Network Security and Contagion*

Daron Acemoglu † Azarakhsh Malekian ‡ Asu Ozdaglar §

June 18, 2013

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. The general presumption in the literature, based on intuitive arguments or analysis of symmetric networks, is that because security investments create positive externalities on other agents, there will be underinvestment in security. We show that this reasoning is incomplete because of a first-order economic force: security investments are also strategic substitutes. In a general (non-symmetric) network, this implies that underinvestment by some agents will encourage overinvestment by others. We demonstrate by means of examples there can be overinvestment by some agents and also that aggregate probabilities of infection can be lower in equilibrium compared to the social optimum. We then provide sufficient conditions for underinvestment. This requires both sufficiently convex cost functions (convexity alone is not enough) and networks that are either symmetric or locally tree-like. We also characterize the impact of network structure on equilibrium and optimal investments. Finally, we show that 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), there is an additional incentive for overinvestment: greater investment by an agent shifts the attack to other parts of the network.

Keywords: cascades, contagion, network security, security investments, strategic substitutes, underinvestment.

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.

†Department of Economics, Massachusetts Institute of Technology, Cambridge, MA, 02139 . daron@mit.edu

‡Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA, 02139 malekian@mit.edu

§Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA, 02139 asu@mit.edu

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 network 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, Draief and Goyal, 2012, Goyal and Vigier, 2011, Larson , 2011). These intuitions, however, are based on analyses of "symmetric networks". In symmetric networks, there is either no network structure 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."

The next example shows that the presumed underinvestment in network security need not hold in non-symmetric networks, and in fact, infection might be much more widespread in the socially optimal allocation than in a decentralized equilibrium.

Example 1.1. Consider the network given in Fig. 1. The underlying network S is a star with 5 nodes, each representing an agent. Each agent can protect herself against infection by investing in security q, defined as the probability that she is "immune" to infection. Suppose that her utility is given by the probability that she is uninfected minus her cost of security investment, assumed to be given by $c(q) = \frac{q^2}{5}(2.9 - 1.33q)$. Suppose also that the initial infection (attack) hits one of the agents uniformly at random. If this node is susceptible, it will get infected. Each infected

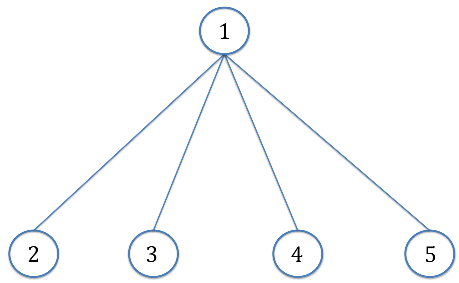

Figure 1: *The equilibrium security profile is* $\mathbf{q}^e = [0.2, 1, 1, 1, 1]$ *and the social optimum is* $\mathbf{q}^s = [1, 0.2, 0.2, 0.2, 0.2]$

agent can infect all its susceptible neighbors. One can verify that $\mathbf{q}^e = (0.2, 1, 1, 1, 1)$ is a pure-strategy Nash equilibrium security profile. However, the social optimum security profile is $\mathbf{q}^s = (1, 0.2, 0.2, 0.2, 0.2)$. The expected (number of) infections in equilibrium is $I(S, \mathbf{q}^e) = 0.16$, but expected infections in the social optimum $I(S, \mathbf{q}^s) = 0.64$.

The key to this example and to the economic richness of security decisions in a non-symmetric network is a simple observation: security decisions of different agents not only create positive externalities but are typically also *strategic substitutes*, meaning that greater investment by an agent reduces the desired investment of others, as can be readily seen in Example 1. This strategic substitutes property makes the analysis of non-symmetric networks particularly important.

This paper studies equilibrium and socially optimal security investments in a general random network subject to attack. 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 investments); (2) *strategic attacks*, where the location of the attack is determined by an adversary wishing to maximize expected infection (see also Bachrach, Draief and Goyal, 2012, Goyal and Vigier, 2011).

We first provide a decomposition of individual payoffs into an own effect and an externality, a tractable decomposition that underpins the rest of our analysis 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.

Second, using these decompositions we establish the existence of a pure-strategy Nash equilibrium in the random attacks model. Example 1 above already shows that such equilibria may feature overinvestment by some nodes and lower than optimal level of infection over the entire network, in contrast to what has generally been presumed on the basis of the positive externality underlying these interactions.

Third, we show that symmetric equilibria of symmetric networks always involve underinvestment as presumed by the existing literature. Intuitively, in a symmetric equilibrium the positive externality dominates the strategic substitutes effect and thus each agent underinvests (it is easy to see why this has to be so; if not, then all agents would overinvest, which would be inconsistent with positive externalities). Nevertheless, we also show that symmetric networks do not preclude non-symmetric equilibria, which may still involve overinvestment as in our Example 1 above. The intuition for this is also simple: once the equilibrium is non-symmetric (even if the underlying network is symmetric), the underinvestment of one agent will trigger overinvestment by some others, which can dominate the underinvestment effect.

Fourth, we introduce a special class of networks, where the network structure is represented by a tree and cost of investments are sufficiently convex (as defined below), and show that such networks always lead to underinvestment in security (though a tree structure is not sufficient for this result by itself as we also illustrate by examples). The intuition for this result can be obtained as follows: sufficiently convex cost functions ensure that when the overall probability of infection reaching agent i increases, this agent does not increase his security investment so much as to reduce its overall probability of infection. This combined with the tree network puts an upper bound on how much an agent will change its investment because some other agents underinvest, enabling us to show that, in equilibrium, all agents underinvest.

Fifth, we show that this result generalizes to random networks with local tree structures (meaning that there exists $\hat{p}$ such that any subcomponent of a certain size of the network does not contain a cycle with probability at least $\hat{p}$). The intuition for this result follows from the previous one, which enables us to bound the network effect of each agent on the rest of the network for each subcomponent of the original network.

Sixth, we strengthen this result for symmetric networks such as Erdos-Renyi graphs and we also provide additional ranking results for symmetric networks comparing equilibrium infection rates across different network structures. These results rely on observing that for this class of symmetric networks not only a symmetric equilibrium exists but is also the only equilibrium.

Seventh, we show that there is an additional reason for overinvestment in the case of strategic attacks, echoing 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. We illustrate this first using a tree network with sufficiently convex cost functions, thus establishing that even in this case overinvestment can easily result. Finally, for a symmetric random graphs and some additional conditions on cost functions, we show that the equilibrium always involves overinvestment.

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 Philipson (1997), Goldman and Lightwood (2002) and Toxvaerd (2009) analyzed certain aspects of precautionary or vaccination behavior in related settings.

More closely related to our paper are Bachrach, Draief and Goyal (2012) and Larson (2011), both analyzing 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. In Larson's model each agent chooses both their expected connectivity and a security level. Both of these papers focus on symmetric networks (e.g., Erdos-Renyi 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.[1]

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, Draief and Goyal (2012), Goyal and Vigier (2011), Kovenock and Roberson (2010), and Hoyer and Jaegher (2010), but once again without focusing on the effects of network structure.

Our results contribute to the literature in two distinct ways. First, we generalize existing models of both random and strategic attacks to (potentially asymmetric) random networks and show how new economic forces arise in the setting that were absent in symmetric equilibria. Second, we provide new and powerful characterization results. We show that the oft-presumed underinvestment in security investments is not generally true and overinvestment arises in a range of settings, with both random and strategic attacks, for well-defined economic reasons. Our characterization results then enable us to determine a range of cases where underinvestment or overinvestment incentives dominate.

Basic Notation and Terminology

Throughout the paper unless otherwise stated, a vector is viewed as a column vector. We denote by x_i, the i^{th} component of a vector $\mathbf{x}$. For a vector $\mathbf{x}$, $\mathbf{x}_{-T}$ denotes the subvector that corresponds to the indices not in set T.

An undirected graph with node set V and edge set E is represented by $G = (V, E)$. We let $|V| = n$ and $|E| = m$. We sometimes use the notation $V(G)$ and $E(G)$ to denote the node set and the edge set of graph G. A graph without edges is called an "empty graph". The *subgraph* of a graph G is a graph H with $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$. The subgraph of $G = (V, E)$ induced by $V' \subset V$, denoted by $G[V']$, is defined as $G[V'] = (V', \{(u, v)|(u, v) \in E,\ u, v \in V'\})$. Also, for a given $\bar{V} \subset V$, we will sometimes use the notation $G_{-\bar{V}}$ as $G[V - \bar{V}]$.

[1]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.

A random graph A is drawn from a probability space $(\Omega, \mathbb{F}[V], \mathbb{P})$, where Ω is the set of all undirected graphs with node set V, $\mathbb{F}$ is the family of all subsets of Ω, and for every $\tilde{A} \in \Omega$, $\mathbb{P}(\tilde{A})$ is the probability of $\tilde{A}$. For a given $i \in V$, A_{-i} is drawn from the probability space $(\Omega_{-i}, \mathbb{F}_{-i}, \mathbb{P}_{-i})$ where Ω_{-i} is the set of all undirected graphs with node set V_{-i}, $\mathbb{F}_{-i}$ is the family of all subsets of Ω_{-i}, and for a given $\tilde{A}' \in \Omega_{-i}$, $\mathbb{P}_{-i}(\tilde{A}') = \sum_{\{\tilde{A} \in \Omega | \tilde{A}_{-i} = \tilde{A}'\}} \mathbb{P}(\tilde{A})$. Similarly, given a random network A, the induced network over the node set $V' \subset V$ is denoted by $A[V']$ and is drawn from the probability space $(\Omega', \mathbb{F}', \mathbb{P}')$, where Ω' is the set of all graphs with node set V', $\mathbb{F}'$ is the family of all subsets of Ω', and for a given $\tilde{A}' \in \Omega'$, $\mathbb{P}'(\tilde{A}') = \sum_{\{\tilde{A} \in \Omega | \tilde{A}[V'] = \tilde{A}'\}} \mathbb{P}(\tilde{A})$.

The rest of the paper is organized as follows. Section 2 presents our basic model, focusing on the case in which attacks are random (undirected with respect to security investments). It shows why, because of the strategic substitutes aspect of investments, the common conjecture that there will necessarily be underinvestment in security does not always hold. Section 4 establishes that when costs functions are "sufficiently convex" and networks are trees, the equilibrium is unique and always involves underinvestment relative to the social optimum. Section 5 extends these results to random networks that are "locally tree-like," meaning that they feature low probability of a cycle within the component of the network attached to any particular agent. Section 6 establishes a similar uniqueness and underinvestment results for symmetric random networks and for island networks (which consist of several symmetric islands sparsely connected to each other). This section also provides a ranking of the extent of contagion across different symmetric networks. Section 7 considers strategic attacks (directed with respect to to the security investment profile of agents), and shows an additional reason for overinvestment. Section 8 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 a random network A drawn from a probability space $(\Omega, \mathbb{F}, \mathbb{P})$, where Ω is the set of undirected networks with node set V.[2] We use A^r to denote a realization of random network A and refer to it as the *interaction network*. We often use the terminology A^r *is generated from* A, denoted by $A^r \sim A$, to highlight the dependence on the random network A.[3]

An attacker exposes one of the agents to an infection (virus), which then spreads dynamically to the other agents. Attacker's decision of which agent to target is represented by the probability vector $\Phi = (\rho_1, \ldots, \rho_n)$, where ρ_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

[2] We will use the terms agent, node and individual interchangeably throughout the paper. Similarly, we will use the terms network and graph interchangeably.

[3] A *deterministic* network $G = (V, E)$ is a special case of this model in which $\mathbb{P}(G) = 1$ and for all $G' \neq G$, $\mathbb{P}(G') = 0$.

on the edges of the interaction network.[4]

Before the interaction network A^r and 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 $\mathbf{q}_{-i} = [q_j]_{j\in V,\, j\neq i}$ to denote the security profiles (short for security investment profiles) of all agents and all agents other than i respectively. 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).[5]

Given network A, security profile $\mathbf{q}$ and attack decision Φ, we denote the probability of node i getting infected by $\mathbf{P}_i(A,\mathbf{q},\Phi)$. The utility function of agent i, denoted by u_i is given by

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

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. However, all the results hold even without this assumption. 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 $\lim_{q\to 1} c'(q) = \infty$.*[6]

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

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

Given network A and security profile $\mathbf{q}$, we define the *transmission network* as the subgraph of the interaction network A^r induced over the set of susceptible agents $V_s \subset V$ and denote it by A^t. The infection is transmitted through the transmission network.[7] In particular, given transmission network A^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 A^t.

[4]For example, when the network A is generated according to an Erdös-Rényi graph with parameter $p \in (0,1)$ (i.e., there exists an edge between any pair of agents independently with probability p), this implies that an infected agent transmits the infection to each of the other agents independently with probability p.

[5]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.

[6]The boundary conditions are imposed to simplify the exposition, and all of our results hold without them.

[7]Formally, given $A^r = (V,E)$ and a set of susceptible agents $V_s \subset V$, the transmission network A^t is given by $A^t \equiv A^r[V_s] = (V_s, \{(i,j) \in E \mid i,j \in V_s\})$. We often use the terminology A^t *is generated from* $(A,\mathbf{q})$, denoted by $A^t \sim (A,\mathbf{q})$, to highlight the dependence on the random network A and the security profile $\mathbf{q}$. The probability of transmission network A^t can be written as

$$P(A^t) = \sum_{\{A^r,V_s \,\mid\, A^t = A^r[V_s]\}} P(A^t \mid A^r, V_s) = \sum_{\{A^r,V_s \,\mid\, A^t = A^r[V_s]\}} \mathbb{P}(A^r) \prod_{i\in V_s}(1-q_i) \prod_{i\notin V_s} q_i.$$

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 $\Phi = (\rho_1, \ldots, \rho_n)$. We first present key properties of equilibria and social optimum for this model, which will also apply (in a slightly modified form) to our analysis of the strategic attack model. Our first result provides a characterization for the infection probability of an agent in terms of his security level q_i and a network effect caused by the other agents. We then show that the network effect admits a simple decomposition that highlights the contribution of the agents on infection one at a time. These characterizations enable us to express individual utility and social welfare in a form that makes the dependence on the security levels explicit. We use these expressions to show the existence of a pure-strategy Nash equilibrium for the resulting game, to characterize the best response and welfare maximizing strategies of agents, and to study the monotonicity behavior of best response strategies in response to changes in security profiles of other agents. In the last subsection, we focus on symmetric networks (defined formally below) and show that while such networks have a unique symmetric equilibrium that features underinvestment, they may also have asymmetric equilibria in which some agents over invest compared to the social optimum.

3.1 Key Properties

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

Proposition 3.1 (Network Effect)**.** *Given network A, security profile $\mathbf{q}$, and attack decision Φ, the infection probability of agent i satisfies*

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

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

[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.

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

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 $\tilde{P}_i(A, \mathbf{q}_{-i}, \Phi)$ as the *network effect* of A 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 3.2 (Decomposition)**.** *Given network A, security profile $\mathbf{q}_{-j}$, and attack decision Φ, the probability of infection reaching agent j, $\tilde{P}_j(A, \mathbf{q}_{-j}, \Phi)$, satisfies the following: For all $i \in V,\ i \neq j$,*

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

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

We refer to $(1-q_i)Q_{j,i}(A, \mathbf{q}_{-\{i,j\}}, \Phi)$ 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 a 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 goes through i. The probability of first event is equal to the probability of infection reaching agent j in the network A_{-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 $(1-q_i)$. Figure 2 illustrates different transmission networks over which infection reaches agent j: Fig. 2(a) shows instances in which event (A) occurs, and Fig. 2(b) shows an instance in which event (B) occurs.

3.2 Existence

Using Proposition 3.1, we can write the utility function of agent i as the following:

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

[9] In a graph $G = (V, E)$, a *path* between nodes u and v corresponds to $u = v_0, e_1, v_1, e_2, \ldots, e_k, v_k = v$ where $e_i = (v_{i-1}, v_i) \in E$, for all $1 \le i \le k$ 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.

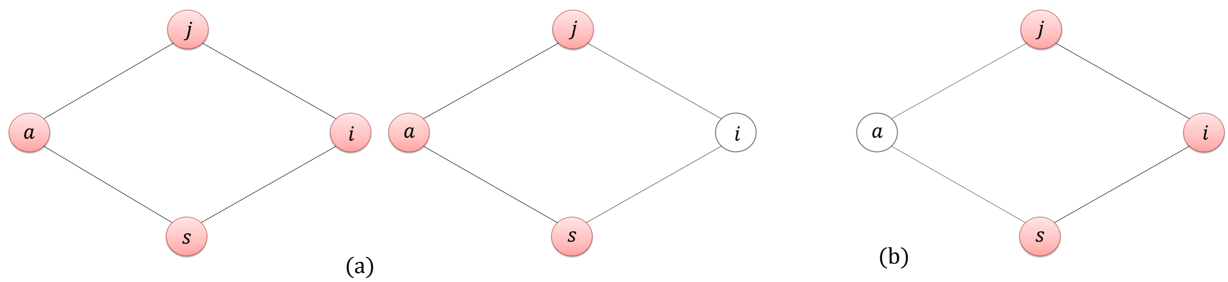

Figure 2: *Transmission networks over which the infection reaches agent j. Figure (a) shows transmission networks in which there exists a path from s to j that does not include i (event (A) occurs). Figure (b) shows the transmission network in which all possible paths from s to j goes through i (event (B) occurs).*

Similarly, fixing any $i \in V$, from Propositions 3.1 and 3.2, social welfare takes the following form:

$$\begin{aligned} W(A, \mathbf{q}) &= \sum_{j \in V} u_j(A, \mathbf{q}, \Phi) \\ &= \Big(1 - (1 - q_i)\tilde{P}_i(A, \mathbf{q}_{-i}, \Phi)\Big) - c_i(q_i) \\ &\quad + \sum_{j \in V\, j \neq i} \left(1 - (1 - q_j)\left(\tilde{P}_j(A_{-\{i\}}, \mathbf{q}_{-\{i,j\}}, \Phi) + (1 - q_i) Q_{j,i}(A, \mathbf{q}_{-\{i,j\}}, \Phi)\right)\right) - c_j(q_j). \end{aligned} \tag{3.1}$$

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

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

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

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

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

Theorem 3.1 (Equilibrium Existence)**.** *In the random attack model, for any network A, there exists a pure-strategy Nash equilibrium.*

The existence of a pure-strategy Nash equilibrium follows from the linearity of the utility function $u_i(A, \mathbf{q}, \Phi)$ in q_i, its continuity in $\mathbf{q}$, and the fact that the strategy spaces are compact, and we omit a formal proof.

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:

$$c_i'(B_i(\mathbf{q}_{-i})) = \tilde{P}_i(A, \mathbf{q}_{-i}, \Phi). \tag{3.2}$$

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

$$c_i'(S_i(\mathbf{q}_{-i})) = \tilde{P}_i(A, \mathbf{q}_{-i}, \Phi) + \sum_{j \neq i}(1 - q_j)Q_{j,i}(A, \mathbf{q}_{-\{i,j\}}, \Phi). \tag{3.3}$$

A comparison of these two expressions immediately establishes that

$$B_i(\mathbf{q}_{-i}) \leq S_i(\mathbf{q}_{-i}). \tag{3.4}$$

Given the profile of security investments of other agents, agent i always invests less in best response strategy than in the welfare maximizing strategy. However, as Example 1 in the Introduction shows, this does not imply underinvestment by all agents.

The network effect satisfies intuitive monotonicity properties given in the following proposition.

Proposition 3.3. *Given network A 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 $\tilde{P}_i(A, \mathbf{q}_{-i}, \Phi) \leq \tilde{P}_i(A, \hat{\mathbf{q}}_{-i}, \Phi)$.

(b) For any $\hat{V} \subset V$, $\tilde{P}_i(A_{-\hat{V}}, \mathbf{q}_{-(\hat{V} \cup \{i\})}, \Phi) \leq \tilde{P}_i(A, \mathbf{q}_{-i}, \Phi)$.

(c) If $\tilde{P}_i(A, \mathbf{q}_{-i}, \Phi) \geq \tilde{P}_i(A, \hat{\mathbf{q}}_{-i}, \Phi)$, 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 probability of the infection reaching agent i is smaller in a subgraph (which is expected since there are more paths along which infection can reach agent i in the original graph). Finally, part (c), which will play an important role in some of our later proofs, shows that the best response strategy of agent i is higher when the network effect of A on i is higher.

3.3 Symmetric Networks

We next focus on *symmetric networks* (with symmetric agents in terms of their cost function c_i, which is denoted by c in this subsection).

Definition 1 (Symmetric Network). *A random network A is symmetric if for any permutation $\pi : V \to V$, $A' = \pi(A)$ has the same distribution as A.*

The preferential attachment networks, Erdos-Renyi random graphs and random graphs with arbitrary degree distributions are examples of symmetric networks.[11]

[11] Note that the interaction network need not be symmetric; rather, agent locations within the network are identical in expectation.

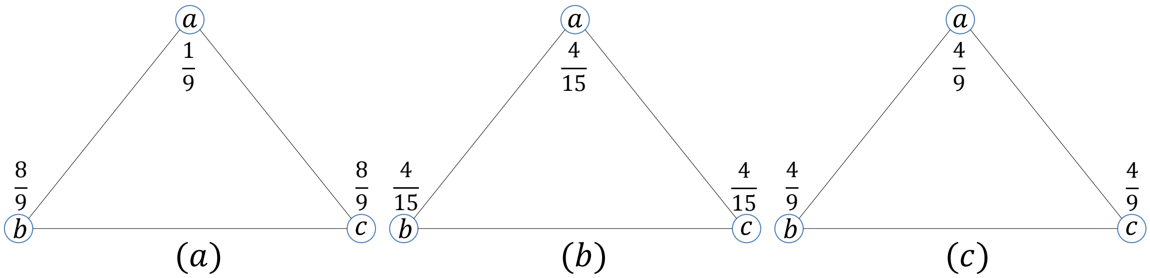

Figure 3: *A 3-cycle network. Figure (a) shows the asymmetric equilibrium security profile, Figure (b) shows the symmetric equilibrium security profile, and Figure (c) shows the symmetric social optimum security profile.*

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

Theorem 3.2. *Suppose Assumption 1 holds. For a symmetric network, there exists a unique symmetric equilibrium (with investment q^e) and a unique symmetric social optimum (with investment q^s). Moreover we have $q^e \leq q^s$.*

The key result in Theorem 3.2 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.(3.4): 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.

This intuition does not extend to asymmetric equilibria of symmetric networks as the next example shows.

Example 3.1. Consider the 3-cycle network illustrated in Fig. 3. We assume that $c(q) = q^2(\frac{49}{24} - \frac{5}{4}q)$. One can verify that the security level at the unique symmetric equilibrium is $q^e = \frac{4}{15}$. This example has an asymmetric equilibrium given by $\hat{\mathbf{q}}^e = (\frac{1}{9}, \frac{8}{9}, \frac{8}{9})$. Moreover, it has a unique social optimum, which is symmetric with security level $q^s = \frac{4}{9}$.

4 Tree Networks with Sufficiently Convex Cost Functions

In this and the subsequent two sections, we focus on tree networks and cost functions that satisfy a stronger requirement than convexity, which we refer to as *sufficiently convexity*. A graph is a *tree* if it is connected and acyclic. A graph is *acyclic* if it has no cycle and is *connected* if between each pair of nodes, a path exists.

We will show that the combination of these two assumptions ensures that expected infections at the social optimum is less than or equal to that in the equilibrium. The role of each of these assumptions will be clarified later in this section.

We first define our new assumption on the investment cost functions.

Assumption 2 (Sufficiently Convex Cost Function)**.** *For each i, the cost function $c_i : [0,1] \to \mathbb{R}_+$ is sufficiently convex if $c_i'(q)(1-q)$ is strictly increasing over $[0,1]$.*

This assumption is equivalent to the function $\tilde{c}(x) = c(1-x)$ having an elasticity of marginal cost greater than or equal to 1. An example of a sufficiently convex cost function is $c(q) = -q - \log(1-q)$.

To understand the implications of sufficiently convex cost functions, recall the first-order condition satisfied by the best response strategy $B_i(\mathbf{q}_{-i})$ of agent i given in Eq. (3.2). In view of Proposition 3.1, the infection probability of agent i, when he selects his best response strategy given the security profile $\mathbf{q}_{-i}$, can be expressed as

$$\mathbf{P}_i(A, (B_i(\mathbf{q}_{-i}), \mathbf{q}_{-i}), \Phi) = (1 - B_i(\mathbf{q}_{-i}))c_i'(B_i(\mathbf{q}_{-i})).$$

The key implication of Assumption 2 is that, when $\mathbf{q}_{-i}$ decreases, even if agent i in response increases his investment, his probability of infection will still increase. Put differently, sufficiently convex cost functions ensure that direct effects (change in others' investments) dominate indirect effects (the response to this change). The next lemma states this result more formally.

