Hindawi
Security and Communication Networks
Volume 2018, Article ID 1821804, 9 pages
https://doi.org/10.1155/2018/1821804

Research Article

A Novel Differential Game Model-Based Intrusion Response Strategy in Fog Computing

Xingshuo An, Fuhong Lin, Shenggang Xu, Li Miao, and Chao Gong

School of Computer and Communication Engineering, University of Science and Technology Beijing (USTB), Beijing 100083, China

Correspondence should be addressed to Fuhong Lin; fhlin@ustb.edu.cn

Received 23 May 2018; Accepted 18 July 2018; Published 1 August 2018

Academic Editor: Liran Ma

Fog computing is an emerging network paradigm. Due to its characteristics (e.g., geo-location and constrained resource), fog computing is subject to a broad range of security threats. Intrusion detection system (IDS) is an essential security technology to deal with the security threats in fog computing. We have introduced a fog computing IDS (FC-IDS) framework in our previous work. In this paper, we study the optimal intrusion response strategy in fog computing based on the FC-IDS scheme proposed in our previous work. We postulate the intrusion process in fog computing and describe it with a mathematical model based on differential game theory. According to this model, the optimal response strategy is obtained corresponding to the optimal intrusion strategy. Theoretical analysis and simulation results demonstrate that our security model can effectively stabilize the intrusion frequency of the invaders in fog computing.

1. Introduction

Fog computing is an emerging network model [1]. As shown in Figure 1, fog computing is a three-layer architecture: user device layer, fog node layer, and cloud computing layer. Fog nodes are service nodes located between cloud and users [2]. Fog nodes [3] are geo-distributed, which can provide low latency services for users. The research in this paper is based on this network architecture.

Fog nodes are located at the edge of the network, which is closer to users. The needs of heterogeneous network access and diverse services make fog nodes face more complex and insecure network environment. The traditional network security technology such as physical security technology [4] is difficult to resist the multisource and cross-domain intrusion [5]. It is necessary to research the network security technology suitable for fog computing to deal with new challenges. Intrusion detection system [6] (IDS) is a measure that can provide effective security for fog network [7]. Our previous work [8, 9] has proposed a general IDS framework to protect cloud servers and fog nodes from security threats. One of the functions of IDS is to make corresponding response strategy based on attackers' behaviors. In this framework, intrusion response is the strategy and action for intrusion when the fog node detects the intrusion. Response strategy selection is the most critical problem in intrusion response [10].

In the fog network, the intruder will attack the fog cluster and carry out an invasion process from fog to cloud. Cloud as a management system for fog cluster needs to respond to such intrusion processes. The intruder implements different frequency attacks on fog nodes. The purpose is to successfully bypass the IDS deployed by the fog node, in order to intrude into the system for further intrusion activities. In other words, the intruder's needs maximized his invasion success expectations. For the system, the cloud server's strategy is to set the access forbidding rate to the fog cluster. In addition to dealing with illegal users, fog cluster also needs to serve legal users. The system needs to serve legal users as much as possible. In order to find the optimal strategy of the intruder and the system, we can regard the problem as a game [10], and the intruder and the system are the players of the game.

In view of intrusion response, some researchers use static game method to model and solve. A universal game model is proposed in [11]. An approach named Response and Recovery Engine (RRE) [12] was proposed. RRE was based on Markov game theory. Reference [13] proposed a dynamic intrusion response model based on game theory to assure the incentives

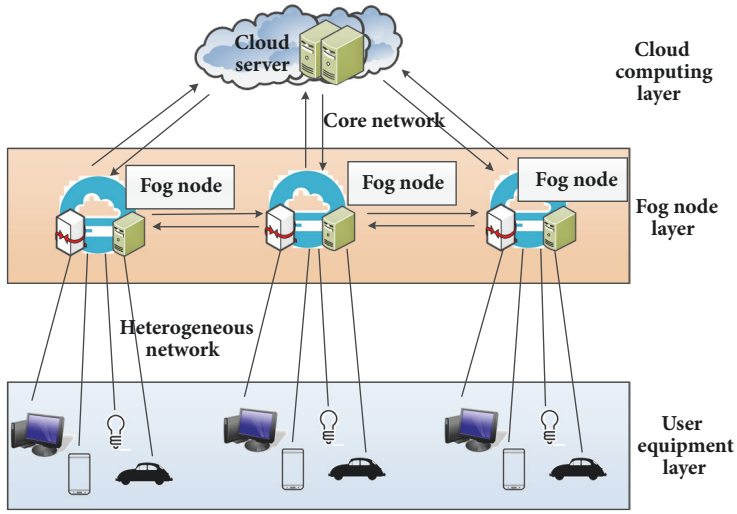

Figure 1: Fog computing network structure.

of system. Noncooperative games model was applied to solve the problem of intrusion response [14]. Using the modeled stochastic game, the authors in [15] proposed a decision working framework to take optimal actions in case of network intrusion.

