Internet Mathematics, 11:23–61, 2015

ISSN: 1542-7951 print/1944-9488 online
DOI: 10.1080/15427951.2013.830583

Taylor & Francis
Taylor & Francis Group

A STOCHASTIC MODEL OF ACTIVE CYBER DEFENSE DYNAMICS

Shouhuai Xu,[1] Wenlian Lu,[2,3] and Hualun Li[3]
[1]*Department of Computer Science, University of Texas at San Antonio, San Antonio, Texas, USA*
[2]*Department of Computer Science, University of Warwick, Coventry, UK*
[3]*School of Mathematical Sciences, Fudan University, Shanghai, P. R. China*

Abstract *The concept of active cyber defense has appeared in the literature in recent years. However, there are no mathematical models for characterizing the effectiveness of active cyber defense. In this paper, we fill the void by proposing a novel Markov process model that is native to the interaction between cyber attack and active cyber defense. Unfortunately, the native Markov process model cannot be tackled by techniques of which we are aware. We therefore simplify, via mean-field approximation, the Markov process model as a dynamical system model that is amenable to analysis. This allows us to derive a set of valuable analytic results that characterize the effectiveness of four types of active cyber defense dynamics. Simulations show that the analytic results are intrinsic to the native Markov process model, and therefore justify the validity of the dynamical system model. We also discuss side effects of the mean-field approximation and their implications.*

1. INTRODUCTION

The concept of *active cyber defense* (e.g., the use of "white" or "good" worms to identify and fight or kill malicious worms) has appeared in the literature in recent years. However, the exploration has primarily focused on legal and policy issues [1, 7, 19, 21, 24, 34, 43, 44]. On the other hand, active cyber defense has already been implemented in some sense (e.g., the `Welchia` worm attempted to "evict" the Blaster worm from infected computers [30, 34]), and full-fledged active cyber defense is seemingly inevitable in the near future [24, 36, 45]. It is therefore more imperative than ever to systematically characterize the effectiveness of active cyber defense. In this paper, we initiate the theoretical study of this aspect of cyber security, with emphasis on addressing the following basic question: How effective is active cyber defense? Such characterization studies not only will deepen our understanding of active cyber defense, but also will help in real-life decision-making (e.g., when to launch active cyber defense) and even policy-making (e.g., whether to launch active cyber defense at all).

Address correspondence to Shouhuai Xu, Department of Computer Science, University of Texas at San Antonio, San Antonio, TX 78249, USA. E-mail: shxu@cs.utsa.edu

Color versions of one or more of the figures in the article can be found online at www.tandfonline.com/uinm.

1.1. Our Contributions

In this paper we have formulated, to the best of our knowledge, the first mathematical model for characterizing the effectiveness of active cyber defense. The interaction between cyber attack and active cyber defense can be naturally modeled as a Markov process (Section 2). Unfortunately, we do not know how to tackle the native Markov process analytically because all the techniques we are aware of do not appear to be applicable (see Section 1.2 for discussion). We therefore simplify, via the mean-field approximation, the native Markov process model as a dynamical system model that is amenable to analysis. In the dynamical system model, we obtain a set of analytic results (Sections 4–6). We then use simulations to validate the accuracy of the dynamical system model (Section 8). Simulations show that the analytic results derived from the dynamical system model are intrinsic to the native Markov process model, and that the accuracy of the dynamical system model, in terms of *dynamics accuracy* and *threshold accuracy* (which will be specified in Section 8), increases with the average node degree. Moreover, the analytic results lead to various insights, with some highlighted (informally) as follows:

- If neither the defender nor the attacker is superior to, or more advanced than, its opponent in terms of cyber combat power (Type-I and Type-II dynamics with a certain threshold), the effectiveness of active cyber defense will depend on (in some quantitative fashion we derive) (i) the attack–defense network structure, (ii) the initial security state of the attack–defense network, (iii) the attacker's and defender's combat power, and (iv) the attacker/defender strategy. We also characterize the benefit to the *strategic* attacker/defender that initially "occupies" the large-degree nodes. Specifically, we show the following: (i) when the attack–defense network structures are Erdős–Rényi (ER) random graphs, a strategic defender/attacker does not gain significant benefit; (ii) when the attack–defense network structures are power-law graphs, a strategic defender/attacker gains significant benefit.[1] Moreover, we obtain the following quantitative result: The benefit to a strategic defender is maximized for the subclass of power-law graphs with exponent $\gamma = 2$. These are described in Sections 4 and 5.
- If the defender is superior to (or more advanced than) the attacker in terms of cyber combat power (Type-III dynamics), the defender can always use active cyber defense to *automatically* "clean up" (i.e., cure) the entire network, regardless of the attack–defense network structure and regardless of whether the attacker is strategic. This suggests that cyber superiority could serve as an effective deterrence, and can be seen as a consequence due to the lack of a certain threshold in the combat-power function. The explorations of Type-III dynamics and its dual, Type-IV dynamics, are described in Section 6.
- As discussed in Section 7, active cyber defense can eliminate the asymmetry that is an intrinsic weakness of reactive cyber defense, where the defender runs antivirus-software-like tools on each computer to detect and cure infections caused by attacks or malware that have penetrated the defense perimeter, such as firewalls. The cause of the asymmetry is that when the defense is reactive, the attack effect is automatically amplified by the network (a kind of network effect).

We stress that the focus of the present paper is to characterize the effectiveness of active cyber defense. This means that we should not make any significant restrictions on

[1]These results are reminiscent of, and in parallel to, the *connectivity-based* robustness characterizations of ER and power-law graphs [2], which is, however, a different perspective from ours because the attacker in our model aims to compromise as many nodes as possible but does not delete any (of the compromised) nodes.

the parameter regimes and network structures. One important research problem, which is orthogonal to our focus and is not addressed in the present paper, is how to extract model parameters and an attack–defense network structure for a given cyber system. In principle, the model parameters can be obtained by analyzing the strengths and weaknesses of the attack and defense tools ("what if" analysis can be used in the absence of sufficient data) and/or observing the outcome of experimental cyber combat.

The network structure can be derived from the cyber system configurations and security policies, which may restrict which computers can directly communicate with which other computers. The characterization results presented in this paper accommodate a large class of parameter and structure scenarios.

1.2. Related Work

We classify related prior work based on two perspectives: one with respect to the problem that is under investigation, and the other to the technique that is exploited to tackle the problem.

From the perspective of the problem under investigation, we note that all existing studies in both the mathematics literature and the physics literature are geared toward, in the terms of the present paper, characterizing the outcome of *reactive* defense under various parameter conditions (see, for example, [3, 4, 6, 8, 9, 12, 13, 28, 29, 40, 42, 46] and the references therein). These studies substantially generalize the pioneering work of [16, 17], which was based on homogeneous epidemic models in biological systems [14, 18, 25]. For example, even for the very recent work [46], which studies the attack–defense dynamics between one defender and multiple attackers that fight against each other as well, the defense is still *reactive*.

In contrast, the present paper introduces a new research problem, namely characterizing the outcome of *active* defense under various model parameter conditions (including the graph/network structure). To the best of our knowledge, we are the first to study the active cyber defense problem mathematically, despite the fact that the technical practice of active cyber defense has been discussed for years [1, 7, 19, 21, 24, 34, 43, 44]. This is so even though our active cyber defense model is reminiscent of the *voter model* (see, for example, [12, 23, 33, 35, 37]), whereby each node can adopt the state of one of its random neighbors at each time step. However, the voter model corresponds to the special case of our active cyber defense model with *linear* combat-power functions (the concept of combat-power functions will be introduced later).

In contrast, we study general *nonlinear* combat-power functions, which explains why the techniques for analyzing the voter model cannot tackle our active cyber defense model (see Section 2.2 for further discussion).

Finally, it is worth mentioning that active cyber defense is different from automatic patching [41], because the attacker may have already compromised many computers, and that our active cyber defense model is different from the Moran process [27, 31], which considers the mutation dynamics of homogeneous nodes.

From the perspective of the techniques that are exploited to tackle the epidemic problem with network structures [3, 4, 6, 8, 9, 13, 28, 29, 40, 42, 46], there are mainly two approaches. The first is to use mean-field approximation (e.g., [32]). Our dynamical system model is also based on mean-field approximation of a native stochastic process model. Mean-field approximation is a plausible first step in studying problems such as the stochastic active cyber defense process we introduce in the present paper. Nevertheless, we empirically characterize the accuracy of the mean-field approximations.

The second approach is to directly tackle the native processes that take place on network structures. This approach is more rigorous than the mean-field approximation approach, but is often pursued after some understanding based on the mean-field approach has been established.

This approach is valuable not only because it can derive rigorous results, but also because it can (in)validate some results obtained via the mean-field models. For example, the threshold behavior and the final outcome of the SIR (susceptible–infectious–removed) epidemic process on random networks with clusters (communities) are studied in [3, 4], which consider the SIR epidemic process in two steps: the SIR epidemic spreading within clusters (local spreading) and then the SIR epidemic spreading across clusters. For those studies, it is reasonable to use the branching process approximation, because it is necessary to consider only the case of small initial infections (i.e., early stage of epidemic spreading) and because the notion of *offspring generation* is well defined in SIR models. The authors derive a rigorous central limit theorem under certain conditions.

In another line of investigation, [6] investigates the SIS (susceptible–infectious–susceptible) contact process [20] on random graphs that are generated via preferential attachment [5]. That rigorous study confirms the threshold result of [32] obtained via mean-field approximation, namely that the epidemic threshold of scale-free networks is 0.

In [9], the authors study both SIR and SIS models on random graphs with power-law degree distributions. Improving on some results in [9], it is shown in [28] that the epidemic extinction time for the contact process on power-law random graphs grows exponentially in the number of nodes, and in [29], bounds are obtained on the density of infected nodes.

The rest of the paper is organized as follows. In Section 2, we present the native Markov process model and then show how to simplify it as a dynamical system model that is amenable to analysis. In Section 3, we briefly review some background knowledge. In Sections 4–6, we characterize four types of active cyber defense dynamics. In Section 7, we explain why active cyber defense can eliminate an intrinsic weakness of reactive cyber defense. In Section 8, we use simulations to show that the analytic results derived from the dynamical system model are intrinsic to the native Markov process model. In Section 9, we conclude the paper with future research directions. Lengthy proofs are deferred to an appendix.

2. ACTIVE CYBER DEFENSE MODEL

A cyber system consists of networked computers/nodes of finite populations. A computer has two states: compromised and secure (i.e., vulnerable but not compromised). We may say that a compromised computer is "occupied" by an adversary/attacker, and a secure computer is "occupied" by the defender. The adversary can compromise a computer by exploiting its (e.g., zero-day or unpatched) vulnerabilities. Attacks are malware-like, meaning that compromised computers can attack vulnerable computers in an epidemic-spreading fashion. With active cyber defense, the defender can spread "good worm"-like mechanisms in networks (just as the malicious worms spread) to identify and "clean up" the compromised computers.

The interaction between cyber attack and active cyber defense creates an attack–defense interaction structure, a graph topology that represents how the compromised nodes attack the secure nodes and how the secure nodes use active cyber defense to clean up the compromised nodes. We say that a defender (attacker) is *strategic* if it initially occupies the large-degree nodes in the graph with higher probabilities. The attack–defense interaction leads to the evolution of the cyber security state of the entire cyber system. We illustrate the

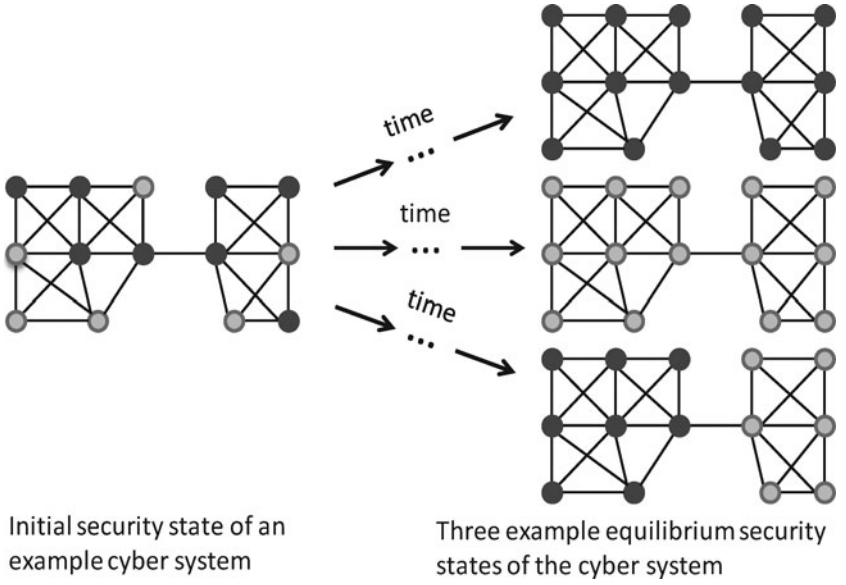


Figure 1 Illustration of cyber security state evolution under active cyber defense, where the same initial state may evolve, under different conditions, toward one of the three example equilibrium states—all nodes are secure (filled circles); all nodes are compromised (open circles); some nodes are secure. The core research issue is to characterize how the initial state, network topology, parameters, and attacker/defender strategies can govern the evolution.

state evolution in Figure 1, where a filled circle means "secure" and an open circle means "compromised." As shown in Figure 1, the state evolution can exhibit rich phenomena (e.g., the existence of multiple kinds of equilibria). At a high level, the research objective is to characterize how the evolution is governed by the initial state, graph topology, parameters, and attacker/defender strategies. The characterization will allow us to answer some basic questions such as under what conditions the cyber security state evolves toward an all-secure equilibrium.

2.1. The Native Markov Process Model

Formally, cyber attack–defense takes place over a finite network/graph structure $G = (V, E)$, where $V = \{1, 2, \ldots, n\}$ is the set of nodes/computers and E is the set of edges/arcs with $(u, u) \notin E$ (i.e., there are no self-loops in the setting of the problem). At any point in time, a node $v \in V$ is in one of two states: `secure`, meaning that it is *secure* (i.e., vulnerable but not compromised by the attacker); or `compromised`, meaning that it is *compromised* by the attacker. Node v's state changes because of some u, where $(u, v) \in E$. Note that $(u, u) \notin E$, because a secure node will not clean itself up, and a compromised node will not attack itself.

Since our study applies to both undirected and directed graphs, we focus on undirected graphs while mentioning the differences between the two types as the need arises. We do not make any significant restrictions on G, because in real life, G can have any topology. This has become a standard practice in characterization studies of cyber security (see, for example, [8, 13, 40, 42, 46]).

The state of node $v \in V$ at time t is a random variable $\xi_v(t) \in \{0, 1\}$:

$$\xi_v(t) = \begin{cases} 1, & v \in V \text{ is secure at time } t, \\ 0, & v \in V \text{ is compromised at time } t. \end{cases}$$

Correspondingly, we define

$$B_v(t) = \mathsf{P}(\xi_v(t) = 1) \quad \text{and} \quad R_v(t) = \mathsf{P}(\xi_v(t) = 0).$$

Denote by $\tilde{\theta}_{v,\mathrm{BR}}(t)$ the rate at which v's state changes from `secure` to `compromised` at time t, which is a random variable because it depends on the states of v's neighbors. Similarly, denote by $\tilde{\theta}_{v,\mathrm{RB}}(t)$ the random rate at which v's state changes from `compromised` to `secure` at time t.

