IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received July 25, 2019, accepted August 23, 2019, date of current version October 11, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2941021

Modeling Ransomware Spreading by a Dynamic Node-Level Method

WANPING LIU, Member, IEEE
College of Computer Science and Engineering, Chongqing University of Technology, Chongqing 400054, China
e-mail: lwphe@163.com

This work was supported in part by the National Natural Science Foundation of China under Grant 61603065, in part by the Chongqing Basic Science and Advanced Technology Research Program under Grant cstc2017jcyjAX0277, in part by the Project of Science and Technology Research Program of Chongqing Education Commission of China under Grant KJQN201901101, and in part by the China Scholarship Council under Grant 201908500031.

ABSTRACT Ransomware attacks are becoming increasingly sophisticated, more damaging to victims and more challenging to prevent. In this paper, a dynamic modelling method is used to study the spreading behaviors of ransomware. The dynamic state of each network node is assumed to be statistically dependent of the states of its neighboring nodes. By incorporating the full topology of the propagating network via its adjacent matrix, a novel node-based model is developed which is also suitable over generic connected networks. The dynamics of the model is theoretically analyzed. Especially, the global stability of its trivial equilibrium is theoretically confirmed depending on a sufficient condition including the leading eigenvalue of the adjacent matrix. We also present results from extensive numerical simulations designed for some specific networks, exhibiting different dynamic properties over distinct networks. Consequently, we suggest that ransomware spreading can be availably contained by properly adjusting the network structure so that its largest eigenvalue satisfies the desired requirement.

INDEX TERMS Blackmail virus, cybersecurity, complex networks, stability analysis, nonlinear system.

I. INTRODUCTION

With advancing antimalware technologies, hackers are seeking easy targets through social engineering and are constantly evolving their attacks for maximum efficiency [1]. In recent years, attacks from new types of cyberthreats have caused great damage [2]. One of them is the ransomware which is a type of malicious software that encrypts the victim's data files to make them inaccessible and requires a ransom payment to decrypt them [3]. For example, CryptoLocker caused an estimated 3 million dollars before taking down by authorities and CryptoWall was estimated to have caused over 18 million dollars by June 2015 [4]. The use of ransomware scams has grown internationally starting from 2012. In June 2013, the data released by McAfee showed that the number of ransomware samples collected in that quarter doubled that of the same period of the previous year. Some unprecedented and devastating ransomware families, such as WannaCrypt, Petya/NotPetya and BadRabbit, brought down critical services like hospitals, transportation, and traffic systems by infecting and encrypting files to prevent access. Especially, the botnet Gamarue has infected more than 23 million IP addresses, and the largest ransomware attack by WannaCrypt infects over 0.23 million computers [5]–[7]. Thus, it is necessary to study the propagating mechanisms and laws of ransomware spreading, and make proper strategies on how to strengthen the security of companies, protect against those cyberthreats and combat them [8]–[10].

Ransomware attacks are usually carried out by employing a Trojan that is disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment or a hyperlink. Websites or webpage links are often employed by attackers to conduct phishing attacks or distribute malware. Online services and financial institutions have become popular phishing targets due to their potential for providing illegal access to victims' private information and even bank accounts. Phishing sites that targeted these two categories of objectives accounted for the leading number of active phishing URLs, and also received the largest share of impressions during the first quarter of 2017 [5]. Some works addressing the dynamics of cyber attacks have appeared [11]–[13]. By incorporating the characteristics of web

The associate editor coordinating the review of this manuscript and approving it for publication was Luis Javier Garcia Villalba.

malware spreading, Liu and Zhong [14] developed a differential model to address the spreading behavior of malicious links over networks. These epidemic compartmental models usually have corresponding propagating thresholds and are mostly established by a homogeneous network assumption [15]–[18]. However, with the deep study of complex networks, the specific topology of spreading networks is also incorporated in the study of malware dynamics [19]–[22]. For example, the quenched mean-field approach is employed to model epidemic dynamics over a specifically given network in terms of nodal probabilities. The results show that the epidemic threshold depends on the inverse of the leading eigenvalue of the adjacency matrix of the fixed network. By introducing probability variables to depict each node's specific state, Van Mieghem *et al.* [23] developed a node-based epidemic model by modifying the traditional SIS model, and derived that whether viruses decline toward extinction depends on the maximum eigenvalue of the underlying network. By examining a node-based SIR model, Youssef and Scoglio [24] indicated that the maximum number of infected nodes is closely related to the spectrum of the network. Later, the dynamics of multivirus was studied by proposing a node-level SIR model [25]. These epidemic models indicate that the spectral radius of the spreading network plays a significant role in determining virus dynamics, i.e., heavily affecting whether viruses approach extinction. For more information about this topic [26]–[28]. Generally, node-level epidemic models can accommodate more knowledge of the network topology, thus the propagating network's topological impact on malware spreading can be more deeply revealed by studying such models.

Motivated by the previous models, in this paper, we will address the spreading of ransomware and develop a new node-based model by assuming that the dynamic state of every node is statistically dependent of the states of its nearest neighbors. The dynamic properties of this model are analyzed. Especially, the global stability of the trivial equilibrium is theoretically proved depending on a condition including the spectral properties of the adjacency matrix (specifically, the value of its maximum eigenvalue). Finally, we also present results from extensive numerical simulations designed over general networks such as complete, star-shaped, and generated scale-free networks. Consequently, we conclude that ransomware spreading can be contained by adjusting the network topology so that its largest eigenvalue falls into the desired interval.

II. MODEL DESCRIPTION

The spreading mechanisms of ransomware have some similar characteristics with Trojan horses. When users visit malicious websites accidentally, ransomware spreading like a homepage Trojan will be automatically downloaded by the browser and runs in the background. Additionally, ransomware can also propagate through other ways, such as email attachments, removable storage medium or being bundled with other malware. Once a computer is intruded by a ransomware, it will prevent users from accessing their systems by locking the system's screen or by locking all data files.

We first refer the device nodes that are not yet (or never been) intruded by ramsomware as susceptible nodes. All these nodes are theoretically possible to suffer from the intrusion of ransomware attacks. After being intruded by ransomware, susceptible nodes will become delitescent ones, which indicate that the ransomware stays in the equipment, but do not show attack features yet. Once the ransomware resident in delitescent devices starts to encrypt files and threatens to perpetually block access to victim's data, then we define that delitescent nodes become infected nodes which usually require ransomware payment for decrypting files. In this situation, the screens of a computer or a mobile terminal will usually be locked, victim users have to recover their systems by paying the ransom according to the hacker's request. We assume that the encrypted files will successfully get recovered after the victims defray the payment of ransomware, making the intruded nodes turn to be recovered nodes for a certain period. However, hackers are not benevolent and they aim to gain as much economic benefits as possible, thus we consider that recovered devices may turn back to be susceptible nodes and suffer from the new ransomware attacks again (see Figure 1).

