Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 6729827, 11 pages
https://doi.org/10.1155/2022/6729827

Research Article

Dynamic Threat Weight of Network Security Communication Based on Multisource Data Analysis

Zhihui Yu,[1] Sitong Liu ,[2] and Weimin Wang[3]

[1]*College of Marxism, Shanghai University of Political Science and Law, Shanghai 201701, China*
[2]*School of Management, Guilin University of Aerospace Technology, Guilin 541004, Guangxi, China*
[3]*School of Government, Shanghai University of Political Science and Law, Shanghai 201701, China*

Correspondence should be addressed to Sitong Liu; liusitong@guat.edu.cn

Received 18 November 2021; Revised 13 January 2022; Accepted 20 January 2022; Published 10 March 2022

Academic Editor: Deepak Kumar Jain

While the internet brings convenience to people, there are also many security problems. This study mainly discusses network security communication and ideological security technology based on multisource data analysis. The situation awareness model based on dynamic threat weight is mainly composed of the fusion module, evaluation module, and prediction module. The situation fusion module is mainly based on the fusion algorithm of distance vector optimal classification to fuse multisource data. The situation assessment module is based on the situation assessment method based on a dynamic threat weight to quantitatively evaluate the situation value. The situation understanding part is the basis of situation awareness. Firstly, a large amount of original security data is merged at the data level to obtain a standardized dataset. Then, the relationship between the data is analyzed by the method of correlation analysis, and the security incident information and threat propagation network are obtained. The knowledge training module accurately feeds back the relevant parameters and data, and the knowledge training module adjusts the data accuracy according to the received data accuracy. The main function of the situation fusion module is to process the multisource data and use the fusion algorithm for data fusion. The situation assessment module uses the fused data combined with a specific method for comprehensive assessment and uses visualization technology to show the final results in front of the administrator, which is convenient for more efficient operation. Based on the data fusion module, the situation assessment module judges the current network security status, detects the assessment results through error checking, and feeds back to the knowledge training module. From the trend of the overall network situation, we can see that the probability of the overall network at 4 is the highest, followed by 5. This study makes an effective evaluation of the overall network security.

1. Introduction

When people read web news every day, they often encounter security incidents, such as hackers swiping bank cards and all kinds of endless Trojans and worms attacking again. Hence, while people enjoy the network, network threats are everywhere. Its appearance is an upgrade and innovation to the traditional security mechanism. With the continuous expansion of network scale and the increasing number of security issues, the current network information systems generally deploy a variety of security detection equipment. The data on which situational awareness is based comes from these pieces of detection equipment deployed in different locations, which can be IDS, firewall, and alarm log of the system. They can also be the detection result of a malicious code detection system, vulnerability scanning system, and penetration testing system.

Network security situation technology will bring more intelligence into the field of network security, embed more new technologies, such as data mining and big data, into data analysis, and integrate more people's good expectations for information security into it. The emergence and development of this technology will be a great leap in the field of network security. The output result of the equipment is huge, for example, the IDS alarm log often shows the amount of data of G level. To apply these detection results to situational awareness, these large amounts of heterogeneous security data must be processed. Situation understanding, as the first

step of the situation awareness process, is to use correlation analysis technology to process massive heterogeneous security data, get standardized data, and provide support for situation assessment.

Zhang et al. reconfigured the equipment and sent the trip command to the intelligent electronic equipment that controls the system breaker. Although he modified and adopted the average destruction time model and estimated the frequency of intrusions through various paths, he did not give a specific network defense strategy [1]. Although Buczak and Guven provided some suggestions on when to use a given method, the research lacked innovation [2]. Kolokoltsov and Bensoussan also considered the random process of infection spread and the customer's decision-making process. Although the execution time of customer decisions (such as opening or closing the defense system) is faster than the infection rate, it does not guarantee that the network is safe [3]. Although Kruse et al. established clear procedures to upgrade software and deal with data leakage, the research process lacked logic [4].

The situation awareness model based on dynamic threat weight is mainly composed of a fusion module, evaluation module, and prediction module. The situation fusion module is mainly based on the fusion algorithm of distance vector optimal classification to fuse multisource data. The situation assessment module is based on the situation assessment method based on dynamic threat weight to quantitatively evaluate the situation value. The knowledge training module transmits relevant parameters data accuracy to the knowledge training module, and the knowledge training module adjusts the data accuracy according to the received data accuracy. The main function of the situation fusion module is to process the multisource data and use the fusion algorithm for data fusion to reduce the amount of data and improve accuracy. The situation assessment module uses the fused data combined with a specific method for comprehensive assessment and uses visualization technology to show the final results in front of the administrator, which is convenient for more efficient operation.

2. Cybersecurity

2.1. Multisource Network Security Data Fusion. They can usually cooperate with each other to complete the detection of network attacks and the overall situation assessment of the network. Therefore, how to integrate multi-source network security data and enhance complementarity is an extremely important issue at present. According to the hierarchical structure and a large amount of redundant information, the following formula can be obtained [5, 6]:

$$S = \min_{i \in [1,l]} \sum_{t=1, t \neq i}^{l} \left\| h_i - h_t \right\|. \tag{1}$$

Another feature used is the block feature [7].

$$\begin{aligned} M_r &= \left| m_{ij} \right|, \quad i, j = 1, 2, \ldots, \eta, \\ m_{ij} &= \frac{1}{l} \sum_{t=1}^{l} v_{i,jt}, \\ \varphi_{\text{patch}}(A) &= \sum_{p_i * q_i = 1}^{n_i} \varphi_{p_i * q_i} \left| a_{p_i} - a_{q_i} \right|^2. \end{aligned} \tag{2}$$

The similarity matrix φ is calculated by Bayesian function, and its formula is defined as follows [8, 9]:

$$\begin{aligned} \varphi_{p_i \cdot q_i} &= \begin{cases} e^{\left(\left| x_{p_i} - x_{q_i} \right| / 2\sigma^2 \right)}, & \text{if } x_{p_i} \in N \text{ or } x_{q_i} \in N, \\ 0, & \text{otherwise}, \end{cases} \\ \phi_{\text{frame}}(A) &= \sum_{j=1}^{m} \phi_{i,j} \left\| A_i - A_j \right\|_F^2, \\ &\min F(X, A, D) \\ &= \left\| X_i - D A_i^2 \right\|_F^2 + \lambda_1 \left\| A_i \right\| + \lambda_2 \varphi_{\text{patch}} \left\| A_i \right\| + \lambda_3 \varphi_{\text{patch}} \left\| A_i \right\|. \end{aligned} \tag{3}$$

Among them, λ_1, λ_2 and λ_3 are three weight variables [10].

