Received January 8, 2020, accepted January 20, 2020, date of publication January 23, 2020, date of current version January 31, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2968916

Dynamical Propagation Model of Malware for Cloud Computing Security

CHENQUAN GAN[1], QINGDONG FENG[1], XULONG ZHANG[2], ZUFAN ZHANG[1], AND QINGYI ZHU[3]

[1]School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
[2]School of Computer and Network Engineering, Shanxi Datong University, Datong 037009, China
[3]School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

Corresponding author: Xulong Zhang (zxl-095@163.com)

This work was supported in part by the Natural Science Foundation of China under Grant 61702066 and Grant 61903056, in part by the Major Project of Science and Technology Research Program of Chongqing Education Commission of China under Grant KJZD-M201900601, in part in part by the Chongqing Research Program of Basic Research and Frontier Technology under Grant cstc2017jcyjAX0256, Grant cstc2019jcyj-msxmX0681, and Grant cstc2018jcyjAX0154, and in part by the Project Supported by Chongqing Municipal Key Laboratory of Institutions of Higher Education under Grant cqupt-mct-201901.

ABSTRACT Cloud-fog-edge computing especially cloud computing is providing a variety of services in many areas around the world and plays a vital role in cyber-physical-social systems (CPSS). Particularly, virtualization is one of main enabling technologies of cloud computing and realizes the dynamic deployment of computing tasks through the migration of virtual machines (VMs), so how to secure the virtual environment in the cloud is very crucial. The purpose of this paper is to address the issue of malware propagation among VMs under the infrastructure as a service (IaaS) architecture. Firstly, a dynamical propagation model is proposed to explore the important factors affecting the spread of malware, especially the impact of installing antivirus software in VMs. On this basis, a theoretical analysis for this model is investigated by means of differential dynamics, from which it is able to understand the dissemination behavior of malware under an infected cloud environment. Finally, some numerical simulations are conducted to verify the applicability and effectiveness of the proposed model.

INDEX TERMS Cloud computing security, virtual environment, malware, propagation model, dynamical behavior.

I. INTRODUCTION

Cyber-physical-social systems (CPSS) are able to make our daily lives more intelligent and convenient through providing forward-looking and personalized services [1]. With the advent of the big data era and the popularity of the Internet of Things in the future, CPSS services will inevitably require various data support including the global historical data and the local real-time data, which will involve many issues such network communication (e.g., [2], [3]), data storage, processing and applications (e.g., [4], [5]). In this context, researchers are vigorously developing cloud-fog-edge computing in recent years. Specifically, fog-edge computing has been widely applied to process the local real-time data, which is an important and effective supplement of cloud computing. As a powerful paradigm for implementing the data-intensive applications, cloud computing has an irreplaceable role in storing and processing data. It can offer services such as infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) for users on demand.

As one of the most significant techniques of cloud computing, virtualization breaks the boundaries of time and space. Particularly, it can divide a physical computing device into more virtual machines (VMs) with the same functionality and realize the dynamic deployment of computing tasks through the migration of VMs. There is no doubt that virtualization will greatly improve resource utilization and save system management costs [6]. Unfortunately, virtualization also introduces new vulnerabilities that are becoming the attack target of malware.

The original malware developed to avoid virtual systems, but due to various factors such as profit and benefit, malware makers began to target all computing devices, including physical and virtual machines [7]. Because the Internet has strong propagation ability and is also the most important carrier of computer virus transmission, so once malware appears in

The associate editor coordinating the review of this manuscript and approving it for publication was Xiaokang Wang.

a physical or virtual machine, it will spread rapidly in the network, which may cause great damage to human beings, ranging from economic losses to serious threats to human life. Consequently, it is essential to investigate how to protect the virtual environment from malware attack in the cloud.

Generally, the following three aspects will accelerate the spread of malware in the cloud. Firstly, the migration of VMs will facilitate the diffusion of malware [8], [9]. By using the vulnerabilities of VMs to implant malware, criminals can utilize the migration of VMs to achieve the purpose of malicious attack. Very importantly, the migration of VMs plays a key role in cloud computing, by which the dynamic deployment of computing tasks can be implemented. Secondly, the homogeneity of VMs will also benefit the propagation of malware [10]. Here, the homogeneity mainly means that VMs have the homogeneous structure and settings, and the installed softwares are similar. In practice, there are a large number of VMs in the cloud, if they are configured one by one, it will not only take a lot of time, but also be prone to errors. For convenience, only one of them is usually configured, and then the others are generated by copying it. These operations can now be done automatically. Obviously, such homogeneity will provide many opportunities and reduce technical difficulty for attackers. Thirdly, the communication among VMs is the another propagation way of malware. Cloud computing is a distributed parallel computing, the completion of many computing tasks requires VMs to communicate and cooperate with each other through virtual networks. The authors [8] claimed that the internal communication in the cloud is one of the most serious threats to cloud computing security. For the other perspectives, the work [11] gave some reasons why the criminals are easy to control multiple VMs and prepare for various attacks. These points are also introduced in detail in [12].

Through the above mentioned vulnerabilities of VMs in the cloud, criminals can indeed easily launch various attacks, such as botnet attack, distributed denial of service (DDoS) attack, ransomware attack and spyware attack. The work [13] described that malware can enter the virtual environment in its own way, and can even create or control VMs to make them owned by itself. Once the number of controlled VMs reaches a certain level, botnets will emerge, and criminals can launch DDoS attacks at any time. In particular, the botnets in the cloud are able to launch the DDoS attacks on targets outside the cloud [14].

