Hindawi
Security and Communication Networks
Volume 2021, Article ID 8896715, 11 pages
https://doi.org/10.1155/2021/8896715

Research Article

Stochastic Differential Game-Based Malware Propagation in Edge Computing-Based IoT

Li Miao and Shuai Li

School of Information Engineering, Ningxia University, Yinchuan 750021, China

Correspondence should be addressed to Li Miao; lmiao1021@gmail.com

Received 5 August 2020; Revised 4 November 2020; Accepted 30 January 2021; Published 23 February 2021

Academic Editor: Qingyi Zhu

Internet of Things (IoT) has played an important role in our daily life since its emergence. The applications of IoT cover from the traditional devices to intelligent equipment. With the great potential of IoT, there comes various kinds of security problems. In this paper, we study the malware propagation under the dynamic interaction between the attackers and defenders in edge computing-based IoT and propose an infinite-horizon stochastic differential game model to discuss the optimal strategies for the attackers and defenders. Considering the effect of stochastic fluctuations in the edge network on the malware propagation, we construct the Itô stochastic differential equations to describe the propagation of the malware in edge computing-based IoT. Subsequently, we analyze the feedback Nash equilibrium solutions for our proposed game model, which can be considered as the optimal strategies for the defenders and attackers. Finally, numerical simulations show the effectiveness of our proposed game model.

1. Introduction

Recently, a rapidly increasing number of physical devices and sensors are connecting to the Internet at an unprecedented rate. It has led to the emergence of the Internet of Things (IoT). By deploying smart devices and sensors to collect and analyze the physical data, the IoT can monitor and control the physical environment [1]. IoT has brought great convenience to our daily life in the past few years. For example, the IoT has been widely used in intelligent transportation, smart home appliances, smart healthcare, and other fields [2, 3].

Since the IoT devices typically have limited resources, it is common to forward the physical data to the cloud computing platform, which will need extra bandwidth or cause data security problem. With the advance of IoT, edge computing has been introduced to address the above issues [4–6]. Generally, edge computing provides powerful computing resources at the edge of the Internet and is close to the IoT devices [7, 8]. Edge computing has relieved the pressure of bandwidth and overcome the latency issue. However, edge computing environment is an open ecosystem and the IoT devices with limited resources are more vulnerable to be attacked [9]. Then, the existing defense mechanisms based on cloud computing cannot be used to edge computing because of the geographically dispersed nature of IoT devices. Thus, how to effectively design defense mechanisms to defend against attackers has become a serious problem that desperately needs to be solved. In this paper, we pay attention to the security problem of malware propagation based on the stochastic differential game; in this framework, we try to model an optimal defense strategy for IoT devices.

In edge computing-based IoT, attackers want to infect more IoT devices with malware to gain illegal gains using the attack strategy, while the defenders want to minimize the damage caused by IoT devices infected with malware using the defense strategy. Meanwhile, the IoT devices join or exit the network randomly, which can affect the stability of the edge network. The dynamic interaction between the attackers and defenders leads to the propagation of the malware, and the influence of network instability can be considered as the stochastic elements. In this paper, we

propose an infinite-horizon stochastic differential game model to research the malware propagation among IoT devices under the dynamic interaction between attackers and defenders in edge computing-based IoT, considering the stochastic fluctuations in the network. The main contributions of our proposed scheme are as follows:

(1)Firstly, we use the infinite-horizon stochastic differential game to model the malware propagation under the dynamic interaction between the attackers and defenders in edge computing-based IoT.

(2) Secondly, the Itô stochastic differential equation is used to characterize the effect of stochastic fluctuations of the edge network on the malware propagation.

(3) Finally, we discuss the feedback Nash equilibrium solutions for our proposed game model, which can be considered as the optimal strategies for both the attackers and defenders.

This paper is organized as follows. Section 2 introduces related works. Section 3 discusses the security problem of the attackers and defenders in a stochastic differential game theory. The feedback Nash equilibrium solutions for our proposed game model are analyzed in Section 4. Numerical simulations are given in Section 5. Finally, we conclude this paper in Section 6.

2. Related Works

Malware propagation problem is one of the most fundamental problems, for which many kinds of research have been proposed in the literature [10–15]. Malware propagation means that the infected legitimate nodes are able to contaminate other noninfected legitimate nodes, in addition to the attack nodes [16]. The edge users achieve shared interactions through smart applications in edge computing-based IoT, which increase the probability of malware download.

Generally, there are two complementary classes of methods to defend against malware threat: detection-based method and prevention-based method. Tobias et al. [10] proposed a novel malware detection approach that used the compression-based graph mining, in which the characteristic behaviors were extracted by the quantitative data flow graphs to derive the detection accuracy. TaeGuen et al. [11] discussed the malware characteristics through the feature vector generation methods and proposed a multimodal deep neural network malware detection model for android applications. The advantage of this method is more suitable for the dynamic environments. Dehghantanha et al. [12] studied the malware detection problem in IoT using the deep learning based method, which provided a new direction for further research. Since various IoT device vulnerabilities, Indre et al. [13] created a system that could detect and prevent malicious connections based on machine learning to enhance network security. Lan et al. [14] researched the propagation of epidemic in complex networks and proposed a dynamic prevention model with a time-varying community network. They considered the subnets of the network as communities and investigated the process of the malware. Khouzani et al. [15] searched the propagation of malware in a battery-constrained mobile device, considering the fact that malware can control the rate of killing the infectives and the scanning rate of the infectives. The maximum damage caused by the malware was quantified with the optimal control theory, through which the network damage can be minimized by adjusting the relevant parameters.

In addition to successful defense mechanisms to defend against malware threat, another effective defense scheme should consider both the limited resources and the dynamic characteristic of network. In recent years, game theory has been used to solve the decision making between the IoT devices and attackers [17, 18]. Game theory provides a mathematical method for the problems that different players compete with each other or with contradictory goals. Similarly, an effective security scheme in edge computing-based IoT depends not only on the successful defense strategies but also on the attackers' behaviors.

