IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 24, 2020, accepted April 17, 2020, date of publication April 23, 2020, date of current version May 14, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2989612

Interplay Between Malware Epidemics and Honeynet Potency in Industrial Control System Network

QIANG FU[1,2], YU YAO[1,2], CHUAN SHENG[1,2], AND WEI YANG[3]

[1] College of Computer Science and Engineering, Northeastern University, Shenyang 110169, China
[2] Engineering Research Center of Security Technology of Complex Network System, Ministry of Education, Shenyang 110169, China
[3] Software College, Northeastern University, Shenyang 110169, China

Corresponding author: Yu Yao (yaoyu@mail.neu.edu.cn)

This work was supported in part by the Key Research and Development Program of Liaoning Province under Grant 2019JH2/10100019, and in part by the Fundamental Research Funds for the Central Universities under Grant N181606001, Grant N2016011, and Grant N2024005-1.

ABSTRACT The Industrial Control System (ICS) is widely used in industrial processes, such as power grids, water conservancy, natural gas, petrochemical and so on. More and more cyber attacks are targeting the ICS worldwide. This paper presents a novel honeynet-based epidemic model in ICS network. The honeynet is an active approach that can attract malware attacks and provide sample information and immunization strategy of the malware. An epidemic model with immunization and quarantine in ICS network is formulated to explore the dynamics of the malware propagation, and the honeynet potency is analyzed as well. Theoretical analysis reveals the disease-free and endemic equilibrium of our model, then the local and global stability of the disease-free (endemic) equilibrium are examined by the basic reproduction number. Furthermore, numerical experiments show that the honeypot with more system vulnerabilities is conducive to suppress the malware epidemic, and the honeynet with lower average degree power low index can be more effectively. In addition, simulation experiments provide the actual behavior of malware propagation in the ICS network and verification of our derivations.

INDEX TERMS ICS network, honeynet, malware propagation model, epidemic dynamics, simulation.

I. INTRODUCTION

A. MOTIVATION

With deep application of the Industrial Control Systems (ICS), ICS network security plays a more and more important role in nowadays. A growing number of cybersecurity incidents indicate that ICS is becoming increasingly susceptible to sophisticated and targeted attacks, and malware plays an important role in the attacks against ICS. ICS usually cover three major types of control systems, namely Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), and Programmable Logic Controller (PLC). Due to the weak network security awareness of the ICS and the extremely high requirements for real-time, reliability and continuity of the industrial control business, ICS security products can not be deployed and used at large scale at this stage. Under the premise of not affecting the current business reliability and network structure, how to carry out ICS security detection, prediction and response is a research hotspot. Nowadays, with the development of industrial informatization, to facilitate operations by engineers, ICS networks are often not physically isolated from external networks. Then protocols and devices used by ICS are often intended to be vulnerable to various cyber-attacks. For instance, the Bushehr Nuclear Power Plant in Iran was attacked by the malicious worm Stuxnet [1], that remind people the serious harm of worms to industry. After that, many cyber-attacks that against ICS network broke out, such as Modbus Stager [2], PLC Blaster [3], Duqu [4] and so on. Especially, PLC Blaster can live solely in PLCs and they can propagate through the control system of Siemens SIMATIC S7−1200 without any computers involved. PLC Blaster can scan ICS network for new targets, attack the PLCs, and replicate itself in the compromised PLCs [3]. The appearance of PLC

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

Blaster means that the security situation of ICS is becoming increasingly severe.

The conventional techniques against malware intrusion are usually based on a known set of malware samples [14]. Since the ICS network is different with the internet and the system can not stop running optionally, restarting and patching are not very suitable methods for ICS network security. However, the honeypot technology provides an approach to solve this problem and it brings a great innovation in ICS network security. The honeypot does not impact the normal operation of the ICS, it is essentially a technique of deceiving an attacker. By arranging some hosts, network services or information as bait, the attacker is induced to attack them, so that the attack behavior can be captured and analyzed. The honeypot can elucidate the malware's characteristics by monitoring and analyzing the attacks, so that it will provide feedback about immunization strategy to defenders. Meanwhile, attacks captured by honeypots can also serve as an "early warning" system for defenders, it can provide more time to deal with the attacks and waste the attacker's time and resources. Based on honeypots, the honeynet is a network system rather than a single honeypot, it looks more like an ordinary network. Usually, the honeynet consists of a large number of honeypots, it is "a security resource whose value lies in being probed, attacked and compromised" [16]. The honeynet does not depend on any specific ICS architecture, and it can respond to attacks to gain information more efficiently. The state of art of study researches that deals with honeynet to get enhance information security against ICS or Internet of things (IoT) system attacks [32]. Even though there are quite a few ways to evade those attacks, there is a crucial need for one which can turn table on attacker by using active approach. Honeynet is a very suitable solution [33].

B. LITERATURE REVIEW

Currently, most studies about honeynet focus on its technology level, such as data capture [16], information collection [17] and virtualization technology [18]. Ren and Xu [19] propose a compartmental model to explore the interplay between disease epidemics and honeynet potency. However, the interplay between disease epidemics and honeynet needs more appropriate discussions, and the communicating rate $\Theta_{ij}(t)$ is neglected in the model, it is exactly an important factor in the coupled complex networks. Honeynet in a systematic framework about malware epidemic has not been widely discussed in ICS network. The dynamics in honeynet is more complicated than that in honeypots. So it is necessary to model and discuss the way that malware spread in a honeynet, the study will help to inhibit the malware propagation, design and deploy the honeynet more effectively and economically.

In the past decades, some traditional epidemic models of infectious diseases are used to describe the propagation of Internet worms [5], the SIS model [6] and SIR model [7] have been proposed later inspired by human infectious disease. Then mathematical models [8]–[12] inspired by the SIR model have been employed to inhibit the spread of worms. In addition, some approaches to detect and constrain malware have been studied, such as firewall, intrusion detection system (IDS) and benign worms defending system [13]. By using mathematical models and computational methods, epidemic dynamics on complex networks has been studied [20]–[22]. And some studies have shown that the topology (such as average degree and power-law index) of networks has significant influence on the propagation of malware [23]–[26]. Wang *et al.* [27] investigate an epidemic propagation on the three-layer interdependent networks, their analysis provides a basic framework for better understanding of epidemic propagation on multi-layered complex networks. A general formal study to obtain the reproduction number and discuss the positivity and stability properties of equilibrium points is proposed and formally discussed [34]. Existence and stability of equilibrium points of the models have been extensively studied [35], [36]. Consequently, epidemic models about malwares is used for reference in our study.

C. PAPER ORGANIZATION

Inspired by the mentioned works above, we propose an epidemic model in the ICS network to study the interplay between malware epidemics and honeynet potency. This paper is organized as follows. Section II introduces a honeynet-based malware propagation model in a two-layer (ICS network and honeynet) complex network. Section III analyzes the epidemic dynamics of our proposed malware propagation system, the disease-free equilibrium, endemic equilibrium and stability are discussed in detail. Numerical and simulation experiments are showed in Section IV and Section V, respectively. Section VI presents the discussion and conclusion for this paper.

II. MODEL FORMULATION

In this section, we aim to formulate an epidemic model with quarantine strategy. Since the two networks (ICS network and honeynet) are connected in some way, a two-layer, coupled network is formed. The basic topology of the two-layer complex network is shown in Figure 1. Each PLC (resp. honeypot) has two types of link-degrees: internal degrees and external degrees. Some models have introduced quarantine strategy into epidemic dynamics, but they are only suitable for a single-layer network [31]. We assume that the PLCs and honeypots in ICS network are the nodes, the links represent the communication relationships among the nodes. Total network size is fixed, and the nodes are divided into two categories, namely, PLCs and honeypots with respective network sizes N_p and N_H.

A. THE PROPAGATION OF MALWARE AMONG PLCS

In our model, the PLC is partitioned into four compartments depending on the states of the nodes under malware attacks: *susceptible* state (S_p, which denotes the number of PLCs vulnerable to malware attacks), *infected* state (I_p, which denotes the number of infected PLCs), *quarantined* state (Q_p, which denotes the number of quarantined PLCs) and *recovered* state

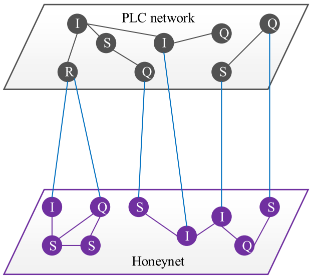


FIGURE 1. Topology of the two-layer complex network.