In addition, when a cloud provider provides services to the user, it allows the user to install software and upload data (e.g., image, video, and other documents) to the cloud. This also provides an opportunity for criminals to implant malware (e.g., ransomware and spyware) in the cloud. Moreover, criminals are increasingly inclined to steal user privacy data for profit, and ransomware attack has been one of the most popular attacks in recent years. In [15], the authors stated that malware can spread by sharing images from the image repositories at VMs. Based on an analysis of 5303 Amazon images of VMs, Balduzzi *et al.* [16] found that 98% of Windows and 58% of Linux images contain applications with severe vulnerabilities. Besides, a malicious user can upload the infected image to propagate malware in the cloud [12].

To deal with these threats in the cloud, many measures have been taken to detect and prevent the spread of malware. Among them, the physical host machines were used to monitor the behavior of the VMs. The virtual network is responsible to the communication between VMs and is a logical network based on a physical network, and the storage and calculation functions of VMs also depend on the physical host machines. However, the work [17] pointed out that malware in the virtual environment is likely to escape the surveillance of security tools.

Additionally, a better way for containing malware is to install antivirus software for all VMs in the cloud just as physical machines prevent computer viruses. It is undeniable that this will indeed curb the spread of malware to a large extent. Nevertheless, this will also increase the cost of antivirus investment and energy consumption. In the end, it will inevitably increase the overhead of cloud providers and users, and even adversely affect the global climate. Li *et al.* [18] discovered by studying CyberGuarder (a security tool designed for the green cloud computing) that the performance cost of CyberGuarder is over 10% and the energy consumption is increased by 5%. This also shows that it is not advisable to install antivirus software on all VMs in the cloud.

To balance the benefits and costs of deploying multiple intrusion detection systems, the work [19] proposed a attack model and compared different intrusion detection systems according to the costs. Later, inspired by the application of the classical epidemic model in epidemiology, the authors [12] explored a susceptible-protected-infected (SPI) cloud malware attack model. As the authors claim, this is the first mathematical model to explore the effect of anti-malware software on the spread of malware in the cloud. Besides, this work does not completely copy the classical epidemic model, and gives the corresponding reasons. The dynamics of the model is also analyzed. But it is worth mentioning that this model is established in an initially uninfected cloud environment. That is to say, all VMs enter the virtual network without infection.

Inspired by the above discussion especially the work [12], this paper aims to address the issue of malware propagation among VMs under an infected cloud environment. Different from the work [12], our work allows the infected VMs access to the virtual network. Indeed, the authors [20] pointed out that antivirus software updates always lag behind the emergence of new viruses, and it is not possible to remove all viruses from the network. In addition, our work is also different from the traditional computer virus propagation model (e.g., [21]–[26]). On the one hand, these traditional models do not consider the cloud environment. On the other hand, the model compartments and their transition are different.

In this paper, a new dynamical propagation model of malware is developed. Specifically, it is found from the model analysis that the proposed model has a unique (viral) equilibrium. Furthermore, the stability of the equilibrium is analyzed. The unique (viral) equilibrium is globally asymptotically stable regardless of any threshold. This implies that once malware appears in a virtual network, it will always exist, and no matter what method is adopted, it cannot be completely eliminated. However, by adjusting system parameters, the proportion of infected VMs can be reduced to a relatively low level. This can provide directional guidance to curb the spread of malware. Finally, some numerical simulations are performed to illustrate the obtained theoretical results and verify the proposed model.

The remaining materials of this paper are organized as follows. Section II formulates the proposed dynamical propagation model of malware. Section III conducts a systematic model analysis, including the equilibrium of the proposed model and its stability. In Section IV, some numerical simulations are performed to illustrate the obtained theoretical results and verify the proposed model. Finally, Section V summarizes this work and gives some outlooks for the future.

II. MODEL DESCRIPTION

Our goals and motivations have been described in the previous section, this section will introduce the proposed dynamical propagation model of malware in detail.

To characterize the spread of malware in the cloud, like work [12], in this paper, each VM under IaaS architecture is in one of three states: susceptible, infected, and protected. Of course, these states can be transformed into each other over time under certain conditions. On this basis, all VMs are divided into three groups: susceptible compartment, infected compartment, and protected compartment. Their meanings are defined as follows.

- Susceptible: the state of an uninfected VM in the cloud that is vulnerable to malware attacks. That is to say, an uninfected VM in the cloud does not install antivirus software or the installed antivirus software has expired.
- Infected: the state of a VM in the cloud that has been infected by malware. That is to say, the malware has not been removed.
- Protected: the state of an uninfected VM in the cloud that is immune to malware attacks. That is to say, an uninfected VM in the cloud install the unexpired antivirus software.
- Susceptible compartment: the set of all susceptible VMs in the cloud.
- Infected compartment: the set of all infected VMs in the cloud.
- Protected compartment: the set of all protected VMs in the cloud.

Based on the above definitions, it is not difficult to find the transition between three states. There are a total of six forms of transition between them, i.e.,

- Susceptible⇆ infected (see Fig. 1);
- Susceptible⇆ protected (see Fig. 2);
- Infected ⇆ protected (see Fig. 3).

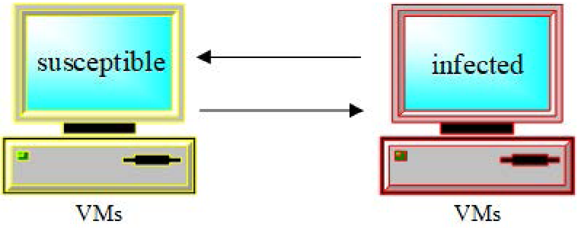

FIGURE 1. Susceptible⇆ infected.