Spyridopoulos et al. [19] proposed a game-based security model to solve the malware dissemination prevention problem and analyzed the optimal defense strategy for the defender to minimize the damage of malware and the security cost with the optimal strategy. Quang et al. [20] modeled the problem of defending against attackers in IoT networks as a Bayesian game of incomplete information and showed that there was a threshold for the frequency of active attackers. Liao et al. [21] designed a zero-sum stochastic game to analyze the effect of malware in IoT and obtained the optimal defense strategy by the feedback Nash equilibrium solutions for the game model. Sedjelmaci et al. [22] presented a game-based detection technology for IoT device, which can not only activate the anomaly detection technology but also balance the energy consumption. Kaur et al. [23] proposed a stochastic game net security model, which combined the advantages of game theory and stochastic Petri nets. Shen et al. [24] proposed a multistage privacy-preserved game model for malware detection in fog-cloud-based IoT networks. In [24], the optimal detection strategy was attained under the consideration of privacy leakage of IoT devices, and the proposed detection scheme overcame the problem of limited resources of IoT devices.

Nevertheless, none of the above research considered the stochastic characteristic of edge network.. In this paper, we introduce an infinite-horizon stochastic differential game to analyze the malware propagation problem in edge computing-based IoT, in which the stochastic characteristic of edge networks is considered.

3. System Model

In this section, we will use the infinite-horizon stochastic differential game to model the malware propagation under the dynamic interaction between the attackers and defenders. An infinite-horizon stochastic differential game involves an m-dimensional vector-valued stochastic differential equation

$$\begin{aligned} &dx(s) = f[x(s), u_1(s), \ldots, u_n(s)]ds + g[x(s)]dB(s), \\ &x(t_0) = x_0, \end{aligned} \tag{1}$$

which describes the evolution of the state and n objective functions

$$\max_{u_i} E_{t_0}\left\{\int_{t_0}^{\infty} h^i[x(s), u_1(s), \ldots, u_n(s)]\exp(-r(s-t_0))ds\right\}, \quad \text{for } i = 1, \ldots, n, \tag{2}$$

where $E_{t_0}\{\cdot\}$ denotes the expectation operation taken at time t_0, $g[x(s)]$ is an $m \times l$ matrix, $B(s)$ is an l-dimensional Brownian motion, and the initial state x_0 is given in [25].

We consider an edge computing-based IoT environment with N IoT devices. Figure 1 shows the architecture of edge computing-based IoT.

We first use the SEIRS model [26] to describe the spread of the malware in edge computing-based IoT. Like the SEIRS model, we divide the IoT devices into susceptible, exposed, infective, and recovered classes. The devices in the infectious state show that the device has been infected by the malware and the susceptible device is prone to be infected, but not infected. The exposed IoT device shows that it has been infected but not yet infectious, and the device in the recovery state represents that it has been immune to malicious attacks. We use $S(t)$, $E(t)$, $I(t)$, and $R(t)$ to denote the number of them at time $t \in [t_0, \infty)$, respectively (that is, $S(t) + E(t) + I(t) + R(t) = N$).

Let β denote the rate of transmitting malware between a susceptible and an infectious IoT device, σ denote the rate of exposed IoT devices becoming infectious, γ denote the rate of infectious IoT devices becoming recovered, ξ denote recovered IoT devices becoming susceptible, $u_0(t)$ denote the number of IoT devices from susceptible to exposed caused by the attacker strategy at time $t \in [t_0, \infty)$, and $u_1(t)$ denote the number of IoT devices from infectious to recovered caused by the defender strategy at time $t \in [t_0, \infty)$. As shown in Figure 2, due to the dynamic interaction between the attackers and defenders, the spread of the malware in edge computing-based IoT can be described as the following differential equations:

$$\begin{aligned} \frac{dS(t)}{dt} &= -\frac{\beta S(t)I(t)}{N} + \xi R(t) - u_0(t), \\ \frac{dE(t)}{dt} &= \frac{\beta S(t)I(t)}{N} - \sigma E(t) + u_0(t), \\ \frac{dI(t)}{dt} &= \sigma E(t) - \gamma I(t) - u_1(t), \\ \frac{dR(t)}{dt} &= \gamma I(t) - \xi R(t) + u_1(t). \end{aligned} \tag{3}$$

In edge computing-based IoT, the parameters β, σ, γ, and ξ also may fluctuate because of the effect of stochastic fluctuations of the edge network on the malware propagation. To characterize the fluctuation of the parameters β, σ, γ, and ξ, we work on a complete probability space $(\Omega, \mathcal{F}, \{\mathcal{F}_t\}_{t\geq 0}, \mathbb{P})$ with a filtration $\{\mathcal{F}_t\}_{t\geq 0}$ satisfying the usual conditions [27]. By the central limit theorem, the fluctuation of the parameters β, σ, γ, and ξ follows a normal distribution. Then, we may replace the parameters β, σ, γ, and ξ by $\beta \longrightarrow \beta + ((\delta_1 dB_1(t))/dt)$, $\sigma \longrightarrow \sigma + ((\delta_2 dB_2(t))/dt)$, $\gamma \longrightarrow \gamma + ((\delta_3 dB_3(t))/dt)$, and $\xi \longrightarrow \xi + ((\delta_4 dB_4(t))/dt)$, respectively, where $B_i(t)$ is standard Brownian motion defined on the complete probability space with $B_i(t_0) = 0$ and δ_i is a positive constant describing the intensity of the fluctuation for $i = 1, 2, 3, 4$. Thus, the differential equations (3) can be rewritten as the following It ô stochastic differential equations:

$$\begin{aligned} dS(t) &= -\frac{\beta S(t)I(t)}{N} + \xi R(t) - u_0(t) - \frac{\delta_1 S(t)I(t)dB_1(t)}{N} + \delta_4 R(t)dB_4(t), \\ dE(t) &= \frac{\beta S(t)I(t)}{N} - \sigma E(t) + u_0(t) + \frac{\delta_1 S(t)I(t)dB_1(t)}{N} - \delta_2 E(t)dB_2(t), \\ dI(t) &= \sigma E(t) - \gamma I(t) - u_1(t) + \delta_2 E(t)dB_2(t) - \delta_3 I(t)dB_3(t), \\ dR(t) &= \gamma I(t) - \xi R(t) + u_1(t) + \delta_3 I(t)dB_3(t) - \delta_4 R(t)dB_4(t). \end{aligned} \tag{4}$$

