Network Risk Assessment Method Based on Residual Risk Analysis

Hao Jing(✉), Peizhi Yan, Gang Wang, Jiewei Liu, and Yige Fang

School of Information Engineering, Inner Mongolia University of Technology, Hohhot, China
543677830@qq.com

Abstract. The existing network security theory usually believes that "residual risks" are acceptable to a certain degree. However, the reality is that most attackers can enter the network by using the residual risks. Therefore Method of cyber risk assessment. First of all, the algorithm uses the access relationship between the network equipment to build an attack graph structure. Secondly, it uses an Grade protection evaluation score to replace the traditional CVSS score and introduce the indicator of the weight of the indicator to obtain a prior risk probability of each node in the network. Finally, according to real-time attack signs, the Bayesian reasoning algorithm calculates the post-test risk probability of the node to evaluate the risk of network in real time.

Keywords: Residual risks · Bayesian · Grade protection evaluation

1 Introduction

With the continuous development of information technology, network attack methods are becoming increasingly diversified, and various security issues have emerged endlessly. How to ensure that network security is currently attracting much attention. Traditionally detected network security protection methods can only perform passive defense after the attack, and cannot solve network security problems from the root cause. Cyber security situation perception technology can actively evaluate security risks and security threats in the target network, and provide a strong guarantee for the implementation of cybersecurity protection.

Among the current model description methods of many network attacks, the most common is the attack chart method. It study's complex multi-step attack behavior by simulating causality between different nodes. However, most of the existing attack charts use vulnerabilities scanning methods to portray the network structure, and use vulnerabilities CVSS scores to calculate network parameters, but the reality is that most of the vulnerabilities in CVSS have been blocked by existing network security boundary protection equipment. It is not easy to find and use Therefore, it is usually difficult for the protection of the network to make a reasonable assessment of the vulnerability level.

B. Tekinerdogan et al. (Eds.): ICIOT 2022, LNCS 13735, pp. 1–18, 2023.
https://doi.org/10.1007/978-3-031-23585-1_1

And with the continuous development of network security protection technology, cyber attacks are no longer limited to the traditional attack on a loophole, but transformed into a high-level sustainable threat attack, that is, APT attacks. This kind of attack has a strong concealment and pertinence. It usually uses various means such as various media, supply chain and social engineering to implement advanced, lasting and effective threats and attacks. Evaluation obviously cannot fully reflect the level of network risk. Not only that, the current network security review theory still has certain problems, that is, when the network already has a reasonable review system, has made complete security protection measures, there are still great security risks. The reason for this situation is that the residual risk can be accepted in theory, but the current successful cases are mostly starting from the residual risks of the Internet. For example, the recent "Learning APP user data leakage" incident, although it has made complete security protection measures, is still found to have XSS vulnerabilities, and the attackers use a large amount of user information.

For the above reasons, this article uses residual risks to portray the network structure. Remnant risk refers to the remaining risks left after new or enhanced security control. In fact, any system is risky, and not all security control can completely eliminate risks. If the residual risk is not reduced to acceptable levels, the risk management process must be repeated to find a method that reduce the residual risk to acceptable level. After a full risk assessment, the following conclusions are obtained: there is no need to use all safety protection measures. Because the risks of these measures may not exist, or they can tolerate and accept these risks. However, it is precisely because of such remnants that cannot be completely eliminated that they usually become the primary goal of attacker attacks.

Moreover, the attack target selected by an attacker is usually a critical part in a network environment, such as a database server. Therefore, in the actual situation, such network devices are usually more comprehensive protection, so that the attacker cannot directly invade the target he chose, but will instead The affiliates invade, and then use this as a springboard to achieve the invasion of the final goal. Shylock bank Trojan is a good example. In July 2014, the SHYLOCK attacker destroyed legal websites through a websites used by creativity and digital institutions. They used the redirect script to talk about the malicious domain sent by the victim to the Sherlock author. From there, Sherlock Malicious Software was downloaded and installed on a system of browsing legal websites. This is a typical network invasion that uses the supply chain as a springboard.

In order to solve the above problems, this article proposes a method based on the residual risk of Bayesian attack map. By analyzing the elements of the situation of network environment information in an all-round way, analyze the equipment that has implemented some degrees of network protection measures, and build the network structure of the attack chart; and analyze the risk of network equipment in combination with the network security level protection and evaluation unit to achieve The reasonable and quantitative network security situation, the auxiliary administrator has comprehensively and accurately grasped the trend of the trend of network security and the most vulnerable network equipment in the target network.

