IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 20, 2017, accepted September 18, 2017, date of publication September 29, 2017,
date of current version October 25, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2757944

Security Evaluation of the Cyber Networks Under Advanced Persistent Threats

LU-XING YANG[1], (Member, IEEE), PENGDENG LI[2], XIAOFAN YANG[2], (Member, IEEE), AND YUAN YAN TANG[3], (Fellow, IEEE)

[1]Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, Delft GA 2600, The Netherlands
[2]School of Software Engineering, Chongqing University, Chongqing 400044, China
[3]Department of Computer and Information Science, University of Macau, Macau 999078, China

Corresponding author: Xiaofan Yang (xfyang1964@gmail.com)

This work was supported in part by the Natural Science Foundation of China under Grant 61572006, in part by the Sci-Tech Support Program of China under Grant 2015BAF05B03, and in part by the Fundamental Research Funds for the Central Universities under Grant 106112014CDJZR008823.

ABSTRACT Advanced persistent threats (APTs) pose a grave threat to cyberspace, because they deactivate all the conventional cyber defense mechanisms. This paper addresses the issue of evaluating the security of the cyber networks under APTs. For this purpose, a dynamic model capturing the APT-based cyber-attack-defense processes is proposed. Theoretical analysis shows that this model admits a globally stable equilibrium. On this basis, a new security metric known as the equilibrium security is suggested. The impact of several factors on the equilibrium security is revealed through theoretical analysis or computer simulation. These findings contribute to the development of feasible security solutions against APTs.

INDEX TERMS Cyberspace, security, measurement, nonlinear dynamical systems, stability.

I. INTRODUCTION

Cyberspace has come to be an integral and indispensable part of modern society. Day and night, massive data are transmitted ceaselessly from host to host through multifarious cyber networks [1], [2]. However, cyberspace is vulnerable to a wide range of cyber threats. Sophisticated cyber perpetrators often exploit cyber attack techniques to achieve their political, economic and military goals. In light of the risk and consequence of cyber attacks, enhancing the security and resilience of cyberspace has become an urgent task in the field of information security [3]–[5]. As a proverb says, however, you cannot manage if you cannot measure. Before a feasible cyber security solution is worked out, the security of cyber networks must be evaluated accurately [6]–[8].

Advanced persistent threats (APTs) are a newly emerging type of cyber attacks. With a clear goal, an APT attack is highly-targeted, well-organized, well-resourced, technologically-advanced, covert and persistent [9]–[11]. In sharp contrast with APTs, all the conventional cyber threats rely on limited available resources and hence can only be conducted in the one-shot or repeated way, leading to a time discontinuity. APTs pose an especially severe threat to cyberspace, because they invalidate all the conventional cyber defense mechanisms developed and implemented for defending against one-shot or/and repeated cyber attacks. Indeed, it was reported that, in the last decade, the number of the APT events all over the world was soaring [12]. To effectively withstand APTs, the security of the cyber networks under APTs must be evaluated accurately. Due to the time continuity of APTs, however, existing security evaluation methods, which were developed to cope with one-shot or repeated cyber attacks, are not applicable to APTs [13]–[17]. Recently, Pendleton *et al.* [18] considered the expected fraction of the compromised nodes in a cyber network as a security metric of the network. However, as the expected fraction is varying over time, the technical feasibility of the suggestion is questionable.

To measure the security of the cyber networks under APTs, a mathematical model accurately capturing the APT-based cyber attack-defense processes is requisite. In view of the time continuity of APT attacks, the resulting model must be dynamic and continuous-time, which can be studied with the aid of the well-established theory on continuous-time dynamical systems. By contrast, the mathematical models characterizing one-shot cyber attacks are static, while the models capturing the repeated cyber attack-defense processes are discrete-time. The modeling technique of individual-level dynamical systems, which has been applied to several

areas such as the epidemic spreading [19]–[21], the malware spreading [22]–[29], the rumor spreading [30], [31] and the viral marketing [32], is especially suited to the accurate modeling and detailed analysis of the APT-based cyber attack-defense processes, because the underlying structure of the cyber network can be fully accommodated [33] and hence the cyber attack-defenses processes can be described more accurately. Towards this direction, a number of APT-based cyber attack-defense models have been suggested [34]–[37]. However, these models either assume that the attacker is within the network [34]–[36] or assume that the attack strengths to all the hosts are always the same [37]. In most cases, the attacker is outside the targeted cyber network. Furthermore, the attacker may be strategic, that is, he may attack different hosts in the network with separate strengths. To our knowledge, to date no APT-based cyber attack-defense model with a strategic external attacker has been reported in literature.

This paper focuses on the evaluation of the security of the cyber networks under APT attacks launched by strategic external attackers. For this purpose, an individual-level continuous-time dynamic model that accurately captures the APT-based cyber attack-defense processes with strategic external attackers is proposed. A detailed theoretical analysis shows that the model admits a globally stable equilibrium. This implies that, starting from any initial state, the model will approach the equilibrium. On this basis, a new security metric of cyber networks, which is referred to as the equilibrium security, is defined as the expected fraction of the compromised nodes in the equilibrium. The impact of several factors on the equilibrium security is determined through theoretical analysis and computer simulation. These findings contribute to our understanding of the security of cyber networks under APTs as well as the development of feasible security solutions against APTs.

The remaining materials are organized in this fashion. Sections 2 and 3 describe and study an APT-based cyber attack-defense model, respectively. Section 4 introduces the notion of equilibrium security. The impact of different factors on the equilibrium security is examined in Sections 5 and 6. Finally, Section 7 closes this work.

II. THE MODELING OF THE CYBER ATTACK-DEFENSE PROCESSES UNDER APTs

For the purpose of evaluating the security of cyber networks under APTs, understanding the relevant cyber attack-defense processes is requisite. And this is the goal of this section.

A. THE CYBER NETWORK AND ITS STATE

Consider a cyber network $G = (V, E)$ interconnecting a set of hosts labeled $1, 2, \cdots, N$, where every node stands for a host, i.e., $V = \{1, 2, \cdots, N\}$, and for $1 \leq i, j \leq N$ $(i \neq j)$, $(i, j) \in E$ if and only if the host i can deliver messages directly to the host j through the network. Let $\mathbf{A}(G) = \left(a_{ij}\right)_{N\times N}$ denote the adjacency matrix for the network, where $a_{ij} = 1$ or 0 according as $(i, j) \in E$ or not. Hereafter, it is always assumed that the cyber network is *strongly connected*, i.e., there is a directed path from any node of the network to any other node. This assumption implies that the adjacency matrix for the network is *irreducible*, i.e., it cannot be recast as a block matrix of the form

$$\begin{pmatrix} \mathbf{A}_{11} & \mathbf{A}_{12} \\ \mathbf{0} & \mathbf{A}_{22} \end{pmatrix} \tag{1}$$

through a series of row-row exchanges and the corresponding column-column exchanges.

Suppose there is an attacker (an individual, a group or a nation state, to name a few) who is outside of the cyber network and will launch an APT attack on the network at time $t = 0$, with the intent of taking over some or all nodes of the network. Meanwhile, there is a defender (the owner or the administrator of the network, say) who will protect the network from the attack, with the goal of keeping the network under control. Henceforth, it is assumed that, at any time, every node of the network is either *secure*, i.e., under the defender's control, or *compromised*, i.e., under the attacker's control. Let $X_i(t) = 0$ and 1 denote that the node i is secure and compromised at time t, respectively. Then the state of the cyber network at time t is represented by the vector

$$\mathbf{X}(t) = (X_1(t), X_2(t), \cdots, X_N(t)). \tag{2}$$

Let $S_i(t)$ and $C_i(t)$ denote the probability of the node i being secure and compromised at time t, respectively.

$$S_i(t) = \Pr\{X_i(t) = 0\}, \tag{3}$$

$$C_i(t) = \Pr\{X_i(t) = 1\}. \tag{4}$$

As $S_i(t) + C_i(t) \equiv 1$, the vector

$$\mathbf{C}(t) = (C_1(t), \cdots, C_N(t))^T \tag{5}$$

represents the expected state of the cyber network at time t.

B. THE ATTACK AND DEFENSE STRATEGIES

In what follows, let $||\cdot||_1$ denote the 1-norm of real vectors. That is, for any $\mathbf{a} = (a_1, \cdots, a_n) \in \mathbb{R}^n$, we have $||\mathbf{a}||_1 = \sum_{i=1}^{n} |a_i|$.

The threat of an APT attack to the cyber network is twofold: the *external attack* and the *internal infection*. The external attack is led by the attacker, with the intent of compromising the secure nodes of the network. The attack strength to the secure node i is measured by αx_i, where the constant $\alpha > 0$ stands for the *attack level*, i.e., the technical level of the external attack, the constant $x_i \geq 0$ stands for the amount of the resources (manpower, money, say) per unit time consumed for attacking the node i. We refer to the vector $\mathbf{x} = (x_1, \cdots, x_N)$ as an *attack strategy*. The amount of the resources per unit time consumed for implementing the attack strategy $\mathbf{x}$ is $\sum_{i=1}^{N} x_i = ||\mathbf{x}||_1 > 0$.

The internal infection is caused by the compromised nodes of the network, with the intent of compromising the secure nodes of the network. At any time, the infection strength

of the compromised node i to the secure node j is βa_{ij}, where the constant $\beta > 0$ stands for the *infection level*, i.e., the technical level of the internal infection. The expected combined infection strength of all the compromised nodes of the network to the secure node i at time t is measured by $f\left(\beta \sum_{j=1}^{N} a_{ji} C_j(t)\right)$, where (a) $f(0) = 0$, because no internal infection occurs almost surely unless currently there is a node that is compromised with a positive probability; (b) $f(x) \leq x$ for all $x \geq 0$, because the combined infection strength of all the compromised nodes to a secure node is bounded from above by the sum of the infection strengths of all the compromised nodes to the secure node; (c) f is strictly increasing and concave, because the combined infection strength of all the compromised nodes to a secure node rises yet flattens out with the increase of the sum of the infection strengths of all the compromised nodes to the secure node; and (d) for technical reasons, f is assumed to be twice continuously differentiable. This set of conditions on the function f is referred to as the *generic conditions*, and those functions that satisfy the generic conditions are referred to as the *generic functions*.

