IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 12, 2018, accepted October 2, 2018, date of publication October 8, 2018, date of current version October 31, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2874446

A Differential Game Approach to Patch Injection

LU-XING YANG[1], (Member, IEEE), PENGDENG LI[2], XIAOFAN YANG[2], (Member, IEEE), YONG XIANG[1], (Senior Member, IEEE), AND WANLEI ZHOU[3], (Senior Member, IEEE)

[1]School of Information Technology, Deakin University, Burwood, VIC 3125, Australia
[2]School of Big Data & Software Engineering, Chongqing University, Chongqing 400044, China
[3]School of Software, University of Technology Sydney, Ultimo, NSW 2007, Australia

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

This work was supported in part by the National Natural Science Foundation of China under Grant 61572006, in part by the Chongqing Basic Research and Front Exploration Project under Grant cstc2018jcyjA3093, and in part by the Australian Research Council under Grant LP170100458.

ABSTRACT To fight against the evolving computer viruses, we must constantly inject new virus patches into the computer networks. This paper addresses the patch injection problem, i.e., the problem of developing a patch injection strategy to mitigate the negative impact of virus attacks. As the impact of an attack depends on not only the patch injection strategy but the unknown virus injection strategy, the patch injection problem is very complicated. This paper initiates the study of the patch injection problem by means of security economics and differential game theory. First, based on a novel virus-patch mixed propagation model, we model the original problem as a differential game. Second, we develop a method for finding a candidate for the Nash equilibrium of the game, examine the structure of the candidate, and give some examples of the candidate. Furthermore, we demonstrate through comparative experiments that the candidate is better in terms of the Nash equilibrium solution concept. Therefore, we recommend the patch injection strategy in the candidate. Finally, we examine the effects of some factors on the performance of the recommended patch injection strategy. Overall, these findings undoubtedly have guiding significance to defense against virus infections.

INDEX TERMS Computer networks, computer security, modeling, nonlinear systems, decision making.

I. INTRODUCTION

Modern society relies heavily on computer networks. On a daily basis, people acquire information through the Web, communicate with each other through online social networks, and buy goods through electronic payment [1]. However, computer networks as a double-edged sword are the paradise of computer virus as well. For instance, the recent Wanna Decryptor ransomware attack is estimated to have caused a total loss of four billion dollars [2], [3]. What is worse, electronic virus is in perpetual evolution. As a matter of fact, currently available antiviruses are often insufficient to tackle future sophisticated viruses. Therefore, fighting against digital infections is a long and arduous task [4], [5].

To defend against evolving computer viruses, we must constantly develop new virus patches and inject them into computer networks [6], [7]. In this setting, we need to develop a patch injection strategy to mitigate the negative impact of virus attacks. We refer to the problem of developing an effective patch injection strategy as the *patch injection problem*. As the impact of a virus attack depends on not only the patch injection strategy but the unknown virus injection strategy, the patch injection problem is very complicated. To our knowledge, the problem has not been tackled previously. This paper approaches this problem by means of two key theories: security economics and differential game theory. Below we give a brief review of the two theories.

Security economics is a powerful way of looking at overall system security [8]. As a complement to cybersecurity engineering approaches, security economics applies economic analysis to information security issues. By taking into account economic parameters, we can propose cybersecurity strategies that minimize risk exposure of systems and networks [9], [10].

Game theory is the study of mathematical models of strategic interaction between rational decision makers [11]. In the past decade, game theory has been widely applied to various aspects of cybersecurity [12], [13]. For instances, [14] and [15] took the game-theoretic approach to address smart grid security and advanced persistent threat defense, respectively.

Differential game theory as a branch of game theory is devoted to the study of game-theoretic problems subject to continuous-time state evolution dynamics [16]. Different from static and repeated games [14], [15], differential games are played continuously in dynamic environments. In recent years, the differential game approach has been applied to some cybersecurity problems. Through the approach, [17]–[22] studied smart grid security, intrusion detection in cloud computing, auditing in cloud storage, malicious fog node identification, intrusion response in fog computing, and misinformation control, respectively.

This paper takes the first step toward solving the patch injection problem by use of security economics and differential game theory. Our main contributions in this work are summarized as follows.

- We establish a virus-patch mixed propagation with patch injection. Thereby, we formulate the attacker's virus injection strategy and the network administrator's patch injection strategy, and we estimate the attack's expected impact as well as the attacker's expected net benefit. On this basis, we model the patch injection problem as a noncooperative differential game in which the goal of the administrator is to seek an open-loop Nash equilibrium of a virus injection strategy and a patch injection strategy.
- By use of differential game theory, we derive a method for finding a candidate for the Nash equilibrium of the proposed game. We then examine the structure of the candidate. Through comparison with a set of heuristic virus and patch injection strategies, we show that the candidate is better in terms of the Nash equilibrium solution concept. Therefore, we recommend the patch injection strategy in the candidate. Finally, we examine the effects of some factors on the performance of the candidate. These findings help to minimize the negative impact and potential consequence of virus attacks.

The remainder of this paper is organized in this fashion. Section 2 reviews the related work. Section 3 models the patch injection problem as a differential game. Section 4 gives a method for finding a candidate for the Nash equilibrium of the game and inspects its structure, and Section 5 evaluates the performance of the candidate. The effects of some factors on the performance of the candidate are examined in Section 6. Section 7 closes this work.

II. RELATED WORK

Computer virus propagation dynamics is a new applied mathematics aiming to understand the laws governing the spread of computer virus and thereby mitigate the impact of virus attacks [23]. Originally, the study was focused on virus propagation based on homogeneous networks [24]–[27]. In particular, as virus patches can be forwarded rapidly through computer networks [28], [29], a number of virus-patch mixed propagation models on homogeneous networks were proposed [30]–[33]. Later, the finding that many real-world networks are scale-free [34], [35] set off a wave of research on virus propagation based on scale-free networks [36], [37]. With the advance in wireless networking technology, today's computer networks may be deployed in any way [38]. To understand a variety of propagation phenomena on arbitrary computer networks, a number of propagation models based on arbitrary networks, which we refer to as node-level propagation models, have been suggested [39]–[43]. In particular, a node-level virus-patch mixed propagation model has recently been reported [44].

As we know, patch forwarding has to be preceded by patch injection. However, all the above virus-patch mixed propagation models neglect patch injection. As a result, neither of them applies to the patch injection problem. In this paper, we introduce a node-novel virus-patch mixed propagation model with patch injection mechanism, which not only is in line with the actual situation but applies to the patch injection problem.

Based on the proposed virus-patch mixed propagation model, we estimate the expected impact of a virus attack as well as the expected net benefit of the attacker. On this basis, we model the patch injection problem as a differential game in which the attacker pursues the highest expected net benefit and the duty of the network administrator is to mitigate the expected impact.

Reference [17] proposed a differential game framework to demonstrate worst-case strategies for stealthy attacker to disrupt the transient stability of an electric power utility by leveraging control over distributed energy resources, showing that if the utility is able to identify uncompromised components, the impact of attack could be legitimated significantly. Reference [18] introduced and studied a differential game model for cloud intrusion detection. This work helps to improve the performance of cloud intrusion detection systems. Reference [19] established and studied a differential game model for cloud storage auditing. This work has potential application in enhancing the auditing level of cloud storage. Reference [20] proposed and studied a differential game model for identifying malicious nodes in fog computing environment. This work contributes to the promotion of fog computing security. Reference [21] suggested a differential game model for intrusion response in fog computing and derived a closed-form formula for closed-loop Nash equilibrium of the game. Inspired by all of these work, our paper addresses a new problem (the patch injection problem) by means of differential game theory. In all of these work, the propagation of cyber attack through heterogeneous network is neglected. In sharp contrast to these work, our work is based on a heterogeneous network-based epidemic model, i.e., the node-level virus-patch mixed propagation model. Hence, our work matches the practice better.

Our work is closely related to [45]. In this paper, the virus-containing problem was studied using game theory. However, this paper assumes the network is homogeneous, not complying with the actual situation. Worse still, this paper leaves patch injection out of consideration. In contrast, our work is grounded in reality and hence has good practical value.

Our work is related to [22] as well. In this paper, a differential game about misinformation control was proposed and studied. As the underlying spreading network of this game is highly averaged through the mean-field approach, the practical applicability of the recommended misinformation control strategy is questionable. Our work has been inspired by this work. However, in our paper the underlying spreading model of the differential game accommodates the complete information on the network topology and hence captures the virus-patch mixed spreading processes relatively accurately. As a result, the recommended patch injection strategy is expected to achieve a better performance.

III. THE PATCH INJECTION PROBLEM AND ITS MODELING

This paper addresses the following problem:

Patch injection problem: Develop a patch injection strategy to mitigate the negative impact of virus attacks.

For this purpose, in this section we model the problem by following these steps: (1) introduce terminologies and notations, (2) establish a state evolution model, (3) formulate the virus and patch injection strategies, (4) quantify the impact of the virus attack as well as the benefit of the attacker, and (5) model the patch injection problem.

A. BASIC TERMINOLOGIES AND NOTATIONS

Consider a computer network with the topology $G = (V, E)$, where $V = \{1, 2, \cdots, N\}$ denotes the set of all the hosts (nodes) in the network, $(i, j) \in E$ denotes that host i has access to host j. In this paper, we assume G is unchanged over time. Let $\mathbf{A} = \left(a_{ij}\right)_{N\times N}$ denote the adjacency matrix of G.

Suppose there is a cyber malefactor who keeps injecting new viruses into the network in the time horizon $[0, T]$. To mitigate the impact of the virus attack, the network administrator has to constantly inject new patches into the network. Assume that at any time $t \in [0, T]$, each and every node in the network is either *susceptible* or *infected* or *patched*. Susceptible nodes are not infected with any virus but are vulnerable to the newest virus, because they have not received the newest patch. Infected nodes are infected with at least one virus. Patched nodes are not infected with any virus and are immune to the newest virus, because they have received the newest patch against the newest virus. Let $X_i(t) = 0$, 1, and 2 denote the events that node i is susceptible, infected, and patched at time t, respectively. Then all $X_i(t)$ are random variables, and the random vector

$$\mathbf{X}(t) = (X_1(t), X_2(t), \cdots, X_N(t)) \tag{1}$$

stands for the state of the network at time t.

Let Pr denote probability. For $1 \le i \le N$, $0 \le t \le T$, let

$$S_i(t) = \Pr\{X_i(t) = 0\}, \quad I_i(t) = \Pr\{X_i(t) = 1\},$$
$$P_i(t) = \Pr\{X_i(t) = 0\}. \tag{2}$$

That is, $S_i(t)$, $I_i(t)$, and $P_i(t)$ denote the probabilities of node i being susceptible, infected, and patched at time t, respectively. As $S_i(t) = 1 - I_i(t) - P_i(t)$, the vector

$$\mathbf{E}(t) = (I_1(t), \cdots, I_N(t), P_1(t), \cdots, P_N(t)) \tag{3}$$

stands for the expected state of the network at time t.

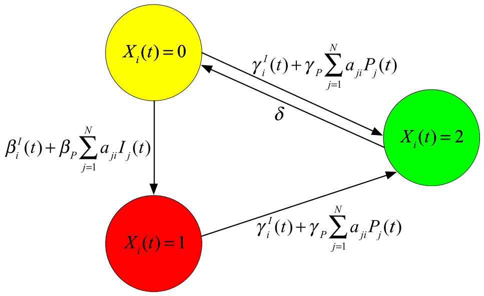
$X_i(t)=0$
$\gamma_i^I(t)+\gamma_P\sum_{j=1}^{N} a_{ji}P_j(t)$
δ
$X_i(t)=2$
$\beta_i^I(t)+\beta_P\sum_{j=1}^{N} a_{ji}I_j(t)$
$X_i(t)=1$
$\gamma_i^I(t)+\gamma_P\sum_{j=1}^{N} a_{ji}P_j(t)$

FIGURE 1. A diagram of the hypotheses (H_1)-(H_5).

Remark 1: The network administrator may collect and analyze virus reports delivered by network users to decide whether one or a few viruses are present and, if so, estimate the network's initial expected state $\mathbf{E}(0)$.

B. A STATE EVOLUTION MODEL OF THE NETWORK

To model the patch injection problem, we need to model the evolution process of the network's expected state over time. To this end, let us introduce a set of rational hypotheses as follows (see Fig. 1).

(H$_1$) For $1 \le i \le N$, $0 \le t \le T$, virus injection renders the susceptible node i to become infected at time t at rate $\beta_i^I(t)$.