2.2. Cybersecurity Situational Awareness. The traditional intrusion detection system (IDS), as an important network security protection method, must be improved and innovated to adapt to the current rapidly changing network security situation. The traditional IDS filters the information in the network according to a certain rule library. Its disadvantage is that the amount of data is very huge. It contains a lot of redundant information, and the false alarm and false alarm rate remain high. In addition, IDS cannot provide system administrators with an intuitive and vivid network security situation, and it requires the administrators to manually process the collected massive amounts of information based on their own experience to form a comprehensive judgment of the current network status [11, 12]. Therefore, when using traditional IDS, experience and technology are indispensable conditions for network administrators. Network security situation awareness (NSSA) technology overcomes the disadvantages of traditional IDS [13]. It is a new technology that combines the advantages of

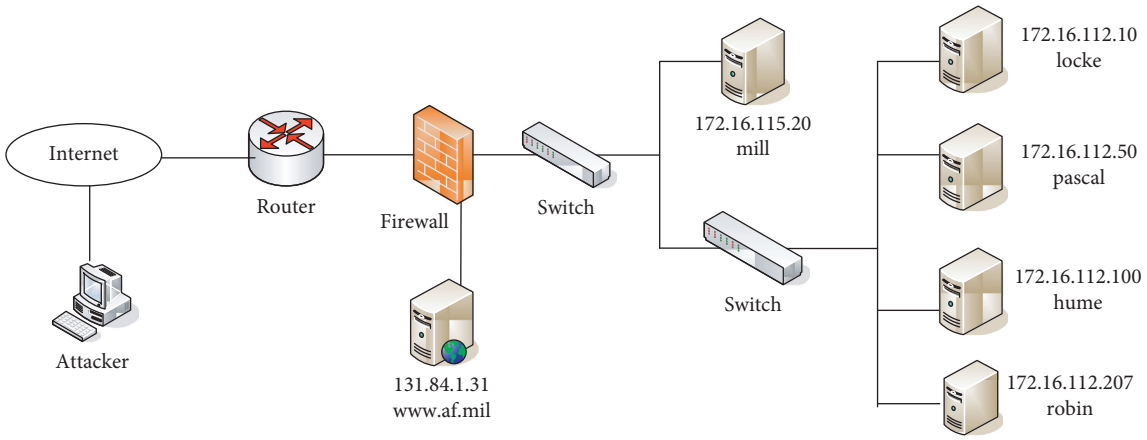

Figure 1: Key network flapping.

various sensing technologies, improves the accuracy of network data collection, reduces the redundancy of data, quantifies the collected data, and presents network threats in numerical or other intuitive forms [14, 15].

Firstly, an effective way to understand the current situation is to collect data. Secondly, after understanding the current situation, make a relatively objective assessment of the current situation. It is usually divided into the following three steps: firstly, acquiring elements, namely data collection. Secondly, understanding the situation, namely analyzing security situation through data. Finally, forecasting the situation [16, 17]. The key network flapping is shown in Figure 1. Endsley defines situational awareness as "the perception of various elements in the environment in a specific time and space, the understanding of its meaning, and the prediction of its future state." Situational awareness is divided into three levels. The first level is clue perception, which is the most basic link in situational awareness. The second level is understanding, i.e., the integration of different information and making decisions about goals. People at the second level can get important information from subjective and objective aspects related to the operation from the clues obtained at the first level. The third level is prediction, i.e., the ability to predict future situational events, which is the highest level of situational awareness.

$$W(t,\vec{d}) = \frac{tf(t,\vec{d}) \times \log(N/n + 0.01)}{\sqrt{\sum_{i\in\vec{d}} [tf(t,\vec{d}) \times \log(N/n + 0.01)]^2}},$$

$$W(t,\vec{d}) = \frac{t\left(1 + \log_2 tf(t,\vec{d})\right) \times \log(N/n)}{\sqrt{\sum_{i\in\vec{d}} \left[\left(1 + \log_2 tf(t,\vec{d})\right) \times (N/n)\right]^2}}, \quad (4)$$

$$p\left(\vec{x}, C_j\right) = \sum_{d_i \in KNN} \mathrm{Sim}(\vec{x},\vec{d})\left(\vec{d}, C_j\right),$$

$\vec{x}$ is the feature vector of the new text [18]. Assume that at time T1, a piece of formatted data $X1 = \{x1, x2, \ldots, xm\}$ from sensor 1 is received. Since the result obtained is inversely proportional to the similarity between the events, the similarity between the final event X1 and the six events is as follows [19, 20]:

$$\left(1 - \frac{s1}{s}, 1 - \frac{s2}{s}, 1 - \frac{s3}{s}, 1 - \frac{s4}{s}, 1 - \frac{s5}{s}, 1 - \frac{s6}{s}\right),$$
$$s = \sum_{i=1}^{6} s_i. \quad (5)$$

After all the values are normalized, it is the Mass function of event X1, which is as follows:

$$m(A) = (p(n), p(p), p(u), p(r), p(d), p(\theta)). \quad (6)$$

The Bayes approximate calculation formula of the Mass function is as follows:

$$m(A) = \frac{\sum_{A\subseteq B} m(b)}{\sum_{C\subseteq\varnothing} m(b) n|C|}. \quad (7)$$

The parameter C in the above formula is a known event. Hence, $|C| = 5$.

