Hindawi
Complexity
Volume 2020, Article ID 7136160, 18 pages
https://doi.org/10.1155/2020/7136160

Research Article

GLIDE: A Game Theory and Data-Driven Mimicking Linkage Intrusion Detection for Edge Computing Networks

Qianmu Li,[1,2] **Jun Hou**,[3] **Shunmei Meng**,[2] **and Huaqiu Long**[1,4,5]

[1]*Intelligent Manufacturing Department, Wuyi University, Jiangmen 529020, China*
[2]*School of Cyber Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China*
[3]*School of Social Science, Nanjing Institute of Industry Technology, Nanjing 210023, China*
[4]*Jiangsu Zhongtian Technology Co., Ltd., Nantong 226463, China*
[5]*Jiangsu Graduate Workstation, Nanjing Liancheng Technology Development Co., Ltd., Nanjing 210012, China*

Correspondence should be addressed to Qianmu Li; qianmu@njust.edu.cn and Jun Hou; houjunnjust@163.com

Received 2 December 2019; Revised 29 January 2020; Accepted 12 February 2020; Published 30 March 2020

Guest Editor: Yuan Yuan

The real-time and high-continuity requirements of the edge computing network gain more and more attention because of its active defence problem, that is, a data-driven complex problem. Due to the dual constraints of the hybrid feature of edge computing networks and the uncertainty of new attack features, implementing active defence measures such as detection, evasion, trap, and control is essential for the security protection of edge computing networks with high real-time and continuity requirements. The basic idea of safe active defence is to make the defence gain more significant than the attack loss. To encounter the new attacks with uncertain features introduced by the ubiquitous transmission network in the edge computing network, this paper investigates the attack behaviour and presents an attack-defence mechanism based on game theory. Based on the idea of dynamic intrusion detection, we utilize the game theory in the field of edge computing network and suggest a data-driven mimicry intrusion detection game model-based technique called GLIDE. The game income of participants and utility computing methods under different deployment strategies are analysed in detail. According to the proof analysis of the Nash equilibrium condition in the model, the contradictory dynamic game relationship is described. Therefore, the optimal deployment strategy of the multiredundancy edge computing terminal intrusion detection service in the edge computing network is obtained by solving the game balance point. The detection probability of the edge computing network for network attacks is improved, and the cost of intrusion detection of the edge computing network is reduced.

1. Introduction

The essence of network attack and defence confrontation is to detect, monitor, and promptly leverage defence mechanisms to interfere with or block attacks [1]. The attacks of the traditional edge computing network target active defence techniques, which can be mitigated to avoid data theft or data tampering by abnormal detection [2–5]. However, it cannot solve the problem of ubiquitous intrusion monitoring identification in edge computing networks. The system services provided by the edge computing terminal and the cloud computing centre still have the possibility of being attacked [6–11]. It is still a challenge to conduct intrusion detection with data-driven analytics in the security of edge computing network, which is supported by edge, given the complexity of complex systems and the unique features of edge computing.

Many researches have been carried out in the academic world to address the network security risks introduced in the development of edge computing networks [12–29]. However, as the edge computing network is a hybrid network architecture that involves multiple links and multiple technologies, a unified international standard has not yet been formed. The security protection technologies for edge computing networks have also experienced password protection, security models, access control policies, host hardening to anomaly detection, and association analysis [30–38]. However, the above technologies are mainly based

on passive defence. In fact, they can only be used to detect attacks and respond afterwards but not to prevent attacks. It is no longer able to adapt to the current open Internet environment that is dynamically changing and requires high real-time performance and reliability. These researches have certain limitations in the context of edge computing networks:

(1) In terms of terminal penetration defence, existing edge computing terminal security mainly uses cryptographic technology and trusted computing technology to achieve terminal security authentication and data storage computing security. Due to the difficulty of key management and the high degree of intervention, the cost of defence is too high, which is not suitable for the security protection of multiple heterogeneous terminals in the edge computing environment. At the same time, the existing terminal trust evaluation technology has limitations such as poor reputation evaluation accuracy and large amount of calculation. Therefore, dynamic learning and dynamic measurement cannot be performed according to the behaviour characteristics of edge computing terminals, penetration attacks by malicious terminals cannot be effectively detected, and advanced defense control cannot be performed. So, the research results cannot be directly used for edge attack detection and active defence of edge computing terminals.

(2) In terms of data security interactions, facing the demand of data security protection of edge computing network, many research studies have paid attention to the privacy protection and secure transmission of edge computing data, which are generally implemented using cryptographic technology and secure transmission protocols. However, most of the researches do not take into account the real-time requirements of data transmission in the edge computing network environment, so it is difficult to apply to the real-time secure interaction of edge computing data. In addition, the existing research results do not consider the impact on the data transmission efficiency in the case of network attacks and cannot adaptively adjust the data transmission scheme according to the degree of network attack damage to ensure transmission efficiency. Therefore, the existing secure transmission technology generally belongs to the passive defence technology, which cannot actively avoid or suppress network attack behaviours and cannot meet the needs of security in edge computing networks.

(3) In terms of network attack detection, the current research studies of mainstream intrusion detection for edge computing networks are focused on anomaly detection. Deep learning techniques are used to build behaviour models of edge computing networks and to detect and identify various types of network attacks based on model deviations. After the abnormality is identified, the implementation mechanism of new or unknown network attacks cannot be analysed, and the detection results cannot be directly used for the normal monitoring of subsequent network attacks nor can they protect the edge computing network protection objects. At the same time, the current intrusion detection technology mainly considers the accuracy of the detection model but has limited consideration of the application scope of the method and pays insufficient attention to the defence cost of intrusion detection. Therefore, according to the definition of active defence of network security, the balance between defence gains and attack losses in the course of offensive and defensive game of existing technology needs to be further studied.

(4) In terms of system attack defence disposal, there are few existing research studies on attack defence technologies for the edge computing network system domain, and only a few research results have emphasized the necessity of cooperative and coordinated processing. At present, the efficient disposal technology of attack linkage is mainly defence disposal technology based on alarm correlation analysis and defence disposal technology based on state attack graph. However, the state attack graph technology has many limitations in the implementation process, such as the failure to accurately quantify the calculation of the attack success probability and the definition of the attack hazard index, making the calculation accuracy in practical applications poor, and it is difficult to effectively defend against low-cost defence. In addition, in the case of a large-scale system in an edge computing network, there is a space explosion problem in generating a state attack graph. How to solve the network security incidents of large-scale interconnected systems in edge computing networks at low cost and high efficiency is the NP problem.

Therefore, the key issue that needs to be addressed is how to establish a linkage closed-loop intrusion detection and disposal mode from the time domain, space domain, and security domain to achieve correlation analysis and optimal disposal, improve the survivability of core business systems in edge computing networks, and provide the system with the ability to deal with various attacks in a complex environment.

To improve the security for the entire edge computing network, we further study the edge computing network intrusion mimicking linkage detection technology. The mimic defence technology uses computing or service components with functional equivalents and different structures as elements, is based on a "nonsimilar redundancy" structure with high availability and reliability, and cooperates with the multimode voting mechanism that does not rely on rules and features. It disturbs the judgment of the attacker through the nonlinear transformation of the system's external characteristics. Mimic defence technology is based on dynamic heterogeneous redundant construction. It uses the harsh conditions that the attacker cannot construct

the attack methods of all heterogeneous components simultaneously to introduce a dynamic scheduling strategy that can avoid collaborative attacks, making it difficult for the attacker to maintain the attack chain through the voting mechanism. Also, it can increase the difficulty for attackers to detect and scan.

In recent years, more and more research works have focused on developing and advancing mimic defence technology. Li et al. [37] proposed a complex attack linkage decision-making method, which provides guiding security architecture for the construction of a mimic defence system. Tong et al. [38] used the multilevel structure of the web server to design a dynamic heterogeneous redundancy foundation at the operating system layer and server software layer and realized the establishment of a mimic defence system in the web server field.

Based on [37, 38], Sang and Li [39] studied mimic defence techniques of edge computing terminal, which is also the basic framework of this paper. However, there are few researches focusing on the security analysis methods of mimic defence systems. In this paper, we propose a multiredundancy voting mechanism for the intrusion detection on the edge computing terminal. Moreover, we achieve the optimal collaborative detection rate by designing the optimal deployment strategy of multiredundancy edge computing terminal intrusion detection service. The purpose of the multiredundancy voting mechanism in the mimicry defence model on the edge computing terminal is to analyse the differences in the execution results of heterogeneous redundant executives. It thus not only implements intrusion detection but also helps to hide and defend real services. Under the edge computing network environment, the intrusion detection capability of the edge computing terminal improves the collaborative detection of network attacks. However, edge computing networks have ubiquitous interconnection characteristics [5, 6]. Therefore, if the intrusion detection measures do not adequately deploy, then the risk of taking control of the business services will be increased. Nevertheless, the capability of the underdeployed edge computing terminal service with intrusion detection will cause attackers to bypass the edge computing terminal to attack the real service directly. On the other hand, to resist the network intrusion, it will undoubtedly increase defence costs and occupy additional edge computing resources when deploying a great deal of multiredundant edge computing terminals [7]. To address this issue, we present a methodology, called Game theory and Data-driven Mimicking Linkage based Intrusion Detection of Edge Computing Network (GLIDE), which combines the multiredundancy edge computing terminal intrusion detection service technique and the game theory. GLIDE calculates the income equilibrium point of the participants according to the equilibrium condition decision. We further implement an optimal defence income deployment strategy for multiredundancy edge computing terminal intrusion detection services in edge computing networks in order to improve the detection rate of network attacks and thus enhance the security of the network. Figure 1 shows the schematic of this study.

The contributions of this paper are summarized as follows:

(i) First of all, we present a novel edge computing network mimic linkage intrusion detection model called GLIDE to resist unpredictable attacks in the edge computing network.

(ii) Secondly, we utilize the game theory in the field of the edge computing network and suggest a game model-based mechanism which employs the optimal intrusion detection deployment strategy considering the perspective of intrusion detection revenue. Also, we analyse the interaction between the attacker and the intrusion detection system to obtain an optimal decision-making scheme for the defence action set using the game model.

(iii) Thirdly, we utilize the Nash equilibrium of attack and defence income in the game model, which can be used to optimize the defence cost and the strategy of the intrusion detection service.

The rest of the paper is organized as follows: Section 2 presents some background and related works. Section 3 introduces the mimic state linkage intrusion detection of edge computing networks and its game model and discusses the advantages and the utility of different participants according to different situations. Section 4 provides the analysis of the Nash equilibrium in the model and designs an optimal deployment strategy for the multiredundancy edge computing terminal mimicry defence intrusion detection service. Section 5 describes the experimental analysis of the proposed model. Section 6 concludes the paper.

