{1}{n}(1-q^s)\left(\frac{1}{\frac{1}{n}+\frac{n-1}{n}(1-q^s)}-1\right)=\frac{n-1}{n}\frac{q^s(1-q^s)}{1+(n-1)(1-q^s)}.$$

One can easily show that the above function is increasing between $q^s\in\left[0,1-\frac{1}{\sqrt{n+1}}\right]$ and decreasing between $q^s\in\left(1-\frac{1}{\sqrt{n+1}},1\right]$. Furthermore, assuming that q^s is the socially optimal solution we have $c'^{-1}\left(\frac{1}{n}\right) \le q^s \le c'^{-1}(n)$. We then consider the following cases **(1)** $c'^{-1}(n) \le 1 - \frac{1}{\sqrt{n+1}}$, **(2)** $c'^{-1}(\frac{1}{n}) \ge 1 - \frac{1}{\sqrt{n+1}}$, and **(3)** $c'^{-1}(\frac{1}{n}) \le 1 - \frac{1}{\sqrt{n+1}} \le c'^{-1}(n)$.

We will only analyze the first case. Other cases can be analyzed similarly. In the first case, R will be minimized when $q^s = c'^{-1}(\frac{1}{n})$. Hence, the sufficient condition for having overinvestment is $\theta \le \frac{n-1}{n^2} \frac{c'^{-1}(\frac{1}{n})(1-c'^{-1}(\frac{1}{n}))}{1+(n-1)(1-c'^{-1}(\frac{1}{n}))}$. The second scenario, will be reduced to having $\theta \le \frac{n-1}{n^2} \frac{c'^{-1}(n)(1-c'^{-1}(n))}{1+(n-1)(1-c'^{-1}(n))}$, and the third scenario will be reduced to $\theta \le \min\left\{\frac{n-1}{n^2} \frac{c'^{-1}(n)(1-c'^{-1}(n))}{1+(n-1)(1-c'^{-1}(n))}, \frac{n-1}{n^2} \frac{c'^{-1}(\frac{1}{n})(1-c'^{-1}(\frac{1}{n}))}{1+(n-1)(1-c'^{-1}(\frac{1}{n}))}\right\}$. Next, we show that when $\theta \ge 1$ then underinvestment always happen. We first show that in the symmetric socially optimal solution, we have $\hat{P}(n,q^s) - (1 - q^s)\frac{\partial}{\partial q^s}\hat{P}(n,q^s) \ge 2\hat{P}(n,q^s)$. Let s denote the seed node. Using Eq. (3) for an agent i in the symmetric socially optimal security profile, we have

$$\begin{aligned}
&-(1-q^s)\frac{\partial}{\partial q^s}\hat{P}(n,q^s) = \sum_{j\neq i} Q_{j,i}(G,\mathbf{q}^s_{-n-2},\Phi)(1-q^s) \\
&\ge \sum_{j\neq i} Q_{j,i}(G,\mathbf{q}^s_{-n-2},\Phi|s=i)(1-q^s)P(s=i) \\
&\quad + \sum_{j\neq i} Q_{j,i}(G,\mathbf{q}^s_{-n-2},\Phi|s\neq i)(1-q^s)P(s\neq i) \\
&\ge \sum_{j\neq i} Q_{j,i}(G,\mathbf{q}^s_{-n-2},\Phi|s=i)(1-q^s)P(s=i) = I(G,\mathbf{q}^s,e_i)\frac{1}{n(1-q^s)} = \hat{P}(n,q^s),
\end{aligned}$$

where the last inequality follows from Lemma 6. As was shown under Assumptions 1 and 2, when $c'(1) \ge \frac{1}{n}$ the utility of each agent with respect to his security level is concave. Hence, to guarantee that $q^e \le q^s$, it suffices to show that

$$\hat{P}(n,q^e) + (1-q)\frac{\hat{P}(n-1,q^e)(1-\hat{P}(n,q^e))}{\theta} \le 2\hat{P}(n,q^e) = g(q^e).$$