In fog computing, the interaction between fog nodes and cloud is real time. In continuous time, the cloud needs to make decisions in real time. Accordingly, intruders need to change their strategy in real time to maximize their gains. Differential game [16], as a game model in continuous time, is more suitable for the network environment of fog computing. At present, there is little reference about the application of differential games in the field of fog computing security. The relevant research is only found in [17]. The author defines the strategy of fog nodes from the perspective of energy consumption. The two players of the game are vulnerable node and the malicious nodes in the fog cluster. In this paper, the two players of the game are defined, and strategic analysis from the perspective of the system composed of fog cluster and the perspective of intruders is made, respectively. The main work of this paper is to analyze the characteristics of intrusion in the environment of fog network, apply differential game to model the invaders and system, respectively, and emphasize the theoretical analysis of defense model of the system. In our model, the cloud server can take the best security strategy to filter the access requests of the illegal users based on the attack of invaders. To our knowledge, this is the first differential game theory approach to model the interactions between the intruder and the system in fog computing.

The main contributions of this paper are as follows:

(1) The path and characteristics of invasion are analyzed in the environment of fog computing. The invader model and defense model of the system are built, respectively, according to the invasion.

(2) We derive the optimal strategy of the system and the rational intruder, i.e., the Nash equilibrium of the game.

(3) The simulation shows the outstanding performance of the proposed strategy.

The rest of the paper is organized as follows. In Section 2, we analyzed the intrusion process in fog computing. In Section 3, the differential game models of intruders and system are established and analyzed, respectively. In Section 4, the feedback Nash equilibrium solution is given. The model simulations are provided in Section 5. Finally, the main conclusions are summarized in Section 6.

2. Intrusion in Fog Network

This study focuses on what strategy the system should take when an intrusion occurs. The process that an invasion starts from the fog nodes to the cloud is given. The ultimate goal of invaders is to gain higher permissions on cloud servers, thus causing greater damage to the entire fog network. From the perspective of network attack, invasions from user device layer to fog node layer and then to cloud servers are implemented through different invasion methods. Figure 2 shows the invasion process mentioned above.

Fog nodes are faced with the heterogeneous network environment and communication protocols, and operating system and program bugs are easy to be exploited by invaders. By detecting fog bugs, invaders can find bug in fog nodes. In this process, an invader needs to send a number of access requests to each fog node to detect the bug. When the number of requests sent is too large, it will also cause a denial of service attack (DoS) to the fog node. When an invader finds an available bug, he will exploit bugs to achieve illegal invasions. Once an invader fatally invades a fog node, it will first cause serious harm to the users in the service range of the fog node, such as Privacy leakage and Malware propagation. Secondly, invaders will directly have a negative impact on the network service of fog nodes, such as U2R on fog nodes. The ultimate goal of the intruder is to gain access to the cloud server and carry out further invasion. When an invader achieves

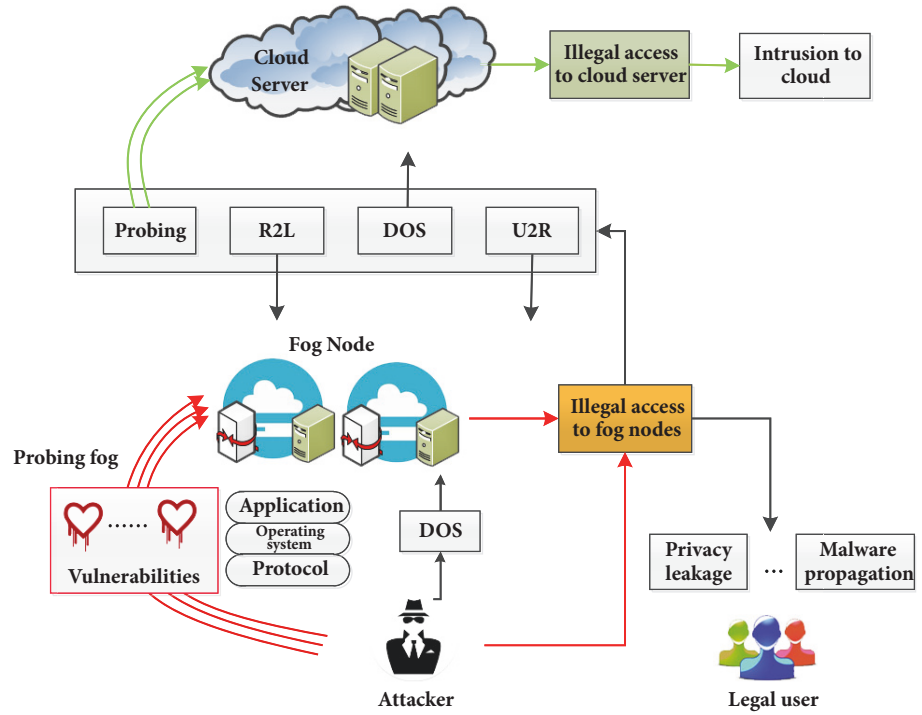

Figure 2: Intrusion process in fog computing.

