Hindawi
Security and Communication Networks
Volume 2022, Article ID 1181398, 15 pages
https://doi.org/10.1155/2022/1181398

Research Article

Mixed Strategy Analysis in Attack-Defense Game Model Based on 5G Heterogeneous Network of CPS Using ncPSO

Ning Liu, Qing-Wei Chai, Shangkun Liu, Fanying Meng, and Wei-Min Zheng

College of Computer Science and Engineering, Shandong University of Science and Technology, Qingdao, Shandong 266590, China

Correspondence should be addressed to Wei-Min Zheng; zhengwm901@126.com

Received 16 July 2022; Revised 20 September 2022; Accepted 5 October 2022; Published 7 November 2022

Academic Editor: Yuanyuan Huang

The development of the 5th Generation Mobile Communication Technology not only brings convenience to people but also brings many network security problems. Based on the static game theory of complete information, a game model of attack and defense with limited resources in heterogeneous networks of Cyber Physical Systems is established. This model analyzes the basic rules of the offensive and defensive strategies of both parties when the offensive and defensive resources are limited in the 5th Generation Mobile Communication Technology network environment. The model can also describe the interaction between attackers and defenders. A novel compact particle swarm optimization algorithm is proposed to solve the difficult problem of solving the Nash equilibrium of this game model. The simulation experiment proves that novel compact particle swarm optimization algorithm has good optimization ability and shows that the algorithm can effectively solve the Nash equilibrium of the model. The simulation experiment provides a strategic reference for the attack-defense game with limited resources.

1. Introduction

In recent years, the 5th Generation Mobile Communication Technology (5G) has developed rapidly and has been widely used in many aspects of the lives of people [1]. 5G is characterized by fast transmission rate and high stability [2]. In the future, 5G will be applied in cyber physical systems (CPS), industry, education, environment, medical care, transportation, and many other aspects to achieve real full coverage [3–5]. Based on these characteristics of 5G, heterogeneous networks of CPS are also developing rapidly. The core goal of heterogeneous networks is to achieve free connectivity of devices [6]. The Internet can be composed of multiple interconnected heterogeneous networks. The devices used to connect heterogeneous networks are routers. A heterogeneous network means that two or more wireless communication systems use different access technologies or use the same wireless access technology but belong to different wireless operators [7]. Heterogeneous networks can make use of existing multiple wireless communication systems, and through the integration of systems to make the multiple systems can learn from each other to meet the needs of future mobile communication services. The intelligent access means of multimode terminals is used by heterogeneous network to make a variety of different types of networks that can jointly provide wireless access anytime and anywhere for users [8]. The CPS is closely related to heterogeneous networks. The CPS is mainly divided into three layers: the perception layer, the network layer, and the control layer. The transmission of information mainly depends on the network layer. The connection of different devices among CPS can be regarded as a heterogeneous network [9]. The significance of CPS is to connect physical devices to the Internet, which enables physical devices to have five functions: computing, communication, precise control, remote coordination, and autonomy [10]. The communication is put on the same level as computing in CPS. The network scale of CPS surpasses that of existing industrial control network. The CPS is thought to connect the whole world. The development of 5G heterogeneous networks also brings opportunities for hackers [11–13]. Hackers can use advanced persistent threat (APT), denial of service (DOS), and other attack methods to attack network devices of CPS and use eavesdropping, interference, and other attack methods to attack the information transmission links of CPS [14–16]. The attacks from hackers are characterized by diversity, large scale, and high density [17–19]. It brings great challenges for defenders to defend against attacks [20, 21]. Firewall and intrusion detection system (IDS) has a delay in attacks from hackers, and reasonable defense measures cannot be taken before attacks from hackers [22, 23]. Therefore, it is particularly important to carry out macro analysis of attack and defense behaviors of hacker and defender through game theory. Through this analysis, defenders can obtain the possible attack strategies of hackers before being attacked and then defenders can take effective defense strategies to reduce the loss.

There have been many studies using game theory to analyze the behaviors of hackers and defenders [24–26]. Researchers build different models for different application environments and use game theory for macro analysis [27–30]. Li et al. propose a zero-sum complete information static game model under the network topology graph and proposes a sensitive cost parameter for attacking and defensing [31]. He only considers two attack strategies, and the model is quite different from the actual situation, so this model is not universally applicable. Min builds a Colonel Blotto game using APT attack and defense [14]. And the Nash equilibrium of the model is solved. Simulation experiments show that a "hotbooting" CPU allocation method proposed by Min has lower computational complexity. Jiang proposes a network security defense graph by the state of devices [32]. Taking into account the three attributes of information confidentiality, availability, and integrity into the model, the optimal defense strategy is obtained through game theory. Leng et al. propose a three-player complete information static game model based on white hat, black hat, and software manufacturers. The simulation experiment shows that the model provides an effective strategy for software manufacturers to reduce the risk of software vulnerabilities [33]. Attiah et al. transform the three-strategy attack-defense game model into a two-strategy game model. And the mixed strategy of the model is solved [34]. Wang and Zeng propose a two-stage game in the process of attack and defense. In the first stage, the attacker scans the port of the defender, and the defender deceives or truthfully responds to the attacker. In the second stage, the two sides play a strategic game [35]. Ferguson-Walter et al. establish an incomplete information dynamic game model for network deception attacks to analyze the strategic choices of both attackers and defenders. This model is more in line with the current offensive and defensive scenarios and has strong reference significance [36]. Shen et al. propose a signal game model for the selection of intrusion detection strategies in the wireless sensor network environment. The model uses detection rate and false alarm rate and analyzes the impact of these two parameters on strategies selection [37].

Although there are many existing studies on attack-defense equilibrium based on game theory, there are not many studies on the attack and defense game in the 5G heterogeneous network environment of CPS. The biggest flaw of the existing research models is that they do not consider whether the communication links are attacked, but only consider whether the heterogeneous devices are attacked. Another flaw is that the scale of attack and defense is too small to meet the conditions of 5G. Intelligent computing provides a solution for solving Nash equilibrium of large-scale offensive and defensive games. The most used and most classic intelligent computing algorithm is the particle swarm optimization (PSO). The PSO is proposed by Kennedy and Russell in 1995 according to the foraging behavior of birds [38]. Different algorithms need to be optimized for different problems, so different heuristic algorithms are constantly proposed, such as genetic algorithm (GA) [39], whale optimization algorithm (WOA) [40], black hole (BH) [41], bat algorithm (BA) [42], and sine cosine algorithm (SCA) [43]. A novel compact particle swarm optimization (ncPSO) that uses less memory space and has stronger optimization ability is proposed to solve the Nash equilibrium of the game model proposed in this paper.

The main contributions of this paper are as follows:

(1) Establish a network topology graph based on 5G heterogeneous network of CPS to analyze the attack and defense behaviors. Increase the number of offensive and defensive strategies.

(2) Consider not only network devices being attacked but also communication links between devices being attacked.

(3) A ncPSO is proposed to solve the mixed strategy Nash equilibrium of the game model.

(4) The strategy selection problem of attackers and defenders under different attack resources and different defense resources is analyzed.

The rest of this paper is structured as follows. A 5G heterogeneous network topology diagram of CPS is constructed in Section 2. A attack and defense game model is established in Section 3. The cPSO is proposed and a method for solving mixed strategy Nash equilibrium using the cPSO is described in Section 4. Simulation experiments to discuss the mixed strategies of attackers and defenders under different resources are conducted in Section 5. A conclusion is given in Section 6.

2. System Model and Symbols

A heterogeneous network of CPS based on 5G can be described as an undirected connection graph. We use $G = (V, E)$ to represent the graph in this paper. $V = \left\{v_1, v_2, \ldots, v_{N_V}\right\}$ is a set containing all vertices. $N_V = |V|$ represents the total number of the vertices. Each v_i is a vertex in G and indicates a device in heterogeneous network of CPS. Devices in a heterogeneous network can be mobile phones, servers, smart appliances, routers, etc. $E = \left\{e_1, e_2, \ldots, e_{N_E}\right\}$ is a set containing all edges. $N_E = |E|$ represents the total number of the edges. Each e_i is an edge in G and indicates a type of communication link in heterogeneous network of CPS. Communication links in a heterogeneous network of CPS contain telephone communication, mobile communication, point to point (P2P), etc. The number of all elements in the graph G is $N_G = N_V + N_E$. We can denote $G = \{g_1, g_2, \ldots, g_{N_G}\}$ by $G = (V, E)$. Every g_i can be an attack target for attacker and a protective target for defender.

We use a diagonal matrix $C_{N_v \times N_v}$ to describe the connectivity of graph G. The detailed representation of C is shown in (1). Let $G_{\max}$ denote the maximum connectivity of graph G.

$$C_{ij} = C_{ji} = \begin{cases} 1, & \text{vertex}i\text{ and vertex } j \text{ are connected,} \\ 0, & \text{vertex}i\text{and vertex } j \text{ are not connected.} \end{cases} \tag{1}$$

Since different devices and different communication links have different functions and roles in heterogeneous networks, they have different importance in networks. We use I_i to denote the importance of the ith element in graph G. For vertices, their importance is represented by the number of edges connected by them. For edges, their importance is represented by the smaller maximum connectivity of the subgraphs on either side of the edge. The importance of each element in graph G is shown in

$$I_i = \begin{cases} \sum_{j=1}^{N_V} C_{ij}, & \text{if} g_i \text{is} a \text{vertex}, \\ \min\left(\max\left(G_{1_{\max}}, G_{2_{\max}}\right)\right), & \text{if} g_i \text{isanedge}, \end{cases} \tag{2}$$

where G_1 and G_2 are subgraphs on either side of the edge g_i. $G_{1_{\max}}$, and $G_{2_{\max}}$ are the maximum connectivity of the subgraph G_1 and subgraph G_2.