2 Related work

In recent years, scholars at home and abroad have studied the application of Bayes's attack map in the field of network security. In 2002, DUMINDA and others proposed a more compact and scalable attack graph model. While bypassing the attack tree steps, it can generate more useful information. At the same time, the complexity of the analysis of the problem is reduced from the index level to the polynomial, thereby making A very large network is also within the scope of analysis; in 2006, Lingyu Wang and others looked for the minimum network reinforcement solution based on the attack map, transformed the attack map into logical propositions, simplified the proposition, and made the enhanced options clear. In these options, the lowest cost solution was selected; in 2011, wei li and others provided a new alternative method to analyze the network vulnerability by using the permeability of the testing tester to the maximum penetration level of the host; Fang Yan [10] and others for the complicated node relationship when the attack map is evaluated, there is a circular attack path, and can only reflect the static risk of the network. The concept of simplifies the attack chart and avoids the generation of circular paths through optimization algorithms; in 2017, Hu Hao [9] and others proposed a method of safety-based security situation based on attack prediction. Ability and vulnerability utilization, infer the subsequent attack behavior; in 2018, Chang Hao [11] et al. Based on the Bayesian attack map network structure, combined with real-time attack sample data obtained by the distribution and invasion detection system The node condition probability table is dynamically adjusted to achieve a dynamic risk assessment of the overall security of the target network; in June of the same year, Zhou Yuyang [6] and others proposed a network attack surface risk assessment method based on the Bayesian attack chart. Resources, vulnerability vulnerabilities and dependence in the system establish the Bayesian attack chart, inferring the probability of the attacker to reach each state and the maximum probability of attack path.

3 Model

3.1 Formation Definition of Attack Graphs

Definition 1. The Bayesian attack map is defined as a directional no-loop map $\mathbf{BAG} = (\boldsymbol{H}, \boldsymbol{E}, \boldsymbol{L_h})$, of which:

(1) $\mathbf{H} = \mathbf{H_{internal}} \cup \mathbf{H_{supply}} \cup \mathbf{H_{branch}} \cup \mathbf{H_{initialization}}$ represents the host, which is the node of the attack chart, $\mathbf{H_{internal}}$ for the host or other network equipment inside the attack process, and $\mathbf{H_{supply}}$ represents the host which is associated with the host or other network equipment associated with the attack process. $\mathbf{H_{branch}}$ represent the host or other network equipment of the subordinate department, initial nodes initiated for network attacks, $\mathbf{H_{initialization}}$**representthehost** which indicate a host or other network equipment in the attack;

(2) $\mathbf{E} = \{\mathbf{e_{ij}}, \mathbf{authority}\}$ is the edge set of the attack chart, indicating the connection relationship between the host, i indicates the first node connected by the edge, j indicates the latter node connected by the edge, **authority** indicating the degree of trust between the source host and the destination host;

(3) R **represent** the relationship between multiple front-drive nodes and the same rear node. Can be used in a binary group $< \boldsymbol{H_i}, \boldsymbol{d_i} >$, where. **AND** means that only the status of all the front-drive nodes that arrive is true that the attack can be completed. In the same way, **OR** means that as long as one of the front-wheel drive nodes is true;

(4) $\mathbf{Q} = \{\boldsymbol{Q_{phy}}, \boldsymbol{Q_{net}}, \boldsymbol{Q_{host}}, \boldsymbol{Q_{data}}\}$ Indicate the collection of the test scores such as the other, where $\mathbf{Q_{phy}} = \{\mathbf{q_1}, \mathbf{q_2}, \ldots, \mathbf{q_n}\}$ indicates the physical security scores of the protection evaluation, $\mathbf{Q_{net}} = \{\mathbf{q_1}, \mathbf{q_2}, \ldots, \mathbf{q_n}\}$ indicates the network security scores of the protection evaluation, $\boldsymbol{Q_{h}}_{\mathbf{ost}} = \{\boldsymbol{q_1}, \boldsymbol{q_2}, \ldots, \boldsymbol{q_n}\}$ indicate the safety scores of the assessment of the evaluation, and $\boldsymbol{Q_{d}}_{\mathbf{ata}} = \{\boldsymbol{q_1}, \boldsymbol{q_2}, \ldots, \boldsymbol{q_n}\}$ indicate the data security score of the assessment of the main engine.

