Hindawi
Security and Communication Networks
Volume 2021, Article ID 4005877, 10 pages
https://doi.org/10.1155/2021/4005877

*Research Article*

# Network Attack and Defense Modeling and System Security Analysis: A Novel Approach Using Stochastic Evolutionary Game Petri Net

**Zenan Wu**,[1] **Liqin Tian**,[1,2] **Yi Zhang**,[2] **Yan Wang**,[3] **and Yuquan Du**[2]

[1]*School of Computer, Qinghai Normal University, Xining 810000, China*
[2]*School of Computer, North China Institute of Science and Technology, Beijing 101601, China*
[3]*Department of Robot, Ningbo University of Technology, Ningbo 315211, China*

Correspondence should be addressed to Liqin Tian; 18511465255@163.com

Received 9 August 2021; Revised 25 October 2021; Accepted 27 October 2021; Published 13 November 2021

Academic Editor: Leandros Maglaras

At present, most network security analysis theory assumes that the players are completely rational. However, this is not consistent with the actual situation. In this paper, based on the effectiveness constraints on both sides with network attack and defense, with the help of stochastic Petri net and evolutionary game theory, the Petri net model of network attack and defense stochastic evolutionary game is reconstructed, the specific definition of the model is given, and the modeling method is given through the network connection relationship and attack and defense strategy set. Using this model, a quantitative analysis of network attack events is carried out to solve a series of indicators related to system security, namely, attack success rate, average attack time, and average system repair time. Finally, the proposed model and analysis method are applied to a classic network attack and defense process for experimental analysis, and the results verify the rationality and accuracy of the model and analysis method.

## 1. Introduction

In recent years, with the rapid development of information technology, it has provided great convenience for the country's scientific and technological development and the people's living needs. However, the increasing complexity of network scale also brings growing security problems since malicious entity behaviors are turning to be more threatening, such as the loss of private data, attacks against the network, and detection of these attacks [1, 2]. It is particularly important to note that the threat behavior of malicious users poses a great threat to the security of the network system [3]. For example, in a network session, when a malicious user pretends to be a normal user to access the system and conducts unsafe behavior, the network system will be misled by fraudulent behavior. If an entity in the network threatens the security of the system, the network administrator should exercise certain control over it.

However, the traditional passive security defense strategy has been unable to meet the actual needs of network development. It is urgent to analyze and predict the network attack events and then implement the new technology of active security defense [4, 5]. In network attack events, the basic characteristics of game theory are target opposition, strategic dependence, and noncooperation. Therefore, game theory has become a popular method for theoretical analysis and modeling of network security proposed in recent years [6, 7]. Roy et al. [8] summarize the application results of existing game theory in solving network security problems and classify the solutions according to the applicability of the method. Anderson [9] applied game theory to the problem of network security offense and defense based on the opposition between the two parties in the game and the interdependence of the two parties' strategy selection. Shamma [10] proposed two person zero sum games and noncooperative intrusion detection system models and introduced the application of game theory in decision system. Wu et al. [11] proposed a two-stage game model to provide the optimal security detection strategy for heterogeneous network systems; Li et al. [12] proposed a Stackelberg game model to solve the problem of interactive decision-making between attackers and defenders in network control systems. Liu et al. [13] proposed a network attack and defense game model based on Bayes Nash equilibrium, solved the attack and defense problem through the utility maximization problem, and focused on the attack and defense game problem of insecure information network based on risk aversion. In Zhang et al. [14], in order to more accurately describe the timely response of network confrontation combining with the theory of differential game, the game model of attack and defense differential game is established. Guan et al. [15] believed that the effectiveness of network attack and defense depends on some network performance indicators, which are defined to evaluate the performance of the whole network system. They propose a networked colonial bottom game for the attack defense strategy, which enables attackers and defenders to reasonably allocate limited network resources on each node. In addition, this paper also proposes a coevolution algorithm to obtain the actual behavior set and finally realizes the Nash equilibrium of the mixed strategy. Tan et al. [16] used game theory to analyze the continuous network attack defense process based on the dynamic spatiotemporal confrontation characteristics of network attack and defense, established a FlipIt-based moving target defense and temporospatial strategies model, and gave the quantitative calculation method for the utility of the attacker and the defender. Gao et al. [17] focused on the research of offensive and defensive games between multiple groups of terminals in wireless networks and proposed an optimal strategy selection algorithm based on differential game between multiple attackers and multiple defenders. Finally, through simulation experiments, we demonstrated the evolution trajectory of the optimal strategy.

In summary, in the early research work of network security game models, most researchers pay more attention to preventing attacks in network systems. Later research focuses on designing the system's security mechanism, which is the system's active defense function of network security by detecting and preventing malicious attacks.

Although the above methods provide a lot of research ideas for network security analysis, these methods also have some limitations [18]. Firstly, in a cyber security incident, the actions of both offensive and defensive parties influence each other, and both parties are in a state of ebb and flow. Pure game theory does not have enough modeling ability to completely describe complex network attack events; secondly, as far as we know, almost all of the existing modeling methods based on game theory set the players in the game as completely rational, but such assumptions are often inconsistent with our actual situation. As a qualitative experimental simulation, sometimes, we can consider this assumption to be reasonable. However, in practical applications, we doubt the rationality of this assumption. In the real network environment, network attack is a kind of man-made behavior. The fundamental reason for its formation is closely related to human interests. The behavior of both sides of the network attack and defense can not be a completely rational behavior; they show more effective rational behavior. Therefore, if we regard both sides of the game as completely rational players for modeling and analysis, the results will deviate from the actual situation. Similarly, this assumption will greatly weaken the accuracy and guiding significance of the results obtained by the model.

In view of the limitations of the above methods, we transform and upgrade the traditional modeling methods. We find that Petri net is a tool with parallel processing ability and graphical problem description [19]. In addition, in the actual process of network attack and defense, the choice of attack and defense strategies, the change of system environment, and the interference of external factors all have a certain randomness. There are many references [20, 21], which have applied the analysis method based on stochastic model to network security evaluation. However, the stochastic Petri net is formed on the basis of the Petri net. In addition to the basic characteristics of the Petri net, it also has the ability to dynamically analyze the concurrency, asynchrony, and uncertainty of the network system [22]. It can be conveniently used to model and analyze complex systems, such as system performance analysis and reliability evaluation. In addition, stochastic Petri nets have good expansibility [23], and new constructions can be added easily. Therefore, we believe that stochastic Petri nets are more suitable for modeling and security analysis of network systems.