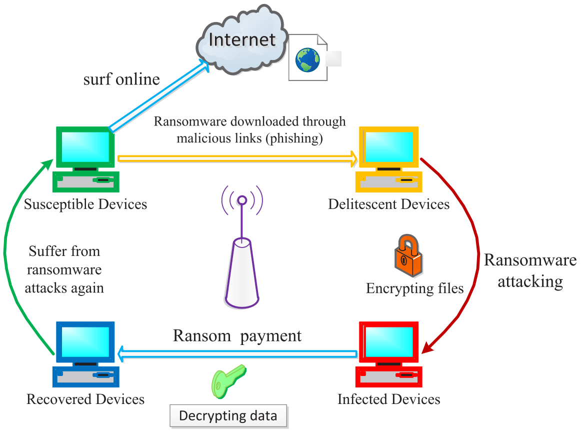


FIGURE 1. Schematic diagram of attack processes of ransomware.

Based on the above discussions, we consider that the state of each node over the network has four possible cases: susceptible (S), delitescent (D), infected (I) and recovered (R). In the sequel, we let $X_i(t) = 0$ (respectively, 1, 2, 3) represent that the i-th node is susceptible (respectively, delitescent, infected, recovered) at time t. Then the state of the whole spreading network at time t can be described by the vector $\boldsymbol{X}(t) = [X_1(t), X_2(t), \ldots, X_N(t)]$, where N is the size of the considered propagating network. The ransomware propagating network can be denoted by a general graph $G = (V, E)$ on N non-isolated nodes which are connected and numbered 1 through N, where nodes represent terminal devices of a network, and edges stand for the links among nodes through which ransomware can proliferate. We also denote by $\boldsymbol{A} = [a_{ij}]_{N\times N}$ the adjacency matrix of the graph G, let

$\{d_k, 1 \leq k \leq N\}$ denote the degree sequence of G, and let $\{\lambda_k, 1 \leq k \leq N\}$ denote the spectrum of the matrix $\boldsymbol{A}$. Let $\lambda_{\max}(\boldsymbol{A})$ denote the greatest eigenvalue of the adjacency matrix $\boldsymbol{A}$, then we can assume that $\lambda_{\max}(\boldsymbol{A}) = \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_N$, since $\boldsymbol{A}$ is real and symmetric.

Next, we will introduce several notations to depict the possibility of a specific node being at a state. That is, let $s_j(t)$ (respectively, $d_j(t)$, $i_j(t)$), $r_j(t)$) denote the probability of the event that the j-th node is susceptible (respectively, delitescent, infected, recovered) at time t, i.e.,

$$\begin{aligned} s_j(t) &= Pr(X_j(t) = 0), \quad d_j(t) = Pr(X_j(t) = 1), \\ i_j(t) &= Pr(X_j(t) = 2), \quad r_j(t) = Pr(X_j(t) = 3). \end{aligned}$$

Note that a susceptible node is infected by a single infected neighbor with the probability of λ per unit time. Then, a susceptible node j gets infected with the average probability of $1 - \prod_k (1 - \lambda i_k(t))$ per unit time, which approximates $\lambda \sum_k a_{jk} i_k(t)$ when the number of infected nodes is small, where $k \in Z_j$, the set of nodes connected to the node j. The following Figure 2 synoptically shows the probability transitions of each node state within per unit time.

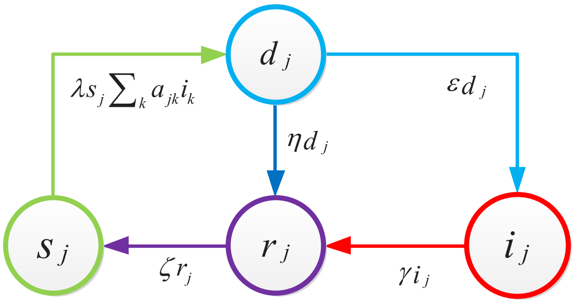


FIGURE 2. Schematic diagram for the probability transitions of states of each node over the network.

Let Δt be a very small time interval, then we get the following equations:

$$\begin{aligned}
&Pr(X_j(t+\Delta t) = 0|X_j(t) = 0) = 1-\lambda\sum_k a_{jk} i_k(t)\Delta t + o(\Delta t),\\
&Pr(X_j(t+\Delta t) = 1|X_j(t) = 0) = \lambda \sum_k a_{jk} i_k(t)\Delta t + o(\Delta t),\\
&Pr(X_j(t+\Delta t) = 2|X_j(t) = 0) = 0,\\
&Pr(X_j(t+\Delta t) = 3|X_j(t) = 0) = 0,\\
&Pr(X_j(t+\Delta t) = 0|X_j(t) = 1) = 0,\\
&Pr(X_j(t+\Delta t) = 1|X_j(t) = 1) = 1 - \varepsilon\Delta t - \eta\Delta t + o(\Delta t)\\
&Pr(X_j(t+\Delta t) = 2|X_j(t) = 1) = \varepsilon\Delta t + o(\Delta t),\\
&Pr(X_j(t+\Delta t) = 3|X_j(t) = 1) = \eta\Delta t + o(\Delta t),\\
&Pr(X_j(t+\Delta t) = 0|X_j(t) = 2) = 0,\\
&Pr(X_j(t+\Delta t) = 1|X_j(t) = 2) = 0,\\
&Pr(X_j(t+\Delta t) = 2|X_j(t) = 2) = 1 - \gamma\Delta t + o(\Delta t),\\
&Pr(X_j(t+\Delta t) = 3|X_j(t) = 2) = \gamma\Delta t + o(\Delta t),\\
&Pr(X_j(t+\Delta t) = 0|X_j(t) = 3) = \zeta\Delta t + o(\Delta t),\\
&Pr(X_j(t+\Delta t) = 1|X_j(t) = 3) = 0,\\
&Pr(X_j(t+\Delta t) = 2|X_j(t) = 3) = 0,\\
&Pr(X_j(t+\Delta t) = 3|X_j(t) = 3) = 1 - \zeta\Delta t + o(\Delta t),
\end{aligned}$$

By the total probability formula, we have the following relations:

$$\begin{aligned}
s_j(t+\Delta t) = \; & s_j(t)\, Pr(X_j(t+\Delta t) = 0|X_j(t) = 0)\\
& + d_j(t)\, Pr(X_j(t+\Delta t) = 0|X_j(t) = 1)\\
& + i_j(t)\, Pr(X_j(t+\Delta t) = 0|X_j(t) = 2)\\
& + r_j(t)\, Pr(X_j(t+\Delta t) = 0|X_j(t) = 3),\\
d_j(t+\Delta t) = \; & s_j(t)\, Pr(X_j(t+\Delta t) = 1|X_j(t) = 0)\\
& + d_j(t)\, Pr(X_j(t+\Delta t) = 1|X_j(t) = 1)\\
& + i_j(t)\, Pr(X_j(t+\Delta t) = 1|X_j(t) = 2)\\
& + r_j(t)\, Pr(X_j(t+\Delta t) = 1|X_j(t) = 3),\\
i_j(t+\Delta t) = \; & s_j(t)\, Pr(X_j(t+\Delta t) = 2|X_j(t) = 0)\\
& + d_j(t)\, Pr(X_j(t+\Delta t) = 2|X_j(t) = 1)\\
& + i_j(t)\, Pr(X_j(t+\Delta t) = 2|X_j(t) = 2)\\
& + r_j(t)\, Pr(X_j(t+\Delta t) = 2|X_j(t) = 3),\\
r_j(t+\Delta t) = \; & s_j(t)\, Pr(X_j(t+\Delta t) = 3|X_j(t) = 0)\\
& + d_j(t)\, Pr(X_j(t+\Delta t) = 3|X_j(t) = 1)\\
& + i_j(t)\, Pr(X_j(t+\Delta t) = 3|X_j(t) = 2)\\
& + r_j(t)\, Pr(X_j(t+\Delta t) = 3|X_j(t) = 3).
\end{aligned}$$

