A Novel Method of Network Security Situation Assessment Based on Evidential Network

Xiang Li[1], Xinyang Deng[1(✉)], and Wen Jiang[1,2]

[1] School of Electronics and Information, Northwestern Polytechnical University, Xi'an, China
xinyang.deng@nwpu.edu.cn
[2] Peng Cheng Laboratory, Shenzhen, China

Abstract. Network security situation awareness is a new type of network security technology. It evaluates the network security situation in real time from a macro perspective. Also it can predict the trend of the development of the network security situation, providing a basis for the decision analysis of administrators. It is difficult to obtain complete and accurate information in network security situation assessment by using evidential network. So we introduce an evidential network based on Bayesian network to solve that problem. Firstly, transform the parent node information and inference rules into plausibility function so as to be compatible with imperfect and inaccurate information. Secondly, we use the full probability formula of Bayesian network as reference to make similar reasoning under the framework of evidence theory. Then transform the inference result to BPA form by using the minimum specificity algorithm, and obtain the final result by projection. Finally, an example of network security situation assessment is given to illustrate the rationality and effectiveness of the method.

Keywords: Network security situation assessment · Evidence theory · Bayesian network · Evidential network

1 Introduction

In recent years, the rapid development of the Internet makes the use of computer systems more and more common and people have become more and more inseparable from the network. Network security has become a key issue related to all areas of the network. How to perceive the situation of network security in time and effectively has aroused enough attention from relevant researchers.

Network security situational awareness refers to that in the large-scale network environment, Network security situation awareness refers to the acquisition, understanding, display and prediction of future development trends of security elements that can cause changes in network security situation in a large-scale network environment [1, 2], which can provide direct and effective global information, real-time response capability "afterwards" and timely early warning capability "in advance" to realize dynamic security protection for security managers. Situation assessment is the core part of the network, which reflects the overall security status of the network by

X. Chen et al. (Eds.): ML4CS 2020, LNCS 12486, pp. 530–539, 2020.
https://doi.org/10.1007/978-3-030-62223-7_46

comprehensively analyzing the security factors of all aspects of the network. Tim Bass [3] introduced situational awareness into the field of network security for the first time. He believes that the fusion of multi-sensor data to form network situational awareness is the key breakthrough of the next generation intrusion detection system. Since then, research teams from different countries have proposed a variety of data models and platforms based on different knowledge systems.

Wen et al. [4] applied Bayesian network to evaluate network security situation. Ye et al. [5] used deep learning to extract the characteristics of large-scale network data, and analyzed and evaluated the network security situation. Vinayakumar [6] proposed a network security situation prediction method based on domain name systems data analysis. Chen et al. [7] proposed a hierarchical evaluation method, and obtained the three-level security threat situation by using the host, service and system for hierarchical calculation. Liu et al. [8] applied cloud models and Markov chain to carry out network security situation assessment.

None of the above methods fully consider the uncertainty and randomness of network security situation assessment. And each method has its own disadvantages, firstly the prior probability of Bayesian network is difficult to obtain. Then, for a deep learning model, it requires a lot of data and a lot of time to train the model and it is difficult to evaluate in real time. Finally, the hierarchical structure model and paired comparison matrix of AHP are mostly determined based on experience, with strong subjectivity.

Based on the comprehensive comparison of various methods, this paper chooses to use evidential network based on Bayesian network for evaluation. The existing evaluation methods mainly analyze the security events caused by attacks, and the threats caused by the peak of normal behavior are not investigated enough. Therefore, this paper comprehensively analyzes the normal behavior and attack behavior in the network environment to evaluate the network security situation.

The rest of the paper is arranged as follows. Section 2 briefly introduces D-S evidence theory and Bayesian network. In Sect. 3, the method proposed in this paper are introduced. An example of network security assessment is given in Sect. 4 to illustrate the effectiveness of the method in this paper. Finally, the conclusion is given in Sect. 5.

2 Preliminaries

2.1 Evidence Theory

Evidence theory [9, 10] is an imprecise reasoning theory first proposed by Dempster and further developed by Shafer, also known as The Dempster-Shafer Theory of Evidence. The subjective Bayes method must give the prior probability, while the evidence theory can deal with the uncertainty caused by ignorance. When the probability value is known, the evidence theory becomes the probability theory.

