A Resource Consumption Attack Identification Method Based on Data Fusion

Libin Jiao[1], Yonghua Huo[1], Ningling Ge[2], Zhongdi Ge[3], and Yang Yang[3(✉)]

[1] Science and Technology on Communication Networks Laboratory, The 54th Research Institute of CETC, Shijiazhuang, Hebei, People's Republic of China
[2] R & D Department, Agricultural Bank of China, Shanghai, People's Republic of China
[3] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, People's Republic of China
yyang@bupt.edu.cn

Abstract. Data fusion can make use of information from different sources or different representations to describe the target more accurately, which has important research significance. Aiming at the network-running node may be attacked or there is measurement error, this paper comprehensively utilizes the information of each node, and proposes a resource consumption attack identification method based on node multi-dimensional data fusion. First, construct a correlation matrix between nodes, identify normal nodes and possible abnormal nodes, and assign different weights to each node. Then, calculating the support of the node's system attributes for the attack type, and adopting the D-S evidence theory to effectively identify the network attack. The simulations demonstrate the effectiveness and certain advantages of the proposed algorithm.

Keywords: Resource consumption attack · Correlation analysis · Data fusion · D-S evidence theory

1 Introduction

The ultimate threat of various attacks or normal behavior peaks is the availability of the network-operating environment, and the availability of the network depends mainly on the occupancy of various network resources, such as network bandwidth, throughput, storage and computing resources. Network resource consumption attacks generally refer to hackers using reasonable service requests to preempt excessive system resources, so that other normal users cannot obtain sufficient resources, causing the system to stop responding to service requests. In the case of a terminal server, since resources such as bandwidth, computing power, and storage have certain limitations, when a hacker generates an excessive number of network server requests, a large amount of resources of the terminal server are abused by the terminal, and normal users cannot use the service. Resource-consumption attacks are always accompanied by anomalies in the system attributes of each node, while nodes do not exist independently in the network environment, and the attribute changes of each node have potential relevance.

M. Cheng et al. (Eds.): SmartGIFT 2020, LNICST 373, pp. 128–139, 2021.
https://doi.org/10.1007/978-3-030-73562-3_11

Data fusion is a multi-level and multi-faceted processing process, which involves detecting, correlating, combining and estimating data to improve the estimation accuracy of states and characteristics, and then obtain a more accurate description of the perceived objects. The current data fusion methods can be roughly divided into two categories: probabilistic statistics methods and artificial intelligence methods. Among them, the probabilistic method mainly has the following types: the first is the weighted average method using the simplest and most intuitive mathematical operation fusion; the second is the Kalman filter method used for real-time fusion of dynamic low-level redundant data; the third is the multi-Bayesian estimation which minimizes the likelihood function of the associated probability distribution function; the fourth is the D-S evidence theory applicable to the inference of uncertain problems. The artificial intelligence mainly includes: fuzzy logic theory based on multi-valued logic reasoning, combined calculation based on fuzzy set theory; neural network method using data processing capability and automatic reasoning ability of neural network to realize data fusion and so on. Each of these methods has its application, and D-S evidence theory can express the correct, incorrect and uncertain probabilities at the same time, and has certain advantages in dealing with the uncertainty of data.

Therefore, this paper proposes a resource consumption attack identification method based on node multi-dimensional data fusion. The research contents and innovations of this paper are as follows:

(1) According to the correlation analysis, construct a correlation matrix between nodes to distinguish between normal nodes and nodes that may be attacked. Then, using the system attribute information of the node, the node data is transformed into the evidence in the D-S evidence theory.
(2) Using the D-S evidence theory, the individual evidence is distributed according to the basic probability of the node, and the network resource consumption attack is effectively identified.