(5) L_h indicates a set of independent probability distribution functions, and each node has a local probability distribution.

3.2 Construction of Attack Graph Structure

The model of building this attack chart includes two steps: structural construction and parameter construction. The goal of structural construction is to establish the initial trust relationship between hosts and form a topology diagram of a host. Structure establishment is completed by **Initialstructure** algorithm.

Initialstructure

input：Host collection H, Set of relationship between front and rear nodes R

output：Nonparametric Bayesian attack graph

```
Initialize  BAG
Add $h_0$ to BAG;
Add $h_0$ to WTJ;
While (WTJ!=NULL && H!=NULL)
 For each $h_J$ in WTJ  {
  For each $h_i$ in H
 {
    If ($h_i, h_j$).authority!=NULL
      {
         Add $h_i$ to BAG;
         Add $h_i$ to WTJ;
         Add ($h_j, h_i$) to E;
         If $e_{ij}$.authority< ($h_i, h_j$).authority
             $e_{ij}$.authority=($h_i, h_j$).authority;
         Add $e_{ij}$ to BAG;
       }
         Remove $h_j$ from WTJ；
 }
      If($h_i, h_j$).authority==admin
        Continue;      }
  END for
 END for
END while
Return BAG;
```

In the above algorithm, the initial external host with no vulnerability is included in the host collection, which represents an attacker. First of all, initialize the attack chart, add the initial node and add it to the to be judged collection. After that, the judgment is aimed at the elements in the set. Like the host collection. When there is an accessible relationship between the two hosts, the edges, nodes and nodes are added to the attack chart. In reality, there may be a variety of trust relationships between hosts in the network. In these cases, this algorithm only retains the highest access level relationship, which is reflected in line 13–14. In order to reduce the cost of calculation, if the access level of the current retrieval is reached the highest, it has reached the highest access level, and the next set of hosts are directly retrieved. Finally output a Bayesian attack chart with only structure without parameters.

The calculation cost of the attack graph established in this paper can be roughly analyzed as follows. In this algorithm, the number of nodes in the network, that is n, the number of hosts, each host pair needs to be analyzed, so it will generate a quadratic number of traversal, that is $\mathbf{n}^2$. . The number of times the loop body (lines 7–18) is executed $\mathbf{n}^2$ times. Further, it is analyzed inside the loop. In the most dense attack graph, all access levels are higher than none, every two host groups must execute a loop. The time cost of a single loop is $10\mathbf{n}^2$, and in the worst case, the time cost of the loop is. Therefore, the total calculated cost of is $10\mathbf{n}^2 + 3$, that is $\mathbf{T}(\mathbf{n}) = \mathbf{O}\left(\mathbf{n}^2\right)$.

3.3 Attack Maps to the Ring Algorithm

However, in order to meet the structural requirements of the Bayesian attack chart, and at the same time, based on actual consideration, the attacker will not launch an attack on the resource that has been broken. Essence The attack chart generated by the algorithm **Initialstructure** is used as the input, which traverses the full chart. After removing the ring, a new diagram is generated, as shown in the algorithm **LoopRemove**.

LoopRemove

input：Original attack graph BAG

output：Acyclic attack graph BAG'

```
For each $h_i$ in H
Initialize $h_i$
For each $h_i$ in H
    For each $h_j$ in H
        If i =n||j=0   continue;
          else   If $h_i \in H$ && $h_j \in H$ && $e_{ij} \in E$ && $e_{ji} \in E$
              If $i < j$
                Remove $e_{ij}$ from BAG;
              Else
                  Remove $e_{ji}$ from BAG;
  Return BAG';
```

The input of the above algorithm is a ray of original attack chart, and the output is an attack graph that is not contained. First initialize all hosts in the set. Then traverse all the hosts, in order to reduce the calculation cost, a stop retrieval mechanism similar to the algorithm is introduced. It is reflected in the fifth line, that is, the source host is the last host or purpose. When the host is the initial host, the follow-up operation is not performed, and the next host pair is directly retrieved.

The time cost analysis required for the specific calculation of the algorithm is as follows. In this algorithm, how many nodes in the network, that is n, how many hosts are costing the time cost in the initial traversal operation. The follow-up is a double cycle. In the worst case, the cycle (5–10 lines) is executed $\mathbf{n} * \mathbf{n}$ times. Analyze the interior of the circular body, the time cost consumed by the judgment statement in line 5 is 1, and the time cost consumed by the judgment statement in line 6 is 4. Each time a judgment is made, only one of the statements in line 8 and line 10 is selected for execution, time cost in the worst case is $1 + 4 + 1 + 1 = 7$. The cost cost consumed by this algorithm is $7\mathbf{n}^2 + \mathbf{n}$, that is $\mathbf{T}(\mathbf{n}) = \mathbf{O}\left(\mathbf{n}^2\right)$.