As mentioned in Section 1, in edge computing-based IoT, attackers want to make malware infect more IoT devices to gain illegal gains using the attack strategy, while defenders want to reduce the damage caused by IoT devices infected with malware using the defense strategy. More accurately, the aim of the attackers includes maximizing the number of infectious IoT devices and the number of IoT devices from susceptible to exposed and reducing the payoff of the attack strategy; the aim of the defenders includes minimizing the number of infectious IoT devices and the number of IoT devices from susceptible to exposed and reducing the payoff of the defense strategy. Inspired by Alpcan and Başar [28], the payoff of the attack strategy and the defense strategy can be described as $((u_0(t)^2)/2c_0)$ and $(((u_1(t)^2)/2c_1))$, respectively, where c_0 and c_1 are positive constants. Thus, the objective functions of the attackers and defenders can be formulated as

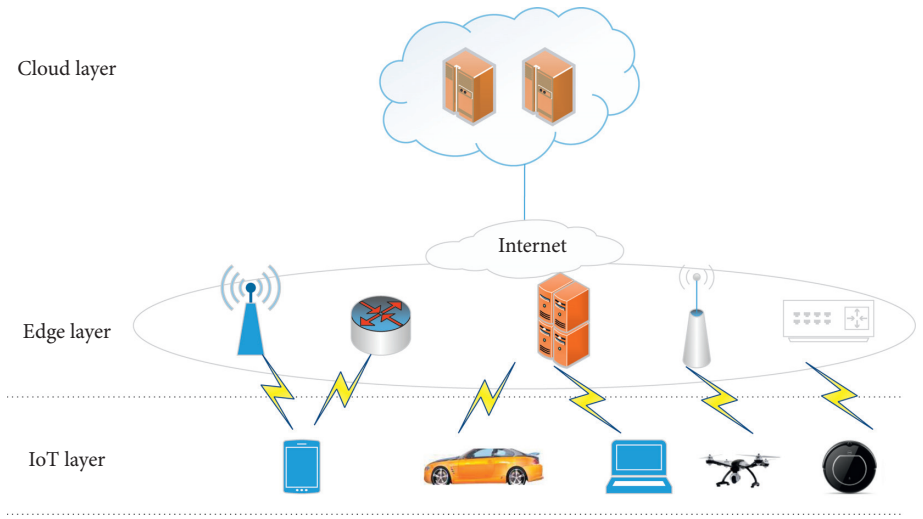

Figure 1: The architecture of edge computing-based IoT.

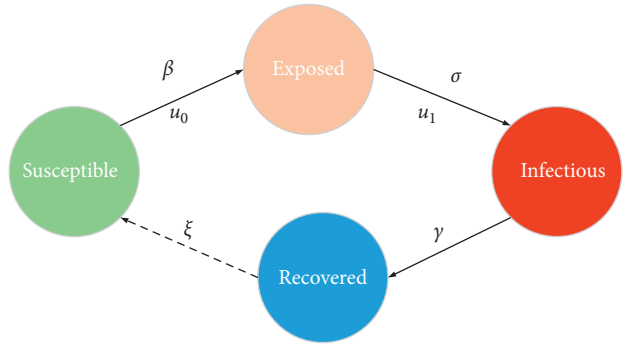

Figure 2: The spread of the malware.

$$\max_{u_0} E_{t_0}\left\{\int_{t_0}^{\infty}\left(a_0 I(t) + b_0 S(t) I(t) - \frac{u_0(t)^2}{2c_0}\right)\exp\left(-r(t-t_0)\right)\mathrm{d}t\right\},$$
$$\max_{u_1} E_{t_0}\left\{\int_{t_0}^{\infty}\left(-a_1 I(t) - b_1 S(t) I(t) - \frac{u_1(t)^2}{2c_1}\right)\exp\left(-r(t-t_0)\right)\mathrm{d}t\right\}, \tag{5}$$

where a_0 and a_1 are positive constants, b_0 and b_1 are constants, and r is the discount factor. Note that a_0 represents the benefits of each infectious IoT devices to the defenders while a_1 represents the losses of each infectious IoT devices to the defenders; c_0 describes that the payoff of the attack strategy is proportional to the number of IoT devices from susceptible to exposed caused by the attack strategy while c_1 describes that the payoff of the defense strategy is proportional to the number of IoT devices from infectious to recovered caused by the attack strategy.

In summary, the malware propagation under the dynamic interaction between the attackers and defenders can be formulated as the infinite-horizon stochastic differential game:

$$\max_{u_i} E_{t_0}\left\{\int_{t_0}^{\infty} h^i\left[x(s), u_0(s), u_1(s)\right]\exp\left(-r(s-t_0)\right)\mathrm{d}s\right\}, \quad \text{for } i = 0, 1, \tag{6}$$

subject to the stochastic dynamics

$$\mathrm{d}x(s) = f\left[x(s), u_0(s), u_1(s)\right]\mathrm{d}s + g\left[x(s)\right]\mathrm{d}B(s), \quad x(t_0) = x_0, \tag{7}$$

where

$$x(s) = (S(s), E(s), I(s), R(s))^T,$$
$$B(s) = \left(B_1(s), B_2(s), B_3(s), B_4(s)\right)^T,$$
$$h^0\left[x(s), u_0(s), u_0(s)\right] = a_0 I(s) + b_0 S(s) I(s) - \frac{u_0(s)^2}{2c_0},$$
$$h^1\left[x(s), u_1(s), u_1(s)\right] = -a_1 I(s) - b_1 S(s) I(s) - \frac{u_1(s)^2}{2c_1}, \tag{8, 9}$$

$$f[x(s),u_0(s),u_1(s)] = \left(-\frac{\beta S(s)I(s)}{N} + \xi R(s) - u_0(s)\frac{\beta S(s)I(s)}{N} - \sigma E(s) + u_0(s)\sigma E(s) - \gamma I(s) - u_1(s)\gamma I(s) - \xi R(s) + u_1(s)\right), \tag{10}$$

$$g[(x(s))] = \begin{pmatrix} -\alpha_1 & 0 & 0 & \alpha_4 \\ \alpha_1 & -\alpha_2 & 0 & 0 \\ 0 & \alpha_2 & -\alpha_3 & 0 \\ 0 & 0 & \alpha_3 & -\alpha_4 \end{pmatrix}, \tag{11}$$

for $\alpha_1 = ((\delta_1 S(s)I(s))/N)$, $\alpha_2 = \delta_2 E(s)$, $\alpha_3 = \delta_3 I(s)$, and $\alpha_4 = \delta_4 R(s)$.

