Alarm-Based Root Cause Analysis Based on Weighted Fault Propagation Topology for Distributed Information Network

LYU Xiaomeng[1], CHEN Hao[1], WU Zhenyu[1],
HAN Junhua[2], GUO Huifeng[2]

(1. Engineering Research Center for Information Networks, Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. ZTE Corporation, Shenzhen 518057, China)

DOI: 10.12142/ZTECOM.202203010

https://kns.cnki.net/kcms/detail/34.1294.TN.20220805.1618.002.html, published online August 8, 2022

Manuscript received: 2021-10-31

Abstract: A distributed information network with complex network structure always has a challenge of locating fault root causes. In this paper, we propose a novel root cause analysis (RCA) method by random walk on the weighted fault propagation graph. Different from other RCA methods, it mines effective features information related to root causes from offline alarms. Combined with the information, online alarms and graph relationship of network structure are used to construct a weighted graph. Thus, this approach does not require operational experience and can be widely applied in different distributed networks. The proposed method can be used in multiple fault location cases. The experiment results show the proposed approach achieves much better performance with 6% higher precision at least for root fault location, compared with three baseline methods. Besides, we explain how the optimal parameter's value in the random walk algorithm influences RCA results.

Keywords: distributed information network; alarm; graph; root cause analysis; random walk

Citation (IEEE Format): X. M. Lyu, H. Chen, Z. Y. Wu, et al., "Alarm-based root cause analysis based on weighted fault propagation topology for distributed information network," *ZTE Communications*, vol. 20, no. 3, pp. 77 – 84, Sept. 2022. doi: 10.12142/ZTECOM.202203010.

1 Introduction

Distributed information networks have been widely used in the Internet, government, military and other important fields because of its reliability, scalability, resource sharing and high performance. However, due to its large-scale system configuration, complex graph structure and operation logic, the frequent occurrences of faults and fault propagation increase the difficulties for locating faults' root causes and troubleshooting the distributed information network.

In recent years, many root cause analysis (RCA) methods have been proposed, which can be divided into two types: knowledge-based and data-driven methods.

1) Knowledge-based: The fault diagnosis methods based on the rules of knowledge generally use the expert experiences to guide the fault diagnosis. ZENG et al.[1] constructed fault reasoning rules with the empirical knowledge of IT operation and maintenance, and then built fault trees to deduce fault root causes. The authors in Ref. [2] proposed an RCA tool inspired by the pattern matching technology. This tool uses the automata built online and the space-time causal relationship between the symbols observed in the log is stored. Its construction does not need annotation and has some interpretability. However, it cannot be used directly and flexibly because of a complex structure.

2) Data-driven: These methods are implemented by multiple technologies including machine learning, causality graph and real graph.

- Machine learning: Bayesian networks (BN) are often used for fault root cause analysis because they contain causal information. LIU et al. [3] proposed a BN construction algorithm based on the alarm seriality, which could reduce the alarm preprocessing time while considering the effectiveness. However, training the network needs a large amount of labeled data to improve the performance generalization of the model. ZHANG et al.[4] trained an attention based autoencoder to predict fault signals. In the case of no labeled samples, this method considered the time dependence, but it is difficult to explain the fault mechanism to some extent.
- Causality graph: A causality graph is a graph based on event co-occurrence or conditional independence test with each event as a node. It locates the root causes by random walk in a causality graph. KALANDER et al. [5] proposed an embedding algorithm based on a causal propagation graph to

This work was supported by ZTE Industry-University-Institute Cooperation Funds under Grant No. HC-CN-20201120009.

infer the weight of the edge, and applied the impact maximization algorithm to determine the root cause alarm. Although it explains the fault mechanism between alarms, the trimming of opposite edges in causal graphs usually requires some expert experience and does not adapt well in a variety of scenarios.

- Real graph: It is more intuitive for random walk in a real relationship graph that is not like the causality graph. ZHAO et al.[6] used performance indicators such as key performance indicators (KPIs) to calculate the similarity of the edges in an anomaly propagation graph, formed the transition probability matrix, and located the fault root by random walk. This method requires such a large amount of performance indicator data for calculation and analysis that the RCA takes a long time.

Compared with the traditional methods based on empirical knowledge, the data-driven methods can better realize real-time analysis with more accuracy and do not need to be greatly adjusted due to the updates of environment configuration. However, the existing data-driven methods often need a large amount of labeled data for supervised training[7]. TraceRCA[8] mined the suspicious nodes by KPIs, which could reduce the locating noise. It inspired us to propose the idea of locating the root causes by alarms. Because common alarms cannot be used to mine more fault root cause information. ZHANG et al.[9] proposed the anomaly propagation graph using system data and used two optional algorithms to locate root causes. This inspires us to construct the fault propagation with alarms to explain the mechanism of fault propagation. Those methods without graphs cannot intuitively explain the mechanism of fault propagation. One the other hand, the other methods of using constructed fault propagation graphs are almost based on KPIs[10 – 12] or other metrics collected from the database. However, these methods have to use acquisition tools and set the collection locations to acquire various kinds of data, which may cost too much labor. A causal graph in alarms also needs expert experience, which cannot adapt well in distributed environments with frequent updates.