Also, the defense of the cyber network against the APT attack is twofold: the *prevention* and the *recovery*. The prevention aims to prevent the secure nodes of the network from being compromised. The prevention strength of the secure node i is measured by δy_i, where the constant $\delta > 0$ stands for the *prevention level*, i.e., the technical level of the prevention, the constant $y_i > 0$ stands for the amount of the resources per unit time consumed for preventing the secure node i. We refer to the vector $\mathbf{y} = (y_1, \cdots, y_N)$ as a *prevention strategy*. The amount of the resources per unit time consumed for implementing the prevention strategy $\mathbf{y}$ is $\sum_{i=1}^{N} y_i = ||\mathbf{y}||_1$.

The recovery is intended to recover the compromised nodes of the network. The recovery strength of the compromised node i is gauged by γz_i, where the constant $\gamma > 0$ stands for the *recovery level*, i.e., the technical level of the recovery, the constant $z_i > 0$ stands for the amount of the resources per unit time consumed for recovering the compromised node i. We refer to the vector $\mathbf{z} = (z_1, \cdots, z_N)$ as a *recovery strategy*. The amount of the resources per unit time consumed for implementing the recovery strategy $\mathbf{z}$ is $\sum_{i=1}^{N} z_i = ||\mathbf{z}||_1$.

Furthermore, we refer to the combination of a prevention strategy and a recovery strategy, denoted $(\mathbf{y}, \mathbf{z})$, as a *defense strategy*. The amount of the resources per unit time consumed for implementing the defense scheme $(\mathbf{y}, \mathbf{z})$ is $\sum_{i=1}^{N} y_i + \sum_{i=1}^{N} z_i = ||\mathbf{y}||_1 + ||\mathbf{z}||_1$.

For later use, let us define three types of strategies as follows. Let $\mathbf{w} = (w_1, \cdots, w_N)$ denote an attack/prevention/recovery strategy. The strategy is *uniform* if all w_i are identical. That is,

$$\mathbf{w} = ||\mathbf{w}||_1 \cdot \left(\frac{1}{N}, \frac{1}{N}, \cdots, \frac{1}{N}\right). \tag{6}$$

The strategy is *degree-first* if w_i is linearly proportional to the out-degree of the node i. That is,

$$\mathbf{w} = ||\mathbf{w}||_1 \cdot \left(\frac{\sum_{j=1}^{N} a_{1j}}{\sum_{i,j=1}^{N} a_{ij}}, \cdots, \frac{\sum_{j=1}^{N} a_{Nj}}{\sum_{i,j=1}^{N} a_{ij}}\right). \tag{7}$$

The strategy is *degree-last* if w_i is inversely linearly proportional to the out-degree of the node i. That is,

$$\mathbf{w} = ||\mathbf{w}||_1 \cdot \left(\frac{\frac{1}{\sum_{j=1}^{N} a_{1j}}}{\sum_{i=1}^{N} \frac{1}{\sum_{j=1}^{N} a_{ij}}}, \cdots, \frac{\frac{1}{\sum_{j=1}^{N} a_{Nj}}}{\sum_{i=1}^{N} \frac{1}{\sum_{j=1}^{N} a_{ij}}}\right). \tag{8}$$

C. THE MODELING OF THE CYBER ATTACK-DEFENSE PROCESSES UNDER APTs

For the purpose of modeling the cyber attack-defense processes under APTs launched by strategic external attackers, the following assumptions are made.

- (A_1) Due to the prevention and the external attack, at any time the secure node i gets compromised at rate $\frac{\alpha x_i}{\delta y_i}$. The rationality of this assumption lies in that the rate is proportional to the attack strength and is inversely proportional to the prevention strength.
- (A_2) Due to the prevention and the internal infection, at time t the secure node i gets compromised at the rate $\frac{f\left(\beta \sum_{j=1}^{N} a_{ji} C_j(t)\right)}{\delta y_i}$. The rationality of this assumption lies in that the rate is proportional to the expected combined infection strength and is inversely proportional to the prevention strength.
- (A_3) Due to the recovery, at any time the compromised node i becomes secure at rate γz_i. The rationality of this assumption lies in that the rate is proportional to the recovery strength.

We are ready to model the APT-based cyber attack-defense processes. Let $\Delta t > 0$ be a very small time interval. Following the above assumptions, we have that, for $t \geq 0$ and $i = 1, \cdots, N$,

$$\begin{aligned} &\Pr\{X_i(t + \Delta t) = 1 \mid X_i(t) = 0\} \\ &\quad = \frac{\Delta t}{\delta y_i}\left[\alpha x_i + f\left(\beta \sum_{j=1}^{N} a_{ji} C_j(t)\right)\right] + o(\Delta t) \end{aligned} \tag{9}$$

and

$$\Pr\{X_i(t + \Delta t) = 0 \mid X_i(t) = 1\} = \gamma z_i \Delta t + o(\Delta t), \tag{10}$$

where the $o(\Delta t)$ terms stand for infinitesimals in Δt, i.e, $\lim_{\Delta t \to 0} \frac{o(\Delta t)}{\Delta t} = 0$. Invoking the total probability formula, rearranging the terms, dividing both sides by Δt, and letting $\Delta t \to 0$, we get a dynamic model as follows.

$$\begin{aligned} \frac{dC_i(t)}{dt} &= \frac{\alpha x_i}{\delta y_i} - \left(\frac{\alpha x_i}{\delta y_i} + \gamma z_i\right) C_i(t) \\ &\quad + \frac{1}{\delta y_i}[1 - C_i(t)] f\left(\beta \sum_{j=1}^{N} a_{ji} C_j(t)\right), \\ &\quad t \geq 0, \quad i = 1, \cdots, N. \end{aligned} \tag{11}$$

We refer to the model as the *generic secure-compromised-secure* (GSCS) model, because the function f is a generic function. The diagram of transitions of the expected state of the node i under this model is shown in Fig. 1. The GSCS model accurately captures the expected attack-defense processes under APTs, provided the generic function f is available.

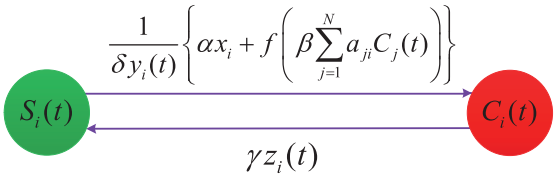

FIGURE 1. Diagram of transitions of the expected state of the node i under the GSCS model.

Let

$$\Omega = \left\{(c_1, c_2, \cdots, c_N)^T \in \mathbb{R}_+^N \mid c_i \le 1, i = 1, \cdots, N\right\}. \tag{12}$$

It is trivial to show that $\mathbf{C}(t) \in \Omega$ for $t \ge 0$.

III. A THEORETICAL ANALYSIS OF THE GSCS MODEL

It will soon be seen that the security of a cyber network under APT attacks is closely related to the dynamics of the relevant GSCS model. This section is dedicated to studying the dynamical properties of the GSCS model.

A. PRELIMINARIES

For our purposes, some preliminaries are needed. For fundamental knowledge on differential dynamical systems, see [38].

Lemma 1 (Chaplygin Lemma, See Theorem 31.4 in [39]): Consider a smooth n-dimensional system of differential equations

$$\frac{d\mathbf{x}(t)}{dt} = \mathbf{f}((\mathbf{x}(t)), \quad t \ge 0 \tag{13}$$

and the corresponding system of differential inequalities

$$\frac{d\mathbf{y}(t)}{dt} \ge \mathbf{f}((\mathbf{y}(t)), \quad t \ge 0 \tag{14}$$

with $\mathbf{x}(0) = \mathbf{y}(0)$. *Suppose that for any* $a_1, \cdots, a_n \ge 0$, *there hold*

$$f_i(x_1 + a_1, \cdots, x_{i-1} + a_{i-1}, x_i, x_{i+1} + a_{i+1}, \cdots, x_n + a_n) \ge f_i(x_1, \cdots, x_n), \quad i = 1, \cdots, n. \tag{15}$$

Then $\mathbf{y}(t) \ge \mathbf{x}(t)$ *for all* $t \ge 0$.

For fundamental knowledge on fixed point theory, see [40].

Lemma 2 (Brouwer Fixed Point Theorem, See Theorem 4.10 in [40]): Let D be a nonempty, bounded, closed and convex subset of $\mathbb{R}^n$, *and let* $f : D \to D$ *be a continuous function. Then f has a fixed point.*

For fundamental knowledge on matrix theory, see [41]. Let $diag(a_i)$ denote the diagonal matrix with diagonal entries $a_1, a_2, \cdots, a_N$, and let $col(a_i)$ denote the column vector of components $a_1, a_2, \cdots, a_N$. This work involves real square matrices only. For a matrix $\mathbf{A}$, let $s(\mathbf{A})$ denote the maximum real part of an eigenvalue of $\mathbf{A}$. $\mathbf{A}$ is *Metzler* if its off-diagonal entries are all nonnegative.

Lemma 3 (Section 2.1 in [42]): Let $\mathbf{A}$ *be an irreducible Metzler matrix. Then the following claims hold.*

(a) *If there is a positive vector* $\mathbf{x}$ *such that* $\mathbf{Ax} < \lambda\mathbf{x}$, *then* $s(\mathbf{A}) < \lambda$.
(b) *If there is a positive vector* $\mathbf{x}$ *such that* $\mathbf{Ax} = \lambda\mathbf{x}$, *then* $s(\mathbf{A}) = \lambda$.
(c) *If there is a positive vector* $\mathbf{x}$ *such that* $\mathbf{Ax} > \lambda\mathbf{x}$, *then* $s(\mathbf{A}) > \lambda$.