Assuming that Θ is the exhaustive set of all possible values variables X, and the elements are mutually exclusive. We call Θ frame of discernment (FOD). Assuming that there are N elements in Θ, $\Theta = \{A_1, A_2, \ldots, A_N\}$, so the number of the elements of the

power set of Θ is 2^N, $2^\Theta = \{\{\emptyset\}, \{A_1\}, \ldots, \{A_N\}, \{A_1, A_2\}, \ldots, \{A_1, A_N\}, \ldots, \{\Theta\}\}$ and each member of the set corresponds to a subset of the values of X.

Definition 2.1. A basic probability assignment (BPA) is a function $m : 2^\Theta \rightarrow [0, 1]$, which satisfies:

$$\begin{cases} m(\emptyset) = 0 \\ \sum\limits_{A \in 2^\Theta} m(A) = 1 \end{cases} \tag{1}$$

where A is any subset of Θ. The function $m(A)$ represents the evidence's support degree for A. A is called the focal element of m when $m(A) > 0$.

Definition 2.2. Given a BPA, the believe function *Bel* and the plausibility function *Pl* represent the lower and upper limits of the degree of trust for each proposition, respectively. The definition is as follows:

$$Bel(A) = \sum_{B \subseteq A} m(B) \qquad \forall A \subseteq \Theta \tag{2}$$

$$Pl(A) = 1 - Bel(\bar{A}) = \sum_{B \cap A \neq \emptyset} m(B) \qquad \forall A \subseteq \Theta \tag{3}$$

Definition 2.3. For a BPA, its specificity was measured by *Sp* function. The definition is as follows:

$$Sp = \sum \frac{m(A)}{|A|} \qquad \forall A \subseteq \Theta \tag{4}$$

Definition 2.4. If m is a BPA on a FOD Θ, a PPT function $BetP_m$ P: $\Theta \rightarrow [0, 1]$ associated with m is defined by

$$BetP_m(x) = \sum_{x \in A, A \in \Theta} \frac{1}{|A|} \frac{m(A)}{1 - m(\emptyset)} \tag{5}$$

where $m(\emptyset) \neq 1$ and $|A|$ is the cardinality of proposition A.

2.2 Bayesian Network

A Bayesian network [11] is a directed acyclic graph (DAG), which is composed of variable nodes and directed edges. The nodes represent random variables, and the directed edges between nodes represent the relations between nodes (from the parent node to the child node). The relationship strength is expressed by conditional probability, and the

information is expressed by prior probability for a node without parents. It is suitable for expressing and analyzing uncertain and probabilistic events, and for making decisions that depend on various control factors conditionally. It can make inferences from incomplete, inaccurate or uncertain knowledge or information [12].

Definition 2.5. Assuming that $G = (I, E)$ represents a DAG, where I represents the set of all nodes in the graph, and E represents the set of directed connection edges. $X = X_i\, i \in I$ is the random variable represented by a node i in the DAG. The conditional probability distribution of node X can be expressed as:

$$p(x) = \prod_{i \in I} p\left(x | x_{pa(i)}\right) \tag{6}$$

where $x_{pa(i)}$ represents the cause of a node i.

For any random variable, its joint distribution can be obtained by multiplying their local conditional probability distributions:

$$P(X_1 = x_1, \ldots, X_n = x_n) = \prod_{i=1}^{n} P(X_i = x_i | X_{i+1} = x_{i+1}, \ldots, X_n = x_n) \tag{7}$$

Bayesian network is probabilistic reasoning, and it can be extended to evidential network reasoning within the framework of evidence theory [13].

3 The Proposed Method

In this section, an evidential network model is introduced to network security assessment based on approaches in evidence theory [14]. There are two problems when reasoning by traditional evidential network [15]: Firstly, the information of the parent node is difficult to express completely and accurately, and it is difficult to obtain the information of the root node when the number of focal elements in the parent nodes is large. Then, for a non-parent node, the size of its conditional belief mass table increases exponentially with the rise of the cardinalities of its parents' FODs. On one hand, the size of such table is huge; On the other hand, it is a big challenge to generate such a huge conditional belief mass table.