The state evolution of $v \in V$ is naturally described as a Markov process (dubbed "Markov process model" or "Markov model" for reference purposes) with the following transition probabilities:

$$\mathsf{P}(\xi_v(t + \Delta t) = 1 \mid \xi_v(t)) = \begin{cases} \Delta t \cdot \tilde{\theta}_{v,\mathrm{RB}}(t) + o(\Delta t), & \xi_v(t) = 0, \\ 1 - \Delta t \cdot \tilde{\theta}_{v,\mathrm{BR}}(t) + o(\Delta t), & \xi_v(t) = 1, \end{cases} \tag{2.1}$$

and

$$\mathsf{P}(\xi_v(t + \Delta t) = 0 \mid \xi_v(t)) = \begin{cases} \Delta t \cdot \tilde{\theta}_{v,\mathrm{BR}}(t) + o(\Delta t), & \xi_v(t) = 1, \\ 1 - \Delta t \cdot \tilde{\theta}_{v,\mathrm{RB}}(t) + o(\Delta t), & \xi_v(t) = 0, \end{cases} \tag{2.2}$$

as $\Delta t \to 0$. Denote by $N_v = \{u \in V : (u, v) \in E\}$ the set of neighbors of node $v \in V$. Since the random rates $\tilde{\theta}_{v,\mathrm{RB}}(t)$ and $\tilde{\theta}_{v,\mathrm{BR}}(t)$ are naturally determined by the random states of node v's neighbors, we use deterministic but possibly nonlinear functions $f_{\mathrm{RB}}(\cdot) : \mathbb{R} \to [0, 1]$ and $f_{\mathrm{BR}}(\cdot) : \mathbb{R} \to [0, 1]$ to define respectively the random rates $\tilde{\theta}_{v,\mathrm{RB}}(t)$ and $\tilde{\theta}_{v,\mathrm{BR}}(t)$, as follows:

$$\tilde{\theta}_{v,\mathrm{RB}}(t) = f_{\mathrm{RB}}\left(\frac{1}{\deg(v)} \sum_{u \in N_v} \xi_u(t)\right),$$

$$\tilde{\theta}_{v,\mathrm{BR}}(t) = f_{\mathrm{BR}}\left(\frac{1}{\deg(v)} \sum_{u \in N_v} (1 - \xi_u(t))\right).$$

We call $f_{\mathrm{RB}}(\cdot)$ and $f_{\mathrm{BR}}(\cdot)$ the *combat-power* functions, because they abstract the attacker's and defender's combat capabilities.

At this point, we do not know how to tackle the above native Markov process model. One may note that the above combat-power functions are reminiscent of the so-called voter model [12], whereby a node changes its opinion (or state) to the opinion of one random neighbor according to a *fixed-rate* Poisson process. This allows the model to be transformed into a *dual* process that works backward in time and becomes a random walk [12], which makes it tractable.

In contrast, in our model, a node changes its state according to a rate that is not fixed but instead depends *nonlinearly* on the states of its neighbors. This nonlinearity prevents us from transforming our native Markov process model into a random walk model, meaning that the technique used in [12] cannot solve the problem we encounter.

This nonlinearity-induced difficulty suggests to us that we should simplify/approximate the native Markov process model as a tractable dynamical system model.

2.2. Simplifying the Markov Process Model as a Dynamical System Model

Now we show how to simplify the native Markov process model into a tractable dynamical system model via the mean-field approximation. From (2.1), we have, for $v \in V$,

$$B_v(t+\Delta t) = \Delta t \cdot \tilde{\theta}_{v,\mathrm{RB}}(t) \cdot R_v(t) + (1 - \Delta t \cdot \tilde{\theta}_{v,\mathrm{BR}}(t)) B_v(t) + o(\Delta t),$$

which can be rewritten as

$$\frac{B_v(t+\Delta t) - B_v(t)}{\Delta t} = \tilde{\theta}_{v,\mathrm{RB}}(t) \cdot R_v(t) - \tilde{\theta}_{v,\mathrm{BR}}(t) \cdot B_v(t) + o(\Delta t).$$

Similarly, from (2.2), we can derive for all $v \in V$,

$$\frac{R_v(t+\Delta t) - R_v(t)}{\Delta t} = \tilde{\theta}_{v,\mathrm{BR}}(t) \cdot B_v(t) - \tilde{\theta}_{v,\mathrm{RB}}(t) \cdot R_v(t) + o(\Delta t).$$

By letting $\Delta t \to 0$, we have for all $v \in V$,

$$\begin{aligned} \frac{d}{dt} B_v(t) &= \tilde{\theta}_{v,\mathrm{RB}}(t) \cdot R_v(t) - \tilde{\theta}_{v,\mathrm{BR}}(t) \cdot B_v(t), \\ \frac{d}{dt} R_v(t) &= \tilde{\theta}_{v,\mathrm{BR}}(t) \cdot B_v(t) - \tilde{\theta}_{v,\mathrm{RB}}(t) \cdot R_v(t). \end{aligned} \tag{2.3}$$

Note that

$$\mathsf{E}\left(\tilde{\theta}_{v,\mathrm{RB}}(t)\right) = \mathsf{E}\left(f_{\mathrm{RB}}\left(\frac{1}{\deg(v)} \sum_{u \in N_v} \xi_u(t)\right)\right).$$

By the idea of mean-field approximation, we can move the expectation inside the combat-power function and replace the mean of the random rate $\tilde{\theta}_{v,\mathrm{RB}}(t)$, denoted by $\theta_{v,\mathrm{RB}}(t)$, with the following term:

$$f_{\mathrm{RB}}\left(\frac{1}{\deg(v)} \sum_{u \in N_v} \mathsf{E}\left[\xi_u(t)\right]\right) = f_{\mathrm{RB}}\left(\frac{1}{\deg(v)} \sum_{u \in N_v} B_u(t)\right).$$

We can treat $\tilde{\theta}_{v,\mathrm{BR}}(t)$ analogously. As a result, we obtain the mean state-transition probabilities $\theta_{v,\mathrm{RB}}(t)$ and $\theta_{v,\mathrm{BR}}(t)$ as

$$\theta_{v,\mathrm{RB}}(t) = f_{\mathrm{RB}}\left(\frac{1}{\deg(v)} \sum_{u \in N_v} B_u(t)\right) \text{ and } \theta_{v,\mathrm{BR}}(t) = f_{\mathrm{BR}}\left(\frac{1}{\deg(v)} \sum_{u \in N_v} R_u(t)\right).$$

Therefore, (2.3) becomes the following dynamical system model for all $v \in V$:

$$\begin{aligned} \frac{d}{dt} B_v(t) &= \theta_{v,\mathrm{RB}}(t) \cdot R_v(t) - \theta_{v,\mathrm{BR}}(t) \cdot B_v(t), \\ \frac{d}{dt} R_v(t) &= \theta_{v,\mathrm{BR}}(t) \cdot B_v(t) - \theta_{v,\mathrm{RB}}(t) \cdot R_v(t). \end{aligned} \tag{2.4}$$

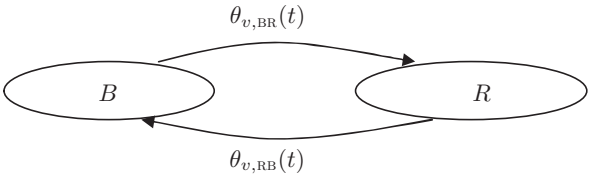
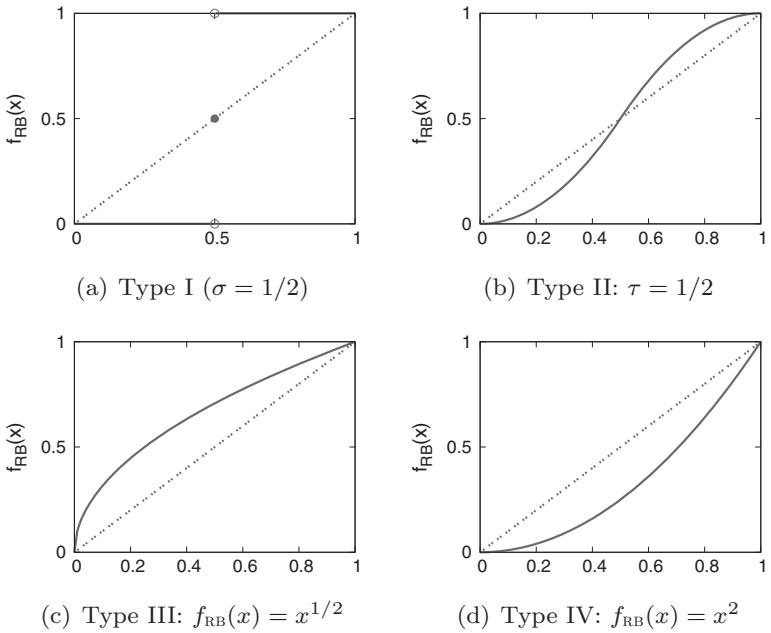


Figure 2 State-transition diagram of a single node $v \in V$ (B: `secure`; R: `compromised`).

Note that the dynamical system model for all $v \in V$ encodes the graph topology via parameters $\theta_{v,\mathrm{BR}}(t)$ and $\theta_{v,\mathrm{RB}}(t)$, which encode the information about node v's neighborhood (including the states of node v's neighbors). The corresponding *state-transition diagram* for a node $v \in V$ is depicted in Figure 2.

2.3. Instantiating the Dynamical System Model via Specific Combat-Power Functions

Recall that the combat-power function $f_{\mathrm{RB}}(\cdot)$ abstracts the defender's power against the attacker. It should satisfy the following properties: (i) $f_{\mathrm{RB}}(0) = 0$; (ii) $f_{\mathrm{RB}}(1) = 1$; (iii) $f_{\mathrm{RB}}(\cdot)$ increases monotonically. This is intuitive, because the more `secure` nodes surrounding an `compromised` node, the greater the chance the `compromised` node will become `secure` (because of the active defense launched by the `secure` nodes). In this paper, we consider four types of $f_{\mathrm{RB}}(\cdot)$ with examples depicted in Figure 3, where the first two types of $f_{\mathrm{RB}}(\cdot)$ have an intrinsic threshold, while the others do not.



(a) Type I ($\sigma = 1/2$) (b) Type II: $\tau = 1/2$

(c) Type III: $f_{\mathrm{RB}}(x) = x^{1/2}$ (d) Type IV: $f_{\mathrm{RB}}(x) = x^2$

Figure 3 $f_{\mathrm{RB}}(\cdot)$ examples (Type II: $f_{\mathrm{RB}}(x) = 2x^2$ for $x \in [0, 0.5]$, $f_{\mathrm{RB}}(x) = -2x^2 + 4x - 1$ for $x \in [0.5, 1]$).

Type I. For a given threshold $\sigma \in (0, 1)$, we define

$$\theta_{v,\mathrm{RB}}(t) = f_{\mathrm{RB}}\left(\frac{1}{\deg(v)}\sum_{u\in N_v} B_u(t)\right) = \begin{cases} 1, & \dfrac{1}{\deg(v)}\displaystyle\sum_{u\in N_v} B_u(t) > \sigma, \\ 0, & \dfrac{1}{\deg(v)}\displaystyle\sum_{u\in N_v} B_u(t) < \sigma, \\ \dfrac{1}{2} & \text{otherwise.} \end{cases} \tag{2.5}$$

Intuitively, the defender is more powerful than the attacker when $\sigma < \frac{1}{2}$, less powerful than the attacker when $\sigma > 1/2$, and equally powerful as the attacker when $\sigma = 1/2$.

Type II. For a given threshold $\tau \in (0, 1)$, we define $f_{\mathrm{RB}}(x)$ to be convex and $f_{\mathrm{RB}}(x) < x$ for $x \in [0, \tau)$; $f_{\mathrm{RB}}(x)$ to be concave and $f_{\mathrm{RB}}(x) > x$ for $x \in (\tau, 1]$; $f_{\mathrm{RB}}(x) = x$ for $x = \tau$, $f_{\mathrm{RB}}(0) = 0$, and $f_{\mathrm{RB}}(1) = 1$. Moreover, $f_{\mathrm{RB}}(\cdot)$ is increasing and continuous in intervals $[0, \tau)$ and $(\tau, 1]$. Such functions are known as "sigmoid" functions. Intuitively, the defender is more powerful than the attacker when $\tau < 1/2$, less powerful than the attacker when $\tau > 1/2$, and equally powerful as the attacker when $\tau = 1/2$.

Type III. $f_{\mathrm{RB}}(\cdot)$ is concave, continuous, and increasing in $[0, 1]$, $f_{\mathrm{RB}}(x) > x$ for $s \in (0, 1)$, and $f_{\mathrm{RB}}(0) = 0$, $f_{\mathrm{RB}}(1) = 1$. Intuitively, the defender is more advanced than the attacker (i.e., the defender has cyber-combat superiority).

Type IV $f_{\mathrm{RB}}(\cdot)$ is convex, continuous, and increasing in $[0, 1]$, $f_{\mathrm{RB}}(x) < x$ for $x \in (0, 1)$, and $f_{\mathrm{RB}}(0) = 0$, $f_{\mathrm{RB}}(1) = 1$. Intuitively, the defender is less advanced than the attacker. Note that a Type-IV $f_{\mathrm{RB}}(\cdot)$ is dual to a Type-III $f_{\mathrm{RB}}(\cdot)$.

Based on the above four types of combat-power functions, we focus on the four types of combat-function combinations that satisfy

$$\theta_{v,\mathrm{BR}}(t) = 1 - \theta_{v,\mathrm{RB}}(t). \tag{2.6}$$

By combining (2.4) and (2.6), we obtain the following master equation for a *single* node $v \in V$:

$$\frac{d}{dt}B_v(t) = \theta_{v,\mathrm{RB}}(t)(1 - B_v(t)) - \theta_{v,\mathrm{BR}}(t)B_v(t) = \theta_{v,\mathrm{RB}}(t) - B_v(t). \tag{2.7}$$

The research task is to characterize Type-I–Type-IV dynamics, namely the dynamics of master equation (2.7) with Type-I–Type-IV combat-power functions, respectively. For example, for the Type-I combat-power function, we have

$$\theta_{v,\mathrm{BR}}(t) = f_{\mathrm{BR}}\left(\frac{1}{\deg(v)}\sum_{u\in N_v}[1 - B_u(t)]\right) \tag{2.8}$$

$$= \begin{cases} 1, & \dfrac{1}{\deg(v)}\displaystyle\sum_{u\in N_v}[1 - B_u(t)] > 1 - \sigma, \\ 0, & \dfrac{1}{\deg(v)}\displaystyle\sum_{u\in N_v}[1 - B_u(t)] < 1 - \sigma, \\ \dfrac{1}{2}, & \text{otherwise.} \end{cases}$$

$G = (V, E)$	graph/network that abstracts a cyber system from a cyber security perspective, where $\|V\| = n$
N_v	$N_v = \{u \in V : (u, v) \in E\}$
$\deg(v)$	v's (in)degree, $\deg(v) = \|N_v\|$
γ	power-law exponent, $\mathsf{P}(\deg(v) = k) \propto k^{-\gamma}$
σ, τ	indicator of defender's relative combat-power in Type-I and Type-II dynamics, respectively
$\xi_v(t)$	state of node v at time t: `secure` (i.e., 1 or "secure") and `compromised` (i.e., 0 or "compromised")
$B_v(t)$	probability $v \in V$ is `secure` at time t
$R_v(t)$	probability $v \in V$ is `compromised` at time t
α	$\alpha = \frac{1}{n}\sum_{v\in V} B_v(0)$, the average fraction of `secure` nodes at time $t = 0$
S	random set of `secure` nodes at time $t = 0$
$\theta_{v,\mathrm{BR}}(t)$	probability that node v's state changes from `secure` to `compromised` at time t
$\theta_{v,\mathrm{RB}}(t)$	probability that node v's state changes from `compromised` to `secure` at time t

Table I Major notation used throughout the article.

We want to characterize, among other things, the roles of the *thresholds* specified in Type-I and Type-II dynamics, and the consequences due to the lack of such thresholds in dynamics of Types III and IV.

Summary of notation. Let $\mathbb{R}$ denote the set of real numbers, $\mathsf{P}(\cdot)$, $\mathsf{E}(\cdot)$, $\mathsf{Var}(\cdot)$ the probability, expectation, and variance functions, respectively. Other major notation is summarized in Table I.

3. PRELIMINARIES

3.1. Arbitrary Networks

By "arbitrary network" we mean a *given* network $G = (V, E)$ that may or may not have a special structure/topology of interest. Most analytic results in this paper are derived from dynamical systems that take place on arbitrary networks. In general, such results are often independent of the statistical properties of the networks (e.g., the degree distribution).

In order to show the existence of the third kind of equilibrium illustrated in Figure 1 (i.e., some nodes `secure` and the other nodes `compromised`), we also consider a given network that has a cluster (or community) structure. A network $G = (V, E)$ has a clustered structure of $V_1, V_2, \ldots, N_K$ if $\bigcup_i V_i = V$, $V_i \bigcap V_j = \emptyset$ for all $i \neq j$, and the nodes belonging to V_i are better connected than the nodes crossing V_i and V_j for every $i \neq j$. More specifically, this special phenomenon is related to the minimum node expansion in cluster V_k for $1 \leq k \leq K$, which is defined as

$$\beta_k = \inf_{v\in V_k} \frac{\left|N_v \bigcap V_k\right|}{\deg(v)}, \quad \text{where } N_v = \{u : (u, v) \in E\}. \tag{3.1}$$

3.2. Generalized Random Graphs

In order to characterize the benefit to the *strategic* defender who initially occupies the large-degree nodes with greater probabilities (a scenario that is often difficult to analyze), we propose to use the generalized random graph model [11]. This means that the result is applicable to a class of random networks (which, however, include the Erdős–Rényi (ER) random graphs and power-law random graphs [11]), rather than arbitrary networks; this slight restriction is compensated with some valuable analytic results. (Characterizing the benefit to the strategic defender in arbitrary networks is left as an open problem.)