Lemma 4.1. *Suppose Assumptions 1 and 2 hold. Let $\mathbf{q}_{-i}$ and $\hat{\mathbf{q}}_{-i}$ be such that $\tilde{P}_i(A, \mathbf{q}_{-i}, \Phi) \geq \tilde{P}_i(A, \hat{\mathbf{q}}_{-i}, \Phi)$. Then $\mathbf{P}_i(A, (B_i(\mathbf{q}_{-i}), \mathbf{q}_{-i}), \Phi) \geq \mathbf{P}_i(A, (B_i(\hat{\mathbf{q}}_{-i}), \hat{\mathbf{q}}_{-i}), \Phi)$.*

This lemma clarifies the role of the sufficiently convex cost assumption in establishing results on "underinvestment in equilibrium" for general networks: even though underinvestment by others triggers overinvestment by agent i, sufficiently convex cost functions ensure that i's overall infection probability increases when this is the case and thus bounding how much i's investment can increase.

Nevertheless, Lemma 4.1 does not immediately imply that expected infections are necessarily higher in the equilibrium than in the social optimum. This can be proven for tree networks, which also guarantees uniqueness of equilibrium.

Theorem 4.1. *Suppose Assumptions 1 and 2 hold. For any tree network, there exists a unique pure-strategy Nash equilibrium security profile.*

Here we provide the intuition for the proof of this result, which illustrates the central roles of both sufficiently convex cost functions and the tree structure. If there exist multiple equilibria $\mathbf{q}^e$ and $\hat{\mathbf{q}}^e$, we can find an edge (x, y) such that $q_x^e > \hat{q}_x^e$, $q_y^e < \hat{q}_y^e$, and for all nodes v in the subtree rooted at y (i.e., nodes that reaches x through y) $q_v^e < \hat{q}_v^e$. By sufficiently convex cost assumption, this implies

$$\mathbf{P}_x(A, \mathbf{q}^e, \Phi) > \mathbf{P}_x(A, \hat{\mathbf{q}}^e, \Phi) \text{ but } \mathbf{P}_y(A, \mathbf{q}^e, \Phi) < \mathbf{P}_y(A, \hat{\mathbf{q}}^e, \Phi). \tag{4.1}$$

The idea is then to exploit the tree network structure and establish a contradiction. In particular, because $q_v^e < \hat{q}_v^e$ for all v in the subtree rooted at y, the probability of infection for agent y coming from this subtree is greater under the profile $\mathbf{q}^e$ than $\hat{\mathbf{q}}^e$. In addition, if the probability of infection for y from its upstream neighbors was also higher under the profile $\mathbf{q}^e$ than $\hat{\mathbf{q}}^e$, then this would contradict (4.1). Moreover, if the probability of infection for y from its upstream neighbors was lower under $\mathbf{q}^e$ than $\hat{\mathbf{q}}^e$, then this would contradict the ranking of the investments of x and y in the two candidate equilibria, again yielding a contradiction. Intuitively, in a tree network with sufficiently convex cost functions, greater investment in one part of the network always translates into higher probability of infection for neighboring agents, and this precludes the possibility of two different equilibrium profiles.

More importantly, tree networks and sufficiently convex cost functions also ensure an unambiguous ranking between expected infections in equilibrium and social optimum as shown in the next theorem.

Theorem 4.2. *Suppose Assumptions 1 and 2 hold. Let $I(A, \mathbf{q}, \Phi)$ denote expected infections in network A with security profile $\mathbf{q}$ and attack decision Φ. Given tree network A, we have $I(A, \mathbf{q^e}, \Phi) \geq I(A, \mathbf{q^s}, \Phi)$ where $\mathbf{q^e}$ and $\mathbf{q^s}$ are the equilibrium and the socially optimal security profiles.*

This theorem also holds for any random network where the realizations correspond to a set of potentially disconnected trees, e.g., we start with a tree, and each edge remains active with probability $p \in (0, 1]$.

The economic intuition of this theorem is related to the reason why such a result is not true in general networks and without sufficiently convex cost functions. We have seen that underinvestment by an agent triggers overinvestment by others (because investments in security are strategic substitutes), and this response can have a greater impact on expected infections than underinvestment by the first agent. Sufficiently convex cost functions limit the extent of the indirect response of an agent, and the tree network by ruling out cycles ensures that we can use this bound to rank expected infections in equilibrium and social optimum.

The technical intuition of the proof of Theorem 4.2 is also instructive, as illustrates why tree networks and sufficiently convex cost functions are important for the result. For this reason, while a formal proof is provided in the Appendix, we discuss the main idea here.

Consider the set $V_1 = \{i \in V \mid q_i^s \leq q_i^e\}$, i.e., V_1 is the set of agents that overinvest in the equilibrium relative to the social optimum (if V_1 is empty, it means that all agents underinvest in the equilibrium and the result follows straightforwardly). For any $\bar{V} \subset V$, let $C_I(i, A_{-\bar{V}})$ denote the contribution of agent i to infection in subgraph $A_{-\bar{V}}$ for a given security profile $\mathbf{q}$, i.e.,

$$C_I(i, A_{-\bar{V}}, \Phi) = (1-q_i)\left(\tilde{P}_i(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}\cup\{i\}}, \Phi) + \sum_{j\in V-\bar{V}\cup\{i\}} (1-q_j) Q_{ji}(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}\cup\{i,j\}}, \Phi)\right). \quad (4.2)$$

The key to the proof of Theorem 4.2 is the following lemma which establishes that for tree networks, the contribution of agents to infection in a subgraph is upper bounded by their contribution to infection in the original graph.

Lemma 4.2. *Given tree network A and node set $\bar{V} \subset V$,*

$$\sum_{i\in V-\bar{V}} C_I(i, A_{-\bar{V}}) \leq \sum_{i\in V-\bar{V}} C_I(i, A).$$

The intuition follows from the fact that for tree networks, if an agent k is removed, then the network effect of agent i on agent j either remains constant (if the path between the two did not include k) or decreases to zero. (if the path did include k.) This is not necessarily true for graphs with cycles as Example A.1 in the Appendix shows.

Using Lemma 4.2, an upper bound for expected infections in the social optimum is the following:

$$I(A, \mathbf{q}^s, \Phi) \leq I(A_{-V_1}, \mathbf{q}^s_{-V_1}, \Phi) + \sum_{i\in V_1} c_i'(q_i^s)(1-q_i^s).$$

Here we used Eq. (3.3) to write $C_I(i, A)$ as $c_i'(q_i^s)(1-q_i^s)$ (and see also Lemma A.1 in the Appendix). Moreover, expected infections in the equilibrium can be lower bounded as follows:

$$I(A, \mathbf{q}^e, \Phi) \geq \sum_{i\in V_1} c_i'(q_i^e)(1-q_i^e) + I(A_{-V_1}, \mathbf{q}^e_{-V_1}, \Phi_{-V_1}).$$

This lower bound is obtained by applying Eq. (3.2) for the agents in V_1 and using Proposition 3.3(b) to provide a lower bound on expected infections among agents outside set V_1.

These two bounds, combined with the following observations, yield the desired result.

(1) $I(A_{-V_1}, \mathbf{q}^e_{-V_1}, \Phi_{-V_1}) \geq I(A_{-V_1}, \mathbf{q}^s_{-V_1}, \Phi_{-V_1})$ since $q_i^s \geq q_i^e$ for all $i \in V - V_1$;

(2) $\sum_{i\in V_1} c_i'(q_i^e)(1-q_i^e) \geq \sum_{i\in V_1} c_i'(q_i^s)(1-q_i^s)$ since investment cost functions are sufficiently convex and $q_i^s < q_i^e$ for all $i \in V_1$.

Example A.2 in the Appendix shows that Assumption 2 cannot be dispensed with for the results of Theorems 4.1 and 4.2, i.e., for tree networks, if the investment cost function is not sufficiently convex, the equilibrium need not be unique and expected infections in equilibrium may be strictly lower than that at the social optimum.

5 Large Networks and Local Tree Structures

The previous section established that expected infections are greater in equilibrium than in the social optimum provided that investment cost functions are sufficiently convex and the network is a tree. The latter assumption is particularly restrictive as communication networks do not generally resemble trees (typically involve cycles, which are ruled out with the tree assumption). In this section, we show that the same efficiency comparison holds for large networks provided that they have a "local tree structure".

5.1 Local Tree Structures

We start by defining the local tree concept formally.

Definition 2 (h-Local Tree Structure). *A random network has h-local tree structure if the connected component attached to each agent of the network is acyclic with probability at least h.*

In other words, a local tree structure only requires a high probability that the components attached to an agent is acyclic (thus it allows some probability of cycles and also cycles in other parts of the network).

Our main result provides a relation between expected infections in equilibrium and in the social optimum for a network with a local tree structure.

Theorem 5.1. *Suppose Assumptions 1 and 2 hold. Given a network with $1-\epsilon$-local tree structure, we have $I(A, p, \mathbf{q}^e, \Phi) + \epsilon n \geq I(A, p, \mathbf{q}^s, \Phi)$ where $\mathbf{q}^e$ and $\mathbf{q}^s$ are the equilibrium and the socially optimal security profiles.*

The economic intuition of this result is closely related to Theorem 4.2, and again exploits sufficiently convex cost functions and the structure of the network, which now, with high probability, rules out cycles in the spread of an infection within the component of the network attached to each agent.The proof also illustrates the relationship between this result and Theorem 4.2. In particular, the proof considers expected infections in cyclic and acyclic components of each interaction network separately. Expected infections in cyclic components is bounded above by expected number of agents belonging to cyclic components and as a result is at most ϵn. We then use a similar argument as in the proof of Theorem 4.2 to show that expected infections in the social optimum in acyclic components of the interaction network is less than or equal to expected infections in the equilibrium.

5.2 Large Networks and Local Tree Structures

One question posed by Theorem 5.1 is whether the remainder term, $n\epsilon$, is truly small in the sense that $n\epsilon(n) \to 0$ as $n \to \infty$ (where we emphasize that this is not trivial because ϵ is a function of n as our notation $\epsilon(n)$ here underscores). We next show that for a random network model in which we first generate the interaction network and then activate the edges independently with probability $p > 0$, the answer is affirmative. In particular, under the right conditions on p, the network in question has a $1 - \epsilon(n)$-local tree structure and $n\epsilon(n) \to 0$ as $n \to \infty$.

In this random network model, we first generate the interaction network and then activate edges independently with activation probability p. We use A^a to denote a realization of random network A under the activation probability p and refer to it as the *activated network*. We will use the terminology A^a *is generated from* (A, p), denoted by $A^a \sim (A, p)$ to represent the dependence on random graph A and the activation probability p. We next provide conditions on (A, p) under which $\lim_{n\to\infty} \epsilon(n)$ as well as $\lim_{n\to\infty} n\epsilon(n)$ is 0.

Let the eigenvalue $\lambda(G)$ represent the second largest in absolute value of the adjacency matrix of the degenerate network G. For a given $d < n$, let $\mathcal{G}_d$ denote the set of $d-$ regular graphs G with $\lambda(G) = o(d)$. Combining Lemma A.5 and Theorem A.1 (see Appendix A.6), we obtain the following theorem.

Theorem 5.2. *Given random network A generated from* $(\Omega, \mathbb{F}, \mathbb{P})$, *where* $\Omega = \{G = (V, E) | E \subset \hat{E}, (V, \hat{E}) \in \mathcal{G}_d\}$,

- *If* $d = \Omega(\sqrt{n})$ *and* $p < \frac{1}{d}$, *the generated random network from* (A, p) *is a* $1 - \epsilon(n)$*-local tree network with* $\lim_{n\to\infty} \epsilon(n) = 0$.
- *If* $p < \frac{1}{n \log^2(n)}$, *the generated random network from* (A, p) *is a* $1 - \epsilon(n)$*-local tree network with* $\lim_{n\to\infty} \epsilon(n)n = 0$.

Intuitively, for p small, all components of the random graph of size n are smaller than $\log n$ with high probability. Then the result follows by bounding the probability of a cycle within each component.

6 Symmetric and Island Networks

The previous two sections establish a comparison between expected infections in equilibrium and social optimum for two classes of special networks (trees and large graphs with locally tree structure) under sufficiently convex cost functions. In this section, we establish a similar comparison for symmetric random networks and for "islands" networks, which consist symmetric "islands" sparsely connected to each other. An important step in our results is to prove the uniqueness of equilibrium, which rules out the possibility of highly asymmetric equilibria with counterintuitive implications as in example in the Introduction. We end this section by providing a ranking of different random symmetric networks in terms of expected equilibrium infections, thus quantifying which sorts of networks are likely to lead to greater contagion of infection.

6.1 Uniqueness of Equilibrium

Our next result establishes the existence of a unique symmetric pure-strategy Nash equilibrium in symmetric networks (and no other equilibria) when the investment cost function is sufficiently convex. An immediate corollary of this result that follows from Theorem 3.2 is then the comparison of expected infections in equilibrium and social optimum.

Theorem 6.1. *Suppose Assumptions 1 and 2 hold. Given symmetric random network A, there exists a unique pure-strategy Nash equilibrium and a unique socially optimal security profile.*

Corollary 6.1. *Suppose Assumptions 1 and 2 hold. Given symmetric random network A, we have $I(A, \mathbf{q}^{\mathbf{e}}, \Phi) \geq I(A, \mathbf{q}^{\mathbf{s}}, \Phi)$ where $\mathbf{q}^{\mathbf{e}}$ and $\mathbf{q}^{\mathbf{s}}$ are the equilibrium and the socially optimal security profiles.*

Recall from Section 3.3 that there is underinvestment in the symmetric equilibrium of symmetric networks (compared to the social optimum). The problem, however, was that there can also be asymmetric equilibria in such symmetric networks which feature overinvestment. By establishing uniqueness, Theorem 6.1 rules out such asymmetric equilibria and thus guarantees equilibrium underinvestment.

6.2 Islands Network

In this subsection, we consider "islands" networks, which can be considered as a generalization of symmetric networks in the sense that it combines a number of symmetric networks (islands). Similar types of networks are also considered Golub and Jackson (2012).

Definition 3 (Islands networks)**.** *An islands network consists of a set of agents denoted by V, a set of islands denoted by $\mathcal{H} = \{H_1, H_2, \ldots, H_n\}$, and a set of edges (or bridges) between the islands (i.e., between randomly selected agents from the islands) denoted by T. Each agent $v \in V$ resides on one island $H_j \in \mathcal{H}$. We assume that each H_i is a symmetric random network and the edges of T form a tree network when we view each island as a supernode.*

In the rest of this section, we use H_i to denote both the symmetric random network and the realized interaction network corresponding to island i. We abuse the notation and denote an islands network by $A = (V, \mathcal{H}, T)$. Our next result establishes uniqueness of equilibrium (again under Assumptions 1 and 2).

Theorem 6.2. *Suppose Assumptions 1 and 2 hold. For any islands network, there exists a unique pure-strategy Nash equilibrium security profile.*

Our main result for this subsection establishes that under Assumptions 1 and 2 in islands networks, expected infections is greater in equilibrium than the social optimum.

Theorem 6.3. *Suppose Assumptions 1 and 2 hold. Given islands network $A = (V, \mathcal{H}, T)$, we have $I(A, \mathbf{q}^{e}, \Phi) \geq I(A, \mathbf{q}^{\mathbf{s}}, \Phi)$ where $\mathbf{q}^{e}$ and $\mathbf{q}^{s}$ are the equilibrium and the socially optimal security profiles.*

The proof and the intuition of this result follow those of Theorem 4.2, and are again based on bounding the contribution of a subset of agents to the expected infections, but now focusing on the contribution of an island (see in particular, Lemma A.6 in the Appendix).

6.3 Ranking Symmetric Networks

Our results so far have not been informative about the extent of contagion and expected infections in a network (except for comparing between equilibrium and social optimum). In this subsection, we provide a ranking across symmetric networks in terms of their expected equilibrium infections.

With this objective in mind, we represent the network structure in symmetric networks using the following equivalent characterization: a symmetric random network can be generated from a distribution over a set of fixed graphs $\mathcal{G}$ (referred to as *base graphs*) and a uniform allocation of each agent to one of the nodes of the base graph. To simplify the exposition, we will focus on a degenerate distribution over the base graphs (we assume there is only one base graph) though our results extend to the more general case. We use G to denote the base graph and $\hat{G}$ to denote the corresponding symmetric random network.

Our next result shows that as the base graph gets denser, expected equilibrium infections increases. We say that a graph G is *denser* than G', if G has additional links relative to G' and denote it by $G' \subset G$. Since the equilibrium security profile in symmetric random graphs is always symmetric, without loss of generality we represent the equilibrium security profile with the symmetric equilibrium security level in the rest of this section.

Theorem 6.4. *Suppose Assumptions 1 and 2 hold. Given two base graphs G_1 and G_2, if $G_1 \subset G_2$ then $I(\hat{G}_1, q_1^e, \Phi) \leq I(\hat{G}_2, q_2^e, \Phi)$ where q_1^e and q_2^e represent the equilibrium security levels for $\hat{G}_1$ and $\hat{G}_2$.*

The economic idea here is simple. A denser network generates more interlinkages and thus more pathways for an infection to spread. Recognizing this, agents will typically increase their security investments in a denser network (relative to a less dense network), but under sufficiently convex cost functions, this response will never dominate the increase in infection probabilities due to the greater density of linkages.

The density of connections does not enable us to compare many important networks, including trees. We next define a partial order on trees that allows us to compare equilibrium behavior. We start by defining the distance vector for a tree network.

Definition 4 (Distance Vector)**.** *For a given tree network T, $\mathbf{d}_T = (d_1, \dots, d_n)$ is the distance vector of T, where d_i is the number of (distinct) pair of nodes that are at distance $i-1$ from each other.*

For example, the distance vector for a star base graph S_n with n nodes is $\mathbf{d}_{S_n} = (0, 2(n-1), (n-1)(n-2), 0, \dots, 0)$. For two tree networks T_1 and T_2, we define a partial order in terms of the distance vector as follows:

Definition 5 (Domination, $\prec$)**.** *For two tree base structures T and T', let $\mathbf{d}_T = (d_1, \ldots, d_n)$ and $\mathbf{d}_{T'} = (d'_1, \ldots, d'_n)$ represent their distance vector. Tree T dominates T', denoted by $T' \prec T$, if for all $1 \leq i \leq n$, $\sum_{j=1}^{i} d'_j \leq \sum_{j=1}^{i} d_j$.*

Proposition 6.1. *Suppose Assumptions 1 and 2 hold. For two symmetric networks with tree base graphs T_1 and T_2, if $T_2 \prec T_1$ then $I(\hat{T}_1, q_1^e, \Phi) \geq I(\hat{T}_2, q_2^e, \Phi)$ where q_1^e and q_2^e denote the equilibrium security levels in $\hat{T}_1$ and $\hat{T}_2$.*

One can show that for symmetric networks with tree base graphs, a star network dominates all the other trees and the path network will be dominated by all trees. Note that this relation does not provide a complete order over tree networks.

Our final result in this subsection provides a comparison of expected infections for any two symmetric networks. For a given base graph G, let $\varrho_G(\frac{k}{n})$ denote the normalized expected size of the connected component attached to a random agent v in the induced subgraph of G over V_k where V_k is the set of k randomly selected agents from G.

Theorem 6.5. *Suppose Assumptions 1 and 2 hold. For two symmetric networks $\hat{G}_1$ and $\hat{G}_2$ with base graphs G_1 and G_2, $I(\hat{G}_1, q_1^e, \Phi) \geq I(\hat{G}_2, q_2^e, \Phi)$ if for all $x \in [0, 1]$, $\varrho_{G_1}(x) \geq \varrho_{G_2}(x)$, and only if there is no $\epsilon > 0$ and an interval $I \subset [0, 1]$ of length at least $\sqrt{\frac{2\ln(2+2/\epsilon)}{n}}$ such that $\varrho_{G_1}(\frac{k}{n}) < \varrho_{G_2}(\frac{k}{n}) - \epsilon$ for all $\frac{k}{n} \in I$.*

This result follows from the following characterization which enables us to express the number of infected agents as a Bernstein polynomial of q with coefficients $\varrho_G(\frac{i}{n})$.

Proposition 6.2. *Given a base graph G with n nodes and a symmetric security profile q, expected equilibrium infections are given by*

$$I(G, q, \Phi) = \sum_{i=1}^{n} n(1-q)^i q^{n-i} \varrho_G\left(\frac{i}{n}\right)\binom{n}{i}.$$

7 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 an attack may not be independent of security investments. In this section, we focus on this latter case. The main insight is that strategic attack generates another reason for overinvestment in security relative to the social optimum, this time even with sufficiently convex cost functions.[12]

[12]One could also consider a hybrid model where the attack can be targeted across agents according to their characteristics (e.g., their cost functions or their position in the network) but not according to their security investments —for example, the attack decision takes place before or at the same time as the investment decisions. From the viewpoint of overinvestment, this hybrid model would be similar to the random attack model, because agents cannot discourage attacks by further increasing their investments.

More specifically, we consider a strategic attacker which, after observing the security profile of agents, selects an attack decision $\Phi = (\rho_1, \ldots, \rho_n)$ (where ρ_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 $\sum_{i=1}^{n} \zeta(\rho_i)$ where ζ is a convex function and twice continuously differentiable. A key assumption in our model is that the attacker observes the security level of all the agents. We therefore analyze the *Stackelberg equilibrium* of the resulting two stage game: the agents select their security levels anticipating the decision of the attacker and the attacker optimizes his attack strategy given the security choices. Given the best response attack strategy of the attacker, we refer to the Nash equilibrium among the agents as the *Nash equilibrium of the security game*.

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. Technically, pure-strategy equilibria may generally fail to exist for reasons similar to the non-existence of pure-strategy equilibria and Bertrand competition with capacity constraints, as the next example illustrates.

Example 7.1. *Consider the network A with 2 singleton agents. We show that attacking a single agent without cost may lead to nonexistence of a pure-strategy Nash 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 the Nash equilibrium and present a profitable unilateral deviation for each candidate, establishing nonexistence of a Nash equilibrium:*

(a) $q_1 < q_2$*: In this case, agent 2 has incentive to decrease* q_2*, decreasing the cost without changing his infection probability.*

(b) $q_1 = q_2 < 1$*: In this case agent 2 has incentive to slightly increase* q_2*. This reduces the probability of him being attacked from* $\frac{1}{2}$ *to 0 while slightly increasing his cost.*

7.1 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 notations. We use 1_n to denote the vector of dimension n with each entry equal to $\frac{1}{n}$. Also we define the vector of all 0 except the ith entity which is 1 by e_i. The utility function of the attacker, given network A, security profile $\mathbf{q}$, and an attack decision $\Phi = (\rho_1, \ldots, \rho_n)$, $u_a(A, \mathbf{q}, \Phi)$ is defined as follows:

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

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 3.1 does not hold for this model. This implies that security investments will no longer satisfy the characterization we used so far, cf. Eq. (3.2).

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 we have analyzed so far (where, recall that, each agent is attacked with equal probability independent of their security investments). This property enables us to use the decomposition in Proposition 3.1 to write the utility function of the attacker in closed form.

Lemma 7.1. *Given random network A and security profile $\mathbf{q}$, expected infections when agent i is attacked is equal to the network size times infection probability of agent i under the random attack model, i.e., $I(A, \mathbf{q}, e_i) = n\mathbf{P}_i(A, \mathbf{q}, 1_n) = n(1 - q_i)\tilde{P}_i(A, \mathbf{q}_{-i}, 1_n)$.*

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 is given by the sum (over all j) of the probability of having a path between i and j, and thus the two are closely linked as shown in the lemma.

Given attack decision $\Phi = (\rho_1, \dots, \rho_n)$ and attack cost function ζ, let $\Psi(\Phi) = \sum_{i=1}^{n} \frac{1}{\zeta''(\rho_i)}$ and $\Upsilon(\Phi) = \max_{1 \leq i \leq n} \frac{|\zeta'''(\rho_i)|}{\zeta''(\rho_i)}$.

Theorem 7.2. *In the strategic attack model with convex cost, assume that $c''^2(\Phi)\Upsilon(1-q) + 2\Psi(\Phi)$ for any attack decision Φ. Then there exists a pure-strategy Nash equilibrium.*

The condition in this theorem ensures that the utility of each agent with respect to their own security level is concave. In the next section, we focus on symmetric random graphs. We show that under some conditions over the attacker cost function, agents overinvest in the equilibrium compared to the socially optimal solution.