B. TWO PRELIMINARY LEMMAS

For the GSCS model (11) and $1 \le i \le N$, let

$$\underline{C_i} = \frac{\alpha x_i}{\alpha x_i + \gamma\delta y_i z_i} \tag{16}$$

and

$$\overline{C_i} = \frac{\alpha x_i + f(\beta\sum_{j=1}^{N} a_{ji})}{\alpha x_i + \gamma\delta y_i z_i + f(\beta\sum_{j=1}^{N} a_{ji})}. \tag{17}$$

The following two lemmas will be useful.

Lemma 4: Suppose the GSCS model (11) admits an equilibrium $\mathbf{C} = (C_1, C_2, \cdots, C_N)^T$. *Then,*

$$\underline{C_i} \le C_i \le \overline{C_i}, \quad 1 \le i \le N. \tag{18}$$

Proof: Straightforward calculations give

$$C_i = \frac{\alpha x_i + f(\beta\sum_{j=1}^{N} a_{ji}C_j)}{\alpha x_i + \gamma\delta y_i z_i + f(\beta\sum_{j=1}^{N} a_{ji}C_j)}. \tag{19}$$

The two claimed inequalities follow directly. □

Lemma 5: Let $\mathbf{C}(t) = (C_1(t), C_2(t), \cdots, C_N(t))^T$ *be a solution to the GSCS model (11). Then there are* $t_0 > 0$ *and* $c > 0$ *such that*

$$\min_{1\le i\le N} C_i(t) \ge c, \quad t \ge t_0. \tag{20}$$

Proof: Without loss of generality, assume $x_{i_0} > 0$. It follows from the GSCS model that

$$\frac{dC_{i_0}(t)}{dt} \ge \frac{\alpha x_{i_0}}{\delta y_{i_0}} - \left(\frac{\alpha x_{i_0}}{\delta y_{i_0}} + \gamma z_{i_0}\right) C_{i_0}(t), \quad t \ge 0. \tag{21}$$

Obviously, the comparison system

$$\frac{du_{i_0}(t)}{dt} = \frac{\alpha x_{i_0}}{\delta y_{i_0}} - \left(\frac{\alpha x_{i_0}}{\delta y_{i_0}} + \gamma z_{i_0}\right) u_{i_0}(t), \quad t \ge 0, \tag{22}$$

with $u_{i_0}(0) = C_{i_0}(0)$ admits $\underline{C_{i_0}} > 0$ as the globally stable equilibrium. By Lemma 1, we have

$$C_{i_0}(t) \ge u_{i_0}(t), \quad t \ge 0. \tag{23}$$

So,

$$\liminf_{t\to\infty} C_{i_0}(t) \ge \lim_{t\to\infty} u_{i_0}(t) = \underline{C_{i_0}}. \tag{24}$$

Thus, for any $0 < \varepsilon < \underline{C_{i_0}}$, there is $t_1 > 0$ such that

$$C_{i_0}(t) \geq \underline{C_{i_0}} - \varepsilon, \quad t \geq t_1. \tag{25}$$

As G is strongly connected, there is $a_{i_0 j_0} = 1$. Hence,

$$\frac{dC_{j_0}(t)}{dt} \geq \frac{1}{\delta y_{j_0}} f\left(\beta\left(\underline{C_{i_0}} - \varepsilon\right)\right) - \left[\frac{1}{\delta y_{j_0}} f\left(\beta\left(\underline{C_{i_0}} - \varepsilon\right)\right) + \gamma z_{j_0}\right] C_{j_0}(t), \quad t \geq t_1. \tag{26}$$

Obviously, the comparison system

$$\frac{dv_{j_0}(t)}{dt} = \frac{1}{\delta y_{j_0}} f\left(\beta\left(\underline{C_{i_0}} - \varepsilon\right)\right) - \left[\frac{1}{\delta y_{j_0}} f\left(\beta\left(\underline{C_{i_0}} - \varepsilon\right)\right) + \gamma z_{j_0}\right] v_{j_0}(t), \quad t \geq t_1 \tag{27}$$

with $v_{j_0}(t_1) = C_{j_0}(t_1)$ admits $\frac{f\left(\beta\left(\underline{C_{i_0}} - \varepsilon\right)\right)}{f\left(\beta\left(\underline{C_{i_0}} - \varepsilon\right)\right) + \gamma \delta y_{j_0} z_{j_0}}$ as the globally stable equilibrium. By Lemma 1, we have

$$C_{j_0}(t) \geq v_{j_0}(t), \quad t \geq t_1. \tag{28}$$

So,

$$\liminf_{t\to\infty} C_{j_0}(t) \geq \lim_{t\to\infty} v_{j_0}(t) = \frac{f\left(\beta\left(\underline{C_{i_0}} - \varepsilon\right)\right)}{f\left(\beta\left(\underline{C_{i_0}} - \varepsilon\right)\right) + \gamma \delta y_{j_0} z_{j_0}}. \tag{29}$$

In view of the arbitrariness of ε, we get that

$$\liminf_{t\to\infty} C_{j_0}(t) \geq \frac{f\left(\beta \underline{C_{i_0}}\right)}{f\left(\beta \underline{C_{i_0}}\right) + \gamma \delta y_{j_0} z_{j_0}} > 0. \tag{30}$$

The lemma follows by repeating the argument. □

C. THE EQUILIBRIUM

An *equilibrium* of a dynamical system is a state of the system such that, when starting from the state, the system will always stay in the state. Clearly, the equilibria of a dynamical system are the most easily understood states of the system. The first step toward the understanding of a dynamical system is to determine all the equilibria of the system. The following theorem determines the number of the equilibria of the GSCS model (11).

Theorem 1: The GSCS model (11) admits a unique equilibrium. Denote this equilibrium by $\mathbf{C}^* = (C_1^*, \cdots, C_N^*)^T$. *Then* $C_i^* > 0$, $\underline{C_i} \leq C_i^* \leq \overline{C_i}$, $1 \leq i \leq N$.

Proof: Let

$$K = \prod_{i=1}^{N} \left[\underline{C_i}, \overline{C_i}\right]. \tag{31}$$

Define a continuous mapping $\mathbf{H} = (H_1, \cdots, H_N)^T : K \to [0, 1]^N$ as follows.

$$H_i(\mathbf{w}) = \frac{\alpha x_i + f(\beta \sum_{j=1}^{N} a_{ji} w_j)}{\alpha x_i + \gamma \delta y_i z_i + f(\beta \sum_{j=1}^{N} a_{ji} w_j)}, \quad \mathbf{w} = (w_1, \cdots, w_N)^T \in K. \tag{32}$$

It is trivial to show that $\mathbf{C}$ is an equilibrium of the GSCS model if and only if $\mathbf{C}$ is a fixed point of the mapping $\mathbf{H}$. Furthermore, it is easy to show that $\mathbf{H}$ maps K into itself. It follows from Lemma 2 that $\mathbf{H}$ has a fixed point, denoted $\mathbf{C}^* = (C_1^*, \cdots, C_N^*)^T$. This implies that $\mathbf{C}^*$ is an equilibrium of the GSCS model. By Lemma 4, $\underline{C_i} \leq C_i^* \leq \overline{C_i}$, $1 \leq i \leq N$. By Lemma 5, $C_i^* > 0$, $1 \leq i \leq N$.

The remaining thing to do is to show that $\mathbf{C}^*$ is the unique fixed point of $\mathbf{H}$. On the contrary, suppose $\mathbf{H}$ has a fixed point other than $\mathbf{C}^*$. Denote this equilibrium by $\mathbf{C}^{**} = (C_1^{**}, \cdots, C_N^{**})^T$. Let

$$\rho = \max_{1\leq i\leq N} \frac{C_i^*}{C_i^{**}}, \tag{33}$$

$$i_0 = \arg \max_{1\leq i\leq N} \frac{C_i^*}{C_i^{**}}. \tag{34}$$

Without loss of generality, assume $\rho > 1$. Then

$$\begin{aligned} C_{i_0}^* &= H_{i_0}(\mathbf{C}^*) \leq H_{i_0}(\rho \mathbf{C}^{**}) \\ &= \frac{\alpha x_{i_0} + f(\rho\beta \sum_{j=1}^{N} a_{ji_0} C_j^{**})}{\alpha x_{i_0} + \gamma \delta y_{i_0} z_{i_0} + f(\rho\beta \sum_{j=1}^{N} a_{ji_0} C_j^{**})} \\ &< \frac{\alpha x_{i_0} + f(\rho\beta \sum_{j=1}^{N} a_{ji_0} C_j^{**})}{\alpha x_{i_0} + \gamma \delta y_{i_0} z_{i_0} + f(\beta \sum_{j=1}^{N} a_{ji_0} C_j^{**})} \\ &\leq \frac{\alpha x_{i_0} + \rho f(\beta \sum_{j=1}^{N} a_{ji_0} C_j^{**})}{\alpha x_{i_0} + \gamma \delta y_{i_0} z_{i_0} + f(\beta \sum_{j=1}^{N} a_{ji_0} C_j^{**})} \\ &< \rho H_{i_0}(\mathbf{C}^{**}) = \rho C_{i_0}^{**}, \end{aligned} \tag{35}$$

where the first inequality follows from the strict monotonicity of f, and the second inequality follows from the concavity of f. This contradicts the assumption that $C_{i_0}^* = \rho C_{i_0}^{**}$. Hence, $\mathbf{C}^*$ is the unique fixed point of $\mathbf{H}$. The proof is complete. □

This theorem manifests that, when starting from the state $\mathbf{C}^*$, the GSCS model will always stay in the state. Due to the complexity of the model, the location of $\mathbf{C}^*$ is beyond the reach.

D. THE GLOBAL STABILITY OF THE EQUILIBRIUM

In reality, the probability of a dynamical system being initially in one of its equilibria is often negligible. Therefore, the second step toward the understanding of a dynamical system is to examine the evolutionary trend of the system when starting from any state other than the equilibria. An equilibrium of a dynamical system is *globally stable* if (a) when starting from any state, the system will always approach the equilibrium, and (b) when starting from a state near the equilibrium, the system will always stay close to the equilibrium.

