Mimic Defense System Security Analysis Model

Li Qinyuan 1, Han Jiajia 1, Sun Xin 1, Qin Junning 2, and Zhang Bo3*

1 State Grid Zhejiang Electric Power Research Institute, Hangzhou, Zhejiang, 310014, China
2 State Grid Zhejiang Electric Power CO., LTD, Hangzhou, Zhejiang, 310007, China
3 Nanjing University of Science & Technology, Nanjing, Jiangsu, 210094, China
*Corresponding author’s e-mail: zhangbo3@epri.sgcc.com.cn

Abstract. In this article, the mimic defense technology based on dynamic heterogeneous redundancy architecture is studied, and the mimic defense system is described formally to improve the proactive defense capability of information systems and key equipment in the network. A method integrating dynamic feature, heterogeneous feature and redundant feature that carries out security analysis of mimic defense system by probabilistic analysis is proposed for the lack of effective security assessment method about mimic defense system. Validated by simulation experiments simulating the attacker and the mimic defense system, this model can calculate the safety of the mimic defense system according to the attack factor, heterogeneity degree, dynamic transformation and other related factors. According to the research results, the proposed model is of certain guiding significance for helping designers to construct mimic defense system.

1. Introduction
During the development plan of the "10th Five-Year Plan" period, it was clearly pointed out that all directions of rapid development in China cannot be separated from the support of the information industry. Information technology plays a role as a booster for the development of various fields such as people's livelihood, economy, and national defense. The information construction can be used to promote the development of new industries. Immediately after the "Thirteenth Five-Year Plan", it was pointed out that while pursuing the rapid development of information technology, we must pay more attention to the construction of network security and ensure the healthy development of information technology. While Internet technology is rapidly promoting the rapid development of power, finance, transportation and other industries, the continuous disclosure of security incidents at home and abroad has fully proved that the security of Internet technology is an important challenge in the current Internet development. Traditional cybersecurity defense techniques have increased the attacker's threshold of intrusion and blocked most types of attacks through a large number of rules. However, the traditional network security defense technology is often static before the attacker successfully invades, which allows the attacker to have sufficient time to study the attack target before the attack. Once obtaining the permission of target system, the attacker can continuously infiltrate the attack. In short, the traditional network security defense technology does not actively change over time, and the attacker's attack capability continues to increase with the increase of the amount of information and the intrusion technology, which makes the defender always in a passive defense position. Therefore, it has become an important research direction in the field of network security to break the situation of network attack and
defense where it is easy to attack but hard to defend, and break through the situation that network security defense relies on prior knowledge of network attacks, and construct a network security proactive defense mechanism[1].

Based on a "non-similar redundancy" structure with high availability and high reliability, the mimic defense technology[2] takes calculations or service components with equivalent function and different structure as element, cooperates with multi-mode voting mechanism without the basis on rules and features, and disturbs the attacker's judgment by nonlinear transformation of the external features of the system. According to the dynamic heterogeneous redundancy structure, using the harsh conditions that an attacker cannot construct an attack that satisfies all heterogeneous components at the same time, a dynamic scheduling policy that avoids coordinated attacks is introduced to make it difficult for an attacker to maintain the attack chain through a voting mechanism, and increase the difficulty of attackers to detect and scan.

In recent years, more and more research work and research results have focused on developing and advancing mimic defense technology. Proposed in Literature[3], a DHR (Dynamic Heterogeneous Redundancy) model with "dynamic heterogeneous redundancy" provides security architecture of guiding significance for the construction of mimic defense system; according to the DHR model, the literature [4] uses the multi-level structure of the web server to design the "dynamic heterogeneous redundancy" basis in the operating system layer and the server software layer, and realize the establishment of the mimic defense system in the field of web servers; in the literature [5], according to the DHR model, seven sets of heterogeneous redundant routing kits, such as ZTE ZXR10, FiberHome Fengine S5800, and Maipu MP3900, are applied in the router application layer to realize the establishment of mimic defense system in the router field. However, very little research has focused on the safety analysis methods of the mimic defense system.

