Research on Smart Home Security Threat Modeling based on STRIDE-IAHP-BN

1st Rongjuan Zhu
School of Artifical Intelligence and Computer Science
Jiangnan University
Wuxi,China
zrj15161@163.com

2nd Xinke Wu
School of Artifical Intelligence and Computer Science
Jiangnan University
Wuxi,China
6191914012@stu.jiangnan.edu.cn

3rd Jun Sun
School of Artifical Intelligence and Computer Science
Jiangnan University
Wuxi,China
junsun@jiangnan.edu.cn

4th Zhihua Li
School of Artifical Intelligence and Computer Science
Jiangnan University
Wuxi,China
w*xzhli@aliyun.com*

***Abstract* - As a common form of Internet of things applications, smart home also faces security threats. Because majority of the network security threat modeling are Internet-oriented. It is a challenging and scientific question to how to treat modeling of smart home. This paper combines the improved analytic hierarchy process with Bayesian network and proposes a method of STRIDE-IAHP-BN for threat quantification and priority definition. Moreover, in order to verify the effectiveness of the method, the DVR system is selected to analyze and verify the method. The results of simulation show that the modeling method can provide effective support for the assessment of smart home security threat.**

Key words: security threat modeling; the method of STRIDE-IAHP-BN; improved analytic hierarchy process; smart home

I. INTRODUCTION

The Internet of Things (IoT) is one of the national key strategic emerging industries recognized by the world with broad development prospects [1]. With the rapid development of IoT, how to improve the security of IoT has become a common challenge for the academic and industrial fields [2]. The hidden danger of IoT not only brings property loss to users, threatens their life security, and even poses a great threat to the security of the country's major infrastructure. Countries all over the world have invested a great deal of money to conduct in-depth research in the field of IoT information security and the security of IoT applications [3]. As a common form of IoT applications, smart home has advantages in low cost, powerful functions and convenient deployment, but there are major security risks such as being vulnerable to remote network attacks and privacy disclosure [4]. Network security threat modeling is a basic technology and method for studying and evaluating network security risks, which can provide a powerful reference for situation awareness and network risk early warning and prevention [5]. Therefore, how to model the security threats of smart home is a challenging and scientifically significant research topic.

At present, research on IoT threat modeling is still in the initial stage. In 1999, Bruce Scheier [6] defined attack tree for the first time. Attack tree is mainly used for description and formal analysis, which has the disadvantage of strong subjectivity. Based on the concept of attack tree, scholars [7] proposed a threat modeling method for IoT, which adopts a strategy similar to brainstorming in the model implementation. Unfortunately, this method is not suitable for specific assessment work, nor is it suitable for large-scale network systems with high

2473-3636/21/$31.00 ©2021 IEEE
DOI 10.1109/DCABES52998.2021.00059

complexity; Microsoft has proposed a STRIDE model, which mainly draws data flow diagrams and obtains threat indicators based on the Microsoft Threat Modeling Tool. However, this model cannot fully express the security concept, data elements, abstraction level, deployment information and simplified system [8]. Zhou Yan [9] proposed an improved STRIDE threat modeling method, in which the dimensional information of the location where the threat occurred was added on the basis of stride, but the critical factors such as severity and priority of threat were not fully considered. In addition, there are some common threat modeling models, such as Common Vulnerability Scoring System (CVSS) [10] and DREAD rating system [11], but they are not intuitive enough for threat modeling, and the measurement basis that the rating relies on is also very general, and it has high professional requirements for the raters. Sun Ao et al. [12] proposed a STRIDE-HMM risk assessment model and method combining STRIDE and Hidden Markov Model (HMM). This method carries out quantitative calculation of threats, but the state transition probability matrix and observation probability matrix are given by subjective experience.