Taking into account the two characteristics of bounded rationality and repeated games in network confrontation games [24], they are the premise of evolutionary game theory; and evolutionary game theory abandons the defect of traditional game theory that players are completely rational. Therefore, evolutionary game theory can be better used to describe the influence of human factors on the development of network attack and defense and is more suitable for the modeling and analysis of network attack and defense confrontation behavior [25].

Therefore, in order to improve the rationality and accuracy of the model, this paper will take the attack and defense sides of the network under the condition of bounded rationality as the problem object, with the help of evolutionary game theory and stochastic Petri net, construct a network attack and defense model based on stochastic evolutionary game Petri net, and analyze the security of the attacked network system.

The contributions of this paper are threefold:

(1) We first analyzed the strategies that the offensive and defensive parties can adopt in a cyber attack event, provided an evaluation program closer to the real world, enabled the research community to conduct systematically, and evaluated a trust model.

(2) We propose to apply stochastic Petri net and evolutionary game theory in the evaluation process of network trust model and discuss the detailed simulation scenarios of modeling.

(3) We apply our stochastic evolutionary game Petri net model to an example classic attack event. The

evaluation results suggest that our model can describe in detail the complete process of an attack event. Since the evolutionary game theory is used in the model, after many games, the malicious entity will converge to a final state, which is also the best state. Therefore, the method we propose is more scientific and accurate for the trust evaluation results of network entities.

The rest of the paper is organized as follows. First, we introduce the basic definition and related attributes of stochastic evolutionary game Petri net model in Section 2. Then, we introduce the specific methods of modeling in Section 3. In Section 4, through an example, the proposed model is applied to the actual network attack and defense events. In Section 5, we analyze the experimental results. Finally, we summarize our paper with feature work in Section 6.

## 2. Petri Net Model of Stochastic Evolutionary Game for Network Attack and Defense

The traditional network attack and defense game model is based on the complete rationality of both sides of the game. In practice, the behavior of both sides of the network attack and defense is a kind of limited rationality. Based on evolutionary game and stochastic Petri net, this paper constructs a Petri net model of network attack defense stochastic evolutionary game.

*Definition 1.* A Petri net model of stochastic evolutionary game of network attack and defense can be represented by a 9-tuple:

$$AD-\mathrm{SEGPN}=\{N,P,T,F,\pi,\lambda,\Delta,U,M\}. \tag{1}$$

(1) $N=\{N_a,N_d\}$ denotes the set of players; $N_a$ is the attacker, and $N_d$ is the defender.

(2) $P=\{P_1,P_2,\ldots,P_n\}$ is a finite set of places; $P_i$ represents the state of the system after the attack event.

(3) $T=T_{N_a}\cup T_{N_d}$ is a finite set of transitions; transition represents the player's behavior strategy. For example, $a$ represents the set of strategies that the defender can adopt.

(4) $F\in I\cup O$ is a set of arcs, where $I\subseteq P\times T$ and $O\subseteq T\times P$ such that $P\cap T\neq\varphi$ and $P\cup T\neq\varphi$, where $\varphi$ is an empty set.

(5) $\pi$: $T\longrightarrow[0,1]$ represents the probability that the transition is selected, that is, the probability that the player chooses a certain behavior strategy.

(6) $\lambda=\{\lambda_1,\lambda_2,\ldots,\lambda_n\}$ is a collection of change implementation rates.

(7) $\Delta=\left\{\delta_{N_a},\delta_{N_b}\right\}$ is the set of random interference intensity coefficients; $\delta_{N_a}$ is the influence strength coefficient of random interference on the attacker; $\delta_{N_d}$ is the influence intensity coefficient of random interference on the defender.

(8) $U=\left\{U_{N_a},U_{N_d}\right\}$ represents the set of game revenue functions; $U_{N_a}$and $U_{N_d}$ represent the game revenue set of attacker and defender, respectively.

(9) $M=\{m_1,m_2,\ldots,m_n\}$ is the set of identifications, and the identifications are the elements in the Markov chain. Every state in the model has its corresponding identifications in the Markov chain.

For AD-SEGPN model, the behavior choice and implementation of each player depend on their own state and the state and potential behavior of other players. Therefore, it is necessary to build an appropriate model and set the rules of transition according to the specific situation. This paper is based on the trigger rule of transition in classical Petri nets. Token is used to mark the state of the players. If there is a mark in $P_i$, it means that the player is in this position. Any change may lead to the change of the player's state, which is graphically displayed in the model by the flow of markers.

*Definition 2.* For a given stochastic evolutionary game Petri net $\mathrm{SEGPN}=\{N,P,T,F,\pi,\lambda,\Delta,U,M\}$, the attacker's strategy can be expressed as follows.

$\pi_{N_a}=\left\{\pi(t_{N_a}^1),\pi(t_{N_a}^2),\ldots,\pi(t_{N_a}^{|T_{N_a}|})\right\}$, and $\pi(t_{N_a}^i)$ is he probability that the attacker chooses to implement behavior $t^i$; the defender's strategy is expressed as $\pi_{N_d}=\left\{\pi(t_{N_d}^1),\pi(t_{N_d}^2),\ldots,\pi(t_{N_d}^{|T_{N_d}|})\right\}$ where $\pi(t_{N_d}^j)$ is the probability that the defender chooses to carry out the action $t^j$.

## 3. Modeling Method in AD-SEGPN

*3.1. Modeling Method.* The Petri net model of stochastic evolutionary game inherits the basic elements of stochastic Petri net, such as position, transition, and arc. At the same time, it absorbs the return, utility, strategy, and other elements of player's behavior in evolutionary game theory, so as to realize the modeling and analysis of game process visualization. The specific modeling steps are as follows:

(1) Determine the players in the game and analyze the types of the game.

(2) Construct the behavior set $T$ of players. The behavior set of players includes the behavior strategies that players may choose in each stage of the game. $t_j^i\in T$ is the behavior of player $i$ in state $j$.