Assuming $\theta \ge 1$, the preceding relation always holds. □

Proof of Theorem 9. In the rest of this proof, let $\bar{P}_i = \mathbf{P}_i(G,\mathbf{q}^e,1_n)$, $\tilde{P}_i = \tilde{P}_i(G,\mathbf{q}^e,1_n)$, $P_i(e_j) = \mathbf{P}_i(G,\mathbf{q}^e,e_j)$, $\tilde{P}_i(e_j) = \tilde{P}_i(G,\mathbf{q}^e,e_j)$, and $Q_{ji} = Q_{ji}(G,\mathbf{q}^e,1_n)(1-q_j)$. Also, let $\text{Sum}(\bar{P}) = \sum_j \bar{P}_j$. We also denote $\tilde{P}_i = Q_{ii}$. As was shown in Theorem 7, for $\theta > n$, we have an interior solution for ϕ always. Hence, assuming that θ is sufficiently large, in the rest of this proof, we only look at the interior solution of ϕ without loss of generality. Using Eq. (A.20) and assuming $\zeta(\phi) = \frac{\theta}{2}\phi^2$, we have

$$\phi_i = \frac{1}{n} + \frac{1}{\theta}\left(\bar{P}_i - \frac{\text{Sum}(\bar{P})}{n}\right). \tag{A.29}$$

The utility of agent i, is $u_i(G,\mathbf{q}^e,\phi) = (1 - \mathbf{P}_i(G,\mathbf{q}^e,\phi)) - c(q_i) = 1 - \sum_{j=1}^n \phi_j P_i(e_j) - c(q_i)$. Using Eq. (A.29), we have

$$\mathbf{P}_i(G,\mathbf{q}^e,\phi) = \sum_j \left(\frac{1}{n} + \frac{1}{\theta}\left(\bar{P}_j - \frac{\text{Sum}(\bar{P})}{n}\right)\right) P_i(e_j)$$

$$
\begin{aligned}
&= \frac{1}{n}\sum_j P_i(e_j) + \frac{1}{\theta}\sum_j \bar{P}_j P_i(e_j) - \frac{\mathrm{Sum}(\bar{P})}{n\theta}\sum_j P_i(e_j) \\
&= \bar{P}_i - \frac{\mathrm{Sum}(\bar{P})}{\theta}\bar{P}_i + \frac{1}{\theta}\sum_j \bar{P}_j P_i(e_j) \\
&= \bar{P}_i\left(1 - \frac{\mathrm{Sum}(\bar{P})}{\theta}\right) + \frac{1}{\theta}\sum_j \bar{P}_j P_i(e_j).
\end{aligned}
$$

Hence, we have

$$
\begin{aligned}
&\frac{d}{dq_i}\mathbf{P}_i(G, \mathbf{q}^e, \phi) \\
&\quad = -\tilde{P}_i\left(1 - \frac{\mathrm{Sum}(\bar{P})}{\theta}\right) + \frac{\bar{P}_i}{\theta}\sum_j Q_{ji} - \frac{1}{\theta}\left(\sum_j \Big(Q_{ji}P_i(e_j) + \bar{P}_j\tilde{P}_i(e_j)\Big)\right), \\
&-\frac{d}{dq_i}\mathbf{P}_i(G, \mathbf{q}^e, \phi) \\
&\quad = \tilde{P}_i(1 - \frac{\mathrm{Sum}(\bar{P})}{\theta}) - \frac{\tilde{P}_i}{\theta}\sum_j Q_{ji}(1-q_i) + \frac{1}{\theta}\left(\sum_j \Big((1-q_i)Q_{ji}\tilde{P}_i(e_j) + \bar{P}_j\tilde{P}_i(e_j)\Big)\right) \\
&\quad = \tilde{P}_i - \frac{\tilde{P}_i}{\theta}\left(\mathrm{Sum}(\bar{P}) + \sum_j Q_{ji}(1-q_i)\right) + \frac{1}{\theta}\left(\sum_j \tilde{P}_i(e_j)\big(Q_{ji}(1-q_i) + \bar{P}_j\big)\right) \\
&\quad = \tilde{P}_i - \frac{\tilde{P}_i}{\theta}\left(\sum_j (\bar{P}_j + Q_{ji}(1-q_i)\right) + \frac{1}{\theta}\left(\sum_j \tilde{P}_i(e_j)\big(Q_{ji}(1-q_i) + \bar{P}_j\big)\right) \\
&\quad = \tilde{P}_i - \frac{1}{\theta}\left(\sum_j \tilde{P}_i(\bar{P}_j + Q_{ji}(1-q_i)\right) + \frac{1}{\theta}\left(\sum_j \tilde{P}_i(e_j)\big(Q_{ji}(1-q_i) + \bar{P}_j\big)\right) \\
&\quad = \tilde{P}_i - \frac{1}{\theta}\sum_j \Big(\tilde{P}_i - \tilde{P}_i(e_j)\Big)\big(\bar{P}_j + Q_{ji}(1-q_i)\big).
\end{aligned}
$$