In the generalized random graph model, we are given an expected (in)degree sequence $(d_1(n), \ldots, d_n(n))$ that defines a family of graphs. Let $d_{\min}(n) = \min\{d_j(n) : 1 \leq j \leq n\}$ and $d_{\max}(n) = \max\{d_j(n) : 1 \leq j \leq n\}$. A random graph instance $G(n) = (V(n), E(n))$ can be obtained by linking each pair of nodes (u, v) with probability

$$p_{vu}(n) = \frac{d_u(n)d_v(n)}{\sum_{k=1}^{n} d_k(n)} \tag{3.2}$$

independently of the others [11], where $0 \leq p_{vu}(n) \leq 1$ under the assumption $(d_{\max}(n))^2 \leq \sum_{k=1}^{n} d_k(n)$.

For simplifying the analysis, we allow self-links while noting that our result can be adapted to accommodate the fact that there are no self-links. In order to attain deeper insight, we will consider two instantiations of the generalized random graph model, namely, the classic Erdős–Rényi (ER) random graphs with $d_1(n) = \cdots = d_n(n)$ or edge probability $p = d_1(n)/n$, and the ubiquitous power-law random graphs with $\#\{v \in V : \deg(v) = k\}/\#V \propto k^{-\gamma}$ for some $\gamma > 0$. Note that γ does not need to be greater than 1, because $d_{\max}(n)$ is finite.

Note that complete graphs are a special case of arbitrary networks and of generalized random graphs. Since the theorems we present below hold both for arbitrary networks and for generalized random graphs, they automatically apply to complete graphs.

4. CHARACTERIZING TYPE-I ACTIVE CYBER DEFENSE DYNAMICS

In this section, we first characterize Type-I active cyber defense dynamics with a *nonstrategic* defender in arbitrary networks, where the initial occupation probability $B_v(0)$ is identical for all nodes. We then investigate the more difficult case of a *strategic* defender with degree-dependent $B_v(0) \propto \deg(v)$ in the generalized random graph model, where the defender initially occupies the large-degree nodes with higher probabilities (i.e., the large-degree nodes are appropriately better protected).

4.1. Characterizing Type-I Dynamics with a Nonstrategic Defender

Type-I dynamics with a nonstrategic defender is characterized through Theorems 4.1–4.6. The characterizations include the conditions under which the defender can or cannot use active cyber defense to automatically clean up the entire network, and a method for deciding whether an equilibrium is stable. Theorem 4.2 requires the following lemma, whose proof is omitted because it is similar to (and simpler than) the proof of Lemma 5.1 that is given in Section 10.3.

Lemma 4.1. *Consider Type-I dynamics with threshold σ and system* (2.7) *in an arbitrary network $G = (V, E)$:*

(i) If $\frac{1}{\deg(v)} \sum_{u \in N_v} B_u(0) > \sigma$ holds for all $v \in V$, then $\frac{1}{\deg(v)} \sum_{u \in N_v} B_u(t) > \sigma$ holds for all $v \in V$ and $t \geq 0$, and $\min_{v \in V} B_v(t)$ increases monotonically.
(ii) If $\frac{1}{\deg(v)} \sum_{u \in N_v} B_u(0) < \sigma$ holds for all $v \in V$, then $\frac{1}{\deg(v)} \sum_{u \in N_v} B_u(t) < \sigma$ holds for all $v \in V$ and $t \geq 0$, and $\max_{v \in V} B_v(t)$ decreases monotonically.

Theorem 4.2. (A sufficient condition under which the defender or the attacker will occupy the entire network.) *Consider Type-I dynamics with threshold σ and arbitrary network $G = (V, E)$. If $\frac{1}{\deg(v)} \sum_{u \in N_v} B_u(0) > \sigma$ for all $v \in V$, then $\lim_{t \to \infty} B_v(t) = 1$. If $\frac{1}{\deg(v)} \sum_{u \in N_v} B_u(0) < \sigma$ for all $v \in V$, then $\lim_{t \to \infty} B_v(t) = 0$.*

Proof. We prove only the first part, because the second part can be proved analogously. According to Lemma 4.1, we know that $\frac{1}{\deg(v)} \sum_{u \in N_v} B_u(t) > \sigma$ for all $t \geq 0$ and $v \in V$. This and (2.5) imply that $\theta_{v,\mathrm{RB}}(t) = 1$ for all $t \geq 0$ and $v \in V$. Thus, system (2.7) becomes

$$\frac{dB_v(t)}{dt} = \theta_{v,\mathrm{RB}}(t) - B_v(t) = 1 - B_v(t).$$

This leads to $B_v(t) = \exp(-t)B_v(0) + 1 - \exp(-t)$ and thus $\lim_{t \to \infty} B_v(t) = 1$. □

Theorem 4.2 holds for arbitrary networks, including the special case of complete graphs. Theorem 4.2 leads to the following insight (informally stated).

Insight 4.3. There is a quantitative relationship between the initial network security state and the combat-power function as indicated by the threshold σ in a Type-I combat-power function. Specifically, when neither the defender nor the attacker is superior to its opponent, active cyber defense can automatically clean up a compromised network only when the defender has occupied more than a threshold proportion σ of the network (or nodes). This means that the defender may need to clean up some compromised nodes manually before using active cyber defense to clean up the entire network automatically.

Theorem 4.4. (A sufficient condition under which neither the defender nor the attacker will occupy the entire network.) *Consider Type-I dynamics with threshold σ and arbitrary clustered network $G = (V, E)$. Let $B_v(0) = \alpha_k$ for every $v \in V_k$ and let β_k be the minimum node expansion as defined in* (3.1). *If $\alpha_k \beta_k > \sigma$, then all nodes in V_k will become* `secure`*; if $(1 - \alpha_k)\beta_k > 1 - \sigma$, all nodes in V_k will become* `compromised`*.*

Proof. If $\alpha_k \beta_k > \sigma$ for all nodes in V_k, then

$$\frac{1}{\deg(v)} \sum_{u \in N_v} B_u(0) \geq \frac{1}{\deg(v)} \alpha_k \cdot |N_v \cap V_k| \geq \alpha_k \beta_k > \sigma.$$

As in Theorem 4.2, we have $\lim_{t \to \infty} B_v(t) = 1$.

If $(1-\alpha_k)\beta_k > 1-\sigma$ for all nodes in V_k, then

$$1 - \frac{1}{\deg(v)} \sum_{u \in N_v} B_u(0) \geq \frac{\deg(v)}{\deg(v)} - \frac{|N_v \cap V_k| \cdot \alpha_k}{\deg(v)} - \frac{|N_v \setminus V_k|}{\deg(v)}$$
$$= \frac{|N_v \cap V_k|}{\deg(v)}(1-\alpha_k) \geq (1-\alpha_k)\beta_k > 1-\sigma.$$

As in Theorem 4.2, we have $\lim_{t\to\infty} B_v(t) = 0$. □

Theorem 4.4, which applies to arbitrary networks with the cluster structure, leads to the following insight.

Insight 4.5. Suppose (i) neither the defender nor the attacker is superior to its opponent and (ii) the initial network security state does not satisfy the conditions of Theorem 4.2. Then the network structure plays an important role. Specifically, in clustered networks, active cyber defense may be able to clean up only some clusters automatically, but not the entire network.

Theorem 4.2 identifies two stable equilibria $B^* = [1, \ldots, 1]$ and $B^* = [0, \ldots, 0]$, while Theorem 4.4 gives a condition under which another kind of stable equilibria exist (i.e., different clusters, some `compromised`, others `secure`). Because the stability of equilibria gives a high-level description of Type-I dynamics (e.g., conditions under which the global network security state evolves toward a particular equilibrium), we need some general method/algorithm to evaluate the stability of equilibria. This is addressed by the following theorem, whose proof is deferred to Section 10.1. Before presenting the theorem, we recall that an equilibrium B^* is *stable* if there exists a neighborhood of B^* such that every trajectory $B(t)$ initially located in the neighborhood converges to B^*. We say that B^* is a *stable equilibrium with exponential convergence* if for each $B(t)$ in the neighborhood, there exist positive constants $\varrho > 0$ and $M > 0$ such that $\|B(t) - B^*\| \leq Me^{-\varrho t}$ for all $t \geq 0$.

Theorem 4.6. (Method/algorithm for determining stability of equilibria and their emergence rates.) *Consider Type-I dynamics with threshold σ and* arbitrary *network $G = (V, E)$. Let $B^* = [B_v^*]_{v\in V}$ be an equilibrium and $\bar{B}^* = [1 - B_v^*]_{v\in V}$.*

(i) If

$$B_v^* = \begin{cases} 1, & \dfrac{1}{\deg(v)} \displaystyle\sum_{u\in N_v} B_u^* > \sigma, \\ 0, & \dfrac{1}{\deg(v)} \displaystyle\sum_{u\in N_v} B_u^* < \sigma, \end{cases} \tag{4.1}$$

holds for all $v \in V$, then both B^* and $\bar{B}^*$ are asymptotically stable equilibria with exponential convergence.

(ii) If $B_v^* = \sigma$ for some $v \in V$, then B^* and $\bar{B}^*$ are unstable.

Recall that Theorem 4.2 says that the system has two equilibria: $[1, \ldots, 1]$ and $[0, \ldots, 0]$. Since both equilibria satisfy condition (4.1), Theorem 4.6 says that the two equilibria are asymptotically stable with exponential convergence.

4.2. Characterizing Type-I Dynamics with a Strategic Defender

Now we investigate Type-I dynamics with a *strategic* defender, where the initial probability that node v is secure is proportional to its degree, namely $B_v(0) \propto \deg(v)$. We analyze this situation in the generalized random graph model discussed above [11]. This means that our analytic result (Theorem 4.7 below) is not necessarily true for arbitrary networks. We compensate this slight restriction with valuable analytic results, including the quantification of the benefits when the attack–defense network structures are ER graphs and power-law graphs. The basic idea behind the proof of Theorem 4.7 is to show that under the given conditions, the event $\frac{1}{\deg(v)} \sum_{u \in N_v} B_u(0) > \sigma$ occurs almost surely. We accomplish this using an asymptotic normal distribution, and by showing that the Lyapunov condition in the central limit theorem and the Kolmogorov condition in the strong law of large numbers [10] are satisfied. The proof details are given in Section 10.2.

Theorem 4.7. (Outcome of active cyber defense with strategic defender.) *Let $G(n) = (V(n), E(n))$ be an instance of an n-node random graph generated according to a given expected (in)degree sequence $(d_1(n), \ldots, d_n(n))$. Given the degree-dependent probability $B_v(0)$, we determine v's state according to $B_v(0)$ independently of everything else. Let $S = \{v : v \in V(n) \wedge B_v(0) = 1\}$ be the set of* `secure` *nodes in $G(n)$ at time $t = 0$, and*

$$\phi(n) = \frac{\sum_{v \in S} \deg(v)}{\sum_{u \in V(n)} \deg(u)},$$

where $\deg(v)$ *is the (in)degree of $v \in V(n)$ in $G(n)$. Let*

$$s_{n,v}^2 = \sum_{u \in V(n)} B_u(0)^2 p_{vu}(n)(1 - p_{vu}(n)), \tag{4.2}$$

$$q_{n,v} = \sum_{u \in V(n)} B_u(0)^3 p_{vu}(n)(1 - p_{vu}(n))\big[(1 - p_{vu}(n))^2 + p_{vu}(n)^2\big], \tag{4.3}$$

$$w_{n,v}^2 = \sum_{u \in V(n)} p_{vu}(n)(1 - p_{vu}(n)), \tag{4.4}$$

$$g_{n,v} = \sum_{u \in V(n)} p_{vu}(n)(1 - p_{vu}(n))\big[(1 - p_{vu}(n))^2 + p_{vu}(n)^2\big]. \tag{4.5}$$

Assume

(i) $\lim_{n \to \infty} \sup_{v \in V(n)} q_{n,v}/s_{n,v}^3 = 0.$
(ii) $\lim_{n \to \infty} \sup_{v \in V(n)} g_{n,v}/w_{n,v}^3 = 0.$
(iii) $\lim_{n \to \infty} \sqrt{\ln(n)}/d_{\min}(n) = 0.$
(iv) $\lim_{n \to \infty} (\sum_{v \in V(n)} g_{n,v})/(\sum_{v \in v(n)} w_{n,v}^2)^{3/2} = 0.$
(v) $\lim_{n \to \infty} (\sum_{v \in V(n)} q_{n,v})/(\sum_{v \in v(n)} s_{n,v}^2)^{3/2} = 0.$
(vi) $\lim_{n \to \infty} \sum_{v \in V(n)} \frac{1}{d_v^2} = 0.$

If $\underline{\lim}_{n\to\infty}\phi(n) > \sigma$ *holds almost surely, then* $\lim_{n\to\infty}\lim_{t\to\infty} B_v(t) = 1$ *holds for all* $v \in V(n)$ *almost surely, namely*

$$\lim_{n\to\infty} \mathsf{P}\left(\lim_{t\to\infty} B_v(t) = 1\right) = 1.$$

If $\overline{\lim}_{n\to\infty}\phi(n) < \sigma$ *holds almost surely, then* $\lim_{n\to\infty}\lim_{t\to\infty} B_v(t) = 0$ *holds for all* $v \in V(n)$ *almost surely, namely*

$$\lim_{n\to\infty} \mathsf{P}\left(\lim_{t\to\infty} R_v(t) = 1\right) = 1.$$

Note that Theorem 4.7 holds for generalized random graphs (rather than arbitrary networks), which, however, are not necessarily dense. To see this, we observe that a sufficient condition for assumption (v) is $d_{\min} \gg \sqrt{n}$, because

$$\sum_{v\in V(n)} \frac{1}{d_v^2(n)} \le \frac{n}{d_{\min}^2(n)}.$$

A necessary condition for assumption (v) is $\langle d_v^2(n)\rangle \gg n$, where $\langle d_v^2(n)\rangle = \frac{1}{n}\sum_{v\in V(n)} d_v^2(n)$, because

$$\sum_{v\in V(n)} \frac{1}{d_v^2(n)} \ge \frac{n}{\frac{1}{n}\sum_{v\in V(n)} d_v^2(n)} = \frac{n}{\langle d_v^2(n)\rangle}.$$

These conditions do not imply that the graphs are dense. For example, the two conditions are satisfied by $d_v(n) = O(\sqrt{n}\log(n))$ for all $v \in V(n)$, which, however, implies that the density of the graph converges to zero as $n \to \infty$.

Theorem 4.7 corresponds to the case of a strategic defender with $B_v(0) \propto \deg(v)$, and it can be adapted to the case of a strategic attacker with $R_v(0) \propto \deg(v)$. In what follows, we discuss the implications of Theorem 4.7 in these two cases separately and then compare them to draw deeper/quantitative insights with respect to ER and power-law graphs.

4.2.1. Characterizing the Qualitative Benefit to a Strategic Defender with $B_v(0) \propto \deg(v)$. Since $B_v(0) \propto \deg(v)$, we have

$$B_v(0) = C_1 \frac{\deg(v)}{\sum_{u\in V(n)} \deg(u)},$$

for some constant $C_1 > 0$. Then the expected number of initial `secure` nodes is

$$\sum_{v\in V(n)} B_v(0) = C_1 \sum_{v\in V(n)} \frac{\deg(v)}{\sum_{u\in V(n)} \deg(u)} = C_1.$$

Define

$$\alpha_{\text{threshold}} = \frac{\sigma}{n} \frac{[\sum_{u\in V(n)} \deg(u)]^2}{\sum_{v\in V(n)} \deg(v)^2}, \tag{4.6}$$

where $\deg(v)$ is the (in)degree of node $v \in V(n)$. With respect to a random set S of `secure` nodes at time $t = 0$, we define the random variable $\chi_v(S)$:

$$\chi_v(S) = \begin{cases} 1, & v \in S, \\ 0, & v \notin S. \end{cases}$$

Since

$$\phi(n) = \frac{\sum_{u \in S} \deg(u)}{\sum_{v \in V(n)} \deg(v)} = \frac{\sum_{u \in V(n)} \deg(u)\chi_u(S)}{\sum_{v \in V(n)} \deg(v)} \approx \frac{\sum_{u \in V(n)} \deg(u) B_v(0)}{\sum_{v \in V(n)} \deg(v)} > \sigma, \quad (4.7)$$

Theorem 4.7 implies the following: if $|S|/n > \alpha_{\text{threshold}}$, then $\lim_{t \to \infty} B_v(t) = 1$ for $v \in V(n)$; if $|S|/n < \alpha_{\text{threshold}}$, then $\lim_{t \to \infty} B_v(t) = 0$ for $v \in V(n)$. Since

$$\frac{[\sum_{u \in V(n)} \deg(u)]^2}{\sum_{v \in V(n)} \deg(v)^2} \leq n,$$

we have $\alpha_{\text{threshold}} \leq \sigma$. This means that a strategic defender can use active cyber defense to clean up the entire network automatically even if the defender initially occupies a proportion less than σ but more than $\alpha_{\text{threshold}}$ ($\leq \sigma$) of the network. This leads to the following insight.