For the above deficiencies, we propose an alarm-based method for root cause analysis of distributed information networks based on a weighted fault propagation topology (WFPT-RCA). It is inspired by the previous work, mainly Refs. [8 – 9]. It trains the classifier using a few historical labeled alarms to mine the effective information of root causes. When a fault occurs, based on the character of alarms, the WFPT-RCA immediately extracts a subgraph from the real graph of the distribute network. Then combined with the information of root causes and alarms' features, our method calculates the weights of nodes and edges in the subgraph. Based on the random walk in the weighted subgraph, it not only explains the behaviors of fault propagation, but also outputs the nodes' list about root causes' scores to help operators to repair the fault. We evaluate WFPT-RCA in two datasets in different scenarios (an e-commerce platform and a transport network). The results show that WFPT-RCA achieves a good performance result, with 90% in precision and 92.7% in mean average precision. It outperforms several other state-of-the-art methods.

In summary, the contributions of this paper are threefold:

1) We propose a two-stage RCA approach. In the offline phase, a few labeled alarms are used to train the classifier for digging more information associated with root causes in order to guide the fault location in the online phase.

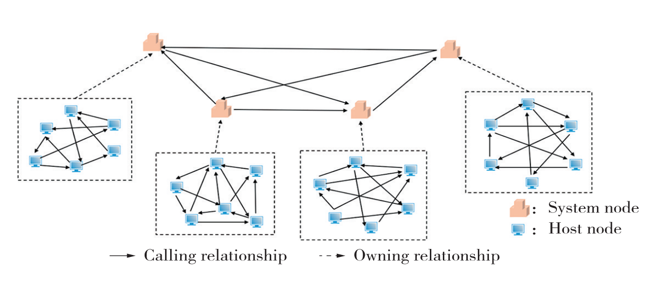
2) We provide a method based on alarms to calculate the nodes' weights as the scores of root causes and edges' weights as the probabilities of the fault propagation in the real graph which adapts well in distribute information network.

3) We evaluate WFPT-RCA in two datasets. The results demonstrate that WFPT-RCA localizes root causes correctly and has a better generalization ability. Our method pays more attention to features related to root causes and does not rely on the experience knowledge of operators.

The remaining of this paper is organized as follows. The framework and details of WFPT-RCA are mainly introduced in Section 2. In Section 3, we show the related experiments' results and conclusion analysis to prove the efficiency of our approach. Finally, Section 4 concludes the paper.

2 Framework of WFPT-RCA

Static topological relationships in a distributed information network are often complex and hierarchical (Fig. 1). An e-commerce platform is often composed of multiple system nodes to achieve efficient work. And there are more host nodes that belong to the system nodes to offer different services. The real lines in nodes represent the calling relationships between the nodes, while the dashed lines represent the owning relationships between system nodes and host nodes. Similarly, Fig. 1 can also be regarded as a graph of the transport network where the host nodes can be represented as the network element (NE) and the links and pseudo-wires are expressed as real edges. Moreover, the transport network includes the core layer, convergence layer and access layer. There are various NEs to transmit data through multiple links in each layer to represent the hierarchy of graph. In real scenarios, such complex and hierarchical relationships often lead to faults due to resource usage and response timeout of a system node. If we directly locate faults based on performance



▲Figure 1. Graph of an e-commerce platform indicators in the original graph, noise interference may occur, resulting in low accuracy. Meanwhile, alarms usually reflect node status. Using alarms to identify abnormal nodes in the graph and extract abnormal subgraphs, noise interference can be reduced and fault location accuracy can be improved.

The framework of WFPT-RCA is shown in Fig. 2, which is mainly divided into offline analysis and online diagnosis. We make full use of the collected and labeled historical alarms of each fault event. Taking the occurrence location as the research object, feature extraction is carried out for the alarms in each location. The root location is identified by the binary classifier training model, and the key features are determined by feature importance analysis. In the online phase, alarms and network graph configuration data are firstly collected if the fault occurs after the fault work order is obtained from the operators. After the features of the nodes where alarms have occurred in the offline phase are extracted from the alarms, an abnormal subgraph (ASG) based on the location of the alarm and an original network graph are extracted and the weights of nodes and edges based on the alarm features of nodes are then calculated to generate a weighted abnormal subgraph called Weighted Fault Propagation Graph. Then, a random walk is carried out in ASG. After iteration convergence, the node with the highest score is output and regarded as the root node according to the ranking of root cause score of each abnormal node.

