Received: 6 May 2019 | Revised: 15 September 2019 | Accepted: 14 November 2019

DOI: 10.4218/etrij.2019-0147

ORIGINAL ARTICLE

ETRI Journal WILEY

Prediction of network security based on DS evidence theory

Dan Liu

Chongqing College of Electronic Engineering, Chongqing, China

Correspondence
Dan Liu, Chongqing College of Electronic Engineering, Chongqing, China.
Email: danliud@yeah.net

Network security situation prediction is difficult due to its strong uncertainty, but DS evidence theory performs well in solving the problem of uncertainty. Based on DS evidence theory, this study analyzed the prediction of the network security situation, designed a prediction model based on the improved DS evidence theory, and carried out a simulation experiment. The experimental results showed that the improved method could predict accurately in the case of a large conflict, and had strong anti-jamming abilities as compared with the original method. The experimental results prove the effectiveness of the improved method in the prediction of the network security situation and provide some theoretical basis for the further application of DS evidence theory.

KEYWORDS

convergence effect, data source correction, DS evidence theory, network security situation awareness, probability analysis

1 | INTRODUCTION

With the rapid development of networks, the problem of network security has become more and more prominent. A method, which can effectively display the network security state, is urgently needed. Prediction of the network security situation is a reflection of network operation conditions, and its objective is to accurately predict network security. In the field of network security situation, data are usually random, vague, and uncertain [1]. DS evidence theory has unique advantages because it has endless potential in the expression and synthesis of randomness and uncertainty and does not need prior probability and conditional probability as preconditions. It has gradually emerged as the focus of current network security situation research. However, due to different methods of data acquisition, the improper distribution of basic credibility may lead to an inconsistency between prediction results and intuition in evidence combination. Many scholars have studied this problem and proposed some improved methods [2–4], which are mainly divided into three categories. The first is to modify the DS synthesis rule, that is to study how to allocate conflict data reasonably. The second is to modify the method of data source acquisition, that is to modify the steps before synthesis to preprocess the data. The third is to use the combination model and DS evidence theory to carry out a combination analysis on the results obtained by multiple data prediction techniques. DS evidence theory has important application values in aspects such as target identification, driving behavioral decision and data fusion [5], which has been extensively studied by researchers. Zhang and Deng [6] proposed a new method based on decision-making and trial evaluation laboratory (DEMATEL) to consider the weight of the evidence and verified its effectiveness in dealing with conflicting evidence and reducing computational complexity by numerical particle. Wang and others [7] modified the classical basic probability allocation before combinations in a closed world using a basic belief function and found that this method had lower computational complexity, better performance, and good applicability in the case of evidence sequential occurrence. Xiao [8] proposed a new belief divergence measure and belief entropy

based on evidence for multisensor data fusion and verified the effectiveness of this method by numerical examples. Xiao and Ding [9] proposed a new bifurcation measure between Pythagorean fuzzy sets by using Jensen-Shannon divergence and designed a new algorithm to solve the problem of medical diagnosis. In addition to data fusion, DS evidence theory has a good application in risk assessment, but its application in network security situational awareness is infrequent. Currently, most of the network security situational awareness methods are based on pure mathematical models or methods that do not consider the actual situation. This makes it difficult to utilize it as effective guidance for network security decision-making. Based on the above studies, this study analyzed the role of DS evidence theory in the prediction of computer network security situation and problems existing in DS evidence theory, and performed real-data experiments using the effective improved method. The results of the study prove the reliability of the proposed method, which contributes to the further application of DS evidence theory in the field of prediction of network security situation, and is beneficial to the better development of the network security situation prediction and improvement in network security.

2 | RELATED BACKGROUND

2.1 | Network security situation prediction technology

Network security situation prediction is a means to obtain possible changes for a period of time in the future by synthetically using the present and past information of the network environment, according to the internal regularity of security situation changes and applying relevant methods, to provide suggestions to decisionmakers. It is an important part of network security situation awareness [10].

Because of different subjects, objectives, contents, and deadlines of network security situation prediction, there has been no universal unified classification system for network security situation prediction technology, to date. Currently, the commonly used prediction methods include regression analysis, neural network forecasting, time series forecasting, grey theory forecasting, and combination forecasting.