From the qualitative perspective, the dynamics of a dynamical system with a globally stable equilibrium is well understood. The following theorem shows the qualitative dynamics of the GSCS model.

Theorem 2: The equilibrium $\mathbf{C}^*$ *of the GSCS model (11) is globally stable.*

Proof: Let $\mathbf{C}(t) = (C_1(t), C_2(t), \cdots, C_N(t))^T$ be a solution to the GSCS model. By Lemma 5, there are $t_0 > 0$ and $c > 0$ such that

$$\min_{1\le i\le N} C_i(t) \ge c, \quad t \ge t_0. \tag{36}$$

Let

$$Z(\mathbf{C}(t)) = \max_{1\le i\le N} \frac{C_i(t)}{C_i^*}, \quad t \ge t_0, \tag{37}$$

$$z(\mathbf{C}(t)) = \min_{1\le i\le N} \frac{C_i(t)}{C_i^*} \quad t \ge t_0. \tag{38}$$

Define a function V as

$$V(\mathbf{C}(t)) = \max\{Z(\mathbf{C}(t)) - 1, 0\} + \max\{1 - z(\mathbf{C}(t)), 0\}. \tag{39}$$

It is easily verified that V is positive definite with respect to $\mathbf{C}^*$, i.e., (a) $V(\mathbf{C}(t)) \ge 0$, and (b) $V(\mathbf{C}(t)) = 0$ if and only if $\mathbf{C}(t) = \mathbf{C}^*$. Next , let us show that $D^+V(\mathbf{C}(t)) \le 0$, $t \ge t_0$, where D^+ stands for the upper-right Dini derivative of V along $\mathbf{C}(t)$. To this end, we need to show the following two claims.

Claim 1: $D^+Z(\mathbf{C}(t)) \le 0$ if $Z(\mathbf{C}(t)) \ge 1$. Moreover, $D^+Z(\mathbf{C}(t)) < 0$ if $Z(\mathbf{C}(t)) > 1$.

Claim 2: $D_+z(\mathbf{C}(t)) \ge 0$ if $z(\mathbf{C}(t)) \le 1$. Moreover, $D_+z(\mathbf{C}(t)) > 0$ if $z(\mathbf{C}(t)) < 1$. Here D_+ stands for the lower-right Dini derivative.

Proof of Claim 1: Choose k_0 such that

$$Z(\mathbf{C}(t)) = \frac{C_{k_0}(t)}{C_{k_0}^*} \tag{40}$$

and

$$D^+Z(\mathbf{C}(t)) = \frac{C_{k_0}^{'}(t)}{C_{k_0}^*}. \tag{41}$$

Then,

$$\begin{aligned}
&\frac{C_{k_0}^*}{C_{k_0}(t)} C_{k_0}^{'}(t) \\
&= \frac{\alpha x_{k_0}}{\delta y_{k_0}} \left(1 - C_{k_0}(t)\right) \frac{C_{k_0}^*}{C_{k_0}(t)} - \gamma z_{k_0} C_{k_0}^* \\
&\quad + \frac{1}{\delta y_{k_0}} \left(1 - C_{k_0}(t)\right) \frac{C_{k_0}^*}{C_{k_0}(t)} f\left(\beta \sum_{j=1}^{N} a_{jk_0} C_j(t)\right) \\
&\le \frac{\alpha x_{k_0}}{\delta y_{k_0}} \left(1 - C_{k_0}^*\right) - \gamma z_{k_0} C_{k_0}^* \\
&\quad + \frac{1}{\delta y_{k_0}} \left(1 - C_{k_0}^*\right) \frac{C_{k_0}^*}{C_{k_0}(t)} f\left(\beta \sum_{j=1}^{N} a_{jk_0} C_j(t)\right) \\
&\le \frac{\alpha x_{k_0}}{\delta y_{k_0}} \left(1 - C_{k_0}^*\right) - \gamma z_{k_0} C_{k_0}^* \\
&\quad + \frac{1}{\delta y_{k_0}} \left(1 - C_{k_0}^*\right) f\left(\beta \frac{C_{k_0}^*}{C_{k_0}(t)} \sum_{j=1}^{N} a_{jk_0} C_j(t)\right) \\
&\le \frac{\alpha x_{k_0}}{\delta y_{k_0}} \left(1 - C_{k_0}^*\right) - \gamma z_{k_0} C_{k_0}^* \\
&\quad + \frac{1}{\delta y_{k_0}} \left(1 - C_{k_0}^*\right) f\left(\beta \sum_{j=1}^{N} a_{jk_0} C_j^*\right) = 0,
\end{aligned} \tag{42}$$

where the second inequality follows from the concavity of f, and the third inequality follows from the monotonicity of f. This implies $D^+Z(\mathbf{C}(t)) \le 0$. As the first inequality is strict if $Z(\mathbf{C}(t)) > 1$, we get that $D^+Z(\mathbf{C}(t)) < 0$ if $Z(\mathbf{C}(t)) > 1$. Claim 1 is proven.

The argument for Claim 2 is analogous to that for Claim 1 and hence is omitted. Next, consider three possibilities.

Case 1: $Z(\mathbf{C}(t)) < 1$. Then $z(\mathbf{C}(t)) < 1$ and

$$V(\mathbf{C}(t)) = 1 - z(\mathbf{C}(t)). \tag{43}$$

Hence,

$$D^+V(\mathbf{C}(t)) = -D_+z(\mathbf{C}(t)) < 0. \tag{44}$$

Case 2: $z(\mathbf{C}(t)) > 1$. Then $Z(\mathbf{C}(t)) > 1$ and

$$V(\mathbf{C}(t)) = Z(\mathbf{C}(t)) - 1. \tag{45}$$

Hence,

$$D^+V(\mathbf{C}(t)) = D^+Z(\mathbf{C}(t)) < 0. \tag{46}$$

Case 3: $Z(\mathbf{C}(t)) \ge 1$, $z(\mathbf{C}(t)) \le 1$. Then

$$V(\mathbf{C}(t)) = Z(\mathbf{C}(t)) - z(\mathbf{C}(t)). \tag{47}$$

Hence,

$$D^+V(\mathbf{C}(t)) = D^+Z(\mathbf{C}(t)) - D_+z(\mathbf{C}(t)) \le 0. \tag{48}$$

Moreover, the equality holds if and only if $\mathbf{C}(t) = \mathbf{C}^*$.

The theorem follows from the LaSalle Invariance Principle. □

This theorem indicates that, regardless of the initial state, the GSCS model will always approach the equilibrium $\mathbf{C}^*$. Therefore, the dynamics of the model is well understood from the qualitative perspective. The following experiment illustrates the time plot of the GSCS model.

Experiment 1: Consider the six instances of the GSCS model, where G assumes one of the six trees shown in Fig. 2, $\alpha = 0.05$, $\beta = 0.01$, $\delta = 1$, $\gamma = 1$, $f(x) = \frac{x}{1+x}$, $||\mathbf{x}||_1 = 1$, $||\mathbf{y}||_1 = ||\mathbf{z}||_1 = \frac{1}{2}$, $\mathbf{x}$, $\mathbf{y}$ *and* $\mathbf{z}$ *are all uniform. Fig. 3 shows the time plot of the network state for each of these instances. It can be seen that, for each of the instances, the expected state of the network approaches the corresponding equilibrium.*

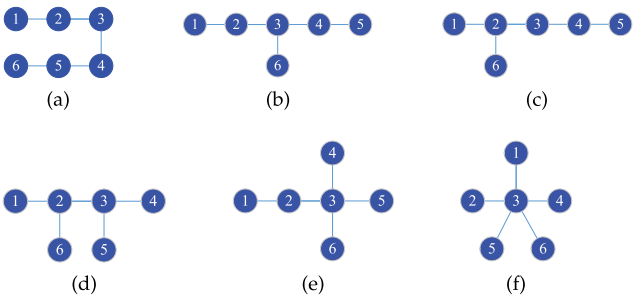

FIGURE 2. Six trees with six nodes and five edges. (a) G_1. (b) G_2. (c) G_3. (d) G_4. (e) G_5. (f) G_6.

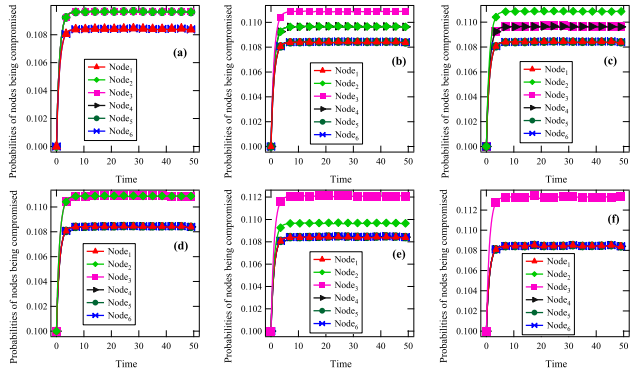

FIGURE 3. The time plot of the expected state of the network for each of the six instances of the GSCS model, where G assumes one of the six trees shown in Fig. 2, $\alpha = 0.05$, $\beta = 0.01$, $\delta = 1$, $\gamma = 1$, $f(x) = \frac{x}{1+x}$, $||\mathbf{x}||_1 = 1$, $||\mathbf{y}||_1 = ||\mathbf{z}||_1 = \frac{1}{2}$, $\mathbf{x}$, $\mathbf{y}$ and $\mathbf{z}$ are all uniform. It can be seen that, for each of the instances, the expected state of the network approaches the corresponding equilibrium.

IV. THE EQUILIBRIUM SECURITY OF CYBER NETWORKS

The goal of this section is to suggest a security metric of cyber networks under APTs. Given a cyber network $G = (V, E)$ and all the relevant factors, α, β, δ, γ, $\mathbf{x}$, $\mathbf{y}$ and $\mathbf{z}$. Consider the corresponding GSCS model (11).

Let $C_G(t)$ denote the expected fraction of the compromised nodes of the network G at time t.

$$C_G(t) = \frac{1}{N}\sum_{i=1}^{N} C_i(t), \quad t \geq 0. \tag{49}$$

Further, define the *point security* of the network G at time t, denoted $S_G(t)$, as follows.

$$S_G(t) = 1 - C_G(t), \quad t \geq 0. \tag{50}$$

Clearly, we have $0 \leq S_G(t) \leq 1$.