2.1 Data Collection

The collected data are mainly from the alarms and graph generated in the distributed information network. After a system fault occurs, a surge in the number of alarms occurs within a few minutes, namely alarm storms[13]. In the online phase, we collect statistics on the number, type and severity of alarms generated in the distributed system every minute. According to the occurrence time sequence, WFPT-RCA constitutes the corresponding time series, respectively adopting S-H-ESD anomaly detection[14] to find outlier points and integrating the occurrence time corresponding to detected outlier points, so as to determine the occurrence time range of faults. The graph is usually extracted from system configuration data when a fault occurs. It analyzes the owning and association relationships of each location based on the location where an alarm occurs.

2.2 Feature Analysis

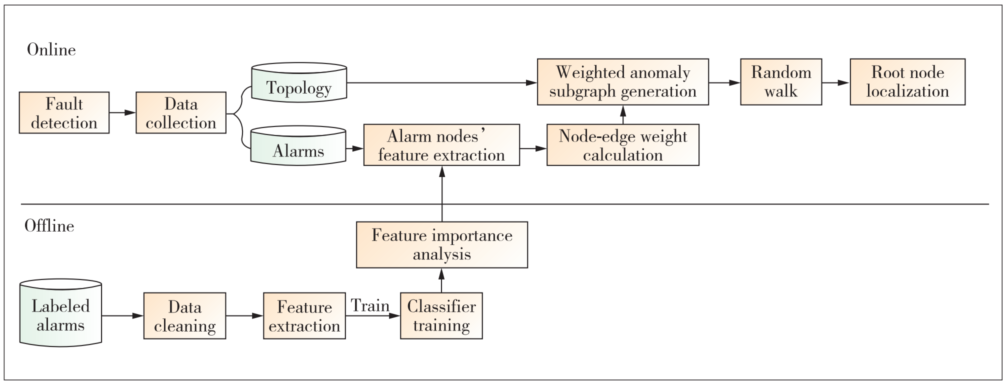
Feature analysis is to mine and analyze the alarm information at the offline stage and find the features related to the root cause. It is mainly divided into four steps: data cleaning, feature extraction, classifier training and feature importance analysis.

1) Data cleaning. WFPT-RCA first collect the alarms based on the operators' fault repair experience and fault work in order to obtain the labeled alarm dataset. The content of the alarms is mainly consisted of the timestamp, location and rich concrete content. Alarm pretreatment is a usual practice to enable the alarm content to become a standard template, such as removal of the IP address and request ID. This approach can reduce the alarm type space and noise, and facilitate subsequent cutting word analysis. The content of the warning words is cut to get rid of some stop words such as "for" and "is", and then text information will be extracted more accurately.

2) Feature extraction. Main features include text, frequency and time.

- Text: After cutting alarm words, we analyze the alarm information based on words to find important words related to faults. Inverse Document Frequency (IDF)[15] is a key feature used to measure the importance of words in text mining, reducing the weight of frequent words and increasing the weight of unfamiliar words; $\mathrm{IDF}(w) = \log\left[N/(N_w + 1)\right]$, where N is the total number of words in all alarms and N_w is the number of alarms containing the word w. After the IDF for the words contained in each alarm is calculated, the information entropy of each alarm will be calculated as $\sum_m IDF(\mathrm{w})/m$, where m is the total number of words in each alarm.
- Frequency: This feature is extracted based on the statistics for the number of alarms, the total number of species, the number of alarms per minute on average from every node, the number of serious alarms and so on. More serious faults and richer node types are to determine a more serious alarm type, such as failure and downtime.
- Time: The occurrence of faults often has a certain time rule. Therefore, the statistics on relative occurrence time (the time difference between the earliest alarm of a node and the earliest alarm of a fault event) and on alarm duration of each node is collected.

3) Classifier training. Based on the occurrence location, WFPT-RCA inputs the extracted alarm features with the la-



▲**Figure 2. Framework of the proposed WFPT-RCA** bels 0 (not root cause) and 1 (root cause) into XGBoost[16] for training until the model has the optimal effect to classify the root cause samples.

4) Feature importance analysis. When we train the binary XGBoost model, the importance of features can be analyzed in the meantime. It is implemented by employing the F score to evaluate the influence of each feature in the dataset on classification decision. The F score is used to measure the discrimination ability of the features to model classification. The higher the F score is, the stronger the distinguishing ability of the feature is. Moreover, the results of feature importance will play a great role in the subsequent root location.