2.2 | Traditional DS evidence theory algorithm

The DS evidence theory algorithm includes the basic probability allocation method and the DS synthesis rule. The traditional basic probability allocation includes the mass function and the reliability function [11].

2.2.1 | Mass function, reliability function, and likelihood measure

1. Mass function: It is assumed that space P is a finite complete set with independent elements, which consists of all possible values of question Q. Then P is called the recognition framework of Q. Moreover, the set of all subsets of set P is expressed as 2^P. Now mapping m is defined, φ represents null set and $A \subseteq P$. If $m(\varphi) = 0$ exists and $\Sigma_A m(A) = 1$, then mapping $m{:}2^P \rightarrow [0, 1]$ is a mass function, representing the probability distribution of all hypotheses in recognition framework P.
2. Reliability function: When $m{:}2^P \rightarrow [0, 1]$ exists, suppose $B \subset A$, if there is $BEL{:}2^P \rightarrow [0, 1]$ and $BEL(A) = \sum_B m(B)$ for $\forall A \subset P$, then the function is called the reliability function on P, representing that the reliability of A is the sum of the basic reliability of its all subsets. $BEL(\phi) = 0$, $BEL(P) = 1$.
3. Likelihood measure: If $L(\varphi) = 0$, $L(P) = 0$, and $L\left(\bigcap_{i=1}^{n} A_i\right) \leq \sum_{I \subseteq \{1,2,\cdots,n\}, I \neq \varphi} (-1)^{|1|+1} L\left(\bigcup_{i \in I} A_i\right)$, then mapping $L{:}H(P) \rightarrow [0, 1]$ is called likelihood measure, representing the probability upper limit of the situation, that the hypothesis stands.

2.2.2 | DS synthesis rule

Suppose m_1 and m_2 are two mutually independent mass functions, and A, M, and N are subsets, then:

$$m(A) = \begin{cases} 0 & A = \varphi, \\ \dfrac{\sum_{M \cap N = A} m_1(M) m_2(N)}{\sum_{M \cap N \neq \varphi} m_1(M) m_2(N)} & A \neq \varphi, \end{cases} \tag{1}$$

is also a mass function.

3 | IMPROVEMENT IN DS EVIDENCE THEORY IN APPLICATION

3.1 | Modification of data source acquisition method

The specific method assigns different weights to the evidence. The evidence set is assumed as $O = \{O_1, O_2, \cdots, O_n\}$, and the weight coefficient of O_i as ω_i, which reflects the importance of evidence. Weight vector $G = (\omega_1, \omega_2, \cdots, \omega_n)$ is established, which satisfies $\omega_i \in [0, 1]$ and $\sum_{i=1}^{n} \omega_i = 1$.

The specific process allocates the basic credibility value to different elements in the identification framework and

establishes the weight vector of the evidence. The relative weight vector is obtained by:

$$G' = \frac{(\omega_1, \omega_2, ..., \omega_n)}{\omega_{\max}}, \tag{2}$$

where $\omega_{\max} = \max\{\omega_1, \omega_2, ..., \omega_n\}$. The discount rate is defined as:

$$\alpha_i = \frac{\omega_{\max} - \omega_i}{\omega_{\max}}, \tag{3}$$

where $i = 1, 2, ..., n$; thus it is obtained that $\alpha_i \in [0, 1]$. The basic credibility of the elements in the identification framework is adjusted as follows:

$$\begin{cases} m_i(O_j') = (1-\alpha_i)m_i(O_j), \\ m(P') = (1-\alpha_i)m(P) + \alpha_i, \end{cases} \tag{4}$$

where $j = 1, 2, ..., k_i$, k_i is the number of non-P basic credibility in the identification framework provided by evidence O_i. New evidence synthesis equations can be obtained by substituting into (1).

3.2 | Modified algorithm of combination prediction model

It is mainly divided into weight extraction and weight-based fusion algorithm. First, the weight of the single-item prediction model is determined through weight extraction. Then the historical weight is fused to obtain the weight of the single-item prediction model at the day of prediction. Details are as follows.