$$p(n)' = \frac{p(n) + p(\theta)}{p(n) + p(p) + p(u) + p(r) + p(d) + 5p(\theta)},$$
$$p(p)' = \frac{p(p) + p(\theta)}{p(n) + p(p) + p(u) + p(r) + p(d) + 5p(\theta)},$$
$$p(u)' = \frac{p(u) + p(\theta)}{p(n) + p(p) + p(u) + p(r) + p(d) + 5p(\theta)}, \quad (8)$$
$$p(r)' = \frac{p(r) + p(\theta)}{p(n) + p(p) + p(u) + p(r) + p(d) + 5p(\theta)},$$
$$p(d)' = \frac{p(d) + p(\theta)}{p(n) + p(p) + p(u) + p(r) + p(d) + 5p(\theta)}.$$

The Mass function transformed by Bayes approximation is $(p(n)', p(p)', p(u)', p(r)', p(d)')$. Finally, D-S data fusion is performed [21, 22]. In the DS evidence theory, a complete set consisting of mutually incompatible basic propositions (hypotheses) is called a recognition framework, which represents all possible answers to a certain question,

however, only one answer is correct. A subset of this framework is called a proposition. The degree of trust assigned to each proposition is called the basic probability distribution.

2.3. Network Situation Assessment. Although its mathematical form is relatively simple, problems may occur in the process of composition [23].

$$S(t) = W(t)nKn2^{P}, \tag{9}$$

$W(t)$ represents the weight of the service targeted by the attack event in the t time period, K represents the credibility of the attack event, and P represents the threat level of the attack event. Different attacks have different impacts on host services, so the threat level of P is divided into three levels: high, medium, and low, and the values are in the three intervals [1, 4], [4, 7], and [7, 10].

Host-level situation assessment is as follows:

$$S(Z) = \sum W(Z)nS(t). \tag{10}$$

Among them, $W(z)$ is the weight of all services to be inspected. It is divided into three levels: high, medium, and low, and each level is represented by 5, 3, and 1. After normalizing the importance of all services to be checked, the final result $W(z)$ is the weight of each service [24].

Network-level situation assessment is as follows:

$$S(w) = \sum W(h)nS(Z). \tag{11}$$

$W(h)$ corresponds to the weight of each host. The evaluation of the weight is determined according to the actual importance of the host. It is divided into three levels: high, medium, and low. Each level is represented by 8, 5, and 1. After normalizing the importance of all hosts, the final result $W(h)$ is the weight of the host. The corresponding sequence satisfies as follows:

$$x_{n,j-1}(k) = x_{2n,j}(k) + x_{2n+1,j}(k). \tag{12}$$

Network security situational awareness will produce different results according to different starting points and needs, which is very subjective and diverse. For example, the network administrators are mainly concerned with the identification of network intrusions and the repair of vulnerabilities; for government agencies and the military units, secrecy is paramount. Its definition is as follows:

$$\mathrm{MSE} = \frac{1}{N}\sum_{k=1}^{N}[x(k) - \hat{x}(k)]^2,$$
$$U_{n,j-1} = U_{2n,j} \oplus U_{2n+1,j}. \tag{13}$$

Among them, $\hat{x}(k)$ is the predicted value.

$$\mathrm{MSE} > \mathrm{MSE}'. \tag{14}$$

Among them, MSE is the actual error. The results of network security situational awareness should have depth and breadth to meet the needs of a variety of users. Situational awareness analyzes the security of the system and provides countermeasures from multilevel, multiangle, and multigranularity, and it presents them to users in the form of graphs, tables, and security reports.

3. Cybersecurity Communication and Ideological Experiments

3.1. Situational Awareness Model Based on Dynamic Threat Weights. The situation awareness model based on dynamic threat weight is mainly composed of the fusion module, evaluation module, and prediction module. The following will give a brief description of each module in detail. The situation fusion module is mainly based on the fusion algorithm of distance vector optimal classification to fuse multisource data. The situation assessment module is based on the situation assessment method based on dynamic threat weight to quantitatively evaluate the situation value. The situational awareness model is shown in Figure 2. Asset evaluation: evaluate the performance status and security status of each asset in the network, including asset performance utilization, importance, the number of existing threats and vulnerabilities, security status, etc. Threat evaluation: evaluate malicious code and network intrusion in the network type, number, distribution nodes, hazard levels, etc. Vulnerability assessment: assess the type, number, distribution nodes, and hazard levels of vulnerabilities in the network and management configuration vulnerabilities.

3.2. Model Composition. Compared with previous models, the overall structure of the situational awareness model based on dynamic threat weights still follows the Endsley model structure. On this basis, the situational awareness part has been improved. The components of the model include a knowledge training module, a situation fusion module, a situation assessment module, a threat weight control module, a situation prediction module, and a multisource sensor database. The modules are interconnected, and multiple modules with relatively independent functions form a unit through data transmission. Multisource data analysis channel: comprehensively analyze the security status of the entire network, and give the security situation value of the network, including the confidentiality, integrity, and availability components of the security situation of the entire network and their comprehensive situation value.

3.3. Functional Module Design

3.3.1. Knowledge Training Module. The main function of the knowledge training module is to use the existing data combined with the K-means clustering algorithm to perform clustering during initialization to provide the required parameters and data. Otherwise, in a real-time operation, based on the original data, combined with the continuous input data, continuously adjust and modify the required parameters and data.

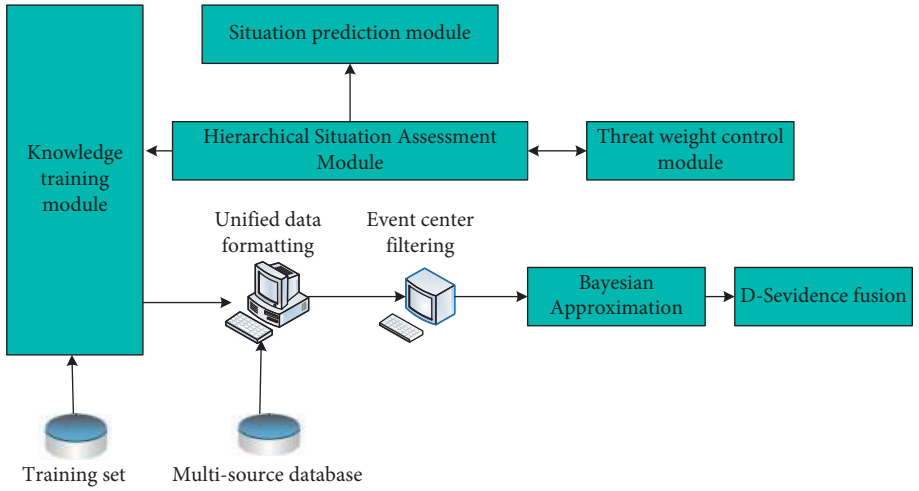

Figure 2: Situational awareness model.