2.3 ASG Generation

As shown in Fig. 3, ASG is constructed based on the actual graph of the distributed information network. Due to the nature of alarms, we select the set of candidate abnormal nodes $V_a = \{v_{a1}, v_{a2}, \cdots, v_{an}\}$, where n is the number of abnormal nodes and v_{a1} is one of the anomaly nodes. The filter rules are based on whether alarms are generated at each location in the graph during the fault occurrence. The ASG is expressed as $\text{ASG}(V_a, E)$, where E is the set of e_{ij} that shows the directed real edge where v_{ai} points to v_{aj}. V_a and E have different physical meanings in different distributed information networks, which can assign different meanings to them based on the graph and alarm location. The ASG corresponding to each fault event varies according to the locations of the alarms. The weights of the nodes and edges of the extracted ASG must be defined to provide physical significance in the scenario of root cause locating and more explanatory for root cause diagnosis. The following is the definitions:

1) Node weight w_v: It calculates nodes' weights based on the alarms of nodes. It can be regarded as the initial root cause score of node failure. The weight of v_{ai} is calculated as follows:

$$w_{vi} = \theta_1 \cdot f_i(1) + \theta_2 \cdot f_i(2) + \cdots + \theta_l \cdot f_i(l)\,, \tag{1}$$

where l is the number of features, k is the k-th feature of the feature set, $k \in [1, l]$, and θ_k and f_k are respectively the normalized feature importance score and the value of k. Finally, all calculated node weights are normalized again. The larger the weight value is, the higher the empirical root score or probability value of the node is considered.

2) Edge weight w_{ij}: It is the weight of the edge between v_{ai} and v_{aj}. The calculation formula is:

$$w_{ij} = \max\left|\text{corr}\left(f_i(k), f_j(k)\right)\right|, \tag{2}$$

where corr(·) is Pearson correlation calculation; $w_{ij} \in [0, 1]$ and its physical meaning is the probability of fault propagation, which is the maximum similarity degree of each feature between nodes. That is, if there are edges between a node and multiple nodes, by calculating the weights of all adjacent edges connected, it can be considered that the edge with a larger weight is more likely to have fault propagation. The edge weights are calculated in order to construct the transition probability matrix in the random walk. By calculating the weights of nodes and edges, we obtain the weighted ASG. The specific process is shown in Algorithm 1.

Algorithm 1 : Weighted ASG

Input: anomalous subgraph ASG, anomalous edge set E, anomalous node set V_a, alarm feature vector $\boldsymbol{f}$, and weight parameters of feature importance obtained by offline training $\boldsymbol{\theta}$

Output: weighted ASG

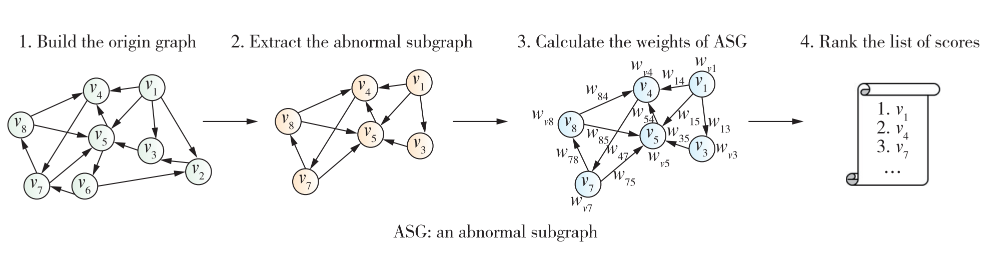
```
for node $\boldsymbol{v_{aj}}$ in $V_a$ do
    Assign $\theta_1 \cdot f_i(1) + \theta_2 \cdot f_i(2) + \cdots + \theta_l \cdot f_i(l)$ to $w_{vi}$;
    for $e_{ij}$ in $E$ of $v_{aj}$ do
        for $k$ in $l$ do
            Assign $\left|corr\left(f_i(k), f_j(k)\right)\right|$ to $w_{ij}(k)$;
        end
        Assign max$(w_{ij}(k))$ to $w_{ij}$;
    end
end
return weighted SG
```

2.4 Root Cause Localization

Root cause localization refers to locating the root node by random walk on the weighted ASG. We define the vector $\boldsymbol{v}$[17] in PageRank as the root score of each node of V_a. Before calculating the root scores, we define the matrix of transition probability $\boldsymbol{P}$ among the nodes of V_a. For instance, v_{ai} points to v_{aj}, and the transfer probability between v_{ai} and v_{aj} is calculated as follows:

$$P_{ij} = \frac{w_{ij}}{\sum_j w_{ij}}\,. \tag{3}$$

If there is no edge between v_{ai} and v_{aj}, $P_{ij} = 0$. $\sum_j w_{ij}$ is the sum of the weights of all the out-edges from v_{ai}. The formula of PageRank is shown in Eq. (4).



▲ **Figure 3. Procedure of ASG generation**

$$\boldsymbol{v}_m = \frac{1-q}{n} + q \cdot \boldsymbol{P} \cdot \boldsymbol{v}_{m-1}, \tag{4}$$

where $\boldsymbol{P}$ is the transition probability matrix made up of P_{ij}, n is the number of nodes, q is the damping factor that means that the node jumps back to a random node with the probability of q in each step and continues to advance along the directed edge in the graph with the probability of 1-q, and $\boldsymbol{v}_m$ is the vector composed of root score from each node obtained by iterating m times. Finally, the abnormal nodes are sorted according to the root score to obtain the list. Operators can check and repair alarms reported by the abnormal nodes and their locations in sequence, which improves the locating efficiency and reduces labor costs.

