Journal of Computers Vol. 34 No. 2, April 2023, pp. 141-160
doi: 10.53106/199115992023043402011

Optimal Defense Strategy for Data Security Based on Improving Evolutionary Game Model between Heterogeneous Groups

Mingxin Yang, Lei Feng*

School of Economics and Management, Hebei University of Science and Technology,
Shijiazhuang, China
yangmingxin72@163.com, 2544398753@qq.com

Received 17 May 2022; Revised 28 September 2022; Accepted 28 October 2022

Abstract. As the information technology develops, network attacks have become complex and diverse. To improve the effectiveness and accuracy of data security defense strategies, an optimal defense method based on improving evolutionary game model between heterogeneous groups is proposed. Specifically, based on traditional evolutionary game theory, the player type space is added to divide the heterogeneous groups, and the group type and game strategy are extended to N to solve the problems in heterogeneous groups. Considering the game is interfered by the environment, a set of dynamic environment functions is added to increase the adaptability of the model when dealing with changing complex networks. Taking into account the influence of information communication within the group, the information flow degree is added to increase the accuracy of evolution rate and solve the problem that traditional model cannot reveal the difference in the evolution rate of players. Based on the new model, taking the game between two types of invaders and one type of defender as an example, the calculation method of evolution direction at any time and the judgment method for the stability of equilibrium point are discussed. Finally, the effectiveness of the improved model is verified through the comparison of simulation experiments, and a new scheme is provided for current network data protection.

Keywords: optimal defense strategy, improved replication dynamic equation, heterogeneous group evolutionary game, dynamic environment, information circulation degree

1 Introduction

With the rapid development of 5G, big data, cloud computing and other new-generation technologies, the network scale and data volume are gradually expanding. Under the special background of travel barriers caused by the global epidemic, human society has entered a new era of network life [1]. However, with the wide application of the internet, the security risks of personal information have gradually been exposed, where system intrusions are rampant; users' personal information is sold on the dark web, and data leakage incidents are frequently exposed. Enterprises fall into public opinion and become the target of public criticism due to the spread of negative information. Moreover it also increases the burden on the government. Information leakage caused by network security threatens personal property, social order and national security, which has become a public problem that perplexs government around the world. As such, the Chinese government clearly proposed in the 14th Five-year Plan to strengthen the protection of personal data [2]. In the context of frequent data leakage, how to ensure the optimal defense strategy to achieve data security is an urgent problem that needs to be solved.

Since the characteristics of target opposition, strategy dependence and non-cooperative relationship in network attack-defense are consistent with the principles of game theory [3-4], using an attack-defense game to solve the problem of network security has become a hotspot. Scholars have made in-depth studies on this issue and experienced a development process from static and complete information to dynamic and incomplete information. Classical network security game models can be divided into four categories according to the dual dimensions of information and time sequence. 1) Research on static game based on complete information [5-8]. Wei Jiang, Binxing Fang et al. (2009) proposed a network defense graph model, a network attack-defense game model and an optimal active defense selection algorithm to realize the defense of network information system [5]. To accurately evaluate the security risks of military network, Zengguang Wang et al. (2019) proposed a risk assessment method based on an attack-defense game, aiming to provide an idea for solving network risk assessment [7]; 2) Research on dynamic game based on complete information [9-11]. Afrand et al. (2007) proposed a game model to calculate the optimal defense strategy for malicious data forwarding behavior of nodes [9]; 3) Research on

* Corresponding Author

static game based on incomplete information [12-15]. To solve the problems of information asymmetry and profit uncertainty between attack-defense sides, Yongqiang Chen et al. (2015) introduced trigonal fuzzy mathematics to quantify the utility functions of both players, and proposed a method of network optimal defense strategy selection based on fuzzy Bayes game model [13]. Dingkun Yu et al. (2015) divided the attack-defense sides into different types. A static Bayes based attack-defense game model was established to analyze the equilibrium and solve the problem that the behaviors of attack-defense are unknown to each other in reality [14]; 4) Research on the dynamic Game based on incomplete information [16-23]. In view of the reality that the actions of invaders rely on network detection, Yongjin Hu et al. (2020) constructed a multi-stage network game model and designed an optimal network defense strategy selection algorithm combining non-cooperative game theory [16]. Yang Yu et al. (2019) proposed a network attack-defense game model based on multi-level asymmetric information of the Internet of Things system to determine an optimal defense strategy [18]. Previous studies on attack-defense are usually based on one-way signal transmission. Xiaohu Liu (2019) proposed an active defense strategy selection method based on game theory from the perspective of two-way signal [20].

Traditional game theory assumes that the premises are perfectly rational (Decisions are completely correct and not influenced by other players). However, this assumption is difficult to satisfy in actual games. In recent years, evolution game has been widely used for considering bounded rationality. Based on the game theory, the concept of biological evolution was introduced, and the evolutionary game theory under the group learning mechanism was formed after the improvement of Smith and Price [24]. The theoretical research on the evolutionary game of network security mainly focuses on the improvement of replication dynamic equation and the game of heterogeneous groups. Considering the influence of strategies, Jianming Huang et al. (2018) improved the replication dynamic equation by introducing the incentive coefficient, and constructed a new network attack-defense evolutionary game model to provide a theoretical basis for solving the real network security problems. However, the effect of information communication between groups and the heterogeneity of groups are not considered [25]. Hao Hu et al. (2018) established a Bayesian attack-defense evolutionary game model to solve the problem of incomplete information. The income uncertainty of attack-defense was transformed into the uncertainty of attack-defense type, and the selection intensity factor was added to improve the replication dynamic equation and verify the feasibility of the model [26]. Regarding the strategy selection of cloud service suppliers in the complex network problems, PanJun Sun (2020) proposed an optimal protection strategy selection algorithm. The dynamic replication equation was improved by using the incentive coefficient and an improved evolutionary game model was constructed. In addition, stability analysis was conducted to prove the validity of the model through experiments [27]. Enning Zhang et al. (2021) proposed a network security defense decision-making method of double heterogeneous groups to solve the problem of heterogeneous groups, and the reflection mechanism of players was transformed into a Poisson process to improve the replication dynamic equation. Although this model overcomes the problem of heterogeneity, it does not pay attention to the interference of in-game environment [28].

When studying the attack-defense evolutionary game theory, the following three points need to be improved: 1) although the replication dynamic equation has been improved (considering the influence between strategies), the influence of transmission rate has not been considered due to information exchange in the group. Differences in the evolution rate at which game players evolve are not reflected. When defenders establish an information exchange mechanism, the evolution rate of strategy is obviously different (the practical basis of the information exchange mechanism is as follows: enterprises achieve the progress of information security communication through regular forums, meetings and more); (2) Most studies cannot be applied to the game of heterogeneous groups. (Heterogeneous group is a biological concept that different populations of the same species have different characteristics due to different living environments. In the research, the objects need to be divided into heterogeneous populations. Similarly, heterogeneous populations of evolutionary games are participants in the same group with different decision-making methods). In reality, the invaders of network security include different levels of hackers and invaders (employees), and the protectors include enterprises of different industries. In other words, the game groups can be divided into different subgroups. Because of different abilities, the subgroups choose different strategies with different game results. The problem of heterogeneous population is shown in Fig. 1; (3) current researches do not take into account the changing characteristics of environments as the game continues. Particularly, the manners of network attack are more and more complex and diverse [29]. Network environment is changing rapidly, and the gains of game change dynamically with the environment. In this way, adding dynamic environment to the evolutionary game model is necessary. Considering the interference of external environments, the model satisfies the game process of attack-defense under modern technologies. This paper mainly discusses the following three problems: 1) How to solve the game problems of heterogeneous groups under similar decision-making groups with differentiated strategies? 2) How to express the influence of inter-group information transmission on the game? 3) Under the complex and changeable network environments, how to improve the adaptability of evolutionary game model to solve the security decision-making problem?

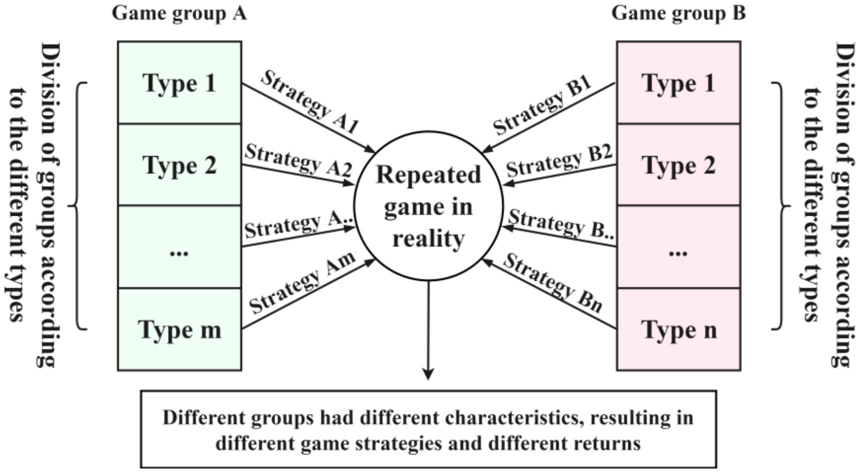

Game group A
Game group B
Division of groups according to the different types
Type 1
Type 2
...
Type m
Strategy A1
Strategy A2
Strategy A..
Strategy Am
Repeated game in reality
Strategy B1
Strategy B2
Strategy B..
Strategy Bn
Type 1
Type 2
...
Type n
Division of groups according to the different types
Different groups had different characteristics, resulting in different game strategies and different returns

Fig. 1. Game problem of heterogeneous groups

Note. Heterogeneity can be understood as different strategies adopted by different groups in the same camp

The main contributions are as follows:

1) An improved evolutionary game model in heterogeneous groups is proposed for data security. Aiming at the problem that traditional evolutionary game models cannot solve the problems of heterogeneous groups and the game process is interfered by dynamic environment, a new game model is proposed by adding the game type space T and the dynamic environment space E to divide heterogeneous groups.