(H$_2$) For $1 \le i, j \le N$, $0 \le t \le T$, virus propagation coming from the infected node j renders the susceptible node i to become infected at time t at average rate $\beta_P a_{ji}$, where β_P is a positive constant we refer to as the *virus propagation rate*. Hence, for $1 \le i \le N$, $0 \le t \le T$, virus propagation renders the susceptible node i to become infected at time t approximately at average rate $\sum_{j=1}^N \beta_P a_{ji}(t) I_j(t)$. This hypothesis implies that virus propagation is a fully spontaneous process and hence is not under the control of the attacker.

(H$_3$) For $1 \le i \le N$, $0 \le t \le T$, patch injection makes the unpatched node i to become patched at time t at rate $\gamma_i^I(t)$.

(H$_4$) For $1 \le i, j \le N$, $0 \le t \le T$, patch forwarding coming from the patched node j makes the unpatched node i to become patched at time t at average rate $\gamma_P a_{ji}$, where γ_P is a positive constant we refer to as the *patch forwarding rate*. Hence, for $1 \le i \le N$, $0 \le t \le T$, patch forwarding makes the unpatched node i to become patched at time t approximately at average rate $\sum_{j=1}^N \gamma_P a_{ji}(t) I_j(t)$. This hypothesis implies that patch forwarding is a fully spontaneous process and hence is not under the control of the network administrator.

(H$_5$) For $1 \le i \le N$, $0 \le t \le T$, the emergence of new virus renders the patched node i to become susceptible at time t at average rate δ, where δ is a positive constant we refer to δ as the *patch failure rate*.

Remark 2: In practice, β_P, γ_P, and δ can be estimated by the network administrator through analyzing the historical data.

Combining the above hypotheses and based on differential dynamical system theory [46], the network's expected state evolves approximately according to the following differential dynamical system:

$$\begin{cases} \dfrac{dI_i(t)}{dt} = \left[\beta_i^I(t) + \beta_P \displaystyle\sum_{j=1}^N a_{ji} I_j(t)\right][1 - I_i(t) - P_i(t)] \\ \qquad - \left[\gamma_i^I(t) + \gamma_P \displaystyle\sum_{j=1}^N a_{ji} P_j(t)\right] I_i(t), \\ \dfrac{dP_i(t)}{dt} = \left[\gamma_i^I(t) + \gamma_P \displaystyle\sum_{j=1}^N a_{ji} P_j(t)\right][1 - P_i(t)] - \delta P_i(t), \\ \qquad 0 \le t \le T, 1 \le i \le N, \end{cases} \tag{4}$$

with the initial condition $\mathbf{E}(0) = \mathbf{E}_0$. We refer to the system as the *Susceptible-Infected-Patched-Susceptible (SIPS) model*.

C. THE VIRUS AND PATCH INJECTION STRATEGIES

The N-dimensional function $\mathbf{x}$ defined by

$$\mathbf{x}(t) = (\beta_1^I(t), \cdots, \beta_N^I(t)), \quad 0 \le t \le T, \tag{5}$$

is under the control of the virus attacker. We refer to $\mathbf{x}$ as the *virus injection strategy*. The N-dimensional function $\mathbf{y}$ defined by

$$\mathbf{y}(t) = (\gamma_1^I(t), \cdots, \gamma_N^I(t)), \quad 0 \le t \le T, \tag{6}$$

is under the control of the network administrator. We refer to $\mathbf{y}$ as the *patch injection strategy*. Let $PC^N[0, T]$ denote the set of all the piecewise continuous N-dimensional functions on the interval $[0, T]$, and let us impose some restrictions on the virus and patch injection strategies as follows.

(H_6) $\mathbf{x}, \mathbf{y} \in PC^N[0, T]$. The hypothesis implies that the virus and patch injection strategies are easily implementable.

(H_7) For $1 \le i \le N$, $0 \le t \le T$, we have $\underline{\beta_i} \le \beta_i(t) \le \overline{\beta_i}$, $\underline{\gamma_i} \le \gamma_i(t) \le \overline{\gamma_i}$, where $\underline{\beta_i}$, $\overline{\beta_i}$, $\underline{\gamma_i}$, and $\overline{\gamma_i}$ are all positive constants.

Remark 3: *$\underline{\beta_i}$ stands for the lowest allowable virus injection rate and measures the lowest attack strength against node i. $\overline{\beta_i}$ stands for the highest allowable virus injection rate and is determined by the highest allowable cost for attacking node i. $\underline{\gamma_i}$ stands for the lowest allowable patch injection rate and measures the lowest defense strength of node i. $\overline{\gamma_i}$ stands for the highest allowable patch injection rate for node i and is determined by the highest allowable cost for patching node i.*

Based on the above two hypotheses, the set of all the admissible virus injection strategies is

$$\mathscr{U}_V = \left\{\mathbf{x} \in PC^N[0, T] \mid \mathbf{x}(t) \in \prod_{i=1}^N [\underline{\beta_i}, \overline{\beta_i}], t \in [0, T]\right\}, \tag{7}$$

and the set of all the admissible patch injection strategies is

$$\mathscr{U}_P = \left\{\mathbf{y} \in PC^N[0, T] \mid \mathbf{y}(t) \in \prod_{i=1}^N [\underline{\gamma_i}, \overline{\gamma_i}], t \in [0, T]\right\}. \tag{8}$$

Let

$$\Omega = \{(I_1, \cdots, I_N, P_1, \cdots, P_N) \in \mathbb{R}_+^{2N} \mid I_i + P_i \le 1, \\ 1 \le i \le N\}. \tag{9}$$

Let Ω denote the interior of Ω. We have the following preliminary result.

Lemma 1: *Suppose* $\mathbf{E}(t)$ $(0 \le t \le T)$ *is a solution to the SIPS model (4). Then* $\mathbf{E}(t) \in \Omega$, $0 < t \le T$.

The proof of this lemma is left to Appendix A.

D. THE BENEFIT OF THE ATTACKER AND THE IMPACT OF THE VIRUS ATTACK

To model the patch injection problem, we need to quantify the benefit of the attacker as well as the impact of the virus attack.

First, define the *value* of each node as the average loss per unit time suffered by the owner of the node. For $1 \le i \le N$, denote the value of node i as v_i units (dollars, say). Let $\mathbf{v} = (v_1, \cdots, v_N)$.

(H_8) For $1 \le i \le N$, v_i is a positive constant.

Based on the hypothesis, the expected loss of the network in the time horizon $[0, T]$ is

$$L(\mathbf{x}, \mathbf{y}) = \int_0^T \sum_{i=1}^N v_i I_i(t) dt \tag{10}$$

units. In what follows, we adopt the quantity as the measure of the loss of the network.

Second, we quantify the cost for implementing a virus injection strategy. For this purpose, let us introduce the following hypothesis.

(H_9) For $1 \le i \le N$, the cost per unit time for injecting viruses into the susceptible node i at the rate of β is $\phi_i(\beta)$ units, where $\phi_i(0) = 0$, ϕ_i is strictly increasing.

Every ϕ_i can be approximated by carrying out simulated virus injections with different rates and then generating a curve fitting all the simulated costs. Based on the hypothesis, the expected cost for implementing the virus injection strategy $\mathbf{x}$ is

$$C_V(\mathbf{x}, \mathbf{y}) = \int_0^T \sum_{i=1}^N \phi_i(\beta_i^I(t))(1 - I_i(t) - P_i(t)) dt \tag{11}$$

units. Henceforth, we adopt the quantity as the measure of the cost for implementing the virus injection strategy $\mathbf{x}$.

Combining the above discussions, we use the quantity

$$J_V(\mathbf{x},\mathbf{y}) = L(\mathbf{x},\mathbf{y}) - C_V(\mathbf{x},\mathbf{y}) = \int_0^T \sum_{i=1}^N \left[v_i I_i(t) - \phi_i\left(\beta_i^I(t)\right)(1 - I_i(t) - P_i(t))\right] dt \tag{12}$$

to measure the benefit of the attacker.

Finally, let us measure the cost for implementing a patch injection strategy. To this end, we introduce the following hypothesis.

1) [(H$_{10}$)] For $1 \le i \le N$, the cost per unit time for injecting patches into the unpatched node i at the rate of γ is $\psi_i(\gamma)$ units, where $\psi_i(0) = 0$, ψ_i is strictly increasing.

Every ψ_i can be approximated by carrying out simulated patch injections with different rates and then generating a curve fitting all the simulated costs. Based on the hypothesis, the expected cost for implementing the patch injection strategy $\mathbf{y}$ is

$$C_P(\mathbf{x},\mathbf{y}) = \int_0^T \sum_{i=1}^N \psi_i(\gamma_i^I(t))(1 - P_i(t))dt \tag{13}$$

units. From now on, we adopt this quantity as the measure of the cost for implementing the patch injection strategy $\mathbf{y}$.

Combining the above discussions, we may use the quantity

$$J_P(\mathbf{x},\mathbf{y}) = L(\mathbf{x},\mathbf{y}) + C_P(\mathbf{x},\mathbf{y}) = \int_0^T \sum_{i=1}^N [v_i I_i(t) + \psi_i\left(\gamma_i^I(t)\right)(1 - P_i(t))]dt. \tag{14}$$

to measure the impact of the virus attack.

E. THE MODELING OF THE PATCH INJECTION PROBLEM

Based on the previous discussions, the patch injection problem comes down to the problem of seeking a patch injection strategy $\mathbf{y} \in \mathscr{U}_P$ to mitigate $J_P(\mathbf{x},\mathbf{y})$. However, $J_P(\mathbf{x},\mathbf{y})$ is dependent on not only $\mathbf{y}$ but the unknown virus injection strategy $\mathbf{x} \in \mathscr{U}_V$. This complicates the patch injection problem.

From the worst-case perspective, we may assume the attacker is aware of the loss of the network and attempts to maximize his benefit $J_V(\mathbf{x},\mathbf{y})$. In this setting, the solution concept of Nash equilibrium is relevant. A strategy pair $(\mathbf{x}^*,\mathbf{y}^*) \in \mathscr{U}_V \times \mathscr{U}_P$ is referred to as a *Nash equilibrium* if

$$J_V(\mathbf{x}^*,\mathbf{y}^*) \ge J_V(\mathbf{x},\mathbf{y}^*), \quad \forall \mathbf{x} \in \mathscr{U}_V, \tag{15}$$

and

$$J_P(\mathbf{x}^*,\mathbf{y}^*) \le J_P(\mathbf{x}^*,\mathbf{y}), \quad \forall \mathbf{y} \in \mathscr{U}_P. \tag{16}$$

This implies that (a) when the network administrator sticks to the patch injection strategy $\mathbf{y}^*$, the attacker has to choose the virus injection strategy $\mathbf{x}^*$ to maximize his benefit, and (b) when the attacker insists on $\mathbf{x}^*$, the administrator cannot reduce the impact of the virus attack by deviating from $\mathbf{y}^*$. Therefore, in the worst-case scenario the patch injection strategy $\mathbf{y}^*$ is acceptable to the network administrator.

Combining the above discussions, we model the patch injection problem as the following noncooperative differential game:

Patch injection game: Suppose the attacker attempts to maximize $J_V(\mathbf{x},\mathbf{y})$, and the network administrator tries to minimize $J_P(\mathbf{x},\mathbf{y})$, where $(\mathbf{x},\mathbf{y}) \in \mathscr{U}_V \times \mathscr{U}_P$. Seek a Nash equilibrium.

Suppose $(\mathbf{x}^*,\mathbf{y}^*)$ is a Nash equilibrium of the patch injection game. We recommend the patch injection strategy $\mathbf{y}^*$ to the network administrator. In the next section, we will try to solve the patch injection game.

IV. A STUDY OF THE PATCH INJECTION GAME

In this section, we study the patch injection game by means of differential game theory. First, we develop a method for seeking a candidate for the Nash equilibrium of the game. Second, we examine the structure of the candidate. Finally, we give some examples of the candidate.

