Hindawi
Complexity
Volume 2021, Article ID 6624612, 9 pages
https://doi.org/10.1155/2021/6624612

Research Article

Virus-Information Coevolution Spreading Dynamics on Multiplex Networks

Jian Wang,[1,2,3] **Xiaolin Qin**,[2] **and Hongying Fang**[4]

[1]*School of Computer Science and Technology, University of Chinese Academy of Sciences, Beijing 100049, China*
[2]*Chengdu Institute of Computer Applications, Chinese Academy of Sciences, Chengdu 610041, China*
[3]*College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China*
[4]*College of Mathematics and Statistics, Chongqing Jiaotong University, Chongqing 400074, China*

Correspondence should be addressed to Hongying Fang; 284199018@qq.com

Received 10 December 2020; Revised 22 December 2020; Accepted 10 February 2021; Published 5 March 2021

Academic Editor: Ning Cai

Virus and information spreading dynamics widely exist in complex systems. However, systematic study still lacks for the interacting spreading dynamics between the two types of dynamics. This paper proposes a mathematical model on multiplex networks, which considers the heterogeneous susceptibility and infectivity in two subnetworks. By using a heterogeneous mean-field theory, we studied the dynamic process and outbreak threshold of the system. Through extensive numerical simulations on artificial networks, we find that the virus's spreading dynamics can be suppressed by increasing the information spreading probability, decreasing the protection power, or decreasing the susceptibility and infectivity.

1. Introduction

Coevolution spreading dynamics, ranging from cyberspace security to epidemic contagions, widely exist in the natural systems, in which there are at least two spreading dynamics evolving and interacting simultaneously [1, 2]. For instance, the virus's information is always spreading on the social network when a computer virus spreads on the Internet. The users whose computers are not infected by the virus will install antivirus software and patches to protect their computers from being infected by the virus [3–6]. In this way, computer viruses can be prevented from spreading widely. Another example is the spreading of the epidemic in society. When a global pandemic was spreading, various kinds of information about the pandemic, such as protecting healthy individuals from infection, spreading on social networks will suppress the pandemic [7–9].

Researchers from the field of computer science and network science have developed some successful mathematical models to model such coevolution spreading dynamics. The state of the art in this field is reviewed in a recent paper by Wang et al. [1]. Historically, Newman [10] studied two viruses spreading on the same computer network in succession, where the two viruses follow the susceptible-infected-recovered model, and the second virus can only infect the remaining susceptible nodes. Using a bond percolation theory, he revealed that a global outbreak of the second virus is possible only if the susceptible nodes form a large cluster of connections and the outbreak threshold of the second virus is much higher than the threshold of the first. Newman and Ferrario [11] further discussed a different situation, i.e., the second virus can only spread on those infected nodes by the first virus. They found that the second virus's outbreak size can be suppressed by decreasing the spreading probability of the first virus. In reality, the spreading dynamics are always simultaneous. Karrer and Newman [12] proposed a model to include this factor and studied the phase transition by using a competing percolation theory.

The two spreading dynamics always evolve on different networks; that is to say, we should use multiplex or multilayer networks to describe the network topology of the coevolution spreading [13–18]. Previous studies have revealed that the topology of multilayer networks markedly affect the dynamics, such as cascading failures [19–21], virus spreading [22, 23], controllability [24], and synchronization [25–27]. For virus-information spreading on multiplex networks, Granell and her colleagues [8] used an unaware-aware-unaware-susceptible-infected-susceptible (UAU-SIS) model. They revealed a metacritical critical point, above which the global virus will break out by using a generalized Markovian approach. Based on the research framework in Reference [8], researchers studied the global information [8], network topology [28, 29], and different interacting mechanisms [30, 31] on the virus spreading. Wang et al. revealed the asymmetric interaction between the virus and information spreading dynamics. They used a susceptible-informed-recovered-susceptible-infected-recovered-vaccination (SIR-SIRV) model. They found that the information can suppress the virus spreading greatly, especially when there is a positive correlation between layers.

Many real-world data analyses proved that the spreading dynamics on the network are heterogeneous. There are three aspects. On the one hand, the network topology is heterogeneous, e.g., heterogeneous degree distribution. Scholars revealed that heterogeneous degree distribution could decrease the virus's outbreak threshold spreading [32–34]. An important result is that Pastor-Satorras and Vespignani [32] used a heterogeneous mean-field theory to describe the computer virus spreading on the Internet and revealed that the existence of some hubs may make the outbreak threshold vanish. On the other hand, infectivity and susceptibility are heterogeneous since different computers have distinct circumstances. Miller [35] revealed that the global virus is more likely to break out for homogeneous infectivity when the average transmissibility is fixed. In addition, he found that the attack rate was highest when the susceptibility was homogeneous and lowest when the variance was maximum. Lastly, the virus and information always transmit through different networks. Generally, the virus spreads on the computer network and the information transmits on the social network. Therefore, the virus-information dynamics spreading on two-layered multiplex networks are more realistic. Previous paragraphs have stated the state-of-the-art progresses for virus-information spreading on multiplex networks. To our best knowledge, systematic study still lacks for the interacting spreading dynamics including the above three aspects. In the paper, we first describe the mathematical model in Section 2. In Section 3, we develop a heterogeneous mean-field theory to describe the spreading dynamics. In Section 4, we perform extensive numerical simulations. Finally, we conclude the paper in Section 5.

2. Model Descriptions

In this section, we propose the virus-information coevolution spreading model on computer-social network M. We first introduce the computer-social network and then present the virus-information spreading model.

2.1. Computer-Social Network. We denote the two subnetworks as L_1 and L_2, respectively. The computer virus spreads on subnetwork L_1, and the information spreads on subnetwork L_2. In subnetwork L_1 (L_2), nodes represent the computers (users), and the edges stand for the relationships among computers (users). To build the two-layered complex networks, we use the following steps: (i) assigning the subnetwork sizes $N_1 = N_2 = N$; (ii) building subnetworks L_1 and L_2 by using the uncorrelated configuration model [36] (the degree distributions of subnetworks L_1 and L_2 are $P_1(k_1)$ and $P_2(k_2)$, respectively); and (iii) randomly matching nodes in two subnetworks. Specifically, we build an interlayer connection e for node i_1 and i_2, which means that the user i_2 uses computer i_1. By using the above methods, there are node inter- and intradegree correlations. As shown in Figure 1, we illustrate the computer-social network.

Mathematically, the computer-social network M can be represented by a adjacency matrix $U = \begin{pmatrix} A^1 & A^{12} \\ A^{21} & A^2 \end{pmatrix}$, where A^1 and A^2, respectively, stand for the adjacency matrixes of subnetworks L_1 and L_2. An element $A^x_{ij} = 1$ of subnetwork $x \in \{1, 2\}$ means that nodes i_x and j_x are connected. The matrixes A^{12} and A^{21} are the adjacency matrixes of interlayer network, where $A^{12}_{i_1 i_2} = 1$ means that node i_1 uses computer i_2. Note that $A^{12}_{i_1 i_2} = A^{21}_{i_2 i_1}$ for any values of i_1 and i_2. The average degrees of the two subnetworks can be denoted as $\langle k_1 \rangle = \sum_{i,j} A^1_{ij} = \sum_{k_1} k_1 P_1(k_1)$ and $\langle k_2 \rangle = \sum_{i,j} A^2_{ij} = \sum_{k_2} k\ _2 P_2(k_2)$, respectively.