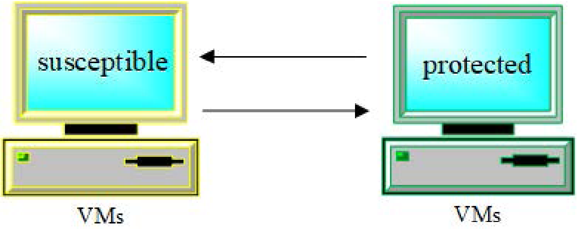

FIGURE 2. Susceptible⇆ protected.

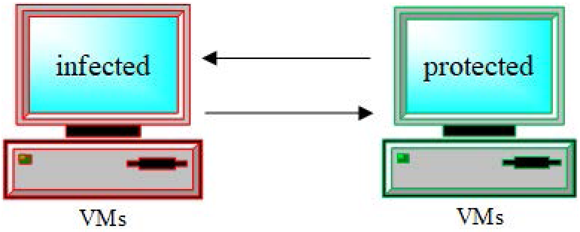

FIGURE 3. Infected ⇆ protected.

Considering the cost of antivirus investment and energy consumption, not all VMs will install antivirus software. Since only by reinstalling the system can be 100% sure that the infected VMs are free of malware, here only consider installing antivirus software to protect susceptible VMs. Therefore, even if the malware in an infected VM is removed, the corresponding VM will not be immune to malware attacks, and will be in a susceptible state. That is to say, infected → protected is impossible. Similarly, protected → infected is also untenable. On the one hand, according to the definition of protected state, a protected VM is impossible to be infected by malware during the entire period of antivirus software. On the other hand, in a protected VM, when the antivirus software is uninstalled or out of date, the corresponding VM will become susceptible. In summary, susceptible⇆ infected and susceptible⇆ protected are possible.

To represent the specific amount of VMs in each compartment at time t, let $S(t)$, $I(t)$, and $P(t)$ (respectively, abbreviated for S, I, P) denote the proportions of susceptible, infected, and protected VMs in the cloud, respectively. In addition, the parameters involved in the state transition are shown in Table 1.

TABLE 1. The parameters involved in the state transition.

Parameter	Definition
η_1	The entering rate of infected VMs
η_2	The entering rate of susceptible VMs
η_3	The entering rate of protected VMs
μ	The shut down rate of each VM
β	The infected rate
δ	The reinstalling system rate of infected VMs
γ	The migration rate of each VM
α	The installing antivirus software rate
α_0	The expired rate of antivirus software

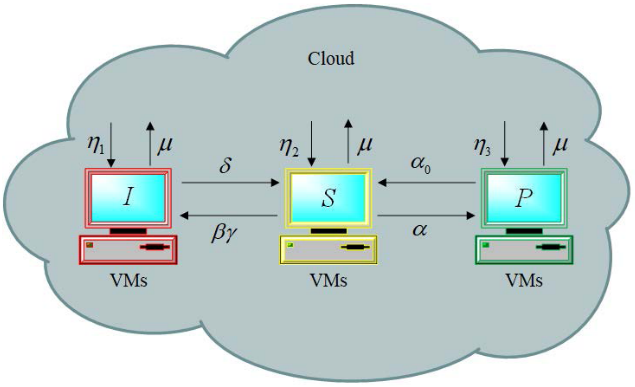

FIGURE 4. The transfer diagram of the proposed dynamical propagation model of malware.

Collecting the foregoing discussions, the transfer diagram of each compartment is depicted in Fig. 4. To further describe the transition between them, the following transfer rules are made according to Table 1 and Fig. 4.

- Each VM in the cloud is shut down with probability μ at time t.
- At time t, the susceptible, infected, and protected VMs enter the cloud with probability η_1, η_2, and η_3, respectively.
- Each susceptible VM in the cloud is infected by malware with probability β at time t.
- Each VM in the cloud migrates from one physical machine to another with probability γ at time t.
- The malware of an infected VM in the cloud is removed with probability δ at time t.
- Due to installing the latest antivirus software, the corresponding susceptible VM in the cloud will be immune to malware with probability α at time t.
- Due to antivirus software failing to work efficiently (e.g., the installed antivirus software is lack of latest update or is out of the date), the corresponding protected VM in the cloud will become susceptible with probability α_0 at time t.

From Fig. 4 and the transfer rules, the proposed dynamical propagation model of malware can be represented by the differential dynamical system as follows.

$$\begin{cases} \dfrac{dS(t)}{dt} = \eta_1 + \delta I(t) + \alpha_0 P(t) - \beta\gamma S(t)I(t) \\ \qquad\qquad -\alpha S(t) - \mu S(t), \\ \dfrac{dI(t)}{dt} = \eta_2 + \beta\gamma S(t)I(t) - \delta I(t) - \mu I(t), \\ \dfrac{dP(t)}{dt}\text{‘} = \eta_3 + \alpha S(t) - \alpha_0 P(t) - \mu P(t), \end{cases} \tag{1}$$

with initial condition $(S(0), I(0), P(0))^T \in \Omega$, where

$$\Omega = \left\{(S, I, P) \in \mathbb{R}^3_+ : S + I + P = 1\right\}$$

is positively invariant for system (1).

Remark 1: In our model, the shut down rate caused by malware attacks is not considered. There are two main reasons. On the one hand, in order to pursue higher profits, the current malware is generally not actively exposed and does not damage the host machine. That is to say, the shut down rate caused by malware attacks can be ignored. On the other hand, the shut down rate in our model covers it. In fact, the shut down rate caused by malware attacks is similar to death rate induced by diseases. The former generally borrows from the latter.

III. MODEL ANALYSIS

Before proceeding with model analysis, let us introduce the meaning of some basic terms, which will be useful in the sequel.