Clearly, the higher the point security of a cyber network at time t, the lower the expected fraction of the compromised nodes of the network at time t will be, and hence the securer the network will be at time t. So, the point security of a cyber network at time t is an indicator of the security of the network at time t. However, the availability of a point security as the security metric of real-world cyber networks is very limited, because it cannot characterize the network security from a holistic perspective. Nevertheless, the notion of point security provides an idea of measuring the security of cyber networks.

Let $\overline{C}_T(G)$ denote the average of $C_G(t)$ over the time horizon $[0, T]$.

$$\overline{C}_T(G) = \frac{1}{T}\int_0^T C_G(t)dt, \quad T \geq 0. \tag{51}$$

Further, define the *interval security* of the network in the time horizon $[0, T]$, denoted $\overline{S}_T(G)$, as follows.

$$\overline{S}_T(G) = 1 - \overline{C}_T(G), \quad T \geq 0. \tag{52}$$

Clearly, we have $0 \leq \overline{S}_T(G) \leq 1$.

The interval security of a cyber network in the time horizon $[0, T]$ is a measure of the security of the network in that time horizon, which applies to the situation where the APT attack terminates at time T. To accurately estimate an interval security, numerous data related to the network state must be sampled densely, sent remotely and processed quickly, which would be very expensive in terms of the computing and network resources. Hence, the interval securities are not good metrics of the security of cyber networks.

Let $\overline{C}(G)$ denote the limit of $\overline{C}_T(G)$ when $T \to \infty$.

$$\overline{C}(G) = \lim_{T\to\infty} \overline{C}_T(t) = \lim_{T\to\infty} \frac{1}{T}\int_0^T C_G(t)dt. \tag{53}$$

The existence of this limit follows from Theorem 2. Further, define the *infinite security* of the network, denoted $\overline{S}(G)$, as follows.

$$\overline{S}(G) = 1 - \overline{C}(G). \tag{54}$$

Obviously, we have $0 \leq \overline{S}(G) \leq 1$.

The infinite security of a cyber network is an index of its security in the infinite time horizon $[0, \infty)$, which is applicable to the situation where the APT attack will persist forever. Still, the infinite security is not an ideal security metric of cyber networks, because (a) due to the limited attack resources, realistic APT attacks cannot persist forever, and (b) the cost needed for estimating the infinite security of a network would be prohibitive.

Let $C^*(G)$ denote the expected fraction of the compromised nodes of the network G when the model is in the equilibrium $\mathbf{C}^*$.

$$C^*(G) = \frac{1}{N}\sum_{i=1}^{N} C_i^*. \tag{55}$$

The following result is a corollary of Theorem 2.

Theorem 3: Consider the GSCS model (11). Then

$$C_G(t) \to C^*(G), \quad t \to \infty. \tag{56}$$

Now, let us define the *equilibrium security* of the network G, denoted $S_E(G)$, as follows.

$$S_E(G) = 1 - C^*(G). \tag{57}$$

Obviously, we have $0 \leq S_E(G) \leq 1$. By Theorem 3, we have the following result.

Theorem 4: Consider the GSCS model (11). Then

$$S_G(t) \to S_E(G), \quad t \to \infty. \tag{58}$$

This theorem reveals the close relationship between the equilibrium security of a network and the point securities of the network: the equilibrium security is exactly the limit of the point securities when the time approaches the infinity.

Theorem 4 suggests that the equilibrium security is a candidate for the security metric of cyber networks. Compared with the point securities, on one hand, the limit security characterizes the inherent security property of a cyber network from a holistic perspective. Compared with the interval securities and the infinite security, on the other hand, the equilibrium security can be estimated using far less sample data and hence comsuming far fewer computing and network resources. Additionally, the estimation of the equilibrium security of a cyber network needs no knowledge of the technical levels, the generic function, and the attack and defense strategies. Therefore, the equilibrium security is expected to be a qualified metric of the security of cyber networks under APTs.

V. THE IMPACT OF THE PARAMETERS ON THE EQUILIBRIUM SECURITY

Clearly, the equilibrium security of a cyber network is dependent upon the four technical levels, the attack strategy, the prevention strategy, and the recovery strategy. These factors can be regarded as the parameters having influence on the equilibrium security. So, the equilibrium security can be written as

$$S_E(G) = S_E(G; \alpha, \beta, \delta, \gamma, \mathbf{x}, \mathbf{y}, \mathbf{z}). \tag{59}$$

This section is committed to examining the impact of all the parameters on the equilibrium security of a cyber network.

A. A preliminary result

For a GSCS model, define an irreducible Metzler matrix, $\mathbf{M}$, as follows.

$$\mathbf{M} = diag\left(\beta\left(1-C_i^*\right)f'\left(\beta\sum_{j=1}^{N}a_{ji}C_j^*\right)\right)\mathbf{A}(G)^T - diag\left(\alpha x_i + \gamma\delta y_i z_i + f\left(\beta\sum_{j=1}^{N}a_{ji}C_j^*\right)\right). \tag{60}$$

To achieve our goal, the following lemma is necessary.

Lemma 6: The matrix $\mathbf{M}$ is invertible. Moreover, $\mathbf{M}^{-1}$ is negative.

Proof: As the generic function f is concave, we have

$$f'\left(\beta\sum_{j=1}^{N}a_{ji}C_j^*\right) \le \frac{f\left(\beta\sum_{j=1}^{N}a_{ji}C_j^*\right)}{\beta\sum_{j=1}^{N}a_{ji}C_j^*}. \tag{61}$$

So,

$$\begin{aligned}\mathbf{M}\mathbf{C}^* &= diag\left(\beta\left(1-C_i^*\right)f'\left(\beta\sum_{j=1}^{N}a_{ji}C_j^*\right)\right)\mathbf{A}(G)^T\mathbf{C}^* \\ &\quad - diag\left(\alpha x_i + \gamma\delta y_i z_i + f\left(\beta\sum_{j=1}^{N}a_{ji}C_j^*\right)\right)\mathbf{C}^* \\ &\le diag\left(\beta\left(1-C_i^*\right)\frac{f\left(\beta\sum_{j=1}^{N}a_{ji}C_j^*\right)}{\beta\sum_{j=1}^{N}a_{ji}C_j^*}\right)\mathbf{A}(G)^T\mathbf{C}^* \\ &\quad - diag\left(\alpha x_i + \gamma\delta y_i z_i + f\left(\beta\sum_{j=1}^{N}a_{ji}C_j^*\right)\right)\mathbf{C}^* \\ &= -col\left(\alpha x_i + f\left(\beta\sum_{j=1}^{N}a_{ji}C_j^*\right)C_i^*\right) < \mathbf{0}.\end{aligned} \tag{62}$$

It follows from Lemma 3(a) that $s(\mathbf{M}) < 0$. This implies that $\mathbf{M}$ is invertible. As $\mathbf{M}$ is Metzler, irreducible and Hurwitz, $\mathbf{M}^{-1}$ is negative [43]. □

B. THE IMPACT OF THE FOUR TECHNICAL LEVELS

Let us first examine the impact of the four technical levels on the equilibrium security of a cyber network. Fot this purpose, we need to understand the way that these factors affect the equilibrium $\mathbf{C}^*$ of the GSCS model. The following result illuminates the impact.

Theorem 5: For the GSCS model (11), there hold

$$\frac{\partial\mathbf{C}^*}{\partial\alpha} > \mathbf{0}, \tag{63}$$

$$\frac{\partial\mathbf{C}^*}{\partial\beta} > \mathbf{0}, \tag{64}$$

$$\frac{\partial\mathbf{C}^*}{\partial\delta} < \mathbf{0}, \tag{65}$$

and

$$\frac{\partial\mathbf{C}^*}{\partial\gamma} < \mathbf{0}. \tag{66}$$

Proof: We prove the second inequality only, because the remaining three inequalities can be shown analogously. As $\mathbf{C}^*$ is an equilibrium of the GSCS model, we have

$$F_i := \alpha x_i - (\alpha x_i + \gamma\delta y_i z_i)C_i^* + \left(1-C_i^*\right)f\left(\beta\sum_{j=1}^{N}a_{ji}C_j^*\right) = 0, \quad 1 \le i \le N. \tag{67}$$

Differentiating with respect to β on both sides of each of these equations, we get

$$\frac{\partial F_i}{\partial\beta} + \sum_{j=1}^{N}\frac{\partial F_i}{\partial C_j^*}\cdot\frac{\partial C_j^*}{\partial\beta} = 0, \quad 1 \le i \le N. \tag{68}$$

Direct calculations give

$$\mathbf{M}\frac{\partial \mathbf{C}^*}{\partial \beta} = -diag\left(\left(1-C_i^*\right)f^{'}(\beta\sum_{j=1}^{N}a_{ji}C_j^*)\right)\mathbf{A}(G)^T\mathbf{C}^*. \tag{69}$$

By Lemma 6, we have

$$\frac{\partial \mathbf{C}^*}{\partial \beta} = -\mathbf{M}^{-1}\cdot diag\left((1-C_i^*)f^{'}(\beta\sum_{j=1}^{N}a_{ji}C_j^*)\right)\mathbf{A}(G)^T\mathbf{C}^*. \tag{70}$$

where $\mathbf{M}^{-1}$ is negative. As the network G is strongly connected, $\mathbf{A}(G)^T\mathbf{C}^*$ is positive. Hence, $\frac{\partial \mathbf{C}^*}{\partial \beta} > \mathbf{0}$. □

This theorem demonstrates that (a) with the rise of the attack or infection level, all components of the equilibrium move up, and (b) with the rise of the prevention or recovery level, all components of the equilibrium move down. As a corollary of this theorem, the following result shows the impact of the four technical levels on the equilibrium security of a cyber network.