2. Related Research

With the diversified, collaborative, and intelligent development of network attack techniques such as advanced persistent attacks (APT) and multistep combined penetrating attacks have become the main form of the threatening network security [8]. These days, unpredictable attack detection techniques have drawn attention from the cybersecurity researchers in the field of attack and defence [9]. The defence of the new attack is also one of the original motivations for the active protection of network security [10]. Fu et al. [11] combined the conventional APT attack technology and principle and classified the attack into six implementation stages: detection preparation, code incoming, initial intrusion, etc., and summarized the attack characteristics. Then, they reviewed the current state of the research on existing APT attack detection defence frameworks. Moreover, they pointed out research content and latest developments of four mainstream APT attack detection technologies, such as network traffic anomaly detection and malicious code anomaly detection. However, the above-explained detection algorithms need to be implemented based on big data analysis technology. In the environment of high real-time performance and extensive data in the edge computing network, there are still problems such as insufficient timeliness and complicated calculation when an

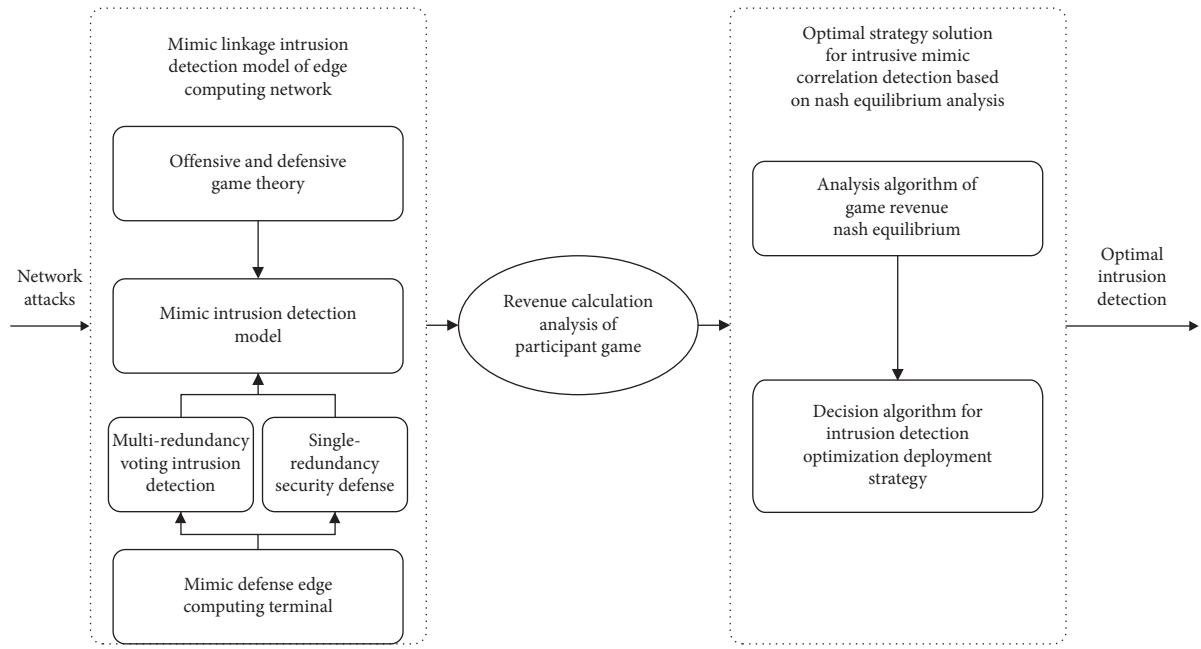

Figure 1: The schematic of the active optimization deception defence of edge computing network attacks.

abnormality is discovered [12, 40]. In the new attacks, such as APT, there is an important feature that is multipoint and multitarget attack, which is different from traditional ones [13–15]. In response to the intrusion detection problem of this type of attack, Qi [16] proposed a distributed intelligent detection model based on multiagent. The model uses a distributed architecture based on a three-level agent. The Management Agent, the Resident Agent, and the Mobile Agent are not only independent but also cooperative with each other. Also, it implements real-time analysis and alerting of network data and hardware information in the target system. Liu et al. [17] introduced agent technique into network intrusion detection and proposed a network intrusion detection framework model based on distributed mobile agent technology. It applies the misuse detection mode and the anomaly detection mode in a coordinated way. There are many similar research studies on distributed collaboration and linkage intrusion detection. Notwithstanding, such research mainly focuses on collaborative strategy between intrusion detection systems. They have not considered factors through the actual network attack and defence processes, such as the asymmetry of information and the asymmetry of the consequences. Therefore, how to develop an adaptive intrusion detection method that adapts to the characteristics of network attack changes has attracted the attention of many scholars [18–21].

According to the confrontational nature of network attack and defence [22], from the view of active defence, the core goal is to seek the optimal network defence benefits that match the cyber-attack hazard. On the contrary, from the perspective of the attacker, the core goal is to find the best damage from the attack [23]. Consequently, relevant research introduces the game theory and studies the optimal strategy of network attack and defence. To carry out the security assessment and active protection of the network, Jiang et al. [24] proposed a network optimal active defence method based on the offensive and defensive game model. It performs the optimal attack and defence strategy selection by solving the game benefit Nash equilibrium condition between the defender and the attacker. To effectively address the network security risk management and reduce the loss of security risk, Gang et al. [8] presented a network security optimal attack and defence decision-making method based on the noncooperative non-zero-sum game model. It generates an optimal attack and defence strategy by analysing the attack and defence interactions of attackers and defenders. Zhang et al. [25] introduced a network security defence decision-making method based on the offensive and defensive differential game. In this study, according to the security evolution model, it analyses the change process of the security state of the network system and constructs the differential game model of attack and defence. Also, this technique presents the solution way of saddle point strategy and gives the optimal defence strategy selection algorithm. Wang et al. [26] suggested an algorithm for selecting the optimal defence strategy based on the static Bayesian game. This algorithm calculates the effectiveness of the defence strategy based on probability and gives the optimal active defence strategy selection algorithm. Also, they have employed the game theory into the study of optimal strategy selection for network intrusion detection. Shen et al. [27] recommended a wireless sensor network intrusion detection approach. From the perspective of saving defence cost, it gives the optimal strategy for intrusion detection service deployment in a wireless sensor network environment. To address the massive linkage control problem of attack detection, Li et al. [28] used game theory to analyse the security combination model of firewall, intrusion detection system (IDS), and vulnerability scanning technology and gave the optimal intrusion detection calculation method. At the same

time, in the particular network environment with obvious resource constraints such as WSN network and mobile Adhoc network, the game theory is also applied to the solution of the optimal intrusion detection strategy [29–34]. Research on mimetic honeypot intrusion detection technology based on game theory is also often involved [35, 36]. In general, game theory has been widely used in the field of network attack and defence and can be used to solve the optimal strategy of network attack and defence.

Game theory is a decision-responsive mathematical model which makes one side of a game to change its strategy according to the decision made by the counterpart. To a certain extent, game theory can be defined as the principle for using mathematical models to study the conflict and cooperation between intelligent and rational decision makers. There are several elements in the game theory model.

Definition 1. Participants: the decision makers in the game model. There must be at least two participants in a game model. Participants perform specific actions which can influence each other in the game model.

Definition 2. Strategy set: the strategy of the game model can be divided into pure strategy and hybrid strategy according to its precise characteristics. If the policies are clearly defined action choices, they are described as pure strategies, while the hybrid strategy uses probability distribution on the purely strategic basis. A collection of policies can be called a response space. The types of response space can be classified into pure strategy space and hybrid policy space according to the corresponding strategy.

Definition 3. Offensive and defensive income: the purposes of participants in the game model are the same: maximize its outcomes while minimizing costs. When game participants fully understand the actions of other participants, they use a game model with complete information rather than a game with incomplete information. In this case, it is impossible to understand the strategies of other participants fully. Moreover, when the utility function and the possible approach are known to all model participants, a game with complete information is performed.

In essence, the core of mimic defence is the voting mechanism. The voter, also known as the voter agent, ensures that no program instance is broken by comparing the output of different variants. The voter is a necessary channel for the heterogeneous redundant executable bodies to output messages. The multiredundancy voter monitors the operating status of all equivalent executives in the mimic defence model. It takes the output of multiple heterogeneous executors as input and performs content-level comparison to realize the abnormality of heterogeneous redundant executors.

In this paper, the multiredundancy voting mechanism of the edge computing terminal mimic defence technology has intrusion detection capabilities. Assume that, for the same request, the response results of different redundant components are equivalent. However, in a real network environment, the system may be attacked or maliciously damaged at any time, and some redundant components may be damaged, leading to service failure. Therefore, the response results may be invalid or wrong, which leads to inconsistent response results of the redundant components, thus achieving the purpose of intrusion detection. Commonly used voting algorithms include majority voting algorithm, large number voting algorithm, median voting algorithm, and unanimous voting algorithm. Voting can be implemented at multiple levels in the software stack, including the application layer and the middleware layer. Several common voting algorithms are summarized in Table 1.

Common voting algorithms ignore the loss and impact on performance, so from the perspective of active defence, the intrusion detection services that rely on multi-redundancy voting mechanisms will inevitably increase the resource overhead of edge computing terminals. From the perspective of network intrusion detection, it can be known that all edge computing terminals in the network exist as intrusion detection nodes. The more intrusion detection services are deployed, the earlier and more comprehensive the attack behaviour can be discovered, thereby preventing the harm caused by the attack. However, in edge computing networks, this is not necessary and is not the optimal deployment method for intrusion detection services. Seeking a reasonable deployment strategy of edge computing terminal intrusion detection service and ensuring the maximization of service revenue and the minimization of defence cost in edge computing network are the best way of active defence. These are the basic characteristics of game theory.

3. Mimetic Intrusion Detection Model Based on Game Theory

The ideal network attack detection should identify most of the possible attacks. At the same time, according to the actual situation, it needs to find a balance between the detection cost and the benefit and also obtains the optimal defence rate by using the minimum cost.

As shown in Figure 2, the mimetic intrusion detection game model is defined as a triple model ADG = (U, S, X), where

$U = (U_1, U_2, \ldots, U_n)$ refers to all participants in the offensive and defensive game model. Participants are the subject of the game, where n represents the number of participants. $\{P, Q\}$ describes all participants in the game according to the actual participation of the offensive and defensive game. $P \triangleq \{P_1, P_2, P_3\}$ denotes three kinds of service existing in the edge computing network, that is, the master station system service, the multiple redundancy edge computing terminal intrusion detection service, and the single-redundancy edge computing terminal service. Among them, the multiredundancy edge computing terminal service has intrusion detection capability. $Q \triangleq \{Q_1, Q_2\}$ represents normal users and attackers (malicious users), respectively.

$S = (S_1, S_2, \ldots, S_n)$ refers to the action set of the participants. Specifically, the action set mainly refers to the

Table 1: Summary of the voting algorithms.