3.4 Attack Figure Parameters Construction

The next step of our model is to measure the probability of the host's attack by the equivalent and evaluation unit of each host. Calculate the condition probability between all hosts in the network, that is, network parameters. Level protection assessment is entrusted by relevant units in accordance with the regulations of the national information security level protection system in accordance with relevant management specifications and technical standards in accordance with the national information security level protection system. For the information system that handles specific applications, the security technical evaluation and safety management evaluation method is used to detect and evaluate the protection status. The conclusions of the set safety level are proposed for safety rectification proposals for safety do not meet the items. Compared with traditional models using vulnerabilities CVSS scores to measure the method of breaking the probability of the host, the scores such as the guarantee evaluation unit can obviously represent the current safety of the host, and the specific operation is shown in the algorithm Paraassign.

ParaAssign

input：Acyclic nonparametric Bayesian attack graph BAG'

output：Bayesian attack graph with parameters BAG"

```
InitQueue(Q);
PushQueue(Q,$h_0$);
While (EmptyQueue(Q))
{
  S=PopQueue(Q)
    For each $s_i \in S$
    For each $h_j \in H$
      If $h_j = s_i$.arrival
           PushQueue(Q, $s_i$);
             If $d_i$=AND
               $L_i$=WNPD($s_i$)= $\begin{cases} 0, & \exists Si \in Pa\left[S_j\right] | S_i = 0 \\ Pr\left(\bigcap_{S_i=1} v_i\right), & 其他 \end{cases}$
         If $d_i$=OR
               $L_i$=WNPD($s_i$)= $\begin{cases} 0, & \forall Si \in Pa[S_j] | S_i = 0 \\ Pr\left(\bigcup_{S_i=1} v_i\right), & 其他 \end{cases}$
      END for
      END for
  END While
```

In the above algorithm, Physical Security (PS), network security (NETWORK Security (NS), host security (HS), and data security (DS) are adopted. The success rate of the host's break is calculated. The following attribute scoring standards corresponding to the indicator are based on physical security and network security as an example. The host safety is similar to the evaluation standards of the first two items.

In this article, the physical security is refined into the choice of physical location, physical access control, anti-theft capacity, anti-natural disaster capacity and power supply situation. Show as Table 1.

Cyber security scores are detailed into network structure security, network invasion prevention, border integrity inspection, and malicious code prevention. The specific scoring standards are similar to the previous two items to data integrity, data confidentiality, and data backup recovery capabilities. This article is no longer explained.

Table 1. Scoring criteria for physical security attributes

Index	Attribute	Attribute rating
Selection of physical location	The wind, water and earthquake resistance of the building is excellent/the wind, water and earthquake resistance of the building is general / the wind, water and earthquake resistance of the building is poor	0.2/0.1/0
Physical access control	The examination and approval system for entering and leaving the machine room is perfect, and the identity of the entering and leaving personnel can be identified/the examination and approval system for entering and leaving the machine room is unreasonable, and the identity of the entering and leaving personnel cannot be identified	0.2/0
Anti theft ability	The security facilities are complete and the anti-theft ability is good/the security facilities in some non key areas are not complete and the anti-theft ability is general/the security facilities in key areas are not complete and the anti-theft ability is poor	0.2/0.1/0
Ability to prevent natural disasters	Good natural disaster prevention ability/general natural disaster prevention ability/poor natural disaster prevention ability	0.2/0.1/0
Power supply	It can fully guarantee the power supply at any time and respond to emergencies/it can guarantee the power supply at any time in most cases / it can not guarantee the power supply at any time, and there is no record of responding to emergencies	0.2/0.1/0

Different types of equipment have different weights on the four unit indicators of the level protection assessment. for example, the database host's requirements for data security will be much higher than that of several items. The quantification standard is shown in Table 2.