(R_p, which represents the number of PLCs that recovered after infection). At every time step, the susceptible PLCs can be infected by the infected PLCs at a rate β_{11}, and the infected PLCs can be restored by using anti-malware software or installing patches at a rate φ_1. In some cases the patches are temporary and they may be loss of function if the system is updated or the malware is mutated. When the malware -variants or unknown malwares appear, recovered PLCs may change to susceptible PLCs at a rate δ_1.

B. THE PROPAGATION OF MALWARE AMONG HONEYPOTS

A honeypot is designed to trap the malwares using the system vulnerabilities, such as opening a service port and proceeding without system patches, thus, the honeypot has two obvious facts [19]. Firstly, an infected honeypot can not infect other connected nodes, including the PLCs and honeypots. Meanwhile, the honeypot is designed to attract the malware attacks, so a honeypot is not immune to malware attacks. However, a honeypot can be quarantined at a rate φ_2. Thus, the honeypot can be in three states: *susceptible* state (S_H, which denotes the number of uninfected honeypots with seductive baits), *infected* state (I_H, which denotes the number of infected honeypots that have successfully captured the malware samples), *quarantined* state (Q_H, which denotes the number of quarantined honeypots). And by reinstalling the system, the honeypot in quarantined state can become susceptible state again at a rate δ_2.

C. INTERACTION BETWEEN HONEYPOTS AND PLCS

In the honeynet context, an infected PLC can infect the honeypot in susceptible state at a rate β_{22}. As it is mentioned above, an infected honeypot can never infect other PLCs, so susceptible nodes can only be infected by the infected PLCs. However, the infected honeypot can capture the malware samples. Once the information related to a malware sample is captured by a honeypot, quarantine strategy for PLCs can be carried out and the PLCs in susceptible state will be quarantined at a rate β_{12}. Then the specific immunization measures to counter the malware should be taken, thus, a part of quarantined PLCs will turn to recovered states at a rate ω.

We assume our model into a heterogeneous honeynet. Then a two-layer complex network which the node degree distribution follows a power law ($P(k) = k^{-\gamma}$) is formed, where $P(k)$ stands for the probability that a randomly chosen node within the network has degree k pointing to this node. For a PLC, we use (i, j) to denote its degree, which means it is connected with i (internal) other PLC nodes and j (external) honeypot nodes. Similarly, for a honeypot, the degree (k, l) means that it is connected with k (internal) honeypot nodes and l (external) PLC nodes. The maximum node degree of the network is $n_{11} = \max_{alli}\{i\}$, $n_{12} = \max_{allj}\{j\}$, $n_{21} = \max_{allk}\{k\}$ and $n_{22} = \max_{alll}\{l\}$. We further define $P_P(i, j)$ and $P_H(k, l)$ as the joint degree distribution in PLCs and honeypots, respectively. And marginal degree distributions are

$$\begin{aligned} P_P(i,j) &= \frac{N^P_{i,j}}{N^P}, \\ P_H(k,l) &= \frac{N^H_{k,l}}{N^H}. \end{aligned} \tag{1}$$

The average degree values are as follows:

$$\begin{aligned} <k>_{11} &= \sum_{i=0}^{n_{11}} iP_P(i,\cdot),\ <k>_{12} = \sum_{j=0}^{n_{12}} jP_P(\cdot,j) \\ <k>_{21} &= \sum_{k=0}^{n_{21}} kP_H(k,\cdot),\ <k>_{22} = \sum_{l=0}^{n_{22}} lP_H(\cdot,l) \\ <k^2>_{11} &= \sum_{i=0}^{n_{11}} i^2P_P(i,\cdot),\ <k^2>_{12} = \sum_{j=0}^{n_{12}} j^2P_P(\cdot,j) \\ <k^2>_{21} &= \sum_{k=0}^{n_{21}} k^2P_H(k,\cdot),\ <k^2>_{22} = \sum_{l=0}^{n_{22}} l^2P_H(\cdot,l) \end{aligned} \tag{2}$$

numbers with node degree k at time t, respectively. Note that there is no recovered state for the honeypots. That is because a honeypot is designed to attract the malware attacks, no honeypots are immune to the malware attacks. Thus, the total number of common nodes and honeypots over the network with degree k at time t is

$$\begin{aligned} N^P_{i,j} &= S^P_{i,j}(t) + I^P_{i,j}(t) + Q^P_{i,j}(t) + R^P_{i,j}(t), \\ N^H_{k,l} &= S^H_{k,l}(t) + I^H_{k,l}(t) + Q^H_{k,l}(t). \end{aligned}$$

Then we have the following equations:

$$\begin{aligned} \sum_{i=0}^{n_{11}}\sum_{j=0}^{n_{12}} N^P_{i,j} &= N^P, \\ \sum_{k=0}^{n_{21}}\sum_{l=0}^{n_{22}} N^H_{k,l} &= N^H. \end{aligned} \tag{3}$$

In our model, we assume that the connectivity of nodes is uncorrelated. Thus, for susceptible PLCs, the probability of communicating with infected PLCs is:

$$\Theta_{11}(t) = \frac{1}{<k>_{11}} \sum_{i=0}^{n_{11}}\sum_{j=0}^{n_{12}} iP_P(i,j)I^P_{i,j}(t), \tag{4}$$

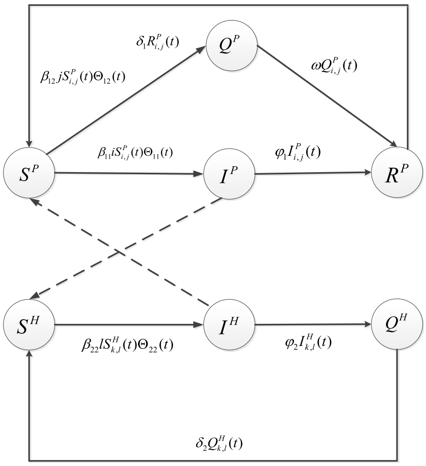


FIGURE 2. The transition diagram among the states of the nodes in the two-layer complex network.

and the probability of communicating with susceptible honeypots is:

$$\Theta_{12}(t) = \frac{1}{<k>_{22}} \sum_{k=0}^{n_{21}} \sum_{l=0}^{n_{22}} l P_H(k,l)\, I^H_{k,l}(t), \tag{5}$$

Similarly, for susceptible honeypots, the probability of communicating with infected honeypots is:

$$\Theta_{21}(t) = \frac{1}{<k>_{21}} \sum_{k=0}^{n_{21}} \sum_{l=0}^{n_{22}} k P_H(k,l) I^H_{k,l}(t), \tag{6}$$

and the probability of communicating with infected PLCs is:

$$\Theta_{22}(t) = \frac{1}{<k>_{12}} \sum_{l=0}^{n_{21}} \sum_{k=0}^{n_{22}} j P_P(i,j) I^P_{i,j}(t). \tag{7}$$

The transition diagram among the states of the nodes in the two-layer complex network is showed in Figure 2 according to the transition relationship and formulations.

$$\begin{cases} \dfrac{dS^P_{i,j}(t)}{dt} = \delta_1 R^P_{i,j}(t) - \beta_{11} i S^P_{i,j}(t)\Theta_{11}(t) - \beta_{12} j S^P_{i,j}(t)\Theta_{12}(t) \\ \dfrac{dI^P_{i,j}(t)}{dt} = \beta_{11} i S^P_{i,j}(t)\Theta_{11}(t) - \varphi_1 I^P_{i,j}(t) \\ \dfrac{dQ^P_{i,j}(t)}{dt} = \beta_{12} j S^P_{i,j}(t)\Theta_{12}(t) - \omega Q^P_{i,j}(t) \\ \dfrac{dR^P_{i,j}(t)}{dt} = \varphi_1 I^P_{i,j}(t) + \omega Q^P_{i,j}(t) - \delta_1 R^P_{i,j}(t) \\ \dfrac{dS^H_{k,l}(t)}{dt} = -\beta_{22} l S^H_{k,l}(t)\Theta_{22}(t) + \delta_2 Q^H_{k,l}(t) \\ \dfrac{dI^H_{k,l}(t)}{dt} = \beta_{22} l S^H_{k,l}(t)\Theta_{22}(t) - \varphi_2 I^H_{k,l}(t) \\ \dfrac{dQ^H_{k,l}(t)}{dt} = \varphi_2 I^H_{k,l}(t) - \delta_2 Q^H_{k,l}(t) \end{cases} \tag{8}$$

TABLE 1. Notations in the paper.