(3) The position set P of players is constructed. The set of players' positions contains all the states produced in the game.

(4) Establish arc connection. The occurrence of players' behavior, that is, triggering the occurrence of changes, will make the state of the whole system change, that is, from one state to another, and connect them by using arcs, so as to form a complete system model.

(5) Determine the utility $R$. In AD-SEGPN model, utility $R$ is the income that the actor can obtain after the implementation of transition $T$, which is recorded as

$R$: $T \longrightarrow (r_1, r_2, \ldots, r_n), r_i \in (-\infty, +\infty)$. If $r_i < 0$, it means that the actor has paid the price. Utility can be expressed by letters or utility function. The variables of the function can be associated with their own state parameters and can also be associated with the state parameters of other players in the game.

(6) Evolutionary equilibrium solution. Under the condition of bounded rationality, both sides of evolutionary game will conduct dynamic repeated game through the process of "imitation-learning-strategy adjustment" and finally reach the stable equilibrium state of the game [26]. Refer to Section 3.2 for the specific method of solving evolutionary equilibrium.

(7) According to the equilibrium strategy obtained in (6), as the probability of transition being selected in the model, and then, given the transition rate, according to the calculation method of stochastic Petri net, the important results related to network security analysis are further calculated.

*3.2. Evolutionary Equilibrium Solution.* In network attack, attacker $N_a$ and defender $N_d$ have a variety of strategies to choose from. Suppose that the attacker $N_a$ can choose $T_{N_a} = \{a_1, a_2, \ldots, a_n\}$ and the defender $N_d$ $T_{N_d} = \{d_1, d_2, \ldots, d_m\}$, where $m, n \in N$ and $m, n \geq 2$. Because network attack event can be regarded as a multistage game process, attackers and defenders will choose strategies with different probabilities in different stages, and the probabilities will change with the passage of time under the effect of learning mechanism, so that the selection of attack and defense strategies will form a dynamic change process. Finally, the attack and defense sides will find their own equilibrium stable strategy (ESS) [27].

*Definition 3.* Equilibrium stable strategy in offensive and defensive events. In a network attack and defense event, there is a strategy; if all members of the attacker or defender adopt it, then any mutation strategy will not invade the population under the influence of natural selection.

The condition for a strategy $x$ to be ESS of the offensive and defensive events is that for any strategy $y \neq x$.

$$\begin{aligned} \mu(x, x) &\geq \mu(y, x), \\ \mu(x, y) &\geq \mu(y, y), \end{aligned} \tag{2}$$

where $\mu(x, y)$ is the payoff of attacker's strategy $x$ when interacting with defensive's strategy $y$.

Let $p_i$ be the probability that the attacker chooses the attack strategy $a_i$, and let $q_j$ be the probability that the defender chooses the attack strategy $d_j$, $i \in n, j \in m$ :

$$\begin{aligned} \sum_{i=1}^{n} p_i &= 1, \\ \sum_{j=1}^{m} q_j &= 1. \end{aligned} \tag{3}$$

$U_{N_a}^{ij}$ and $U_{N_d}^{ij}$ are the respective gains of the attacker and the defender when they tke $a_i$ and $d_j$, respectively. In the attack event, the two sides of the game adopt different strategies, which will produce the corresponding income value. The benefits obtained by the attacker and the defender after choosing strategies with different probabilities at a certain stage of the game are shown in Figure 1.

Furthermore, we can calculate the expected return and average return of different strategies chosen by both sides of the game:

(1) The expected revenue $U_{N_a}^{i}$ and average revenue $\overline{U}_{N_a}$ of the attacker are as follows:

$$\begin{aligned} U_{N_a}^{1} &= q_1 \cdot U_{N_a}^{11} + q_2 \cdot U_{N_a}^{12} + q_3 \cdot U_{N_a}^{13} + \cdots + q_m \cdot U_{N_a}^{1m}, \\ U_{N_a}^{2} &= q_1 \cdot U_{N_a}^{21} + q_2 \cdot U_{N_a}^{22} + q_3 \cdot U_{N_a}^{23} + \cdots + q_m \cdot U_{N_a}^{2m}, \\ &\vdots \qquad\qquad\qquad \vdots, \\ U_{N_a}^{n} &= q_1 \cdot U_{N_a}^{n1} + q_2 \cdot U_{N_a}^{n2} + q_3 \cdot U_{N_a}^{n3} + \cdots + q_m \cdot U_{N_a}^{nm}, \\ \overline{U}_{N_a} &= p_1 \cdot U_{N_a}^{1} + p_2 \cdot U_{N_a}^{2} + q_3 \cdot U_{N_a}^{3} + \cdots + p_n U_{N_a}^{n}. \end{aligned} \tag{4}$$

(2) The expected return $U_{N_d}^{j}$ and average return $\overline{U}_d$ of the defender are as follows:

$$\begin{aligned} U_{N_d}^{1} &= p_1 \cdot U_{N_d}^{11} + p_2 \cdot U_{N_d}^{21} + p_3 \cdot U_{N_d}^{31} + \cdots + p_n \cdot U_{N_d}^{n1}, \\ U_{N_d}^{2} &= p_1 \cdot U_{N_d}^{12} + p_2 \cdot U_{N_d}^{22} + p_3 \cdot U_{32}^{32} + \cdots + p_n \cdot U_{N_d}^{n2}, \\ &\vdots \qquad\qquad\qquad \vdots, \\ U_{N_d}^{m} &= p_1 \cdot U_{N_d}^{1m} + p_2 \cdot U_{N_d}^{2m} + p_3 \cdot U_{N_d}^{3m} + \cdots + p_n \cdot U_{N_d}^{nm}, \\ \overline{U}_{N_d} &= q_1 \cdot U_{N_d}^{1} + q_2 \cdot U_{N_d}^{2} + q_3 \cdot U_{N_d}^{3} + \cdots + q_m U_{N_d}^{m}. \end{aligned} \tag{5}$$

In the evolutionary game of network attack and defense, when the attacker chooses a strategy that leads to low profit, he will adjust the current strategy to improve his own profit; similarly, it is the same for the defender. Therefore, for both sides of the game, the probability of the behavior strategy available for them to choose is a time function, which can be expressed by $p_i(t)$ and $q_j(t)$, and its dynamic change rate can be expressed by copying the dynamic equation:

$$A(p) = \frac{dp_i(t)}{dt} = p\left(U_{a_i} - \overline{U}_a\right), \tag{6}$$

$$D(p) = \frac{dq_j(t)}{dt} = p\left(U_{d_j} - \overline{U}_d\right). \tag{7}$$

By combining formulas (6) and (7), let $Y = \begin{bmatrix} A(p) \\ D(P) \end{bmatrix} = f(Y, t) = 0$ be solved, and the evolutionary stable equilibrium solution of both attack and defense sides of the network can be obtained. The calculation results provide a basis for the selection probability of transition in AD-SEGPN model.

