Frontiers in Educational Research
ISSN 2522-6398 Vol. 2, Issue 11: 142-154, DOI: 10.25236/FER.2019.021124

# The game analysis of the optimal configuration strategy of the intrusion detection system and intrusion detection system

**Rong Chen[1,2,*], Qiying Cao[1]**

*1 School of information science and technology, Donghua University, China*
*2 Shanghai Customs College, China*
**Corresponding Author Email:ch30n@126.com*

***ABSTRACT.*** *With the increasingly rampant intrusion, it is found that it is not enough to construct the security system from the Angle of defense. On how the computer and network resources malicious use behavior recognition and response, proposes the web application level intrusion detection defense system and intrusion detection system, the optimal allocation strategy game analysis. By comparison with literature analysis method, this paper expounded the basic structure of the intrusion detection system, using the game theory to establish virtual private networks (VPNS) and intrusion detection system model of information security technology combination, design companies and hackers mixed strategy Nash equilibrium in the game model analysis, and applied to the example analysis. The study finds that the manual survey strategy configured with two technologies was the same as when IDS is configured separately. Under certain conditions, it is better to configure two technical combinations to prevent hackers from intruding.*

***KEYWORDS:*** *Intrusion detection system; Private network; Optimal allocation strategy; Game analysis*

## 1. Introduction

Intrusion Detection can be traced back to 1986, when a paper published by SRI Dorothy E.Denning, “ane-detection Model” was published. This paper probes into the intrusion detection technology and retrieves the basic mechanism of behavior analysis. For the first time the concept of intrusion detection, as a kind of computer security defense measures are put forward, and set up an independent system, program application environment and the fragility of the general intrusion detection system model [1]. Prior to the 1990s, SRI and Los Alamos LABS mainly focused on mainframe IDS and developed the IDES, Haystack and other intrusion detection systems respectively. In 1990, the network security monitor designed by UCD marked the entry of intrusion detection system into the network domain [2]. There

ISSN 2522-6398 Vol. 2, Issue 11: 142-154, DOI: 10.25236/FER.2019.021124

are two main research methods of network IDS: one is to analyze the audit data of each host, and analyze the relationship between the audit data of each host. Second, analyze network packets. Due to the development of Internet in the 1990s and the increase of communication and network bandwidth, the interconnectivity of the system has improved significantly. So people started trying to integrate the mainframe and network IDS [3]. Distributed intrusion detection system (DIDS) attempts to integrate the method based on host and network monitoring methods together, the development of intrusion detection system mainly experienced three stages: the host IDS research, the study of the network IDS, finally will host and network IDS integration. For a successful intrusion detection system, it not only enables the system administrator to understand any changes in the network system at all times, but also provides guidance for the development of security policies [4]. Intrusion detection is a reasonable complement to the firewall, which can help the system to deal with cyber attacks and improve the integrity of the information security infrastructure.

## 2. State of the art

The security of network information system is a very complex problem, involving many aspects such as technology, management and use. Traditional network security tools are firewalls. It is a special network connecting device used to strengthen access control between networks. By checking the data packets and links transmitted between two or more networks according to a certain security policy, it determines whether the communication between networks is allowed [5]. In this demand background, intrusion detection technology and even intrusion prevention have emerged, which can make up for the lack of firewall and provide real-time monitoring for the network. Combined with other network security products, the real-time response to the intrusion behavior before the network system is threatened [6]. This paper presents a comprehensive description of various network intrusion detection and defense techniques. This paper points out their respective advantages and disadvantages, and discusses and studies the future development trend of network intrusion detection defense technology. At present, researches on information security economics at home and abroad mainly focus on the information security investment strategy, and the research literature on information security technology portfolio allocation strategy is relatively few [7]. With the development and popularization of computer network technology, global informationization has become a major trend of human development. Due to network connection form of diversity, uneven distribution of terminal and network features such as openness, interconnectedness, the network highly vulnerable to hackers, malicious software and other misconduct, the security problem of computer network is becoming more and more prominent. Network security has become a core issue involving various fields of social life [8].