2) The calculation method of the replication dynamic equation and the judgment condition of stability are given. Aiming at the evolution rate difference caused by information exchange of players, the information flow degree parameter is added to improve the replication dynamic equation and the accuracy. Additionally, the Nash equilibrium judgment condition of the new method is supplemented.

3) The optimal defense strategy selection algorithm for data security is designed to realize the decision-making of optimal strategy combination, and the dynamic environment function is added to make the algorithm solution more practical and improve the adaptability to complex and changeable attacks.

4) The methods to determine the evolution direction and analyze the stability at any time are listed. Taking the game between two types of invaders and one type of defender as an example, the method to determine the evolution direction at any time is introduced, and the stability of the equilibrium point is analyzed by the Jacobian matrix method.

The structure of this paper is as follows: Section 2 proposes an improved evolutionary game model between heterogeneous groups for data security. Section 3 introduces the calculation method of the improved replication dynamic equation, Nash equilibrium judgment and optimal defense strategy selection algorithm. In Section 4, some game cases are designed to determine the evolution direction and give the stability analysis method. In Section 5, the experimental simulation and analysis are carried out, and the superiority of the scheme is compared. Finally, Section 6 summarizes the conclusions and shortcomings of the paper and introduces the direction of future research.

2 Construction of Improved Attack-Defense Evolutionary Game Model between Heterogeneous Groups for Data Security

Aiming at the data security problem in dynamic environment, the improved network attack-defense evolutionary game model between heterogeneous groups can be expressed as a 6-tuple. ADEGM = (N, T, S, P, U, E).

1) $N = (N_A, N_D)$ is the participant space of the evolutionary game. N_A represents the group of invaders and N_D represents the group of defenders.

2) $T = (T_A, T_D)$ is the type space of players; $T_A = \{TA_1, TA_2, ..., TA_\lambda\}$ represents the group types of invaders, and $T_D = \{TD_1, TD_2, ..., TD_\gamma\}$ represents the group types of defenders. λ, γ represents the total number of invader types and defender types respectively. Note: $\lambda,\ \gamma \in N^+,\ \lambda,\ \gamma \geq 2$.

3) $S = (S_k^A, S_l^D)$ is the game strategy space. $S_K^A = \{A_{k1}, A_{k2}, ..., A_{kn}\}$ represents the strategy set of k - type invaders, and $S_l^D = \{D_{l1}, D_{l2}, ..., D_{lm}\}$ represents the strategy set of l -type defenders, $1 \leq k \leq \lambda$, $1 \leq l \leq \gamma$.

4) P=$(P_T^A, P_T^D, P_k^A, P_l^D)$ is the game belief set; $P_T^A = \{\varepsilon_1, \varepsilon_2, ..., \varepsilon_\lambda\}$ represents the probability set of invader type; $P_T^D = \{\zeta_1, \zeta_2, ..., \zeta_\gamma\}$ represents the probability set of defender type; $P_k^A = \{p_{k1}, p_{k2}, ..., p_{kn}\}$ represents the probability set of invader strategies, and $P_l^D = \{q_{l1}, q_{l2}, ..., q_{lm}\}$ represents the probability set of defender strategies. $n, m \in N^+$, $n, m \geq 2$, n, m respectively represent the maximum number of invaders and defenders per subgroup.

5) $U = (U_A, U_D)$ is the set of game payoff functions; U_A and U_D are the payoff function sets of invaders and defenders, respectively. Note: the payoff function is obtained by the sum of dynamic environment functions of income-type and loss-type.

6) $E = (E_A, E_D)$ is the set of dynamic environment functions, $E_A = \{B_{klij}^A(t), C_{klij}^A(t)\}$ and $E_D = \{B_{klij}^D(t), C_{klij}^D(t)\}$. $B_{klij}^A(t)$ represents the income-type dynamic environment functions set of invaders when k -type invader adopts i strategy and l -type defenders adopt j strategy; $C_{klij}^A(t)$ represents the loss-type dynamic environment functions set of invaders when k -type invader adopts i strategy and l -type defender adopts j strategy; $B_{klij}^D(t), C_{klij}^D(t)$ respectively represent the sets of corresponding income type, loss-type functions of defenders.

A dynamic environment means that the values of parameters such as profit, loss and cost will change as the game progresses, i.e., the payoff is different when the environment is different. In the game between invaders and defenders, the cost of invasion decreases with the accumulation of invaders' experience. The defense capability of the system becomes stronger with the accumulation of defender's investment. At the same time, defenders realize the seriousness of data leakage and gradually increase the punishment.

In the evolution process of attack-defense, different strategies have different effects. Driven by interests, decision-makers improve their strategies by comparing, imitating and learning the results of other strategies, making the evolutionary game continue to iterate and show a trend of continuous exploration. The heterogeneous attack-defense game tree is shown in Fig. 2. The framework of payoff matrix is shown in Table 1, and the parameters and meanings are shown in Table 2.

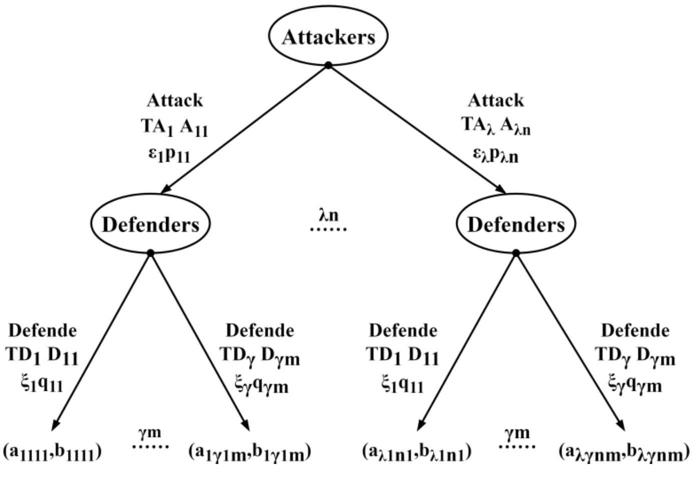


Fig. 2. Basic network attack-defense game tree

TA_k and TD_l indicates the types of invaders and defenders respectively, and A_{ki} and D_{lj} indicates the strategies of invaders and defenders respectively. The attack-defense game tree represents the game between λ -type invaders (*n* strategies for each type) and γ -type defenders (*m* strategies for each type). The payoff matrix can be summarized in Table 1.

Table 1. Framework of game benefit functions

	$N_A \setminus N_D$		Type	TD_1			TD_2			…	TD_γ		
			Probability	ξ_1			ξ_2			…	ξ_γ		
			Strategy	D_{11}	…	D_{1m}	D_{21}	…	D_{2m}	…	$D_{\gamma 1}$	…	$D_{\gamma m}$
Type	Probability	Strategy	Probability	q_{11}	…	q_{1m}	q_{21}	…	q_{2m}	…	$q_{\gamma 1}$	…	$q_{\gamma m}$
		A_{11}	p_{11}										
TA_1	ε_1	…	…	M_{11}			M_{12}			…	$M_{1\gamma}$		
		A_{1n}	p_{1n}										
		A_{21}	p_{21}										
TA_2	ε_2	…	…	M_{21}			M_{22}			…	$M_{2\gamma}$		
		A_{2n}	p_{2n}										
…	…	…	…	…			…			…	…		
		$A_{\lambda 1}$	$p_{\lambda 1}$										
TA_λ	ε_λ	…	…	$M_{\lambda 1}$			$M_{\lambda 2}$			…	$M_{\lambda\gamma}$		
		$A_{\lambda n}$	$p_{\lambda n}$										

$$\mathbf{M}_{kl} = \begin{bmatrix} a_{kl11}, d_{kl11} & a_{kl12}, d_{kl12} & \cdots & a_{kl1m}, d_{kl1m} \\ a_{kl21}, d_{kl21} & a_{kl22}, d_{kl22} & \cdots & a_{kl1m}, d_{kl1m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{kln1}, d_{kln1} & a_{kln2}, d_{kln2} & \cdots & a_{klnm}, d_{klnm} \end{bmatrix}$$

$\mathbf{M}_{kl}$ represents the payoff matrix of the game between k -type invaders and l -type defenders; a_{klij} represents the profit of invaders when k -type invaders adopt i strategy and l -type defenders adopt j strategy, and d_{klij} represents the profits of defenders; a_{klij} and d_{klij} are all functions about *t*.

Table 2. Parameters and meanings

Parameters	Meanings
$ADEGM = (N, T, S, P, U, E)$	Attack-defense evolutionary game model in heterogeneous groups
N_A , N_D	Insider, Defender
TA_k , TD_l	Types of invaders and defenders
A_{ki} , D_{lj}	Strategies of invaders and defenders
ε_i , ξ_j	Type probabilities of invaders and defenders
p_{ki} , q_{lj}	Strategy probability of invaders and defenders
U_A , U_D	Payoff function sets of invaders and defenders
$B^A_{klij}(t)$, $B^D_{klij}(t)$	Income type dynamic environment function set of invaders and defenders
$C^A_{klij}(t)$, $C^D_{klij}(t)$	Loss type dynamic environment function set of invaders and defenders
$\mathbf{M}_{kl}$	Payoff matrix of invader and defenders
$x_{ki}(t)$, $y_{lj}(t)$	The number of A_{ki} and D_{lj} strategies selected by invaders and defenders respectively
θ , ϑ	Information circulation degree of invaders and defenders
ϕ_{ki} , φ_{lj}	Influencing factors of strategy of invaders and defenders