Insight 4.8. If the large-degree nodes are better protected by the strategic defender, the strategic defender can use active cyber defense to clean up the network automatically even if it occupies only a proportion $\alpha_{\text{threshold}}$ ($\leq \sigma$) of the network.

4.2.2. Characterizing the Qualitative Benefit to a Strategic Attacker with $R_v(0) \propto \deg(v)$. When $R_v(0) \propto \deg(v)$, we have $R_v(0) = C_2 \deg(v) / \sum_{u \in V} \deg(u)$ for some constant $C_2 > 0$. According to (2.8), $f_{\text{BR}}(\cdot)$ is discontinuous at $1 - \sigma$. The `compromised`-node initial occupation threshold is

$$\frac{1 - \sigma}{n} \frac{[\sum_{u \in V} \deg(u)]^2}{\sum_{v \in V} \deg(v)^2}.$$

Thus, the `secure`-node initial occupation threshold is

$$\beta_{\text{threshold}} = 1 - \frac{1 - \sigma}{n} \frac{[\sum_{v \in V} \deg(v)]^2}{\sum_{v \in V} \deg(v)^2}. \quad (4.8)$$

If $|S|/n > \beta_{\text{threshold}}$, then $\lim_{t \to \infty} B_v(t) = 1$; if $|S|/n < \beta_{\text{threshold}}$, then we have $\lim_{t \to \infty} B_v(t) = 0$. Since $\beta_{\text{threshold}} \geq \sigma$, this leads to the following insight.

Insight 4.9. If the large-degree nodes are compromised by a strategic attacker, the defender can use active defense to clean up the network only after the defender occupies a proportion $\beta_{\text{threshold}}$ ($\geq \sigma$) of the network.

4.2.3. Characterizing the Quantitative Benefit to a Strategic Defender in ER Graphs. For ER graphs with edge probability p, the degree distribution follows a

binomial distribution $B(n, p)$:

$$\mathsf{P}(\deg(v) = k) = \binom{n}{p} p^k (n-p)^k, \quad k = 0, 1, \ldots .$$

Above, we showed that

$$\alpha_{\text{threshold}} = \sigma \frac{p}{p + p(1-p)/n}, \quad \beta_{\text{threshold}} = 1 - (1-\sigma)\frac{p}{p + p(1-p)/n}.$$

As $n \to \infty$, both $\alpha_{\text{threshold}}$ and $\beta_{\text{threshold}}$ converge to the threshold σ. More specifically,

$$\beta_{\text{threshold}} - \alpha_{\text{threshold}} = 1 - \frac{p}{p + p(1-p)/n}$$

converges to 0, while

$$\frac{\beta_{\text{threshold}}}{\alpha_{\text{threshold}}} = 1 + \frac{1-p}{\sigma n}$$

converges to 1. This leads to the following insight.

Insight 4.10. For large ER graphs, the security benefit obtained by a strategic defender/attacker is not significant, because the node degrees are relatively homogeneous. (This is reminiscent of, and parallel to, the *connectivity-based* robustness of ER networks, namely that ER networks are resilient against strategic deletion of large-degree nodes [2]. Note, however, that in our model, the attacker aims to compromise nodes but does not delete any nodes.)

4.2.4. Characterizing the Quantitative Benefit to a Strategic Defender in Power-Law Graphs. Consider power-law graphs with exponent γ. Let

$$C = \int_{d_{\min}(n)}^{d_{\max}(n)} k^{-\gamma}\, dk = \frac{d_{\max}(n)^{1-\gamma} - d_{\min}(n)^{1-\gamma}}{1-\gamma}.$$

By replacing the sum with integral in (4.6), we can define

$$\begin{aligned}
\alpha_{\text{threshold}} &= \sigma \left(\frac{n}{C} \int_{d_{\min}(n)}^{d_{\max}(n)} k^{1-\gamma} dk \right)^2 \Bigg/ \left(\frac{n}{C} \int_{d_{\min}(n)}^{d_{\max}(n)} k^{2-\gamma} dk \right) \\
&= \frac{\sigma}{n} \left(\frac{n^2 (d_{\max}(n)^{2-\gamma} - d_{\min}(n)^{2-\gamma})^2/(2-\gamma)^2}{(d_{\max}(n)^{1-\gamma} - d_{\min}(n)^{1-\gamma})^2/(1-\gamma)^2} \right) \\
&\quad \Bigg/ \left(\frac{n(d_{\max}(n)^{3-\gamma} - d_{\min}(n)^{3-\gamma})/(3-\gamma)}{(d_{\max}(n)^{1-\gamma} - d_{\min}(n)^{1-\gamma})/(1-\gamma)} \right).
\end{aligned}$$

This leads to four cases: $\gamma \notin \{1, 2, 3\}$, $\gamma = 1$, $\gamma = 2$, $\gamma = 3$. Let $z = d_{\max}(n)/d_{\min}(n)$. For $\gamma \notin \{1, 2, 3\}$, one can show that

$$\frac{(d_{\max}(n)^{2-\gamma} - d_{\min}(n)^{2-\gamma})^2/(2-\gamma)^2}{(d_{\max}(n)^{1-\gamma} - d_{\min}(n)^{1-\gamma})^2/(1-\gamma)^2} \Big/ \frac{(d_{\max}(n)^{3-\gamma} - d_{\min}(n)^{3-\gamma})/(3-\gamma)}{(d_{\max}(n)^{1-\gamma} - d_{\min}(n)^{1-\gamma})/(1-\gamma)}$$

$$= \frac{(z^{2-\gamma}-1)^2}{(z^{1-\gamma}-1)(z^{3-\gamma}-1)} \frac{(3-\gamma)(1-\gamma)}{(2-\gamma)^2}.$$

For $\gamma = 1, 2, 3$, we can reason in a similar fashion. As a result, we can define

$$h(z,\gamma) = \begin{cases} \dfrac{(z^{2-\gamma}-1)^2}{(z^{1-\gamma}-1)(z^{3-\gamma}-1)} \dfrac{(3-\gamma)(1-\gamma)}{(2-\gamma)^2}, & \gamma \neq 1, 2, 3, \\ 2\dfrac{z-1}{z+1}\dfrac{1}{\ln(z)}, & \gamma = 1, \\ \dfrac{z(\ln(z))^2}{(z-1)^2}, & \gamma = 2, \\ 2\dfrac{z-1}{z+1}\dfrac{1}{\ln(z)}, & \gamma = 3. \end{cases}$$

If the defender is strategic, a sufficient condition for $\lim_{t\to\infty} B_v(t) = 1$ is $|S|/n > \alpha_{\text{threshold}} = \sigma \cdot h(z,\gamma)$; if the attacker is strategic, a sufficient condition for $\lim_{t\to\infty} B_v(t) = 1$ is $|S|/n > \beta_{\text{threshold}} = 1 - (1-\sigma)h(z,\gamma)$. Therefore, we have

$$\beta_{\text{threshold}} - \alpha_{\text{threshold}} = 1 - h(z,\gamma), \tag{4.9}$$

$$\frac{\beta_{\text{threshold}}}{\alpha_{\text{threshold}}} = \frac{1-(1-\sigma)h(z,\gamma)}{\sigma \cdot h(z,\gamma)} = 1 + \frac{1-h(z,\gamma)}{\sigma \cdot h(z,\gamma)}. \tag{4.10}$$

Equations (4.9) and (4.10) reach their maximum at $\gamma = 2$. This leads to the following insight.

Insight 4.11. For power-law graphs, the benefit to a strategic defender/ attacker is significant. (This is also reminiscent of, and parallel to, the *connectivity-based* robustness of power-law networks, namely that power-law networks are easily disrupted by strategic deletion of large-degree nodes [2]. Again, in our model the attacker aims to compromise nodes but does not delete any nodes.) Moreover, the benefit to a strategic defender is maximized for the subclass of power-law networks with exponent $\gamma = 2$.

5. CHARACTERIZING TYPE-II ACTIVE CYBER DEFENSE DYNAMICS

Type-II dynamics is similar to Type-I dynamics, except the following: A Type-I combat-power function is discontinuous near the threshold σ, whereas a Type-II combat-power function is continuous and differentiable near the threshold τ. For the case of a *nonstrategic* defender with node-independent $B_v(0)$, we obtain the following theorems, which are analogous to Theorems 4.2–4.6. Theorem 5.2 requires the following lemma, whose proof is given in Section 10.3.

Lemma 5.1. *Consider Type-II dynamics with threshold τ and system* (2.7) *in an arbitrary network $G = (V, E)$.*

(i) *If $\frac{1}{\deg(v)} \sum_{u \in N_v} B_u(0) > \tau$ holds for all $v \in V$, then $\frac{1}{\deg(v)} \sum_{u \in N_v} B_u(t) > \tau$ holds for all $v \in V$ and $t \geq 0$, and $\min_{v \in V} B_v(t)$ increases monotonically.*
(ii) *If $\frac{1}{\deg(v)} \sum_{u \in N_v} B_u(0) < \tau$ holds for all $v \in V$, then $\frac{1}{\deg(v)} \sum_{u \in N_v} B_u(t) < \tau$ holds for all $v \in V$ and $t \geq 0$, and $\max_{v \in V} B_v(t)$ decreases monotonically.*

A proof of the following theorem, which holds for arbitrary networks, is given in Section 10.4.

Theorem 5.2. (A sufficient condition under which the defender or the attacker will occupy the entire network.) *Consider Type-II dynamics with threshold τ and arbitrary network $G = (V, E)$. If $\frac{1}{\deg(v)} \sum_{u \in N_v} B_u(0) > \tau$ for all $v \in V$, then $\lim_{t \to \infty} B_v(t) = 1$ for all $v \in V$. If $\frac{1}{\deg(v)} \sum_{u \in N_v} B_u(0) < \tau$ for all $v \in V$, then $\lim_{t \to \infty} B_v(t) = 0$ for all $v \in V$.*

Theorem 5.3. (A sufficient condition under which neither the defender nor the attacker will occupy the entire network.) *Consider Type-II dynamics with threshold τ and arbitrary network $G = (V, E)$ with the cluster structure. Let $B_v(0) = \alpha_k$ for every $v \in V_k$, and let β_k be the minimum node expansion as defined in* (3.1). *If $\alpha_k \beta_k > \tau$, then all nodes in V_k will become* `secure`*, while if $(1 - \alpha_k)\beta_k > 1 - \tau$, then all nodes in V_k will become* `compromised`*.*

The proof of Theorem 5.3 is similar to that of Theorem 4.4. A proof of the following theorem is given in Section 10.5. Both theorems hold for arbitrary networks.

Theorem 5.4. (Method/algorithm for determining stability of equilibria.) *Consider Type-II dynamics with threshold τ and arbitrary network $G = (V, E)$. Let $B^* = [B_v^*]_{v \in V}$ be an equilibrium and $\bar{B}^* = [1 - B_v^*]_{v \in V}$.*

(i) *Equilibria $B^* = [1, \ldots, 1]$ and $B^* = [0, \ldots, 0]$ are asymptotically stable with exponential convergence.*
(ii) *If $B_v^* = \tau$ for some $v \in V$, then B^* and $\bar{B}^*$ are unstable.*

For the case of a strategic defender with $B_v(0) \propto \deg(v)$, we can obtain a result for generalized random graphs in parallel to Theorem 4.7 via a similar proof. We omit the lengthy details. In summary, we have the following insight.

Insight 5.5. Insights 4.3–4.11 above are equally applicable to Type-II dynamics.

6. CHARACTERIZING TYPE-III AND TYPE-IV ACTIVE CYBER DEFENSE DYNAMICS

Type-III and Type-IV combat-power functions represent that the defender (attacker) is superior to, or more advanced than, its opponent. Due to the lack of threshold in the

computer-power functions, an immediate consequence is that there is no difference between the case of a nonstrategic defender and that of a strategic defender. Further consequences due to the lack of a threshold are characterized as follows.

Theorem 6.1. (Characterizing Type-III dynamics.) *Consider Type-III dynamics in an arbitrary network $G = (V, E)$.*

(i) *If $B_v(0) > 0$ for all $v \in V$, then $\lim_{t\to\infty} B_v(t) = 1$ for all $v \in V$.*
(ii) *The equilibrium $B_v(0) = [1, \ldots, 1]$ is asymptotically stable with exponential convergence.*
(iii) *The equilibrium $B_v(0) = [0, \ldots, 0]$ is unstable.*

Part (i) of Theorem 6.1 can be proved like the first half of Theorem 5.2. Parts (ii) can be proved like part (i) of Theorem 5.4. Part (iii) can be proved like part (ii) of Theorem 5.4. Since Type-IV dynamics is dual to Type-III dynamics, from Theorem 6.1 we obtain the following result.

Theorem 6.2. (Characterizing Type-IV dynamics.) *Consider Type-IV dynamics in an arbitrary network $G = (V, E)$.*

(i) *If $B_v(0) < 1$ for all $v \in V$, then $\lim_{t\to\infty} B_v(t) = 0$ for all $v \in V$.*
(ii) *The equilibrium $B_v(0) = [0, \ldots, 0]$ is asymptotically stable with exponential convergence.*
(iii) *The equilibrium $B_v(0) = [1, \ldots, 1]$ is unstable.*

Theorems 6.1–6.2, which hold for *arbitrary* networks, lead to the following insight.

Insight 6.3. If the defender is superior to the attacker in terms of cyber combat power, the defender can always use active defense to automatically clean up the entire network as long as there are a few computers that are not compromised. In the extreme case in which the attacker has compromised the entire network, the defender needs to clean up only a few computers manually before launching active defense to clean up the entire network automatically. This suggests that cyber combat superiority can serve as an effective deterrence.

7. ADVANTAGE OF ACTIVE CYBER DEFENSE OVER REACTIVE CYBER DEFENSE

Current cyber defense is mainly reactive, whereby the defender runs "antivirus software"-like tools on each computer to scan and cure infections, which are caused by attacks and/or malware that have penetrated the defense perimeter, such as firewalls. Reactive cyber defense inevitably causes an asymmetry that is advantageous to the attacker, because the attack effect is automatically amplified by the network (a kind of "network effect"). Specifically, reactive cyber defense may be modeled using the well-known SIS (susceptible–infectious–susceptible) model while accommodating arbitrary attack–defense network topologies.

A sufficient condition for the epidemic to die out is [8]

$$\lambda_{1,\mathsf{A}} < \frac{\text{cure capability}}{\text{spreading capability}},$$

where $\lambda_{1,\mathsf{A}}$ is the largest eigenvalue of the adjacency matrix corresponding to the attack–defense structure and is in a sense the average node degree or connectivity [22]; cure capability abstracts the defender's reactive defense power (i.e., the probability that a compromised node becomes a susceptible node in a single time step), and spreading capability abstracts the attacker's attack power (i.e., the probability that a compromised node successfully attacks a susceptible neighboring node at a single time step). This means that the attacker always benefits from rich connectivity, because the attack effect is amplified by $\lambda_{1,\mathsf{A}}$, which explains why the asymmetry phenomenon is advantageous to the attacker [26, 38, 39].

On the other hand, Sections 4–6 show that the asymmetry disappears with active cyber defense because $\lambda_{1,\mathsf{A}}$ (or its like) does not play a role in the analytic results. This justifies the use of model-based characterization studies. In summary, we have the following insight.

Insight 7.1. Active cyber defense eliminates the attack amplification phenomenon, namely the asymmetry between cyber attack and reactive cyber defense.

8. VALIDATING THE DYNAMIC SYSTEM MODEL VIA SIMULATION

The above characterizations of active cyber defense dynamics are based on the dynamical system model, which is the mean-field approximation of the native Markov process model. Therefore, we need to show whether the analytic results derived from the dynamical system model are intrinsic to the Markov process model.