ISSN 2522-6398 Vol. 2, Issue 11: 142-154, DOI: 10.25236/FER.2019.021124

## 3. Methodology

### *3.1 The basic structure of intrusion detection system.*

The basic structure of the intrusion detection system is shown in the figure. Mainly consists of the following four parts:

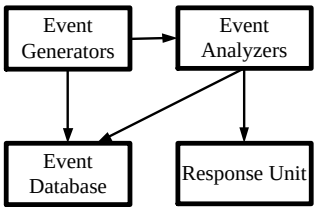


*Figure.1 Basic structure*

Event generator: the event generator is essentially a link in the intrusion detection system for initial data collection. Adopt scientific and reasonable technology to track data flow and log files effectively. The resulting initial data is then effectively converted to a specific event, which is provided to the rest of the system. Event analyzer: the primary role is to implement the receiving of event information and then analyze the relevant data information effectively. Make a comprehensive analysis of the information received and infer whether it is an intrusion or an anomaly. Finally, the judgment structure needs to be converted into corresponding warning information. Event database: store each type of intermediate and final data. Data is often stored and managed effectively for a long time. Response unit: the response unit responds to a warning message. It can make a strong reaction to cut off the connection, change the file property, etc., and can also indicate the simple alarm [9].

According to the technology of intrusion detection, it can be divided into abnormal detection system and misuse detection system. Anomaly intrusion detection systems: anomaly detection is based on the user's behavior or the condition of resource use to judge whether the intrusion events, and does not depend on whether to detect specific behavior, therefore is based on the behavior of the test. The main idea is to establish a feature file based on the normal activities of the system, and identify the intruders by counting all the system states that are different from the established feature files of the user [10]. Misuse of intrusion detection system: the premise of using this system is to assume that all network attack behavior and operation mode methods have certain patterns or functional characteristics. On this basis, the database creation is realized, and the obtained information is compared with the existing network intrusion and system misuse mode database. Compare the relevant behaviors of the security policy and timely find and deal with them effectively.

ISSN 2522-6398 Vol. 2, Issue 11: 142-154, DOI: 10.25236/FER.2019.021124

### *3.2 Build the basic game model.*

Consider two types of users: legal and illegal. The reasonable definition of legitimate users is actually to access the company system to provide positive benefits for the company; Illegal users refer to access to the company's systems that do not provide positive revenue for the company in any case. In the professional category this behavior is called “intruder” or “hacker”. Assuming the total number of users is n, the proportion of legitimate users is:

$$\xi, \quad \xi \in [0,1] \tag{1}$$

The number of legitimate users is $n\xi$ and the number of hackers is $n(1-\xi)$. The goal of IDS is to detect the hacker's intrusion, and the user's probability of invasion is $\psi$. If a hacker has not been detected, the gain is $\mu$; if an intrusion is detected, the penalty is $\beta$. Set $\mu \le \beta$, that is, the hacker has no positive return after being tested. The benefit of every legal user access system is $w$; when the hacking system was not detected, the company suffered a loss of d. The cost of carrying out the manual investigation is $c_1$. If the company detects an invasion, the proportion of d is prevented or fixed.

$$\varphi \le 1 \tag{2}$$

Set $c_1 \le \varphi d$, that is, the company's investigation cost is not higher than the revenue it has repaired. Assuming that $P_D$ is the probability of IDS issuing an alarm when the user intrudes, that is, the detection rate of IDS; $P_F$ is the probability of IDS issuing an alert when the user is not intruding, that is, the false alarm rate of IDS.

VPNS have two effects on network security: expanding access to legitimate users without the need to add other devices. Let's say that this factor is $f_1$, and $f_1$ is a function of $\xi$. define

$$f_1(\xi) = \sqrt{\xi} \tag{3}$$

VPN can reduce the false alarm rate of IDS. To make this action factor $f_2$, define $f_2 \in [0,1]$ as VPN to reduce the degree of the false alarm rate of IDS, and then the IDS false alarm rate of the configured VPN will be.

$$P_F^{'} = f_2 P_F \tag{4}$$

VPNS can be disconnected due to low traffic problems. The probability of setting up the VPN to work is the same as the value of theρ0. The cost of recovering the fault is $c_2$ Q. When a VPN fails, all users of the company cannot access the system until the fault is repaired.