In this paper, STRIDE-IAHP-BN, a comprehensive quantitative modeling method for threat quantification and priority definition is proposed based on the Improved Analytic Hierarchy Process (IAHP) combined with Bayesian Network (BN). The STRIDE-IAHP-BN method scores based on the index risk value (high, median or low) obtained by STRIDE and the number of the third-level indexes belonging to the second-level indexes, which can reduce the influence of subjective factors to a certain extent; furthermore, the consistency problem is transformed into a constrained programming problem and solved by CPLEX Optimizer; finally, the probability obtained by IAHP is taken as the prior probability of BN, and combined with the joint probability distribution table of BN, the final risk probability of the threat is calculated. In this way, security personnel can take corresponding countermeasures more accurately based on the probabilistic priority and severity of threats. In addition, in order to verify the effectiveness of the model, the DVR system is selected to analyze and verify the model. The experimental results show that the model can provide effective decision support for threat assessment of smart home security.

The rest chapters are arranged as follows: The first chapter mainly introduces IAHP and the proposed modeling method of Stride-IAHP-BN; the second chapter mainly introduces the threat modeling method based on Stride-IAHP-BN proposed in this paper and the example demonstration in the DVR system, and finally, the conclusion is drawn.

II. STRIDE-IAHP-BN MODEL

A. Improved Analytic Hierarchy Process

In order to make the initial weights of the second and third level index nodes more objective and maneuverable, the analytic hierarchy process is improved in this paper. Firstly, the acquisition of traditional judgment Matrix relies on the experience and knowledge of experts, which is relatively subjective. In this paper, we adopt the strategy of scoring the quantity of third-level indexes to which second-level indexes belong according to STRIDE's analysis, the more the number, the higher the score; the third-level indexes are scored according to the risk level of high, median, and low. The higher the risk level, the higher the score. the benefits of doing so is that the difficulty and subjectivity of scoring are reduced to a certain extent; secondly, in calculating the weights, the traditional AHP methods such as geometric mean, arithmetic mean, eigenvector, least squares and so on are avoided, instead, the consistency problem is transformed into a mathematical programming problem, which effectively circumvents the requirement of consistency; finally, the mainstream solver CPLEX and YALMIP are imported into MATLAB R2016b, and the judgment Matrix is weighted by least squares. The objective function and constraints are shown in formula 6. Based on the above improvements, an improved AHP (IAHP) method is proposed.

$$\min Z = \sum_{i=1}^{n}\sum_{j=1}^{n}(a_{ij}w_j - w_i)^2 \qquad (6)$$

$$s.t.\sum_{i=1}^{n} w_i = 1(w_i > 0, i = 1,2,...,n)$$

where i=1,2…n; ω_i is the weight of evaluation factor i; n is the number of evaluation factors and a_{ij} is the judgment matrix.

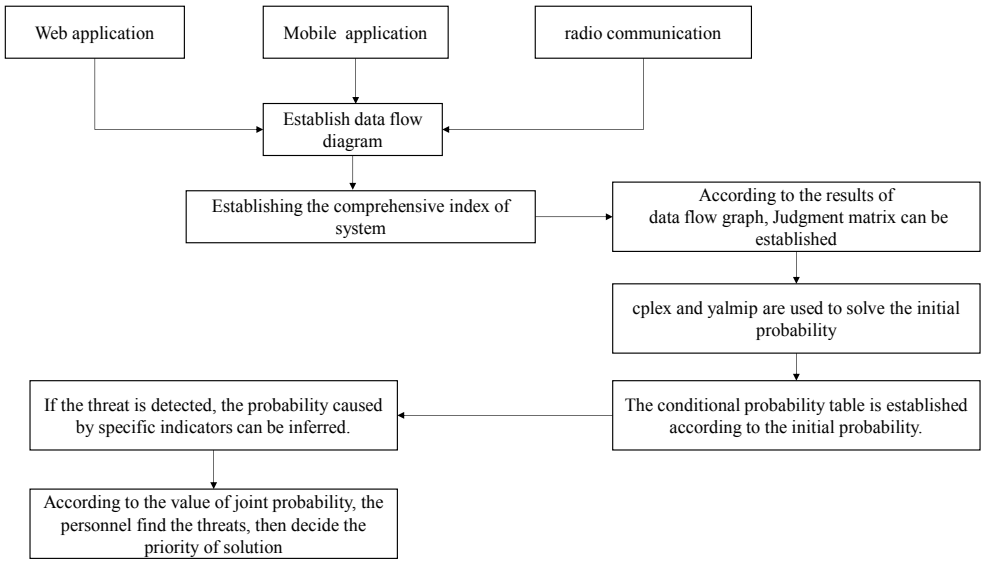
The IAHP algorithm is described as follows:

```
Input: N*N      //* judgement matrix
Output:1*N      //* weight of index
       C = [
       x>0
       sum(x)
       ]                    //*constraint condition
       for i=1:N
            for j=1:N
                 z=z+(n(i,j))*x(j)-x(i))^2   //*objective
function
            end
       end
       if result.problem == 0    //* success
       else
            failure
end
```