Established in this paper based on the network attack chain and the dynamic heterogeneous redundancy characteristics of the mimic defense system, a security analysis model can be used to calculate the possibility that each key node in the mimic defense system can be successfully attacked, so that different parameters can be used to analyze the security defense effectiveness of the mimic defense system, which makes it easy for system designers to better understand how to use mimic defense technology to improve the security of key information systems.

2. Construction of mimic defense system security analysis model

2.1. Construction of mimic defense
The basic model of the dynamic heterogeneous redundancy model is mainly iPo model [6]. As shown in Figure 1, when entering the system, the submitted request input is first copied into n parts to be transmitted to the execution set through the input proxy unit. The execution set contains n non-similar redundant executables (P1, P2, P3, ..., Pn), where P1, P2, P3, ..., Pn are executive bodies with the same functions but different implementation methods; each executive body accepts a copy of the request and processes it; the response of processing result of each executive body is outputted after voting by the voter. Taking advantage of the cyber attack's dependence on the environment, an attack against a specific vulnerability cannot be effectively played in the heterogeneous executive body (P1, P2, P3, ..., Pn), thus achieving the defense against the vulnerability attack. At present, systems with mimic defense structure such as the mimic defense construction router, the mimic defense construction distributed storage system and mimic defense construction web server have been formed based on the mimic defense technology.
On this basis, the dynamic heterogeneous redundancy (DHR) model [7] adds heterogeneous component sets, dynamic scheduling algorithms [8] and heterogeneous element pools. The heterogeneous element pool provides the diversity design of components at various levels, which can form a heterogeneous set of heterogeneous components to improve the security of the system. When the executive body is attacked by the executive body set, the system selects the component in the heterogeneous component set to replace the executed body that is attacked in the execution body set according to the dynamic scheduling algorithm. The environment necessary for attack triggering is eliminated to make it difficult for the same attack to occur continuously. On the other hand, the existence of a dynamic scheduling algorithm causes the system to present different system attributes during the period change, which disturbs the attacker's judgment and increases the attacker's scanning detection difficulty. If the system has a DHR model, it is said to conform to the structure of mimic defense.

Fig. 1 iPo model

Fig. 2 dynamic heterogeneous redundancy model

2.2. Model introduction
The mimic defense system security analysis model is designed to deeply understand how key features in the mimic defense system affect the security defense capabilities of the system and guide the design and implementation of the mimic defense system. Therefore, the model should have good computational efficiency and scalability, and clearly demonstrate the security defense capabilities of the mimic defense system. The key challenge in designing a security analysis model for mimic defense systems is the non-monotonic nature of the mimic defense system. Because the heterogeneous nature of the mimic defense system and the multi-mode arbitration mechanism can block the information chain between the attacker and the attack target, and the multidimensional dynamic performance of the mimic defense system can disrupt the judgment of the attacker, the typical assumption in the security analysis model—the attacker
has enough time to discover, infiltrate, exploit the vulnerability, can not be applied to the mimic defense system.

If the mimic defense system is modeled by Markov chain [9], the explosive growth state space of the model will appear with the increase of network scale, which makes the difficulty of analysis increased. In addition, the non-monotonicity of the mimic defense system does not conform to the assumption that the current node state in the Markov chain depends only on the state of its previous node.

Based on the above situation, the model is made in this paper according to the state of the node, that the attacker's location is transferred from the current node to its next node is taken as the successful invasion of current node by attacker; that the attacker's location is transferred from the current node to its previous node is considered as and the control loss of current node by attacker. This situation in the mimic defense system is usually expressed as the heterogeneous dynamic transformation of the node or an abnormality in the voting output of the voter. In order to avoid the difficulty of model analysis increased by the forward and backward transfer between a large number of nodes with the increase of network scale, the model only focuses on the attacker's invasion of the next node from the current node and staying at the current node, and the transfer situation of the attacker to the previous node is indirectly analyzed to reduce the complexity of the transfer between nodes.

