Hindawi
Mathematical Problems in Engineering
Volume 2020, Article ID 9302619, 12 pages
https://doi.org/10.1155/2020/9302619

Research Article

Efficient Defense Decision-Making Approach for Multistep Attacks Based on the Attack Graph and Game Theory

Jing Liu, Yuchen Zhang, Hao Hu, Jinglei Tan, Qiang Leng, and Chaowen Chang

Zhengzhou Information Science and Technology Institute, Zhengzhou 450001, China

Correspondence should be addressed to Yuchen Zhang; 2744190810@qq.com

Received 19 August 2019; Revised 27 April 2020; Accepted 7 July 2020; Published 11 August 2020

Academic Editor: Francesca Vipiana

In the multistep attack scenario, each rational attack-defense player tries to maximize his payoff, but the uncertainty about his adversary prevents him from taking the favorable actions. How to select the best strategy from the candidate strategies to maximize the defense payoff becomes the core issue. For this purpose, the paper innovatively designs a game theory model from the point of network survivability in combination with the attribute attack graph. The attack graph is created based on the network connectivity and known vulnerabilities using the MulVAL toolkit, which gives the full view of all the known vulnerabilities and their interdependence. Then, we use the attack graph to extract attack-defense actions, candidate attack-defense strategies, attack-defense payoffs, and network states, as well as other game modeling elements. Afterwards, the payoffs of attack-defense strategies are quantified by integrating attack-defense strength and network survivability. In addition, we input the above elements into the game model. Through repeated learning, deduction, and improvement, we can optimize the layout of defense strategies. Finally, the efficient strategy selection approach is designed on the tradeoff between defense cost and benefit. The simulation of attack-defense confrontation in small-scale LAN shows that the proposed approach is reliable and effective.

1. Introduction

With the expansion of network scale as well as the increase of complexity and the continuous development of attack technology, it is impossible to absolutely prevent the network from being attacked. A large number of network key service nodes may meet the network attack, and the defender should provide enough network services to meet the normal operation of the network through conducting defense strategies. Therefore, the strategy selecting both sides of attack-defense starts around the survivability of the network. For the defender, the survivability of the network is the key to analyze the security and effectiveness of the defense strategy.

The purpose of the attack graph [1–5] is to analyze the attack-defense actions of the network through nodes and edges in the graph. Attribute attack graph regards the condition or attribute of the network as a node in the attack graph. When studying network security, it can accurately depict an event as a node in the network. Attribute attack graph has become the main method of mitigating network security in recent years [6–8]. In this paper, we propose a selection approach of optimal strategy for multistep attacks using the attack graph and game theory. In detail, the related attack-defense elements are extracted and taken into the game model for defense strategy deduction. We mainly focus on the continuous decision-making in the process of attack-defense dynamic confrontation. With invasion going, the attacker masters more defense information and can find a better attack path. Accordingly, the defender can also adjust the related defense strategy based on the attack path predictions. In contrast to other models, the proposed model guides the generation and optimization of the defense strategy during attack-defense adversary.

The main contributions are as follows:

(1) The attack-defense model for defense decision-making using the dynamic game theory is constructed. In the multistep attack scenario, attack-defense has the characteristics of collaborative

evolution. The proposed model comprehensively considers the network environment and attack-defense security mechanism information, which can accurately reflect the dynamic adversary process of attack and defense in the multistep attack scenario. Compared with the previous decision-making models based on the finite state machine, cybernetics, expert system, case reasoning, impact network, etc., which do not fully consider defense information and are only applicable to the analysis and statistics of simple attack-defense laws, the proposed dynamic attack-defense game model has better capability of interpretability. It can depict the adversary evolution process of complex multistep attack-defense scenarios and continuously guide the optimization and arrangement of defense strategies in the process of dynamic game between the two sides of attacker and defender. Hence, the proposed model enhances the defense perspectiveness and decision-making continuity.

(2) The improved strategy payoff calculation method is put forward. Existing methods only consider the direct security payoff, which affects the accuracy of strategy selection. In fact, the defense of multistep attack is often difficult to achieve by relying only on a single strategy, while it requires the combination of various defense strategies to maximize the comprehensive defense payoff. Therefore, the accuracy of strategy payoff quantification is significant. This paper further considers the indirect payoffs brought by legal blame and counterattacks (see in Section 4). For example, the defender can trace the attacks by collecting the attack evidences, including the port scanning time, port number, source IP address, and destination IP address, so as to obtain the indirect payoff through attack deterrence. The indirect payoff can lead to the increase of defense payoff and decrease of attack payoff. In addition, through adjusting the game payoff values, we can analyze the effect of defense strategy selection. Our model avoids the aggravation of attack-defense confrontation, enhances the ability of network security governance, and improves the flexibility and accuracy of defense decision-making.

(3) The optimal defense strategy selection approach for multistep attacks is designed. The complex attack-defense scenario has the characteristics of multistate and multistep. With the penetration of network attack, the information gained by the attacker will gradually increase. Based on the new information, the attacker can implement new attack strategies. Accordingly, the defender needs to adjust the defense strategies in different attack stages to improve the defense effect. To depict the interaction process of the attacker and defender, we employ the dynamic game theory to illustrate the decision interaction and behavior evolution of two sides. By calculating the game equilibriums in different game stages, we can calculate the optimal defense strategy arrangements in each moment. It enhances the pertinence and reliability of defense decision-making.

The rest of this paper is organized as follows. Section 2 describes the related work. Section 3 designs the game model for network survivability. The general strategy payoff analysis is provided in Section 4. Section 5 performs specific attack strategy payoff analysis towards multistep attacks including the single-step attack payoff and multistep attack payoff. Section 6 provides the analyses of defense payoff and best strategy selection. The experiments and analyses are demonstrated in Section 7. Finally, we conclude this paper in Section 8.

2. Related Works

In order to maintain the normal operation of the network, most network security managers need to take a series of defense measures to make the network survive. In recent years, game theory has gradually become a mainstream method to study network security defense decision-making. For example, Wang et al. [9] studied the survivability of the network in the process of attack-defense and quantitatively analysed the security states of the network. Chen et al. and Wang et al. [2, 10] built a dynamic network attack-defense game model to carry out network defense decision-making. Shen et al. [11] regarded the behavior of selecting the attack-defense strategy as a multistage game process and dynamically analyzed the impacts of selecting the network security strategy on the network system. Similar studies include the following. The repeated attack-defense game theory is used in the wireless network for resisting DDoS attack [12]. The differential attack-defense game model is constructed in [13], and the calculation method of saddle-point strategy and the optimal strategy selection algorithm are given. Tan et al. [14] quantified the benefits of both sides of attacker and defender based on the bounded rational game model and studied the dynamic and evolution of both sides of network attack-defense. However, in the above research, network state change is regarded as the power of the game. The best defense strategy cannot be explored well.