The time cost of IAHP mainly comes from the double-loop statement to solve the objective function, so the complexity of the algorithm is $0(N^2)$. The improved analytic hierarchy process makes the calculation of index weight easier and quicker by improving the procedure of judging consistency, thus speeds up the convergence speed of the algorithm.

B. Construction Method of IAHP Threat Assessment Model

With the quantitative assessment of smart home security threats as the demand, the following discussion is made on the construction process of threat assessment model. Firstly, based on the Threat Modeling Tool, the data flow diagram is constructed from the three aspects of web application, mobile application and radio communication, and the smart home security threat index system is constructed, and all the threat indexes are divided into three levels: high, median, and low； secondly, the proposed IAHP method is used to calculate the weight of indexes, and the weights obtained are used as the initial probabilities of the second-level and third-level index nodes; finally, the joint probability that the final security risk may occur can be calculated according to the Bayesian inference model by setting joint probability table of nodes. Thus, based on this joint probability, security practitioners can conduct threat detection, threat early warning, and determine the priorities of response measures. It can be seen that the method is universal to a certain extent. To sum up, a model for quantitative security threat assessment (STRIDE-IAHP-BN) is proposed, as shown in Figure 1.



III. APPLICATION OF STRIDE-IAHP-BN MODEL

The number of stencils available in the Threat Modeling Tool for representing devices, communication transfers, and input/output trusted boundaries is limited, so you need to create your own stencils during the actual drawing process. Figure 2 shows the interface for adding a stencil by yourself; Figure 3 shows the Web application

data flow diagram of DVR system; Figure 4 shows the mobile application data flow diagram of DVR system; Figure 5 shows the radio communication data flow diagram of DVR system.