3 Experimental Evaluation

In this section, we mainly introduce the experimental setup, show experimental results, compare the results with other state-of-the-art methods, and analyze the advantages of our method.

3.1 Experimental Setup

In order to verify the effectiveness of the proposed WFPT-RCA, we totally choose two different types of datasets in two distribute scenarios.

The former called Dataset A is adopted in the experiment of an e-commerce platform to release the actual production in a scenario of the real dataset[1] that contains the topological relationship and the alarms of 50 failure events. The topological relationship refers to the invocation relationship data between systems, between systems and hosts, and between hosts. Table 1 lists the format of alarms. Alarms of each fault event are sorted by timestamp and stored in a csv file, in which root cause alarms (system/host/alarm content) are labeled and only one root cause exists.

The latter called Dataset B is from a transport network in the telecommunication system provided by ZTE Corporation. It also has the system configurations to describe the topology relationship and alarms. Unlike the former dataset, its graph includes the NEs, links, tunnels and pseudo-wires, and presents the data transmission in L2/L3VPN. The difference of the two datasets also reflects in the content of alarms: Dataset B has alarm codes and types instead of content as shown in Table 2. In Dataset B, there are 38 fault events and the root cause location (NE) labeled by the operators who have rich experience.

We compare WFPT-RCA with three baseline methods as follows.

1) MicroRCA: It is a way to locate root causes in microservices and uses the metrics to construct the weighted graph for random walk. Different from our method, it uses the anomaly detection confidence to calculate weights of edges in the graph.

2) Microscope[18]: It is another graph-based approach to identify faults in microservice environment. To implement it, we construct the causality graph with alarms and then use cause inference to find the root causes.

3) Association Rules[19]: It is a traditional method to mine the rules between alarms for assisting the operators to locate root causes.

To implement the proposed WFPT-RCA method, we adapt the frequent item mining to outputing the association rules for potential alarms.

3.2 Evaluation Metrics

In order to evaluate the effectiveness of the RCA methods, the following indicators are adopted in the fault event set A:

1) Precision at the top k: The precision is denoted as $PR@k$ which means the real root is in the the top k output results. When k is small, the bigger the value is, the higher the accu-

▼**Table 1. Examples of alarms generated during a fault in Dataset A**

Timestamp	System	Host	Alarm content	Is_root
2019/6/14 1:14	SYS_5	Host_14	I/O wait load exceeds 10% for 15 minutes	0
2019/6/14 1:14	SYS_4	Host _9	The log generates ERROR information	0
2019/6/14 1:14	SYS_9	Host _92	On CPU Steal Time lasts 5 minutes over 10%	0
2019/6/14 1:14	SYS_9	Host _75	Free swap space is less than 50%	0
2019/6/14 1:14	SYS_5	Host _60	The communication on port 80 is abnormal	1
2019/6/14 1:14	SYS_5	Host _76	The upper I/O wait load is greater than 50%	0
2019/6/14 1:14	SYS_4	Host _23	Ping packet loss rate is 100%, and the server breaks down	0
2019/6/14 1:14	SYS_9	Host _75	The Slot00 status of the hard disk is failed	0
2019/6/14 1:14	SYS_9	Host _60	Number of FullGC: 32 (greater than threshold: 10)	0
2019/6/14 1:14	SYS_5	Host _97	Average heap memory usage: 94.61% (greater than threshold: 90%)	0
2019/6/14 1:14	SYS_5	Host _32	Average FullGC time: 2 118 ms (greater than threshold: 1 000 ms)	0
2019/6/14 1:14	SYS_4	Host _3	Nic traffic unknown	0

[1] http://www.cnsoftbei.com/plus/view.php?aid=479.

▼Table 2. Examples of alarms generated during a fault in Dataset B

Timestamp	NE	Duration	System Type	Code	Severity	Alarm Type	Root
2020/2/27 10:01	4 167	1 000	4 198	964	1	0	0
2020/2/27 10:01	4 715	12 000	4 590	18 956	2	3	0
2020/2/27 10:01	4 167	15 000	4 197	43	4	0	1
2020/2/27 10:01	4 167	11 000	4 590	18 956	4	3	0
2020/2/27 10:01	4 166	5 000	4 590	18 956	3	3	0
2020/2/27 10:01	4 595	10 000	4 198	964	1	0	0
2020/2/27 10:01	5 496	6 000	4 590	18 956	3	1	0
2020/2/27 10:01	5 497	5 000	4 197	43	4	4	0

NE: network element

racy of location becomes. The detail is shown in Eq. (5).

$$\mathrm{PR}@k = \frac{1}{|A|}\sum\nolimits_{a \in A}\frac{\sum_{i<k}(R[i] \in v_c)}{(\min(k,|v_c|))}\ , \tag{5}$$

where $R[i]$ is the results of the top k obtained by root score sorting in each fault event and v_c is a set of real causes in fault events.