7.2 Strategic Attacks over Symmetric Graphs

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 investment of one agent creates a positive externality on other agents. Our results so far have shown that, under some assumptions, this force ensures that expected equilibrium infections are greater than (or equal to) expected infections in the social optimum — even though, without these assumptions, overinvestment is also possible in the random attack model. 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 7.2. Consider the line network discussed in Fig. 4 with investment cost function $c'(q) = \frac{q}{2(1-q)}$ for both agents, and attacker cost function $\zeta(\rho) = \frac{\rho^2}{24}$. It can be verified that the unique

Figure 4: *Agents overinvest in the equilibrium relative to social optimum. For investment cost function* $c'(q) = \frac{q}{2(1-q)}$ *and the attack cost function* $\zeta(\rho) = \frac{\rho^2}{20}$*, the security investments in the equilibrium is* $\mathbf{q}^e = (0.66, 0.66)$ *and the security investment in the social optimum is* $\mathbf{q}^s = (0.63, 0.63)$*.*

(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 rest of this subsection provides sufficient conditions for overinvestment or underinvestment. The next assumption ensures that the cost function of the attacker is not "too convex" because otherwise strategic attacks would be essentially like random attacks (deviating from uniform probabilities of attack would be too costly).

Assumption 3 (Boundedly Convex Cost Function)**.** *The function* $\zeta : [0,1] \to \mathbb{R}^+$ *is* boundedly convex *with* $\alpha, \beta > 0$ *if*

- ζ *is twice continuously differentiable, strictly increasing and strictly convex on* $(0, 1]$*,*
- $\zeta(0) = 0$*,* $\zeta'(0) = 0$*,*
- $-\alpha \leq \zeta'''(x) < -\beta$ *where* $0 \leq x \leq 1$*.*

Theorem 7.3. *Suppose Assumption 3 holds with* $\alpha, \beta > 0$*. Given symmetric random network A with* $n \geq \sqrt{\frac{\alpha}{\beta}} + 1$*, a pure-strategy Nash equilibrium always exists.*

The proof of this theorem is straightforward and involves showing that the utility of each agent is concave under Assumption 3.

Our main results in this section is presented next and provides sufficient conditions for overinvestment and underinvestment.

Theorem 7.4. *Suppose Assumption 3 holds. Given symmetric random network A agents will overinvest in the symmetric equilibrium relative to the symmetric socially optimal solution if*

- $\zeta''(\frac{1}{n}) \leq \frac{n-1}{n^2} \frac{c'^{-1}(\frac{1}{n})(1-c'^{-1}(\frac{1}{n}))}{1+(n-1)(1-c'^{-1}(\frac{1}{n}))}$ *when* $c'^{-1}(n) \leq 1 - \frac{1}{\sqrt{n}+1}$*,*
- $\zeta''(\frac{1}{n}) \leq \frac{n-1}{n^2} \frac{c'^{-1}(n)(1-c'^{-1}(n))}{1+(n-1)(1-c'^{-1}(n))}$*, when* $c'^{-1}(\frac{1}{n}) \geq 1 - \frac{1}{\sqrt{n}+1}$*,*
- $\zeta''(\frac{1}{n}) \leq \min(\frac{n-1}{n^2} \frac{c'^{-1}(n)(1-c'^{-1}(n))}{1+(n-1)(1-c'^{-1}(n))}, \frac{n-1}{n^2} \frac{c'^{-1}(\frac{1}{n})(1-c'^{-1}(\frac{1}{n}))}{1+(n-1)(1-c'^{-1}(\frac{1}{n}))})$*. when* $c'^{-1}(\frac{1}{n}) \leq 1 - \frac{1}{\sqrt{n}+1} \leq c'^{-1}(n)$*.*

Also if $\zeta''(\frac{1}{n}) \geq 1$ then agents always underinvest in the symmetric equilibrium relative to the symmetric socially optimal solution.

The various conditions in this theorem are intuitive. They link under/overinvestment to the convexity of the attacker's cost function. Overinvestment requires this cost function not to be "too convex" since, otherwise, the attacker would choose probabilities very close to those in the random attack model (uniform across all agents), thus muting negative externalities. When either of these three conditions in the first part of the theorem is satisfied, negative externalities are non-trivially present because when an agent increases its security investment, it anticipates that this will trigger a large decline in its own probability of being the target of the attack. This creates an "arms race" between agents and leads to overinvestment. In contrast, when the attacker's cost function is sufficiently convex, there will be little response of attack probabilities to security investments, in which case the same forces as in the random attack model dominate and ensure underinvestment (recall that under conditions of Theorem 7.4, there is underinvestment with random attacks).

8 Conclusion

This paper has developed a model of investment in security in a network of interconnected agents. Our baseline model is one of random attacks. Network connections introduce the possibility of cascading failures depending on the profile of security investments by the agents. The existing literature has identified a central positive externality in this environment: security investments reduce the likelihood of an infection spreading to other agents, and because each agent ignores this effect, the existing literature has presumed that there will be underinvestment in security.

We first show that this reasoning is incomplete because of another first-order economic force: security investments are also strategic substitutes. In a general (non-symmetric) network, this implies that underinvestment by some agents will encourage overinvestment by others. We demonstrate by means of examples that not only can there be overinvestment by some agents but also aggregate probabilities of infection can be lower in equilibrium compared to the social optimum.

The bulk of the paper provides a detailed characterization of investment decisions over general networks and sufficient conditions for underinvestment. Our results here rely on a new and tractable decomposition of the probability of infection of an individual into an own and an externality effect. Using this result, we show that there will be equilibrium underinvestment when (1) networks are locally tree-like, symmetric or comprised of sparsely connected islands of symmetric networks; (2) cost functions are sufficiently convex, which guarantee that when an agent faces a higher likelihood of being infected because of others' choices, his or her investment does not increase so much as to reduce her overall probability of infection.

We also characterize the impact of network structure on equilibrium and optimal investments.

Finally, we also extend our analysis to an environment with strategic attacks, where the attacker chooses a probability distribution over the location of the attack in order to maximize damage. We first relate probabilities of infection under strategic attacks to those under random attacks, and then provide sufficient conditions for over and underinvestment in this case. The intuition for overinvestment in this case is simple: greater investment by an agent shifts the attack to other parts of the network.

We view our paper as a first step towards a systematic analysis of contagion over networks in the presence of precautionary behavior and security investments. Obvious next steps include more dynamic models and models in which contagion takes different forms reflecting different economic forces (e.g., resulting from the bankruptcy of a financial institution indebted to others as in Acemoglu, Ozdaglar and Tahbaz-Salehi, 2013).

References

[1] D. ACEMOGLU, A. OZDAGLAR, and A. TAHBAZ-SALEHI, "Systemic risk and stability in financial networks," NBER working paper, National Bureau of Economic Research, 2013.

[2] R. ANDERSON and T. MOORE, "The economics of information security," *Science*, vol. 314, no. 5799, pp. 610–613, 2006.

[3] M. BACCARA and H. BAR-ISAAC, "How to organize crime," *Review of Economic Studies*, vol. 75, no. 4, pp. 1039–1067, 2008.

[4] Y. BACHRACH, M. DRAIEF, and S. GOYAL, "Competig for security," working paper, 2012.

[5] V. BALA and S. GOYAL, "A noncooperative model of network formation," *Econometrica*, vol. 68, no. 5, pp. 1181–1230, 2000.

[6] L. BLUME, D. EASLEY, J. KLEINBERG, R. KLEINBERG, and E. TARDOS, "Network formation in the presence of contagious risk," in *12th ACM conference on Electronic commerce*, pp. 1–10, 2011.

[7] D. L. BRITO, E. SHESHINSKI, and M. D. INTRILIGATOR, "Externalities and compulsary vaccinations," *Journal of Public Economics*, vol. 45, no. 1, pp. 69 – 90, 1991.

[8] F. CHUNG and L. LU, "Connected components in random graphs with given expected degree sequences," *ANNALS OF COMBINATORICS*, vol. 6, no. 2, pp. 125–145, 2002.

[9] D. DE MEZA and J. R. GOULD, "The social efficiency of private decisions to enforce property rights," *Journal of Political Economy*, vol. 100, no. 3, pp. 561–80, 1992.

[10] P. GEOFFARD and T. PHILLIPSON, "Disease eradication: Private versus public vaccination," *American Economic Review*, vol. 87, no. 1, pp. 222–30, 1997.

[11] S. M. GOLDMAN and J. LIGHTWOOD, "Cost optimization in the SIS model of infectious disease with treatment," working paper, University of California at Berkeley, 1995.

[12] B. GOLUB and M. JACKSON, "How homophily affects the speed of learning and best-response dynamics," *The Quarterly Journal of Economics*, vol. 127, no. 3, 2012.

[13] S. GOYAL and A. VIGIER, "Robust networks," Mimeo, Cambridge University, 2011.

[14] S. GOYAL and A. VIGIER, "Social interaction, vaccination, and epidemics," working paper, 2013.

[15] B. HOYER and K. D. JAEGHER, "Strategic network disruption and defense," working paper, Utrecht School of Economics, 2010.

[16] M. O. JACKSON, *Social and Economic Networks*. Princeton University Press, 2008.

[17] M. JACKSON and A. WOLINSKY, "A strategic model of social and economic networks," *Journal of Economic Theory*, vol. 71, no. 1, pp. 44 – 74, 1996.

[18] D. KOVENOCK and B. ROBERSON, "The optimal defense of networks of targets," working paper, 2010.

[19] N. LARSON, "Network security," MPRA paper, University Library of Munich, Germany, 2011.

[20] M. MOLLOY and B. REED, "The size of the giant component of a random graph with a given degree sequence," *Combinatorics, Probability and Computing*, vol. 7, pp. 295–305, 1998.

[21] M. MOLLOY and B. REED, "A critical point for random graphs with a given degree sequence," *Random Structures and Algorithms*, no. 6, pp. 161–180, 2000.

[22] M. E. J. NEWMAN, S. H. STROGATZ, and D. J. WATTS, "Random graphs with arbitrary degree distributions and their applications," *Physical Review E*, vol. 64, p. 026118, 2001.

[23] J. L. SANDERS, "Quantitative guidelines for communicable disease control programs," *Biometrics*, vol. 27, no. 4, pp. 883–893, 1971.

[24] S. P. SETHI, "Quantitative guidelines for communicable disease control program: A complete synthesis," *Biometrics*, vol. 30, no. 4, pp. 681–691, 1974.

[25] F. TOXVAERD, "Foundations of strategic epidemiology: Recurrent infection and treatment," working paper, 2009.

[26] VEGA-REDONDO, *Complex Social Networks*. Cambridge University Press, 2007.

A Appendix

A.1 Background Material

Theorem A.1 (Frieze, Krivelevich, Martin 2003). *Let G be a $d-$ regular graph with $\lambda = o(d)$. Let G_p with $p = \frac{\alpha}{d}$ be obtained from G by including each edge with probability p. If $\alpha < 1$, with high probability the maximum component size of G_p is $O(\log(n))$.*

Theorem A.2 (Bernstein Polynomials). *The $n+1$ Bernstein basis polynomials of degree n are defined as $b_{\nu,n}(x) = \binom{n}{\nu} x^{\nu} (1-x)^{n-\nu}, \quad \nu = 0, \ldots, n.$*

Let f be a continuous function on the interval $[0,1]$. Consider the Bernstein polynomial

$$B_n(f)(x) = \sum_{\nu=0}^{n} f\left(\frac{\nu}{n}\right) b_{\nu,n}(x).$$

Then we have,

$$\lim_{n\to\infty} B_n(f)(x) = f(x)$$

uniformly on the interval $[0,1]$.

Theorem A.3 (Hoeffding's Inequality). *Let $Z_1, \ldots, Z_n$ be independent, identically distributed random variables, such that $0 \le Z_i \le 1$. Then,*

$$Pr\left(\left|\frac{1}{n}\sum_{i=1}^{n} Z_i - E[Z]\right| > \epsilon\right) \le 2e^{-2n\epsilon^2}.$$

A.2 Proofs of Section 3: Random Attack Model

Proof of Proposition 3.1 (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,

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

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

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

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

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

∎

Proof of Proposition 3.2 (Decomposition). As in the previous proof, let (X_i) denote the event that agent i is susceptible and $i \xrightarrow{A^t} j$ denote the event that i is connected to j in A^t. In the given network A, denote the seed node by s. In the transmission network $A^t \sim (A, \mathbf{q})$, 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 A^t_{-i}.

(B) s is not connected to j in ${A^t}_{-i}$, but is connected to j in A^t.

(C) s is not connected to j in A^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 $i \xrightarrow{A} j$ denote the event that i is connected to j in A. Also, let $\mathbb{A}^j$ denote the collection of transmission networks in which j is connected to s, i.e., $\mathbb{A}^j = \{A^t \sim (A, \mathbf{q}) | j \xrightarrow{A^t} s\}$. The infection probability of agent j can be written as

$$\mathbf{P}_j(A, \mathbf{q}, \Phi) = \sum_{A^t \in \mathbb{A}^j} P_{(A,\mathbf{q})}(A^t) = \sum_{\{A_t | A^t_{-i} \in \mathbb{A}^j_{-i}\}} P_{(A,\mathbf{q})}(A^t) + \sum_{\{A^t | A^t_{-i} \notin \mathbb{A}^j_{-i} \bigcap A^t \in \mathbb{A}^j\}} P_{(A,\mathbf{q})}(A^t), \quad \text{(A.2)}$$

where the first term is the probability of event (A) and the second term is the probability of event (B).

We first show that the first term in Eq. (A.2) can be written as

$$\sum_{\{A^t | A^t_{-i} \in \mathbb{A}^j_{-i}\}} P_{(A,\mathbf{q})}(A^t) = \mathbf{P}_j(A_{-i}, \mathbf{q}_{-i}, \Phi). \quad \text{(A.3)}$$

By definition

$$\mathbf{P}_j(A_{-i}, \mathbf{q}_{-i}, \Phi) = \sum_{\{\bar{A}^t | \bar{A}^t \in \mathbb{A}^j_{-i}\}} P_{(A_{-i},\mathbf{q}_{-i})}(\bar{A}^t). \quad \text{(A.4)}$$

The probability of the transmission network $\bar{A}^t$ generated from $(A_{-i}, \mathbf{q}_{-i})$ can be written as the marginal probability of the transmission network A^t that satisfies $A^t_{-i} = \bar{A}^t$, i.e.,

$$P_{(A_{-i},\mathbf{q}_{-i})}(\bar{A}^t) = \sum_{\{A^t | A^t_{-i} = \bar{A}^t\}} P_{(A,\mathbf{q})}(A^t).$$

Combining the preceding relation with Eq. (A.4), we obtain

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

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:

$$\sum_{\{A^t | A^t_{-i} \notin \mathbb{A}^j_{-i} \bigcap A^t \in \mathbb{A}^j\}} P_{(A,\mathbf{q})}(A^t) = (1-q_i)(1-q_j) \sum_{\{A^t | A^t_{-i} \notin \mathbb{A}^j_{-i} \bigcap A^t \in \mathbb{A}^j\}} P_{(A,\mathbf{q})}(A^t | (X_i) \cap (X_j)). \quad \text{(A.5)}$$

Let $Q_{j,i}()$ be the function that represents the probability of event (B) conditional on the event $(X_i) \cap (X_j)$. Clearly, $\sum_{\{A^t | A^t_{-i} \notin \mathbb{A}^j_{-i} \cap A^t \in \mathbb{A}^j\}} P_{(A,\mathbf{q})}(A^t | (X_i) \cap (X_j))$ only depends on $\mathbf{q}_{-\{i,j\}}$ and A and is independent of q_i and q_j. Hence, $Q_{j,i}()$ is a function of A, $\mathbf{q}_{-\{i,j\}}$, and Φ. Hence, it can be expressed as $Q_{j,i}(A, \mathbf{q}_{-\{i,j\}}, \Phi)$. Combining the preceding relation with Eqs. (A.2),(A.3), and (A.5) and using Proposition 3.1, we obtain

$$\begin{aligned}\mathbf{P}_j(A, \mathbf{q}, \Phi) &= \mathbf{P}_j(A_{-i}, \mathbf{q}_{-i}, \Phi) + (1-q_i)(1-q_j) Q_{j,i}(A, \mathbf{q}_{-\{i,j\}}, \Phi) \\ &= (1-q_j)\left(\tilde{P}_j(A_{-i}, \mathbf{q}_{-i}, \Phi) + (1-q_i) Q_{j,i}(A, \mathbf{q}_{-\{i,j\}}, \Phi)\right).\end{aligned}$$

By applying Proposition 3.1 to the preceding equation, we obtain

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

which shows the desired result. ∎

Proof of Proposition 3.3. **(a) Network Effect Monotonicity in Security Profile** We first show that given network A and two security profiles $\mathbf{q}_{-i}$ and $\hat{\mathbf{q}}_{-i}$ with $\mathbf{q}_{-i} \geq \hat{\mathbf{q}}_{-i}$, we have $\tilde{P}_i(A, \mathbf{q}_{-i}, \Phi) \leq \tilde{P}_i(A, \hat{\mathbf{q}}_{-i}, \Phi)$.

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, $\tilde{P}_i(A, \mathbf{q}_{-i}, \Phi) = \tilde{P}_i(A, \hat{\mathbf{q}}_{-i}, \Phi)$.

We next assume that for an integer $m > 0$, if $|\hat{V}| = m$, the claim holds, i.e., $\tilde{P}_i(A, \mathbf{q}_{-i}, \Phi) \leq \tilde{P}_i(A, \hat{\mathbf{q}}_{-i}, \Phi)$ (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 $\tilde{P}_i(A, \mathbf{q}_{-i}, \Phi) \leq \tilde{P}_i(A, \tilde{\mathbf{q}}_{-i}, \Phi)$. Using Proposition 3.2 (with the identification $j = i$ and $i = 1$), we can rewrite $\tilde{P}_i(A, \mathbf{q}_{-i}, \Phi)$ as

$$\begin{aligned}\tilde{P}_i(A, \mathbf{q}_{-i}, \Phi) &= \tilde{P}_i(A_{-1}, \mathbf{q}_{-\{1,i\}}, \Phi) + Q_{i,1}(A, \mathbf{q}_{-\{i,1\}}, \Phi)(1 - q_1) \\ &\leq \tilde{P}_i(A_{-1}, \mathbf{q}_{-\{1,i\}}, \Phi) + Q_{i,1}(A, \mathbf{q}_{-\{i,1\}}, \Phi)(1 - \tilde{q}_1) \\ &= \tilde{P}_i(A_{-1}, \tilde{\mathbf{q}}_{-\{1,i\}}, \Phi) + Q_{i,1}(A, \tilde{\mathbf{q}}_{-\{i,1\}}, \Phi)(1 - \tilde{q}_1) = \tilde{P}_i(A, \tilde{\mathbf{q}}_{-i}, \Phi). \end{aligned} \tag{A.6}$$

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 $\tilde{P}_i(A, \tilde{\mathbf{q}}_{-i}, \Phi)$ with $\tilde{P}_i(A, \hat{\mathbf{q}}_{-i}, \Phi)$. First note that $\tilde{\mathbf{q}} \geq \hat{\mathbf{q}}$. Moreover, we have $|\{j \in V_{-i} \mid \tilde{q}_j > \hat{q}_j\}| = m$. By induction hypothesis, it implies that

$$\tilde{P}_i(A, \tilde{\mathbf{q}}_{-i}, \Phi) \leq \tilde{P}_i(A, \hat{\mathbf{q}}_{-i}, \Phi). \tag{A.7}$$

Combining Eqs. (A.6) and (A.7), we obtain $\tilde{P}_i(A, \mathbf{q}_{-i}, \Phi) \leq \tilde{P}_i(A, \hat{\mathbf{q}}_{-i}, \Phi)$.

(b) Network Effect Monotonicity in Network Density We show that given $\hat{V} \subset V$ and agent $i \in V - \hat{V}$, $\tilde{P}_i(A_{-\hat{V}}, \mathbf{q}_{-\hat{V} \cup \{i\}}, \Phi) \leq \tilde{P}_i(A, \mathbf{q}_{-i}, \Phi)$. Using Proposition 3.1, we have

$$\mathbf{P}_i(A_{-\hat{V}}, \mathbf{q}_{-\hat{V}}, \Phi) = (1 - q_i)\tilde{P}_i(A_{-\hat{V}}, \mathbf{q}_{-(\hat{V} \cup \{i\})}, \Phi).$$

By definition, $\tilde{P}_i(A_{-\hat{V}}, \mathbf{q}_{-(\hat{V} \cup \{i\})}, \Phi)$ is the probability of infection reaching agent i in $A_{-\hat{V}}$. Consider a transmission network $\bar{A}^t$ generated from $(A_{-\hat{V}}, \mathbf{q}_{-\hat{V}})$ in which infection can reach agent i. The probability of the transmission network $\bar{A}^t$ can be written as the marginal probability of the transmission networks A^t generated from $(A, \mathbf{q})$ that satisfies $A^t_{-\hat{V}} = \bar{A}^t$. Furthermore, in any transmission network A^t that satisfies $A^t_{-\hat{V}} = \bar{A}^t$, infection can reach agent i. Hence, the probability of infection reaching agent i in a transmission network generated from $(A, \mathbf{q})$ is at least $\tilde{P}_i(A_{-\hat{V}}, \mathbf{q}_{-(\hat{V} \cup \{i\})}, \Phi)$. In other words,

$$\tilde{P}_i(A_{-\hat{V}}, \mathbf{q}_{-\hat{V} \cup \{i\}}, \Phi) \leq \tilde{P}_i(A, \mathbf{q}_{-i}, \Phi).$$

(c) Best Response Monotonicity in Network Effect Given network A and security profiles $\mathbf{q}_{-i}$ and $\hat{\mathbf{q}}_{-i}$, if $\tilde{P}_i(A, \mathbf{q}_{-i}, \Phi) \geq \tilde{P}_i(A, \hat{\mathbf{q}}_{-i}, \Phi)$, then $B_i(\mathbf{q}_{-i}) \geq B_i(\hat{\mathbf{q}}_{-i})$. Using Eq. 3.2, it implies that

$$c_i'(B_i(\mathbf{q}_{-i})) = \tilde{P}_i(A, \mathbf{q}_{-i}, \Phi) \geq \tilde{P}_i(A, \hat{\mathbf{q}}_{-i}, \Phi) = c_i'(B_i(\hat{\mathbf{q}}_{-i})).$$

Combining the preceding inequality with Assumption 1, it follows that $B_i(\mathbf{q}_{-i}) \geq B_i(\hat{\mathbf{q}}_{-i})$ which shows the desired result.

∎

Proof of Eq. (3.4). Let $B_i(\mathbf{q}_{-i})$ and $S_i(\mathbf{q}_{-i})$ denote the best response strategy and welfare maximizing strategy of agent i. We show that $B_i(\mathbf{q}_{-i}) \leq S_i(\mathbf{q}_{-i})$. Using Eq. 3.2, we have

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

Moreover, it follows from Eq. 3.3 that

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

By definition, $Q_{j,i}(A, \mathbf{q}_{-\{i,j\}}, \Phi)(1 - q_j)$ is a probability. Therefore,

$$\tilde{P}_i(A, \mathbf{q}_{-i}, \Phi) + \sum_{j \neq i} Q_{j,i}(A, \mathbf{q}_{-\{i,j\}}, \Phi)(1 - q_j) \geq \tilde{P}_i(A, \mathbf{q}_{-i}, \Phi),$$

implying that $c_i'(S_i(\mathbf{q}_{-i})) \geq c_i'(B_i(\mathbf{q}_{-i}))$. The claim follows by the assumption that $c_i()$ is strictly convex (cf. Assumption 1), and therefore $c_i'()$ is a strictly increasing function.

∎

A.3 Proofs of Subsection 3.3: Symmetric Networks

Proof of Theorem 3.2.

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

$$\frac{\partial}{\partial q_i} u(A, \mathbf{q}, \Phi)|_{\mathbf{q}=\mathbf{q}_n} = \frac{\partial}{\partial q_j} u(A, \mathbf{q}, \Phi)|_{\mathbf{q}=\mathbf{q}_n} \; \forall \, i, j \in V. \tag{A.8}$$

Let

$$f(x) = \frac{\partial}{\partial q_j} u(A, \mathbf{q}, \Phi)|_{\mathbf{q}=\mathbf{x}_n}.$$

We next show that, $f(x)$ is a decreasing function in x.

The continuity and differentiability of $u(A, \mathbf{q}_n, \Phi)$ follows from Propositions 3.1, 3.2 and Assumption 1. By definition,

$$u(A, \mathbf{q}_n, \Phi) = 1 - (1 - q)\tilde{P}(A, \mathbf{q}_{n-1}, \Phi) - c(q).$$

Hence,

$$f(q) = \tilde{P}(A, \mathbf{q}_{n-1}, \Phi) - c'(q).$$

Using Proposition 3.3(a), we have $\tilde{P}(A, \mathbf{q}_{n-1}, \Phi)$ 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 $0 \leq \tilde{P}(A, \mathbf{q}_{n-1}, \Phi) \leq 1$, 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.8), $\mathbf{q}_n^e$ is the unique symmetric equilibrium.