Usually, the available resources for attackers and defenders to attack and defense network components are limited. Source_A and Source_D are used to denote the total available resources of attackers and defenders, respectively. An attacker can attack one or more elements according to the attack resources. For example, an attacker can use DOS to attack a server, use routing spoofing to attack a router, use flooding to attack a switch, and use APT to attack a specific device. They also can use eavesdropping, truncation, jamming, and tampering to attack the communication links between devices. The defender can defense the network elements using limited resources at the same time. For example, a defender can use blacklist to prohibit attackers attacking server, use flow cleaning to protect routers, and use protection software to defense application devices. Defenders also can use encryption, filter, and VPN to defense the communication links.

3. Attack and Defense Game Model

Based on the model graph proposed in Section 2, we establish a game model $M = (A, D, S_A, S_D, U_A, U_D)$ to analyze behaviors of attacker and defender. In this game model, the attacker and defender take measures at the same time and there is no cooperative relationship between them, but the benefit calculation is different for both attacker and defender, so this game model is a nonzero sum game model. The meanings of the six tuple in the game model M are as follows:

(1) A: An attacker in a 5G heterogeneous network. The attacker can adopt different attack strategies to attack different components in the heterogeneous network.

(2) D: A defender in a 5G heterogeneous network. The defender also can take feasible measures to protect components in the heterogeneous network.

(3) S_A: $S_A = \{S_{A_1}, S_{A_2}, \ldots S_{A_i}, \ldots, S_{A_M}\}$ is the attack action set for attacker, where M represents the total number of the attack strategies. $S_{A_i} = (a_1, a_2, \ldots, a_j, \ldots, a_{N_G}) \in S_A$ is an attack strategy combination in S_A. The value of a_j is shown in

$$a_j = \begin{cases} 1, & \text{if} g_j \text{is attacked,} \\ 0, & \text{if} g_j \text{is not attacked.} \end{cases} \tag{3}$$

(4) S_D: $S_D = \{S_{D_1}, S_{D_2}, \ldots S_{D_i}, \ldots, S_{D_N}\}$ is the defense action set for defender, where N represents the total number of the defense strategies. $S_{D_i} = (d_1, d_2, \ldots, d_j, \ldots, d_{N_G}) \in S_D$ is a defense strategy combination in S_D. The value of d_j is shown in

$$d_j = \begin{cases} 1, & \text{if} g_j \text{is defensed,} \\ 0, & \text{if} g_j \text{is not defensed.} \end{cases} \tag{4}$$

(5) U_A: $U_A\,(S_{A_i}, S_{D_j})$ is the attack profit after the attacker and defender adopt strategy S_{A_i} and S_{D_j}.

(6) U_D: $U_D\,(S_{A_i}, S_{D_j})$ is the defense profit after the attacker and defender adopt strategy S_{A_i} and S_{D_j}.

In the game, the available resources of both sides cannot be infinite. Taking human, material, and financial resources into consideration, Source_A and Source_D are used to denote the total available resources of attackers and defenders, respectively. Each element g_i in G has different attack costs and defense costs for attackers and defenders according to its own characteristics, denoted by Cost_i^A and Cost_i^D. Therefore, the offensive and defensive behaviors must meet the following:

$$\sum_{i=1}^{N_G} a_i \times \text{Cost}_i^A \leq \text{Source}_A, \tag{5}$$

$$\sum_{i=1}^{N_G} d_i \times \text{Cost}_i^D \leq \text{Source}_D. \tag{6}$$

Whether a network element g_i in G is breached depends on the strategies from attacker and defender. It can be described by

$$B_i = \begin{cases} 1, & (a_i = 1\&\&d_i = 0), \\ 0, & (a_i = 1\&\&d_i = 1)\|(a_i = 0), \end{cases} \tag{7}$$

where $B_i = 1$ represents that g_i is breached and $B_i = 0$ represents that g_i is not breached. When element g_i is breached, we remove it from G, then we obtain a new graph G' after the game.

For the attacker, the gain function in the model M is represented by the loss connectivity of the graph G. For the defender, the gain function is represented by the maximum connectivity of the network after the game. We have assumed the maximum connectivity before game is denoted as $G_{\max}$ in Section 2. Then we assume the maximum connectivity after the game as $G_{\max'}$. So the U_A and U_D can be calculated by (8). The profit matrix can be represented in Table 1.

$$\begin{aligned} U_A &= G_{\max} - G_{\max'}, \\ U_D &= G_{\max'}, \\ \text{s.t.} &\sum_{i=1}^{N_G} a_i \times \text{Cost}_i^A \le \text{Source}_A, \\ &\sum_{i=1}^{N_G} d_i \times \text{Cost}_i^D \le \text{Source}_D. \end{aligned} \tag{8}$$

In the game, both the attacker and the defender hope to achieve their maximum benefits. So they choose to use the strategy that could maximize their benefits. They also need to consider the strategies form another on their own returns. Eventually, they will reach a strategic equilibrium. In the game, there may exist a pure strategy and a mixed strategy Nash equilibrium. We assume that the optimal policy of attacker is S_A^*, and the optimal policy of defender is S_D^*. If S_A^* and S_D^* satisfy (9), they are a set of Nash equilibrium solutions.

$$\begin{cases} \forall S_{A_i}, U_A\left(S_A^*, S_D^*\right) \ge U_A\left(S_{A_i}, S_D^*\right), \\ \forall S_{D_j}, U_D\left(S_A^*, S_D^*\right) \ge U_D\left(S_A^*, S_{D_j}\right). \end{cases} \tag{9}$$

4. Game Solution

A solution to solve the equilibrium strategy of M is proposed in this section. This paper takes the attacker as an example to discuss, and the analysis method of the defender is similar to attacker. In this model game M, there may be a pure strategy and a mixed-strategy Nash equilibrium.

For pure-policy Nash equilibrium, we use the traditional min-max theorem to solve [44]. The idea of this theorem is to choose the optimal strategy under various worst-case scenarios [45]. When the profit matrix of model M satisfies (10), strategy (S_A^*, S_D^*) is a pure strategy equilibrium.

$$\max_{1\le i\le M} \min_{1\le j\le N} U_{A_{ij}} = \min_{1\le j\le N} \max_{1\le i\le M} U_{A_{ij}} = U_{A_{i^* j^*}}. \tag{10}$$

Pure strategy is a special form of mixed strategy. When the probability of one strategy is 1, and the probabilities of other strategies are 0, it is a pure strategy. First of all, a strategy choice is given for one participant, another participant chooses the strategy that brings the highest profit among the different strategies. Second, the optimal strategy of another participant is given, and the first participant compare whether the strategy which another participant chooses is also optimal for him. Third, if the strategy combination is the optimal strategy for both participants, then it is a pure strategy Nash equilibrium of the game. When a Nash equilibrium is reached, both offense and defense are reluctant to change their strategies because changing strategies will make their gains less. When there is more than one pure-strategy Nash equilibrium, both sides can choose mixed strategies to maximize their gains. Mixed strategies also occur when the game does not have a pure strategy Nash equilibrium. Taking the chicken game as an example, there are two pure strategy Nash equilibrium in the chicken game. But to participants, they want to take two strategies with a certain probability combination to obtain greater benefits, so the Nash equilibrium of mixed strategies is more important. Therefore, we mainly solve the Nash equilibrium of the mixed strategy. Mixed strategy means that players choose strategies according to probability. We set $P = (p_1, p_2, \ldots, p_M)$ and $Q = (q_1, q_2, \ldots, q_N)$ to represent the probability of the attacker and defender using different strategies, respectively. Therefore, the P and Q should satisfy

$$\left\{ \sum_{i=1}^{M} p_i = 1, \sum_{j=1}^{N} q_j = 1. \right. \tag{11}$$

According to Table 1, the expected returns of the attacker U_A' and the defender U_D' can be expressed as (12). Taking the attacker as an example, if P^* and Q^* are a Nash equilibrium of mixed strategies, then any individual modification of P or Q alone cannot increase the profit. Another solution to mixed strategies is that optimal mixed strategy of every player must make the expected profit of another choosing different strategies the same. The strategy of attacker should consider the profit of defender, it should satisfy (13). The strategy of defender should consider the profit of attacker, it should satisfy

$$\begin{aligned} U_A' &= \max\left(\sum_{i=1}^{M}\sum_{j=1}^{N} p_i \cdot q_j \cdot U_A\left(S_{A_i}, S_{D_j}\right)\right), \\ U_D' &= \max\left(\sum_{i=1}^{M}\sum_{j=1}^{N} p_i \cdot q_j \cdot U_D\left(S_{A_i}, S_{D_j}\right)\right), \\ s.t. &\sum_{i=1}^{N_G} a_i \times \text{Cost}_i^A \le \text{Source}_A, \\ &\sum_{i=1}^{N_G} d_i \times \text{Cost}_i^D \le \text{Source}_D, \\ &\sum_{i=1}^{M} p_i = 1, \\ &\sum_{i=1}^{N} q_i = 1. \end{aligned} \tag{12}$$

$$\begin{aligned} \sum_{i=1}^{M} p_i \cdot U_D\left(S_{A_i}, S_{D_1}\right) &= \sum_{i=1}^{M} p_i \cdot U_D\left(S_{A_i}, S_{D_2}\right) = \ldots \\ &= \sum_{i=1}^{M} p_i \cdot U_D\left(S_{A_i}, S_{D_N}\right), \end{aligned} \tag{13}$$

Table 1: The profit matrix of attacker and defender.

	S_{D_1}	S_{D_2}	$\cdots$	S_{D_N}
S_{A_1}	$U_{A_{11}}, U_{D_{11}}$	$U_{A_{12}}, U_{D_{12}}$	$\cdots$	$U_{A_{1N}}, U_{D_{1N}}$
S_{A_2}	$U_{A_{21}}, U_{D_{21}}$	$U_{A_{22}}, U_{D_{22}}$	$\cdots$	$U_{A_{2N}}, U_{D_{2N}}$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
S_{A_M}	$U_{A_{M1}}, U_{D_{M1}}$	$U_{A_{M2}}, U_{D_{M2}}$	$\cdots$	$U_{A_{MN}}, U_{D_{MN}}$

$$\begin{aligned}\sum_{j=1}^{N} p_j \cdot U_A\left(S_{A_1}, S_{D_j}\right) &= \sum_{j=1}^{N} p_j \cdot U_A\left(S_{A_2}, S_{D_j}\right) = \ldots \\ &= \sum_{j=1}^{N} p_j \cdot U_A\left(S_{A_M}, S_{D_j}\right).\end{aligned} \tag{14}$$

With the development of 5G, the means of network attack are diversified, large scale, and intelligent. The equilibrium solution under large-scale attack and defense strategies is a difficult problem. The high-speed and low-latency 5G make offensive and defensive strategies grow exponentially. Under the large-scale attack and defense strategies, the traditional Nash equilibrium solution method is no longer applicable. As an optimization algorithm, intelligent computing has a good effect on solving high-dimensional complex problems.