Combining the above equations and letting $\Delta t \to 0$, we get the following $4N$-dimensional differential dynamical system

$$\begin{cases}
\dfrac{ds_j(t)}{dt} = \zeta r_j(t) - \lambda s_j(t) \displaystyle\sum_k a_{jk} i_k(t), & j = 1, \ldots, N,\\
\dfrac{dd_j(t)}{dt} = \lambda s_j(t) \displaystyle\sum_k a_{jk} i_k(t) - (\varepsilon + \eta) d_j(t), & j = 1, \ldots, N,\\
\dfrac{di_j(t)}{dt} = \varepsilon d_j(t) - \gamma i_j(t), & j = 1, \ldots, N,\\
\dfrac{dr_j(t)}{dt} = \eta d_j(t) + \gamma i_j(t) - \zeta r_j(t), & j = 1, \ldots, N.
\end{cases} \tag{1}$$

As $s_j(t) + d_j(t) + i_j(t) + r_j(t) = 1$, this system is equal to the following $3N$-dimensional system

$$\begin{cases}
d_j'(t) = \lambda(1 - d_j(t) - i_j(t) - r_j(t)) \sum_k a_{jk} i_k(t) & \\
\qquad\quad -(\varepsilon + \eta) d_j(t), & j = 1, \ldots, N,\\
i_j'(t) = \varepsilon d_j(t) - \gamma i_j(t), & j = 1, \ldots, N,\\
r_j'(t) = \eta d_j(t) + \gamma i_j(t) - \zeta r_j(t), & j = 1, \ldots, N.
\end{cases} \tag{2}$$

Note that $\sum_k a_{jk} i_k(t) = \vec{\boldsymbol{a}}_j \vec{\boldsymbol{i}}_N$, where $\vec{\boldsymbol{a}}_j$ is the jth row vector of $\boldsymbol{A}$ and $\boldsymbol{i}_N = (i_1, \ldots, i_N)^T$. Next, we refer to system (1) or system (2) as the node-based model for ransomware spreading. Obviously, system (2) always has an equilibrium $\boldsymbol{E}_0 = \boldsymbol{0}$. This trivial equilibrium means that the epidemic ransomware over the network will finally disappear almost surely.

$$
\boldsymbol{B}=\begin{bmatrix}
-(\varepsilon+\eta) & 0 & \cdots & 0 & \lambda a_{11} & \lambda a_{12} & \cdots & \lambda a_{1N} & 0 & 0 & \cdots & 0\\
0 & -(\varepsilon+\eta) & \cdots & 0 & \lambda a_{21} & \lambda a_{22} & \cdots & \lambda a_{2N} & 0 & 0 & \cdots & 0\\
\vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots\\
0 & 0 & \cdots & -(\varepsilon+\eta) & \lambda a_{N1} & \lambda a_{N2} & \cdots & \lambda a_{NN} & 0 & 0 & \cdots & 0\\
\varepsilon & 0 & \cdots & 0 & -\gamma & 0 & \ldots & 0 & 0 & 0 & \cdots & 0\\
0 & \varepsilon & \cdots & 0 & 0 & -\gamma & \ldots & 0 & 0 & 0 & \cdots & 0\\
\vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots\\
0 & 0 & \cdots & \varepsilon & 0 & 0 & \ldots & -\gamma & 0 & 0 & \cdots & 0\\
\eta & 0 & \cdots & 0 & \gamma & 0 & \ldots & 0 & -\zeta & 0 & \cdots & 0\\
0 & \eta & \cdots & 0 & 0 & \gamma & \ldots & 0 & 0 & -\zeta & \cdots & 0\\
\vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots\\
0 & 0 & \cdots & \eta & 0 & 0 & \ldots & \gamma & 0 & 0 & \cdots & -\zeta
\end{bmatrix} \tag{5}
$$

III. STABILITY OF THE TRIVIAL EQUILIBRIUM E_0

This section focuses on the stability properties of the trivial equilibrium. First, we consider the asymptotic stability of the trivial equilibrium of system (2). For that purpose, let $\mathbb{R}_+^{3\,N} = \{(x_1, x_2, \ldots, x_{3\,N})^T \in \mathbb{R}^{3\,N} | x_j \geq 0, j = 1, 2, \ldots, 3\,N\}$, and the meaningful domain for system (2) is denoted by $\Omega = \{\boldsymbol{y} = (y_1, y_2, \ldots, y_{3\,N})^T \in \mathbb{R}_+^{3N} | y_j + y_{N+j} + y_{2N+j} \leq 1, j = 1, \ldots, N\}$, which can be confirmed as positively invariant for system (2) in the following.

Let $z(t) = (d_1(t), \ldots, d_N(t), i_1(t), \ldots, i_N(t), r_1(t), \ldots, r_N(t))^T$, and system (2) can be rewritten in matrix-vector notation as

$$\frac{dz(t)}{dt} = \boldsymbol{B}z(t) + \boldsymbol{G}(z(t)), \tag{3}$$

with the initial vector $z(0) \in \Omega$, the matrix $\boldsymbol{B}$ defined in (5), as shown at the top of this page, and

$$\boldsymbol{G}(z(t)) = (g_1, g_2, \ldots, g_N, \boldsymbol{0}_{2N})^T,$$

where $g_j = -\lambda(z_j(t) + z_{j+N}(t) + z_{j+2N}(t))\sum_k a_{jk}z_{k+N}(t)$, $j = 1, 2, \ldots, N$.

Let $\boldsymbol{E}_N$ stand for the N-order unit matrix, then the above matrix $\mathbf{B}$ can be rewritten as

$$\boldsymbol{B} = \begin{bmatrix} -(\varepsilon+\eta)\boldsymbol{E}_N & \lambda\boldsymbol{A} & \boldsymbol{0}\\ \varepsilon\boldsymbol{E}_N & -\gamma\boldsymbol{E}_N & \boldsymbol{0}\\ \eta\boldsymbol{E}_N & \gamma\boldsymbol{E}_N & -\zeta\boldsymbol{E}_N \end{bmatrix}.$$

Now, it is ready to present a criterion for the asymptotic stability of the trivial equilibrium.

Theorem 1: Let $\boldsymbol{A} = [a_{ij}]_{N\times N}$ be the adjacency matrix of the spreading network, and denote $\mathcal{T}_1 = \gamma(\varepsilon+\eta)/(\lambda\varepsilon)$. Consider system (2), then the trivial equilibrium $\boldsymbol{E}_0$ is asymptotically stable if $\lambda_{\max}(\boldsymbol{A}) < \mathcal{T}_1$, where $\lambda_{\max}(\boldsymbol{A})$ represents the largest eigenvalue of the adjacent matrix of the considered spreading network.