Underinvestment in the symmetric equilibrium We next show that in the symmetric equilibrium, $q^e \leq q^s$. 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. (3.2), (3.3), and the fact that $\tilde{P}(A, \mathbf{q}_{n-1}, \Phi)$ is decreasing in q, the following relations hold.

$$\begin{aligned} c'(q^s) &= \tilde{P}(A, \mathbf{q}_{n-1}^s, \Phi) - (1 - q^s)\frac{\partial}{\partial q^s}\tilde{P}(A, \mathbf{q}_{n-1}^s, \Phi) \\ &\geq \tilde{P}(A, \mathbf{q}_{n-1}^s, \Phi) \\ &\geq \tilde{P}(A, \mathbf{q}_{n-1}^e, \Phi) \\ &= c'(q^e), \end{aligned}$$

where the second inequality follows from Proposition 3.3(a). Nevertheless, Assumption 1 implies that $c'(q^e) > c'(q^s)$ assuming $q^e > q^s$. This contradicts the preceding inequality, completing the proof.

∎

A.4 Proofs of Section 4: Sufficiently Convex Cost Functions

Proof of Lemma 4.1. Since $\mathbf{q}_{-i}$ and $\hat{\mathbf{q}}_{-i}$ satisfy $\tilde{P}_i(A, \mathbf{q}_{-i}, \Phi) \geq \tilde{P}_i(A, \hat{\mathbf{q}}_{-i}, \Phi)$, it follows from Proposition 3.3 (c) that $B_i(\mathbf{q}_{-i}) \geq B_i(\hat{\mathbf{q}}_{-i})$. Using Proposition 3.1 and the characterization of the best response strategy of an agent given in Eq. (3.2), we obtain

$$\mathbf{P}_i(A, (B_i(\mathbf{q}_{-i}), \mathbf{q}_{-i}), \Phi) = \tilde{P}_i(A, \mathbf{q}_{-i}, \Phi)(1 - B_i(\mathbf{q}_{-i})) = c_i'(B_i(\mathbf{q}_{-i}))(1 - B_i(\mathbf{q}_{-i})).$$

Similarly, we have

$$\mathbf{P}_i(A, (B_i(\hat{\mathbf{q}}_{-i}), \hat{\mathbf{q}}_{-i}), \Phi) = c_i'(B_i(\hat{\mathbf{q}}_{-i}))(1 - B_i(\hat{\mathbf{q}}_{-i})).$$

Since c_i is sufficiently convex (cf. Assumption 2) and $B_i(\mathbf{q}_{-i}) \geq B_i(\hat{\mathbf{q}}_{-i})$, we have

$$c_i'(B_i(\mathbf{q}_{-i}))(1 - B_i(\mathbf{q}_{-i})) \geq c_i'(B_i(\hat{\mathbf{q}}_{-i}))(1 - B_i(\hat{\mathbf{q}}_{-i})),$$

which using the preceding relations implies

$$\mathbf{P}_i(A, (B_i(\mathbf{q}_{-i}), \mathbf{q}_{-i}), \Phi) \geq \mathbf{P}_i(A, (B_i(\hat{\mathbf{q}}_{-i}), \hat{\mathbf{q}}_{-i}), \Phi).$$

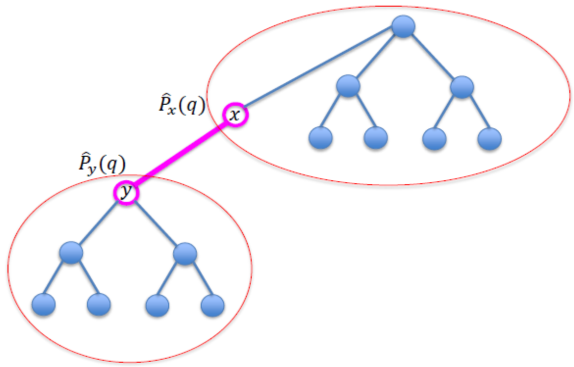

Figure 5: Tree uniqueness

∎

Proof of Theorem 4.1. Assume to arrive at a contradiction that we have two different equilibrium security profiles $\mathbf{q}^e$ and $\hat{\mathbf{q}}^e$. Using $\mathbf{q}^e$ and $\hat{\mathbf{q}}^e$, we can partition the nodes into three sets V_1, V_2 and V_3 as follows:

$$q_i^e > \hat{q}_i^e \text{ for all } i \in V_1,$$
$$q_i^e = \hat{q}_i^e \text{ for all } i \in V_2,$$
$$q_i^e < \hat{q}_i^e \text{ for all } i \in V_3.$$

We first show that the sets V_1 and V_3 are non-empty. Assume the contrary and suppose V_3 is empty. This implies that $\mathbf{q}^e \geq \hat{\mathbf{q}}^e$. Moreover, since $\mathbf{q}^e \neq \hat{\mathbf{q}}^e$, there exists an agent $i \in V_1$ with $q_i^e > \hat{q}_i^e$. Since $q_{-i}^e \geq \hat{q}_{-i}^e$, Proposition 3.3(a) implies that $\tilde{P}_i(A, \mathbf{q}_{-i}^e, \Phi) \leq \tilde{P}_i(A, \hat{\mathbf{q}}_{-i}^e, \Phi)$. Using Proposition 3.3(c), it follows that $q_i^e = B_i(\mathbf{q}_{-i}^e) \leq B_i(\hat{\mathbf{q}}_{-i}^e) = \hat{q}_i^e$, yielding a contradiction. A similar argument can be used to show that the set V_1 is nonempty.

For the rest of the proof, we use the notation $L(i)$ to denote the set V_j, $j = 1, 2, 3$, that node i belongs to, i.e., $L(i) = V_j$ if and only if $i \in V_j$. Furthermore, we define the *tree order with respect to a node* r as the partial order on the nodes of a tree with $u < v$ if and only if the unique path from r to v passes through u. For a tree order (with respect to an arbitrary node r), it follows immediately that there exists an edge $(x, y) \in E$ such that **(a)** $L(x) \neq L(y)$, $x < y$, and **(b)** For all $v' \in V$ such that $y < v'$, we have $L(y) = L(v')$. Let $Y = \{v \in V \mid v > y\}$.[13]

[13]Since both V_1 and V_3 are non-empty, there always exists an edge (x, y) with $L(x) \neq L(y)$ and $x < y$: among these edges, pick the one with the largest distance from r.

Assume without loss of generality that $x \in V_1$ and $y \in V_3$, i.e.,[14]

$$q_x^e > \hat{q}_x^e, \qquad q_y^e < \hat{q}_y^e, \qquad q_v^e < \hat{q}_v^e \quad \text{for all } v \in Y.$$

Hence, agent x invests more in security in $\mathbf{q}^e$ than in $\hat{\mathbf{q}}^e$, and agent y and agents in set Y invest in more security in $\hat{\mathbf{q}}^e$ than in $\mathbf{q}^e$. This is illustrated in Fig. 5. Using the sufficiently convex cost assumption (cf. Assumption 2) and Lemma 4.1, we have

$$\mathbf{P}_x(A, \mathbf{q}^e, \Phi) > \mathbf{P}_x(A, \hat{\mathbf{q}}^e, \Phi), \tag{A.9}$$

$$\mathbf{P}_y(A, \mathbf{q}^e, \Phi) < \mathbf{P}_y(A, \hat{\mathbf{q}}^e, \Phi). \tag{A.10}$$

In view of the tree network structure, we can decompose infection probability of agents x and y using the network effect on x when y is removed from the network and the network effect on y when x is removed from the network. More specifically, let $\hat{P}_x$ and $\hat{P}_y$ denote infection probabilities of agents x and y when agents y and x are removed from the network respectively, i.e.,

$$\hat{P}_x(\mathbf{q}) = \tilde{P}_x(A_{-y}, \mathbf{q}_{-\{x,y\}}, \Phi)(1 - q_x),$$
$$\hat{P}_y(\mathbf{q}) = \tilde{P}_y(A_{-x}, \mathbf{q}_{-\{x,y\}}, \Phi)(1 - q_y).$$

Using $\hat{P}_x$ and $\hat{P}_y$, we can write down infection probabilities of agents x and y as follows:

$$\mathbf{P}_x(A, \mathbf{q}^e, \Phi) = \hat{P}_x(\mathbf{q}^e) + (1 - q_x^e)\hat{P}_y(\mathbf{q}^e), \tag{A.11}$$

$$\mathbf{P}_y(A, \mathbf{q}^e, \Phi) = \hat{P}_y(\mathbf{q}^e) + (1 - q_y^e)\hat{P}_x(\mathbf{q}^e). \tag{A.12}$$

Substituting $\hat{P}_x(\hat{\mathbf{q}}^e)$ and $\hat{P}_y(\hat{\mathbf{q}}^e)$ for $\hat{P}_x(\mathbf{q}^e)$ and $\hat{P}_y(\mathbf{q}^e)$ in the above equations, we obtain similar relations for $\mathbf{P}_x(A, \hat{\mathbf{q}}^e, \Phi)$ and $\mathbf{P}_y(A, \hat{\mathbf{q}}^e, \Phi)$.

Since all agents in Y belong to set V_3, it follows from Proposition 3.3(a) that

$$\hat{P}_y(\mathbf{q}^e) \geq \hat{P}_y(\hat{\mathbf{q}}^e). \tag{A.13}$$

There are two cases to consider:

(*a*) $\hat{P}_x(\mathbf{q}^e) \geq \hat{P}_x(\hat{\mathbf{q}}^e)$: In this case, using Eqs. (A.12) and (A.13), we obtain $\mathbf{P}_y(A, \mathbf{q}^e, \Phi) \geq \mathbf{P}_y(A, \hat{\mathbf{q}}^e, \Phi)$, contradicting Eq. (A.10).

[14] The argument that follows will also hold if we assume one of these agents belong to V_2.

(*b*) $\hat{P}_x(\mathbf{q}^e) < \hat{P}_x(\hat{\mathbf{q}}^e)$: Using Eq. (A.13) and the fact that $q_x^e > \hat{q}_x^e$, we obtain

$$\begin{aligned}\hat{P}_y(\mathbf{q}^e) - \hat{P}_y(\hat{\mathbf{q}}^e) &\geq \Big(\hat{P}_y(\mathbf{q}^e) - \hat{P}_y(\hat{\mathbf{q}}^e)\Big)(1-\hat{q}_x^e) \\ &\geq \hat{P}_y(\mathbf{q}^e)(1-q_x^e) - \hat{P}_y(\hat{\mathbf{q}}^e)(1-\hat{\mathbf{q}}_x^e). \end{aligned} \tag{A.14}$$

Furthermore, since $\hat{P}_x(\mathbf{q}^e) < \hat{P}_x(\hat{\mathbf{q}}^e)$ and $q_y^e < \hat{q}_y^e$, we obtain

$$\begin{aligned}\hat{P}_x(\mathbf{q}^e)(1-q_y^e) - \hat{P}_x(\hat{\mathbf{q}}^e)(1-\hat{q}_y^e) &\geq \Big(\hat{P}_x(\mathbf{q}^e) - \hat{P}_x(\hat{\mathbf{q}}^e)\Big)(1-\hat{q}_y^e) \\ &\geq \hat{P}_x(\mathbf{q}^e) - \hat{P}_x(\hat{\mathbf{q}}^e). \end{aligned} \tag{A.15}$$

Combining Eqs. (A.14) and (A.15), we have

$$\begin{aligned}&(\hat{P}_y(\mathbf{q}^e) + \hat{P}_x(\mathbf{q}^e)(1-q_y^e)) - (\hat{P}_y(\hat{\mathbf{q}}^e) + \hat{P}_x(\hat{\mathbf{q}}^e)(1-\hat{q}_y^e)) \\ &\qquad \geq (\hat{P}_x(\mathbf{q}^e) + \hat{P}_y(\mathbf{q}^e)(1-q_x^e)) - (\hat{P}_x(\hat{\mathbf{q}}^e) + \hat{P}_y(\hat{\mathbf{q}}^e)(1-\hat{q}_x^e)).\end{aligned}$$

Using the expressions in Eqs. (A.11) and (A.12), this implies

$$\mathbf{P}_y(A, \mathbf{q}^e, \Phi) - \mathbf{P}_y(A, \hat{\mathbf{q}}^e, \Phi) \geq \mathbf{P}_x(A, \mathbf{q}^e, \Phi) - \mathbf{P}_x(A, \hat{\mathbf{q}}^e, \Phi) \geq 0,$$

where the last inequality follows from Eq. (A.9) and yields a contradiction.

∎

Proof of Lemma 4.2. We first show the following stronger statement: Given tree network A and set $\bar{V} \subset V$, for any $i, j \in V - \bar{V}$, we have

$$Q_{j,i}(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}\cup\{j,i\}}, \Phi) \leq Q_{j,i}(A, \mathbf{q}_{-\{j,i\}}, \Phi). \tag{A.16}$$

Given tree network A, one of the following mutually exclusive events happens:

(A) The unique path between s (seed node) and j in the tree network includes i.

(B) The unique path between s and j in the tree network does not include i.

If event (B) happens, the probability that infection reaches j stays unchanged after i is removed from the tree in both A and $A_{-\bar{V}}$ which implies

$$Q_{j,i}(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}\cup\{j,i\}}, \Phi|(B)) = Q_{j,i}(A, \mathbf{q}_{-\{j,i\}}, \Phi|(B)) = 0. \tag{A.17}$$

Suppose next that event (A) happens.
We denote the unique path between s and j by $s, v_1, v_2, \ldots, v_k = i, \ldots, v_m = j$. Node j gets infected in A if and only if for all $1 \leq i \leq m$, v_i is susceptible. However, in $A_{-\bar{V}}$, j gets infected if and only

if for all $1 \leq i \leq m$, v_i is susceptible and $v_i \notin \bar{V}$. Hence,

$$\mathbf{P}_j(A, \mathbf{q}, \Phi|(A)) \geq \mathbf{P}_j(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}}, \Phi|(A)).$$

Furthermore, we have

$$\mathbf{P}_j(A, \mathbf{q}, \Phi|(A)) = (1-q_j)(1-q_i)Q_{j,i}(A, \mathbf{q}_{-\{j,i\}}, \Phi|(A)),$$

$$\mathbf{P}_j(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}}, \Phi|(A)) = (1-q_j)(1-q_i)Q_{j,i}(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}\cup\{j,i\}}, \Phi|(A)).$$

Combining the preceding relations with Eq. (A.17), we obtain

$$\begin{aligned}
Q_{j,i}(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}\cup\{j,i\}}, \Phi) &= Q_{j,i}(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}\cup\{j,i\}}, \Phi|(A))P((A)) \\
&= \frac{1}{(1-q_i)(1-q_j)}\mathbf{P}_j(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}}, \Phi|(A))P((A)) \\
&\leq \frac{1}{(1-q_i)(1-q_j)}\mathbf{P}_j(A, \mathbf{q}, \Phi|(A))P((A)) \\
&= Q_{j,i}(A, \mathbf{q}_{-\{j,i\}}, \Phi|(A))P((A)) \\
&= Q_{j,i}(A, \mathbf{q}_{-\{j,i\}}, \Phi),
\end{aligned}$$

completing the proof of Eq. (A.16). Combining this result with Eq. (4.2) and Proposition 3.3(b), we obtain

$$\begin{aligned}
C_I(i, A) &= (1-q_i)(\tilde{P}_i(A, \mathbf{q}_{-i}, \Phi) + \sum_{j\in V_{-i}}(1-q_j)Q_{ji}(A, \mathbf{q}_{-\{i,j\}}, \Phi)) \\
&\geq (1-q_i)(\tilde{P}_i(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}\cup\{i\}}, \Phi) + \sum_{j\in V_{-i}}(1-q_j)Q_{ji}(A, \mathbf{q}_{-\{i,j\}}, \Phi)) \\
&\geq (1-q_i)(\tilde{P}_i(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}\cup\{i\}}, \Phi) + \sum_{j\in V_{-\bar{V}\cup\{i\}}}(1-q_j)Q_{ji}(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}\cup\{i,j\}}, \Phi)) \\
&= C_I(i, A_{-\bar{V}}),
\end{aligned}$$

which shows the desired result. ∎

Proof of Theorem 4.2. If $\mathbf{q}^s > \mathbf{q}^e$ then by using Propositions 3.1 and 3.3(a), we have $\mathbf{P}_i(A, \mathbf{q}^s, \Phi) < \mathbf{P}_i(A, \mathbf{q}^e, \Phi)$ for all $i \in V$ implying that $I(A, \mathbf{q}^s, \Phi) \leq I(A, \mathbf{q}^e, \Phi)$. Otherwise, let $V_1 = \{i \in V \mid q_i^s \leq q_i^e\}$, i.e., V_1 is the set of agents that overinvest compared to the social optimum. We first provide a recursive characterization of expected infections in a given network A, using the decomposition result presented in Proposition 3.2.

Lemma A.1. *Given network A and security profile $\mathbf{q}$, the expected total number of infected people satisfies* *the following: for all $\bar{V} \subset V$ and $i \in V - \bar{V}$,*

$$I(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}}, \Phi) = C_I(i, A_{-\bar{V}}) + I(A_{-\bar{V}\cup\{i\}}, \mathbf{q}_{-\bar{V}\cup\{i\}}, \Phi),$$

where $C_I(i, A_{-\bar{V}})$ is the contribution of agent i to infection in network $A_{-\bar{V}}$.

Proof of Lemma A.1. The expected infections in a network $A_{-\bar{V}}$ for a security profile $\mathbf{q}_{-\bar{V}}$, can be stated as

$$I(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}}, \Phi) = \sum_{j \in V-\bar{V}} \mathbf{P}_j(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}}, \Phi).$$

Using Proposition 3.2, we have

$$\begin{aligned}
I(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}}, \Phi) &= \sum_{j \in V-\bar{V}} \mathbf{P}_j(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}}, \Phi) \\
&= \mathbf{P}_i(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}}, \Phi) + \sum_{j \in V-\bar{V}\cup\{i\}} \mathbf{P}_j(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}}, \Phi) \\
&= \mathbf{P}_i(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}}, \Phi) + \sum_{j \in V-\bar{V}\cup\{i\}} (1-q_j)(\tilde{P}_j(A_{-\bar{V}\cup\{i\}}, \mathbf{q}_{-\bar{V}\cup\{i\}}, \Phi) \\
&\qquad + (1-q_i)Q_{ji}(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}\cup\{i,j\}}, \Phi)) \\
&= \mathbf{P}_i(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}}, \Phi) + \sum_{j \in V-\bar{V}\cup\{i\}} \mathbf{P}_j(A_{-\bar{V}\cup\{i\}}, \mathbf{q}_{-\bar{V}\cup\{i\}}, \Phi) \\
&\qquad + \sum_{j \in V-\bar{V}\cup\{i\}} (1-q_i)(1-q_j)Q_{ji}(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}\cup\{i,j\}}, \Phi) \\
&= C_I(i, A_{-\bar{V}}) + I(A_{-\bar{V}\cup\{i\}}, \mathbf{q}_{-\bar{V}\cup\{i\}}, \Phi),
\end{aligned}$$

showing the desired result.

∎

We next present the proof of Theorem 4.2 using Lemma A.1. We first show that given tree network A, for all $\hat{V} \subset V$,

$$I(A, \mathbf{q}, \Phi) \leq I(A_{-\hat{V}}, \mathbf{q}_{-\hat{V}}, \Phi) + \sum_{v \in \hat{V}} C_I(v, A). \tag{A.18}$$

The proof is by induction on $|\hat{V}|$. If $|\hat{V}| = 1$, then by applying Lemma A.1 and setting $\bar{V} = \emptyset$, we obtain Eq. (A.18).

Suppose next that Eq. (A.18) holds for all $\hat{V}$ with $|\hat{V}| = m$ for an integer $m > 1$. We will show that it also holds for $\hat{V}$ with $|\hat{V}| = m + 1$. Consider an agent $i \in \hat{V}$ and let $\hat{V}_{-i} = \hat{V} - \{i\}$. Since

$|\hat{V}_{-i}| = m$, using induction hypothesis we have

$$I(A, \mathbf{q}, \Phi) \leq I(A_{-\hat{V}_{-i}}, \mathbf{q}^s_{-\hat{V}_{-i}}, \Phi) + \sum_{v \in \hat{V}_{-i}} C_I(v, A). \tag{A.19}$$

Moreover, using Lemma A.1 and setting $\bar{V} = \hat{V}_{-i}$, we obtain

$$I(A_{-\hat{V}_{-i}}, \mathbf{q}_{\hat{V}_{-i}}, \Phi) = C_I(i, A_{-\hat{V}_{-i}}) + I(A_{-\hat{V}}, \mathbf{q}_{-\hat{V}}, \Phi). \tag{A.20}$$

Using Lemma 4.2, we have

$$C_I(i, A_{-\hat{V}_{-i}}) \leq C_I(i, A). \tag{A.21}$$

Putting Eqs. (A.19), (A.20), and (A.21) together shows that Eq. (A.18) holds for the $\hat{V}$ with $|\hat{V}| = m + 1$ completing the proof of Eq. (A.18).

Using Eq. (A.18) with $\hat{V} = V_1$ and setting $\mathbf{q} = \mathbf{q}^s$, we obtain

$$I(A, \mathbf{q}^s, \Phi) \leq I(A_{-V_1}, \mathbf{q}^s_{-V_1}, \Phi) + \sum_{i \in V_1} C_I(i, A).$$

Since $\mathbf{q}^s$ is the socially optimal security profile, by Eq. (3.3) we have

$$\sum_{i \in V_1} C_I(i, A) = \sum_{i \in V_1} c_i'(q_i^s)(1 - q_i^s).$$

Combining the preceding relations, we obtain

$$I(A, \mathbf{q}^s, \Phi) \leq I(A_{-V_1}, \mathbf{q}^s_{-V_1}, \Phi) + \sum_{i \in V_1} c_i'(q_i^s)(1 - q_i^s). \tag{A.22}$$

Moreover, for the equilibrium security profile $\mathbf{q}^e$, using Eq. (3.2) and Proposition 3.3(b), we obtain

$$\begin{aligned} I(A, \mathbf{q}^e, \Phi) &= \sum_{v \in V_1} \mathbf{P}_v(A, \mathbf{q}^e, \Phi) + \sum_{v \in V - V_1} \mathbf{P}_v(A, \mathbf{q}^e, \Phi) \\ &= \sum_{v \in V_1} c_v'(q_v^e)(1 - q_v^e) + \sum_{v \in V - V_1} \mathbf{P}_v(A, \mathbf{q}^e, \Phi) \\ &\geq \sum_{v \in V_1} c_v'(q_v^e)(1 - q_v^e) + I(A_{-V_1}, \mathbf{q}^e_{-V_1}, \Phi). \end{aligned} \tag{A.23}$$

Using the sufficiently convex cost assumption and the fact that $q_i^e > q_i^s$ for all $i \in V_1$, it follows that

$$\sum_{i\in V_1} c_i'(q_i^s)(1-q_i^s) < \sum_{i\in V_1} c_i'(q_i^e)(1-q_i^e). \tag{A.24}$$

Moreover, since $q_i^e \leq q_i^s$ for all $i \in V - V_1$, Proposition 3.3(b) implies

$$I(A_{-V_1}, \mathbf{q}^s_{-V_1}, \Phi) \leq I(A_{-V_1}, \mathbf{q}^e_{-V_1}, \Phi). \tag{A.25}$$

Combining Eqs. (A.22), (A.23), (A.24), and (A.25) we obtain

$$\begin{aligned} I(A, \mathbf{q}^s, \Phi) &\leq I(A_{-V_1}, \mathbf{q}^s_{-V_1}, \Phi) + \sum_{i\in V_1} c_i'(q_i^s)(1-q_i^s) \\ &\leq I(A_{-V_1}, \mathbf{q}^e_{-V_1}, \Phi) + \sum_{i\in V_1} c_i'(q_i^e)(1-q_i^e) \\ &\leq I(A, \mathbf{q}^e, \Phi), \end{aligned}$$

completing the proof of Theorem 4.2. ∎

A.5 Proofs of Section 5

Before providing the proof of Theorem 5.1, we first extend the decomposition property (i.e., Proposition 3.2) and Lemma A.1 for acyclic components of a network. We then use the same line of argument as Theorem 4.2, to prove Theorem 5.1.

We use the following notation in the rest of this section. Given random network A, for each agent v, let (D_v^A) be the event that the attached connected component to v in $A^r \sim A$ is acyclic and (O_v^A) be the event that the attached connected component to v in A^r has a cycle. Let $P((D_v^A))$ and $P((O_v^A))$ be the probability of these events.