We use the game theory to study network security, in which the game information is a key problem. Some scholars use the complete information game model. For example, Lye and Wing [15] defined the complete information static game model with the recovery time needed after the network is invaded as the payoff. In [16], the theory of complete information dynamic game is used to convert the network attack graph into the network game tree to study the active defense. In the network, there is information asymmetry between the attacker and the defender, and both sides cannot fully understand each other, which limits the application of the complete information game model. In order to solve the problem of incomplete game information, Lee et al. [17] established a static game model of incomplete information and analyzed the vulnerability risk. However, only one static game is used to predict the invasion behavior, that is, the attacker will not change the invasion strategy in the invasion

process. In reality, the attacker often has limited information collection ability and cannot fully understand the target network before the invasion, so he can only make a local high payoff attack strategy based on the existing information. With the development of intrusion, the attacker may have a further understanding of the target network and will find a higher payoff intrusion path and then constantly adjust the attack strategy. Hence, the actual intrusion is composed of different stages, and the attacker in different stages of the target network information is different. The attacker in each stage will adjust the strategy to get more payoffs. The dynamic game of incomplete information considers the factors of information update and strategy adjustment of the attacker. For example, the attack-defense signal game model is established, and the algorithm of selecting the optimal defense strategy is designed by Liu et al. [18]. The attacker can adjust the attack strategy through receiving the defense signals released by the defender, but the approach is limited to the bounded defense signals of the attacker. Considering that the lack of vulnerability information may make errors in the prediction of the attack path, the defender needs to solve two key problems to accurately select the best strategy. The first problem is information update. The defender needs to predict the vulnerability information of the attacker in different attack stages. The second problem is strategy adjustment. When the attacker obtains the new information of the target network, he will adjust his strategy to get more payoffs. The defender needs to predict the strategy adjusted by each step of the attacker in order to get more defense payoff.

For this aim, this paper proposes a method of dynamic game strategy analysis about network survivability based on the attribute attack graph. We quantify attack-defense action strength as well as provide suggestions for network security administrators to implement single-stage and multistage defense measures. Firstly, we use a matrix to depict the IP address, attack action, and attack path of network nodes. Secondly, we quantify the impact of the attack-defense strategy on the survivability of the network system. Thirdly, according to different payoffs of candidate attack-defense strategies, we calculate the optimal defense strategy and provide more understandable and reasonable defense decision for network security mitigation.

3. Construction of the Network Survivability Game Model

The process of network attack-defense is a multistage game process. In each stage, both sides of attacker and defender select and execute attack-defense actions and get immediate returns. The cumulative sum of immediate returns in each stage is the total gains of both sides in the whole process of confrontation. The maximization of total payoff is the goal of the game between the attack-defense sides. The game process can be described in Figure 1(a). In each attack step, both attackers and defenders detect the current network state and select attack-defense actions according to the state and the adversary's former action. The network system transfers from one state to another under the joint action of attack-defense. The steps of attack-defense interaction are as follows:

(1) Both sides of attacker and defender detect the current network state at time t firstly

(2) Both sides of attacker and defender implement their attack-defense strategies one after the other according to their expected strategy payoff functions

(3) Both sides of attacker and defender calculate their real payoffs after performing the strategies

(4) The network system transfers to the next security state at time t+1

(5) Steps (1)–(4) are repeated until the attack-defense reaches a balance state at time $t + k$

The network state transition during the attack process is shown in Figure 1(b). The network state is denoted as $s_i = \langle \text{host, privilege} \rangle$, where host is the identity of certain host in the network. Privilege = {none, user, root} indicates that the attacker does not have any privilege, has normal user privilege, and has administrator privilege, respectively. $\tau = S \times S$ is the set of state transition relationships, which are determined by host information, vulnerability information, network topology, network connectivity, and attack-defense mechanism. Because of the non-cooperation and conflicted-goal features of the attacker and defender, the confrontation leads to the transition of the network state. The attacker's goal is to gain more advanced network access. The defense's goal is to prevent illegal access.

The game model includes players, attack-defense strategies, attack-defense payoffs, and other security elements. On the basis of measuring security states of network survivability, we add the network survivability measures, and the payoff values of attack-defense strategies on network security are quantified. The definition of the dynamic survivability game model is given below.

Definition 1. Network survivability game model (NSGM) is represented by 7-tuples, NSGM = $(N, S, V, \text{SI}, g, U, f)$.

(1) $N = (N_A, N_D)$ represents the set of players in the attack-defense game; N_A and N_D represent the attacker and the defender, respectively.

(2) $S = (S_A, S_D)$ represents the payoff matrix of the attack-defense strategy:

$$S_A = \begin{bmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{bmatrix}, \quad S_D = \begin{bmatrix} d_{1k} & \cdots & d_{1k} \\ \vdots & \ddots & \vdots \\ da_{n1} & \cdots & d_{nk} \end{bmatrix}. \tag{1}$$

n denotes the number of nodes in the attack path, and the order of attack is $1 \longrightarrow n$. m denotes the maximum number of attack strategies when

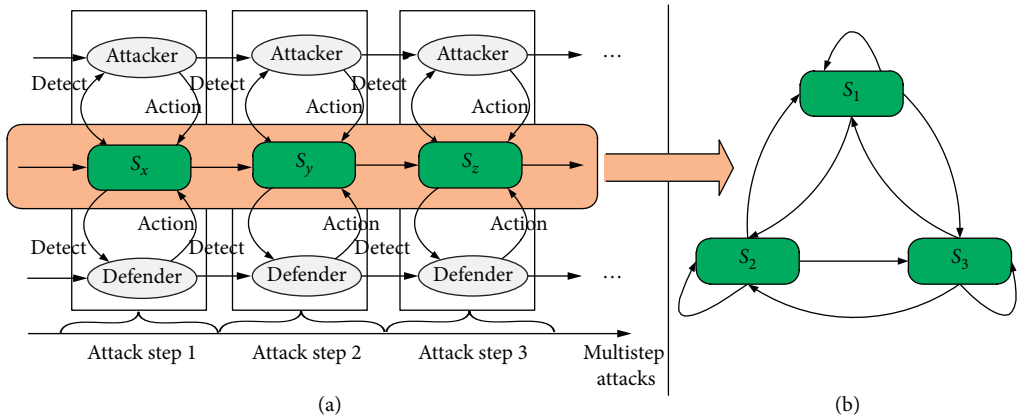

Figure 1: The process of network attack-defense. (a) Attack-defense process of multistep attacks. (b) Network security state transition.

attacking n nodes, k denotes the maximum number of defense strategies of the defender against n nodes, and a_{ij} denotes the j-th attack strategy of the i-th node. Matrix element is 0 or 1, which indicates whether an attacker or defender selects the strategy. In order to promote the analysis of security strategies, the defense strategy vectors and attack strategy vectors of each node are given as $S_D = (\vec{d}_1, \vec{d}_2, \ldots, \vec{d}_n)^T$ and $S_A = (\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_n)^T$.