For weight extraction, it is assumed that relevant results have been obtained from h prediction models, and the prediction results are P_i, $i = 1, 2, ..., h$. The true value of the security situation is R. Prediction error $e_i = |P_i - R|$ is obtained after calculation, where $i = 1, 2, ..., h$. If μ_i, $i = 1, 2, ..., h$ is the corresponding weight coefficient then the result of the combination prediction can be expressed as:

$$P = \sum_{i=1}^{h} \mu_i P_i, \tag{5}$$

where $\sum_{i=1}^{h} \mu_i = 1$. The total error of the prediction result is:

$$E = \sum_{i=1}^{h} \mu_i e_i. \tag{6}$$

The variance is:

$$D(E) = \sum_{i=1}^{h} \mu_i^2 D(e_i) + \sum_{i \neq j, i, j = 1, 2, ..., h} \mu_i \mu_j \operatorname{cov}(e_i, e_j), \tag{7}$$

where $\operatorname{cov}(e_i, e_j)$ $(i, j = 1, 2, ..., h)$ is the covariance of error e_i and e_j, and $D(e_i)$ is the variance of error e_i. If the prediction of the same group of events is mutually independent, then $\operatorname{cov}(e_i, e_j) = 0$ $(i, j = 1, 2, ..., h$ and $i \neq j)$. The minimum value of $D(E)$ is calculated, therefore $\partial D(E)/\partial \mu_i = 0$. Thus, the expression of μ_i is:

$$\mu_i = \frac{1}{D(e_i) \sum_{i=1}^{h} \frac{1}{D(e_i)}}. \tag{8}$$

Weight fusion is analogical to the DS synthesis rule. It is assumed that relevant results have been obtained by h prediction models, and the predicted value of the security situation is P_i, $i = 1, 2, ..., h$. The weight coefficient μ_i, $i = 1, 2, ..., h$ has been obtained. The basic probability assignment mapping m is obtained, therefore the allocation value of the corresponding basic reliability is:

$$m(P_i) = \mu_i. \tag{9}$$

Assume the basic belief value of the network security situation value in the 5 days before the date of the prediction as $m_j(P_i)$, $i = 1, 2, ..., h$, $j = 1, 2, 3, 4, 5$. The corresponding belief function is $BEL_j (j = 1, 2, 3, 4, 5)$. The belief functions of the first 2 days are fused, and the basic belief value of the fusion result is m. The belief function after synthesis is denoted as $BEL = BEL_1 \oplus BEL_2$, and the synthesis process is:

$$m(P_i) = \frac{m_1(P_i)m_2(P_i)}{1 - \sum_{i \neq j, i, j = 1, 2, \cdots, h} m_1(P_i)m_2(P_j)}. \tag{10}$$

The belief functions of the days 3, 4, and 5 are then fused, and the fusion result is denoted as $BEL_1 \oplus BEL_2 \oplus \cdots \oplus BEL_5$. The basic belief value of the result is denoted as $m_c(P_i)$, $i = 1, 2, ..., h$, which is regarded as the fusion weight of the network security situation prediction model of the test day.

4 | DATA SIMULATION EXPERIMENT OF DS EVIDENCE THEORY

In order to verify the accuracy and universality of DS evidence theory in network security situation prediction, an experimental case was constructed, wherein real data were substituted for calculation, and the original DS evidence theory method was compared with the DS evidence theory method obtained after modifying the technique of data source acquisition.

4.1 | Experimental methods and procedures

Windows 7 system and 100 M LAN were used.

1. Two more advanced detection systems, Snort 3.0 and NIP 5000D, were used for the layout in the intranet Samba

server, web server, and FTP server. The data sources of the experiment included intrusion detection system (IDS) alarm/attack information, router NetFlow traffic information, and Nessus vulnerability information. The data units detected were the number of system alarms, network inflow, and the total number of system vulnerabilities per unit time. The results of the two detection systems were combined and analyzed to provide evidence for future predictions.