Using Proposition 3.2, one can easily show that

Lemma A.2. *Given network A and two nodes i and j in A, we have,*

$$\tilde{P}_j(A, \mathbf{q}_{-j}, \Phi|(D_j^A)) = \tilde{P}_j(A_{-i}, \mathbf{q}_{-\{i,j\}}, \Phi|(D_j^A)) + (1-q_i)Q_{j,i}(A, \mathbf{q}_{-\{i,j\}}, \Phi|(D_j^A)), \tag{A.26}$$

where $Q_{j,i}(A, \mathbf{q}_{-\{i,j\}}, \Phi|(D_j^A))$ is the probability that infection reaches agent j only through a path that contains agent i conditional on i being susceptible and event (D_j^A) happens.

We next extend Lemma A.1.

Lemma A.3. *Given network A and security profile $\mathbf{q}$, we have: For all $\bar{V} \subset V$ and $i \in V - \bar{V}$,*

$$\sum_{v \in V - \bar{V}} \mathbf{P}_v(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}}, \Phi|(D_v^A))P((D_v^A)) \\ = C_I(i, A_{-\bar{V}}|(D_i^A))P((D_i^A)) + \sum_{v \in V - \bar{V} \cup \{i\}} \mathbf{P}_v(A_{-\bar{V} \cup \{i\}}, \mathbf{q}_{-\bar{V} \cup \{i\}}, \Phi|(D_v^A))P((D_v^A)), \tag{A.27}$$

where,

$$C_I(i, A_{-\bar{V}}|(D_i^A)) \\ = (1 - q_i)(\tilde{P}_i(A_{-\bar{V}}, \mathbf{q}_{-\bar{V} \cup \{i\}}, \Phi|(D_i^A)) + \sum_{j \in V - \bar{V} \cup \{i\}} (1 - q_j)Q_{ji}(A_{-\bar{V}}, \mathbf{q}_{-\bar{V} \cup \{i,j\}}, \Phi|(D_i^A))).$$

Proof. Given network $A_{-\bar{V}}$ and security profile $\mathbf{q}_{-\bar{V}}$, by using Lemma A.2, we have

$$\begin{aligned} &\sum_{v \in V - \bar{V}} \mathbf{P}_v(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}}, \Phi|(D_v^A))P((D_v^A)) \\ &= \sum_{j \in V - (\bar{V} \cup \{i\})} \mathbf{P}_j(A_{-(\bar{V} \cup \{i\})}, \mathbf{q}_{-(\bar{V} \cup \{i\})}, \Phi|(D_j^A))P((D_j^A)) + \mathbf{P}_i(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}}, \Phi|(D_i^A))P((D_i^A)) \\ &\quad + (1 - q_i) \sum_{j \in V - (\bar{V} \cup \{i\})} (1 - q_j)Q_{j,i}(A_{-\bar{V}}, \mathbf{q}_{-(\bar{V} \cup \{i,j\})}, \Phi|(D_j^A))P((D_j^A)) \\ &= (1 - q_i)\tilde{P}_i(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}}, \Phi|(D_i^A))P((D_i^A)) \\ &\quad + (1 - q_i) \sum_{j \in V - (\bar{V} \cup \{i\})} (1 - q_j)Q_{j,i}(A_{-\bar{V}}, \mathbf{q}_{-(\bar{V} \cup \{i,j\})}, \Phi|(D_j^A))P((D_j^A)) \\ &\quad + \sum_{j \in V - (\bar{V} \cup \{i\})} \mathbf{P}_j(A_{-(\bar{V} \cup \{i\})}, \mathbf{q}_{-(\bar{V} \cup \{i\})}, \Phi|(D_j^A))P((D_j^A)). \end{aligned} \tag{A.28}$$

Using Lemma A.3, we obtain

$$C_I(i, A_{-\bar{V}}|(D_i^A)) \\ =(1 - q_i)(\tilde{P}_i(A_{-\bar{V}}, \mathbf{q}_{-(\bar{V} \cup \{i\})}, \Phi|(D_i^A)) + \sum_{j \in V - (\bar{V} \cup \{i\})} (1 - q_j)Q_{ji}(A_{-\bar{V}}, \mathbf{q}_{-(\bar{V} \cup \{i,j\})}, \Phi|(D_i^A))).$$

We next show that

$$\sum_{j \in V - (\bar{V} \cup \{i\})} (1 - q_j)Q_{ji}(A_{-\bar{V}}, \mathbf{q}_{-(\bar{V} \cup \{i,j\})}, \Phi|(D_i^A))P((D_i^A)) \\ = \sum_{j \in V - (\bar{V} \cup \{i\})} (1 - q_j)Q_{ji}(A_{-\bar{V}}, \mathbf{q}_{-(\bar{V} \cup \{i,j\})}, \Phi|(D_j^A))P((D_j^A)). \tag{A.29}$$

In the interaction network $A^r \sim A$, either $i \overset{A^r}{\not\longrightarrow} j$, in which case infection can not reach i through

j, or $i \xrightarrow{A^r} j$, which implies that i and j belong to the same connected component. In this case, the event (D_i^A) happens if and only if the event (D_j^A) happens. Hence,

$$Q_{ji}(A_{-\bar{V}}, \mathbf{q}_{-(\bar{V}\cup\{i,j\})}, \Phi|(D_j^A))P((D_j^A)) = Q_{ji}(A_{-\bar{V}}, \mathbf{q}_{-(\bar{V}\cup\{i,j\})}, \Phi|(D_i^A))P((D_i^A)). \tag{A.30}$$

Combining Eqs. (A.28), (A.29), and (A.30) we obtain Eq. (A.27), completing the proof. ∎

Finally, we extend Lemma 4.2 for acyclic components.

Lemma A.4. *Given network A and security profile $\mathbf{q}$, $C_I(i, A|(D_i^A)) \geq C_I(i, A_{-\bar{V}}|(D_i^A))$.*

Proof of Lemma A.4. We show a stronger statement. We show that for any $i, j \in V - \bar{V}$,

$$Q_{j,i}(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}\cup\{j,i\}}, \Phi|(D_i^A)) \leq Q_{j,i}(A, \mathbf{q}_{-\{j,i\}}, \Phi|(D_i^A)).$$

Let the random variable s denote the seed node. Conditional on the event (D_i^A), one of the following mutually exclusive event happens:

(A) The only path between s and j includes i.

(B) The path(s) between s and j do not include i.

Let $P((A))$ and $P((B))$ be the probability of each event conditional on the event (D_i^A). Note that $P((A)) + P((B)) = 1$. Therefore,

$$Q_{j,i}(A, \mathbf{q}_{-\{j,i\}}, \Phi|(D_i^A)) = Q_{j,i}(A, \mathbf{q}_{-\{j,i\}}, \Phi|(A))P((A)) + Q_{j,i}(A, \mathbf{q}_{-\{j,i\}}, \Phi|(B))P((B)). \tag{A.31}$$

If event (B) happens, the probability that infection reaches j through i in both A and $A_{-\bar{V}}$ is 0. In other words,

$$Q_{j,i}(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}\cup\{j,i\}}, \Phi|(B)) = Q_{j,i}(A, \mathbf{q}_{-\{j,i\}}, \Phi|(B)) = 0 \tag{A.32}$$

We next analyze $C_I()$ when event (A) happens. Under this event, we have

$$\mathbf{P}_j(A, \mathbf{q}, \Phi|(A)) = (1 - q_j)(1 - q_i)Q_{j,i}(A, \mathbf{q}_{-\{j,i\}}, \Phi|(A))$$

Similarly,

$$\mathbf{P}_j(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}}, \Phi|(A)) = (1 - q_j)(1 - q_i)Q_{j,i}(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}\cup\{j,i\}}, \Phi|(A)).$$

Conditional on (A), the path between s and j is unique and includes i. We denote this path by $s, v_1, v_2, \ldots, v_k = i, \ldots, v_m = j$ without loss of generality. Under this event, j gets infected in A if and only if for all $1 \leq i \leq m$, v_i is susceptible. However, in $A_{-\bar{V}}$, j gets infected if and only if for all $1 \leq i \leq m$, v_i is susceptible and $v_i \notin \bar{V}$. Hence,

$$\mathbf{P}_j(A, \mathbf{q}, \Phi|(A)) \geq \mathbf{P}_j(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}}, \Phi|(A)). \tag{A.33}$$

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

$$\begin{aligned} Q_{j,i}(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}\cup\{j,i\}}, \Phi|(D_i^A)) &= \frac{1}{(1-q_i)(1-q_j)} \mathbf{P}_j(A_{-\bar{V}}, \mathbf{q}_{-\bar{V}}, \Phi|(A))P((A)) \\ &\leq \frac{1}{(1-q_i)(1-q_j)} \mathbf{P}_j(A, \mathbf{q}, \Phi|(A))P((A)) \\ &= Q_{j,i}(A, \mathbf{q}_{-\{j,i\}}, \Phi|(D_i^A)), \end{aligned}$$

completing the proof. ∎

Using Lemmas A.2, A.3, and A.4, we next present the proof of the main result of this section.

Proof of Theorem 5.1. The proof of this theorem uses the same line of argument as Theorem 4.2. In this proof, we analyze expected infections in acyclic components and cyclic components separately. Let $\mathbf{q}^e$ be the equilibrium security profile and $\mathbf{q}^s$ be the socially optimal security profile. If $\mathbf{q}^s > \mathbf{q}^e$, then $I(A, \mathbf{q}^s, \Phi) \leq I(A, \mathbf{q}^e, \Phi)$.

Otherwise, similar to the previous section, partition the nodes into three sets V_1, V_2 and V_3 such that:

$$\begin{cases} q_i^s \leq q_i^e & \text{for all } i \in V_1, \\ q_i^e = q_i^s & \text{for all } i \in V_2, \\ q_i^s \geq q_i^e & \text{for all } i \in V_3. \end{cases}$$

The proof follows a number of steps:

- We first show that in the equilibrium, expected infections satisfies [15]

$$I(A, \mathbf{q}^e, \Phi) \geq \sum_{i \in V_1} c'(q_i^e)(1-q_i^e) + \sum_{i \in V - V_1} \mathbf{P}_i(A_{-V_1}, \mathbf{q}^e_{-V_1}, \Phi).$$

- We then show that in the social optimum, the expected infections is at most

$$I(A, \mathbf{q}^s, \Phi) \leq \sum_{i \in V_1} c'(q_i^s)(1-q_i^s) + \sum_{i \in V - V_1} \mathbf{P}_i(A_{-V_1}, \mathbf{q}^s_{-V_1}, \Phi) + \epsilon n. \tag{A.34}$$

- Putting these two steps together, we then conclude that $I(A, \mathbf{q}^s, \Phi) \leq I(A, \mathbf{q}^e, \Phi) + \epsilon n$.

We first analyze expected infections in the equilibrium. Using a similar argument as Theo-

[15]The attack decision in $\mathbf{P}_i(A_{-V_1}, \mathbf{q}^e_{-V_1}, \Phi)$ is Φ_{-V_1} where Φ is the attack decision of A.

rem 4.2, we have

$$\begin{aligned}I(A,\mathbf{q}^e,\Phi) &= \sum_{i\in V}\mathbf{P}_i(A,\mathbf{q}^e,\Phi)\\ &\geq \sum_{v\in V_1} c'(q_i^e)(1-q_i^e) + \sum_{i\in V-V_1}\mathbf{P}_i(A_{-V_1},\mathbf{q}^e_{-V_1},\Phi).\end{aligned} \tag{A.35}$$

We next present an upper bound for expected infections in the social optimum. By law of total probability, we obtain

$$I(A,\mathbf{q}^s,\Phi) = \sum_{i\in V}\mathbf{P}_i(A,\mathbf{q}^s,\Phi|(D_i^A))P((D_i^A)) + \mathbf{P}_i(A,\mathbf{q}^s,\Phi|(O_i^A))P((O_i^A)). \tag{A.36}$$

We prove Eq. (A.34) in two steps:

1. We first show that in a $(1-\epsilon)$-local tree network A, we have

$$\sum_{v\in V}\mathbf{P}_v(A,\mathbf{q},\Phi|(O_v^A))P((O_v^A)) \leq \epsilon n.$$

2. We then show that, given random network A, if $\mathbf{q}^s$ is the socially optimal security profile, then the following inequality holds:

$$\sum_{v\in V}\mathbf{P}_v(A,\mathbf{q}^s,\Phi|(D_v^A))P((D_v^A)) \leq \sum_{i\in V_1} c'(q_i^s)(1-q_i^s) + \sum_{i\in V-V_1}\mathbf{P}_i(A_{-V_1},\mathbf{q}^s_{-V_1},\Phi|(D_v^A))P((D_v^A)).$$

We start by proving the first step and providing an upperbound for expected infections in cyclic components. For each agent v, by definition of local tree, the probability that v belongs to a cyclic component is at most ϵ. Therefore, the probability that v belongs to a cyclic component and gets infected is also at most ϵ. Summing over all agents v, we have

$$\sum_{v\in V}\mathbf{P}_v(A,\mathbf{q},\Phi|(O_v^A))P((O_v^A)) \leq nP((O_v^A)) = n\epsilon. \tag{A.37}$$

We next analyze expected infections in acyclic components in the social optimum. We show that for any security profile $\mathbf{q}$ and for any $\hat{V}\subset V$,

$$\begin{aligned}&\sum_{v\in V}\mathbf{P}_v(A,\mathbf{q},\Phi|(D_v^A))P((D_v^A))\\ &\qquad\leq \sum_{v\in V-\hat{V}}\mathbf{P}_v(A_{-\hat{V}},\mathbf{q}_{-\hat{V}},\Phi|(D_v^A))P((D_v^A)) + \sum_{v\in\hat{V}} C_I(v,A|(D_v^A))P((D_v^A)).\end{aligned} \tag{A.38}$$

The proof of Eq. (A.38) follows the same line of the argument used for Eq. (A.18) in Lemma A.1. The proof is by induction on $|\hat{V}|$. If $|\hat{V}|=1$, then by setting $\bar{V}=\emptyset$ and applying Lemma A.3, we obtain Eq. (A.38). We next assume that for any $\hat{V}$, if $|\hat{V}|\leq m$, then Eq. (A.38) holds (Induction hypothesis). We then prove that if $|\hat{V}| = m+1$, the statement holds still. Consider an agent $i \in \hat{V}$ and define $\hat{V}_{-i} = \hat{V} - \{i\}$. With a similar argument presented for Eq. (A.18) in Lemma A.1, we obtain

$$\begin{aligned}
&\sum_{v\in V}\mathbf{P}_v(A,\mathbf{q},\Phi|(D_v^A))P((D_v^A)) \\
&\quad\le \sum_{v\in V}\mathbf{P}_v(A_{-\hat{V}_{-i}},\mathbf{q}_{-\hat{V}_{-i}},\Phi|(D_v^A))P((D_v^A)) + \sum_{v'\in\hat{V}_{-i}} C_I(v',A|(D_{v'}^A))P((D_{v'}^A)) \\
&\quad= \sum_{v\in V}\mathbf{P}_v(A_{-\hat{V}},\mathbf{q}_{-\hat{V}},\Phi|(D_v^A))P((D_v^A)) + C_I(i,A_{-\hat{V}}|(D_i^A))P((D_i^A)) \\
&\qquad\qquad + \sum_{v'\in\hat{V}_{-i}} C_I(v',A|(D_{v'}^A))P((D_{v'}^A)) \\
&\quad\le \sum_{v\in V}\mathbf{P}_v(A_{-\hat{V}},\mathbf{q}_{-\hat{V}},\Phi|(D_v^A))P((D_v^A)) + \sum_{v\in\hat{V}} C_I(v,A|(D_v^A))P((D_v^A)).
\end{aligned}$$

The first inequality follows from the induction hypothesis. The first equation is implied by Lemma A.2 and the second inequality follows from Lemma A.4. Furthermore, using Lemmas 4.1, A.4, Eq. (3.3), and assuming that $c(q)$ is sufficiently convex, for the socially optimal security profile we have

$$C_I(v,A|(D_v^A))P((D_v^A)) \le C_I(v,A) = c'(q_v^s)(1-q_v^s). \tag{A.39}$$

Combining Eqs. (A.35), (A.38), and (A.39), we obtain

$$\begin{aligned}
&\sum_{v\in V}\mathbf{P}_v(A,\mathbf{q}^s,\Phi|(D_v^A))P((D_v^A)) && \text{(A.40)}\\
&\qquad\le \sum_{v\in V-V_1}\mathbf{P}_v(A_{-V_1},\mathbf{q}^s_{-V_1},\Phi|(D_v^A))P((D_v^A)) + \sum_{v\in V_1} C_I(v,A|(D_v^A))P((D_v^A)) \\
&\qquad\le \sum_{v\in V-V_1}\mathbf{P}_v(A_{-V_1},\mathbf{q}^s_{-V_1},\Phi|(D_v^A))P((D_v^A)) + \sum_{v\in V_1} c'(q_v^s)(1-q_v^s) \\
&\qquad\le \sum_{v\in V-V_1}\mathbf{P}_v(A_{-V_1},\mathbf{q}^e_{-V_1},\Phi) + \sum_{v\in V_1} c'(q_v^e)(1-q_v^e) \\
&\qquad\le I(A,\mathbf{q}^e,\Phi). && \text{(A.41)}
\end{aligned}$$

The third inequality holds because

1. For all $v \in V_1$, $q_v^s < q_v^e$. Hence, by Lemma 4.1 we have

$$c'(q_v^s)(1-q_v^s) < c'(q_v^e)(1-q_v^e).$$

2. For all $v \in V - V_1$, $q_v^s \ge q_v^e$. Hence, by Proposition 3.3(a), for all $v \in V - V_1$,

$$\mathbf{P}_v(A_{-V_1},\mathbf{q}^s_{-V_1},\Phi|(D_v^A))P((D_v^A)) \le \mathbf{P}_v(A_{-V_1},\mathbf{q}^s_{-V_1},\Phi) \le \mathbf{P}_v(A_{-V_1},\mathbf{q}^e_{-V_1},\Phi).$$

By combining the preceding steps we obtain the third inequality. The last inequality was proven in Eq. (A.35).

Finally combining Eqs. (A.36), (A.37), and (A.40), we obtain

$$I(A, \mathbf{q}^s, \Phi) \leq I(A, \mathbf{q}^e, \Phi) + \epsilon n,$$

completing the proof. ∎

A.6 Proofs of Subsection 5.2

In the rest of this section, we denote the component attached to v in the activated network A^a by A^a_v, i.e., $A^a_v = A^a[\bar{V}]$ such that $\bar{V} = \{j \in V | j \xrightarrow{A^a} v\}$. By Definition 2, the random network generated from (A, p) has h-local tree structure if the attached component to each agent is acyclic with probability at least h. Let $(D_v^{(A,p)})$ be the event that the component attached to v in the activated network from (A, p) is acyclic. Hence, a lower bound on $P((D_v^{(A,p)}))$ is also a lower bound on the h parameter of the local tree structure. Given interaction network $A^r \sim A$ and an agent $v \in V$, we obtain a lower bound on $P((D_v^{(A,p)}))$ via the following steps:

1. We first introduce an algorithm that specifies the activation order of the edges in multiple stages to obtain the activated network A^a_v.

2. We then present a recursive computation of the lower bound of having an acyclic component attached to v after the kth stage of the algorithm.

3. We finally bound the maximum number of stages of the algorithm and consequently $P((D_v^{(A,p)}))$ for a class of random networks (A, p).

In order to generate A^a_v, one can first focus on A^r, and starting from a particular node v, activate edges independently with probability p. For the sake of analysis, we use the following order on activating the edges.

Algorithm A.1 (Activation(A^r, p, v)).

- *Initialize* $C_1^v = \{v\}$. *Initialize* $k = 1$.
- *Initialize* $\bar{C}^v = \emptyset$. $E_1^a = \emptyset$.
- *While* $V - C_k^v - \bar{C}^v \neq \emptyset$ *do*
  - *For an agent* $v_k'^v - \bar{C}^v$, *activate the edges between* v' *and* C_k^v *in* A^r. *Denote the set of active edges by* $E_{v'}$.

* *If at least one of these edges between v' and C_k^v are active, then,* $C_{k+1}^v = C_k^v \cup \{v'\}$*,* $k = k+1$*,* $\bar{C}^v = \emptyset$*,* $E_k^a = E_{k-1}^a \cup E_{v'}$*.*
* *Otherwise,* $\bar{C}^v = \bar{C}^v \cup \{v'\}$*.*

This algorithm (starting from v) considers one node at a time and activates all edges between that node and all "activated nodes" (i.e., endpoints of all activated edges). The set C_k^v contains activated nodes and the set E_k^a contains the set of activated edges at the end of stage k.[16] The set $\bar{C}^v$ is used at each stage k, to discover nodes which are one hop away from the set C_k^v.

Let $A_v^{r,k} = (C_k^v, E_k^a)$ and let $(D_v^{(A^r,k)})$ denote the event that $A_v^{r,k}$ is acyclic. Also, let $\hat{k}$ be the number of stages of Algorithm Activation(A^r, p, v).

Lemma A.5. *Given interaction network A^r and activation probability p, the following holds. For all $2 \leq k \leq \hat{k}$,*

$$P((D_v^{(A^r,k)})) = (1-p)^{|E[A_v^{r,k}]|-k+1} \geq (1-p)^{\frac{(k-1)(k-2)}{2}}. \tag{A.42}$$

Proof. We first show the equality. The proof is by induction. In stages 1 and 2, $P((D_v^{(A^r,1)})) = 1$ and hence the induction basis holds. We then assume that for all $k < m \leq \hat{k}$, Eq. (A.42) holds. We next show that this equation holds for $k = m$. Let v' be the agent that is added to C^v at stage m. The attached component to v is acyclic at the end of stage m if the following holds:

- The component attached to v is acyclic at the end of stage $m-1$, i.e., event $(D_v^{(A^r,m-1)})$ happens, and
- For $v' = C_m^v - C_{m-1}^v$, we have $|E_{v'}| = 1$.

By induction hypothesis, we have $P((D_v^{(A^r,m-1)})) = (1-p)^{|E[A_v^{r,m-1}]|-(m-1)+1}$. We next show that the second event happens with probability $(1-p)^{|E[A_v^{r,m}]|-|E[A_v^{r,m-1}]|-1}$. This equation follows from the fact that the number of edges between v' and C_{m-1}^v is exactly equal to $|E[A_v^{r,m}]| - |E[A_v^{r,m-1}]|$. Conditional on one of the edges being active, the probability of all the other edges being inactive is equal to $(1-p)^{|E[A_v^{r,m}]|-|E[A_v^{r,m-1}]|-1}$. Combining the preceding relation with the induction hypothesis, we obtain

$$\begin{aligned}
P((D_v^{(A^r,m)})) &= P((D_v^{(A^r,m-1)}))(1-p)^{|E[A_v^{r,m}]|-|E[A_v^{r,m-1}]|-1} \\
&= (1-p)^{|E[A_v^{r,m-1}]|-(m-1)+1}(1-p)^{|E[A_v^{r,m}]|-|E[A_v^{r,m-1}]|-1} \\
&= (1-p)^{|E[A_v^{r,m}]|-m+1},
\end{aligned}$$

completing the proof of the equality. The inequality in Eq. (A.42) is implied by the fact that in stage m, $|C_m^v| = m$. Hence, the induced subgraph over C_m^v has at most $\frac{m(m-1)}{2}$ edges. In other words,

[16] At each stage k, one node is added to C_k^v implying that the algorithm will terminate.

$|E[A_v^{r,m}]| \leq \frac{m(m-1)}{2}$. Combining the preceding relation with the fact that $1-p \leq 1$, we obtain

$$(1-p)^{|E[A_v^{r,m}]|-m+1} \geq (1-p)^{\frac{m(m-1)}{2}},$$

completing the proof. ∎

Using the previous result, it follows that

$$P((D_v^{(A,p)})) \geq (1-p)^{\frac{(\hat{k}-1)(\hat{k}-2)}{2}}.$$

Hence, by obtaining an upperbound on $\hat{k}$, we can get a lower bound on $P((D_v^{(A,p)}))$. We obtain the upperbound on $\hat{k}$ using Theorem A.1 given in subsection A.1. Combining these two results, we provide conditions on (A,p) under which, $P((D_v^{(A,p)})) \geq 1-\epsilon(n)$ with $\lim_{n\to\infty} \epsilon(n) \to 0$.

Let $\lambda(G)$ represent the second largest eigenvalue in absolute value of the adjacency matrix of the degenerate network G. For a given $d < n$, let $\mathcal{G}_d$ denote the set of $d-$ regular graphs G with $\lambda(G) = o(d)$. Consider a random network A generated from $(\Omega, \mathbb{F}, \mathbb{P})$, where $\Omega = \{G = (V,E) | E \subset \hat{E}, (V, \hat{E}) \in \mathcal{G}_d\}$.

Combining Lemma A.5 and Theorem A.1, we present the proof of the main theorem of this section.