ISSN 2522-6398 Vol. 2, Issue 11: 142-154, DOI: 10.25236/FER.2019.021124

When the company configures the VPN and IDS, the user policy for access rights is.

$$S^U \in \{H, NH\} \tag{5}$$

Where H is an intrusion system and NH is a non-invasive system. The company's strategy is.

$$S^F \in \{(I,I),(I,NI),(NI,I),(NI,NI)\} \tag{6}$$

Where I is conducting a manual investigation and NI is not conducting a manual investigation. Two kinds of state of IDS for "alarm" and "alarm", the SF, set the first element of each pair of say the actions of IDS when the alarm company, said the second element IDS do not alarm when the company's actions. For example, (I, NI) indicates that if the company has received an IDS alert, it will use a manual investigation. If it does not receive the IDS, it will not investigate. $\rho_1$ is the probability that the company will use the manual investigation when the IDS alarm. $\rho_2$ is the probability that the company adopts the manual investigation when the IDS does not alarm.

### *3.3 Model analysis*

In today's information age, the computer network technology is gradually enhanced, and the security incident and intrusion detection technology are becoming more and more mature in this form. Mobile communication can show the effect of movement in practical application, so that the air wireless interface between mobile and base station is an open form of the task of completing each stage. The communication, the creation of link, transmission information and other links in the whole communication are presented in front of the third party; Mobile user and network have fixed physical connection characteristics in whole mobile communication system. This optimization feature enables mobile users to use wireless channels to effectively transfer the relevant identity information to the system. This identity information is likely to be intercepted and tampered with by the illegal, causing serious harm to the application and functional realization of the system model; and wireless networks are vulnerable to hackers and viruses. Therefore, IDS has a wide application prospect in wireless network. Home network security. Due to the development of online banking, online payment system, B2C and C2C websites, the network security of family users has become more prominent. There will be a market for demand, and IDS will gradually enter the family in the near future. The following is an analysis of the simultaneous configuration of VPN and IDS technologies.

The expected return of the company and the hacker. The probability of IDS issuing alarm is:

$$p_1^{'} = P_D\psi + f_2 P_F(1-\psi) \tag{7}$$

ISSN 2522-6398 Vol. 2, Issue 11: 142-154, DOI: 10.25236/FER.2019.021124

The probability that IDS does not alarm is:

$$p_2^{'} = 1 - P_D\psi - f_2 P_F\left(1-\psi\right) \tag{8}$$

The probability of the user's IDS issuing an alarm is.

$$p_3^{'} = \frac{P_D\psi}{P_D\psi + f_2 P_F\left(1-\psi\right)} \tag{9}$$

The probability that the user IDS does not issue an alarm is.

$$p_3^{'} = \frac{\left(1-P_D\right)\psi}{1-P_D\psi - f_2 P_F\left(1-\psi\right)} \tag{10}$$

The probability that the user does not have an IDS to send an alarm is.

$$p_5^{'} = \frac{f_2 P_F\left(1-\psi\right)}{P_D\psi + f_2 P_F\left(1-\psi\right)} \tag{11}$$

The probability that the user does not have an alarm is not issued by IDS.

$$p_6^{'} = \frac{\left(1-f_2 P_F\right)\left(1-\psi\right)}{1-P_D\psi - f_2 P_F\left(1-\psi\right)} \tag{12}$$

The expected revenue of the company in IDS alarm and unalarm state is $F_A^{'}$ and $F_{NA}^{'}$

$$F_A^{'}\left(\rho_0,\rho_1,\psi\right) = nwf_1 p_5^{'} - \rho_1 c_1 - c_2 + \rho_0 c_2 - \rho_0 p_3^{'}\left(1-\rho_1\varphi\right)d \tag{13}$$

$$F_{NA}^{'}\left(\rho_0,\rho_2,\psi\right) = nwf_1 p_6^{'} - \rho_2 c_1 - c_2 + \rho_0 c_2 - \rho_0 p_4^{'}\left(1-\rho_2\varphi\right)d \tag{14}$$

The company's total expected return is.

$$F^{'}\left(\rho_0,\rho_1,\rho_2,\psi\right) = p_1^{'}F_A^{'}\left(\rho_0,\rho_1,\psi\right) + p_2^{'}F_{NA}^{'}\left(\rho_0,\rho_2,\psi\right) \tag{15}$$

First, the company and the hacker game Nash equilibrium mixed strategy.