Let $L_j = (\tilde{P}_i - \tilde{P}_i(e_j))$ and $M_j = (\bar{P}_j + Q_{ji}(1-q_i))$. We next calculate L_j and M_j. We have $L_j = (\tilde{P}_i - \tilde{P}_i(e_j)) = 1 - \sum_{k\neq i} a_i^k q_k - (1 - \sum_k a_{ij}^k q_k + o(\mathbf{q})) = \sum_k (a_{ij}^k - a_i^k)q_k + o(\mathbf{q})$, and we have

$$
\begin{aligned}
M_j = (\bar{P}_j + Q_{ji}(1-q_i)) &= (1 - \sum_k a_j^k q_k) + \frac{1}{n}\sum_k Prob(j \overset{i}{\leftrightarrow} k) \\
&= (1 - \sum_k a_j^k q_k) + \frac{1}{n}\sum_k \left(a_{jk}^i(1-q_i) - \sum_{t\neq i}\Big(a_{jk}^i a_{jk}^t - b_{jk}^{(i,t)}\Big)\right) = 1 + a_j^i + O(\mathbf{q}).
\end{aligned}
$$

Combining together we obtain

$$
-\frac{d}{dq_i}\mathbf{P}_i(G, \mathbf{q}^e, \phi) = \tilde{P}_i - \frac{1}{\theta}(\sum_j (\tilde{P}_i - \tilde{P}_i(e_j))(\bar{P}_j + Q_{ji}(1-q_i)) \tag{A.30}
$$

$$= \tilde{P}_i - \frac{1}{\theta}(\sum_j L_j M_j)$$

$$= \tilde{P}_i - \frac{1}{\theta}(\sum_j \sum_{k \neq i} \left((a_i^k - a_{ij}^k) q_k + o(\mathbf{q})\right) \left(1 + a_j^i + O(\mathbf{q})\right)$$

$$= \tilde{P}_i - \frac{1}{\theta} \sum_{k \neq i} q_k \sum_j (1 + a_j^i)(a_{ij}^k - a_i^k) + o(\mathbf{q})$$

$$= \tilde{P}_i - \frac{1}{\theta} \sum_{k \neq i} q_k \left(\sum_j a_{ij}^k - \sum_j a_i^k + \sum_j a_j^i a_{ij}^k - \sum_j a_j^i a_i^k \right) + o(\mathbf{q})$$

$$= \tilde{P}_i - \frac{1}{\theta} \sum_{k \neq i} q_k \left(n a_i^k - n a_i^k + n a_i^k a_k^i - b_i a_i^k \right) + o(\mathbf{q})$$

$$= \tilde{P}_i - \frac{1}{\theta} \sum_{k \neq i} q_k \left(n a_i^k a_k^i - b_i a_i^k \right) + o(\mathbf{q}).$$

Using the first order condition, in the equilibrium, we have $c'(q_i) = \frac{-d}{dq_i} \mathbf{P}_i(G, \mathbf{q}^e, \phi)$. Using a similar argument as given for Theorem 3, we can show that when Assumption 1 holds, for α sufficiently large, we can approximate $\frac{-d}{dq_i} \mathbf{P}_i(G, \mathbf{q}^e, \phi)$ with first order terms. Combining Eq. (A.30) and the first order condition equation, then we have

$$\alpha q_i^{stattack} \overset{\alpha}{\approx} 1 - \sum_j a_i^j q_j - \frac{1}{\theta} \sum_{k \neq i} q_k \left(n a_i^k a_k^i - b_i a_i^k \right) = 1 - \sum_j a_i^j q_j - \frac{1}{\theta} \sum_{j \neq i} d_i^j q_j$$

$$= 1 - \sum_{j \neq i} q_j \left(a_i^j + \frac{1}{\theta} \sum_{j \neq i} d_i^j \right).$$

Rewriting in terms of matrix D, we have $\mathbf{q}^{stattack} \overset{\alpha}{\approx} \frac{1}{\alpha} \left(I - \frac{D}{\alpha} \right) e$, completing the proof. □

Lemma A.2. *For a tree network, we have* $d_i = \frac{\sum_{j=1}^k C_j^2}{n} \left(\frac{\sum_{j=1}^k \Delta_j C_j^2}{\sum_{j=1}^k C_j^2} - \frac{\sum_{j=1}^k \Delta_j C_j}{\sum_{j=1}^k C_j} \right)$.