Proof of Theorem 5.2. We first show that if $d \in \Omega(\sqrt{n})$ and $p < \frac{1}{d}$, the generated random network from (A,p) is a $1-\epsilon(n)$-local tree network with $\lim_{n\to\infty}\epsilon(n) = 0$. We show that:

- If $p < \frac{1}{d}$, by Theorem A.1 for all $v \in V$, C^v is of size at most $O(\log(n))$, with probability $1-\epsilon_1(n)$, where $\lim_{n\to\infty}\epsilon_1(n) = 0$.
- If C^v is of size $O(\log(n))$, by Lemma A.5, the attached component to v in the transmission network is acyclic with probability at least $1-\epsilon(n)$ where $\lim_{n\to\infty}\epsilon(n) = 0$.

Combining the above steps implies the desired result. Theorem A.1 implies that if $d \in \Omega(\sqrt{n})$ and $p < \frac{1}{d}$, the maximum component size of the transmission network is $O(\log(n))$ with probability $1-\epsilon_1(n)$. In other words, with probability $1-\epsilon_1(n)$ for all $v \in V$, C^v is of size $O(\log(n))$. Let (A) be the event that the maximum component size of the transmission network is $O(\log(n))$.

Moreover, by using Lemma A.5 we have

$$\begin{aligned} P((D_v^{(A,p)})) &\geq \sum_{A^a \sim (A,p)} (1-p)^{\frac{(|V[A_v^a]|-1)(|V[A_v^a]|-2)}{2}} P_{(A,p)}(A^a) \\ &\geq \sum_{\{A^a\sim(A,p)|\ |V[A_v^a]|=O(\log(n))\}} (1-p)^{\frac{(|V[A_v^a]|-1)(|V[A_v^a]|-2)}{2}} P_{(A,p)}(A^a). \end{aligned} \tag{A.43}$$

Assuming $d = \Omega(\sqrt{n})$, $p < \frac{1}{d}$ and $|V[A_v^a]| = O(\log(n))$, we obtain

$$(1-p)^{\frac{(|V[A_v^a]|-1)(|V[A_v^a]|-2)}{2}} \geq 1 - \epsilon(n), \tag{A.44}$$

where $\lim_{n\to\infty} \epsilon(n) = 0$. Combining Eqs. (A.43) and (A.44), we have

$$\begin{aligned}
&\lim_{n\to\infty} P((D_v^{(A(n),p)})) \\
&\quad \geq \lim_{n\to\infty} \sum_{\{A^a(n)\sim(A(n),p)|\ |V[A_v^a(n)]|=O(\log(n))\}} (1-p)^{\frac{(|V[A_v^a(n)]|-1)(|V[A_v^a(n)]|-2)}{2}} P_{(A(n),p)}(A^a(n)) \\
&\quad \geq \lim_{n\to\infty} (1-\epsilon_1(n))(1-\epsilon(n)) = 1,
\end{aligned}$$

completing the proof of the first part of the theorem. Using a similar argument, we can show that if $p < \frac{1}{n\log^2(n)}$, the generated random network from (A, p) is a $1-\epsilon(n)$-local tree network with $\lim_{n\to\infty} \epsilon(n)n = 0$. ∎

A.7 Proofs of Section 6

Proof of Theorem 6.1. As we have shown in Theorem 3.2, for any symmetric network A there exists a unique symmetric equilibrium. We show that under Assumption 2, for any symmetric random network, this is in fact the only equilibrium security profile.

Assume the contrary. This implies that the symmetric random network A has an asymmetric equilibrium security profile. Let q^e be the security level in the symmetric equilibrium, $\mathbf{q}_n^e$ denote the symmetric equilibrium security profile and $\hat{\mathbf{q}}^e$ be an asymmetric equilibrium security profile. We then show that there exist two agents $i, j \in V$ such that $\hat{q}_i^e > q^e$ and $\hat{q}_j^e < q^e$.

Assume to arrive at a contradiction that for all $i \in V$, $\hat{q}_i^e \geq q^e$. Using Proposition 3.3(a), this implies that for all $i \in V$, $\mathbf{P}_i(A, \hat{\mathbf{q}}^e, \Phi) \leq \mathbf{P}_i(A, \mathbf{q}_n^e, \Phi)$. Moreover, since $\hat{\mathbf{q}}^e \neq \mathbf{q}^e$, this implies that $\hat{q}_i^e > q^e$ for some agent i. Under Assumption 2, by Lemma 4.1, we obtain $\mathbf{P}_i(A, \hat{\mathbf{q}}^e, \Phi) > \mathbf{P}_i(A, \mathbf{q}_n^e, \Phi)$, yielding a contradiction. Similarly, one can extend the argument and reach a contradiction if for all $i \in V$, $\hat{q}_i^e \leq q^e$. Hence, there exist two agents $i, j \in V$ such that $\hat{q}_i^e > q^e$ and $\hat{q}_j^e < q^e$.

We next show that

$$\mathbf{P}_i(A, \hat{\mathbf{q}}^e, \Phi) \leq \mathbf{P}_j(A, \hat{\mathbf{q}}^e, \Phi), \tag{A.45}$$

using Proposition 3.2 and symmetry. Consider two agents $i, j \in V$ such that $\hat{q}_i^e > q^e$ and $\hat{q}_j^e < q^e$. By Proposition 3.2

$$\begin{aligned}
\mathbf{P}_i(A, \hat{\mathbf{q}}^e, \Phi) &= (1-\hat{q}_i^e)\tilde{P}_i(A_{-i}, \hat{\mathbf{q}}^e_{\{-i,-j\}}, \Phi) + (1-\hat{q}_i^e)(1-\hat{q}_j^e)Q_{i,j}(A, \hat{\mathbf{q}}^e_{-\{i,j\}}, \Phi), \\
\mathbf{P}_j(A, \hat{\mathbf{q}}^e, \Phi) &= (1-\hat{q}_j^e)\tilde{P}_j(A_{-i}, \hat{\mathbf{q}}^e_{\{-i,-j\}}, \Phi) + (1-\hat{q}_j^e)(1-\hat{q}_i^e)Q_{j,i}(A, \hat{\mathbf{q}}^e_{-\{i,j\}}, \Phi).
\end{aligned} \tag{A.46}$$

Also since A is symmetric, it follows that

$$\tilde{P}_i(A_{-j}, \hat{\mathbf{q}}^e_{\{-i,-j\}}, \Phi) = \tilde{P}_j(A_{-i}, \hat{\mathbf{q}}^e_{\{-i,-j\}}, \Phi),$$
$$Q_{i,j}(A, \hat{\mathbf{q}}^e_{-\{i,j\}}, \Phi) = Q_{j,i}(A, \hat{\mathbf{q}}^e_{-\{i,j\}}, \Phi). \tag{A.47}$$

Combining Eqs. (A.46), (A.47) and the fact that $\hat{q}^e_i > q^e > \hat{q}^e_j$, we obtain Eq. (A.45).

Finally, assuming $\hat{\mathbf{q}}^e$ and $\mathbf{q}^e_n$ are both equilibrium security profiles, $\hat{q}^e_i > \hat{q}^e_j$ and assuming $c(q)$ is sufficiently convex, using Eq. (3.2) we obtain

$$\mathbf{P}_i(A, \hat{\mathbf{q}}^e, \Phi) = c'(\hat{q}^e_i)(1 - \hat{q}^e_i) > c'(\hat{q}^e_j)(1 - \hat{q}^e_j) = \mathbf{P}_j(A, \hat{\mathbf{q}}^e, \Phi),$$

which contradicts Eq. (A.45) and shows the uniqueness of the equilibrium. With a similar line of argument, one can show that under Assumption 2 for any symmetric random network, the socially optimal security profile is unique and symmetric. ∎

A.8 Proofs of Subsection 6.2

Proof of Theorem 6.2. The proof follows the proof of Theorem 3.2 and Theorem 4.1 closely. We prove the following steps:

1. We show that in any equilibrium security profile, all agents residing on the same island select the same security level.
2. Given that the individuals on the same island use the same security level in the equilibrium, we show that the equilibrium security profile for the whole network is unique.

The proof of step(1) is the same as the proof of Theorem 3.2 despite the fact that the whole network is not a symmetric random network. However, given that the individuals residing on the same island are connected symmetrically to other islands, in expectation the location of the individuals on the same island are symmetric with respect to each other. We next show the proof of step(2). Given that all agents residing on the same island play symmetrically in the equilibrium security profile, without loss of generality the equilibrium security profile for all agents on the same island can be expressed via a scalar. In the rest of the proof, the equilibrium security profile $\mathbf{q}^e$ denote the equilibrium security profile of the islands and q^e_i denote the equilibrium security level of island i. We next show that the equilibrium security profile $\mathbf{q}^e$ is unique. Assume to arrive at a contradiction that we have two different equilibrium security profiles $\mathbf{q}^e$ and $\hat{\mathbf{q}}^e$. Similar to Theorem 4.1 we partition the islands into three sets $\mathcal{H}^1$, $\mathcal{H}^2$ and $\mathcal{H}^3$ as follows:

$$q^e_i > \hat{q}^e_i \text{ for all } H_i \in \mathcal{H}^1,$$
$$q^e_i = \hat{q}^e_i \text{ for all } H_i \in \mathcal{H}^2,$$
$$q^e_i < \hat{q}^e_i \text{ for all } H_i \in \mathcal{H}^3.$$

Following the same line of argument as Theorem 4.1, we show that for any tree order of the bridges without loss of generality, we can assume that there exists a bridge $(H_x, H_y) \in T$ such that $H_x \in \mathcal{H}^1$, $H_y \in \mathcal{H}^3$, and for all $H_v \in Y$ where $Y = \{H_v \in H \mid H_v > H_y\}$, we have $H_v \in \mathcal{H}^3$.

We will abuse the notation and denote the infection probability of an agent residing on island H_i, by $\mathbf{P}_{H_i}()$. We next show that we can decompose the infection probability reaching to the agents of island H_x and island H_y using the network effect on H_x when island H_y is removed from the network and the network effect on H_y when island H_x is removed from the network. More specifically, let $\hat{P}_x$ and $\hat{P}_y$ denote infection probabilities reaching to the agents of island H_x and H_y when island H_y and H_x are removed from the network respectively, i.e.,

$$\hat{P}_x(\mathbf{q}) = \tilde{P}_{H_x}(A_{-H_y}, \mathbf{q}_{-y}, \Phi)(1 - q_x),$$
$$\hat{P}_y(\mathbf{q}) = \tilde{P}_{H_y}(A_{-H_x}, \mathbf{q}_{-x}, \Phi)(1 - q_y).$$

and let $\bar{P}_x$ (and $\bar{P}_y$) denote infection probability that reaches to the agents in island H_x if the underlying network is H_x and the seed node is on island H_x, i.e., for all $i \in H_x$ and for all $j \in H_y$,

$$\bar{P}_x(q) = \mathbf{P}_i(H_x, \mathbf{q}_x, \hat{1}),$$
$$\bar{P}_y(q) = \mathbf{P}_j(H_y, \mathbf{q}_y, \hat{1}).$$

Using $\hat{P}_x$, $\hat{P}_y$, $\bar{P}_x$, and $\bar{P}_y$ we can write down infection probabilities of agents x and y as follows:

$$\mathbf{P}_x(A, \mathbf{q}^e, \Phi) = \hat{P}_x(\mathbf{q}^e) + \bar{P}_x(q_x^e)\hat{P}_y(\mathbf{q}^e), \tag{A.48}$$
$$\mathbf{P}_y(A, \mathbf{q}^e, \Phi) = \hat{P}_y(\mathbf{q}^e) + \bar{P}_y(q_y^e)\hat{P}_x(\mathbf{q}^e). \tag{A.49}$$

The rest of the proof follows the same line of argument as Theorem 4.1. ∎

Define $C_I^H(H_i, A)$ as the contribution of island H_i to infection in network A, i.e.,

$$C_I^H(H_i, A) = I(A, \mathbf{q}, \Phi) - I(A_{-H_i}, \mathbf{q}, \Phi). \tag{A.50}$$

We show that for any islands connection network, the contribution of islands to infection in a subgraph is upper bounded by their contribution to infection in the original network.

Lemma A.6. *Given an islands connection network $A = (V, H, T)$, for any $\bar{\mathcal{H}} \subset \mathcal{H}$ and $H_i \notin \bar{\mathcal{H}}$,*

$$C_I^H(H_i, A_{-\bar{\mathcal{H}}}) \leq C_I^H(H_i, A).$$

Proof of Lemma A.6. Expanding Eq. (A.50), we have

$$\begin{aligned} C_I^H(H_i, A) &= I(A, \mathbf{q}, \Phi) - I(A_{-H_i}, \mathbf{q}, \Phi) \\ &= |V(H_i)| \mathbf{P}_{H_i}(A, \mathbf{q}, \Phi) + \sum_{H_j \in \mathcal{H} - \{H_i\}} |V(H_j)| (\mathbf{P}_{H_j}(A, \mathbf{q}, \Phi) - \mathbf{P}_{H_j}(A_{-H_i}, \mathbf{q}, \Phi)). \end{aligned}$$

Similarly, we can define $C_I^H(H_i, A_{-\bar{\mathcal{H}}})$. We next show the following:

(a) For any island $H_i \in \mathcal{H} - \bar{\mathcal{H}}$, $\mathbf{P}_{H_i}(A, \mathbf{q}, \Phi) \geq \mathbf{P}_{H_i}(A_{-\bar{\mathcal{H}}}, \mathbf{q}, \Phi)$.

(b) For any island $H_j \in \mathcal{H} - \bar{\mathcal{H}} - H_i$, $\mathbf{P}_{H_j}(A, \mathbf{q}, \Phi) - \mathbf{P}_{H_j}(A_{-H_i}, \mathbf{q}, \Phi) \geq \mathbf{P}_{H_j}(A_{-\bar{\mathcal{H}}}, \mathbf{q}, \Phi) - \mathbf{P}_{H_j}(A_{-(\{H_i\} \cup \bar{\mathcal{H}})}, \mathbf{q}, \Phi)$.

Combining steps (a) and (b) implies that $C_I^H(H_i, A_{-\bar{\mathcal{H}}}) \leq C_I^H(H_i, A)$, proving Lemma A.6.

Since $A_{-\bar{\mathcal{H}}} \subset A$, by Proposition 3.3(c) it follows that for any $H_i \in \mathcal{H} - \bar{\mathcal{H}}$, $\mathbf{P}_{H_i}(A, \mathbf{q}, \Phi) \geq \mathbf{P}_{H_i}(A_{-\bar{\mathcal{H}}}, \mathbf{q}, \Phi)$, establishing step (a). We next present the proof of step (b).

Let the random variable H_s denote the island that the seed node resides on. In the islands connection network, one of the following mutually exclusive events happens:

(A) The unique path over bridges between island H_s and H_j in the tree T includes H_i.

(B) The unique path of bridges between H_s and H_j in the tree T does not include H_i.

If event (B) happens, the probability that infection reaches H_j stays unchanged after H_i is removed from the network in both A and $A_{-\bar{\mathcal{H}}}$, which implies

$$\mathbf{P}_{H_j}(A, \mathbf{q}, \Phi|(B)) - \mathbf{P}_{H_j}(A_{-H_i}, \mathbf{q}, \Phi|(B)) = \mathbf{P}_{H_j}(A_{-\bar{\mathcal{H}}}, \mathbf{q}, \Phi|(B)) - \mathbf{P}_{H_j}(A_{-(\{H_i\} \cup \bar{\mathcal{H}})}, \mathbf{q}, \Phi|(B)) = 0. \tag{A.51}$$

Suppose next that event (A) happens. The unique path between H_s and H_j then includes H_i and can be represented as $H_s, H_1, \ldots, H_k = H_i, \ldots, H_m = H_j$. An agent in island H_j gets infected in A if and only if for all $1 \leq r \leq m$, the agents corresponding to the endpoints of the bridges between (H_r, H_{r+1}) are being infected. However, in $A_{-\bar{\mathcal{H}}}$, H_j gets infected if and only if for all $1 \leq r \leq m$, the agents corresponding to the endpoints of the bridge between (H_r, H_{r+1}) are being infected and $H_r \notin \bar{\mathcal{H}}$. Hence,

$$\mathbf{P}_{H_j}(A, \mathbf{q}, \Phi|(A)) - \mathbf{P}_{H_j}(A_{-H_i}, \mathbf{q}, \Phi|(A)) \geq \mathbf{P}_{H_j}(A_{-\bar{\mathcal{H}}}, \mathbf{q}, \Phi|(A)) - \mathbf{P}_{H_j}(A_{-(\{H_i\} \cup \bar{\mathcal{H}})}, \mathbf{q}, \Phi|(A)).$$

Combining the preceding relations with Eq. (A.51), we obtain

$$\begin{aligned}
&\mathbf{P}_{H_j}(A,\mathbf{q},\Phi)-\mathbf{P}_{H_j}(A_{-H_i},\mathbf{q},\Phi)\\
&=(\mathbf{P}_{H_j}(A,\mathbf{q},\Phi|(A))-\mathbf{P}_{H_j}(A_{-H_i},\mathbf{q},\Phi|(A)))P((A))\\
&\qquad\qquad+(\mathbf{P}_{H_j}(A,\mathbf{q},\Phi|(B))-\mathbf{P}_{H_j}(A_{-H_i},\mathbf{q},\Phi|(B))P((B))\\
&\geq(\mathbf{P}_{H_j}(A_{-\bar{\mathcal{H}}},\mathbf{q},\Phi|(A))-\mathbf{P}_{H_j}(A_{-(\bar{\mathcal{H}}\cup\{H_i\})},\mathbf{q},\Phi|(A)))P((A))\\
&\qquad\qquad+(\mathbf{P}_{H_j}(A_{-\bar{\mathcal{H}}},\mathbf{q},\Phi|(B))-\mathbf{P}_{H_j}(A_{-(\bar{\mathcal{H}}\cup\{H_i\})},\mathbf{q},\Phi|(B)))P((B))\\
&=\mathbf{P}_{H_j}(A_{-\bar{\mathcal{H}}},\mathbf{q},\Phi)-\mathbf{P}_{H_j}(A_{-(\{H_i\}\cup\bar{\mathcal{H}})},\mathbf{q},\Phi),
\end{aligned}$$

completing the proof of step (b). The result then follows from the definition of C_I^H. ∎

Proof of Theorem 6.3. By Theorem 6.2, in the equilibrium and the social optimum, all agents on the same island play symmetrically. Hence without loss of generality, we can denote the equilibrium and the socially optimal security profiles of all agents residing on an island via a scalar. Similar to Theorem 6.2, let $\mathbf{q}^e$ and $\mathbf{q}^s$ denote the equilibrium and the socially optimal security profiles of the islands. If $\mathbf{q}^s > \mathbf{q}^e$ then by Propositions 3.3(a) and 3.1, we have $\mathbf{P}_v(A,\mathbf{q}^s,\Phi) < \mathbf{P}_v(A,\mathbf{q}^e,\Phi)$ for all $v \in V$ implying that $I(A,\mathbf{q}^s,\Phi) \leq I(A,\mathbf{q}^e,\Phi)$. Otherwise, let $\mathcal{H}^1 = \{H_i \in \mathcal{H} \mid q_i^s \leq q_i^e\}$, i.e., $\mathcal{H}^1$ is the set of islands that overinvest compared to the social optimum. The rest of the proof follows from the following steps:

1. We first present an upper bound for expected infections of the social optimum. We show that, $I(A,\mathbf{q}^s,\Phi) \leq I(A_{-\mathcal{H}^1},\mathbf{q}^s_{-\mathcal{H}^1},\Phi) + \sum_{H_i\in\mathcal{H}^1}|V(H_i)|c_i'(q_i^s)(1-q_i^s)$. To obtain this result, we show that

    - For any $\hat{\mathcal{H}} \subset \mathcal{H}$, $I(A,\mathbf{q},\Phi) \leq I(A_{-\hat{\mathcal{H}}},\mathbf{q}_{-\hat{\mathcal{H}}},\Phi) + \sum_{H_i\in\hat{\mathcal{H}}} C_I^H(H_i,A)$.
    - Furthermore, $C_I^H(H_i,A) \leq |H_i|c'(q_i^s)(1-q_i^s)$.

    Combining the preceding relations, implies the desired inequality.

2. We then compare this upper bound with the expected infections in the equilibrium that was expressed in Eq. (A.23), i.e.,

$$I(A,\mathbf{q}^e,\Phi) \geq \sum_{H_i\in\mathcal{H}^1}|H_i|c'(q_i^e)(1-q_i^e) + I(A_{-\mathcal{H}^1},\mathbf{q}^e_{-\mathcal{H}^1},\Phi).$$

We start by proving step (1). We show that for any $\hat{\mathcal{H}} \subset \mathcal{H}$,

$$I(A,\mathbf{q},\Phi) \leq I(A_{-\hat{\mathcal{H}}},\mathbf{q}_{-\hat{\mathcal{H}}},\Phi) + \sum_{H_i\in\hat{\mathcal{H}}} C_I^H(H_i,A). \tag{A.52}$$

The proof is by induction on $|\hat{\mathcal{H}}|$. If $|\hat{\mathcal{H}}| = 0$, then $C_I^H(\hat{\mathcal{H}},A) = 0$. Hence, Eq. (A.52) trivially holds (the induction basis). We next assume that if $|\hat{\mathcal{H}}| = m$, then Eq. (A.52) holds (induction hypothesis) and we then prove that it would hold if $|\hat{\mathcal{H}}| = m + 1$ as well. Consider an island $H_i \in \hat{\mathcal{H}}$ and let $\hat{\mathcal{H}}_{-i} = \hat{\mathcal{H}} - \{H_i\}$. Since $|\hat{\mathcal{H}}_{-i}| = m$, by induction hypothesis we have

$$I(A, \mathbf{q}, \Phi) \leq I(A_{-\hat{\mathcal{H}}_{-i}}, \mathbf{q}^s_{-\hat{\mathcal{H}}_{-i}}, \Phi) + \sum_{H_j \in \hat{\mathcal{H}}_{-i}} C_I^H(H_j, A). \tag{A.53}$$

Furthermore, by Eq. (A.50) we have

$$I(A_{-\hat{\mathcal{H}}_{-i}}, \mathbf{q}^s_{-\hat{\mathcal{H}}_{-i}}, \Phi) = I(A_{-\hat{\mathcal{H}}}, \mathbf{q}^s_{-\hat{\mathcal{H}}}, \Phi) + C_I^H(H_i, A_{-\hat{\mathcal{H}}_{-i}}) \leq I(A_{-\hat{\mathcal{H}}}, \mathbf{q}^s_{-\hat{\mathcal{H}}}, \Phi) + C_I^H(H_i, A), \tag{A.54}$$

where the inequality follows from Lemma A.6. Combining Eqs. (A.53) and A.54, we obtain

$$I(A, \mathbf{q}, \Phi) \leq I(A_{-\hat{\mathcal{H}}_{-i}}, \mathbf{q}^s_{-\hat{\mathcal{H}}_{-i}}, \Phi) + \sum_{H_j \in \hat{\mathcal{H}}_{-i}} C_I^H(H_j, A) \leq I(A_{-\hat{\mathcal{H}}}, \mathbf{q}^s_{-\hat{\mathcal{H}}}, \Phi) + \sum_{H_j \in \hat{\mathcal{H}}} C_I^H(H_j, A),$$

completing the proof of Eq. (A.52).
We next show that in an islands connection network, when agents select the socially optimal security profile, we have

$$C_I^H(H_i, A) \leq |V(H_i)| c'(q_i^s)(1 - q_i^s). \tag{A.55}$$

Using Eq. (A.50), $C_I^H(H_i, A)$ can be written as follows:

$$\begin{aligned} C_I^H(H_i, A) &= I(A, \mathbf{q}^s, \Phi) - I(A_{-H_i}, \mathbf{q}^s, \Phi) \\ &= |V(H_i)| \mathbf{P}_{H_i}(A, \mathbf{q}^s, \Phi) + \sum_{d \in V - V(H_i)} \mathbf{P}_d(A, \mathbf{q}^s, \Phi) - \mathbf{P}_d(A_{-H_i}, \mathbf{q}^s, \Phi). \end{aligned} \tag{A.56}$$

We next show that in an islands connection network $A = (V, \mathcal{H}, T)$, given an island $H_i \in \mathcal{H}$, and two agent $v, d \in V$ such that $v \in V(H_i)$ and $d \in V(H_j)$, we have

$$(1 - q_i) Q_{d,v}(A, \mathbf{q}^s, \Phi) \geq \frac{1}{|V(H_i)|} (\tilde{P}_d(A, \mathbf{q}^s, \Phi) - \tilde{P}_d(A_{-H_i}, \mathbf{q}^s, \Phi)). \tag{A.57}$$

Let H_s denote the island that the seed node resides on. Since A is an island connection network one of the following mutually exclusive events happens:

(A) The unique path of bridges between H_s and H_j in T includes H_i.