2 Related Work

Network attacks can be divided into two categories: 1) Using information system security vulnerabilities to bypass information system security protection measures and enter information systems to achieve the purpose of controlling information systems. Such attacks are generally called control attacks. 2) Although such a network attack cannot control the information system, the information system's service capability is degraded or the service capability is completely lost due to the large consumption of information system resources, such as memory resources, computing resources, bandwidth resources, and the like. Such attacks are generally called resource consumption attacks. The resource consumption attack is mainly to exhaust a certain network resource. In the attack process, the terminal server attacks the terminal server, and the terminal server's CPU, memory, communication link and other resources are overloaded. The traditional means of network resource consumption attack countermeasures are intrusion detection and intrusion response. For example, the detection method based on anomaly detection can be used for detecting network resource consumption type attacks.

Palmieri F et al. [1] proposed a two-stage anomaly detection strategy, using independent component analysis modeling as a blind source separation problem, and constructing a baseline traffic distribution, thereby transforming network attack detection into anomalous/normal classification problem. Aborujilah A et al. [2] focused on the impact of DoS attacks on CPU power performance and network bandwidth. In order to evaluate CPU and bandwidth power performance, real flood attacks were implemented in different scenarios. Harshaw C R et al. [3] proposed a graph parsing method for detecting network stream data anomalies, which represents a time slice of traffic as a graph, and identifies an abnormal interval by performing anomaly detection on the graph primitive count sequence.

Palmieri F et al. [4] proposed a network-based anomaly detection method based on the analysis of non-fixed attributes and the "hidden" recurrence pattern that occurs in aggregated IP traffic flows. Recursive quantitative analysis was used to explore the hidden dynamics and temporal correlation of statistical time series. A Chaudhary et al. [7] used the ability to deeply learn the topological features of social networks to detect anomalies in email networks and Twitter networks, and proposed a model neural network model and applied it to social contact graphs. Considering the combination of various social network statistical measures, the structure and function of the abnormal nodes are studied by using deep neural networks on them, which found that the hidden layer of the neural network plays an important role in discovering the impact of statistical metric combinations in anomaly detection.

X. Chun-Hui et al. [8] proposed an adaptive method based on the iForest algorithm. Some feature extractors are constructed by statistical methods to highlight different anomalous behaviors in different indicators, and then the extracted feature data is used for iForest construction and prediction. Combined with a specific feature extractor, you can eliminate periodic effects or specify peaks or valleys to accommodate different metrics. Rapid detection of large data sets with the iForest algorithm with linear time complexity and low memory requirements. R. Liu et al. [9] proposed a network anomaly detection method (NAD-NNG) based on the idea of natural neighborhood graph. In order to eliminate noise points or mark erroneous points and reduce the time complexity of anomaly detection, the algorithm clusters the normal data set using a natural neighborhood map, and adaptively obtains a percentage value β for setting an abnormal threshold.

Q. Su et al. [10] proposed a genetic algorithm based on Management Information Base (MIB) to detect network anomalies. The algorithm is based on the classification theory using integrated IF-THEN rules, proposes a new chromosome-coding scheme, and discusses a new charging function design method. Ç. Ateş et al. [11] proposed a new method for network anomaly detection based on the probability distribution of header information. The Greedy algorithm is used to calculate the distance between the header distributions to reflect the main features of the network, eliminating some of the requirements associated with Kullback-Leibler divergence. The support vector machine classifier is then used during the detection phase to reduce the false alarm rate and adapt the system to different networks.

The traditional attack detection technology focuses on system intrusion detection, anti-virus software or firewall of the user network. The biggest problem is that when the attack data stream reaches a peak, a large amount of data is collected on the victim side,

and there is no effective way to filter the data. Thus, the user network can only be in a state of passive defense. In order to effectively prevent attacks on the victim side, it is necessary to find the attack behavior at an early stage. However, it is difficult to distinguish normal users and attack data in the early stage of the attack, which brings difficulties for resource consumption attack identification. In addition, once the attack occurs, whether the malicious data seriously affects the victim, the data has been transmitted in the network, causing actual waste of network resources. Because resource consumption attack types are complex and versatile, it is unrealistic to detect whether a single packet is a malicious attack. Therefore, we analyze the trend of node resources in the network and the correlation between them to achieve early detection and identification of resource consumption attacks.