A ncPSO is proposed to solve the Nash equilibrium of mixed strategies. The ncPSO is an improvement over PSO. The position of each particle donated as X_i represents a strategic choice of the attacker. PSO will record the global optimal position gBest and the individual optimal position *pBest* of the particle swarm. Then particles move according to gBest and pBest, and the movement equation refers to (15) and (16). w is the inertia weight, and g is the number of iterations.

$$\begin{aligned}V_i^{g+1} &= wV_i^g + c_1 \times r\text{and} \times \left(p\text{Best}_i - X_i^g\right) \\ &\quad + c_2 \times r\text{and} \times \left(g\text{Best} - X_i^g\right),\end{aligned} \tag{15}$$

$$X_i^{g+1} = X_i^g + V_i^{g+1}. \tag{16}$$

The movement process of the particle swarm is shown in Figure 1. V_1, V_2, and V_3 represent three speeds in (15). V_i^{g+1} is the combination of the three speeds. The new position of X_i^{g+1} is based on X_i^g and V_i^{g+1}.

PSO is an iterative optimization algorithm, and gBest and pBest are updated according to the fitness value of particles. Considering that PSO requires larger memory, we apply compact strategy and propose ncPSO to optimize and reduce memory usage [46]. Instead of recording the position of each particle in each iteration, the compact strategy uses a mathematical distribution to record the position of the entire swarm of particles. The compact strategy that we proposed uses a Pareto distribution to describe the location of the particle swarm. The Pareto distribution contains three important parameters: shape parameter k, scale parameter σ, and threshold parameter θ [47]. Among the three parameters, AA and BB play a decisive role in the optimization and convergence of the algorithm, so AA and BB are used to update the particle swarm position. Taking 50 particles with 40 dimensions as an example, the original PSO needs to record the position of each particle in each dimension, so $50 \times 40 = 2000$ memory units are required. The ncPSO only needs to record the AA and BB of entire swarm of particles in each dimension, so the ncPSO only needs $2 \times 40 = 80$ memory units. Compared with traditional PSO, ncPSO can reduce a large number of memory units. The process of the compact strategy is shown as follows. First, generate a probability distribution function (PDF) according to θ and σ. Second, calculate cumulative distribution function (CDF) by PDF. Finally, a random number will be generated to calculate an inverse cumulative distribution function (iCDF). The value of iCDF is the position of the particle swarm. The figures of PDF and CDF of Pareto are shown in Figure 2. The equations of PDF and CDF of Pareto are shown in (17) and (18).

$$\text{PDF} = \frac{1}{\sigma}\left(1 + k\frac{(x-\theta)}{\sigma}\right)^{-1-1/k}, \tag{17}$$

$$\text{CDF} = \begin{cases} 1 - \left(1 + k\dfrac{(x-\theta)}{\sigma}\right)^{-1/k}, & k \neq 0, \\ 1 - \exp\left(-\dfrac{(x-\theta)}{\sigma}\right), & k = 0. \end{cases} \tag{18}$$

The ncPSO generates a winner and a loser through a competitive strategy and then updates σ and θ through the winner and loser. The update formulas for σ and θ are shown in (19) and (20), where Np is the virtual number of particles. For the attacker, the condition for winning the competition in the model can be expressed as how to choose the probability of using each attack strategy to make the defender get the same benefit adopting any defensive strategy. The ith dimension of the particle represents the probability that the attacker chooses the attack strategy S_{A_i}. The fitness value of ncPSO can be expressed as the standard deviation of the profit of defender. Its mathematical representation is shown in

$$\sigma^{g+1} = \sqrt{\left(\sigma^g\right)^2 + \left(\theta^g\right)^2 - \left(\theta^{g+1}\right)^2 + \frac{1}{Np}\left(\text{winner}^2 - \text{loser}^2\right)}, \tag{19}$$

$$\theta^{g+1} = \sigma^g + \frac{1}{Np}(\text{winner} - \text{loser}), \tag{20}$$

$$\begin{aligned}\text{Total Fitness}U_A(j) &= \sum_{i=1}^{M} p_i \cdot U_D\left(S_{A_i}, S_{D_j}\right)j \\ &= 1, 2, \ldots, N\text{fitness}U_A = \text{std}\left(\text{Total Fitness}U_A\right).\end{aligned} \tag{21}$$

For an attacker, let P^* be the optimal probability distribution for choosing different attack strategies. The process of the ncPSO to calculate the P^* is shown in Algorithm 1. In the same way, we can obtain the optimal probability distribution for the defender to choose different defense strategies.

The whole algorithm can be divided into the following six parts:

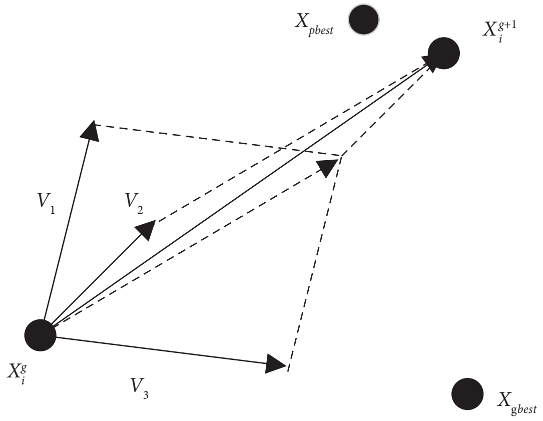


Figure 1: The movement process of the particle swarm.

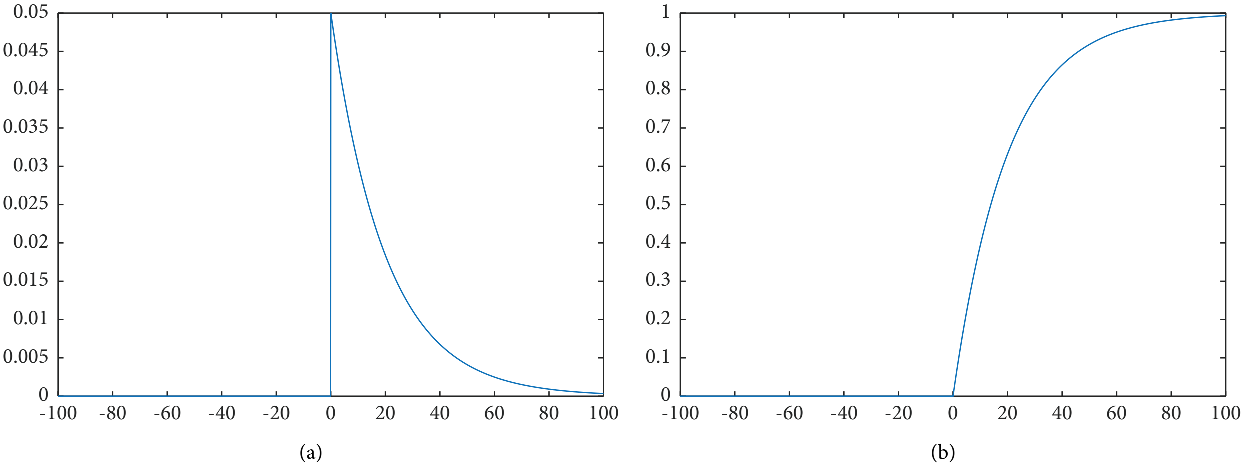


Figure 2: PDF and CDF of Pareto distribution. (a) PDF of Pareto distribution. (b) CDF of Pareto distribution.

(1) The network model is established according to the connection relationship between the actual heterogeneous network devices.

(2) Calculate the importance of each element.

(3) Initialize attack and defense costs for each element. Initialize the total available resources of the attacker and defender.

(4) Build a set of strategies for attacker and defender to attack and defense network element.

(5) Calculate the profit matrix for attacker and defender.

(6) Calculate the mixed strategy Nash equilibrium of attacker and defender using ncPSO.

5. Simulation Experiment and Analysis

In this section, the performance of ncPSO is compared with GA, PSO, WOA, BH, BA, and SCA in 28 test functions in CEC2013. CEC2013 contains 28 different performance test functions, which have good representation. Then, we research the mixed strategy Nash equilibrium using a simple topology diagram. But in real life, the topology diagram of heterogeneous network is much more complicated. Our purpose is to analyze the attack and defense behavior under different attack and defense resources, so using a simple topology diagram can also get the desired results. Four sets of simulation experiments are tested to illustrate the validity of the equilibrium solution and the feasibility of the assignment of offensive and defensive strategies in the game model. First, simulation experiments are carried out to demonstrate the effectiveness of solving Nash equilibrium using ncPSO. Second, simulation experiments are carried out to demonstrate the losses of the defender under different attack and defense resources. Third, strategies of attacker and defender with different defense resources are discussed through simulation experiments. Lastly, strategies of attacker and defender with different attack resources are discussed through simulation experiments. The simulation tools in this section all use Matlab2021B.