3 Construction of Improved Replication Dynamic Equation, Nash Equilibrium Judgment and Algorithm

3.1 Construction of Improved Replication Dynamic Equation

Based on the above game model, there are λ types of invaders, and each type has n strategies. Setting the number of invaders selecting A_{ki} is $x_{ki}(t)$ at time t. The proportion of $x_{ki}(t)$ in total number of k-type invaders is $p_{ki}(t)$. The expected return of invaders selecting A_{ki} strategy is $U_{ki}^{A}(t)$, and the average return is $\overline{U_{k}^{A}}(t)$ at time t. The basic equation is as follows:

$$\overset{n}{\underset{i=1}{}}\; p_{ki}\,\boxed{t} \;=\; \;. \tag{1}$$

$$p_{ki}(t)=\frac{x_{ki}(t)}{\sum\limits_{i=1}^{n}x_{ki}(t)}. \tag{2}$$

$$U_{ki}^{A}(t)=\sum_{l=1}^{\gamma}\sum_{j=1}^{m}\xi_{l}(t)q_{lj}(t)a_{klij}(t). \tag{3}$$

$$\overline{U_{k}^{A}}(t)=\sum_{i=1}^{n}p_{ki}(t)U_{ki}^{A}(t). \tag{4}$$

As the game of attack-defense continues, the individuals choosing strategies A_{ki} will change due to the differences between strategies. The essence of this change is that the result information of the game is transmitted between groups, leading to individuals improve strategies. In fact, the rate is affected by the interaction between strategies, whether there is a mechanism of information exchange between groups, the expected return of strategies, and the number of selected individuals.

$$x_{ki}'(t)=\theta\cdot\phi_{ki}\cdot x_{ki}(t)\cdot U_{ki}^{A}(t). \tag{5}$$

θ represents the information flow degree of invaders, which depends on whether an information exchange mechanism is established within the group. ϕ_{ki} is the strategic influence factors of invaders [25], indicating the influence degree of A_{ki} strategy. As ϕ_{ki} increases, the influence of A_{ki} strategy becomes stronger, and it will be favored by more invaders; otherwise, the invaders would prefer to choose other strategies. Due to the differences in group information dissemination mechanism, different influence and return of strategies, the strategies chosen by players spread at different speed.

Solving the derivative of Eq. (2), the replication dynamic equation of A_{ki} strategy could be inferred as follows:

$$\begin{aligned}
p_{ki}'(t)&=\frac{x_{ki}'(t)\sum\limits_{i=1}^{n}x_{ki}(t)-x_{ki}(t)\sum\limits_{i=1}^{n}x_{ki}'(t)}{\left[\sum\limits_{i=1}^{n}x_{ki}(t)\right]^{2}}=\frac{x_{ki}(t)}{\sum\limits_{i=1}^{n}x_{ki}(t)}\left[\frac{x_{ki}'(t)}{x_{ki}(t)}-\frac{\sum\limits_{i=1}^{n}x_{ki}'(t)}{\sum\limits_{i=1}^{n}x_{ki}(t)}\right]\\
&=p_{ki}(t)\left[\frac{\theta\cdot\phi_{ki}\cdot x_{ki}(t)\cdot U_{ki}^{A}(t)}{x_{ki}(t)}-\frac{\sum\limits_{i=1}^{n}\theta\cdot\phi_{ki}\cdot x_{ki}(t)\cdot U_{ki}^{A}(t)}{\sum\limits_{i=1}^{n}x_{ki}(t)}\right]\\
&=\theta\phi_{ki}p_{ki}(t)\left[U_{ki}^{A}(t)-\overline{U_{k}^{A}}(t)+\sum_{j=1}^{n}(1-\frac{\phi_{kj}}{\phi_{ki}})\cdot p_{kj}(t)\cdot U_{kj}^{A}(t)\right].
\end{aligned} \tag{6}$$

Similarly, there are *γ* types of defenders, and each type has *m* strategies. Setting the number of defenders selecting D_{lj} at time t is $y_{lj}(t)$. The proportion of $y_{lj}(t)$ in total number of l-type defenders is $q_{lj}(t)$. The expected return of defenders selecting D_{lj} strategy is $U_{lj}^{D}(t)$, and the average return is $\overline{U}\ \ (t)$ at time *t*. The basic equation is as follows:

$$\sum_{j=1}^{m} q_{lj}\,\square t\ =\ \ . \tag{7}$$

$$q_{lj}(t)=\frac{y_{lj}(t)}{\sum_{i=1}^{n} y_{lj}(t)} . \tag{8}$$

$$U_{lj}^{D}(t)=\sum_{k=1}^{\lambda}\sum_{i=1}^{n}\varepsilon_{k}(t)p_{ki}(t)d_{klij}(t) . \tag{9}$$

$$\overline{U_{l}^{D}}(t)=\sum_{j=1}^{n} q_{lj}(t)U_{lj}^{D}(t) . \tag{10}$$

The rate of change in the number of individuals selecting D_{lj} strategy is affected by the interaction between strategies, whether there is a mechanism of information exchange between groups, the expected return of strategies, and the number of selected individuals.

$$y_{lj}'(t)=\vartheta\cdot\varphi_{lj}\cdot y_{lj}(t)\cdot U_{lj}^{D}(t) . \tag{11}$$

ϑ represents the information flow degree of defenders, and it depends on whether an information exchange mechanism is established within the group. φ_{lj} is the strategic influence factors of defenders [25], indicating the influence degree of D_{lj} strategy. As φ_{lj} increases, the influence of D_{lj} strategy becomes stronger, and it will be favored by more defenders; otherwise, the defenders would prefer to choose other strategies.

Solving the derivative of Eq, (8), the copying dynamic equation of D_{lj} strategy could be inferred as follows:

$$\begin{aligned} q_{lj}'(t)\ \square\ & \frac{y_{lj}'(t)\sum_{j\square\square}^{\square} y_{lj}(t)-y_{lj}(t)\sum_{j} y_{lj}'(t)}{\left[\sum_{j=1}^{m} y_{lj}(t)\right]^{2}}\quad \frac{y_{lj}(t)}{\sum_{j=1}^{m} y_{lj}(t)}\left[\frac{y_{lj}'(t)}{y_{lj}(t)}\quad \frac{\sum_{j} y_{lj}'(t)}{\sum_{j=1}^{m} y_{lj}(t)}\right] \\ =q_{lj}(t)&\left[\frac{\vartheta\cdot\varphi_{lj}\cdot y_{lj}(t)\cdot U_{lj}^{D}(t)}{y_{lj}(t)}-\frac{\sum_{j=1}^{m}\vartheta\cdot\varphi_{lj}\cdot y_{lj}(t)\cdot U_{lj}^{D}(t)}{\sum_{j=1}^{m} y_{lj}(t)}\right] \\ =\vartheta\varphi_{lj}q_{lj}(t)&\left[U_{lj}^{D}(t)-\overline{U_{l}^{D}}(t)+\sum_{i=1}^{m}(1-\frac{\varphi_{li}}{\varphi_{lj}})\cdot q_{li}(t)\cdot U_{li}^{D}(t)\right] . \end{aligned} \tag{12}$$

Combined with Eq. (6) and Eq. (12), the improved replicative dynamic equation system is as follows:

$$\begin{cases} p'_{ki}(t)=\theta\phi_{ki}p_{ki}(t)\left[U_{ki}^{\square}(t)-\overline{U_{k}}(t)+\sum_{j=1}^{n}(1-\dfrac{\phi_{kj}}{\phi_{ki}})\cdot p_{kj}(t)\cdot U_{kj}(t)\right] \\ q'_{lj}(t)=\vartheta\varphi_{lj}q_{lj}(t)\left[U_{lj}^{D}(t)-\overline{U_{l}^{D}}(t)+\sum_{i=1}^{m}(1-\dfrac{\varphi_{li}}{\varphi_{lj}})\cdot q_{li}(t)\cdot U_{li}^{D}(t)\right] \end{cases}. \tag{13}$$

It can be known that when the information flow degrees of the invaders group θ and the defender group ϑ are both 1, the strategic influence factors of the invader ϕ_{ki} and the defender φ_{lj} are both 1. The replication dynamic equation proposed by Taylor and Jonker [30] can be obtained as follows:

$$\begin{cases} p'_{\square}(t)=p\ (t)[U^{A}(t)-\overline{U^{A}}(t)] \\ q'_{\square}(t)=q\ \ (t)[U^{D}(t)-\overline{U^{D}}(t)] \end{cases}. \tag{14}$$

By solving the improved replicative dynamic Eq. (13) = 0, the equilibrium point can be obtained and the optimal strategy can be selected.

3.2 Nash Equilibrium Judgment

According to evolutionary game theory, there is a mixed strategy set $\square p_{ki}^{*}\ q_{lj}^{*}$ that makes the game reach Nash equilibrium. According to the definition of Nash equilibrium, $\square p_{ki}^{*}\ q_{lj}^{*}$ satisfies the following conditions:

$$\begin{cases} \forall p_{ki},\sum_{k=1}^{\lambda}\sum_{l=1}^{\gamma}\sum_{i=1}^{n}\sum_{j=1}^{m}p_{ki}^{\square}(\xi_{l}q_{lj}a_{klij})\geq\sum_{k=1}^{\lambda}\sum_{l=1}^{\gamma}\sum_{i=1}^{n}\sum_{j=1}^{m}p_{ki}(\xi_{l}q_{lj}a_{klij}) \\ \forall q_{lj},\sum_{k=1}^{\lambda}\sum_{l=1}^{\gamma}\sum_{i=1}^{n}\sum_{j=1}^{m}q_{lj}^{*}(\varepsilon_{i}p_{ki}^{*}d_{klij})\geq\sum_{k=1}^{\lambda}\sum_{l=1}^{\gamma}\sum_{i=1}^{n}\sum_{j=1}^{m}q_{lj}(\varepsilon_{i}p_{ki}^{*}d_{klij}) \\ \sum_{i=1}^{n}p_{ki}=1,\ \ \sum_{k=1}^{\lambda}\sum_{i=1}^{n}\varepsilon_{i}p_{ki}=1,\ \ p_{ki},\varepsilon_{i}\geq 0 \\ \sum_{j=1}^{m}q_{lj}=1,\ \ \sum_{l=1}^{\gamma}\sum_{j=1}^{m}\xi_{l}q_{lj}=1,\ \ q_{lj},\xi_{l}\geq 0 \end{cases}. \tag{15}$$

The first condition guarantees that under Strategy $\square p_{ki}^{*}\ q_{lj}^{*}$, the invader will not benefit from a unilateral change in strategy. The second condition guarantees that under strategy $\square p_{ki}^{*}\ q_{lj}^{*}$, the defender will not profit from a change in strategy. In this way, $\square p_{ki}^{*}\ q_{lj}^{*}$ is a strategy for Nash equilibrium.