Voting algorithms	Advantage	Common defect
Majority voting	Direct voting, shielding single points of failure	Ignore the loss of performance and affect system availability
K out of N voting	At least K of N results are correct	
Large number of voting	Shield faulty replicas from malicious spread	
Probability-based voting	Improve the probability of consistent correct voting	
Unanimous voting	History information applied to consensus vote	

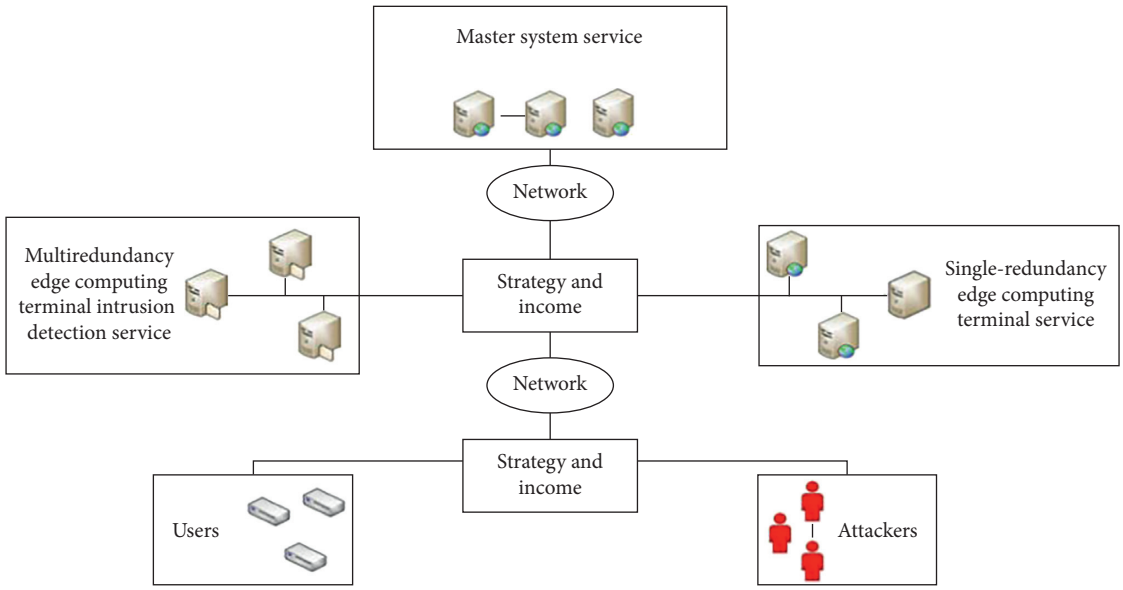

Figure 2: Game-based mimic linkage intrusion detection model.

attack action set and the defence action set in this paper. We use $\{Z_P, Z_Q\}$ to denote the action set of the defender and the action set of attacker, i.e., $\{Z_P, Z_Q\}$ is the set of the attack and defence actions, where $Z_P \triangleq \{s_s^{open}, s_s^{close}\}$ expresses the set of defender's actions. S_s^{open} is the edge computing network providing this type of service. S_s^{close} describes that the edge computing network does not provide this type of service. $Z_Q \triangleq \{s_u^{permit}, s_u^{deny}\}$ represents the set of attacker's actions. S_u^{permit} denotes that this type of user can access services in the edge computing network. S_u^{deny} denotes that this type of user cannot access services in the edge computing network. Table 2 shows the details.

$X = (X_1, X_2, \ldots, X_n)$ expresses the offensive and defensive utility of the participants. Here, different participants have different levels of utility. $\{X_P, X_Q\}$ represents the utility set of the game participants, where X_P denotes the utility of each type of service in the edge computing network. X_Q denotes the accessible utility of normal users and attackers.

3.1. Participants' Income. From game theory, the key process of the game is maximizing the income of the game participants. In the proposed model, we assume that the edge computing network has the prior knowledge of the attack, i.e., the identity of the visitor is known when the service is provided. The assumption is shown in Section 4.

Given a game model ADG = (U, S, X), we define the probability for the visitor as $\{F(Q_1) = 1 - \partial, F(Q_2) = \partial\}$ which denotes the distribution probability of normal users and attackers using the probability and statistical methods. Following the definition, we get the probability distribution of the services (the master station system service, the multiredundancy edge computing terminal intrusion detection service, and the single-redundancy edge computing terminal service) provided by the edge computing network, which is $\{F(P_1) = 1 - \tau - \upsilon, F(P_2) = \upsilon, F(P_3) = \tau\}$.

Table 2: Action set of the participants.

Participants	Action set	
Master system service	s_s^{open}	s_s^{close}
Multiredundancy edge computing terminal intrusion	s_s^{open}	s_s^{close}
Single-redundancy edge computing terminal service	s_s^{open}	s_s^{close}
Normal users	S_u^{permit}	S_u^{deny}
Attackers (malicious users)	S_u^{permit}	S_u^{deny}

Definition 4. Game strategy: in the game model, the probability distribution of the action set participant selected is called the game strategy. When using binary 0 or 1 decision, the probability distribution is called pure approach. On the contrary, the procedure is hybrid when using different probability values decision.

In the proposed game model, the participants' game stage and action set are clear. The game strategy, therefore, exploits a pure approach. This section analyses the benefits of various game scenarios based on different system services and different participants.

3.1.1. Master Station System Services. The master station system service is the real service of the business system in the edge computing network. If the user is normal and accesses the master station system service, the benefit of the master station system service and the access revenue of the normal user are both $\alpha(\alpha > 0)$. If the attacker can access the primary system services, then the master station system service will be damaged, leading to deterioration of the capability of the master station system service on the edge computing network. Therefore, we define the attacker's income $\rho\alpha$, where $\rho \geq 1$ represents the attacker's attack damage factor. At this point, the service income of the real system is $-\rho\alpha$.

3.1.2. Multiredundancy Edge Computing Terminal Intrusion Detection Services. Multiredundancy edge computing terminal intrusion detection service, i.e., the edge computing terminal service, detects the network intrusion by using the multiredundancy heterogeneous executable bodies and the multiredundancy voting mechanisms when the edge computing network is enabled. Normal users cannot access this kind of intrusion detection service, regardless of the multiredundancy edge computing terminal intrusion detection service, which means that the service does not increase their access income of the regular business. Therefore, the normal user's access income is 0. Equivalently, the service income of the edge computing terminal intrusion detection service is 0 as well. From the counterpart perspective, when the multiredundancy edge computing terminal intrusion detection service detects an attacker successfully, the service income is $\mu\beta$, where $\beta > 0$ and $\mu \geq 1$ is the intrusion detection factor (i.e., an attacker's success intrusion probability). At this point, the attacker's access income is $-\mu\beta$.

3.1.3. Single-Redundancy Edge Computing Terminal Service. Single-redundancy edge computing terminal service, i.e., an edge computing terminal service, uses a single redundant executive body in an edge computing network. This kind of service has a capability of preventing the network intrusion but a deficient capability of detecting the network intrusion; due to that it cannot exploit the multiredundancy voting mechanism. Under the normal situation, the normal user's access income of the single-redundancy edge computing terminal service is 0. However, if the attacker accesses the single-redundancy edge computing terminal service, it may be attacked and damaged. The service income thus is $-\rho\alpha$. At this point, the attacker's access income is $\rho\alpha - \varepsilon\beta$, where $\beta > 0$, and $\varepsilon \geq 1$ represents a single-redundancy edge computing terminal service defence factor.

3.2. Participants' Utility. In this subsection, we consider the dynamic gaming phase of five roles (master station system service, the multiredundancy edge computing terminal intrusion detection service, the single redundancy of the edge computing terminal service, the normal user, and the attacker). Moreover, we comprehensively calculate the offensive and defensive utilities of all participants' game based on the change of corresponding participants during the game process and achieve the optimal strategy using the duction of the Bayesian principle.

3.2.1. Utility Analysis of Master Station System Service. Considering the instantiating executing strategy s_s^{open} (i.e., the normal users and attackers can access the master system service at the same time), the total service utility of the master station system service (i.e., X_{P_1}) can be calculated by

$$\begin{aligned} X_{P_1}\left(s_s^{\text{open}}\right) &= F(Q_1) * \alpha + F(Q_2)(-\rho\alpha) \\ &= (1 - \partial - \partial\rho)\alpha. \end{aligned} \tag{1}$$

Similarly, when the system service is in a situation exposed to attack s_s^{close} (i.e., the master system service is in the extreme case of being unable to provide services due to occurring an attack), the total service utility of the actual system is

$$\begin{aligned} X_{P_1}\left(s_s^{\text{close}}\right) &= F(Q_1) * (-\alpha) + F(Q_2) * 0 \\ &= (\partial - 1)\alpha. \end{aligned} \tag{2}$$

3.2.2. Utility Analysis of Multiredundancy Edge Computing Terminal Intrusion Detection Service. The executing strategy is s_s^{open} (i.e., the multiredundancy edge computing terminal intrusion detection service provides access to normal users and attackers at the same time); the total service utility of the multiredundancy edge computing terminal intrusion detection service (i.e., X_{P_2}) can be calculated by

$$\begin{aligned} X_{P_2}\left(s_s^{\text{open}}\right) &= F(Q_1) * 0 + F(Q_2) * \mu\beta \\ &= \partial\alpha, \end{aligned} \tag{3}$$

where the executing strategy is s_s^{close} (i.e., there is no multiredundancy edge computing terminal intrusion detection service into the edge computing network); the total service utility is

$$\begin{aligned} X_{P_2}\left(s_s^{\text{close}}\right) &= F(Q_1) * 0 + F(Q_2) * 0 \\ &= 0. \end{aligned} \tag{4}$$

3.2.3. Utility Analysis of Single-Redundancy Edge Computing Terminal Service. The executing strategy is s_s^{open} (i.e., the single-redundancy edge computing terminal service provides access to normal users and attackers at the same time); the total service utility of the single-redundancy edge computing terminal service (i.e., X_{P_3}) can be calculated by

$$\begin{aligned} X_{P_3}\left(s_s^{\text{open}}\right) &= F(Q_1) * 0 + F(Q_2) * (-\rho\alpha) \\ &= -\partial\rho\alpha. \end{aligned} \tag{5}$$

In the case of executing strategy s_s^{close} (i.e., there is no single-redundancy edge computing terminal service in the edge computing network), the total service utility is

$$X_{P_3}\left(s_s^{\text{close}}\right) = F(Q_1) * 0 + F(Q_2) * 0 = 0. \tag{6}$$

3.2.4. Utility Analysis of Normal Users. In a situation where the normal user executes the strategy s_u^{permit}, the summation of access utility can be calculated by considering the access of the master station system service, the multiredundancy edge computing terminal intrusion detection service, and the single-redundancy edge computing terminal service, which is

$$X_{Q_1}\left(s_u^{\text{permit}}\right) = F(P_1) * (\alpha) + F(P_2) * 0 + F(P_3) * 0 = (1 - \tau - \upsilon)\alpha. \tag{7}$$

When the normal user executes strategy s_u^{deny} (i.e., a normal user does not access the services in the edge computing network due to the network attacks), the summation of access utility is

$$X_{Q_1}\left(s_u^{\text{deny}}\right) = F(P_1) * 0 + F(P_2) * 0 + F(P_3) * 0 = 0. \tag{8}$$

3.2.5. Utility Analysis of Attackers. For the attackers during the game, where the attacker executes the strategy s_u^{permit}, the summation of access utility is calculated by utilization of attacker on accessing the master station system service, multiredundancy edge computing terminal intrusion detection service, and the single-redundancy edge computing terminal service, which is

$$\begin{aligned} X_{Q_2}\left(s_u^{\text{permit}}\right) &= F(P_1) * \rho\alpha + F(P_2) * (-\mu\beta) + F(P)_3 * (\rho\alpha - \varepsilon\beta) \\ &= (1 - \tau - \upsilon) * \rho\alpha + \upsilon * (-\mu\beta) + \tau * (\rho\alpha - \varepsilon\beta) \\ &= \rho\alpha - \upsilon\rho\alpha - \upsilon\mu\beta - \tau\varepsilon\beta \\ &= \rho\alpha - \upsilon(\rho\alpha + \mu\beta) - \tau\varepsilon\beta. \end{aligned} \tag{9}$$

On the other hand, when the attacker does not access the services in the edge computing network, that is, in the case of executing strategy s_u^{deny}, the utility of the attacker is

$$X_{Q_2}\left(s_u^{\text{deny}}\right) = F(P_1) * 0 + F(P_2) * 0 + F(P_3) * 0 = 0. \tag{10}$$

Considering the calculations mentioned above, we can obtain the utility for normal users and attackers performing different game actions when accepting different services, respectively.