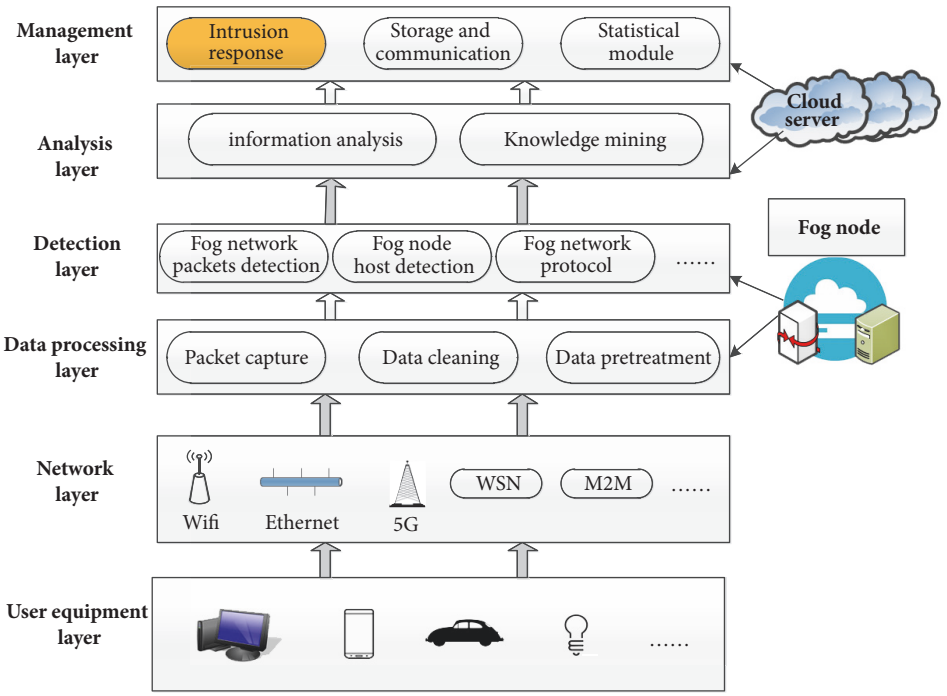

Figure 3: The general framework for fog computing intrusion detection system.

a user-to-root attack (U2R) on a fog node, the bugs of the cloud server will be continuously scanned and utilized by the invader to seek access to the cloud. Reducing the invasion frequency of invaders and improving the traffic of legal users in the system are against the invasion in fog computing. The focus of this study is on the intrusion response. Intrusion response is an important function of IDS framework [8] as shown in Figure 3.

The framework is a 6-layer IDS framework. It contains a series of functional modules, such as detection and response,

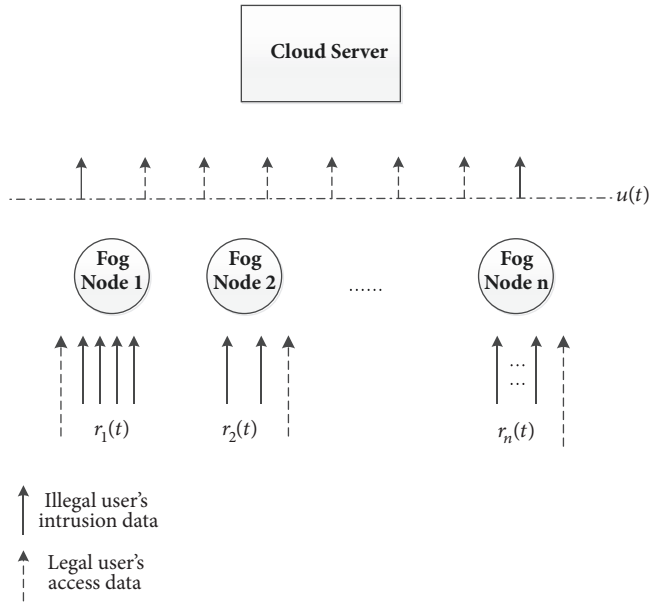

Figure 4: Attack strategy and response strategy in fog computing.

Table 1: The list of symbols' meanings.

Symbol	Notation
$r_i(t)$	Attacker's strategy: intrusion frequency for each fog node at time t, and it is the control variable of the attackers
$u(t)$	Defender's strategy: forbidding rate for system access at time t, and it is the control variable of the IDS
$x(t)$	System memory resource occupancy
W_A	The incomes of the attacker: expectation of invasion success
W_D	The incomes of the defender: access amount of legal users
J_A	The gains of the attacker
J_D	The gains of the defender
χ	Total access amount of system at t
α	Forbidding factor
θ	System capacity: $u(t)$ is enabled when the total access amount exceeds θ
β	Proportion of legal users in χ

which can ensure the security of fog computing. It shows that intrusion response is deployed in the cloud. The defense strategy of the cloud server is based on the whole system in order to defend against invasion from illegal users and minimize the loss of fog nodes after invasion. The invasion from illegal users and the response of the cloud server are regarded as the two players of attack-defense, and the problem is modeled and described in Section 3.

3. Differential Game Models

In this section, we model the two players of attack-defense in fog computing. In the process of invasion and response, intruders and system can be viewed as two players of the game, and their purpose is to maximize their benefits. The invader invades every fog node. The invasion frequency of each fog node is the attacker's strategy, aiming to access the fog node as much as possible so as to make illegal access. For defenders, restricting the invasion of illegal users and letting more legal users get access to fog network are the purpose of the system. The cloud server is mainly responsible for the implementation of the system response strategy. The forbidding rate of accessing users, u(t), is the control strategy of the cloud server. The process of intrusion and the process of response are shown in Figure 4.

The invaders and defenders in fog computing are analyzed and modeled, respectively, showing the relationship between the strategy of both invaders and defenders and their benefits. The list of symbols' meanings, which can be used during modeling, is shown in Table 1.

As shown in Figure 4, intruders start attack at fog nodes. The frequency of invasion against fog nodes is $r_i(t)$. The expectation of successful invasion is defined as the incomes of invaders, which is $W_A = r_i(t) \cdot \varphi_i(t)$, and $\varphi_i(t)$ is the probability of a single successful invasion. The probability of a round of successful invasion detected on the fog node i will increase when $r_i(t)$ is increased. When $r_i(t)$ increases, the probability of detecting attacks on the fog node will increase.