(3) Network survivability metric V is a quantitative value to measure whether a critical task can be accomplished or service continuity can be guaranteed when a network is compromised. In order to quantify the impact of attack-defense behavior on the network system, this paper uses the attack-defense action strength in Lincoln Laboratory Attack-Defense Behavior Database [19] to analyze the payoff of the attack-defense strategy on the system.

(4) $\mathrm{SI} = (\mathrm{SI}_A, \mathrm{SI}_D)$ is the strategy strength. SI_A and SI_D represent the strengths of attack and defense strategies, respectively; $\mathrm{SI} \in [0, 1]$.

$$V = \mathrm{SI}_D - \mathrm{SI}_A. \tag{2}$$

$V \in [0, 1]$ indicates that the network system is safe and has the capability to keep providing the necessary services. $V \in [-1, 0)$ indicates that the network system is in risk with low survivability and hard to provide the normal services.

(5) g denotes the function of attack-defense strategy selection. When an attacker invades the system, there is an attack vector $\vec{a}_i$ corresponding to the attack path. The attacker selects an element a_{ij} in the vector. For defenders, in order to maintain the security of the network system, when facing an attack, they need to react to the attack action. Therefore, a set of defense strategies is obtained. When the attacker selects the attack strategy a_{ij}, the defender selects related element of the defense strategy set to make $V \geq 0$. Then, there exists a function as follows:

$$\mathrm{Sup}\, S_{D_i} = g\left(S_A\left(a_{ij}\right)\right). \tag{3}$$

The defense strategy set is indicated by the upper bound expression in the set. Formula (3) denotes that when an attacker selects an attack strategy a_{ij}, in order to maintain the security of the network system, the defense measures can only be selected in $\mathrm{Sup}\, S_{D_i} \in S_{D_i}(\vec{d}_i)$, where $S_{D_i}(\vec{d}_i)$ represents the set of strategies for defending node i.

(6) $U = (U_A, U_D)$ denotes the corresponding payoff matrix of the strategy selected by the attacker and defender.

$$U_A = \begin{bmatrix} u_{a_{11}} & \cdots & u_{a_{1m}} \\ \vdots & \ddots & \vdots \\ u_{a_{n1}} & \cdots & u_{a_{nm}} \end{bmatrix},$$
$$U_D = \begin{bmatrix} u_{d_{11}} & \cdots & u_{d_{1k}} \\ \vdots & \ddots & \vdots \\ u_{a_{n1}} & \cdots & u_{a_{nk}} \end{bmatrix}. \tag{4}$$

U_A and $U_D$represent attack and defense payoff matrix, respectively. Attack payoff U_{aij} is the profit of attacking node i when adopting defense strategy j. Defense payoff $U_{di\,j}$ is the profit of taking defense strategy j to defend attack strategy i.

(7) f is the payoff function to calculate the attack-defense payoff matrices. When the attacker takes the attack measure j on the node i of the system, the defense measure of the defender is $\mathrm{Sup}\, S_{D_i}$. Then, we have $f_A = u_{a_{ij}}$ and $f_D \in \mathrm{Sup}\, U_{D_i}$.

The attribute attack graph is created based on the network connectivity and known vulnerabilities using the MulVAL toolkit [20] in this paper, which gives the full view of all the known vulnerabilities and their interdependence. Then, we use the attack graph to extract attack-defense actions, candidate attack-defense strategies, attack-defense

payoffs, network states, and other game modeling elements. Afterwards, we input the above elements into the game model. Through repeated learning, deduction, and improvement, the game model can output the optimal defense strategy.

4. Payoff Analyses of Attack-Defense

The quantitative calculation of the strategic payoff of both sides of the attacker and defender is the basis of the subsequent game analysis. It directly affects the results of the strategy selection. Therefore, it is necessary to quantify the payoffs of the strategies of both sides accurately. Present quantitative methods are not comprehensive enough. On the basis of summarizing the previous work, this paper puts forward an improved quantitative index set of attack-defense strategy payoff shown in Figure 2, which explains how to obtain the quantitative value of system cost and benefit in detail.

4.1. Payoff Quantification of Attack

4.1.1. Attack Strategy Cost. Attack cost (AC) refers to the cost of using the attack strategy, which includes resource consumption and camouflage cost.

In the dynamic game scenario, if the attacker fails to achieve the goal, he will take measures to conceal his attack behavior so that the defender cannot accurately identify the attack. The cost of attack camouflage indicates spending of concealing attack behaviors.

Definition 2. AOC (attack operation cost) is defined as the cost of system resources and attack skills consumed by an attacker to launch an attack. Based on CVSS evaluation, we select three parameters, vulnerability exploiting mode, attack complexity, and vulnerability availability, to evaluate the attack operation cost which is given as the following formula:

$$\mathrm{AOC} = \left(\omega_{\mathrm{Av}} \times V\_\mathrm{Av} + \omega_{\mathrm{Ac}} \times V\_\mathrm{Ac} + \omega_{\mathrm{Exp}} \times V\_\mathrm{Exp}\right) \times \rho^{i-1}, \tag{5}$$

V_Av, V_Ac, and V_Exp are the assessment values of the vulnerability utilization mode, complexity, and availability, and ω_{Av}, ω_{Ac}, and ω_{Exp} are weights, $\omega_{\mathrm{Av}} + \omega_{\mathrm{Ac}} + \omega_{\mathrm{Exp}} = 1$; ρ is the cost attenuation factor of attack operation, which means that the cost will be reduced if the vulnerability has been attacked again. i is the number of times that the vulnerability has been attacked.

V_Av, V_Ac, and V_Exp are measured according to the CVSS corresponding item. The level and value of specific V_Av and V_Ac can be obtained from the NVD database. The level and value of V_Exp are obtained by searching the public Bugtraq number of vulnerability.

Definition 3. ACC (attack configuration cost) is the index to describe the cost of attack camouflage in attack-defense interchange. Attacker often conceals his attack purpose and leads the defender implement the wrong defense. In order to achieve this purpose, attackers often need to take multiple types of attacks in parallel. Therefore, the camouflage cost is the sum of the attack operation cost (AOC) of the attack actions taken to camouflage attacks.