Fig. 3 The structure diagram of security analysis model

The model structure is shown in Figure 3, where the node a represents the attacker; the node i represents the input proxy module in the mimic defense system; the logical P node is represented by the executive body set in the mimic defense system, where P1, P2, ..., Pn represents specific executive body nodes; the o node is represented as the voter in the mimic defense system. These two nodes are the mimic defense boundary of the system without heterogeneous redundancy features. Therefore, the dynamic defense technology is used to prevent the attacker from using the input agent as a springboard to continuously attack the executable body of P1, P2, ..., Pn and the hijacking voter to tamper with the correct output of the system.

The 1, 2, 3, 4, and 5 processes in the model represent the transfer process between nodes, where 1, 3, and 5 represent the process of the attacker invading the next node from the current node; 2, 4 represents the process of attacker staying at the current node.

3. Model security analysis

3.1. Model assumptions and input parameters

It is assumed when this model is used to evaluate the security of the mimic defense system that there is sufficient heterogeneous executive body to construct the mimic defense structure for any kind of attack,
which is not subject to the diversity of hardware and software. At the same time, the model has the following input parameters:

- **T_{\text{dynamic}}**: It is the time period of the dynamic transformation when proxy node, the executive body node, and the voter node are input in the model, which reflects the dynamic characteristics of the mimic defense structure. **T_{\text{dynamic}}** can be fixed values and random values. In this paper, only fixed values of **T_{\text{dynamic}}** are considered;

- **T_{\text{attack}}**: It is the time required for the attacker to successfully invade its next node in the model, which reflects the complexity of the attacker successfully implementing an attack;

- **p_h**: It is the probability that the heterogeneous attributes are expressed for a certain attack among the execution body nodes in the model. That is, the probability that two executive body nodes produce different results in a certain attack is **p_h**, which reflects the heterogeneous characteristics in the mimic defense structure;

- **p_{(i,j)}**: It is the probability that an attacker successfully invades from node **i** to the next node **j** in a static system without heterogeneous characteristics and dynamics, which reflects the difficulty of the attacker successfully implementing the attack.

### 3.2. Model analysis

In order to analyze the security of the model, **p_1**, **p_2**, **p_3**, **p_4**, **p_5** are respectively used to indicate that the possibilities of the invasion of node a into the input agent node i, continuing to stay at the i node, the invasion from i node to logic P node, continuing to stay at a logic P node, and invasion of logic P-node to voter o node. The derivation process of **p_1** is as follows: node i is near any time node that dynamically changes, the probability that the specific attack initiated by the attacker is heterogeneous is **h_p**. Therefore, the probability that node i does not affect the continuous implementation of attack at any time of dynamical change is **1 - h_p**. Node i can undergo up to **T_{\text{attack}} / T_{\text{dynamic}}** dynamic transformations during a period of successful attack implementation **T_{\text{attack}}**. Therefore, the probability that dynamic transformation does not affect the attack for the node i within the unit time required to complete the intrusion attack is **(1 - h_p)^{T_{\text{attack}} / T_{\text{dynamic}}}**. Based on the above analysis, the possibility that an attacker successfully invades node i from node a can be expressed as:

\[
p_1 = p_{(a,i)} \times (1 - p_h)^{T_{\text{attack}} / T_{\text{dynamic}}} \tag{1}
\]

After successfully invading the node i, the attacker can initiate **T_{\text{dynamic}} / T_{\text{attack}}** times of attacks to the executive body node P in each dynamic transformation period. Then the possibility that all the intrusion attacks from node i to node P fail is **(1 - p_{(i,P)})^{T_{\text{attack}} / T_{\text{dynamic}}}**. Therefore, the possibility of successful intrusion from node i to node P during the dynamic transformation period **T_{\text{dynamic}}** is:

\[
1 - (1 - p_{(i,P)})^{T_{\text{attack}} / T_{\text{dynamic}}} \tag{2}
\]