We define $\varphi(t) = 1 - r_i(t)/r_{i-\max}$, and $r_{i-\max}$ is the upper limit of the invasion frequency on the *ith* fog node. The incomes of invaders are

$$W_A = \sum_{i=1}^{n} r_i(t) \cdot \left[1 - \frac{r_i(t)}{r_{i-\max}}\right] \tag{1}$$

Cloud servers are as a defender of the system and the defense strategy is deployed from the perspective of fog cluster. The fog cluster is viewed as a system. When the number of system's access is too large, the system needs to take corresponding response strategy. The functional relationship between the system income and the access traffic of system is given and the functional relationship between the response strategy of system and the access traffic of system is also given:

$$W_D = \begin{cases} \beta\chi, & (\chi \le \theta) \\ [1 - u(t)] \cdot \chi, & (\chi > \theta) \end{cases} \tag{2}$$

θ is the capacity of the system. When $\chi \le \theta$, it represents the traffic of the legal access in the system. β represents the proportion of legal users in χ and it is obvious that $\beta \le 1$. $W_D = \beta\chi$. When $\chi > \theta$, it represents the traffic of the abnormal access in the system. Obviously, the proportion of illegal users is larger than legal access traffic. The original forbidding rate will no longer apply to the response of the system and the defense strategy $u(t)$ should be started at this time.

The larger χ is, the greater proportion of illegal users is. The forbidding peer rate of system needs to be larger. So $u(t) = \alpha \cdot \chi$, and α represents the forbidding factor.

When $\chi > \theta$

$$W_D = (1 - \alpha\chi) \cdot \chi = -\alpha\chi^2 + \chi \tag{3}$$

According to formula (3), W_D exhibits an impact of quadric relationship on χ. Based on the properties of quadratic function, we give Theorem 1.

Theorem 1. *When the system starts the defense policy, the maximum capacity of the system cannot exceed* $1/\alpha$.

Proof. When χ becomes large to $\chi = 1/\alpha$, $W_D = 0$. When χ continues to become larger, $W_D < 0$, the incomes of the system are negative and legal users cannot make access and the system is down. There is no meaning to start the strategy. □

Corollary 2. *Condition 1 for the system to take the response strategy is that the value of* χ *is between* θ *and* $1/\alpha$. $\chi \in (\theta, 1/\alpha)$.

The range of forbidding factor α is as follows:

Based on the properties of quadratic function, $\max(W_D) = 1/4\alpha$. $\theta \ge 1/4\alpha$ because W_D represents access amount of legal users. When $\chi = \theta$, the system reaches its critical point.

If $\theta < (1-\beta)/\alpha$, then $\beta\cdot\theta < -\alpha\cdot\theta^2 + \theta$. $\beta\cdot\theta$ is $\max\{W_D\}_{\chi\le\theta}$, which is the maximal incomes of system before taking the strategy.

From $(2\alpha\cdot\theta - 1)^2 \ge 0$, it can be concluded that $-\alpha\cdot\theta^2 + \theta \le 1/4\alpha$.

Because of the properties of quadratic function, $1/4\alpha$ is the maximal incomes of the system after taking the strategy.

$\beta \cdot \theta < 1/4\alpha$, which is $\max\{W_D\}_{\chi>\theta} \ge \max\{W_D\}_{\chi\le\theta}$.

The relationship between θ and α is as follows:

$$\frac{1}{4\alpha} \le \theta < \frac{1-\beta}{\alpha} \tag{4}$$

The inequality needs to satisfy $1/4\alpha < (1-\beta)/\alpha$, and the range of β is further determined: $\beta \in (0, 0.75)$

According to inequality (4), the range of forbidding factor α is as follows: $\alpha \in [1/4\theta, (1-\beta)/\theta)$.

Corollary 3. *Condition 2 for the system to take the response strategy* $u(t)$ *is as follows:* $\alpha \in [1/4\theta, (1-\beta)/\theta)$, $\beta \in (0, 0.75)$.

Corollary 4. *The maximal incomes of the system can be improved when the response strategy is used.*

Following the above, a precise function of income can be obtained:

$$W_D = \begin{cases} \beta\chi, & \chi \in [0, \theta] \\ [1 - u(t)] \cdot \chi, & \chi \in \left(\theta, \dfrac{1}{\alpha}\right] \end{cases} \qquad \alpha \in \left[\frac{1}{4\theta}, \frac{1-\beta}{\theta}\right), \ \beta \in (0, 0.75) \tag{5}$$

In the further discussion, when $\chi > \theta$, the relationship between incomes of the system and the strategy of the system is important. From $u(t) = \alpha \cdot \chi$, the income after the strategy being used is

$$W_D = -\frac{u^2(t)}{\alpha} + \frac{u(t)}{\alpha} \tag{6}$$

The process of game is dynamic and continuous. Both the invasion against fog nodes started by invaders and the corresponding strategy executed by the system have a direct impact on memory occupancy. Memory occupancy can be dynamically represented as $x(t)$:

$$\frac{dx(t)}{dt} = \left[\sum_{i=1}^{n} a r_i^2(t)\right] + b \cdot u(t) + x(t) \tag{7}$$