3 Data Fusion Algorithm

3.1 Algorithm Flow

This paper proposes a resource consumption attack identification method based on node multi-dimensional data fusion. According to the resource consumption type attacks that may exist in the network, the correlation matrix between the nodes is constructed according to the correlation analysis, and the normal nodes and the nodes that may be attacked are distinguished. Then, the system attribute information of the integrated node is used to convert the node data into evidence in the D-S evidence theory. Finally, using the D-S evidence theory, each evidence is distributed according to the basic probability of the node, so as to effectively identify the resource-consuming attack. The specific steps of the algorithm are as follows, as shown in Fig. 1.

Input: system attribute data of the node.
Output: resource consumption attack identification result.
Step 1: construct a correlation matrix of nodes by using the maximum information coefficient, and identify possible abnormal nodes;
Step 2: Integrate all node information, convert the node data into evidence in D-S evidence theory, and assign different weights to different evidences to describe the credibility of each evidence;
Step 3: According to the basic probability allocation BPA evaluates the source of evidence, so as to effectively identify the resource-consuming attack.

3.2 Basic Probability Allocation Based on Correlation Analysis

According to the possible existence of attack behavior in the network, the correlation matrix between nodes is constructed according to the correlation analysis to distinguish the normal node from the node that may be attacked. Then, the system attribute information of the node is comprehensively utilized to convert the node data into evidence. Different weights are assigned to describe the credibility of each evidence. The treatment of conflict evidence is to assign smaller weights instead of removing conflict evidence,

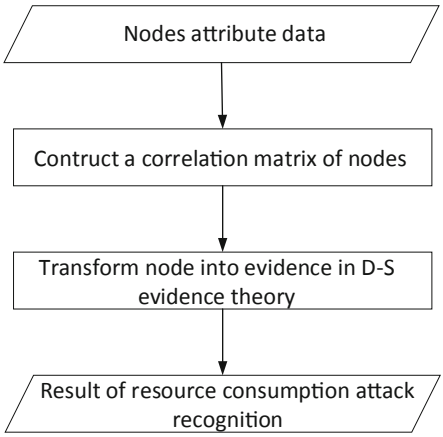

Fig. 1. Overall flowchart of the algorithm

mainly for two reasons: (1) When the amount of evidence is small, it is impossible to determine which evidence is conflict evidence, and appropriate weight can reduce the negative impact of conflict evidence on the fusion result. When the number of evidence is large, the weight of the conflict evidence will be approximately zero, and its impact on the fusion result is negligible. (2) Unless it is impossible to determine which evidence is conflict evidence or which raw data is erroneous data before knowing the correct decision, and because of the universality of noise in the data, the fusion rule must be able to adapt to the existence of conflict evidence.

Suppose the network has a certain number of nodes, each of which has a series of system attributes such as CPU utilization, latency, bandwidth, packet loss rate, and number of connections. First, the correlation between nodes is calculated using the maximum information coefficient, thereby constructing a node correlation matrix. Note that the attribute of a node s_i at a certain time is a random variable s_X, and the attribute of the other node s_j in the same time is a random variable s_Y, so that a finite data set D is formed between any two nodes, $\mathrm{D} = \{s_X, s_Y\}$. The correlation of nodes s_i and s_j can be calculated as follows:

$$Sim(s_i, s_j) = \max_{a*b<B} \{M(D)_{a,b}\} = \max_{a*b<B} \left\{ \frac{I^*(s_X, s_Y)}{\log \min\{a, b\}} \right\} \tag{1}$$