4. Nash Equilibrium Solution

In this section, we will discuss the feedback Nash equilibrium solutions for game 6-7 to obtain the optimal strategies for the defender and attackers. Each participant is assumed to be rational and the decision making of each participant depends on their own objective functions in this game. The feedback Nash equilibrium solutions for game 1-2 can be characterized by the following theorem [25].

Theorem 1. *An n-tuple of strategies* $\{u_i^* = \phi_i^*(x): i \in N\}$ *provides a feedback Nash equilibrium solution to game 1-2 if there exist continuously twice differentiable functions* $W^i(x)$: $R^m \longrightarrow R$, $i \in N$, *satisfying the following set of partial differential equations:*

$$\begin{aligned} rW^i(x) - \frac{1}{2}\sum_{h,k=1}^{m}\Omega^{hk}(x)W^i_{x_h x_k}(x) &= \max_{u_i}\left\{h^i[x,\phi_1^*(x),\ldots,\phi_{i-1}^*(x),u_i(x),\phi_{i+1}^*(x),\ldots,\phi_n^*(x)]\right\} \\ &\quad + W_x^i(x)f[x,\phi_1^*(x),\ldots,\phi_{i-1}^*(x),u_i(x),\phi_{i+1}^*(x),\ldots,\phi_n^*(x)] \\ &= h^i[x,\phi_1^*(x),\ldots,\phi_n^*(x)] + W_x^i(x)f[x,\phi_1^*(x),\ldots,\phi_n^*(x)], \quad \text{for } i = 1,\ldots,n, \end{aligned} \tag{12}$$

where $\Omega[x(s)] = g[x(s)]g[x(s)]^T$ *denotes the covariance matrix with its element in row h and column k denoted by* $\Omega^{hk}[x(s)]$.

To obtain the feedback Nash equilibrium solutions for game 6-7, we consider the alternative problem

$$\max_{u_i} E_{t_0}\left\{\int_{t_0}^{\infty} h^i[x(s),u_0(s),u_1(s)]\exp(-r(s-t_0))\mathrm{d}s\right\}, \quad i = 0,1, \tag{13}$$

subject to the stochastic dynamics

$$\mathrm{d}x(s) = f[x(s),u_0(s),u_1(s)]\mathrm{d}s + g[x(s)]\mathrm{d}B(s), \quad x(t) = x_t, \tag{14}$$

where $h^i[x(s),u_0(s),u_1(s)]$ for $i = 0,1$, $f[x(s),u_0(s),u_1(s)]$, and $g[x(s)]$ are given by equations (9)–(11).

Invoking Theorem 1, we obtain two feedback strategies $u_0^* = \phi_0^*(x)$ and $u_1^* = \phi_1^*(x)$ constituting the feedback Nash equilibrium solutions for game 13-14, if there exist continuously twice differentiable functions $W^i(x)$: $R^4 \longrightarrow R$, $i = 0,1$, satisfying the following set of partial differential equations:

$$\begin{aligned} rW^0(x) - \frac{1}{2}\sum_{h,k=1}^{4}\Omega^{hk}(x)W^0_{x_h x_k}(x) &= \max_{u_0}\left\{h^0(x,u_0,\phi_1^*) + W_x^0(x)f(x,u_0,\phi_1^*)\right\}, \\ &= h^0(x,\phi_0^*,\phi_1^*) + W_x^0(x)f(x,\phi_0^*,\phi_1^*), \\ rW^1(x) - \frac{1}{2}\sum_{h,k=1}^{4}\Omega^{hk}(x)W^1_{x_h x_k}(x) &= \max_{u_1}\left\{h^1(x,u_0,\phi_1^*) + W_x^1(x)f(x,\phi_0^*,u_1)\right\}, \\ &= h^1(x,\phi_0^*,\phi_1^*) + W_x^0(x)f(x,\phi_0^*,\phi_1^*), \end{aligned} \tag{15}$$

where $\Omega[x(s)] = g[x(s)]g[x(s)]^T$ is given by

$$\begin{pmatrix} \alpha_1^2 + \alpha_3^2 & -\alpha_1^2 & 0 & -\alpha_4^2 \\ -\alpha_1^2 & \alpha_1^2 + \alpha_2^2 & -\alpha_2^2 & 0 \\ 0 & -\alpha_2^2 & \alpha_2^2 + \alpha_3^2 & -\alpha_3^2 \\ -\alpha_4^2 & 0 & -\alpha_3^2 & \alpha_3^2 + \alpha_4^2 \end{pmatrix}, \tag{16}$$

for $\alpha_1 = ((\delta_1 S(s) I(s))/N)$, $\alpha_2 = \delta_2 E(s)$, $\alpha_3 = \delta_3 I(s)$, and $\alpha_4 = \delta_4 R(s)$.

Applying the maximization operator in equation (15), we obtain the feedback Nash equilibrium solutions for game 13-14:

$$\begin{aligned} \phi_0^*(x) &= c_0\left(W_E^0(x) - W_S^0(x)\right), \\ \phi_1^*(x) &= c_1\left(W_R^1(x) - W_I^1(x)\right). \end{aligned} \tag{17}$$

Substituting $\phi_1^*(x)$ and $\phi_2^*(x)$ in equations (17) into (15), we obtain the following proposition upon solving equation (15).