8.1. Validation Methodology

Our validation methodology is centered on examining the *dynamic accuracy* and the *threshold accuracy* of the dynamical system model. For examining the dynamic accuracy, we compare the mean `secure` occupation probability in the dynamical system model, namely $\langle B_v(t)\rangle = \frac{1}{|V|}\sum_{v\in V} B_v(t)$, and the simulation-based mean fraction of `secure` nodes in the Markov process model, namely $\langle \xi_v(t)\rangle = \frac{1}{|V|}\sum_{v\in V} \xi_v(t)$. If $\langle \xi_v(t)\rangle$ and $\langle B_v(t)\rangle$ exhibit a similar, if not exactly the same, dynamic behavior, we conclude that the analytic results derived from the dynamical system model are intrinsic to the Markov process model. (i) Our simulation of the Markov process model is based on (2.1), namely

$$\mathsf{P}\{\xi_v(t+\Delta t) = 1 \mid \xi_v(t),\ v \in N\} = \begin{cases} \Delta t \cdot \tilde{\theta}_{v,\mathrm{RB}}(t), & \xi_v(t) = 0, \\ 1 - \Delta t \cdot \tilde{\theta}_{v,\mathrm{BR}}(t), & \xi_v(t) = 1, \end{cases}$$

where the random rate $\tilde{\theta}_{v,\mathrm{RB}}$ is replaced with its mean $\theta_{v,\mathrm{RB}}$ as specified in (2.5). Simulation results are based on the average of 50 simulation runs. (ii) Our numerical calculation in the dynamical system model is based on (2.7), namely

$$B_v(t+\Delta t) = B_v(t) + [\theta_{v,\mathrm{RB}}(t) - B_v(t)]\Delta t.$$

In both cases, we set $\Delta t = 0.01$.

For examining the threshold accuracy, we study whether the threshold σ in the dynamical system model is faithful to the threshold σ_{markov} in the Markov process model. In order to to compute σ_{markov}, we use the following numerical method. Since the convergence of $\langle \xi_v(t) \rangle$ is probabilistic in a very small interval that contains σ, we define σ_{markov} as the median value in that interval. Specifically, let a_1 be the smallest value such that an initial `secure` occupation greater than a_1 will cause all nodes to become `secure` in all 50 runs. Let b_1 be the largest value such that an initial `secure` occupation smaller than b_1 will cause all nodes to become `compromised` in all 50 runs. We set $\sigma_{\text{markov}} = \frac{1}{2}(a_1 + b_1)$.

In our simulation, we use two kinds of graphs:

- ER random graph: It has $n = 2000$ nodes and independent link probability $p = 0.02$.
- Power-law random graph: It has $n = 2000$, exponent $\gamma = 2.5$, minimum node degree 2, and maximum node degree 120.

8.2. Dynamics Accuracy of the Dynamical System Model

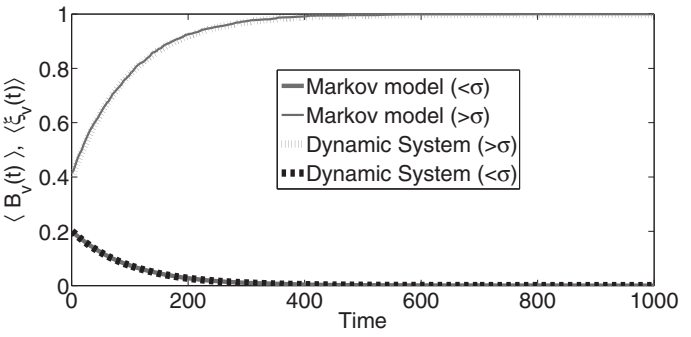
Overall dynamics accuracy. First, let us consider Type-I dynamics and a nonstrategic defender with node-independent identical initial occupation probability $B_v(0)$. Figure 4 confirms that Theorem 4.2, which was proven in the dynamical system model, is indeed intrinsic to the Markov process model. Specifically, in the dynamical system model, the $\langle B_v(t) \rangle$'s corresponding to $B_v(0) = 0.4 > \sigma = 1/3$ all converge to 1, and the $\langle B_v(t) \rangle$'s corresponding to $B_v(0) = 0.2 < \sigma = 1/3$ all converge to 0. In the Markov process model, the $\langle \xi_v(t) \rangle$'s corresponding to $\mathsf{P}\{\xi_v(0) = 1\} = 0.4$ all converge to 1, and the $\langle \xi_v(t) \rangle$'s corresponding to $\mathsf{P}\{\xi_v(0) = 1\} = 0.2$ all converge to 0. Therefore, the dynamic behavior indicated by Theorem 4.2 is also exhibited by the Markov process model.

Second, let us look at Type-I dynamics and a strategic defender with $B_v(0) \propto \deg(v)$. Define

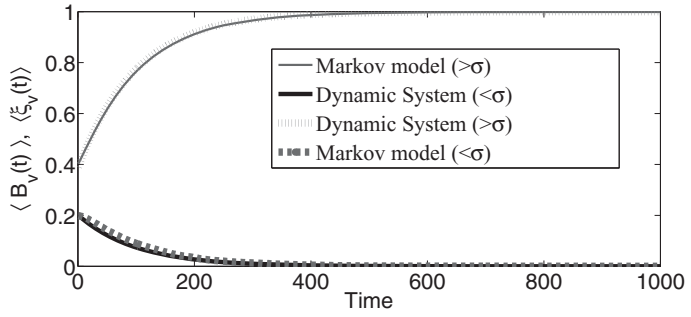
$$\eta = \frac{\sum_{u \in S} \deg(u)}{\sum_{v \in V} \deg(v)},$$

where S is the set of `secure` nodes at time $t = 0$. Inequality (4.7) indicates that if $\eta > \sigma$, then all nodes will become `secure`, while if $\eta < \sigma$, all nodes will become `compromised`. In our simulation, we set $\sigma = 0.5$. Figure 5(a) shows that in the ER graph, both $\langle B_v(t) \rangle$ in the dynamical system model and $\langle \xi_v(t) \rangle$ in the Markov process model converge to 1 when $\eta = 0.52 > \sigma = 0.5$ and converge to 0 when $\eta = 0.45 < \sigma = 0.5$. Figure 5(b) shows that in the power-law network, both $\langle B_v(t) \rangle$ and $\langle \xi_v(t) \rangle$ converge to 1 when $\eta = 0.45$ ($< \sigma = 0.5$) and converge to 0 when $\eta = 0.35$ (far smaller than $\sigma = 0.5$). These confirm the phenomenon that is implied by Theorem 4.7, namely that the effect of strategic defense is not significant in ER networks but significant in power-law networks. In any case, the simulation results demonstrate that the phenomenon exhibited by the dynamical system model is intrinsic to the Markov process model.

Third, let us look at dynamics of Types II–IV and a nonstrategic defender with node-independent identical initial occupation probability $B_v(0)$. Consider a Type-II combat-power function with $\tau = 0.5$, $f_{\text{RB}}(x) = 2x^2$ for $x \in [0, 0.5]$, and $f_{\text{RB}}(x) = -2x^2 + 4x - 1$ for $x \in [0.5, 1]$. For the dynamical system model, Figures 6(a) and 6(b) show that $B_v(0) = 0.4 < \tau = 0.5$ implies that all nodes will become `compromised`, and $B_v(0) = 0.6 > \tau = 0.5$ implies that all nodes will become `secure`.



(a) ER graph

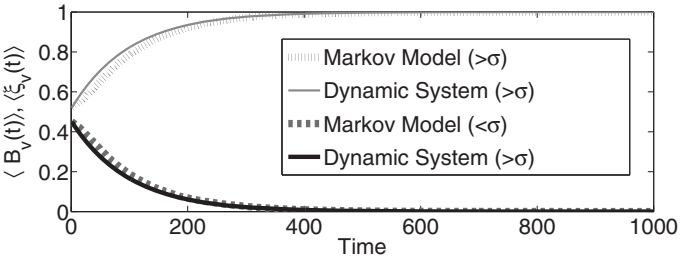


(b) Power-law graph

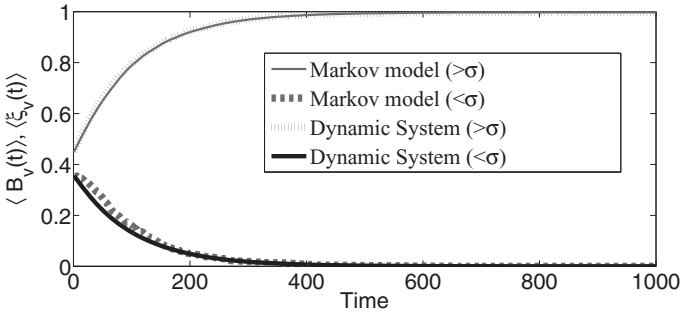
Figure 4 $\langle B_v(t)\rangle$ vs. $\langle \xi_v(t)\rangle$ in Type-I dynamics with $\sigma = 1/3$ and nonstrategic defender.

In the Markov process model, the same phenomenon is exhibited with the same initial condition $\mathsf{P}\{\xi_v = 1\} = B_v(0)$. This validates Theorem 5.2. For a Type-III combat-power function with $f_{\text{RB}}(x) = x^{1/2}$, Figures 6(c) and 6(d) demonstrate that $\langle B_v(t)\rangle$ corresponding to $B_v(0) = 0.02$ converges to 1 in the dynamical system model. The same phenomenon is exhibited in the Markov process model. This validates Theorem 6.1. For a Type-IV combat-power function $f_{\text{RB}}(x) = x^2$, Figures 6(e) and 6(f) validate that $\langle B_v(t)\rangle$ corresponding to $B_v(0) = 0.98$ converges to 0. The same phenomenon is exhibited in the Markov process model. This confirms that the dynamic behavior indicated by Theorem 6.2 is also exhibited by the Markov process model.

Fourth, for power-law networks and a strategic defender with $B_v(0) \propto \deg(d)$, we derived the sufficient condition $|S|/n > \sigma \cdot h(z, \gamma)$ for $\lim_{t\to\infty} B_v(t) = 1$, meaning that in order for the defender to use active cyber defense to automatically clean up the network, the defender needs to occupy more than a proportion $\sigma \cdot h(z, \gamma)$ of the nodes, which is minimum when $h(z, \gamma)$ is minimum. As shown in Figure 7(a), for fixed z, $h(z, \gamma)$ is minimum at $\gamma = 2$, which corresponds to the subclass of power-law networks that maximize the benefit to the strategic defender. Figure 7(b) plots the simulation results in the Markov process model. We observe that σ_{markov} is minimum at $\gamma = 2$ in the Markov model as well. This further confirms that the particular conclusion drawn in the dynamic model, that the benefit to the strategic defender is maximized for power-law graphs with exponent $\gamma = 2$, is also intrinsic to the Markov process model.



(a) ER graph



(b) Power-law graph

Figure 5 $\langle B_v(t)\rangle$ vs. $\langle \xi_v(t)\rangle$ in Type-I dynamics with $\sigma = 1/2$ and strategic defender.

Dynamics inaccuracy: cause and characteristics. In the above, our simulation results show, from the perspective of system state dynamics, that the dynamical system model offers overall accurate approximation to the Markov process model. Still, Figures 4–6 visually exhibit the following phenomenon: the dynamical system model sometimes underestimates and sometimes overestimates the dynamics simulated from the Markov process model. What is the cause of this phenomenon? To answer this question, we observe that the master equation (2.3) can be rewritten as

$$\frac{d}{dt}\tilde{B}_v(t) = \tilde{\theta}_{v,\mathrm{RB}}(t) - \tilde{B}_v(t), \tag{8.1}$$

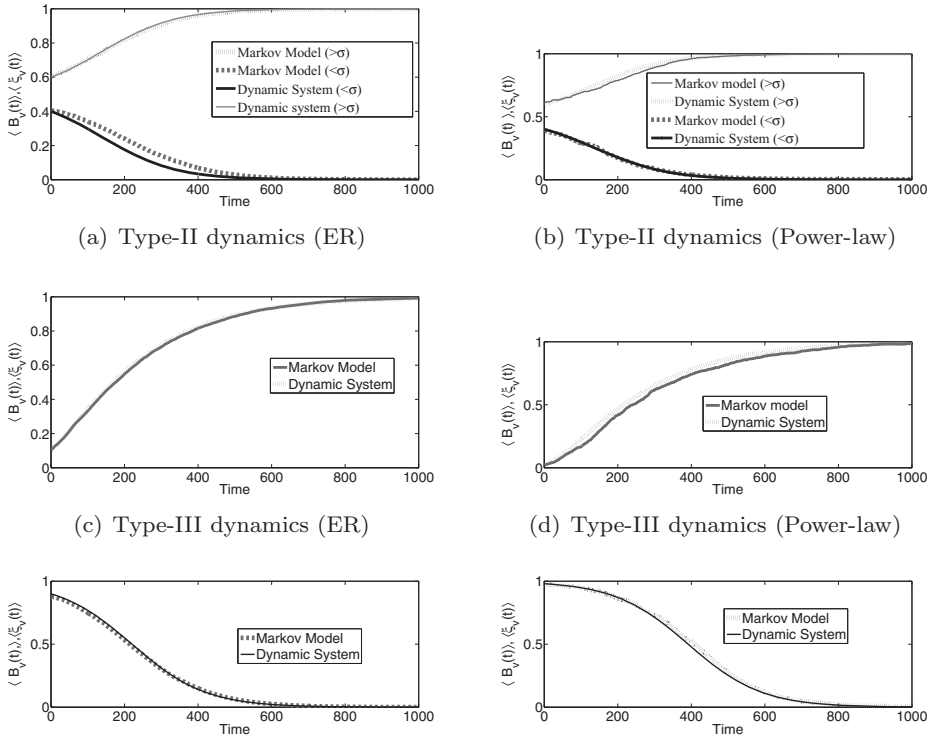
where

$$\tilde{\theta}_{v,\mathrm{RB}}(t) = \mathsf{E}\left(f_{\mathrm{RB}}\left(\frac{1}{\deg(v)}\sum_{u\in N_v}\xi_v(t)\right)\right)$$

and $\tilde{\theta}_{v,\mathrm{RB}}(t) = 1 - \tilde{\theta}_{v,\mathrm{BR}}(t)$, to be consistent with (2.6). It can be seen that if $f_{\mathrm{RB}}(\cdot)$ is convex, then

$$\begin{aligned}\tilde{\theta}_{v,\mathrm{RB}}(t) &= \mathsf{E}\left(f_{\mathrm{RB}}\left(\frac{1}{\deg(v)}\sum_{u\in N_v}\xi_v(t)\right)\right) \geq f_{\mathrm{RB}}\left(\mathsf{E}\left(\frac{1}{\deg(v)}\sum_{u\in N_v}\xi_v(t)\right)\right)\\ &= \theta_{v,\mathrm{RB}}(t).\end{aligned}$$

Analogously, if $f_{\mathrm{RB}}(\cdot)$ is concave, then $\tilde{\theta}_{v,\mathrm{RB}}(t) \leq \theta_{v,\mathrm{RB}}(t)$.



(a) Type-II dynamics (ER)

(b) Type-II dynamics (Power-law)

(c) Type-III dynamics (ER)

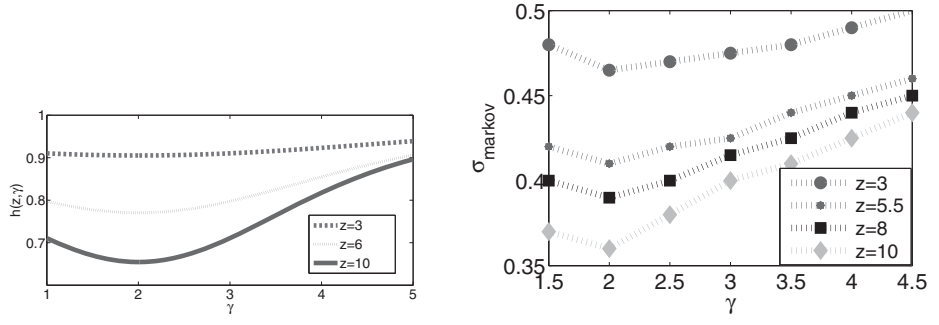
(d) Type-III dynamics (Power-law)

(e) Type-IV dynamics (ER)

(f) Type IV-dynamics (Power-law)

Figure 6 $\langle \xi_v(t) \rangle$ vs. $\langle B_v(t) \rangle$ in dynamics of Types II–IV with nonstrategic defender.