Proof: The Jacobian matrix of system (2) evaluated at the trivial equilibrium $\boldsymbol{E}_0$ is

$$\boldsymbol{J} = \begin{bmatrix} -(\varepsilon+\eta)\boldsymbol{E}_N & \lambda\boldsymbol{A} & \boldsymbol{0}\\ \varepsilon\boldsymbol{E}_N & -\gamma\boldsymbol{E}_N & \boldsymbol{0}\\ \eta\boldsymbol{E}_N & \gamma\boldsymbol{E}_N & -\zeta\boldsymbol{E}_N \end{bmatrix}.$$

Then, the characteristic equation of the above Jacobian matrix can be calculated as

$$
\begin{aligned}
&\det(\boldsymbol{J} - x\boldsymbol{E}_{3N})\\
&= \det\begin{bmatrix} -(\varepsilon+\eta)\boldsymbol{E}_N - x\boldsymbol{E}_N & \lambda\boldsymbol{A} & \boldsymbol{0}\\ \varepsilon\boldsymbol{E}_N & -\gamma\boldsymbol{E}_N - x\boldsymbol{E}_N & \boldsymbol{0}\\ \eta\boldsymbol{E}_N & \gamma\boldsymbol{E}_N & -\zeta\boldsymbol{E}_N - x\boldsymbol{E}_N \end{bmatrix}\\
&= \det(-\zeta\boldsymbol{E}_N - x\boldsymbol{E}_N)\det\\
&\quad\times\begin{bmatrix} -(\varepsilon+\eta)\boldsymbol{E}_N - x\boldsymbol{E}_N & \lambda\boldsymbol{A}\\ \varepsilon\boldsymbol{E}_N & -\gamma\boldsymbol{E}_N - x\boldsymbol{E}_N \end{bmatrix}\\
&= (-\zeta - x)^N \det((\varepsilon+\eta+x)(\gamma+x)\boldsymbol{E}_N - \varepsilon\lambda\boldsymbol{A})\\
&= (-\zeta - x)^N(\varepsilon\lambda)^N \det\left[\frac{(\varepsilon+\eta+x)(\gamma+x)}{\varepsilon\lambda}\boldsymbol{E}_N - \boldsymbol{A}\right] = 0.
\end{aligned} \tag{4}
$$

This equation has $-\zeta$ as a root with multiplicity N, and has the following N pairs

$$\frac{-(\gamma+\varepsilon+\eta) \pm \sqrt{(\gamma+\varepsilon+\eta)^2 + 4[\lambda\varepsilon\lambda_k - \gamma(\varepsilon+\eta)]}}{2},$$

as the remaining $2N$ roots, where $k = 1, \ldots, N$. So, if $\lambda_{\max}(\boldsymbol{A}) < \gamma(\varepsilon+\eta)/(\lambda\varepsilon)$, then for all $k = 1, \ldots, N$ we get $\lambda\varepsilon\lambda_k - \gamma(\varepsilon+\eta) \leq \lambda\varepsilon\lambda_{\max}(\boldsymbol{A}) - \gamma(\varepsilon+\eta) < 0$, which implies the real parts of the above $2N$ roots are negative. Thus, all the roots of (4) have negative real parts, and the trivial equilibrium of system (2) is asymptotically stable. The proof is complete.

The following lemma is necessary to prove that Ω is a positive invariant for system (3), also see [16], [22].

Lemma 1: Consider a system $d\boldsymbol{x}/dt = \boldsymbol{f}(\boldsymbol{x})$ which is defined at least in a compact set $\mathcal{C}$. Then, $\mathcal{C}$ is invariant if, for every point $\boldsymbol{y}$ on $\partial\mathcal{C}$ (the boundary of $\mathcal{C}$), the vector $\boldsymbol{f}(\boldsymbol{y})$ is tangent to or pointing into $\mathcal{C}$.

Next, we consider the global stability of the trivial equilibrium of system (2). For that purpose, the following two lemmas are necessary.

Lemma 2: The set Ω is positively invariant for system (2). That is, each $\boldsymbol{y}(0) \in \Omega$ implies $\boldsymbol{y}(t) \in \Omega$ for all $t > 0$.

Proof: The boundary of Ω, denoted by $\partial\Omega$, consists of the following $4N$ hyperplanes:

$$\begin{aligned}
X_j &= \{\boldsymbol{y} \in \Omega | y_j = 0\}, \quad j = 1, 2, \ldots, N,\\
Y_j &= \{\boldsymbol{y} \in \Omega | y_{j+N} = 0\}, \quad j = 1, 2, \ldots, N,\\
Z_j &= \{\boldsymbol{y} \in \Omega | y_{j+2N} = 0\}, \quad j = 1, 2, \ldots, N,\\
H_j &= \{\boldsymbol{y} \in \Omega | y_j + y_{j+N} + y_{j+2N} = 1\}, \quad j = 1, 2, \ldots, N.
\end{aligned}$$

For $1 \le j \le N$, $X_j, Y_j, Z_j, H_j (j = 1, 2, \ldots, N)$ have

$$\begin{aligned}
\phi_j &= \{0, \ldots, 0, \overset{j}{-1}, 0, \ldots, 0\}, \quad j = 1, 2, \ldots, N,\\
\varphi_j &= \{0, \ldots, 0, \overset{j+N}{-1}, 0, \ldots, 0\}, \quad j = 1, 2, \ldots, N,\\
\vartheta_j &= \{0, \ldots, 0, \overset{j+2N}{-1}, 0, \ldots, 0\}, \quad j = 1, 2, \ldots, N,\\
\psi_j &= \{\ldots, \overset{j}{1}, 0, \ldots, 0, \overset{j+N}{1}, 0, \ldots, 0, \overset{j+2N}{1}, \ldots\},
\end{aligned}$$

as their respective outer normal vectors. Let $\boldsymbol{y}$ be a smooth point of $\partial\Omega$. Consider system (3), we distinguish among four possibilities. That is, for all $j = 1, 2, \ldots, N$, we have

$$\begin{aligned}
\left(\frac{dz}{dt}|_{z\in X_j}, \phi_j\right) &= -\lambda(1 - i_j(t) - r_j(t)) \sum_k a_{jk} i_k(t) \le 0,\\
\left(\frac{dz}{dt}|_{z\in Y_j}, \varphi_j\right) &= -\varepsilon d_j(t) \le 0,\\
\left(\frac{dz}{dt}|_{z\in Z_j}, \vartheta_j\right) &= -(\eta d_j(t) + \gamma i_j(t)) \le 0,\\
\left(\frac{dz}{dt}|_{z\in H_j}, \psi_j\right) &= -\zeta r_j(t) \le 0.
\end{aligned}$$

Combining the above discussions, we get that for each $\boldsymbol{y} \in \partial\Omega$, $\boldsymbol{z}(\boldsymbol{y})$ is pointing into or tangent to $\partial\Omega$. The claimed result then follows from Lemma 1. The proof is complete.

Consider an $n \times n$ matrix $\boldsymbol{M}$, denote $s(\boldsymbol{M}) = \max_{1\le i\le n}\{\mathrm{Re}\,\lambda_i\}$, where λ_i, $i = 1, \ldots, n$ are the eigenvalues of the matrix $\boldsymbol{M}$, and $\mathrm{Re}(\cdot)$ denotes the real part. The following lemma is very important, see also Ref. [16].