2.2. Virus-Information Spreading Model. We here adopt a susceptible-infected-recovered (SIR) model to describe the virus spreading on subnetwork L_1. A node in the susceptible state means that it does not get infected by the computer virus. An infected node represents that it is infected by the virus and can transmit it to one of its neighbors. A node in the recovered state means that it has recovered and does not change its state.

For the information spread on subnetwork L_2, we consider using the irreversible susceptible-informed-recovered (SIR) model [37]. A susceptible node means that it does not obtain information about the virus. An informed node indicates that it knows information about the virus and is willing to share it with its neighbors. A node in the recovered state means that it loses interest in the information and will not transmit it to its neighbors. In this paper, we denote the virus-information coevolution spreading as a SIR-SIR model.

The virus-information coevolution spreading dynamic evolves as follows. Initially, we randomly select a node i_1 in subnetwork L_1, that is to say, the computer virus infects node i_1. The corresponding node i_2, i.e., the user of computer i_1, is also set to be the infected state, since the user can release the information of his infection to his neighbors. At every time step t, each infected node v_1 in subnetwork L_1 tries to transmit the computer virus to one of its neighbors u_1, since every infected node usually communicates with one neighbor at a short time interval. In reality, the infection transmission depends on the "source" and "target" nodes [35]. That is to say, the infectivity and susceptibility of the system are distinct for different nodes. To include this factor,

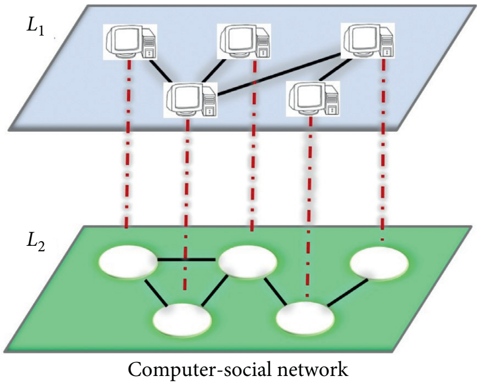


FIGURE 1: Illustration of computer-social networks. Subnetwork L_1 represents the computer network, and subnetwork L_2 stands for the social network.

we assume that nodes' infectivity and susceptibility depend on the degree of nodes. More specifically, the infectivity of node v_1 with degree k_1 is

$$\omega_{k_1}^1 = 1 - (1 - \alpha_1)^{k_1}, \tag{1}$$

where α_1 is the unit infectivity for a node with degree 1. Similarly, the susceptibility of node u_1 with degree k_1' is

$$\varpi_{k_1'}^1 = 1 - (1 - \alpha_1')^{k_{1'}}, \tag{2}$$

where α_1' is the unit susceptibility for node with degree 1. Varying the values of α_1 and α_1', we get different infectivities and susceptibilities of the system. If node u_1 is susceptible, two different situations should be considered. (i) If the user u_2 of computer u_1 is in the susceptible state, the computer u_1 infects the virus with probability λ_1. Meanwhile, node u_2 obtains the information. Otherwise, u_2 is in the infected or recovered state, and nothing happens. (ii) If the user u_2 has already obtained the information before, the computer u_1 is infected by the virus with probability $q\lambda_1$, where $0 \leq q \leq 1$. We here use the parameter q to describe the degree of protection when a user knows the virus's spreading. The smaller the value of q, the stronger the protection against computer viruses. Every infected node recovers with probability γ_1.

The information about the virus spread on the subnetwork L_2 is as follows. At each time step t, every informed node v_2 transmits the information to one of its neighbor u_2 in subnetwork L_2 depending on the infectivity of v_2 and the susceptibility of u_2. The infectivity of v_2 with degree k_2 is

$$\omega_{k_2}^2 = 1 - (1 - \alpha_2)^{k_2}, \tag{3}$$

where α_2 is the unit infectivity. The susceptibility of u_2 with degree k_2' is

$$\varpi_{k_2'}^2 = 1 - (1 - \alpha_2')^{k_{2'}}, \tag{4}$$

where α_2' is the unit susceptibility. The infection probability is λ_2. Finally, every informed node loses interest in transmitting the information with probability γ_2. The spreading ends when there are no nodes in the infected or informed state. In Table 1, we present the definitions of parameters and abbreviations.

3. Heterogeneous Mean-Field Theory

In this section, we develop a heterogeneous mean-field approach to describe the evolution of the virus-information spreading dynamics. In theory, we assume that nodes with same degrees have the same infection probability in statistical [32, 33, 38, 39]. In other words, the probability of nodes with the degree k is the same as each other.

We use the following parameters to describe the coevolution process. Denote $s_{k_1}^1(t)$, $\rho_{k_1}^1(t)$, and $r_{k_1}^1(t)$ as the probability that a node with degree k_1 is in the susceptible, infected, and recovered states at time t in subnetwork L_1, respectively. Similarly, we denote $s_{k_2}^2(t)$, $\rho_{k_2}^2(t)$, and $r_{k_2}^2(t)$ as the probability of node with degree k_2 in the susceptible, informed, and recovered states at time t in subnetwork L_2, respectively. Considering the degree distributions of subnetworks L_1 and L_2, we know the fraction of nodes in each state. For instance, the fraction of nodes in the susceptible state at time t is $S_1(t) = \sum_{k_1} P_1(k_1) s_{k_1}^1(t)$. In the final state, i.e., $t \longrightarrow \infty$, the fraction of nodes in the susceptible state is $S_1(\infty) \equiv S_1$.

Now we derive the expressions of the probability of nodes in each state. We know that $s_{k_1}^1(t)$ decreases with time t when nodes are infected by the virus. A susceptible computer u_1 with degree k_1 infected by the virus has two situations. (1) The corresponding node (i.e., the user) u_2 of node u_1 is in the susceptible state. In this situation, the infection transmitted to node u_1 should fulfill two necessary conditions.