TABLE 1 Detection results of Snort 3.0

Number of days	Alarm times	Network inflow	Number of vulnerabilities
1	240	3000	10
2	270	3200	13
3	300	3800	15
4	340	4000	16
5	280	3000	10
6	220	2600	8
7	180	2400	5
8	160	2500	6
9	200	2900	9
10	220	3000	10

TABLE 2 Detection results of NIP 5000D

Number of days	Alarm times	Network inflow	Number of vulnerabilities
1	250	3000	10
2	260	3200	13
3	300	3600	15
4	320	3800	17
5	270	3100	11
6	230	2700	8
7	200	2500	4
8	210	2600	6
9	220	2900	8
10	210	2800	9

The data sources examined were from 15 July 2018 to 25 July 2018, totaling 10 days, and were designated as 1–10.

The results of detection by Snort 3.0 are shown in Table 1. The results of detection by NIP 5000D are shown in Table 2.

2. The detection results of the two detectors were fused using relevant network security situation awareness technology, and the information was extracted and refined to obtain the data stream to be analyzed and calculated. The data flow was understood and the information of possible threats was obtained. The basic probability assignment value based on that information was given.
3. Data were processed by using the original DS evidence theory method and the DS evidence theory method obtained after modifying the data source acquisition method. The predicted results were obtained according to different combinations of the evidence and compared with the real results.
4. The basic probability assignment value was adjusted, and the change of the predicted results of the two methods was observed to analyze the results and draw conclusions.

4.2 | Experimental results and analysis

According to the results of perceptual analysis, there were three types of threats, which were identified as threat α, β, and γ here. The corresponding basic probability assignment values were given:

$$\begin{cases} m_1{:}m_1(\alpha)=0.6, m_1(\beta)=0.2, m_1(\gamma)=0.2 \\ m_2{:}m_2(\alpha)=0.4, m_2(\beta)=0.4, m_2(\gamma)=0.2 \\ m_3{:}m_3(\alpha)=0.7, m_3(\beta)=0.28, m_3(\gamma)=0.02 \\ m_4{:}m_4(\alpha)=0.6, m_4(\beta)=0.28, m_4(\gamma)=0.12 \\ m_5{:}m_5(\alpha)=0.6, m_5(\beta)=0.24, m_5(\gamma)=0.16 \\ m_6{:}m_6(\alpha)=0.6, m_6(\beta)=0.31, m_6(\gamma)=0.09 \end{cases}. \quad (11)$$

TABLE 3 Predicted result Table 1

Evidence combination	Prediction method	$m(\alpha)$	$m(\beta)$	$m(\gamma)$	Prediction results
$m_1 \oplus m_2 \oplus m_3 \oplus m_4$	Original method	0.83673	0.14621	0.01706	α
	Improved method	0.83673	0.14621	0.01706	α
$m_1 \oplus m_2 \oplus m_3 \oplus m_4 \oplus m_5$	Original method	0.91524	0.08323	0.00153	α
	Improved method	0.91524	0.08323	0.00153	α
$m_1 \oplus m_2 \oplus m_3 \oplus m_4 \oplus m_5 \oplus m_6$	Original method	0.98957	0.01031	0.00012	α
	Improved method	0.98957	0.01031	0.00012	α

TABLE 4 Predicted result Table 2

Evidence combination	Prediction method	$m(\alpha)$	$m(\beta)$	$m(\gamma)$	Predicted results
$m_1 \oplus m_2 \oplus m_3 \oplus m_4$	Original method	0.1205	0.8351	0.0444	β
	Improved method	0.8227	0.1682	0.0091	α
$m_1 \oplus m_2 \oplus m_3 \oplus m_4 \oplus m_5$	Original method	0.2525	0.7329	0.0146	β
	Improved method	0.9164	0.0812	0.0024	α
$m_1 \oplus m_2 \oplus m_3 \oplus m_4 \oplus m_5 \oplus m_6$	Original method	0.3960	0.6022	0.0018	β
	Improved method	0.9601	0.0397	0.0002	α

The predicted results obtained by the original DS evidence theory method and the modified DS evidence theory method were compared, presented in Table 3.

The actual results were known, that is, the source of threat was α. The basic probability assignment value given by the analysis showed that $m_i(\alpha)$ had obvious representation, and there was no large conflict between the data results. Analysis of the prediction results in Table 1 showed that both methods could correctly predict the source of the threat when the evidence given was less conflicting or there was no conflict. As the number of evidence increased, $m(\alpha)$ gradually increased, and $m(\gamma)$ gradually decreased, indicating that both methods had convergence and could aggregate the predicted results around the actual results when there was sufficient evidence.