2) Mean average precision (MAP): It measures the average location performance of the algorithm and the equation is shown in Eq. (6):

$$\mathrm{MAP} = \frac{1}{|A|}\sum\nolimits_{a \in A}\sum\nolimits_{1 \leqslant k \leqslant N}\mathrm{PR}@k. \tag{6}$$

3.3 Experimental Results

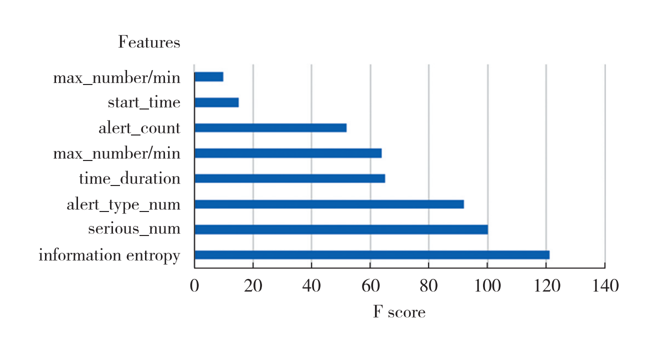
3.3.1 Feature Importance

The details of the offline analysis in Dataset A are represented to show how our method extracts the information of root causes. The alarm features of nodes are extracted from each fault event, and the detailed features and meanings are shown in Table 3.

▼Table 3. Features used for feature importance analysis in Dataset A

Feature	Meaning
information entropy	Average IDF of the system node
max_number/min	Maximum number of alarms per minute
node_num	Number of nodes in same systems
alert_count	Total number of alarms
alert_type_num	Number of alarm types
start_time	Relative start time
time_duration	Time span (minutes)
serious_num	Number of serious type alarms

These features labeled by the root cause of alarms are input into the classifier for training, so as to obtain the analysis results of the feature importance (Fig. 4).



▲Figure 4. Results of feature importance analysis

It shows that the IDF and the number of serious alarms mined from the alarm information are most related to root causes. The information entropy describes the richness of alarm content on each node. A higher value states the more information about root causes in the nodes. Serious alarms usually indicate the severity of faults and the root causes may have more serious alarms. The F score of each feature is normalized and used as the feature weight parameter θ. The parameter not only completes the subsequent node weight calculation that can be seen in Algorithm 1, but also helps us understand the root causes reflected on alarms without the operational experience.

3.3.2 RCA Results

Table 4 shows the performance of the compared methods. WFPT-RCA (no ASG) directly locates root causes without extracting abnormal subgraphs. The compared results prove that the ASG can effectively reduce the noise of fault location and improve the accuracy and efficiency. The results of WFPT-RCA (no feature analysis) illustrate the importance and effectiveness of the offline analysis to obtain the feature weight parameter θ. It also shows that the analysis of feature samples of historical alarms in the offline phase can affect the initial root scores of nodes, thus determining the accuracy of location. MicroRCA is also based on random walk. Different from our method, the prior knowledge is added in the calculation of node edge weights. However, the prior knowledge often does

▼Table 4. Performance in Datasets A and B

Metrics	Dataset A				Dataset B			
	PR@1	PR@3	PR@5	MAP	PR@1	PR@3	PR@5	MAP
WFPT-RCA	**0.90**	**0.92**	**0.96**	**0.927**	**0.89**	**0.95**	**1.00**	**0.947**
WFPT-RCA (no ASG)	0.64	0.70	0.84	0.727	0.53	0.63	0.74	0.633
WFPT-RCA (no feature analysis)	0.28	0.54	0.90	0.573	—	—	—	—
MicroRCA	0.84	0.92	0.94	0.900	0.79	0.84	0.89	0.840
Microscope	0.82	0.88	0.90	0.867	0.74	0.79	0.84	0.790
Association rules	0.36	0.56	0.78	0.567	0.47	0.58	0.63	0.560

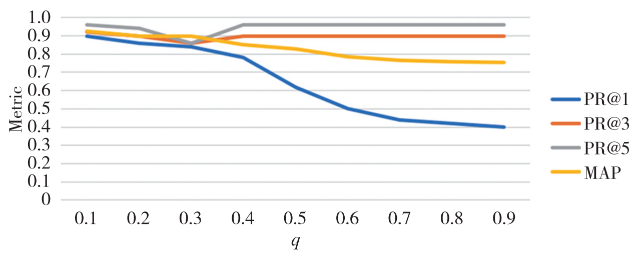
ASG: anomaly subgragh　MAP: mean average precision　RCA: root cause analysis
PR: precision　WFPT: weighted fault propagation topology