(i) An infected neighbor v_1 of node u_1 contacts node u_1. In uncorrelated complex networks, the probability of node u_1 connecting to an infected neighbor v_1 with degree is k_1' is $((k_1' - 1)/\sum_{k_1} k_1 P_1(k_1))$, where k_1' is the degree of node v_1. Considering the degree distribution of subnetwork L_1, the average probability that a node connects to an infected neighbor through an edge is

$$\Theta_1(t) = \frac{1}{\langle k_1 \rangle} \sum_{k_1'} \omega_{k_1'}^1 (k_1' - 1) P_1(k_1') \rho_{k_1'}^1(t). \tag{5}$$

(ii) The infection is transmitted successfully with probability λ_1. According to the description of the model, for a node u_1 in the susceptible state, its corresponding node must also be in the susceptible state. However, the opposite situation does not always exist. Combining conditions (i) and (ii), we know situation (1) happens with probability $\lambda_1 k_1 \varpi_{k_1}^1 s_{k_1}^1(t) \Theta_1(t)$. Situation (2) indicates that node u_2 of node u_1 is in the informed state. Using a similar discussion with situation (1), we obtain the probability of situation (2) as follows: $q\lambda_1 k_1 \varpi_{k_1}^1 s_{k_1}^1(t) \Theta_1(t) [\sum_{k_2} P_2(k_2) \lambda_2 k_2 \varpi_{k_2}^2 \Theta_2(t)]$, where $\sum_{k_2} P_2(k_2) \lambda_2 k_2 \varpi_{k_2}^2 \Theta_2(t)$ is the probability that the corresponding node u_2 of u_1 is informed by neighbors in subnetwork L_2 at time t. $\Theta_2(t)$ will be defined later. The rate equation of $s_{k_1}^1(t)$ is

Table 1: Definitions of parameters and abbreviations.

Parameter	Definition
N_1	Subnetwork size of computer network L_1
N_2	Subnetwork size of social network L_2
$P_1(k_1)$	Degree distribution of computer network L_1
$P_2(k_2)$	Degree distribution of social network L_2
$\langle k_1\rangle$	Average degree of computer network L_1
$\langle k_2\rangle$	Average degree of social network L_2
$\omega_{k_1}^1$	Infectivity of node v_1 with degree k_1 in subnetwork L_1
$\omega_{k_2}^2$	Infectivity of node v_2 with degree k_2 in subnetwork L_2
$\varpi_{k_1'}^1$	Susceptibility of u_1 with degree k_1' in subnetwork L_1
$\varpi_{k_2'}^2$	Susceptibility of u_2 with degree k_2' in subnetwork L_2
α_1	Unit infectivity in subnetwork L_1
α_2	Unit infectivity in subnetwork L_2
α_1'	Unit susceptibility in subnetwork L_1
α_2'	Unit susceptibility in subnetwork L_2
q	Protection power
λ_1	Computer virus transmission probability
λ_2	Information transmission probability
γ_1	Computer virus recovery probability
γ_2	Information recovery probability
$s_{k_1}^1(t)$	Probability of node with degree k_1 in the susceptible state at time t in subnetwork L_1
$\rho_{k_1}^1(t)$	Probability of node with degree k_1 in the infected state at time t in subnetwork L_1
$r_{k_1}^1(t)$	Probability of node with degree k_1 in the recovered state at time t in subnetwork L_1
$s_{k_2}^2(t)$	Probability of node with degree k_2 in the susceptible state at time t in subnetwork L_2
$\rho_{k_2}^2(t)$	Probability of node with degree k_2 in the infected state at time t in subnetwork L_2
$r_{k_2}^2(t)$	Probability of node with degree k_2 in the recovered state at time t in subnetwork L_2
$\Theta_1(t)$	Average probability that a node connects to an infected neighbor through an edge in subnetwork L_1
$\Theta_2(t)$	Average probability that a node connects to an informed neighbor through an edge in subnetwork L_2

$$\frac{\mathrm{d}s_{k_1}^1(t)}{\mathrm{d}t} = -\lambda_1 k_1 \varpi_{k_1}^1 \Theta_1(t)\left[s_{k_1}^1(t) + q\sum_{k_2} P_2(k_2)\lambda_2 k_2 \varpi_{k_2}^2 \Theta_2(t)\right]. \tag{6}$$

The evolution of $\rho_{k_1}^1(t)$ is

$$\begin{aligned}\frac{\mathrm{d}\rho_{k_1}^1(t)}{\mathrm{d}t} =& \lambda_1 k_1 \varpi_{k_1}^1 \Theta_1(t)\left[s_{k_1}^1(t) + q\sum_{k_2} P_2(k_2)\lambda_2 k_2 \varpi_{k_2}^2 \Theta_2(t)\right] \\ & - \gamma_1\rho_{k_1}^1(t),\end{aligned} \tag{7}$$

where $\gamma_1\rho_{k_1}^1(t)$ is the fraction of nodes recovered at time t. Finally, the evolution of $r_{k_1}^1(t)$ is

$$\frac{\mathrm{d}r_{k_1}^1(t)}{\mathrm{d}t} = \gamma_1\rho_{k_1}^1(t). \tag{8}$$

According to equations (6)–(8), we obtain the evolution of computer virus spreading on subnetwork L_1.

Now, we study the rate equations of the information about the virus spreading on social network L_2. There are two different situations for the reduction of $s_{k_2}^2(t)$. For the first situation, the susceptible node u_2 with degree k_2 is infected by its informed neighbor v_2. The infection probability is $\lambda_2 k_2 \varpi_{k_2}^2 s_{k_2}^2(t)\Theta_2(t)$, where $\Theta_2(t)$ denotes the probability of an edge connecting to an informed neighbor in subnetwork L_2. The expression of $\Theta_2(t)$ can be expressed as

$$\Theta_2(t) = \frac{1}{\langle k_2\rangle}\sum_{k_2'} \omega_{k_2'}^2 (k_2'-1) P_2(k_2')\rho_{k_2'}^2(t). \tag{9}$$

The second situation of node u_2 obtaining the information is that the corresponding node u_1 of u_2 is infected by the computer virus through an edge of u_1 with probability $\lambda_1 k_1 \varpi_{k_1}^1 s_{k_2}^2(t)\Theta_1(t)$. Since u_2 and u_1 are randomly coupled, the averaged infection probability of u_1 is $\lambda_1\langle k_1\rangle\langle\varpi_{k_1}^1\rangle s_{k_2}^2(t)\Theta_1(t)$, where $\langle\varpi_{k_1}^1\rangle = \sum_{k_1} P_1(k_1)\varpi_{k_1}^1$. Combining the two situations, we obtain the rate equation of $s^2k_2(t)$ as

$$\frac{\mathrm{d}s_{k_2}^2(t)}{\mathrm{d}t} = -s_{k_2}^2(t)\left[\lambda_2 k_2 \varpi_{k_2}^2 \Theta_2(t) + \lambda_1\langle k_1\rangle\langle\varpi_{k_1}^1\rangle\Theta_1(t)\right]. \tag{10}$$

With the similar discussion about the virus spreading on subnetwork L_1, we have

$$\frac{\mathrm{d}\rho^2_{k_2}(t)}{\mathrm{d}t} = s^2_{k_2}(t)\left[\lambda_2 k_2 \varpi^2_{k_2}\Theta_2(t) + \lambda_1 \langle k_1\rangle\langle\varpi^1_{k_1}\rangle\Theta_1(t)\right] - \gamma_2 \rho^1_{k_2}(t), \tag{11}$$

$$\frac{\mathrm{d}r^2_{k_2}(t)}{\mathrm{d}t} = \gamma_2 \rho^2_{k_2}(t). \tag{12}$$

With the above equations, we know the fraction of nodes in each state at subnetworks L_1 and L_2.