4.1.2. Attack Strategy Benefit

Definition 4. AB (attack benefit) indicates the benefits gained by the attacker in the attack. According to the benefit type, we can divide into direct benefit and indirect benefit.

Definition 5. AL (attack lethality) indicates the inherent damage degree of a certain type of attack. The attack lethality should be related to the attack cost. The higher the lethality is, the higher the attack cost is. Therefore, different types of attackers should adopt different lethal atomic attack strategies. For example, strong attackers tend to adopt high lethal atomic attack strategies.

Definition 6. D cost (damage cost) indicates the loss of system resources caused by the attacks to the defender. The system loss can be quantified by criticality and security attribute damages. In this paper, the damage of security attributes can be divided into integrity cost, confidentiality cost, and availability cost. The damage of security attributes has a certain bias to the cost of each security attribute. From the three aspects of information integrity, confidentiality, and availability cost, denote as (P_i, P_c, P_v), where $P_i + P_c + P_v = 1$. The value of the security attribute cost can be evaluated by three levels by the following formula, where m is the number of attacked hosts:

$$\begin{aligned}\mathrm{D\,cost}(a) = \sum_{1}^{m} \mathrm{AL} \times \mathrm{criticality} \times \big(&\mathrm{I\,cost} \times P_i \\ &+ \mathrm{C\,cost} \times P_c + \mathrm{A\,cost} \times P_v\big).\end{aligned} \tag{6}$$

Definition 7. ADR (attack direct benefit) indicates the benefits that an attacker can get directly from the defender to make a successful attack. ADR is generally smaller than D cost. The system loss cost (D cost) can be regarded as the direct benefit of the attacker.

Definition 8. AIR (attack indirect benefit) is to the immediate benefit after a successful attack. The indirect benefit of the attack refers to the social loss that the defender may suffer in a period of time after the successful attack, such as the loss of users and the decline of service quality, which need to be calculated according to the environment and assessments.

4.2. Payoff Quantification of Defense

4.2.1. Defense Strategy Cost. According to the different ways that defense affects the system, defense cost (DC) can be divided into DDC (defense direct cost) and DIL (defense indirect loss). Compared with the traditional approaches, the index of defense indirect loss (DIL) is added, and the

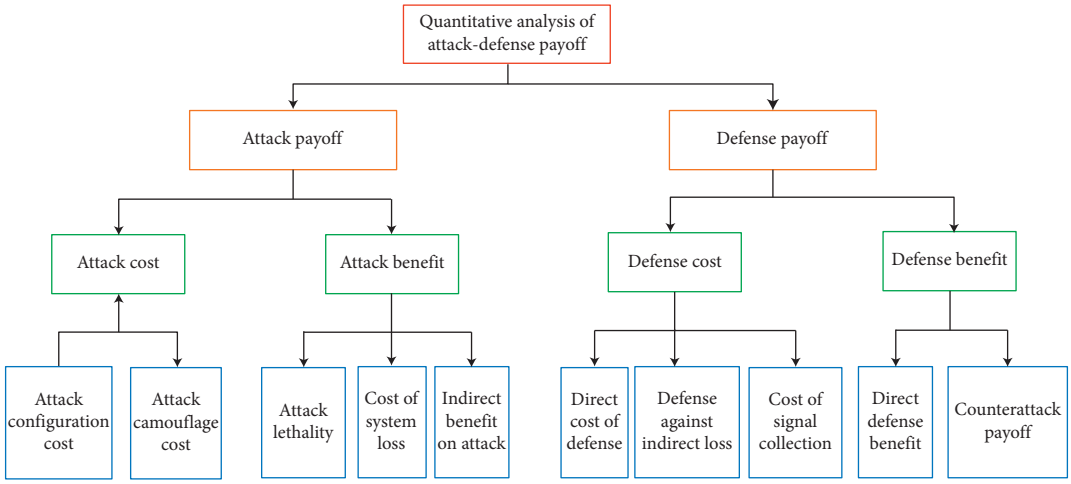

Figure 2: Quantitative index set of attack-defense strategy payoff.

quantitative process of defense direct cost is refined. Defense direct cost (DDC) is an adverse effect on the information system that may be caused by the defense strategy adopted by the defender. Among them, DDC can be expressed by the sum of operational cost, negative cost, and residual cost of the defense strategy and indirect loss of defense (negative value), namely,

$$\begin{aligned}\text{DDC} = {} & \text{O cost} + \text{N cost} + \text{R cost} = \text{O cost}(d) \\ & + \text{A cost} \times r(a,d) + \text{D cost}(a) \times \varepsilon(a,d).\end{aligned} \tag{7}$$

In the process of the attack-defense game, the defender needs to collect the signals released by the attacker, which also needs to consume a certain cost. Therefore, the cost of signal collection (SCC) is added to describe this cost. DDC is defined as follows:

$$\text{DDC} = \text{O cost} + \text{N cost} + \text{R cost} + \text{SCC}. \tag{8}$$

Definition 9. O cost (operation cost) indicates the system resources and time consumed by the defender when adopting relevant strategies. According to the complexity of defense operations, it can be divided into the following three levels:

(i) OL1 (low level of O cost): there is little impact on the information system during operation

(ii) OL2 (middle level of O cost): the resources of the information system are occupied for a long time

(iii) OL3 (high level of O cost): it takes a long time to operate the information system and takes up a lot of resources

According to the security threat assessment scenario, O cost can be given different relative values for quantification. For example, the O cost of OL1 can be 1–10, the O cost of OL2 can be 10–50, and the O cost of OL3 can be 50–100.

Definition 10. N cost (negative cost) is the cost of the information system abnormal operation caused by the defender's execution of relevant strategies. The calculation formula is N cost = A cost × $r(a, d)$, where $r(a, d)$ indicates the degree of negative impact of attack a on system availability with defense strategy d.

Definition 11. R cost (rest cost) is the impact or loss of the residual attacks on the information system after the defense strategy is adopted. It can be expressed as the residual coefficient R cost (a, d) = D cost $(a) \times e(a, d)$, where $\varepsilon(a, d)$ is the residual impact of attack a on the information system when the defender adopts strategy d and the attacker adopts strategy a.

Definition 12. DIL (defense indirect lost) is the social loss that the defender may suffer after being attacked for a period of time, such as the loss of users and the decline of service quality. Its value is the same as the IAR of indirect attack benefit (refer to the calculation of indirect attack benefit above).

Definition 13. SCC (signal collect cost) is defined to describe the cost of the defender monitoring the attacker's signal in the attack-defense game. The attacker's signal is mainly collected and processed by the IDS. Therefore, the cost of signal collection and monitoring is mainly measured by the amount of time and computer resources consumed by the IDS to collect, analyze, and process signals. The cost of signal collection can be quantified according to the amount of time and network resources.