Table 2. Quantitative standards for indicators of the third class insurance evaluation unit

Equipment type	Attribute relationship	Lay particular stress on	Biased value (PS, NS, HS, DS)
Normal host	PS = NS = HS = DS	NULL	0.25/0.25/0.25/0.25
Database host	DS > PS > NS = HS	Data security	0.3/0.1/0.1/0.5
	DS > NS > PS = HS		0.1/0.3/0.1/0.5
	DS > HS > PS = NS		0.1/0.1/0.3/0.5
Network connection device	NS > DS > HS = PS	Network security	0.1/0.5/0.1/0.3
	NS > HS > DS = PS		0.1/0.5/0.3/0.1
	NS > PS > DS = HS		0.3/0.5/0.1/0.1
Network defense equipment	HS > DS > NS = PS	Host securityHost security	0.1/0.1/0.5/0.3
	HS > NS > PS = DS		0.1/0.3/0.5/0.1
	HS > PS > NS = DS		0.3/0.1/0.5/0.1
The server	PS > NS > HS = DS	Physical security	0.5/0.3/0.1/0.1
	PS > DS > HS = NS		0.5/0.1/0.1/0.3
	PS > HS > NS = DS		0.5/0.1/0.3/0.1
Supply chain equipment	NS > DS > HS = PS	Network security	0.1/0.5/0.1/0.3
	NS > HS > DS = PS		0.1/0.5/0.3/0.1
	NS > PS > DS = HS		0.3/0.5/0.1/0.1

Combined with the index index bias standardization standards and the measurement scores such as each unit, the probability formula of the host is broken:

$$\Pr(h) = 1 - Q_{PS} * W_{PS} + Q_{NS} * W_{NS} + Q_{HS} * W_{HS} + Q_{DS} * W_{DS} \tag{1}$$

Risk assessment can find the potential danger of the target network, helping network security officers to understand the situation of the network. In the Bayesian attack chart, the node risk is generally evaluated based on the probability of the first test. The prior probability of a node is the combined probability of the local conditions of the node and its parent node. Therefore, in order to calculate the node first check the probability, the local condition probability of the node must be calculated first. Local conditional probability reflects the risks that a resource state node may suffer. The local condition probability of any node is related to its parent node. There are two dependencies between the parent nodes in the Bayesian attack map AND and OR. The calculation formula of the local condition probability of the status node is as follows:

The occurrence of attack events in the network, changes in the physical environment, and changes in security conditions will affect the probability of resource nodes. In order to dynamically evaluate the risk of network risks, the postpartum probability of the node after the attack is required. The reasoning algorithm combines security incident information, corresponding to the prerequisites of security incident atom attacks, and calculating the probability of the Bayesian network after network network, updating the probability of node. After the combination of security incidents, the probability of pushing down the risk value of various nodes of the Bayesian network attack chart is of great significance for network evaluation. The attack events observed are O and the post-mobility calculation definition formula is as follows:

$$P_o(S_i|O) = \frac{P(O|S_i) \times P(S_i)}{P(O)} \tag{2}$$

4 Experiment

In order to verify the feasibility and effectiveness of the network attack surface risk assessment method based on the Bayesian attack chart, this section first uses the network topology as shown in the figure to build a small experimental network environment. Then use the network attack graph model method introduced by Sect. 3 to achieve the probability of the construction of the attack chart and the corresponding host node. Finally, through the security risk assessment method, combined with the relationship between the parent nodes, the condition probability of the entire node was calculated, and the construction of the Bayesian attack chart was finally realized (Table 3).

Table 3. Residual risk description

Node number	Node name	Network segment	Residual risk description	Equipment category	Attribute relationship
H_1	Supply chain host	1	Ports 22 and 23 are open to hosts in network segment 0 and 1, which may cause attacks against telnet and SSH services	Supply chain equipment	NS > DS > HS = PS

(*continued*)

Table 3. (*continued*)

Node number	Node name	Network segment	Residual risk description	Equipment category	Attribute relationship
H_2	Database service host	2	Port 9200 is open to hosts in the same network segment, which may cause database attacks against elasticsearch service	Database host	DS > PS > NS = HS
H_3	Web service host	2	Ports 135 and 139 are open to network segment 1 and hosts in the same network segment, which may generate scanning and detection behaviors against TCP, UDP or ICMP	The server	PS > NS > HS = DS
H_4	Firewall	/	Allow network segment 0 to access port 22 of network 1	Network defense equipment	HS > NS > PS = DS
H_5	Switch	2	/	Network connections	NS > DS > HS = PS
H_6	Router	/	The path from network segment 0 to network segment 1 exists in the routing table	Network connection device	NS > DS > HS = PS