3.3 Optimal Defense Strategy Selection Algorithm for Data Security

Algorithm
Optimal defense strategy selection algorithm for data security base on improving evolutionary game between heterogeneous groups

Input Different subjects of data leakage events, historical invasion behavior and collecting configuration information of defense devices, statistical event frequency, and historical trends in gains and losses
Output Optimal defense strategy Q

```
BEGIN
1) Initialize ADEGM = (N, T, S, P, U, E)
// Initialize an improved evolutionary game model between heterogeneous groups
{
1-1) Construct $T_A = \{TA_1, TA_2, ..., TA_\lambda\}$ , $T_D = \{TD_1, TD_2, \ldots, TD\ \}$ $\lambda,\ \gamma \in N^+,\ \lambda,\ \gamma \geq 2$ .
// According to the different subjects of data leakage events, the types of invaders and defenders are established respectively
1-2) Construct $S_k^A = \{A_{k1}, A_{k2}, ..., A_{kn}\}$ , $S_l^D = \{D_{l1}, D_{l2}, ..., D_{lm}\}$ $1 \leq k \leq \lambda$ , $1 \leq l \leq$ .
// Through analyzing the historical invasion behavior and collecting the configuration information of defense devices, the strategy space of invaders and defenders is constructed.
1-3) Construct $P_T^A = \{\varepsilon_1, \varepsilon_2, ..., \varepsilon_\lambda\}$ , $P_T^D = \{\square_1,\ {}_2, ...,\ {}_\gamma\}$ , $p_k^A = \{p_{k1}, p_{k2}, ..., p_{kn}\}$ , $P_l^D = \{q_{l1}.q_{l2}, ..., q_{lm}\}$
$n, m \in N^+,\ n, m \geq 2$
// Based on the statistical event frequency, the game belief sets for type probabilities and strategy probabilities of invaders and defenders are constructed, respectively.
1-4) Construct $U = (\ U_A, U_D)$
// Construct the set of game payoff functions. The payoff functions are obtained by the sum of dynamic environment functions and are used to calculate the replication dynamic equation.
1-5) Construct $E_A = \{B_{klij}^A(t), C_{klij}^A(t)\}$ , $E_D = \{B_{klij}^D(\ t), C_{klij}^D(\ t)\}$
// Construct the set of dynamic environment functions based on historical trends in gains and losses.
}

2) Set $\theta, \vartheta \in [0,1]$
// Set the information flow degree of invaders and defenders according to the actual status of players.
Set $\phi_{ki}, \varphi_{lj} \in [0,1]$
// Set the strategic influence factors of invaders and defenders according to the historical selections of players.
3) Calculate $\begin{cases} U_A = B_{klij}^A(t) - C_{klij}^A(t) \\ U_D = B_{klij}^D(\ t) - C_{klij}^D(t) \end{cases}$ in which, $\begin{cases} U_A = \{U_{11}^A, U_{12}^A, ..., U_{ki}^A, ..., U_{\lambda n}^A\} \\ U_D = \{U_{11}^D, U_{12}^D, ..., U_{lj}^D, ..., U_{\gamma m}^D\} \end{cases}$
// Through traversing each invader type and defender type, the invader payoff and the defense payoff under different strategies combinations are calculated.
4) Calculate $U_{ki}^A(t) = \sum_{l=1}^{\gamma}\sum_{j=1}^{m} \xi_l(t) q_{lj}(t) a_{klij}(t)$ and $U_{lj}^D(t) = \sum_{k=1}^{\lambda}\sum_{i=1}^{n} \varepsilon_k(t) p_{ki}(t) d_{klij}(t)$
$\overline{U_k^A}(t) = \sum_{i=1}^{n} p_{ki}(t) U_{ki}^A(t)$ and $\overline{U_l^D}(t) = \sum_{j=1}^{n} q_{lj}(t) U_{lj}^D(t)$
// According to the payoff function calculated above, the expected return and average return for invaders and defenders are calculated, respectively.
5) Construct $p'_{ki}(t) = \theta\phi_{ki} p_{ki}(t)\left[U_{ki}^A(t) - \overline{U_k^A}(t) + \sum_{j=1}^{n}(1 - \frac{\phi_{kj}}{\phi_{ki}}) \cdot p_{kj}(t) \cdot U_{kj}^A(t)\right]$
// Construct the replication dynamic equation for each strategy of invader with type $TA_k$ .
6) Construct $q'_{lj}(t) = \vartheta\varphi_{lj} q_{lj}(t)\left[U_{lj}^D(t) - \overline{U_l^D}(t) + \sum_{i=1}^{m}(1 - \frac{\varphi_{li}}{\varphi_{lj}}) \cdot q_{li}(t) \cdot U_{li}^D(t)\right]$
// Construct the replication dynamic equation for each strategy of defender with type $TD_l$ .
7) Calculate $Y = \begin{bmatrix} p'_{ki}(t) \\ q'_{lj}(t) \end{bmatrix} = 0$
// Calculate the evolutionary stable equilibrium.
8) Output $Q = \{q_{l1}, q_{l2}, ..., q_{lm}\}$
// Output the optimal defense strategies.
END
```

The time in the above algorithm focuses on the solution of the replication dynamic equation (step 7), and the time complexity of Step 7 is O((m+n)^3). The storage of the algorithm focuses on the storage of payoff matrix, and the space complexity of payoff matrix is O($\gamma m\times\lambda n$). The algorithmic complexity depends on the types and strategies of players, and its parameters can be designed according to actual issues.

4 Determination of Evolution Direction and Stability Analysis Method

Based on the above improved model, considering that enterprises often face multiple types of invaders, two types of invaders and one type of defenders with two strategies are taken as an example to solve the improved replication dynamic equation, analyze the stability and obtain the optimal strategy. The set payoff is shown in Table 3. Note: the strategy probabilities p_{ki} and q_{lj} , and the payoff value (a_{klij}, d_{klij}) are all functions of t, which is not written due to the long formula.

Table 3. Benefits of the attack-defense game

$N_A \setminus N_D$			Type	Enterprises TD_1	
			Probability	ξ_1	
			strategy	D_{11}	D_{12}
Type	Probability	Strategy	Probability	q_{11}	q_{12}
Hackers TA_1	ε_1	A_{11}	p_{11}	(a_{1111}, d_{1111})	(a_{1112}, d_{1112})
		A_{12}	p_{12}	(a_{1121}, d_{1121})	(a_{1122}, d_{1122})
Insiders TA_2	ε_2	A_{21}	p_{21}	(a_{2111}, d_{2111})	(a_{2112}, d_{2112})
		A_{22}	p_{2n}	(a_{2121}, d_{2121})	(a_{2122}, d_{2122})

For two kinds of invaders, the following formula can be obtained:

$$\begin{cases} U_{11}^{A}(t) = q_{11}a_{1111} + q_{12}a_{1112} \\ U_{12}^{A}(t) = q_{11}a_{1121} + q_{12}a_{1122} \\ U_{21}^{A}(t) = q_{11}a_{2111} + q_{12}a_{2112} \\ U_{22}^{A}(t) = q_{11}a_{2121} + q_{12}a_{2122} \\ \overline{U_{1}^{A}}(t) = p_{11}U_{11}^{A}(t) + p_{12}U_{12}^{A}(t) \\ \overline{U_{2}^{A}}(t) = p_{21}U_{21}^{A}(t) + p_{22}U_{22}^{A}(t) \end{cases} . \tag{16}$$

For defenders, the following formula can be obtained:

$$\begin{cases} U_{11}^{D}(t) = \varepsilon_1 p_{11} d_{1111} + \varepsilon_1 p_{12} d_{1121} + \varepsilon_2 p_{21} d_{2111} + \varepsilon_2 p_{22} d_{2121} \\ U_{12}^{D}(t) = \varepsilon_1 p_{11} d_{1112} + \varepsilon_1 p_{12} d_{1122} + \varepsilon_2 p_{21} d_{2112} + \varepsilon_2 p_{22} d_{2122} \\ \overline{U_{1}^{D}}(t) = q_{11}U_{11}^{D}(t) + q_{12}U_{12}^{D}(t) \end{cases} . \tag{17}$$

Additionally,

$$p_{11} + p_{12} = 1,\ p_{21} + p_{22} = 1,\ q_{11} + q_{12} = 1 . \tag{18}$$

As such, $p'_{11} = -p'_{12},\ p'_{21} = -p'_{22},\ q'_{11} = -q'_{12}$. Only p'_{11}、p'_{21}、q'_{11} are needed to analyze for the game situation. According to Eq. (13), the replicate dynamic equation system can be obtained as follows:

$$\begin{cases} p_{11}'(t)=\theta\phi_{11}p_{11}(1-p_{11})\left[q_{11}a_{1111}+q_{12}a_{1112}-(\phi_{12}/\phi_{11})(\,q_{11}a_{1121}+q_{12}a_{1122})\right] \\ p_{21}'(t)=\theta\phi_{21}p_{21}(1-p_{21})\left[q_{11}a_{2111}+q_{12}a_{2112}-(\phi_{22}/\phi_{21})(\,q_{11}a_{2121}+q_{12}a_{2122})\right] \\ q_{11}'(t)=\vartheta\varphi_{11}q_{11}(1-q_{11})\begin{bmatrix}\varepsilon_1 p_{11}d_{1111}+\varepsilon_1 p_{12}d_{1121}+\varepsilon_2 p_{21}d_{2111}+\varepsilon_2 p_{22}d_{2121}-(\varphi_{12}/\varphi_{11}) \\ (\varepsilon_1 p_{11}d_{1112}+\varepsilon_1 p_{12}d_{1122}+\varepsilon_2 p_{21}d_{2112}+\varepsilon_2 p_{22}d_{2122})\end{bmatrix} \end{cases}. \tag{19}$$

