Attack and Defense Strategy for Infection Network System with Two Early Warning Mechanism

Jiaheng Wang¹, Die Chen¹ and Fu Chen²

1. School of Mathematical Sciences, University of Electronic Science and Technology of China, Chengdu, Sichuan, 611731, P.R. China
2. National Demonstration Center for Experimental Computer Education, University of Electronic Science and Technology of China, Chengdu, Sichuan, 611731, P.R. China

E-mail: chenfu@uestc.edu.cn

Abstract. As the progress of IoT technology, Cyber-Physical System gradually becomes the basic pillar of people's daily life. Contrary to its convenience, Cyber-Physical System could be easily broken by attackers and these attacks infect the system and affect more systems, thus interfering with people's normal work and life. In this context, this paper establishes a system defense model for the propagable network with the warning mechanism as the core. The system defense model includes warning components, which trigger the first and second warning mechanisms, and components protection and camouflage components. After deducing the reliability of the defense model system, this paper considers the influence of different parameters about the system reliability and analyzes the relationship between warning components, camouflage components, and system reliability. Based on the different parameters that affect the system reliability, this paper proposes the optimal defense deployment strategy under the attack optimal strategy and obtains the basic principles of the deployment of defense measures through numerical analysis. Finally, the simulation experiments of different systems prove the rationality and correctness of the proposed model.

1. Introduction

Network systems have become the basic part of various infrastructures and physical systems. However, risk of system damage is coexisting with the convenience of life. Recently, information security problems have slowly emerged. The system is often paralyzed by attacks, affecting people’s work and life. Due to the complexity and variability of cyberspace, attacks have become a serious threat to cyberphysical systems. What’s more, the network system will infect other components, which greatly reduces the reliability of the system. Therefore, the defense research of the system under attack has received extensive attention.

At present, the defense research of the system can be classified according to the system structure, defense measures and attack strategy [1]. Among them, the system structure is further divided into unit system, series system, parallel system, series-parallel system, network system, multiple system, interdependence system and other types of system structures. Defense measures are divided into system component separation, redundancy, protection, multi-level defense, camouflage deployment, and preventive strikes. Attack strategies and attack environments are divided into attacks on single elements, attacks on multiple elements, sequence attacks, random attacks, combined attacks...
(attacks and faults) with intentional and unintentional effects, incomplete information attacks, and variable resource attacks.

To improve system reliability, the best way is to reduce the probability of system being destroyed [2]. Nowadays, to improve the system reliability, researchers mainly use three methods, including protection method, camouflaging method, and redundancy method. In addition to deploying defensive measures, we also need to find the optimal defensive resource distribution plan to improve system reliability.

Using these methods and finding the optimal defensive resource distribution plan are extremely important. Hausken and Levitin [4] studied the optimal defense resource allocation between protecting real system elements and deploying camouflage elements in tandem systems. It is assumed that an attacker cannot distinguish between a disguised element and a real element, and if any real element is destroyed, the system will also be destroyed. Deploying camouflage components can reduce the probability of critical components being attacked [5]. Levitin [6] considered the optimal component separation and protection of complex multi-state serial-parallel systems, and proposed an algorithm to determine the expected damage of strategic attackers. Levitin and Hausken ([7]) studied the optimal strategies for attack and defense when two attackers attacked the system continuously. Analyze the pseudo-target and resource allocation of the protection core components, and adopt the minimum and maximum two-stage countermeasures. [8,9] studied the optimal strategy of an attacker to a parallel system under limited attack resources.

There are also many literatures studying system reliability and defense strategy of the network system. Bell et al. [10] designed a method of road network vulnerability analysis based on game theory is proposed. Gharbi et al. [11] designed a branch-and-bound algorithm, with the minimum attack cost as the target, and the optimal attack strategy for disconnecting the network is determined. Levitin et al. [12] propose a method for evaluating the expected damage caused by a deliberate attack on a randomly selected network link, which decomposes a complex network with a given topology into isolated subnetworks (cluster). Lin et al. [13] have proposed an effective resource allocation strategy to maximize the cost of the attacker and minimize the probability of damage to the “core node” of the network, thereby improving the protection capabilities of the network. Ramirez-Marquez et al. [14] provide optimal protection configurations for a network with components vulnerable to an interdictor with potentially different attacking strategies.