Proposition 1. *The set of partial differential equation (15) admits a solution:*

$$\begin{aligned} W^0(x) &= \frac{a_0\sigma E}{(\sigma - r)(\gamma - r)} + \frac{a_0 I}{\gamma - r} - \frac{a_0^2 c_0 \sigma^2}{2r(\sigma - r)^2(\gamma - r)^2} \\ &\quad - \frac{a_0 a_1 c_1}{r(\gamma - r)^2}, \\ W^1(x) &= \frac{a_1\sigma E}{(\sigma - r)(\gamma - r)} + \frac{a_1 I}{\gamma - r} + \frac{a_0 a_1 c_0 \sigma^2}{r(\sigma - r)^2(\gamma - r)^2} \\ &\quad + \frac{a_1^2 c_1}{2r(\gamma - r)^2}, \end{aligned} \tag{18}$$

where

$$\begin{aligned} a_0\beta\sigma + b_0(\sigma - r)(\gamma - r) &= 0, \\ a_1\beta\sigma + b_1(\sigma - r)(\gamma - r) &= 0. \end{aligned} \tag{19}$$

Proof. By equation (18), we have

$$\begin{aligned} W_x^0(x) &= \left(0, \frac{a_0\sigma}{(\sigma - r)(\gamma - r)}, \frac{a_0}{\gamma - r}, 0\right), \\ W_x^1(x) &= \left(0, \frac{a_1\sigma}{(\sigma - r)(\gamma - r)}, \frac{a_1}{\gamma - r}, 0\right), \\ W_{x_h x_k}^0(x) &= W_{x_h x_k}^1(x) = 0, \quad \text{for } 1 \le h, k \le 4. \end{aligned} \tag{20}$$

Combining equations (17) and (20), we obtain

$$\begin{aligned} \phi_0^*(x) &= \frac{a_0 c_0 \sigma}{(\sigma - r)(\gamma - r)}, \\ \phi_1^*(x) &= \frac{a_1 c_1}{\gamma - r}. \end{aligned} \tag{21}$$

Substituting equations (20) and (21) into equation (15), we obtain

$$\begin{aligned} a_0\beta\sigma + b_0(\sigma - r)(\gamma - r) &= 0, \\ a_1\beta\sigma + b_1(\sigma - r)(\gamma - r) &= 0. \end{aligned} \tag{22}$$

Thus, this proposition holds. □

According to the proof of Proposition 1, the feedback Nash equilibrium solutions for game 6-7 is given by equation (21). In other words, the optimal strategies for the defenders and attackers are derived. The optimal state for game 6-7 describes the propagation of the malware in edge computing-based IoT when both the attackers and defenders adopt the optimal strategy. Substituting (21) into (7), we obtain the optimal state for game 6-7, i.e.,

$$\begin{aligned} \mathrm{d}S(t) &= -\frac{\beta S(t) I(t)}{N} + \xi R(t) - \frac{a_0 c_0 \sigma}{(\sigma - r)(\gamma - r)} - \frac{\delta_1 S(t) I(t) \mathrm{d}B_1(t)}{N} + \delta_4 R(t) \mathrm{d}B_4(t), \\ \mathrm{d}E(t) &= \frac{\beta S(t) I(t)}{N} - \sigma E(t) + \frac{a_0 c_0 \sigma}{(\sigma - r)(\gamma - r)} + \frac{\delta_1 S(t) I(t) \mathrm{d}B_1(t)}{N} - \delta_2 E(t) \mathrm{d}B_2(t), \\ \mathrm{d}I(t) &= \sigma E(t) - \gamma I(t) - \frac{a_1 c_1}{\gamma - r} + \delta_2 E(t) \mathrm{d}B_2(t) - \delta_3 I(t) \mathrm{d}B_3(t), \\ \mathrm{d}R(t) &= \gamma I(t) - \xi R(t) + \frac{a_1 c_1}{\gamma - r} + \delta_3 I(t) \mathrm{d}B_3(t) - \delta_4 R(t) \mathrm{d}B_4(t), \\ S(t_0) &= S_0, \\ E(t_0) &= E_0, \\ I(t_0) &= I_0, \\ R(t_0) &= R_0. \end{aligned} \tag{23}$$

Input: $x(S(T), E(t), I(t), R(t))$;
Output: optimal state trajectory $x(s)$ and optimal strategies $\phi_0^*(x), \phi_1^*(x)$;
(1) Initialize game parameters $N, \delta_1, \delta_2, \delta_3, \delta_4, a_0, b_0, c_0, a_1\, b_1, c_1$, and r;
(2) Set the rate parameters $\beta, \sigma, \gamma, \xi$;
(3) For $t = 0$ to T;
(4) If the infected nodes $x(I(t)) > 0$
(5) Response the defense mechanism;
(6) Calculate the optimal state trajectory in equation (4);
(7) Calculate the optimal strategies in equation (21);
(8) Analyze the influence of parameters a_0, c_0, a_1, c_1 on the optimal strategies;
(9) Else
(10) $t = t + 1$;
(11) End if
(12) Update $x(s)$ and store it;
(13) End for;
(14) Return $(x(x), \phi_0^*(x), \phi_1^*(x))$.

Algorithm 1: The stochastic game algorithm for the defenders and attackers (the optimal strategies for the defenders and attackers).

Table 1: Values of parameters.

β	σ	γ	ξ
0.249	0.147	0.870	0.012
δ_1	δ_2	δ_3	δ_4
0.187	0.110	0.652	0.009
a_0	b_0	c_0	a_1
0.993	0.348	0.437	0.295
b_1	c_1	r	N
3.554	0.351	0.346	10000

5. Numerical Simulations

In this section, we discuss the implementation of the stochastic game algorithm which is given in Table 1 and analyze the proposed infinite-horizon stochastic differential game model by simulations.

The algorithm is divided into two parts. One is the "feedback Nash equilibrium of defenders" part, which is used to calculate the optimal defense strategies during the attacks. The other is the "feedback Nash equilibrium of attackers," which is used to calculate the optimal attack strategies. The time and space complexity is O (n), respectively, because the proposed algorithm should be solved in a finite time horizon [0, T] for all the attackers and defenders. Besides, all the functions need to be invoked at each time.