In the following, we study the global outbreak conditions of the computer virus and information spreading. For global information outbreak condition, we can linearize equations (7) and (11) around the initial conditions, i.e., $s^1_{k_1} \approx 1$, $s^2_{k_2} \approx 1$. We know that $s^1_{k_1} = 1$, $s^2_{k_2} = 1$, $\rho^1_{k_1} = 0$, and $\rho^2_{k_2} = 0$ are trivial solutions. Denote a vector $\overrightarrow{\rho} = (\overrightarrow{\rho_1}, \overrightarrow{\rho_2})^T$, where $\overrightarrow{\rho_1} = (\rho^1_{k_1=1}, \dots, \rho^1_{k_{1,\max}})$, $\overrightarrow{\rho_2} = \rho^2_{k_2=1}, \dots, \rho^2_{k_{2,\max}}$, and $k^1_{1,\max}$ and $k^2_{2,\max}$ represent the maximal degrees of subnetworks L_1 and L_2, respectively. We perform a Taylor expansion for equations (7) and (11) at $s^1_{k_1} = 1$, $s^2_{k_2} = 1$, $\rho^1_{k_1} = 0$, and $\rho^2_{k_2} = 0$ and neglect the high order of $\overrightarrow{\rho}$. We have

$$\frac{\mathrm{d}\overrightarrow{\rho}}{\mathrm{d}t} = \mathbf{J}\overrightarrow{\rho}, \tag{13}$$

where $\mathbf{J}$ is the Jacobian matrix. The expression of $\mathbf{J}$ is

$$\mathbf{J} = \begin{pmatrix}
\frac{\partial\rho^1_1}{\partial\rho^1_1} & \frac{\partial\rho^1_1}{\partial\rho^1_2} & \cdots & \frac{\partial\rho^1_1}{\partial\rho^1_{1,\max}} & \frac{\partial\rho^1_1}{\partial\rho^2_1} & \frac{\partial\rho^1_1}{\partial\rho^2_2} & \cdots & \frac{\partial\rho^1_1}{\partial\rho^2_{2,\max}} \\
\frac{\partial\rho^1_2}{\partial\rho^1_1} & \frac{\partial\rho^1_2}{\partial\rho^1_2} & \cdots & \frac{\partial\rho^1_2}{\partial\rho^1_{1,\max}} & \frac{\partial\rho^1_2}{\partial\rho^2_1} & \frac{\partial\rho^1_2}{\partial\rho^2_2} & \cdots & \frac{\partial\rho^1_2}{\partial\rho^2_{2,\max}} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\frac{\partial\rho^1_{1,\max}}{\partial\rho^1_1} & \frac{\partial\rho^1_{1,\max}}{\partial\rho^1_2} & \cdots & \frac{\partial\rho^1_{1,\max}}{\partial\rho^1_{1,\max}} & \frac{\partial\rho^1_{1,\max}}{\partial\rho^2_1} & \frac{\partial\rho^1_{1,\max}}{\partial\rho^2_2} & \cdots & \frac{\partial\rho^1_{1,\max}}{\partial\rho^2_{2,\max}} \\
\frac{\partial\rho^2_1}{\partial\rho^1_1} & \frac{\partial\rho^2_1}{\partial\rho^1_2} & \cdots & \frac{\partial\rho^2_1}{\partial\rho^1_{1,\max}} & \frac{\partial\rho^2_1}{\partial\rho^2_1} & \frac{\partial\rho^2_1}{\partial\rho^2_2} & \cdots & \frac{\partial\rho^2_1}{\partial\rho^2_{2,\max}} \\
\frac{\partial\rho^2_2}{\partial\rho^1_1} & \frac{\partial\rho^2_2}{\partial\rho^1_2} & \cdots & \frac{\partial\rho^2_2}{\partial\rho^1_{1,\max}} & \frac{\partial\rho^2_2}{\partial\rho^2_1} & \frac{\partial\rho^2_2}{\partial\rho^2_2} & \cdots & \frac{\partial\rho^2_2}{\partial\rho^2_{2,\max}} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\frac{\partial\rho^2_{1,\max}}{\partial\rho^1_1} & \frac{\partial\rho^2_{1,\max}}{\partial\rho^1_2} & \cdots & \frac{\partial\rho^2_{1,\max}}{\partial\rho^1_{1,\max}} & \frac{\partial\rho^2_{1,\max}}{\partial\rho^2_1} & \frac{\partial\rho^2_{1,\max}}{\partial\rho^2_2} & \cdots & \frac{\partial\rho^2_{1,\max}}{\partial\rho^2_{2,\max}}
\end{pmatrix}. \tag{14}$$

The Jacobian matrix $\mathbf{J}$ can be further expressed as block matrix as

$$\mathbf{J} = \begin{pmatrix} C^1 & D^2 \\ D^1 & C^2 \end{pmatrix}, \tag{15}$$

where dimensions of C^1, C^2, D^1, and D^2 are $k_{1,\max} \times k_{1,\max}$, $k_{2,\max} \times k_{2,\max}$, $k_{2,\max} \times k_{1,\max}$, and $k_{1,\max} \times k_{2,\max}$, respectively. When the global information on subnetwork L_2 breaks out, the largest eigenvalue of $\mathbf{J}$ is larger than zero. The global information outbreak condition is

$$\Lambda_1(\mathbf{J}) = 0, \tag{16}$$

where $\Lambda_1(\mathbf{J})$ is the largest eigenvalue of $\mathbf{J}$. For the virus outbreak condition, we cannot solve it directly. When the network is extensive, we can use the competing percolation theory [40]. That is to say, we can process the information spreading on subnetwork L_2 first and then the virus spreading on subnetwork L_1.

4. Simulation Results

In this section, we perform numerical simulations to study the virus-information spreading dynamics on computer-social network. To build the computer-social network, we use the uncorrelated configuration model [36]. We set the degree distributions of subnetworks L_1 and L_2 as $P_1(k_1) \sim k^{-\chi_1}$ and $P_2(k_2) \sim k^{-\chi_2}$, respectively, where χ_1 and χ_2, respectively, represent the degree exponents. There is no inter- and intralayer degree-degree correlations. In numerical simulations, we set the average degrees of the two subnetworks as $\langle k_1\rangle = \langle k_2\rangle = 8$, the network sizes as $N_1 = N_2 = 10^4$, and the degree exponent as $\chi_1 = \chi_2 = 3.0$. We set $\alpha_1 = \alpha_1'$ and $\alpha_2 = \alpha_2'$. Initially, we randomly select 5 seeds in subnetwork L_1. All results presented in this paper are averaged over at least 2000 times.