Lemma 3: Consider an n-dimensional autonomous system

$$\frac{d\boldsymbol{x}(t)}{dt} = \boldsymbol{B}\boldsymbol{x}(t) + \boldsymbol{H}(\boldsymbol{x}(t)), \quad \boldsymbol{x}(t) \in \mathcal{D},$$

where $\mathcal{D}$ is a region containing the origin, $\boldsymbol{H}(\boldsymbol{x}(t)) \in C^1(\mathcal{D})$, $\lim_{\boldsymbol{x}\to\boldsymbol{0}} \|\boldsymbol{H}(\boldsymbol{x})\|/\|\boldsymbol{x}\| = 0$. Assume that there are a positively invariant compact convex set $\mathcal{C} \subset \mathcal{D}$ containing the origin, a positive number r, and a real eigenvector ω of $\boldsymbol{B}^{\mathrm{T}}$ such that

(C1) $(\boldsymbol{x}, \omega) \ge r\|\boldsymbol{x}\|$ for all $\boldsymbol{x} \in \mathcal{C}$,
(C2) $(\boldsymbol{H}(\boldsymbol{x}), \omega) \le 0$ for all $\boldsymbol{x} \in \mathcal{C}$,
(C3) the origin forms the largest positively invariant set included in the set $\{\boldsymbol{x} \in \mathcal{C} | (\boldsymbol{H}(\boldsymbol{x}), \omega) = 0\}$.

Let $\lambda_{\max}(\boldsymbol{B})$ denote the maximum real part of all eigenvalues of $\boldsymbol{B}$. Then we get

(1) $\lambda_{\max}(\boldsymbol{B}^{\mathrm{T}}) < 0$ implies that the origin is globally asymptotically stable in $\mathcal{C}$,
(2) $\lambda_{\max}(\boldsymbol{B}^{\mathrm{T}}) > 0$ implies that there exists $m > 0$ such that $\boldsymbol{x}(0) \in \mathcal{C} - \{\boldsymbol{0}\}$ implies $\liminf_{t\to\infty} \|\boldsymbol{x}(t)\| \ge m$.

By the lemmas above, we can derive the following theorem.

Theorem 2: Consider system (3). Then, $\boldsymbol{E}_0 = \boldsymbol{0}$ is globally asymptotically stable with respect to Ω if $\lambda_{\max}(\boldsymbol{A}) < \gamma(\varepsilon + \eta)/(\lambda\varepsilon)$.

Proof: Let $\mathcal{C} = \Omega$. Note that the matrix $\boldsymbol{B}^T$ is irreducible, and all of its non-diagonal entries are nonnegative, thus it follows by [16] that $\boldsymbol{B}^T$ has a positive eigenvector $\vec{\omega} = (\omega, \ldots, \omega_{3\,N})$ corresponding to its eigenvalue $s(\boldsymbol{B}^T)$.

Let $\omega_0 = \min_{1\le j\le 3N}\{\omega_j\} > 0$. Then, for all $\boldsymbol{y} \in \Omega$, we have

$$\begin{aligned}
(\boldsymbol{y}, \vec{\omega}) &\ge \omega_0 \sum_{i=1}^{3N} y_i \ge \omega_0 \left(\sum_{i=1}^{3N} y_i^2\right)^{\frac{1}{2}} = \omega_0\|\boldsymbol{y}\|,\\
(\boldsymbol{G}(\boldsymbol{y}), \vec{\omega}) &= -\lambda \sum_{j=1}^{N} \left[\omega_j(z_j + z_{j+N} + z_{j+2N}) \sum_{k=1}^{N} a_{jk} z_{k+N}\right]\\
&\le 0.
\end{aligned}$$

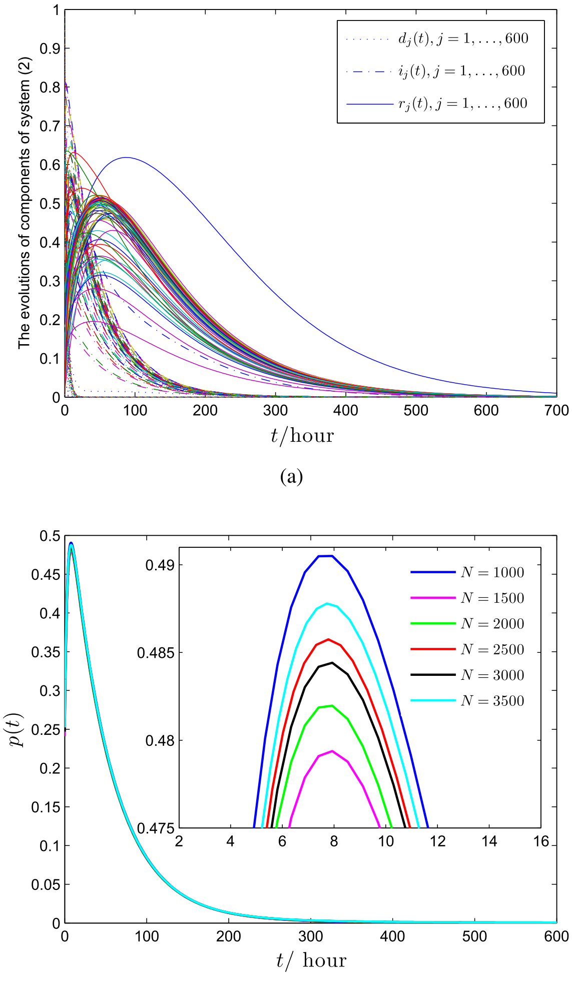
Moreover, $(\boldsymbol{G}(\boldsymbol{y}), \vec{\omega}) = 0$ implies that $\boldsymbol{y} = 0$. In the above, we have proved that $s(\boldsymbol{B}^T) < 0$ if $\lambda_{\max}(\boldsymbol{A}) < \gamma(\varepsilon + \eta)/(\lambda\varepsilon)$, hence, the claimed result follows from assertion (1) of Lemma 3.

IV. NUMERICAL SIMULATIONS

In this section, several numerical examples will be designed to verify the theoretical results derived above. For that purpose, we denote $I(t) = \sum_{j=1}^{N} i_j(t)$ the number of intruded nodes at time t, and $p(t)$ the percentage of intruded nodes, i.e., $p(t) = \frac{1}{N}\sum_{j=1}^{N} i_j(t)$. That is, $p(t)$ means $I(t)$ over the total number of network nodes at time t. To make the following simulations more practical, we set the time evolution by hour, i.e., a unit time representing one hour. The parameter values of the model need to be appropriately given, and then the parameters specifically mean corresponding transition probabilities per hour. To explore ransomware spreading over general networks, we first consider two kinds of networks with simple topology structures: star-shaped networks and complete networks.

Firstly, for a star-shaped propagating network of size N, the characteristic equation for its adjacency matrix can be explicitly computed as $\mathcal{P}_{star}(x) = x^{N-2}(x^2 - (N-1)) = 0$, which obviously implies that the maximum eigenvalue is $\sqrt{N-1}$ (the other eigenvalues are a unique negative eigenvalue $-\sqrt{N-1}$, and zero with multiplicity $N-2$). Therefore, for this kind of networks, Theorem 2 guarantees the global stability of the trivial equilibrium $\boldsymbol{E}_0$ if $N < [\gamma(\varepsilon + \eta)/(\lambda\varepsilon)]^2 + 1$. That is, once the parameter values are specifically fixed, then the dynamics of ransomware spreading over star-networks are dependent on the network size.