We assume that the number of IoT devices is $N = 10000$ and consider the time horizon to be $T = 20$ minutes. The rest of the related simulation parameters are shown in Table 1.

Figure 3 shows the optimal trajectory $x(t)$ with time t. It can be seen that the number of the susceptible devices is rapidly decreased with the time variation, while the number of the infected devices increases at the beginning and then gradually decreases to zero. The dynamic evolution of the number of the exposed devices is similar to that of the infected devices. In addition, the number of the recovered devices is increased with the time variation. It means that defenders can respond their defense mechanism against attackers, which is consistent with the practical network environment, where the infected devices are always recovered and the exposed devices always exist.

Based on equation (21), we discuss the optimal strategies of the attackers and defenders in Figure 4. As shown in the results, the variation of the optimal defense strategy is increased with the time variation while the variation of optimal strategy of the attackers is decreased and then tends to be stable.

Figure 5 shows the change of the optimal strategy of the attackers with a_0 and c_0 while Figure 6 shows the change of the optimal strategy of the defenders with a_1 and c_1, where a_0 represents the benefits of each infectious IoT device to the defenders while a_1 represents the losses of each infectious IoT devices to the defenders; c_0 describes that the payoff of the attack strategy is proportional to the number of IoT devices from susceptible to exposed caused by the attack strategy while c_1 describes that the payoff of the defense strategy is proportional to the number of IoT devices from infectious to recovered caused by the attack strategy. It can It

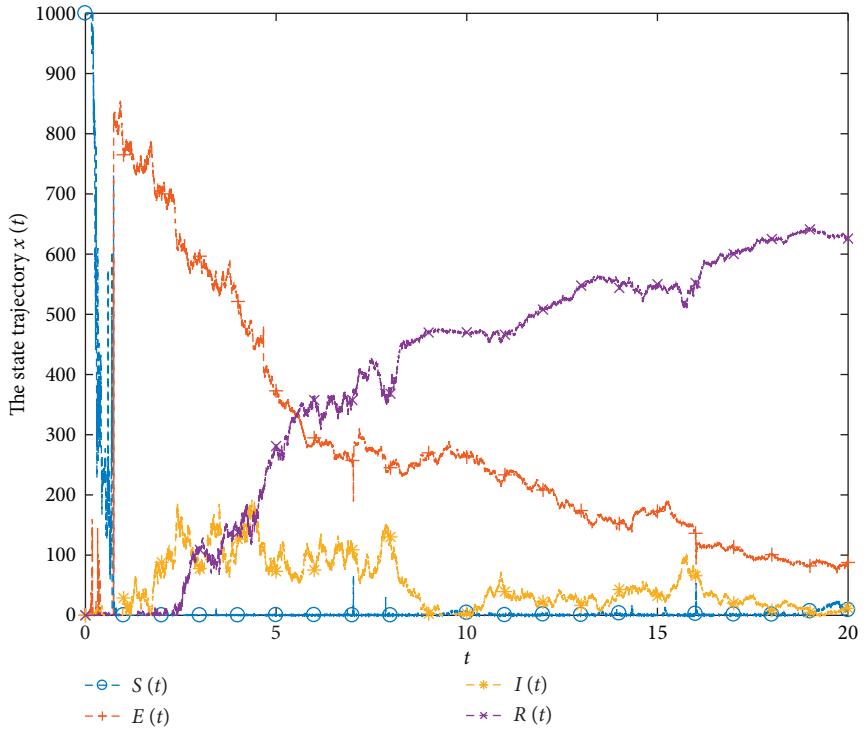

Figure 3: The state trajectory $x(t)$.

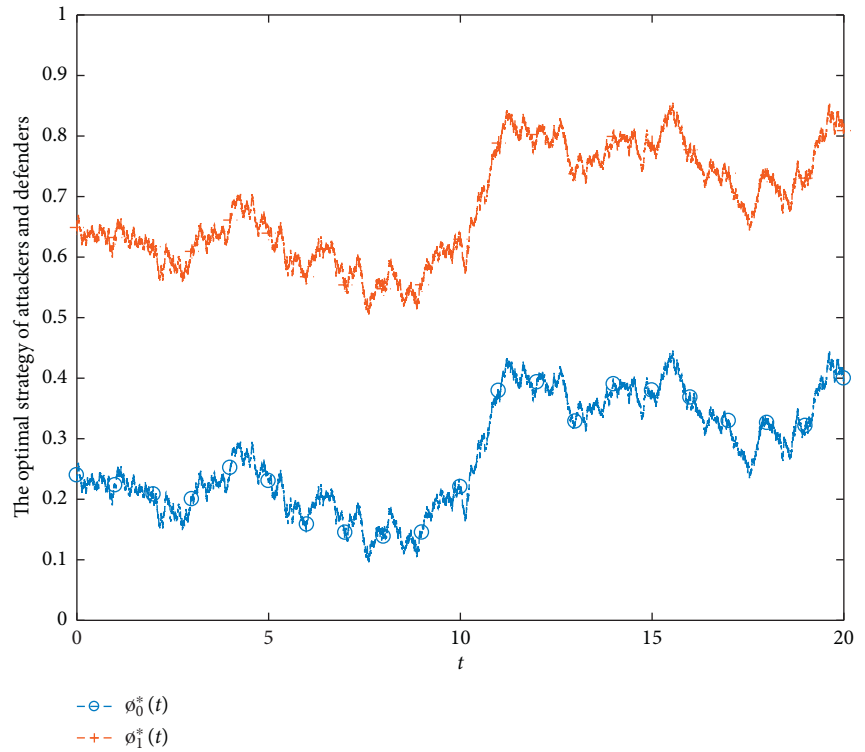

Figure 4: The optimal strategy with given parameters.