- Dynamical system: dynamics is primarily the study of the time-evolutionary process and the corresponding system of equations is known as dynamical system [27]. In this paper, system (1) is a differential dynamical system.
- Equilibrium: equilibrium is a fixed point of a dynamical system, which is important in analyzing the local and global behaviors of the dynamical system. In this paper, an equilibrium represents a possible final propagation level of malware, which can be obtained by solving the first order differential dynamical system (1).
- Viral equilibrium: in this paper, if the component of infected VMs in an equilibrium is not zero, this equilibrium is called viral equilibrium.
- Stability: long-term behavior of an equilibrium of a dynamical system. In this paper, by analyzing the stability of equilibrium of dynamical system (1), the final propagation level and behavior of malware in the cloud can be predicted.

Note that S, I, and P denote the proportions of susceptible, infected, and protected VMs in the cloud, respectively. Thus, $S + I + P = 1$. Furthermore, adding the three equations of system (1) gives: $\mu = \eta_1 + \eta_2 + \eta_3$. Then, system (1) can be rewritten as the following system:

$$\begin{cases} \dfrac{dI(t)}{dt} = \eta_2 + (\beta\gamma - \delta - \mu)I(t) - \beta\gamma P(t)I(t) - \beta\gamma I^2(t), \\ \dfrac{dP(t)}{dt} = \alpha + \eta_3 - \alpha I(t) - (\alpha + \alpha_0 + \mu)P(t), \end{cases} \tag{2}$$

with initial condition $(I(0), P(0))^T \in \tilde{\Omega}$, where

$$\tilde{\Omega} = \{(I, P) \in \mathbb{R}_+^2 : I + P \leq 1\}$$

is also positively invariant for system (2).

For brevity, let us analyze the dynamical behavior of system (2) instead of system (1), from which one can get the same results for system (1).

A. EQUILIBRIUM

Firstly, let us consider the equilibrium of system (2). According to the definition of equilibrium, the following result about system (2) can be obtained.

Theorem 1: System (2) has a unique equilibrium $E_* = (I_*, P_*)$ and E_* is a viral equilibrium, where

$$\begin{aligned} I_* &= \frac{-B + \sqrt{B^2 - 4AC}}{2A}, \\ P_* &= \frac{\alpha + \eta_3 - \alpha I_*}{\alpha + \alpha_0 + \mu}, \\ A &= \beta\gamma\,(\alpha_0 + \mu), \\ B &= \beta\gamma(\alpha + \eta_3) - (\alpha + \alpha_0 + \mu)(\beta\gamma - \delta - \mu), \\ C &= -\eta_2(\alpha + \alpha_0 + \mu). \end{aligned}$$

Proof: Assume that $\bar{E} = (\bar{I}, \bar{P})$ is an equilibrium of system (2). According to the definition of equilibrium, let

$$\begin{cases} \dfrac{dI(t)}{dt} = \eta_2 + (\beta\gamma - \delta - \mu)I(t) - \beta\gamma P(t)I(t) - \beta\gamma I^2(t) = 0, \\ \dfrac{dP(t)}{dt} = \alpha + \eta_3 - \alpha I(t) - (\alpha + \alpha_0 + \mu)P(t) = 0. \end{cases}$$

Then $\bar{E} = (\bar{I}, \bar{P})$ is a nonnegative solution to the following system:

$$\begin{cases} \eta_2 + (\beta\gamma - \delta - \mu)\bar{I} - \beta\gamma\bar{I}\bar{P} - \beta\gamma\bar{I}^2 = 0, \\ \alpha + \eta_3 - \alpha\bar{I} - (\alpha + \alpha_0 + \mu)\bar{P} = 0. \end{cases} \tag{3}$$

Now, it suffices to prove that there is a unique positive solution for system (3).

Simplifying the second equation of system (3), one can get

$$\bar{P} = \frac{\alpha + \eta_3 - \alpha\bar{I}}{\alpha + \alpha_0 + \mu}.$$

Then substituting $\bar{P}$ into the first equation of system (3), the following equation can be obtained:

$$A\bar{I}^2 + B\bar{I} + C = 0,$$

where A, B, and C are constants, which are defined in Theorem 1.

As $\bar{I} > 0$, it follows from a direct calculation that $\bar{I} = I_*$, and $\bar{P} = P_*$. That is to say, $\bar{E} = E_*$. Hence, E_* is a viral equilibrium of system (2), and is a unique equilibrium. The proof is complete. □

B. LOCAL STABILITY

Theorem 1 has shown that the considered system (2) has a unique (viral) equilibrium E_*. This means that malware may always be in the cloud. To verify this guess, let us first study the local stability of the unique (viral) equilibrium E_* of system (2). Then, the following result about local stability of system (2) is obtained.

Theorem 2: The unique (viral) equilibrium E_* is locally asymptotically stable for system (2).

