Fault Diagnosis Algorithm Based on Service Characteristics Under Software Defined Network Slicing

Wei Li[1], Hao Cai[1], Chunxia Jiang[1], Ping Xia[1], Song Jiang[1], and Peng Lin[2(✉)]

[1] Communication Branch, State Grid Jiangsu Electric Power Co., Ltd., Jiangsu, China
[2] Beijing Vectinfo Technologies Co., Ltd., Beijing, China
linpeng@vectinfo.com

Abstract. In order to solve the problem of low accuracy of fault diagnosis algorithms brought by network dynamics, this paper proposes a fault diagnosis algorithm based on service characteristics under software defined network slicing. In order to reduce the problem of inaccurate symptom information caused by network dynamics, the credibility of symptoms is calculated based on the alternative probabilistic characteristics of network nodes, and the symptom information is corrected. The node importance is analyzed from the two dimensions of node centrality and number of links. Based on the node importance and symptom information, the reliability of the node failure is ranked. Finally, based on the maximum coverage algorithm, the optimal set of suspected faults is selected from the set of suspected faults as the final set of faults. The experiment compares the algorithm in this paper with the existing algorithm, and verifies that the algorithm in this paper effectively improves the accuracy of fault diagnosis.

Keywords: Software defined network · Network slicing · Fault diagnosis · Network characteristics

1 Introduction

With the rapid construction and operation of future networks, the advantages of 5G networks such as high bandwidth, low latency, and high number of connections have become more prominent, and the types and number of services have increased rapidly. Taking into account the different requirements of different services on the network and the rapid increase of new service types, network slicing technology with Software Defined Networks (SDN) has been proposed and gradually accepted by global network operators and equipment vendors and has become the mainstream technology [1]. In the network slicing environment, the traditional physical network is divided into the underlying network and the virtual network. The underlying network provider is responsible for building the underlying nodes and underlying links. The virtual network service provider leases the underlying nodes and links from the underlying network to construct a virtual network.

M. Cheng et al. (Eds.): SmartGIFT 2020, LNICST 373, pp. 65–76, 2021.
https://doi.org/10.1007/978-3-030-73562-3_6

Various services are carried on the virtual network. In order to ensure the stable and reliable operation of 5G services, fast and accurate fault location technology has become an important task for network managers.

From the proactive perspective of fault diagnosis, fault diagnosis algorithms can be divided into two types: active diagnosis and passive diagnosis. Active diagnosis is fault location of specific network resources based on the network environment and business characteristics, through the selection of detection sites and implementation of detection [2]. Passive diagnosis means that after network managers receive network alarms, they locate faults based on the alarm information and network information [3]. From the perspective of the mathematical model of fault diagnosis, fault diagnosis algorithms can be divided into binary dependent fault models, graph dependent fault models, Bayesian dependent matrix models, etc. [4]. By constructing a fault model and using mathematical tools, the complexity of fault diagnosis can be better solved [5]. Aiming at the fault diagnosis problem in the network virtualization environment, literature [6] proposed a rule-based hybrid tracking mechanism, which better solved the problem of low fault diagnosis performance caused by heterogeneous networks in the SDN environment.

Based on the correlation between faults and symptoms, existing studies have achieved good results in the accuracy rate of fault diagnosis, false alarm rate, diagnosis time and other indicators by constructing fault diagnosis models. However, because software defined network slicing technology realizes the dynamic migration and on-demand allocation of resources, the relationship between faults and symptoms is more complicated, resulting in a decrease in the accuracy of the fault diagnosis model, thereby affecting the performance of fault diagnosis. In order to solve the problem of low performance of fault diagnosis algorithms caused by network dynamics, this paper proposes a fault diagnosis algorithm based on service characteristics under software defined network slicing. Based on the relationship between network resources and services, the algorithm corrects symptom information and ranks the reliability of node failures. In the experimental link, it is verified that the algorithm in this paper effectively improves the performance of the fault diagnosis algorithm.

2 Problem Description

The biggest difference between network slicing and the current Internet is that the current Internet is composed of a single role of an Internet service provider, while network slicing is composed of two different roles, an infrastructure provider and a network service operator. This division of labor realizes the separation of network equipment and terminal services, and facilitates the deployment of users' target requirements on network slicing. In addition, each network slicing can use independent protocol architectures, and can dynamically adjust and re-allocate node resources and link resources in the network according to user needs, so as to achieve efficient and reasonable use of network resources and improve network performance. Service quality reduces network operation and maintenance costs. The business model of network slicing mainly includes three entities: infrastructure providers, network service operators, and end users.

In the network slicing environment, the infrastructure provider is responsible for the construction and maintenance of the underlying physical network, ensuring the normal

operation of the physical network, and providing physical resources to different network service operators through open and standard programmable interfaces. Different infrastructure providers provide differentiated services in terms of resource quality and freedom of use. Multiple infrastructure providers communicate and combine based on mutually agreed interconnection protocols to create an end-to-end physical architecture. Among them, the task of some infrastructure providers is to use different network technologies to provide network service operators with connection services, such as optical fiber, satellite, etc., which are called equipment providers. Another part of infrastructure provider is responsible for connecting customer premises equipment to the core network and is called access provider.

By purchasing or renting physical network resources provided by infrastructure providers, network service operators build virtual networks according to their own needs and provide them to end users, and network service operators can also rent their own resources to other network service operators. Therefore, the resources of the virtual network may come from multiple types of providers. Network service operators are mainly responsible for the creation, modification and cancellation of virtual networks, and have the ability to monitor resources on the virtual network, obtain network operating parameters in real time, and detect failures.