A. SEEKING A CANDIDATE FOR THE NASH EQUILIBRIUM

To develop a method for finding a candidate for the Nash equilibrium of the game, we need to derive a necessary condition for the Nash equilibrium. This involves the following two Hamiltonians.

$$H_V(\mathbf{E},\mathbf{x},\mathbf{y},\lambda) = \sum_{i=1}^N \left[v_i I_i - \phi_i(\beta_i^I)(1 - I_i - P_i)\right] + \sum_{i=1}^N \lambda_i^I \frac{dI_i}{dt} + \sum_{i=1}^N \lambda_i^P \frac{dP_i}{dt}, \tag{17}$$

where $\lambda = (\lambda_I, \lambda_P) = (\lambda_1^I, \cdots, \lambda_N^I, \lambda_1^P, \cdots, \lambda_N^P)$ is the continuous and piecewise differentiable adjoint function.

$$H_P(\mathbf{E},\mathbf{x},\mathbf{y},\mu) = \sum_{i=1}^N \left[v_i I_i + \psi_i(\gamma_i^I)(1 - P_i)\right] + \sum_{i=1}^N \mu_i^I \frac{dI_i}{dt} + \sum_{i=1}^N \mu_i^P \frac{dP_i}{dt}, \tag{18}$$

where $\mu = (\mu_I, \mu_P) = (\mu_1^I, \cdots, \mu_N^I, \mu_1^P, \cdots, \mu_N^P)$ is the continuous and piecewise differentiable adjoint function.

We are ready to give the necessary condition.

Theorem 1: Suppose $(\mathbf{x},\mathbf{y})$ *is a Nash equilibrium of the patch injection game,* $\mathbf{E}$ *the solution to the associated SIPS model. Then there exist* λ *and* μ *with* $\lambda(T) = \mu(T) = \mathbf{0}$ *such that the system (19), as shown at the top of the next page, holds. Moreover,*

$$\begin{aligned} \beta_i^I(t) &\in \arg \max_{\beta \in [\underline{\beta_i}, \overline{\beta_i}]} f_i(\beta; t), \\ \gamma_i^I(t) &\in \arg \min_{\gamma \in [\underline{\gamma_i}, \overline{\gamma_i}]} g_i(\gamma; t), \quad 0 \le t \le T, 1 \le i \le N, \end{aligned} \tag{20}$$

where

$$\begin{aligned} f_i(\beta; t) &= \lambda_i^I(t)\beta - \phi_i(\beta), \\ g_i(\gamma; t) &= \left[\mu_i^P(t)(1 - P_i(t)) - \mu_i^I(t) I_i(t)\right]\gamma \\ &\quad + (1 - P_i(t))\psi_i(\gamma). \end{aligned} \tag{21}$$

$$\begin{cases} \dfrac{d\lambda_i^I(t)}{dt} = -v_i - \phi_i(\beta_i^I(t)) - \beta_P \displaystyle\sum_{j=1}^{N} a_{ij}\lambda_j^I(t)\left[1 - I_j(t) - P_j(t)\right]\lambda_i^I(t)\left[\beta_i^I(t) + \gamma_i^I(t) + \sum_{j=1}^{N} a_{ji}\left(\beta_P I_j(t) + \gamma_P P_j(t)\right)\right], \\ \dfrac{d\lambda_i^P(t)}{dt} = -\phi_i(\beta_i^I(t)) + \gamma_P \displaystyle\sum_{j=1}^{N} a_{ij}\lambda_j^I(t) I_j(t) - \gamma_P \sum_{j=1}^{N} a_{ij}\lambda_j^P(t)(1 - P_j(t)) + \lambda_i^I(t)\left[\beta_i^I(t) + \beta_P \sum_{j=1}^{N} a_{ji} I_j(t)\right] \\ \qquad + \lambda_i^P(t)\left[\delta + \gamma_i^I(t) + \gamma_P \displaystyle\sum_{j=1}^{N} a_{ji} P_j(t)\right], \\ \dfrac{d\mu_i^I(t)}{dt} = -v_i - \beta_P \displaystyle\sum_{j=1}^{N} a_{ij}\mu_j^I(t)\left[1 - I_j(t) - P_j(t)\right] + \mu_i^I(t)\left[\beta_i^I(t) + \gamma_i^I(t) + \sum_{j=1}^{N} a_{ji}\left(\beta_P I_j(t) + \gamma_P P_j(t)\right)\right], \\ \dfrac{d\mu_i^P(t)}{dt} = \psi_i(\gamma_i^I(t)) + \gamma_P \displaystyle\sum_{j=1}^{N} a_{ij}\mu_j^I(t) I_j(t) - \gamma_P \sum_{j=1}^{N} a_{ij}\mu_j^P(t)(1 - P_j(t)) + \mu_i^I(t)\left[\beta_i^I(t) + \beta_P \sum_{j=1}^{N} a_{ji} I_j(t)\right] \\ \qquad + \mu_i^P(t)\left[\delta + \gamma_i^I(t) + \gamma_P \displaystyle\sum_{j=1}^{N} a_{ji} P_j(t)\right], \\ \qquad 0 \le t \le T, 1 \le i \le N. \end{cases} \tag{19}$$

We refer to the system consisting of Eqs. (4), Eqs. (19)-(20), $\mathbf{E}(0) = \mathbf{E}_0$, and $\lambda(T) = \mu(T) = \mathbf{0}$ as the *candidate system* for the patch injection game, and the strategy pair obtained by solving the system as the *candidate strategy-pair* of the game, denoted $(\mathbf{x}_{\text{CA}}, \mathbf{y}_{\text{CA}})$, because it is likely to be a Nash equilibrium of the game. Further, we refer to $\mathbf{x}_{\text{CA}}$ and $\mathbf{y}_{\text{CA}}$ as the *candidate virus injection strategy* and the *candidate patch injection strategy*, respectively.

Eqs. (19) imply that all disjoints rely on the network's expected states at all time. So, Eqs. (20)-(21) demonstrate that the candidate virus injection strategy and the candidate patch injection strategy both rely on the network's expected states at all time.

We shall invoke the Forward-Backward Sweep Method [47] to solve the candidate system to get the candidate strategy-pair of the patch injection game. The CS-FBS (abbreviation of candidate system forward-backward sweep) algorithm given below is a pseudo-code description of the method.

In all the following experiments, we will use the CS-FBS algorithm to solve the candidate system, where the convergence error $\epsilon = 10^{-6}$, the iteration bound $K = 10^3$.

B. THE STRUCTURE OF THE CANDIDATE STRATEGY-PAIR

Now, let us examine the structure of the candidate strategy-pair of the patch injection game. Let $(\mathbf{x}, \mathbf{y})$ be the candidate strategy-pair, $\mathbf{E}$ the solution to the associated SIPS model, (λ, μ) the associated adjoints. For technical reason, we will show the following lemma in Appendix B.

Lemma 2: $\lambda_I(t) > \mathbf{0}$, $\mu_I(t) > \mathbf{0}$, $\mu_P(t) < \mathbf{0}$, $t \in [0, T)$.

For brevity, let

$$\theta_i = \frac{\phi_i(\overline{\beta_i}) - \phi_i(\underline{\beta_i})}{\overline{\beta_i} - \underline{\beta_i}}, \quad 1 \le i \le N, \tag{22}$$

$$\eta_i = \frac{\psi_i(\overline{\gamma_i}) - \psi_i(\underline{\gamma_i})}{\overline{\gamma_i} - \underline{\gamma_i}}, \quad 1 \le i \le N, \tag{23}$$

$$h_i(t) = \mu_i^I(t)\frac{I_i(t)}{1 - P_i(t)} - \mu_i^P(t), \quad 0 \le t \le T,\ 1 \le i \le N. \tag{24}$$

Below we present a set of four theorems characterizing the structure of the candidate strategy-pair.

Theorem 2: Suppose ϕ_i is concave. Then

$$\beta_i^I(t) = \begin{cases} \underline{\beta_i} & \textit{if}\ \lambda_i^I(t) < \theta_i, \\ \overline{\beta_i} & \textit{if}\ \lambda_i^I(t) > \theta_i, \end{cases} \quad 0 \le t \le T. \tag{25}$$

Moreover, if

$$\theta_i < \frac{v_i + \phi_i(\underline{\beta_i})}{\overline{\beta_i} + \overline{\gamma_i} + \max\{\beta_P, \gamma_P\} d_i^-}, \tag{26}$$

then either (a) $\beta_i^I(t) = \underline{\beta_i}$ for $t \in [0, T]$, or (b) there exists $t_i \in [0, T)$ such that $\beta_i^I(t) = \overline{\beta_i}$ for $t \in [0, t_i)$ and $\beta_i^I(t) = \underline{\beta_i}$ for $t \in (t_i, T]$.

Theorem 3: Suppose ϕ_i is differentiable and strictly convex. Then

$$\beta_i^I(t) = \begin{cases} \underline{\beta_i} & \textit{if}\ \lambda_i^I(t) < \phi_i^{'}(\underline{\beta_i}), \\ \overline{\beta_i} & \textit{if}\ \lambda_i^I(t) > \phi_i^{'}(\overline{\beta_i}), \\ \left[\phi_i^{'}\right]^{-1}(\lambda_i^I(t)) & \textit{otherwise}, \end{cases} \quad 0 \le t \le T. \tag{27}$$

Algorithm 1 CS-FBS

Input: patch injection game given by $G_{PI} = \left(G, \mathbf{v}, f, \beta_P, \gamma_P, \delta, T, \{\phi_i\}_{i=1}^N, \{\psi_i\}_{i=1}^N, \mathbf{E}_0\right)$, convergence error ϵ, iteration bound K.

Output: strategy pair $(\mathbf{x}, \mathbf{y})$.

```
$k := 0$;
$\mathbf{x}^{(0)}(t) := (\underline{\beta_1}, \cdots, \underline{\beta_N}), 0 \leq t \leq T$;
$\mathbf{y}^{(0)}(t) := (\underline{\gamma_1}, \cdots, \underline{\gamma_N}), 0 \leq t \leq T$;
use the system (4) with $\mathbf{x} = \mathbf{x}^{(0)}, \mathbf{y} = \mathbf{y}^{(0)}$, and $\mathbf{E}(0) = \mathbf{E}_0$ to forwardly calculate $\mathbf{E}(t), 0 \leq t \leq T$;
$\mathbf{E}^{(1)} := \mathbf{E}$;
use the system (19) with $\mathbf{x} = \mathbf{x}^{(0)}, \mathbf{y} = \mathbf{y}^{(0)}, \mathbf{E} = \mathbf{E}^{(1)}$, and $\lambda(T) = \mu(T) = \mathbf{0}$ to backwardly calculate $\lambda(t)$ and $\mu(t), 0 \leq t \leq T$;
$\lambda^{(1)} := \lambda, \mu^{(1)} = \mu$;
use the systems (20)-(21) with $\mathbf{E} = \mathbf{E}^{(1)}, \lambda = \lambda^{(1)}$, and $\mu = \mu^{(1)}$ to calculate $\mathbf{x}(t)$ and $\mathbf{y}(t), 0 \leq t \leq T$;
$\mathbf{x}^{(1)} = \mathbf{x}, \mathbf{y}^{(1)} = \mathbf{y}$;
while $||\mathbf{x}^{(k+1)} - \mathbf{x}^{(k)}|| + ||\mathbf{y}^{(k+1)} - \mathbf{y}^{(k)}|| \geq \epsilon$ or $k < K$ do
    $k = k + 1$;
    use the system (4) with $\mathbf{x} = \mathbf{x}^{(k)}, \mathbf{y} = \mathbf{y}^{(k)}$, and $\mathbf{E}(0) = \mathbf{E}_0$ to forwardly calculate $\mathbf{E}(t), 0 \leq t \leq T$;
    $\mathbf{E}^{(k+1)} := \mathbf{E}$;
    use the system (19) with $\mathbf{x} = \mathbf{x}^{(k)}, \mathbf{y} = \mathbf{y}^{(k)}, \mathbf{E} = \mathbf{E}^{(k+1)}$, and $\lambda(T) = \mu(T) = \mathbf{0}$ to backwardly calculate $\lambda(t)$ and $\mu(t), 0 \leq t \leq T$;
    $\lambda^{(k+1)} := \lambda, \mu^{(k+1)} = \mu$;
    use the systems (20)-(21) with $\mathbf{E} = \mathbf{E}^{(k+1)}, \lambda = \lambda^{(k+1)}$, and $\mu = \mu^{(k+1)}$ to calculate $\mathbf{x}(t)$ and $\mathbf{y}(t)$, $0 \leq t \leq T$;
    $\mathbf{x}^{(k+1)} = \mathbf{x}, \mathbf{y}^{(k+1)} = \mathbf{y}$;
end while
return$(\mathbf{x}^{(k+1)}, \mathbf{y}^{(k+1)})$.
```

Moreover, if

$$\phi_i^{'}(\overline{\beta_i}) < \frac{v_i + \phi_i(\underline{\beta_i})}{\overline{\beta_i} + \overline{\gamma_i} + \max\{\beta_P, \gamma_P\}d_i^-}, \tag{28}$$

then either (a) $\beta_i^I(t) = \underline{\beta_i}$ for $t \in [0, T]$, or (b) there exists $t_i \in [0, T)$ such that β_i^I is strictly decreasing in $[0, t_i)$ and $\beta_i^I(t) = \underline{\beta_i}$ for $t \in (t_i, T]$, or (c) there exist $t_i^{(1)}, t_i^{(2)} \in [0, T)$, $t_i^{(1)} < t_i^{(2)}$, such that $\beta_i^I(t) = \overline{\beta_i}$ for $t \in [0, t_i^{(1)})$, $\beta_i^I(t)$ is strictly decreasing in $(t_i^{(1)}, t_i^{(2)})$, and $\beta_i^I(t) = \underline{\beta_i}$ for $t \in (t_i^{(2)}, T]$.