Deploying the early warning mechanism is also particularly a important way to enhance system reliability. In the study of system reliability, the early warning mechanism is that the system uses network threat intelligence to mitigate possible damage caused by the threat. The network early warning mechanism can take various forms such as proxy firewall, network monitoring, honeypot and intrusion prevention module. Chen [15] has verified that the early warning mechanism has a great effect on improving the reliability of the parallel network.

The rest of the paper is organized as follows. In the second chapter, by deploying pseudo-target components and early warning components, the early warning mechanism is designed, and the system defense model of the infectious network is constructed. The third chapter analyzes the system defense model of infectious networks and examines the impact of different variables on system reliability. Chapter four designs an algorithm to calculate the optimal system defense resource allocation strategy and its system reliability. Chapter 5 simulates the model to verify the consistency of the model theory and experiment. Table 1 shows the main symbols used in this article:
Table 1. Notations.

| Notation | Description                        |
|----------|------------------------------------|
| $N_p$    | amount of working components       |
| $N_c$    | amount of camouflage components   |
| $N_w$    | amount of early warning components |
| $N_s$    | amount of total components         |
| $R_d$    | defense resource                   |
| $R_a$    | attack resource                    |
| $r_d$    | defense resource on one working component |
| $r_a$    | attack resource on one attack      |

2. Establishment of defense model

Introduction of Model

The establishment and derivation of the model is based on two assumptions:
1. The attacker is not able to distinguish the components of the system and the attacks will randomly hit on the components of the system.
2. The infection process begins only after the attack process is completely completed.

In this paper, protection, camouflage components and early warning components are taken as the defense measures of the cyber system. The core of these measures is the early warning mechanism. The early warning mechanism we adopt is divided into two types:
1. The first type of early warning mechanism is triggered by an early warning component, which is called No. 1 warning. When the warning component is under attacked, the No. 1 warning is activated. The No. 1 early warning will prevent attacks process and the infection process of the attack source in the system network.
2. The second type of early warning mechanism is the self-protection early warning mechanism of the network system, which is called No. 2 warning. When a working component in the system is damaged due to infection, the No. 2 warning is activated to block the next round of infection in the network system. A round of infection means that all the damaged working components transmit the attack to the unbroken working components.

Suppose that the cyber system deploys $N_p$ working components, $N_c$ camouflage components, $N_w$ early warning components. The cyber system is compromised if and only if all the working components are destroyed. As a defender, we can allocate the defense resources for system defense. Assume the resources required to build a camouflage component is $C$, the resources required to deploy an early warning component is $W$, the resources required to build a network system early warning mechanism (No.2 warning) is $Y$. Then, the rest of resources are used to protect working components, so the resources on one working component is

$$r_d = \frac{R_d - N_c \times C - N_c \times W - Y}{N_p} \quad (1)$$

On the other hand, suppose that the attack resource is $R_a$, the number of attacks $N_a$ can be determined by the attacker, then the cost of each attack is $r_a = R_a/N_a$.

Since the working component is equipped with protection measures, so when considering the probability of the working component being destroyed, We decide to utilize the Contest Success Function (CSF) Tullock [16] to calculate the probability of the damage of a component. The success function is as follows

$$v(r_a, r_d) = \frac{r_a^m}{r_a^m + r_d^m} \quad (2)$$
where $r_a$ represents the resources on one attack, $r_d$ represents the resources on one working component, assume $m \geq 0$.

Figure 1 shows the attack process. Suppose that the system contains 3 working components, 2 camouflage components and 1 early warning component. According to the model assumption, the attacker will randomly launch an attack on the system. In Figure 1, it can be seen that working components and camouflage components are hit by first six attacks and the early warning component is hit by the seventh attack. When the No.1 warning is triggered, the remaining attacks are blocked.

**Figure 1** No.1 warning mechanism and attack process.

Figure 2 shows the infection process. Since the attack infection process does not involve other components, only the working components are shown here. The system consists of three working components, of which component 1 was destroyed during the attack process. It was not transmitted to component 3 during the first round of infection, but was transmitted to component 2. At this time, the No. 2 early warning is triggered to cut off the next round of infection, so the system is protected.

**Figure 2** No.2 warning mechanism and infection process.
2.1. Derivation of system reliability

In order to compromise a network system, an attacker must destroy all of working components. The reliability of an infectious network system with two early warning mechanisms are shown as follows. Some text.