Notation	Definition
N^P	total number of PLCs
N^H	total number of honeypots
$N^A_{i,j}$	number of PLCs whose degree is (*i, j*) at all times
$N^B_{k,l}$	number of honeypots whose degree is (*k, l*) at all times
$S^P_{i,j}(t)$	number of susceptible PLCs whose degree is (*i, j*) at time *t*
$I^P_{i,j}(t)$	number of infected PLCs whose degree is (*i, j*) at time *t*
$Q^P_{i,j}(t)$	number of quarantined PLCs whose degree is (*i, j*) at time *t*
$R^P_{i,j}(t)$	number of recovered PLCs whose degree is (*i, j*) at time *t*
$S^H_{k,l}(t)$	number of susceptible honeypots whose degree is (*k, l*) at time *t*
$I^H_{k,l}(t)$	number of infected honeypots whose degree is (*k, l*) at time *t*
$Q^H_{k,l}(t)$	number of quarantined honeypots whose degree is (*k, l*) at time *t*
β_{11}	infection rate of susceptible PLCs that are infected by PLCs
β_{12}	quarantine rate of susceptible PLCs
β_{22}	infection rate of susceptible honeypots that are infected by PLCs
φ_1	recovery rate of infected PLCs
φ_2	quarantine rate of infected honeypots
δ_1	rate at which the recovered PLCs lose immunity
δ_2	redeployed rate of the quarantined honeypots
ω	recovery rate of quarantined PLCs

III. EQUILIBRIUM AND STABILITY ANALYSIS OF THE MODEL

The dynamical behaviors of (8) proposed in Section II is studied in this section. An equilibrium of (8) under which the malware remain epidemics or become extinct is determined, that is, the *disease-free equilibrium* and *endemic equilibrium*. Then the local and global stability of the disease-free (endemic) equilibrium is examined by the basic reproduction number R_0.

A. DISEASE-FREE EQUILIBRIUM

For PLCs and the honeypots, we have

$$\begin{aligned} S^P_{i,j}(t) + I^P_{i,j}(t) + Q^P_{i,j}(t) + R^P_{i,j}(t) &= N^P, \\ S^H_{k,l}(t) + I^H_{k,l}(t) + Q^H_{k,l}(t) &= N^H. \end{aligned} \tag{9}$$

$$P_A(i,j) = \frac{N^P_{i,j}}{N^P}, \quad P_B(k,l) = \frac{N^H_{k,l}}{N^H}. \tag{10}$$

To express the disease-free equilibrium, we set all equations in (8) to be zero with $I^P_{i,j}(t) = 0$ for all i and j, and $I^H_{k,l}(t) = 0$ for all k and l. Then we have

$\Theta_{11}(t) = \Theta_{12}(t) = \Theta_{21}(t) = \Theta_{22}(t) = 0$, and

$$\begin{cases} \delta_1 R^P_{i,j}(t) = 0 \\ -\omega Q^P_{i,j}(t) = 0 \\ \omega Q^P_{i,j}(t) - \delta_1 R^P_{i,j}(t) = 0 \\ \delta_2 Q^H_{k,l}(t) = 0 \end{cases}. \tag{11}$$

Obviously, the disease-free equilibrium is $E^0\left(S_{i,j}^{P^0}, I_{i,j}^{P^0}, Q_{i,j}^{P^0}, R_{i,j}^{P^0}, S_{k,l}^{H^0}, I_{k,l}^{H^0}, Q_{k,l}^{H^0}\right)$, where

$$\begin{cases} S_{i,j}^{P*}(t) = N^P, I_{i,j}^{P*}(t) = 0, Q_{i,j}^{P*}(t) = 0, R_{i,j}^{P*}(t) = 0 \\ S_{k,l}^{H*}(t) = N^H, I_{k,l}^{H*}(t) = 0, Q_{k,l}^{H*}(t) = 0, \end{cases}$$

and

$$\begin{aligned} i &= 1, 2, \cdots, n_{11}, \\ j &= 1, 2, \cdots, n_{12}, \\ k &= 1, 2, \cdots, n_{21}, \\ l &= 1, 2, \cdots, n_{22}. \end{aligned}$$

B. ENDEMIC EQUILIBRIUM

The endemic equilibrium means that there are no more state changes in our model, and infected PLCs and honeypots are present in the complex network. In our model, the endemic equilibrium is equivalent to setting all equations in (8) to be zero (no more state changes), which will lead to the following equations,

$$\begin{cases} \delta_1 R_{i,j}^P(t) - \beta_{11} i S_{i,j}^P(t)\Theta_{11}(t) - \beta_{12} j S_{i,j}^P(t)\Theta_{12}(t) = 0 \\ \beta_{11} i S_{i,j}^P(t)\Theta_{11}(t) - \varphi_1 I_{i,j}^P(t) = 0 \\ \beta_{12} j S_{i,j}^P(t)\Theta_{12}(t) - \omega Q_{i,j}^P(t) = 0 \\ \varphi_1 I_{i,j}^P(t) + \omega Q_{i,j}^P(t) - \delta_1 R_{i,j}^P(t) = 0 \\ -\beta_{22} l S_{k,l}^H(t)\Theta_{22}(t) + \delta_2 Q_{k,l}^H(t) = 0 \\ \beta_{22} l S_{k,l}^H(t)\Theta_{22}(t) - \varphi_2 I_{k,l}^H(t) = 0 \\ \varphi_2 I_{k,l}^H(t) - \delta_2 Q_{k,l}^H(t) = 0. \end{cases}$$

However, since there are infectious nodes, the condition $I_{i,j}^P(t) = 0$ and $I_{k,l}^H(t) = 0$ do not hold anymore. Instead, $I_{i,j}^P(t)$ and $I_{k,l}^H(t)$ are now of some positive values. Thus, all the derivatives on the left of equal sign in (8) are set to be zero and assuming given $I_{i,j}^{P*}$ and $I_{i,j}^{H*}$, then we can derive the endemic equilibrium point: $E^*\left(S_{i,j}^{P*}, I_{i,j}^{P*}, Q_{i,j}^{P*}, R_{i,j}^{P*}, S_{k,l}^{H*}, I_{k,l}^{H*}, Q_{k,l}^{H*}\right)$, where

$$\begin{cases} S_{i,j}^{P*}(t) = \dfrac{\varphi_1}{\beta_{11} i \Theta_{11}(t)} I_{i,j}^{P*}(t) \\ Q_{i,j}^{P*}(t) = \dfrac{\varphi_1 \beta_{22} l \Theta_{22}(t)}{\omega \beta_{11} i \Theta_{11}(t)} I_{i,j}^{P*}(t) \\ R_{i,j}^{P*}(t) = \dfrac{\varphi_1 \beta_{11} i \Theta_{11}(t) + \varphi_1 \beta_{22} l \Theta_{22}(t)}{\delta_1 \beta_{11} i \Theta_{11}(t)} I_{i,j}^{P*}(t) \\ S_{k,l}^{H*}(t) = \dfrac{\varphi_2}{\beta_{22} l \Theta_{22}(t)} I_{k,l}^{H*}(t) \\ Q_{k,l}^{H*}(t) = \dfrac{\varphi_2}{\delta_2} I_{k,l}^{H*}(t). \end{cases} \tag{12}$$

C. STABILITY OF THE MODEL

To analyze the stability of the model, we calculate the basic reproduction number R_0 in this subsection. The basic reproduction number R_0 is an important threshold parameter in epidemiology, which is "the expected number of secondary cases produced, in a completely susceptible population, by a typical infective individual" [27]. Driessche *et al.* depict a general compartmental disease transmission model suited to heterogeneous populations and demonstrate a detailed calculation method of the basic reproduction number [28]. It is shown that, if $R_0 < 1$, then the malware will be extinct; whereas if $R_0 > 1$, there will exist an endemic equilibrium. For a heterogeneous population, R_0 is characterized as the spectral radius of the next generation matrix. Driessche and Watmough [29] put forward a general compartmental disease transmission model suitable to heterogeneous populations and illustrated a detailed calculation method of R_0. Because the joint degree distributions are assumed independent in this paper, thus,

$$\begin{aligned} P_P(i,j) &= P_P(i,\cdot)\, P_P(\cdot,j), \\ P_H(k,l) &= P_H(k,\cdot)\, P_H(\cdot,l). \end{aligned} \tag{13}$$