Theorem 1: when configuring VPN and IDS technology at the same time, the Nash equilibrium hybrid strategy of the company and hacker game is:

When $\frac{\mu}{\beta} \le P_D$:

ISSN 2522-6398 Vol. 2, Issue 11: 142-154, DOI: 10.25236/FER.2019.021124

$$\begin{cases} \rho_1^* = \dfrac{\mu}{P_D\beta}, \rho_2^* = 0 \\ \rho_0^* = \dfrac{\left[c_2\left(P_D - f_2P_F\right) + \left(1-P_D\right)f_2P_F d\right]c_1}{d\varphi P_D c_2\left(1-f_2P_F\right)} \\ \psi^* = \dfrac{c_2\left(1-f_2P_F\right)}{d\left(1-P_D\right)+c_2\left(1-f_2P_F\right)} \end{cases} \tag{16}$$

When $\dfrac{\mu}{\beta} > P_D$:

$$\begin{cases} \rho_1^* = 1, \rho_2^* = \dfrac{\mu - P_D\beta}{\left(1-P_D\right)\beta} \\ \rho_0^* = \dfrac{\left[-c_2\left(P_D - f_2P_F\right) + \left(1-\varphi\right)\left(1-f_2P_F\right)P_D d\right]c_1}{d\varphi P_F c_2 f_2\left(1-P_D\right)} \\ \psi^* = \dfrac{c_2 f_2 P_F}{d\left(1-\varphi\right)P_D + c_2\left(f_2P_F - P_D\right)} \end{cases} \tag{17}$$

Conclusion: the company also configures VPNS and IDS with the same manual survey strategy that configures IDS separately. The hacker's optimal intrusion strategy has changed: when IDS has a higher detection rate, which is $d < c_2$ or $c_1 < \dfrac{\varphi d}{2}$. Configuring IDS separately is more likely to prevent hackers from hacking than configuring two combinations of technologies at the same time. The detection probability of IDS is low, which is $d\left(1-\varphi\right) < c_2$ or $c_1 < \dfrac{c_2\varphi d}{2c_2 - d\left(1-\varphi\right)}$. Configuring IDS separately is a better way to prevent hackers from hacking than configuring two combinations of technologies at the same time.

Configuring two information security technology combinations and configuring IDS only has the same manual investigation optimal strategy. The optimal intrusion strategy of hackers is divided into two situations:

When $\dfrac{\mu}{\beta} \le P_D$:

$$\psi^*|_{VPN\&IDS} = \frac{c_2\left(1-f_2P_F\right)}{d\left(1-P_D\right)+c_2\left(1-f_2P_F\right)} > \psi^*|_{IDS} = \frac{c_1P_F}{d\varphi P_D - c_1\left(P_D - P_F\right)} \tag{18}$$

When $\dfrac{\mu}{\beta} > P_D$:if $\psi^*|_{VPN\&IDS} > \psi^*|_{IDS}$,

ISSN 2522-6398 Vol. 2, Issue 11: 142-154, DOI: 10.25236/FER.2019.021124

$$d(1-\varphi) < c_2, c_1 < \frac{c_2 \varphi d}{2c_2 - d(1-\varphi)} \tag{19}$$

Conclusion: the system has a high safety performance when it is not equipped with more information security technology. If IDS has good detection, VPN repair failures will cost a lot of money. In the case of low cost of enterprise investigation, the configuration and implementation effect of IDS strategy alone is much higher than that of VPN and IDS technology policy configuration. On the other hand, if the VPN to repair failure in the process of low cost of capital, or the link will take more investigation on the artificial cost, at the same time was taken to the VPN and IDS technology strategy configuration can be effective to prevent hacker intrusion behavior, for the safety performance of the system maintenance. Adopt the same concept to analyze the comprehensive interpretation of the low IDS detection rate.

In the process of the company's simultaneous VPN and IDS technology policy configuration, if the IDS detection rate is relatively high, VPN will need to fully meet the following conditions to reduce the false alarm rate of IDS:

$$f_2 = \frac{c_1 c_2 P_D - d\varphi P_D c_2 \rho_0^*}{P_F c_1 \left[c_2 - (1-P_D) d\right] - P_F d\varphi P_D c_2 \rho_0^*} \tag{20}$$

At this point, the probability that the VPN works normally $\rho_0^*$ is larger, and the smaller the $f_2$ is, the smaller the $P_F^{'} = f_2 P_F$ is. If the detection rate of IDS is low, VPN will reduce the degree of false alarm rate of IDS:

$$f_2 = \frac{\left[c_2 - (1-P_D)\varphi\right] c_1 P_D}{c_1 c_2 P_F - P_F c_2 \rho_0^* (1-P_D) - (1-\varphi) P_D P_F d c_1} \tag{21}$$