4.1 Evolution Direction Determination Method

Under the conditions of dynamic environment changes, the evolution path and evolution direction may change over time. Here is the calculation method of evolution direction at any time. The first derivative of the replication dynamic equation is as follows:

$$\begin{aligned} &dp_{11}'(t)/dp_{11}(t)=\theta\phi_{11}(1-2p_{11})\left[q_{11}a_{1111}+q_{12}a_{1112}-(\phi_{12}/\phi_{11})(q_{11}a_{1121}+q_{12}a_{1122})\right] \\ &dp_{12}'(t)/dp_{12}(t)=\theta\phi_{21}(1-2p_{21})\left[q_{11}a_{2111}+q_{12}a_{2112}-(\phi_{22}/\phi_{21})(q_{11}a_{2121}+q_{12}a_{2122})\right] \\ &dq_{11}'(t)/dq_{11}(t)=\vartheta\varphi_{11}(1-2q_{11})\begin{bmatrix}\varepsilon_1 p_{11}d_{1111}+\varepsilon_1 p_{12}d_{1121}+\varepsilon_2 p_{21}d_{2111}+\varepsilon_2 p_{22}d_{2121}- \\ (\varphi_{12}/\varphi_{11})(\varepsilon_1 p_{11}d_{1112}+\varepsilon_1 p_{12}d_{1122}+\varepsilon_2 p_{21}d_{2112}+\varepsilon_2 p_{22}d_{2122})\end{bmatrix} \end{aligned}$$

When the condition $(1-2p_{11})\left[q_{11}a_{1111}+q_{12}a_{1112}-(\phi_{12}/\phi_{11})(q_{11}a_{1121}+q_{12}a_{1122})\right]>0$ is satisfied, the hackers evolve into A_{11}; otherwise they evolve into A_{12}. When condition $(1-2p_{21})\left[q_{11}a_{2111}+q_{12}a_{2112}-(\phi_{22}/\phi_{21})(q_{11}a_{2121}+q_{12}a_{2122})\right]$ >0 is satisfied, the insiders evolve into A_{21}; otherwise they evolve into A_{22}. When the condition $\vartheta\varphi_{11}(1-2q_{11})\begin{bmatrix}\varepsilon_1 p_{11}d_{1111}+\varepsilon_1 p_{12}d_{1121}+\varepsilon_2 p_{21}d_{2111}+\varepsilon_2 p_{22}d_{2121}- \\ (\varphi_{12}/\varphi_{11})(\varepsilon_1 p_{11}d_{1112}+\varepsilon_1 p_{12}d_{1122}+\varepsilon_2 p_{21}d_{2112}+\varepsilon_2 p_{22}d_{2122})\end{bmatrix}$>0 is satisfied, the enterprises evolve into D_{11}; otherwise they evolve into D_{12}.

4.2 Analysis of Evolutionary Stability

Equilibrium Solution. When $p_{11}'(t)=0$, $p_{21}'(t)=0$, and $q_{11}'(t)=0$ in the replication dynamic equation, least eight solutions $E_1(0,0,0)$, $E_2(0,0,1)$, $E_3(0,1,0)$, $E_4(1,0,0)$, ${}_5(1,1,0)$, $E_6(1,0,1)$, $E_7(0,1,1)$, $E_8(1,1,1)$ and $E_{9\text{-}13}(p_{11}^*,p_{21}^*,q_{11}^*)$ of the evolutionary system can be obtained by solving the equations. $E_{9\text{-}13}(p_{11}^*,p_{21}^*,q_{11}^*)$ is all the solutions that satisfy Eqs. (20) and (21).

$$\begin{cases} q_{11}a_{1111}+(1-q_{11})a_{1112}-(\phi_{12}/\phi_{11})(\,q_{11}a_{1121}+(1-q_{11})a_{1122})=0 \\ p_{11}=0\ or\ 1 \\ \begin{bmatrix}\varepsilon_1 p_{11}d_{1111}+\varepsilon_1 p_{12}d_{1121}+\varepsilon_2 p_{21}d_{2111}+\varepsilon_2 p_{22}d_{2121}- \\ \dfrac{\varphi_{12}}{\varphi_{11}}(\,\varepsilon_1 p_{11}d_{1112}+\varepsilon_1 p_{12}d_{1122}+\varepsilon_2 p_{21}d_{2112}+\varepsilon_2 p_{22}d_{2122})\end{bmatrix}=0 \end{cases}. \tag{20}$$

$$\begin{cases} q_{11}a_{1111}+(1-q_{11})a_{1112}-(\phi_{12}/\phi_{11})(\,q_{11}a_{1121}+(1-q_{11})a_{1122})=0 \\ p_{21}=0\ or\ 1 \\ \begin{bmatrix}\varepsilon_1 p_{11}d_{1111}+\varepsilon_1 p_{12}d_{1121}+\varepsilon_2 p_{21}d_{2111}+\varepsilon_2 p_{22}d_{2121}- \\ \dfrac{\varphi_{12}}{\varphi_{11}}(\,\varepsilon_1 p_{11}d_{1112}+\varepsilon_1 p_{12}d_{1122}+\varepsilon_2 p_{21}d_{2112}+\varepsilon_2 p_{22}d_{2122})\end{bmatrix}=0 \end{cases}. \tag{21}$$

Stable Point Judgment. Whether the equilibrium point is a stable point (i.e., the evolutionary stability strategy, ESS) needs further discussion. According to the Jacobian matrix solution method proposed by Friedman [31], the asymptotic stability of an equilibrium point is analyzed.

The partial derivatives of p_{11},p_{21},q_{11} in Eq. (19) are taken respectively, and the Jacobian determinant is constructed as follows:

$$\mathbf{J}=\begin{bmatrix} J_{11} & J_{12} & J_{13} \\ J_{21} & J_{22} & J_{23} \\ J_{31} & J_{32} & J_{33} \end{bmatrix} \quad \begin{cases} J_{11}=\partial p'_{11}/\partial p_{11}=\theta\phi_{11}(1-2p_{11})\left[q_{11}a_{1111}+q_{12}a_{1112}-(\phi_{12}/\phi_{11})(q_{11}a_{1121}+q_{12}a_{1122})\right] \\ J_{12}=\partial p'_{11}/\partial p_{12}=0 \\ J_{13}=\partial p'_{11}/\partial q_{11}=\theta\phi_{11}p_{11}(1-p_{11})\left[a_{1111}-a_{1112}-(\phi_{12}/\phi_{11})(a_{1121}-a_{1122})\right] \\ J_{21}=\partial p'_{12}/\partial p_{11}=0 \\ J_{22}=\partial p'_{12}/\partial p_{12}=\theta\phi_{21}(1-2p_{21})\left[q_{11}a_{2111}+q_{12}a_{2112}-(\phi_{22}/\phi_{21})(q_{11}a_{2121}+q_{12}a_{2122})\right] \\ J_{23}=\partial p'_{12}/\partial q_{11}=\theta\phi_{21}p_{21}(1-p_{21})\left[a_{2111}-a_{2112}-(\phi_{22}/\phi_{21})(a_{2121}-a_{2122})\right] \\ J_{31}=\partial q'_{11}/\partial p_{11}=\vartheta\varphi_{11}q_{11}(1-q_{11})\begin{bmatrix}\varepsilon_1 p_{11}d_{1111}-\varepsilon_1 p_{11}d_{1121}-(\varphi_{12}/\varphi_{11}) \\ (\varepsilon_1 p_{11}d_{1112}-\varepsilon_1 p_{11}d_{1122})\end{bmatrix} \\ J_{32}=\partial q'_{11}/\partial p_{12}=\vartheta\varphi_{11}q_{11}(1-q_{11})\begin{bmatrix}\varepsilon_2 p_{21}d_{2111}+\varepsilon_2 p_{21}d_{2121}-(\varphi_{12}/\varphi_{11}) \\ (\varepsilon_2 p_{21}d_{2112}-\varepsilon_2 p_{21}d_{2122})\end{bmatrix} \\ J_{33}=\partial q'_{11}/\partial q_{11}=\vartheta\varphi_{11}(1-2q_{11})\begin{bmatrix}\varepsilon_1 p_{11}d_{1111}+\varepsilon_1 p_{12}d_{1121}+\varepsilon_2 p_{21}d_{2111}+\varepsilon_2 p_{22}d_{2121}- \\ (\varphi_{12}/\varphi_{11})(\varepsilon_1 p_{11}d_{1112}+\varepsilon_1 p_{12}d_{1122}+\varepsilon_2 p_{21}d_{2112}+\varepsilon_2 p_{22}d_{2122})\end{bmatrix} \end{cases}$$

Substituting the solutions $E_{1\text{-}13}$ into the Jacobian matrices, their eigenvalues can be obtained. When all eigenvalues are less than 0, it is the ESS. Due to the complexity of the matrix, only the method is given here, and the specific values are not listed.

5 Experimental Simulation and Analysis

On the basis of being familiar with relevant facts and setting reasonable parameters, MATLAB 2015 software is used for programming, and simulation experiments were conducted to verify the effectiveness of the proposed method.

5.1 Real Case Description

This paper is based on two cases reported by CNR News in 2018 about hackers invading express companies to steal personal information [32] and People's Daily Online in 2020 about insiders leaking personal information of express companies [33]. According to the research [34] and *Data Leakage Cost Report 2021* (IBM), it is generally thought that data leakage can be divided into hacker theft and insider leakage. There are two types of invaders and one type of defenders, and each player has two strategies. A_{11} is a high-tech attack including two or more complex attacks such as infiltration technology, web monitoring, database monitoring, password attack, protocol vulnerability attack, spoofing attack, denial of service attack, Trojan horse, and buffer overflow attack. A_{12} is a low-tech attack that represents a single simple attack. A_{21} is a high-level malicious access, that is, stealing data with anti-detection awareness, accessing the system multiple times, stealing a small amount of data each time, and not easily detected. A_{22} refers to a low-level malicious access, which means a large amount of data is stolen at one time and easily detected by the system. D_{11} means that the enterprise takes protective measures, that is, through risk control measures such as external safety equipment, traffic analysis and abnormal data detection technology. D_{12} indicates that the enterprise takes basic measures to protect the system through its anti-virus software [35-37]. The network topology of the game is shown in Fig. 3.