For briefness, we denote $i_{0,0}^P = y_1, \ldots, i_{0,n_{12}}^P = y_{n_{12}+1}$, $i_{1,0}^P = y_{n_{12}+2}, \ldots, i_{1,n_{12}}^P = y_{2n_{12}+2}, \ldots, i_{n_{11},0}^P = y_{n_{11}(n_{12}+1)+1}, \ldots, i_{n_{11},n_{12}}^P = y_{(n_{11}+1)(n_{12}+1)}$. Similarly, $i_{0,1}^H = y_{(n_{11}+1)(n_{12}+1)+1}, \ldots, i_{n_{21},n_{22}}^H = y_n$, where $n = (n_{11}+1)(n_{12}+1) + (n_{21}+1)(n_{22}+1)$. Also, it is denoted that $f = (f_1, f_2, \cdots, f_n)$, where f_i represents the rate of change of infection compartment i and $dy(t)/dt = f(y(t))$. Obviously, when the disease-free equilibrium E^0 is obtained, $y_i = 0$, $i = 1, \cdots, n$. Then the basic reproduction number of model is $R_0 = \rho(\mathbf{\Gamma})$, where $\rho(\mathbf{\Gamma})$ is the spectral radius of matrix $\mathbf{\Gamma}$ [30], and

$$\mathbf{\Gamma} = \mathbf{F}\mathbf{V}^{-1}. \tag{14}$$

$\mathbf{F}$ is the rate of new occurring infections, $\mathbf{V}$ is a diagonal matrix, and it is the rate of transferring individuals out of the original group, and $\rho(\mathbf{\Gamma})$ is the spectral radius of the next generation matrix $\mathbf{\Gamma}$. $\mathbf{\Gamma}$ is a complex matrix:

$$\mathbf{\Gamma} = \begin{pmatrix} (\mathbf{A}_{i,j})_{(n_{11}+1)\times(n_{11}+1)} & (\mathbf{B}_{i,j})_{(n_{11}+1)\times(n_{21}+1)} \\ (\mathbf{C}_{i,j})_{(n_{21}+1)\times(n_{11}+1)} & (\mathbf{D}_{i,j})_{(n_{21}+1)\times(n_{21}+1)} \end{pmatrix}, \tag{15}$$

where $\mathbf{A}_{i,j}$, $\mathbf{B}_{i,j}$, $\mathbf{C}_{i,j}$ and $\mathbf{D}_{i,j}$ are block matrices, and each element of them represents a sub-matrix satisfying is obtained by the equation as shown at the bottom of next page. Through a series of similarity transformations, matrix (15) can be simplified to is obtained by the equation as shown at the bottom of next page.

Because the joint degree distributions are independent in our model, through a series of transformations, matrix (15) can be further simplified to:

$$\mathbf{\Gamma} = \begin{bmatrix} \frac{\beta_{11}<k^2>_{11}}{\varphi_1<k>_{11}} & \frac{\beta_{11}}{\varphi_1} < k >_{12} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{\beta_{22}}{\varphi_2} < k >_{21} & \frac{\beta_{22}<k^2>_{22}}{\varphi_2<k>_{22}} \end{bmatrix}. \tag{16}$$

$\mathbf{E}$ is the unit matrix of (16), then let

$$|\lambda\mathbf{E} - \mathbf{\Gamma}| = 0, \tag{17}$$

and we can calculate the eigenvalues of matrix (17),

$$\lambda_1 = \frac{\beta_{11} < k^2 >_{11}}{\varphi_1 < k >_{11}}, \quad \lambda_2 = \frac{\beta_{22} < k^2 >_{22}}{\varphi_2 < k >_{22}}. \tag{18}$$

According to paper [29],

$$R_0 = \rho(\mathbf{\Gamma}) = \max\{|\lambda_1|, |\lambda_2|\}. \tag{19}$$

Since $\mathbf{\Gamma}$ is a nonnegative matrix, and according to Perron–Frobenius theorem, $R_0 = \max\{|\lambda_1|, |\lambda_2|\}$ is a positive eigenvalue of matrix $\mathbf{\Gamma}$. Based on [28], Chavez *et al.* outline the second generation operator approach developed and collaborators for the computation of the basic reproductive number [37], it is denoted that $s(\mathbf{F} - \mathbf{V}) = \max\{Re\lambda_i\}$, where λ_i is an eigenvalue of $\mathbf{\Gamma}$ and $Re\lambda_i$ is the real part of λ_i. In paper, the following formula is given,

$$s(\mathbf{F} - \mathbf{V}) \leq 0 \Leftrightarrow \rho(\mathbf{F}\mathbf{V}^{-1}) < 1,$$
$$s(\mathbf{F} - \mathbf{V}) > 0 \Leftrightarrow \rho(\mathbf{F}\mathbf{V}^{-1}) > 1.$$

The results in paper [28] are suited to heterogeneous group, and the PLCs and honeypots in our model are heterogeneous and the coupled network in our model is a heterogeneous complex network, so the results of [28] are applicable to our model. Therefore, we can obtain the following theorems.

Theorem 1: If the basic reproduction number $R_0 < 1$, the disease-free equilibrium E^0 is locally asymptotically stable; if $R_0 > 1$, E^0 is unstable. Then the positivity and boundedness of the solutions of (8) are examined.

Theorem 2: For (8), the set

$$\Omega \equiv \{y = \{y_1, y_2, \cdots, y_n\} \in R_+^n : 0 \leq y_i \leq 1, i = 1, \cdots, n\} \tag{20}$$

is positive invariant.

Proof: For all $t > 0$, $y_i(t) \geq 0$, where $i = 1, \cdots, n$, and the initial value $y(0) \in \Omega$. Besides, there would exist $k_0 \in \{1, \cdots, n\}$ and $t_0 > 0$, such that $y_{k_0}(t_0) = 0$. To ensure the generality, let $y_{k_0} = i^P_{i_0,j_0}$ and $t^* = \inf\{t > 0, i^P_{i_0,j_0}(t) = 0\}$. It follows from (8):

$$\frac{di^P_{i_0,j_0}(t^*)}{dt} = \beta_{11} i_0 \Theta_{11}(t^*) > 0. \tag{21}$$

However, the definition of t^* yields $di^P_{i_0,j_0}(t^*)\Big/dt \leq 0$, which leads to a contradiction. Then based on the Theorem 3.2 in [38], we derive the global stability of the disease-free equilibrium of (8).

Lemma 1: For a constant differential autonomous system

$$dy(t)/dt = f(y) \tag{22}$$

where $y \in R^n$ and $f : R_+^n \to R^n$ is a continuously differentiable map. The following conditions are assumed.

1) f is cooperative in R, that is, for $\forall y \in R_+^n$ and $i, j = 1, 2, \cdots, n$, if $i \neq j$, then $\partial f_i/\partial x_j \geq 0$. Meanwhile, $Df(y) = (\partial f_i/\partial x_j)_{1 \leq i,j \leq n}$ is irreducible for $\forall y \in R_+^n$;

2) $f(0) = 0$ and for all $y \in R_+^n$, if $y_i = 0$, then $f_i(y) \geq 0$, $i = 1, 2, \cdots, n$;

3) f is strictly nonlinear in R_+^n, that is, for $\forall \alpha \in (0, 1)$ and $y \gg 0$, $f(\alpha y) > \alpha f(y)$. Then the following two results are obtained:

a) If $s(Df(0)) = \max\{Re\lambda; \det(\lambda - Df(0))\} \leq 0$, $y = 0$ is globally asymptotically stable in R_+^n;

b) If $s(Df(0)) = \max\{Re\lambda; \det(\lambda - Df(0))\} > 0$, then eighter

i) For $\forall y \in R_+^n$, $\lim_{t \to \infty} |\varphi(t, y)| = +\infty$, or ii) Equation (22) has a unique positive equilibrium point $y^* \gg 0$, and $y = y^*$ is globally asymptotically stable in R_+^n.