At this point, the probability that the VPN works normally $\rho_0^*$ is larger, and the larger the $f_2$ is, the larger the $P_F^{'} = f_2 P_F$ is. Conclusion: the technology interaction between VPN and IDS is explained. The results show that the better the working status of VPN, the greater the decrease of the false alarm rate of IDS. This seems to contradict the “conventional” idea. In fact, the configuration of VPN affects the false alarm rate of IDS, and is also affected by the testing performance of IDS. If the IDS detection rate is high, it can provide accurate and efficient feedback to the intruder information of the VPN. The VPN can use technology to upgrade and maintenance way of making further enhance the work efficiency, and the ability to scientific analyze the users access to the accuracy of identification, the IDS misstatement cases been optimized. However, if the detection probability of IDS is low, it is not detailed and accurate to collect the information of the hacker. Even if the VPN has a high normal working probability, it will not identify the effective user access system more accurately. This requires the company to configure VPN and IDS in the real world, not to increase the access rate of VPN, increase investment in VPN, and ignore the configuration of the detection rate of IDS itself. In order to achieve a satisfactory standard for the role of VPN in IDS, various factors need to be taken

ISSN 2522-6398 Vol. 2, Issue 11: 142-154, DOI: 10.25236/FER.2019.021124

into consideration.

## 4. Result analysis and discussion

### *4.1 Experimental results and analysis.*

In order to further compare the Nash equilibrium hybrid strategy of the company and the hacker, and the impact of VPN on reducing the false alarm rate of IDS, etc. We use the mathematical tool MATLAB for numerical simulation analysis. The parameters are assigned as follows.

Numerical simulation 1: parameter setting is shown in table 1. $\psi^*$ is the y-coordinate, $P_D$ is the x-coordinate. When IDS is configured, the relationship between IDS detection probability and hacker invasion probability is shown in figure 2.

*Table 1 Parameter setting value*

| $n$ | $\xi$ | $c_1$ | $d$ | $\mu$ | $\beta$ | $P_F$ | $\varphi$ |
|---|---|---|---|---|---|---|---|
| 100 | 0.01 | 100 | 300 | 100 | 200 | 0.2 | 0.5 |

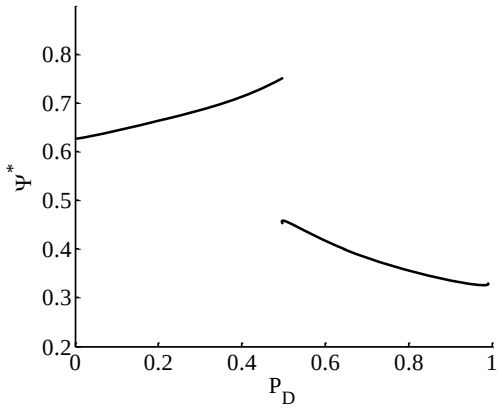


*Figure.2 The relationship between IDS detection rate and hacker's intrusion probability when configuring IDS only*

FIG. 2 shows that under known parameters, when 0. $5 \leq P_D$, high enough IDS detection rates can reduce the rate of hacker intrusion; when $P_D < 0.5$, low IDS detection rates can lead to high rate of intrusion.

Numerical simulation 2: parameter setting is shown in table 2. $\psi^*$ is the

ISSN 2522-6398 Vol. 2, Issue 11: 142-154, DOI: 10.25236/FER.2019.021124

y-coordinate, $P_D$ is the x-coordinate. When IDS detection rates are high, analyze the situation where VPN and IDS are configured at the same time. If $c_1 < \frac{\varphi d}{2}$, specially, and $c_1 = 20$, the relationship between IDS detection probability and hacker invasion probability is shown in figure 3.