Because of $x(t)$, when the gains of both system and invaders are calculated, the impact on the gains caused by $x(t)$ needs to be considered. If the memory occupancy of system increases, this may be due to the resource occupation caused by the successful invasion. This is what invaders want, as the starter of the invasion from outside. The impact of $x(t)$ on the gains needs to be considered when the gains are calculated. On the contrary, for the system, the start of the response strategy requires system memory. $x(t)$ is as the cost of response when calculating gains, it should deduct the

impact of $x(t)$ on its gains from W_D. The object functions [16] of system gains and invader gains are

$$J_D = \max_{u(t)} \int_{t_0}^{T} e^{-r(t-t_0)} \left[(1-u(t)) \frac{u(t)}{\alpha} - c \cdot x(t) \right] dt + q_1 (x(T)) e^{-r(T-t_0)} \tag{8}$$

$$J_A = \max_{r_i(t)} \int_{t_0}^{T} e^{-r(t-t_0)} \left[\left(1 - \frac{r_i(t)}{r_{i-\max}} \right) r_i(t) + d \cdot x(t) \right] dt + q_2 (x(T)) e^{-r(T-t_0)} \tag{9}$$

c and d are influence factors of $x(t)$ on the gains of invaders and gains of the system.

4. Solution of Optimal Strategy

In Section 3, intruders attack and system defense in fog network are regarded as dynamic game processes, and a differential game model is established. In this section, the optimal strategy of differential game model established in Section 3 will be solved [16, 18].

From Bellman equation, formula (8) can be changed to

$$-V_t(t,x) = \max_{u(t)} \left\{ \left[(1-u(t)) \frac{u(t)}{\alpha} - c \cdot x(t) \right] e^{-r(t-t_0)} + V_x(t,x) \left[\left[\sum_{i=1}^{n} a r_i^2(t) \right] + b \cdot u(t) + x(t) \right] \right\} \tag{10}$$

$$V(T,x) = q_1 (x(T)) \exp\left(-r(T-t_0)\right) \tag{11}$$

From the derivation of formula (10) with respect to $u(t)$, we can obtain the optimal response strategy as

$$u^*(t) = \frac{1}{2} \left(1 + V_x(t,x) \alpha b e^{r(t-t_0)} \right) \tag{12}$$

We assume that

$$V(t,x) = e^{-r(t-t_0)} (A(t) x + B(t)) \tag{13}$$

Substituting formula (12) into (10) and (11), we can get

$$V_t(t,x) = e^{-r(t-t_0)} \left(-rA(t) + A'(t) \right) x + e^{-r(t-t_0)} \left(-rB(t) + B'(t) \right) \tag{14}$$

$$V_x(t,x) = e^{-r(t-t_0)} A(t) \tag{15}$$

Then the optimal intrusion response strategy can be represented in terms of $A(t)$ as

$$u^*(t) = \frac{1}{2} (1 + A(t) \alpha b) \tag{16}$$

where we need to solve the expression of $A(t)$ firstly.

$V_x(t,x)$ can be changed into

$$V_x(t,x) = \mathrm{e}^{-r(t-t_0)} \left(rA(t) x + rB(t) - A'(t) x - B'(t) \right) = \frac{1 + A(t) \alpha b}{2\alpha} - \frac{1}{4\alpha} (1 + A(t) \alpha b)^2 + A(t) \cdot \left[\sum_{i=1}^{n} \frac{a \left[r_i^*(t) \right]^2}{2} + \frac{b}{2} (1 + A(t) \alpha b) + x(t) \right] \tag{17}$$

from which we can deduce that

$$\begin{aligned} rA(t) - A'(t) &= A(t) - c \\ rB(t) - B'(t) &= \frac{1}{4\alpha} \left(1 - A^2(t) a^2 b^2 \right) + \frac{b}{2} (1 + A(t) ab)^2 + A(t) \sum_{\mathrm{i}=1}^{\mathrm{n}} a \left(\mathrm{r}_{\mathrm{i}}^*(\mathrm{t}) \right)^2 \end{aligned} \tag{18}$$

Formula (18) gives rise to the expression of $A(t)$

$$A(t) = q_1 e^{(r-1)(t-T)} + \frac{c \cdot e^{(r-1)(t-T)}}{r-1} - \frac{c}{r-1} \tag{19}$$

The optimal response strategy of system response is finally presented

$$u^*(t) = \frac{1}{2} (1 + \alpha b A(t)) = \frac{1}{2} + \frac{\alpha b}{2} \left[q_1 e^{(r-1)(t-T)} + \frac{c \cdot e^{(r-1)(t-T)}}{r-1} - \frac{c}{r-1}] \right] \tag{20}$$

Then we solve the optimal intrusion strategy. From Bellman equation, formula (9) can be changed into

$$-W_t(t,x) = \max_{r_i(t)} \left\{ \left[r_i(t) \left(1 - \frac{r_i(t)}{r_{i-\max}} \right) + d \cdot x(t) \right] e^{-r(t-t_0)} + W_x(t,x) \left[\left[\sum_{i=1}^{n} a r_i^2(t) \right] + b \cdot u(t) + x(t) \right] \right\} \tag{21}$$

$$W(T,x) = q_2 (x(T)) \exp\left(-r(T-t_0)\right) \tag{22}$$

In formula (21), the derivation with respect to $r_i(t)$ leads to the optimal intrusion strategy

$$r_i^*(t) = \frac{r_{i-\max}}{2 - 2 r_{i-\max} C(t) a} \tag{23}$$

In the same way, to solve the expression of $C(t)$, we assume

$$W(t,x) = e^{-r(t-t_0)} (C(t) x + D(t)) \tag{24}$$

Table 2: Range of parameters in the model.