Where $1 < \mathrm{B} \leq N^{1-\varepsilon}$, $0 < \varepsilon < 1$. In general, $\varepsilon = 0.4$ can be used to obtain better results, so $\mathrm{B} = N^{0.6}$ is taken in this paper. $a * b$ represents a different division of the data set D, and $I(s_X, s_Y)$ represents mutual information of the random variables s_X and s_Y.

$$I(s_X, s_Y) \approx I_{D|G}(s_X, s_Y) = \sum_{j=1}^{b} \sum_{i=1}^{a} \rho_{(x,y)}(i,j) \log \frac{\rho_{(x,y)}(i,j)}{\rho_x(i)\rho_y(j)} \tag{2}$$

Where $\rho_x(i) \approx \frac{n_x(i)}{N}$, $\rho_y(j) \approx \frac{n_y(j)}{N}$, $\rho_{(x,y)}(i,j) \approx \frac{n_{(x,y)}(i,j)}{N}$, $n_x(i)$ is the number of samples falling into the i-th division grid of the random variable s_X, $n_y(j)$ is the number

of samples falling into the j-th division grid of the random variable s_Y, $n_{(x,y)}(i, j)$ is the number of samples that fall into the i-th division grid of the random variable s_X and the j-th division grid of the random variable s_Y at the same time.

According to the correlation matrix, the normal node set and the possible abnormal node set are distinguished, which are respectively recorded as S_0 and S_1.

$$Sim(s_i) = \frac{1}{n-1} \sum_{j=1}^{n-1} Sim\left(s_i, s_j\right) \tag{3}$$

$$\overline{Sim} = \frac{1}{n} \sum_{i=1}^{n} Sim(s_i) \tag{4}$$

Where $Sim(s_i)$ represents the overall correlation of the node s_i in the network, n represents the number of nodes in the network, and $\overline{Sim}$ represents the average correlation of all nodes in the network. Put all the nodes of $Sim(s_i) \geq \overline{Sim}$ into the set S_0 and mark them as normal nodes, put all the nodes of $Sim(s_i) < \overline{Sim}$ into the set S_1 and mark them as possible abnormal nodes.

Then, the set of node system attributes associated with each resource-consuming attack type is recorded as $V = \{V_1, V_2, \cdots, V_k\}$. The evidence generated by each node is calculated for the mass function generated by different attack types as follows:

$$m(s_i) = \sum_{j=1}^{k} \beta_{ij} \tag{5}$$

$$\beta_{ij} = \frac{\mathrm{V}_i^j - \overline{V_j}}{\mathrm{V}_{max}^j - \mathrm{V}_{min}^j} \tag{6}$$

Where β_{ij} represents the support degree of the j-th system attribute of each node to the attack type, V_{min}^j and V_{max}^j respectively represent the minimum and maximum values of the j-th system attribute of the normal node set S_0, $\overline{V_j}$ denotes the average value of the j-th system attribute of the set S_0, and V_i^j represents the j-th system attribute value in the node s_i that is higher than the average of the set S_0. Because the resource consumption attack behavior is mainly to maliciously seize the system resources, the node attribute value is too high, so this paper only considers the attribute higher than the average value of the normal node.

So far, n pieces of evidence are generated by n nodes. The resource usage anomaly caused by the resource consumption attack behavior is mainly manifested in the system attribute of the abnormal node, and the normal node has a relatively small effect on the attack type identification. In order to further improve the fusion precision, the weight of the evidence generated by each node will be calculated and used as the correction coefficient of the evidence.

$$w_i = \frac{\sum_{i=1}^{n} Sim(s_i)}{Sim(s_i)} \tag{7}$$

Finally, using the correction factor to normalize the weighted correction of each evidence, the BPA of the revised evidence is as follows:

$$m'(s_i) = \frac{w_i m(S_i)}{\sum_{p=1}^{N} w_p m\left(S_p\right)} \tag{8}$$

The evidence theory was first proposed by Dempster, who gave the concept of upper and lower probabilities and gave the principle of synthesis of two independent sources of information. Later, his student Shafer further improved and perfected his theory. Therefore, the evidence theory is also called Dempster-Shafer evidence theory, referred to as D-S evidence theory. The core content of D-S evidence theory is "evidence" and "combination". "Evidence" refers to data containing uncertain information. "Combination" refers to the synthesis rule. The synthesis formula can combine the information represented by the data to get more reliable and effective conclusions, which makes D-S evidence theory widely used in many fields such as financial analysis and intelligence analysis.

