A Method of Network Security Risk Measurement Based on Improved D-S Evidence Theory

Xiaolin Zhao*, Mingzhe Pei, Meijing Wu, Yaoyuan Liang and Hui Peng

School of Computer Science & Technology, Beijing Institute of Technology, 100081, China

*Corresponding author email: zhaoxl@bit.edu.cn

Abstract. This paper applies Dempster-Shafer (D-S) evidence theory to network security measurement and assessment, which improved the accuracy of network security measurement results. The main contents include improving the composition rules to solve the paradox, establishing a security measurement model, and proving the rationality of the improved method by three Distributed Denial of Service (DDoS) attacks experiment. The results show that this method is more accurate in detecting traffic attacks.

Keywords: D-S evidence theory; Synthesis rules; Evidence source; Security measurement model.

1. Introduction

With the development of Internet technology, network security is facing new challenges. Network security risk measurement and assessment is an emerging technology, which can provide help to network security problems [1].

Among the evaluation methods, there are more studies on attack graph technology and Analytic Hierarchy Process (AHP). As an effective tool for complex decision-making problems, AHP can help decision makers to prioritize and make the best choice.

This paper applies D-S evidence theory to network security measurement and assessment. First, this paper introduced two conflicts and solutions of D-S evidence synthesis; Then, basing on D-S evidence theory and the hierarchical security evaluation model [2], specific indicators data that can represent the real network environment was selected to establish a security measurement model. Finally, a network simulation environment was set up, DDoS attack experiments were conducted, and the corresponding indicators data was taken to calculate and verify the improved D-S evidence theory and corresponding security measurement models.

2. Related Research

Commonly used index-based network security assessment methods include AHP, Grey System Theory, Fuzzy Evaluation, D-S evidence theory, etc.

Based on AHP, Wengang Wu et al. proposed a security risk assessment model combined with fuzzy comprehensive evaluation [3]. Wang H et al. constructed three evaluation indexes and solved large index and low efficiency problems of evaluation [4].

Based on Grey System Theory and fuzzy theory, some researchers proposed a combination-based model for network risk prediction [5]. Zouzhen Wan et al. proposed a security assessment model based on fuzzy theory to quantify the security assessment of industrial control network systems [6].
Combined with entropy weight method and fuzzy comprehensive, Zeng Z et al. established an AHP evaluation model [7]. Based on the D-S evidence theory, [8] proposed an improved D-S evidence theory based on grey relational analysis and verified its effectiveness through experiments. The literatures [9] and [10] combined D-S evidence theory with rough sets and Compressed Sensing Error Back-Propagation (CS-BP) neural network, respectively, to conduct network situation assessment, and effectively reduced the intervention of human factors and improved the accuracy of the assessment. Combined with effective discount evidence sources and D-S theory, Lan L et al. proposed a conflict evidence synthesis method [11]. Wenjun Ma et al. made patching improvements to the D-S theory for Dempster composition rules [12].

The research methods and results used in the references are shown in Table 1:

| Researchers       | Method and Theory                  | Achievements                                                                 |
|-------------------|------------------------------------|------------------------------------------------------------------------------|
| Wengang Wu, etc.  | Fuzzy comprehensive and AHP        | Security risk assessment model                                               |
| Wang H, etc.      | AHP and D-S evidence theory        | Security situation assessment model and quantification method                |
| YuQ, etc.         | Grey System Theory                | Security risk prediction model                                               |
| Zouzhen Wan, etc. | Fuzzy theory                      | Security assessment model                                                    |
| Zeng Z, etc.      | AHP, entropy weight, fuzzy theory | Security evaluation model                                                    |
| Baozhen Du, etc.  | Gray Relational Analysis          | Improved D-S Evidence Theory                                                |
| YuX, etc.         | D-S evidence theory, rough set     | Network situation assessment                                                 |
| J. Qiang, etc.    | D-S evidence theory, CS-BP network| Network situation assessment                                                 |
| Lan L, etc.       | D-S evidence theory                | Conflict evidence synthesis method                                           |
| Wenjun Ma, etc.   | D-S evidence theory                | Improved composition rules                                                  |

Although AHP can simplify the abstract problems, the lack of certain objectivity, resulting in a certain degree of subjectivity in the measurement results. When researchers apply D-S evidence theory to the study of network situation assessment, they often choose information about vulnerability and threat as evidence, and do not select specific indicators data, which is not representative.