When the attack process is completed, the working components damaged by attacks will spread the attack to the rest of working components. We assume that the infection matrix as follow

\[
P = \begin{pmatrix}
  0 & P_{12} & P_{13} & \cdots & P_{1n} \\
  P_{21} & 0 & P_{23} & \cdots & P_{2n} \\
  P_{31} & P_{32} & 0 & \cdots & P_{3n} \\
  \vdots & \vdots & \vdots & \ddots & \vdots \\
  P_{n1} & P_{n2} & P_{n3} & \cdots & 0
\end{pmatrix}
\]

(3)

where \( P_{ij} \) represents the probability that the \( i \)-th working component is infected to the \( j \)-th working component.

For the \( i \)-th working component, as shown by equation (2), its destruction probability can be expressed as

\[
p_i = 1 - (1 - v(r_i, r_d))^{k_i}
\]

(4)

Where \( k_i \) represents the number of attacks on the \( i \)-th working component.

Theorem 1. The infection network system reliability is

\[
S = 1 - P_1 - P_2 - P_3
\]

(5)

where

\[
P_i = \sum_k \frac{1}{(N_k^s)^N_p} \prod_{t=1}^{N_p} \left( N_a - \sum_{j=1}^{t-1} k_j \right) \left( N_a - \sum_{j=1}^{N_p} k_j \right)^{N_a - \sum_{j=1}^{N_p} k_j} \times \prod_{i=1}^{N_p} p_i
\]

(6)

with \( K = \{(k_1, \ldots, k_{N_p})|k_1 + \ldots + k_{N_p} \leq N_a\} \).

and

\[
P_2 = \sum_{j=1}^{N_p} \sum_{j_1}^{N_p} \frac{N_w}{(N_0^s)^j} \prod_{m=1}^{j} \left( j - 1 - \sum_{s=1}^{m-1} l_s \right) \times N_a^{j-1} \sum_{i=1}^{N_0^s} \prod_{s=1}^{N_0^s} p_i
\]

(7)

with \( L = \{(l_1, \ldots, l_{N_0^s})|l_1 + \ldots + l_{N_0^s} \leq j - 1\} \)

and

\[
P_3 = \sum_{k} \left( \frac{1}{(N_0^s)^N_p} \prod_{t=1}^{N_p} \left( N_a - \sum_{j=1}^{t-1} k_j \right) \left( N_a - \sum_{j=1}^{N_p} k_j \right)^{N_a - \sum_{j=1}^{N_p} k_j} \times \sum_{m=1}^{N_0^s} \sum_{s=1}^{N_0^s} \prod_{i=1}^{N_0^s} \left( 1 - p_s \right) \times \prod_{s=1}^{N_0^s} \prod_{s=1}^{N_0^s} P_{i,s}^{b_{i,s}} \right)
\]

(8)

with \( P_{b_{i,s}}^{b_{i,s}} = 1 - (1 - P_{b_{i,s}}) \cdots (1 - P_{b_{i,s}}) \), \( B_s = \{ (\beta_1, \ldots, \beta_{N_p}) | \beta_i \neq \beta_j, k \neq j, \beta_k \in \{1, 2, \ldots, N_p\} \} \), \( \beta_k \in b_{i,s} \in B_s \).

Next, we give an example.

Example 1. Assume that an infectious network system consists of \( N_p = 3 \), \( N_a = 1 \), \( N_e = 2 \), \( R_d = 15 \). The resources required for the deployment of early warning components \( W = 3 \), the deployment of camouflage components \( C = 1 \), the deployment of No.2 warning mechanism \( Y = 4 \).

The total attack resources are \( R_a = 10 \). Assume \( N_a = 5 \). According to equation (1), we use \( m=1 \) during the calculation.
According to equation (6), we have

\[ v(r_a, r_b) = \frac{r_a}{r_a + r_b} = 0.5 \]

According to equation (7), we have

\[ P_1 = \sum_k \left( \frac{1}{(6)^3} \prod_{t=1}^{3} \left( 5 - \sum_{j=1}^{t-1} k_j \right) \right)^2 \sum_{j=1}^{3} k_j \times \prod_{i=1}^{3} \left( 1 - 0.5^i \right) = 0.01748 \]

