Hindawi
Security and Communication Networks
Volume 2020, Article ID 3417039, 15 pages
https://doi.org/10.1155/2020/3417039

Research Article

Study on Stochastic Differential Game Model in Network Attack and Defense

Xiaotong Xu, Gaocai Wang, Jintian Hu, and Yuting Lu

School of Computer, Electronics, and Information, Guangxi University, Nanning, China

Correspondence should be addressed to Gaocai Wang; wanggcgx@163.com

Received 28 August 2019; Revised 5 December 2019; Accepted 19 February 2020; Published 8 June 2020

Academic Editor: David Megias

In recent years, evolutionary game theory has been gradually applied to analyze and predict network attack and defense for maintaining cybersecurity. The traditional deterministic game model cannot accurately describe the process of actual network attack and defense due to changing in the set of attack-defense strategies and external factors (such as the operating environment of the system). In this paper, we construct a stochastic evolutionary game model by the stochastic differential equation with Markov property. The evolutionary equilibrium solution of the model is found and the stability of the model is proved according to the knowledge of the stochastic differential equation. And we apply the explicit Euler numerical method to analyze the evolution of the strategy selection of the players for different problem situations. The simulation results show that the stochastic evolutionary game model proposed in this paper can get a steady state and obtain the optimal defense strategy under the action of the stochastic disturbance factor. In addition, compared with other kinds of literature, we can conclude that the return on security investment of this model is better, and the strategy selection of the attackers and defenders in our model is more suitable for actual network attack and defense.

1. Introduction

With the development of the Internet, the security of the network and the privacy of users have been greatly disturbed. Therefore, the issues of cybersecurity have caused people's high attention. The security of the Internet has become one of the important factors hindering the development of information technology. It is impossible to guarantee the security of cyberspace by relying on some passive defense measures in the increasing complexity of the network environment. Therefore, it is especially necessary to find new technologies that can detect the potential danger of network environment and take defense measures.

In the network attack and defense, intruders can carry out an intrusion and the computer network can resist attack, which is similar to the process of the evolutionary game. Therefore, quite a lot of research studies have established a network attack and defense game model to select the optimal strategy [1–6]. The study of game theory first appeared in the field of economics research. In 1944, John von Neumann and Oskar Morgenstern proposed "game theory and economics," which received wide attention [7]. Evolutionary game is a theory that combines game theory with the dynamic evolution process. It adopts the evolutionary theory of biology based on traditional game theory. The development of evolutionary game theory in various fields can be attributed to Smith (1973) and Price (1974) [8], who proposed the basic concept: Evolutionary Stable Strategy (ESS). Among them, the participants are the bounded rationality (between completely rational and incompletely rational). The players between groups constantly correct, imitate, and improve during the evolution process. They gradually tend to a certain stability strategy and eventually reach a state of equilibrium in the game. And players get the best strategy (to maximize their profits) in this state. In the field of cybersecurity, the traditional evolutionary game model does not consider the external environment and strategy mutation, which leads to the limitation of the evolution trend. The prejudgment of network attack and defense is also not accurate enough. Therefore, researchers tried to further

improve the effectiveness of the model and more accurately describe the evolutionary game of attack and defense by using stochasticity [9–25]. In the stochastic game of this paper, the attackers will try to interfere or destroy the network environment. The defenders (network environment) can enhance the defensive ability by increasing defensive investments. Based on the principle of bounded rationality, the players gradually evolve into a stable state by learning and improving. The accuracy of the defenders' choice of the optimal strategy has been effectively improved and the security of cyberspace has been guaranteed.

The main contributions of this paper are as follows.

(1) The network attack and defense stochastic game model is constructed under incompletely rational conditions. We use stochastic differential equations to consider the randomness caused by external factors in the process of attack-defense. And we construct the stochastic replication dynamic equation to further accurately describe the evolution of the network attack and defense strategy.

(2) The attack lethality coefficient is used to describe the impact of different attack strategies on players. Furthermore, the model proposed in this paper is compared with other kinds of literature by the defenders' payoffs, which further proves that the model proposed in this paper is more suitable for the actual situation of the network attack and defense.

(3) The selection algorithm of the optimal defense strategy under this model is designed. This algorithm can provide effective support for active defense in the process of network attack and defense.

The remainder of this paper is organized as follows. Related work is discussed in Section 2. In Section 3, the network attack and defense stochastic differential game model and corresponding concepts are described and analyzed. In Section 4, the stochastic differential game optimal defense strategy algorithm is introduced. Simulation experiments and results analysis are presented in Section 5. Finally, this paper is concluded in Section 6.

2. Related Work

The application of evolutionary game theory in cybersecurity has become a study boom in recent years. In the actual attack and defense process, the change of the system operating environment and the disturbance of other external factors have stochasticity. Therefore, researchers began to introduce stochastic evolutionary game theory into the study of cybersecurity. There are two main aspects of concern: the first is to consider the offensive and defensive process as a random jump between multistates. The other is to construct a stochastic evolutionary game using stochastic differential equations.

In the analysis of the vulnerability of the network environment, the authors in [9] studied the security and reliability issues of software and hardware services. They built the Markov chain to construct a stochastic evolution alliance game to evaluate the optimal strategy, and the model can be applied to various defensive scenarios in the cloud computing network. From the perspective of attack and defense, the authors in [10] utilized the game model to find network vulnerability state and established the mapping relationship between attack and defense states. They quantified the level of network vulnerability and proposed a hidden Markov model. On this basis, they accurately inferred the attacking intent using the Viterbi algorithm. Govaert et al. modeled system dynamics as a discrete-time Markov process [11], which identifies equilibrium states and periods. And, in any initial state, it can converge to a balanced state for a limited time. The above literature [9–11] utilizes the Markov process, which can accurately characterize the stochastic behavior of the network system and the interrelationship between components. And it is convenient for calculating various safety targets. Wang et al. established an attack and defense game model based on stochastic Petri nets [12], which can analyze and evaluate the attack success rate, average attack time, vulnerable nodes, and potential attack paths of the target network. He et al. [13] defined the Stochastic Colored Petri Nets (SCPN) based on the Internet of Things (IoT) when studying the offensive and defensive scenarios of the smart home and obtained the game model of security situational awareness. It can effectively predict the attacker's potential attack strategy and achieve the purpose of promoting defense strategy selection. Talukder et al. [14] found that it is necessary to construct a suitable model to express the spread of threats in mobile IP. Talukder proposed four common mobile IP attacks and used SCPN as model, which effectively reduced the probability of successful attackers. To assess the risk of intrusion, El Bouchti and Nahhal [15] introduced the process and rules of constructing an SCPN model using attack trees and showed how to transform and analyze the attack tree in Stochastic Game Nets (SGN). Fanti et al. [16] proposed a network model of satellite base station (SBS) affected by attack and defense. The optimal defense strategy was obtained by calculating the Nash equilibrium, and the model was able to obtain the evolution equilibrium state under the stochastic game rules. The above literature [12–16] has a strong dynamic analysis ability for the concurrency, asynchrony, and uncertainty of the system. It has the advantages of less modeling language and intuitive graphical representation that can describe the state and behavior of the system. It has some functions that other methods do not have, such as system description, security analysis, and system testing. It can be accomplished graphically in the system model framework. However, these methods do not consider the issue of the participants' payoffs and costs.

Huang et al. [17] found that the attack and defense strategy usually changes dynamically and continuously. Therefore, Huang used the Ito stochastic differential equation to construct a stochastic evolutionary game from the perspective of the actual attack and defense. The model accurately shows the evolution process of attack and defense by analyzing the continuous game evolution. The process of path discovery was modeled as a noncooperative stochastic evolution game when Wang et al. [18] studied radio network

security. It was carried out by distributed strategy learning at each stage of the game process, which effectively bypassed the malicious nodes of the hybrid attack strategy. Wei et al. [19] designed the optimal load shedding technique to quantify the physical impact of the coordinated attack. For the interaction between attackers and defenders, the stochastic game model is proposed to select the optimal defense strategy and protect the network. The above literature [17–19] uses stochastic differential equations to describe the stochastic evolution process. It considers the direct impact of network security incidents and can effectively prevent malicious threats.

In addition, Riehl and Cao [20] introduced a hierarchical approximation algorithm while studying the stochastic evolutionary games. It can search the required strategies in stochastic evolutionary games and find the optimal results of the network attack and defense. Liu et al. [21] integrated multiple network security elements (such as assets, threats, and vulnerabilities) of multisensor mobile phones into standard data sets to improve the awareness of network security. The Nash equilibrium of the hybrid strategy is calculated by the stochastic game model, and the security status of the network is evaluated effectively, comprehensively, and accurately. Subbulakshmi et al. [22] constructed a stochastic evolutionary game model to analyze the destructive techniques related to radio networks. The model evaluated the optimal solution to improve network performance. Kumar et al. [23] proposed a stochastic alliance game to realize data distribute in-vehicle network physical systems (VCPS) when studying the safety and comfort of the in-vehicle network. Vehicles can access various resources from the cloud environment. These resources help people find optimized strategy selection by transmitting short-range, medium-range, and remote information. Arfaoui et al. [24] proposed a stochastic game model to balance network performance and security. The model is more efficient than the basic algorithm in terms of network lifecycle and throughput. Chen and Yeh [25] discussed the robustness of noncooperative evolutionary game strategies from the perspective of stochastic Nash Equilibrium and then explored the application of stochastic evolutionary game theory.