Example 1: Consider the node-based SDIRS model (1), and take a star-shaped graph of size N as the spreading network. The probabilistic parameters in system (2) are specifically given by $\lambda = 5 \times 10^{-4}$, $\gamma = 0.02$, $\varepsilon = 0.2$, $\eta = 0.1$, $\zeta = 0.01$. Then, by certain calculations, we can derive that $\mathcal{T}_1 = \gamma(\varepsilon + \eta)/(\lambda\varepsilon) = 60$.



(a)

(b)

FIGURE 3. Ransomware dynamics over star networks with parameters shown in Example 1. a) Evolutions for some components of system (2) with $N = 600$ and a set of randomly-given initial values. For each linestyle, various colors correspond to the different index $j = 1, \dots, N$. b) Evolutions of percentage of I-nodes with various network size N.

For this case, it follows by Theorem 2 that Example 1 implies the global stability of the trivial equilibrium $\boldsymbol{E}_0 = \boldsymbol{0}$ provided that the network size $N \leq 3600$. Consider a star network of $N = 600$ nodes, Fig. 3(a) shows the evolutions of components $d_j(t), i_j(t), r_j(t), j = 1, \dots, N$ of system (2), where the solutions with different degrees are distinguished by various colors. It can be seen in Fig. 3(a) that the solutions of system (2) finally tend to zero, in agreement with the theoretical prediction. The evolutions of percentages of I-nodes over different star-networks with $N = 1000, \dots, 3500$ are shown in Fig. 3(b), where it can be seen that all the curves coincide generally with a little differences (leading to a certain greater number difference on larger networks), and reach the peak rapidly, and then gradually decrease and tend to zero. This implies that for star networks with different size, almost same percentage of the whole nodes will be intruded by ransomware at any time t.

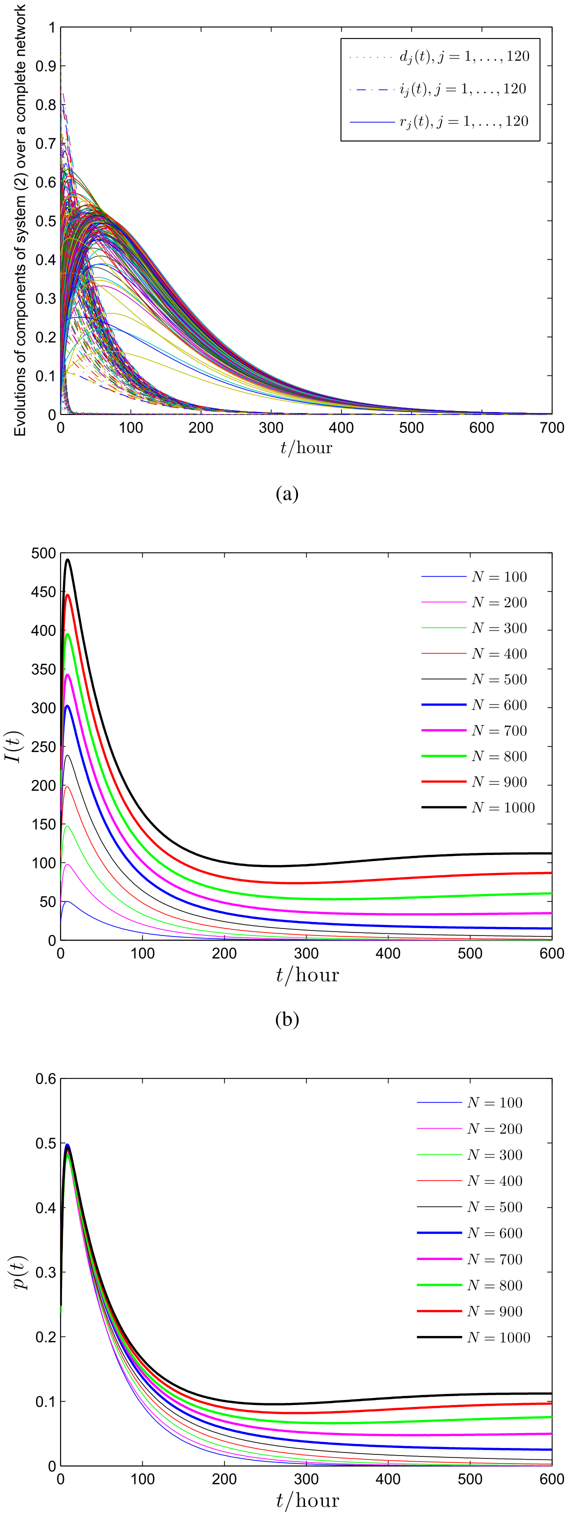
Secondly, consider a fully-connected network of N nodes, the characteristic equation of its adjacency matrix can be calculated as $\mathcal{P}_{full}(x) = (x+1)^{N-1}(x-(N-1)) = 0$, which implies only two eigenvalues: one is negative $x_1 = -1$ with multiplicity $N-1$, and the other is positive $x_2 = N-1$ (the largest eigenvalue).

Example 2: Consider the node-based SDIRS model, and take a complete graph of size N as the propagation network. The parameters in system (2) are specifically given by $\lambda = 5.5 \times 10^{-5}$, $\gamma = 0.02$, $\varepsilon = 0.2$, $\eta = 0.1$, $\zeta = 0.01$. Then, we have $\gamma(\varepsilon + \eta)/(\lambda\varepsilon) = 545.4545$.

According to Theorem 2, the case shown in Example 2 implies that the trivial equilibrium $\boldsymbol{E}_0 = \boldsymbol{0}$ of system (2) is always globally stable provided the network size $N \leq 546$. For $N = 120$, it can be seen in Fig. 4(a) that ransomware tends to extinction very quickly, in consistency with the prediction. Fig. 4(b) shows the number evolutions of intruded nodes over ten different complete networks with size $N = 100, \dots, 1000$. It can be observed in Fig. 4(b) that the numbers of I-nodes for all considered cases reach their peaks rapidly, and then gradually decrease and tend to balance. Specifically, for the cases $N = 100, \dots, 500$, it is shown in Fig. 4(b) that the numbers of I-nodes eventually converge to zero, agreeing with the above result. However, for the other cases $N = 600, \dots, 1000$ shown in Fig. 4(b), the numbers of intruded nodes finally tend to corresponding different constants, which imply that ransomware spreading will persist over the network. The evolutions of percentages of intruded nodes over ten different networks are shown in Fig. 4(c), where it can be found that all the trajectories with $N \leq 500$ finally converge to zero, agreeing with the prediction. It is shown in Fig. 4(b) that the number of I-nodes over a larger-size network is always greater than that over a smaller-size network, whereas it is shown in Fig. 4(c) that the fractions of I-nodes for all the considered cases are nearly same for the early stage.

It is well known that a multitude of real-world networks are scale-free, i.e., their degree distributions approximately follow a power law [29]. The properties of approximate power-law degree distribution over scale-free networks are considered in the model of Ref. [19]. In this work, the adjacency matrix of the spreading network involved in model (2) can more fully reflect the topology of the network. Thus, the new complex-network model can be used to depict ransomware spreading over a larger number of networks including scale-free networks. In the sequel, we will simulate the ransomware spreading over a scale-free network. The method proposed by Barabási and Albert [29] can be applied to generate scale-free networks.