Aiming at the two problems, the solution of this paper is proposed as follows: Firstly, Transform the parent node information from the expression of BPA to the expression of plausibility function *Pl*. Then, transform the reasoning rules from the conditional belief mass table to conditional plausibility function table. This makes the network still able to reason in the case of incomplete inference rules. As shown in Fig. 1 shows the process of this method.

Step 1. Construct an evidential network. An evidential network is defined as a directed acyclic graph (DAG). For example, there are three nodes, including two parent nodes X with FOD $\Theta_X = \{X_1, X_2\}$, Y with FOD $\Theta_Y = \{Y_1, Y_2\}$, and a child

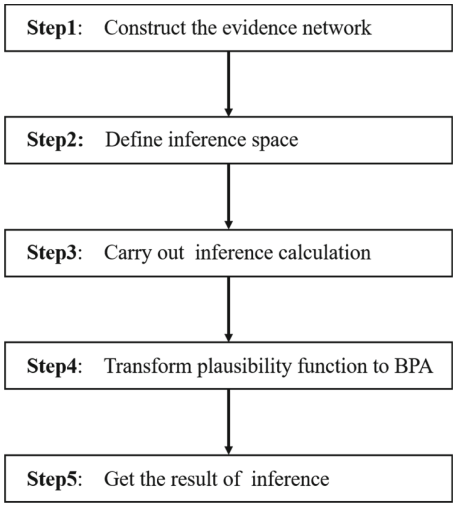

Fig. 1. A flowchart of the introduced evidential network.

node of X and Y called Z with FOD $\Theta_Z = \{Z_1, Z_2\}$. We can construct an evidential network show in Fig. 2. The parent node represents the network parameters obtained, and the child node represents the network security situation evaluation results. The evidence network may have more than one layer.

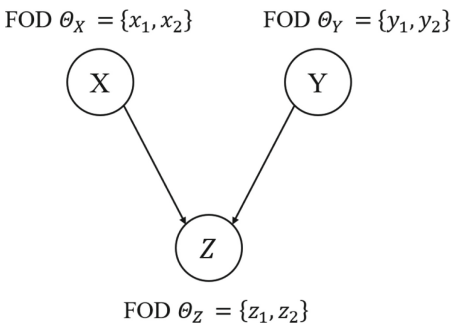

Fig. 2. An example of evidential network.

Step 2. By simplifying an extension operator given in [14], we use it to do the evidential network reasoning. As modelled in [14], the space composed of the parent node FOD called E_e, the space composed of the child node FOD called E_s. For example, in the evidential network shows in Fig. 2, $E_e = \{\Theta_X, \Theta_Y\}$ and $E_s = \{\Theta_Z\}$. $Pl_e(\cdot)$ is the plausibility function on E_e, which may be incomplete; $Pl_s(\cdot|B \subseteq E_e)$ is the plausibility function on E_s, which may be incomplete, and is valid when the subset B of E_e is definitely true. If the information we obtain on parent nodes is BPA and the rules we obtain is conditional belief mass table, we can

use the formula (3) to transform to the plausibility function $Pl_e(\cdot)$ and the conditional plausibility function table $Pl_s(\cdot|B\subseteq E_e)$. If the information on parent nodes and rules are plausibility function and conditional plausibility function table respectively, we can skip this step.

Step 3. Determination of the $Pl_{sr}(A \times B)$ values on $E_s \times E_r$, for all available data, using the formula from [14]:

$$Pl_{sr}(A \times B) = Pl_s(A|B\subseteq E_r)Pl_e(B) \tag{8}$$

where $Pl_{sr}(\cdot)$ represents a joint distribution plausibility function.

Step 4. There are many such $m(\cdot)$ functions, rather than just one, will satisfy an incompletely defined plausibility function. In order to obtain the $m(\cdot)$ on space E and keep as much information as we can and don't impose information, we use the minimum specificity algorithm proposed by Appriou [14] to transform plausibility function to BPA. Thus, out of all the possible functions, we look for the function that has least specificity $Sp(m)$.