The attacker will continue to stay at node i with **T_{\text{attack}}** if one of the following two situations occur: First, the penetration attack initiated by the attacker from the node i to the node P fails, and the dynamic transformation of the node i does not affect the attack initiated by the attacker. In this case, the probability that the attacker continues to stay at the node i is:

\[
(1 - p_{(i,P)})^{T_{\text{dynamic}} / T_{\text{attack}}} \times (1 - p_h)^{T_{\text{attack}} / T_{\text{dynamic}}} \tag{3}
\]
Second, the penetration attack initiated by the attacker from node i to node P is successful, and the dynamic transformation of node i does not affect the attack initiated by the attacker. But the dynamic transformation of node P affects the effective implementation of the attack. In this case, the probability that the attacker continues to stay at node i is:

\[
\frac{\tau_{\text{dynamic}}}{{\tau_{\text{attack}}}} \left( 1 - \left( 1 - p_i \right)^{T_{\text{dynamic}}/T_{\text{attack}}} \right) \times \left( 1 - \left( 1 - p_h \right)^{T_{\text{attack}}/T_{\text{dynamic}}} \right)
\]  

Combining the above two cases, the ultimate possibility that the attacker continues to stay at node i is expressed as:

\[
p_2 = \left( 1 - p_{(i,P)} \right)^{T_{\text{dynamic}}/T_{\text{attack}}} \times \left( 1 - p_h \right)^{T_{\text{attack}}/T_{\text{dynamic}}} + \left( 1 - \left( 1 - p_{(i,P)} \right)^{T_{\text{dynamic}}/T_{\text{attack}}} \right) \times \left( 1 - \left( 1 - p_h \right)^{T_{\text{attack}}/T_{\text{dynamic}}} \right)
\]  

Similarly, under the situation that dynamical changes initiated by the attacker at the node i and the node P do not affect the attack initiated by the attacker, the probability of successful invasion from the node i to the node P is \((1 - \left(1 - p_{(i,P)}\right)^{T_{\text{dynamic}}/T_{\text{attack}}} \times \left(1 - p_h\right)^{T_{\text{attack}}/T_{\text{dynamic}}} \), and thus \(p_3\) can be expressed as:

\[
p_3 = \left(1 - \left(1 - p_{(i,P)}\right)^{T_{\text{dynamic}}/T_{\text{attack}}} \times \left(1 - p_h\right)^{2T_{\text{attack}}/T_{\text{dynamic}}}
\]

Through the expression of \(p_1\), \(p_2\), \(p_3\), the possibility \(p_o\) that the attacker successfully invades the node P from the node a can be calculated as:

\[
p_o = p_1 \times (p_2^0 + p_2^{-1} + \ldots + p_2^{-a}) \times p_3 \times \left(1 - \left(1 - p_{(a,i)}\right)^{T_{\text{dynamic}}/T_{\text{attack}}} \times \left(1 - \left(1 - p_{(i,P)}\right)^{T_{\text{dynamic}}/T_{\text{attack}}} \times \left(1 - p_h\right)^{3T_{\text{attack}}/T_{\text{dynamic}}}
\]

Next, the possibility of successful invasion from node a to node o is calculated. First, \(p_4\) and \(p_5\) should be calculated, which represents the possibility that the attacker continues to stay at the node P, the possibility of successful invasion from the node P to the node o, and the possibility of continuously staying at the node o. According to process representation and analysis method of \(p_1\), \(p_2\) and \(p_3\), the expressions of \(p_4\) and \(p_5\) are calculated as follows:

\[
p_4 = \left(1 - p_h\right)^{T_{\text{attack}}/T_{\text{dynamic}}} \times (1 - \left(1 - p_{(P,o)}\right)^{T_{\text{dynamic}}/T_{\text{attack}}} \times \left(1 - p_h\right)^{2T_{\text{attack}}/T_{\text{dynamic}}}
\]