5.1. Performance Test Experiment of ncPSO and Other Algorithms.

In this subsection, the performance of different algorithms is compared on 28 test functions of CEC2013. Different algorithms search for the minimum value on the test function. The smaller the function value found, the stronger the optimization ability of the algorithm. Each

```
Initialize the $\theta$ and $\sigma$ of Pareto
Initialize the $X$ by uniform distribution
Initialize the $V$ by uniform distribution
Initialize the $g$Best, $p$Best, fitness$P$Best, fitness$G$Best
while $g < \; = \max\_\mathrm{iteration}$ do
    $pBest$ = compact $(\theta, \sigma)$ according to (17) and (18)
    Calculate the fitness$P$Best of the $p$Best by (21)
    Update $X$ and $V$ of each particle according to (15) and (16)
    Calculate the fitness of the new $X$ by (21)
    if fitness$(X)$ < fitness$P$Best then
        winner = $X$
        loser = $p$Best
    else
        winner = $p$Best
        loser = $X$
    end if
    Update $\theta$ and $\sigma$ according to (19) and (20)
    $p$Best = winner
    fitness$P$Best = fitness(winner)
    if fitness$(X)$ < fitness$G$Best then
        $g$Best = $X$
        fitness$G$Best = fitness$(X)$
    end if
    $g = g + 1$
end while
```

Algorithm 1: The process for calculating P^* using cPSO.

algorithm is run 20 times on each test function, and the mean of the 20 experimental data is taken as the final experimental result. In addition to the performance test experiments, this section also performs Wilcoxon signed rank sum test with significant level $\alpha = 0.05$ on the test results to illustrate the validity of the experimental data. According to the relevant references of different algorithms, the parameter settings of different algorithms are shown in Table 2.

In Table 2, D represents the dimension of the problem, N represents the number of populations, and other parameters are unique to each algorithm and take values according to relevant references. The results of performance test experiments and rank sum verification are shown in Table 3. In Table 3, $>, =, <$, respectively, indicates that ncPSO has better, same, and worse optimization effects on the test function than other algorithms.

The last row of Table 3 gives the number of better, the same, and worse performance of ncPSO compared to other algorithms in the 28 test functions. The experimental results in Table 3 show that ncPSO has the same optimization effect as all optimization algorithms on the two test functions $f8$ and $f20$. Compared with GA, ncPSO performs better than GA in other 26 test functions. Compared with PSO, ncPSO performs better than PSO on 18 test functions, but not as good as PSO on 8 test functions. Compared with WOA and SCA, ncPSO performs better than WOA and SCA on 24 test functions, but worse than WOA and SCA on $f4$ and $f25$. Compared with BH, ncPSO performs better than BH on 21 test functions, but not as good as BH on 4 test functions. Compared with BA, ncPSO performs better than BA on 18 test functions, but worse than BA on 7 test functions.

Table 2: Parameter settings for different algorithms.

Name	Parameter
ncPSO	$D = 50$; $c1 = 2.0$; $c2 = 2.0$;
GA	$D = 50$; $N = 60$; crossover rate = 0.01; mutation rate = 0.9
PSO	$D = 50$; $N = 60$; $c1 = 1.0$; $c2 = 2.0$
WOA	$D = 50$; $N = 60$; probability switch = 0.5
BH	$D = 50$; $N = 60$
BA	$D = 50$; $N = 60$; pulse rate = 0.5; loudness = 0.6; $f_{\min} = 0$; $f_{\max} = 1$
SCA	$D = 50$; $N = 60$; probability switch = 0.5

In order to better show the optimization performance of the algorithms, 9 optimization process diagrams with obvious effects are selected for display in Figure 3. After the algorithm iteration in each graph, the lower the curve, the stronger the optimization ability of the algorithm, and the faster the curve declines, the faster the convergence speed of the algorithm.

As can be seen in Figure 3, ncPSO has better optimization performance and faster convergence speed than other algorithms in functions $f9$, $f11$, $f13$, $f14$, $f17$, $f22$, $f24$, and $f26$. On the function $f12$, ncPSO has worse optimization performance compared with PSO, but has better optimization performance than GA, WOA, BH, BA, and SCA.

5.2. Effectiveness of Solving Nash Equilibrium Using ncPSO.

The graph that we use in the simulation experiment is shown in Figure 4. Because a heterogeneous network of CPS is formed by various devices and different access technologies, the heterogeneous network of CPS is simplified as Figure 4.

Table 3: Experiment results of performance test and rank sum test.

	GA		PSO		WOA		BH		BA		SCA		ncPSO
f1	1.63E + 05	>	−1.33E + 03	>	−1.34E + 03	>	−1.40E + 03	=	−1.39E + 03	>	2.91E + 04	>	−1.40E + 03
f2	5.40E + 09	>	8.83E + 06	>	8.07E + 07	>	2.78E + 07	>	5.86E + 06	>	5.49E + 08	>	1.74E + 06
f3	2.37E + 20	>	2.65E + 09	>	3.47E + 10	>	7.94E + 09	>	6.09E + 08	<	1.05E + 11	>	1.04E + 09
f4	6.79E + 05	>	1.11E + 03	<	5.90E + 04	<	3.18E + 04	<	1.91E + 04	<	6.65E + 04	<	8.12E + 04
f5	8.68E + 04	>	−9.76E + 02	>	−7.96E + 02	>	−9.01E + 02	>	−9.96E + 02	>	2.26E + 03	>	−1.00E + 03
f6	2.78E + 04	>	−8.04E + 02	>	−6.79E + 02	>	−7.96E + 02	>	−8.28E + 02	<	1.12E + 03	>	−8.23E + 02
f7	6.05E + 06	>	−6.76E + 02	>	9.12E + 02	>	−6.19E + 02	>	1.26E + 04	>	−5.81E + 02	>	−6.84E + 02
f8	−6.79E + 02	=	−6.79E + 02	=	−6.79E + 02	=	−6.79E + 02	=	−6.79E + 02	=	−6.79E + 02	=	−6.79E + 02
f9	−5.19E + 02	>	−5.44E + 02	>	−5.30E + 02	>	−5.31E + 02	>	−5.33E + 02	>	−5.26E + 02	>	−5.44E + 02
f10	2.32E + 04	>	−4.43E + 02	>	−1.79E + 02	>	−4.67E + 02	>	−4.96E + 02	>	3.38E + 03	>	−4.99E + 02
f11	2.17E + 03	>	5.13E + 01	>	4.10E + 02	>	4.33E + 02	>	7.43E + 02	>	3.31E + 02	>	−3.84E + 02
f12	1.96E + 03	>	2.29E + 02	<	6.05E + 02	>	5.53E + 02	>	9.23E + 02	>	4.75E + 02	>	2.73E + 02
f13	2.15E + 03	>	4.06E + 02	>	7.97E + 02	>	6.43E + 02	>	1.21E + 03	>	5.60E + 02	>	3.51E + 02
f14	1.66E + 04	>	6.47E + 03	>	9.10E + 03	>	8.57E + 03	>	8.88E + 03	>	1.35E + 04	>	1.84E + 03
f15	1.61E + 04	>	8.53E + 03	<	1.15E + 04	>	8.89E + 03	<	9.14E + 03	<	1.48E + 04	>	9.55E + 03
f16	2.05E + 02	>	2.03E + 02	>	2.03E + 02	>	2.02E + 02	>	2.02E + 02	>	2.04E + 02	>	2.02E + 02
f17	5.37E + 03	>	7.99E + 02	>	1.45E + 03	>	1.35E + 03	>	2.69E + 03	>	1.30E + 03	>	3.51E + 02
f18	5.51E + 03	>	8.68E + 02	<	1.56E + 03	>	1.45E + 03	>	2.81E + 03	>	1.41E + 03	>	9.85E + 02
f19	2.32E + 07	>	5.30E + 02	>	6.81E + 02	>	6.14E + 02	>	5.64E + 02	>	4.31E + 04	>	5.02E + 02
f20	6.25E + 02	=	6.24E + 02	=	6.25E + 02	=	6.24E + 02	=	6.25E + 02	=	6.24E + 02	=	6.25E + 02
f21	1.27E + 04	>	1.67E + 03	>	1.93E + 03	>	1.68E + 03	>	1.48E + 03	<	4.58E + 03	>	1.64E + 03
f22	1.87E + 04	>	1.02E + 04	>	1.29E + 04	>	1.27E + 04	>	1.24E + 04	>	1.54E + 04	>	4.31E + 03
f23	1.83E + 04	>	1.20E + 04	<	1.41E + 04	>	1.28E + 04	<	1.19E + 04	<	1.61E + 04	>	1.40E + 04
f24	1.99E + 03	>	1.38E + 03	>	1.41E + 03	>	1.43E + 03	>	1.44E + 03	>	1.43E + 03	>	1.36E + 03
f25	1.73E + 03	>	1.54E + 03	<	1.53E + 03	>	1.54E + 03	<	1.47E + 03	<	1.55E + 03	>	1.60E + 03
f26	1.79E + 03	>	1.65E + 03	>	1.67E + 03	>	1.61E + 03	>	1.68E + 03	>	1.62E + 03	>	1.48E + 03
f27	4.72E + 03	>	3.32E + 03	<	3.56E + 03	>	3.56E + 03	>	3.47E + 03	>	3.64E + 03	>	3.32E + 03
f28	1.70E + 04	>	4.44E + 03	<	8.75E + 03	>	7.50E + 03	>	1.04E + 04	>	6.62E + 03	>	5.16E + 03
>/ = /<	26/2/0		18/2/8		24/2/2		21/3/4		18/3/7		24/2/2		

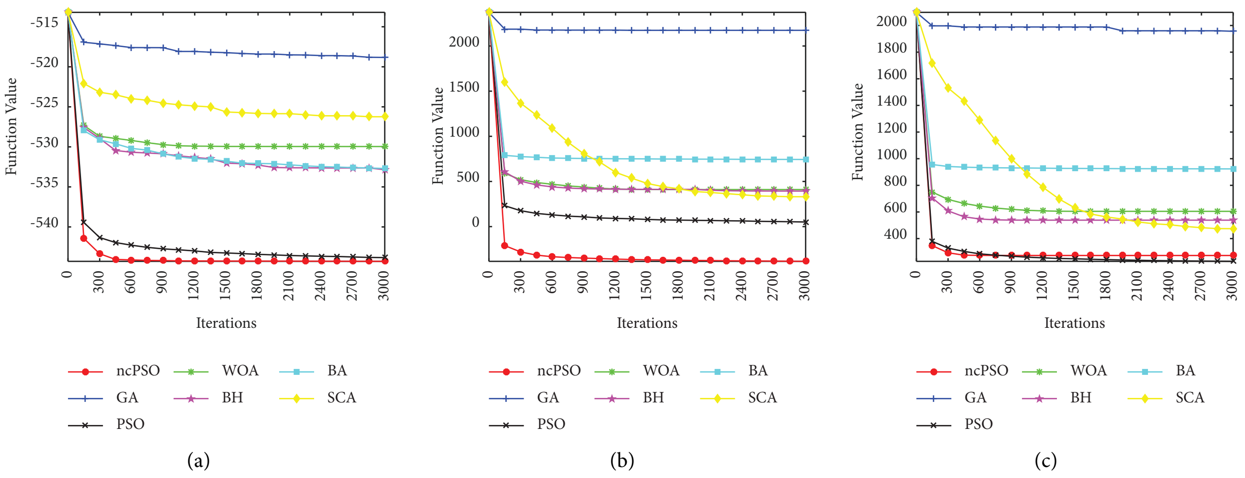


Figure 3: Continued.