Then according to **lemma 1**, **Theorem 3** can be obtained.

Theorem 3: If $R_0 \leq 1$, the disease-free equilibrium is globally asymptotically stable in Ω; and if $R_0 > 1$, the model (8) has a unique positive equilibrium E^* which is globally asymptotically stable in $\Omega - \{0\}$.

Proof: Obviously, the function $f : \Omega \to R^n$ is continuously differentiable and $f(0) = 0$, $f_i(y) \geq 0$ for all $y \in \Omega$ with $y_i = 0, i = 1, 2, \cdots, n$. In addition, $\partial f_i/\partial y_j \geq 0$ for $y \in \Omega, i \neq j$. Thus, the function f is a cooperative system. Particularly, for all $y \in \Omega$, $Df = (\partial f_i/\partial y_j)_{1 \leq i,j \leq n}$ is irreducible; and for any $\varepsilon \in (0, 1)$ and $y \in \Omega, f_i(\varepsilon y) \geq \varepsilon f_i(y)$

$$\mathbf{A}_{i,j} = \frac{\beta_{11} ij}{<k>_{11}} \begin{pmatrix} P_P(j,0) & P_P(j,1) & \cdots & P_P(j,n_{12}) \\ P_P(j,0) & P_P(j,1) & \cdots & P_P(j,n_{12}) \\ \cdots & \cdots & \cdots & \cdots \\ P_P(j,0) & P_P(j,1) & \cdots & P_P(j,n_{12}) \end{pmatrix}_{(n_{12}+1)(n_{12}+1)}$$

$$\mathbf{B}_{i,j} = 0$$

$$\mathbf{C}_{i,j} = 0$$

$$\mathbf{D}_{i,j} = \frac{\beta_{22}}{<k>_{22}} \begin{pmatrix} P_H(j,1) & 2P_H(j,2) & \cdots & n_{22}P_H(j,n_{22}) \\ 2P_H(j,1) & 4P_H(j,2) & \cdots & 2n_{22}P_H(j,n_{22}) \\ \cdots & \cdots & \cdots & \cdots \\ n_{22}P_H(j,1) & 2n_{22}P_H(j,2) & \cdots & n_{22}^2 P_H(j,n_{22}) \end{pmatrix}_{(n_{22}+1)(n_{22}+1)}$$

$$\mathbf{\Gamma} = \begin{pmatrix} \beta_{11} \sum_{i=0}^{n_{11}} \sum_{j=0}^{n_{12}} \frac{i^2 P_P(i,j)}{\varphi_1 <k>_{11}} & \beta_{11} \sum_{i=0}^{n_{11}} \sum_{j=0}^{n_{12}} \frac{ij P_P(i,j)}{\varphi_1 <k>_{11}} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \beta_{22} \sum_{i=0}^{n_{21}} \sum_{j=0}^{n_{22}} \frac{ij P_H(i,j)}{\varphi_2 <k>_{22}} & \beta_{22} \sum_{i=0}^{n_{21}} \sum_{j=0}^{n_{22}} \frac{j^2 P_H(i,j)}{\varphi_2 <k>_{22}} \end{pmatrix},$$

TABLE 2. Parameters for disease-free equilibrium.

Notation	Value
N^P	10000
N^H	10000
$n_{11}, n_{12}, n_{21}, n_{22}$	50
$\langle k \rangle_{11}, \langle k \rangle_{12}, \langle k \rangle_{21}, \langle k \rangle_{22}$	6
β_{11}	0.0000015
β_{22}	0.0000016
β_{12}	0.0000016
φ_1	0.049
φ_2	0.04
δ_1	0.012
δ_1	0.014
ω	0.01

with $i = 1, 2, \cdots, n$. It implies that f is strictly sublinear in Ω. So the proof is completed by applying **lemma 1**.

From **Theorem 3**, we prove that equation (19) is an accurate threshold for disease transmission. If there are infected nodes at the initial moment, no matter what the number of infected nodes are, as long as $R_0 \leq 1$, the malware will slowly die out. According to equation (19), it is related to the average degrees ($< k >_{11}$, $< k >_{22}$), recovery (quarantine) rate (φ_1, φ_2), and the infection rate (β_{11}, β_{22}) in our model.

IV. NUMERICAL EXPERIMENTS

In this section, numerical experiments in the complex network is conducted to verify our theoretical research above, and some dynamical properties of our model is showed. In the following experiments, it is assumed that there are 10000 PLCs and 10000 honeypots in, and there are 250 infected PLCs. The complex network is supposed to be *scale-free,* and the node-degree follows the *power-low* distribution.

A. DISEASE-FREE EQUILIBRIUM

Three parts experiments are presented as following, disease-free equilibrium, endemic equilibrium and the effectiveness of the honeynet.

The parameters for disease-free equilibrium are listed in Table 2. And the power-low index of the complex network is set $\gamma = 3$. Figure 3 and Figure 4 show the variation of every state in the complex network. With the parameters given in Table 2, a disease-free equilibrium is revealed before 500 time units.

B. ENDEMIC EQUILIBRIUM

To contrast with the disease-free equilibrium, the endemic equilibrium is showed in Figure 5 and Figure 6. The parameters are listed in Table 3.

The power-low index of the complex network is also set $\gamma = 3$. According to the physics significance, the parameters are adjusted to show the endemic equilibrium. Then we can see that before 1000 time units, the number of PLCs and honeypots reaches about 1500 and 2800, respectively.

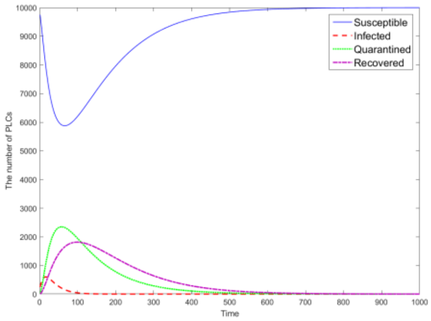


FIGURE 3. The propagation of PLCs (disease-free equilibrium).

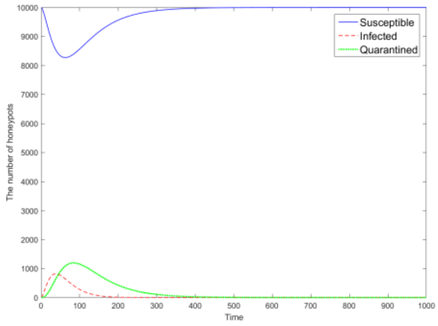


FIGURE 4. The propagation of honeypot (disease-free equilibrium).

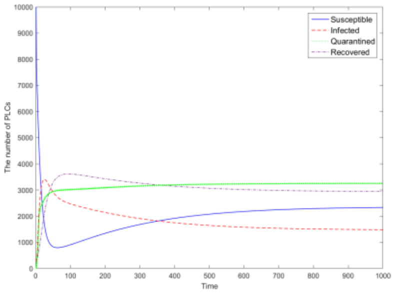


FIGURE 5. The propagation of PLCs (endemic equilibrium).

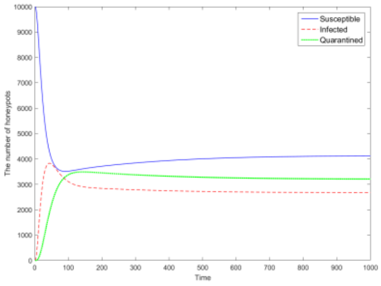


FIGURE 6. The propagation of honeypots (endemic equilibrium).