The following introduces the basic concepts of D-S evidence theory:

(1) Identification framework

Suppose there is a finite set of non-empty hypotheses Θ as the identification framework for evidence theory, consisting of N mutually exclusive hypotheses, defined as:

$$\Theta = \{H_1, H_2, \cdots, H_N\} \tag{9}$$

Where N is the number of hypotheses in the recognition system, H is to identify each hypothesis in the system, and all decision plan sets made by the system are a subset of the power set 2^{Θ} of the identification framework Θ.

(2) Basic probability allocation

The basic probability allocation (BPA) under the identification framework Θ is a function under the mapping m: $2^{\Theta} \rightarrow [0, 1]$, which satisfies the following constraints:

$$\begin{cases} m(\emptyset) = 0 \\ \sum_{A \subseteq \Theta} m(A) = 1 \end{cases} \tag{10}$$

Where A is a proposition containing one or more hypotheses in the identification framework Θ, $m(A)$ represents the degree of support of the evidence for Proposition A, and any proposition A that satisfies $m(A) > 0$ is called a focal element.

(3) Belief function

The belief function (Bel) of Proposition A indicates the degree of trust in the event that Proposition A is true. The trust function under the identification framework Θ is defined as:

$$\text{Bel(A)} = \sum\nolimits_{B \subseteq A} m(B) \qquad A, B \subseteq \Theta \tag{11}$$

Among them, A and B are propositions in 2^{Θ}, and m is the basic probability distribution function on Θ. If an interval is used to indicate the strength of support for any one proposition, then the belief function is the lower bound of this interval.

(4) Plausibility function

The plausibility function (Pl) under the recognition framework Θ is defined as:

$$\mathrm{Pl(A)} = \sum_{B \cap A \neq \emptyset} m(B) \qquad A, B \subseteq \Theta \tag{12}$$

Among them, A and B are propositions in 2^{Θ}, and m is the basic probability distribution function on Θ. If an interval is used to indicate the strength of support for any one proposition, then the belief function is the upper bound of this interval.

(5) Synthetic rule

Assuming that m_1 and m_2 are two independent basic probability distribution functions defined on the identification framework, set $A, B, C \subseteq \Theta$, then the Dempster synthesis rule is defined as:

$$m(A) = \begin{cases} \frac{\sum_{B \cap C = A} m_1(B) \cdot m_2(C)}{1-k}, & A \neq \emptyset \\ 0, & A = \emptyset \end{cases} \tag{13}$$

Where k is the evidence conflict factor. When $k = 1$, the evidence completely conflicts, and the denominator of the synthetic rule formula is 0, and the synthesis rule loses its meaning. In the case of $0 < k < 1$, the basic probability allocation of Proposition B and Proposition C can be fused using a synthesis rule.

Because the evidence theory can deal with the uncertainty of the data well, and can express the correct, incorrect and uncertain probabilities at the same time, it is very suitable for the identification of network resource-consuming attacks. Based on evidence-based fusion formulas, one or more sets of evidence can be combined into a new piece of evidence.

3.3 Resource Consumption Attack Identification Method Based on Data Fusion with D-S Theory

Since the nodes in the network may not only be subjected to various attacks, the data may have different degrees of measurement errors. Therefore, the attack behavior needs to be identified for subsequent better prevention. In this paper, the D-S evidence theory is used to distribute and fuse each evidence according to the basic probability of nodes to effectively identify network resource consumption attacks.