Step5. Determination of the mass function $m_s(\cdot)$ on Es on the basis of $m_{sr}(\cdot)$, using the formula:

$$m_s(A) = \sum_{B\subseteq E_r} m_{sr}(A \times B) \tag{9}$$

So far, we have obtained the inference result of the child node, and we can proceed to the next inference or evaluate the situation of the child node according to this result.

4 Case Study

In this section, an example mentioned in paper [16] will be used to confirm the effectiveness of the proposed method. Because the security of network will be affected by the peak of normal behavior and attack behavior, this paper divides the network security into normal behavior and attack behavior to consider the network security situation. The change of network resources will reflect the change of network security situation. CPU resources and memory resources are important resources in the network. Improper use of the network or when the network is attacked, the two resources may be exhausted, resulting in network performance degradation or even crash. Therefore, this paper selects CPU utilization and memory consumption as security factors to evaluate the network security situations.

Step 1. According to the above analysis, an evidential network is constructed as follows (Fig. 3):

In the evidential network MC, CPU, NB, AB and NS represent memory consumption, CPU utilization, normal behavior, attack behavior and network security respectively. And the FOD of MC, CPU, NB, AB have two elements $\Theta = \{G_1, G_2\}$, G_1 and G_2 represent the good and bad for assessment of the FOD.

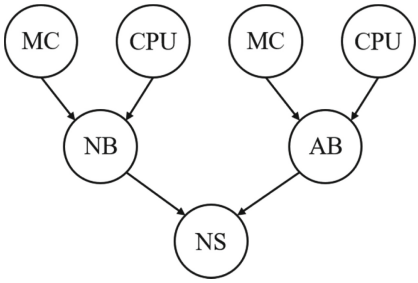

Fig. 3. The evidential network we construct for network security situation assessment [16].

The FOD of NS have four elements $\Theta = \{G_1, G_2, G_3, G_4\}$. Elements from G_1 to G_4 means excellent, good, ordinary and bad.

Step 2. Network security has a greater impact on CPU utilization. Compared with normal behavior, the harm caused by attack behavior to network environment is much more serious. In order to simplify the calculation, we assume that the conditional plausibility function table between memory consumption, CPU utilization and normal behavior and attack behavior is same. For the evidential network, suppose we have the following conditional plausibility function Tables 1 and 2.

Table 1. The conditional plausibility function table between {CPU, MC} and {NB}/{AB}.

CPU / MC	$\{G_1^1\}$	$\{G_2^1\}$	$\{G_1^1, G_2^1\}$
$\{G_1^2\}$	$Pl(G_1) = 1$ $Pl(G_2) = 0.1$ $Pl(G_1, G_2) = 1$	$Pl(G_1, G_2) = 1$	
$\{G_2^2\}$	$Pl(G_1) = 0.8$ $Pl(G_2) = 0.3$ $Pl(G_1, G_2) = 1$	$Pl(G_1) = 1$ $Pl(G_2) = 0.8$ $Pl(G_1, G_2) = 1$	
$\{G_1^2, G_2^2\}$			

From the conditional plausibility function table, we can see that the inference rules are incomplete and imprecise. For example, we do not have the information when CPU is G_1, G_2 while MC is G_1. And the description of child node is fuzzy when CPU is G_1 while MC is G_1.

Table 2. The conditional plausibility function table between {AB, NB} and {NS}.

AB \ NB	$\{G_1^3\}$	$\{G_2^3\}$	$\{G_1^3, G_2^3\}$
$\{G_1^4\}$	$Pl(G_1, G_2) = 1$ $Pl(G_3, G_4) = 0.2$	$Pl(G_1, G_2) = 0.8$ $Pl(G_3, G_4) = 0.3$	
$\{G_2^4\}$	$Pl(G_1) = 0.8$ $Pl(G_2) = 0.6$ $Pl(G_3, G_4) = 0.4$	$Pl(G_1, G_2) = 0.3$ $Pl(G_3) = 0.6$ $Pl(G_4) = 0.5$	
$\{G_1^4, G_2^4\}$			