The knowledge training module transmits relevant parameters to the situation fusion module. The situation assessment module feeds back the accuracy of the data to the knowledge training module, and the knowledge training module makes corresponding adjustments based on the accuracy of the received data.

3.3.2. Situation Integration Module. The main function of the situation fusion module is to process multisource data and use the fusion algorithm for data fusion to reduce the amount of data and improve accuracy. The situation fusion module is a data processing module, and its workflow is that the data collected by multisource sensors enter it first. Because of the differences in the content of the data collected by different types of sensors, the data formats are very different. To eliminate the incompatibility between this kind of data, the first step in the situation fusion module will be completed soon.

The collected data is uniformly formatted. The second step is to pass the uniformly formatted data through the event center, and the event center will filter and classify the formatted data. The third step will be filtered, and the filtered data is further simplified and subtracted by Bayesian approximation. Finally, the mutually compatible multisource data is merged.

3.3.3. Situation Assessment Module. To ensure the accuracy and comprehensiveness of the situational awareness results, the integrity of the data should be ensured to the utmost extent. The original data obtained by all testing equipment needs to be analyzed. The amount of processed data is large. If more complex correlation technologies are adopted, the processing time will be longer. The real-time performance of the system is poor. To meet the real-time requirements of the system, the situation understanding process, firstly, adopts simple data-level fusion, and it then analyzes the correlation of the fused data.

Situation assessment plays the role of a judge in network security situation awareness. The fused data shows the current network security state using a specific value or waveform with amplitude change through assessment. The situation assessment module uses the fused data combined with a specific method for comprehensive assessment and uses visualization technology to show the final results in front of the administrator, which is convenient for more efficient operation.

Based on the data fusion module, the situation assessment module judges the current network security status, detects the assessment results through error checking, and feeds back to the knowledge training module.

3.3.4. Threat Weight Control Module. As an auxiliary module of the situation assessment module, the threat weight control module greatly improves the accuracy and rationality of the situation assessment. In situation assessment, threat weight, as an extremely important parameter, plays a major role in the final assessment result, however, absolute threat weight sometimes causes errors or even misjudgments in the final assessment result. The threat weight control module can accumulate the same type of attacks. As the number of attacks of the same type continues to increase, the threat weight control module will appropriately increase the weight of such threats. When the number of attacks of the same kind gradually stabilizes or gradually decreases within a certain period of time, the threat weight control module will gradually reduce the weight of such threats. The threat weight control module uses the dynamic change of the threat weight to make the final evaluation result more reasonable and accurate.

3.3.5. Situation Prediction Module. In the Endsley model, situation prediction has already been mentioned, i.e., by analyzing the existing data and making judgments about the future situation. However, because of time constraints and various factors, this article does not conduct an in-depth study of this.

3.3.6. Multisource Database. The model mainly includes a knowledge training database and a multisource sensor database. The knowledge training database stores the existing network data and uses these obvious and complete data to carry out corresponding knowledge training. As the name implies, the multisource sensor database stores the information collected by each sensor.

3.4. Perception Process. Before the entire sensing process, firstly, multisource sensors conduct network data collection and then conduct the entire sensing process based on this. Because of the differences in the network data collected by different sensors, it is necessary to format the data according to certain specific requirements. After the formatted multisource data passes through the situation fusion module, the data redundancy problem is greatly alleviated, and finally, the false alarm rate is also greatly reduced. The amount of data after fusion has been greatly reduced, which is helpful for the quantitative assessment of the situation. In the process of situation assessment, the abstract and incomprehensible multidimensional data is converted into intuitive and easy-to-see numerical types, and the abstract virtual network security situation is clear at a glance.

Optimal classification of distance vector: firstly, the center of various security events is obtained by the K-means clustering of the training set, and the multisource data is classified according to the optimal classification of distance vector. Because of the existence of uncertain events, it not only affects the accuracy of the final fusion results but also greatly increases the calculation amount of data fusion.

Bayes approximation fusion: in this paper, Bayes approximation is used to avoid the adverse effect of uncertain events on the data fusion process. Bayes approximation is the development of D-S evidence theory, and it is a compromise method to improve the fusion efficiency on the premise of ensuring a subtle influence on the final accuracy of fusion.

3.5. Situation Assessment Based on Dynamic Threat Weight. Hierarchical dynamic threat weights were built based on fused D-S evidence. The algorithm includes two parts: dynamic threat factor generation and hierarchical situation assessment. The determination of dynamic threat factors will be described in detail in the service-level assessment. The various threats in the network are mainly for a certain service in the host. Hence, the security situation assessment of the service layer and the network-level situation assessment is based on the results of the host and service-level situation assessment. Based on basic calculations, in the end, the administrator will understand and judge the current results of the network-level assessment.

3.5.1. Service-Level Situation Assessment. After determining the threat level, the threat value changes with the continuous change of this type of attack event within the determined level range, thereby enhancing the sensitivity to the attack event. Based on this, a dynamic threat weight situation assessment algorithm is proposed.

3.5.2. Host-Level Situation Assessment. The host-level situation assessment is based on the service-level situation assessment, which evaluates the importance of the integrated host in the network.

3.5.3. Network-Level Situation Assessment. The network-level situation assessment, as the top and final stage in the entire hierarchical assessment process, undoubtedly played a decisive role in the overall situation assessment. The network-level situation assessment will make a final assessment in accordance with the rules based on the results of the lower-level assessment, combined with the current network conditions.