(i) SL1: signal collection is only carried out at the beginning of the attack event, and analyzing and processing of the attack signal hold very little resources

(ii) SL2: signal collection is carried out at any time node of the attack event, and the signal should be analyzed and processed in the whole process of the event, which take up more resources

(iii) SL3: in a period of time, it is necessary to monitor the signal of several attacks, as well as to analyze and

process the signal in each event, which take up a lot of resources

According to the requirements of security threat assessment, specific values can be used to measure the cost of signal collection at different levels.

4.2.2. Defense Strategy Benefit. DR (defense benefit) indicates the benefits gained by the defender after adopting the defense strategy. To our best knowledge, no rest D cost is considered in existing methods, however, without considering the benefits of the defenders' counterattack. The metric deviates from the actual value. Our improved strategy measurement is as follows.

Definition 14. DDR (defense direct benefit) is the direct benefit obtained by the defender after adopting the defense strategy. It is expressed as a defense strategy against an attack, and the information system is free from loss, which is generally expressed by the cost of system loss, D cost.

Definition 15. CR (counterattack benefit) is the profit that the defender uses the information left by the attacker to trace and counterattack the attacker. It is generally believed that the higher the cost of defense, the more attention the defenders attach to defense and the more rewards they will get from counterattack. The profit on counterattack can be classified and quantified according to the defense cost as follows:

(i) CL1: defenders do not pay attention to information system security and invest less in defense and have low defense cost.

(ii) CL2: defenders pay attention to information system security and invest in defense generally.

(iii) CL3: defenders attach great importance to the security of the information system. They invest a lot in defense, and the cost of defense is high.

The security threat assessment scenario can use specific benefit value to measure the relative benefit of each level.

Therefore, we can get the payoff functions of attack-defense strategies as follows:

$$\begin{aligned} \text{attack strategy payoff} &= f(\text{AR}, \text{AC}), \\ \text{defense strategy payoff} &= f(\text{DR}, \text{DC}). \end{aligned} \tag{9}$$

The following are the equations of the payoff functions of attack-defense strategies in the game process. The cost and benefit of attackers are as follows:

$$\begin{aligned} \text{AC} &= -\text{ACC}, \\ \text{AR} &= \text{ADR} + \text{AIR} = \text{D cost} + \text{AIR}. \end{aligned} \tag{10}$$

The cost and benefit of defenders are

$$\begin{aligned} \text{DC} &= -\text{DDC} - \text{DIL} - \text{SCC}, \\ \text{DR} &= \text{DDR} + \text{CR}. \end{aligned} \tag{11}$$

The strategy payoffs of both sides are as follows:

$$\begin{aligned} U_A(A, D) &= \text{D cost} + \text{AIR} - \text{AOC} - \text{ACC}, \\ U_D(A, D) &= \text{DDR} + \text{CR} - \text{DDC} - \text{DIL} - \text{SCC}. \end{aligned} \tag{12}$$

The sum of the profits of the attacker and defender in the attack-defense game is as follows, respectively:

$$\begin{aligned} U_A(A, D) + U_D(A, D) &= 2\text{D cost} - \text{DDC} - \text{AOC}, \\ U_A(A, D) + U_D(A, D) &= 2\text{D cost} - \text{DDC} - \text{AOC} \\ &\quad - \text{ACC} - \text{SCC}. \end{aligned} \tag{13}$$

Suppose in a network game scenario, the attacker selects not to attack and the defender selects a defense strategy. In this scenario, the payoffs of the attacker and defender are as follows:

$$\begin{aligned} U_A(\text{noattack}, D) &= 0, \\ U_D(\text{noattack}, D) &= -\text{DDC}. \end{aligned} \tag{14}$$

The sum of the payoffs of both sides in the above game scenario is

$$U_A(\text{not attack}, D) + U_D(\text{not attack}, D) = -\text{DDC}. \tag{15}$$

From the above, it is easy to derive that whether the attacker attacks or not, the sum of the game payoff of the attacker and defender is a constant; that is to say, the information security of the attack-defense game is a nonzero sum game.

5. Multistep Attack Strategy Payoff Calculation

5.1. Single-Step Attack Payoff. First, according to the network topology and network vulnerabilities, we can derive that the attack strategy matrix S_A with size $n \times m$ is composed of 0, 1. For example,

$$S_{Ai} = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & 1_{ij} & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}. \tag{16}$$

Only one element (i, j) is 1, and the rest is 0 in S_{A_i}, which indicates the single-step attack action of the attacker implementing attack strategy j on node i.

In order to calculate the attack strategy payoff matrix more objective, we use the database of Lincoln Laboratory Attack-Defense Behavior [19].

If there is a matrix B, then we get $\|B\|_p$ according to [21]

$$\|B\|_p = \left(\sum_{i=1}^{n} \sum_{j=1}^{m} \left| b_{ij} \right|^p \right)^{(1/p)}. \tag{17}$$

According to the function relationship between the attack-defense payoff matrix and the attack payoff, the payoff of single-step attack action is obtained as follows:

$$f_A^1 = f_{A_1} = \left\| S_{A_1} \times U_A^T \times S_{A_1}^T \right\|_1, \tag{18}$$

where $f_A{}^i$ represents the cost of attack step i and f_{A_1} represents the cost of attack stepA_1.

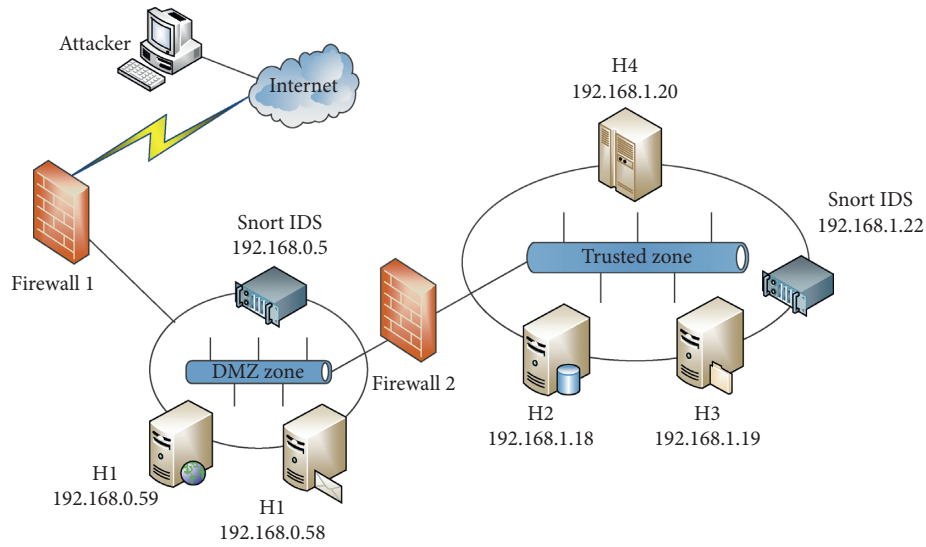

Figure 3: Experiment topology.