C. THE EFFECT OF THE HONEYNET

Our goal is to deploy honeypots in the honeynet more effectively and economically, so comparisons are made between different parameters to optimize the honeynet deployment

TABLE 3. **Parameters for endemic equilibrium.**

Notation	Value
N^P	10000
N^H	10000
$n_{11}, n_{12}, n_{21}, n_{22}$	50
$\langle k\rangle_{11}, \langle k\rangle_{12}, \langle k\rangle_{21}, \langle k\rangle_{22}$	6
β_{11}	0.0000035
β_{22}	0.0000024
β_{12}	0.0000038
φ_1	0.028
φ_2	0.024
δ_1	0.036
δ_1	0.02
ω	0.018

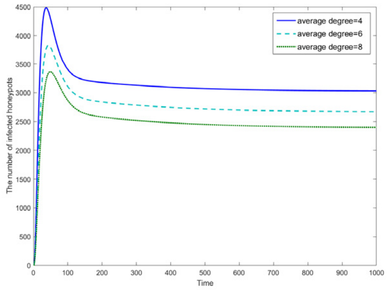


FIGURE 7. **Comparison of infected honeypots with different average degrees.**

strategy. As we know, honeypots are utilized to attract the malware attacks and provide quarantine strategy. Considering (8) with the parameters given in Table 3 except for the average degree. A comparison about different average degrees is made. Figure 7 shows that the number of infected honeypots changes with different average degrees when the system reaches the endemic equilibrium. The experiment show that the number of infected honeypots increases as the average degree decreases. It means that the honeynet with lower average degree is more attractive to the attackers, and more honeypots are infected so that the honeynet can collect the information of malware more effectively.

In Figure 8, we consider (8) with the parameters given in Table 3 except for the parameter β_{12}. And it exhibits the variation trend of infected PLCs with different β_{12}. When tending to the equilibrium state, the number of infected PLCs decreases with β_{12} increases, and larger β_{12} means that the honeypot in the honeynet exists more system vulnerabilities. So the honeypots with more system vulnerabilities is conducive to ensure the malware epidemic to a lower level.

In addition, the power-law index of the complex network plays an important role in the propagation of malware. Figure 9 shows that the evolution of the number of infected honeypots with different power-law index of honeynet in the case of endemic equilibrium. We can find that the number of infected honeypots increases with the power-law index decreases when tending to the equilibrium state. That is the honeynet with lower power-law index will be more attractive to the attackers. Another interesting phenomenon is that the number of infected honeypots decreases much more when the power-law index $\gamma = 3.2$ in the case of endemic equilibrium. It indicates that it is better to keep the power-law index $\gamma \leq 3$ when deploying honeynet.

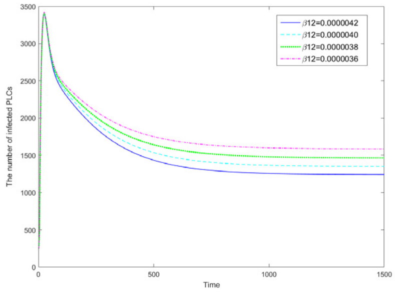


FIGURE 8. **Comparison of infected PLCs with different parameter β_{12}.**

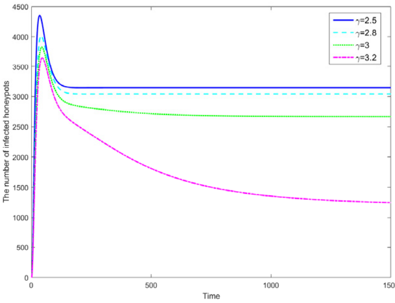


FIGURE 9. **Comparison of infected honeypots with different power-law index γ.**

V. SIMULATIONS EXPERIMENTS

In this section, simulation results are presented to verify the actual behavior of malware propagation in the complex network. The topology of the network is set to be *scale-free*, identical to Section IV, meaning that the node degree distribution follows the *power-law distribution* ($P^k = k^{-3}$). The simulations are built on the scale-free network generated by the simulation software MATLAB, the physical process of worm propagation in the network is implemented by C++ programming language. There are 10,000 PLCs and 10,000 honeypots in our simulation experiments, and the parameters are the same as which we use in numerical experiments (Table 3). The epidemic simulation process is consistent with the state transition diagram in Figure 2, so it will not be covered here again. The detailed process of our simulation experiments are presented as follows:

1) Firstly, we randomly choose 250 infected PLCs and other nodes are susceptible. In each round of the simulation experiments, all nodes in various states perform according to (8);
2) For susceptible PLCs which connected with infected PLCs, they can be infected by infected PLCs with

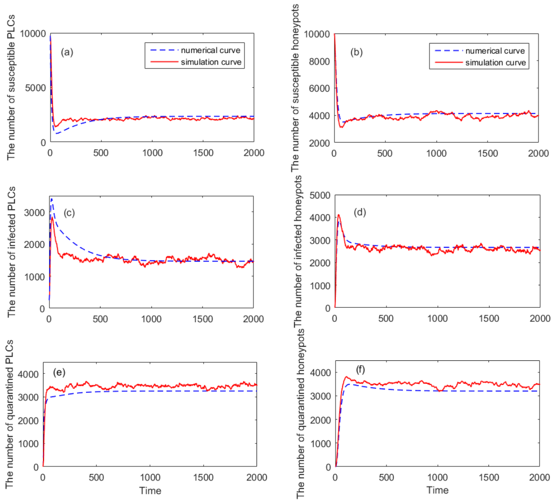


FIGURE 10. Comparisons between numerical and simulation curves in the two-layer complex network.

rate β_{11}. This process also applies to susceptible honeypots with rate β_{22};

3) Then the susceptible PLCs can be quarantined with rate β_{12}, and the infected PLCs can be recovered with probability φ_1. The infected honeypots can be quarantined with probability φ_2.
4) The quarantined PLCs will be recovered with probability ω.
5) Recovered PLCs (honeypots) transform into susceptible state again with probability δ_1 (δ_2).

Figure 10 (a-f) shows the comparisons between numerical (dashed curves) and simulation (solid curves) results of susceptible, infected, and quarantined PLCs (honeypots), and it implies that the simulation curves match the numerical curves well. We can find that there are some differences between numerical and simulation curves because of the high precision of numerical experiments. Namely, the data in simulation experiments is double type and the data in simulation experiments is integer type. However, the small differences do not affect the validity of our results.

VI. DISCUSSION

In our proposed model, the honeynet is introduced as inhibition strategy to suppress the malware propagation. And the honeynet is a key factor to inhibit the propagation of malware. Thus, a comparison is showed in a numerical experiment to verify the effect of the honeynet. At first we replace the honeynet with an ICS network. It means that all nodes are PLCs in the two-layer ICS network. It is different form (8), the infected PLCs in both two layers can infect other PLCs. The parameters and the process of malware propagation is same as (8). Then the infected PLCs in the same layer of the two models are compared.

It is easy to confirm that the effect of honeynet in Figure 11. When the system reach endemic equilibrium, the number of infected PLCs without honeynet is much larger than that with honeynet. And the peak in the model with honeynet is much lower than that without honeynet. The result indicates that the honeynet can inhibit the propagation of malware in ICS network effectively. Figure 12 is a partially enlarged view of Figure 10 (b) that shows the tiny propagation tendency in the simulation experiment. Actually, the number of infected PLCs always fluctuates within an interval. And the infected honeypots also performs like this. It means that the defense strategy can control the malware in a quantity interval.

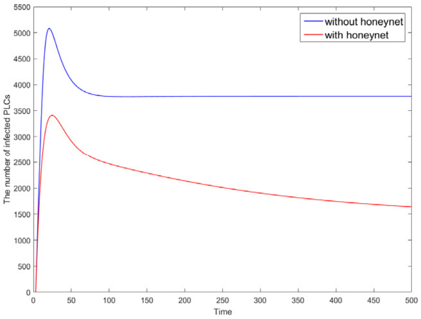


FIGURE 11. Comparison of infected PLCs for two models.

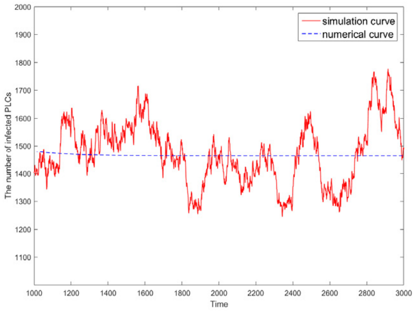


FIGURE 12. Partially enlarged view of the comparison between numerical and simulation curves.