First, the BPA evaluates the source of evidence according to the basic probability, and calculates the trust function and likelihood function of each proposition; Secondly, the interval number is constructed by the trust function and the likelihood function to obtain the trust interval of each proposition; Finally, using the D-S evidence theory, the individual evidence is distributed according to the basic probability of the node, by sorting the results of the aggregation, the recognition result of the resource-consuming attack is obtained.

4 Simulation and Analysis

The simulation uses the public dataset to verify the algorithm, which is compared with the classical D-S evidence theory algorithm [12] and the recent improved algorithm [13, 14]. It proves that our algorithm is effective in solving the evidence conflict problem and has a high correct rate. The experimental algorithm is written in Python language and implemented in the operating environment of ASUS notebook (CPU 1.80GHz, memory 8GB, hard disk 512GB SSD, Win10 operating system).

(1) Public datasets

In order to verify the accuracy and validity of the algorithm fusion results, the algorithm is validated by Iris dataset [5] and KDD CUP 99 dataset [6]. The Iris dataset contains 150 data, divided into 3 categories, 50 data per category, and each data contains 4 attributes. Use the attributes of flower length (SL), flower width (SW), petal length (PL), and petal width (PW) to predict the flower belongs to which category. The KDD CUP 99 dataset is a nine-week network connection data collected from a simulated US Air Force LAN, containing one normal identification type and 22 training attack types. Each connection record contains 41 fixed feature attributes and a class identifier. The identifier is used to indicate whether the connection record is normal or a specific attack type (Table 1).

Assuming the identification framework of the Iris data set $\Theta = \{S, E, V\}$, the existing four evidences are the attribute length (SL), the width of the flower (SW), the length of the petal (PL), and the width of the petal (PW), which BPA are expressed as follows:

Table 1. The BPA of different resources

Resource	BPA
SL	$m_1(S) = 0.41, m_1(E) = 0.29, m_1(S, E) = 0.3$
SW	$m_2(S) = 0.58, m_2(E) = 0.07, m_2(S, V) = 0.35$
PL	$m_3(S) = 0.3, m_3(E) = 0.15, m_3(S, E) = 0.2, m_3(S, V) = 0.35$
PW	$m_4(S) = 0.2, m_4(E) = 0.3, m_4(S, V) = 0.5$

It can be seen that all the evidence supports the proposition S is relatively large, so the fusion result should support the proposition S. The comparison between the classic D-S improved algorithm and the recent improved algorithm and the proposed algorithm fusion result is shown in Fig. 2. All algorithms have the highest support for Proposition S. Among them, the support of the proposed algorithm for the propositions S, E and V are 0.6261, 0.2023 and 0.1716 respectively, and the support of the proposition S is significantly higher than the proposition E and the proposition V. Moreover, the support of our algorithm for correct proposition S is 46.08%, 30.11% and 12.39% higher than that of Yager, Zhao and Jiang respectively. It can be seen that the algorithm of this paper can correctly process the Iris data set.