not have good generalization and the effect may vary greatly in different scenarios. This shows the operational experience may not adapt well in different distribute information networks. Microscope uses the causal graph to explore the relationship between alarms, so as to locate the root causes. The reason for its unsatisfactory effect is that the nodes downstream of the root cause is often located in the random walk of the causal graph rather than real adjacent nodes. The method lacks of the certain interpretability compared with the fault propagation in a real graph. The performance of the association rules based on frequent item mining mainly lies in the fact that different faults present different behaviors, and the rules are difficult to be used in multiple scenarios. Unless they are updated with the change for environments. Through the comparison in two datasets, it can be found that our method has great advantages in the RCA. Because the features are extracted and analyzed offline, the offline feature analysis effectively reduces the impact of environmental changes on locating accuracy in different scenarios. The method of locating faults based on the real graph as fault propagation is able to help operators understand the propagation way of faults. In a word, WFPT-RCA has wider usage, higher precision, efficient computation and some comprehensibility.

3.3.3 Experimental Results of Parameter Adjustment

Because the damping factor q in PageRank has its unique physical meaning, its value also straightly impacts the metrics of RCA. Therefore, we analyze and evaluate the influence of the value of q on the WFPT-RCA final results in Dataset A.

As can be seen from Fig. 5, the trends of PR@3 and PR@5 are similar, which shows the change in q does not make much difference to them. PR@1 decreases gradually with the increase of the q value until the results of each index reach the optimal level when q = 0.1. We can see that PR@1 decreases obviously at $q \in [0.1, 0.2, 0.3, 0.4]$, which indicates that the transition probability of random jump back to a node has a great influence on fault location. If the q value is too large, it directly interferes with the random walk on the ASG. As a result, the constraints of the real graph on the location result are reduced and the random transfer between nodes plays a leading role in the location. Therefore, we generally keep the q value in the range of 0.1 – 0.15 to ensure that our method achieve better performance.



MAP: mean average precision

▲**Figure 5. Results of each metric for fault location at different *q* values in Dataset A**

3.4 Discussion

Here we discuss the significance of the proposed approach.

1) Generalization performance: The weighted fault propagation graph is constructed without the operational experience. As system configuration is updated, it does not need to adjust the method completely. In addition, the experimental results in two different datasets also present better adaption. The characteristic reduces the operators’ pressure of work and improves the availability of distributed information networks.

2) Intelligibility: Unlike the other compared methods, WPFT-RCA mines the features of root causes from alarms. The alarms directly filter the nodes from the real graph to construct a weighted fault propagation graph, which can decrease the complexity of fault location. Therefore, operators can analyze the behaviors of fault propagation caused by the root cause with the weighted graph. For example, the higher the root score is, the more related the root cause fault is. The larger the edge weight is, the more likely fault propagation will occur. Based on the above rules, it shows that WPFT-RCA has better intelligibility in the cases of fault propagation.

4 Conclusions

In this paper, we propose an alarm-based method for root cause analysis of distributed information networks based on a weighted fault propagation topology, which is constructed in real graph relationship and calculates weights of nodes and edges in the ASG by the features using historical offline analysis. The experimental results on public datasets in real scenarios show that our method can achieve 90% precision and 92.7% mean average precision. Our method is based on the analysis of historical alarms and real graphs, which can effectively reduce the impact of environmental configuration changes on fault location results. In addition, the location based on real graph helps operators understand the mechanism of fault propagation. Verification in various kinds of large, dynamic environments are our main future work.

References

[1] ZENG M F, XIE P Y. Research on fault location of information system based on CMDB and rule inference [J]. Journal of Guangxi academy of sciences, 2017, 33 (1): 53 – 58. DOI: 10.46960/2658-6754_2019_3_4

[2] BOUILLARD A, BUOB M-O, RAYNAL M, et al. Log analysis via space-time pattern matching [C]//14th International Conference on Network and Service

Management (CNSM). IEEE, 2018: 303 – 307

[3] LIU M L, QI X G, LIU L F, et al. Roots-tracing of communication network alarm: A real-time processing framework [J]. Computer networks, 2021, 192: 108037. DOI: 10.1016/j.comnet.2021.108037

[4] ZHANG C X, SONG D J, CHEN Y C, et al. A deep neural network for unsupervised anomaly detection and diagnosis in multivariate time series data [C]//33th AAAI Conference on Artificial Intelligence. AAAI, 2019: 1409 – 1416. DOI: 10.1609/aaai.v33i01.33011409

[5] ZHANG K L, KALANDER M, ZHOU M, et al. An influence-based approach for root cause alarm discovery in telecom networks [C]//Service-Oriented Computing ICSOC 2020 workshops, 2021: 124 – 136. DOI: 10.1007/978-3-030-76352-7_16

[6] ZHANG L Y, ZHAO J B, ZHANG M. Root cause analysis of concurrent alarms based on random walk over anomaly propagation graph [C]//IEEE International Conference on Networking, Sensing and Control. IEEE, 2020: 1 – 6. DOI: 10.1109/ICNSC48988.2020.9238084