(B) The unique path of bridges between H_s and H_j in T does not include H_i.

If event (B) happens, then the probability of infection reaching to d stays unchanged after H_i is removed which implies

$$(1 - q_i^s) Q_{d,v}(A, \mathbf{q}^s, \Phi | (B)) = \tilde{P}_d(A, \mathbf{q}^s, \Phi | (B)) - \tilde{P}_d(A_{-H_i}, \mathbf{q}^s, \Phi | (B)) = 0.$$

Suppose next that event (A) happens. In this scenario, $\tilde{P}_d(A_{-H_i}, \mathbf{q}^s, \Phi)|(A)) = 0$. Let $S, H_1, \ldots, H_k = H_i, \ldots, H_t = H_j$ denote the unique path over the bridges in T, between islands H_s and H_j. Let (A^m) denote the event in which agent m is the randomly selected agent from H_i that is connected to H_{k+1}. By law of total probability and assuming that the security profiles as well as the islands are symmetric, we have: For any $m \in V(H_i)$,

$$\tilde{P}_d(A, \mathbf{q}^s, \Phi|(A)) = \sum_{m \in V(H_i)} \tilde{P}_d(A, \mathbf{q}^s, \Phi|(A^m))P((A^m)) = \tilde{P}_d(A, \mathbf{q}^s, \Phi|(A^m)). \tag{A.58}$$

Also if event (A^m) happens, the only way to reach from H_s to H_j is through agent m. That implies

$$(1 - q_i^s)Q_{d,v}(A, \mathbf{q}^s, \Phi|(A)) \geq \tilde{P}_d(A, \mathbf{q}^s, \Phi|(A^m))P((A^m)) = \frac{1}{|V(H_i)|}\tilde{P}_d(A, \mathbf{q}^s, \Phi|(A^m)). \tag{A.59}$$

Combining Eqs. (A.59) and (A.58), we obtain

$$\begin{aligned}
(1 - q_i^s)Q_{d,v}(A, \mathbf{q}^s, \Phi) &= (1 - q_i)Q_{d,v}(A, \mathbf{q}^s, \Phi|(A))P((A)) + (1 - q_i)Q_{d,v}(A, \mathbf{q}^s, \Phi|(B))P((B)) \\
&= (1 - q_i^s)Q_{d,v}(A, \mathbf{q}^s, \Phi|(A))P((A)) \\
&\geq \frac{1}{|V(H_i)|}\tilde{P}_d(A, \mathbf{q}^s, \Phi|(A^m))P((A)) \\
&= \frac{1}{|V(H_i)|}(\tilde{P}_d(A, \mathbf{q}^s, \Phi) - \tilde{P}_d(A_{-H_i}, \mathbf{q}^s, \Phi)).
\end{aligned}$$

Combining the preceding relation with Eqs. (A.50) and (3.3), in the socially optimal solution for each agent $m \in V(H_i)$, the following relations hold:

$$\begin{aligned}
|V(H_i)|c'(q_i^s)(1 - q_i^s) &= |V(H_i)|\mathbf{P}_i(A, \mathbf{q}^s, \Phi) + |V(H_i)| \sum_{d \in V}(1 - q_i^s)(1 - q_d^s)Q_{d,v}(A, \mathbf{q}^s, \Phi) \\
&\geq |V(H_i)|\mathbf{P}_i(A, \mathbf{q}^s, \Phi) + \sum_{d \in V - V(H_i)} (\mathbf{P}_d(A, \mathbf{q}^s, \Phi) - \mathbf{P}_d(A_{-H_i}, \mathbf{q}^s, \Phi)) \\
&= C_I^H(H_i, A),
\end{aligned}$$

completing the proof of Eq. (A.55). Combining Eqs. (A.54) and (A.55), we obtain

$$\begin{aligned}
I(A, \mathbf{q}^s, \Phi) &\leq I(A_{-\mathcal{H}^1}, \mathbf{q}_{-\mathcal{H}^1}, \Phi) + \sum_{H_i \in \mathcal{H}^1} C_I^H(H_i, A) \\
&\leq I(A_{-\mathcal{H}^1}, \mathbf{q}^s_{-\mathcal{H}^1}, \Phi) + \sum_{H_i \in \mathcal{H}^1} |V(H_i)|c_i'(q_i^s)(1 - q_i^s),
\end{aligned}$$

completing the proof of step (1). Finally, by combining steps (1) and (2), we obtain

$$\begin{aligned}
I(A, \mathbf{q}^s, \Phi) &\leq I(A_{-\mathcal{H}^1}, \mathbf{q}^s_{-\mathcal{H}^1}, \Phi) + \sum_{H_i \in \mathcal{H}^1} |V(H_i)| c_i'(q_i^s)(1 - q_i^s) \\
&\leq I(A_{-\mathcal{H}^1}, \mathbf{q}^e_{-\mathcal{H}^1}, \Phi) + \sum_{H_i \in \mathcal{H}^1} |H_i| c'(q_i^e)(1 - q_i^e) \\
&\leq I(A, \mathbf{q}^e, \Phi),
\end{aligned}$$

where the second inequality follows from Proposition 3.3(a) and Lemma 4.1, and the third inequality from Eq. (A.23), completing the proof of the Theorem. ∎

A.9 Proofs of Subsection 6.3

Lemma A.4. *Suppose Assumptions 1 and 2 hold. Given two symmetric networks $\hat{G}_1$ and $\hat{G}_2$, $I(\hat{G}_1, q_1^e, \Phi) \geq I(\hat{G}_2, q_2^e, \Phi)$ if and only if $I(\hat{G}_1, q, \Phi) \geq I(\hat{G}_2, q, \Phi)$ for all $q \in [0, 1]$.*

Proof of Theorem A.4. Consider two symmetric random networks $\hat{G}_1$ and $\hat{G}_2$. We first show that if for all $q \in [0, 1]$,

$$I(\hat{G}_1, q, \Phi) \geq I(\hat{G}_2, q, \Phi), \tag{A.60}$$

then $q_1^e \geq q_2^e$ where q_1^e and q_2^e are the symmetric equilibrium security levels of $\hat{G}_1$ and $\hat{G}_2$. Assume to arrive at a contradiction that $q_1^e < q_2^e$. Hence, we have

$$c'(q_1^e) = \tilde{P}_i(\hat{G}_1, q_1^e, \Phi) \geq \tilde{P}_i(\hat{G}_2, q_1^e, \Phi) \geq \tilde{P}_i(\hat{G}_2, q_2^e, \Phi) = c'(q_2^e). \tag{A.61}$$

First equation is implied by Eq. (3.2). First inequality is obtained by the assumption in the statement, and the second inequality is the combination of Proposition 3.3(a) and the fact that $q_1^e < q_2^e$. Moreover, since by Assumption 1, the function c is strictly convex, we have $c'(q_1^e) < c'(q_2^e)$ which is in contrast with Eq. (A.61) and shows that $q_1^e \geq q_2^e$.

Combined with Lemma 4.1, this implies $\mathbf{P}_i(\hat{G}_1, q_1^e, \Phi) \geq \mathbf{P}_i(\hat{G}_2, q_2^e, \Phi)$ which completes the proof of the first part.

We next show that if the condition in Eq. (A.60) does not hold, then we can find two sufficiently convex cost functions c and $\hat{c}$ such that

$$I(\hat{G}_1, q_1^e, \Phi) > I(\hat{G}_2, q_2^e, \Phi), \text{ and } I(\hat{G}_1, \hat{q}_1^e, \Phi) < I(\hat{G}_2, \hat{q}_2^e, \Phi), \tag{A.62}$$

where q_1^e and q_2^e are the symmetric equilibrium security levels of $\hat{G}_1$ and $\hat{G}_2$ for cost function c, and $\hat{q}_1^e$ and $\hat{q}_2^e$ are the symmetric equilibrium security levels of $\hat{G}_1$ and $\hat{G}_2$ for cost function $\hat{c}$, establishing that a ranking of equilibrium in terms of expected infections is not possible. Let $\bar{q}, \tilde{q} \in [0, 1]$ be such that

$$I(\hat{G}_1, \bar{q}, \Phi) > I(\hat{G}_2, \bar{q}, \Phi), \text{ and } I(\hat{G}_1, \tilde{q}, \Phi) < I(\hat{G}_2, \tilde{q}, \Phi). \quad \text{(A.63)}$$

We first present two sufficiently convex cost functions $c(q)$ and $\hat{c}(q)$ such that $q_1^e = \bar{q}$ and $\hat{q}_1^e = \tilde{q}$. We then show that $q_2^e < q_1^e$ and $\hat{q}_2^e > \hat{q}_1^e$. Combining these inequalities with Lemma 4.1 gives the desired result. Let $c(q)$ and $\hat{c}(q)$ be such that

$$c'(q) = \frac{\bar{a}q}{(1-q)} \text{ and } \hat{c}'(q) = \frac{\tilde{a}q}{(1-q)},$$

where $\bar{a} = \frac{I(\hat{G}_1, \bar{q}, \Phi)}{\bar{q}n}$ and $\tilde{a} = \frac{I(\hat{G}_1, \tilde{q}, \Phi)}{\tilde{q}n}$.

One can verify that $q_1^e = \bar{q}$ and $\hat{q}_1^e = \tilde{q}$. We next show that $q_2^e < q_1^e$ and $\hat{q}_2^e > \hat{q}_1^e$. We first show that $q_2^e < q_1^e$. Assume to arrive at a contradiction that $q_2^e \geq q_1^e$. Substituting q_1^e with $\bar{q}$ and combining with the preceding equation we have

$$c'(q_2^e) \geq c'(q_1^e) = c'(\bar{q}) = \frac{I(\hat{G}_1, \bar{q}, \Phi)}{n(1-\bar{q})} > \frac{I(\hat{G}_2, \bar{q}, \Phi)}{n(1-\bar{q})} \geq \frac{I(\hat{G}_2, q_2^e, \Phi)}{n(1-\hat{q}_2^e)}.$$

First inequality follows from the fact that $c'(q)$ is convex and $q_2^e \geq q_1^e$. Second equality follows from Eq. (3.2), second inequality from Eq. (A.63), and the third inequality from Proposition 3.3(a). Using Eq. (3.2), we obtain $c'(q_2^e) = \frac{I(\hat{G}_2, q_2^e, \Phi)}{n(1-\hat{q}_2^e)}$ which is a contradiction and shows the desired result. Using a similar line of argument, one can show that $\hat{q}_2^e > \hat{q}_1^e$.

Using $q_2^e < q_1^e$ and $\hat{q}_2^e > \hat{q}_1^e$ together with Lemma 4.1, we obtain Eq. (A.62), completing the proof. ∎

***Proof of Theorem 6.4**.* We first show the following:

Lemma A.7. *Given two symmetric random networks $\hat{G}_1$ and $\hat{G}_2$ generated from two base graphs G_1 and G_2, if $G_1 \subset G_2$, then $\boldsymbol{P}_i(\hat{G}_1, q, \Phi) \leq \boldsymbol{P}_i(\hat{G}_2, q, \Phi)$ for all $i \in V$ and for all $q \in [0, 1]$.*

The proof of this lemma follows the same line of argument as Proposition 3.3(c) closely. The preceding lemma together with Theorem A.4 establishes our desired result. ∎

***Proof of Proposition 6.1**.* The infection probability of an agent in a symmetric random tree T with distance vector $\mathbf{d}$ and the symmetric security level q is defined as follows:

$$\mathbf{P}_i(T, q, \Phi) = \frac{1}{n^2} \sum_{i=1}^{n} d_i (1-q)^i.$$

We first show that for two symmetric random trees $(T, \mathbf{d})$ and $(T', \mathbf{d}')$ and a given vector $\mathbf{z} =$

$(z_1, \ldots, z_n)$ such that $z_1 \geq z_2 \geq \ldots \geq z_n \geq 0$, if $T' \prec T$, then we have

$$\sum_{i=1}^{j}(d_i - d_i')z_i \geq z_j \sum_{i=1}^{j}(d_i - d_i') \text{ for all } 1 \leq j \leq n. \tag{A.64}$$

To prove this, we use induction on j. For $j = 1$ (i.e., the induction basis) the statement trivially holds. We assume that the statement holds for $j \leq m < n$. We then prove that the statement holds for $j = m + 1$.

Expanding the left hand side and substituting j with $m + 1$ we obtain

$$\begin{aligned}
\sum_{i=1}^{j}(d_i - d_i')z_i = \sum_{i=1}^{m+1}(d_i - d_i')z_i &= \sum_{i=1}^{m}(d_i - d_i')z_i + z_{m+1}(d_{m+1} - d'_{m+1}) \\
&\geq z_m \sum_{i=1}^{m}(d_i - d_i') + z_{m+1}(d_{m+1} - d'_{m+1}) \\
&\geq z_{m+1}(\sum_{i=1}^{m} d_i - d_i') + z_{m+1}(d_{m+1} - d'_{m+1}) \\
&= z_{m+1}(\sum_{i=1}^{m+1} d_i - d_i')
\end{aligned}$$

where the first inequality follows from the induction hypothesis and the second inequality is due to the fact that $\mathbf{d} \succ \mathbf{d}'$ and $z_{m+1} < z_m$.

Using this result, we next show that if $T' \prec T$ then $I(\hat{T}, q, \Phi) \geq I(\hat{T}', q, \Phi)$. By the definition of the distance function we have

$$I(\hat{T}, q, \Phi) - I(\hat{T}', q, \Phi) = \frac{n}{n^2}\sum_{i=1}^{n}(d_i - d_i')(1-q)^i \geq \frac{1}{n}(1-q)^n \sum_{i=1}^{n}(d_i - d_i') \geq 0.$$

The preceding inequality follows from Eq. (A.64) when z is replaced by $\bar{\mathbf{q}}$ where $\bar{\mathbf{q}} = ((1-q), (1-q)^2, \ldots, (1-q)^n)$. Note that $\bar{q}_i \geq \bar{q}_j \geq 0$ for all $i \leq j$, hence Eq. (A.64) holds. Finally by applying Theorem A.4, we obtain $I(\hat{T}, q^e, \Phi) \geq I(\hat{T}', \hat{q}^e, \Phi)$ where q^e and $\hat{q}^e$ denote the equilibrium security levels of $\hat{T}$ and $\hat{T}'$ respectively. ∎

Proof of Proposition 6.2. Let (α^i) be the event in which exactly i agents are susceptible. The expected infections can be stated as

$$I(\hat{G}, \mathbf{q}, \Phi) = \sum_{i=1}^{n} I(\hat{G}, \mathbf{q}, \Phi|(\alpha^i))P((\alpha^i)), \tag{A.65}$$

where $P((\alpha^i))$ denotes the probability that event (α^i) happens.

We first show that $I(\hat{G}, \mathbf{q}, \Phi|(\alpha^i)) = n\varrho_G(\frac{i}{n})$. Let V^i denote the set of subsets of agents of size i, i.e., $V^i = \{V' \subset V || V'| = i\}$. We have

$$I(\hat{G}, \mathbf{q}, \Phi | (\alpha^i)) = \sum_{\bar{V} \in V^i} I(\hat{G}[\bar{V}], \mathbf{q}, \Phi) P(\bar{V} | (\alpha^i)) = \frac{1}{\binom{n}{i}} \sum_{\bar{V} \in V^i} I(\hat{G}[\bar{V}], \mathbf{q}, \Phi). \tag{A.66}$$

Here, the second equality follows from the fact that for all $\bar{V} \in V^i$, $P(\bar{V})$ which is the probability of having all agents in $\bar{V}$ susceptible and all agents in $V - \bar{V}$ immune, is the same and is equal to $(1-q)^i q^{n-i}$. Hence, for all $\bar{V} \in V^i$, $P(\bar{V}|(\alpha^i)) = \frac{1}{\binom{n}{i}}$.

Now, note that for a given base graph G, $\varrho_G(\frac{i}{n})$ denotes the normalized expected size of the connected component attached to a randomly selected seed node v from G, in the induced subgraph of G over i randomly selected agents from G. In other words, $\varrho_G(\frac{i}{n})$ denotes expected infection rate in $\hat{G}$ when i randomly selected agents are susceptible and the rest of the agents are immune, which implies the following:

$$\frac{1}{\binom{n}{i}} \sum_{\bar{V} \in V^i} I(\hat{G}[\bar{V}], \mathbf{q}, \Phi) = \frac{n}{\binom{n}{i}} \binom{n}{i} \varrho_G(\frac{i}{n}) = n \varrho_G(\frac{i}{n}).$$

The result follows by combining this with the fact that $P((\alpha^i)) = \binom{n}{i}(1-q)^i q^{n-i}$. ∎

Proof of Theorem 6.5. The proof consists of two parts. Given two base structures $G_1[n]$ and $G_2[n]$, we first show that if for all $r \in [0,1]$ $\varrho_{G_1}(r) \geq \varrho_{G_2}(r)$, then $I(\hat{G}_1, q_1^e, \Phi) \geq I(\hat{G}_2, q_2^e, \Phi)$ for any sufficiently convex cost function. As in the rest of the paper, let q_1^e and q_2^e denote the equilibrium security levels of $\hat{G}_1$ and $\hat{G}_2$. By Proposition 6.2 and assuming that $\varrho_{G_1}(r) \geq \varrho_{G_2}(r)$ for all $r \in [0,1]$, we have,

$$I(\hat{G}_1, \mathbf{q}, \Phi) = \sum_{i=1}^{n} n \binom{n}{i} (1-q)^i q^{n-i} \varrho_{G_1}(\frac{i}{n}) \geq \sum_{i=1}^{n} n \binom{n}{i} (1-q)^i q^{n-i} \varrho_{G_2}(\frac{i}{n}) = I(\hat{G}_2, \mathbf{q}, \Phi). \tag{A.67}$$

Combining Eq. (A.67) with Theorem A.4 shows the desired result. To prove the only if part, we will first show the following:

Theorem A.5. *For any n and $\epsilon > 0$ there exists $\delta(n)$ such that for all G_1 and G_2 if there exists an interval $I \subset [0,1]$ of length at least δ for which $\varrho_{G_1}(\frac{k}{n}) \geq \varrho_{G_2}(\frac{k}{n}) + \epsilon$ for all $\frac{k}{n} \in I$, then there exists q such that $I(\hat{G}_1, q, \Phi) > I(\hat{G}_2, q, \Phi)$. Furthermore, $\lim_{n\to\infty} \delta(n) = 0$.*

Proof. Let $q = (\max(I) + \min(I))/2$. Consider a Binomial random variable X with parameters n

and q. Let $\hat{X} = \frac{X}{n}$.

$$\begin{aligned}\frac{1}{n}(I(\hat{G}_1, q, \Phi) - I(\hat{G}_2, q, \Phi)) &= E[\varrho_{G_1}(\hat{X}) - \varrho_{G_2}(\hat{X})] \\ &= E[\varrho_{G_1}(\hat{X}) - \varrho_{G_2}(\hat{X})|\hat{X} \in I]Pr[\hat{X} \in I] + E[\varrho_{G_1}(\hat{X}) - \varrho_{G_2}(\hat{X})|\hat{X} \notin I]Pr[\hat{X} \notin I] \\ &\geq E[\epsilon|\hat{X} \in I](1 - 2e^{-n\delta^2/2}) + E[-1|\hat{X} \notin I]2e^{-n\delta^2/2} \\ &= \epsilon - (1+\epsilon)2e^{-n\delta^2/2}.\end{aligned}$$

The first equation follows from the definition of ϱ_{G_1} and the linearity of expectation, and the second equation follows from the law of total probability. By applying Theorem A.3, we obtain $Pr[\hat{X} \notin I] \leq 2e^{-n\delta^2/2}$. Combining with the fact that $\varrho_{G_1}(\hat{X}) - \varrho_{G_2}(\hat{X}) \geq -1$, we obtain the first inequality.

By choosing any $\delta > \sqrt{\frac{2\ln(2+2/\epsilon)}{n}}$ we can ensure that $I(\hat{G}_1, q) - I(\hat{G}_2, q) > 0$ which proves the claim. Note that $\lim_{n\to 0}\sqrt{\frac{2\ln(2+2/\epsilon)}{n}} = 0$. ∎

Combining the preceding theorem with Theorem A.4 shows the desired result. ∎

A.10 Proofs of Section 7

Proof of Theorem 7.1. 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 can be stated as follows:

$$\mathbf{P}_i(A, \mathbf{q}, \Phi) = \mathbf{P}_i(A, \mathbf{q}, \Phi|(X_i))(1 - q_i). \tag{A.68}$$

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 $A^t \sim (A, \mathbf{q})$, i.e.,

$$\mathbf{P}_i(A, \mathbf{q}, 1_n|\mathbf{X}_i) = \frac{1}{n}\sum_{s\in V}\sum_{\{A^t|(s\in A^t)\cap i\xrightarrow{A^t}s\}}\mathbf{P}_{(A,\mathbf{q})}(A^t|(X_i)).$$

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 $I(A, \mathbf{q}, e_i) = n\mathbf{P}_i(A, \mathbf{q}, \hat{1}_n)$. Using Proposition 3.2, we have $I(A, \mathbf{q}, e_i) = \tilde{P}_i(A, \mathbf{q}_{-i}, \hat{1}_n)(1 - q_i)n$. ∎

Proof of Theorem 7.2. To show the existence of the Nash equilibrium of the security game, we show that the utility of each agent with respect to his security level is always concave if

$$c''(q) \geq \Psi^2(\Phi)\Upsilon(\Phi)(1-q) + 2\Psi(\Phi). \tag{A.69}$$

Given network A and security profile $\mathbf{q}$, let $\Phi = (\rho_1, \ldots, \rho_n)$ denote the attack decision selected by the strategic attacker. The utility of an agent j can be written as follows:

$$\begin{aligned} u_j(A, \mathbf{q}, \Phi) &= \big(1 - \mathbf{P}_j(A, \mathbf{q}, \Phi)\big) - c(q_j) \\ &= \left(1 - (1 - q_j)\sum_{i=1}^{n} \tilde{P}_j(A, \mathbf{q}_{-j}, e_i)\rho_i\right) - c(q_j). \end{aligned} \tag{A.70}$$

For ease of notation, let $\alpha_i = \tilde{P}_j(A, \mathbf{q}_{-j}, e_i)$. We show that if the inequality (A.69) holds, then $\frac{\partial^2 u_j(A,\mathbf{q})}{\partial {q_j}^2} \leq 0$, proving that the utility of agent j is concave with respect to his security level. Using Eq. (A.70), we have

$$\begin{aligned} \frac{\partial^2 u_j(A, \mathbf{q}, \Phi)}{\partial {q_j}^2} &= \frac{\partial}{\partial q_j} \frac{\partial u_j\left(A, \mathbf{q}, \Phi\right)}{\partial q_j} \\ &= \frac{\partial}{\partial q_j}\Big(\sum_{i=1}^{n} \alpha_i \rho_i - (1 - q_j)\sum_{i=1}^{n} \alpha_i \frac{\partial \rho_i}{\partial q_j} - c'(q_j)\Big) \\ &= 2\sum_{i=1}^{n} \alpha_i \frac{\partial \rho_i}{\partial q_j} - (1 - q_j)\sum_{i=1}^{n} \alpha_i \frac{\partial^2 \rho_i}{\partial {q_j}^2} - c''(q_j). \end{aligned} \tag{A.71}$$

To show the concavity of the utility function we also need to analyze the attacker's response to a given security profile $\mathbf{q}$. The attacker's value after attacking agent i is equal to the expected infections after the attack. Using Theorem 7.1, expected infections is a linear function of q_j and is obtained from the following equation:

$$I(A, \mathbf{q}, e_i) = n(1 - q_i)\tilde{P}_i(A_{-\{j\}}, \mathbf{q}_{-\{i,j\}}, \hat{1}_n) + n(1 - q_j)(1 - q_i)Q_{i,j}(A, \mathbf{q}_{-\{i,j\}}, \hat{1}_n).$$

For ease of notation, let $\gamma_i(A, \mathbf{q}) = (1-q_i)\tilde{P}_i(A_{-j}, \mathbf{q}_{-i,j}, \hat{1}_n)$ and $\beta_i(A, \mathbf{q}) = (1-q_i)Q_{i,j}(A, \mathbf{q}_{-\{i,j\}}, \hat{1}_n)$. Given network A and security profile $\mathbf{q}$, the optimal attack decision $\Phi = (\rho_1, \ldots, \rho_n)$ is obtained from the following program:

$$\begin{aligned} \text{Maximize} \quad & \sum_{i=1}^{n} \rho_i(\beta_i(A, \mathbf{q})(1 - q_j) + \gamma_i(A, \mathbf{q})) - \zeta(\rho_i) \\ \text{subject to} \quad & \sum_{i=1}^{n} \rho_i = 1 && (\lambda) \\ & \rho_i \geq 0 \qquad \text{forall } i \in [n] && (\mu_i) \end{aligned}$$