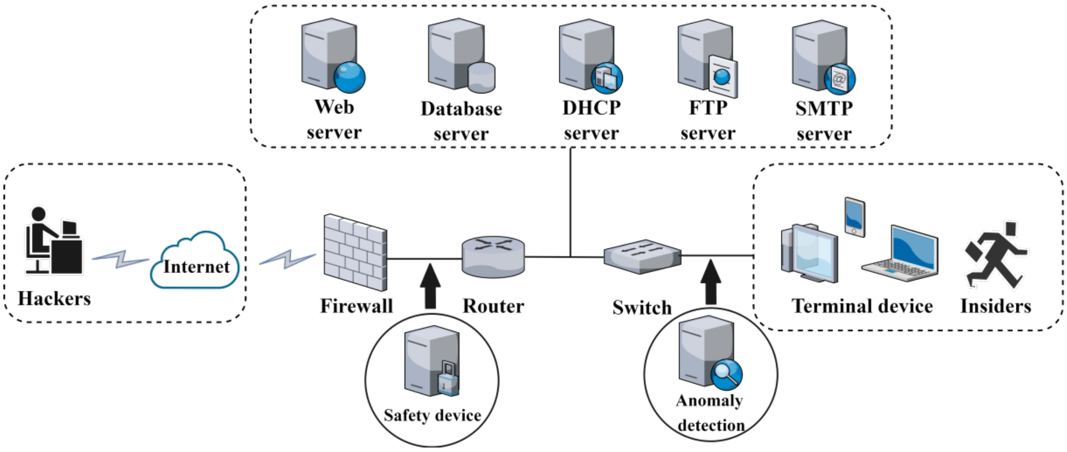


Fig. 3. Network topology

5.2 Parameter Settings

The difference between hackers and insiders is that a hacker obtains system permissions through network attack technology to steal information and sell data on the dark net for profit. Insiders and information middlemen cooperate to form a black industry chain, using their position to steal data (at almost no cost) and obtain fixed income. Insiders are often hard to be found. The characteristics of hackers and insiders can be summarized as the profit values of hackers are greater than that of insiders, and the concealment of insiders is better than that of hackers.

The set of dynamic environment functions is constructed as follows: The benefit value of each strategic game is closely related to income, cost, punishment and loss. When an invader attacks, $B_{klij}^{A}(t)$ includes the income from stealing information; $C_{klij}^{A}(t)$ includes the cost and punishment of invasion; $B_{klij}^{D}(t)$ includes the compensation income obtained by enterprises, and $C_{klij}^{D}(t)$ includes the investment cost of protection measures and the loss of data leakage. It is well known that hackers commit more crimes than insiders, ε_1 =0.6 and ε_2 =0.4. Other parameters are constructed as follows:

1) When a hacker attacks the system, the profit is always I_1=1, and the penalty function of enterprises F=1+0.1t when an intrusion behavior is discovered. The invasion cost of hackers decreases with the accumulation of experience. When adopting high-tech attack strategy, the cost is set as C_1=0.2-0.001t, and the probability of success is 100%. When enterprises take protective measures, the probability function of hacker detection is $a_1(t)=\begin{cases}0.5+0.01\text{t} & \text{t}\le 40\\ 0.9 & \text{t}>40\end{cases}$, indicating that the probability increases with the increase of investment, with an initial value of 0.5 and a maximum value of 0.9 (the same below). When enterprises take basic measures, the probability of hackers being detected is always $a_2=0.2$. Under the low-tech attack strategy, the cost is C_2 = 0.1-0.001t, and the probability of success is 50% (e.i., Revenue is I_2 = 0.5). When enterprises take protective measures, the probability function of hacker detection is $a_3(t)=\begin{cases}0.8+0.01\text{t} & \text{t}\le 10\\ 0.9 & \text{t}>10\end{cases}$; when enterprises take basic measures, the probability of hackers being detected is always $a_4=0.5$.

2) When an insider steals data, the revenue is I_3 = 0.5, and the penalty function of enterprises when the behavior of stealing data is discovered is F = 1+0.1t. In the case of high-level malicious access strategy, the probability of success is 1. When enterprises select protective measures, the probability of being discovered is $a_5(t)=\begin{cases}0.4+0.01\text{t} & \text{t}\le 50\\ 0.9 & \text{t}>50\end{cases}$; when enterprises take basic measures, the probability of an insider being dis-

covered is always a_6 0.1. Under the low-level malicious access strategy, the probability of success is 50% ($I_4 = 0.25$). When enterprises take protective measures, the probability function of an insider being detected is $a_7(t)=\begin{cases}0.6+0.01\text{t} & \text{t}\le 30\\ 0.9 & \text{t>30}\end{cases}$; when enterprises take basic measures, the probability of an insider being detected is always $a_8 = 0.4$.

3) When an enterprise takes protective measures, the investment increases gradually over time, and the investment function is $C_3 = 0.1+0.05\text{t}$. Enterprises only rely on basic measures without investment.

Let $\varphi_{11}=\phi_{11}=\phi_{21}= 1$, the incentive coefficient is $\varphi_{12}/\varphi_{11}=\phi_{12}/\phi_{11}=\phi_{22}/\phi_{21} = 0.5$. The dynamic environment functions of both sides in the game are shown in Table 4 and Table 5, and the benefits are shown in Table 6.

Table 4. Dynamic environment function EA of invaders

	Strategy group	Profit	Cost	Punishment	Probability of behavior being discovered
Hackers	A_{11} D_{11}	$I_1=1$	$C_1(t)$= 0.2-0.001t	$F(t)$= 1+0.1t	$a_1(t)=\begin{cases}0.5+0.01t & t\le 40\\ 0.9 & t>40\end{cases}$
	A_{11} D_{12}				$a_2(t)=0.2$
	A_{12} D_{11}	$I_2=0.5$	$C_2(t)$= 0.1-0.001t		$a_3(t)=\begin{cases}0.8+0.01t & t\le 10\\ 0.9 & t>10\end{cases}$
	A_{12} D_{12}				$a_4(t)=0.5$
Insiders	A_{21} D_{11}	$I_3=0.5$	0		$a_5(t)=\begin{cases}0.4+0.01t & t\le 50\\ 0.9 & t>50\end{cases}$
	A_{21} D_{12}				$a_6(t)=0.1$
	A_{22} D_{11}	$I_4=0.25$			$a_7(t)$ $\begin{cases}0.6+0.01t & t\le 30\\ 0.9 & t>30\end{cases}$
	A_{22} D_{12}				$a_8(t)=0.4$

Table 5. Dynamic environment function ED of defenders

	Strategy group	Profit	Probability of gain	Cost
Enterprises	A_{11} D_{11}	$F(t)$=1+0.1t	Consistent with the probability of behavior being discovered	$C_3(t)$=0.1+0.05t
	A_{11} D_{12}			0
	A_{12} D_{11}			$C_3(t)$=0.1+0.05t
	A_{12} D_{12}			0
	A_{21} D_{11}			$C_3(t)$=0.1+0.05t
	A_{21} D_{12}			0
	A_{22} D_{11}			$C_3(t)$=0.1+0.05t
	A_{22} D_{12}			0

Table 6. Game benefit matrix of both parties in dynamic environment

			Type	Enterprises TD_1	
$N_A \setminus N_D$			Probability	ξ_1	
			Strategy	D_{11}	D_{12}
Type	Probability	Strategy	Probability	q_{11}	q_{12}
Hackers TA_1	1	A_{11}	p_{11}	$(I_1 - C_1 - Fa_1, Fa_1 - C_3 - I_1)$	$(I_1 - C_1 - Fa_2, Fa_2 - I_1)$
		A_{12}	p_{12}	$(I_2 - C_2 - Fa_3, Fa_3 - C_3 - I_2)$	$(I_2 - C_2 - Fa_4, Fa_4 - I_2)$
Insiders TA_2	ε_2	A_{21}	p_{21}	$(I_3 - Fa_5, Fa_5 - I_3 - C_3)$	$(I_3 - Fa_6, Fa_6 - I_3)$
		A_{22}	p_{2n}	$(I_4 - Fa_7, Fa_7 - I_4 - C_3)$	$(I_4 - Fa_8, Fa_8 - I_4)$

5.3 Rationality Analysis of Parameter Settings

To ensure the effectiveness of the simulation results, the rationality of the above parameters is analyzed as follows:

1) Rationality analysis of income

The profit I_1 of hacker's A_{11} strategy is greater than the profit I_2 of hacker's A_{12} strategy, and the profit I_3 of insider's A_{21} strategy is greater than the profit I_4 of hacker's A_{22} . The results show that under the same subject, the income of high-level intrusions is better than that of low-level intrusions. At the same time, the profit I_1 of hacker's A_{11} strategy is greater than the profit I_3 of insider's A_{21} strategy, and the profit I_3 of hacker's A_{12} strategy is greater than the profit I_2 of insider's A_{22} strategy. The results show that under the same intrusion strategies, the profit value of hackers is better than that of moles. The income parameter setting is accordance with the basic fact that "the income value of hackers is better than that of insiders, and the income of high-level invasions is better than that of low-level invasions".

2) Rationality analysis of the probability of being discovered

The detection probability setting of intrusion behavior is shown in Fig. 4 $a_1(t) > a_2(t)$, $a_3(t) > a_4(t)$, $a_5(t) > a_6(t)$, and $a_7(t) > a_8(t)$ satisfy the objective fact that "the return of high-skill strategies is better than that of low-skill strategies". $a_1(t) > a_4(t)$, $a_2(t) > a_5(t)$, $a_3(t) > a_7(t)$, and $a_4(t) > a_8(t)$ satisfy the objective fact that the concealment of insiders is better than that of hackers.