Then for the evidential network, assume we have the information of the parent node as follows:

$$m_{MC1}(\{G_1\}, \{G_2\}, \{G_1, G_2\}) = (0.6, 0.3, 0.1)$$
$$m_{CPU1}(\{G_1\}, \{G_2\}, \{G_1, G_2\}) = (0.8, 0.1, 0.1)$$
$$m_{MC2}(\{G_1\}, \{G_2\}, \{G_1, G_2\}) = (0.7, 0, 0.3)$$
$$m_{MCPU2}(\{G_1\}, \{G_2\}, \{G_1, G_2\}) = (0.9, 0.05, 0.05)$$

When reasoning from MC and CPU to NB, we can find that $E_r = \{MC, CPU\}$, $E_s = \{NB\}$. Other reasoning processes are similar as above.

Step 3. Compute the $Pl_{sr}(A \times B)$ values on $E_s \times E_r$ with formal (8). When reasoning from MC and CPU to NB, the result of $Pl_{sr}(A \times B)$ as follow:

$$Pl_{sr}\left(\{G_1, G_2\} \times \left\{G_1^1, G_1^2\right\}\right) = 0.63 \qquad Pl_{sr}\left(\{G_1, G_2\} \times \left\{G_2^1, G_1^2\right\}\right) = 0.36$$
$$Pl_{sr}\left(\{G_1, G_2\} \times \left\{G_2^1, G_2^2\right\}\right) = 0.08 \qquad Pl_{sr}\left(\{G_1, G_2\} \times \left\{G_1^1, G_2^2\right\}\right) = 0.14$$
$$Pl_{sr}\left(\{G_2\} \times \left\{G_1^1, G_1^2\right\}\right) = 0.063 \qquad Pl_{sr}\left(\{G_1\} \times \left\{G_2^1, G_1^2\right\}\right) = 0.288$$
$$Pl_{sr}\left(\{G_2\} \times \left(G_2^1, G_1^2\right)\right) = 0.108 \qquad Pl_{sr}\left(\{G_1\} \times \left\{G_2^1, G_2^2\right\}\right) = 0.08$$
$$Pl_{sr}\left(\{G_2\} \times \left\{G_2^1, G_2^2\right\}\right) = 0.064$$

By the same way, we can obtain $Pl_{sr}(A \times B)$ between {MC, CPU} and {AB}.

Step 4. Transform $Pl_{sr}(A \times B)$ to $m_{sr}(A \times B)$ by minimum specificity algorithm in Sect. 3. The result are as follows:

$$m_{sr}\left(\{G_1, G_2\} \times \left\{G_2^1, G_1^2\right\}\right) = 0.108 \qquad m_{sr}\left(\{G_1, G_2\} \times \left\{G_1^1, G_1^2\right\}\right) = 0.063$$
$$m_{sr}\left(\{G_1\} \times \left\{G_2^1, G_1^2\right\}\right) = 0.497 \qquad m_{sr}\left(\{G_1, G_2\} \times \left\{G_1^1, G_2^2\right\}\right) = 0.072$$
$$m_{sr}\left(\{G_1\} \times \left\{G_1^1, G_1^2\right\} \cap \{G_1, G_2\} \times \left\{G_2^1, G_2^2\right\}\right) = 0.064$$
$$m_{sr}\left(\{G_1, G_2\} \times \left\{G_1^1, G_2^2\right\} \cap \{G_1\} \times \left\{G_2^1, G_1^2\right\}\right) = 0.058$$
$$m_{sr}\left(\{G_1, G_2\} \times \left\{G_1^1, G_2^2\right\} \cap \{G_1\} \times \left\{G_2^1, G_2^2\right\}\right) = 0.01$$
$$m_{sr}\left(\{G_1\} \times \left\{G_2^1, G_1^2\right\}\right) = 0.122$$

Step 5. Compute the mass function $m_s(\cdot)$ on Es on the basis of $m_{sr}(\cdot)$ by formal (9). The result are as follows:

$$m_{NB}(\{G_1\}, \{G_1, G_2\}) = (0.625, 0.375)$$
$$m_{AB}(\{G_1\}, \{G_1, G_2\}) = (0.7455, 0.2545)$$

So far, we obtain the information on nodes NB and AB. In order to obtain the information on node NS, we just need to regard the NB and AB as parent nodes and repeat the above procedures. Finally, the BPA on node NS as follows:

$$m_{NS}(\{G1, \mathrm{G2}\}, \{G1, \mathrm{G2}, G3\}, \{G1, \mathrm{G2}, G4\}, \{G1, G2, \mathrm{G3}, \mathrm{G4}\}) = (0.4687, 0.0573, 0.0477, 0.4265)$$

We can assess the network security situation according to the result. For example, we transform the BPA to probability by PPT function to make the assessment more intuitive.