Theorem 6: For the GSCS model (11), there hold

$$\frac{\partial S_E(G)}{\partial \alpha} < 0, \tag{71}$$

$$\frac{\partial S_E(G)}{\partial \beta} < 0, \tag{72}$$

$$\frac{\partial S_E(G)}{\partial \delta} > 0, \tag{73}$$

and

$$\frac{\partial S_E(G)}{\partial \gamma} > 0. \tag{74}$$

This theorem declares that (a) the equilibrium security of a cyber network descends with the rise of the attack or infection level, and (b) the equilibrium security of a cyber network ascends with the rise of the prevention or recovery level. These results accord with our intuitive sense of the security of cyber networks, which partly justifies the equilibrium security as a security metric of cyber networks. In practice, the defender of cyber networks should try his best to enhance the prevention and recovery levels.

C. THE IMPACT OF THE ATTACK AND DEFENSE STRATEGIES

We now examine the impact of the attack and defense strategies on the equilibrium security of a cyber network. To this end, we need to understand how these factors affect the equilibrium $\mathbf{C}^*$ of the GSCS model. The following result expounds the impact.

Theorem 7: For the GSCS model (11), there hold

$$\frac{\partial \mathbf{C}^*}{\partial x_i} > \mathbf{0}, \quad 1 \le i \le N, \tag{75}$$

$$\frac{\partial \mathbf{C}^*}{\partial y_i} < \mathbf{0}, \quad 1 \le i \le N, \tag{76}$$

and

$$\frac{\partial \mathbf{C}^*}{\partial z_i} < \mathbf{0}, \quad 1 \le i \le N. \tag{77}$$

The proof of the theorem is analogous to that of the previous theorem and hence is omitted. This theorem tells us that (a) with the increase of the resources per unit time used for attacking a node, all components of the equilibrium move up, and (b) with the increase of the resources per unit time used for preventing or recovering a node, all components of the equilibrium move down. As a corollary of this theorem, the following result exhibits the impact of the attack and defense strategies on the equilibrium security of a cyber network.

Theorem 8: For the GSCS model (11), there hold

$$\frac{\partial S_E(G)}{\partial x_i} < 0, \quad 1 \le i \le N \tag{78}$$

$$\frac{\partial S_E(G)}{\partial y_i} > 0, \quad 1 \le i \le N \tag{79}$$

and

$$\frac{\partial S_E(G)}{\partial z_i} > 0, \quad 1 \le i \le N. \tag{80}$$

This theorem confirms that (a) the equilibrium security of a cyber network descends with the increase of the resources per unit time used for attacking a node, and (b) the equilibrium security of a cyber network ascends with the increase of the resources per unit time used for preventing or recovering a node. These results conform to our sense of the security of cyber networks, which again justifies the equilibrium security as a measure of the security of cyber networks. In practice, the defenders are suggested to configure more defense resources for their cyber networks, so as to enhance the security.

VI. FURTHER DISCUSSIONS

The previous section has ascertained the impact of all the basic parameters of the GSCS model on the equilibrium security of a cyber network. Additionally, the equilibrium security of a cyber network is also affected by three factors: the network topology, the ratio of the amount of the prevention resources to that of the recovery resources, and the amount of the defense resources per unit time given the ratio of the amount of the attack resources to that of the defense resources. This section is dedicated to inspecting the impact of these factors on the equilibrium security of a cyber network.

A. THE IMPACT OF THE NETWORK TOPOLOGY

We first examine the impact of the network topology on the equilibrium security of a cyber network. To achieve the goal, we need to understand the way that the network topology affects the equilibrium $\mathbf{C}^*$ of the GSCS model. The following result reveals the impact.

Theorem 9: For the GSCS model (11), there hold

$$\frac{\partial \mathbf{C}^*}{\partial a_{ij}} > \mathbf{0}, \quad 1 \le i,\ j \le N,\ i \ne j. \tag{81}$$

The argument for the theorem is analogous to that for Theorem 5 and hence is omitted. This theorem implies that, with the addition of new edges to the network, all components of the equilibrium move up. As a corollary of this theorem, the following result discloses the impact of the topology of a cyber network on its equilibrium security.

Theorem 10: For the GSCS model (11), there hold

$$\frac{\partial S_E(G)}{\partial a_{ij}} < 0, \quad 1 \le i,\ j \le N,\ i \ne j. \tag{82}$$

This theorem states that, with the addition of new edges to the network, the equilibrium security of a cyber network declines. So, cyber networks with dense connections are more vulnerable to APT attacks than those with sparse connections. In practice, the defenders of cyber networks are suggested to properly limit the traffic over the networks, so as to enhance the security.

B. THE IMPACT OF THE PREVENTION-RECOVERY RATIO

For a GSCS model, define the *prevention-recovery ratio*, denoted r_{PR}, as the radio of the amount of the prevention resources to that of the recovery resources.

$$r_{PR} = \frac{||\mathbf{y}||_1}{||\mathbf{z}||_1}. \tag{83}$$

Given the amount of the defense resources per unit time, how the prevention-recovery ratio affects the equilibrium security of a cyber network is still unclear. Now, let us check the impact through computer simulations.

Experiment 2: Consider 504 instances of the GSCS model, where G assumes one of the six trees shown in Fig. 2, $\alpha = 0.05$, $\beta = 0.01$, $\delta = 1$, $\gamma = 1$, $f(x) = \frac{x}{1+x}$, $||\mathbf{x}||_1 = 1$, $||\mathbf{y}||_1 = \frac{r}{1+r}$, $||\mathbf{z}||_1 = \frac{1}{1+r}$, $r \in \{\frac{1}{4}, \frac{1}{3}, \frac{1}{2}, 1, 2, 3, 4\}$, *with (a) uniform* $\mathbf{x}$, $\mathbf{y}$ *and* $\mathbf{z}$*; (b) uniform* $\mathbf{x}$ *and* $\mathbf{y}$*, degree-first* $\mathbf{z}$*; (c) uniform* $\mathbf{x}$ *and* $\mathbf{z}$*, degree-first* $\mathbf{y}$*; (d) uniform* $\mathbf{x}$*, degree-first* $\mathbf{y}$ *and* $\mathbf{z}$*; (e) degree-first* $\mathbf{x}$*, uniform* $\mathbf{y}$ *and* $\mathbf{z}$*; (f) degree-first* $\mathbf{x}$ *and* $\mathbf{z}$*, uniform* $\mathbf{y}$*; (g) degree-first* $\mathbf{x}$ *and* $\mathbf{y}$*, uniform* $\mathbf{z}$*; (h) degree-first* $\mathbf{x}$*,* $\mathbf{y}$ *and* $\mathbf{z}$*; (i) degree-last* $\mathbf{x}$*, uniform* $\mathbf{y}$ *and* $\mathbf{z}$*; (j) degree-last* $\mathbf{x}$*, uniform* $\mathbf{y}$*, degree-first* $\mathbf{z}$*; (k) degree-last* $\mathbf{x}$*, degree-first* $\mathbf{y}$*, uniform* $\mathbf{z}$*; (l) degree-last* $\mathbf{x}$*, degree-first* $\mathbf{y}$ *and* $\mathbf{z}$*. For each of the instances, the equilibrium security of the cyber network is shown in Fig. 4. It can be seen that, with the increase of* r_{PR}*, the equilibrium security of a cyber network goes up first but then it goes down. Moreover, the equilibrium security attains the maximum in the proximity of* $r_{PR} = 1$.

Many similar experiments exhibit qualitatively similar phenomena. It is concluded that, with the increase of the prevention-recovery ratio, the equilibrium security of a cyber network first goes up then goes down. Moreover, the equilibrium security attains the maximum when the amount of the prevention resources is close to that of the recovery resources. Based on these findings, the defenders of cyber networks are suggested to distribute the available defense resources equally to prevention and recovery, so as to maximize the security.

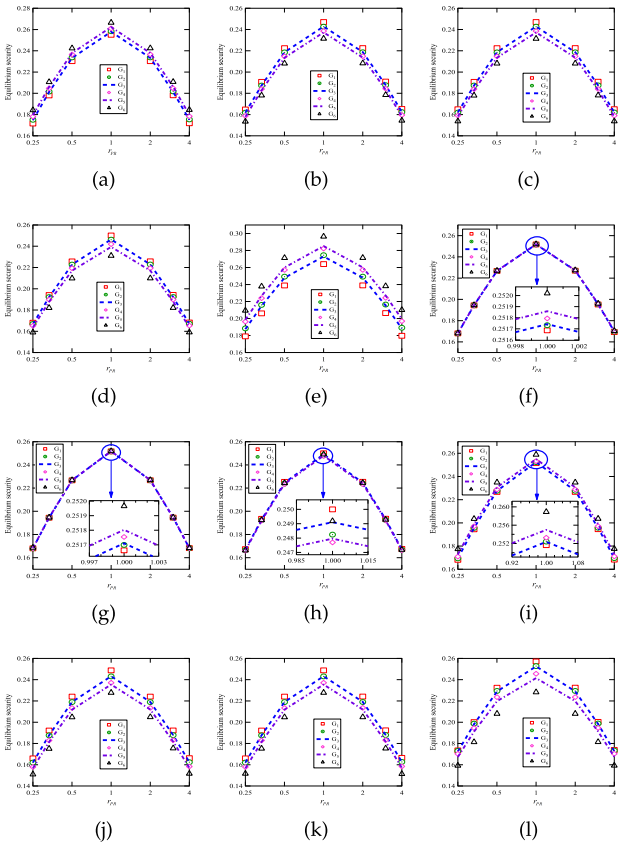

FIGURE 4. The equilibrium security of the cyber network for each of the 504 instances of the GSCS model, where $\alpha = 0.05$, $\beta = 0.01$, $\gamma = 1$, $\delta = 1$, G varies from G_1 to G_6, $||\mathbf{x}||_1 = 1$, $||\mathbf{y}||_1 = \frac{r}{1+r}$, $||\mathbf{z}||_1 = \frac{1}{r}$, $r \in \{\frac{1}{4}, \frac{1}{3}, \frac{1}{2}, 1, 2, 3, 4\}$, with (a) uniform x, y and z; (b) uniform x and y, degree-first z; (c) uniform x and z, degree-first y; (d) uniform x, degree-first y and z; (e) degree-first x, uniform y and z; (f) degree-first x and z, uniform y; (g) degree-first x and y, uniform z; (h) degree-first x, y and z; (i) degree-last x, uniform y and z; (j) degree-last x, uniform y, degree-first z; (k) degree-last x, degree-first y, uniform z; (l) degree-last x, degree-first y and z. It can be seen that, with the increase of r_{PR}, the equilibrium security of a cyber network goes up first but then it goes down. Moreover, the equilibrium security attains the maximum in the proximity of $r_{PR} = 1$.