4. Solution of Optimal Strategy for GLIDE

Game participants often have difference and balance on strategy selection. For example, when an attacker finds that the object being attacked is a multiredundancy edge computing terminal intrusion detection service system, the rational attacker will pursue the maximum attack damage with the minimum attack cost. In this case, it is obvious that the attacker will not continue to execute the attack method but will alter other strategies or actively stop the attack. For defence system services, when there are no attackers in the network, the approach will be adjusted to minimize the provision of intrusion detection services to save network resources. Similar strategic changes and the game between the offensive and defensive sides are constantly changing. The game of this technique will achieve the optimal income of the participants when the offense and defence sides implement a certain mechanism, respectively, namely, the Nash equilibrium state.

Definition 5. Nash equilibrium: for the attackers and defenders in the game, if and only if each participant's strategy is the best countermeasure against another.

This section provides the analysis and certification for that the Nash equilibrium state exists in the GLIDE model proposed in the paper. Based on this inspiration, the Nash equilibrium calculation results are used as the basis for decision-making, which guides the optimal deployment strategy of multiredundancy edge computing terminal intrusion detection services in edge computing networks.

Since each participant can adopt many types of strategy combinations in the game model, this section first discusses the execution of the S_s^{open} strategy by each servant and the execution of the S_u^{permit} strategy by normal users and attackers (i.e., the Nash equilibrium condition is on the case that the edge computing network executes the strategy $\{(S_s^{\text{open}}, S_s^{\text{open}}, S_s^{\text{open}})(S_u^{\text{permit}}, S_u^{\text{permit}})\}$).

According to the definition of Nash equilibrium, we first know that $X_{P_1}(s_s^{\text{open}})$ should dominate under Nash equilibrium condition from the perspective of the master system service. Assume $X_{P_1}(s_s^{\text{open}}) = X_{P_1}(s_s^{\text{close}})$; we can obtain

$$\partial = \frac{2}{2 - \rho}. \tag{11}$$

If so, the utility of providing the normal service by the master station system $X_{P_1}(s_s^{\text{open}})$ is greater than that of not providing service $X_{P_1}(s_s^{\text{close}})$, which should be the optimal target pursued by the edge computing network. $\partial < 2/(2 - \rho)$ is the preferred condition. We thus infer that the edge computing network will choose to provide the master system service when $\partial < 2/(2 - \rho)$. On the contrary, $\partial > 2/(2 - \rho)$; the strategy s_s^{close} will be selected as the executed one. However, according to the game, when the primary station system provides the service, the preferred strategy of the multiredundancy edge computing terminal intrusion detection service and the single-redundancy edge computing terminal service must be S_s^{open}.

We further assume that $X_{Q_1}(s_u^{\text{permit}}) = X_{Q_1}(s_u^{\text{deny}})$ and $X_{Q_2}(s_u^{\text{permit}}) = X_{Q_2}(s_u^{\text{deny}})$; the following can be derived:

$$\upsilon = 1 - \tau, \tag{12}$$

$$\upsilon = \frac{\rho\alpha - \tau\varepsilon\beta}{\rho\alpha + \mu\beta}. \tag{13}$$

From (11) and (12), we can obtain

$$1-\tau=\frac{\rho\alpha-\tau\varepsilon\beta}{\rho\alpha+\mu\beta},$$
$$\tau=\frac{\mu\beta}{\rho\alpha+\mu\beta-\varepsilon\beta}. \tag{14}$$

We then derive

$$\partial<\frac{2}{2-\rho}\upsilon<1-\tau\tau<\frac{\mu\beta}{\rho\alpha+\mu\beta-\varepsilon\beta}. \tag{15}$$

According to equation (15), when the edge computing network executes $\{(S_s^{\text{open}}, S_s^{\text{open}}, S_s^{\text{open}})(S_u^{\text{permit}}, S_u^{\text{permit}})\}$, in order to optimize the utility of each participant, the Nash equilibrium conditions are

$$\partial<\frac{2}{2-\rho},$$
$$\upsilon<1-\tau, \tag{16}$$
$$\tau<\frac{\mu\beta}{\rho\alpha+\mu\beta-\varepsilon\beta}.$$

Theorem 1. *Consider the execution* $\{(S_s^{open}, S_s^{open}, S_s^{open})(S_u^{permit}, S_u^{permit})\}$*; the model has a Bayesian Nash equilibrium and needs to satisfy these conditions:*

$$\partial<\frac{\rho}{2+\rho},$$
$$\upsilon<\frac{1}{2}, \tag{17}$$
$$\tau<\frac{\upsilon\alpha-\mu\beta}{2(\mu+\varepsilon)}.$$

Similarly, when an attacker stops attacking, i.e., the edge computing network executes the strategy $\{(S_s^{\text{open}}, S_s^{\text{open}}, S_s^{\text{open}})(S_u^{\text{permit}}, S_u^{\text{deny}})\}$, the conditions that participant obtains the utility Nash equilibrium are

$$\partial<\frac{2}{2-\rho},$$
$$\upsilon<1-\tau, \tag{18}$$
$$\tau>\frac{\mu\beta}{\rho\alpha+\mu\beta-\varepsilon\beta}.$$

Since the multiredundancy edge computing terminal intrusion detection service and the single-redundancy edge computing terminal service are S_s^{open}, we only need to consider the case when the normal user executes the strategy S_u^{deny}. That is, when the strategy $\{(S_s^{\text{open}}, S_s^{\text{open}}, S_s^{\text{open}})(S_u^{\text{deny}}, S_u^{\text{deny}})\}$ is executed by GLIDE, the Nash equilibrium conditions are

$$\partial<\frac{2}{2-\rho},$$
$$\upsilon>1-\tau, \tag{19}$$
$$\tau>\frac{\mu\beta}{\rho\alpha+\mu\beta-\varepsilon\beta}.$$

According to the solution results that use the Nash equilibrium condition under the above different strategies, this section can be used to solve the optimal algorithm of the mimic state linkage intrusion detection optimal strategy for edge computing networks, which is depicted in Algorithm 1.

5. Security Analysis of GLIDE

At present, the single-redundancy defence model based on the mimic defence idea is basically an iPo model. As shown in Figure 3, when a submitted request is entered into the system, it is first copied by the input proxy unit into n copies and forwarded to the executive body set. The executive body set contains n similar redundant executors, of which $P_1, P_2, P_3, \ldots, P_n$ are executors with the same function but different implementation methods; each executor accepts a copy of the request and processes it. The processing result of each executor outputs a response after voting by the voter. Taking advantage of the dependence of network attacks on the environment, an attack targeting a specific vulnerability cannot be effectively played in heterogeneous executors $(P_1, P_2, P_3, \ldots, P_n)$ at the same time, thereby achieving a defence effect against the vulnerability attack. The multi-redundancy voter mainly compares the differences in the execution results of redundant executors, so as to vote whether the mimic defence system has suffered network intrusion and achieve the purpose of intrusion detection. Based on mimic defence technology, mimic defence structure routers, mimic defence structure distributed storage systems, mimic defence structure web servers, and other systems with mimic defence structures have been formed.

Based on the existing mimic defence, this paper uses the Dynamic Heterogeneous Redundancy model to design and build a dynamic heterogeneous redundant mimic defence model for edge computing terminals, as shown in Figure 4. It adds a heterogeneous component set, a dynamic scheduling algorithm, and a heterogeneous element pool. Heterogeneous element pool provides diversified design of components at various levels and can form a heterogeneous component set, which improves the security of the system. When the executor in the executive body set is attacked, the system selects components from the heterogeneous component set to replace the attacked executor in the executive body set according to the dynamic scheduling algorithm, so

Input: $\partial, \rho, \upsilon, \tau, \alpha, \mu, \varepsilon, \beta$
Output: Optimized Solution
(1) *if* $\partial < 2/(2-\rho)$ *then*
(2) *if* $(\upsilon < 1-\tau) \wedge (\tau < (\mu\beta/(\rho\alpha + \mu\beta - \varepsilon\beta)))$*then*
(3) executes $\{(S_s^{open}, S_s^{open}, S_s^{open})(S_u^{permit}, S_u^{permit})\}$ strategy
(4) *end*
(5) *else*
(6) *There is no optimal strategy.*
(7) *end*
(8) *if* $(\upsilon < 1-\tau) \wedge (\tau > (\mu\beta/(\rho\alpha + \mu\beta - \varepsilon\beta)))$*then*
(9) executes $\{(S_s^{open}, S_s^{open}, S_s^{open})(S_u^{permit}, S_u^{deny})\}$ strategy
(10) *end*
(11) *else*
(12) *There is no optimal strategy.*
(13) *end*
(14) *end*
(15) *else*
(16) *if* $(\upsilon > 1-\tau) \wedge (\tau > (\mu\beta/(\rho\alpha + \mu\beta - \varepsilon\beta)))$*then*
(17) executes $\{(S_s^{open}, S_s^{open}, S_s^{open})(S_u^{deny}, S_u^{deny})\}$ strategy
(28) *end*
(19) *else*
(20) *There is no optimal strategy.*
(21) *end*
(22) *end*
(23) *End*

Algorithm 1: Solving algorithm for optimal strategy of intrusive mimic relation detection.

as to eliminate the environment necessary for the triggering of the attack, making it difficult for the same attack to occur continuously. On the other hand, the existence of a dynamic scheduling algorithm makes the system show different system attributes to the outside during the period, which disturbs the judgment of the attacker and increases the difficulty of scanning and detection by the attacker.

In order to better understand how the key features in the dynamic heterogeneous redundant mimic defence model of the edge computing terminal affect the system's security defence capabilities, this paper conducts security analysis model based on the states of different components in the dynamic heterogeneous redundant mimic defence model of the edge computing terminal. In the model, the transfer of the attacker's position from the current component to its next component is considered as the attacker successfully invaded the current component. The transfer of the attacker's position from the current component to its previous component is considered as the attacker has lost control of the current component. This situation usually manifests itself as a heterogeneous dynamic change of components in the mimic defence system, or an abnormal result is found in the voting output of the voter. In order to avoid that, as the network scale increases, the forward and backward transfer between many components will increase the difficulty of model analysis. This model only focuses on the situation where the attacker invades the next component and stays in the current component from the current component, thereby reducing the complexity of transferring between components.