Example 3: Consider the node-based SDIRS model, and generate a scale-free network with a given number of N nodes using the Barabási-Albert method. Take this network as the propagation network. The parameters in system (2) are specifically given by $\lambda = 5 \times 10^{-4}$, $\gamma = 0.02$, $\varepsilon = 0.2$, $\eta = 0.1$, $\zeta = 0.01$. Then, we have $\mathcal{T}_1 = \gamma(\varepsilon + \eta)/(\lambda\varepsilon) = 60$.

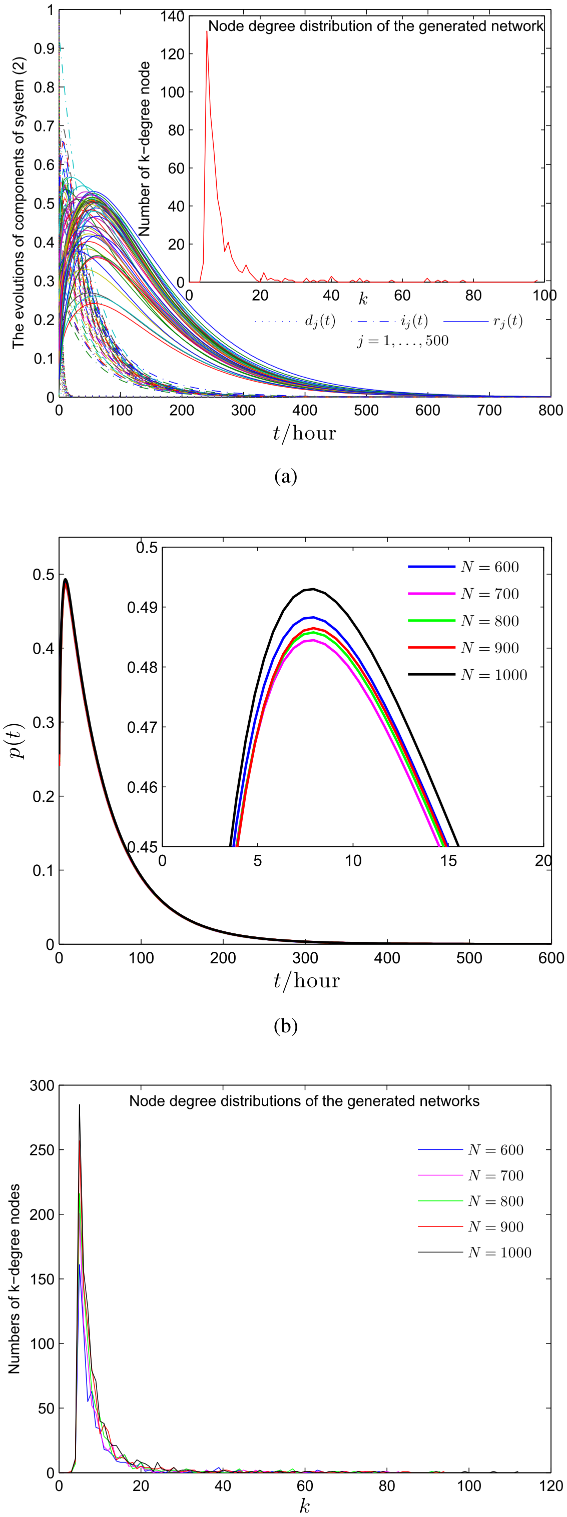


(a)

(b)

(c)

FIGURE 4. Ransomware dynamics of model (2) over complete networks with the parameters shown in Example 2. a) Evolutions for all components of system (2) with a set of randomly-given initial values and $N = 120$. For each linestyle, various colors correspond to the different index $j = 1, \ldots, 120$. b) Number evolutions of I-nodes with different values of network size. c) Percentages of I-nodes on several networks with different sizes.



(a)

(b)

(c)

FIGURE 5. Evolutions of ransomware over generated scale-free networks. a) Evolutions for some components of system (2) over a generated network of size $N = 500$ and a set of randomly-given initial values. For each linestyle, various colors correspond to the different index $j = 1, \ldots, 500$. b) Evolutions of percentage of I-nodes with various network size N. c) Distributions of node degree corresponding to the generated networks used in Fig. 5(b).

The dynamics of system (2) with parameters given in Example 3 are numerically shown in Fig. 5. First, we generate a scale-free network of size $N = 500$ by the Barabási and Albert method, whose node degree distribution is shown in Fig. 5(a). For this case, numerical calculations give that its leading eigenvalue is $\lambda_{\max} = 19.1$, which is obviously less than 60. Thus, it follows by Theorem 2 that the trivial equilibrium $\boldsymbol{E}_0 = \mathbf{0}$ is globally stable. By randomly fixing a set of initial values, Fig. 5(a) shows the evolutions for some components of system (2), which finally tend to zero. Fig. 5(b) shows the fractions of I-nodes over time on several generated networks with $N = 600, \ldots, 1000$ shown in Fig. 5(c). It can be observed that all the curves coincide nearly in the whole process, except for slight differences around the peaks, and all of them reach their corresponding peaks quickly and then gradually decrease to zero.

Remark 1: In the above experiments, we just verify the theoretical results by considering ransomware spreading over ordinary and complex networks. Actually, to verify the effectiveness of the method and the proposed model in this paper, it will be more meaningful to compare the theoretical results with real ransomware attacks. Theoretically, we think that this is practicable. However, it is very hard for us to derive real data of ransomware attacks. Moreover, in the processes of analyzing real data, we possibly face two problems: one is that we need to adjust suitable parameters for the real case, the other is that it may be complicated to calculate the eigenvalues of the adjacency matrix when the real attacking network is large enough. Thus, we propose to carry out further research on model (1) and we will also consider to practically verify the effectiveness of this model in future works.

Combined with the above theoretical and numerical analysis, some practical recommendations can be suggested. In order to effectively prevent ransomware diffusion, it is necessary to find the attacks of ransomware as quickly as possible, e.g., using solutions that apply advanced machine learning to detect all types of ransomware. It will be helpful to backup your data so that it can be recovered in case of a ransomware attack. Furthermore, it is also important to enhance the safety awareness of network users. For example, employees should be trained on identifying and reporting suspicious phishing links to cut off ransomware attacks before causing damage.

V. CONCLUSION

In this study, we mainly explore how the topology of propagating networks affects ransomware spreading processes. By incorporating the network structure using the adjacent matrix of the spreading network, an analytical network-based model is newly developed. This is a much more complicated high-dimensional model, and the topology of the network can be general and arbitrary. The properties of the model system are carefully analyzed, theoretically proving the global stability of the trivial equilibrium under a condition involving in the leading eigenvalue of the adjacent matrix.

The idea of our work, especially the proposed novel model, is heuristic and significant in the area of modeling ransomware spreading. Compared with the previous models which are limited to describe epidemic dynamics over homogeneous networks, the node-based model incorporating the adjacent matrix is applicable over a wide range of general networks including real networks. Our numerical simulations suggest that ransomware prevalence over networks, to a certain degree, can be effectively prevented and controlled by properly modifying the network topology such that the characteristics of the propagating networks satisfy the requirements. However, system (1) is also a fundamental model, thus more in-depth research on this model is needed for enhancing the ability to prevent and control ransomware attacks.