Parameters		θ	β	α	a	b	c	d	r	q_1	q_2	$r_{i-\max}$
Range of value	Upper limit	250	0.5	0.001	0.5	20	0.1	0.01	0.1	0.2	0.8	50
	Lower limit			0.002	5	100	0.5	0.1	0.9			100

Substituting formula (23) into (21) and (22), we can get

$$W_t(t,x) = e^{-r(t-t_0)}\left(-rC(t)x + C'(t)x - rD(t) + D'(t)\right) \tag{25}$$

$$W_x(t,x) = e^{-r(t-t_0)}C(t) \tag{26}$$

From formula (24), $W(t,x)$ can be written as

$$\begin{aligned} W(t,x) = {} & \frac{r_{i-\max}}{2 - 2r_{i-\max}C(t)a} \\ & - \left[\frac{r_{i-\max}}{4\left(1 - r_{i-\max}C(t)a\right)^2}\right] + C(t) \\ & \cdot \left[\sum_{i=1}^{n} \frac{ar^2{}_{i-\max}}{4\left(1 - r_{i-\max}C(t)a\right)^2} + bu^*(t)) + x(t)\right] \\ & - d \cdot x(t) \end{aligned} \tag{27}$$

From formula (27), we can deduce that

$$\begin{aligned} rC(t) - C'(t) &= d + C(t) \\ rD(t) - D'(t) &= Q \end{aligned} \tag{28}$$

where $Q = r_{i-\max}/(2 - 2r_{i-\max}C(t)a) - r_{i-\max}/4(1 - r_{i-\max}C(t)a)^2 + \sum_{i=1}^{n}(C(t)ar^2{}_{i-\max}/4(1 - r_{i-\max}C(t)a)^2) + (bC(t)/2)(1 + A(t)\alpha b)$.

We can get the expression of $C(t)$ as

$$C(t) = q_2 e^{(r-1)(t-T)} + \frac{d \cdot e^{(r-1)(t-T)}}{r-1} - \frac{d}{r-1} \tag{29}$$

Therefore, the optimal invasion strategy of each fog node is

$$r_i{}^*(t) = \frac{r_{i-\max}}{2 - 2r_{i-\max}\left[q_2 e^{(r-1)(t-T)} + d \cdot e^{(r-1)(t-T)}/(r-1) - d/(r-1)\right]a} \tag{30}$$

From formula (7), we can update the equation of state

$$\begin{aligned} \frac{dx^*(t)}{dt} = {} & \left[\sum_{i=1}^{n} a\left(\frac{r_{i-\max}}{2 - 2r_{i-\max}\left[q_2 e^{(r-1)(t-T)} + d \cdot e^{(r-1)(t-T)}/(r-1) - d/(r-1)\right]a}\right)^2\right] \\ & + b\left[\frac{1}{2} + \frac{\alpha b}{2}\left[q_1 e^{(r-1)(t-T)} + \frac{c \cdot e^{(r-1)(t-T)}}{r-1} - \frac{c}{r-1}\right]\right] + x^*(t) \end{aligned} \tag{31}$$

In summary, we get the optimal response strategy and the optimal intrusion strategy. They are described with formula (20) and (30), respectively.

5. Numerical Simulation

In this section, Matlab 2014a software is used for simulation. According to the model, the tendency of the optimal response strategy changing with time and the tendency of the optimal invasion strategy changing with time are analyzed, respectively. In the limited time domain, 5 fog nodes are analyzed in 20 minutes to obtain the dynamic rules of system strategy and intruder strategy. The parameters used in the simulation are shown in Table 2.

The access capacity of the system is $\theta = 250$ and the proportion of legal users in the system is $\beta = 0.5$. From (5), the range of α is fixed. $r_{i-\max}$ is the invasion limit on each fog node, its domain is between 50 and 100. For a and b, they represent the influence factors of intrusion strategy and the influence factors of response strategy on $x(t)$, respectively. Since the influence of intruders on $x(t)$ is indirect and the response strategy adopted by the system is direct to $x(t)$, assuming a is less than b, d and c are the influence factor of $x(t)$ on gains of invaders and the influence factor of $x(t)$ on gains of system so c needs to be between 0.1 and 0.5 and d needs to be between 0.01 and 0.1. r is a discount factor, which needs to be between 0 and 1.

First, the response strategy of the system $u(t)$ is stimulated. Figure 5 shows the changing rule of $u(t)$ in different limiting factors α. It can be seen that the value of α has an impact on the initial value of the game. However, when the game begins, no matter what α is, $u(t)$ will converge and be stable at around 10 minutes. This shows that when the system capacity of θ and β is fixed, the value of α has a little influence on the option of response strategy, which means when choosing strategy, the attempts to choose limiting factor α do not have to be frequent, for the cloud server choosing the strategy.