## 4. Experimental Simulation

In this section, we will analyze the rationality and accuracy of our scheme by experimental evaluation.

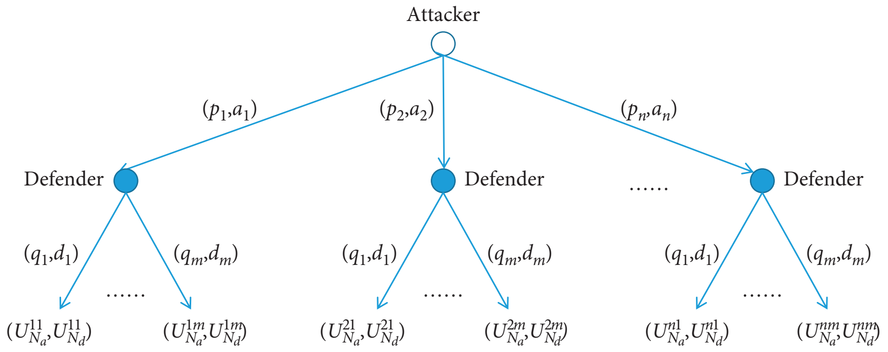
Attacker
$(p_1,a_1)$
$(p_2,a_2)$
$(p_n,a_n)$
Defender
Defender
......
Defender
$(q_1,d_1)$
$(q_m,d_m)$
......
$(q_1,d_1)$
$(q_m,d_m)$
......
$(q_1,d_1)$
$(q_m,d_m)$
......
$(U^{11}_{N_a},U^{11}_{N_d})$
$(U^{1m}_{N_a},U^{1m}_{N_d})$
$(U^{21}_{N_a},U^{21}_{N_d})$
$(U^{2m}_{N_a},U^{2m}_{N_d})$
$(U^{n1}_{N_a},U^{n1}_{N_d})$
$(U^{nm}_{N_a},U^{nm}_{N_d})$

Figure 1: Attack and defense game trees.

*4.1. Experiment Simulation Environment.* Figure 2 shows a typical network topology, which consists of Internet and intranet. Among them, intranet includes web server, information center, and some private PCs, which are usually chosen by attackers as the target of stealing confidential information. In addition, in the basic network system, IDS is often used to build the basic security control defense system. In practical applications, attackers will steal the confidential information in the system by installing sniffers. The responsibility of network administrators is to obtain the attacker's evidence and relevant information as much as possible and organize the occurrence of attacks.

*4.2. Attack and Defense Information.* When attackers and defenders choose different behavior strategies with different probabilities, the system will transfer from one state to another in a probabilistic way. According to the network topology shown in Figure 2, we can describe the attack and defense process as follows.

*4.2.1. Attack Process*

(i) The attacker scans the port of the web server in the target network and analyzes the network services provided by the target server

(ii) The attacker takes advantage of the vulnerability of the web server to obtain the login account and password

(iii) The attacker successfully logs into the system and obtains the root operation permission

(iv) The attacker uses the root privilege to install sniffer on the web server to steal the confidential information on the terminal host

*4.2.2. Defense Process*

(i) IDS detects the attack and reports it to the server

(ii) According to the reported dangerous behavior information, the server notifies the firewall and trap machine for further observation and tracking

(iii) The trap machine induces the attacker to continue to visit the server, records the attack behavior, and obtains the attack evidence of the attacker

(iv) The server blocks the attacker's IP and clears the sniffer

Based on the above attack and defense process, we can get the behavior set of attack and defense in AD-SEGPN model, as shown in Table 1.

### 4.3. Modeling and Parameter Setting

*4.3.1. Modeling Analysis.* According to the definition of AD-SEGPN model in Section 3.1 and the attack information in Sections 4.1 and 4.2, we can build a Petri net model of network attack defense stochastic evolutionary game.

The detailed description of the location set and transition set in the model is shown in Table 2.

*4.3.2. Parameter Setting.* According to the model diagram of Figure 3, the parameter information needed in the AD-SEGPN model is given in Table 3, where $\lambda$ represents the behavior ability of transition and $\pi$ represents the probability of behavior being selected. The exact value of $\lambda$ can be assumed according to the difficulty in the actual attack process, and the exact value of $\pi$ is the calculation result of evolutionary equilibrium strategy in Section 3.2.

## 5. Network System Security Analysis

After modeling the network system based on the model proposed above, we use the pipe software to calculate and analyze the AD-SEGPN model shown in Figure 3. Next, we analyze the security of the network system from two aspects. Firstly, we discussed the typical evaluation factors of network system security; then, we made an overall evaluation of network system security from two aspects.