In summary, the researchers regard the attack and defense process as the process of random hopping in multistate when using SCPN for modeling. It can better describe the offensive and defensive processes, but it is difficult to avoid the conditions that need to satisfy the complete information. Researchers constructed stochastic differential models with incomplete information by using stochastic differential equations, which can effectively describe the network attack and defense process. However, most literature is limited to a specific network environment for attack and defense confrontation, which leads to low versatility. Aiming at the existing research results, this paper studies and proposes a stochastic differential game model of network attack and defense that introduces the stochastic differential equation, and the model has Markov property. Based on the network attack and defense scenario, the evolution trend of the behavior strategies of the network attack and defense groups is analyzed. We find the optimal defense strategy and effectively analyze the behaviors of the attack and defense strategy on this basis.

3. Network Attack and Defense Stochastic Differential Game Model

The attack and defense groups choose different strategies for the game based on the incomplete rationality of attackers and defenders. Both sides constantly try to adjust and improve their decision-making methods in the process of attack and defense and form a new situation of the game finally. This process also highlights the dynamic equilibrium of evolutionary game theory.

3.1. Model Definition. The players will always suffer from some uncertain factors in the actual network attack and defense. Therefore, this paper defines the Network Attack-Defense Stochastic Differential Game Model (NADSDGM).

Definition 1. The network attack and defense stochastic differential game model is defined as a quaternion model NADSDGM = (N, S, U, τ), where we have the following:

(a) $N = (N_A, N_D)$ represents the players in the attack and defense evolution game, that is, the participants who adopt strategies in the game. The participants have different meanings in different environments. They can represent individuals and can also represent a team or a group of multiple teams. Among them, N_A are the attackers and N_D are the defenders (defense system).

(b) $S = (S_A, S_D)$ represents the set of strategies of the players in the game; it is the tool and means for the players to play the game, where $S_A = (S_{A1}, S_{A2}, \ldots, S_{Am})$ represents the set of attack strategies and $S_D = (S_{D1}, S_{D2}, \ldots, S_{Dn})$ represents the set of defense strategies. For the attackers, there are m strategies for attacking. Correspondingly, there are n strategies for implementing defense by the defenders.

(c) $U = (U_A, U_D)$ is the set of payoff functions of the players. $U_A = (U_A^0, U_A^1)$. U_A^0 represents the payoffs of the attackers when the attack is not performed, and U_A^1 represents the payoffs of the successful attack by the attackers. $U_D = (U_D^0, U_D^1)$. U_D^0 represents the expected payoffs when the defenders do not make a defensive investment, and U_D^1 represents the expected payoffs of the defenders after defensive investment.

(d) $\tau = (\tau_0, \tau_1)$ indicates stochasticity. Among them, $\tau_0 = 0$ indicates that the model does not use stochastic disturbance factors. $\tau_1 = 1$ indicates that the model uses stochastic disturbance factors.

3.2. Parameter Quantization. In the analysis of the attack and defense evolution game, we first define some relevant parameters to be convenient for the quantification of the payoffs.

Definition 2. Attack cost C_A: this indicates the financial and material resources that the attackers need to perform the attack.

The defenders do not invest in a defensive strategy, whether the attackers can successfully implement the attack depends only on the defenders' system vulnerabilities, and the attack cost at this time is C_A^0. When the defenders make defensive investments, it will increase the attacking difficulty of the attackers, and the attack cost is C_A^1 . Obviously, $C_A^0 < C_A^1$.

Definition 3. Incentive mechanism remuneration R: this represents the third-party regulator's reward for the defenders.

In today's information age, the degree of possession of information resources and monopoly determine benefits. The main reason why the target network is attacked is that the information is not public and opaque, and the attackers want to obtain certain information through the attack. Therefore, social regulators use incentive mechanisms to motivate defenders to properly publish information and share resources without harming their interests. The society that benefits from this will also reward defenders. To reduce the damage caused by the defense system being attacked, the defenders choose appropriate public information to receive social rewards. The more beneficial the public information is to society, the more rewards the incentives will generate. R represents the remuneration for the incentive mechanism. The remuneration is R_0 when the defenders do not make a defensive investment. When the defenders make defensive investments, the remuneration is R_1.

Definition 4. Penalty cost G: this means that the third-party regulator punishes attackers who have committed attacks.

Internet attacks can lead to a series of cybersecurity issues, such as the users' data being leaked and the network's services being forced to be interrupted. It affects people's daily work and life and even affects the country's safety in case of seriousness. Therefore, it is the responsibility of the third-party regulatory authority to punish the attackers for violating the cybersecurity. G is used to indicate the punishment of the attackers by the supervisor. When the defenders do not make a defensive investment, the attackers receive the penalty of G_0. Correspondingly, when the defenders take defensive investments, the attackers receive the penalty of G_1.

Definition 5. Attack lethality coefficient λ and defender loss l.

In actual network attack and defense, for different attack strategies, the defenders' loss is affected by the lethality of the attack. Assume that the total loss caused by a network attack to the defenders is l. The more lethal the attack strategy is, the less likely the defenders are to resist successfully, and the greater the loss suffered, that is, the greater the loss suffered by the defenders. On the contrary, the weaker the lethality of the attack strategy, the smaller the loss suffered by the defenders.

Let attack lethality coefficient be

$$\lambda = \lambda(k) = \begin{cases} 1, & k = m, \\ e^{-(1/k)}, & 1 \le k < m, \\ 0, & k = 0. \end{cases} \quad (1)$$

Among them, m represents the attack dangerous level ($m \in N^*$), and the lethality coefficient of attack changes under the influence of the dangerous degree of attack strategy.

We define $l = \lambda L$. When the attack dangerous level is not enough to hurt the defenders, the loss of the defenders is 0. When the attack dangerous level is at $1 \le k \le m$, the defenders can take remedial measures in time to reduce part of the loss. At this time, the attack lethality coefficient is $e^{-(1/k)}$, and the defenders' loss is $l = e^{-(1/k)}L$. When the attack dangerous level is large enough, it can be regarded as attack lethality coefficient being 1 and defenders' loss being $l = L$.

Definition 6. Total return E: this represents the total return that the attackers can obtain from a successful attack.

When the defenders adopt defensive investment strategies, the payoffs of the attackers' successful attack are $P_1E - C_A^1 - G_1$. When the defenders do not adopt defensive investment strategies, the payoffs of the attackers' successful attack are $P_0E - C_A^0 - G_0$.

Additionally, the defenders as the target network are also capable of a certain defense. But to protect their infrastructure and information assets from harm, defenders can choose to increase their defensive investments against network attacks. Assume that the defenders' original defensive infrastructure and informational assets are collectively called the original asset V_0, and the investment cost per time is V_{add}. Therefore, before and after the defensive investment by the defenders, the losses caused by the network attack are P_0l and P_1l, respectively. When the attackers successfully attack, if the defenders choose defensive investment strategies, their expected payoffs are $V_0 - V_{\text{add}} - P_1l + R_1$. And if the defenders do not adopt a defense investment strategy, the expected payoffs are $V_0 - P_0l + R_0$. On the contrary, when the attackers do not take any attack, the attackers' expected payoffs are 0. And the defenders' expected payoffs before and after the defensive investment strategy are $V_0 + R_0$ and $V_0 - V_{\text{add}} + R_1$.

The main parameters and descriptions involved above are shown in Table 1.

3.3. Stochastic Differential Equation. Assume that, in the process of attack and defense games, the proportion of attack strategies adopted by the attackers' groups is x, and the proportion of adopting nonattack strategies is $1 - x$. The proportion of defensive investment strategies and nondefensive investment strategies in the defenders' group is y and $1 - y$, respectively. Using the above parameters, the payoff matrix of the network attack and defense evolutionary game model is shown in Table 2.

Use U_D^1 to indicate the expected payoffs of the defenders when the defenders choose to invest in the defense strategy, and U_D^0 indicates the expected payoffs of the defenders when

Table 1: Main parameters and descriptions.