As a result, the above phenomenon can be explained as follows: For Type-I and Type-II combat-power functions, the dynamics in the dynamical system model underestimates the dynamics in the native Markov process model when $\frac{1}{\deg(v)} \sum_{u \in N_v} \xi_v(t)$ is below the threshold in the combat-power function, and overestimates the dynamics in the Markov process model when $\frac{1}{\deg(v)} \sum_{u \in N_v} \xi_v(t)$ is above the threshold (see Figures 4



(a) Numerical $h(z, \gamma)$

(b) Simulation-based σ_{markov}

Figure 7 Power-law networks with exponent $\gamma = 2$ maximize the benefit to strategic defenders.

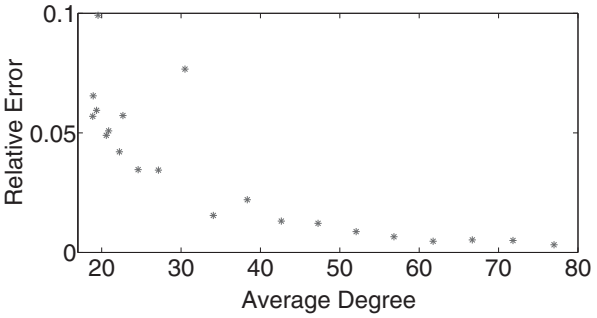


Figure 8 Relative error vs. average node degree.

and 5 and Figures 6(a) and 6(b)). For Type-III combat-power functions, which can be regarded as concave over the region [0, 1], the dynamics in the dynamical system model overestimates the dynamics in the Markov process model (see Figures 6(c) and 6(d)). Analogously, for Type-IV combat-power functions, the dynamics of the dynamical system model underestimates the dynamics in the Markov process model (see Figures 6(e) and 6(f)).

Having explained the cause of the slight dynamic inaccuracy, we want to establish some deeper understanding of it. In particular, we want to know how the inaccuracy may depend on the average node degree. For this purpose, we consider the following notion of *relative error* between the dynamical system model and the Markov process model:

$$\mathrm{RE} = \frac{\int_0^T [\tilde{B}_v(t) - B_v(t)]^2\, dt}{\int_0^T \tilde{B}_v^2(t)\, dt},$$

where $\tilde{B}_v(t)$ is the probability that node v is `secure` in the Markov process model, and $B_v(t)$ is the dynamic system state.

To investigate the impact of average node degree, we fix the variance of the node degrees, denoted by dvar. Consider the generalized random graph model with a given expected degree sequence that follows the power-law distribution. By fixing the variance dvar and the ratio r between the minimum and maximum expected degrees as $d_{\max} = \mathsf{r} * d_{\min}$, we derive $d_{\min}$ with respect to the varying power-law exponent γ from 1 to 6, as follows:

$$d_{\min} = \sqrt{\frac{\mathrm{dvar}}{\frac{1-\gamma}{3-\gamma}\frac{\mathsf{r}^{3-\gamma}-1}{\mathsf{r}^{1-\gamma}-1} - \frac{1-\gamma}{(2-\gamma)^2}\frac{\mathsf{r}^{2-\gamma}-1}{(\mathsf{r}^{1-\gamma}-1)^2}}}.$$

With $\mathsf{r} = 20$ and $\mathsf{dvar} = 400$, we obtain a series of generalized random graphs of 2000 nodes.

Although we cannot precisely fix the variance, the actual standard deviation of degrees for different values of γ is quite stable: 20.47 ± 0.48. We run the Markov process model and the dynamical system model on the random graphs to calculate the relative errors. We find, as shown in Figure 8, that the relative errors decrease with the average node degree.

8.3. Threshold Accuracy of the Dynamic System Model

Now we examine the accuracy of the dynamical system model from a different perspective: *threshold accuracy*. That is, we examine the accuracy of the threshold σ derived from the dynamical system model with respect to the threshold σ_{markov}, which is numerically derived from the Markov process model. For the special case of Type-III and Type-IV combat-power functions, which have no threshold, we observe the following: For Type-III combat-power functions, if $\tilde{B}_v(0) > 0$ for some nodes that can reach all other nodes, then $\lim_{t\to\infty} \tilde{B}_v(t) = 1$ for all $v \in V$. For Type-IV combat-power functions, if $\tilde{R}_v(0) > 0$ for some nodes that can reach all other nodes, then $\lim_{t\to\infty} \tilde{B}_v(t) = 0$ for all $v \in V$. To see this, we note that in the case of Type-III combat-power functions, the following holds:

$$\tilde{\theta}_{v,\text{RB}}(t) = \mathsf{E}\left[f\left(\frac{1}{\deg(v)} \sum_{u\in N_v} \xi_u(t) \right) \right] \geq \mathsf{E}\left[\frac{1}{\deg(v)} \sum_{u\in N_v} \xi_u(t) \right]$$
$$= \left[\frac{1}{\deg(v)} \sum_{u\in N_v} \tilde{B}_u(t) \right].$$

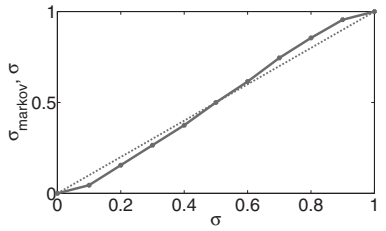
The case of Type-IV combat-power functions can be treated analogously. However, the situation for Type-I and Type-II combat-power functions is very different, as we elaborate below.

Threshold (in)accuracy for Type-I and Type-II combat-power functions: cause and characteristics. We illustrate the following *threshold-drifting* phenomenon with a specific $f_{\text{RB}}(\cdot)$ in Type-I dynamics. Figures 9(a) and 9(b) plot σ_{markov} and σ in the case of a nonstrategic defender with node-independent identical probability $B_v(0)$. Figures 9(c) and 9(d) plot σ_{markov} and σ in the case of a strategic defender with $B_v(0) \propto \deg(v)$. We observe that Figure 9(d) exhibits a pattern that is different from the others, which we cannot explain at the moment but which we plan to investigate in the future. In all other cases, we observe the following: if $\sigma < 0.5$, then $\sigma_{\text{markov}} < \sigma$; if $\sigma > 0.5$, then $\sigma_{\text{markov}} > \sigma$. We call this the *threshold-drifting* phenomenon, which indicates that the threshold σ in the dynamical system model may deviate from the threshold σ_{markov} in the Markov process model.

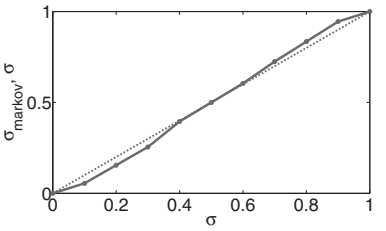
What is the cause of the threshold-drifting phenomenon? In order to answer this question, let us define $\alpha = \frac{1}{n}\sum_{v\in V} B_v(0)$, namely the average fraction of `secure` nodes at time $t = 0$. The probability that k out of node v's $\deg(v)$ neighbors are initially `secure` is

$$Q(\deg(v), \alpha, k) = \binom{\deg(v)}{k} \alpha^k (1-\alpha)^{\deg(v)-k}.$$

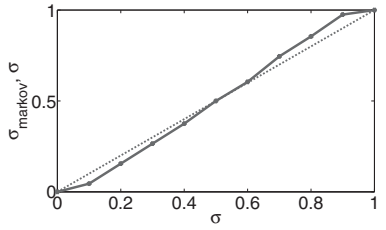
Suppose that at each time step, the occupation probability approximately follows the binomial distribution. For a random node $\bar{v}$, its expected degree is $\langle \deg(v) \rangle$ and the probability that $\bar{v}$ is `secure` is $\nu(t) = \langle \mathsf{P}\{\xi_v = 1\} \rangle$, with $\nu(0) = \alpha$. Now we consider the dynamical system model. The mean of $\theta_{\bar{v},\text{RB}}(t)$ is the probability that the actual number of `secure` neighbors is greater than $\sigma \cdot \langle \deg(v) \rangle$. Denote this probability by $\theta_\sigma(\nu(t), \langle \deg(v) \rangle)$.



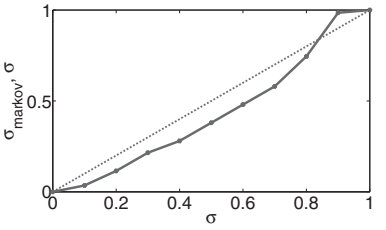
(a) Node-independent $B_v(0)$: ER graph



(b) Node-independent $B_v(0)$: Power-law graph



(c) Degree-dependent $B_v(0)$: ER graph



(d) Degree-dependent $B_v(0)$: Power-law graph

Figure 9 Threshold-drifting phenomenon: dotted diagonal line corresponds to σ and solid curves correspond to σ_{markov}.

Then,

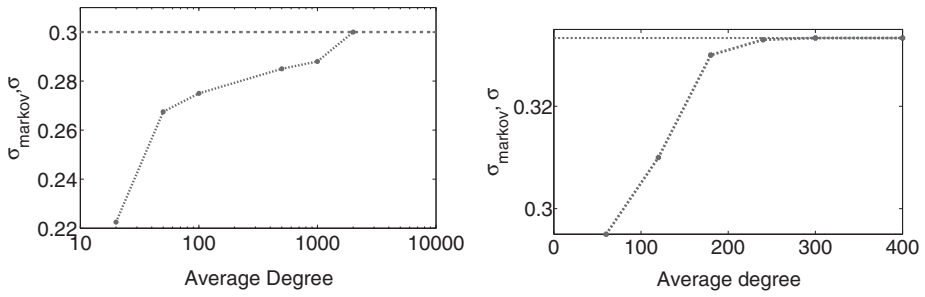
$$\theta_\sigma(\nu(t), \langle \deg(v) \rangle) = \begin{cases} \displaystyle\sum_{k > \nu(t) \cdot \langle \deg(v) \rangle} Q(\langle \deg(v) \rangle, \nu(t), k) \\ \quad \text{if } \sigma \cdot \langle \deg(v) \rangle \text{ is not an integer,} \\ \displaystyle\sum_{k > \nu(t) \cdot \langle \deg(v) \rangle} Q(\langle \deg(v) \rangle, \nu(t), k) + \frac{1}{2} Q(\langle \deg(v) \rangle, \nu(t), \sigma \cdot \deg(v)) \\ \quad \text{if } \sigma \cdot \langle \deg(v) \rangle \text{ is an integer.} \end{cases}$$

Hence, we can use the following equation to approximate the Markov process model:

$$\frac{d\nu(t)}{dt} = \theta_\sigma(\nu(t), \langle \deg(v) \rangle) - \nu(t).$$

This one-dimensional differential equation has two stable equilibria, $\nu = 0$ (i.e., all nodes are `compromised`) and $\nu = 1$ (i.e., all nodes are `secure`). The critical value of the initial condition between the attracting basins $\nu = 0$ and $\nu = 1$ is the nontrivial solution of $\theta_\sigma(\nu, \langle \deg(v) \rangle) - \nu = 0$, namely the solution other than the trivial solutions 0 and 1. The critical value in the dynamical system model approximates σ_{markov}. As shown in Figure 9, $\sigma_{\text{markov}} \neq \sigma$, which explains the threshold-drifting phenomenon.

Having explained the cause of the threshold-drifting phenomenon, we suspect that the degree of threshold-drifting also depends on the average node degree (more specifically, the threshold-drifting phenomenon disappears with the average degree). To confirm/disconfirm this, we compare in Figure 10 the threshold σ_{markov} in the Markov process model and the



(a) ER graph ($\sigma = 0.3$) (b) Power-law graph ($\sigma = 1/3$)

Figure 10 The greater the average node degree, the better the approximation of σ_{markov} (curve) to σ (line).

threshold σ in the dynamical system model, with respect to identical initial `secure`-occupation probability $B_v(0)$. In both ER and power-law graphs, we observe that σ_{markov} asymptotically converges to σ as the average node degree $\langle \deg(v) \rangle$ increases.

The implication of the threshold-drifting phenomenon is that the threshold σ may need to be adjusted in practice when $\sigma > 1/2$ (i.e., for some small $\Delta\sigma$ using $\sigma_{\text{markov}} = \sigma + \Delta\sigma$ instead). For the case $\sigma < 1/2$, adjustment is not necessary, because σ ($> \sigma_{\text{markov}}$) is sufficient for governing the dynamics toward the all-`secure` equilibrium (i.e., active cyber defense is effective for automatically cleaning up the network).

9. CONCLUSIONS

We have presented the first mathematical model and characterization of active cyber defense dynamics. The analytic results give conditions under which (strategic) active cyber defense is effective, and lead to practical insights that can be adopted for decision-making and policy-making in real life.

Our study brings a range of interesting research problems: How should we accommodate more sophisticated combat-power functions? How can we analyze a strategic defender/attacker, including $B_v(0) \propto \deg(v)$ and possibly other scenarios, in arbitrary networks (rather than in the generalized random graph model)? How can we analyze the native Markov process model without using the dynamical system approximation (while noting that the difficulty lies mainly in the nonlinearity of the combat-power functions)?

10. APPENDIX: PROOFS

10.1. Proof of Theorem 4.6

Proof. For (i), note that the equilibrium of (2.7) satisfies

$$f_{\text{RB}}\left(\frac{1}{\deg(v)}\sum_{u\in N_v} B_u^*\right) = B_v^*.$$

Consider a small perturbation $B(0) = B_v^* + \delta B$. If $B_v^* = 1$, then $\theta_{v,\text{RB}}(0) = 1$, and $B_v(t)$ increases toward 1; if $B_v^* = 0$, then $\theta_{v,\text{RB}}(0) = 0$, and $B_v(t)$ decreases toward 0. In any case, the sign of $\frac{1}{\deg(v)}\sum_{u\in N_v} B_u(t) - \sigma$ in a small time interval $[0, t_0)$ for some t_0 is unchanged. Let t_1 be the maximum time at which all the signs of $\frac{1}{\deg(v)}\sum_{u\in N_v} B_u(t) - \sigma$

are respectively the same as the signs of $\frac{1}{\deg(v)}\sum_{u\in N_v} B_u(0)-\sigma$. If t_1 is finite, then all signs in a small time interval starting at time t_1 are respectively the same as the signs at time t_1. This implies that $t_1=+\infty$. So the sign of $\frac{1}{\deg(v)}\sum_{u\in N_v} B_u(t)-\sigma$ is the same as the sign of $\frac{1}{\deg(v)}\sum_{u\in N_v} B_u(0)-\sigma$ for all $v\in V$, which implies that the system is asymptotically stable.

To see that $\bar{B}^*$ is also an equilibrium, consider the dynamic behavior of $R_v(t)$ in (2.7), namely $dR_v(t)/dt=\theta_{v,\mathrm{BR}}(t)-R_v(t)$, where

$$\theta_{v,\mathrm{BR}}(t)=f_{\mathrm{BR}}\left(\frac{1}{\deg(v)}\sum_{u\in N_v}R_v(t)\right)=1-f_{\mathrm{RB}}\left(\frac{1}{\deg(v)}\sum_{u\in N_v}B_v(t)\right).$$

Since $B_v(t)+R_v(t)=1$ always holds for all v, $\bar{B}^*$ is an equilibrium of (4.1) and thus an equilibrium of (2.7).

To see the rates of convergence to the above equilibria, we note $\theta_{v,\mathrm{BR}}(t)=0$ or 1 for all t and $v\in V$. Thus, (2.7) becomes either $dB_v(t)/dt=1-B_v(t)$ or $dB_v(t)/dt=-B_v(t)$. In any case, the convergence rate is $O(\exp(-t))$.

For (ii), we first note that the definition of Type-I combat-power function implies $\theta_{v,\mathrm{RB}}\in\{0,1,\sigma\}$. Suppose at equilibrium B^* that $B^*_{v_k}=\sigma$ for $v_k\in V_1=\{v_1,\ldots,v_r\}$, where $1\le k\le r$. In other words, for every $v\in V\setminus V_1$, we have $B^*_v\in\{0,1\}$. For $\epsilon>0$, it is always possible to find a sufficiently small δB from a set of positive Lebesgue measures and impose a perturbation near B^*: $B^{**}=B^*+\delta B$ such that $\|\delta B\|<\epsilon$ and

$$\begin{cases}\dfrac{1}{\deg(v)}\displaystyle\sum_{u\in N_v}B^{**}_u>\sigma & \text{if } v\in V_1 \text{ or } B^*_v=1,\\[2ex] \dfrac{1}{\deg(v)}\displaystyle\sum_{u\in N_v}B^{**}_u<\sigma & \text{if } B^*_v=0.\end{cases}$$

By treating B^{**} as the initial security state at time $t=0$, there exists a time interval $[0,t_0)$ such that

- for every node v with $B^*_v=\sigma$, $B_v(t)$ increases strictly monotonically toward 1 for $t\in[0,t_0)$;
- for every node v with $B^*_v=1$, we have $B_v(t)=1$ for $t\in[0,t_0)$;
- for every node v with $B^*_v=0$, $B_v(t)$ does not decrease for $t\in[0,t_0)$.