3. D-S Evidence Theory Paradox Resolution

3.1. D-S Synthesis Rules

D-S evidence theory was a mathematical reasoning theory [13]. The core idea of D-S evidence theory is to make an evaluation decision on the uncertainty of network security by combining multiple types of evidence.

Here are the synthetic rules for D-S evidence theory:

For $\forall A \subseteq \Theta$, the finite mass function on the recognition frame $\Theta$, the Dempster synthesis rule for $m_1, m_2, ..., m_n$ is:

$$m_1 \oplus m_2 \oplus \cdots \oplus m_n(A) = \frac{1}{K} \sum_{A_1 \cap A_2 \cap \cdots \cap A_n = A} m_1(A_1) \cdot m_2(A_2) \cdots m_n(A_n)$$

(1)

K in above:

$$K = \sum_{A_1 \cap A_2 \cap \cdots \cap A_n \neq \emptyset} m_1(A_1) \cdot m_2(A_2) \cdots m_n(A_n) = 1 - \sum_{A_1 \cap A_2 \cap \cdots A_n = \emptyset} m_1(A_1) \cdot m_2(A_2) \cdots m_n(A_n)$$

In the above formula, K stands for normalization factor and 1-K represents the coefficient of conflict, which reflects the degree of conflict of evidence.
3.2. Paradox of Synthesis Rule

In D-S evidence theory, synthesizing highly conflicting evidence may invalidate its synthesis rules or produce results contrary to common sense. According to the research of domestic and foreign experts and scholars, paradox problems can be generally classified into the following three types:

(1) The complete conflict paradox, as shown in Table 2. Among them, the evidence \( E_1 \) and \( E_2 \) are completely conflicting. Then the synthetic rule [13] in D-S evidence theory is invalid.

| Evidence | \( A_1 \) | \( A_2 \) |
|----------|----------|----------|
| \( E_1 \) | 1        | 0        |
| \( E_2 \) | 0        | 1        |

Dempster-Shafer Composition rule is invalid

(2) 0-trust paradox, as shown in Table 3. Since the basic probability assignment value of evidence \( E_3 \) to proposition \( A_1 \) is 0, no matter how large \( A_1 \) is, the final composite result is always 0. Among them, the conflict coefficient \( 1 - K \) is 0.98, so the final synthesized result is contrary to the facts.

| Evidence | \( A_1 \) | \( A_2 \) |
|----------|----------|----------|
| \( E_1 \) | 0.9      | 0.1      |
| \( E_2 \) | 0.8      | 0.2      |
| \( E_3 \) | 0        | 1        |

Dempster-Shafer Composition rule is invalid

(3) 1-Trust paradox, as shown in Table 4. Although the evidence \( E_1 \) and \( E_2 \) have a low basic probability distribution for proposition \( A_2 \), but in the final synthesis result, proposition \( A_3 \) is true, and the conflict coefficient \( 1 - K \) is 0.99. Therefore, the result of the final synthesis is contrary to the facts.

| Evidence | \( A_1 \) | \( A_2 \) | \( A_3 \) |
|----------|----------|----------|----------|
| \( E_1 \) | 0.9      | 0.1      | 0        |
| \( E_2 \) | 0        | 0.1      | 0.9      |
| Dempster-Shafer | 0          | 1        | 0        |

3.3. Paradox Solution

Aiming at the paradox or conflict problem of D-S evidence theory, researchers mainly used two methods to solve the conflict problem: Improve the synthesis rule, improve the source of evidence. [14] and [15] respectively proposed an improved method for synthesis rules and evidence sources. The two methods are described in detail below.

(1) Improvements to synthesis rules:

\[
m(\emptyset) = 0 \\
m(A) = P(A) + k \cdot \varepsilon \cdot q(A), \quad A \neq \emptyset
\]  

(2) Improvement of evidence source:

First modify the basic probability distribution value according to the formula:

\[
m_i(A_j) = \begin{cases} 
10^{m(A_j) - 1/n} m_i(A_j) & \text{if} \quad \frac{1}{n} < m_i(A_j) < \frac{1}{n} \\
10^{m(A_j) + 1/n} m_i(A_j) & \text{if} \quad m_i(A_j) \geq \frac{1}{n}
\end{cases}
\]
Among them, \( n \) is the number of propositions in the recognition frame, and \( 1/n \) is the average basic probability value, which is used as the minimum criterion for judging whether the evidence recognition result is credible.