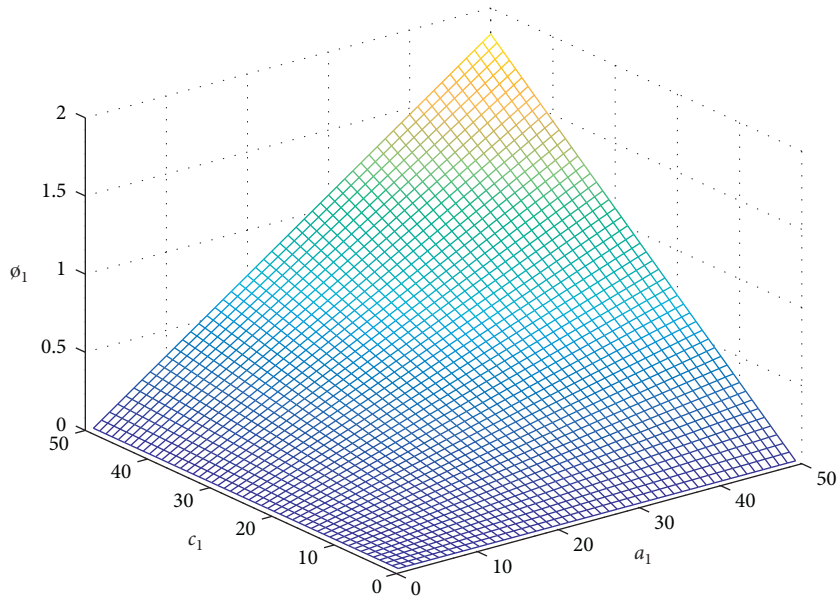

Figure 5: The change of the optimal strategy of the attackers with a_0 and c_0.

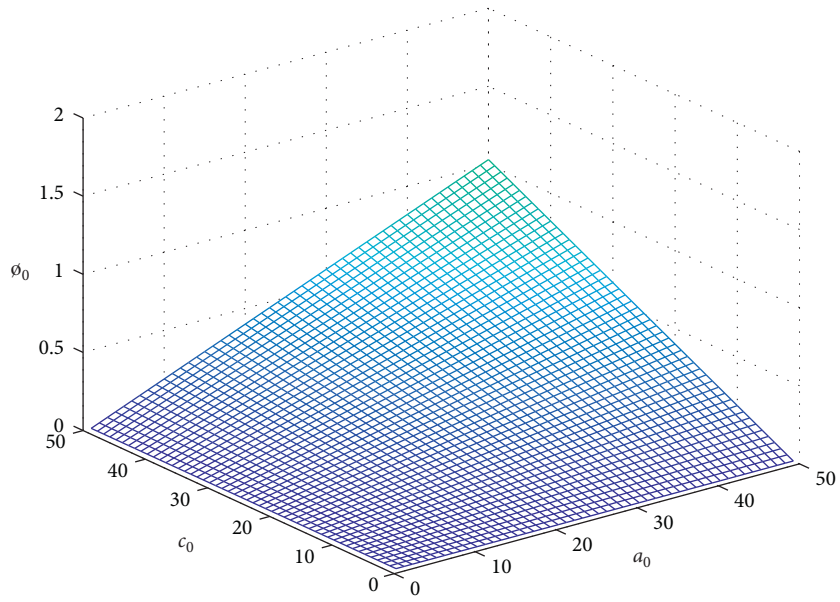

Figure 6: The change of the optimal strategy of the defenders with a_1 and c_1.

can be seen that the level of the optimal strategy of attackers increases with the increase of a_0 and c_0 while the level of the optimal strategy of defenders increases with the increase of a_1 and c_1. As shown in the results, the level of the optimal strategy of defenders grows faster.

The comparison of proposed model with the existing model [23] is shown in Figure 7; it can be seen that the number of infected devices in both models is rapidly increased with the time variation and then decreased. The number of infected devices in the proposed model is less

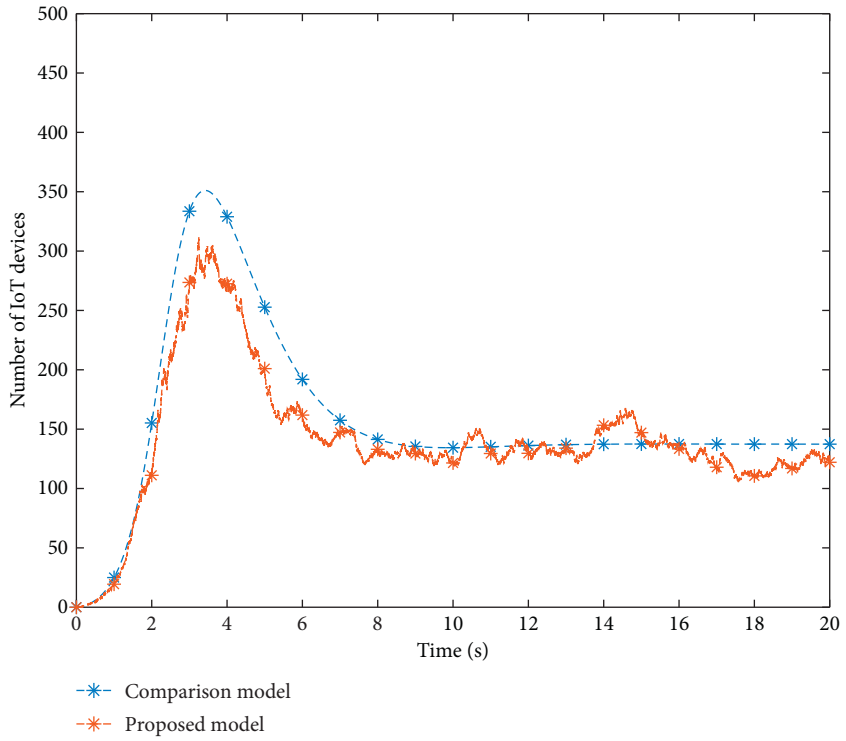

Figure 7: The comparison between the proposed model and the comparative model.

than that of the comparative model, which means that the proposed security strategy is more effective and more suitable for IoT environment.