Proof: According to the definition of local stability, the Jacobian matrix of system (2) can be calculated at E_* as:

$$\begin{pmatrix} \beta\gamma(1 - P_* - 2I_*) - \delta - \mu & -\beta\gamma I_* \\ -\alpha & -(\alpha + \alpha_0 + \mu) \end{pmatrix},$$

and the corresponding characteristic equation is

$$\lambda^2 + a_1\lambda + a_2 = 0, \tag{4}$$

where

$$\begin{aligned} a_1 &= \beta\gamma(P_* + 2\,I_* - 1) + \delta + \mu + \alpha + \alpha_0 + \mu \\ &= \alpha + \alpha_0 + \mu + \frac{\eta_2}{I_*} + \beta\gamma I_* \\ &> 0, \\ a_2 &= [\beta\gamma(1 - P_* - 2\,I_*) - \delta - \mu]\,(\alpha + \alpha_0 + \mu) - \alpha\beta\gamma I_* \\ &= \frac{\alpha\eta_2}{I_*} + (\alpha_0 + \mu)\left(\frac{\eta_2}{I_*} + \beta\gamma I_*\right) \\ &> 0. \end{aligned}$$

As $a_1 > 0$ and $a_2 > 0$, then the two roots of characteristic equation (4) both have negative real parts. Therefore, it follows form the Lyapunov stability theorem [28] that the unique (viral) equilibrium E_* of system (2) is locally asymptotically stable. The proof is complete. □

C. GLOBAL STABILITY

Theorem 2 has revealed that the unique (viral) equilibrium E_* of the considered system (2) is locally asymptotically stable. This implies that malware can always exist in the cloud under a certain condition. To investigate whether malware can always exist in the cloud without any conditions, let us focus on the global stability of the unique (viral) equilibrium E_* of the considered system (2).

Before addressing the global stability of E_*, let us firstly introduce the following lemma, which will be useful in the sequel.

Lemma 1: There is no periodic orbit within $\tilde{\Omega}$ for system (2).

Proof (Define):

$$h_1(I, P) = \eta_2 + (\beta\gamma - \delta - \mu)I - \beta\gamma PI - \beta\gamma I^2,$$

$$h_2(I, P) = \alpha + \eta_3 - \alpha I - (\alpha + \alpha_0 + \mu)P,$$

$$D(I, P) = \frac{1}{IP}.$$

In the interior of $\tilde{\Omega}$, one can get

$$\frac{\partial(Dh_1)}{\partial I} + \frac{\partial(Dh_2)}{\partial P}[0.2cm] = -\frac{\beta\gamma}{P} - \frac{\eta_2}{I^2\,P} - \frac{\eta_3 + \alpha(1-I)}{IP^2} < 0.$$

Thus, it follows from the Bendixson-Dulac criterion [28] that there is no periodic orbit in the interior of $\tilde{\Omega}$ for system (2).

After considering the interior area, let us move on to the boundary of $\tilde{\Omega}$. Assume that $(\tilde{I}, \tilde{P})$ is an arbitrary point on the boundary of $\tilde{\Omega}$. Then there are three possibilities to discuss.

1) Case 1: When $0 < \tilde{I} \leq 1, \tilde{P} = 0$. Then,

$$\left.\frac{dP}{dt}\right|_{(\tilde{I},\tilde{P})} = \eta_3 + \alpha(1 - \tilde{I}) > 0.$$

2) Case 2: When $0 < \tilde{P} \leq 1, \tilde{I} = 0$. Then,

$$\left.\frac{dI}{dt}\right|_{(\tilde{I},\tilde{P})} = \eta_2 > 0.$$

3) Case 3: When $\tilde{I} + \tilde{P} = 1, \tilde{I} \neq 0, \tilde{P} \neq 0$. Then,

$$\left.\frac{d\,(I+P)}{dt}\right|_{(\tilde{I},\tilde{P})} = -\eta_1 - \delta\tilde{I} - \alpha_0\tilde{P} < 0.$$

Hence, it follows from the above three cases that there is no periodic orbit passing through $(\tilde{I}, \tilde{P})$ for system (2). In summary, there is no periodic orbit within $\tilde{\Omega}$ for system (2). The proof is complete.

Now, let us consider the global stability of the unique (viral) equilibrium E_* of system (2).

Theorem 3: The unique (viral) equilibrium E_* is globally asymptotically stable for system (2).

Proof: According to the Theorems 1 and 2 and Lemma 1, it follows from the generalized Poincare-Bendixson theorem [28] that the unique (viral) equilibrium E_* is globally asymptotically stable for system (2). The proof is complete. □

Remark 2: Theorems 1-3 have displayed the fact that once malware appears in the cloud, it will always exist, and no matter what method is adopted, it cannot be completely eliminated. But from the representation of I_* in Theorem 1, one can observe the effect of some parameters on I_*. In other words, by adjusting these related parameters, the proportion of infected VMs can be reduced to a relatively low level. This also provide directional guidance to curb the spread of malware in the cloud.

IV. NUMERICAL SIMULATIONS

The previous sections have carried out a systematic description and theoretical analysis of the proposed dynamical propagation model of malware under IaaS architecture. This section is to give some numerical simulations for illustrating the obtained main results. The following examples are conducted with different conditions.

Example 1: Illustrate the effect of different initial values on system (1).

1) $(S(0), I(0), P(0)) = (0.5, 0.4, 0.1)$;
2) $(S(0), I(0), P(0)) = (0.6, 0.1, 0.3)$;
3) $(S(0), I(0), P(0)) = (0.3, 0.5, 0.2)$;
4) $(S(0), I(0), P(0)) = (0.2, 0.3, 0.5)$.

The common system parameters are listed in Table 2. On this basis, Fig. 5 demonstrates the time plots of system (1).

TABLE 2. The system parameters for Example 1.

Parameter	Value
η_1	0.045
η_2	0.035
η_3	0.02
μ	0.1
β	0.12
δ	0.03
γ	0.5
α	0.02
α_0	0.01

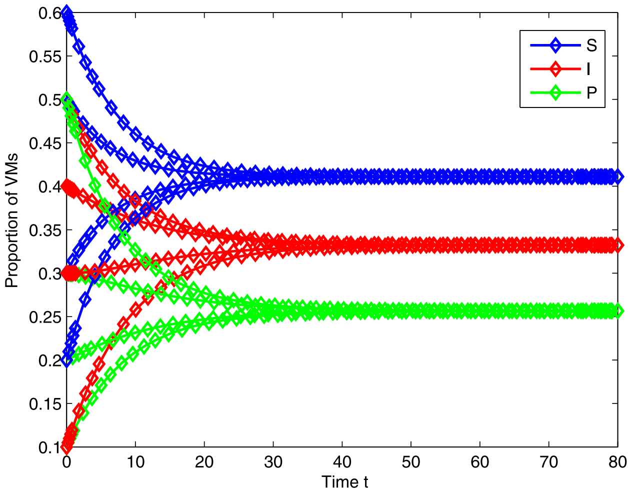

FIGURE 5. Time plots of system (1) under conditions given in Example 1.