On this basis, the obtained basic probability value is normalized according to the following formula:

\[
m_i(A_j) = \frac{m_i(A_j)}{\sum_j m_i(A_j)}
\]  

(4)

It can be deduced through computational verification, both improved methods can effectively solve the three paradox problems, as shown in Tables 5, 6, and 7. Multiple fusion results show that using the improved method for data fusion can not only make the synthesis result more accurate, but also have a higher degree of credibility.

### Table 5. Complete conflict paradox

| Evidence | \( A_1 \) | \( A_2 \) |
|----------|-----------|-----------|
| \( E_1 \) | 1         | 0         |
| \( E_2 \) | 0         | 1         |
| Dempster-Shafer | Composition rule is invalid |
| Synthesis rules | 0.5 | 0.5 |
| Evidence source | 0.5 | 0.5 |

### Table 6. 0-trust paradox

| Evidence | \( A_1 \) | \( A_2 \) |
|----------|-----------|-----------|
| \( E_1 \) | 0.9       | 0.1       |
| \( E_2 \) | 0.8       | 0.2       |
| \( E_3 \) | 0         | 1         |
| Dempster-Shafer | 0 | 1 |
| Synthesis rules | 0.555 | 0.445 |
| Evidence source | 0.962 | 0.038 |

### Table 7. 1-Trust Paradox

| Evidence | \( A_1 \) | \( A_2 \) | \( A_3 \) |
|----------|-----------|-----------|-----------|
| \( E_1 \) | 0.9       | 0.1       | 0         |
| \( E_2 \) | 0         | 0.1       | 0.9       |
| Dempster-Shafer | 0 | 1 | 0 |
| Synthesis rules | 0.297 | 0.406 | 0.297 |
| Evidence source | 0.488 | 0.024 | 0.488 |

### 4. Network Security Measurement Model Based on D-S Evidence Theory

#### 4.1. Model Design

In this chapter, we combined D-S evidence theory with the hierarchical security assessment model introduced in [2] to establish a security measurement model as shown in Figure 1, including the indicators layer, D-S evidence theory fusion evidence, host layer and network system layer.

The metric calculation flowchart of this model is shown in Figure 2:
The layers and steps in this model are described in detail below:

4.2. Indicator Layer
The indicator layer is the indicators data that can reflect the occurrence of the attack when the host in the network system is under attack. You can choose different indicator data according to different attacks. For example, when a DDoS attack occurs, the indicators that can be collected include Central Processing Unit (CPU) utilization, disk utilization, Transmission Control Protocol (TCP) segments, Internet Protocol (IP) datagrams, User Datagram Protocol (UDP) datagrams, and the number of transmitted data packets. The indicator set of the second host is:

\[ \text{Index}_i = \{\text{index}_{i1}, \text{index}_{i2}, \ldots, \text{index}_{im}\} \]

4.3. D-S Evidence Theory Fusion Evidence
The indicator data collected at the indicator layer is fused to obtain the measurement result value of the host layer. The specific fusion process is as follows:

In this article, define the probability distribution function of each indicator for the first host, as follows:

\[ m_{ij}(\{\text{safe}\}, \{\text{unsafe}\}) = (1 - \text{Index}_{ij}, \text{Index}_{ij}) \]

Where \( \text{Index}_{ij} \) is the index\( _{ij} \) in the host \( i \).
Then, according to formula (2), the synthesis rule of host \( i \) can be obtained, that is, the measurement value of host \( i \), as follows:

\[
M_i = m(\text{unsafe}) = \prod_{j=1}^{n} \text{index}_{ij} + k \cdot q
\]  

(6)

\( k, q \) in above, \( k = 1 - \prod_{i} \text{index}_{ij} - \prod_{i} (1 - \text{index}_{ij}) \), \( q = \frac{1}{n} \sum_{i=1}^{n} \text{index}_{ij} \)

The above formulas (5) and (6) are the improvements to the synthesis rules in Chapter 3. The following are the improvements to the source of evidence:

First improve the evidence according to (3):

\[
m_{ij}(\{\text{unsafe}\}) = \begin{cases} 
10^{\text{index}_{ij} - 1/m} & \text{if } \text{index}_{ij} < \frac{1}{m} \\
10^{\text{index}_{ij} + 1/m} & \text{if } \text{index}_{ij} \geq \frac{1}{m}
\end{cases}
\]  

(7)

Then normalize it according to (4):

\[
m_{ij}(\{\text{unsafe}\}) = \frac{\text{index}_{ij}}{\sum_{j} \text{index}_{ij}}
\]  

(8)

Finally, calculate the metric of host \( i \) according to (1):

\[
MV_i = m(\text{unsafe}) = \frac{1}{1-k} \prod_{i} \text{index}_{ij}
\]  

(9)

Among them, \( 1 - k = \prod_{i} \text{index}_{ij} + \prod_{i} (1 - \text{index}_{ij}) \). \( 1 - K \) is the normalization factor, and \( n \) is the number of propositions. The propositions in this section are network security and insecurity, so the value of \( n \) is 2.