Figure 6 shows the convergence of the optimal defense strategy of the system when the discount factor r takes

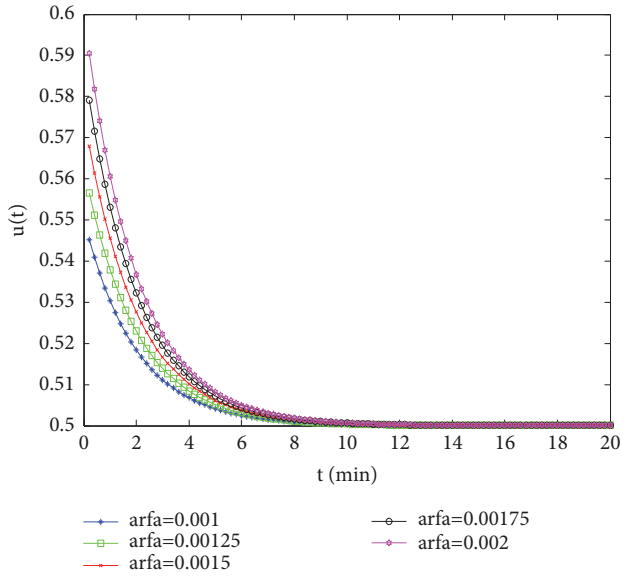

Figure 5: The variation of optimal response strategy over time with different α.

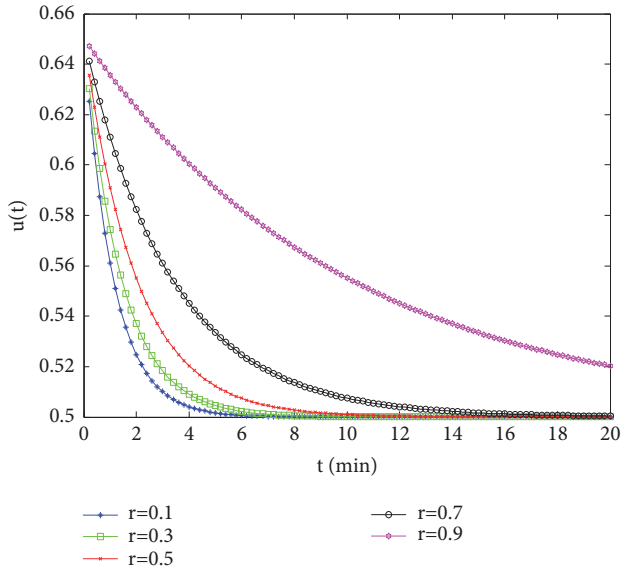

Figure 6: The variation of optimal response strategy over time with different r.

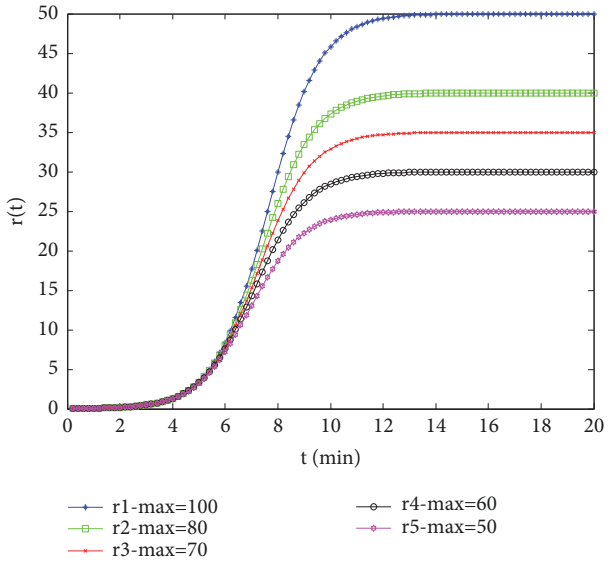

Figure 7: The optimal intrusion strategy when 5 fog nodes are invaded.

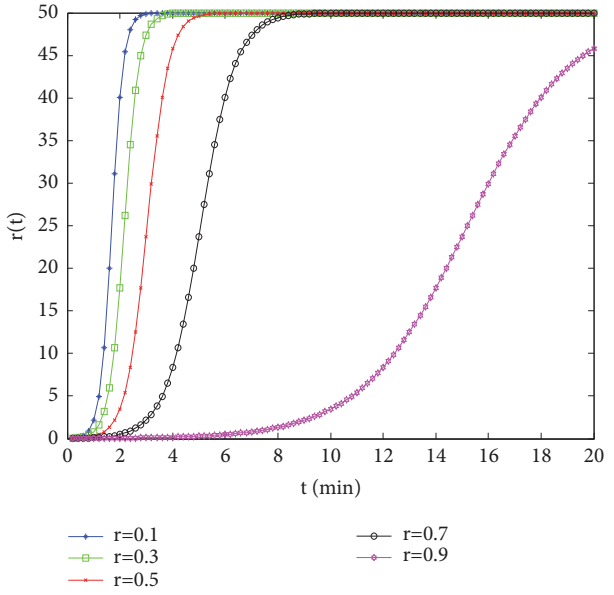

Figure 8: The variation of optimal intrusion strategy over time with different r.

different values. The smaller r is, the faster optimal strategy converges. When r is 0.9, the terminal time of the game is still not convergent. The reason for it is that r, as the main parameter of the ultimate gains, will directly affect choosing system response strategy in the process of dynamic game.