The security analysis abstract model structure of the dynamic heterogeneous redundant mimicry defence model of the edge computing terminal is shown in Figure 5. The *a* component represents the attacker, the *i* component represents the input proxy module in the mimic defence system, and the logical *P* component represents the set of executive bodies in the mimic defence system, where P_1, $P_2, \ldots, P_n$ represent the specific executor. The *o* component represents the voter in the mimic defence system. These two components are the mimic defence boundary of the system and do not have heterogeneous redundancy features. Therefore, dynamic defence technology is used to prevent the attacker from using the input proxy as a springboard to continuously attack the executive bodies $P_1, P_2, \ldots, P_n$ and hijacking the correct output of the voting system.

The numbers 1, 2, 3, 4, and 5 in the model represent the transfer process of the attack between components, in which 1, 3, and 5 represent the process of the attacker invading the next component from the current component; 2 and 4 represent the process of the attacker staying in the current component.

Assumption 1. When using this model to evaluate the security of a mimic defence system, it is assumed that, for any kind of attack, there will be sufficient heterogeneous executors to build a mimic defence structure without being restricted by the diversity of software and hardware.

Definition 6. Mimic defence component transformation period $T_{dynamic}$: the time period during which the input agent component, executor component, and voter component are dynamically transformed in the model, reflecting

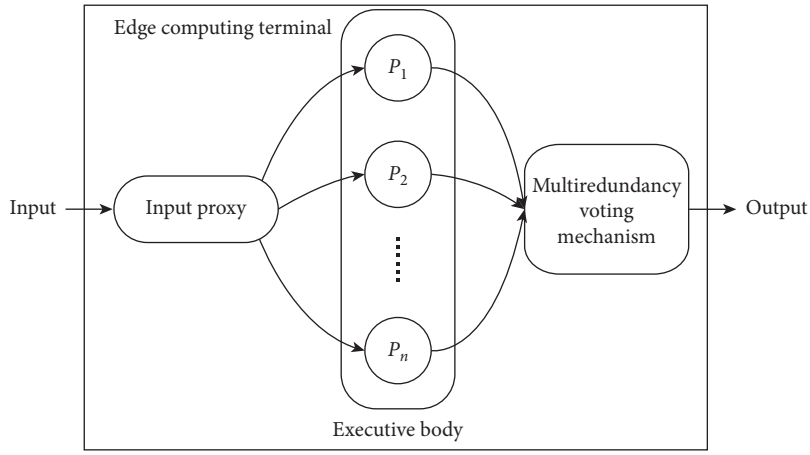

Figure 3: Single-redundancy mimic defence iPo model.

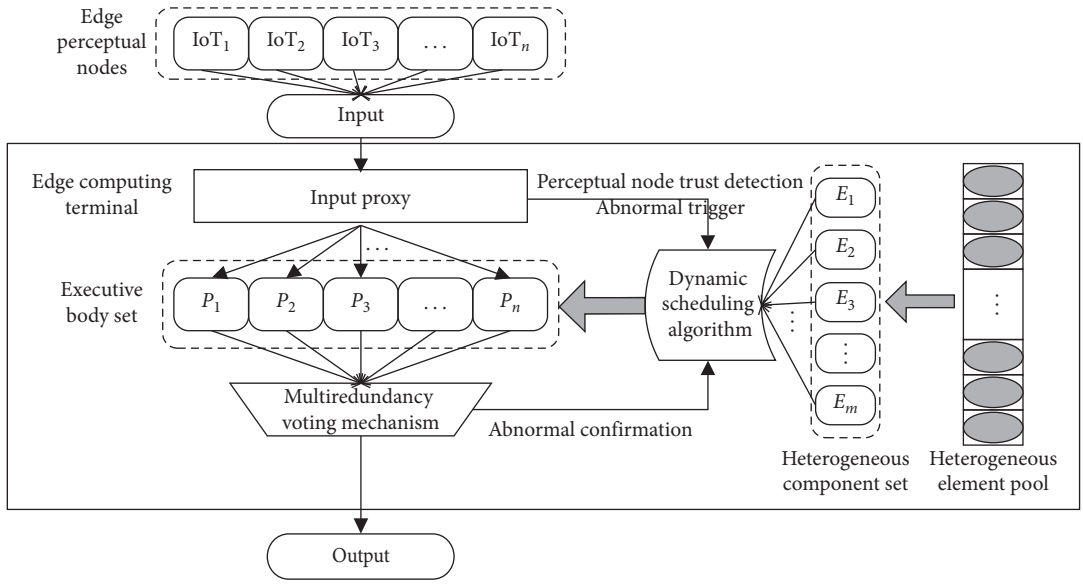

Figure 4: Dynamic multiredundancy mimic defence model.

the dynamic characteristics of the mimic defence structure, which can be fixed or random values.

Definition 7. The time required for the successful implementation of the attack T_{attack}: the time required for the attacker to successfully invade from a component to its next component in the model, reflecting the complexity of the attacker's successful implementation of an attack.

Definition 8. The probability of performance difference p_h between mimic defence executors after being attacked: the probability of heterogeneous attributes between the execution components of the model for an attack, that is, the probability that different execution components will produce different results in an attack is p_h, which reflects the heterogeneous characteristics in the mimic defence structure.

Definition 9. The probability of successful attack transfer by the attacker $p_{(i,j)}$ is the probability that the attacker successfully invades from component i to the next component j in a static system without heterogeneous characteristics and dynamics, reflecting the difficulty of the attacker's successful attack.

5.1. Single-Redundancy Attack Defence Analysis. When the mimic defence system uses single redundancy, the model of the system is shown in Figure 6. The attacker invades the mimic defence system by component a. $p_1, p_2, p_3, p_4, p_5.$, respectively, represent the probability of a component invading the input agent i component, continuing to stay in the i component, invading from the i component to the logical P component, continuing to stay in the logical P component, the logic P component invading the voter o component. The derivation process of p_1 is as follows: before and after any time when component i dynamically changes, the probability that a particular attack launched

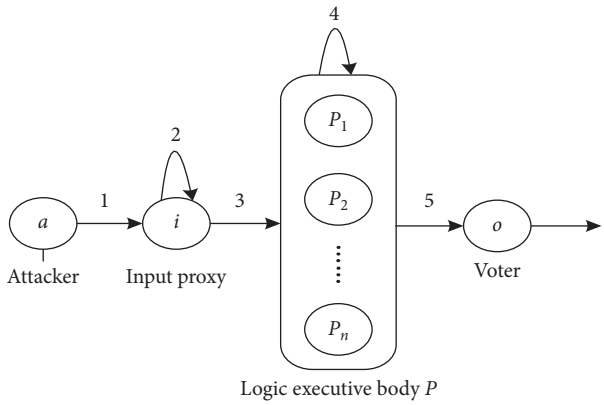

Figure 5: Abstract model for mimic defence security analysis of edge computing terminal.

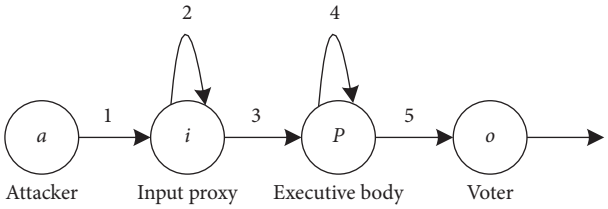

Figure 6: single redundancy mimic defence system security analysis model.

by an attacker is heterogeneous is p_h, so the probability that any dynamic change of component i will not affect the continued implementation of the attack is $1 - p_h$. Component i can have up to $T_{\text{attack}}/T_{\text{dynamic}}$ dynamic transformations during the successful implementation period T_{attack} of an attack. Therefore, the probability that an attacker dynamically changes the component i within the unit time required to complete an intrusion attack does not affect the attack is $(1 - p_h)^{T_{\text{attack}}/T_{\text{dynamic}}}$. Based on the above analysis, the probability of an attacker successfully invading component i by component a can be expressed as

$$p_1 = p_{(a,i)} \times (1 - p_h)^{T_{\text{attack}}/T_{\text{dynamic}}}. \tag{20}$$

After successfully invading component i, an attacker can launch $T_{\text{dynamic}}/T_{\text{attack}}$ attacks against the execution component P in each dynamic transformation period. Then the probability of failure of all intrusion attacks from component i to component P is $(1 - p_{(i,P)})^{T_{\text{dynamic}}/T_{\text{attack}}}$, so the probability of successful intrusion from component i to component P within the dynamic transformation period T_{dynamic} is

$$1 - \left(1 - p_{(i,P)}\right)^{T_{\text{dynamic}}/T_{\text{attack}}}. \tag{21}$$

The attacker will stay on component i during time T_{attack} in the following two cases:

(1) An attacker's infiltration attack from component i to component P fails, and the dynamic transformation of component i does not affect the attack initiated by the attacker. In this case, the probability that the attacker will stay on component i is

$$\left(1 - p_{(i,P)}\right)^{T_{\text{dynamic}}/T_{\text{attack}}} \times (1 - p_h)^{T_{\text{attack}}/T_{\text{dynamic}}}. \tag{22}$$

(2) An attacker's infiltration attack from component i to component P succeeds, and the dynamic transformation of component i does not affect the attack initiated by the attacker, but the dynamic transformation of component P affects the effective implementation of the attack. In this case, the probability that the attacker will stay on component i is

$$\left(1 - \left(1 - p_{(i,P)}\right)^{T_{\text{dynamic}}/T_{\text{attack}}}\right) \times (1 - p_h)^{T_{\text{attack}}/T_{\text{dynamic}}} \times \left(1 - (1 - p_h)^{T_{\text{attack}}/T_{\text{dynamic}}}\right). \tag{23}$$

Combined with the above two situations, the ultimate possibility that the attacker will stay on component i is expressed as

$$\begin{aligned} p_2 &= \left(1 - p_{(i,P)}\right)^{T_{\text{dynamic}}/T_{\text{attack}}} \times (1 - p_h)^{T_{\text{attack}}/T_{\text{dynamic}}} \\ &\quad + \left(1 - \left(1 - p_{(i,P)}\right)^{T_{\text{dynamic}}/T_{\text{attack}}}\right) \times (1 - p_h)^{T_{\text{attack}}/T_{\text{dynamic}}} \\ &\quad \times \left(1 - (1 - p_h)^{T_{\text{attack}}/T_{\text{dynamic}}}\right) \\ &= (1 - p_h)^{T_{\text{attack}}/T_{\text{dynamic}}} - \left(1 - \left(1 - p_{(i,P)}\right)^{T_{\text{dynamic}}/T_{\text{attack}}}\right) \\ &\quad \times (1 - p_h)^{2T_{\text{attack}}/T_{\text{dynamic}}}. \end{aligned} \tag{24}$$

Similarly, when the dynamic transformation between component i and component P does not affect the attack initiated by the attacker, the probability that component i successfully invades component P is $(1 - (1 - p_{(i,P)})^{T_{\text{dynamic}}/T_{\text{attack}}})$, so p_3 can be expressed as

$$p_3 = \left(1 - \left(1 - p_{(i,P)}\right)^{T_{\text{dynamic}}/T_{\text{attack}}}\right) \times (1 - p_h)^{2T_{\text{attack}}/T_{\text{dynamic}}}. \tag{25}$$