**4.4. Host Layer**

This layer includes multiple hosts in a network system. Through the data fusion process of D-S evidence theory, the measurement results of each host in the network system can be obtained, laying a foundation for measuring the entire network system.

**4.5. Network System Layer**

The network system layer measures and assess the entire network system. The measurement value of the network system is a weighted calculation of the host measurement value and the host weight. The importance of the host depends on the type of service, the importance of the data, etc. This is still a dynamic, multi-variable, and relatively subjective issue. The measurement results of the network system are as follows:

\[
NV = \sum_{i=1}^{n} w_i \cdot MV_i
\]  

(10)

Where \( w_i \) is the weight of the host \( i \). Host weight is related to the type of service provided on the host. The importance of the service can be divided into three levels: high, medium, and low. The importance calculation formula of the host is as follows:

\[
HI_i = K_h N_h + K_m N_m + K_l N_l
\]  

(11)

Among them, \( K_h, K_m \) and \( K_l \) are quantitative scores of three important levels: high, medium, and low. \( N_h, N_m \) and \( N_l \) are three levels of service data on a certain host. The weight of host \( i \) is:

\[
w_i = \frac{HI_i}{\sum_{i=1}^{n} HI_i}
\]  

(12)

**5. Experiment Verification and Analysis**

**5.1. Experiment Scheme Design**

In order to experimentally verify the feasibility of the proposed measurement and evaluation model in practical networks, this article designed and simulated a DDoS attack experiment. During the
simulated attack, multiple significantly changed indicators can be collected, which can be used for dynamic network security measurement and assessment. The network topology diagram constructed in this experiment is shown in Figure 3. This attack experiment is to attack from the outside of the network system, and use the corresponding tools to collect and record the indicator data in preparation for the subsequent calculation of network security metrics.

There are four attack hosts in this experiment, which launched the attack outside the network system. Host7 in the lower right sub-net in Figure3 is the target host, which has SSH service, Redis service, and Web service installed on it, and is attacked by four hosts outside the system.

![DDos attack network topology](image)

**Figure 3.** DDos attack network topology

### 5.2 Experiment Process

There were three attacks in this experiment, which totaled 3 hours and 18 minutes. The indicator collection time was 176 minutes, and a total of 176 sets of data were collected. Spotlight and Wireshark tools were used to collect indicators in the network at an interval of 1 minute. Collected indicators include CPU utilization, disk utilization, TCP segments, IP datagrams, UDP datagram, and transmission packet transmission volume. The above indicators are selected for measurement.

### 5.3 Experiment Data

Seven indicators are selected, as shown in Table 8.

| Indicator | Index explanation |
|-----------|-------------------|
| CPU Utilization | CPU utilization. The collected data is the utilization rate of eight cores. The average value needs to be calculated. |
| Disk Load | Disk utilization. Except for drive C, the utilization of other drives has not changed significantly. Therefore, the occupancy rate of drive C is used for calculation. |
| IP Datagram Post | IP datagram post volume |
| IP Datagram Recv | IP Datagram Received |
| UDP Datagram Post | UDP datagram post volume |
| UDP Datagram Recv | UDP Datagram Received |
| Packets | Transmission of data packets, including post, receive, and total number of packets |

**Table 8.** Indicators used for calculations
Normalize the indicator data collected above. The normalization processing formula is shown in (13):

\[ X^* = \frac{x - \text{min}}{\text{max} - \text{min}} \]  

(13)

After the normalization process is completed, the processed data is substituted into the security measurement model for calculation, and the experiment results are shown below. The measurement results of the security measurement model proposed in this paper are compared with the measurement models using the traditional AHP method. The results are shown in Figures 4 and 5, which are the methods of improving the composition rule and the evidence source, respectively.

Figure 4. Comparison of security measurement model with traditional AHP (improved synthesis rules)

Figure 5. Comparison of security measurement model with traditional AHP (improved evidence source)

5.4. Experiment Results and Analysis

It can be seen from Figure 4 that the measurement result using the improved synthesis rule method has a measurement value of 0 most of the time and a small number of results of 1, which is inaccurate and unreasonable. The result of improved source of evidence shows that attacks occurred in three time periods, which are consistent with the actual attack situation. Therefore, the use of improved methods of evidence sources is more accurate and advantageous. According to the experimental results, the hierarchical security measurement model proposed in this paper, after applying D-S theoretical
evidence for data fusion, is also more reasonable and feasible than traditional AHP models, and more sensitive to data traffic (especially IP datagrams). This model has good availability for security measurement of traffic-type attacks in the network.