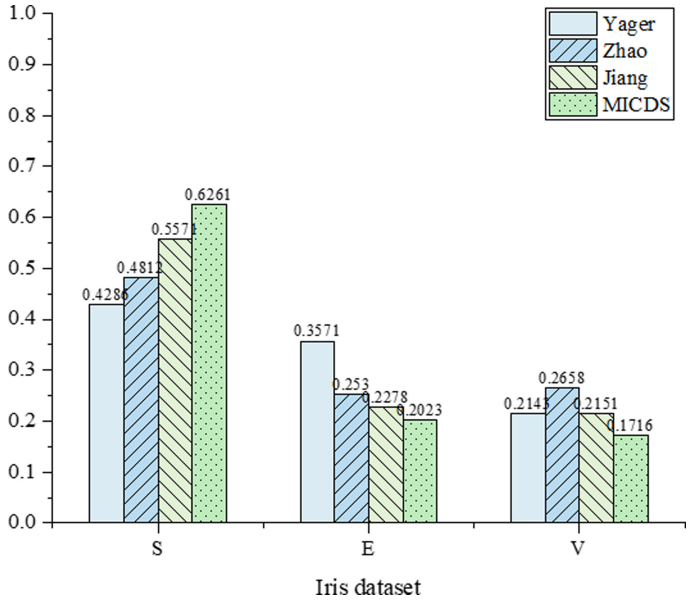

Fig. 2. Iris dataset fusion result

In addition, the accuracy of data fusion results relative to real results (Accuracy) is used as the evaluation index of the algorithm. Each experimental result is obtained from the average of 10 data sets each consisting of 100 sample points. The accuracy of fusion of abnormal points at different scales is shown in Fig. 3 and Fig. 4. As shown in Fig. 3, when there is no abnormal evidence, the accuracy of the algorithm is 89.3%, 92.5%, 93.1%, 95.7%. The accuracy of our algorithm is the highest, which is 7.16%, 3.46% and 2.80%

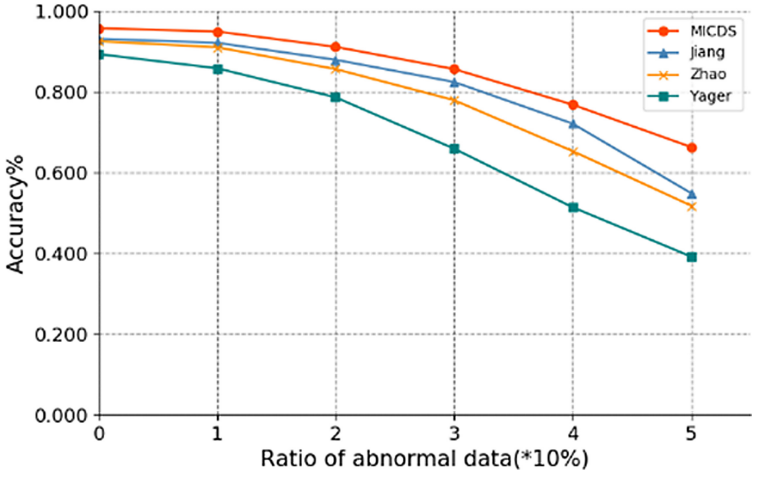

Fig. 3. Accuracy of the Iris dataset

higher than the other three algorithms. The accuracy of the four algorithms gradually decreases with the increase of the proportion of abnormal evidence, but the decrease of our algorithm is the slowest. As shown in Fig. 4, when all data are normal, the algorithm accuracy rates respectively are 83.1%, 87.5%, 89.1%, and 92.7%. The accuracy of the four algorithms decreases with the increase of the proportion of abnormal evidence, but our algorithm has the slowest decline rate. When mixed with 50% abnormal evidence, the accuracy rate remains at 61.6%, which is 64.7%, 24.9% and 14.9% higher than other algorithms. It can be seen that our algorithm can better deal with abnormal evidence and obtain higher recognition accuracy.