Since for every v with $B^{**}_v=\sigma$, we have $B_v(t)\to 1$ as $t\to\infty$, it follows that B^* with $B^*_v=\sigma$ for some v is unstable. □

10.2. Proof of Theorem 4.7

Proof. From the condition $\underline{\lim}_{n\to\infty}\phi(n)>\sigma$, for almost every sequence of $\phi(n)$ we can pick some $\mu>\mu'>0$ such that $\phi(n)>\sigma+\mu>\sigma+\mu'$ for sufficiently large n. Recall the random variable $\chi_v(S)$:

$$\chi_v(S)=\begin{cases}1, & v\in S,\\ 0, & v\notin S.\end{cases}$$

Note that $\mathsf{P}(\chi_v(S) = 1) = B_v(0)$. Let ζ_{vu} be a random variable indicating the link between (from) node u and (to) node v, namely

$$\zeta_{vu} = \begin{cases} 1, & (u, v) \in E(n), \\ 0, & (u, v) \notin E(n). \end{cases}$$

According to (3.2), we have

$$\mathsf{P}(\zeta_{vu} = 1) = p_{vu}(n) = \frac{d_v(n)d_u(n)}{\sum_{k\in V(n)} d_k(n)}.$$

Since we assumed that the $B_v(0)$'s are independent of each other and also independent of the linking of edges in $G(n)$, ζ_{vu} and $\chi_u(S)$ are independent with respect to u. Our goal is to estimate the probability of event A_v as defined by

$$A_v = \left\{ \frac{1}{\deg(v)} \sum_{u\in N_v} B_u(0) < \sigma \right\} = \left\{ \frac{1}{\deg(v)} \sum_{u\in V(n)} B_u(0) \cdot \zeta_{vu} < \sigma \right\},$$

namely $\mathsf{P}(A_v) = \mathsf{P}(\sum_{u\in V(n)} \zeta_{vu} \cdot B_u(0) < \sigma \cdot \deg(v))$.

Note that the random variables ζ_{vu} for all $u \in V(n)$ are independent of each other. The expectation is $\mathsf{E}(\zeta_{vu}) = p_{vu}(n)$, and the variance is $\mathsf{Var}(\zeta_{vu}) = p_{vu}(n)(1 - p_{vu}(n))$. Because $\mathsf{E}(\chi_u(S) \cdot \zeta_{vu}) = B_u(0)p_{vu}(n)$ and the random variable has only two states, we have

$$\begin{aligned}
\mathsf{P}(A_v) &= \mathsf{P}\left(\frac{1}{\sqrt{\sum_{u\in V(n)} \mathsf{Var}(\zeta_{vu})B_u^2(0)}} \sum_{u\in V(n)} [\zeta_{vu}B_u(0) - \mathsf{E}(\zeta_{vu})B_u(0)] \right. \\
&\quad \left. < \frac{\sigma \cdot \deg(v) - \sum_{u\in V(n)} \mathsf{E}(\zeta_{vu} \cdot \chi_u(S))}{\sqrt{\sum_{u\in V(n)} \mathsf{Var}(\zeta_{vu} \cdot \chi_u(S))}} \right) \\
&= \mathsf{P}\left(\frac{1}{\sqrt{\sum_{u\in V(n)} \mathsf{Var}(\zeta_{vu})B_u^2(0)}} \sum_{u\in V(n)} [\zeta_{vu} \cdot B_u(0) - B_u(0) \cdot p_{vu}(n)] \right. \\
&\quad < \frac{d_v}{s_{n,v}} \left[\sigma - \frac{\sum_{u\in V(n)} \chi_u(S) \cdot \deg(u)}{\sum_{p\in V(n)} \deg(p)} \right] + \sigma \frac{\deg(v) - d_v}{s_{n,v}} \\
&\quad + \frac{d_v}{s_{n,v}} \left[\frac{\sum_{u\in V(n)} \chi_u(S) \deg(u)}{\sum_{p\in V(n)} \deg(p)} \frac{\sum_{v\in V(n)} d_v - \sum_{v\in V(n)} \deg(v)}{\sum_{v\in V(n)} d(v)} \right. \\
&\quad \left. \left. + \frac{\sum_{u\in V(n)} \deg(u)\chi_u(S) - \sum_{u\in V(n)} d_u B_u(0)}{\sum_{p\in V(n)} d_p} \right] \right),
\end{aligned}$$

where $s_{n,v}^2$ is defined in (4.2). Since $\mathsf{Var}[\zeta_{v,u}B_u(0)] = B_u(0)^2 p_{vu}(1 - p_{vu})$, we have $\sum_{u\in V(n)} \mathsf{Var}[\zeta_{v,u}B_u(0)] = s_{n,v}^2$.

Note that assumption (i) implies

$$\lim_{n\to\infty} \frac{1}{s_{n,v}^3} \sum_{u\in V(n)} \{\mathsf{E}\left|\zeta_{v,u} B_u(0) - \mathsf{E}(\zeta_{v,u} B_u(0))\right|^3\} = \lim_{n\to\infty} \frac{q_{n,v}}{s_{n,v}^3} = 0,$$

with $q_{n,v}$ defined in (4.3). This guarantees the Lyapunov condition in the central limit theorem (with $\delta = 1$) [10]. So as $n \to \infty$,

$$\frac{1}{\sqrt{s_{n,v}^2}} \sum_{u\in V(n)} [\zeta_{v,u} B_u(0) - B_u(0) p_{vu}] \to N(0, 1) \tag{10.1}$$

in distribution uniformly as $n \to \infty$. We call this asymptotic normal random variable ϕ_v.

In addition, we observe that

$$\sigma \frac{\deg(v) - d_v}{s_{n,v}} = \sigma \frac{d_v}{s_{n,v}} \frac{\deg(v) - d_v}{d_v} = \sigma \frac{d_v}{s_{n,v}} \frac{\deg(v) - d_v}{w_{n,v}} \frac{w_{n,v}}{d_v} \to o(1) \frac{d_v}{s_{n,v}}, \tag{10.2}$$

with $w_{n,v}$ defined in (4.4), with probability 1. This is because the term $(\deg(v) - d_v)/w_{n,v}$ converges to the standard Gaussian random variable owing to the Lyapunov central limit theorem, where the Lyapunov condition is guaranteed by assumption (ii) with $g_{n,v}$, which is defined in (4.5), denoting the third-order moment of $\zeta_{v,u}$ for all $u \in V(n)$, and because

$$\frac{w_{n,v}}{d_v} \le \frac{1}{\sqrt{d_v}} \to 0$$

as $n \to \infty$, owing to assumption (iii). Furthermore, we observe that

$$\begin{aligned} &\frac{\sum_{v\in V(n)} d_v - \sum_{v\in V(n)} \deg(v)}{\sum_{v\in V(n)} d(v)} \\ &= \frac{\sum_{v\in V(n)} d_v - \sum_{v\in V(n)} \deg(v)}{\sqrt{\sum_{v\in V(n)} w_{n,v}^2}} \frac{\sqrt{\sum_{v\in V(n)} w_{n,v}^2}}{\sum_{v\in V(n)} d(v)} \to 0 \end{aligned} \tag{10.3}$$

almost surely, because

$$\frac{\sum_{v\in V(n)} d_v - \sum_{v\in V(n)} \deg(v)}{\sqrt{\sum_{v\in V(n)} w_{n,v}^2}}$$

converges to the standard Gaussian random variable, owing to the Lyapunov central limit theorem, where the Lyapunov condition is guaranteed by assumption (iv), and

$$\frac{\sqrt{\sum_{v\in V(n)} w_{n,v}^2}}{\sum_{v\in V(n)} d(v)} \le \frac{1}{\sqrt{\sum_{v\in V(n)} d_v}} \to 0,$$

owing to assumption (iii). We further observe that

$$\begin{aligned}&\frac{\sum_{u\in V(n)}\deg(u)\chi_u(S)-\sum_{u\in V(n)}d_uB_u(0)}{\sum_{p\in V(n)}d_p}\\&=\frac{\sum_{u\in V(n)}\deg(u)\chi_u(S)-\sum_{u\in V(n)}d_uB_u(0)}{\sqrt{\sum_{v\in v(n)}s_{n,v}^2}}\frac{\sqrt{\sum_{v\in v(n)}s_{n,v}^2}}{\sum_{p\in V(n)}d_p}\to 0\end{aligned}\tag{10.4}$$

almost surely, because

$$\frac{\sum_{u\in V(n)}\deg(u)\chi_u(S)-\sum_{u\in V(n)}d_uB_u(0)}{\sqrt{\sum_{v\in v(n)}s_{n,v}^2}}$$

converges to the standard Gaussian random variable, owing to the Lyapunov central limit theorem, where the Lyapunov condition is guaranteed by assumption (v), and

$$\frac{\sqrt{\sum_{v\in v(n)}s_{n,v}^2}}{\sum_{p\in V(n)}d_p}\le\frac{1}{\sqrt{\sum_{p\in V(n)}d_p}},$$

owing to assumption (iii). Combining (10.1), (10.2), (10.3), and (10.4) with the fact

$$\frac{\sum_{u\in V(n)}\chi_u(S)\deg(u)}{\sum_{p\in V(n)}\deg(p)}\le 1,$$

we conclude that there exists a random variable $\epsilon_{n,v}$ that converges to zero uniformly with probability 1 such that

$$\begin{aligned}\mathsf{P}(A_v)=\mathsf{P}\Bigg(&\frac{1}{\sqrt{\sum_{u\in V(n)}\mathsf{Var}(\zeta_{vu})B_u^2(0)}}\sum_{u\in V(n)}[\zeta_{vu}B_u(0)-\mathsf{E}(\zeta_{vu})B_u(0)]\\&<\frac{d_v}{s_{n,v}}\Big(\sigma-\phi(n)+\epsilon_{n,v}\Big)\Bigg).\end{aligned}$$

Finally, we observe that $\sigma-\phi(n)\le-\mu$ holds with probability 1. This inequality, together with the convergence rate in the central limit theorem [15], implies

$$\left|\mathsf{P}(A_v\mid\eta\ge\sigma+\mu)-\Phi(t_n(v))\right|\le C\frac{q_{n,v}/s_{n,v}^3}{(1+|t_n(v)|^3)},$$

where $t_n(v)=-\mu'\deg(v)/s_{n,v}$, where we note that $\mu'<\mu$, for sufficiently large n, $\Phi(\cdot)$ is the probability function of the standard normal distribution, and C is a universal constant.

Since

$$\Phi(t_n(v))=\frac{2}{\sqrt{\pi}}\int_{-\infty}^{t_n(v)}\exp\left(-\frac{y^2}{2}\right)dy$$

and

$$\int_{-\infty}^{x} \exp\left(-y^2/2\right)\, dy \le \frac{\exp\left(-x^2/2\right)}{-x} \quad \text{for all } x \le 0,$$

we have

$$\sum_{v\in V(n)} \Phi\left(t_n(v)\right) < \frac{2n}{\sqrt{\pi}} \frac{\exp\left[-(\min_v t_n(v))^2/2\right]}{\min_v t_n(v)}. \tag{10.5}$$

Under assumption (iii), the limit superior of the logarithm of the right-hand side of (10.5) becomes

$$\overline{\lim}_{n\to\infty} \left\{ \ln\left(\frac{2}{\sqrt{\pi}}\right) + \ln(n) - [\min_v t_n(v)]^2/2 - \ln[\min_v t_n(v)] \right\} = -\infty.$$

This implies $\sum_{v\in V(n)} \Phi\left(t_n(v)\right) \to 0$ as $n \to \infty$. In addition, we observe that

$$\sum_{v\in V(n)} \frac{C q_{n,v}}{1+|t_{n,v}|^3} \le C \sum_{v\in V(n)} \frac{q_{n,v}}{d_v^3} \le C \sum_{v\in V(n)} \frac{1}{d_v^2}$$

converges to zero, owing to assumption (vi).

Putting the above together, we have

$$\begin{aligned}
\lim_{n\to\infty} \mathsf{P}\left(\bigcup_{v\in V(n)} A_v \right) &\le \overline{\lim}_{n\to\infty} \sum_{v\in V(n)} \mathsf{P}\left(A_v\right) \\
&\le \overline{\lim}_{n\to\infty} \sum_{v\in V(n)} \Phi\left(t_n(v)\right) + C\overline{\lim}_{n\to\infty} \sum_{v\in V(n)} \frac{C q_{n,v}}{1+|t_n(v)|^3} \\
&= 0.
\end{aligned}$$

Applying Theorem 4.2, we see that for each event not belonging to $\bigcup_v A_v$, we have $\lim_{t\to\infty} B_v(t) = 1$ for all $v \in V(n)$. This proves the first part of the theorem.

We can prove the second part analogously. This completes the proof. □

10.3. Proof of Lemma 5.1

Proof. We only prove part (i), because part (ii) can be proved analogously. In order to simplify the presentation, let $Y_v(t) = \frac{1}{\deg(v)} \sum_{u\in N_v} B_u(t)$ be the average portion of v's `secure` neighbors at time t.

First, we need to show that $Y_v(t) > \tau$ holds for all $v \in V$ and $t \ge 0$. For this purpose, we let $\tau^* > \tau$ be such that $Y_v(0) > \tau^*$ holds for all $v \in V$, and we show that $Y_v(t) > \tau^*$ holds for all $t \ge 0$. We observe that $Y_v(t) > \tau^*$ holds in a small time interval starting at time $t = 0$, because of the continuity of the $B_v(t)$ with respect to t. Let t_1 be the first time at which $\min_{v\in V} Y_v(t) = \tau^*$, namely

$$t_1 = \inf\{\mathsf{t} : \min_{v\in V} Y_v(t) > \tau^* \text{ for all } t \in [0, \mathsf{t}) \in V\}.$$

We show that $t_1 = +\infty$ as follows.

Suppose $t_1 < +\infty$. We claim that $\min_{v\in V} Y_v(t)$ is nonincreasing in an interval starting at time t_1; otherwise, $d(\min_{v\in V} Y_v(t))/dt > 0$ in a small interval starting at time t_1, and $\min_v Y_v(t) > \tau^*$ in that small interval, which contradicts the definition of t_1.

Let $V^* = \arg\min_{v\in V} Y_v(t_1)$. For each $v' \in V^*$, we have

$$\begin{aligned}\frac{d}{dt}\left[\frac{1}{\deg(v')}\sum_{u\in N_{v'}} B_u(t)\right]\Bigg|_{t=t_1} &= \frac{1}{\deg(v')}\sum_{u\in N_{v'}} \frac{dB_u(t)}{dt}\Bigg|_{t=t_1}\\ &= \frac{1}{\deg(v')}\sum_{u\in N_{v'}}\left[f_{\mathrm{RB}}\left(\frac{1}{\deg(u)}\sum_{w\in N_u} B_w(t_1)\right) - B_u(t_1)\right]\\ &\geq \frac{1}{\deg(v')}\sum_{u\in N_{v'}} f_{\mathrm{RB}}(\tau^*) - \tau^* = f_{\mathrm{RB}}(\tau^*) - \tau^* > 0,\end{aligned}$$

owing to $\tau^* > \tau$. Hence $\min_v Y_v(t)$ is strictly increasing in an interval starting at time t_1. This contradicts that $\min_{v\in V} Y_v(t)$ is nonincreasing in an interval starting at time t_1. The contradiction was caused by the assumption $t_1 < +\infty$. Therefore, we have $t_1 = +\infty$.

Second, we need to show that $\min_{v\in V} B_v(t)$ increases monotonically. Let $V_t = \{u : B_u(t) = \arg\min_v B_v(t)\}$, which may not be a singlet. For $t = 0$, the given initial condition $\frac{1}{\deg(v)}\sum_{u\in N_v} B_u(0) > \tau$ for all $v \in V$ implies that for each $v_* \in V_0$, we have

$$\begin{aligned}\frac{dB_{v_*}(t)}{dt}\Bigg|_{t=0} &= f_{\mathrm{RB}}\left(\frac{1}{\deg(v_*)}\sum_{u\in N_{v_*}} B_u(0)\right) - B_{v_*}(0)\\ &> \frac{1}{\deg(v_*)}\sum_{u\in N_{v_*}} B_u(0) - B_{v_*}(0) \geq 0,\end{aligned}$$

because $f_{\mathrm{RB}}(s) > s$ for $s > \tau$. This means that $\min_v B_v(t)$ is strictly increasing in a small time interval starting at $t = 0$.