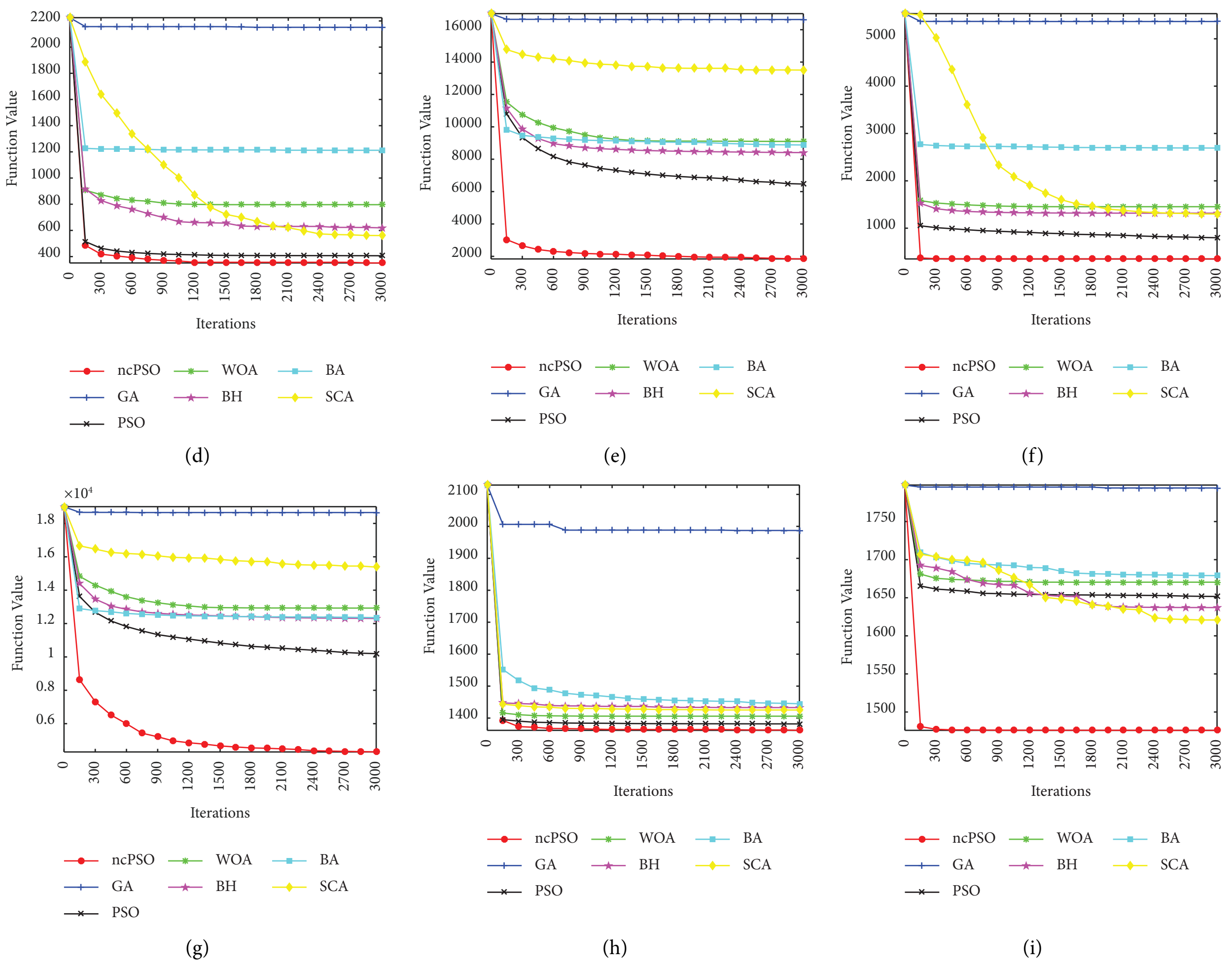


Figure 3: Performance comparison between GA, PSO, WOA, BH, BA, SCA, and ncPSO. (a) *f*9. (b) *f*11. (c) *f*12. (d) *f*13. (e) *f*14. (f) *f*17. (g) *f*22. (h) *f*24. (i) *f*26.

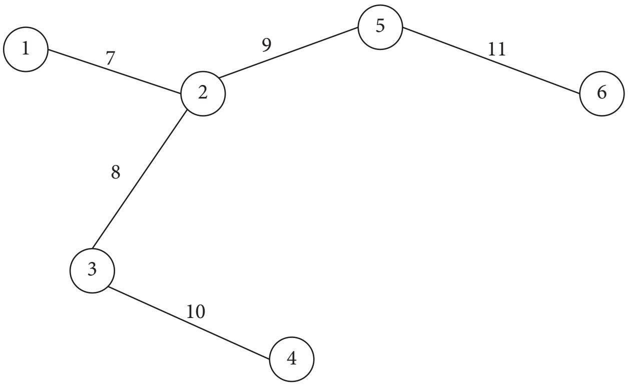


Figure 4: The graph of the simulation experiment.

Each node in the diagram represents a terminal device in the network of CPS, such as terminal servers, mobile phones, sensors, and drones. Each edge in the graph represents a communication link in the network of CPS, such as optical fibers to transmit signals, radiowaves to transmit signals. We set the cost of attacking and defending each element in the graph to be 1. When the offensive and defensive resources are 2, 4, 6, 8, and 10, respectively, the number of strategies of attackers and defenders is shown in Table 4.

From Table 4, it can be seen that there are a large number of offensive and defensive strategies compared to previous studies. There are so many strategies in the small network in Figure 4, which is in line with the large scale of attack and defense in the 5G heterogeneous network environment.

In this subsection, simulation experiments are performed to demonstrate the effectiveness of using intelligent computing to solve the Nash equilibrium. When the defense resources are 4 and 6, respectively, attack and defense experiments are performed ten times when the attack resources are 2, 4, 6, 8, and 10, respectively. A solution to mixed strategies is that optimal mixed strategy of every player must make the expected profit of another choosing different strategies the same. In other words, no single player can change the combination of strategies he adopts to increase his own profit.

First of all, the defense balance strategy is found through ncPSO. Then, ten times attacks are randomly performed under the defense equilibrium strategy calculated by ncPSO,

Table 4: The number of strategies under different offensive and defensive resources.

	2	4	6	8	10
The number of strategies	$C_{11}^{2} = 55$	$C_{11}^{4} = 330$	$C_{11}^{6} = 462$	$C_{11}^{8} = 165$	$C_{11}^{10} = 10$

Table 5: The attack profit when defense resource is 4 and attack resources are 2, 4, 6, 8, and 10, respectively.

	1	2	3	4	5	6	7	8	9	10	Average	Std
2	1.5939	1.5756	1.5776	1.6153	1.5623	1.5709	1.5761	1.5824	1.5859	1.5787	1.5819	**0.0145**
4	2.7161	2.7045	2.7013	2.6899	2.7041	2.6968	2.6870	2.6902	2.7026	2.7084	2.7001	**0.0091**
6	3.5247	3.5234	3.5240	3.5326	3.5276	3.5248	3.5292	3.5229	3.5309	3.5194	3.5259	**0.0040**
8	4.1195	4.1272	4.1271	4.1162	4.1216	4.1284	4.1225	4.1187	4.1272	4.1249	4.1233	**0.0043**
10	4.7563	4.7561	4.7562	4.7564	4.7562	4.7559	4.7564	4.7561	4.7561	4.7565	4.7562	**0.0002**

The bold values are the standard deviations of the ten experiments. The bolded data are used to show that ncPSO is effective in solving Nash equilibrium.

Table 6: The attack profit when defense resource is 6 and attack resources are 2, 4, 6, 8, and 10, respectively.

	1	2	3	4	5	6	7	8	9	10	Average	Std
2	1.1381	1.1597	1.1563	1.1622	1.1636	1.1473	1.1629	1.1638	1.1544	1.1611	1.1569	**0.0084**
4	2.1160	2.1169	2.1136	2.1206	2.1188	2.1157	2.1238	2.1208	2.1183	2.1199	2.1184	**0.0030**
6	2.8821	2.8819	2.8810	2.8752	2.8750	2.8779	2.8787	2.8811	2.8809	2.8796	2.8793	**0.0026**
8	3.5171	3.5166	3.5126	3.5154	3.5144	3.5183	3.5045	3.5107	3.5087	3.5192	3.5137	**0.0047**
10	4.0934	4.0932	4.0937	4.0931	4.0934	4.0939	4.0931	4.0937	4.0932	4.0930	4.0934	**0.0003**

The bold values are the standard deviations of the ten experiments. The bolded data are used to show that ncPSO is effective in solving Nash equilibrium.

and the profit of attacker is calculated. The experimental results are shown in Tables 5 and 6.

The first row in Tables 5 and 6 represents ten times random attacks, the average and standard deviation of these ten attacks. The first column in Tables 5 and 6 represents different attack resources. It can be seen from Tables 5 and 6 that under the condition of the same attack resources, the profit of the attacker is roughly the same in ten attacks. The values of the standard deviations of ten attacks are very small. The standard deviation indicates how spread out the data are. The smaller the standard deviation value, the smaller the difference between the data. The small standard deviation in the experimental results also indicates that the profit from ten attacks are approximately equal. This proves that using ncPSO to solve mixed-strategy Nash equilibrium is effective.