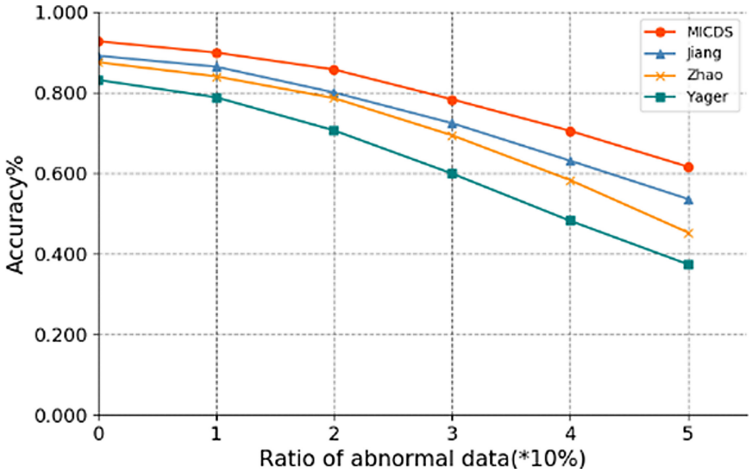

Fig. 4. Accuracy of the KDD dataset

5 Conclusion

Aiming at the network running node may be attacked or there is measurement error, this paper comprehensively utilizes the information of each node, and proposes a resource consumption attack identification method based on node multi-dimensional data fusion. Using correlation, the normal nodes and possible abnormal nodes are divided, and each node is assigned different weights, thus converting the nodes into evidence in D-S evidence theory. Then, according to the basic probability distribution function of the node to the attack type, the D-S evidence theory is used for fusion, and the resource consumption type attack is effectively identified. The simulation is carried out on the public datasets. The effectiveness and certain advantages of the proposed algorithm are proved by comparing the correctness of the algorithm and the comparison algorithm. The algorithm in this paper can realize the identification of resource-consuming attack types, but its fusion accuracy rate needs to be improved. The next step is to conduct in-depth research on this aspect.

Acknowledgement. This work was supported by National Key R&D Program of China (2019YFB2103202, 2019YFB2103200), Open Subject Funds of Science and Technology on Communication Networks Laboratory (6142104200106).

References

1. Palmieri, F., Fiore, U., Castiglione, A.: A distributed approach to network anomaly detection based on independent component analysis. Concurr. Comput. Pract. Exp. **26**(5), 1113–1129 (2014)
2. Aborujilah, A., Musa, S.: Detecting TCP SYN based flooding attacks by analyzing CPU and network resources performance. In: International Conference on Advanced Computer Science Applications & Technologies. IEEE (2015)
3. Harshaw, C.R., Bridges, R.A., Iannacone, M.D. et al.: GraphPrints: towards a graph analytic method for network anomaly detection (2016)
4. Palmieri, F., Fiore, U.: Network anomaly detection through nonlinear analysis. Comput. Secur. **29**(7), 737–755 (2010)
5. https://archive.ics.uci.edu/ml/datasets/Iris/
6. https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html
7. Chaudhary, A., Mittal, H., Arora, A.: Anomaly detection using graph neural networks. In: 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), Faridabad, India, pp. 346–350 (2019)
8. Chun-Hui, X., Chen, S., Cong-Xiao, B., Xing, L.: Anomaly detection in network management system based on isolation forest. In: 2018 4th Annual International Conference on Network and Information Systems for Computers (ICNISC), Wuhan, China, pp. 56–60 (2018)
9. Liu, R., Zhu, Q.: A network anomaly detection algorithm based on natural neighborhood graph. In: 2018 International Joint Conference on Neural Networks (IJCNN), Rio de Janeiro, pp. 1–7 (2018)
10. Su, Q., Liu, J.: A network anomaly detection method based on genetic algorithm. In: 2017 4th International Conference on Systems and Informatics (ICSAI), Hangzhou, pp. 1029–1034 (2017)
11. Ateş, Ç., Özdel, S., Yıldırım, M., Anarım, E.: Network anomaly detection using header information with greedy algorithm. In: 2019 27th Signal Processing and Communications Applications Conference (SIU), Sivas, Turkey, pp. 1–4 (2019)
12. Yager, R.R.: On the aggregation of prioritized belief structures. IEEE Trans. Syst. Man Cybern. Part A: Syst. Hum. **26**(6), 708–717 (2002)
13. Zhao, Y., Jia, R., Shi, P.: A novel combination method for conflicting evidence based on inconsistent measurements. Inf. Sci. **367**, 125–142 (2016)
14. Jiang, W.: A correlation coefficient for belief functions. Int. J. Approx. Reason. **103**, 94–106 (2018)