We first study the virus and information spreading sizes, respectively, denoted as $R_1 = 1 - S_1$ and $R_2 = 1 - S_2$, versus virus transmission probability λ_1 as shown in Figure 2. We find that R_1 increases with $\alpha_1 = \alpha_2$, i.e., the virus is more likely to spread when the infectivity and susceptibility are large. Specifically, we note that the virus cannot spread for any values of λ_1 when $\alpha_1 = \alpha_2$ are small, e.g., $\alpha_1 = \alpha_2 = 0.0$ and 0.2. When $\alpha_1 = \alpha_2$ are large enough, enlarging their values cannot promote the virus spreading. When comparing the effects of information spreading on virus spreading, i.e., increasing λ_2, the virus spreading can be suppressed, as shown in Figures 2(a)–2(d). That is to say, to contain the virus spreading, we can transmit more information about the virus on the social network. For the information spreading on subnetwork L_2, i.e., the social network, we find that R_2 increases with λ_1, λ_2, and $\alpha_1 = \alpha_2$, since the users have more chances to obtain the information.

In Figure 3, we further investigate the effects of protection power q on the virus-information spreading for different values of $\alpha_1 = \alpha_2$ and λ_2. Generally speaking, we find similar results with that discussed in Figure 2. When the protection power is large, we find that the virus spreading size is relatively smaller, i.e., $R_1(q = 0.8) \geq R_1(q = 0.5)$, since the susceptible nodes are less likely to be infected by neighbors. We also note that R_2 $(q =$

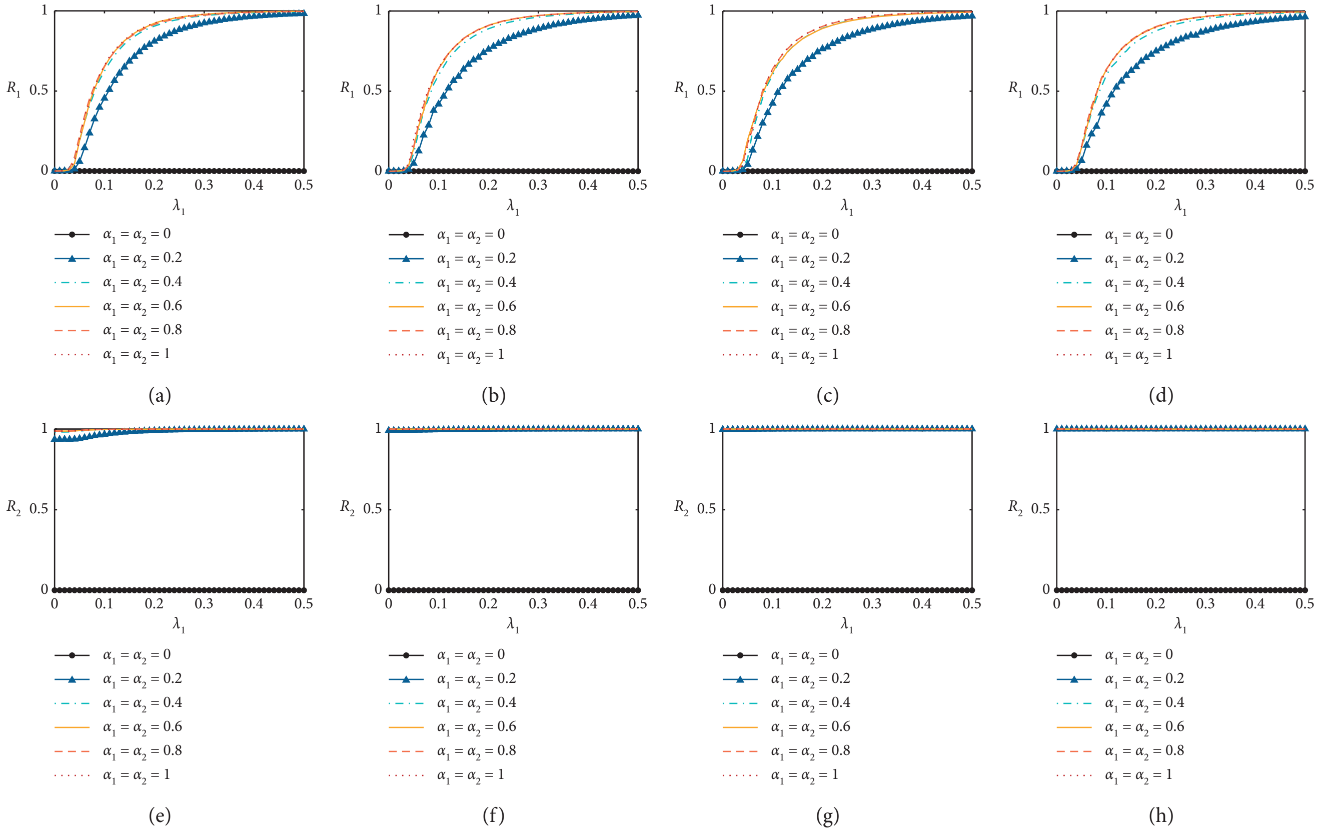


FIGURE 2: Virus spreading size R_1 and information spreading size R_2 versus computer virus transmission probability λ_1 with $q = 0.5$. R_1 versus λ_1 with (a) $\lambda_2 = 0.2$, (b) $\lambda_2 = 0.4$, (c) $\lambda_2 = 0.6$, and (d) $\lambda_2 = 0.8$. R_2 versus λ_1 with (e) $\lambda_2 = 0.2$, (f) $\lambda_2 = 0.4$, (g) $\lambda_2 = 0.6$, and (h) $\lambda_2 = 0.8$. Other parameters are set to be $\gamma_1 = \gamma_2 = 0.2$ and $\lambda_2 = 0.8$.