According to equation (8), we have

\[ P_2 = \sum_{j=1}^{5} \sum_{m=1}^{3} \left( \frac{1}{(6)^3} \prod_{m=1}^{3} \left( j - 1 - \sum_{s=1}^{m-1} t_s \right) \right)^2 \sum_{s=1}^{3} t_s \times \prod_{n=1}^{3} \left( 1 - 0.5^n \right) = 0.0022 \]

According to equation (8), we have

\[ P_3 = \sum_k \left( \frac{1}{(6)^6} \prod_{t=1}^{3} \left( 5 - \sum_{j=1}^{t-1} k_j \right) \right)^2 \prod_{s=1}^{3} k_s \times \prod_{m=1}^{3} \prod_{n=1}^{3} p_i \prod_{x \in \mathbb{N}} \prod_{y \in \mathbb{N}} P_{m_x} = 0.0525 \]

Therefore, the system reliability is

\[ S = 1 - P_1 - P_2 - P_3 = 0.9278 \]

### 3. Analysis of System Reliability

In this chapter, we do a study about different parameters which affect the reliability of the system. Since the infection matrix will vary with the network structure of the cyber system and the allocation of resources, in order to eliminate the influence of the infection matrix, the infection matrix is set to be 0.2 except for diagonal elements, the infection matrix shows as follow:

\[
P = \begin{pmatrix}
0 & 0.2 & 0.2 & \cdots & 0.2 \\
0.2 & 0 & 0.2 & \cdots & 0.2 \\
0.2 & 0 & 0.2 & \cdots & 0.2 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0.2 & 0.2 & 0.2 & \cdots & 0
\end{pmatrix}
\]

In the various cases studied below, the resources required as \( W = 3 \), \( C = 1 \) and No.2 warning mechanism \( Y = 4 \).

Number of attacks. Suppose that the infect network system consists of \( N_p = 3 \), \( N_a = 1 \), \( N_i = 4 \), \( R_i = 15 \). Figure 3 shows the system reliability with \( R_a = 20, 30, 40 \). It is obvious that when the number of attacks increases, the system reliability shows a U-shaped curve. This case can be explained as follows: When the number of attacks is small, the probability of the early warning mechanism being triggered is very low, and the attack poses a great threat to the system, so the reliability of the system begins to decline significantly. When the number of attacks increases to a larger number, the probability of the occurrence of the No. 1 and No. 2 early warning mechanisms increases. The early warning mechanism begins to work, shielding the launch of attacks and preventing the spread of attacks in the system. Although the number of attacks is increasing, the early warning mechanism of the system defense is more powerful. Thus, as the number of attacks increases, the system reliability also increases, resulting in a U-shaped curve.
Figure 3 The system reliability with different number of attacks.

Camouflage components. We assume the infect network system consists of $N_p = 3$, $R_d = 55$, the attack resources are $R_a = 30$. Figure 4 shows the system reliability with $N_a = 5, 10, 15$.

Figure 4 The system reliability with different number of camouflage components.

From Figure 4, it can be seen that the camouflage components cause a great influence on protecting the system when the number of attacks is small. But when the number of attacks is large, increasing the number of camouflage components will reduce the system reliability. This is because when the number of attacks is small, the probability that the attack hits the working component of the system is also very small, so the increase of the camouflage components is able to protect the working component. However, when the number of attacks is much greater than the number of working components, the increase in camouflage components only cause the probability of triggering the early warning mechanism to be greatly reduced, thereby reducing the system reliability.

Early warning components. Suppose that the infect network system consists of $N_p = 3$, $N_e = 4$ and $R_d = 55$, $R_a = 30$. Figure 5 shows the system reliability under different numbers of attacks, with $N_a = 5, 10, 15$. 

![Graph](image)
Figure 5 The system reliability with...

It can be observed that the overall of the three curves are monotonically increasing and tending to a stable trend. When $N_c$ is small, the system reliability increases greatly with the increase of $N_c$; but when $N_c$ is large, the reliability of the system increases slightly, and eventually stabilizes. It can be seen from the Figure 5 that after designing the early warning component, the more the system suffers from attacks, the higher the system reliability. This is because the more attacks the attacker launches, the higher the probability of hitting the early warning component. It is more possible to trigger No.1 warning mechanism to protect the system and obtain higher system reliability. However, after $N_c$ reaches a certain level, the system reliability no longer increases, indicating that the early warning components do not need to be designed too much to ensure high system reliability.