Form Fig. 5, it is easy to see that no matter where the initial value starts, the curve of the same representation will eventually be close to the same level. This not only illustrates the global stability of the system (1), but also shows that the global stability is independent of the initial value. This is in good agreement with the result in Theorem 3. Therefore, by adjusting the initial value, it is impossible to control the the long-term propagation behavior of malware in the cloud.

Example 2: Illustrate the impact of different system parameters on system (1). The system parameters are shown in Table 3. The common initial condition is $(S(0), I(0), P(0)) = (0.5, 0.3, 0.2)$. *On this basis, Fig. 6 displays the time plots of system (1).*

TABLE 3. The system parameters for Example 2.

Parameter	Value 1	Value 2	Value 3
η_1	0.035	0.05	0.065
η_2	0.055	0.025	0.025
η_3	0.02	0.025	0.01
μ	0.1	0.1	0.1
β	0.15	0.18	0.12
δ	0.01	0.05	0.03
γ	0.5	0.4	0.4
α	0.02	0.02	0.02
α_0	0.05	0.01	0.02

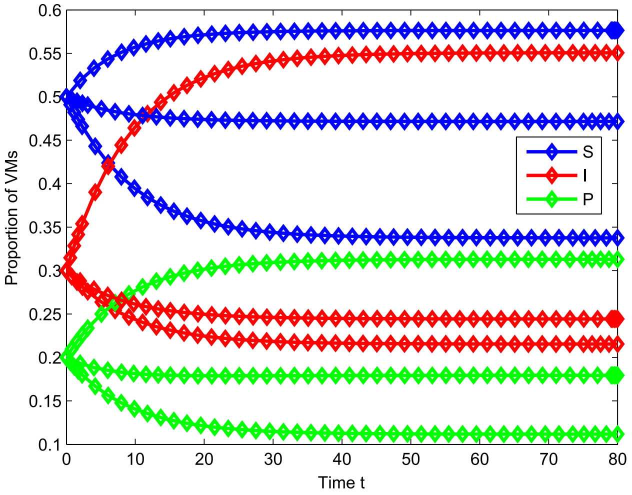

FIGURE 6. Time plots of system (1) under conditions given in Example 2.

In Fig. 6, three different systems under the same initial condition are compared. One can get the similar conclusions as in Example 1. But the curve of the same representation will approach different value. This means that system parameters can affect the propagation of malware in the cloud. Combining the actual physical meaning of the system parameters, one can find corresponding methods to prevent the spread of malware.

Example 3: Illustrate the global stability of the unique (viral) equilibrium of system (1). The system parameters are depicted in Table 4. On this basis, Fig. 7 shows the phase portrait of system (1).

TABLE 4. The system parameters for Example 3.

Parameter	Value
η_1	0.055
η_2	0.035
η_3	0.01
μ	0.1
β	0.15
δ	0.01
γ	0.2
α	0.02
α_0	0.05

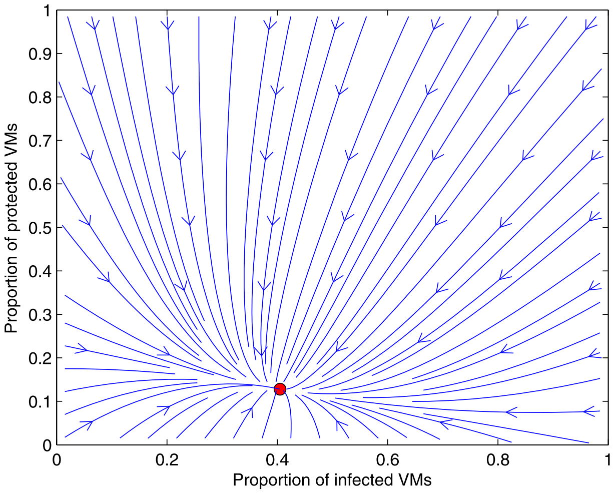

FIGURE 7. The phase portrait of system (1) under conditions given in Example 3.

Although the global stability of the unique (viral) equilibrium of system (1) can be seen in Figs. 5-6, in order to make the representation more intuitive, Fig. 7 gives a phase diagram of global stability, and the red point is the viral equilibrium. It is easy to obtain the similar result as in Examples 1 and 2.

Example 4: Illustrate the influence of different migration rate $\gamma = \{0.1, 0.3, 0.5, 0.7, 0.9\}$ *on system (1). The system parameters are given in Table 5. The common initial condition is* $(S(0), I(0), P(0)) = (0.5, 0.3, 0.2)$. *On this basis, Fig. 8 depicts time plots of proportion of infected VMs of system (1).*

Since the migration of VMs plays an important role in cloud computing, which has been described in the Introduction, Fig. 8 shows time plots of proportion of infected VMs with varied migration rate γ. From this figure, it can be seen that the higher the frequency of migration of VMs from

TABLE 5. The system parameters for Example 4.