### 5.1. Typical Network Security Factors

*5.1.1. Attack Success Rate.* Attack success rate is the probability that an attacker can attack a target successfully. In our model, the initial position $P_0$ contains a token, which represents the normal state of the system at the beginning. With the attack, the identity begins to flow. When the identity flows to the location $P_i$, it means that the attacker has successfully invaded a part of the system. Therefore, the

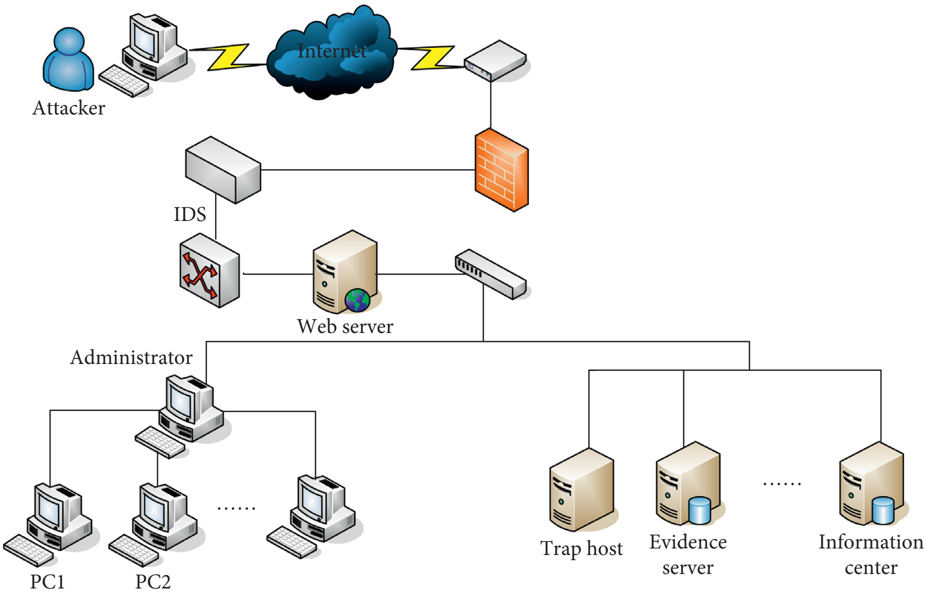

Figure 2: Simulation experiment system structure.

Table 1: Attack and defense behavior set.

| Players | Action | Symbol | Description |
|---|---|---|---|
| Attacker | Scan_Vulnerability | $a_1$ | Vulnerability scan of network system |
| | Crack_Password | $a_2$ | Obtain user login information |
| | Enhance_permission | $a_3$ | Enhance the operating permission |
| | Install_sniffer | $a_4$ | Install sniffer software to invade the host |
| | Steal_information | $a_5$ | Steal system confidential data resources |
| | $\varphi$ | $a_6$ | Do nothing |
| Defender | IDS_scan | $d_1$ | Delete the threatening account and restart |
| | Cheat_attacker | $d_2$ | Restore the network and delete the threatening account |
| | Blockade_IP | $d_3$ | Install sniffer monitoring program |
| | Remove_sniffer | $d_4$ | Clear sniffer monitoring program |
| | $\varphi$ | $d_5$ | Do nothing |

Table 2: The meaning of place and transition.

| Place | Meaning | Transition | Meaning |
|---|---|---|---|
| $P_0$ | The normal state of the system | $T_0$ | Vulnerability scan of network system |
| $P_1$ | The vulnerability of the web server was discovered | $T_1$ | Obtain user login information |
| $P_2$ | Get normal operation permission | $T_2$ | Enhance the operating permission |
| $P_3$ | Get root operation authority | $T_3$ | Install sniffer software to invade the host |
| $P_4$ | Implant sniffer | $T_4$ | Steal system confidential data resources |
| $P_5$ | System confidential data resources was stolen | $T_5, T_6, T_7 T_8, T_9$ | IDS_scan |
| $P_6$ | Admin_know | $T_{10}$ | Blockade_IP |
| $P_7$ | Attack_terminated | $T_{11}$ | Remove_sniffer |
| $P_8$ | Sniffer_removed | $T_{12}$ | Return |

attack success rate of the attacker to the system component $i$ can be expressed as

$$P(N_a \longrightarrow P_i) = P\{m(P_i) = 1\} = 1 - P\{m(P_i) = 0\}, \quad (8)$$

where $P\{m(P)_i = 1\}$ is the probability that the location $P_i$ contains a token.

The calculation results are obtained by the software package pipe. In Figure 4, we get the change of attack success rate with system time under different attack rates.

It can be seen from the figure that, with the increase of attack rate, the probability of successful attack also increases. However, after a period of time, the time required for successful attack becomes longer. This is because the higher the attack rate is, the more frequent the attack occurs, and the easier it is to be detected by the defender. At the same time, when the attack rate is greater than 10, and the system time tends to be stable, the attack success rate is no longer affected by the attack rate. This is an important result.

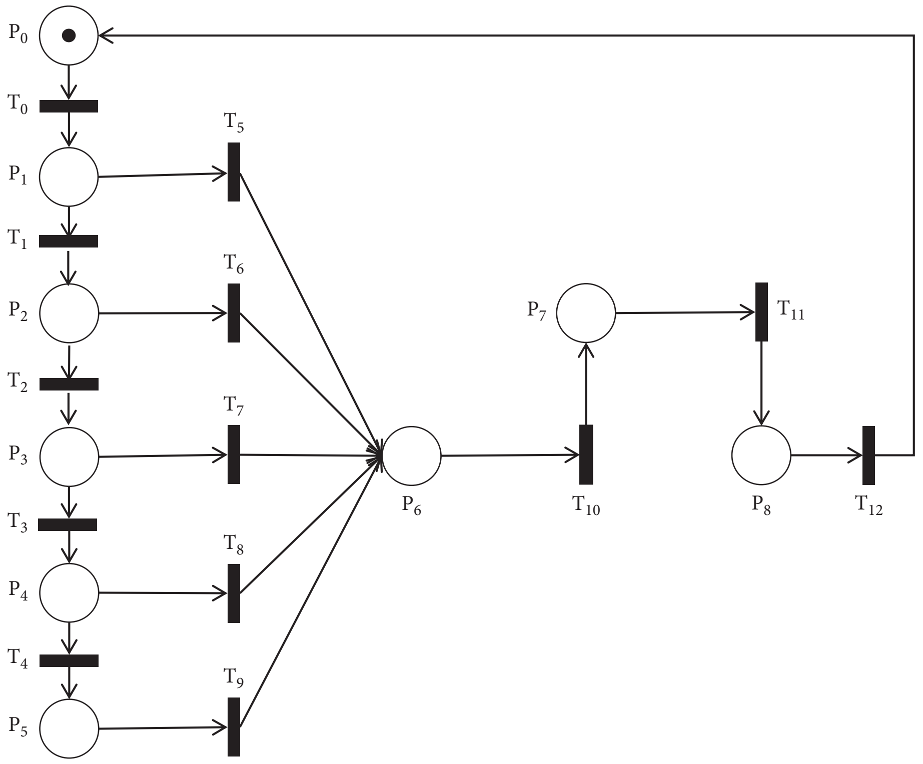

Figure 3: Structure of AD-SEGPN model.