Theorem 4: Suppose ψ_i is concave. Then

$$\gamma_i(t) = \begin{cases} \underline{\gamma_i} & \text{if } h_i(t) < \eta_i, \\ \overline{\gamma_i} & \text{if } h_i(t) > \eta_i. \end{cases} \quad 0 \leq t \leq T. \tag{29}$$

Moreover, if

$$\eta_i < \frac{\psi_i(\underline{\gamma_i})}{\delta + \overline{\alpha_i} + \overline{\gamma_i} + \gamma_P d_i^-}, \tag{30}$$

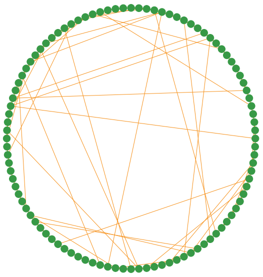

FIGURE 2. A synthetic small-world network G_{SW}.

then either (a) $\gamma_i(t) = \underline{\gamma_i}$ for $t \in [0, T]$, or (b) there exists $t_i \in [0, T)$ such that $\gamma_i^I(t) = \overline{\gamma_i}$ for $t \in [0, t_i)$ and $\gamma_i^I(t) = \underline{\gamma_i}$ for $t \in (t_i, T]$.

Theorem 5: Suppose ψ_i is differentiable and strictly convex. Then

$$\gamma_i^I(t) = \begin{cases} \underline{\gamma_i} & \text{if } h_i(t) < \psi_i^{'}(\underline{\gamma_i}), \\ \overline{\gamma_i} & \text{if } h_i(t) > \psi_i^{'}(\overline{\gamma_i}), \\ \left[\psi_i^{'}\right]^{-1}(h_i(t)) & \text{otherwise}, \end{cases} \quad 0 \leq t \leq T. \tag{31}$$

Moveover, if

$$\psi_i^{'}(\overline{\gamma_i}) < \frac{\psi_i(\underline{\gamma_i})}{\delta + \overline{\alpha_i} + \overline{\gamma_i} + \gamma_P d_i^-}, \tag{32}$$

then either (a) $\gamma_i(t) = \underline{\gamma_i}$ for $t \in [0, T]$, or (b) there exists $t_i \in [0, T)$ such that γ_i is strictly decreasing in $[0, t_i)$ and $\gamma_i(t) = \gamma_i$ for $t \in (t_i, T]$, or (c) there exist $t_i^{(1)}, t_i^{(2)} \in [0, T)$, $t_i^{(1)} < t_i^{(2)}$, such that $\gamma_i(t) = \overline{\gamma_i}$ for $t \in [0, t_i^{(1)})$, $\gamma_i(t)$ is strictly decreasing in $(t_i^{(1)}, t_i^{(2)})$, and $\gamma_i(t) = \underline{\gamma_i}$ for $t \in (t_i^{(2)}, T]$.

The proofs of the first two theorems are left to Appendixes C and D, respectively. The proofs of the last two theorems are omitted, because they are similar to those of the first two theorems, accompanied with tedious calculations.

C. EXAMPLES OF THE CANDIDATE STRATEGY-PAIR

Next, let us give some candidate strategy-pairs by solving the associated candidate systems.

Many real-world networks are small-world, i.e., they each admit a small diameter [48]. By using the Pajek software [49], we get a synthetic small-world network G_{SW} with $N = 100$ nodes, which is shown in Fig. 2.

Example 1: Consider the pair of patch injection games with $G = G_{SW}$, $\mathbf{v} = (1, \cdots, 1)$, $T = 10$, $\beta_P = 0.2$, $\gamma_P = 0.1$, $\delta = 0.15$, $\underline{\beta_i} = 0.1$, $\overline{\beta_i} = 0.4$, $\underline{\gamma_i} = 0.2$, $\overline{\gamma_i} = 0.5$, $\mathbf{E}(0) = (0.1, \cdots, 0.1)$,

(a) $\phi_i(\beta) = \sqrt{\beta}$, $\psi_i(\gamma) = \sqrt{\gamma}$, $1 \leq i \leq N$; *or*
(b) $\phi_i(\beta) = \beta^2$, $\psi_i(\gamma) = \gamma^2$, $1 \leq i \leq N$.

For the two games, the candidate virus and patch injection strategies for three nodes are plotted in Fig. 3(a)-(c) and Fig. 3(d)-(f), respectively, agreeing with Theorems 2-5.

Many real-world networks are scale-free, i.e, they each approximately follow a power-law degree distribution [34], [35]. By using Pajek [49], we get a synthetic

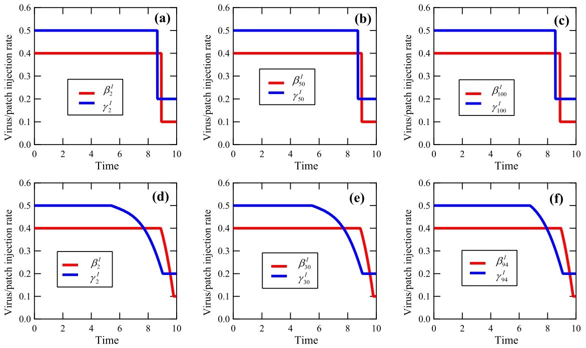

FIGURE 3. A glance of the candidate virus and patch injection strategies in Example 1.

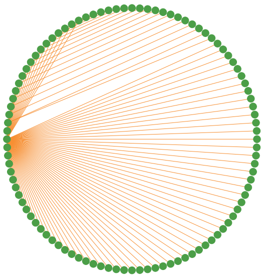

FIGURE 4. A synthetic scale-free network G_{SF}.

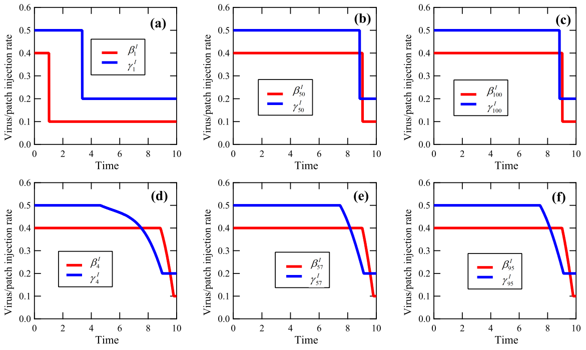

FIGURE 5. A glance of the candidate virus and patch injection strategies in Example 2.

scale-free network G_{SF} with $N = 100$ nodes, which is exhibited in Fig. 4.

Example 2: For the two patch injection games with the same parameters as those in Example 1 except $G = G_{SF}$, the candidate virus and patch injection strategies for three nodes are plotted in Fig. 5(a)-(c) and 5(d)-(f), respectively, matching Theorems 2-5.

Fig. 6 exhibits a subnet G_{FN} with $N = 100$ nodes of the facebook network [50].

Example 3: For the two patch injection games with the same parameters as those in Example 1 except $G = G_{FN}$, the candidate virus and patch injection strategies for three nodes are exhibited in Fig. 7(a)-(c) and Fig. 7(d)-(f), respectively, conforming to Theorems 2-5.

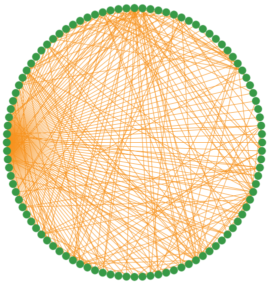

FIGURE 6. A subnet of the facebook network G_{FN}.

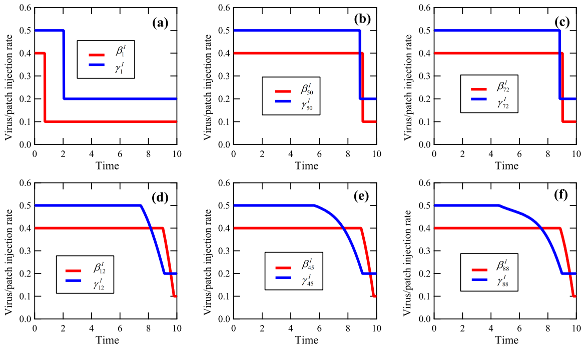

FIGURE 7. A glance of the candidate virus and patch injection strategies in Example 3.

V. PERFORMANCE EVALUATION OF THE CANDIDATE STRATEGY-PAIR

In [18]–[21], the closed-form formula of a closed-loop Nash equilibrium was given by analyzing the corresponding Bellman equation of each of the differential games. In [22], an open-loop equilibrium of the proposed differential game was calculated numerically. In the previous section, we presented a method for finding a candidate for the open-loop Nash equilibrium of the patch injection game. Due to the inherent complexity of the game, it seems impossible to show that the game admits a Nash equilibrium. As a result, the candidate strategy-pair is probably not a Nash equilibrium of the game. Therefore, it is necessary to evaluate the performance of the candidate strategy-pair through comparative experiments. This section is devoted to this work. For convenience, let $(\mathbf{x}_{\mathrm{CA}}, \mathbf{y}_{\mathrm{CA}})$ denote the candidate strategy-pair.

A. A SET OF HEURISTIC VIRUS AND PATCH INJECTION STRATEGIES

For the comparison purpose, we give a set of heuristic virus/patch injection strategies as follows.

The first virus (resp. patch) injection strategy is to always achieve the highest allowable virus (resp. patch) injection rate of each susceptible (resp. unpatched) node. We refer to the virus (resp. patch) injection strategy as the *highest rate (HR) virus (resp. patch) injection strategy*, denoted $\mathbf{x}_{\mathrm{HR}}$ (resp. $\mathbf{y}_{\mathrm{HR}}$). Formally,

$$\begin{aligned}\mathbf{x}_{\mathrm{HR}}(t) &= \left(\overline{\beta_1}, \cdots, \overline{\beta_N}\right), \quad t \in [0, T],\\ \mathbf{y}_{\mathrm{HR}}(t) &= \left(\overline{\gamma_1}, \cdots, \overline{\gamma_N}\right), \quad t \in [0, T]. \qquad (33)\end{aligned}$$

The second virus (resp. patch) injection strategy is to always achieve the lowest allowable virus (resp. patch) injection rate of each susceptible (resp. unpatched) node. We refer to the virus (resp. patch) injection strategy as the *lowest rate (LR) virus (resp. patch) injection strategy*, denoted $\mathbf{x}_{\text{LR}}$ (resp. $\mathbf{y}_{\text{LR}}$). Formally,

$$\begin{aligned} \mathbf{x}_{\text{LR}}(t) &= \left(\underline{\beta_1}, \cdots, \underline{\beta_N}\right), \quad t \in [0, T], \\ \mathbf{y}_{\text{LR}}(t) &= \left(\underline{\gamma_1}, \cdots, \underline{\gamma_N}\right), \quad t \in [0, T]. \end{aligned} \tag{34}$$

The third virus (resp. patch) injection strategy is to always achieve a virus (resp. patch) injection rate of each susceptible (resp. unpatched) node that is linearly increasing with the out-degree of the node. We refer to the virus (resp. patch) injection strategy as the *out-degree first (OF) virus (resp. patch) injection strategy*, denoted $\mathbf{x}_{\text{OF}}$ (resp. $\mathbf{y}_{\text{OF}}$). Formally,

$$\begin{aligned} \mathbf{x}_{\text{OF}} &= \left(\underline{\beta_1} + (\overline{\beta_1} - \underline{\beta_1})d_1^*, \cdots, \underline{\beta_N} + (\overline{\beta_N} - \underline{\beta_N})d_N^*\right), \\ &\qquad t \in [0, T], \\ \mathbf{y}_{\text{OF}} &= \left(\underline{\gamma_1} + (\overline{\gamma_1} - \underline{\gamma_1})d_1^*, \cdots, \underline{\gamma_N} + (\overline{\gamma_N} - \underline{\gamma_N})d_N^*\right), \\ &\qquad t \in [0, T], \end{aligned} \tag{35}$$

where $d_i^* = \frac{d_i^+}{\max_{1 \le j \le N} d_j^+}$, $d_i^+ = \sum_{j=1}^N a_{ij}$ denotes the out-degree of node i, respectively.