Based on the influence of different variables, the study of optimal strategy is as follow.

4. Optimal strategy
In this chapter, we discuss the optimal defense strategy of network system. Through this strategy, we will achieve maximum system reliability when faced with different attack strategy.

4.1. Optimal Defense Strategy
Consider a max–min problem as follows:

$$S_{\text{max}\text{min}} = \max \min \{S(N_c, N_w, N_a)\}$$

where the $S(N_c, N_w, N_a)$ represents system reliability when the system deploys $N_c$ camouflage components, $N_w$ early warning components and is attacked by $N_a$ attacks.

Assume that the defense resources available for the system are $R_d$, then the maximum deployable number of pseudo-target components is $\lfloor R_d / C \rfloor$, the maximum number of deployable warning components is $\lfloor R_d / W \rfloor$, then we can calculate the system reliability matrix

$$M = (S_{ik})_{\lfloor R_d / W \rfloor \times \lfloor R_d / C \rfloor \times N_a}$$

Where i represents $N_c$, j represents $N_w$, and k represents $N_a$. $S_{ik}$ represents the system reliability. Then, the defense strategy of the system can be defined as $\text{strategy}(i,j)$. We can use algorithm 1 to calculate the optimal strategy and its system reliability.
Table 2. Algorithm 1 Optimal defense strategy algorithm.

| Algorithm 1 Optimal defense strategy algorithm |
|-----------------------------------------------|
| **Input:**                                     |
| System reliability matrix: $M = (S_{ik})$       |
| Zero vector: $Z_{ik} = 0$                      |
| **Output:**                                    |
| Best strategy: $strategy(i^*, j^*)$            |
| System reliability: $S_{\text{maximin}}$       |

1: $S_{\text{maximin}} = 0$
2: for $i \leftarrow 0$ to $\lfloor R_a/W \rfloor$ do
3:     for $j \leftarrow 0$ to $\lfloor R_a/C \rfloor$ do
4:         $Z_{ij} = 1$
5:         if $W \times i + C \times j \leq R_a$ then
6:             for $k \leftarrow 0$ to $N_a$ do
7:                 if $Z_{ik} > S_{ijk}$ then
8:                     $Z_{ik} \leftarrow S_{ijk}$
9:             end if
10:         end for
11:     end if
12:     end for
13:     if $S_{\text{maximin}} < Z_{ij}$ then
14:         $S_{\text{maximin}} \leftarrow Z_{ij}$; $i^* \leftarrow i$; $j^* \leftarrow j$
15:     end if
16: end for
17: end for
18: **return** $(S_{\text{maximin}}, strategy(i^*, j^*))$

4.2. Examples

In this section, for the purpose of explaining the optimal defense strategy algorithm, we conduct a study of actual numerical cases. In the research, the element of the attack infection matrix is set to 0.2.

Example 2. Suppose that the system consists of $N_x = 3$. The resources required as $W = 5$, $C = 1$ and No.2 warning mechanism $Y = 10$. Consider the defender owns defense resource $R_d = 25$ and the attacker owns attack resource $R_a = 30$ with maximum number of attacks $N_a = 25$. From Figure 6, we can clearly observe that the system reliability increases as $N_a$ increases. And the system reliability increases first and then decreases with $N_a$. This is because too many camouflage components will greatly reduce the probability of the early warning component being hit, thereby reducing the probability of the system being protected by the early warning mechanism. Also, allocating too many camouflage components will cause the working component to be protected resources too low, so when allocating resources to camouflage components, we should choose a moderate amount to allocate.

As can be seen from Figure 6, the inspiration from this experiment is that when deploying defensive measures, $N_a$ should be set as large as possible, and $N_c$ should be set to moderate.
Example 3. Assume that the system consists of 3 working components. The resources required to deploy a camouflage component are $C = 1$ and the resources required to deploy an early warning component are $W = 7$, and the resources required to deploy No.2 warning are $Y = 10$. Consider the defender owns defense resource $R_d = 20, 30, ..., 90$ and the attacker owns attack resource $R_a = 30$ with maximum number of attacks $N_a = 25$. The right y axis shows the amount of components with the optimal strategy, and the left y axis is the system reliability corresponding to optimal strategy. We obviously saw that when the defense resources increase, the system reliability also increases. It shows that with fewer defense resources prioritizing early warning components is a best choice. With larger the defense resources are large, we need to set the camouflage component first.