[7] YUAN Y N, YANG J L, DUAN R, et al. Anomaly detection and root cause analysis enabled by artificial intelligence [C]//IEEE Globecom Workshops. IEEE, 2020: 1 – 6. DOI: 10.1109/GCWkshps50303.2020.9367508

[8] LI Z Y, CHEN J J, JIAO R, et al. Practical root cause localization for microservice systems via trace analysis [C]//29th International Symposium on Quality of Service(IWQOS). IEEE, 2021: 1 – 10. DOI: 10.1109/IWQOS52092.2021.9521340

[9] ZHANG L Y, ZHAO J B, ZHANG M. Root cause analysis of concurrent alarms based on random walk over anomaly propagation graph [C]//IEEE International Conference on Networking, Sensing and Control. IEEE, 2020: 1 – 6. DOI: 10.1109/ICNSC48988.2020.9238084

[10] SHARMA B, JAYACHANDRAN P, VERMA A, et al. CloudPD: problem determination and diagnosis in shared dynamic clouds [C]//43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). IEEE, 2013: 1 – 12. DOI: 10.1109/DSN.2013.6575298

[11] LIN J Y, ZHANG Q, BANNAZADEH H, et al. Automated anomaly detection and root cause analysis in virtualized cloud infrastructures [C]//IEEE/IFIP Network Operations and Management Symposium. IEEE, 2016: 550 – 556. DOI: 10.1109/NOMS.2016.7502857

[12] CHEN P F, QI Y, HOU D. CauseInfer: automated end-to-end performance diagnosis with hierarchical causality graph in cloud environment [J]. IEEE transactions on services computing, 2019, 12(2): 214 – 230. DOI: 10.1109/TSC.2016.2607739

[13] ZHAO N W, CHEN J J, PENG X, et al. Understanding and handling alert storm for online service systems [C]//42nd International Conference on Software Engineering: Software Engineering in Practice. ACM, 2020: 162 – 171. DOI: 10.1145/3377813.3381363

[14] GOLIĆ M, ŽUNIĆ E, ĐONKO D. Outlier detection in distribution companies business using real data set [C]//18th International Conference on Smart Technologies. IEEE, 2019: 1 – 5. DOI: 10.1109/EUROCON.2019.8861526

[15] MANNING C D, RAGHAVAN P, SCHUTZE H. Introduction to information-retrieval [J]. Information retrieval, 2010, 13: 192 – 195. DOI: 10.1007/s10791-009-9115-y

[16] CHEN T Q, GUESTRIN C. XGBoost: a scalable tree boosting system [C]//22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM, 2016: 785 – 794. DOI: 10.1145/2939672.2939785

[17] WU L, TORDSSON J, ELMROTH E, et al. MicroRCA: root cause localization of performance issues in microservices [C]//IEEE/IFIP Network Operations and Management Symposium. IEEE, 2020: 1 – 9. DOI: 10.1109/NOMS47738.2020.9110353

[18] LIN J J, CHEN P F, ZHENG Z B. Microscope: pinpoint performance issues with causal graphs in micro-service environments [C]//ICSOC 2018: Service-Oriented Computing. ICSOC, 2018: 3 – 20. DOI: 10.1007/978-3-030-03596-9_1

[19] HRYCEJ T, STROBEL C M. (2008) Extraction of maximum support rules for the root cause analysis [M]//Computational Intelligence in Automotive Applications. Berlin Heidelberg, Germany: Springer. 2008: 117 – 131. DOI: 10.1007/978-3-540-79257-4_6

Biographies

LYU Xiaomeng (lvxiaomeng@bupt.edu.cn) is studying for her master's degree at Beijing University of Posts and Telecommunications (BUPT), China and received her bachelor's degree in information and communication engineering from BUPT in 2019. Her main research interests include fault prediction and fault diagnosis. She has published one paper in disks fault prediction and two patents in the AIOps.

CHEN Hao is studying for his master's degree at Beijing University of Posts and Telecommunications (BUPT), China and received his bachelor's degree in 2020 at the Faculty of the Information and Communication Engineering, BUPT. His main research interests are fault recognition and prediction.

WU Zhenyu received his BS and PhD degrees from Beijing University of Posts and Telecommunications (BUPT), China in 2008 and 2013. He is currently an associate professor of School of Information and Communication Engineering at BUPT. His research interests include AIOps, intelligent fault diagnostics, machine learning and prognostics and health management (PHM) technology.

HAN Junhua received his master's degree from Graduate School of the Chinese Academy of Sciences (now University of the Chinese Academy of Sciences) in 2005. He is currently an engineer of ZTE Corporation. His research interests include intelligent operation and maintenance, intelligent fault diagnosis, knowledge graph and graph neural network.

GUO Huifeng received her master's degree from Huazhong University of Science and Technology (HUST), China. She is currently an engineer of ZTE Corporation. Her research interests include intelligent network and fault management.