Parameter	Description
C_A^0	Attackers' required attack cost before defensive investment
C_A^1	Attackers' required attack cost after defensive investment
P_0	Probability of successful attack before defensive investment
P_1	Probability of successful attack after defensive investment
V_0	Defenders' original defensive ability (original assets)
V_{add}	Defenders' increased defensive ability (defensive investment)
R	The social rewards for defenders' public information
G	The attackers are punished for the attack
l	The loss suffered by the defenders after being attacked
E	The total return from a successful attack by the attackers

the defenders do not invest in the defense strategy. From the above payoff matrix, we can know

$$\begin{aligned} U_D^1 &= x\left(V_0 - V_{\text{add}} - P_1 l + R_1\right) + (1-x)\left(V_0 - V_{\text{add}} + R_1\right) \\ &= -xP_1\lambda L + V_0 - V_{\text{add}} + R_1, \end{aligned} \tag{2}$$

$$\begin{aligned} U_D^0 &= x\left(V_0 - P_0 l + R_0\right) + (1-x)\left(V_0 + R_0\right) \\ &= -xP_0\lambda L + V_0 + R_0. \end{aligned} \tag{3}$$

Use $\overline{U_D}$ to indicate the average payoffs of the defenders, which can be obtained by equations (2) and (3)

$$\begin{aligned} \overline{U_D} &= yU_D^1 + (1-y)U_D^0 \\ &= y\left[x\lambda L\left(P_0 - P_1\right) + \left(R_1 - R_0\right) - V_{\text{add}}\right] - x\lambda P_0 L + V_0 + R_0. \end{aligned} \tag{4}$$

Correspondingly, U_A^1 indicates the expected payoffs of the attackers when the attackers adopt the attack strategy, and U_A^0 indicates the payoffs of the attackers when the attackers do not adopt the attack strategy; that is,

$$\begin{aligned} U_A^1 &= y\left(P_1 E - C_A^1 - G_1\right) + (1-y)\left(P_0 E - C_A^0 - G_0\right) \\ &= -y\left[\left(P_0 E - P_1 E_1\right) + \left(G_1 - G_0\right) + \left(C_1 - C_0\right)\right] \\ &\quad + \left(P_0 E - C_0 - G_0\right), \end{aligned} \tag{5}$$

$$U_A^0 = 0. \tag{6}$$

Use $\overline{U_A}$ to indicate the average payoffs of the attackers, which is available from equation (5) and (6)

$$\begin{aligned} \overline{U_A} &= xU_A^1 + (1-x)U_A^0 \\ &= -xy\left[\left(P_0 E - P_1 E_1\right) + \left(G_1 - G_0\right) + \left(C_1 - C_0\right)\right] \\ &\quad + x\left(P_0 E - C_0 - G_0\right). \end{aligned} \tag{7}$$

According to the above analysis, the replication dynamic equation of the offensive and defensive evolution game model is obtained. From (5) and (7), the attackers' replication dynamic equation is

$$\begin{aligned} \mathrm{d}x(t) &= x\left(U_A^1 - \overline{U_A}\right)\mathrm{d}t \\ &= x(1-x)\{-y\left[\left(P_0 E - P_1 E_1\right) + \left(G_1 - G_0\right) + \left(C_1 - C_0\right)\right] \\ &\quad \left(P_0 E - C_0 - G_0\right)\}\mathrm{d}t. \end{aligned} \tag{8}$$

The defenders' replication dynamic equation is obtained by equation (2) and (4)

$$\begin{aligned} \mathrm{d}y(t) &= y\left(U_D^1 - \overline{U_D}\right)\mathrm{d}t \\ &= y(1-y)\left[x\lambda L\left(P_0 - P_1\right) + \left(R_1 - R_0\right) - V_{\text{add}}\right]\mathrm{d}t. \end{aligned} \tag{9}$$

In order to characterize stochastic disturbance factors, the common method is to add a stochastic disturbance after replication dynamic equation. It satisfies the Gaussian hypothesis and obeys the normal distribution, which can reflect the stochastic effects caused by many tiny factors. Common Markov processes include Poisson process and Wiener process, and white noise has become a kind of stochastic disturbance commonly used in system analysis [17]. Therefore, this paper uses the white noise process as a stochastic disturbance in the game process, and (8) and (9) are modified to obtain

$$\begin{cases} \mathrm{d}x(t) = x(1-x)\{\left(V_0 - V_{\text{add}} + R_1\right) - \left(V_0 + R_0\right) + \left[\lambda L\left(P_0 - P_1\right)\right]y\}\mathrm{d}t + \tau x(1-x)y\,\mathrm{d}\theta_1(t), \\ \mathrm{d}y(t) = y(1-y)\{\left(P_0 E - C_A^0 - G_0\right) + \left[\left(P_1 E - C_A^1 - G_1\right) - \left(P_0 E - C_A^0 - G_0\right)\right]x\}\mathrm{d}t + \tau y(1-y)x\,\mathrm{d}\theta_2(t), \\ \mathrm{d}\theta_1(t)\mathrm{d}\theta_2(t) = \mathrm{d}t, \end{cases} \tag{10}$$

where $\mathrm{d}\theta_1(t)\mathrm{d}\theta_2(t)$ represents the Wiener process; it has Markov property.

4. Optimal Defense Strategy Selection

In this section, the evolutionary equilibrium solution and stability analysis of the stochastic equation are firstly proved, and then the optimal strategy selection algorithm is given.

4.1. Evolutionary Equilibrium Solution. Because the stochastic game model proposed in this paper is composed of nonlinear Ito stochastic differential equations, the analytical solution of the equations cannot be obtained directly. Therefore, in this section, we first prove that the stochastic differential equation presented in this paper has a unique solution (i.e., satisfying the local Lipschitz condition and the linear growth condition [26–29]). And in the following

Table 2: Differential game expectation payoff matrix.

Defender/attacker	Attack	No attack
Investment	$V_0 - V_{\text{add}} - P_1 l + R_1$ and $P_1 E - C_A^1 - G_1$	$V_0 - V_{\text{add}} + R_1$, 0
No investment	$V_0 - P_0 l + R_0$ and $P_0 E - C_A^0 - G_0$	$V_0 + R_0$, 0

Section 5.2, we use the explicit Euler numerical method to find the solution, so as to obtain the corresponding evolutionary equilibrium solution of attack and defense.

Theorem 1. *The parameters in Table 1 are known, for $x \in [0,1]$, $y \in [0,1]$, $q \in [0,1]$, $t \in [0,T]$, and $\tau = 1$; equation (10) has a unique solution.*

Proof. We rewrite equation (10)

$$\mathrm{d}x(t) = f_1(x,y)\mathrm{d}t + g_1(x,y)\mathrm{d}\theta_1(t), \tag{11}$$

$$\mathrm{d}y(t) = f_2(x,y)\mathrm{d}t + g_2(x,y)\mathrm{d}\theta_2(t). \tag{12}$$

Among them,

$$\begin{aligned} f_1(x,y) &= x(1-x)\{(V_0 - V_{\text{add}} + R_1) - (V_0 + R_0) \\ &\quad + [\lambda L(P_0 - P_1)]y\}, \\ f_2(x,y) &= (1-y)\left\{\left(P_0 E - C_A^0 - G_0\right) + \left[\left(P_1 E - C_A^1 - G_1\right)\right.\right. \\ &\quad \left.\left. - \left(P_0 E - C_A^0 - G_0\right)\right]x, \\ g_1(x,y) &= x(1-x)y, \\ g_2(x,y) &= y(1-y)x. \end{aligned} \tag{13}$$

Obviously, $f_1(x,y)$, $f_2(x,y)$, $g_1(x,y)$, and $g_2(x,y)$ are continuous on $[0,1] \times [0,1]$.

For equation (11), we first verify that it satisfies the local Lipschitz condition. For any x and x^* in $[0,1]$, then

$$\begin{aligned} \left|f_1(x,y) - f_1(x^*,y)\right| &= \left|x(1-x)\{(V_0 - V_{\text{add}} + R_1) - (V_0 + R_0) + [\lambda L(P_0 - P_1)]y\} - x^*(1 - x*)\right. \\ &\quad \left. \cdot \{(V_0 - V_{\text{add}} + R_1) - (V_0 + R_0) + [\lambda L(P_0 - P_1)]y\}\right| \\ &= \left|\{(V_0 - V_{\text{add}} + R_1) - (V_0 + R_0) + [\lambda L(P_0 - P_1)]y\}[x(1-x) - x^*(1-x^*)]\right| \\ &= \left|(V_0 - V_{\text{add}} + R_1) - (V_0 + R_0) + [\lambda L(P_0 - P_1)]y\right| \cdot \left|x - x^*\right| \cdot \left|1 - x - x^*\right| \\ &\le \left|x - x^*\right|\left\{\left|(V_0 - V_{\text{add}} + R_1) - (V_0 + R_0)\right| + \left|[\lambda L(P_0 - P_1)]y\right|\right\} \cdot \left|1 - x - x^*\right| \\ &\le \left|x - x^*\right|\left[\left|(V_0 - V_{\text{add}} + R_1) - (V_0 + R_0)\right| + \left|\lambda L(P_0 - P_1)\right|\right]. \end{aligned} \tag{14}$$

Therefore,

$$\left|f_1(x,y) - f_1(x^*,y)\right|^2 \le M_1 \left|x - x^*\right|^2, \tag{15}$$

where $M_1 = [|(V_0 - V_{\text{add}} + R_1) - (V_0 + R_0)| + |\lambda L(P_0 - P_1)|]^2$ is the positively constant.