So this experiment inspires us that when the system defense resources are small, we should give priority to increase $N_w$ and choose a moderate $N_c$; and when the system defense resources are large, we should deploy a large amount of camouflage components to increase system reliability.

5. Simulation
In this part, we give a simulation on the model and the element of the attack infection matrix is set to 0.2. Suppose that the system consists of $N_p = 3, N_w = 1, N_c = 4$. The resources required as $W = 3$,
\( C = 1 \) and No.2 warning mechanism \( Y = 5 \). Consider the defender owns defense resource \( R_d = 18 \) and the attacker owns attack resource \( R_a = 30 \).

![3 Components System Simulation](image)

**Figure 8** The simulation for the network system.

6. Conclusions

This paper studies the attack defense strategies of infectious network systems and establishes a defense model that includes camouflage components, protection and with early warning mechanisms as the core. We theoretically derive the system reliability, and analyzes the different parameters in the model. The optimal strategy is calculated by using the thought of max-min game. The simulation proves that the experiment of the model is highly consistent with the theory.

For the follow-up work in the future, we provide some new research directions according to the shortcomings of the system reliability research in this article. For example, the attacker can probably identify which components of a system are truly working components and launch different kinds of attack. Also, we assume that the infection process is based on rounds of infection, and future research can adjust the mode of infection to improve it. We hope that these studies will inspire more researches and help design a more safe network system.

Acknowledgements

D. Chen acknowledges the financial supports of The National Natural Science Foundation of China (No: 71871046) and The National Natural Science Foundation of China (No:11701070).

Appendix

Proof of Theorem 1: The proof contains three situations: first, the warning component is not hit and the system is destroyed; second, the warning component is hit and the system is destroyed; third, the system is destroyed by infection.

Case 1: The warning component is not hit and the system is destroyed. For this case, it means that all attacks are launched on working components or camouflage components. Suppose that the number of attacks on the i-th working component is \( k_i, i = 1, 2, ..., N_w \). Define this event as A. The probability of A is

\[
P(A) = \sum_{\mathcal{K}} \frac{1}{N_a^{N_a}} \prod_{t=1}^{N_w} \left( \frac{N_a - \sum_{j=1}^{t-1} k_j}{k_i} \right) \left( \frac{N_a - \sum_{j=1}^{t} k_j}{N_a - \sum_{j=1}^{t-1} k_j} \right)
\]

where \( \mathcal{K} = \{ (k_1, ..., k_{N_w}) | k_1 + ... + k_{N_w} \leq N_a \} \)

The compromise probability for the system in this case is
Case 2: The warning component is hit and the system is destroyed. Assume that the early warning components is attacked by the jth attack, which means the first j attacks are all on other components, where \( j = 1, 2, \ldots, N_p \). Assume that during the first \( j-1 \) attacks, the working components have been attacked \( l_1, l_2, \ldots, l_{N_p} \) times. The probability for this event, define it as \( B \), is

\[
P(B) = \sum_{j=1}^{N_a} \left( \frac{N_w}{N_b} \right)^j \prod_{m=1}^{N_p} \left( \frac{N_a - \sum_{s=1}^{m-1} l_s}{l_m} \right) \times \left( \frac{N_e - \sum_{s=1}^{m-1} l_s}{N_e - \sum_{s=1}^{m-1} l_s} \right) \times \prod_{i=1}^{N_p} p_i
\]

where \( L_j = \{ (l_1, \ldots, l_{N_p}) | l_1 + \ldots + l_{N_p} \leq j-1 \} \). For this case, the probability of this event is

\[
P_2 = \sum_{j=1}^{N_a} \left( \frac{N_w}{N_b} \right)^j \prod_{m=1}^{N_p} \left( \frac{N_a - \sum_{s=1}^{m-1} l_s}{l_m} \right) \times \left( \frac{N_e - \sum_{s=1}^{m-1} l_s}{N_e - \sum_{s=1}^{m-1} l_s} \right) \times \prod_{i=1}^{N_p} p_i
\]

Case 3: If there are \( N_p \) working components in the system and there are working components that are destroyed. We first calculate the probability of each \( b_m \in B_m \) infecting to the \( k \)-th unbroken working component according to the infection matrix and the number of damaged working components, the probability is as follow

\[
P_{b_m} = 1 - \left( 1 - P_{b_m} \right) \ldots \left( 1 - P_{b_m} \right)
\]

where \( B_k = \{ \beta_1, \ldots, \beta_k, k \neq j, \beta_k \subseteq \{ 1, 2, \ldots, N_p \} \} \)