Security managers often think that they should invest more in prevention, while recovery is just a backup plan; this is especially the case for small organizations with limited resources. However, our findings show that, in the context of APTs, recovery is as important as prevention. This may be because the huge threat and serious consequence of APTs invalidate the traditional idea of prevention first.

C. THE IMPACT OF THE AMOUNT OF DEFENSE RESOURCES PER UNIT TIME GIVEN THE ATTACK-DEFENSE RATIO

For a GSCS model, define the *attack-defense ratio*, denoted r_{AD}, as the ratio of the amount of the attack resources

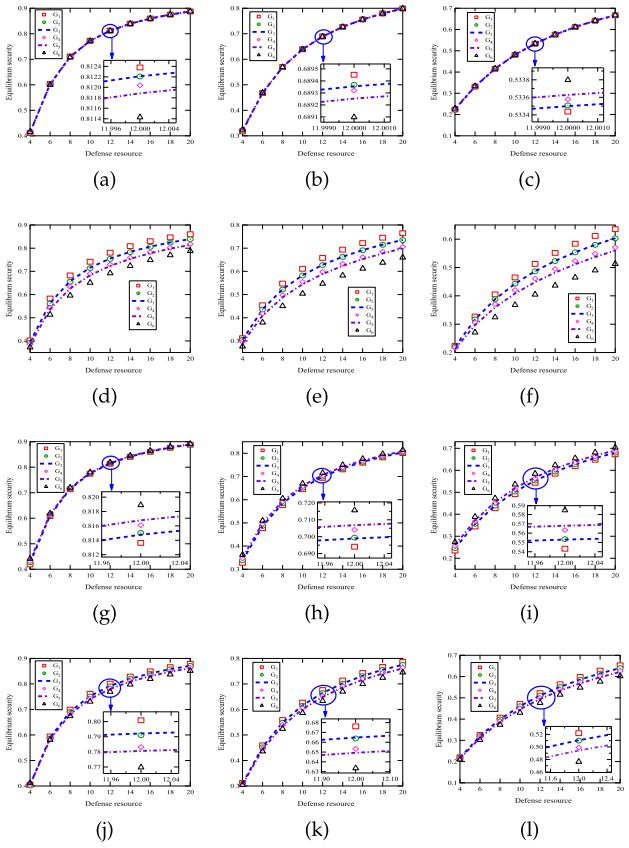

FIGURE 5. The equilibrium security of the cyber network for each of the 504 instances of the GSCS model, where $\alpha = 0.1$, $\beta = 0.05$, $\gamma = 0.5$, $\delta = 1$, G varies from G_1 to G_6, $r_{AD} = r$, $||\mathbf{y}||_1 = ||\mathbf{z}||_1 = s$, $s \in \{2, 3, \cdots, 10\}$, $||\mathbf{y}||_1 = s_1$, with (a) $r = \frac{1}{2}$, uniform x, y and z; (b) $r = 1$, uniform x, y and z; (c) $r = 2$, uniform x, y and z; (d) $r = \frac{1}{2}$, uniform x, degree-first y and z; (e) $r = 1$, uniform x, degree-first y and z; (f) $r = 2$, uniform x, degree-first y and z; (g) $r = \frac{1}{2}$, degree-first x, uniform y and z; (h) $r = 1$, degree-first x, uniform y and z; (i) $r = 2$, degree-first x, uniform y and z; (j) $r = \frac{1}{2}$, degree-first x, y and z; (k) $r = 1$, degree-first x, y and z; (l) $r = 2$, degree-first x, y and z. It can be seen that the equilibrium security of a cyber network ascends with the increase of s.

to that of the defense resources.

$$r_{AD} = \frac{||\mathbf{x}||_1}{||\mathbf{y}||_1 + ||\mathbf{z}||_1}. \tag{84}$$

Obviously, the equilibrium security of a cyber network declines with the rise of the attack-defense ratio. At present we wonder how the amount of defense resources per unit time affects the security of a cyber network, provided the attack-defense ratio is given. Now, let us study the problem through computer simulations.

Experiment 3: Consider 504 instances of the GSCS model, where G assumes one of the six trees shown in Fig. 2, $\alpha = 0.05$, $\beta = 0.01$, $\delta = 1$, $\gamma = 1$, $f(x) = \frac{x}{1+x}$, $r_{AD} = r$, $||\mathbf{y}||_1 = ||\mathbf{z}||_1 = s$, $s \in \{2, 3, \cdots, 10\}$, *(a)* $r = \frac{1}{2}$, *uniform* **x**, **y** *and* **z**; *(b)* $r = 1$, *uniform* **x**, **y** *and* **z**; *(c)* $r = 2$, *uniform* **x**, **y** *and* **z**; *(d)* $r = \frac{1}{2}$, *uniform* **x**, *degree-first* **y** *and* **z**; *(e)* $r = 1$, *uniform* **x**, *degree-first* **y** *and* **z**; *(f)* $r = 2$, *uniform* **x**, *degree-first* **y** *and* **z**; *(g)* $r = \frac{1}{2}$, *degree-first* **x**, *uniform* **y** *and* **z**; *(h)* $r = 1$, *degree-first* **x**, *uniform* **y** *and* **z**; *(i)* $r = 2$, *degree-first* **x**, *uniform* **y** *and* **z**; *(j)* $r = \frac{1}{2}$, *degree-first* **x**, **y** *and* **z**; *(k)* $r = 1$, *degree-first* **x**, **y** *and* **z**; *(l)* $r = 2$, *degree-first* **x**, **y** *and* **z**. *For each of the GSCS models, the equilibrium security of the cyber network is shown in Fig. 5. It can be seen that the equilibrium security of a cyber network ascends with s.*

Many similar experiments exhibit qualitatively similar phenomena. It is concluded that, given the attack-defense ratio, the equilibrium security of a cyber network goes up with the increase of the defense resources per unit time. This finding sounds a good news to the defenders of cyber networks, because the economic motivation of cyber malefactors to conduct APT attacks to well-protected cyber networks subsides. In practice, configuring more defense resources for cyber networks is always an effective means of protecting against APTs.

VII. CONCLUDING REMARKS

This paper has addressed the evaluation of the security of the cyber networks under APTs. Based on a dynamic model capturing the APT-based cyber attack-defense processes and its proved global stability, a new security metric of cyber networks known as the equilibrium security has been introduced. The impact of several factors on the equilibrium security of a cyber network has been examined. The equilibrium security is potentially applicable to the evaluation of the security of real-world cyber networks under APTs, because the estimation of the equilibrium security requires only a small number of sample data on the network state and needs no knowledge of the model. To achieve the goal, a cost-efficient sampling method must be developed.

There are still lots of open problems concerning the security evaluation of the cyber networks under APTs. In the situation that the attack strategy is already known, the defender should determine a defense strategy that maximizes the equilibrium security of the network among all feasible defense strategies, which we refer to as a *max defense strategy* of the network under the attack strategy, as well as the corresponding equilibrium security, which we refer to as the *max equilibrium security* of the network under the attack strategy. However, when the attack strategy is not known, the defender must solve a two-step optimization problem: (a) for every admissible defense strategy, find out an attack strategy that minimizes the equilibrium security of the network among all possible attack strategies, which we refer to as a *min attack strategy* to the network under the defense strategy, as well as the corresponding equilibrium security, which we refer to as the *min equilibrium security* of the network under the defense strategy; and (b) determine a defense strategy that maximizes the min equilibrium security among all the feasible defense strategies, which we refer to as a *max-min defense strategy* of the network, as well as the corresponding equilibrium security, which we refer to as the *max-min equilibrium security* of the network. In this work, the attack and defense strategies are both assumed to be unvaried over time. In most cases,

the attacker may flexibly alter the attack strategy, and the defender may accordingly change the defense strategy. In this context, the security evaluation of cyber networks would involve the optimal control theory [44]–[46] or the dynamic game theory [47], [48].

ACKNOWLEDGMENTS

The authors are grateful to the two anonymous reviewers and the editor for their valuable comments and suggestions that have improved the quality of the paper greatly.