3) Rationality analysis of other parameters

Since moles cost almost nothing to steal data, the cost parameter is set to zero. C1>C2 indicates that the cost of high-level intrusions is greater than that of low-level intrusions. If enterprises take basic measures, the original software of the system is applied and the cost parameter is 0.

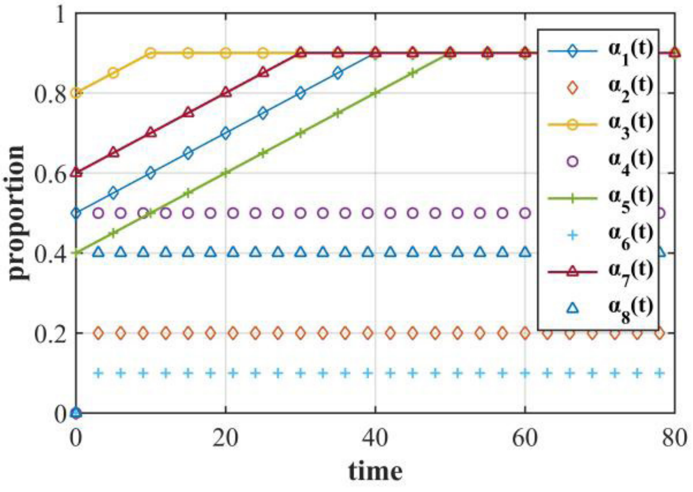
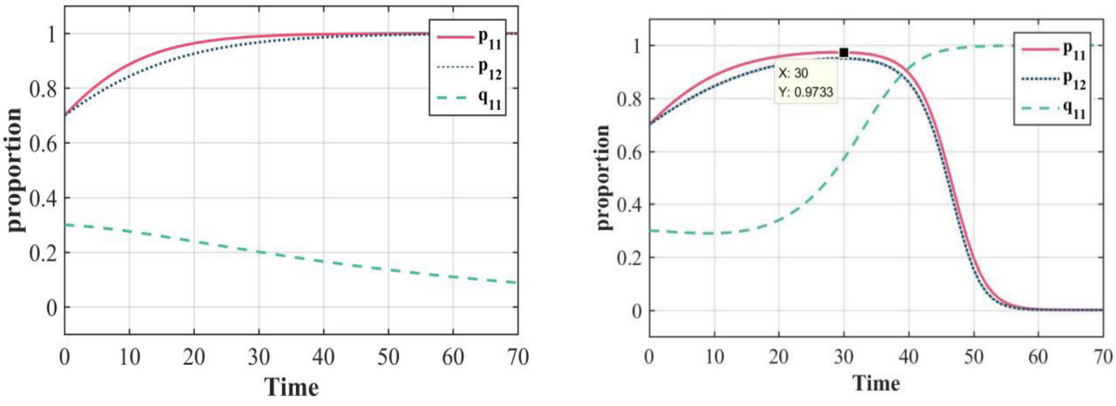


Fig. 4. Probability of intrusion detection

From the above analysis, the data settings are in line with the invasion characteristics of hackers and insiders, and could reflect the objective laws.

5.4 Simulation Experiment

Effect Comparison Experiment of Dynamic Environment. Considering the realistic background of high-frequency system intrusions, in the initial state, invaders are more likely to launch attacks and enterprises are more likely to use basic defenses. As such, the probability for invaders is set to $p_{11} = p_{21} = 0.7$ and for enterprises to $q_{11} = 0.3$. Under the condition that the information flow degree of invaders and defenders is 0.2, two groups of experiments are set respectively: 1) Evolutionary game simulation in static environments (i.e., static value evolution based on the benefit matrix at t = 0); 2) Evolutionary game simulation in dynamic environments (i.e., evolution based on the parameters set in Section 4.2). The simulation results are shown in Fig. 5. The horizontal axis represents the simulation time, and the vertical axis represents the proportion of strategy selection.



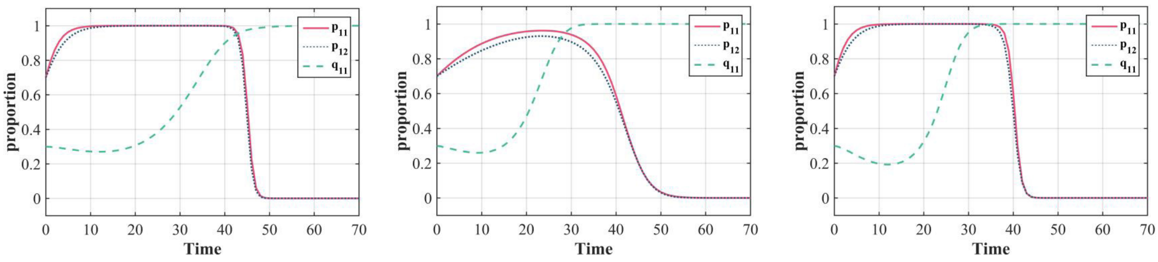
(a) Simulation results instatic Environments (b) Simulation results in dynamic environments

Fig. 5. Comparison of simulation effects in static and dynamic environments

It could be seen from Fig. 5(a) that in static environments, hackers and insiders are stable at t = 30, while enterprises do not reach the stable state at t = 70. The simulation results of the evolutionary game show that hackers attack the system with high-tech attacks; insiders choose high-level malicious access, and enterprises take basic measures. It could be seen from Fig. 5 (b) that in dynamic environments, as enterprises gradually increases the investment and punishment, the cost of invaders decreases, and the detection probability increases under the influence of multiple factors. The probability of hackers and insiders choosing to invade increases gradually, and the probability of strategy selection reaches a peak (0.9733) at t = 30. As the investment increases, the strategy selection of invaders begins to gradually reduce the attack level, and the evolution results tend to be stable until t = 60. At this time, hackers and the insiders choose low-level strategies to invade the system. As the investment of enterprises increase, the probability of intrusion detection increases, and the evolution results tend to be stable at t = 50. Enterprises choose protective measures to effectively protect data.

Obviously, the traditional models can only analyze parameter values at a certain time, which has great limitations in practice. The simulation results in dynamic environments show that the strategy choice of invaders first increase then decreases with the change of enterprise investment. This indicates that dynamic environments can adapt to complex and changeable decision-making situations and have higher practical values.

Effect Comparison Experiment under Different Information Flow Degree. Comparing the effects under different information fluidity conditions, the effectiveness of the model in the dynamic rate of replication is presented. Making other parameters unchanged, three groups of experiments are set respectively: 1) The information exchange system was established between invaders, and enterprises do not : $\theta = 0.8$, and $\vartheta = 0.2$; 2) The information exchange system was established between groups of enterprises, and invaders does not: $\theta = 0.2$, and $\vartheta = 0.8$; 3) An information exchange mechanism should be established between enterprises and invaders: θ = 0.8, and ϑ = 0.8. The simulation results under three groups of parameters are shown in Fig. 6. The horizontal axis represents simulation time, and the vertical axis represents the proportion of strategy selection.



(a) $\theta = 0.8$, $\vartheta = 0.2$ (b) $\theta = 0.2$, $\vartheta = 0.8$ (c) $\theta = 0.8$, $\vartheta = 0.8$

Fig. 6. Effect comparison under different information flow degrees

The evolution rate is summarized in Table 7. When invaders establish the information communication mechanism, the evolution rate of invaders converges fast when t is 40-50, and that of enterprises converge when t is 15-45. When enterprises establish the information communication mechanism, the evolution rate of enterprises converges fast when t is 10-30, while the evolution of invaders converges when t is 25-50. When invaders and enterprises establish an information communication mechanism, the evolution rate of invaders and enterprises would vary quickly. Invaders and enterprises converge when t is 40-50 and 10-30 respectively.

Table 7. Comparison of evolutionary game rates

Invaders	Convergence range	Duration	Rate	Enterprises	Convergence range	Duration	Rate
(a)	40-50	10	0.1	(a)	15-45	30	0.023
(b)	25-50	25	0.04	(b)	10-30	20	0.035
(c)	40-50	10	0.1	(c)	10-30	20	0.035

It can be seen from Fig. 6 that the information flow degree can affect the convergence rate of players. Adding the information flow degree parameter into the evolutionary game model can reflect the different strategy iterations of players. The convergence rate of strategy selection is more accurate, and the theory of replication dynamic equation is more perfect. Its practical guiding significance lies in that it can more accurately simulate the actual situation of strategy evolution, and ensure that enterprises adjust their strategies according to real-time dynamic changes, so as to better deal with complex and diverse network intrusions.

Model and Method Comparison. It can be seen from the comparative experiments that with the continuous evolution of the strategy in the model, the final stable result, that is, the optimal defense strategy for data security, can be obtained. Comparison of this model method with other methods is shown in Table 8.

The original evolutionary game model can only solve the game problems of homogeneous groups, and the accuracy is not high. The incentive coefficients are added in the models to improve the replication dynamic equation, such as network attack, defense security, and cloud service security [25, 27]. Both methods solve the game problems of heterogeneous groups in [26, 28]. In addition, the method in [26] introduced the selection strength to improve the replication dynamic equation, and the method in [28] treated the learning mechanism as a Poisson process to improve the accuracy of the evolution rate.

Compared with the models of other scholars, this paper first solves the heterogeneity problems of game players. Then the influence of information circulation on group decision-making is considered in the calculation of replication dynamic equation. Finally the dynamic environment factor is added to the model to improve the accuracy of the revenue matrix.

The results show that the model has obvious advantages in the accuracy of replication dynamics and the accuracy of benefit matrix, and can guide the practical data security decision-making problems.