In addition,

$$\begin{aligned} \left|g_1(x,y) - g_1(x^*,y)\right|^2 &= \left|x(1-x)y - x^*(1-x^*)y\right|^2 \\ &= \left|(x - x^*)(1 - x - x^*)y\right|^2 \\ &= \left|x - x^*\right|^2 \cdot \left|1 - x - x^*\right|^2 \cdot |y|^2 \\ &\le \left|x - x^*\right|^2. \end{aligned} \tag{16}$$

Let $M = \max\{M_1, 1\}$; then

$$\begin{aligned} &\max\left\{\left|f_1(x,y) - f_1(x^*,y)\right|^2, \left|g_1(x,y) - g_1(x^*,y)\right|^2\right\} \\ &\quad \le M \cdot \left|x - x^*\right|^2. \end{aligned} \tag{17}$$

Therefore, when $y \in [0,1]$, equation (11) satisfies the local Lipschitz condition.

Next, we verify that equation (11) satisfies the condition of linear growth. For any x in $[0,1]$, then

$$\begin{aligned} \left|f_1(x,y)\right|^2 &= \left|x(1-x)\{(V_0 - V_{\text{add}} + R_1) - (V_0 + R_0) + [\lambda L(P_0 - P_1)]y\}\right|^2 \\ &= |x(1-x)|^2 \cdot \left|(V_0 - V_{\text{add}} + R_1) - (V_0 + R_0) + [\lambda L(P_0 - P_1)]y\right|^2 \\ &\le |x(1-x)|^2 \cdot \left[\left|(V_0 - V_{\text{add}} + R_1) - (V_0 + R_0)\right| + \left|\lambda L(P_0 - P_1)\right|\right]^2 \\ &\le \left(1 + |x|^2\right) \cdot \left[\left|(V_0 - V_{\text{add}} + R_1) - (V_0 + R_0)\right| + \left|\lambda L(P_0 - P_1)\right|\right]^2 \\ &= B_1\left(1 + |x|^2\right), \end{aligned} \tag{18}$$

where $B_1 = [|(V_0 - V_{\text{add}} + R_1) - (V_0 + R_0)| + |\lambda L(P_0 - P_1)|]^2$ is the positively constant.

For $|g_1(x,y)|^2$, we construct function $k(x) = (x^2(1-x)^2y^2)/(1+x^2)$.

By deriving x, we can get $k'(x) = ((2x(1-x)(1-2x-x^3))/(1+x^2)^2)y^2$. Because of $x \in [0,1]$, $y \in [0,1]$, so let $k'(x) > 0$; we can get $2x(1-x)(1-2x-x^3) > 0$. Therefore, let $\eta \in (0,1)$; when $0 < x < \eta < 1$, $z(x)$ is an increasing function. When $0 < \eta < x < 1$, $k(x)$ is an decreasing function.

Consequently,

$$\max_{0 \le x \le 1} k(x) = k(\eta) = \frac{\eta^2(1-\eta^2)y^2}{1+\eta^2} \le \frac{\eta^2(1-\eta^2)}{1+\eta^2}, \tag{19}$$

namely $((x^2(1-x)^2y^2)/(1+x^2)) \le (\eta^2(1-\eta^2)/1+\eta^2)$; that is $|g_1(x,y)|^2 \le B_2(1+x^2)$.

Among them, $B_2 = (\eta^2(1-\eta^2))/1+\eta^2$. Let $B = \max\{B_1, B_2\}$; then

$$\max\left\{\left|f_1(x,y)\right|^2, \left|g_1(x,y)\right|^2\right\} \le B\left(1+|x|^2\right). \tag{20}$$

Therefore, equation (11) satisfies the condition of linear growth.

Well, given $y \in [0,1]$, equation (11) has a unique solution x. Similarly, given $x \in [0,1]$, equation (12) has a unique solution y.

In summary, equation (10) has a unique solution. □

4.2. Evolutionary Stability Analysis. For the stochastic game model constructed, the stability of the game model is proved according to the conclusion described in [26–29], that is, the expected operation of the Ito integral and the exchangeable property of the integral operation.

Theorem 2. *The parameters in Table 1 are known, for $x \in [0,1]$, $y \in [0,1]$, $q \in [0,1]$, $t \in [0,T]$, and $\tau = 1$; the zero solution of equation (10) is stable in the sense of mean square exponential.*

Proof. Equations (11) and (12) are expressed as integral equations as

$$\begin{aligned} x(t) &= x(0) + \int_0^t f_1(x,y)\mathrm{d}q + \int_0^t g_1(x,y)\mathrm{d}\theta_1(q), \\ y(t) &= y(0) + \int_0^t f_2(x,y)\mathrm{d}q + \int_0^t g_2(x,y)\mathrm{d}\theta_2(q), \end{aligned} \tag{21}$$

where $x(0)$ and $y(0)$ are the values when $t = 0$.

Let $m(x,y) = (1/|x(0)|^2)e^{zt}E(|x(t)|^2)$. Among them, $E(\Theta)$ is the expectation and z is the positively constant.

Then,

$$\begin{aligned} m(x,y) &= \frac{1}{|x(0)|^2}e^{zt} \cdot E\left(|x(t)|^2\right) \\ &= \frac{1}{|x(0)|^2}e^{zt} \cdot E\left(\left|x(0) + \int_0^t f_1(x,y)\mathrm{d}q + \int_0^t g_1(x,y)\mathrm{d}\theta_1(q)\right|^2\right) \\ &\le \frac{1}{|x(0)|^2}e^{zt} \cdot E\left(|x(0)|^2 + \left|\int_0^T f_1(x,y)\mathrm{d}q\right|^2 + 2\left|x(0)\int_0^T f_1(x,y)\mathrm{d}q\right| + 2\left|x(0)\int_0^T g_1(x,y)\mathrm{d}\theta_1(q)\right|\right. \\ &\quad \left. + 2\left|\int_0^T f_1(x,y)\mathrm{d}q \int_0^T g_1(x,y)\mathrm{d}\theta_1(q)\right|\right) \\ &\le \frac{1}{|x(0)|^2}e^{zt} \cdot \left\{|x(0)|^2 + \frac{T}{16}\left|\left|(V_0 - V_{add} + R_1) - (V_0 + R_0)\right| + \left|-P_1(L-\lambda L) + P_0(L-\lambda L)\right|\right|^2\right. \\ &\quad + \frac{T}{2}|x(0)|\left(\left|(V_0 - V_{add} + R_1) - (V_0 + R_0)\right| + \left|-P_1(L-\lambda L) + P_0(L-\lambda L)\right|\right) + 4|x(0)| \cdot E\left(\left.\int_0^T \mathrm{d}\theta_1(q)\right)\right\} \\ &= \frac{1}{|x(0)|^2}e^{zt} \cdot \left\{|x(0)|^2 + \frac{T}{2}\left(\left|(V_0 - V_{add} + R_1) - (V_0 + R_0)\right| + \left|-P_1(L-\lambda L) + P_0(L-\lambda L)\right|\right)\right. \\ &\quad \left. \cdot \left[\frac{1}{8}\left(\left|(V_0 - V_{add} + R_1) - (V_0 + R_0)\right| + \left|-P_1(L-\lambda L) + P_0(L-\lambda L)\right|\right) + |x(0)|\right]\right\}. \end{aligned} \tag{22}$$

Thereby,

$$E\left(|x(t)|^2\right) \le N|x(0)|^2 e^{-\mu t}. \tag{23}$$

Among them,

$$\begin{aligned} N = {} & |x(0)|^2 + \frac{T}{2}\left(\left|(V_0 - V_{\text{add}} + R_1) - (V_0 + R_0)\right|\right. \\ & \left.+\left|-P_1(L-\lambda L) + P_0(L-\lambda L)\right|\right) \\ & \cdot \left[\frac{1}{8}\left(\left|(V_0 - V_{\text{add}} + R_1) - (V_0 + R_0)\right|\right.\right. \\ & \left.\left.+\left|-P_1(L-\lambda L) + P_0(L-\lambda L)\right|\right) + |x(0)|\right] > 0, \\ & \mu = z > 0. \end{aligned} \tag{24}$$

That is, for any X_0, there is a constant of $\mu > 0$, $N > 0$, and when $0 \le t \le T$, there is $E(|x(t)|^2) \le N|x(0)|^2 e^{-\mu t}$; then the zero solution of equation (11) can be called the stability on the mean square exponential.

Similarly, for the zero solution of equation (12), the mean square exponential is also stable. □

4.3. The Optimal Defense Strategy Selection Algorithm. In the process of the network attack and defense, the attackers and the defenders play opposite to each other. Each player in the game is constantly testing, adjusting, and improving in the game to maximize their expected returns. Under the guidance of this principle, both attacker's strategy and defenders' strategy will gradually tend to balance. Neither party will try to change this strategy because the party that does not tend to balance will be reducing payoffs. That is to say, the strategy of achieving balance at this time is the optimal strategy. The specific Algorithm 1 is described as follows.

5. Simulation Results and Analysis

In this section, we first set up a network experimental environment. Due to the nonlinearity of the stochastic game model, the model is simulated by the explicit Euler numerical method.