REFERENCES

[1] R. Kitchin, *Cyberspace: The World in the Wires*. Hoboken, NJ, USA: Wiley, 1998.
[2] M. Dodge and R. Kitchin, *Mapping Cyberspace*. Evanston, IL, USA: Routledge, 2000.
[3] D. Shoemaker and W. A. Conklin, *Cybersecurity: The Essential Body of Knowledge*. Boston, MA, USA: Cengage Learning, 2011.
[4] G. K. Kostopoulos, *Cyberspace and Cybersecurity*. New York, NY, USA: Taylor & Francis, 2012.
[5] P. W. Singer and A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*. London, U.K.: Oxford Univ. Press, 2014.
[6] A. Jaquith, *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. Reading, MA, USA: Addison-Wesley, 2007.
[7] W. Jensen, "Directions in security metrics research," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NISTIR7564, 2009.
[8] Y. Cheng, J. Deng, J. Li, S. A. DeLoach, A. Singhal, and X. Ou, "Metrics of security," in *Cyber Defense and Situational Awareness* (Advances in Information Security), vol. 62, A. Kott, C. Wang, and R. Erbacher, Eds. Switzerland: Springer, 2014.
[9] C. Tankard, "Advanced persistent threats and how to monitor and deter them," *Netw. Secur.*, vol. 8, pp. 16–19, Aug. 2011.
[10] P. Chen, L. Desmet, and C. Huygens, "A study on advanced persistent threats," in *Communications and Multimedia Security* (Lecture Notes in Computer Science), vol. 8735, B. De Decker and A. Zuquete, Eds. Berlin, Germany: Springer, 2014.
[11] P. Hu, H. Li, H. Fu, D. Cansever, and P. Mohapatra, "Dynamic defense strategy against advanced persistent threat with insiders," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2015, pp. 747–756.
[12] S. Rass, S. König, and S. Schauer, "Defending against advanced persistent threats using game-theory," *PLoS ONE*, vol. 12, no. 1, p. e0168675, 2017.
[13] C. Phillips and L. P. Swiler, "A graph-based system for network-vulnerability analysis," in *Proc. Workshop New Secur. Paradigms*, 1998, pp. 71–79.
[14] I. Kotenko and M. Stepashkin, "Attack graph based evaluation of network security," in *Proc. 10th IFIP Int. Conf. Commun. Multimedia Secur.*, 2006, pp. 216–227.
[15] M. Frigault and L. Wang, "Measuring network security using Bayesian network-based attack graphs," in *Proc. 32nd Annu. IEEE Int. Conf. Comput. Softw. Appl. (COMPSAC)*, Jul. 2008, pp. 698–703.
[16] R. P. Lippmann, J. F. Riordan, T. H. Yu, and K. K. Watson, "Continuous security metrics for prevalent network threats: Introduction and first four metrics," Massachusetts Inst. Technol., Cambridge, MA, USA, Tech. Rep. ESC-TR-2010-099, 2012.
[17] S. E. Yusuf, J. B. Hong, M. Ge, and D. S. Kim, "Composite metrics for network security analysis," *Softw. Netw.*, vol. 2017, no. 1, pp. 137–160, 2017.
[18] M. Pendleton, R. Garcia-Lebron, J.-H. Cho, and S. Xu, "A survey on systems security metrics," *ACM Comput. Surv.*, vol. 49, no. 4, 2017, Art. no. 62.
[19] P. V. Mieghem, J. Omic, and R. Kooij, "Virus spread in networks," *IEEE/ACM Trans. Netw.*, vol. 17, no. 1, pp. 1–14, Feb. 2009.
[20] P. Van Mieghem, "The N-intertwined SIS epidemic network model," *Computing*, vol. 93, nos. 2–4, pp. 147–169, 2011.
[21] F. D. Sahneh, F. N. Chowdhury, and C. M. Scoglio, "On the existence of a threshold for preventive behavioral responses to suppress epidemic spreading," *Sci. Rep.*, vol. 2, p. 623, Sep. 2012.
[22] S. Xu, W. Lu, and Z. Zhan, "A stochastic model of multivirus dynamics," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 1, pp. 30–45, Jan. 2012.
[23] S. Xu, W. Lu, and L. Xu, "Push- and pull-based epidemic spreading in networks: Thresholds and deeper insights," *ACM Trans. Auto. Adapt. Syst.*, vol. 7, no. 3, 2012, Art. no. 32.
[24] S. Xu, W. Lu, L. Xu, and Z. Zhan, "Adaptive epidemic dynamics in networks: Thresholds and control," *ACM Trans. Auto. Adapt. Syst.*, vol. 8, no. 4, 2014, Art. no. 19.
[25] L.-X. Yang, M. Draief, and X. Yang, "The impact of the network topology on the viral prevalence: A node-based approach," *PLoS ONE*, vol. 10, no. 7, p. e0134507, 2015.
[26] L. X. Yang, M. Draief, and X. Yang, "Heterogeneous virus propagation in networks: A theoretical study," *Math. Methods Appl. Sci.*, vol. 40, no. 5, pp. 1396–1413, 2017.
[27] L.-X. Yang, X. Yang, and Y. Wu, "The impact of patch forwarding on the prevalence of computer virus: A theoretical assessment approach," *Appl. Math. Model.*, vol. 43, pp. 110–125, Mar. 2017.
[28] Y. Wu, P. Li, L.-X. Yang, X. Yang, and Y. Y. Tang, "A theoretical method for assessing disruptive computer viruses," *Phys. A, Stat. Mech. Appl.*, vol. 482, pp. 325–336, Sep. 2017.
[29] L.-X. Yang, P. Li, X. Yang, and Y. Y. Tang. (May 2017). "Distributed interaction between computer virus and patch: A modeling study." [Online]. Available: https://arxiv.org/abs/1705.04818
[30] L.-X. Yang, P. Li, X. Yang, Y. Wu, and Y. Y. Tang. (May 2017). "Analysis of the effectiveness of the truth-spreading strategy for inhibiting rumors." [Online]. Available: https://arxiv.org/abs/1705.06604
[31] L.-X. Yang, T. Zhang, X. Yang, Y. Wu, and Y. Y. Tang. (May 2017). "On the effectiveness of the truth-spreading/rumor-blocking strategy for restraining rumors." [Online]. Available: https://arxiv.org/abs/1705.10618
[32] T. Zhang, X. Yang, L.-X. Yang, Y. Y. Tang, and Y. Wu. (Apr. 2017). "A discount strategy in word-of-mouth marketing and its assessment." [Online]. Available: https://arxiv.org/abs/1704.06910
[33] S. Xu, "Cybersecurity dynamics," in *Proc. Symp. Bootcamp Sci. Secur. (HotSoS)*, 2014, Art. no. 14.
[34] W. Lu, S. Xu, and X. Yu, "Optimizing active cyber defense," in *Decision and Game Theory for Security* (Lecture Notes in Computer Science), vol. 8252, S. K. Das, C. Nita-Rotaru and M. Kantarciolu, Eds. Switzerland: Springer, 2013.
[35] S. Xu, W. Lu, and H. Li, "A stochastic model of active cyber defense dynamics," *Internet Math.*, vol. 11, no. 1, pp. 28–75, 2015.
[36] R. Zheng, W. Lu, and S. Xu, "Active cyber defense dynamics exhibiting rich phenomena," in *Proc. HotSoS*, 2015, Art. no. 2.
[37] R. Zheng, W. Lu, and S. Xu, "Preventive and reactive cyber defense dynamics is globally stable," *IEEE Trans. Netw. Sci. Eng.*, to be published, doi: 10.1109/TNSE.2017.2734904.
[38] H. K. Khalil, *Nonlinear Systems*, 3rd ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 2002.
[39] J. Szarski, *Differential Inequalities*. Warszawa, Poland: Polish Scientific Publishers, 1965.
[40] R. P. Agarwal, M. Meehan, and D. O'Regan, *Fixed Point Theory and Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2001.
[41] R. A. Horn and C. R. Johnson, *Matrix Analysis*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2013.
[42] R. Varga, *Matrix Iterative Analysis*. New York, NY, USA: Springer-Verlag, 2000.
[43] K. S. Narendra and R. Shorten, "Hurwitz stability of Metzler matrices," *IEEE Trans. Autom. Control*, vol. 55, no. 6, pp. 1484–1487, Jun. 2010.
[44] E. K. Donald, *Optimal Control Theory: An Introduction*. New York, NY, USA: Dover, 2012.
[45] L.-X. Yang, M. Draief, and X. Yang, "The optimal dynamic immunization under a controlled heterogeneous node-based SIRS model," *Phys. A, Stat. Mech. Appl.*, vol. 450, pp. 403–415, May 2016.
[46] T. Zhang, L.-X. Yang, X. Yang, Y. Wu, and Y. Y. Tang, "Dynamic malware containment under an epidemic model with alert," *Phys. A, Stat. Mech. Appl.*, vol. 470, pp. 249–260, Mar. 2017.
[47] R. Isaacs, *Differential Games: A Mathematical Theory with Applications to Warfare and Pursuit, Control and Optimization*. New York, NY, USA: Dover, 1999.
[48] A. Bressan, "Noncooperative differential games," *Milan J. Math.*, vol. 79, no. 2, pp. 357–427, 2011.

LU-XING YANG received the B.Sc. degree from the College of Mathematics and Statistics, Chongqing University, Chongqing, China, in 2012, and the Ph.D. degree from the College of Computer Science, Chongqing University, in 2015. He is currently a Post-Doctoral Researcher with the Delft University of Technology, Delft, The Netherlands. He visited Imperial College London, U.K., from 2014 to 2015. He has authored or co-authored over 30 papers in peer-reviewed international journals. His research interests include networks, epidemic modeling, and cybersecurity dynamics.

PENGDENG LI received the B.Sc. degree from Chongqing University, China, in 2015. He is currently pursuing the Ph.D. degree. His research interests include cybersecurity.

XIAOFAN YANG received the B.Sc. degree from the Department of Mathematics, Sichuan University, in 1985, the M.Sc. degree from the Department of Applied Mathematics, Chongqing University, in 1988, and the Ph.D. degree from the Department of Computer Science, Chongqing University in 1994. He is a Professor of computer science with Chongqing University. He joined Chongqing University in 1987. He visited the University of Reading in England from 1998 to 1999, Hong Kong Baptist University in 2005, 2007, and 2009, and the University of Macau in 2016 and 2017. He has authored or co-authored over 150 papers in peer-reviewed international journals, and over 20 students have received the Ph.D. degree under his supervision. His research interests include computer virus spreading, cybersecurity and fault tolerant computing, and applied nonlinear dynamics.

YUAN YAN TANG is a Chair Professor with the Faculty of Science and Technology, University of Macau, Macau, China, and a Professor/Adjunct Professor/Honorary Professor with several institutes, including Chongqing University, Chongqing, China, Concordia University, Montréal, QC, Canada, and Hong Kong Baptist University, Hong Kong. He has authored or co-authored over 400 academic papers and authored/co-authored over 25 monographs/books/book chapters. His current research interests include wavelets, pattern recognition, and image processing. He is a fellow of IAPR. He is the Founder and the Editor-in-Chief of the *International Journal on Wavelets, Multiresolution, and Information Processing* and an Associate Editor of several international journals. He is the Founder and the Chair of pattern recognition committee in the IEEE SMC.