5.3. Losses of Defender under Different Attack and Defense Resources.

In this subsection, simulation experiments are performed to discuss the losses of defender under different attack and defense resources. When the attack resources and defense resources are 2, 4, 6, 8, and 10, respectively, ten times simulation experiments are performed to calculate the losses of defender. Then the average and standard deviation of the losses of defender over ten experiments are calculated. The results of ten times experiments are shown in Table 7.

Table 5 shows the defense losses obtained by using ncPSO to solve the Nash equilibrium under different attack and defense resources. The smaller standard deviation of each group of experiments indicates the stability of the experiment. The experimental results show that the more defense resources, the less defense loss of the defender. The more resources to attack, the greater the defense loss of the defender. At the same time, the experimental results show that when the offensive and defensive resources are equal and equal to about half of all the offensive and defensive resources, it is most unfavorable to the defender.

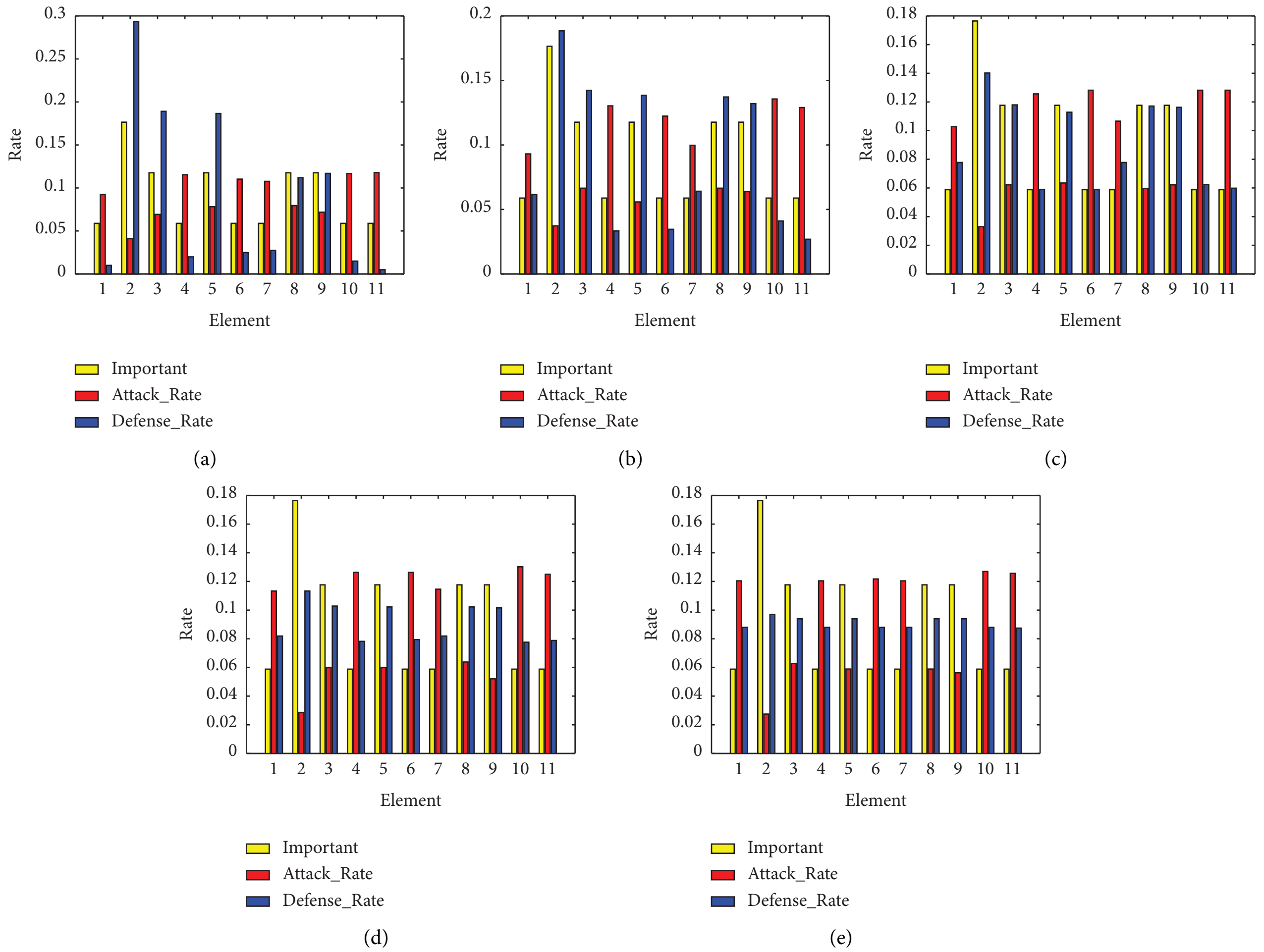
5.4. Strategies of Attacker and Defender with Different Defense Resources.

In this section, the attack resource is fixed as 4, and the strategy selection of the attacker and the defender is discussed when the defense resource is 2, 4, 6, 8, and 10, respectively. In order to prevent the chance of the results, each group of experiments was carried out 10 times, and then the mean value was taken as the experimental result. After using ncPSO to calculate the mixed-strategy Nash equilibrium of both players of the game, we map it to the probability of attacking and defending each element to analyze the attack and defense behaviors. The experimental results are shown in Figure 5.

From subfigures a, b, and c, it can be seen that when there are fewer defensive resources, the defender will spend more resources on elements of higher importance. The attacker will attack less important elements to avoid the defense of defender to obtain a higher profit. As can be seen from subfigures d and e, when defense resources are sufficient, the defender will evenly allocate defense resources to each element. Because the attacker does not know the resource allocation of the defender, he will guess that the defender allocates most of the resources to the elements of high importance, so the attacker will still allocate the attack resources to the elements of lower importance.

Table 7: The losses of defender under different attack and defense resources.

		Defense resources									
		2		4		6		8		10	
		Average	Std	Average	Std	Average	Std	Average	Std	Average	Std
Attack resources	2	−2.1073	0.0296	−1.5819	0.0145	−1.1569	0.0084	−0.7155	0.0021	−0.2417	0.0003
	4	−3.3408	0.0121	−2.7001	0.0091	−2.1184	0.0030	−1.3748	0.0011	−0.4854	0.0001
	6	−4.2067	0.0119	−3.5259	0.0040	−2.8793	0.0026	−1.9765	0.0011	−0.7312	0.0002
	8	−4.7108	0.0068	−4.1233	0.0043	−3.5137	0.0047	−2.4765	0.0017	−0.9691	0.0002
	10	−4.9809	0.0001	−4.7562	0.0002	−4.0934	0.0003	−3.0077	0.0018	−1.2180	0.0003

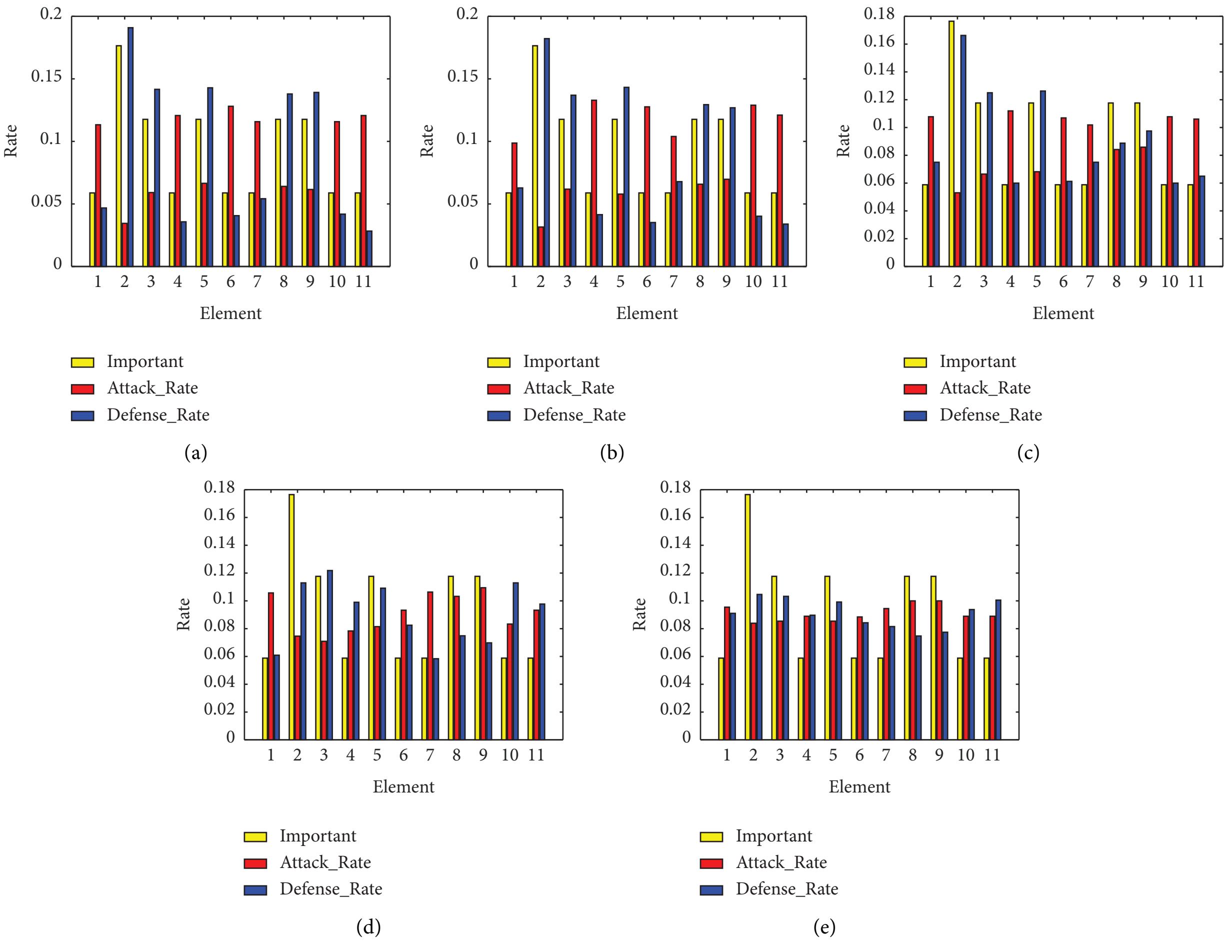


(a) (b) (c) (d) (e)

Figure 5: Experimental results under different defense resources. (a) Defense resources = 2. (b) Defense resources = 4. (c) Defense resources = 6. (d) Defense resources = 8. (e) Defense resources = 10.