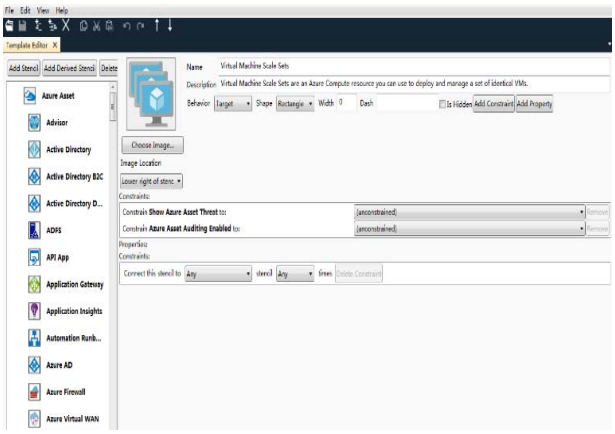


Figure 2. Interface for adding a stencil by yourself

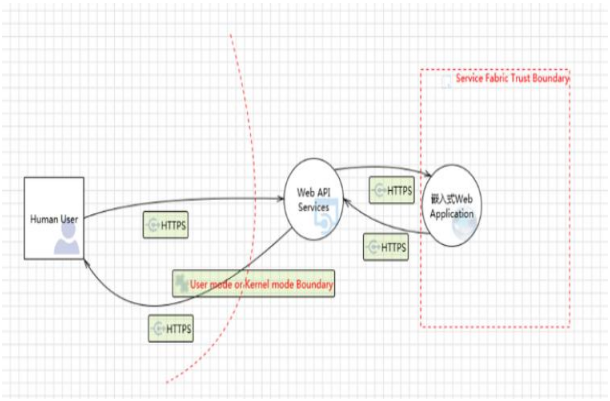


Figure 3. Web application data flow diagram of DVR system

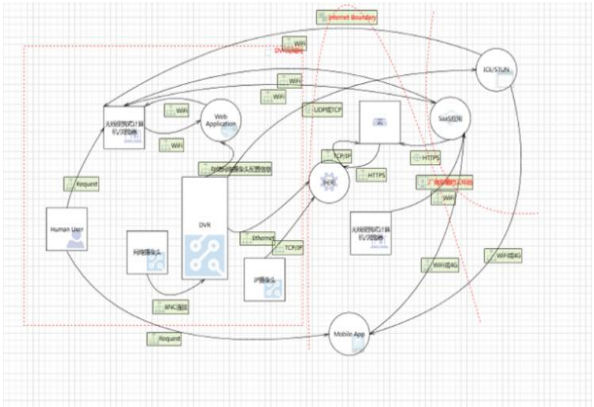


Figure 4. mobile application data flow diagram of DVR system

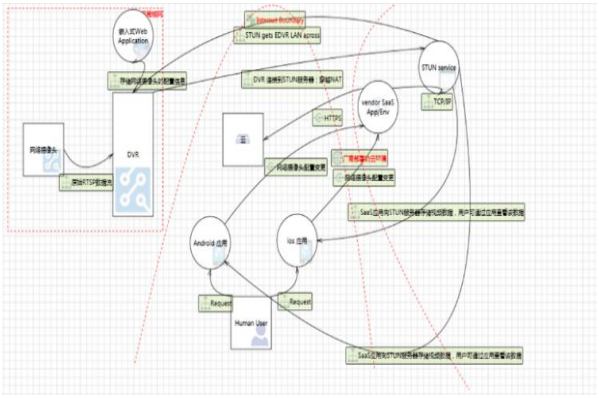


Figure 5. radio communication data flow diagram of DVR system

Furthermore, taking the Web application data flow diagram of DVR system as an example, the threat analysis diagram shown in Figure 6 can be generated by running the data flow diagram.

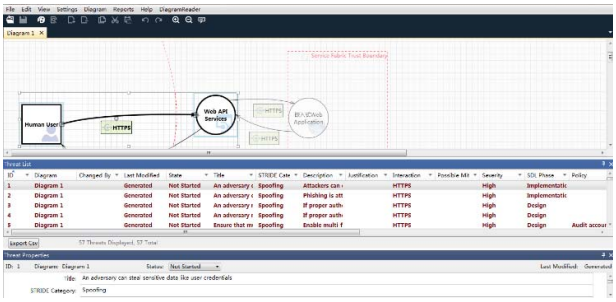


Figure 6. Threat analysis diagram

Finally, a threat analysis report as shown in Figure 7 is generated by Microsoft Threat Modeling Tool.

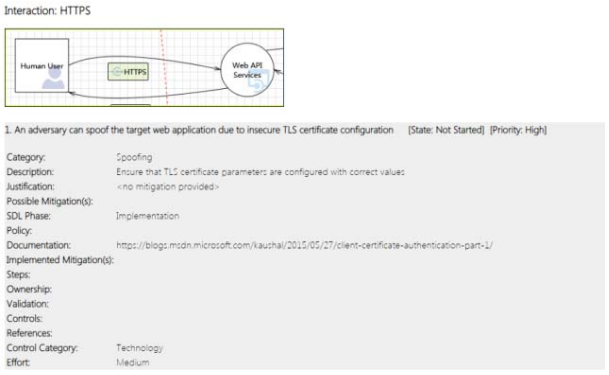


Figure 7. Threat analysis report

Through the analysis of the report shown in Figure 7, it is found that there is a total of 50 threats in all links. The quantity of each threat type is shown in Table 1.