6. Conclusion
This article first briefly introduces the network security assessment method based on D-S evidence theory, and describes three paradoxical problems and two different improvement methods to solve them. Then, a new model of the measurement method is established, and calculation formulas for the measurement values of each host and the entire network system are given. Finally, a DDoS attack experiment was designed and simulated. The indicators data was collected and two improved D-S evidence theory methods were calculated to verify its rationality and feasibility of the security measurement model. Experimental results show that this method is suitable for the measurement of traffic-type attacks. Compared with the traditional method, this method selects specific indicators data that can represent the real network environment when measuring. It can measure traffic attacks more accurately. At the same time, human intervention factors are also reduced in the calculation process, which makes the results more objective.

Acknowledgement
This work was supported by National Key P&D Program of China (Grant No.2 2016YFB0800700).

References
[1] L. Hu, H. Li, Z. Wei, S. Dong and Z. Zhang, Summary of Research on IT Network and Industrial Control Network Security Assessment, in: 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), 2019 (2019).
[2] X. Z. Chen, Q. H. Zheng, X. H. Guan, Quantitative Hierarchical Threat Evaluation Model for Network Security, Journal of Software. 17 (2006) 885-897.
[3] W. G. Wu, Z. W. Zhang, Q. S. Wang, A Information Security Risk Assessment Model Based on AHP and Fuzzy Comprehensive Evaluation, Journal of Chongqing University of Technology. 31 (2017) 156-161.
[4] H. Wang, Z. F. Chen, X. Feng, Research on Network Security Situation Assessment and Quantification Method Based on Analytic Hierarchy Process, Wireless Personal Communications. 102 (2018) 1401-1420.
[5] Q. Yu, Y. J. Shen, Research of information security risk prediction based on grey theory and ANP, in: Advanced Information Management, Communicates, Electronic & Automation Control Conference, 2017 (2017).
[6] Z. W. Zou, X. Wang, F. Li, J. Y. Zhang, Q. Song, A safety assessment model of industrial control system based on fuzzing synthesis theory, in: 2017 IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), 2017 (2017).
[7] Z. Zeng, Q. Gong, Fuzzy Comprehensive Evaluation of Security Maintenance Ability Base on AHP-Entropy, in: 2019 3rd International Conference on Circuits, System and Simulation (ICCSS), 2019 (2019).
[8] B. Z. Du, H. J. Xu, H. L. Xiong, Z. F. Du, Q. H. Xing, An Improved D-S Evidence Theory Based on Gray Relational Analysis, in: 2019 IEEE 4th International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), 2019 (2019).
[9] X. Y. Yu, T. J. Chen, Y. B. Bai, Y. Ling, Situation Assessment Method Based on Rough-Vague Sets and D-S Evidence Theory, in: IEEE International Conference on Software Engineering & Service Science, 2013 (2013).
[10] J. Qiang, F. Wang, X. L. Dang, Network Security Based on D-S Evidence Theory Optimizing CS-BP Neural Network Situation Assessment, in: IEEE International Conference on Cyber Security & Cloud Computing & IEEE International Conference on Edge Computing & Scalable Cloud. 2018 (2018).
[11] L. Luo, J. Y. Xiao, Conflict Evidence Synthesis Method of Effective Discount Evidence Sources, Computer Engineering and Applications. 55 (2019) 154-158.
[12] W. J. Ma, Y. C. Jiang, X. D. Luo, A flexible rule for evidential combination in Dempster-Shafer theory of evidence, Applied Soft Computing. 85 (2019) 105512.

[13] W. Zhang, X. L. Ji, Y. Yang, J. W. Chen, X. S. Qiu, Data Fusion Method Based on Improved D-S Evidence Theory, in: 2018 IEEE International Conference on Big Data and Smart Computing (BigComp). 2018 (2018).

[14] G. N. Yang, X. F. Feng, A New Conflict Evidence Fusion Method in D-S Evidence Theory, Computer Applications & Software. 31 (2014) 82-85.

[15] Y. Wang, Y. A. Liu, Q. Zhang, Conflict Solution in D-S Evidence Theory, Journal of Jiangnan University. 14 (2015) 269-272.