The fourth virus (resp. patch) injection strategy is (1) to always achieve the highest allowable virus (resp. patch) injection rate of each susceptible (resp. unpatched) node in the time horizon$[0, T/2)$, and (2) to always achieve the lowest allowable virus (resp. patch) injection rate of each susceptible (resp. unpatched) node in the time horizon$[T/2, T]$. We refer to the virus (resp. patch) injection strategy as the *high-low (HL) virus (resp. patch) injection strategy*, denoted $\mathbf{x}_{\text{HL}}$ (resp. $\mathbf{y}_{\text{HL}}$). Formally,

$$\begin{aligned} \mathbf{x}_{\text{HL}}(t) &= \begin{cases} (\overline{\beta_1}, \cdots, \overline{\beta_N}), & t \in [0, T/2), \\ (\underline{\beta_1}, \cdots, \underline{\beta_N}), & t \in [T/2, T], \end{cases} \\ \mathbf{y}_{\text{HL}}(t) &= \begin{cases} (\overline{\gamma_1}, \cdots, \overline{\gamma_N}), & t \in [0, T/2), \\ (\underline{\gamma_1}, \cdots, \underline{\gamma_N}), & t \in [T/2, T]. \end{cases} \end{aligned} \tag{36}$$

The fifth virus (resp. patch) injection strategy is to reduce the virus (resp. patch) injection rate of each susceptible (resp. unpatched) node linearly from the highest allowable virus (resp. patch) injection rate to the lowest allowable virus (resp. patch) injection rate. We refer to the virus (resp. patch) injection strategy as the *linear descent (LD) virus (resp. patch) injection strategy*, denoted $\mathbf{x}_{\text{LD}}$ (resp. $\mathbf{y}_{\text{LD}}$). Formally,

$$\begin{aligned} \mathbf{x}_{\text{LD}}(t) &= \left(\overline{\beta_1} - \frac{\overline{\beta_1} - \underline{\beta_1}}{T}t, \cdots, \overline{\beta_N} - \frac{\overline{\beta_N} - \underline{\beta_N}}{T}t\right), \\ &\qquad t \in [0, T], \end{aligned} \tag{37}$$

$$\begin{aligned} \mathbf{y}_{\text{LD}}(t) &= \left(\overline{\gamma_1} - \frac{\overline{\gamma_1} - \underline{\gamma_1}}{T}t, \cdots, \overline{\gamma_N} - \frac{\overline{\gamma_N} - \underline{\gamma_N}}{T}t\right), \\ &\qquad t \in [0, T]. \end{aligned} \tag{38}$$

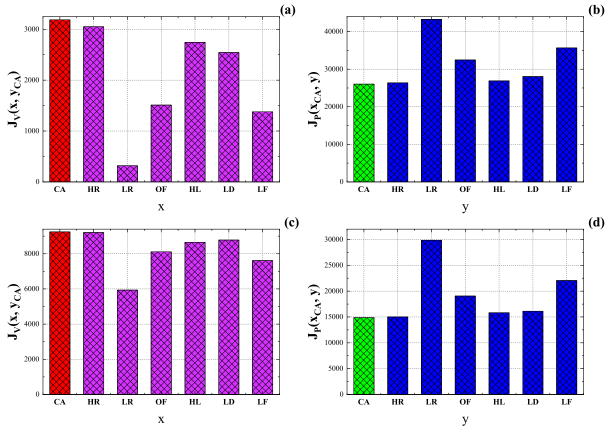

FIGURE 8. The comparison results in Experiment 1.

The sixth and last virus (resp. patch) injection strategy is to achieve a virus (resp. patch) injection rate of each node that is linearly increasing with the probability of the node being susceptible (resp. unpatched). We refer to the virus (resp. patch) injection strategy as the *linear-feedback (LF) virus (resp. patch) injection strategy*, denoted $\mathbf{x}_{\text{LF}}$ (resp. $\mathbf{y}_{\text{LF}}$). Formally,

$$\begin{aligned} \mathbf{x}_{\text{LF}}(t) &= \left(\underline{\beta_1} + (\overline{\beta_1} - \underline{\beta_1})S_1(t), \cdots, \underline{\beta_N} + (\overline{\beta_N} - \underline{\beta_N})S_N(t)\right), \\ &\qquad t \in [0, T], \\ \mathbf{y}_{\text{LF}}(t) &= \Big(\underline{\gamma_1} + (\overline{\gamma_1} - \underline{\gamma_1})(1 - P_1(t)), \cdots, \\ &\qquad \underline{\gamma_N} + (\overline{\gamma_N} - \underline{\gamma_N})(1 - P_N(t))\Big), \quad t \in [0, T]. \end{aligned} \tag{39}$$

B. COMPARATIVE EXPERIMENTS

Now, let us evaluate the performance of the candidate strategy-pair through a comparison with the proposed heuristic virus and patch injection strategies. Let

$$\begin{aligned} A &= \{\mathbf{x}_{\text{CA}}, \mathbf{x}_{\text{HR}}, \mathbf{x}_{\text{LR}}, \mathbf{x}_{\text{OF}}, \mathbf{x}_{\text{HL}}, \mathbf{x}_{\text{LD}}, \mathbf{x}_{\text{LF}}\}, \\ B &= \{\mathbf{y}_{\text{CA}}, \mathbf{y}_{\text{HR}}, \mathbf{y}_{\text{LR}}, \mathbf{y}_{\text{OF}}, \mathbf{y}_{\text{HL}}, \mathbf{y}_{\text{LD}}, \mathbf{y}_{\text{LF}}\}. \end{aligned}$$

Experiment 1: Consider the pair of patch injection games with $G = G_{SW}$, $\mathbf{v} = (1, \cdots, 1)$, $T = 10$, $\beta_P = 0.2$, $\gamma_P = 0.1$, $\delta = 0.1$, $\underline{\beta_i} = 0.1$, $\overline{\beta_i} = 0.4$, $\underline{\gamma_i} = 0.1$, $\overline{\gamma_i} = 0.4$, $\mathbf{E}(0) = (0.1, \cdots, 0.1)$,

(a) $\phi_i(\beta) = \sqrt{\beta}$, $\psi_i(\gamma) = \sqrt{\gamma}$, $1 \le i \le N$; *or*
(b) $\phi_i(\beta) = \beta^2$, $\psi_i(\gamma) = \gamma^2$, $1 \le i \le N$.

For the two games, $J_V(\mathbf{x}, \mathbf{y}_{CA})$ $(\mathbf{x} \in A)$ *and* $J_P(\mathbf{x}_{CA}, \mathbf{y})$ $(\mathbf{y} \in B)$ *are plotted in Fig. 8(a)-(b) and Fig. 8(c)-(d), respectively. It is seen that* $(\mathbf{x}_{CA}, \mathbf{y}_{CA})$ *is the best in terms of Nash equilibrium, provided* $(\mathbf{x}, \mathbf{y}) \in A \times B$.

Experiment 2: For the two patch injection games with the same parameters as those in Experiment 1 except $G = G_{SF}$, $J_V(\mathbf{x}, \mathbf{y}_{CA})$ $(\mathbf{x} \in A)$ *and* $J_P(\mathbf{x}_{CA}, \mathbf{y})$ $(\mathbf{y} \in B)$ *are given in Fig. 9(a)-(b) and Fig. 9(c)-(d), respectively. Again,* $(\mathbf{x}_{CA}, \mathbf{y}_{CA})$ *is the best in terms of Nash equilibrium, provided* $(\mathbf{x}, \mathbf{y}) \in A \times B$.

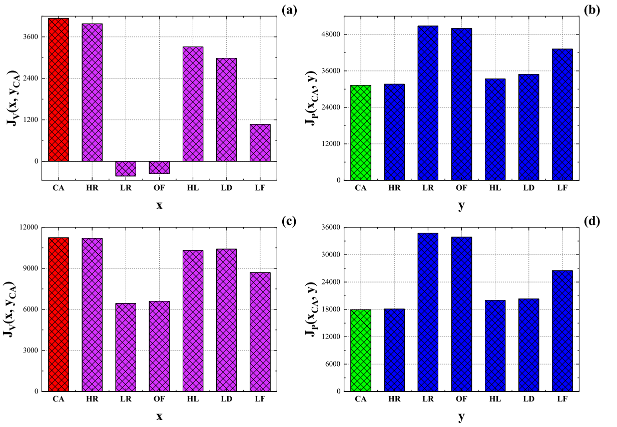

FIGURE 9. The comparison results in Experiment 2.

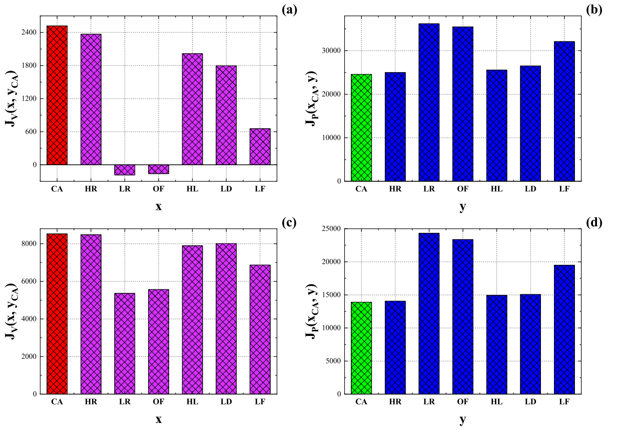

FIGURE 10. The comparison results in Experiment 3.

Experiment 3: For the two patch injection games with the same parameters as those in Experiment 1 except $G = G_{FN}$, $J_V(\mathbf{x}, \mathbf{y}_{CA})$ ($\mathbf{x} \in A$) and $J_P(\mathbf{x}_{CA}, \mathbf{y})$ ($\mathbf{y} \in B$) are exhibited in Fig. 10(a)-(b) and Fig. 10(c)-(d), respectively. Also, $(\mathbf{x}_{CA}, \mathbf{y}_{CA})$ is the best in terms of Nash equilibrium, provided $(\mathbf{x}, \mathbf{y}) \in A \times B$.

We conclude from the above experiments that the strategy-pair $(\mathbf{x}_{\mathrm{CA}}, \mathbf{y}_{\mathrm{CA}})$ is the best in terms of Nash equilibrium, provided $(\mathbf{x}, \mathbf{y}) \in A \times B$. Further, we speculate that $(\mathbf{x}_{\mathrm{CA}}, \mathbf{y}_{\mathrm{CA}})$ is a Nash equilibrium of the patch injection game.

Based on the above discussions, we find that the candidate patch injection strategy is likely to be superior to most heuristic patch injection strategies in terms of Nash equilibrium. On the other hand, the candidate patch injection strategy is easily implementable, because it has a relatively simple structure. For instance, when all the conditions in Theorem 4 are met, the patch injection strategy of the corresponding node goes through a single jump from the highest allowable injection rate to the lowest allowable injection rate. Therefore, we recommend the candidate patch injection strategy to the network administrator.

One remarkable advantage of adopting the recommended patch injection strategy is that no matter what virus injection strategy the attacker uses, the impact of the virus attack can be controlled satisfactorily in the sense of Nash equilibrium solution concept.

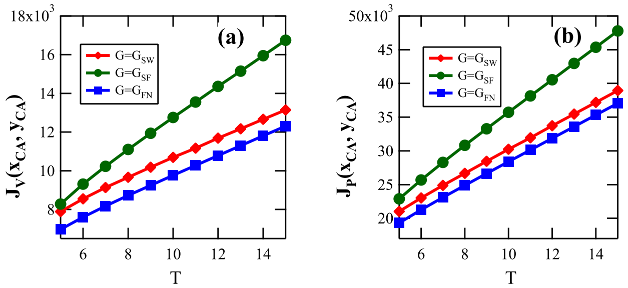

FIGURE 11. The effects of T on $J_V(\mathbf{x}_{CA}, \mathbf{y}_{CA})$ and $J_P(\mathbf{x}_{CA}, \mathbf{y}_{CA})$ in Experiment 4.