5.1. Experimental Environment. We deploy a network topology environment to simulate the network attack and defense evolution game model proposed in this paper. The validity of the model is proved by analyzing the evolutionary stability strategy.

As shown in Figure 1, in the network topology environment, attack host A is located on the external network and it is used to simulate a variety of attack strategies of attackers. The intranet contains three servers, namely, MySQL Server B, Web Server C, and FTP Server D. The internal network is isolated from the external network by the firewall.

Since the firewall separates the internal network from the external network, the external host can only access Web Server C and FTP Server D through the network. In the intranet, MySQL Server B, Web Server C, and FTP Server D can access each other by using user rights. The Nessus vulnerability scanner is used to perform vulnerability scanning on three server nodes in the network. The server node information is shown in Table 3.

Through the analysis of the vulnerability and attack behavior of each host node in the network, combined with the China National Vulnerability Database of Information Security (CNNVD), the network attack and defense strategies are designed in the experiment, as shown in Tables 4 and 5. Assuming that the network attack strategy is S_{A1} and S_{A2}, the strategy S_{A1} has a high cost, high attack effectiveness, and strong pertinence. Strategy S_{A2} has low cost and low attack effectiveness, which can be considered as not attacking. In addition, assuming that the network defense strategy is S_{D1} and S_{D2} when defending against external attacks, the defenders can increase the cost to take defensive investments or can rely on the existing defense ability to passively defend.

5.2. Explicit Euler Numerical Results. For equation (10), we use the explicit Euler numerical method to simulate it [27]. N is the number of iterations, T is the game time, and the average step size is $H = T/N$.

Let $N(0, 1)$ denote the standard normal distribution and divide $t \in [0, T]$ into $N \in N^+$ equal parts; that is, interval $[0, T]$ is divided into $0 = t_0 < t_1 < \cdots < t_{N-1} < t_N = T$, the average step size is $H = T/N$, and the node is $t_n = nH$.

The Wiener increment is $\Delta w_i(t_n) = w_i(t_n) - w_i(t_{n-1}) \sim \sqrt{H}N(0, 1)$, $i = (1, 2)$, $n = (1, 2, \ldots, N)$, assuming $x_n = x(t_n)$, $y_n = y(t_n)$, $\Delta w_i(t_n) = w_i(t_n)$, and the explicit Euler iteration formula is

$$\begin{cases} x_{n+1} = x_n + x_n(1 - x_{n-1})\{(V_0 - V_{\text{add}} + R_1) - (V_0 + R_0) + [\lambda L(P_0 - P_1)]y_n\} + \tau x_n(1 - x_n)y_n \cdot \Delta w_{1n}, \\ y_{n+1} = y_n + y_n(1 - y_n)\{(P_0 E - C_A^0 - G_0) + [(P_1 E - C_A^1 - G_1) - (P_0 E - C_A^0 - G_0)]x_n\} + \tau y_n(1 - y_n)x_n \cdot \Delta w_{2n}. \end{cases} \tag{25}$$

5.3. Attack-Defense Simulation and Analysis. Stochastic evolutionary game is a kind of stochastic theory which combines game theory analysis with dynamic evolutionary process analysis. In the following, according to the problem situation of x and y, multiple simulation experiments are carried out on the constructed network environment. From the obtained simulation results, the dynamic evolution law of attackers x and defenders y can be analyzed intuitively; the

Input N_A, N_D who participated in the game and host node information.
Output Attack strategy S_A^*, optimal defense strategy S_D^*.
Begin
(1) Initialize NADSDGM = (N, S, U, τ) /∗ Initialize stochastic evolutionary game model∗/
(2) Construct x, y/∗ Construct the group probability of the selected strategy set of both attack and defense ∗/
(3) Constructing a stochastic evolution game matrix between attack and defense
(4) Construct the stochastic differential equation of the attackers and defenders, and see equation (10) for details.
(5) Numerical analysis of the equation using the explicit Euler equation
(6) Back S_A^*, S_D^*
End

Algorithm 1: Optimal defense strategy selection algorithm.

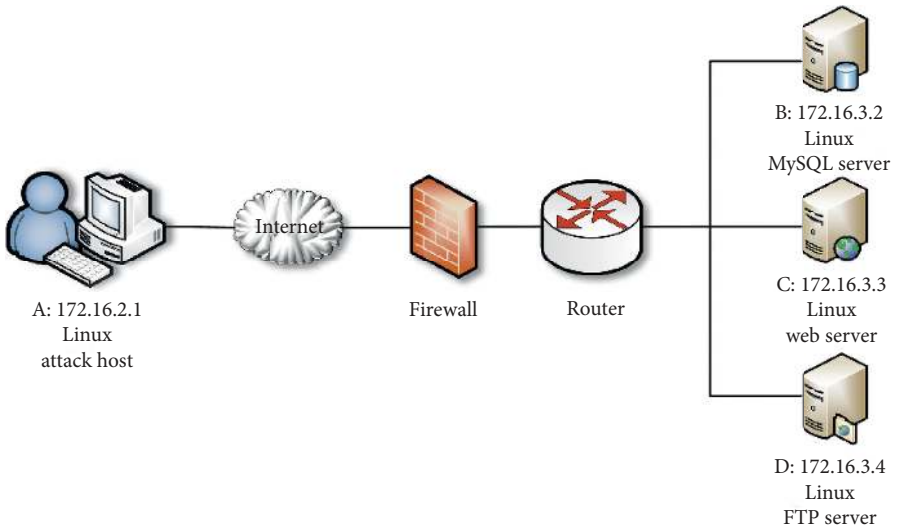

Figure 1: Network topology environment.

Table 3: Server node information.

Host/IP	OS	Server	Vulnerability ID
B 172.16.3.2	Linux	MySQL	CVE-2018-10757
C 172.16.3.3	Linux	ssh	CVE-2016-10012
D 172.16.3.4	Linux	ftp	CVE-2016-9499

Table 4: Atomic attack information.

ID/name	Network attack strategy	
	S_{A1}	S_{A2}
1 Remote buffer overflow		
2 Buffer error	√	
3 Install Web Listener program		√
4 Install delete Trojan	√	
5 Trying to steal account		√
6 FTP server information disclosure	√	
7 Homepage attack	√	
8 Check Point ZoneAlarm		
9 LPC to LSASS process		√
10 SQL injection vulnerability	√	

prediction of attack and defense strategies can be realized. And the evolutionary stability strategy is found, that is, the optimal defense strategy in this state. In the simulation experiment, it is assumed that $\tau = 0$ indicates the evolution of the attack and defense strategy without considering the stochastic disturbance factor. It is too ideal and the

Table 5: Defense strategy information.

ID/name	Network defense strategy	
	S_{D1}	S_{D2}
1 Install MySQL patches	√	
2 Uninstall delete Trojan		√
3 Install sshd patches	√	
4 Limit packets from ports		
5 Delete suspicious account		√
6 Restart database server	√	√
7 Install ftp patches	√	
8 Repair database		
9 Close homepage		√
10 Add physical recourse	√	

stochastic disturbance in the actual attack and defense is not solved. $\tau = 1$ indicates that the game evolution after considering the stochastic disturbance factor is more realistic and more effective.

The problem situation is $x = 0.4$, $y = 0.7$; that is, the attackers in the group select the hybrid strategy $\{S_{A1}, S_{A2}\}$ with the probability of {0.4, 0.6}, and the defenders in the group select the hybrid strategy $\{S_{D1}, S_{D2}\}$ with the probability of {0.7, 0.3}. It can be seen from Figure 2 that, after continuous evolution, the probability of the attackers selecting the strategy S_{A1} gradually tends to 0 and the probability that the defenders select the strategy S_{D1} gradually tends to 1. Both of them reach an evolutionarily stable state. The optimal defense strategy at this time is S_{D1}. Therefore, in this situation, the defenders belong to a more active state of defense. The defense groups are willing to adopt defensive investment strategies for its vulnerability, and it is gradually increasing. The attacker groups gradually turn to the passive state of not taking the attack. The network environment is safer.

Figure 3 shows the experimental results obtained when the problem situation is $x = 0.5$ and $y = 0.6$. The situation indicates that the attackers in the group select the hybrid strategy $\{S_{A1}, S_{A2}\}$ with the probability of {0.5, 0.5} and the defenders select the hybrid strategy $\{S_{D1}, S_{D2}\}$ with the probability of {0.6, 0.4}. As shown in Figure 3, after continuous evolution, the probability that the attackers finally select the attack strategy S_{A1} gradually tends to 1 and the probability that the defenders select the defense strategy S_{D1} gradually tends to 1. Both of them reach an evolutionarily stable state, and the optimal defense strategy at this time is S_{D1}. Analysis of the situation at this moment shows that the attackers and the defenders are actively adopting strategies to participate in the game; the network environment is in a relatively fierce state.