REFERENCES

[1] S. Grzonkowski, A. Mosquera, L. Aouad, and D. Morss, "Smartphone Security: An overview of emerging threats," *IEEE Consum. Electron. Mag.*, vol. 3, no. 4, pp. 40–44, Oct. 2014.

[2] P. O'Kane, S. Sezer, and D. Carlin, "Evolution of ransomware," *IET Netw.*, vol. 7, no. 5, pp. 321–327, 2018.

[3] J. Chen, C. Wang, Z. Zhao, K. Chen, R. Du, and G.-J. Ahn, "Uncovering the face of Android ransomware: Characterization and real-time detection," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 5, pp. 1286–1300, May 2018.

[4] K. Cabaj and W. Mazurczyk, "Using software-defined networking for ransomware mitigation: The case of cryptowall," *IEEE Netw.*, vol. 30, no. 6, pp. 14–20, Nov./Dec. 2016.

[5] E. Avena. (Jan./Mar. 2017). *Microsoft Security Intelligence Report*, vol. 22. Accessed: May 12, 2019. [Online]. Available: https://www.microsoft.com/en-us/security/intelligence-report

[6] I. Ghafir, V. Prenosil, M. Hammoudeh, T. Baker, S. Jabbar, S. Khalid, and S. Jaf, "BotDet: A system for real time Botnet command and control traffic detection," *IEEE Access*, vol. 6, pp. 38947–38958, 2018.

[7] S. Yu, G. Zhao, S. Guo, Y. Xiang, and A. V. Vasilakos, "Browsing behavior mimicking attacks on popular Web sites for large botnets," in *Proc. IEEE INFOCOM*, Shanghai, China, Apr. 2011, pp. 947–951.

[8] A. Kharraz, W. Robertson, and E. Kirda, "Protecting against ransomware: A new line of research or restating classic ideas?" *IEEE Secur. Privacy*, vol. 16, no. 3, pp. 103–107, May/Jun. 2018.

[9] Q. Liu, P. Li, W. Zhao, W. Cai, S. Yu, and V. C. M. Leung, "A survey on security threats and defensive techniques of machine learning: A data driven view," *IEEE Access*, vol. 6, pp. 12103–12117, 2018.

[10] C. Xu, L. Zhu, Y. Liu, J. Guan, and S. Yu, "DP-LTOD: Differential privacy latent trajectory community discovering services over location-based social networks," *IEEE Trans. Serv. Comput.*, to be published. doi: 10.1109/TSC.2018.2855740.

[11] W. Liu, C. Liu, X. Liu, S. Cui, and X. Huang, "Modeling the spread of malware with the influence of heterogeneous immunization," *Appl. Math. Model.*, vol. 40, no. 4, pp. 3141–3152, 2016.

[12] C. J. D'Orazio, L. Rongxing, C. K.-K. Raymond, and A. V. Vasilakos, "A Markov adversary model to detect vulnerable iOS devices and vulnerabilities in iOS apps," *Appl. Math. Comput.*, vol. 293, pp. 523–544, Jan. 2017.

[13] J. Singh, D. Kumar, Z. Hammouch, and A. Atangana, "A fractional epidemiological model for computer viruses pertaining to a new fractional derivative," *Appl. Math. Comput.*, vol. 316, pp. 504–515, Jan. 2018.

[14] W. Liu and S. Zhong, "Web malware spread modelling and optimal control strategies," *Sci. Rep.*, vol. 7, p. 42308, Feb. 2017.

[15] C. Xia, L. Wang, S. Sun, and J. Wang, "An SIR model with infection delay and propagation vector in complex networks," *Nonlinear Dyn.*, vol. 69, no. 3, pp. 927–934, 2012.

[16] A. Lajmanovich and J. A. Yorke, "A deterministic model for gonorrhea in a nonhomogeneous population," *Math. Biosci.*, vol. 28, nos. 3–4, pp. 221–236, 1976.

[17] W. Liu, X. Wu, W. Yang, X. Zhu, and S. Zhong, "Modeling cyber rumor spreading over mobile social networks: A compartment approach," *Appl. Math. Comput.*, vol. 343, pp. 214–229, Feb. 2019.

[18] J. D. H. Guillén and A. Martín del Rey, "Modeling malware propagation using a carrier compartment," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 56, pp. 217–226, Mar. 2018.

[19] W. Liu and S. Zhong, "A novel dynamic model for Web malware spreading over scale-free networks," *Phys. A, Stat. Mech. Appl.*, vol. 505, pp. 848–863, Sep. 2018.

[20] W. Pan and Z. Jin, "Edge-based modeling of computer virus contagion on a tripartite graph," *Appl. Math. Comput.*, vol. 320, pp. 282–291, Mar. 2018.

[21] Y. Zhang, P. Dong, S. Yu, H. Luo, T. Zheng, and H. Zhang, "An adaptive multipath algorithm to overcome the unpredictability of heterogeneous wireless networks for high-speed railway," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 11332–11344, Dec. 2018.

[22] W. Liu, C. Liu, Z. Yang, X. Liu, Y. Zhang, and Z. Wei, "Modeling the propagation of mobile malware on complex networks," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 37, pp. 249–264, 2016.

[23] P. V. Mieghem, J. Omic, and R. Kooij, "Virus spread in networks," *IEEE/ACM Trans. Netw.*, vol. 17, no. 1, pp. 1–14, 2009.

[24] M. Youssef and C. Scoglio, "An individual-based approach to SIR epidemics in contact networks," *J. Theor. Biol.*, vol. 283, pp. 136–144, Aug. 2011.

[25] S. Xu, W. Lu, and Z. Zhan, "A stochastic model of multivirus dynamics," *IEEE Trans. Depend. Sec. Comput.*, vol. 9, no. 1, pp. 30–45, Jan. 2012.

[26] Y. Wang, J. Cao, A. Alofi, A. AL-Mazrooei, and A. Elaiw, "Revisiting node-based SIR models in complex networks with degree correlations," *Phys. A, Stat. Mech. Its Appl.*, vol. 437, pp. 75–88, Nov. 2015.

[27] W. Liu and S. Zhong, "Modeling and analyzing the dynamic spreading of epidemic malware by a network eigenvalue method," *Appl. Math. Model.*, vol. 63, pp. 491–507, Nov. 2018.

[28] L.-L. Xia, Y.-R. Song, C.-C. Li, and G.-P. Jiang, "Improved targeted immunization strategies based on two rounds of selection," *Phys. A, Stat. Mech. Appl.*, vol. 496, pp. 540–547, Apr. 2018.

[29] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, pp. 509–512, Oct. 1999.

[30] P. van den Driessche and J. Watmough, "Reproduction numbers and subthreshold endemic equilibria for compartmental models of disease transmission," *Math. Biosci.*, vol. 180, no. 12, pp. 29–48, Nov./Dec. 2002.

WANPING LIU received the B.S. degree in mathematical science and the Ph.D. degree in computer science from Chongqing University, China, in 2009 and 2014, respectively. He was a visiting Ph.D. Student with the University of Waterloo, Canada, from 2012 to 2013. He also did his Postdoctoral Research with the University of Electronic Science and Technology of China, from 2016 to 2019. He is currently an Associate Professor with the Chongqing University of Technology, China. He has published more than 60 publications in these research areas. His research interests include mathematical modeling, complex systems, social networks, and cybersecurtiy.