In practice, the network administrator may divide the whole time horizon into a number of small time intervals. At the initial time point of each interval, he may collect and analyze recent virus reports to decide on the current expected state of the network. Then, he may apply the recommended patch injection strategy to the interval. Therefore, although the patch injection game per se is open-loop and hence lacks flexibility, the administrator is capable of managing the network in a closed-loop manner, further mitigating the negative impact of virus attacks.

VI. FURTHER DISCUSSIONS

For an patch injection game, we refer to the attacker's benefit and the attack's impact associated with the candidate strategy-pair as the *candidate benefit* and the *candidate impact*, respectively. In this section, we examine the effects of some factors on the two quantities through computer experiments.

A. THE EFFECT OF THE ATTACK DURATION

First, we examine the effect of the attack duration T on the two candidate quantities.

Experiment 4: Consider the family of patch injection games with $G \in \{G_{SW}, G_{SF}, G_{FN}\}$, $T \in \{5, 6, \cdots, 15\}$, $\mathbf{v} = (1, \cdots, 1)$, $\beta_P = 0.2$, $\gamma_P = 0.1$, $\delta = 0.15$, $\underline{\beta_i} = 0.1$, $\overline{\beta_i} = 0.4$, $\underline{\gamma_i} = 0.1$, $\overline{\gamma_i} = 0.4$, $\phi_i(\beta) = \beta^2$, $\psi_i(\gamma) = \sqrt{\gamma}$, $1 \leq i \leq N$. Fig. 11 exhibits the effect of T on $J_V(\mathbf{x}_{CA}, \mathbf{y}_{CA})$ and $J_P(\mathbf{x}_{CA}, \mathbf{y}_{CA})$.

It is concluded from this experiment that the attacker's candidate benefit and the attack's candidate impact are both increasing with the attack duration. In practice, the network administrator should take measures to reduce the attack duration to mitigate its negative impact and potential consequence.

B. THE EFFECT OF THE COMMON VALUE

Second, suppose all the nodes in the network share a common value, and let us inspect the effect of the common value on the two candidate quantities.

Experiment 5: Consider the family of patch injection games with the same parameters as those in Experiment 4

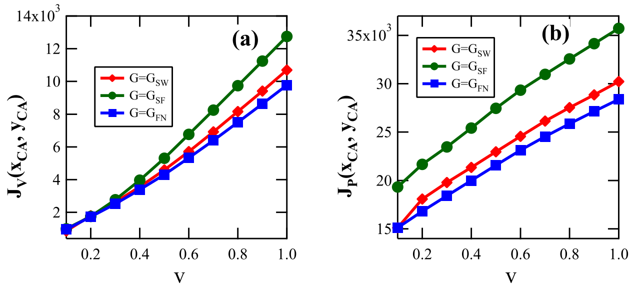

FIGURE 12. The effects of v on $J_V(\mathbf{x}_{CA}, \mathbf{y}_{CA})$ and $J_P(\mathbf{x}_{CA}, \mathbf{y}_{CA})$ in Experiment 5.

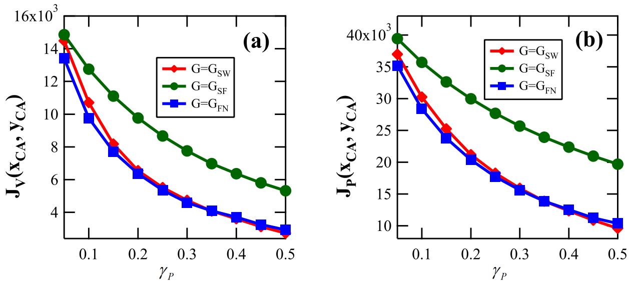

FIGURE 14. The effect of γ_P on $J_V(\mathbf{x}_{CA}, \mathbf{y}_{CA})$ and $J_P(\mathbf{x}_{CA}, \mathbf{y}_{CA})$ in Experiment 7.

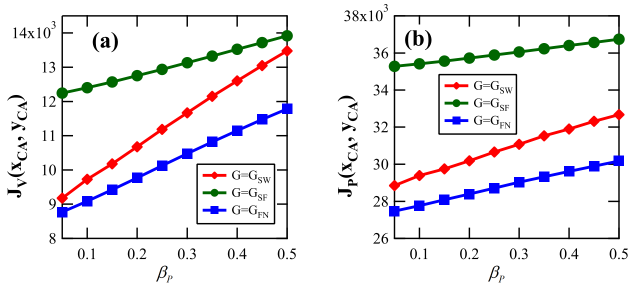

FIGURE 13. The effect of β_P on $J_V(\mathbf{x}_{CA}, \mathbf{y}_{CA})$ and $J_P(\mathbf{x}_{CA}, \mathbf{y}_{CA})$ in Experiment 6.

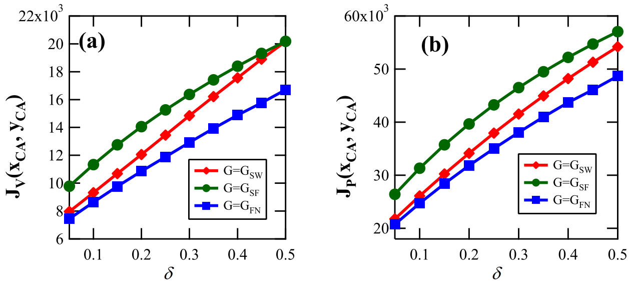

FIGURE 15. The effect of δ on $J_V(\mathbf{x}_{CA}, \mathbf{y}_{CA})$ and $J_P(\mathbf{x}_{CA}, \mathbf{y}_{CA})$ in Experiment 8.

expect $T = 10$ and $v_i = v \in \{0.1, 0.2, \cdots, 1\}$, $1 \leq i \leq N$. Fig. 12 shows the effect of v on $J_V(\mathbf{x}_{CA}, \mathbf{y}_{CA})$ and $J_P(\mathbf{x}_{CA}, \mathbf{y}_{CA})$.

From this experiment, we conclude that the attacker's candidate benefit and the attack's candidate impact are both increasing with the common value of all the nodes. Hence, the same virus attack has a greater impact on high-valued networks.

C. THE EFFECT OF THE VIRUS PROPAGATION RATE

Third, let us inspect the effect of the virus propagation rate β_P on the two candidate quantities.

Experiment 6: Consider the family of patch injection games with the same parameters as those in Example 4 except $T = 10$ and $\beta_P \in \{0.05, 0.1, \cdots, 0.5\}$. Fig. 13 show the effect of β_P on $J_V(\mathbf{x}_{CA}, \mathbf{y}_{CA})$, and $J_P(\mathbf{x}_{CA}, \mathbf{y}_{CA})$, respectively.

It is inferred from this experiment that the attacker's candidate benefit and the attack's impact are both increasing with the virus propagation rate. Therefore, virus attackers prefer to enhance the virus propagation rate to enhance their benefits.

D. THE EFFECT OF THE PATCH FORWARDING RATE

Next, we examine the effect of the patch propagation rate γ_P on the two candidate quantities.

Experiment 7: Consider the family of patch injection games with the same parameters as those in Example 4 except $T = 10$ and $\gamma_P \in \{0.05, 0.1, \cdots, 0.5\}$. Fig. 14 shows the effect of γ_P on $J_V(\mathbf{x}_{CA}, \mathbf{y}_{CA})$ and $J_P(\mathbf{x}_{CA}, \mathbf{y}_{CA})$.

It is concluded from this experiment that the attacker's benefit and the attack's impact are both decreasing with the patch forwarding rate. In practice, new patches should be forwarded as fast as possible to reduce the impact of virus attacks.

E. THE EFFECT OF THE PATCH FAILURE RATE

Finally, let us examine the effect of the patch failure rate δ on the two candidate quantities.

Experiment 8: Consider the family of patch injection games with the same parameters as those in Experiment 4 except $T = 10$ and $\delta \in \{0.05, 0.1, \cdots, 0.5\}$. Fig. 15 shows the effect of δ on $J_V(\mathbf{x}_{CA}, \mathbf{y}_{CA})$ and $J_P(\mathbf{x}_{CA}, \mathbf{y}_{CA})$.

From this experiment, we infer that the attacker's benefit and the attack's impact are both increasing with the patch failure rate. In reality, we should develop new patches with longer period of validity.

VII. CONCLUDING REMARKS

This paper has addressed the issue of developing a patch injection strategy to minimize the impact of virus attacks. We have modeled the patch injection problem as a differential game in which the objective is to seek a Nash equilibrium. We have derived a candidate for the Nash equilibrium of the proposed game and have shown that the candidate is better in term of the Nash equilibrium solution concept. Therefore, we have recommended the patch injection strategy in the candidate.

There are some relevant research topics that are worth further investigation. First, the proposed patch injection strategy should be implemented in practice. Second, in this paper it is assumed that virus propagation and patch forwarding are both spontaneous processes. In the actual situation, the attacker is likely to get control of the virus propagation process to enhance his benefit, whereas the network administrator might control the patch forwarding process to reduce the impact of the virus attack. In this situation, we have to develop a patch injection-forwarding strategy to mitigate the impact of the attack, and this problem may be modeled as a more complicated differential game. Third, with the proliferation of mobile adhoc networks, the patch injection problem should be modified to adapt to the time-varying network situation [51], [52]. Last, the methodology developed in this work could be applied to other areas of cybersecurity such as rumor control [53], [54], intrusion detection [55], proactive cyber defense [56], [57], and privacy protection [58].

APPENDIX A
PROOF OF LEMMA 1

It follows from the model (4) that

$$\lim_{t\to 0^+}\frac{dP_i(t)}{dt}=\gamma_i^I(0)\geq \underline{\gamma_i}>0,\quad 1\leq i\leq N. \tag{40}$$

In view of the continuity of $\mathbf{P}(t)$, there exists $t_0\in(0,T]$ such that $0<P_i(t)<1$ for all i and $0<t\in(0,t_0]$. We show that

$$0<P_i(t)<1,\quad 0<t\leq T,\ 1\leq i\leq N. \tag{41}$$

On the contrary, suppose there exist i^* and $t^*\in(t_0,T]$ such that (a) either $P_{i^*}(t^*)=0$ or $P_{i^*}(t^*)=1$, and (b)

$$0<P_i(t)<1,\quad 0<t<t^*,\ 1\leq i\leq N. \tag{42}$$

If $P_{i^*}(t^*)=0$, then

$$\lim_{t\to t^{*-}}\frac{dP_{i^*}(t)}{dt}=\gamma_{i^*}^I(t^{*-})+\gamma_P\sum_{j=1}^N a_{ji^*}P_j(t^*)>0. \tag{43}$$

This implies that there exists $t_1\in[0,t^*)$ such that $P_{i^*}(t_1)<0$, contradicting Eqs. (42). Hence, $P_{i^*}(t^*)\neq 0$. If $P_{i^*}(t^*)=1$, then

$$\lim_{t\to t^{*-}}\frac{dP_{i^*}(t)}{dt}=-\delta<0. \tag{44}$$

This implies that there exists $t_2\in[0,t^*)$ such that $P_{i^*}(t_2)>1$, again contradicting Eqs. (42). Hence, $P_{i^*}(t^*)\neq 1$. Therefore, Eqs. (41) hold. On this basis and by an analogous argument, we can show that $I_i(t)>0$, $0<I_i(t)+P_i(t)<1$, $0<t\leq T$, $1\leq i\leq N$. The proof is complete.

APPENDIX B
PROOF OF THEOREM 1

According to the Pontryagin Maximum/Minimum Principle [16], there exist λ and μ such that for $1\leq i\leq N$, $0\leq t\leq T$, we have

$$\begin{cases}\dfrac{d\lambda_i^I(t)}{dt}=-\dfrac{\partial H_V(\mathbf{E}(t),\mathbf{x}(t),\mathbf{y}(t),\lambda(t))}{\partial I_i},\\ \dfrac{d\lambda_i^P(t)}{dt}=-\dfrac{\partial H_V(\mathbf{E}(t),\mathbf{x}(t),\mathbf{y}(t),\lambda(t))}{\partial P_i},\\ \dfrac{d\mu_i^I(t)}{dt}=-\dfrac{\partial H_P(\mathbf{E}(t),\mathbf{x}(t),\mathbf{y}(t),\mu(t))}{\partial I_i},\\ \dfrac{d\mu_i^P(t)}{dt}=-\dfrac{\partial H_P(\mathbf{E}(t),\mathbf{x}(t),\mathbf{y}(t),\mu(t))}{\partial P_i}.\end{cases} \tag{45}$$

Thus, Eqs. (19) follow by direct calculations. As the terminal cost is unspecified and the final state is free, we have the transversality condition $\lambda(T)=\mu(T)=\mathbf{0}$. Moreover, for $0\leq t\leq T$, we have

$$\begin{aligned}\mathbf{x}(t)&\in\arg\max_{\widetilde{\mathbf{x}}\in\prod_{i=1}^N[\underline{\beta_i},\overline{\beta_i}]}H_V(\mathbf{E}(t),\widetilde{\mathbf{x}},\mathbf{y}(t),\lambda(t)),\\ \mathbf{y}(t)&\in\arg\min_{\widetilde{\mathbf{y}}\in\prod_{i=1}^N[\underline{\gamma_i},\overline{\gamma_i}]}H_P(\mathbf{E}(t),\mathbf{x}(t),\widetilde{\mathbf{y}},\mu(t)).\end{aligned} \tag{46}$$

Eqs. (20)-(21) follow by direct calculations.