The problem situation is $x = 0.4$ and $y = 0.3$; that is, the attackers in the group select the hybrid strategy $\{S_{A1}, S_{A2}\}$ with the probability of {0.4, 0.6}, and the defenders select the hybrid strategy $\{S_{D1}, S_{D2}\}$ with the probability of {0.3, 0.7}. After continuous evolution, the probability that the attackers finally select the attack strategy S_{A1} gradually tends to 0 and the probability that the defenders select the defense strategy S_{D1} gradually approaches 0. Both of them reach an evolutionarily stable state. The optimal defense strategy at this moment is S_{D2}. Figure 4 is a figure of experimental results in the situation of this problem. Analysis of the situation currently shows that although the network environment is relatively stable, the state of both offense and defense is relatively negative.

The problem situation is $x = 0.7$ and $y = 0.2$; that is, the attackers select the hybrid strategy $\{S_{A1}, S_{A2}\}$ with the probability of {0.7, 0.3}, and the defenders select the hybrid strategy $\{S_{D1}, S_{D2}\}$ with the probability of {0.2, 0.8}. The experimental results obtained in this situation are shown in Figure 5. It can be observed from Figure 5 that, after continuous evolution, the probability that the attackers finally select the attack strategy S_{A1} gradually tends to 1 and the probability that the defenders select the defense strategy S_{D1} gradually approaches 0. Both of them reach an evolutionarily stable state. At this moment, the optimal defense strategy is S_{D2}. In summary, the analysis of the situation at this time shows that the defenders choose defensive investment strategies with a small probability. It is more passive in the offensive and defensive confrontation, and the attackers gradually adopt effective attack strategies; the overall network environment is paralyzed.

5.4. The Attack Dangerous Level Analysis. Figure 6 shows the effect of the attack dangerous level on attack strategies. As we can see from Figure 6, when the attack strategy S_{A1} is not dangerous enough to hurt the defenders (that is, when $k = 0$ or 1), after the evolution equilibrium is reached, the probability that the attackers continue to select the strategy S_{A1} is about 0. That is to say, the attackers tend not to adopt the strategy S_{A1}. When the attack strategy S_{A1} is more dangerous (that is, when $k = 55$), the defenders suffered losses but were not fatal. After the evolution equilibrium is reached, the probability that the attackers continue to select the strategy S_{A1} is about 0.3. When the attack dangerous level is $k = m$, the strategy S_{A1} is lethal to the defenders. At this time, the attackers' payoffs increase; the probability that the attackers continue to select the strategy S_{A1} is about 0.9.

Figure 7 is the effect of the attack dangerous level on the defense strategy. As shown in Figure 7, regardless of how many times the attackers use the strategy S_{A1}, the defenders actively select the strategy S_{D1} to respond. However, when $k = 55$, after about 0.2 h, the probability that the defenders

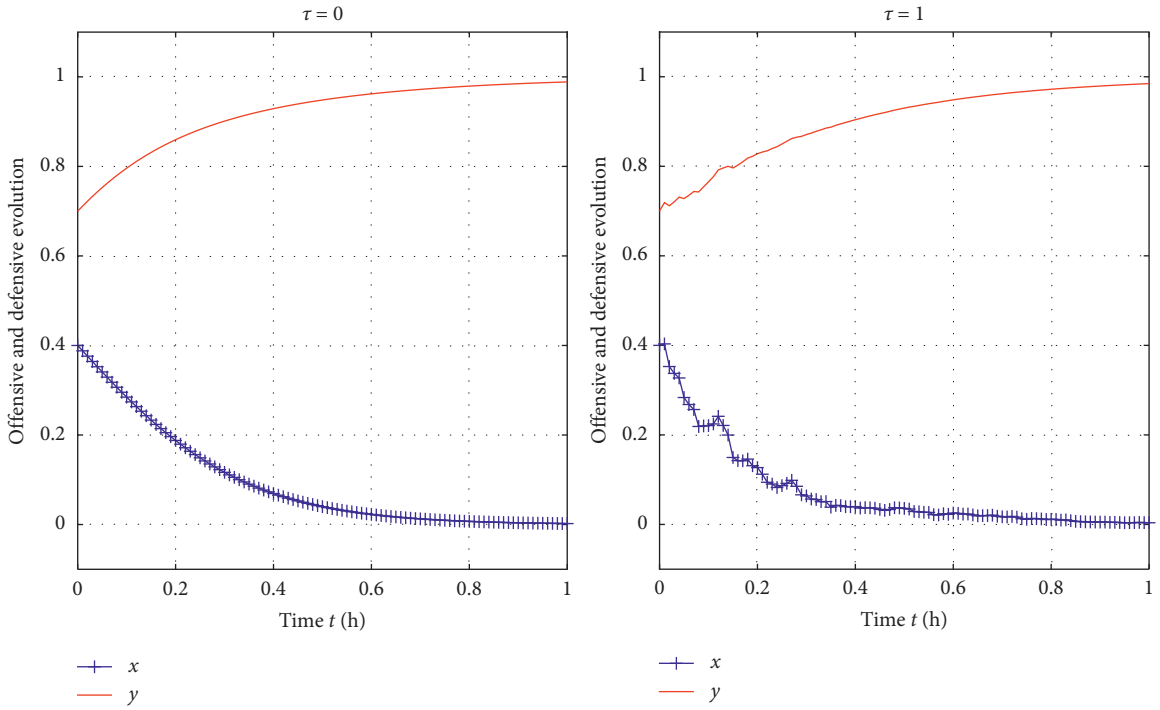

Figure 2: Group evolution trend when $x = 0.4$ and $y = 0.7$.

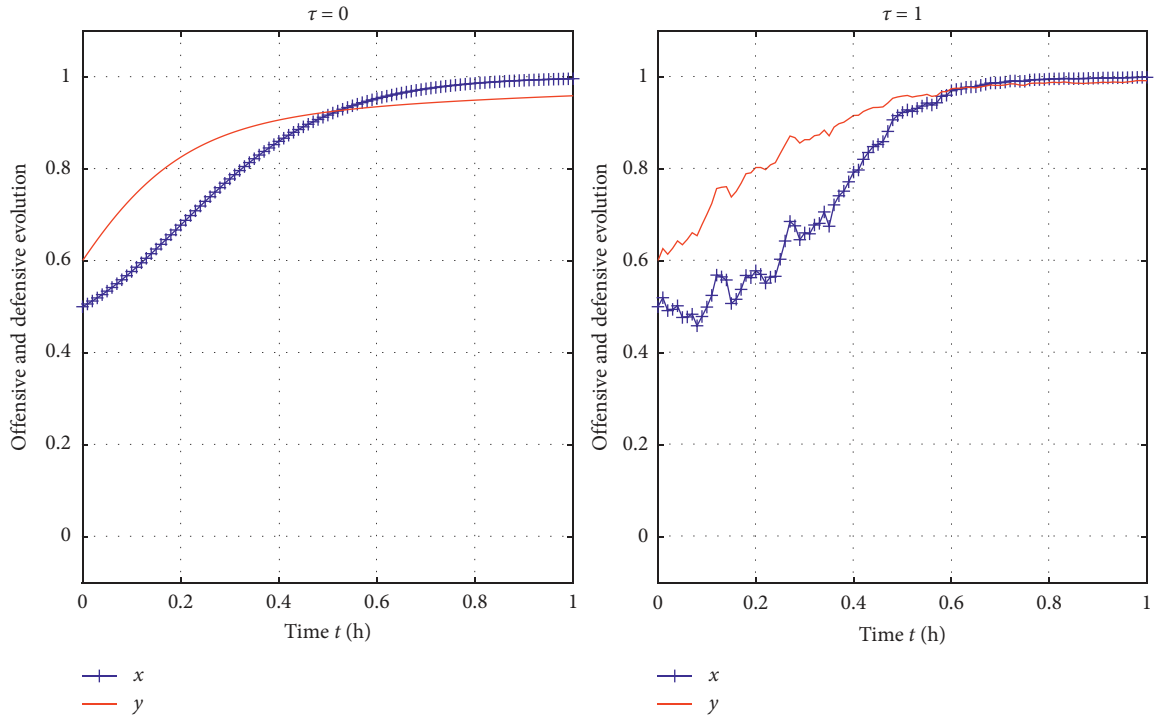

Figure 3: Group evolution trend when $x = 0.5$ and $y = 0.6$.

choose the strategy S_{D1} to deal with is gradually less than 1. This is because the strategy S_{A1} does less damage to the defenders, and the attackers gradually choose not to adopt the strategy S_{A1}. Accordingly, the defenders also began to show that they did not adopt the strategy S_{D1}.