Table 2. Quantity of each threat type

Threat type	Quantity
S	14
T	12

R	3
I	10
D	2
E	9

The identified threat examples are described into a document, which contains the description of the threat, the target of the threat, the attack technology, countermeasures, and the risk level.

The traditional AHP is subjective in scoring and the initial judgment Matrix usually does not meet the requirements of consistency, which need to be adjusted several times, therefore, in this paper, the IAHP method proposed is adopted to calculate the weight of indexes, and the STRIDE method is used, in addition, the consistency problem is transformed into a constrained programming problem, so as to effectively overcome the above shortcomings. As for the scoring method of the B-C judgment matrix between the index level and the criterion level, if the two indexes have the same risk, i.e. both of them are high risk, median risk or low risk, the score is 1; if the risk values of the two indexes are respectively one high, one median or one median, one low, the score is 5 or 3, and one high, one low, the score is 9 or 7. This method greatly reduces the influence of subjectivity.

Finally, after the evaluation is completed, the corresponding judgment matrix is input into the CPLEX Optimizer to obtain the weight of each index. Here, only the weights of prior probabilities of indexes required by the following Bayesian network are listed: 0.0673 for B3, 0.0192 for C27, 0.0388 for C28, and 0.0094 for C29.

The relationship between the number of nodes n in the Bayesian network structure diagram and the joint probability distribution table is 2^n. To carry out the Bayesian network precise reasoning shown in Figure 7, we need 2^{57} combined conditional probability tables [23]. Therefore, only B3 (denial) branch is selected for discussion. Convert C27 (an attacker can deny access to the cloud gateway due to lack of audit) , C28 (an attacker can deny the API malicious behavior on the API that caused the denial problem) , and C29 (an attacker can reject the attack footprint of a malicious problem) to Bayesian root nodes, and convert event B3 into a leaf node of Bayesian Network. Figure 9 shows the Bayesian network model of this branch.

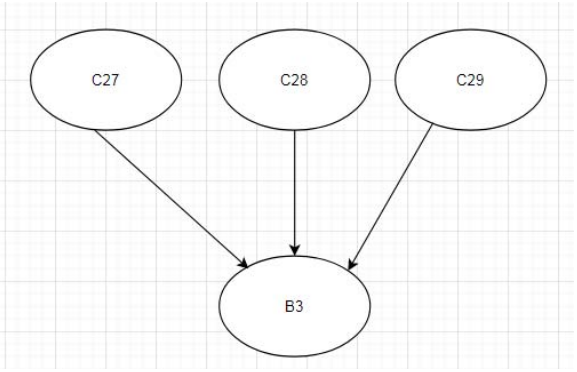


Figure 9. Bayesian network model

Further, the weights obtained in the parameter learning stage based on AHP are set as the prior probability of each node, and the conditional probability table is set. As shown in Figure 10, 1 corresponds to Fault, that is, the probability of a threat, and 0 corresponds to OK, that is, probability that the system is safe without threat.