Proof. By definition, we have

$$-d_i = \sum_{j \neq i} d_i^j = \sum_{j \neq i} \sum_k a_k^i (a_{ik}^j - a_i^j) = \sum_k a_k^i \sum_{j \neq i} a_{ik}^j - \sum_{j \neq i} a_i^j \sum_k a_k^i.$$

We first interpret $n \sum_k a_k^i \sum_{j \neq i} a_{ik}^j$. In tree networks, $a_{ik}^j = 1$, if j is on the unique path between i and k, therefore, $\sum_{j \neq i} a_{ik}^j = Dist(i,k)$, where $Dist(i,k)$ denotes the distance of i and k in the tree. We then have

$$\sum_k a_k^i \sum_{j \neq i} a_{ik}^j = \sum_k a_k^i Dist(i,k) = \frac{1}{n} \sum_j (n - C_j) \sum_{k \in \text{Subtree } j} Dist(i,k)$$

$$= \frac{1}{n} \sum_j (n - C_j) \Delta_j C_j. \tag{A.31}$$

Note that for all nodes k belonging to subtree j of i, $a_k^i = \frac{n-C_j}{n}$, which gives us the second equation. We next interpret the second term of d_i. From subsection 3.4, recall that for tree networks, we have

$$\sum_{j\neq i} a_i^j = \frac{1}{n}\sum_k Dist(i,k) = \frac{1}{n}\sum_j \Delta_j C_j, \tag{A.32}$$

$$\sum_k a_k^i = \frac{1}{n}\sum_k \sum_j a_{jk}^i = \frac{1}{n}\sum_j C_j(n-C_j). \tag{A.33}$$

Combining Eqs. (A.31), (A.32), and (A.33), we obtain

$$\begin{aligned}
d_i &= \sum_{j\neq i} a_i^j \sum_k a_k^i - \sum_k a_k^i \sum_{j\neq i} a_{ik}^j \\
&= \frac{1}{n}\sum_j C_j(n-C_j)\frac{1}{n}\sum_k \Delta_k C_k - \frac{1}{n}\sum_j (n-C_j)\Delta_j C_j \\
&= \frac{1}{n^2}(n^2 - \sum_j C_j^2)\sum_k \Delta_k C_k - \sum_j \Delta_j C_j + \frac{1}{n}\sum_j \Delta_j C_j^2 \\
&= \frac{1}{n}\left(\sum_j \Delta_j C_j^2 - \frac{1}{n}(\sum_j C_j^2)\sum_k \Delta_k C_k\right) \\
&= \frac{(\sum_j C_j^2)}{n}\left(\sum_j \Delta_j \frac{C_j^2}{(\sum_k C_k^2)} - \sum_j \Delta_j \frac{C_j}{(\sum_k C_k)}\right),
\end{aligned}$$

establishing Eq. (25). □

References

Acemoglu, D., Ozdaglar, A., Tahbaz-Salehi, A., 2015. Systemic risk and stability in financial networks. Am. Econ. Rev. 105 (2), 564–608.

Allouch, N., 2015. On the private provision of public goods on networks. J. Econ. Theory 157, 527–552.

Anderson, R., Moore, T., 2006. The economics of information security. Science 314 (5799), 610–613.

Baccara, M., Bar-Isaac, H., 2008. How to organize crime. Rev. Econ. Stud. 75 (4), 1039–1067.

Bachrach, Y., Draief, M., Goyal, S., 2012. Competing for Security. Working paper.

Bala, V., Goyal, S., 2000. A noncooperative model of network formation. Econometrica 68 (5), 1181–1230.

Ballester, C., Calvo-Armengol, A., Zenou, Y., 2006. Who's who in networks. Wanted: the key player. Econometrica 74 (5), 1403–1417.

Bavelas, A., 1950. Communication patterns in task-oriented groups. J. Acoust. Soc. Am. 22 (6), 725–730.

Bier, V., Oliveros, S., Samuelson, L., 2007. Choosing what to protect: strategic defensive allocation against an unknown attacker. J. Public Econ. Theory 9 (4), 563–587.