Another influence to the honeynet is the network traffic. In this paper, the infection rate β_{22} is used to represent the amount of traffic, because the larger the amount of attack traffic, the more susceptible honeypots are to infection, vice versa. When all of the traffic from honeypot nodes is allow to be transmitted in the honeynet, like the traffic from PLC nodes, the infection rate β_{22} obtains its maximum value β_{22}^{*}. The intrusion detection system (IDS) can detect related attack traffic with the generated detection signatures. Referring to the experimental results in [39], [40], we define the detection rate d as follows,

$$d = 1 - e^{\beta_{22}}/\beta_{22} - \beta_{22}^{*}. \tag{23}$$

If we want to know the relationship between the traffic and infected honeypots, we will study the relationship between infection rate β_{22} and detection rate d. We assume that $\beta_{22}^{*} = 2.4 \times 10^{-5}$, and it is shown in Figure 13. Obviously, the infection rate β_{22} and detection rate d is positively related. Then Figure 14 shows the relationship between infection rate β_{22} and infected honeypots. When infection rate β_{22} increases,

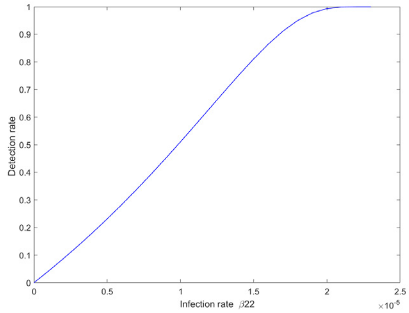


FIGURE 13. The relationship between infection rate β_{22} and detection rate d.

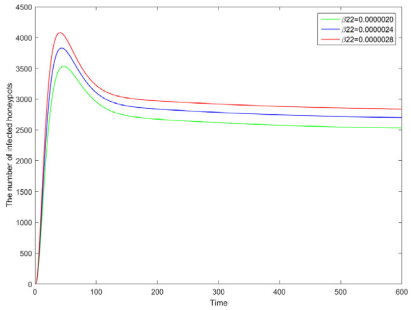


FIGURE 14. Comparison of infected honeypots with different infection rate β_{22}.

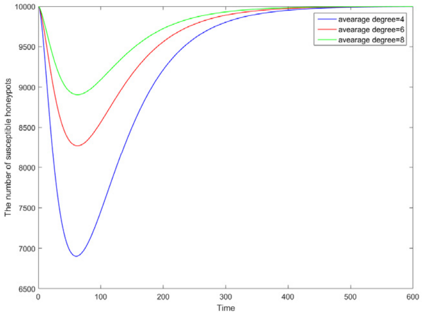


FIGURE 15. Comparison of susceptible honeypots with different average degrees in the case of disease-free equilibrium.

the detection rate d increases as well, it means that the traffic increases. Thus, we can find that the increasing traffic will cause more honeypots to be infected.

In Figure 7 and Figure 9, the comparison of infected honeypots with different average degrees and power-law index are studied when the system reaches the endemic equilibrium. Moreover, the influence of the honeynet topologies (power-law index) and connectivity (average degree) also needs to be studied when the system reaches disease-free equilibrium. Figure 15 shows the the comparison of susceptible honeypots with different average degrees. It shows that decreasing average degree will lead the minimum value of susceptible honeypots to decrease in the case of the disease-free equilibrium. It means that if the average degree is lower, fewer honeypots are susceptible. Then the attraction of the honeynet to the attackers may decrease. However, Figure 7 shows that more honeypots will be infected with lower average degree so that the honeynet can collect the information of malware more effectively. Then we know that the effectiveness of average degree depends on the state of our model. For the honeynet topologies (power-law index), Figure 16 shows that the number of infected honeypots increases much more when the power-law index $\gamma = 2.5$. The different performances of the honeynet in the case of endemic equilibrium and disease-free equilibrium are very interesting. Therefore, a dynamic connection mode of the honeynet may protect the ICS network more efficiently, which happened to be the excellent ability of the intelligent honeynet. And we will focus on the model of intelligent honeynet and study the intelligent honeynet detailedly in our future work.

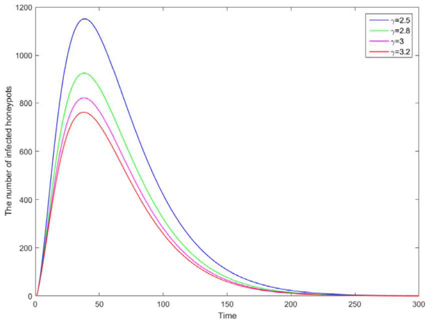


FIGURE 16. Comparison of infected honeypots with different power-law index γ.

VII. CONCLUSION

In summary, we introduce a new mathematical honeynet-based model in ICS network, and the epidemic dynamics in the two-layer complex network is analyzed. Theoretical analysis has revealed the relations between disease epidemics and honeynet potency. The influence of the average degree and the power-law index in the two-layer complex network has been analyzed. In particular, the following conclusions can be obtained,

1) A honeynet-based malware propagation model with immunization and isolation as the defensive measures in a two-layer (ICS network and honeynet) complex network is proposed.
2) The epidemic dynamics of our proposed malware propagation system is analyzed, it has a disease-free equilibrium E^0 and an endemic equilibrium E^*. And the local and global stabilities of the disease-free equilibrium are proved.
3) Numerical experiments are conducted to reveal the dynamics of malware propagation. It shows honeypots with more system vulnerabilities is conducive to ensure the malware epidemic to a lower level. In addition, simulation experiments provide the actual behavior of malware propagation and verification of our derivations.
4) The effect of the honeynet is discussed and it is demonstrated that the honeynet with lower average degree or lower power low index is more attractive to

the attackers. The results provide proper advice about how to deploy honeypots within a honeynet more effectively.

Our analysis provides a better understanding of the interaction relations between malware epidemics and honeynet potency. Based on the analysis results, several practical suggestions are also proposed about how to deploy honeypots more effectively (honeynet with more system vulnerabilities, lower average degree, or lower power low index). Furthermore, the comparison in discussion also indicates that the number of infected PLCs can be controlled to a smaller range under the potency of honeynet. In a word, the honeynet brings a great change in the area of ICS network security.

REFERENCES

[1] N. Falliere, L. O. Murchu, and E. Chien, "W32. Stuxnet dossier," Symantec Corp., Secur. Response, White Paper 2011.

[2] B. Merino. (2016). *Modbus Stager: Using PLCs as a Payload/Shellcode Distribution System*. [Online]. Available: http://www.shelliscoming.com/2016/12/modbus-stager-using-plcs-as.html

[3] R. Spenneberg, M. Brüggemann, and H. Schwartke, *Plc-Blaster: A Worm Living Solely in the PLC*, vol. 16. Black Hat Asia, 2016.

[4] P. Maynard, K. McLaughlin, and S. Sezer, "Modelling duqu 2.0 malware using attack trees with sequential conjunction," in *Proc. 2nd Int. Conf. Inf. Syst. Secur. Privacy*, 2016, pp. 465–472.

[5] S. Staniford, V. Paxson, and N. Weaver, "How to own the Internet in your spare time," in *Proc. 11th Usenix Secur. Symp.*, Aug. 2002, pp. 149–169.

[6] J. C. Martin, L. L. Burge III, J. I. Gill, A. N. Washington, and M. Alfred, "Modelling the spread of mobile malware," *Int. J. Comput. Aided Eng. Technol.*, vol. 2, no. 1, p. 3, 2010.

[7] S. Qing and W. Wen, "A survey and trends on Internet worms," *Comput. Secur.*, vol. 24, no. 4, pp. 334–346, Jun. 2005.

[8] B. K. Mishra and D. K. Saini, "SEIRS epidemic model with delay for transmission of malicious objects in computer network," *Appl. Math. Comput.*, vol. 188, no. 2, pp. 1476–1482, May 2007.

[9] R. Xu, Z. Ma, and Z. Wang, "Global stability of a delayed SIRS epidemic model with saturation incidence and temporary immunity," *Comput. Math. Appl.*, vol. 59, no. 9, pp. 3211–3221, May 2010.

[10] C. C. Zou, W. Gong, and D. Towsley, "Worm propagation modeling and analysis under dynamic quarantine defense," in *Proc. ACM workshop Rapid Malcode WORM*, Washington, DC, USA, 2003, pp. 51–60.

[11] B. K. Mishra and N. Keshri, "Mathematical model on the transmission of worms in wireless sensor network," *Appl. Math. Model.*, vol. 37, no. 6, pp. 4103–4111, Mar. 2013.

[12] R. Albert and A. L. Barabasi, "Statistical mechanics of complex networks," *Rev. Modern Phys.*, vol. 74, no. 1, pp. 47–97, Jan. 2002.