The optimal intrusion strategy of the invaders is stimulated, assuming that an invader invades 5 fog nodes and Figure 7 shows five intrusion strategies against 5 fog nodes of different $r_{i-\max}$. At the initial time, the frequency of invasion is 0. As time goes on, the invaders will increase the frequency of invasion to gain higher gains. However, as the game continues, the invasion strategy $r_i(t)$ will also reach a steady state. Similar to the system response strategy, it also converges at a certain time. Similarly, in order to observe the convergence of $r_i(t)$, discount factor r takes different values. Figure 8 shows the tendency of optimal intrusion strategy changing with time when r takes different value. Obviously, the smaller r is, the faster the optimal strategy converges.

A comprehensive analysis shows that the system broadens the restrictions on access traffic in the process of reducing the forbidding rate $u(t)$ of the system. At the same time, in order to maximize the incomes, the intruders will also enhance the intrusion level on the fog nodes. As the game continues, the system and intruders will adjust their strategy to maximize their incomes. The system state $x(t)$ will also change when

the strategy is changed. $r_i(t)$ and $u(t)$ will also affect the incomes of players. Therefore, this process is a game between two players adjusting the optimal strategy and making the optimal strategy converge.

6. Conclusions

Fog computing is a new computing paradigm, and its security problem can not be ignored. As the manager of fog cluster, cloud server needs to respond in time when intrusion occurs. Firstly, the characteristics of intrusion in fog computing are analyzed, and the invaders and system in fog computing are modeled, respectively. Then the differential game model is solved, and the optimal strategy of intruders and system is obtained. Finally, we simulated the optimal intrusion strategy and the optimal response strategy, and we analyzed the experimental results. The results show that our game model and the optimal strategy can guarantee the security of fog cluster.

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 work is supported by the National Key R&D Program of China (2017YFC0820700), the Foundation of Science and Technology on Information Assurance Laboratory (no. KJ-17-101), and the National Science Foundation Project of China (no. 61701020).

References

[1] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proceedings of the 1st ACM Mobile Cloud Computing Workshop, MCC 2012*, pp. 13–16, ACM, Helsinki, Finland, August 2012.

[2] Y. Huo, C. Yong, and Y. Lu, "Re-ADP: Real-time Data Aggregation with Adaptive w-event Differential Privacy for Fog Computing," *Wireless Communications and Mobile Computing*, pp. 1–13, 2018.

[3] J. Su, F. Lin, X. Zhou, and X. Lu, "Steiner tree based optimal resource caching scheme in fog computing," *China Communications*, vol. 12, no. 8, Article ID 7224698, pp. 161–168, 2015.

[4] Y. Huo, Y. Tian, L. Ma, X. Cheng, and T. Jing, "Jamming Strategies for Physical Layer Security," *IEEE Wireless Communications*, vol. 25, no. 1, pp. 148–153, 2018.

[5] B. Z. Abbasi and M. A. Shah, "Fog computing: Security issues, solutions and robust practices," in *Proceedings of the 2017 23rd International Conference on Automation and Computing (ICAC)*, pp. 1–6, IEEE, Huddersfield, UK, 2017.

[6] D. E. Denning, "An Intrusion-Detection Model," in *IEEE Symposium on Security and Privacy*, IEEE, Oakland, CA, USA, 1986.

[7] Y. Huo, C. Hu, X. Qi, and T. Jing, "LoDPD: A Location Difference-Based Proximity Detection Protocol for Fog Computing," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1117–1124, 2017.

[8] X. An et al., "Sample Selected Extreme Learning Machine Based Intrusion Detection in Fog Computing and MEC," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 7472095, 10 pages, 2018.

[9] Lin. Fuhong et al., "Fair Resource Allocation in Intrusion Detection System for Edge Computing," *IEEE Consumer Electronics Magazine*, 2018.

[10] N. Stakhanova, S. Basu, and J. Wong, "A taxonomy of intrusion response systems," *International Journal of Information and Computer Security*, vol. 1, no. 1-2, pp. 169–184, 2007.

[11] Y. B. Guo and M. A. J. Feng, "Game theoretical framework for adaptive intrusion detection and response," *System Engineering and Electronics*, 2005.

[12] S. A. Zonouz et al., "RRE: A Game-Theoretic Intrusion Response and Recovery Engine," *IEEE Transactions on Parallel and Distributed System*, vol. 25, no. 2, pp. 395–406, 2013.

[13] S. Jin, L. Yin, and A. X. Li, "Dynamic Intrusion Response Based on Game Theory," *Journal of Computer Research and Development*, vol. 45, no. 5, pp. 747–757, 2013.

[14] W. P. Wang and W. W. Zhu, "Network Security Behavior Model Based on Dynamic Non-Cooperative Game Model with Incomplete Information," *Journal of Chinese Computer System*, vol. 27, no. 2, pp. 253–256, 2006.

[15] A. Kundu and S. K. Ghosh, "Game Theoretic Attack Response Framework for Enterprise Networks," in *Distributed Computing and Internet Technology*, vol. 8337, pp. 263–274, Springer International Publishing, New york, NY, USA, 2014.

[16] D. W. Yeung and L. A. Petrosyan, *Cooperative Stochastic Differential Games*, Springer, New York, NY, USA, 2006.

[17] Z. Li, X. Zhou, Y. Liu, H. Xu, and L. Miao, "A non-cooperative differential game-based security model in fog computing," *China Communications*, vol. 14, no. 1, pp. 180–189, 2017.

[18] A. Dixit, "A model of duopoly suggesting a theory of entry barriers," *Bell Journal of Economics*, vol. 10, no. 1, pp. 20–32, 1979.