5.5. Comparison Consequence with Other Literatures. Compared with other kinds of literature, we introduce the concept of the Return on Security Investment (ROSI) to measure the effectiveness of the attack and defense game model. ROSI is an important benchmark to decide the

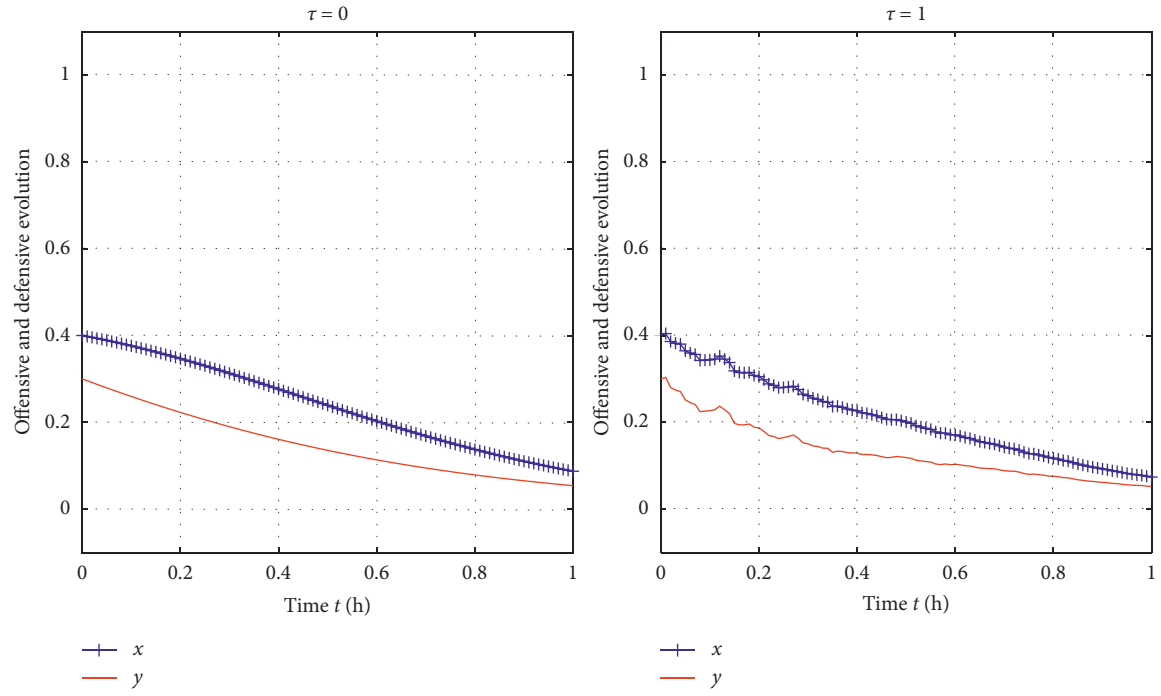

Figure 4: Group evolution trend when $x = 0.4$ and $y = 0.3$.

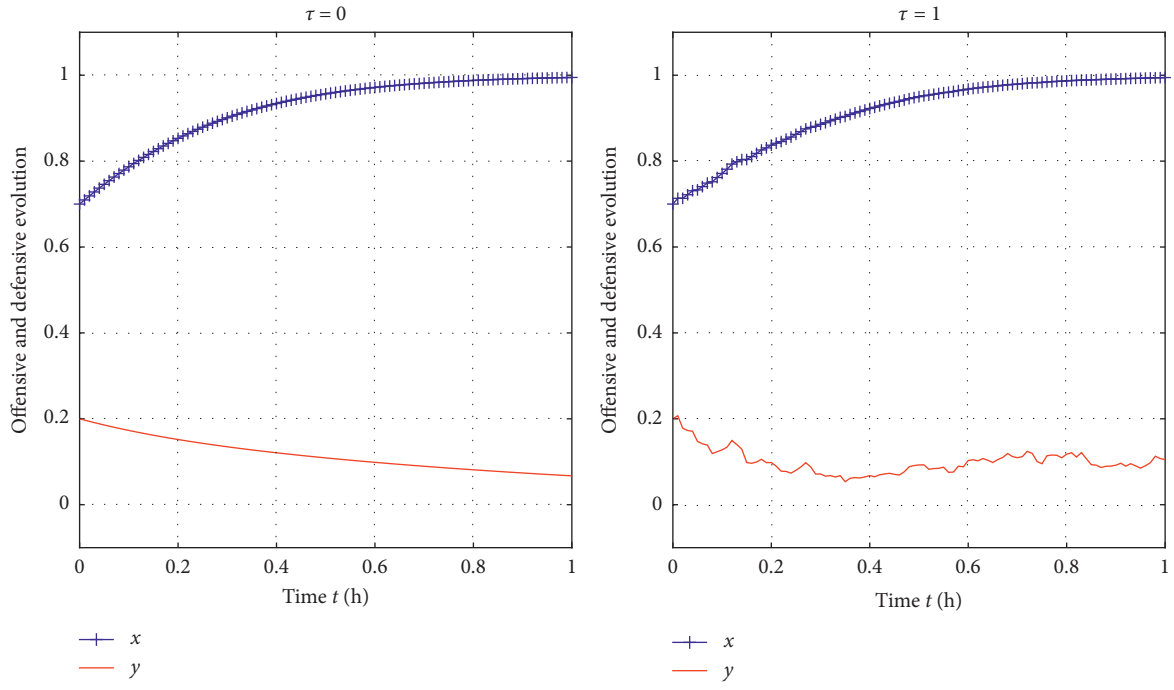

Figure 5: Group evolution trend when $x = 0.7$ and $y = 0.2$.

optimal security investment level; researchers have used ROSI to measure the benefits of defenders. According to the Sonnenreich equation [30], we can get ROSI of attack and defense game model. Figure 8 is a comparison of ROSI. As shown in Figure 8, we can draw a conclusion that ROSI of literature [4] and this paper are better and more suitable for the real network attack and defense environment.

In addition, we also made a comprehensive comparison with some typical research results; as shown in Table 6, we can see that the traditional game model constructed in [1] is

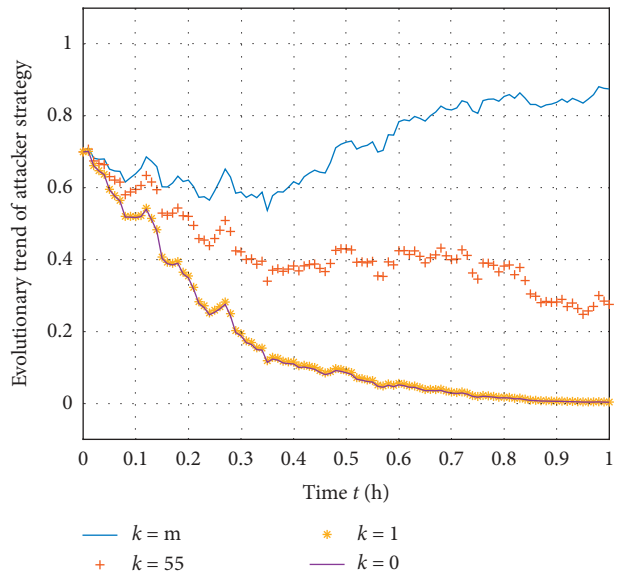

Figure 6: Impact of the attack dangerous level on attack strategies.

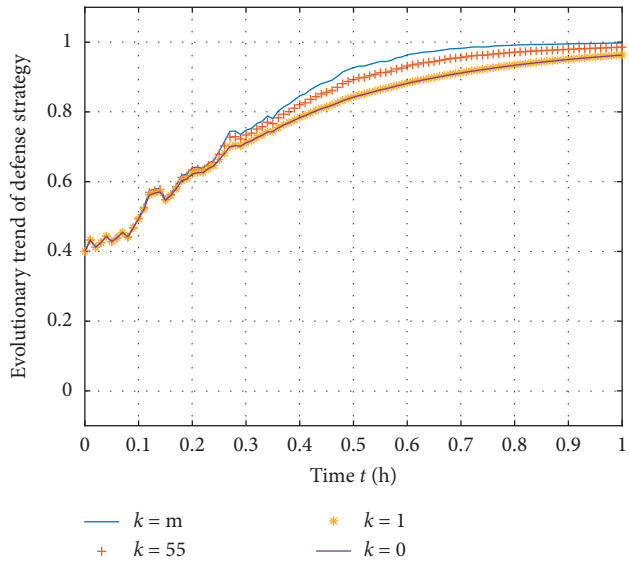

Figure 7: Impact of the attack dangerous level on defense strategies.

dynamic but not as good as the evolutionary game. The literature [4] adopts the evolutionary game. It has good versatility, but it is difficult to accurately describe the evolution process of attack and defense because the model does not consider stochasticity. The literature [6] adopts dynamic detection game, which improves the APT (Advanced Persistent Threats) detection performance in the dynamic games and has better data protection ability, but it does not consider the influence of stochasticity on strategy and its application field is data protection. The literature [12] regards the offensive and defensive evolution game as the random jump process of multistate, but the condition of complete information is challenging to meet in the actual network attack and defense. The literature [9] considers stochasticity, but the model has a small scope of application and its versatility in general. In this paper, the stochasticity of the model is considered based on the condition of incomplete information, and the model is constructed by using stochastic differential equations, which improves the effectiveness of the model.