[13] Y. Yang, Y. Fang, and L.-Y. Li, "The analysis of propagation model for Internet worm based on active vaccination," in *Proc. 4th Int. Conf. Natural Comput.*, Oct. 2008, pp. 682–688.

[14] (2006). *Intrusion Detection Working Group, Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML) Document Type Definition*. [Online]. Available: http://www3.itef.org/proceedings/oodec/I-D/draft-ieff-idug-idmef-xml-01.txt

[15] L. Spitzer. (2002). *Honeypots: Tracking Hackers, Addison-Wesley*. [Online]. Available: http://www.tracking-hackers.com/book

[16] Á. Herrero, U. Zurutuza, and E. Corchado, "A neural-visualization IDS for honeynet data," *Int. J. Neural Syst.*, vol. 22, no. 2, Apr. 2012, Art. no. 1250005.

[17] H.-S. Yang, "A study on attack information collection using virtualization technology," *Multimedia Tools Appl.*, vol. 74, no. 20, pp. 8791–8799, Oct. 2015.

[18] D. K. Kang, L. C. Euom, and C. S. Kim, "A development of novel attack detection methods using virtual honeynet," *J. Korea Inst. Electron. Commun. Sci.*, vol. 5, no. 4, pp. 406–411, 2010.

[19] J. Ren and Y. Xu, "A compartmental model to explore the interplay between virus epidemics and honeynet potency," *Appl. Math. Model.*, vol. 59, pp. 86–99, Jul. 2018.

[20] R. Pastor-Satorras and A. Vespignani, "Epidemic spreading in scale-free networks," *Phys. Rev. Lett.*, vol. 86, no. 14, pp. 3200–3203, Apr. 2001.

[21] M. J. Keeling and K. T. D. Eames, "Networks and epidemic models," *J. Roy. Soc. Interface*, vol. 2, no. 4, pp. 295–307, Sep. 2005.

[22] C. Castellano and R. Pastor-Satorras, "Competing activation mechanisms in epidemics on networks," *Sci. Rep.*, vol. 2, no. 1, pp. 371–376, Dec. 2012.

[23] L.-X. Yang and X. Yang, "The effect of network topology on the spread of computer viruses: A modelling study," *Int. J. Comput. Math.*, vol. 94, no. 8, pp. 1591–1608, Aug. 2017.

[24] C. Zhang and H. Huang, "Optimal control strategy for a novel computer virus propagation model on scale-free networks," *Phys. A, Stat. Mech. Appl.*, vol. 451, pp. 251–265, Jun. 2016.

[25] L.-X. Yang and X. Yang, "The spread of computer viruses over a reduced scale-free network," *Phys. A, Stat. Mech. Appl.*, vol. 396, pp. 173–184, Feb. 2014.

[26] C. Nowzari, V. M. Preciado, and G. J. Pappas, "Stability analysis of generalized epidemic models over directed networks," in *Proc. 53rd IEEE Conf. Decis. Control*, Dec. 2014, pp. 6197–6202.

[27] L. Wang, G. Zhu, H. Kang, and X. Fu, "Epidemic spreading on three-layer interdependent networks," *J. Biol. Syst.*, vol. 24, no. 4, pp. 469–494, Dec. 2016.

[28] O. Diekmann, J. A. P. Heesterbeek, and J. A. J. Metz, "On the definition and the computation of the basic reproduction ratio r 0 in models for infectious diseases in heterogeneous populations," *J. Math. Biol.*, vol. 28, no. 4, pp. 365–682, Jun. 1990.

[29] P. van den Driessche and J. Watmough, "Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission," *Math. Biosciences*, vol. 180, nos. 1–2, pp. 29–48, Nov. 2002.

[30] X. Fu, M. Small, and G. Chen, *Propagation Dynamics on Complex Networks (Models, Methods and Stability Analysis)|| Introduction*. Hoboken, NJ, USA: Wiley, 2014, pp. 1–9.

[31] S. Wen, W. Zhou, J. Zhang, Y. Xiang, W. Zhou, and W. Jia, "Modeling propagation dynamics of social network worms," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 8, pp. 1633–1643, Aug. 2013.

[32] Z. Ammar and A. AlSharif, "Deployment of IoT-based honeynet model," in *Proc. 6th Int. Conf. Inf. Technol., IoT Smart City ACM*, 2018, pp. 134–139.

[33] A. D. Oza, G. N. Kumar, M. Khorajiya, and V. Tiwari, "Snaring Cyber attacks on IoT devices with Honeynet," in *Computing and Network Sustainability*. Singapore: Springer, 2019, pp. 1–12.

[34] M. De la Sen, R. Nistal, S. Alonso-Quesada, and A. Ibeas, "Some formal results on positivity, stability, and endemic steady-state attainability based on linear algebraic tools for a class of epidemic models with eventual incommensurate delays," *Discrete Dyn. Nature Soc.*, vol. 2019, Jul. 2019, Art. no. 8959681.

[35] J. D. Hernández Guillén, A. Martín del Rey, and L. Hernández Encinas, "Study of the stability of a SEIRS model for computer worm propagation," *Phys. A, Stat. Mech. Appl.*, vol. 479, pp. 411–421, Aug. 2017.

[36] Z. Zhang, R. K. Upadhyay, D. Bi, and R. Wei, "Stability and hopf bifurcation of a delayed epidemic model of computer virus with impact of antivirus software," *Discrete Dyn. Nature Soc.*, vol. 2018, pp. 1–18, Nov. 2018.

[37] C. Chavez, Z. Feng, and W. Huang, "On the computation of Ro and its role on global stability," *Inst. Math. Appl.*, vol. 125, pp. 31–65, 2002.

[38] X. Zhao and J. Zhu, "Global asymptotic behavior in some cooperative systems of functional differential equations," *Canad. Appl. Math. Quart*, vol. 4, no. 4, pp. 421–444, 1996.

[39] Z. Wang, G. Li, Y. Chi, J. Zhang, Q. Liu, T. Yang, and W. Zhou, "Honeynet construction based on intrusion detection," in *Proc. 3rd Int. Conf. Comput. Sci. Appl. Eng. CSAE*, 2019, pp. 1–5.

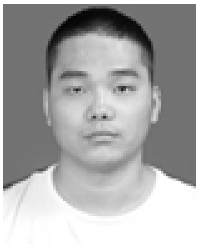
[40] H. Kim and B. Karp, "Autograph: Toward automated, distributed worm signature detection," in *Proc. USENIX Secur. Symp.*, vol. 286, Aug. 2004, pp. 1–16.

QIANG FU received the B.Sc. and M.Sc. degrees in physics from the Nanjing University of Information Science and Technology, Nanjing, China, in 2013 and 2016, respectively. He is currently pursuing the Ph.D. degree with Northeastern University, Shenyang, China, under the supervision of Prof. Yu Yao.

He joined the Engineering Research Center of Security Technology of Complex Network System, Shenyang, in 2018. His research interests include network security, nonlinear dynamic system analysis, and malware propagation modeling.

YU YAO received the B.Sc., M.Sc., and Ph.D. degrees in computer science from Northeastern University, Shenyang, China, in 1998, 2001, and 2005, respectively.

He has been a Professor and a Ph.D. Tutor with Northeastern University, since 2011. He was a Deputy Director of the Shenyang Big Data Administration Bureau, from 2015 to 2018. He is currently a Director of the Engineering Research Center of Security Technology of Complex Network System, Ministry of Education. His research interests include cyber security in industrial control networks, data analysis and modeling, and nonlinear dynamic system analysis.



CHUAN SHENG received the B.Sc. and M.Sc. degrees in computer science from Northeastern University, Shenyang, China, in 2014 and 2016, respectively, where he is currently pursuing the Ph.D. degree with the College of Computer Science and Engineering, under the supervision of Prof. Yu Yao.

He joined the Engineering Research Center of Security Technology of Complex Network System, Shenyang, in 2018. His research interests include network security situation awareness, network intrusion detection, network threat intelligence analysis, and big data of cybersecurity.

WEI YANG received the B.Sc., M.Sc., and Ph.D. degrees in computer science from Northeastern University, Shenyang, China, in 1998, 2001, and 2012, respectively.

She has been a Lecturer with Northeastern University, since 2004. She is currently a Visiting Scholar with The University of British Columbia, in 2019. Her main research interests include network security, malware propagation modeling, and nonlinear dynamic system analysis.