Through the equations of p_1, p_2, and p_3, the probability that an attacker can successfully invade component P by component a can be calculated as

$$\begin{aligned} p_P &= p_1 \times \left(p_2^0 + p_2^1 + \cdots + p_2^n\right) \times p_3 \\ &= \frac{1}{1 - p_2} \times p_{(a,i)} \times \left(1 - \left(1 - p_{(i,P)}\right)^{T_{\text{dynamic}}/T_{\text{attack}}}\right) \\ &\quad \times (1 - p_h)^{3T_{\text{attack}}/T_{\text{dynamic}}}. \end{aligned} \tag{26}$$

Next, calculate the probability that component a successfully invades component o. First, we need to calculate p_4 and p_5. According to the process representations and analysis methods of p_1, p_2, and p_3, the expressions of p_4 and p_5 are as follows:

$$p_4 = \left(1 - p_h\right)^{T_{\text{attack}}/T_{\text{dynamic}}} - \left(1 - \left(1 - p_{(P,o)}\right)^{T_{\text{dynamic}}/T_{\text{attack}}}\right) \times \left(1 - p_h\right)^{2T_{\text{attack}}/T_{\text{dynamic}}},$$

$$p_5 = \left(1 - \left(1 - p_{(P,o)}\right)^{T_{\text{dynamic}}/T_{\text{attack}}}\right) \times \left(1 - p_h\right)^{2T_{\text{attack}}/T_{\text{dynamic}}}. \tag{27}$$

Through the equations of p_1, p_2, p_3, p_4, p_5, the probability that an attacker can successfully invade component o by component a can be calculated as

$$\begin{aligned} p_o &= p_1 \times \left(p_2^0 + p_2^1 + \cdots + p_2^n\right) \times p_3 \times \left(p_4^0 + p_4^1 + \cdots + p_4^n\right) \times p_5 \\ &= \frac{1}{1 - p_2} \times p_{(a,i)} \times \left(1 - \left(1 - p_{(i,P)}\right)^{T_{\text{dynamic}}/T_{\text{attack}}}\right) \\ &\quad \times \left(1 - p_h\right)^{3T_{\text{attack}}/T_{\text{dynamic}}} \times \frac{1}{1 - p_4} \\ &\quad \times \left(1 - \left(1 - p_{(P,o)}\right)^{T_{\text{dynamic}}/T_{\text{attack}}}\right) \times \left(1 - p_h\right)^{2T_{\text{attack}}/T_{\text{dynamic}}} \\ &= \frac{1}{1 - p_2} \times \frac{1}{1 - p_4} \times p_{(a,i)} \times \left(1 - \left(1 - p_{(i,P)}\right)^{T_{\text{dynamic}}/T_{\text{attack}}}\right) \\ &\quad \times \left(1 - \left(1 - p_{(P,o)}\right)^{T_{\text{dynamic}}/T_{\text{attack}}}\right) \times \left(1 - p_h\right)^{5T_{\text{attack}}/T_{\text{dynamic}}}. \end{aligned} \tag{28}$$

5.2. 3-Redundancy Attack Defence Analysis. When the mimic defence system adopts 3-redundancy, the model of the system is shown in Figure 7. When an attacker launches an attack from component i to logical execution body P, according to the mimic defence principle, an attacker can successfully invade the logical executable body P only when the executable bodies P_1, P_2, and P_3 are completely isomorphic. According to the above analysis, the probability that P_1, P_2, and P_3 are completely isomorphic is $(1 - p_h)^2$. In this case, the probability of successful invasion from component i to logical component P within the dynamic transformation period T_{dynamic} is $(1 - p_h)^2 \times (1 - (1 - p_{(i,P)}{}^3)^{T_{\text{dynamic}}/T_{\text{attack}}})$. The analysis method of single redundancy mimicry defense system can also be used. In time Ta, the second situation that the attacker will stay at component i can be described as follows an attacker's infiltration attack from component i to component P succeeds, and the dynamic transformation of component i does not affect the attack initiated by the attacker, but the dynamic transformation of the execution component P_i in logic component P affects the effectiveness implementation of the attack. Therefore, the probability that the attacker will stay on component i is denoted as p_2:

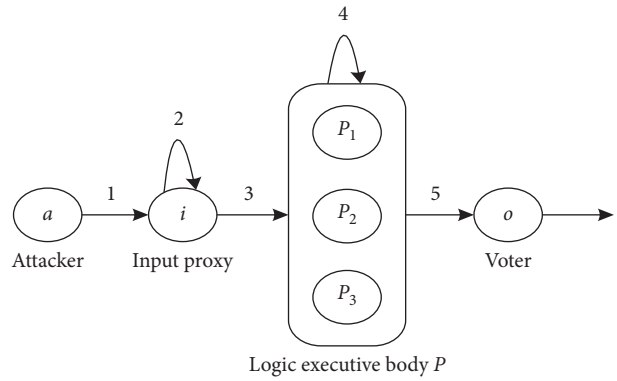

Figure 7: 3-redundancy mimic defence system security analysis model.

$$\begin{aligned} p_2 = {} & \left(1 - \left(1 - p_h\right)^2\right) \times \left(1 - p_h\right)^{T_{\text{attack}}/T_{\text{dynamic}}} + \left(1 - p_h\right)^2 \\ & \times \left(1 - \left(1 - p_{(i,P)}^3\right)^{T_{\text{dynamic}}/T_{\text{attack}}}\right) \times \left(1 - p_h\right)^{T_{\text{attack}}/T_{\text{dynamic}}} \\ & \times \left(1 - \left(1 - p_h\right)^{3T_{\text{attack}}/T_{\text{dynamic}}}\right). \end{aligned} \tag{29}$$

The probability of successfully invading component P by component i is denoted as p_3:

$$\begin{aligned} p_3 &= \left(1 - p_h\right)^2 \times \left(1 - \left(1 - p_{(i,P)}^3\right)^{T_{\text{dynamic}}/T_{\text{attack}}}\right) \\ &\quad \times \left(1 - p_h\right)^{4T_{\text{attack}}/T_{\text{dynamic}}} \\ &= \left(1 - \left(1 - p_{(i,P)}^3\right)^{T_{\text{dynamic}}/T_{\text{attack}}}\right) \\ &\quad \times \left(1 - p_h\right)^{2+\left(4T_{\text{attack}}/T_{\text{dynamic}}\right)}. \end{aligned} \tag{30}$$

Through the equations of p_1, p_2, and p_3, the probability that the component a successfully invades the logical component P can be calculated; p_P is

$$\begin{aligned} p_P &= p_1 \times \left(p_2^0 + p_2^1 + \cdots + p_2^n\right) \times p_3 \\ &= \frac{1}{1 - p_2} \times p_{(a,i)} \times \left(1 - \left(1 - p_{(i,P)}^3\right)^{T_{\text{dynamic}}/T_{\text{attack}}}\right) \\ &\quad \times \left(1 - p_h\right)^{2+\left(5T_{\text{attack}}/5T_{\text{attack}}\right)}. \end{aligned} \tag{31}$$

At the same time, the first case where the attacker will continue to stay at the logic component P during time T_{attack} changes: the attacker launches an infiltration attack from all the execution bodies in the logic component P to the component o, there is an attack failure initiated by the execution body P_i, and the dynamic transformation of all the execution bodies in the logic component P does not affect the attack initiated by the attacker. In this case, the probability that the attacker continues to stay in the logic component P is

$$\left(1 - p_{(P,o)}^3\right)^{T_{\text{dynamic}}/T_{\text{attack}}} \times \left(1 - p_h\right)^{3T_{\text{attack}}/T_{\text{dynamic}}}. \tag{32}$$

Based on the above analysis, p_4 can be expressed as

$$\begin{aligned} p_4 = &\left(1 - p_{(P,o)}^3\right)^{T_{\text{dynamic}}/T_{\text{attack}}} \times (1 - p_h)^{3T_{\text{attack}}/T_{\text{dynamic}}} \\ &+ \left(1 - \left(1 - p_{(P,o)}^3\right)^{T_{\text{dynamic}}/T_{\text{attack}}}\right) \times (1 - p_h)^{3T_{\text{attack}}/T_{\text{dynamic}}} \\ &\times \left(1 - (1 - p_h)^{T_{\text{attack}}/T_{\text{dynamic}}}\right). \end{aligned} \tag{33}$$

p_5 is calculated as follows:

$$p_5 = \left(1 - \left(1 - p_{(P,o)}^3\right)^{T_{\text{dynamic}}/T_{\text{attack}}}\right) \times (1 - p_h)^{2+\left(4T_{\text{attack}}/T_{\text{dynamic}}\right)}. \tag{34}$$

Therefore, when the mimic defence system adopts 3-redundancy, the probability that an attacker can successfully invade component o by component a can be denoted as

$$\begin{aligned} p_o &= p_1 \times \left(p_2^0 + p_2^1 + \cdots + p_2^n\right) \times p_3 \times \left(p_4^0 + p_4^1 + \cdots + p_4^n\right) \times p_5 \\ &= \frac{1}{1 - p_2} \times p_{(a,i)} \times \left(1 - \left(1 - p_{(i,P)}^3\right)^{T_{\text{dynamic}}/T_{\text{attack}}}\right) \\ &\quad \times (1 - p_h)^{2+\left(5T_{\text{attack}}/T_{\text{dynamic}}\right)} \times \frac{1}{1 - p_4} \\ &\quad \times \left(1 - \left(1 - p_{(P,o)}^3\right)^{T_{\text{dynamic}}/T_{\text{attack}}}\right) \times (1 - p_h)^{4T_{\text{attack}}/T_{\text{dynamic}}} \\ &= \frac{1}{1 - p_2} \times \frac{1}{1 - p_4} \times p_{(a,i)} \times \left(1 - \left(1 - p_{(i,P)}^3\right)^{T_{\text{dynamic}}/T_{\text{attack}}}\right) \\ &\quad \times \left(1 - \left(1 - p_{(P,o)}^3\right)^{T_{\text{dynamic}}/T_{\text{attack}}}\right) \times (1 - p_h)^{4+\left(9T_{\text{attack}}/T_{\text{dynamic}}\right)}. \end{aligned} \tag{35}$$

6. Experimental Analysis

6.1. Setting of Experimental Environment. In this section, we built an edge computing network test platform to evaluate the performance of the solution. We first explain the experimental setup and then give detailed experimental results. As illustrated in Figure 8, at first, the edge computing network test platform is designed on the NS2 simulation platform. To simulate the real network environment, we deploy the corresponding network components in the network, such as routers, real system servers, single-redundancy edge computing terminal servers and multiredundancy edge computing terminal servers, and edge computing control centres. The core of the edge computing network is to make full use of the computing power of the edge computing terminal. Therefore, in this experiment, we deployed a large number of edge computing terminal groups and relied on the edge computing control centre for management and interconnection. In this experiment, 500 edge computing terminals were set up for simulation experiments. Due to the limited computing power and resources of the edge computing terminal, we considered the simulation time to be 10 minutes to ensure the accuracy and rationality of the experiment.