Next, a simple example is given to illustrate the attack cost of a single attack strategy. Assuming that the node n in the network system has i number of vulnerabilities and each vulnerability has an attack strategy, the attack strategy matrix S_{A_n} is defined as follows:

$$S_{A_n} = [a_{11}a_{12}\cdots a_{1i}]. \tag{19}$$

The attack payoff matrix for compromising i vulnerabilities is

$$U_{A_n} = [u_{11}u_{12}\cdots u_{1i}]. \tag{20}$$

According to formula (18), the attacker's attack payoff of attacking node n is as follows:

$$f_{A_n} = \left\| S_{A_n} \times U_{A_n}^T \times S_{A_n}^T \right\|_1 = \sum_{j=1}^{i} \left(a_{1j} \times u_{1j}\right) S_{A_{n1}}^T. \tag{21}$$

When an attacker attacks vulnerability $l\,(1 \le l \le i)$, the attack payoff is

$$f_{A_n} = \left\| S_{A_n} \times U_{A_n}^T \times S_{A_n}^T \right\|_1 = u_{1l}[0\cdots 1\cdots 0]_1^T = u1l. \tag{22}$$

5.2. Multistep Attack Payoff. First, we analyze the attack steps as follows. When an attacker invades a targeted network system, due to the lack of information with the system, some attack actions may fail, and the attacker may take the same attack actions on the same attack targets. Suppose that the attacker attacked the same node, and then, the more the number of attack times, the less the attack cost. Given the parameter $\lambda \in (0, 1)$, when the same attack action was executed on the same target n times, the n-th attack cost was λ^n times as much as the first one. Since multistep attacks can be divided into several single-step attack actions, the multistep attack analysis can be divided into multiple single-step attack action analyses such as the following example.

Table 1: Strength and payoff of attack action.

No.	Description	Strength	Payoff
a_1	Remote buffer overflow	0.95	
a_2	Install Trojan	0.8	3
a_3	Steal account and crack it	0.7	
a_4	Send abnormal data to GIOP	0.5	
a_5	Shut down database server	0.45	2
a_6	LPC to LSASS	0.4	
a_7	Oracle TNS Listener	0.35	
a_8	Ftp RHOST attack	0.3	1
a_9	Sr-Hard blood	0.25	

When an attacker carries out a multistep attack, the attacker's multistep attack cost is calculated, and the attacker's q-step attack strategy is $S_{A_1}, S_{A_2}, \ldots, S_{A_q}$; then, the attack cost of the q-th step is given as follows:

$$f_A^q = \sum_{i=1}^{q} f_{A_i}. \tag{23}$$

Because of the repeated game between attack-defense, when calculating the attack payoff, we consider the function f_A^q with the median coefficient as follows:

$$\begin{aligned} f_A^q &= v_{11}u_{a_{11}} + v_{12}u_{a_{12}} + \cdots + v_{nm}u_{a_{nm}} \\ &= \sum_{j=1}^{m}\sum_{i=1}^{n}\sum_{k=1}^{v_{ij}} \lambda^{k-1} u_{a_{ij}}. \end{aligned} \tag{24}$$

The number of attacks for the corresponding attack strategies is $v_{11}, v_{12}, \ldots, v_{nm} \in \{0, 1, 2, \ldots\}$, respectively.

Table 2: Strength and payoff of defense action.

No.	Description	Strength	Payoff
D_1	Limit packets form ports	0.8	
D_2	Install Oracle patch	0.8	
D_3	Reinstall Listener program	0.8	3
D_4	Uninstall, delete Trojan	0.7	
D_5	Limit access to MDSYS.SDO_CS	0.7	
D_6	Renew root data	0.6	
D_7	Restart database server	0.6	
D_8	Limit SYN/ICMP packets	0.5	2
D_9	Add physical resource	0.5	
d_{10}	Repair database	0.4	
d_{11}	Correct homepage	0.4	
d_{12}	Delete suspicious account	0.3	1
d_{13}	Redeploy firewall rule and filtrate malicious packets	0.3	
d_{14}	Patch SSH on Ftp	0.2	

6. Defense Strategy Payoff Calculation and Strategy Selection

6.1. Single-Step Defense Payoff. When the attacker takes a single-step attack action and no other attack action is implemented, the defender has the selection of different defense strategies, and the defense strategy payoff of the defender is expressed in the form of a set.

Denote the attacker's attack strategy as a_{ij}; the defense strategy set $\mathrm{Sup}\, S_{D_i}$ of the defender adopted by the defender has the least payoff of guaranteeing the survival of the network system, which is called the optimal defense strategy. Therefore, we can get

$$u_{il} = \min\left(\mathrm{Sup}\, U_{D_i}\right). \tag{25}$$

By formula (25), we can obtain the optimal defense strategy d_{il}, where $d_{il} \in \mathrm{Sup}\, S_{D_i}$. The defense strategy matrix is

$$S_{D_i} = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & 1_{il} & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}. \tag{26}$$

In S_{D_i}, only element d_{il} is 1, and the rest is 0. A simple example is given to illustrate the calculation of the defense strategy payoff.

Assuming that the vulnerability i of attack node m is exploited and that there are j kinds of vulnerability for strategy i, the defense strategy matrix S_{D_m} is

$$S_{D_m} = \begin{bmatrix} d_{m1} & d_{m2} & \cdots & d_{mj} \end{bmatrix}. \tag{27}$$

According to the optimal defense decision-making principle, the defense strategy with the least payoff under the condition of network survivability is the optimal defense strategy. According to formula (3), the proposed defense strategy in the defense matrix S_{D_m} is $S_{D_m} =$ $[\, 0 \ \ldots \ d_{ml} \ \ldots \ 0\,]$., where $SI_{d_{ml}} > SI_{a_{ml}}$ and $u_{ml} > \min(\mathrm{Sup}\, U_{D_m})$. Similar to the single-attack strategy payoff, the single-defense strategy payoff is obtained as follows:

$$\begin{aligned} f_{D_m} &= \left\| S_{D_m} \times U_{D_m}^T \times S_{D_m}^T \right\|_1 = \left\| u_{ml} \left[0 \ldots 1_{ml} \ldots 0 \right]^T \right\|_1 \\ &= u_{ml}. \end{aligned} \tag{28}$$

Table 3: Node information.