However, in the actual operation of network security situation awareness, there are always various problems caused by the instability of the network security environment, such as interference and conflict items. In order to study this situation and make m_4 reflect the unstable interference effect of external factors, m_4 was corrected as m_4:$m_4(\alpha)=0.01$, $m_4(\beta)=0.39$, $m_4(\gamma)=0.6$. Then the original DS evidence theory method and the modified DS evidence theory method predicted the situation again. The results are presented in Table 4.

Although α was still the actual result, the representation data conflicted with other data due to the interference. The analysis results showed that when there was a large conflict, the original DS evidence theory method had obvious deviation, which leads to incorrect predicted results. However, the DS evidence theory method obtained after modifying the data source acquisition method, tended to aggregate to the actual results more obviously, had little fluctuation, and it could correctly predict the results under the support of a large number of data, suggesting a strong anti-interference performance.

The results of the two experiments suggested that the DS evidence theory obtained after modifying the data source acquisition method was feasible and effective in the prediction of network security situation, and could ensure accuracy and good convergence when compared to the original DS evidence theory method in the case of no large conflict. These results provide powerful support for decisionmakers in the rapidly changing network environment.

5 | CONCLUSION

In the current environment where the requirement of network security situation awareness is becoming stricter and demand is increasing, this study was performed to analyze the method of network security situation prediction, that is DS evidence theory. It explained the basic principle of DS evidence theory, emphasized the problems existing in DS evidence theory, presented the improved method, and performed the experiment to prove the effectiveness of the improved method. This study provides a direction for the future development of network security situation prediction.

ORCID

Dan Liu https://orcid.org/0000-0002-3559-7666

REFERENCES

1. Q. Wang and H. J. Chen, *Computer network security and defense technology research*, in Proc. Eighth Int. Conf. Meas. Tech. Mech. Autom. (Macau, China), 2016, pp. 155–157.
2. J. Mi *et al.*, *Reliability analysis of complex multi-state system with common cause failure based on DS evidence theory and bayesian network*, in Recent Advances in Multi-state Systems Reliability, Springer, 2018, pp. 19–38.
3. X. W. Liu, *Network Security Situation Quantification Aware - ness and Evaluation Based on Multi-source Fuson*, Harbin Engineering University, Harbin, China, 2009.
4. C. Yi, Q. Huang, and Y. Chen, *An improve information fusion algorithm based on BP neural network and D-S evidence theory*, in Proc. Third Int. Conf. Digital Manuf. Autom. (CuiLin, China), 2012, pp. 179–181.
5. T. Leibovich and D. Ansari, *The symbol-grounding problem in numerical recognition: A review of theory, evidence, and outstanding questions*, Can. J. Exp. Psychol. **70** (2016), no. 1, 12–23.
6. W. Q. Zhang and Y. Deng, *Combining conflicting evidence using the DEMATEL method*, Soft Comput. **23** (2018), 8207–8216.

7. Y. Wang, K. Zhang, and Y. Deng, *Base belief function: an efficient method of conflict management*, J. Amb. Intel. Hum. Comp. **10** (2019), 3427–3437.
8. F. Xiao, *Multi-sensor data fusion based on the belief divergence measure of evidences and the belief entropy*, Inform. Fusion **46** (2019), 23–32.
9. F. Y. Xiao and W. P. Ding, *Divergence measure of Pythagorean fuzzy sets and its application in medical diagnosis*, Appl. Soft Comput. **79** (2019), 254–267.
10. J. Wu *et al*., *Big data analysis-based security situational awareness for smart grid*, IEEE Trans. Big Data **4** (2016), no. 3, 408–417.
11. F. Xiang and Z. Jian, *A D-S evidence weight computing method for conflict evidence*, Comput. Eng. **2016–2** (2016).

AUTHOR BIOGRAPHY

Dan Liu received her MS degree in software engineering from Chongqing University, Chongqing, Rep. of China, in June 2010. She is working at the Chongqing College of Electronic Engineering as a lecturer and is interested in computer science and technology, software engineering and computer networks.