Through the expressions of \(p_1\), \(p_2\), \(p_3\), \(p_4\), \(p_5\), the possibility \(p_o\) that the attacker successfully invades the node o by the node a is calculated as:
\[ p_o = p_1 \times (p_2^0 + p_2^1 + \ldots + p_2^\mu) \times p_3 \times \]
\[ (p_4^0 + p_4^1 + \ldots + p_4^\nu) \times p_5 \]
\[ = \frac{1}{1 - p_2} \times p_{(a,i)} \times (1 - (1 - p_{(i,p)})^{T_{\text{dynamic}}/T_{\text{attack}}}) \times \]
\[ (1 - p_h)^{3T_{\text{attack}}/T_{\text{dynamic}}} \times \frac{1}{1 - p_4} \times \]
\[ (1 - (1 - p_{(P,o)})^{T_{\text{dynamic}}/T_{\text{attack}}}) \times (1 - p_h)^{2T_{\text{attack}}/T_{\text{dynamic}}} \]
\[ = \frac{1}{1 - p_2} \times \frac{1}{1 - p_4} \times p_{(a,i)} \times (1 - (1 - p_{(i,p)})^{T_{\text{dynamic}}/T_{\text{attack}}}) \]
\[ \times (1 - (1 - p_{(P,o)})^{T_{\text{dynamic}}/T_{\text{attack}}}) \times (1 - p_h)^{5T_{\text{attack}}/T_{\text{dynamic}}} \]  

4. Conclusion

This paper proposes a model integrating dynamic feature, heterogeneous feature and redundant feature that performs the safety analysis of the mimic defense system using the probabilistic analysis method, which provides innovative ideas to solve the problem of the lack of effective safety assessment methods for the mimic defense system. However, some simplifications and assumptions have been made during the construction of the model. For example, the attacker's attack ability and the heterogeneity of the system are expressed by probability, which is impossible to comprehensively consider different attack types and mimic defense systems. In order to improve the accuracy and applicability of the model, key factors such as how to assess the attacker's attack ability and the heterogeneity of the system will be studied in the future.

Acknowledgments

Supported by the science and technology project of State Grid Zhejiang Electric Power CO.,LTD (Grand No. SGGR0000XTJS1800310).

References

[1] Yang lin, Yu Quan. Dynamically-enabled Cyber Defense [M]. Posts & telecom Press, 2016.
[2] Wu Jiangxing. Meaning and Vision of Mimic Computing and Mimic Security Defense [J]. Telecommunications Science, 2014, 30(7): 1-7.
[3] Wu Jiangxing. Research on Cyber Mimic Defense [J]. Journal of Cyber Security, 2016, 1(4): 1-10.
[4] Tong Qing, Zhang Zheng, Wu Jiangxing. The Active Defense Technology Based on the Software/Hardware Diversity [J]. Journal of Cyber Security, 2017, 2(1): 1-12.
[5] Ma Hailong, Yi Peng, Jiang Yiming, He Lei. Dynamic Heterogeneous Redundancy based Router Architecture with Mimic Defenses [J]. Journal of Cyber Security, 2017, 2(1): 29-42.
[6] Luo Xingguo, Tong Qing, Zhang Zheng. Mimic Defense Technology [J]. Engineering Science, 2016, 18(6): 69-73.
[7] Hu Hongchao, Chen Fucai, Wang Zhenpeng. Performance Evaluations on DHR for Cyberspace Mimic Defense [J]. Journal of Cyber Security, 2016, 1(4): 40-51.
[8] Ma B, Zhang Z. Security Research of Redundancy in Mimic Defense System [C]. Advanced Information Management, Communicates, Electronic and Automation Control Conference, 2017: 1447-1451.
[9] Xie G. RELIABILITY THEORY OF THE GENERALIZED GAUSS-MARKOFF MODEL AND ITS SIMPLE APPLICATION[J], 1989.
[10] Ma B, Zhang Z, Zhu Y. A formalization research on web server and scheduling strategy for
heterogeneity[C]. Advanced Information Management, Communicates, Electronic and Automation Control Conference, 2017: 1447-1451.