Host/server	Protocol/vulnerability	Port
Web	IIS	445
Data	Apache	80
H_1	HIDP	445
H_2	GUN Wget	80
H_3	NDproxy	445

Table 4: Candidate attack-defense actions for vulnerabilities.

	IIS	Apache	HIDP	GUN Wget	NDproxy
Attack action	a_2, a_7	a_1	a_4, a_5, a_8	a_2, a_7, a_8	a_3, a_7
Defense action	d_3, d_4	D_1, d_8, d_{13}	d_1, d_6, d_7, d_{10}	d_3, d_4, d_{12}	d_3, d_6

6.2. Multistep Defense Payoff and Strategy Selection. The defender selects multiple optimal defense strategies according to multiple attack actions, which makes the maximum survivability of the network system. The payoff analysis of is the same. First, it is assumed that the attacker and the defender have the same business capability. When the defender implements the same defense strategy many times, the defense payoff decreases correspondingly, and herein, the parameter is λ. According to formulae (23) and (24), the payoff of the multistep defense strategy is as follows:

Table 5: Performance comparison.

	Attack strategy	Defense strategy	Attack payoff	Defense payoff	Strategy explainability	Security quantification	Quantitative strategy strength	Attack early warning
Wang et al. [9]	✓	✓	×	×	Weak	✓	×	×
Wang et al. [10]	✓	✓	✓	✓	Weak	×	×	×
Shen et al. [11]	✓	✓	✓	✓	Weak	×	×	×
Agah and Das [12]	✓	✓	×	×	Strong	×	×	×
Zhang et al. [13]	✓	✓	×	×	Weak	×	✓	×
Tan et al. [14]	✓	✓	✓	✓	Weak	×	×	×
Ours	✓	✓	✓	✓	Strong	✓	✓	✓

× indicates that the item is not studied.

$$\begin{aligned} f_D^p &= \sum_{i=1}^{p} f_{D_i} \\ &= \eta_{11} u_{d_{11}} + \eta_{12} u_{d_{12}} + \cdots + \eta_{nk} u_{d_{nk}} \\ &= \sum_{i=1}^{n} \sum_{j=1}^{k} \sum_{l=1}^{\eta_{ij}} \lambda^{l-1} u_{d_{ij}}. \end{aligned} \tag{29}$$

When $p = 1$, it is formula (18) of calculating the payoff of a special single-step defense strategy. The number of times of defense strategy implementing is $\eta_{11}, \eta_{12}, \ldots, \eta_{nk} \in \{0, 1, 2, \ldots\}$ for $\exists \eta_{ij} \neq 0$. The defense strategy is selected according to the attacker's attack strategy of making the maximized survivability $V \geq 0$.

7. Experiments and Analysis

7.1. Experiments. In order to verify the impact of defense strategy selection on network system security, the network environment is constructed as shown in Figure 3, which includes three hosts and two servers, as well as two firewalls and two IDS.

In the experimental environment of Figure 3, the attacker attacks the host and server in the system through the network. First, the attack-defense action strengths in Tables 1 and 2 are given. The attack-defense payoff is determined on the basis of the capabilities of attackers and defenders of the same levels. Different attack-defense strengths correspond to different attack-defense payoffs. In order to improve the decision-making accuracy, we divide the attack-defense payoff into three levels corresponding to attack-defense strengths as shown in Tables 1 and 2. The configuration information of experimental environment is given in Table 3. Table 4 is obtained by querying CVE [22]. U.S. National Vulnerability Database (NVD) [23] is used to get specific vulnerability attack-defense action table.

According to attack action a_5, we can get $\lambda = 0.7$. According to formula (24), attack payoff is

$$f_A^4 = f^3_{a_{192.168.1.5}, a_5} + f^1_{a_{192.168.1.7}, a_e} = 7.38. \tag{30}$$

According to the IP address, the attack strategy matrix is S_{iii}, and $\mathrm{SI}_{a_5} = 0.45$ and $\mathrm{SI}_{a_3} = 0.7$. According to formula (3), we can derive

$$\begin{aligned} \mathrm{Sup}\, S_{D_{iii}} &= \left\{ d_{192.168.1.5.d_1}, d_{192.168.1.5, d_6}, d_{192.168.1.5, d_7} \right\}, \\ d_{ij}\, \mathrm{Sup}\, S_{D_{iii}} &= \left\{ d_{192.168.1.7, d_3} \right\}. \end{aligned} \tag{31}$$

According to formula (29), the three situations of the defense payoff are as follows:

$$\begin{aligned} f_D^4 &= f^3_{a_{192.168.1.5}, d_1} + f^1_{a_{192.168.1.7}, d_3} = 9.87, \\ f_D^4 &= f^3_{a_{192.168.1.5}, d_6} + f^1_{a_{192.168.1.7}, d_3} = 7.38, \\ f_D^4 &= f^3_{a_{192.168.1.5}, d_7} + f^1_{a_{192.168.1.7}, d_3} = 7.38. \end{aligned} \tag{32}$$

The best defense strategies are $\left\{ d_{192.168.1.5, d_6}, d_{192.168.1.7, d_3} \right\}$ and $\left\{ d_{192.168.1.5, d_7}, d_{192.168.1.7, d_3} \right\}$.

7.2. Comparisons and Analysis. The interpretability of the generated strategy is better than other approaches, namely, the proposed approach can clearly explain what a strategy is and how it is generated. In this paper, we first introduce the attack graph to enhance the visual expression of the attack-defense strategy. The nodes and edges in the graph represent the network states and the set of possible candidate attack and defense actions, respectively. It intuitively explains the attack-defense strategies.

Second, the game theory is employed to model the attacker and defender. Game theory has the characteristics of objective opposition and non-cooperative and strategic interdependence, all of which are in line with the basic characteristics of cyberattack-defense. By calculating the game equilibrium point, we can better understand the evolution process of strategy derivation, generation, and adjustment.

Compared with other methods [9, 10, 13, 14] using game theory or attack graph alone, our method is more interpretable by combining attack graph and game theory. [9–14] are investigated based on the state attack graph to consider the impact of the attack strategy and defense strategy on the security state of the system. Most of the research studies do not give the quantitative method of the security state of the network system as well as the analysis of the attack strategies of the network system. Decision-making is actually the arrangement of different strategies, but in the process of

network system attack-defense, managers cannot achieve unlimited trial and error opportunities, and there are difficulties in understanding the maximum payoff of the strategy arrangement. Therefore, this paper studies the impact of the network attack-defense strategy set on the survivability of the network system based on the attribute attack graph. Table 5 gives the performance comparison.