Specifically, in GLIDE, only the multiredundancy edge computing terminal service has an intrusion detection function, and the service inevitably consumes more network resources. The proposed model considers the proportion of the multiredundancy edge computing terminal intrusion detection service in the three types of core services that directly determine the performance of the model. Therefore, during the experiment, we changed the number-ratio relationship between the single-redundancy edge computing terminal server and the multiredundancy edge computing terminal server. Moreover, by compromising the two specific indicators, which are the number of edge computing terminals and the capture rate of malicious packets, the performance of the proposed model concerning edge computing resource consumption and intrusion prevention is comprehensively considered.

6.2. Analysis of the Experimental Results. This section tests the defence performance of the proposed attack and defence game model through the performance of network resource consumption and detection rate. We compare and prove it with the performance of the existing Fog-IDS model [14] and the EIDS model [15]. According to the above theoretical analysis, this paper adopts three different edge computing network service-deployment strategies and allocates them with a probability of $\{\tau, \upsilon\} = \{(0.5, 0.3), (0.3, 0.5)\}$, where τ, υ respectively represent single-redundancy edge computing terminal service and multiredundancy edge computing terminal service, and the latter has intrusion detection capabilities. Through the comparison of these different probabilities, this paper will get different compromise edge computing terminals' number and malicious packets' capture rate. These results can help find a reasonable service strategy deployment method in the edge computing network.

6.2.1. Analysis of the Results of Compromising the Number of Edge Nodes. Due to the limited existing computing power of the edge computing terminal in edge networks, edge computing terminals are vulnerable to be attacked from the network or maliciously exploited by illegal users. Therefore, it is particularly important to properly allocate the intrusion detection service of the edge computing terminal, that is, to properly deploy the multiredundancy edge computing terminal intrusion detection service in the GLIDE. Next, we find a reasonable deployment plan by comparative verification experiment.

By comparing the model of this paper with the existing Fog-IDS model and EIDS model. the relationship between the number of compromised edge computing terminals and the life cycle of the edge computing terminal is shown in Figure 9. It can be observed that the life cycle of the edge computing terminal has become longer, and the number of compromised edge computing terminals of the three models tends to increase. However, by comparison, during the terminal life cycle, the number of compromised edge computing terminals of the GLIDE is controlled to be less than 200, which is significantly less than the Fog-IDS model

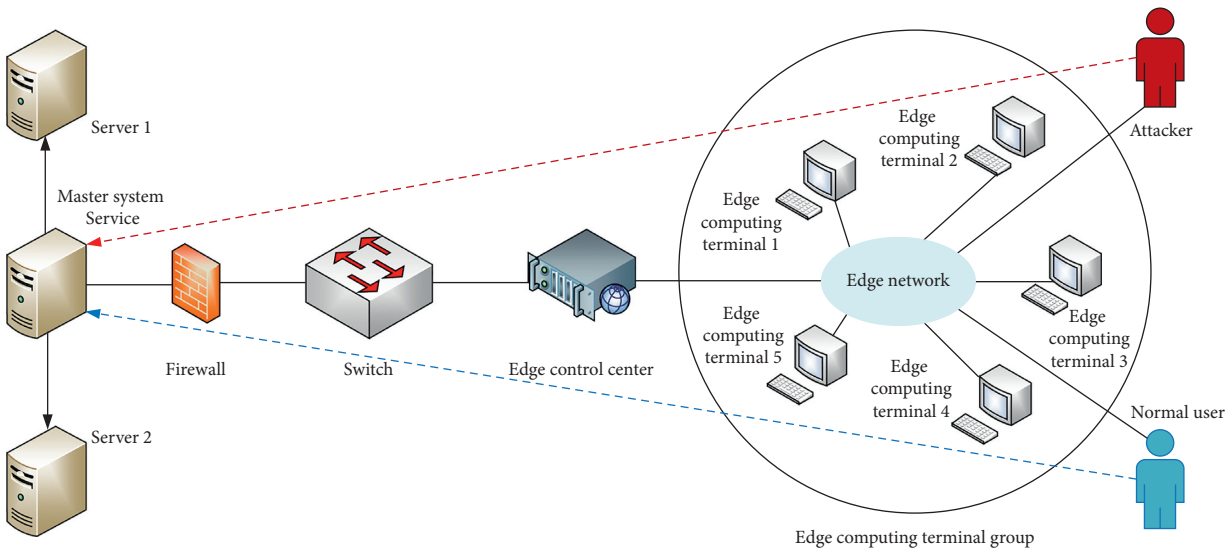

Figure 8: Edge computing network test platform with NS2.

and the EIDS model. It confirms that deploying multiredundancy edge computing terminal services in the network model has specific intrusion detection and defence effects.

When the probability of deploying intrusion detection service of the multiredundancy edge computing terminal has increased, the security in the network is further improved because the service has certain intrusion detection capability. Further comparison with Figure 10 illustrates that when the multiredundancy edge computing terminal service probability was raised to 0.5, the number of compromised edge computing terminals was controlled to be about 150.

In summary, it can be identified that, in the edge computing network, the upward curve trend of the number of compromised edge computing terminals in this model is relatively smooth, which means that the proposed multiredundancy edge computing terminal intrusion detection service in this model is efficient. On the other hand, it is not difficult to see that as the life cycle of edge computing terminals increases, more edge computing terminals are compromised. This also depicts that the computing power of the edge computing terminal is relatively weak. Therefore, it is a breakthrough of the model in this paper to make full use of the reliable resources of the edge computing terminal in the life cycle of the limited edge computing terminal and improve its computational efficiency while ensuring its security.

6.2.2. Analysis of the Results of Malicious Packet Capture Rate. This section is further considered from a security perspective. The malicious packet capture rate is intuitively reflected in the defensive performance when using different service-deployment strategies $\{\tau, \upsilon\} = \{(0.5, 0.3), (0.3, 0.5)\}$. In different intrusion detection service rates of single-redundancy edge computing terminal services and multiredundancy edge computing terminal services, for the malicious packet capture rate of the attack behaviour as depicted in Figures 6 and 7, the change line chart includes

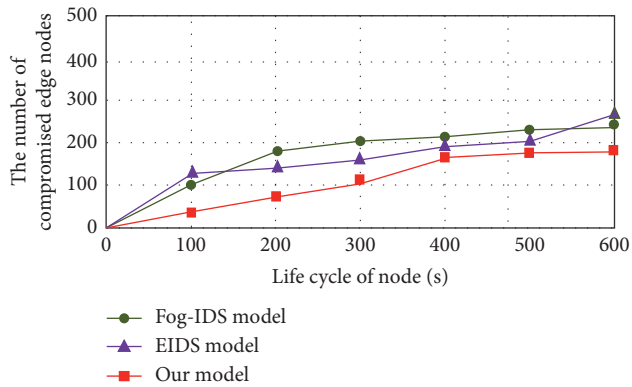

Figure 9: The number of compromised nodes under $(\tau, \upsilon) = (0.5, 0.3)$.

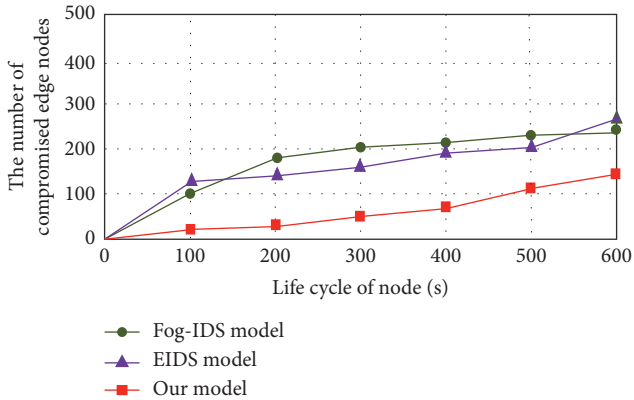

Figure 10: The number of compromised nodes under $(\tau, \upsilon) = (0.3, 0.5)$.

the Fog-IDS model, the EIDS model, and the GLIDE (our model).

As illustrated in Figure 11, the service distribution rate in the model is 0.2 for the master system service, 0.5 for the

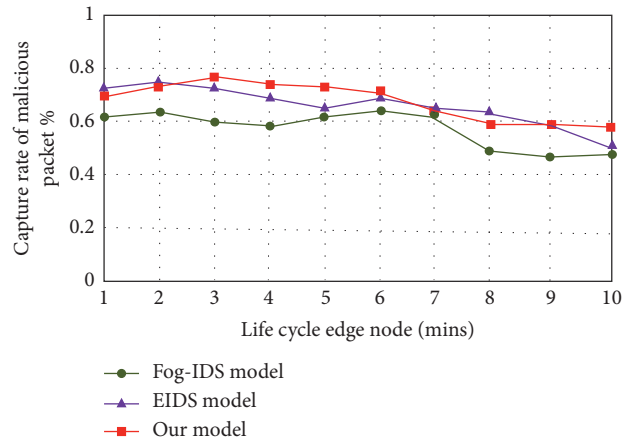

Figure 11: Malicious packet capture rate under $(\tau, \upsilon) = (0.5, 0.3)$.

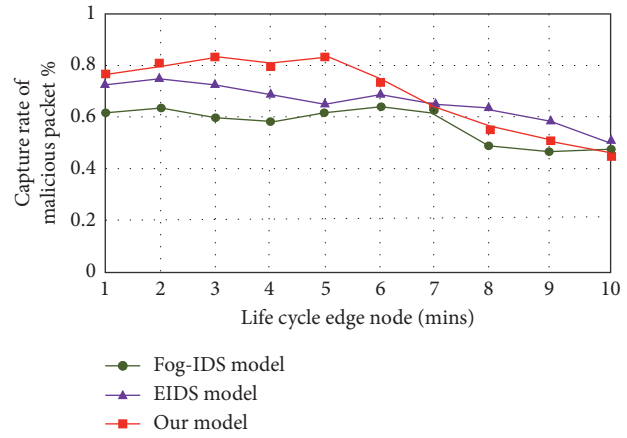

Figure 12: Malicious packet capture rate under $(\tau, \upsilon) = (0.3, 0.5)$.

single-redundancy edge computing terminal service, and 0.3 for the multiredundancy edge computing terminal service. As can be seen from Figure 6, the malicious packet capture rate of the Fog-IDS model and the EIDS model is not stable. Specifically, the capture rate of the Fog-IDS model is between 0.5 and 0.6, and the capture rate of the EIDS model is between 0.5 and 0.7. As compared with the other models, the overall malicious packet capture performance of our model is better than the existing Fog-IDS model and EIDS model, and its trend tends to be stable.

As depicted in Figure 12, the service distribution rate in the model is 0.2 for the master station system service, 0.3 for the single-redundancy edge computing terminal service, and 0.5 for the multiredundancy edge computing terminal service. When the edge node life cycle is relatively small, the malicious packet capture rate of the GLIDE model is kept at around 0.8, which is obviously better than the Fog-IDS model and the EIDS model. However, as the node life cycle becomes longer, the malicious packet capture rate of these three models shows a downward trend. We can speculate that the multiredundancy edge computing terminal service consumes a lot of computing power of the node, making its computing resources consume too much. Therefore, when the node life cycle is gradually increased, the malicious packet capture rate will drop significantly.