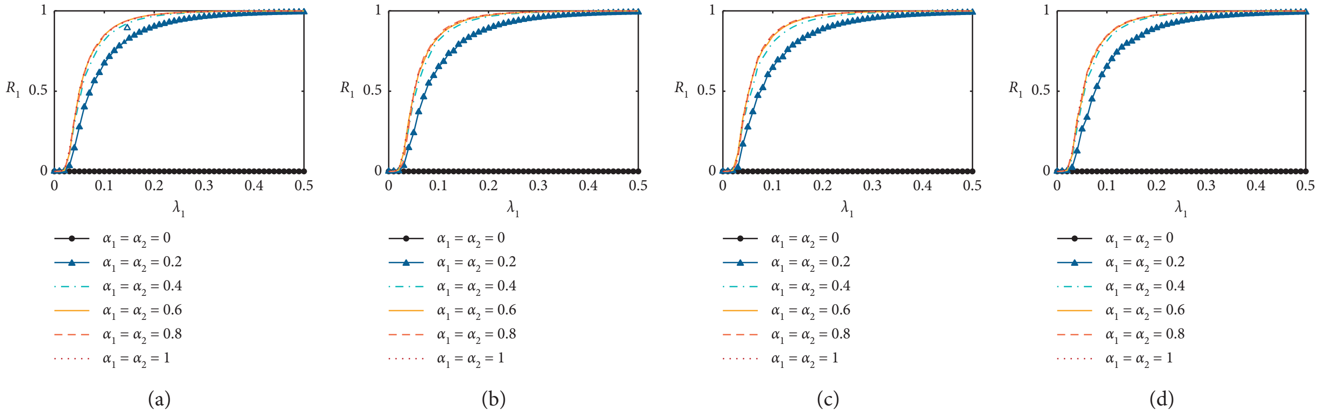
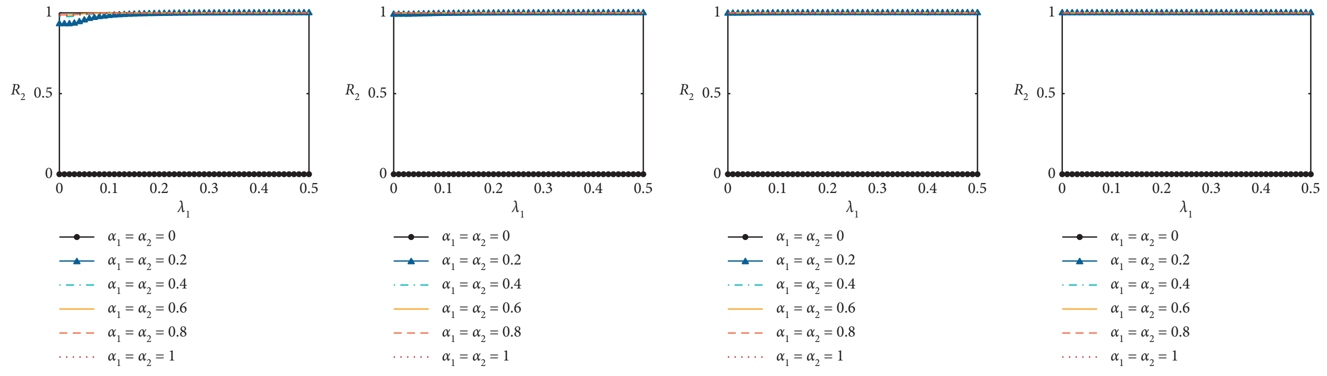
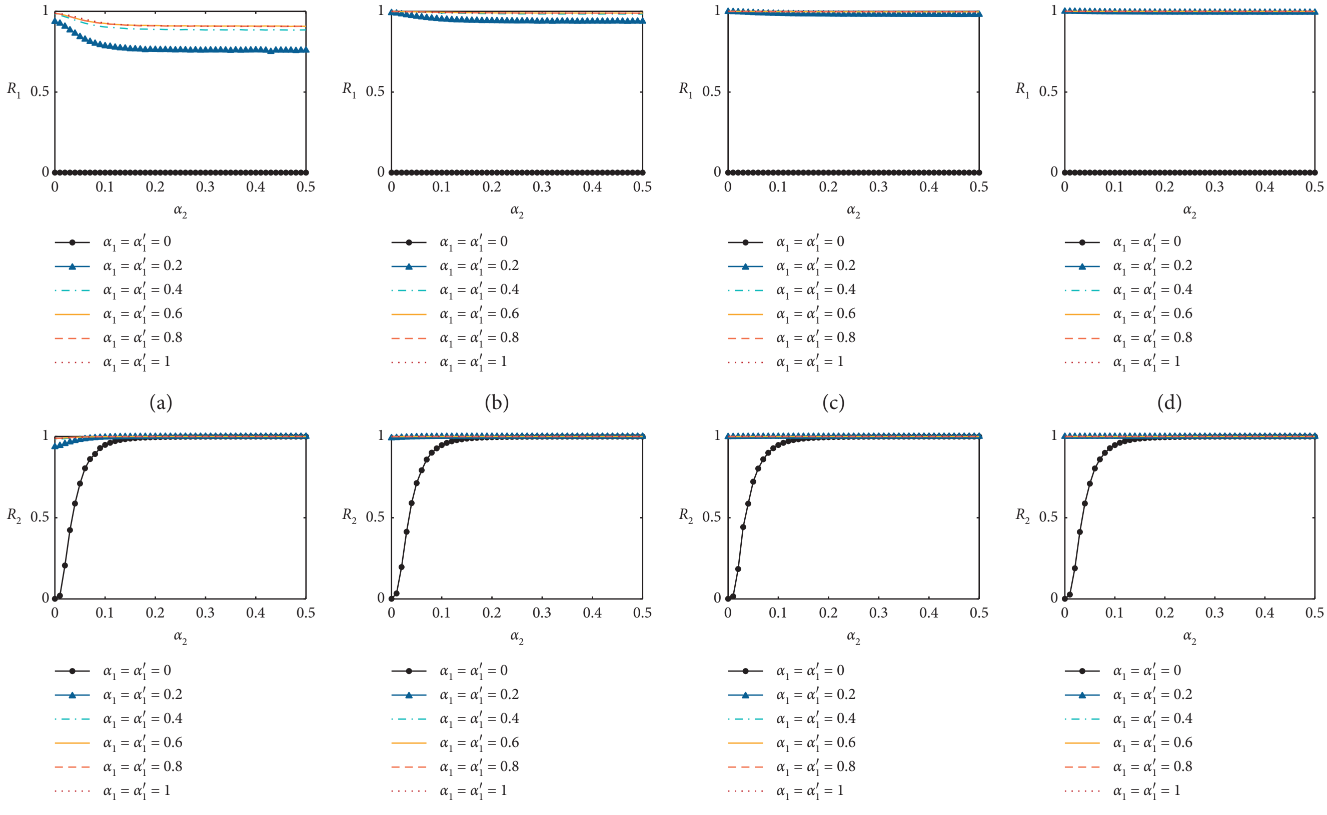


FIGURE 3: Continued.



(e) (f) (g) (h)

FIGURE 3: Virus spreading size R_1 and information spreading size R_2 versus computer virus transmission probability λ_1 with $q = 0.8$. R_1 versus λ_1 with (a) $\lambda_2 = 0.2$, (b) $\lambda_2 = 0.4$, (c) $\lambda_2 = 0.6$, and (d) $\lambda_2 = 0.8$. R_2 versus λ_1 with (e) $\lambda_2 = 0.2$, (f) $\lambda_2 = 0.4$, (g) $\lambda_2 = 0.6$, and (h) $\lambda_2 = 0.8$. Other parameters are set to be $\gamma_1 = \gamma_2 = 0.2$ and $\lambda_2 = 0.8$.



(e) (f) (g) (h)

FIGURE 4: Virus spreading size R_1 and information spreading size R_2 versus computer virus transmission probability λ_1 with $q = 0.5$. R_1 versus α_2 with (a) $\lambda_1 = 0.2$, (b) $\lambda_1 = 0.4$, (c) $\lambda_1 = 0.6$, and (d) $\lambda_1 = 0.8$. R_2 versus α_2 with (e) $\lambda_1 = 0.2$, (f) $\lambda_1 = 0.4$, (g) $\lambda_1 = 0.6$, and (h) $\lambda_1 = 0.8$. Other parameters are set to be $\gamma_1 = \gamma_2 = 0.2$ and $\lambda_2 = 0.5$.