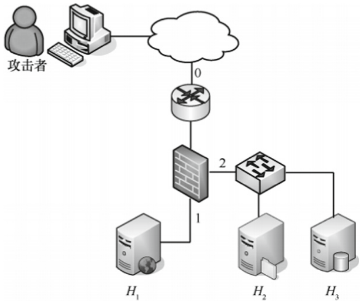

Fig. 1. Network topology environment

The firewall divides the overall experimental network environment into 3 network segments. Among them, the external network is the network segment 0, $\mathbf{H}_1$ belongs to the network segment 1, and the $\mathbf{H}_2$, $\mathbf{H}_3$ belong to the network segment 2. The specific implementation strategy of the firewall is shown in Table 2. The intercourse follows the access of the port open ports on the network segment, and other visits that are not in the firewall strategy are deemed to be illegal access.

According to the host information and firewall strategies, and the attack graph generation method proposed in Sect. 3, the attack graph structure shown in the figure can be generated. Among them, Where $\mathbf{H}_0$ is the initial node of the attacker, $\mathbf{H}_1$**and** $\mathbf{H}_2$ are host node, and edge is the access relationship between hosts (Fig. 1).

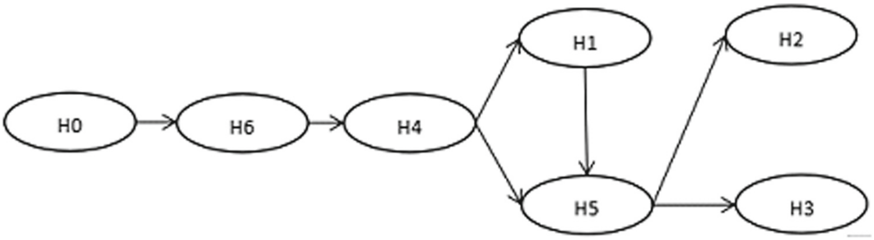

Fig. 2. Structure of attack graph

First, detect the hosts in the experimental network in the experimental network environment, summarize the detected node resource information, and extract the resources that may be used by the attackers in combination with the firewall configuration rules in Table 2, as shown in Table 4. Since this paper mainly investigates the impact of equipment equal guarantee evaluation scores on the probability of equipment being breached, combined with the quantitative standard of the indicators of equal guarantee evaluation units, according to the index scores of equal guarantee evaluation units shown in Table 4, and according to their attribute relations, the corresponding successful utilization rate of equipment being breached can be obtained through formula (1) (Fig. 2).

After obtaining the probability of each device, according to the relationship between nodes and formulas, the local condition probability table of each node in the attack chart can be calculated.

Table 4. Probability of equipment being breached

NODE	PS	NS	HS	DS	Attribute relationship	$Pr(s_i)$
H_1	0.7	0.5	0.75	0.66	NS > DS > HS = PS	0.407
H_2	0.5	0.5	1	0.66	PS > NS > HS = DS	0.434
H_3	0.5	0.25	0.5	1	HS > NS > PS = DS	0.525
H_4	0.6	0.75	0.5	0.33	HS > NS > PS = DS	0.432
H_5	0.8	0.5	0.5	0.33	NS > DS > HS = PS	0.521
H_6	0.6	0.5	0.25	1	NS > DS > HS = PS	0.365

After that, the traditional CVSS vulnerability scoring standard evaluation method was used to evaluate the same network parameters, and compared with the method of this article for comparison experiments. First of all, the host network in the target network is performed for fragile points, summarized the detected vulnerabilities, and selected the invasion pathway, identity authentication and attack complexity as an indicator of the probability calculation of the atom attack node. In the CVSS basic measurement indicator, query the score of the basic quantity group of each fragile point. Table 5 gives the score of the CVSS score basic measurement standard indicator, and Table 6 gives a detailed list of the fragile points that may be detected.

Table 5. Scores of CVSS basic metrics

Metrics	Measurement level	Grade score
AV	Network	0.85
	Proximity network	0.62
	Local	0.55
	Physics	0.20
AC	Low	0.78
	Middle	0.56
	High	0.24
AU	Null	0.85
	Low	0.62
	High	0.27

Through the invasion detection system, the occurrence of an attack event was detected. After analysis, it was determined that it was an attack on the device, and the attacker had obtained the ROOT permissions of the device $\mathbf{H}_1$. The calculation of the after-evaluation of the attack diagram after the attack graph is shown in Table 4, and the CVSS post-probability update calculation of the Bayesian network attack chart is shown in Table 5. The prior probability and post-test probability in this article refer to the probability of successful attack in the corresponding condition probability table. Figures 3 and 4 gives the comparison of the probability of waiting for the evaluation and CVSS respectively (Tables 7 and 8).