4. Results and Discussion

According to the experimental requirements, the KDDCup99 intrusion detection data set is used as the training set and test data of the event center, and 220 pieces of attack data are used to test the fusion results. In the situation assessment performance analysis, the network security situation fusion awareness technology realized in this paper is used as an experimental platform to carry out the assessment performance analysis. In this simulation experiment, a total of 220 attacks were performed, and the distance vector optimal classification algorithm was used to identify the attack type. The recognition rate for Probe and Dos attacks is high, while the recognition rate for U2R and R2L is low, indicating that the training for U2R and R2L attack types is not ideal. The recognition rate under different attack types is shown in Table 1.

From the overall fusion, the distance vector optimal classification fusion algorithm security events are compared with the traditional DS fusion algorithm, however, a clean and effective training set will have a very obvious impact on the accuracy of the recognition rate. Therefore, the method still needs to be improved, and it is necessary to further strengthen the adaptiveness of the algorithm and reduce the dependence on the training set. The security event recognition rate comparison is shown in Table 2.

The evolution curve of the final situation value obtained using the dynamic threat weight evaluation algorithm and the constant threat weight evaluation algorithm is shown in Figure 3. From the constant threat weight evaluation algorithm, it can be seen that at 10:30:27–10:30:31, the host's security status is good and there is no attack event. At 10:30:32–10:30:46, DoS attacks continue to occur, and the situation value curve changes upward, however, under the traditional constant threat weight algorithm, this section of the situation value curve is a horizontal straight line, which cannot intuitively reflect the further deterioration of the threat situation. From the experiments of the dynamic threat weight evaluation algorithm and the constant threat weight evaluation algorithm, we can conclude that the dynamic threat weight evaluation algorithm and the traditional

Table 1: Recognition rate under different attack types.

Attack type	Quantity (times)	Actual capture (times)	Recognition rate%
Probe	60	56	93.3
U2R	40	11	27.5
R2L	50	28	56.0
DoS	70	59	84.3

Table 2: Comparison of security incident recognition rate.

Parameter	Traditional D-S	Experience weighted D-S	Distance vector optimal classification
Detection rate%	50	56	62

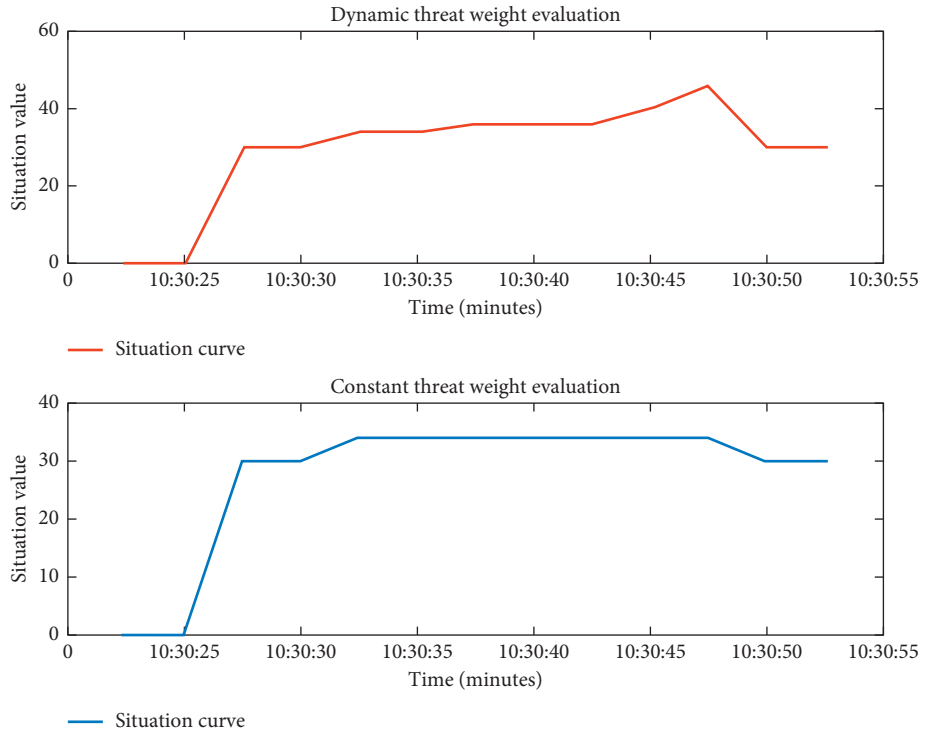

Figure 3: The evolution curve of the final situation value obtained by the dynamic threat weight evaluation algorithm and the constant threat weight evaluation algorithm.

constant threat weight evaluation algorithm can reflect the occurrence of the attack to a certain extent. When a certain type of attack event continues to occur, the situation value obtained according to the dynamic threat weight algorithm is more accurate than the result of the constant threat weight evaluation algorithm, and the dynamic threat weight is more sensitive at this time.

The calculation of the service importance index adopts the scaling method, which means that the importance of the service is divided into three levels: high, medium, and low, and the values are 3, 2, and 1, respectively. Because of the uncertainty of factors and the complexity of logical relationships, it is difficult to establish a dynamic service importance evaluation model. The importance of services in this article is determined by the following two key factors. The importance of ensuring that the host completes its specific functions is of high importance. For example, the importance of the FTP service is high access statistics. The higher the number of visiting users and the higher the visiting frequency, the higher the service importance index. The principles for judging the importance of services are shown in Table 3.

This article combines objective statistical information and subjective experience knowledge. The more the mainstream service users, the greater the access frequency, and the higher the importance of the service. The mainstream service is a Boolean variable: a value of 1 means a mainstream service. Otherwise, it is a nonmainstream service. Service importance is shown in Table 4.

Service 1 suffered 1 attack with a difficulty level of easy and a high severity level on the first day, 30 times with a difficulty level of easy and a medium severity level, and 16 attacks with a difficulty level of easy and a low severity level. On the second day, there were only 20 attacks with easy difficulty and high severity. In the same way, the security

Table 3: Judgment principles of service importance.