Parameter	Value
η_1	0.008
η_2	0.006
η_3	0.006
μ	0.02
β	0.08
δ	0.01
α	0.01
α_0	0.03

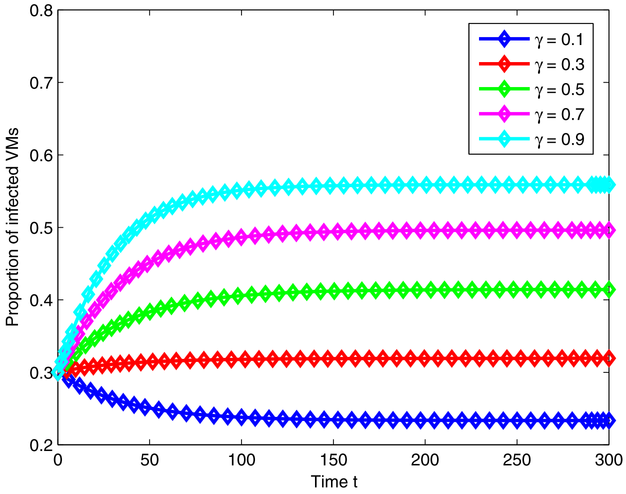

FIGURE 8. Time plots of proportion of infected VMs of system (1) with conditions given in Example 4.

physical machines, the greater the proportion of infected VMs in the cloud.

V. SUMMARY

In this paper, a dynamical propagation model of malware for cloud computing security has been proposed. To better understand how malware propagates in an infected cloud environment, a comprehensive analysis including the equilibrium and its stability for the proposed model has been conducted. It is found from the model analysis that once malware appears in a virtual network, it will always exist, and no matter what method is adopted, it cannot be completely eliminated. However, by adjusting system parameters, the proportion of infected VMs can be reduced to a relatively low level. Finally, some numerical simulations have been given to illustrate the obtained main results.

Although our work has achieved some results about the propagation behavior of malware under an infected cloud environment, in our view, there is still much work to do in the future. Firstly, our work has proved that the final level of infection depends on system parameters. But it is lack of further research on control strategies, which limits its practicality to a certain extent. Therefore, it is essential to study the specific control strategies (e.g., [29], [30]). In addition, it is worth trying to apply deep learning methods (e.g., [31], [32]) to explore the propagation behavior of malware in the cloud.

REFERENCES

[1] X. Wang, L. T. Wang, X. Xie, J. Jin, and M. J. Deen, "A cloud-edge computing framework for cyber-physical-social services," *IEEE Commun. Mag.*, vol. 55, no. 11, pp. 80–85, Nov. 2017.

[2] C. Zhu, J. J. P. C. Rodrigues, V. C. M. Leung, L. Shu, and L. T. Yang, "Trust-based communication for the industrial Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 16–22, Feb. 2018.

[3] X. Wang, L. T. Yang, H. Li, M. Lin, J. Han, and B. O. Apduhan, "NQA: A nested anti-collision algorithm for RFID systems," *ACM Trans. Embed. Comput. Syst.*, vol. 18, no. 4, p. 32, Jul. 2019.

[4] L. Kuang, L. T. Yang, X. Wang, P. Wang, and Y. Zhao, "A tensor-based big data model for QoS improvement in software defined networks," *IEEE Netw.*, vol. 30, no. 1, pp. 30–35, Jan. 2016.

[5] X. Wang, L. T. Yang, L. Kuang, X. Liu, Q. Zhang, and M. J. Deen, "A tensor-based big data-driven routing recommendation approach for heterogeneous networks," *IEEE Netw. Mag.*, vol. 33, no. 1, pp. 64–69, Jan. 2019.

[6] X. Zhu, J. Wang, H. Guo, D. Zhu, L. T. Yang, and L. Liu, "Fault-tolerant scheduling for real-time scientific workflows with elastic resource provisioning in virtualized clouds," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 12, pp. 3501–3517, Dec. 2016.

[7] C. Wueest. (2012). *Security for Virtualization: Finding the Right Balance*. Accessed: Jul. 15, 2015. [Online]. Available: www.kaspersky.co.uk/downloads/pdf/virtualization.pdf

[8] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," *Inf. Sci.*, vol. 305, pp. 357–383, Jun. 2015.

[9] P. D. Ezhilchelvan and I. Mitrani, "Evaluating the probability of malicious co-residency in public clouds," *IEEE Trans. Cloud Comput.*, vol. 3, no. 5, pp. 420–427, Jul. 2015.

[10] D. C. Marinescu, *Cloud Computing: Theory and Practice*, 2nd ed. London, U.K.: Elsevier, 2017.

[11] C. J. Chung, P. Khatkar, T. Xing, J. Lee, and D. Huang, "NICE: Network intrusion detection and countermeasure selection in virtual network systems," *IEEE Trans. Dependable Secure Comput.*, vol. 10, no. 4, pp. 198–211, Jul. 2013.

[12] F. Abazari, M. Analou, and H. Takabi, "Effect of anti-malware software on infectious nodes in cloud environment," *Comput. Secur.*, vol. 58, pp. 139–148, May 2016.

[13] T. Katsuki. (2014). *Crisis the Advanced Malware*. Accessed: Jul. 15, 2015. [Online]. Available: www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/crisis_the_advanced_malware.pdf

[14] J. Latanicki, P. Massonet, S. Naqvi, B. Rochwerger, and M. Villari, "Scalable cloud defenses for detection, analysis and mitigation of DDoS attacks," in *Towards the Future Internet*. 2010.

[15] W. A. Jansen, "Cloud hooks: Security and privacy issues in cloud computing," in *Proc. 44th Hawaii Int. Conf. Syst. Sci. (HICSS)*, Jan. 2011, pp. 1–10.