APPENDIX C
PROOF OF LEMMA 2

We prove only the first claim, because the remaining two claims can be shown analogously.

By the first N equations of the system (19) and $\lambda_I(T)=0$, we get

$$\lim_{t\to T^-}\frac{d\lambda_i^I(t)}{dt}=-v_i-\phi_i(\beta_i^I(T^-))<0,\quad 1\leq i\leq N. \tag{47}$$

As λ_i^I is continuous, there exists $t_0\in[0,T)$ such that $\lambda_i^I(t)>0$ for all i and $t\in(t_0,T)$. On the contrary, suppose there exist i^* and $t^*\in[0,t_0]$ such that (a) $\lambda_{i^*}^I(t^*)=0$, (b) $\lambda_{i^*}^I(t)>0$ for $t\in(t^*,T)$, and (c) $\lambda_i^I(t)\geq 0$ for all $i\neq i^*$ and $t\in(t^*,T)$. On one hand, (a) and (b) imply $\lim_{t\to t^{*+}}\frac{d\lambda_{i^*}^I(t)}{dt}\geq 0$. On the other hand, (c) and the continuity of λ_I imply that $\lambda_i^I(t^*)\geq 0$ for all i. Thus,

$$\begin{aligned}\lim_{t\to t^{*+}}\frac{d\lambda_{i^*}^I(t)}{dt}&=-v_{i^*}-\phi_i(\beta_{i^*}^I(t^{*+}))\\ &\quad-\beta^P\sum_{j=1}^N a_{i^*j}\lambda_j^I(t^*)\left[1-I_j(t^*)-P_j(t^*)\right]<0.\end{aligned} \tag{48}$$

A contradiction occurs. Therefore, the claim holds.

APPENDIX D
PROOF OF THEOREM 2

Look at Eqs. (20)-(21). As $\phi_i(\beta)$ is concave, $f_i(\beta;t)$ is convex. So, $f_i(\beta;t)$ attains the maximum at either $\underline{\beta_i}$ or $\overline{\beta_i}$. By comparing $f_i(\underline{\beta_i};t)$ and $f_i(\overline{\beta_i};t)$, we deduce Eq. (25).

Now, suppose Eq. (26) holds. Observe that $\lambda_i^I(T)=0<\theta_i$. We distinguish between two possibilities.

Case 1: $\lambda_i^I(t) < \theta_i$ for $t \in [0, T)$. Then $\beta_i^I(t) = \underline{\beta_i}$ for all $t \in [0, T]$. Claim (a) holds.

Case 2: There exists $t^{'} \in [0, T)$ such that $\lambda_i^I(t^{'}) \geq \theta_i$. Let

$$t_i = \sup\{t \in [0, T) : \lambda_i(t) \geq \theta_i\}. \tag{49}$$

Then $\lambda_i^I(t) < \theta_i$ for $t \in (t_i, T]$, which implies $\beta_i^I(t) = \underline{\beta_i}$ for $t \in (t_i, T]$. As λ_i^I is continuous, we have $\lambda_i^I(t_i) = \theta_i$. If $t_i = 0$, claim (b) already holds. Now, assume $t_i > 0$. By Eqs. (19), Lemma 2 and Eq. (26), we have

$$\frac{d\lambda_i^I(t_i)}{dt} \leq -v_i - \phi_i(\underline{\beta_i}) + \theta_i\left[\overline{\beta_i} + \overline{\gamma_i} + \max\{\beta_P, \gamma_P\}d_i^-\right] < 0. \tag{50}$$

So, there exists $\varepsilon > 0$ such that $\lambda_i^I(t) > \theta_i$ for $t \in (t_i - \varepsilon, t_i)$. Next, we show that $\lambda_i^I(t) > \theta_i$ for $t \in [0, t_i)$. On the contrary, suppose there exists $t_i^{'} < t_i$ such that $\lambda_i^I(t_i^{'}) = \theta_i$ and

$$\lambda_i^I(t) > \theta_i, \quad t_i^{'} < t < t_i. \tag{51}$$

Again by Eqs. (19), Lemma 2 and Eq. (26), we get $\frac{d\lambda_i^I(t_i^{'})}{dt} < 0$. Thus, there exists $t_i^{''} \in (t_i^{'}, t_i)$ such that $\lambda_i^I(t_i^{''}) < \theta_i$. This contradicts Eq. (51). Hence, $\lambda_i^I(t) > \theta_i$ for $t \in [0, t_i)$. This implies $\beta_i^I(t) = \overline{\beta_i}$ for all $t \in [0, t_i)$. Claim (b) holds.

APPENDIX E
PROOF OF THEOREM 3

Look at Eqs. (20)-(21). As $\phi_i(\beta)$ is strictly convex, $f_i(\beta; t)$ is strictly concave. We distinguish among three possibilities.

Case 1: $f_i(\beta; t)$ is strictly decreasing, which is equivalent to $\lambda_i^I(t) < \phi_i^{'}(\underline{\beta_i})$. Then $\beta_i^I(t) = \underline{\beta_i}$.

Case 2: $f_i(\beta; t)$ is strictly increasing, which is equivalent to $\lambda_i^I(t) > \phi_i^{'}(\underline{\beta_i})$. Then $\beta_i^I(t) = \overline{\beta_i}$.

Case 3: f_i is first increasing then decreasing. Then $\frac{df_i(\beta_i^I(t);t)}{d\beta} = 0$, which implies $\beta_i^I(t) = \left[\phi_i^{'}\right]^{-1}(\lambda_i^I(t))$.

Combining the above discussions, we get Eq. (27).

Now, suppose Eq. (28) holds. Observe that $\lambda_i^I(T) = 0 < \phi_i^{'}(\underline{\beta_i})$. We distinguish among three possibilities.

Case 1: $\lambda_i^I(t) < \phi_i^{'}(\underline{\beta_i})$ for $t \in [0, T)$. Then $\beta_i^I(t) = \underline{\beta_i}$ for $t \in [0, T]$. Claim (a) holds.

Case 2: There exists $t' \in [0, T)$ such that $\lambda_i^I(t^{'}) \geq \phi_i^{'}(\underline{\beta_i})$, but $\lambda_i^I(t) \leq \phi_i^{'}(\overline{\beta_i})$ for $t \in [0, T)$. It follows by Eqs. (19), Lemma 2 and Eq. (28) that for $t \in [0, T)$,

$$\frac{d\lambda_i^I(t)}{dt} \leq -v_i - \phi_i(\underline{\beta_i}) + \phi_i^{'}(\overline{\beta_i})\left[\overline{\beta_i} + \overline{\gamma_i} + \max\{\beta_P, \gamma_P\}d_i^-\right] < 0. \tag{52}$$

So, λ_i^I is strictly decreasing. As λ_i^I is continuous, there exists $t_i \in [0, T)$ such that $\lambda_i^I(t_i) = \phi_i^{'}(\underline{\beta_i})$. Hence, $\lambda_i^I(t) < \phi_i^{'}(\underline{\beta_i})$ for $t \in (t_i, T)$, and $\lambda_i^I(t) > \phi_i^{'}(\underline{\beta_i})$ for $t \in [0, t_i)$. This implies that $\beta_i^I(t) = \underline{\beta_i}$ for $t \in (t_i, T]$, and $\beta_i^I(t) = \left[\phi_i^{'}\right]^{-1}(\lambda_i^I(t))$ is strictly decreasing in $[0, t_i)$. Claim (b) holds.

Case 3: There exists $t' \in [0, T)$ such that $\lambda_i^I(t^{'}) > \phi_i^{'}(\overline{\beta_i})$. Then there exist $t^{''}, t^{'''} \in [0, T)$ such that $\lambda_i^I(t_i^{''}) = \phi_i^{'}(\overline{\beta_i})$, $\lambda_i^I(t_i^{'''}) = \phi_i^{'}(\underline{\beta_i})$. Let

$$t_i^{(1)} = \sup\{t \in [0, T) : \lambda_i^I(t) \geq \phi_i^{'}(\overline{\beta_i})\}, \tag{53}$$

$$t_i^{(2)} = \sup\{t \in [0, T) : \lambda_i^I(t) \geq \phi_i^{'}(\underline{\beta_i})\}. \tag{54}$$

Then $0 < t_i^{(1)} < t_i^{(2)} < T$, $\lambda_i^I(t) < \phi_i^{'}(\overline{\beta_i})$ for $t \in (t_i^{(1)}, T]$, $\lambda_i^I(t) < \phi_i^{'}(\underline{\beta_i})$ for $t \in (t_i^{(2)}, T]$, $\lambda_i^I(t_i^{(1)}) = \phi_i^{'}(\overline{\beta_i})$, and $\lambda_i^I(t_i^{(2)}) = \phi_i^{'}(\underline{\beta_i})$. Similarly to the argument for Claim (b), we get that $\beta_i^I(t) = \underline{\beta_i}$ for $t \in (t_i^{(2)}, T]$, and $\beta_i^I(t) = \left[\phi_i^{'}\right]^{-1}(\lambda_i^I(t))$ is strictly decreasing in $[t_i^{(1)}, t_i^{(2)})$. By Eqs. (19), Lemma 2 and Eq. (28), we have

$$\frac{d\lambda_i^I(t_i^{(1)})}{dt} \leq -v_i - \phi_i(\underline{\beta_i}) + \phi_i^{'}(\overline{\beta_i})\left[\overline{\beta_i} + \overline{\gamma_i} + \max\{\beta_P, \gamma_P\}d_i^-\right] < 0. \tag{55}$$

Thus, there exists $\varepsilon > 0$ such that $\lambda_i^I(t) > \phi_i^{'}(\overline{\beta_i})$ for $t \in (t_i^{(1)} - \varepsilon, t_i^{(1)})$. We show that $\lambda_i^I(t) > \phi_i^{'}(\overline{\beta_i})$ for $t \in [0, t_i^{(1)})$. On the contrary, suppose there exists $t_i^{(3)} < t_i^{(1)}$ such that $\lambda_i^I(t_i^{(3)}) = \phi_i^{'}(\overline{\beta_i})$ and

$$\lambda_i^I(t) > \phi_i^{'}(\overline{\beta_i}), \quad t_i^{(3)} < t < t_i^{(1)}. \tag{56}$$

Again by Eqs. (19), Lemma 2 and Eq. (28), we get $\frac{d\lambda_i(t_i^{(3)})}{dt} < 0$. So, there exists $t_i^{(4)} \in (t_i^{(3)}, t_i^{(1)})$ such that $\lambda_i^I(t_i^{(4)}) < \phi_i^{'}(\overline{\beta_i})$. This contradicts Eq. (56). Thus, $\lambda_i^I(t) > \phi_i^{'}(\overline{\beta_i})$ for $t \in [0, t_i^{(1)})$. This implies $\beta_i(t) = \overline{\beta_i}$ for $t \in [0, t_i^{(1)})$. Claim (c) holds.

ACKNOWLEDGMENTS

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

REFERENCES

[1] B. A. Forouzan and F. Mosharraf, *Computer Networking: A Top-Down Approach*. New York, NY, USA: McGraw-Hill, 2012.

[2] A. L. Young and M. Yung, "Cryptovirology: The birth, neglect, and explosion of ransomware," *Commun. ACM*, vol. 60, no. 7, pp. 24–26, 2017.

[3] P. O'Kane, S. Sezer, and D. Carlin, "The evolution of ransomware," *IET Netw.*, vol. 7, no. 5, pp. 321–327, May 2018, doi: 10.1049/iet-net.2017.0207.

[4] J. Aycock, *Computer Viruses and Malware*. New York, NY, USA: Springer-Verlag, 2006.