5.5. Strategies of Attacker and Defender with Different Attack Resources. In this section, the defense resource is fixed as 4, and the strategy selection of the attacker and the defender is discussed when the attack resource is 2, 4, 6, 8, and 10, respectively. In order to prevent the chance of the results, each group of experiments was carried out 10 times, and then the mean value was taken as the experimental result. After using ncPSO to calculate the mixed-strategy Nash equilibrium of both players of the game, we map it to the probability of attacking and defending each element to analyze the attack and defense behaviors. The experimental results are shown in Figure 6.

As can be seen from subfigures a, b, and c, when there are few attack resources, the defender will allocate more defense resources to the elements with high importance, so that the attacker will attack the elements that allocate less defense resources to obtain profit successfully. As can be seen from subfigures d and e, when there are many attack resources, the attacker no longer considers the strategy choice of defender, but randomly attacks each element. In this case, the defender



(a)

(b)

(c)

(d)

(e)

Figure 6: Experimental results under different attack resources. (a) Attack resources = 2. (b) Attack resources = 4. (c) Attack resources = 6. (d) Attack resources = 8. (e) Attack resources = 10.

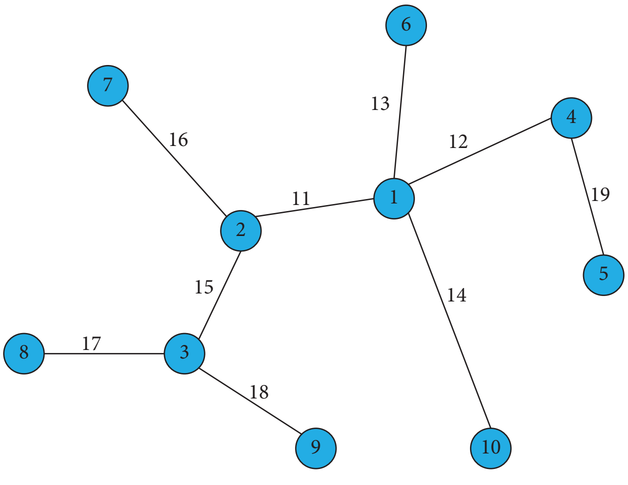


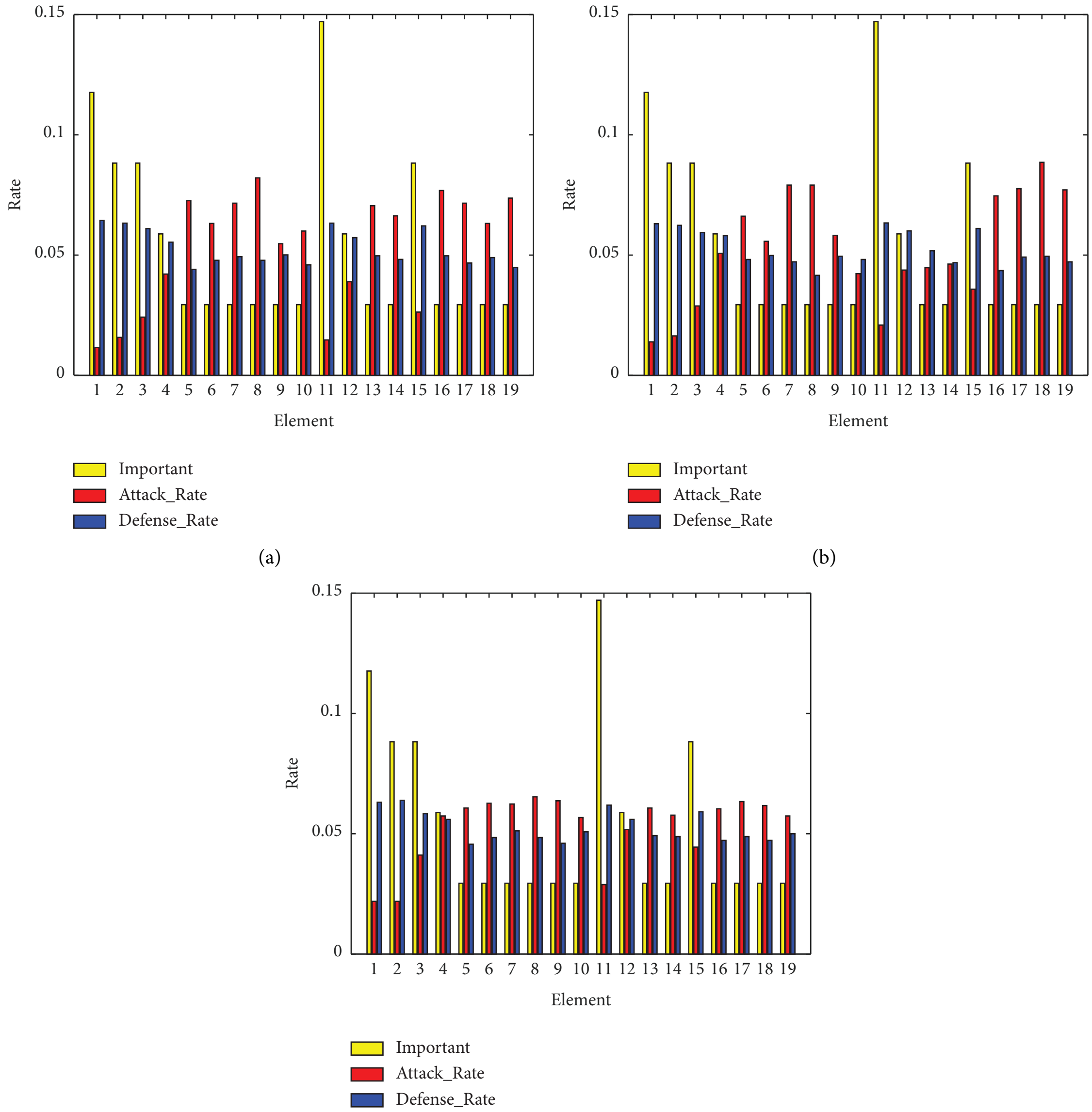
Figure 7: The graph of this simulation experiment.

also distributes defense resources equally to defense each element.

5.6. Strategies of Attacker and Defender with Different Attack Resources in Another Network. In this subsection, the network scale is expanded, and a simulation experiment with 10 nodes and 19 elements is carried out. The experimental diagram is shown in Figure 7. In this experiment, the defense resources are set to 15, and the attack resources are set to 5, 10, and 15, respectively. When the attack resources are set to 5, 10, and 15, the number of strategies from attacker is shown in Table 8. Compared with the network graph in Figure 4, although Figure 8 only

Table 8: The number of strategies under different attack resources.

	5	10	15
The number of strategies	$C_{19}^{5} = 11628$	$C_{19}^{10} = 92378$	$C_{19}^{15} = 3876$



(a)

(b)

(c)

Figure 8: Experimental results under different attack resources. (a) Attack resources = 5. (b) Attack resources = 10. (c) Attack resources = 15.

increases a little network size, the attack and defense strategies increase a lot. The ncPSO is used to solve the Nash equilibrium of the game, and the probability of each element being attacked and defended is calculated. The average of 10 experimental results is taken to ensure the reliability of the experiment. The experimental results are shown in Figure 8.

As can be seen from the figure, the importance of the communication link cannot be ignored, and the importance of the communication link is not lower than that of the communication equipment. Figure 8 shows that when the defense resource is 15 and the attack resource is 5, the defender will allocate resources evenly to deal with the attacks of attacker, and the attacker predicts that defender will allocates more resources to protect more important elements, so attacker will attack less important elements to obtain profit. When the defense resource is 15 and the attack resource is 15, the defender will select elements with higher importance to strengthen protection to reduce losses, and the attacker chooses the element that the defender allocates less defense resources to attack to maximize the benefit of benefit (see Table 9).

6. Conclusion

5G heterogeneous network of CPS is a more intelligent and open network system based on software defined network (SDN) and network function virtualization (NFV). The macro analysis of hacking behavior through game theory is an effective method to prevent hacking attacks. Therefore, we established a system model and a game model based on 5G heterogeneous networks of CPS, respectively. The solution of mixed-strategy Nash equilibrium in game models is the most important part of analyzing attack and defense behaviors. A ncPSO is proposed to solve the mixed-strategy Nash equilibrium and analyze the strategy choices of attacker and defender under different attack and defense resources through simulation experiments. Experiments demonstrate the effectiveness and superiority of the proposed ncPSO. The research in this paper provides a feasible macro analysis for defenders to defend against attacks of hacker.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This project was funded by the National Natural Science Foundation of China, under No. 61932005.

References

[1] S. Wijethilaka, M. Wijethilaka, and M. Liyanage, "Survey on network slicing for internet of things realization in 5g networks," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 957–994, 2021.

[2] F Qamar, M. H. D. N. Hindia, K Dimyati et al., "Interference management issues for the future 5g network: a review," *Telecommunication Systems*, vol. 71, no. 4, pp. 627–643, 2019.

[3] H. Hui, Y. Ding, Q Shi, F Li, Y. Song, and J. Yan, "5g network-based internet of things for demand response in smart grid: 5G network-based Internet of Things for demand response in smart grid: A survey on application potential survey on application potential," *Applied Energy*, vol. 257, Article ID 113972, 2020.