[16] M. Balduzzi, J. Zaddach, D. Balzarotti, E. Kirda, and S. Loureiro, "A security analysis of Amazon's elastic compute cloud service," in *Proc. 27th Annu. ACM Symp. Appl. Comput.*, 2012, pp. 1427–1434.

[17] C. Wueest. (2014). *Threats to Virtual Environments*. Accessed: Jul. 15, 2015. [Online]. Available: www.symantec.com/content/en/us/enterprise/media/ security_response/whitepapers/threats_to_virtual_environments.pdf

[18] J. Li, B. Li, T. Wo, C. Hu, J. Huai, L. Liu, and K. P. Lam, "Cyberguarder: A virtualization security assurance architecture for green cloud computing," *Future Gener. Comput. Syst.*, vol. 28, no. 2, pp. 379–390, Feb. 2012.

[19] S. A. Zonouz, K. R. Joshi, and W. H. Sanders, "Cost-aware systemwide intrusion defense via online forensics and on-demand detector deployment," in *Proc. 3rd ACM Workshop Assurable Usable Secur. Configuration*, 2010, pp. 71–74.

[20] Z. Zuo, Q. Zhu, and M. Zhou, "On the time complexity of computer viruses," *IEEE Trans. Inf. Theory*, vol. 51, no. 8, pp. 2962–2966, Aug. 2005.

[21] L. Feng, X. Liao, Q. Han, and H. Li, "Dynamical analysis and control strategies on malware propagation model," *Appl. Math. Model.*, vol. 37, nos. 16–17, pp. 8225–8236, Sep. 2013.

[22] C. Gan, X. Yang, W. Liu, and Q. Zhu, "A propagation model of computer virus with nonlinear vaccination probability," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, pp. 92–100, Jan. 2014.

[23] J. Ren, J. Liu, and Y. Xu, "Modeling the dynamics of a network-based model of virus attacks on targeted resources," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 31, no. 1, pp. 1–10, Feb. 2016.

[24] B. K. Mishra, K. Haldar, and D. N. Sinha, "Impact of information based classification on network epidemics," *Sci. Rep.*, vol. 6, Jun. 2016, Art. no. 28289.

[25] 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.

[26] Y. Yao, C. Sheng, Q. Fu, H. Liu, and D. Wang, "A propagation model with defensive measures for PLC-PC worms in industrial networks," *Appl. Math. Model.*, vol. 69, pp. 696–713, May 2019.

[27] G. C. Layek, *An Introduction to Dynamical Systems and Chaos*. Springer, 2015.

[28] R. C. Robinson, *An introduction to Dynamical Systems: Continuous and Discrete*. Upper Saddle River, NJ, USA: Prentice-Hall, 2004.

[29] Q. Zhu, X. Yang, L.-X. Yang, and C. Zhang, "Optimal control of computer virus under a delayed model," *Appl. Math. Comput.*, vol. 218, no. 23, pp. 11613–11619, Aug. 2012.

[30] C. Gan, M. Yang, Z. Zhang, and W. Liu, "Global dynamics and optimal control of a viral infection model with generic nonlinear infection rate," *Discrete Dyn. Nature Soc.*, vol. 2017, Feb. 2017, Art. no. 7571017.

[31] Z. Zhang, C. Wang, C. Gan, S. Sun, and M. Wang, "Automatic modulation classification using convolutional neural network with features fusion of SPWVD and BJD," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 5, no. 3, pp. 469–478, Sep. 2019.

[32] C. Gan, L. Wang, Z. Zhang, and Z. Wang, "Sparse attention based separable dilated convolutional neural network for target entities sentiment analysis," *Knowl.-Based syst.*, vol. 188, 10487, Jan. 2020.

CHENQUAN GAN received the B.S. degree from the Department of Mathematics, Inner Mongolia Normal University, Huhhot, China, in 2010, and the Ph.D. degree from the Department of Computer Science, Chongqing University, Chongqing, China, in 2015. He is currently an Associate Professor with the School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications (CQUPT), Chongqing. His research interests include difference equations, computer virus propagation dynamics, and deep learning.

QINGDONG FENG received the B.E. degree in electronic and information engineering from Sichuan Normal University, Sichuan, China, in 2016. He is currently pursuing the master's degree in electronic and communication engineering with the Chongqing University of Posts and Telecommunications, Chongqing, China. His research interests include computer virus propagation dynamics and sentiment analysis.

XULONG ZHANG received the M.Sc. and Ph.D. degrees from the College of Computer Science, Chongqing University, in 2011 and 2017, respectively. He is currently a Lecturer with the School of Computer and Network Engineering, Shanxi Datong University, Datong, China. He has published more than five academic articles in peer-reviewed international journals. His research interests include computer virus propagation dynamics, wireless sensor networks, and big data.

ZUFAN ZHANG received the B.Eng. and M.Eng. degrees from the Chongqing University of Post and Telecommunications (CQUPT), Chongqing, China, in 1995 and 2000, respectively, and the Ph.D. degree in communications and information systems from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2007. From February 2011 to January 2012, he was a Visiting Professor with the Centre for Wireless Communications (CWC), Oulu of University, Finland. He is currently a Professor with the School of Communication and Information Engineering, CQUPT. His current main research interest concerns wireless and mobile communication networks.

QINGYI ZHU received the B.E. and Ph.D. degrees from the College of Computer Science, Chongqing University, in 2009 and 2014, respectively. He is currently an Associate Professor with the Chongqing University of Posts and Telecommunications, China. He has published more than 20 academic articles in peer-reviewed international journals. His current research interests include cybersecurity dynamics, complex systems, and blockchain. He has also served as an invited reviewer for various international journals and conferences.