$0.8) \geq R_2\,(q = 0.5)$ since the promotion of virus spreading on information spreading is decreased.

In Figure 4, we study the effects of susceptibility and infectivity in detail. We find that R_1 decreases with the increase of susceptibility and infectivity of L_2. That is to say, the virus spreading can be suppressed by increasing the susceptibility and infectivity. We can explain the results as follows. Increasing susceptibility and infectivity, the information will be widely spread on social network (see Figures 4(e)–4(g)), and more susceptible nodes in subnetwork L_1 will take measures to protect themselves from being infected. As a result, R_1 decreases with α_2.

Finally, we studied the virus-information spreading as a function of α_2 when the protection power is lower with $q = 0.8$ in Figure 5. We reveal similar phenomena as shown in Figure 4.

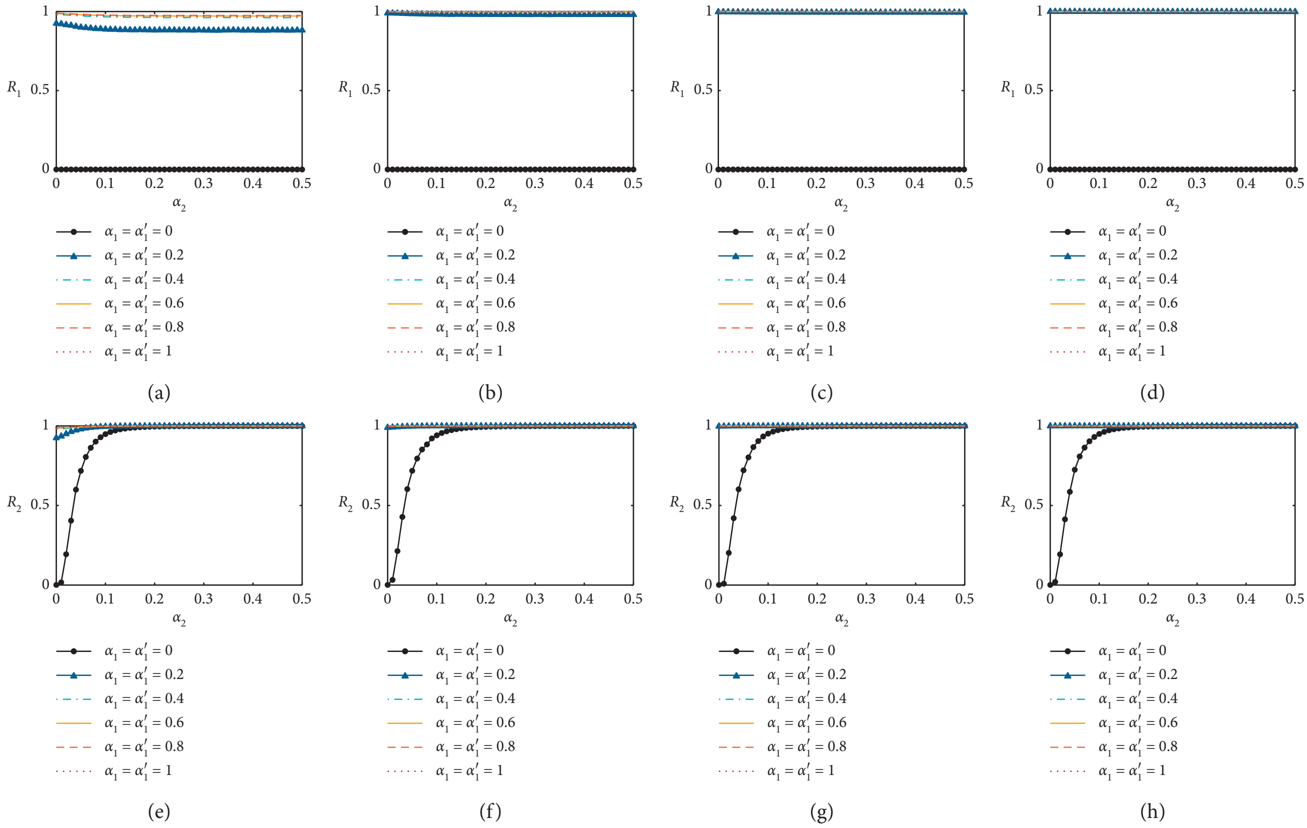


FIGURE 5: Virus spreading size R_1 and information spreading size R_2 versus computer virus transmission probability λ_1 with $q = 0.8$. R_1 versus α_2 with (a) $\lambda_1 = 0.2$, (b) $\lambda_1 = 0.4$, (c) $\lambda_1 = 0.6$, and (d) $\lambda_1 = 0.8$. R_2 versus α_2 with (e) $\lambda_1 = 0.2$, (f) $\lambda_1 = 0.4$, (g) $\lambda_1 = 0.6$, and (h) $\lambda_1 = 0.8$. Other parameters are set to be $\gamma_1 = \gamma_2 = 0.2$ and $\lambda_2 = 0.5$.

We note that $R_1(q = 0.5) \geq R_1(q = 0.8)$ and $R_2(q = 0.5) \geq R_2(q = 0.8)$ since the protection power is decreased.

5. Discussion

In this paper, we studied the virus-information spreading dynamics on computer-social multiplex networks. We first proposed a mathematical model to describe the co-evolution spreading dynamics. In this model, we assumed that nodes' susceptibility and infectivity are heterogeneous and positively correlated with the node's degree. To describe the spreading dynamics, we adopt a generalized heterogeneous mean-field approach. Using extensive numerical simulations, we revealed that the virus spreading dynamics can be significantly suppressed by promoting the information spreading on the computer network or decreasing the susceptibility and infectivity of nodes. Our results provide some insight into containing the virus spreading.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This study was partially supported by the Sichuan Science and Technology Program (2020YFG0010).

References

[1] W. Wang, Q.-H. Liu, J. Liang, Y. Hu, and T. Zhou, "Co-evolution spreading in complex networks," *Physics Reports*, vol. 820, p. 1, 2019.

[2] S. Lehmann and Y.-Y. Ahn, *Complex Spreading Phenomena in Social Systems*, Springer, Berlin, Germany, 2018.

[3] P. Szor, *The Art of Computer Virus Research and Defense: Art Comp Virus Res Defense _p1*, Pearson Education, London, UK, 2005.

[4] L.-X. Yang, X. Yang, L. Wen, and J. Liu, "A novel computer virus propagation model and its dynamics," *International Journal of Computer Mathematics*, vol. 89, no. 17, p. 2307, 2012.

[5] F. D. Sahneh and C. Scoglio, "Competitive epidemic spreading over arbitrary multilayer networks," *Physical Review E*, vol. 89, Article ID 062817, 2014.

[6] L.-X. Yang, X. Yang, and Y. Y. Tang, "An effective rumor-containing strategy," *IEEE Transactions on Network Science and Engineering*, vol. 5, p. 2, 2017.