Assume the system consists of \( N_p \) working components and there are working components destroyed. Define the event \( F_m \) as the system is attacked and destroyed, then the probability of the event is

\[
P(F_m) = \sum_{b_m} \prod_{t \in b_m} p_t \prod_{s \notin b_m} (1 - p_s) \times \prod_{s \notin b_m} P_{b_m}
\]

Then, the system is destroyed by infection

\[
P(F) = \sum_{m=1}^{N_p-1} \sum_{b_m} \prod_{t \in b_m} p_t \prod_{s \notin b_m} (1 - p_s) \times \prod_{s \notin b_m} P_{b_m}
\]

Finally, the probability of this case is

\[
P_3 = \sum_{k} \left( \frac{1}{N_b} \right)^N \prod_{t=1}^{N_p} \left( N_a - \sum_{j=1}^{t-1} k_j \right) \times \sum_{m=1}^{N_p} \sum_{b_m} \prod_{t \in b_m} p_t \prod_{s \notin b_m} (1 - p_s) \times \prod_{s \notin b_m} P_{b_m}
\]

References

[1] KJELL HAUSKEN and GREGORY LEVITIN, 2012 Review of Systems Defense and Attack Models J. International Journal of Performability Engineering, 8(4)

[2] Levitin G and Lisnianski A, 2003 Optimizing survivability of vulnerable series-parallel multi-state systems J. Reliab. Eng. Syst. Saf. 79(3) 319–31

[3] Levitin G and Hausken K, 2009 Redundancy vs. protection vs. false targets for systems under attack. J. IEEE Trans Relia 58(1) 58–68

[4] Hausken K and Levitin G, 2009 Protection vs. false targets in series systems. J. Reliab. Eng. Syst. Saf. 94(5) 973–81
[5] McQueen MA, Boyer WF, Flynn MA and Beitel GA, 2006 Time-to-compromise model for cyber risk reduction estimation. Quality of protection, 23. Springer, pp 49–64

[6] R. Peng, G. Levitin, M. Xie and et al, 2011 “Optimal defence of single object with imperfect false targets,” J. Journal of the Operational Research Society, 62 134–41

[7] G. Levitin and K. Hausken, 2013 “Is it wise to leave some false targets unprotected?” J. Reliability Engineering & System Safety, 112 176–86

[8] K. Hausken, and G. Levitin, 2009 “Parallel systems with different types of defence resource expenditure under two sequential attacks,” J. Journal of Risk & Reliability, 223, 71–85

[9] G. Levitin and K. Hausken, 2009 “Parallel systems under two sequential attacks,” J. Reliability Engineering & System Safety, 94 763–72

[10] Bell, M.G.H., Kanturska, U, Schmocker, J.-D., and Fonzone, A. 2008 Attacker-defender models and road network vulnerability. Philosophical Transactions of the Royal Society A: Mathematical, J. Physical and Engineering Sciences, 366(1872) 1893–906

[11] Gharbi, A., Azaiez, M.N., and Kharbeche, M. 2010 Minimizing Expected Attacking Cost in Networks. J. Electronic Notes in Discrete Mathematics, 36(August 1) 947–54

[12] Levitin, G., Gertsbakh, I., and Shpungin, Y. 2011 Evaluating the damage associated with the intentional network disintegration. J. Reliability Engineering & System Safety, 96(4) 433–9

[13] Lin, F.Y.-S., Tsang, P.H. and Lin, Y.L. 2007 Near Optimal Protection Strategies against Targeted Attacks on the Core Node of a Network. Proc. ARES’07

[14] Ramirez-Marquez, J.E. Rocco, C.M., and Levitin, G. 2011 Optimal Network Protection Against Diverse Interdictor Strategies. J. Reliability Engineering & System Safety, 96(3) 374–82

[15] D. Chen, M. Xu., and W. Shi, 2018 “Defending a cyber system with early warning mechanism,” J. Reliability Engineering and System Safety, 169 224–34

[16] G. Tullock, 1983 “Toward a theory of the rent-seeking society,” J. Southern Economic Journal, 48, 823