8. Conclusions and Future Works

This paper studies the strategy selection with maximum payoff in the network attack-defense dispute based on the attribute attack graph. Firstly, the attack-defense matrix is used to represent the attack-defense strategy and path. Secondly, Lincoln Lab's attack-defense action data are used to quantify attack-defense strength and network survivability. Thirdly, combined with the attack-defense strategy strength and payoff, network system security is studied against multistep attack threats in the small-scale network system. Fourth, the interpretability and implementation of our strategy are better through using visual attack-defense paths. Finally, according to the attack strategy matrix, the proposed approach is designed to predict the possible attack behaviors and targets in the next step in multistep attacks.

Future work is combining with machine learning to achieve automatic analysis of attack-defense strategies so as to implement faster strategy implementation. In addition, how to improve the smart level of the proposed decision-making is in the next step of our research. We try to introduce knowledge graph, artificial intelligence, and other emerging technologies to enhance the ability of immediate decision-making response and strategy continuous optimization. Due to the sensitivity of attack-defense data, there are few open labeled datasets on the internet. The lack of labeled data restricts the supervised or semisupervised machine learning algorithm in the field of intelligent decision-making. In this case, the sample distribution is difficult to cover the decision space, and the generalization and applicability of our training model for strategy learning are not strong. How to introduce small sample learning, incremental learning, reinforcement learning, and make full use of the limited data so that the defender can learn new knowledge from the new sample continuously in the process of adversary with the attacker is the key point. Through the intelligent game model, the defender can gain online decision-making capacity immediately and optimize the precision of strategy selection faster.

Data Availability

The data that support the findings of this study are not publicly available due to restrictions as the data contain sensitive information about a real-world enterprise network. Access of the dataset is restricted by the original owner. The data can be made available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Key Research and Development Program of China (2019QY1301, 2019QY1303, and 2018YFB0803602) and the National Natural Science Foundation of China (Grant no. 61902427).

References

[1] A. N. Mehran, B. Behnam, K. Mehdi, and F. Benjamin, "Detecting new generations of threats using attribute-based attack graphs," *IET Information Security*, vol. 13, no. 4, pp. 293–303, 2019.

[2] C. Chen, J. Hu, T. Qiu, M. Atiquzzaman, and Z. Ren, "CVCG: cooperative V2V-aided transmission scheme based on coalitional game for popular content distribution in vehicular ad-hoc networks," *IEEE Transactions on Mobile Computing*, vol. 18, no. 12, pp. 2811–2828, 2019.

[3] C. Chen, L. Liu, T. Qiu, K. Yang, F. Gong, and H. Song, "ASGR: an artificial spider-web-based geographic routing in heterogeneous vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 5, pp. 1604–1620, 2019.

[4] H. Hu, Y. Liu, H. Zhang, and Y. Zhang, "Security metric methods for network multistep attacks using AMC and big data correlation analysis," *Security and Communication Networks*, vol. 2018, Article ID 5787012, 14 pages, 2018.

[5] A. T. Ghazo, M. Ibrahim, H. Ren, and R. Kumar, "Automatic attack graph generation and visualization and its applications to computer and SCADA networks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2019.

[6] H. S. Lallie, K. Debattista, and J. Bal, "A review of attack graph and attack tree visual syntax in cyber security," *Computer Science Review*, vol. 35, Article ID 100219, 2020.

[7] H. Hu, Y. Liu, C. Chen, H. Zhang, and Y. Liu, "Optimal decision making approach for cyber security defense using evolutionary game," *IEEE Transactions on Network and Service Management*, 2020.

[8] H. Hu, Y. Liu, Y. Yang, H. Zhang, and Y. Zhang, "New insights into approaches to evaluating intention and path for network multistep attacks," *Mathematical Problems in Engineering*, vol. 2018, Article ID 4278632, 13 pages, 2018.

[9] H. Wang, Z. Chen, J. Zhao, X. Di, and D. Liu, "A vulnerability assessment method in industrial internet of things based on attack graph and maximum flow," *IEEE Access*, vol. 6, pp. 8599–8609, 2018.

[10] Y. Wang, C. Lin, and X. Cheng, "Evolutionary game model and analysis methods for network group behavior," *Chinese Journal of Computers*, vol. 38, no. 2, pp. 282–300, 2015.

[11] S. Shen, Y. Li, 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.

[12] A. Agah and S. K. Das, "Preventing DoS attacks in wireless sensor networks: a repeated game theory 2011 approach," *International Journal of Network Security*, vol. 5, no. 2, pp. 145–153, 2007.

[13] H. Zhang, T. Li, and S. Huang, "Network defense decision-Making method based on attack-defense differential game," *Acta Electronica Sinica*, vol. 46, no. 6, pp. 1428–1435, 2018.

[14] J.-L. Tan, C. Lei, H.-Q. Zhang, and Y.-Q. Cheng, "Optimal strategy selection approach to moving target defense based on Markov robust game," *Computers & Security*, vol. 85, no. 5, pp. 63–76, 2019.

[15] K.-W. Lye and J. M. Wing, "Game strategies in network security," *International Journal of Information Security*, vol. 4, no. 1-2, pp. 71–86, 2005.

[16] S. Sahar, F. Abdollahi, and K. Khorasani, "Model predictive and non-cooperative dynamic game fault recovery control strategies for a network of unmanned underwater vehicles," *International Journal of Control*, vol. 92, no. 3, pp. 489–517, 2019.

[17] S. Lee, S. Kim, K. Choi, and T. Shon, "Game theory-based security vulnerability quantification for social internet of things," *Future Generation Computer Systems*, vol. 82, pp. 752–760, 2018.

[18] M. Liu, Q. Zhang, W. Yu, and H. Zhang, "Preliminary study on creative thinking mechanism of market information integration," *Acta Psychologica Sinica*, vol. 50, no. 1, pp. 82–89, 2018.

[19] L. Gordon, M. Loeb, W. Lucyshyn, and R. Richardson, "2015 CSI/FBI computer crime and security survey," in *Proceeding of IEEE Computer Security Institute*, pp. 48–64, San Francisco, CA, USA, 2015.

[20] X. Ou, S. Govindavajhala, and A. W. Appel, "MulVAL: a logicbased network security analyzer," in *Proceeding of the 14th conference on USENIX Security Symposium*, p. 8, Berkeley, CA, USA, 2005.

[21] F. Peldschus and E. K. Zavadskas, "Fuzzy matrix games multicriteria model for decision-making in engineering," *Informatica*, vol. 16, no. 1, pp. 107–120, 2005.

[22] CVE, "Common vulnerabilities and exposures," http://cve.mitre.org/.

[23] NVD, "National vulnerability database," https://nvd.nist.gov/.