*Table 2 Parameter setting value*

| $n$ | $\xi$ | $c_1$ | $d$ | $\mu$ | $\beta$ | $P_F$ | $\varphi$ | $f_2$ | $c_2$ |
|---|---|---|---|---|---|---|---|---|---|
| 100 | 0.01 | 100 | 300 | 100 | 200 | 0.2 | 0.5 | 0.6 | 80 |

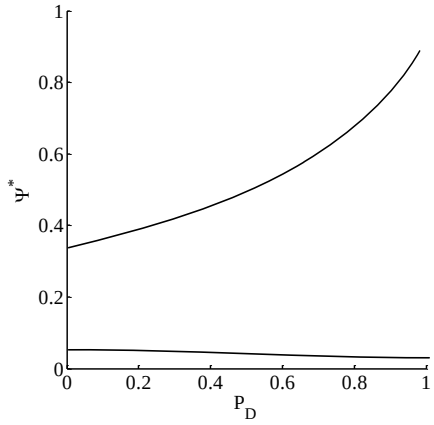


*Figure.3 when configuring VPN, IDS and $c_1 < \frac{\varphi d}{2}$, the IDS detection rate the relationship of hacker intrusion probability*

Figure 3 shows that when IDS is configured separately, the penetration rate of the hacker is lower than the configuration of the two technologies. That is, the more information security technology is not configured, the higher the security of the system. If $c_1 > \frac{\varphi d}{2}$, specially, and $c_1 = 140$ are satisfied, the relationship between IDS detection probability and hacker invasion probability is shown in figure 4.

ISSN 2522-6398 Vol. 2, Issue 11: 142-154, DOI: 10.25236/FER.2019.021124

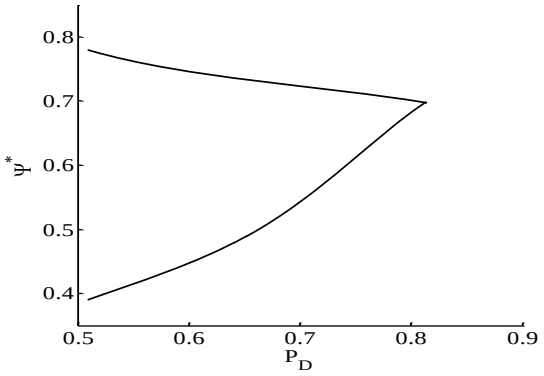


*Figure.4 when configuring VPN, IDS and* $c_1 > \frac{\varphi d}{2}$*, the IDS detection rate the relationship of hacker intrusion probability*

Figure 4 shows that when the cost of manual investigation is high, configuring VPNS and IDS can prevent hackers from intruding and ensure system security.

Numerical simulation 3: parameter setting is shown in table 3. $\rho_0^* = [0,1]$, $f_2$ is the y-coordinate and $\rho_0^*$ is the x-coordinate. When the IDS detection rate is low, and the VPN and IDS are configured at the same time, the interaction relationship between VPN and IDS technology parameters is shown in figure 5.

*Table 3 Parameter setting value*

| $n$ | $\xi$ | $c_1$ | $d$ | $\mu$ | $\beta$ | $P_D$ | $P_F$ | $\varphi$ | $f_2$ | $c_2$ |
|---|---|---|---|---|---|---|---|---|---|---|
| 100 | 0.01 | 20 | 300 | 100 | 200 | 0.4 | 0.2 | 0.5 | 0.6 | 160 |

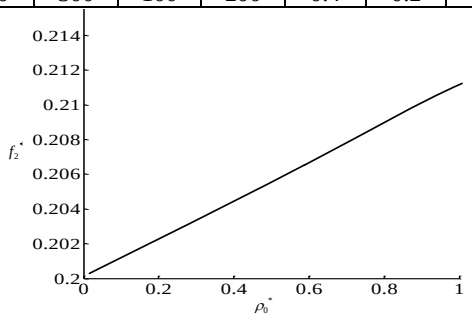


*Figure.5 The interaction between VPN and IDS technical parameters when configuring VPN and IDS*

ISSN 2522-6398 Vol. 2, Issue 11: 142-154, DOI: 10.25236/FER.2019.021124

Figure 5 shows that the greater the probability $\rho_0^*$ of the normal working of the VPN, the greater the $f_2$. That is, the better the working status of the VPN is, the greater the decrease of the false alarm rate of IDS. The numerical simulation $P_D$ is larger, and the user scale is different, and the optimal configuration strategy of the company. The parameter setting is shown in table 4. The expected return of the company is the vertical coordinate, and the number of users (scale) is the horizontal coordinate. For example, when IDS detection rate is high, the optimal allocation strategy of the company is analyzed based on the company's expected revenue maximization.