[5] E. M. Rudd, A. Rozsa, M. Günther, and T. E. Boult, "A survey of stealth malware attacks, mitigation measures, and steps toward autonomous open world solutions," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1145–1172, 2nd Quart., 2017.

[6] P. Szor, *The Art of Computer Virus Research and Defense*. Reading, MA, USA: Addison-Wesley, 2005.

[7] M. Vojnovic and A. Ganesh, "On the race of worms, alerts, and patches," *IEEE/ACM Trans. Netw.*, vol. 16, no. 5, pp. 1066–1079, Oct. 2008.

[8] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 4, pp. 438–457, 2002.

[9] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Decision support approaches for cyber security investment," *Decis. Support Syst.*, vol. 86, pp. 13–23, Jun. 2016.

[10] A. Fielder, S. König, E. Panaousis, S. Schauer, and S. Rass, "Risk assessment uncertainties in cybersecurity investments," *Games*, vol. 9, no. 2, p. 34, 2018.

[11] T. Başar and G. J. Olsder, *Dynamic Noncooperative Game Theory*, 2nd ed. Philadelphia, PA, USA: SIAM, 1999.

[12] T. Alpcan and T. Başar, *Network Security: A Decision and Game-Theoretic Approach*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[13] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Comput. Surv.*, vol. 45, no. 3, 2013, Art. no. 25.

[14] A. Sanjab and W. Saad, "Data injection attacks on smart grids with multiple adversaries: A game-theoretic perspective," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2038–2049, Jul. 2016.

[15] L.-X. Yang, P. Li, X. Yang, and Y. Y. Tang, "A risk management approach to defending against the advanced persistent threat," *IEEE Trans. Dependable Secure Comput.*, to be published, doi: 10.1109/TDSC.2018.2858786.

[16] T. L. Friesz, *Dynamic Optimization and Differential Games*. New York, NY, USA: Springer, 2010.

[17] P. Srikantha and D. Kundur, "A DER attack-mitigation differential game for smart grid security analysis," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1476–1485, May 2016.

[18] Z. Li, H. Xu, and Y. Liu, "A differential game model of intrusion detection system in cloud computing," *Int. J. Distrib. Sensor Netw.*, vol. 13, no. 1, 2017, doi: 10.1177/1550147716687995.

[19] Z. Li and Y. Liu, "A differential game-theoretic model of auditing for data storage in cloud computing," *Int. J. Comput. Sci. Eng.*, vol. 14, no. 4, pp. 341–348, 2017.

[20] Z. Li, X. Zhou, Y. Liu, H. Xu, and L. Miao, "A non-cooperative differential game-based security model in fog computing," *China Commun.*, vol. 14, no. 1, pp. 180–189, 2017.

[21] X. An, F. Lin, S. Xu, L. Miao, and C. Gong, "A novel differential game model-based intrusion response strategy in fog computing," *Secur. Commun. Netw.*, vol. 2018, Aug. 2018, Art. no. 1821804.

[22] N. Abuzainab and W. Saad. (Jan. 2018). "A multiclass mean-field game for thwarting misinformation spread in the Internet of Battlefield Things (IoBT)." [Online]. Available: https://arxiv.org/abs/1802.06887

[23] J. O. Kephart and S. R. White, "Directed-graph epidemiological models of computer viruses," in *Proc. IEEE Comput. Soc. Symp. Res. Secur. Privacy*, May 1991, pp. 343–359.

[24] J. R. C. Piqueira, A. A. de Vasconcelos, C. E. C. J. Gabriel, and V. O. Araujo, "Dynamic models for computer viruses," *Comput. Secur.*, vol. 27, nos. 7–8, pp. 355–359, 2008.

[25] L. Feng, X. Liao, H. Li, and Q. Han, "Hopf bifurcation analysis of a delayed viral infection model in computer networks," *Math. Comput. Model.*, vol. 56, nos. 7–8, pp. 167–179, 2012.

[26] Y. Yao, L. Guo, H. Guo, G. Yu, F.-X. Gao, and X. Tong, "Pulse quarantine strategy of Internet worm propagation: Modeling and analysis," *Comput. Elect. Eng.*, vol. 38, no. 5, pp. 1047–1061, 2012.

[27] Y. Muroya, Y. Enatsu, and H. Li, "Global stability of a delayed SIRS computer virus propagation model," *Int. J. Comput. Math.*, vol. 91, no. 3, pp. 347–367, 2014.

[28] L.-C. Chen and K. M. Carley, "The impact of countermeasure propagation on the prevalence of computer viruses," *IEEE Trans. Syst. Man, Cybern. B, Cybern.*, vol. 34, no. 2, pp. 823–833, Apr. 2004.

[29] J. Goldenberg, Y. Shavitt, E. Shir, and S. Solomon, "Distributive immunization of networks against viruses using the 'honey-pot' architecture," *Nature Phys.*, vol. 1, pp. 184–188, Dec. 2005.

[30] Q. Zhu, X. Yang, L.-X. Yang, and X. Zhang, "A mixing propagation model of computer viruses and countermeasures," *Nonlinear Dyn.*, vol. 73, no. 3, pp. 1433–1441, 2013.

[31] L.-X. Yang and X. Yang, "The effect of infected external computers on the spread of viruses: A compartment modeling study," *Phys. A, Statist. Mech. Appl.*, vol. 392, no. 24, pp. 6523–6535, 2013.

[32] A. K. Misra, M. Verma, and A. Sharma, "Capturing the interplay between malware and anti-malware in a computer network," *Appl. Math. Comput.*, vol. 229, pp. 340–349, Feb. 2014.

[33] L.-X. Yang and X. Yang, "A novel virus-patch dynamic model," *PLoS ONE*, vol. 10, no. 9, p. e0137858, 2015.

[34] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, 1999.

[35] R. Albert and A. Barabási, "Statistical mechanics of complex networks," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 47–97, Jan. 2002.

[36] R. Pastor-Satorras and A. Vespignani, "Epidemic dynamics in finite size scale-free networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 65, no. 3, p. 035108, 2002.

[37] R. Pastor-Satorras, C. Castellano, P. Van Mieghem, and A. Vespignani, "Epidemic processes in complex networks," *Rev. Mod. Phys.*, vol. 87, no. 3, p. 925, 2015.

[38] S. Rackley, *Wireless Networking Technology: From Principles to Successful Implementation*. Amsterdam, The Netherlands: Elsevier, 2007.

[39] 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.

[40] 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.

[41] S. Xu, W. Lu, and L. Xu, "Push- and pull-based epidemic spreading in networks: Thresholds and deeper insights," *ACM Trans. Auton. Adapt. Syst.*, no. 7, no. 3, 2012, Art. no. 32.

[42] L. 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.

[43] L.-X. Yang, X. Yang, and Y. Y. Tang, "A bi-virus competing spreading model with generic infection rates," *IEEE Trans. Netw. Sci. Eng.*, vol. 5, no. 1, pp. 2–13, Jan./Mar. 2018.

[44] 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.

[45] S. Shen, H. Li, R. Han, A. V. Vasilakos, Y. Wang, and Q. Cao, "Differential game-based strategies for preventing malware propagation in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 11, pp. 1962–1973, Nov. 2014.

[46] R. C. Robinson, *An Introduction to Dynamical Systems: Continuous and Discrete*. London, U.K.: Pearson Education, 2004.

[47] K. Atkinson, W. Han, and D. Stewart, *Numerical Solution of Ordinary Differential Equations*. Hoboken, NJ, USA: Wiley, 2009.

[48] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, pp. 440–442, Jun. 1998.

[49] W. De Nooy, A. Mrvar, and V. Batagelj, *Exploratory Social Network Analysis With Pajek*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[50] J. Leskovec and J. J. Mcauley, "Learning to discover social circles in ego networks," in *Proc. Adv. Neural Inf. Process. Syst.*, 2012, pp. 539–547.

[51] Y. Wang, F. R. Yu, H. Tang, and M. Huang, "A mean field game theoretic approach for security enhancements in mobile ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1616–1627, Mar. 2014.

[52] N. Masuda and P. Holme, *Temporal Network Epidemiology*. Singapore: Springer, 2017.

[53] L.-X. Yang, P. Li, X. Yang, Y. Wu, and Y. Y. Tang, "On the competition of two conflicting messages," *Nonlinear Dyn.*, vol. 91, no. 3, pp. 1853–1869, 2018.

[54] L.-X. Yang, T. Zhang, X. Yang, Y. Wu, and Y. Y. Tang, "Effectiveness analysis of a mixed rumor-quelling strategy," *J. Franklin Inst.*, to be published, doi: 10.1016/j.jfranklin.2018.07.040.

[55] Q. Zhu, R. Boutaba, C. Fung, and T. Başar, "GUIDEX: A game-theoretic incentive-based mechanism for intrusion detection networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 11, pp. 2220–2230, Dec. 2012.

[56] L. X. Yang, P. Li, X. Yang, L. Wen, Y. Wu, and Y. Y. Tang, "Security evaluation of the cyber networks under advanced persistent threats," *IEEE Access*, vol. 5, pp. 20111–20123, 2017.

[57] R. Zheng, W. Lu, and S. Xu, "Preventive and reactive cyber defense dynamics is globally stable," *IEEE Trans. Netw. Sci. Eng.*, vol. 5, no. 2, pp. 156–170, Apr./Jun. 2018.

[58] R. Shokri, G. Theodorakopoulos, and C. Troncoso, "Privacy games along location traces: A game-theoretic framework for optimizing location privacy," *ACM Trans. Privacy Secur.*, vol. 19, no. 4, 2017, Art. no. 11.

LU-XING YANG received the B.Sc. degree from the School of Mathematics and Statistics, Chongqing University, in 2012, and the Ph.D. degree from the College of Computer Science, Chongqing University, in 2015. He visited Imperial College London from 2014 to 2015. He was a Post-Doctoral Researcher at the Delft University of Technology from 2016 to 2017. He is currently a Post-Doctoral Researcher at Deakin University, Australia. He has published over 40 academic papers in peer reviewed international journals. His research interests include epidemic dynamics and cybersecurity.

PENGDENG LI received the B.Sc. degree from the School of Software Engineering, Chongqing University, in 2015, where he is currently pursuing the Ph.D. degree. He has published eight academic papers in peer-reviewed international journals. His research interests include epidemic dynamics and 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 joined Chongqing University in 1987. He visited the University of Reading, U.K., from 1998 to 1999, the Hong Kong Baptist University in 2005, 2007, and 2009, respectively, and the University of Macau in 2016 and 2017, respectively. He is currently a Professor of computer science at Chongqing University. He has published over 150 papers in peer-reviewed international journals, and more than 20 students have received Ph.D. degree under his supervision. His research interests include computer virus spreading, cybersecurity and fault tolerant computing, and applied nonlinear dynamics.

YONG XIANG (SM'12) received the B.E. and M.E. degrees from the University of Electronic Science and Technology of China, China, and the Ph.D. degree from The University of Melbourne, Australia. He is currently a Professor with the School of Information Technology, Deakin University, Australia. He is also the Associate Head of School (Research) and the Director of the Artificial Intelligence and Data Analytics Research Cluster. He has obtained many research grants, including five Discovery and Linkage Grants from the Australian Research Council. He has published two monographs, over 100 refereed journal articles, and numerous conference papers in these areas. He is the co-inventor of two U.S. patents and some of his research results have been commercialized. His current research interests include information security and privacy, signal and image processing, data analytics and machine intelligence, and Internet of Things. He is the Associate Editor of the IEEE Signal Processing Letters and the IEEE Access. He has been invited to give keynote speeches and chair committees in a number of international conferences.

WANLEI ZHOU (SM'91) received the B.Eng. and M.Eng. degrees from the Harbin Institute of Technology, Harbin, China, in 1982 and 1984, respectively, the Ph.D. degree from The Australian National University, Canberra, Australia, in 1991, all in computer science and engineering, and the D.Sc. degree (a higher Doctorate degree) from Deakin University in 2002. He is currently the Head of the School of Software, University of Technology Sydney. His research interests include security and privacy, bioinformatics, and e-learning. He has received over 10 ARC grants in the last 10 years and has published over 400 papers in refereed international journals and refereed international conferences proceedings, including many articles in IEEE transactions and journals. He has also chaired many international conferences, including TrustCom, ISPA, IUCC, CSS, ICA3PP, EUC, NSS, HPCC, and PRDC, and has been invited to deliver keynote address in a number of international conferences, including SKG, NSS, PDCAT, NSS, EUC, ICWL, CIT, ISPA, and ICA3PP.