C27	P(C27)
1	0.0192
0	0.9808

C28	P(C28)
1	0.0388
0	0.9612

C29	P(C29)
1	0.0094
0	0.9906

C27	C28	C29	P(B3)
0	0	0	OK
0	0	1	Fault
0	1	0	Fault
0	1	1	Fault
1	0	0	Fault
1	0	1	Fault
1	1	0	Fault
1	1	1	Fault

Figure 10. Prior/conditional probability table of Bayesian network

Table 9. Joint probability of Bayesian network

C27	C28	C29	B3	P(C27)	P(C28)	P(C29)	P(B3|C27,C28,C29)	Product
OK	OK	OK	OK	0.9808	0.9612	0.9906	1	0.933883
OK	OK	Fault	OK	0.9808	0.9612	0.0094	0	0
OK	Fault	OK	OK	0.9808	0.0388	0.9906	0	0
OK	Fault	Fault	OK	0.9808	0.0388	0.0094	0	0
Fault	OK	OK	OK	0.0192	0.9612	0.9906	0	0
Fault	OK	Fault	OK	0.0192	0.9612	0.0094	0	0
Fault	Fault	OK	OK	0.0192	0.0388	0.9906	0	0
Fault	Fault	Fault	OK	0.0192	0.0388	0.0094	0	0
OK	OK	OK	Fault	0.9808	0.9612	0.9906	0	0
OK	OK	Fault	Fault	0.9808	0.9612	0.0094	1	0.008862
OK	Fault	OK	Fault	0.9808	0.0388	0.9906	1	0.037697
OK	Fault	Fault	Fault	0.9808	0.0388	0.0094	1	0.000358
Fault	OK	OK	Fault	0.0192	0.9612	0.9906	1	0.018282
Fault	OK	Fault	Fault	0.0192	0.9612	0.0094	1	0.000173
Fault	Fault	OK	Fault	0.0192	0.0388	0.9906	1	0.000737
Fault	Fault	Fault	Fault	0.0192	0.0388	0.0094	1	0.000007

It is not difficult to find from Table 9 that if a threat is detected, that is, if the detection result is Fault, then the result is the probability caused by C27, which is calculated as follows:

$$P(C27 = \text{Fault}|D = \text{Fault}) = \frac{0.18282+0.000173+0.000737+0.000007}{0.008862+0.037697+0.000358+0.018282+0.000173+0.000737+0.000007} = 29.0\%$$

. Similarly, if a threat is detected in the system, but no C28 threat is found after investigation, then under this condition, the probability of C27 occurrence is as follows:

$$P(C27 = \text{Fault}|B3 = \text{Fault}, C28 = OK) = \frac{0.0128282+0.000737}{0.008862+0.018282+0.000173} = 70.0\%$$

. Obviously, the security personnel may refer to the probability value for threat detection and response.

IV. CONCLUSION

In this paper, based on the method of STRIDE, a quantitative method combining the improved analytic hierarchy process and Bayesian network, which can reduce the demand for prior knowledge of the scorer and the difficulty of analysis compared with the CVSS scoring system and the DREAD rating system, is proposed; the improved analytic hierarchy process reduces the scale, and the risk level and the quantity of indexes obtained by STRIDE greatly reduce the subjectivity of scoring; in addition, the consistency problem is circumvented by turning it into a constraint programming problem. The prior probabilities in the Bayesian network are derived from an improved analytic hierarchy process, which is more accurate than the prior probabilities based on experience. The Bayesian Model replaces the Hidden Markov Model and provides a more accurate fine-grained model. Once the risk probability of the index reaches a certain threshold, it is necessary for the security personnel to take security policies for adjustment. In addition, measures to mitigate the threat are provided. This threat modeling method can provide security personnel with a basis for decision-making, so as to build a safe and reliable defense.

REFERENCES

[1]. Wu H, Han H, Wang X, et al. Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey[J]. IEEE Access, 2020, 8: 153826-153848.