*Table 4 Parameter setting value*

| $n$ | $\xi$ | $w$ | $c_1$ | $d$ | $\mu$ | $\beta$ | $P_D$ | $P_F$ | $\varphi$ | $f_2$ | $c_2$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 100~10000 | 0.01 | 200 | 100 | 300 | 100 | 200 | 0.7 | 0.2 | 0.5 | 0.1 | 80 |

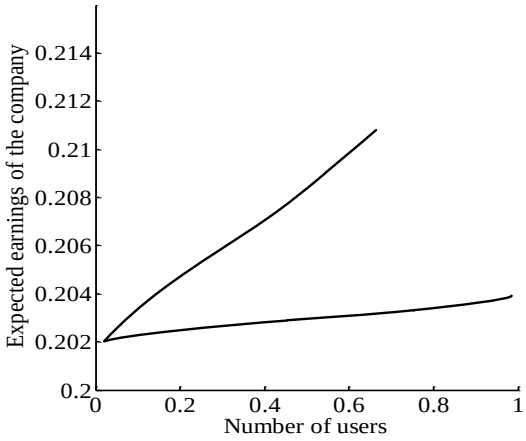


*Figure.6 The relationship between the size of the user and the expected earnings of the company*

Figure 6 shows that when IDS has a high detection rate, the more users there are, the greater the expected revenue from the combination of two technologies.

## 5. Conclusion

Due to the threat of new viruses and Trojan horses flooding the network environment, different security technology combinations are needed to reduce network security risks. To prevent hacking and decrease the cost of information security technology configuration strategy, put forward the web application level

ISSN 2522-6398 Vol. 2, Issue 11: 142-154, DOI: 10.25236/FER.2019.021124

intrusion detection defense system and intrusion detection system, the optimal allocation strategy game analysis. Comprehensive utilization of the theoretical knowledge of information security economics, the configuration of VPN and IDS science is constructed with two kinds of information security technology combination game model. Then the optimization configuration strategy of VPN and IDS is adopted. In the practical application, it is concluded that the combination of two technologies can reduce the probability of hacking system under certain technical conditions. The better the performance of VPN, the greater the contribution to reduce the false alarm rate of IDS. IDS has a high probability of detection and a large number of users, and the combination of two technologies will bring more expected benefits to the company. The optimal configuration strategy is proved to be effective, and the calculation is moderate, which provides a basis for timely detection and processing of intrusion events.

**Reference**

[1] Horng S J, Su M Y, Chen Y H, et al (2011). A novel intrusion detection system based on hierarchical clustering and support vector machines. Expert Systems with Applications, vol.38, no.1, pp.306-313.
[2] Zhang Y, Wang L, Sun W, et al (2011). Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids. IEEE Transactions on Smart Grid, vol.2, no.4, pp.796-808.
[3] Lo C C, Huang C C, Ku J (2010). A Cooperative Intrusion Detection System Framework for Cloud Computing Networks. IEEE, pp.280-284.
[4] Koc L, Mazzuchi T A, Sarkani S (2012). A network intrusion detection system based on a Hidden Naïve Bayes multiclass classifier. Expert Systems with Applications, vol.39, no.18, pp.13492-13500.
[5] Lauf A P, Peters R A, Robinson W H (2010). A distributed intrusion detection system for resource-constrained devices in ad-hoc networks. Ad Hoc Networks, vol.8, no.3, pp.253-266.
[6] Lin W C, Ke S W, Tsai C F (2015). CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. Knowledge-Based Systems, vol.78, no.1, pp.13-21.
[7] Yu Z, Zinger D, Bose A (2011). An innovative optimal power allocation strategy for fuel cell, battery and supercapacitor hybrid electric vehicle. Journal of Power Sources, vol.196, no.4, pp.351-2359.
[8] He L, Liang Z (2013). Optimal dynamic asset allocation strategy for ELA scheme of DC pension plan during the distribution phase. Insurance Mathematics & Economics, vol.52, no.2, pp.04-410.
[9] Kaibo Liu, Jianjun Shi (2013). Objective-oriented optimal sensor allocation strategy for process monitoring and diagnosis by multivariate analysis in a Bayesian network. Iie Transactions, vol.45, no.6, pp.630-643.
[10] Soury H, Bader F, Shaat M, et al (2012). Near Optimal Power Allocation Algorithm for OFDM-Based Cognitive Using Adaptive Relaying Strategy. IEEE, pp.212-217.