Table 3: Parameter setting.

|  | Transition | $\lambda$ | $\pi$ |
|---|---|---|---|
| Offensive behavior | Scan_Vulnerability | 6 | 0.2365 |
|  | Crack_Password | 10 | 0.3768 |
|  | Enhance_permission | 6 | 0.6679 |
|  | Install_sniffer | 5 | 0.9013 |
|  | Steal_information | 10 | 0.8451 |
| Defensive behavior | IDS_scan | 8 | 0.3256 |
|  | Cheat_attacker | 8 | 0.4531 |
|  | Blockade_IP | 8 | 0.8215 |
|  | Remove_sniffer | 10 | 0.9324 |

According to this result, in this case, the defense mechanism of the system only needs to care about the attacker's attack ability and expected benefits and can not consider the attacker's attack rate.

*5.1.2. Average Time of Successful Intrusion.* Because the whole attack process is a progressive process, the attacker through step-by-step intrusion system components ultimately achieves the goal of stealing system confidential data. Therefore, the average time $\overline{T}_a$ of an attacker's successful intrusion can be calculated as follows.

First of all, the response time $T_a^i = 1/TH_a$ of an attacker to complete an attack on a subtarget, where $TH_a$ is the throughput of transition in the model.

Secondly, $TH_a = \sum_{M\in H} P[M]\lambda_a$, where $H$ is the marker set of attack transition, and $\lambda_a$ is the rate of attack transition;

Finally, $\overline{T}_a = \sum_{i=1}^{n} T_a^i/n$, where $n$ refers to the number of subattack targets protected in the whole attack process.

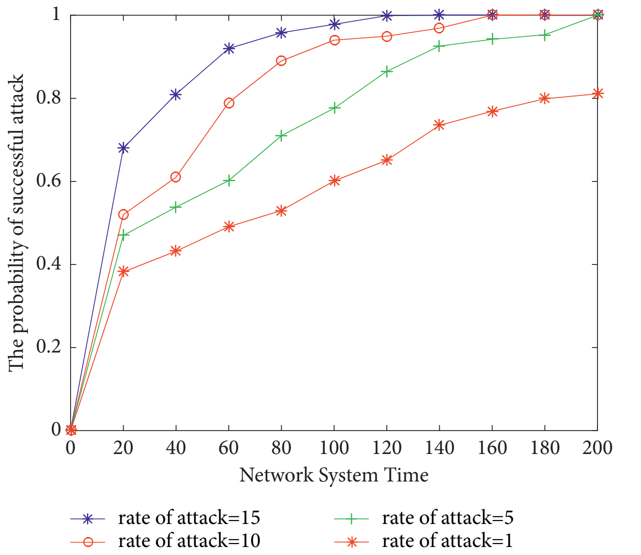

Figure 4: The probability of successful attack changes in the network, with $\lambda = 1, 5, 10, 15$, respectively.

Figure 5 shows that the average time of successful intrusion of attackers varies with the system time under different attack rates.

We find that the attack time of attackers increases with time under different attack rates. Moreover, the higher the attack rate is, the more attack time is needed. This is because the higher the attack rate is, the easier the attack behavior is to be found. On the contrary, the smaller the attack rate is, the less it is to be found. Therefore, less time is needed for the successful attack. This result is completely in line with the actual situation.

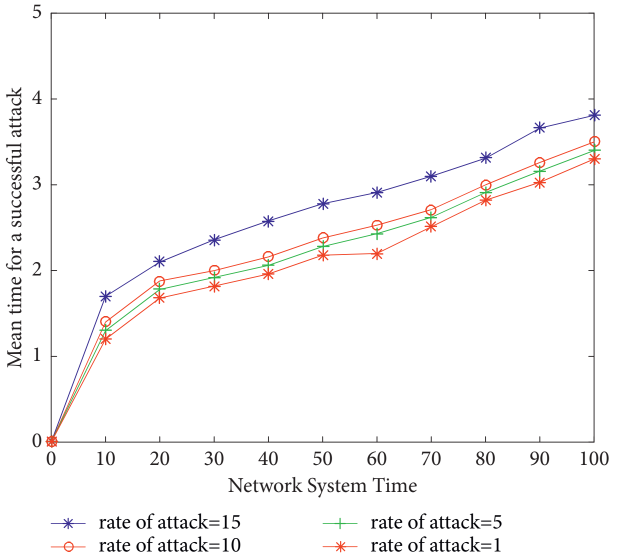

Figure 5: Mean time for a successful attack changes in the network, with $\lambda = 1, 5, 10, 15,$ respectively.

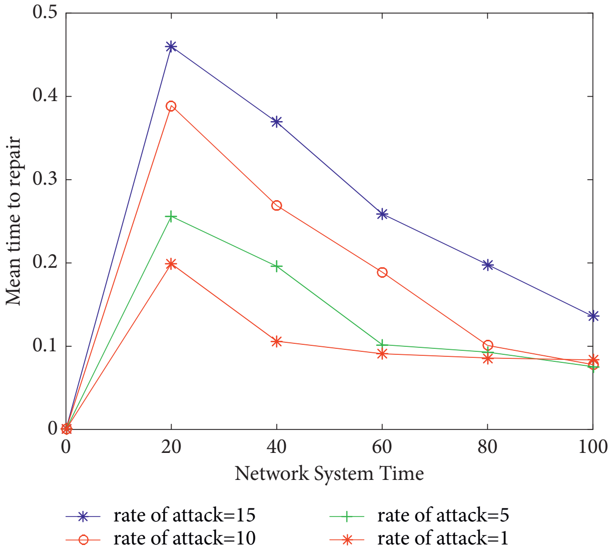

Figure 6: Mean time to repair (MTTR), with $\lambda = 1, 5, 10, 15,$ respectively.