[4] S. J. Yang, Y. M. Pan, L. Y. Shi et al., "Millimeter-wave dual-polarized filtering antenna for 5g application," *IEEE Transactions on Antennas and Propagation*, vol. 68, no. 7, pp. 5114–5121, 2020.

[5] M. Zhao, "Research on the effect of iot wireless network technology on the educational management of Research on the Effect of IOT Wireless Network Technology on the Educational Management of China's Universitieshina's universities," *Security and Communication Networks*, vol. 2022, Article ID 9405897, 9 pages, 2022.

[6] M. A. Ouamri, M. E. Oteşteanu, A Isar, M.-E. Azni, A. Isar, and A. Mohamed, "Coverage, handoff and cost optimization for 5g heterogeneous network," *Physical communication*, vol. 39, Article ID 101037, 2020.

[7] Y. Xu, G. Gui, H. Gacanin, F. Adachi, H. Gacanin, and F. Adachi, "A survey on resource allocation for 5g heterogeneous networks: A Survey on Resource Allocation for 5G Heterogeneous Networks: Current Research, Future Trends, and Challengesurrent research, future trends, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 668–695, 2021.

[8] J. Arroyo, A. Athreya, J. Cape et al., "Inference for multiple heterogeneous networks with a common invariant subspace," *Journal of machine learning research: JMLR*, vol. 22, no. 141, pp. 1–49, 2021.

[9] M. Krishna, S. Mohan Babu Chowdary, P. Nancy, and V. Arulkumar, "A survey on multimedia analytics in security systems of cyber physical systems and iot," in *Proceedings of the 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)*, pp. 1–7, IEEE, Trichy, India, October 2021.

[10] D. Almeida, L. F. Da Rosa Righi, R. Rodrigues et al., "Cyber-physical systems architectures for industrial internet of things applications in industry 4.0: Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review literature review," *Journal of Manufacturing Systems*, vol. 58, pp. 176–192, 2021.

[11] M. A. Hasnat, S. T. Ahmed Rumee, M. A. Razzaque, and M. Mamun-Or-Rashid, "Security study of 5g heterogeneous network: current solutions, limitations & future direction," in *Proceedings of the 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, pp. 1–4, IEEE, Cox'sBazar, Bangladesh, February 2019.

[12] Y. Wu, A. Khisti, C. Xiao et al., "A survey of physical layer security techniques for 5g wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, 2018.

[13] B. Jia, X. Zhang, J. Liu et al., "Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in iiot," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 4049–4058, 2022.

[14] M. Min, L. Xiao, C. Xie et al., "Defense against advanced persistent threats in dynamic cloud storage: Defense Against Advanced Persistent Threats in Dynamic Cloud Storage: A Colonel Blotto Game Approach colonel blotto game approach," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4250–4261, 2018.

[15] K. Wang, L. Yuan, T. Miyazaki et al., "Jamming and eavesdropping defense in green cyber–physical transportation systems using a stackelberg game," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, pp. 4232–4242, 2018.

[16] L. Xinlong, C. Zhibin, and Z. Chen, "Ddos attack detection by hybrid deep learning methodologies," *Security and*

Communication Networks, vol. 2022, Article ID 7866096, 7 pages, 2022.

[17] F. Chaoqi, G. Yangjun, Z. Jilong, S. Yun, Z. Pengtao, and W. Tao, "Attack-defense game for critical infrastructure considering the cascade effect," *Reliability Engineering & System Safety*, vol. 216, Article ID 107958, 2021.

[18] H.-W. Zhang, L. I. Tao, and S.-R. Huang, "Network defense decision-making method based on attack-defense differential game," *ACTA ELECTONICA SINICA*, vol. 46, no. 6, p. 1428, 2018.

[19] B. Schneier, "Artificial intelligence and the attack/defense balance," *IEEE security & privacy*, vol. 16, no. 2, p. 96, 2018.

[20] H. Wu, J. Fan, C. Lai, and J. Liu, "Website defense strategy selection method based on attack-defense game and Monte Carlo simulation," *Journal on Communications*, vol. 39, no. 8, p. 48, 2018.

[21] Y. Li, Y. Deng, Y. Xiao, J. Wu, Y. Xiao, and J. Wu, "Attack and defense strategies in complex networks based on game theory," *Journal of Systems Science and Complexity*, vol. 32, no. 6, pp. 1630–1640, 2019.

[22] L. Leneutre, J. Chen, and L. Jean, "A game theoretical framework on intrusion detection in heterogeneous networks," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 2, pp. 165–178, 2009.

[23] X. Liu, B. Cui, J. Fu et al., "Secure data publishing of private trajectory in edge computing of iot," *Security and Communication Networks*, vol. 2022, Article ID 2045586, 14 pages, 2022.

[24] Q. Xu, Z. Su, Q. Zheng, M. Luo, B. Dong, and K. Zhang, "Game theoretical secure caching scheme in multihoming edge computing-enabled heterogeneous networks," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4536–4546, 2019.

[25] Y. Sun, Z. Tian, M. Li et al., "Automated attack and defense framework toward 5g security," *IEEE Network*, vol. 34, no. 5, pp. 247–253, 2020.

[26] T. Olivier, Y. Hayel, C. Kamhoua, and D. Gabriel, "Game theoretic modeling of cyber deception against epidemic botnets in internet of things," *IEEE Internet of Things Journal*, vol. 9, 2021.

[27] R. O. O. Adeogun, "A novel game theoretic method for efficient downlink resource allocation in dual band 5g heterogeneous network," *Wireless Personal Communications*, vol. 101, no. 1, pp. 119–141, 2018.

[28] Z.-L. Chang, C.-Y. Lee, C.-H. Lin, C.-Y. Wang, and H.-Y. Wei, "Game-theoretic intrusion prevention system deployment for mobile edge computing," in *Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, IEEE, Madrid, Spain, December 2021.

[29] F. He, J. Zhuang, N. S. V. Rao, J. Zhuang, and N. S. V. Rao, "Discrete game-theoretic analysis of defense in correlated cyber-physical systems," *Annals of Operations Research*, vol. 294, no. 1-2, pp. 741–767, 2020.

[30] M. Kim, "Game theoretic approach of eavesdropping attack in millimeter-wave-based wpans with directional antennas," *Wireless Networks*, vol. 25, no. 6, pp. 3205–3222, 2019.

[31] Y. Li, Y. Xiao, Y. Li, J. Wu, Y. Li, and J. Wu, "Which targets to protect in critical infrastructures-a game-theoretic solution from a network science perspective," *IEEE Access*, vol. 6, pp. 56214–56221, 2018.

[32] W. Jiang, B. X. Fang, Z. H. Tian, H. L. Zhang, Z. Tian, and H. Zhang, "Evaluating Network Security and Optimal Active Defense Based on Attack-Defense Game Model," *Chinese Journal of Computers*, vol. 32, no. 4, pp. 817–827, 2009.

[33] Q. Leng, Y. Yang, R. Pan, H. Yang, R. Pan, and H. Hu, "Research of complete information static game model for software manufacturer, white hats and black hats," *Procedia Computer Science*, vol. 131, pp. 832–840, 2018.

[34] A. Attiah, M. Chatterjee, and C. C. Zou, "A game theoretic approach to model cyber attack and defense strategies," in *Proceedings of the 2018 IEEE International Conference on Communications (ICC)*, pp. 1–7, IEEE, Kansas, MO, USA, May 2018.

[35] W. Wang and B. Zeng, "A two-stage deception game for network defense," in *Proceedings of the International conference on decision and game theory for security*, pp. 569–582, Springer, Seattle, WA, USA, October 2018.

[36] K. Ferguson-Walter, S. Fugate, J. Mauger, and M. Major, "Game theory for adaptive defensive cyber deception," in *Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security*, pp. 1–8, Nashville, TN, USA, April 2019.

[37] S. Shen, Y. Li, H. Xu, Q. Cao, H. Xu, and Q. Cao, "Signaling game based strategy of intrusion detection in wireless sensor networks," *Computers & Mathematics with Applications*, vol. 62, no. 6, pp. 2404–2416, 2011.

[38] J. Kennedy and E. Russell, "Particle swarm optimization,"vol. 4, pp. 1942–1948, in *Proceedings of the ICNN'95-international conference on neural networks*, vol. 4, pp. 1942–1948, IEEE, Perth, WA, Australia, November 1995.

[39] J. R. Sampson, *Adaptation in Natural and Artificial Systems*, MIT Press, Cambridge, MA, USA, 1976.

[40] S. Mirjalili, A. Lewis, and A. Lewis, "The whale optimization algorithm," *Advances in Engineering Software*, vol. 95, pp. 51–67, 2016.

[41] A. Hatamlou, "Black hole: Black hole: A new heuristic optimization approach for data clustering new heuristic optimization approach for data clustering," *Information Sciences*, vol. 222, pp. 175–184, 2013.

[42] X. S. Yang, X.-S. He, and X. He, "Bat algorithm: literature review and applications," *International Journal of Bio-Inspired Computation*, vol. 5, no. 3, pp. 141–149, 2013.

[43] S. M. Mirjalili, S. Z. Mirjalili, S. Saremi, and S. Mirjalili, "Sine cosine algorithm: theory, literature review, and application in designing bend photonic crystal waveguides," *Nature-inspired optimizers*, vol. 811, pp. 201–217, 2020.

[44] C. Y.-Y. Lee, "Mixed-strategy nash equilibrium in data envelopment analysis," *European Journal of Operational Research*, vol. 266, no. 3, pp. 1013–1024, 2018.

[45] H. J. Hilhorst, C.-J. Appert-Rolland, and C. Appert-Rolland, "Mixed-strategy nash equilibrium for a discontinuous symmetric n-player game," *Journal of Physics A: Mathematical and Theoretical*, vol. 51, no. 9, Article ID 095001, 2018.

[46] F. Neri, E. Mininno, G. Iacca, E. Mininno, and G. Iacca, "Compact particle swarm optimization," *Information Sciences*, vol. 239, pp. 96–121, 2013.

[47] B. C. Arnold, *Pareto Distribution*, pp. 1–10, Wiley, Hoboken, NJ, USA, 2014.