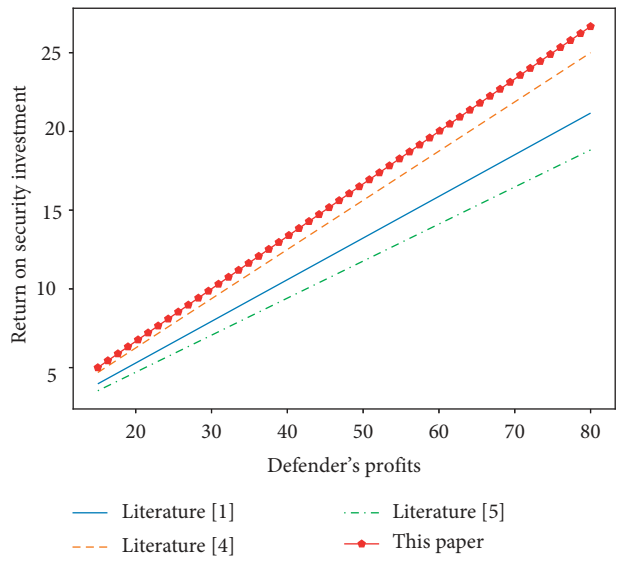

Figure 8: ROSI comparison.

Table 6: Comparison consequence with other literatures.

Literature	Game type	Behavioral information	Model versatility	Model accuracy	Concrete application
[1]	Dynamic game	Incomplete information	General	General	Strategy selection
[6]	Dynamic game	Incomplete information	Good	Good	Data protection
[4]	Evolutionary game	Incomplete information	Good	General	Security defense
[12]	Stochastic game	Complete information	Good	General	Security defense
[9]	Stochastic evolutionary game	Incomplete information	General	Good	Strategy selection
This paper	Stochastic differential game	Incomplete information	Good	Good	Strategy selection

6. Conclusion

Nowadays, the analysis method based on the traditional dynamic game cannot meet the actual demand. In this paper, we construct a stochastic differential game model in network attack and defense by using stochastic differential equations based on Markov property. In different problem situations, the attackers and defenders will eventually tend to a stable state via continuous evolution. Compared with the strategy model without considering stochastic factors, it is proved that the model proposed in this paper is more suitable for the actual network attack and defense.

By comparison, we can intuitively find that the theoretical analysis is consistent with the conclusions obtained by the simulation experiment, which proves the significance of the attack and defense evolutionary game model proposed in this paper. Compared with other related kinds of literature, we can conclude that the return on security investment of this model is better. Applying the model to the actual network environment can provide the choice of the defenders' optimal defense strategy and have a certain positive effect on the maintenance of cybersecurity.

Data Availability

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

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was supported by the National Natural Science Foundation of China under Grant no. 61562006 and in part by the Natural Science Foundation of Guangxi Province under Grant no. 2016GXNSFBA380181.

References

[1] M. Liu, Q. Zhang, W. Yu, and H. Zhang, "Preliminary study on creative thinking mechanism of market information integration," *Acta Psychologica Sinica*, vol. 50, no. 1, pp. 82–89, 2018.

[2] R. N. Borkovsky, D. Ulrich, and K. Yaroslav, "A user's guide to solving dynamic stochastic games using the homotopy method," *Operations Research*, vol. 58, no. 4-part-2, pp. 1116–1132, 2010.

[3] P. D. Taylor and L. B. Jonker, "Evolutionary stable strategies and game dynamics," *Mathematical Biosciences*, vol. 40, no. 1-2, pp. 145–156, 1978.

[4] H. Hu, Y. Liu, H. Zhang, and R. Pan, "Optimal network defense strategy selection based on incomplete information evolutionary game," *IEEE Access*, vol. 6, pp. 29806–29821, 2018.

[5] W. Jiang, B.-X. Fang, Z.-H. Tian, and H.-L. Zhang, "Evaluating network security and optimal active defense based on attack-defense game model," *Chinese Journal of Computers*, vol. 32, no. 4, pp. 817–827, 2009.

[6] L. Xiao, D. J. Xu, N. Mandyam et al., "Attacker-centric view of a detection game against advanced persistent threats," *IEEE Transactions on Mobile Computing*, vol. 17, no. 11, pp. 2512–2523, 2018.

[7] C. Schmidt, "Game theory and economics: an historical survey," *Revue D'économie Politique 100*, vol. 5, pp. 589–618, 1990.

[8] D. Balkenborg and K. Schlag, *On the Interpretation of Evolutionary Stable Sets in Symmetric and Asymmetric Games*, Mimeo, Bonn University Economics Department, New York, NY, USA, 1994.

[9] J. Liu, S. Shen, G. Yue, R. Han, and H. Li, "A stochastic evolutionary coalition game model of secure and dependable virtual service in sensor-cloud," *Applied Soft Computing*, vol. 30, pp. 123–135, 2015.

[10] S. Liu and Y. Liu, "Network security risk assessment method based on HMM and attack graph model," in *Proceedings of the 2016 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, May 2016.

[11] A. Govaert, Y. Qin, and M. Cao, "Necessary and sufficient conditions for the existence of cycles in evolutionary dynamics of two-strategy games on networks," in *Proceedings of the 2018 European Control Conference (ECC)*, June 2018.

[12] Y.-Z. Wang, C. Lin, X.-Q. Cheng, and B.-X. Fang, "Analysis for network attack-defense based on stochastic game model," *Chinese Journal of Computers*, vol. 33, no. 9, pp. 1748–1762, 2010.

[13] F. He, Y. Zhang, H. Liu, and W. Zhou, "SCPN-based game model for security situational awareness in the Intenet of things," in *Proceedings of the 2018 IEEE Conference on Communications and Network Security (CNS)*, May 2018.

[14] S. Talukder, I. I. Sakib, F. Hossen, Z. R. Talukder, and S. Hossain, "Attacks and defenses in mobile ip: modeling with stochastic game petri net," in *Proceedings of the 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC)*, IEEE, September 2017.

[15] A. El Bouchti and T. Nahhal, "Cyber security modeling for SCADA systems using stochastic game nets approach," in *Proceedings of the 2016 Fifth International Conference on Future Generation Communication Technologies (FGCT)*, August 2016.

[16] M. P. Fanti, M. Nolich, S. Simié, and W. Ukovich, "Modeling cyber attacks by stochastic games and Timed Petri Nets," in *Proceedings of the 2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, October 2016.

[17] S. Huang, H. Zhang, J. Wang et al., "Network defense decision-making method based on stochastic differential game model," in *Proceedings of the International Conference on Cloud Computing and Security*, Springer, Haikou, China, June 2018.

[18] W. Wang, A. Kwasinski, D. Niyato, and Z. Han, "Learning for robust routing based on stochastic game in cognitive radio networks," *IEEE Transactions on Communications*, vol. 66, no. 6, pp. 2588–2602, 2018.

[19] L. Wei, A. I. Sarwat, W. Saad, and S. Biswas, "Stochastic games for power grid protection against coordinated cyber-physical attacks," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 684–694, 2016.

[20] J. R. Riehl and M. Cao, "Control of stochastic evolutionary games on Networks∗∗This work was supported in part by the European research council (ERCStG-307207)," *IFAC-PapersOnLine*, vol. 48, no. 22, pp. 76–81, 2015.

[21] J. Liu, F. Weng, R. Zhang et al., "Network security situation assessment approach based on attack-defense stochastic game model," in *Proceedings of the International Conference on Cloud Computing and Security*, Springer, Haikou, China, June 2018.

[22] P. Subbulakshmi, M. Prakash, and V. Ramalakshmi, "Honest auction based spectrum assignment and exploiting spectrum sensing data falsification attack using stochastic game theory in wireless cognitive radio network," *Wireless Personal Communications*, vol. 102, no. 2, pp. 799–816, 2018.

[23] N. Kumar, R. S. Bali, R. Iqbal, N. Chilamkurti, and S. Rho, "Optimized clustering for data dissemination using stochastic coalition game in vehicular cyber-physical systems," *The Journal of Supercomputing*, vol. 71, no. 9, pp. 3258–3287, 2015.

[24] A. Arfaoui, A. ben Letaifa, A. Kribeche et al., "A stochastic game for adaptive security in constrained wireless body area networks," in *Proceedings of the 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, January 2018.

[25] B.-S. Chen and C.-H. Yeh, "Stochastic noncooperative and cooperative evolutionary game strategies of a population of biological networks under natural selection," *Biosystems*, vol. 162, pp. 90–118, 2017.

[26] S. Cai, *Stochastic Control Theory*, Shanghai Jiaotong University Press, Shanghai, China, 1987.

[27] H.-S. Guo, *Stability of Numerical Scheme for Stochastic Differential Equations*, Donghua University, Shanghai, China, 2010.

[28] G. S. Chirikjian and A. B. Kyatkin, *Engineering Applications of Noncommutative Harmonic Analysis: With Emphasis on Rotation and Motion Groups*, CRC Press, Boca Raton, FL, USA, 2000.

[29] X. R. Mao, *Exponential Stability of Stochastic Differential Equations*, CRC Press, Boca Raton, FL, USA, 1994.

[30] C. Zhang, R. Pan, A. Chaudhury et al., "Effect of security investment on evolutionary games," *Journal of Information Science and Engineering*, vol. 30, no. 6, pp. 1695–1718, 2014.