Blume, L., Easley, D., Kleinberg, J., Kleinberg, R., Tardos, E., 2011. Network formation in the presence of contagious risk. In: 12th ACM Conference on Electronic Commerce, pp. 1–10.

Bramoulle, Y., Kranton, R., 2007a. Public goods in networks. J. Econ. Theory 135 (1), 478–494.

Bramoulle, Y., Kranton, R., 2007b. Risk-sharing networks. J. Econ. Behav. Organ. 64 (3–4), 275–294.

Bramoullé, Y., Kranton, R., D'Amours, M., 2014. Strategic interaction and networks. Am. Econ. Rev. 104 (3), 898–930.

Brito, D.L., Sheshinski, E., Intriligator, M.D., 1991. Externalities and compulsory vaccinations. J. Public Econ. 45 (1), 69–90.

Calvo-Armengol, A., Patacchini, E., Zenou, Y., 2009. Peer effects and social networks in education. Rev. Econ. Stud. 76 (4), 1239–1267.

Chung, F., Lu, L., 2002. Connected components in random graphs with given expected degree sequences. Ann. Comb. 6 (2), 125–145.
de Meza, D., Gould, J.R., 1992. The social efficiency of private decisions to enforce property rights. J. Polit. Econ. 100 (3), 561–580.
Galeotti, A., Rogers, B.W., 2013. Strategic immunization and group structure. Am. Econ. J. Microecon. 5 (2), 1–32.
Galeotti, A., Goyal, S., Jackson, M., Vega-Redondo, F., Yariv, L., 2010. Network games. Rev. Econ. Stud. 77 (1), 218–244.
Geoffard, P., Phillipson, T., 1997. Disease eradication: private versus public vaccination. Am. Econ. Rev. 87 (1), 222–230.
Goldman, S.M., Lightwood, J., 1995. Cost Optimization in the SIS Model of Infectious Disease with Treatment. Working paper. University of California at Berkeley.
Golub, B., Jackson, M., 2012. How homophily affects the speed of learning and best-response dynamics. Q. J. Econ. 127 (3).
Goyal, S., Vigier, A., 2011. Robust networks. Mimeo. Cambridge University.
Goyal, S., Vigier, A., 2013. Social Interaction, Vaccination, and Epidemics. Working paper.
Goyal, S., Vigier, A., 2014. Attack, defence, and contagion in networks. Rev. Econ. Stud. 81 (4), 1518–1542.
Hopcroft, J., Tarjan, R., 1973. Dividing a graph into triconnected components. SIAM J. Comput. 2 (3), 135–158.
Hoyer, B., Jaegher, K.D., 2010. Strategic Network Disruption and Defense. Working paper. Utrecht School of Economics.
Jackson, M.O., 2008. Social and Economic Networks. Princeton University Press.
Jackson, M., Wolinsky, A., 1996. A strategic model of social and economic networks. J. Econ. Theory 71 (1), 44–74.
Kempe, D., Kleinberg, J., Tardos, É., 2003. Maximizing the spread of influence through a social network. In: Proceedings of the Ninth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM, pp. 137–146.
Kovenock, D., Roberson, B., 2010. The Optimal Defense of Networks of Targets. Working paper.
Larson, N., 2011. Network Security. MPRA paper. University Library of Munich, Germany.
Molloy, M., Reed, B., 1998. The size of the giant component of a random graph with a given degree sequence. Comb. Probab. Comput. 7, 295–305.
Molloy, M., Reed, B., 2000. A critical point for random graphs with a given degree sequence. Random Struct. Algorithms 6, 161–180.
Newman, M.E.J., Strogatz, S.H., Watts, D.J., 2001. Random graphs with arbitrary degree distributions and their applications. Phys. Rev. E 64, 026118.
Rosen, J.B., 1965. Existence and uniqueness of equilibrium points for concave n-person games. Econometrica 33 (3), 520–534.
Sanders, J.L., 1971. Quantitative guidelines for communicable disease control programs. Biometrics 27 (4), 883–893.
Sethi, S.P., 1974. Quantitative guidelines for communicable disease control program: a complete synthesis. Biometrics 30 (4), 681–691.
Toxvaerd, F., 2009. Foundations of Strategic Epidemiology: Recurrent Infection and Treatment. Working paper.
Vega-Redondo, F., 2007. Complex Social Networks. Cambridge University Press.