User number	Visit frequency (times/day)	Service importance index	Value
[0, 20)	[0, 50)	Low	2
[20, 50)	[50, 100)	Medium	3
[50,100)	[100,+)	High	2
[0, 20)	[100,+)	Medium	3
[20, 50)	[0, 50)	Low	2
[20, 50)	[100,+)	High	3

Table 4: Service importance.

Numbering	Mainstream service	User number	Visit rate (times/day)	Importance of service
1	1	(0,20)	[0,50)	6
2	1	[20,50)	[50,100)	8
3	1	[50,∞)	[100,∞)	10
4	1	(0,20)	[50,100)	7
5	1	(0,20)	[100,∞)	8
6	1	[20,50)	[0,50)	7
7	1	[20,50)	[100,∞)	9

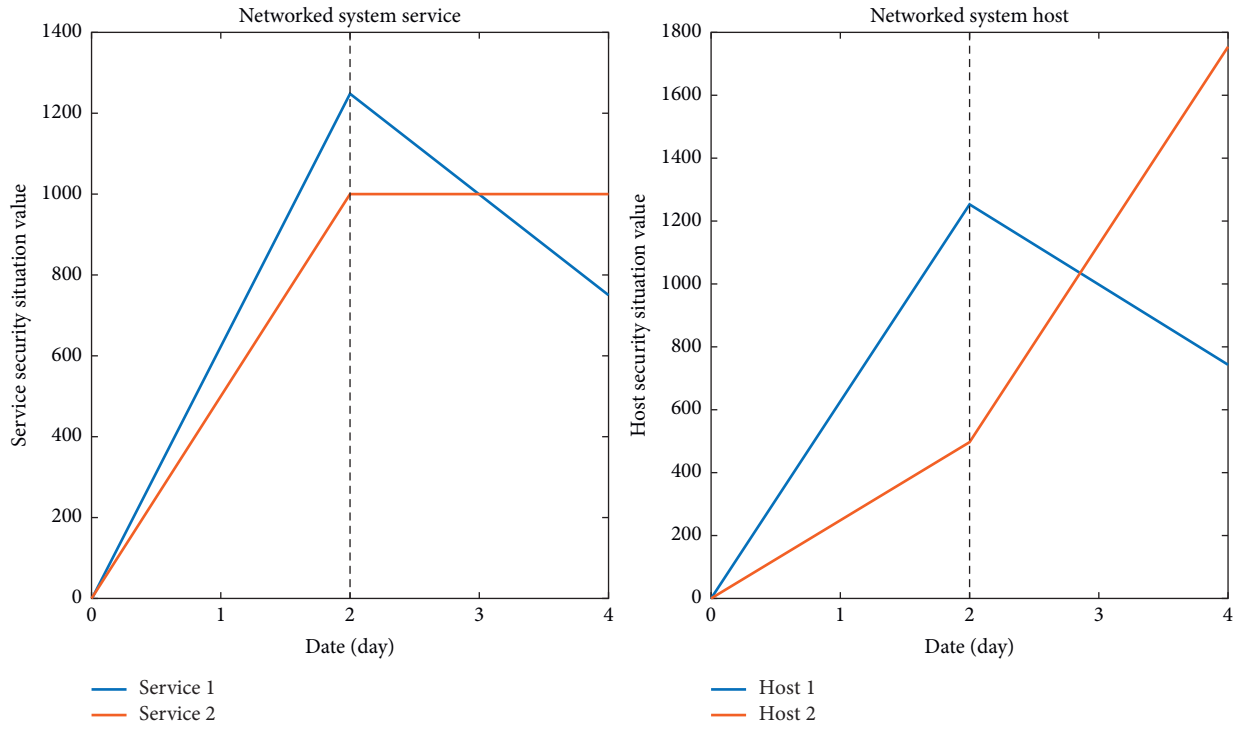

Figure 4: The security situation of networked system services and the security situation of networked system hosts.

situation during the two days of service is basically the same. Since host 2 was severely attacked a large number of times (80 times) the next day and the attacked service had a large weight in the host, the security situation of host 2 deteriorated rapidly. Relatively speaking, the two-day attack on host 1 did not change significantly from the frequency of attacks, however, as the attacks on the second day were mainly concentrated on services with smaller weights, the security posture value of host 1 declined. The security situation of the networked system services and the security situation of the networked system hosts are shown in Figure 4.

The service threat index depends on the normal traffic volume, attack threat level, and attack intensity within a certain period of time. The degree of attack threat judgment is shown in Table 5.

The host vulnerability index mainly depends on the vulnerabilities of the host, including the type, popularity, ease, and damage of the vulnerabilities. According to the vulnerability scanning information provided by the underlying module, a vulnerability database is established as shown in Table 6.

Suppose there is a virtual network, which is composed of two subnets, as shown in Figure 5. Subnet 1 includes an FTP

Table 5: Judgment of attack threat degree.

Attack type	Attack description	Attack threat level	Value
Attack manager type	Attempt to gain admin rights	High	3
Types of attacking users	Attempt to gain user rights	High	2
Types of denial-of-service attacks	Attempts to disrupt service availability	Medium	1

Table 6: A vulnerability database based on the vulnerability scanning information provided by the underlying module.

Vulnerability name	Host	As a result of	Popularity	Ease	Hazard
Weak passwords for ordinary users	A	Obtain normal user permissions	0.2	0.2	0.2
Newgrp buffer overflow	A	Obtain root user rights	0.9	0.8	0.867
SSH privilege escalation	B	Get admin rights	0.9	0.9	0.9
MrYSQL default configuration	C	Can access and change the database	0.9	0.9	0.93

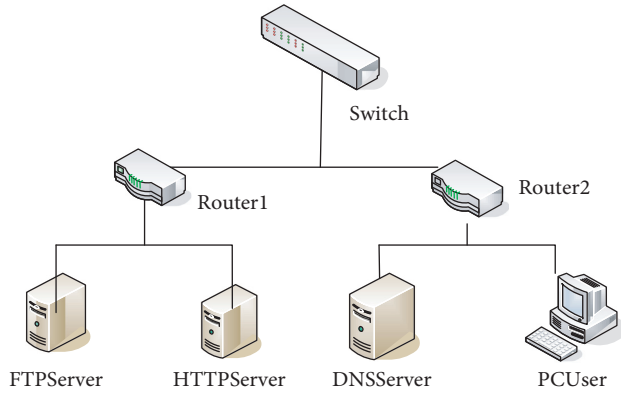

Figure 5: Organizational diagram of the virtual network.