Table 8. Comparison results of model and method

Method	Group types	The accuracy of evolution rate	The accuracy of the benefit matrix	Value
Primitive evolutionary game model	Homogeneous	Low	Low	General
The method of reference 25	Homogeneous	Medium (Introducing incentive coefficient)	Low	Medium
The method of reference 26	Heterogeneous	Medium (Introducing strength of selection)	Low	Medium
Method of reference 27	Homogeneous	Medium (Introducing incentive coefficient)	Low	Medium
The method of reference 28	Heterogeneous	High (Using the distribution of poisons)	Low	Medium
The method of this paper	Heterogeneous	High (Considering the influence between the strategy and the group information circulation effect)	High (considering complex dynamic environmental changes)	High

6 Conclusion

In view of the three shortcomings of traditional evolutionary game theory: the difference in evolution rate caused by information exchange, the game problems of heterogeneous groups and the interference of dynamic environment, this paper proposes a new optimal defense strategy for data security by improving the evolutionary game theory. The main work is as follows:

Based on the 4-tuple of traditional evolutionary game theory, the player type space T and dynamic environment functions set E are added to form a 6-tuple, to solve the heterogeneity problem of players and improve the adaptability to complex attacks.

2) The replication dynamic equation is improved. Specifically, based on the original replication dynamic equation, the information flow degree is introduced to reflect the evolution rate difference of players.

3) Taking two types of invaders and one type of defenders as examples, the calculation method of evolution direction at any time and the judgment method of evolution stability strategy are given to judge the final evolution stability of Jacobian determinant.

4) A real case is used to verify the above method. Given the value of each game parameter, the effectiveness of heterogeneity, dynamic environment and information circulation is verified by numerical simulation.

In particular, this method is not a single model, but a comprehensive improvement scheme in three aspects (improving replication dynamics, heterogeneity and environmental change). We can deal with practical problems by setting relevant parameters. For example, when $\theta = 1$ and $\vartheta = 1$, information communication within the group is not considered; when $\lambda = 1$, $\gamma = 1$, heterogeneity is not considered; when the income is not a function t, the dynamic environment is not considered in the model. As such, the parameters can be adjusted appropriately to meet the specific problems.

There are the following shortcomings in this research: 1) this paper considers the heterogeneous game problems of two kinds of players, and the heterogeneity problems of multiple players deserves further study; 2) this paper builds a dynamic function set and transforms each parameter into a function time t. However, the selection of relevant parameter values is a tricky problem in simulation experiments. In the future, time series analysis will be used to fit the function to solve the problem of difficult to select relevant parameters.

Acknowledgement

This work was supported by Hebei Higher Education Teaching Reform Research and Practice Project [2020GJJG44I]; Hebei Innovation Capacity Improvement Plan Project [22550103D].

References

[1] X.D. Fang, F. Yan, Z.L. Xu, Social Changes, Risk Characteristics and Governance Measures Driven by 5G——Based on the 50 Years of Internet Technology Evolution and the Transformation of Communication Mechanism, Journal of Xinjiang Normal University (Philosophy and Social Sciences) 42(2)(2021) 51-62+2.

[2] Xinhuanet, The 14th five year plan for national economic and social development of the people's Republic of China and the outline of long-term objectives for 2035. <http://www.xinhuanet.com/politics/2021lh/2021-03/13/c_1127205564.htm> 2021 (accessed 13.03.21).

[3] W. Jiang, B. Fang, Z. Tian, H. Zhang, Research on Defense Strategies Selection Based on Attack-Defense Stochastic Game Model, Journal of Computer Research and Development 47(10)(2010) 1714-1723.

[4] H. Zhang, J. Zhang, J. Han, Defense Strategies Selection Method Based on Non-cooperative Game Attack Forecast, Computer Science 43(1)(2016) 195-201.

[5] W. Jiang, B. Fang, Z. Tian, H. Zhang, Evaluating Network Security and Optimal Active Defense Based on Attack-Defense Game Model, Chinese Journal of Computers 32(4)(2009) 817-827.

[6] P. Liu, W. Zang, M. Yu, Incentive-based modeling and inference of attacker intent, objectives, and strategies, ACM Transactions on Information and System Security 8(1)(2005) 108-118.

[7] Z. Wang, Y. Lu, X. Li, Military information network security risk assessment based on attack defense game, Military Operations Research and Systems Engineering 33(2)(2019) 35-40+7.

[8] Y. Chen, Y. Fu, X. Wu, Active defense strategy selection based on non-zero-sum attack-defense game model, Journal of Computer Applications 33(5)(2013) 1347-1349+52.

[9] A. AGah, S.K. Das, Preventing DoS Attacks in Wireless Sensor Networks: A Repeated Game Theory Approach, International Journal of Network Security 5(2)(2007) 145-153.

[10] W. Lin, H. Wang, J. Liu, L. Deng, A. Li, Q. Wu, Y. Jia, Research on Active Defense Technology in Network Security Based on Non-Cooperative Dynamic Game Theory, Journal of Computer Research and Development 48(2)(2011) 306-316.

[11] Q. Sun, L. Gao, T. Liu, J. Yao, J. Zheng, H. Wang, Defense descision-making method for multi-path combined attack based on non-zero-sum game, Journal of Northwest University (Natural Science Edition) 49(3)(2019) 343-350.

[12] J. Wang, D. Yu, H. Zhang, N. Wang, Active defense strategy selection based on the static bayesian game, Xi'an Dianzi Keji Daxue Xuebao/Journal of Xidian University 43(1)(2016) 144-150.

[13] Y. Chen, X. Wu, Y. Fu, X. Luo, Active defense strategy selection of network based on fuzzy static Bayesian game model, Application Research of Computers 32(3)(2015) 887-889+899.

[14] D. Yu, J. Wang, H. Zhang, N. Wang, Y. Chen, Risk assessment selection based on static bayesian game, Jisuanji Gongcheng yu Kexue/Computer Engineering & Science 37(6)(2015) 1079-1086.

[15] Y. Liu, D. Feng, L. Wu, Y. Lian, Performance Evaluation of Worm Attack and Defense Strategies Based on Static Bayesian Game, Journal of Software 23(3)(2012) 712-723.

[16] Y. Hu, J. Ma, Y. Guo, H. Zhang, Research on active defense based on multi-stage cyber deception game, Tongxin Xuebao/Journal on Communications 41(8)(2020) 32-42.

[17] Y. Hu, J. Ma, Y. Guo, H. Zhang, Research on active defense based on multi-stage cyber deception game, Journal on Communications 41(8)(2020) 32-42.

[18] Y. Yang, B. Che, Y. Zeng, C. Yang, C. Li, MAIAD: A Multistage Asymmetric Information Attack and Defense Model Based on Evolutionary Game Theory, Symmetry 11(2)(2019) 1-14.

[19] X. Chen, X. Liu, L. Zhang, C. Tang, Optimal Defense Strategy Selection for Spear-Phishing Attack Based on a Multistage Signaling Game, IEEE Access 7(2019) 19907-19921.

[20] X. Liu, H. Zhang, Y. Zhang, L. Shao, J. Han, Active Defense Strategy Selection Method Based on Two-Way Signaling Game, Security and Communication Networks (2019) 1-14.

[21] A. Aydeger, M. Manshaei, M. Rahman, K. Akkaya, Strategic Defense against Stealthy Link Flooding Attacks: A Signaling Game Approach, IEEE Transactions on Network Science and Engineering 8(1)(2021) 751-764.

[22] J. Pawlick, E. Colbert, Q. Zhu, Modeling and Analysis of Leaky Deception Using Signaling Games with Evidence, IEEE Transactions on Information Forensics and Security 14(7)(2019) 1871-1886.

[23] J. Pawlick, Q. Zhu, Deception by Design: Evidence-Based Signaling Games for Network Defense. <https://arxiv.org/abs/1503.05458>, 2015 (accessed 23.06.15).

[24] D. Balkenborg, K. Schlag, On the interpretation of evolutionary stable sets in symmetric and asymmetric games, Mimeo: Bonn University Economics Department, 1994.

[25] J. Huang, H. Zhang, Improving replicator dynamic evolutionary game model for selecting optimal defense strategies, Journal on Communications, 39(1)(2018) 170-182.

[26] H. Hu, Y. Liu, H. Zhang, R. Pan, Optimal Network Defense Strategy Selection Based on Incomplete Information Evolutionary Game, IEEE Access 6(2018) 29806-29821.

[27] P.J. Sun, The optimal privacy strategy of cloud service based on evolutionary game, Cluster Computing 25(1)(2022) 13-31.

[28] E. Zhang, G. Wang, R. Ma, W. Wu, L. Yan, Network Security Defense Decision Making Method Based on Dual

Heterogeneous Population Evolutionary Game Model, Journal of Xi'an JiaoTong University 55(9)(2021) 178-188.

[29] X. Liang, X. Yang, Game Theory for Network Security, IEEE Communications Surveys & Tutorials 15(1)(2013) 472-486.

[30] P.D. Taylor, L.B. Jonker, Evolutionary Stable Strategies and Game Dynamics, Mathematical Biosciences 40(1-2)(1978) 145-156.

[31] D. Friedman, Evolutionary Games in Economics, Econometrica 59(3)(1991) 637-666.

[32] CNR News, Nine people have been detained for stealing 20 million pieces of citizen information from express delivery companies and selling them for money. <http://www.cnr.cn/hubei/jmct/20180608/t20180608_524262457.shtml>, 2018 (accessed 08.06.18).

[33] People's Daily Online, Yuantong insider divulges 400000 pieces of personal information, How does the law work? <http://yuqing.people.com.cn/n1/2020/1118/c209043-31935294.html>, 2020 (accessed 18.11.20).

[34] Y. Ma, F. Xu, Disclosure and Dissemination of Citizen's Personal Information, Credit Reference 32(5)(2014) 33-37.

[35] F. Chen, Y. Luo, X. Chen, X. Gong, D. Fang, A survey of the research on network attack technologies, Journal of Northwest University (Natural Science Edition) 37(2)(2007) 208-212.

[36] J. Zhang, Analysis of network attack technology and network security, Computer Knowledge and Technology 17(18)(2021) 70-71.

[37] C. Xu, Research on Network Attack Prevention Methods for Enterprise Information Security, Journal of China Acadewy of Electronics and Information Technology 15(5)(2020) 483-487.