Define

$$L(\Phi, \lambda, \mu) = \sum_{i=1}^{n} \rho_i(\beta_i(A, \mathbf{q})(1 - q_j) + \gamma_i(A, \mathbf{q})) - \zeta(\rho_i) + \lambda\left(\sum_{i=1}^{n} \rho_i - 1\right) + \sum_{i=1}^{n} \mu_i \rho_i,$$

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

$$\frac{\partial}{\partial \rho_i} L = \beta_i(A, \mathbf{q})(1 - q_j) + \gamma_i(A, \mathbf{q}) - \frac{\partial}{\partial \rho_i}\zeta(\rho_i) + \lambda + \mu_i = 0$$
$$\mu_i \rho_i = 0 \qquad \text{(for all } i \in [n]).$$

Furthermore, assuming that $\zeta()$ is a convex increasing function with $\zeta(0) = 0$, we have

$$\rho_i = \frac{\partial}{\partial \rho_i}\zeta^{-1}\left(\max(0, \beta_i(A, \mathbf{q})(1 - q_j) + \gamma_i(A, \mathbf{q}) + \lambda)\right). \tag{A.72}$$

Given that $\sum_i \rho_i = 1$, we have, $\sum_i \frac{\partial}{\partial \rho_i}\zeta^{-1}\left(\max(0, \beta_i(A, \mathbf{q})(1 - q_j) + \gamma_i(A, \mathbf{q}) + \lambda)\right) = 1$. [17] To evaluate Eq. (A.71), we need to analyze the second derivative of ρ_i with respect to q_j. Having $\sum_{i=1}^{n} \rho_i = 1$ implies that,

$$\sum_{i=1}^{n} \frac{\partial \rho_i}{\partial q_j} = 0. \tag{A.73}$$

Combining with Eq. (A.72), we obtain

$$\sum_{i=1}^{n} \frac{\partial \rho_i}{\partial q_j} = \frac{-\beta_i(A, \mathbf{q}) - \frac{\partial \lambda}{\partial q_j}}{\zeta''(\rho_i)} \tag{A.74}$$
$$= \sum_{i=1}^{n} \frac{-\beta_i(A, \mathbf{q})}{\zeta''(\rho_i)} - \Psi \frac{\partial \lambda}{\partial q_j} \tag{A.75}$$
$$= 0. \tag{A.76}$$

Hence, we have

$$\frac{\partial \lambda}{\partial q_j} = \frac{\sum_{i=1}^{n} \frac{-\beta_i(A, \mathbf{q})}{\zeta''(\rho_i)}}{\Psi}. \tag{A.77}$$

The second order derivative of ρ_i and λ with respect to q_j is obtained by the following equations.

$$\frac{\partial^2 \rho_i}{\partial {q_j}^2} = \frac{-\frac{\partial^2 \lambda}{\partial {q_j}^2}}{\zeta''(\rho_i)} - \left(\frac{\partial \rho_i}{\partial q_j}\right)^2 \frac{\zeta'''(\rho_i)}{\zeta''(\rho_i)}. \tag{A.78}$$

[17] Since $\frac{\partial}{\partial \rho_i}\zeta^{-1}()$ is also an increasing function, we can compute λ for each choice of q by doing a binary search.

$$\frac{\partial^2 \lambda}{\partial {q_j}^2} = -\frac{\sum_{i=1}^{n} (\frac{\partial \rho_i}{\partial q_j})^2 \frac{\zeta'''(\rho_i)}{\zeta''(\rho_i)}}{\Psi}. \tag{A.79}$$

Replacing Eqs. (A.78) and (A.79) in Eq. (A.71), we obtain:

$$\frac{\partial^2 u_j(A, \mathbf{q}, \Phi)}{\partial {q_j}^2} =$$

$$\sum_{i=1}^{n} \alpha_i \left(2\frac{\partial \rho_i}{\partial q_i} + \left(\frac{\frac{\partial^2 \lambda}{\partial {q_j}^2}}{\zeta''(\rho_i)} + (\frac{\partial \rho_i}{\partial q_j})^2 \frac{\zeta'''(\rho_i)}{\zeta''(\rho_j)} \right) (1 - q_j) \right) - c''(q_j)$$

We next show that if Eq. (A.69) holds, the utility of each agent is concave with respect to his security level. We consider two cases:

(a) $\zeta'''() < 0$.

(b) Or $\zeta'''() \geq 0$.

In case (a), combining Eq. (A.79) and the fact that $\zeta'''() < 0$ and $\zeta''() \geq 0$, implies that $\frac{\partial^2 \lambda}{\partial {q_j}^2} > 0$. Furthermore, since $0 \leq \beta_i \leq 1$, it is implied that $-1 \leq \frac{\partial \lambda}{\partial q_j} \leq 0$. Replacing these inequalities in Eq. (A.71), we obtain,

$$\begin{aligned}
\frac{\partial^2 u_j(A, \mathbf{q}, \Phi)}{\partial {q_j}^2} &= \\
&\sum_{i=1}^{n} \alpha_i \left(2\frac{\partial \rho_i}{\partial q_i} + \left(\frac{\frac{\partial^2 \lambda}{\partial {q_j}^2}}{\zeta''(\rho_i)} + (\frac{\partial \rho_i}{\partial q_j})^2 \frac{\zeta'''(\rho_i)}{\zeta''(\rho_j)} \right) (1 - q_j) \right) - c''(q_j) \\
&\leq \sum_{i=1}^{n} \alpha_i \left(2\frac{\partial \rho_i}{\partial q_i} + \frac{\frac{\partial^2 \lambda}{\partial {q_j}^2}}{\zeta''(\rho_i)}(1 - q_j) \right) - c''(q_j) \\
&= \sum_{i=1}^{n} \alpha_i \left(2\frac{-\beta_i - \frac{\partial \lambda}{\partial q_j}}{\Psi} + \frac{\frac{\partial^2 \lambda}{\partial {q_j}^2}}{\zeta''(\rho_i)}(1 - q_j) \right) - c''(q_j) \\
&\leq -2\frac{\partial \lambda}{\partial q_j} \sum_{i=1}^{n} \frac{\alpha_i}{\zeta''(\rho_i)} + (1 - q_j)\frac{\partial^2 \lambda}{\partial {q_j}^2} \sum_{i=1}^{n} \frac{\alpha_i}{\zeta''(\rho_i)} - c''(q_j) \\
&\leq -2\sum_{i=1}^{n} \frac{\alpha_i}{\zeta''(\rho_i)} + (1 - q_j)\frac{\partial^2 \lambda}{\partial {q_j}^2} \sum_{i=1}^{n} \frac{\alpha_i}{\zeta''(\rho_i)} - c''(q_j) \\
&\leq 2\Psi + (1 - q_j) \sum_{i=1}^{n} \frac{-\zeta'''(\rho_i)}{{\zeta''(\rho_i)}^3} - c''(q_j) \\
&\leq 2\Psi + \Psi^2 \Upsilon (1 - q_j) - c''(q_j).
\end{aligned}$$

Hence, if Eq. (A.69) holds, the utility of each agent is concave in his security level.

With a similar argument, one can show that if Eq. (A.69) holds, then in case (b) the utility of each agent with respect to his security level is concave, completing the proof. ∎

Proof of Theorem 7.3. We first investigate the symmetric equilibrium security profile. 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, $\mathbf{q}_i$ denotes a vector of size i with all entries equal to q. Assuming that the attack cost function is convex, for a symmetric random network, the attack decision of the strategic attacker can be stated as,

$$\Phi = (\rho_1, \ldots, \rho_n) \text{ where } \rho_i = \rho, \text{ for all } j \neq i \ \rho_j = \frac{1-\rho}{n-1}.$$

Let $\hat{P}(n) = \tilde{P}(A, \mathbf{q}^e, 1_n)$ and $\hat{P}(n-1) = E_{v \in V}[\tilde{P}(A_{-v}, \mathbf{q}^e_{-v}, \hat{1}_n)]$.

The optimal value of ρ is obtained from the following program:

$$\text{maximize} \tag{A.80}$$

$$\rho(1-q')\hat{P}(n) + (1-\rho)(1-q^e)(\hat{P}(n-1) + (1-q')\frac{\hat{P}(n) - \hat{P}(n-1)}{1-q^e}) - \zeta(\rho) - (n-1)\zeta(\frac{1-\rho}{n-1})$$

$$\text{subject to} \qquad \rho \geq 0 \tag{A.81}$$

We first show that the utility of agent i with respect to q' is always concave if Assumption 3 holds. Using Proposition 3.1, we can rewrite the utility of agent i as follows:

$$u_i(A, (q', \mathbf{q}^e_{n-1}), \Phi) = 1 - (1-q')(\rho\frac{n}{n-1}(1-\hat{P}(n)) + \frac{1}{n-1}(n\hat{P}(n) - 1)) - c(q'). \tag{A.82}$$

Hence, we have

$$\frac{\partial^2}{\partial q'^2} u_i(A, (q', \mathbf{q}^e_{n-1}), \hat{1}_n) = -c''(q') + \frac{n}{n-1}(\hat{P}(n) - 1)\left(-2\frac{\partial \rho}{\partial q'} + \frac{\partial^2 \rho}{\partial q'^2}(1-q')\right). \tag{A.83}$$

We next show that if Assumption 3 holds, $\frac{\partial \rho}{\partial q'} < 0$ and $\frac{\partial^2 \rho}{\partial q'^2} > 0$. Showing these two inequalities, in combination with the fact that $\tilde{P}(A, q, \Phi) \leq 1$ will guarantee that the utility of agent i is concave.

Applying the optimality condition of ρ on Eq. (A.81), we obtain

$$\hat{P}(n-1)(q^e - q') = \zeta'(\rho) - \zeta'(\frac{1-\rho}{n-1}). \tag{A.84}$$

Using Eq. (A.84), we can restate $\frac{\partial \rho}{\partial q'}$ and $\frac{\partial^2 \rho}{\partial q'^2}$ as follows:

$$\frac{\partial \rho}{\partial q'} = \frac{-\hat{P}(n-1)}{\zeta''(\rho) + \frac{1}{n-1}\zeta''(\frac{1-\rho}{n-1})}, \tag{A.85}$$

$$\frac{\partial^2 \rho}{\partial q'^2} = \frac{(\frac{\partial \rho}{\partial q'})^2 \left(-\zeta'''(\rho) + \frac{1}{(n-1)^2}\zeta'''(\frac{1-\rho}{n-1})\right)}{\zeta''(\rho) + \frac{1}{n-1}\zeta''(\frac{1-\rho}{n-1})}. \tag{A.86}$$

Assuming that $\zeta()$ is convex, using Eq. (A.85) it immediately follows that $\frac{\partial \rho}{\partial q'} < 0$. Furthermore, assuming that $n \geq \sqrt{\frac{\alpha}{\beta}} + 1$, using Eq. (A.85) and if Assumption 3 holds, we obtain $\frac{\partial^2 \rho}{\partial q'^2} > 0$. Combining these two inequalities with Eq. (A.83), it implies that given a symmetric random network, if Assumption 3 holds then $\frac{\partial}{\partial^2 q'} u(A, (q', q^e), \Phi) < 0$. Furthermore, using Eq. (A.84), one can show that ρ is continuous in $(q', \mathbf{q}^e)$, therefore $u(A, (q', \mathbf{q}^e), \Phi)$ is continuous in $(q', \mathbf{q}^e)$, completing the proof.

∎

Proof of Theorem 7.4. As was shown in Theorem 7.3 if Assumption 3 holds, for symmetric large networks the utility of each agent is always concave. We first study the symmetric socially optimal solution. Let us denote the symmetric socially optimal security level by q^s. In the symmetric socially optimal solution we have:

$$c'(q^s) = \tilde{P}(A, \mathbf{q}^s_{n-1}, \hat{1}_n) - (1 - q^s)\frac{\partial}{\partial q^s}\tilde{P}(A, \mathbf{q}^s_{n-1}, \hat{1}_n).$$

We next consider the symmetric equilibrium. Since all agents play the same strategy we have $\rho = \frac{1}{n}$. Let us call the symmetric equilibrium security level, q^e. Using Eq. (A.82), we can rewrite the first order condition in the equilibrium as follows:

$$c'(q^e) = \tilde{P}(A, \mathbf{q}^e_{n-1}, \hat{1}_n) - (1 - q^e)(\frac{n}{n-1}(1 - \tilde{P}(A, \mathbf{q}^e_{n-1}, \hat{1}_n))\frac{\partial \rho}{\partial q'}|_{q'=q^e}).$$

Applying Eq. (A.85) to the preceding equation, we obtain

$$c'(q^e) = \tilde{P}(A, \mathbf{q}^e_{n-1}, \hat{1}_n) + (1 - q^e)((1 - \tilde{P}(A, \mathbf{q}^e_{n-1}, \hat{1}_n))\frac{E_{v\in V}[\tilde{P}(A_{-v}, \mathbf{q}^e_{n-2}, \hat{1}_n)]}{\zeta''(\frac{1}{n})}).$$

Knowing that the utility of each agent with respect to his security level is concave, to show that $q^e \geq q^s$ it is enough to show that:

$$\tilde{P}(A, \mathbf{q}^s_{n-1}, \hat{1}_n) + (1 - q^s)((1 - \tilde{P}(A, \mathbf{q}^s_{n-1}, \hat{1}_n))\frac{E_{v\in V}[\tilde{P}(A_{-v}, \mathbf{q}^s_{n-2}, \hat{1}_n)]}{\zeta''(\frac{1}{n})})$$
$$\geq \tilde{P}(A, \mathbf{q}^s_{n-1}, \hat{1}_n) - (1 - q^s)\frac{\partial}{\partial q^s}\tilde{P}(A, \mathbf{q}^s_{n-1}, \hat{1}_n).$$

We first show that $-\frac{\partial}{\partial q^s}\tilde{P}(A, \mathbf{q}^s_{n-1}, \hat{1}_n) \leq \frac{n\tilde{P}(A,\mathbf{q}^s_{n-1},\hat{1}_n)}{1-q^s}$ in the symmetric settings for the symmetric security profile $\mathbf{q}^s_n$. For a given symmetric security profile $\mathbf{q}_n$ we can rewrite $\tilde{P}(A, \mathbf{q}_{n-1}, \hat{1}_n)$ as follows:

$$\begin{aligned}
\tilde{P}(A, \mathbf{q}_{n-1}, \hat{1}_n) &= \sum_{i=0}^{n-1} b_i q^i (1-q)^{n-i-1}, \\
\frac{\partial}{\partial q}\tilde{P}(A, \mathbf{q}_{n-1}, \hat{1}_n) &= \sum_{i=1}^{n-1} i b_i q^{i-1}(1-q)^{n-i-1} - \sum_{i=0}^{n-2}(n-i-1) b_i q^i (1-q)^{n-i-2} \\
&\geq -\sum_{i=0}^{n-2}(n-i-1) b_i q^i (1-q)^{n-i-2} \\
&\geq -n \sum_{i=0}^{n-2} b_i q^i (1-q)^{n-i-2} \\
&\geq \frac{-n}{1-q} \sum_{i=0}^{n-2} b_i q^i (1-q)^{n-i-1} \\
&\geq \frac{-n}{1-q} \tilde{P}(A, \mathbf{q}_{n-1}, \hat{1}_n).
\end{aligned}$$

Now the condition that should be satisfied will be reduced to,

$$((1 - \tilde{P}(A, \mathbf{q}^s_{n-1}, \hat{1}_n))\frac{E_{v\in V}[\tilde{P}(A_{-v}, \mathbf{q}^s_{n-2}, \hat{1}_n)]}{\zeta''(\frac{1}{n})}) \geq \frac{n\tilde{P}(A, \mathbf{q}^s_{n-1}, \hat{1}_n)}{1-q^s}.$$

Put differently, it is sufficient to show that

$$n\zeta''(\frac{1}{n}) \leq (1-q^s)((1 - \tilde{P}(A, \mathbf{q}^s_{n-1}, \hat{1}_n))\frac{E_{v\in V}[\tilde{P}(A_{-v}, \mathbf{q}^s_{n-2}, \hat{1}_n)]}{\tilde{P}(A, \mathbf{q}^s_{n-1}, \hat{1}_n)}.$$

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

$$\begin{aligned}
\frac{1}{n} &\leq \tilde{P}(A, \mathbf{q}^s_{n-1}, \hat{1}_n) \leq \frac{1}{n} + \frac{n-1}{n}(1-q^s), \\
\frac{1}{n} &\leq E_{v\in V}[\tilde{P}(A_{-v}, \mathbf{q}^s_{n-2}, \hat{1}_n)] \leq \frac{1}{n} + \frac{n-2}{n}(1-q^s).
\end{aligned}$$

Using the preceding inequalities, it is easy to show that

$$\begin{aligned}
R &\geq \frac{1}{n}(1-q^s)(\frac{1}{\frac{1}{n} + \frac{n-1}{n}(1-q^s)} - 1) \\
&= \frac{n-1}{n}\frac{q^s(1-q^s)}{1+(n-1)(1-q^s)}.
\end{aligned}$$

One can easily show that the above function is increasing between between $q^s \in [0, 1 - \frac{1}{\sqrt{n+1}}]$ and decreasing between $q^s \in (1 - \frac{1}{\sqrt{n+1}}, 1]$. Furthermore, assuming that q^s is the socially optimal solution we have

$$c'^{-1}(\frac{1}{n}) \leq q^s \leq c'^{-1}(n).$$

We then consider the following cases:

- $c'^{-1}(n) \leq 1 - \frac{1}{\sqrt{n+1}}$,
- $c'^{-1}(\frac{1}{n}) \geq 1 - \frac{1}{\sqrt{n+1}}$,
- $c'^{-1}(\frac{1}{n}) \leq 1 - \frac{1}{\sqrt{n+1}} \leq c'^{-1}(n)$.

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,

$$\zeta''(\frac{1}{n}) \leq \frac{n-1}{n^2} \frac{c'^{-1}(\frac{1}{n})(1 - c'^{-1}(\frac{1}{n}))}{1 + (n-1)(1 - c'^{-1}(\frac{1}{n}))}.$$

Second scenario, will be reduced to:

$$\zeta''(\frac{1}{n}) \leq \frac{n-1}{n^2} \frac{c'^{-1}(n)(1 - c'^{-1}(n))}{1 + (n-1)(1 - c'^{-1}(n))}.$$

And the third scenario will be reduced to

$$\zeta''(\frac{1}{n}) \leq \min(\frac{n-1}{n^2} \frac{c'^{-1}(n)(1 - c'^{-1}(n))}{1 + (n-1)(1 - c'^{-1}(n))}, \frac{n-1}{n^2} \frac{c'^{-1}(\frac{1}{n})(1 - c'^{-1}(\frac{1}{n}))}{1 + (n-1)(1 - c'^{-1}(\frac{1}{n}))}).$$

Next, we show that when $\zeta''(\frac{1}{n}) \geq \frac{1}{n}$ then underinvestment always happen. We first show that in the symmetric socially optimal solution, we have

$$\tilde{P}(A, \mathbf{q}^s_{n-1}, \hat{1}_n) - (1 - q^s) \frac{\partial}{\partial q^s} \tilde{P}(A, \mathbf{q}^s_{n-1}, \hat{1}_n) \geq 2\tilde{P}(A, \mathbf{q}^s_{n-1}, \hat{1}_n).$$

Let s denote the seed node. Using Eq. (3.3) for an agent i in the symmetric socially optimal security profile, we have

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

where the last inequality follows from Theorem 7.1. Since under Assumption 3, the utility of each agent with respect to his security level is concave, to guarantee that $q^e \leq q^s$, it suffice to show that

$$
\begin{aligned}
\tilde{P}(A,\mathbf{q}^s_{n-1},\hat{1}_n)+(1-q^s)((1-\tilde{P}(A,\mathbf{q}^s_{n-1},\hat{1}_n))\frac{E_{v\in V}[\tilde{P}(A_{-v},\mathbf{q}^s_{n-2},\hat{1}_n)]}{\zeta''(\frac{1}{n})})\\
\leq 2\tilde{P}(A,\mathbf{q}^s_{n-1},\hat{1}_n).
\end{aligned}
$$

Assuming $\zeta''(\frac{1}{n})\geq 1$, the preceding relation always hold.

∎

A.11 Examples

Example A.1. Consider the network A in Fig. 6. Let $n=100$, $q_a=q_{a_1}=q_{a_2}=0.5$, and $q_b=q_{b_1}=\ldots=q_{b_{n-2}}=0.25$. Suppose also $\Phi_i=0.01$ for all $i=1,\ldots,100$. We show that $C_I(a_1,A)<C_I(a_1,A_{-a_2})$. By definition, we have

$$
\begin{aligned}
C_I(a_1,A)&=P_{a_1}(A,\mathbf{q},\Phi)+\sum_{j\in V-\{a_1\}}(1-q_j)(1-q_{a_1})Q_{j,a_1}(A,\mathbf{q}_{-\{a_1,j\}},\Phi)\\
&=(1-q_a)\left(\tilde{P}_{a_1}(A,\mathbf{q}_{-\{a_1\}},\Phi)+\sum_{j\in V-\{a_1\}}(1-q_j)Q_{j,a_1}(A,\mathbf{q}_{-\{a_1,j\}},\Phi)\right).
\end{aligned}
$$

The network effect on a_1 can be written as

$$
\tilde{P}_{a_1}(A,\mathbf{q}_{-\{a_1\}},\Phi)=\frac{1}{n}(1+(n-2)(1-q_b)+(1-q_a)(1-q_b^{n-2})).
$$

The second term on the right hand side of this equation corresponds to the event that the seed agent is in $\{b_1,\ldots,b_n\}$ and is susceptible and the third term to the event that the seed agent is a_2, is susceptible and at least one agent in set $\{b_1,\ldots,b_n\}$ is susceptible. Also for each $j\in\mathbf{B}=$

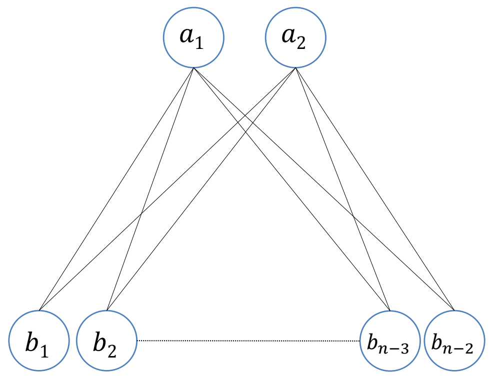

Figure 6: *For the security profile* $\mathbf{q}$ *where* $q_a = q_{a_1} = q_{a_2} = 0.5$ *and* $q_b = q_{b_1} = \ldots = q_{b_{n-2}} = 0.25$, $C_I(a_1, A) < C_I(a_1, A_{-a_2})$.

$\{b_1, \ldots, b_{n-2}\}$, we have

$$Q_{j,a_1}(A, \mathbf{q}_{-\{a_1,j\}}, \Phi) = \frac{1}{n}(1 + (n-3)q_a(1-q_b)).$$

The first term on the right hand side of the above equation corresponds to the event that the seed agent is a_1 and the second term to the event that the seed agent is in $\mathbf{B} - \{j\}$ and a_2 is not susceptible. Similarly, we have

$$Q_{a_2,a_1}(A, \mathbf{q}_{-\{a_1,a_2\}}, \Phi) = \frac{1}{n}(1 - q_b^{n-2}).$$

The right hand side of the above equation is the probability of the event that the seed agent is a_1 and at least one of the agents in $\mathbf{B}$ is susceptible. Putting these equations together, we obtain

$$C_I(a_1, A) = \frac{1-q_a}{n}(1 + 2(n-2)(1-q_b) + 2(1-q_a)(1-q_b^{n-2}) + (n-2)(n-3)q_a(1-q_b)^2) \approx 14.112.$$

Using similar approach, we obtain

$$C_I(a_1, A_{-a_2}) = \frac{1-q_a}{n}(1 + 2(n-2)(1-q_b) + (n-3)(n-2)(1-q_b)^2) \approx 27.47.$$

Comparing the preceding equations, we observe that $C_I(a_1, A) < C_I(a_1, A_{-a_2})$.

Example A.2. Consider the 5-node star network given in Fig. 1. Let $c(q) = 0.2q^2(2.9 - 1.33q)$, and $\Phi_i = \frac{1}{5}$, for $i = 1, \ldots, 5$. Note that $c(q)$ is not sufficiently convex. One can verify that $\mathbf{q}^e = (0.2, 1, 1, 1, 1)$ is a pure-strategy Nash equilibrium security profile and $\mathbf{q}^s = (1, 0.2, 0.2, 0.2, 0.2)$ is a socially optimal security profile. The expected infections in the equilibrium is $I(A, \mathbf{q}^e, \Phi) = 0.16$. However, expected infections in the social optimum is $I(A, \mathbf{q}^s, \Phi) = 0.64$.