[2]. Mishra P, Biswal A, Garg S, et al. Software Defined Internet of Things Security: Properties, State of the Art, and Future

Research[J]. IEEE Wireless Communications, 2020, 27(3): 10-16.
[3]. [American] Brian•Russell Drew•van•durren By. Internet of things security[M]. translated by Li Wei Shen Xin Hou Jingyi Wang Ziliang Beijing: China Machine Press,2018.
[4]. Agrawal D, Bhagwat R, Bandopadhyay R, et al. Enhancing Smart Home Security using Co-Monitoring of IoT Devices[C]//Companion of the 2020 ACM International Conference on Supporting Group Work. 2020: 99-102.
[5]. Li, Zhang,Xin, Tong. Threat Modeling and Countermeasures Study for the Internet of Things[J]. Journal of Convergence Information Technology,2013,8(5).
[6]. Dewri R, Poolsappasit N, Ray I, et al. Optimal security hardening using multi-objective optimization on attack tree models of networks[C]//Proceedings of the 14th ACM conference on Computer and communications security. 2007: 204-213.
[7]. Lallie H S, Debattista K, Bal J. A review of attack graph and attack tree visual syntax in cyber security[J]. Computer Science Review, 2020, 35: 100219.
[8]. Stone E E, Skubic M. Passive in-home measurement of stride-to-stride gait variability comparing vision and Kinect sensing[C]//2011 Annual international conference of the IEEE engineering in medicine and biology society. IEEE, 2011: 6491-6494.
[9]. Zhou Yan. Research on improved STRIDE threating model[D].Wuhan: Huazhong University of Science and Technology,2015.
[10]. Mell P, Scarfone K, Romanosky S. Common vulnerability scoring system[J]. IEEE Security & Privacy, 2006, 4(6): 85-89.
[11]. Burke M J, Salvador R O, Smith-Crowe K, et al. The dread factor: how hazards and safety training influence learning and performance[J]. Journal of Applied Psychology, 2011, 96(1): 46.
[12]. Sun Ao, Yin Xiaochuan, Li Xiaoqing. A task oriented network risk assessment model[J]. Journal of Air Force Engineering University,2020,20(5):105-110.
[13]. Danielis P, Beckmann M, Skodzik J. An ISO-Compliant Test Procedure for Technical Risk Analyses of IoT Systems Based on STRIDE[C]//2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC). IEEE, 2020: 499-504.
[14]. Ghosal A, Halder S, Conti M. STRIDE: Scalable and Secure Over-The-Air Software Update Scheme for Autonomous Vehicles[C]//ICC 2020-2020 IEEE International Conference on Communications (ICC). IEEE, 2020: 1-6.
[15]. Saaty T L. Decision making with the analytic hierarchy process[J]. International journal of services sciences, 2008, 1(1): 83-98.
[16]. Saaty T L. What is the analytic hierarchy process[M]//Mathematical models for decision support. Springer, Berlin, Heidelberg, 1988: 109-121.
[17]. Hosseini S, Ivanov D, Dolgui A. Ripple effect modelling of supplier disruption: integrated Markov chain and dynamic Bayesian network approach[J]. International Journal of Production Research, 2020, 58(11): 3284-3303.
[18]. Boutkhamouine B, Roux H, Pérés F. Data‐driven model for river flood forecasting based on a Bayesian network approach[J]. Journal of Contingencies and Crisis Management, 2020, 28(3): 215-227.
[19]. [American]By Adam Stark.threating model[M]. translated by Jiang Changqing,and so on.Beijing: China Machine Press:2015.
[20]. By [American] Alan • guzman Aditia • Gupta. Internet of things penetration test[M].tanslated by Wang Bin.Beijing: China Machine Press,2019.
[21]. Sion L, Yskout K, Van Landuyt D, et al. Security Threat Modeling: Are Data Flow Diagrams Enough? [C]//IEEE/ACM 42nd International Conference on Software EngineeringWorkshops (ICSEW'20). IEEE/ACM, 2020.
[22]. Li M, Wang H, Wang D, et al. Risk assessment of gas explosion in coal mines based on fuzzy AHP and bayesian network[J]. Process Safety and Environmental Protection, 2020, 135: 207-218.
[23]. He Yongchang,Chen Zhiguang,Wang haifeng and so on. Research on Bayesian network model of Missile Fault Diagnosis Based on netica[J]. Aviation Weapon,2020,27(1):89-95.