In summary, since the edge network is characterized by fully utilizing the computing power of each terminal to solve the computational problem of the core service, the multiredundancy edge computing terminal service cannot be deployed excessively. Although this can improve the security performance for a certain period of time, the computing resources of the edge computing terminal are excessively consumed. It is not worth the loss. Combined with the experimental results, the following conclusions can be drawn: through multiple NS2 simulation test platform experiments, the model can achieve optimal performance when the parameters satisfy $\{\tau, \upsilon\} = \{(0.5, 0.3)\}$. In an actual complex network environment, due to factors such as the constant changes of the attack and defence strategies, excessive deployment of multiple redundant edge computing terminal services does not improve detection performance. On the contrary, it may cause excessive consumption of computing resources. After repeated experiments, when the network resource consumption and detection rate performance reach a dynamic balance, there is always an optimal income solution in this paper that satisfies both the offense and defence.

7. Conclusions

In this paper, we introduced an edge computing network mimic linkage intrusion detection model called GLIDE based on the multiredundancy edge computing terminal intrusion detection service to conduct distributed linkage monitoring of attacks. We first employed the game theory into the GLIDE model by considering the problem of occupying the edge computing terminal resources by the terminal intrusion detection service based on the multiredundancy edge calculation. We then utilized the Nash equilibrium of attack and defence income in the game model and the Nash equilibrium condition under different dynamic deployment conditions to analyse the deployment strategy of the terminal intrusion detection service based on multiredundancy edge calculation. This procedure can be optimized to ensure the optimal balance of attack and defence revenue. Finally, we implemented the GLIDE model on 500 edge computing terminals that were set up for simulation experiments. The experimental results confirm that the GLIDE model can determine the optimal deployment strategy for intrusion detection service of multiredundancy edge computing terminal based on the probability of attackers. Also, it can realize the intrusion detection with an optimal defence cost.

This paper is based on the assumption of complete rationality to analyse. Next, we will use Darwin's theory of biological evolution and Lamarck's genetic theory as the ideological foundation. From the perspective of system theory, the adjustment process of group behaviour will be regarded as a dynamic system, in which each individual's invasion behaviour and the invasion relationship with the group are individually characterized. The formation mechanism from individual behaviours to group behaviours and the various factors involved can be incorporated into the

evolutionary game model to form a macro model with a microfoundation, which more truly reflects the diversity and complexity of behavioural subjects.

Data Availability

The binary text data used to support the findings of this study are available from the corresponding author or the experimenter upon request, including all experimental data.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the 2019 Industrial Internet Innovation and Development Project from Ministry of Industry and Information Technology of China, 2018 Jiangsu Province Major Technical Research Project "Information Security Simulation System," Fundamental Research Funds for the Central Universities (30918012204), Military Common Information System Equipment Pre-research Special Technology Project (315075701), the National Science Youth Foundation of China under Grant no. 61702264, and Shanghai Aerospace Science and Technology Innovation Fund (SAST2018-103).

References

[1] J. Hou, Q. Li, S. Cui et al., "Low-cohesion differential privacy protection for industrial internet," *The Journal of Supercomputing*, vol. 7, pp. 1–23, 2020.

[2] F. Wang, J. Xu, X. Wang, and S. Cui, "Joint offloading and computing optimization in wireless powered mobile-edge computing systems," *IEEE Transactions on Wireless Communications*, vol. 17, no. 3, pp. 1784–1797, 2018.

[3] Y. Tian, J. Guo, Y. Wu, and H. Lin, "Towards attack and defense views of rational delegation of computation," *IEEE Access*, vol. 7, no. 1, pp. 44037–44049, 2019.

[4] S. Wan, Y. Zhao, T. Wang, Z. Gu, Q. H. Abbasi, and K.-K. Raymond Choo, "Multi-dimensional data indexing and range query processing via Voronoi diagram for internet of things," *Future Generation Computer Systems*, vol. 91, pp. 382–391, 2019.

[5] H. Huang, H. Yin, G. Min, J. Zhang, Y. Wu, and X. Zhang, "Energy-aware dual-path geographic routing to bypass routing holes in wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 17, no. 6, pp. 1339–1352, 2018.

[6] J. Hou, Q. Li, R. Tan, S. Meng, H. Zhang, and S. Zhang, "An intrusion tracking watermarking scheme," *IEEE Access*, vol. 7, pp. 141438–141455, 2019.

[7] J. Ni, K. Zhang, X. Lin et al., "Securing fog computing for internet of things applications: challenges and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 601–628, 2018.

[8] G. Liu, H. Zhang, and Q. M. Li, "Network security optimal attack and defence decision-making method based on game model," *Journal of Nanjing University of Technology (Natural Science Edition)*, vol. 38, no. 1, pp. 12–21, 2014.

[9] T. E. Carroll and D. Grosu, "A game theoretic investigation of deception in network security," *Security and Communication Networks*, vol. 4, no. 10, pp. 1162–1172, 2011.

[10] V.-H. Pham and M. Dacier, "Honeypot trace forensics: the observation viewpoint matters," *Future Generation Computer Systems*, vol. 27, no. 5, pp. 539–546, 2011.

[11] Y. Fu, H. C. Li, X. P. Wu, and J. S. Wang, "Detecting APT attacks: a survey from the perspective of big data analysis," *Journal on Communications*, vol. 36, no. 11, pp. 1–14, 2015.

[12] X. Xu, C. He, Z. Xu, L. Qi, S. Wan, and M. Z. A. Bhuiyan, "Joint optimization of offloading utility and privacy for edge computing enabled IoT," *IEEE Internet of Things Journal*, vol. 6, no. 9, 2019.

[13] R. Pettersen, H. Johansen, and D. Johansen, "Secure edge computing with ARM TrustZone," in *Proceedings of the Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security*, pp. 102–109, Porto, Portugal, 2017.

[14] S. Tan, D. De, W.-Z. Song, J. Yang, and S. K. Das, "Survey of security advances in smart grid: a data driven approach," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 397–422, 2017.

[15] Y. Ma, Y. Wu, J. Ge, and J. Li, "An architecture for accountable Anonymous access in the internet-of-things network," *IEEE Access*, vol. 6, pp. 14451–14461, 2018.

[16] L. Qi, X. Zhang, W. Dou, C. Hu, C. Yang, and J. Chen, "A two-stage locality-sensitive hashing based approach for privacy-preserving mobile service recommendation in cross-platform edge environment," *Future Generation Computer Systems*, vol. 88, pp. 636–643, 2018.

[17] H. Liu, H. Kou, C. Yan, and L. Qi, "Link prediction in paper citation network to construct paper correlation graph," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, 2019.

[18] W. Gong, L. Qi, and Y. Xu, "Privacy-aware multidimensional mobile service quality prediction and recommendation in distributed Fog environment," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 3075849, 8 pages, 2018.

[19] Y. Xu, L. Qi, W. Dou, and J. Yu, "Privacy-preserving and scalable service recommendation based on SimHash in A distributed cloud environment," *Complexity*, vol. 2017, Article ID 3437854, 9 pages, 2017.

[20] X. Xu, S. Fu, L. Qi et al., "An IoT-Oriented data placement method with privacy preservation in cloud environment," *Journal of Network and Computer Applications*, vol. 124, pp. 148–157, 2018.

[21] X. Xu, Y. Li, T. Huang et al., "An energy-aware computation offloading method for smart edge computing in wireless metropolitan area networks," *Journal of Network and Computer Applications*, vol. 133, pp. 75–85, 2019.

[22] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Proceedings of the Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010*, Stockholm, Sweden, 2010.

[23] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, Fog et al.: a survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, no. 2, pp. 680–698, 2018.

[24] 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.

[25] H. W. Zhang, T. Li, and S. R. Huang, "Network defence decision-making method based on attack-defence differential

game," *Acta Electronica Sinica*, vol. 46, no. 6, pp. 1428–1435, 2018.

[26] J. D. Wang, D. K. Yu, and H. W. Zhang, "Active defence strategy selection based on the static Bayesian game," *Journal of Xidian University*, vol. 1, pp. 144–150, 2016.

[27] S. Shen, Y. Li, H. Xu et al., "Signaling game based strategy of intrusion detection in wireless sensor networks," *Computers & Mathematics with Applications*, vol. 62, no. 2, pp. 2404–2416, 2011.

[28] Q. Li, Y. Wang, Z. Pu, S. Wang, and W. Zhang, "Time series association state analysis method for attacks on the smart internet of electric vehicle charging network," *Transportation Research Record: Journal of the Transportation Research Board*, vol. 2673, no. 4, pp. 217–228, 2019.

[29] P. Yi, A. Iwayemi, and C. Zhou, "Developing ZigBee deployment guideline under WiFi interference for smart grid applications," *IEEE Transactions on Smart Grid*, vol. 2, no. 1, pp. 110–120, 2011.

[30] X. Xu, X. Zhang, H. Gao, X. Yuan, L. Qi, and W. Dou, "BeCome: blockchain-enabled computation offloading for IoT in mobile edge computing," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4187–4195, 2020.

[31] Q. Li, S. Meng, S. Zhang et al., "Safety risk monitoring of cyber-physical power systems based on ensemble learning algorithm," *IEEE Access*, vol. 7, pp. 24788–24805, 2019.

[32] X. Xu, Y. Chen, X. Zhang, Q. Liu, X. Liu, and L. Qi, "A blockchain-based computation offloading method for edge computing in 5G networks," *Software: Practice and Experience*, vol. 49, no. 9, 2019.

[33] L. Qi, Q. He, F. Chen et al., "Finding all you need: web APIs recommendation in web of things through keywords search," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 5, pp. 1063–1072, 2019.

[34] Q. Li, S. Meng, S. Wang, J. Zhang, and J. Hou, "CAD: command-level anomaly detection for vehicle-road collaborative charging network," *IEEE Access*, vol. 7, pp. 34910–34924, 2019.

[35] X. Xu, Q. Liu, Y. Luo et al., "A computation offloading method over big data for IoT-enabled cloud-edge computing," *Future Generation Computer Systems*, vol. 95, pp. 522–533, 2019.

[36] J. Hou, Q. Li, S. Meng, Z. Ni, Y. Chen, and Y. Liu, "DPRF: a differential privacy protection random forest," *IEEE Access*, vol. 7, pp. 130707–130720, 2019.

[37] Q. Li, S. Meng, S. Zhang, J. Hou, and L. Qi, "Complex attack linkage decision-making in edge computing networks," *IEEE Access*, vol. 7, pp. 12058–12072, 2019.

[38] Q. Tong, H. Zhang, and J. Tong, "The active defence technology based on the software/hardware diversity," *Journal of Cyber Security*, vol. 2, no. 1, pp. 1–12, 2017.

[39] X. Sang and Q. Li, "Mimic defense techniques of edge-computing terminal," in *Proceedings of the 2019 IEEE Fifth International Conference on Big Data Computing Service and Applications (BigDataService)*, pp. 247–251, Newark, CA, USA, 2019.

[40] Z. Liu, K.-K. R. Choo, and J. Grossschadl, "Securing edge devices in the post-quantum internet of things using lattice-based cryptography," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 158–162, 2018.