Table 7: The risk value of three services in one week.

Service	Time						
	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
DNS	850.20	1298.00	1073.18	826.20	898.20	951.82	2421.82
HTTP	195.38	1129.50	413.20	242.25	242.00	262.00	236.50
RPC	365.25	560.86	400.73	515.75	519.44	695.1 1	440.60

server and an HTTP server. Subnet 2 includes a DNS server and a client. The two subnets are connected by switches. This paper simulates the operation information of the network from Monday to Sunday, including the attack and the number of visits to each machine. According to the operation information, the daily risk situation of the network is evaluated. The following is a hierarchical analysis of the test results. FTP is a file transfer protocol, and HTTP is a hypertext transfer protocol. In essence, they are two different transfer protocols, one for files and one for hypertext. The HTTP protocol is based on the request/response paradigm. The simplest case may be a separate connection between the user agent and the origin server. FTP has two transmission modes, ASCII, and binary, and the operation under different transmission modes is different. FTP has a very high latency, which means that the time from the start of the request to the first receipt of the required data will be very long. From time to time, some lengthy login processes must be performed. Since the HTTP connection is real-time, even if there is a delay, there is a very slight gap.

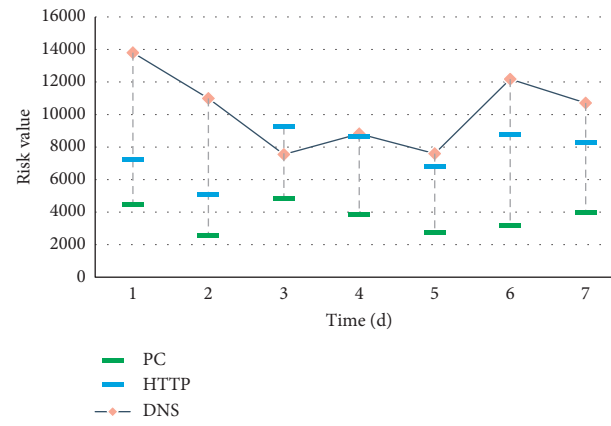

Figure 6: HTTP server, DNS server, and PC client test.

DNS service, HTTP service, and RPC service are running on the DNS server, and there are two system vulnerabilities in SSH privilege escalation and MYSQL default configuration. Take the three services running on the DNS server as an

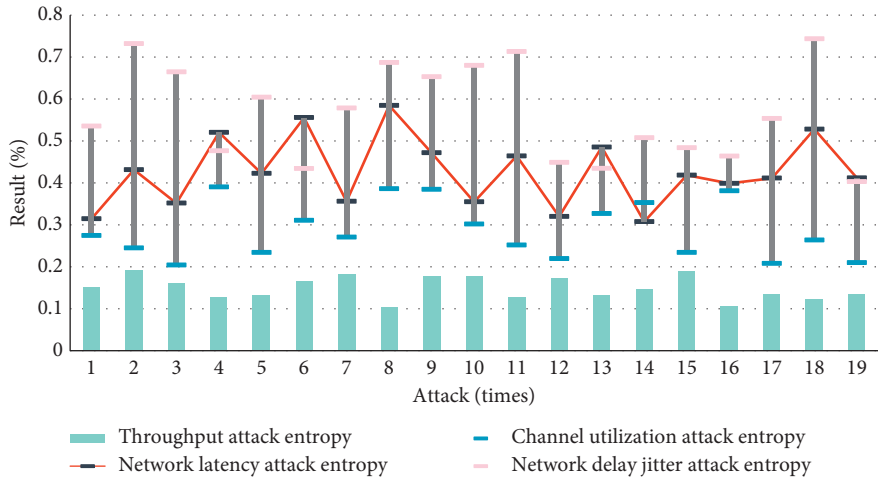

Figure 7: Changes in the entropy of network security indicators before and after the attack and the evaluation results of the attack effect.

example to analyze the test results of the service layer. The risk values of the three services in one week are shown in Table 7. It is not difficult to find that the risk value of the DNS service is always higher than the risk value of the other two services. It is because the DNS service is the main service provided by the DNS server, and the importance index of the DNS service is high. In this way, the risk value will be higher when it is under the same threat, which is consistent with the test result.

The test of the HTTP server, DNS server, and PC user machine is shown in Figure 6. In the test results, the risk value of the PC user machine is always lower than the risk value of the other two servers. It is because the PC user machine does not provide network services. Hence, its importance is relatively low. In this way, its risk value is low. Comparing the two servers, we will find that the DNS server has a higher risk value than the HTTP server. It is because the vulnerability of the DNS server has a greater impact on the security of the host, and the vulnerability of the DNS server is high, which affects the risk value of the host. It is consistent with the test results.

For the test of the attack evaluation module, a DoS attack and a Ping attack occurred on this virtual network. Record the network security feature indicators before and after the attack, calculate the changes in the entropy of the network security indicators before and after the attack, and the evaluation results of the attack effect as shown in Figure 7. Among them, the highest probability is 4, followed by 5. Therefore, the network status is relatively dangerous, and remedial measures should be taken in time. At the same time, it can be calculated that the 19^{th} attack period overall situation of the network is 4.4.