The result computed by the formal (5) is as follows:

$$P(G_1) = 0.3759 \qquad P(G_2) = 0.3759$$
$$P(G_3) = 0.1257 \qquad P(G_4) = 0.1225$$

We can conclude that the current network security situation is at a good level.

5 Conclusion

This paper has mainly studied the evaluation of network security situation based on evidential network and evaluate the network security situation by evidential network based on Bayesian network. Firstly, D-S evidence theory and Bayesian network are introduced, and then an evidential network based on Bayesian network is proposed to evaluate network security situation. Finally, an example is given to verify the feasibility of the method.

Acknowledgment. The work is partially supported by National Natural Science Foundation of China (61703338, 61671384), Equipment Pre-Research Fund (61400010109).

References

1. Li, Z., Goyal, A., Chen, Y., et al.: Towards situational awareness of large-scale botnet probing events. IEEE Trans. Inf. Foren. Secur. **6**(1), 175–188 (2011)
2. Gong, Z., Zhuo, Y.: Research on network situational awareness. J. Softw. **7**, 131–145 (2010)
3. Bass, T.: Intrusion detection systems and multisensor data fusion: creating cyberspace situational awareness. Commun. ACM **43**(4), 99–105 (2000)
4. Wen, Z., Cao, C., Zhou, H.: Network security situation assessment method based on naive Bayesian classifier. Comput. Appl. **35**(8), 2164–2168 (2015)
5. Ye, L., Tan, Z.: A network security situation assessment method based on deep learning. Intell. Comput. Appl. **9**(06), 73–75+82 (2019)
6. Vinayakumar, R., Poornachandran, P., Soman, K.P.: Scalable framework for cyber threat situational awareness based on domain name systems data analysis. In: Roy, S.S., Samui, P., Deo, R., Ntalampiras, S. (eds.) Big Data in Engineering Applications. SBD, vol. 44, pp. 113–142. Springer, Singapore (2018). https://doi.org/10.1007/978-981-10-8476-8_6
7. Chen, X., Zheng, Q., Guan, X., et al.: Quantitative hierarchy threat evaluation model for network security. J. Softw. **17**(4), 885–897 (2006)
8. Liu, H., Liu, J., Hui, X.: Network security situation assessment based on cloud model and Markov Chain. Comput. Dig. Eng. **47**(6), 1432–1436 (2019)
9. Dempster, A.P.: Upper and lower probabilities induced by a multivalued mapping. Ann. Math. Stat. **38**(2), 325–339 (1967)
10. Shafer, G.: A Mathematical Theory of Evidence. Princeton University Press, Princeton (1976)
11. Yakowitz, J.: An introduction to Bayesian Networks. Technometrics **39**(3), 336–337 (1997)
12. Terent'Yev, A.N., Bidyuk, P.I.: method of probabilistic inference from learning data in Bayesian networks. Cybern. Syst. Anal. **43**(3), 391–396 (2007)
13. Simon, C., Weber, P., Evsukoff, A.: Bayesian networks inference algorithm to implement Dempster Shafer theory in reliability analysis. Reliab. Eng. Syst. Saf. **93**(7), 950–963 (2008)
14. Appriou, A.: Uncertainty theories and multisensor data fusion. In: ISTE (2014)
15. Deng, X., Jiang, W.: Dependence assessment in human reliability analysis using an evidential network approach extended by belief rules and uncertainty measures. Ann. Nucl. Energy **117**, 183–193 (2018)
16. Cheng, S., Niu, Y., Li, J., Tong, K., et al.: A method of network security situation assessment based on evidential reasoning rules. Comput. Dig. Eng. **46**(8), 1603–1607 (2018)