*5.1.3. Mean Time to Repair (MTTR) of the System.* System repair time refers to the time from system failure to normal operation. If the location of the identifier in the model is regarded as a queue, the average repair time of the system can be understood as the average time of the identifier starting from $P_1$ and returning to $P_0$. Therefore, we define the average repair time of the system as follows: $\text{MTTR} = \overline{N}/\lambda^*$, where $\overline{N}$ is the average length of the queue and $\lambda^*$ is the average rate of arrival of the queue.

Figure 6 shows the average system repair time versus system time under different attack rates.

As shown in Figure 6, the average repair time of the system increases first and then decreases. This is because, in the initial stage of system attack, the system needs to spend a certain amount of time to find the intrusion point and then repair it. Moreover, we also found that the higher the attack rate, the longer the average repair time of the system. This is because higher intrusion frequency will bring more difficulties to the repair of the system.

In addition, through the analysis of the above experiments, we should note that, in the initial stage of the attack, the lower the frequency of the attack, the smaller the intrusion time, ultimately making the average repair time of the system not lower than that of the high-frequency attack, which is an important conclusion that is easy to be ignored. From this result, we conclude that low-frequency attack behaviors will also have a serious impact on the security of the system, and sometimes even more destructive than high-frequency behaviors, because it occurs at the beginning of the attack event.

### *5.2. Overall Evaluation of Network System Security*

*5.2.1. Reliability.* Reliability refers to the probability that the network system will continue to provide a certain network service within a certain period of time, and it reflects the continuity of the network system's safe operation [28]. Therefore, in the security research of the network system, we are concerned about the ability of the network system to provide certain network services normally and continuously.

If $S_R$ is the state set when the system provides a certain normal network service, and $X(t)$ represents the state of the system at time $t$, the mathematical expression of the instantaneous reliability $A_{\text{reliablitty}}(t)$ of the system in time $[0, t]$ is as follows.

Suppose $X(0) \in S_R, \tau = \inf\{t\colon X(t) \notin S_R\}$, and then $A_{\text{reliability}}(t) = P\{\tau > t\}$.

When performing quantitative calculations, we generally use MTTF to describe the steady-state reliability of the system, also known as the inherent reliability of the system, which can express mathematical expectations:

$$\text{MTTF} = E[\tau]. \tag{9}$$

*5.2.2. Availability.* Availability refers to the ability to complete the specified functions in a repairable network system in a specified manner of use and maintenance, and within a given time [29]. In the security research of the network system, we are concerned about the steady-state availability of the repairable system, which is mainly used to reflect the specific performance of the process of alternate changes (normal↔failure) between the state of the network system. Suppose that $X(u)$ represents the state of the system at time $u$, $S_A$ is the set of the system in a normal operating state, and $\pi_i$ is the steady-state probability of the system at time $i$. Then, the mathematical expression of the steady-state availability $A_{\text{availability}}$ of the network system in time $[0, t]$ is

$$A_{\text{availability}} = \lim_{t \longrightarrow \infty} \frac{\int_0^t P\{X(u) \in S_A\} \mathrm{d}u}{t} = \sum_{i \in s_A} \pi_i. \tag{10}$$

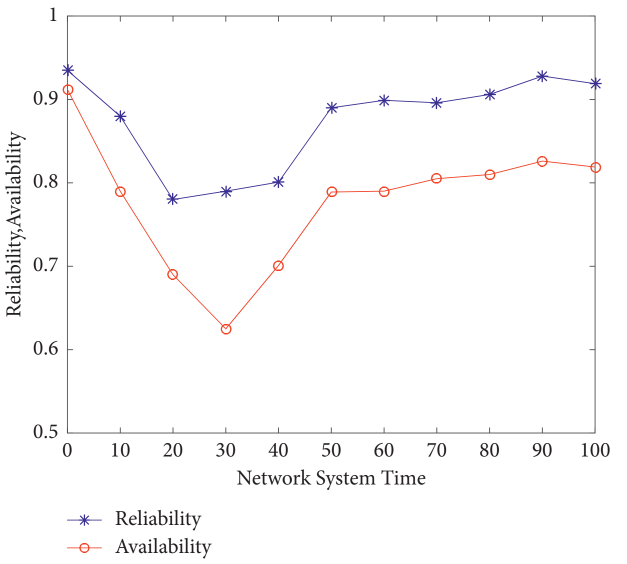

Figure 7: The changes of reliability and availability with system time.

According to the above formula and the parameter settings in Section 4, we can obtain the changes of reliability and availability with system time, as shown in Figure 7.

From the figure, we can clearly find that the change trend of reliability and availability is that it will gradually decrease at the beginning and then slowly rise to a certain value over time. This performance result is fully in line with the development trend of network attack events. Therefore, for network system administrators, attack behavior should be detected as early as possible, or the attack behavior can be predicted in advance, which is very important to the security of the network system.

## 6. Conclusion

This paper presents a novel modeling method for analyzing network attack events (AD-SEGPN), which can deal with the dynamic game problems in network attack and defense environment. This model not only inherits the game framework of evolutionary game theory, but also fully absorbs the advantages of stochastic Petri net, which can be used to model flexibly.

Through a series of experimental analysis, we can conclude that when the system is in a stable state, the success rate of the attacker's attack has little to do with the rate of attack behavior, which is an important conclusion. According to this conclusion, for a network system, if the system has established a defense mechanism, then the administrator of the system should focus on the attacker's attack ability and his expected return, regardless of the attacker's attack frequency. In addition, we also calculate the trend of intrusion success rate, average intrusion time, and average system repair time with system time under different attack rates. The results show that, for a repairable network system, the lower the attack frequency, the greater the damage to the network, which requires the administrator of the network system to pay attention to the low-frequency detection and prevention of frequent attacks. In the future, our work will focus on optimizing models to meet the needs of more complex network environments and multiple types of network systems [30].

## Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

This study was supported by Hebei Province Key Research and Development Program (19270318D), Hebei Province Internet of Things Monitoring Engineering Technology Research Center (no. 3142018055), National Key Research and Development Program of China (no. 2018YFC0808306), and Qinghai Province Internet of Things Key Laboratory (no. 2017-ZJ-Y21) project.

## References

[1] F. Jiang, Y. Fu, B. B. Gupta et al., "Deep learning based multi-channel intelligent attack detection for data security," *IEEE Transactions on Sustainable Computing*, vol. 5, no. 2, pp. 204–212, 2020.