5. Conclusion

To improve the processing speed of the situation understanding process and meet the real-time requirements of situation awareness, a simple data-level fusion method is adopted. A large amount of heterogeneous security data output by the detection equipment is classified into four types of data: asset data, threat data, vulnerability data, and network structure data. The relationship between the data types is not analyzed. The situation awareness model based on dynamic threat weight provides the basis for the follow-up research. Based on the reality of multidata sources, a dynamic threat weight situation assessment method based on hierarchical quantitative evaluation is proposed on the premise of D-S evidence fusion. The research goal of detecting the host security situation in the actual network environment is achieved. At present, the implementation of fusion perception technology still focuses on situation awareness at the host level, and in the future, it will focus on the network level situation awareness technology. In addition, in the process of technology realization, there is no interaction with the software engineering department. The setting of the technology realization goal is relatively rough, and the whole development process lacks reasonable and effective planning, which leads to many unnecessary problems and difficulties in the development. In the future, we need to learn lessons from the continuous improvement process and try to make the realization of the technology in a more perfect manner. Improving the display content of situational awareness results, providing a visual and easy-to-interact situational awareness interface, and generating situational awareness reports in various formats are all areas that need to continue to be studied in the future.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by Youth Fund for Humanities and Social Sciences Research of the Ministry of Education under Grant no. 18YJC710092, General Project of Philosophy and Social Science Planning in Shanghai under Grant no. 2017BKS011, and the Youth Fund for Humanities and Social

Sciences Research of the Ministry of Education "Research on the Audience Communication of Internet Rumors in the Era of Big Data"(Project number: 18YJC860021).

References

[1] Y. Zhang, L. Wang, Y. Xiang, and C. W. Ten, "Power system reliability evaluation with SCADA cybersecurity considerations," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1707–1721, 2017.

[2] A. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2017.

[3] V. N. Kolokoltsov and A. Bensoussan, "Mean-field-game model for botnet defense in cyber-security," *Applied Mathematics & Optimization*, vol. 74, no. 3, pp. 1–24, 2016.

[4] C. S. Kruse, B. Frederick, T. Jacobson, and D. K. Monticone, "Cybersecurity in healthcare: a systematic review of modern threats and trends," *Technology & Health Care*, vol. 25, no. 1, pp. 1–10, 2016.

[5] R. H. Weber and E. Studer, "Cybersecurity in the internet of things: legal aspects," *Computer Law & Security Review*, vol. 32, no. 5, pp. 715–728, 2016.

[6] S. Mahdavifar and A. A. Ghorbani, "DeNNeS: deep embedded neural network expert system for detecting cyber attacks," *Neural Computing and Applications*, vol. 32, no. 18, pp. 14753–14780, 2020.

[7] F. Khorrami, P. Krishnamurthy, and R. Karri, "Cybersecurity for control systems: a process-aware perspective," *IEEE Design & Test*, vol. 33, no. 5, pp. 75–83, 2016.

[8] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommunications Policy*, vol. 41, no. 10, pp. 1027–1038, 2017.

[9] J. C. Balda, A. Mantooth, R. Blum, and P. Tenti, "Cybersecurity and power electronics: addressing the security vulnerabilities of the internet of things," *IEEE Power Electronics Magazine*, vol. 4, no. 4, pp. 37–43, 2017.

[10] S. Saran, "Striving for an international consensus on cyber security: lessons from the 20th century," *Global Policy*, vol. 7, no. 1, pp. 93–95, 2016.

[11] R. Atat, L. Liu, H. Chen, J. Wu, H. Li, and Y. Yi, "Enabling cyber-physical communication in 5G cellular networks: challenges, spatial spectrum sensing, and cyber-security," *IET Cyber-Physical Systems: Theory & Applications*, vol. 2, no. 1, pp. 49–54, 2017.

[12] M. Anwar, W. He, I. Ash, X. Yuan, L. Li, and L. Xu, "Gender difference and employees' cybersecurity behaviors," *Computers in Human Behavior*, vol. 69, no. APR, pp. 437–443, 2017.

[13] S. Mckenna, D. Staheli, C. Fulcher, and M. Meyer, "BubbleNet: a cyber security dashboard for visualizing patterns," *Computer Graphics Forum*, vol. 35, no. 3, pp. 281–290, 2016.

[14] A. Nagurney and S. Shukla, "Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability," *European Journal of Operational Research*, vol. 260, no. 2, pp. 588–600, 2017.

[15] S. Nazir, S. Patel, and D. Patel, "Assessing and augmenting SCADA cyber security: a survey of techniques," *Computers & Security*, vol. 70, no. sep, pp. 436–454, 2017.

[16] J. Zerlang, "GDPR: a milestone in convergence for cybersecurity and compliance," *Network Security*, vol. 2017, no. 6, pp. 8–11, 2017.

[17] L. Bader, J. Pennekamp, R. Matzutt et al., "Blockchain-based privacy preservation for supply chains supporting lightweight multi-hop information accountability," *Information Processing & Management*, vol. 58, no. 3, Article ID 102529, 2021.

[18] M. Hashem Eiza and Q. Ni, "Driving with sharks: rethinking connected vehicles with vehicle cybersecurity," *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 45–51, 2017.

[19] H. de Bruijn and M. Janssen, "Building cybersecurity awareness: the need for evidence-based framing strategies," *Government Information Quarterly*, vol. 34, no. 1, pp. 1–7, 2017.

[20] S. Hennessey, "Deterring cyberattacks: how to reduce vulnerability: the cybersecurity dilemma: hacking, trust, and fear between nations: cyberspace in peace and war," *Foreign Affairs*, vol. 96, no. 6, pp. 39–46, 2017.

[21] R. Parthasarathy, D. K. Wyant, P. Bingi, J. R. Knight, and A. Rangarajan, "DeTER framework," *International Journal of Intelligent Information Technologies*, vol. 17, no. 2, pp. 1–24, 2021.

[22] N. Buchler, P. Rajivan, L. R. Marusich, L. Lightner, and C. Gonzalez, "Sociometrics and observational assessment of teaming and leadership in a cyber security defense competition," *Computers & Security*, vol. 73, no. MAR, pp. 114–136, 2018.

[23] K. M. Ball, "African union convention on cyber security and personal data protection," *International Legal Materials*, vol. 56, no. 1, pp. 164–192, 2017.

[24] G. Wen, Y. U. Wenwu, Y. U. Xinghuo et al., "Complex cyber-physical networks: from cybersecurity to security control," *Journal of Systems Science & Complexity*, vol. 30, no. 1, pp. 46–67, 2017.