[7] C. Granell, S. Gómez, and A. Arenas, "Dynamical interplay between awareness and epidemic spreading in multiplex networks," *Physical Review Letters*, vol. 111, Article ID 128701, 2013.

[8] C. Granell, S. Gómez, and A. Arenas, "Competing spreading processes on multiplex networks: awareness and epidemics," *Physical Review E*, vol. 90, Article ID 012808, 2014.

[9] P. C. Ventura, Y. Moreno, and F. A. Rodrigues, "The role of time scale in the spreading of asymmetrically interacting diseases," 2020, http://arxiv.org/abs/2007.02774.

[10] M. E. Newman, "Threshold effects for two pathogens spreading on a network," *Physical Review Letters*, vol. 95, Article ID 108701, 2005.

[11] M. E. Newman and C. R. Ferrario, "Interacting epidemics and coinfection on contact networks," *PLoS One*, vol. 8, Article ID e71321, 2013.

[12] B. Karrer and M. E. Newman, "Competing epidemics on complex networks," *Physical Review E*, vol. 84, Article ID 036106, 2011.

[13] M. Kivelä, A. Arenas, M. Barthelemy, J. P. Gleeson, Y. Moreno, and M. A. Porter, "Multilayer networks," *Journal of Complex Networks*, vol. 2, no. 3, p. 203, 2014.

[14] M. De Domenico, A. Solé-Ribalta, E. Cozzo et al., "Mathematical formulation of multilayer networks," *Physical Review X*, vol. 3, Article ID 041022, 2013.

[15] M. De Domenico, V. Nicosia, A. Arenas, and V. Latora, "Structural reducibility of multilayer networks," *Nature Communications*, vol. 6, p. 1, 2015.

[16] G. Bianconi, *Multilayer Networks: Structure and Function*, Oxford University Press, Oxford, UK, 2018.

[17] Z. Wang, L. Wang, A. Szolnoki, and M. Perc, "Evolutionary games on multilayer networks: a colloquium," *The European Physical Journal B*, vol. 88, p. 1, 2015.

[18] X. Zhang, S. Boccaletti, S. Guan, and Z. Liu, "Explosive synchronization in adaptive and multilayer networks," *Physical Review Letters*, vol. 114, Article ID 038701, 2015.

[19] J. Gao, S. V. Buldyrev, H. E. Stanley, and S. Havlin, "Networks formed from interdependent networks," *Nature Physics*, vol. 8, no. 1, p. 40, 2012.

[20] D. Zhou, J. Gao, H. E. Stanley, and S. Havlin, "Percolation of partially interdependent scale-free networks," *Physical Review E*, vol. 87, Article ID 052812, 2013.

[21] F. Radicchi and A. Arenas, "Abrupt transition in the structural formation of interconnected networks," *Nature Physics*, vol. 9, no. 11, p. 717, 2013.

[22] S. Gomez, A. Diaz-Guilera, J. Gomez-Gardenes, C. J. Perez-Vicente, Y. Moreno, and A. Arenas, "Diffusion dynamics on multiplex networks," *Physical Review Letters*, vol. 110, Article ID 028701, 2013.

[23] M. Dickison, S. Havlin, and H. E. Stanley, "Epidemics on interconnected networks," *Physical Review E*, vol. 85, Article ID 066109, 2012.

[24] M. Pósfai, J. Gao, S. P. Cornelius, A.-L. Barabási, and R. M. D'Souza, "Controllability of multiplex, multi-timescale networks," *Physical Review E*, vol. 94, Article ID 032316, 2016.

[25] L. V. Gambuzza, M. Frasca, and J. Gómez-Gardeñes, "Intralayer synchronization in multiplex networks," *EPL (Europhysics Letters)*, vol. 110, no. 2, Article ID 20010, 2015.

[26] L. Tang, X. Wu, J. Lü, J.-a. Lu, and R. M. D'Souza, "Master stability functions for complete, intralayer," *Physical Review E*, vol. 99, Article ID 012304, 2019.

[27] S. Jalan, V. Rathore, A. D. Kachhvah, and A. Yadav, "Inhibition-induced explosive synchronization in multiplex networks," *Physical Review E*, vol. 99, Article ID 062305, 2019.

[28] Z. Wang, Q. Guo, S. Sun, and C. Xia, "The impact of awareness diffusion on SIR-like epidemics in multiplex networks," *Applied Mathematics and Computation*, vol. 349, p. 134, 2019.

[29] C. Zheng, C. Xia, Q. Guo, and M. Dehmer, "Interplay between SIR-based disease spreading and awareness diffusion on multiplex networks," *Journal of Parallel and Distributed Computing*, vol. 115, p. 20, 2018.

[30] J.-Q. Kan and H.-F. Zhang, "Effects of awareness diffusion and self-initiated awareness behavior on epidemic spreading-an approach based on multiplex networks," *Communications in Nonlinear Science and Numerical Simulation*, vol. 44, p. 193, 2017.

[31] E. Massaro and F. Bagnoli, "Epidemic spreading and risk perception in multiplex," *Physical Review E*, vol. 90, Article ID 052817, 2014.

[32] R. Pastor-Satorras and A. Vespignani, "Epidemic dynamics and endemic states in complex networks," *Physical Review E*, vol. 63, Article ID 066117, 2001.

[33] R. Pastor-Satorras and A. Vespignani, "Epidemic dynamics in finite size scale-free networks," *Physical Review E*, vol. 65, Article ID 035108, 2002.

[34] R. Pastor-Satorras, C. Castellano, P. Van Mieghem, and A. Vespignani, "Epidemic processes in complex networks," *Reviews of Modern Physics*, vol. 87, no. 3, p. 925, 2015.

[35] J. C. Miller, "Natural visions: the power of images in american environmental reform," *Physical Review E*, vol. 76, Article ID 010101, 2007.

[36] M. Catanzaro, M. Boguñá, and R. Pastor-Satorras, "Diffusion-annihilation processes in complex networks," *Physical Review E*, vol. 71, Article ID 027103, 2005.

[37] Z.-K. Zhang, C. Liu, X.-X. Zhan, X. Lu, C.-X. Zhang, and Y.-C. Zhang, "Dynamics of information diffusion and its applications on complex networks," *Physics Reports*, vol. 651, p. 1, 2016.

[38] W. Wang, M. Tang, H. E. Stanley, and L. A. Braunstein, "Unification of theoretical approaches for epidemic spreading on complex networks," *Reports on Progress in Physics*, vol. 80, Article ID 036603, 2017.

[39] Y. Moreno, R. Pastor-Satorras, and A. Vespignani, "Epidemic outbreaks in complex heterogeneous networks," *The European Physical Journal B*, vol. 26, no. 4, p. 521, 2002.

[40] B. Karrer and M. E. J. Newman, "Random graphs containing arbitrary distributions of subgraphs," *Physical Review E*, vol. 82, Article ID 016101, 2010.