6. Conclusions

In this paper, we have proposed an infinite-horizon stochastic differential game model to study the malware propagation problem under the dynamic interaction between the attackers and defenders in the edge computing-based IoT environment that is composed by N IoT devices and to maximize the profit for both the attackers and defenders. In terms of model construction, we assumed that the states of IoT devices were infected, susceptible, exposed, and recovered and considered the effect of the stochastic fluctuations of the network on the state of the IoT devices. By solving the feedback Nash equilibrium solutions for our proposed game model, we obtained the optimal strategies for both the attackers and defenders. Based on the simulations results, it can be seen that the proposed model can prevent the malware propagation in edge computing-based IoT. In future work, we will apply this model to other resource-constrained environments.

Data Availability

The data used in this paper are given in Table 1.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was supported by the Science and Technology Innovation Team of Big Data Intelligent Technology and Application (030103060053) and the Computer Science and Technology (030900002009).

References

[1] D. He, S. Chan, and M. Guizani, "Security in the internet of things supported by mobile edge computing," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 56–61, 2018.

[2] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[3] C. Majumdar, M. López-Benítez, and S. N. Merchant, "Real smart home data-assisted statistical traffic modeling for the internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4761–4776, 2020.

[4] N. Hassan, S. Gillani, E. Ahmed, I. Yaqoob, and M. Imran, "The role of edge computing in internet of things," *IEEE Communications Magazine*, vol. 99, pp. 1–6, 2018.

[5] Y. Zhang, Y. Wu, H. Moustafa, A. Leon-Garcia, and U. Javaid, "Multi-access mobile edge computing for heterogeneous iot," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 12-13, 2018.

[6] J. Pan and J. McElhannon, "Future edge cloud and edge computing for internet of things applications," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 439–449, 2018.

[7] P. Guan, X. Deng, Y. Liu, and H. Zhang, "Analysis of multiple clients' behaviors in edge computing environment," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 9052–9055, 2018.

[8] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey and open issues," *IEEE Access*, vol. 6, pp. 18209–18237, 2018.

[9] Ai Yuan, M. Peng, and K. Zhang, "Edge computing technologies for internet of things: a primer," *Digital Communications and Networks*, vol. 4, no. 2, pp. 77–86, 2018.

[10] W. Tobias, A. Cislak, M. Ochoa, and P. Alexander, "Leveraging compression-based graph mining for behavior-based malware detection," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 1, 2017.

[11] T. Kim, B. Kang, M. Rho, S. Sezer, and E. G. Im, "A multimodal deep learning method for android malware detection using various features," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 3, pp. 773–788, 2019.

[12] A Dehghantanha, A Azmoodeh, and K.-K. R Choo, "Robust malware detection for internet of (battlefield) things devices using deep eigenspace learning," *IEEE Transactions On Sustainable Computing*, vol. 99, 2018.

[13] I. Indre and C. Lemnaru, "Detection and prevention system against cyber attacks and botnet malware for information systems and internet of things," in *2016 IEEE 12th International Conference on Intelligent Computer Communication and Processing (ICCP)*, pp. 175–182, Cluj-Napoca, Romania,, September 2016.

[14] L. Liu and K. L Ryan, G. Ren and X. Xu, Malware propagation and prevention model for time-varying community networks within software defined networks." *Security and Communication Networks*, vol. 2017, Article ID 2910310, 10 pages, 2017.

[15] M. H. R. Khouzani, S. Sarkar, and E. Altman, "Maximum damage malware attack in mobile wireless networks," *IEEE/ACM Transactions on Networking*, vol. 20, no. 5, pp. 1347–1360, 2012.

[16] V. Karyotis and M. H. R Khouzani, *Malware Diffusion Models for Modern Complex Networks: Theory and Applications*, Morgan Kaufmann, Burlington, MA, USA, 2016.

[17] J. Moura and D. Hutchison, "Game theory for multi-access edge computing: survey, use cases, and future trends," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 260–288, 2019.

[18] M. Abdalzaher, K. Seddik, M. Elsabrouty, O. Muta, H. Furukawa, and A. Abdel-Rahman, "Game theory meets wireless sensor networks security requirements and threats mitigation: a survey," *Sensors*, vol. 16, no. 7, p. 1003, 2016.

[19] T. Spyridopoulos, K. Maraslis, A. Mylonas, T. Tryfonas, and O. George, "A game theoretical method for cost-benefit analysis of malware dissemination prevention," *Information Security Journal: A Global Perspective*, vol. 24, no. 4–6, pp. 164–176, 2015.

[20] D. L. Quang, Q. S Tony, J. Lee, S. Jin, and H. Zhu, "Deceptive attack and defense game in honeypot-enabled networks for the internet of things," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 1025–1035, 2016.

[21] W. Liao, S. Salinas, M. Li, P. Li, and K. A. Loparo, "Cascading failure attacks in the power system: a stochastic game perspective," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 2247–2259, 2017.

[22] H. Sedjelmaci, S. M. Senouci, and T. Taleb, "An accurate security game for low-resource iot devices," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 10, pp. 9381–9393, 2017.

[23] R. Kaur, N. Kaur, and S. K. Sood, "Security in iot network based on stochastic game net model," *International Journal of Network Management*, vol. 27, no. 4, Article ID e1975, 2017.

[24] S. Shen, L. Huang, H. Zhou, S. Yu, E. Fan, and Q. Cao, "Multistage signaling game-based optimal detection strategies for suppressing malware diffusion in fog-cloud-based iot networks," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1043–1054, 2018.

[25] D. W. K Yeung and L. A Petrosjan, *Cooperative Stochastic Differential Games*, Springer Science & Business Media, Berlin, Germany, 2006.

[26] R. M Anderson and R. M May, *Infectious Diseases of Humans: Dynamics and Control*, Oxford University Press, Oxford, UK, 1992.

[27] X. Mao, *Stochastic Differential Equations and Applications*, Elsevier, Amsterdam, Netherlands, 2007.

[28] T. Alpcan and T. Başar, *Network Security: A Decision and Game-Theoretic Approach*, Cambridge University Press, Cambridge, UK, 2010.