Let t_2 be the maximum time that $\min_v B_v(t)$ is strictly increasing, namely

$$t_2 = \sup\left\{\mathsf{t} : \min_v B_v(t) \text{ is strictly increasing in } [0, \mathsf{t})\right\}.$$

We now show that $t_2 = +\infty$. Suppose $t_2 < +\infty$, meaning that $\min_v B_v(t)$ is not strictly increasing at $t = t_2$. However, for each $v_2 \in V_{t_2}$, we have

$$\begin{aligned}\frac{dB_{v_2}(t)}{dt}\Bigg|_{t=t_2} &= f_{\mathrm{RB}}\left(\frac{1}{\deg(v_2)}\sum_{u\in N_{v_2}} B_u(t_2)\right) - B_{v_2}(t_2)\\ &> \frac{1}{\deg(v_2)}\sum_{u\in N_{v_2}} B_u(t_2) - B_{v_2}(t_2) \geq 0,\end{aligned}$$

because $\frac{1}{\deg(v_2)}\sum_{u\in N_{v_2}} B_u(t_2) > \tau$ and $f_{\mathrm{RB}}(s) > s$ for all $s > \tau$. This implies that $\min_v B_v(t)$ is strictly increasing at $t = t_2$, which contradicts the definition of t_2. Therefore, $t_2 = +\infty$, namely $\min_v B_v(t)$ is strictly increasing for all $t \geq 0$. □

10.4. Proof of Theorem 5.2

Proof. We prove the first part only, since the second part can be proved analogously. Lemma 5.1 shows that $\min_v B_v(t)$ increases monotonically, meaning that $\lim_{t\to\infty} \min_v B_v(t)$ exists. In order to show that $\lim_{t\to\infty} B_v(t) = 1$ for all $v \in V$, it suffices to show that $\lim_{t\to\infty} \min_v B_v(t) = 1$. Suppose $\lim_{t\to\infty} \min_v B_v(t) < 1$. There are two cases, but both cause contradictions, as we elaborate below. Therefore, we have $\lim_{t\to\infty} \min_v B_v(t) = 1$.

Case 1: $\tau < \lim_{t\to\infty} \min_v B_v(t) < 1$. There exist $\tau < \tau_1 < \tau_2 < 1$ and $T > 0$ such that $\tau_1 \le \min_v B_v(t) \le \tau_2$ for all $t \ge T$. Since $f_{\text{RB}}(x) - x > 0$ for all $x \in [\tau_1, \tau_2]$ and f_{RB} is continuous, we can find some $\delta > 0$ such that $f_{\text{RB}}(x) - x > \delta$ for all $x \in [\tau_1, \tau_2]$. Let V_t be the index set of $\arg\min_v B_v(t)$. For each $v_* \in V_t$, we have

$$\frac{dB_{v_*}(t)}{dt} = f_{\text{RB}}\left(\frac{1}{\deg(v_*)} \sum_{u\in N_{v_*}} B_u(t)\right) - B_{v_*}(t) \ge f_{\text{RB}}(B_{v_*}(t)) - B_{v_*}(t) > \delta \tag{10.6}$$

for all $t > T$. This leads to

$$\min_v B_v(t) > \min_v B_v(T) + \delta(t - T).$$

Since $\min_v B_v(T) + \delta(t - T) \to +\infty$ as $t \to \infty$, this contradicts $B_v(t) \le 1$.

Case 2: $\lim_{t\to\infty} \min_v B_v(t) \le \tau$. Let V_t be the index set of $\arg\min_v B_v(t)$. Since $\frac{1}{\deg(v)} \sum_{u\in N_v} B_u(t) > \tau$ for all v and t, there exist $T' > 0$ and $\delta' > 0$ such that for each $v_* \in V_t$,

$$f_{\text{RB}}\left(\frac{1}{\deg(v_*)} \sum_{u\in N_{v_*}} B_u(t)\right) - B_{v_*}(t) > \delta'$$

holds for all $t > T'$. By the same argument as in Case 1, we can show that

$$\lim_{t\to\infty} \min_v B_v(t) = +\infty,$$

which contradicts $B_v(t) \le 1$. □

10.5. Proof of Theorem 5.4

Proof. Part (i) can be seen by considering any perturbation near each equilibrium B^*. For these equilibria, we can use linearization to analyze the convergence rates. Let $B(t) = ([B_v(t)]_{v\in V})^\top$, let A be the adjacency matrix of G, $D = \text{diag}\left([\deg(v)]_{v=1}^n\right)$, $\mathbf{1} = [1, \ldots, 1]^\top$, $\mathbf{0} = [0, \ldots, 0]^\top$, let δB be the variation of $B(t)$ near $\mathbf{1}$ or $\mathbf{0}$, let I_n denote the n-dimensional identity matrix, let $z = 1$ indicate that we are considering the convergence rate of stable equilibrium $\mathbf{1}$, and let $z = 0$ indicate that we are considering the convergence rate of stable equilibrium $\mathbf{0}$. Then linearization leads to

$$\frac{d\delta B(t)}{dt} = \left[f'_{\text{RB}}(z)D^{-1}A - I_n\right]\delta B.$$

The convergence rate is estimated by the largest real part of all eigenvalues of the matrix $f'_{\text{RB}}(z)D^{-1}A - I_n$. Since the largest eigenvalue of $D^{-1}A$ equals 1, the convergence rate is estimated as $O(\exp[(f'_{\text{RB}}(z) - 1)t]$ for both $z = 0$ and $z = 1$.

For proving part (ii), suppose at equilibrium B^* that $B^*_{v_k} = \tau$ for $v_k \in V_1 = \{v_1, \ldots, v_r\}$, where $1 \le k \le r \le n$. In other words, for every $v \in V \setminus V_1$, we have $B^*_v \in \{0, 1\}$. For $\epsilon > 0$, it is always possible to find a sufficiently small δB from a set of positive Lebesgue measures and impose a perturbation near B^* while satisfying the following: $B^{**} = B^* + \delta B$ such that $\|\delta B\| < \epsilon$ and

$$\frac{1}{\deg(v)} \sum_{u \in N_v} B^{**}_u \begin{cases} > \tau & \text{if } B^*_v \ge \tau, \\ < \tau & \text{if } B^*_v < \tau. \end{cases} \tag{10.7}$$

Let us treat B^{**} as the initial security state at time $t = 0$. For every node v with $B^*_v \ge \tau$, we have

$$\left.\frac{dB_v(t)}{dt}\right|_{t=0} = f_{\text{RB}}\left(\frac{1}{\deg(v)} \sum_{u \in N_v} B^{**}_u\right) - B^*_v > \frac{1}{\deg(v)} \sum_{u \in N_v} B^{**}_u - B^{**}_v \ge 0.$$

This means that there is a time interval $[0, t_0)$ in which for every node v with $B^*_v \ge \tau$, $B_v(t)$ is strictly monotonically increasing. For every node v with $B^*_v < \tau$, we have

$$\left.\frac{dB_v(t)}{dt}\right|_{t=0} = f_{\text{RB}}\left(\frac{1}{\deg(v)} \sum_{u \in N_v} B^{**}_u\right) - B^*_v < \frac{1}{\deg(v)} \sum_{u \in N_v} B^{**}_u - B^{**}_v \le 0,$$

which means that the corresponding $B_v(t)$'s are strictly decreasing for a small time interval $t \in [0, t_0)$. In summary, for any small perturbation with (10.7) as the initial security state, $B_v(t)$ leaves the equilibrium. Therefore, B^* with $B^*_v = \tau$ for some v is unstable. □

ACKNOWLEDGMENTS

We thank the reviewers for their helpful comments that allowed us to improve the paper.

FUNDING

Shouhuai Xu was supported in part by ARO Grant #W911NF-12-1-0286, AFOSR MURI Grant #FA9550-08-1-0265, and NSF Grant #1111925. Wenlian Lu was jointly supported by the Marie Curie International Incoming Fellowship from the European Commission (no. FP7-PEOPLE-2011-IIF-302421), the National Natural Sciences Foundation of China (no. 61273309), the Shanghai Guidance of Science and Technology (SGST) (no. 09DZ2272900), and the Laboratory of Mathematics for Nonlinear Science, Fudan University. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of any of the funding agencies.

REFERENCES

[1] D. Aitel. "Nematodes—Beneficial Worms." Available online (http://www.immunityinc.com/downloads/nematodes.pdf), September 2005.

[2] R. Albert, H. Jeong, and A. Barabasi. "Error and Attack Tolerance of Complex Networks." *Nature* 406 (2000), 378–482.

[3] F. Ball, D. Sirl, and P. Trapman. "Threshold Behaviour and Final Outcome of an Epidemic on a Random Network with Household Structure." *Adv. in Appl. Probab* 41:3 (2009), 765–796.

[4] F. Ball, D. Sirl, and P. Trapman. "Analysis of a Stochastic {SIR} Epidemic on a Random Network Incorporating Household Structure." *Mathematical Biosciences* 224:2 (2010), 53–73.

[5] A. Barabasi and R. Albert. "Emergence of Scaling in Random Networks." *Science* 286 (1999), 509–512.

[6] N. Berger, C. Borgs, J. Chayes, and A. Saberi. "On the Spread of Viruses on the Internet." In *Proceedings of the Sixteenth Annual ACM–SIAM Symposium on Discrete Algorithms, SODA '05*, pp. 301–310, 2005.

[7] F. Castaneda, E. Sezer, and J. Xu. "Worm vs. Worm: Preliminary Study of an Active Counter-attack Mechanism." In *Proceedings of the 2004 ACM Workshop on Rapid Malcode (WORM '04)*, pp. 83–93, 2004.

[8] D. Chakrabarti, Y. Wang, C. Wang, J. Leskovec, and C. Faloutsos. "Epidemic Thresholds in Real Networks." *ACM Trans. Inf. Syst. Secur.* 10:4 (2008), 1–26.

[9] S. Chatterjee and R. Durrett. "Contact Processes on Random Graphs with Power Law Degree Distributions Have Critical Value 0." *Ann. Probab.* 37:6 (2009), 2332–2356.

[10] K. Chung. *A Course in Probability Theory*, 2nd edition. Academic Press, 2000.

[11] F. Chung and L. Lu. *Complex Graphs and Networks*, CBMS Regional Conference Series in Mathematics. American Mathematical Society, 2006.

[12] R. Durrett. *Random Graph Dynamics*. Cambridge University Press, 2007.

[13] A. Ganesh, L. Massoulie, and D. Towsley. "The Effect of Network Topology on the Spread of Epidemics." In *Proceedings of IEEE Infocom 2005*, 2005.

[14] H. Hethcote. "The Mathematics of Infectious Diseases." *SIAM Rev.* 42:4 (2000), 599–653.

[15] P. Hill. *Rates of Convergence in the Central Limit Theorem.* Pitman Advanced Publisher, 1982.

[16] J. Kephart and S. White. "Directed-Graph Epidemiological Models of Computer Viruses." In *IEEE Symposium on Security and Privacy*, pp. 343–361, 1991.

[17] J. Kephart and S. White. "Measuring and Modeling Computer Virus Prevalence." In *IEEE Symposium on Security and Privacy*, pp. 2–15, 1993.

[18] W. Kermack and A. McKendrick. "A Contribution to the Mathematical Theory of Epidemics." *Proc. of Roy. Soc. Lond. A* 115 (1927), 700–721.

[19] J. Kesan and C. Hayes. "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace." *Harv. J. L. & Tech.* 25:2 (2012), 417–527.

[20] T. Liggett. *Stochastic Interacting Systems: Contact, Voter and Exclusion Processes*. Springer-Verlag, 1999.

[21] H. Lin. "Lifting the Veil on Cyber Offense." *IEEE Security & Privacy* 7:4 (2009), 15–21.

[22] L. Lovasz. "Eigenvalues of Graphs." Available online (http://www.cs.elte.hu/~lovasz/eigenvals-x.pdf), 2007.

[23] N. Masuda, N. Gibert, and S. Redner. "Heterogeneous Voter Models." *Phys. Rev. E* 82 (2010), 010103.

[24] W. Matthews. "U.S. Said to Need Stronger, Active Cyber Defenses." Available online (http://www.defensenews.com/story.php?i=4824730), October 2010.

[25] A. McKendrick. "Applications of Mathematics to Medical Problems." *Proc. of Edin. Math. Society* 14 (1926), 98–130.

[26] D. Moore, C. Shannon, G. Voelker, and S. Savage. "Internet Quarantine: Requirements for Containing Self-Propagating Code." In *INFOCOM'03*, 2003.

[27] P. A. P. Moran. *The Statistical Processes of Evolutionary Theory*. Clarendon Press, 1962.

[28] T. Mountford, J.-C. Mourrat, D. Valesin, and Q. Yao. "Exponential Extinction Time of the Contact Process on Finite Graphs". arXiv:1203.2972, 2012.

[29] T. Mountford, D. Valesin, and Q. Yao. "Metastable Densities for Contact Processes on Power Law Random Graphs." arXiv:1106.4336, 2012.

[30] R. Naraine. "'Friendly' Welchia Worm Wreaking Havoc." Available online (http://www.internetnews.com/ent-news/article.php/3065761/Friendly-Welchia-Worm-Wreaking-Havoc.htm), August 19, 2003.

[31] M. A. Nowak, *Evolutionary Dynamics: Exploring the Equations of Life*. Harvard University Press, 2006.

[32] R. Pastor-Satorras and A. Vespignani. "Epidemic Spreading in Scale-Free Networks." *Phys. Rev. Lett.* 86:14 (2001), 3200–3203.

[33] E. Pugliese and C. Castellano. "Heterogeneous Pair Approximation for Voter Models on Networks." *Europhysics Letters* 88:5 (2009), 58004.

[34] B. Schneier. "Benevolent worms." Available online (http://www.schneier.com/blog/archives/2008/02/benevolent_worm_1.html), February 19, 2008.

[35] F. Schweitzer and L. Behera. "Nonlinear Voter Models: The Transition from Invasion to Coexistence." *European Physical Journal B* 67 (2009), 301–318.

[36] L. Shaughnessy. "The Internet: Frontline of the Next War?" Available online (http://www.cnn.com/2011/11/07/us/darpa/), November 7, 2011.

[37] V. Sood, T. Antal, and S. Redner. "Voter Models on Heterogeneous Networks." *Physical Review E* 77:4 (2008), 1–13.

[38] S. Staniford, V. Paxson, and N. Weaver. "How to Own the Internet in Your Spare Time." In *Proceedings of the 11th USENIX Security Symposium*, pp. 149–167, 2002.

[39] S. Staniford, D. Moore, V. Paxson, and N. Weaver. "The Top Speed of Flash Worms." In *Proceedings of the 2004 ACM Workshop on Rapid Malcode (WORM'04)*, pp. 33–42. ACM Press, 2004.

[40] P. Van Mieghem, J. Omic, and R. Kooij. "Virus Spread in Networks." *IEEE/ACM Trans. Netw.* 17 (2009), 1–14.

[41] M. Vojnovic and A. Ganesh. "On the Race of Worms, Alerts, and Patches." *IEEE/ACM Trans. Netw.* 16 (2008), 1066–1079.

[42] Y. Wang, D. Chakrabarti, C. Wang, and C. Faloutsos. "Epidemic Spreading in Real Networks: An Eigenvalue Viewpoint." In *Proc. of the 22nd IEEE Symposium on Reliable Distributed Systems (SRDS'03)*, pp. 25–34, 2003.

[43] N. Weaver and D. Ellis. "White Worms Don't Work." *;login:* (Usenix) 31 (2006), 33–38.

[44] H. S. N. Wire. "Active Cyber-Defense Strategy Best Deterrent against Cyber-Attacks." Available online (http://www.homelandsecuritynewswire.com/active-cyber-defense-strategy-best-deterrent-against-cyber-attacks), June 28, 2011.

[45] J. Wolf. "Update 2-U.S. Says Will Boost Its Cyber Arsenal." Available online (http://www.reuters.com/article/2011/11/07/cyber-usa-offensive- idUSN1E7A61YQ20111107), November 7, 2011.

[46] S. Xu, W. Lu, and Z. Zhan. "A Stochastic Model of Multivirus Dynamics." *IEEE Trans. Dependable Sec. Comput.* 9:1 (2012), 30–45.