[2] A. K. Chorppath and H. Boche, "Bayesian mechanisms and detection methods for wireless network with malicious users," *IEEE Transactions on Mobile Computing*, vol. 15, no. 10, pp. 2452–2465, 2016.

[3] L. Tingting, "Research on hidden malicious user detection problem," *Security and Communication Networks*, vol. 7, no. 6, pp. 958–963, 2014.

[4] H. Zhou, C. Wu, M. Jiang et al., "Evolving defense mechanism for future network security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 45–51, 2015.

[5] G. Zhao and J. Song, "Network security model based on active defense and passive defense hybrid strategy," *Journal of Intelligent & Fuzzy Systems*, vol. 39, no. 6, pp. 8897–8905, 2020.

[6] X. Liang and Y. Xiao, "Game theory for network security," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 472–486, 2013.

[7] M. H. Manshaei, Q. Zhu, T. Alpcan, and J. P. Hubaux, "Game theory meets network security and privacy," *ACM Computing Surveys*, vol. 45, no. 3, pp. 1–39, 2013.

[8] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," *Book A Survey of Game Theory as Applied to Network Security Series A Survey of Game Theory as Applied to Network Security*, 'University of Hawai'i'; Shidler College of Business, Honolulu, Hawaii, 2010.

[9] R. Anderson, "Why information security is hard-an economic perspective," in *Proceedings of the Seventeenth Annual Computer Security Applications Conference*, pp. 358–365, IEEE Computer Society, New Orleans, LA, USA, 2001.

[10] J. S. Shamma, "Game theory, learning, and control systems," *National Science review*, vol. 7, no. 7, pp. 1118-1119, 2020.

[11] H. Wu, W. Wang, C. Wen, and Z. Li, “Game theoretical security detection strategy for networked systems,” *Information Sciences*, vol. 453, pp. 346–363, 2018.

[12] Y. Li and T. Chen, “False data injection attacks on networked control systems: a Stackelberg game analysis,” *IEEE Transactions on Automatic Control*, vol. 63, no. 10, pp. 3503–3509, 2018.

[13] L. Liu, C. Huang, Y. Fang, and Z. Wang, “Network attack and defense game theory based on Bayes-nash equilibrium,” *KSII Transactions on Internet and Information Systems*, vol. 13, no. 10, pp. 5260–5275, 2019.

[14] H. Zhang, L. Jiang, S. Huang, J. Wang, and Y. Zhang, “Attack-defense differential game model for network defense strategy selection,” *IEEE Access*, vol. 7, pp. 50618–50629, 2019.

[15] S. Guan, J. Wang, H. Yao, C. Jiang, Z. Han, and Y. Ren, “Colonel blotto games in network systems: models, strategies, and applications,” *IEEE Transaction on Network Science and Engineering*, vol. 7, no. 2, pp. 637–649, 2020.

[16] J. Tan, H. Zhang, H. Zhang, H. Hu, C. Lei, and Z. Qin, “Optimal temporospatial strategy selection approach to moving target defense: a FlipIt differential game model,” *Computers & Security*, vol. 108, Article ID 102342, 2021.

[17] Q. Gao, H. Wu, Y. Zhang, and X. Tao, “Differential game-based analysis of multi-attacker multi-defender interaction,” *Science China Information Sciences*, vol. 64, no. 12, 2021.

[18] H. Zhang, W. Han, X. Lai, D. Lin, J. Ma, and J. Li, “Survey on cyberspace security,” *Science China Information Sciences*, vol. 58, no. 11, pp. 1–43, 2015.

[19] F. Čapkovič, “Petri nets at modelling and control of discrete-event systems containing nondeterminism -- Part 1,” *Computing and Informatics*, vol. 37, no. 5, pp. 1258–1292, 2018.

[20] X. Xiaohu Li, P. Parker, and S. Shouhuai Xu, “A stochastic model for quantitative security analyses of networked systems,” vol. 8, no. 1, pp. 28–43, 2011.

[21] A. Ramos, M. Lazar, and J. J. P. C. Rodrigues, “Model-based quantitative network security metrics: a survey,” *IEEE Communications Surveys and Tutorials*, vol. 19, no. 4, pp. 2704–2734, 2017.

[22] R. Rongfei Zeng, Y. Yixin Jiang, C. Xuemin Shen, and X. Shen, “Dependability analysis of control center networks in smart grid using stochastic Petri nets,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1721–1730, 2012.

[23] L. S. Shapley, “Stochastic games,” *Proceedings of the National Academy of Sciences*, vol. 39, no. 10, pp. 1095–1100, 1953.

[24] W. Sun, X. Kong, D. He, and X. You, “information security problem research based on game theory,” in *Proceedings of the 2008 International Symposium on Electronic Commerce and Security*, pp. 554–557, IEEE, Guangzhou, China, 2008.

[25] X. Liu, H. Zhang, Y. Zhang, and L. Shao, “Optimal network defense strategy selection method based on evolutionary network game,” *Security and Communication Networks*, vol. 2020, Article ID 5381495, 2020.

[26] J. Li, G. Kendall, and R. John, “Computing Nash equilibria and evolutionarily stable states of evolutionary games,” *IEEE Transactions on Evolutionary Computation*, vol. 20, no. 3, pp. 460–469, 2016.

[27] D. Balkenborg and D. Vermeulen, “Where strategic and evolutionary stability depart-A study of minimal diversity games,” *Mathematics of Operations Research*, vol. 41, no. 1, pp. 278–292, 2016.

[28] X. G. Chen, “Research on reliability of complex network for estimating network reliability,” *Journal of Intelligent & Fuzzy Systems*, vol. 32, no. 5, pp. 3551–3560, 2017.

[29] X. Hao, P. Fu, Y. Huang, M. Mao, and J. Zhang, “Availability and determinacy evaluation of ITER-PPEN communication network,” *Journal of Fusion Energy*, vol. 35, no. 4, pp. 626–633, 2016.

[30] H. Kwon, Y. Kim, H. Yoon, and D. Choi, “Optimal cluster expansion-based intrusion tolerant system to prevent denial of service attacks,” *Applied Sciences*, vol. 7, no. 11, 2017.