Table 6. Success rate of vulnerability utilization

Node number	CVE number	AV	AC	AU	Pr(s_i)
H_1	CVE-2009–1012	0.85	0.56	0.27	0.129
H_2	CVE-2011–4800	0.62	0.56	0.62	0.215
H_3	CVE-2006–0408	0.62	0.78	0.62	0.300

Table 7. Posterior probability of equal guarantee evaluation

Node number	Prior probability	Posterior probability
H_1	0.407	1
H_2	0.434	0.760
H_3	0.525	0.798
H_4	0.432	0.531
H_5	0.521	0.845
H_6	0.365	0.511

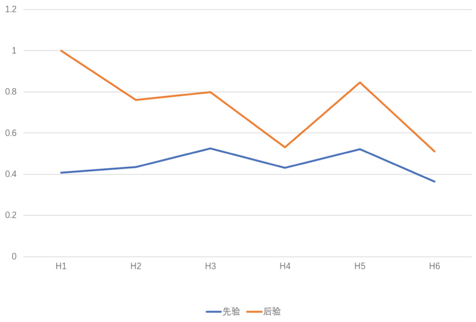

Fig. 3. Comparison of prior and posterior probabilities of equal assurance test evaluation

In this paper, the method of evaluating network parameters by using equal protection evaluation score is better than CVSS score. First, CVSS score only evaluates the vulnerability itself, but the evaluation range of grade protection evaluation score is more comprehensive and comprehensive. The grade protection evaluation score comprehensively considers various factors of the real system, and can correctly reflect the

Table 8. Posterior probability of CVSS score

Node number	Prior probability	Posterior probability
H_1	0.129	1
H_2	0.215	0.318
H_3	0.300	0.385

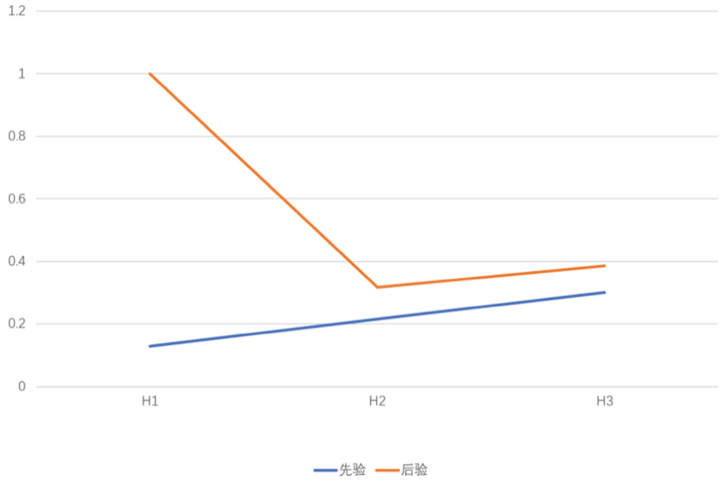

Fig. 4. Comparison of prior probabilities of CVSS

comprehensive protection level of the tested system in management and technology. Secondly, it can be seen from the two groups of comparison graphs that in the comparison graph of equal protection evaluation, it is obvious that the probability of nodes being breached has been improved. Except for the host $\mathbf{H}_1$ being attacked, the increase of device H5 is the most obvious compared with other devices, which indicates that in this attack event, the threat of device $\mathbf{H}_5$ has increased the most, and it is most likely to become the next attack target of the attacker, The defense strategy shall be taken against the device $\mathbf{H}_5$ to resist the attack means of the attacker. However, such a conclusion can not be reached in the CVSS score comparison chart. We can only feel that the overall network risk value has improved after the network intrusion.

5 Summary

In order to effectively evaluate the security risks of the network system, this article proposes a network attack risk assessment method based on the Bayesian attack chart. By analyzing the residual risk analysis of various devices in the network system Evaluate the risk of breaking the attack on each network equipment. This article uses equal inspection unit scores such as combination and other guarantee evaluation unit indicators to portray the probability of being broken, which improves the accuracy of risk assessment, and more in line with the actual scenario. The experimental results show that the work of this article can effectively obtain the Bayesian attack map that conforms to the actual attack scene. The probability of being broken by each host can provide a good support for the defensive work.

For the work that can be carried out in the future, the current modeling work is mainly based on a small experimental network. There is still a large amount of calculation during the promotion of large-scale networks. How to achieve large-scale automatic attack graph construction will be a subsequent research one of the subsequent research The direction and parallelization may be a way to solve this problem.

References

1. Li, J., et al.: Dynamic network security analysis based on bayesian attack graph. Comput. Sci. **49**(03), 62–69 (2022)
2. Yang, X.: Analysis of Network Attack Defense Based on Bayesian Attack Graph and Markov Process. Harbin University of Science and Technology (2021).https://doi.org/10.27063/d.cnki.ghlgu.2021.000028
3. Hui, W., Juan, Z., Ya, Z., Kun, L., Wenfeng, F.: A new Bayesian model for network risk assessment. Small Microcomput. Syst. **41**(09), 1898–1904 (2020)
4. Yang, Y.: Research on threat assessment method and defense mechanism of multi-step attack scenarios. Beijing Jiaotong University (2019)
5. Huan, L.: Research on dynamic risk assessment method based on Bayesian network attack graph. Yanshan University (2019).https://doi.org/10.27440/d.cnki.gysdu.2019.000535
6. Yuyang, Z., Guang, C., Chunsheng, G.: A network attack surface risk assessment method based on Bayesian attack graph. J. Netw. Inf. Secur. **4**(06), 11–22 (2018)
7. Fan, W.: Research on network security risk assessment method based on Bayesian attack graph. Northwestern University (2018)
8. Shixing, G.: Analysis of probability calculation of cluster tree propagation algorithm in Bayesian network attack graph. Softw. Guide **16**(07), 174–178 (2017)
9. Hao, H., Runguo, Y., Hongqi, Z., Yingjie, Y., Yuling, L.: Network security situation quantification method based on attack prediction. J. Commun. **38**(10), 122–134 (2017)
10. Yan, F., Xiaochuan, Y., Jingzhi, L.: Research on quantitative assessment of network security based on Bayesian attack graph. Comput. App. Res. **30**(09), 2763–2766 (2013)
11. Hao, C., Qin, Y., Zhou, C.: Dynamic risk assessment of industrial control system based on bayesian attack graph. Inf. Technol. **42**(10), 62–67+72 (2018). https://doi.org/10.13274/j.cnki.hdzj.2018.10.013
12. Mehta, V., Bartzis, C., Zhu, H., Clarke, E., Wing, J.: Ranking attack graphs. In: Zamboni, D., Kruegel, C. (eds.) Recent Advances in Intrusion Detection. LNCS, vol. 4219, pp. 127–144. Springer, Heidelberg (2006). https://doi.org/10.1007/11856214_7
13. Xie, P., Li, J.H., Ou, X., et al.: Using Bayesian networks for cyber security analysis. In: IEEE/IFIP International Conference on Dependable Systems and Networks, Chicago (2010)
14. Cunningham, W.H.: Optimal attack and reinforcement of a network. J. ACM **32**(3), 549–561 (1985)
15. Ou Xinming, H.J.Z.S.: MulVal project at Kansas State University, 7 Sep 2016. http://people.cs.ksu.edu/~xou/mulval/
16. Dagum, P., Chavez, R.M.: Approximating Probabilistic Inference in Bayesian Belief Networks. IEEE Trans. Pattern Anal. Mach. Intell. **15**(3), 246–255 (1993)

17. Minka, T.P.: Expectation propagation for approximate Bayesian inference. In: Seventeenth Conference on Uncertainty in Artificial Intelligence (2013)
18. Larra, A.P., Kuijpers, C.M.H., et al.: Decomposing Bayesian networks: triangulation of the moral graph with genetic algorithms. Statist. Comput. **7**(1), 19–34 (1997)
19. Rose, D.J., Tarjan, R.E.: Algorithmic aspects of vertex elimination on directed graphs. Stanford University (1975)
20. Kenig, B., Gal, A.: On the impact of junction-tree topology on weighted model counting. In: Beierle, C., Dekhtyar, A. (eds.) Scalable Uncertainty Management. LNCS (LNAI), vol. 9310, pp. 83–98. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-23540-0_6
21. Venkatraman, S., Yen, G.G.: A generic framework for constrained optimization using genetic algorithms. IEEE Trans. Evol. Comput. **9**(4), 424–435 (2005)