End users in the network virtualization environment are similar to current users on the Internet, but they have more choices. Each terminal user can establish different connections with one or more network service operators at the same time through the mapping agent, use the network protocol of the virtual network to access the services provided by the virtual network, and obtain matching services according to business requirements.

In the software defined network slicing environment, use $G_S = (N_S, E_S)$ to represent the underlying network topology and $G_V = (N_V, E_V)$ to represent the virtual network topology. N_S and E_S respectively represent the bottom layer node set and the bottom layer link set. N_V and E_V respectively represent a set of virtual nodes and a set of virtual links. Suppose a service $s_i \in S$ is running on a virtual network. If service $s_i \in S$ is abnormal, the cause of the failure generally includes service software failure and underlying network failure. If it is a service software failure, service providers on the virtual network can quickly resolve service abnormalities through strategies such as software reconfiguration or software upgrades.

However, if the cause of the failure is an underlying network failure, the virtual network operator needs to report the service abnormality to the underlying network operator, and the underlying network operator will locate the fault. Fault management in the network management system is the core function of network management. Fault management is a series of management activities for abnormal situations in the managed network and its environment. Its work includes timely and accurate detection and location of faults, activation of fault control functions to eliminate and isolate faults or perform fault recovery. Fault management includes three stages: fault detection, fault diagnosis and fault recovery. The purpose of fault detection is to monitor whether a fault occurs in the network by collecting and analyzing network data. The purpose of fault diagnosis is to use further means to determine the root cause of the fault when a fault occurs in the

network. Fault recovery is to perform corresponding fault correction measures on the faulty node after finding the root cause of the fault.

This article mainly studies how the underlying network operator can quickly locate faults based on the service exception information reported by the virtual network operator. Considering that the underlying network operator has real-time virtual network resource allocation information to the underlying network, how to map the virtual network resources used by the service to the underlying network resources is a relatively easy problem for the underlying network service provider. This article mainly studies the fault diagnosis between the service and the underlying network.

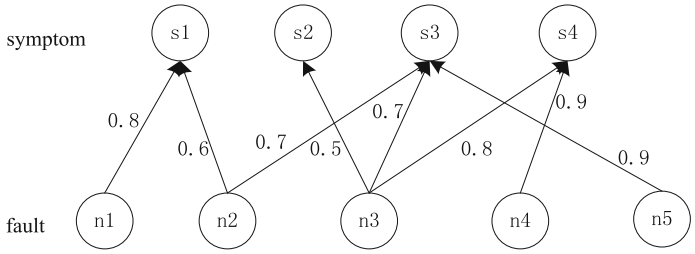

Fig. 1. Fault propagation model based on Bayesian network

Based on the fault data of the service and the underlying network, the fault diagnosis model is constructed as shown in Fig. 1. It can be seen from the figure that the Bayesian network-based fault propagation model includes symptom nodes, fault nodes, and directed lines from fault nodes to symptom nodes. A faulty node refers to the probability of a network node failure, denoted by $p(n_j)$. The symptom node refers to the probability that the service is abnormal, denoted by $p(s_j)$. The directed line from the fault node to the symptom node refers to the probability that the symptom of the service s_i is abnormal when the underlying node n_j fails, and is represented by $p(s_i|n_j)$.

This article mainly solves the problem of how to quickly infer the location of the underlying network failure after the underlying network operator receives the service exception information. Using $p(n_j|s_i)$ to represent the probability of failure of network node n_j based on an extrapolation of the known state of service s_i. Based on Bayesian inference, $p(n_j|s_i)$ can be calculated using formula (1). From the formula (1), we can see that to calculate the root cause failure of all abnormal services, we need to know the values of $p(n_j)$, $p(s_i)$, and $p(s_i|n_j)$. The more accurate these values, the more accurate the inferred underlying network node.

$$p(n_j|s_i) = \frac{p(s_i|n_j) \cdot p(n_j)}{\sum_{n_i \in N_s} p(s_i|n_j) \cdot p(n_j)} \tag{1}$$

Generally speaking, the values of $p(n_j)$, $p(s_i)$, and $p(s_i|n_j)$ can be obtained based on long-term network operation data. However, considering the software defined network environment, the network becomes more and more dynamic. Therefore, how to optimize the values of $p(n_j)$, $p(s_i)$, and $p(s_i|n_j)$ has become an effective measure to improve the performance of the fault diagnosis algorithm. For ease of description, the following

describes the values of $p(n_j)$, $p(s_i)$, and $p(s_i|n_j)$ in a formal way. For a faulty node, if $p(n_j) = 1$ it means that node n_j has a fault, it is called a faulty node; if $p(n_j) = 0$, it means that node n_j has no fault, it is called a faultless node; when $0 \leq p(n_j) \leq 1$, it is called a suspected fault node. For the symptom node, if $p(s_i) = 1$, it means that the status of service s_i is abnormal, which is called negative symptom; if $p(s_i) = 0$, it means that the state of service s_i is normal, which is called positive symptom; when $0 \leq p(s_i) \leq 1$, it is called a suspected negative symptom node.

3 Fault Propagation Model

It can be seen from the fault propagation model that faults and symptoms are the main elements of the fault propagation model. If you want to improve the performance of the fault diagnosis algorithm, the best strategy is to ensure the accuracy of the fault and symptom data. Based on this, this section analyzes and optimizes the key elements of the fault propagation model from the two dimensions of symptom optimization and fault sequencing.

3.1 Symptom Optimization

Because of its high reliability and saving network resources, dynamic routing has gradually become the main routing protocol. However, the dynamic routing strategy can easily cause the faulty node to be replaced by the available node, and the network management system cannot detect the real fault. For negative symptoms, there must be a faulty node in the node that it passes through. For a positive symptom, there is a situation where an available node is used instead of a faulty node, so there may be a faulty node in the symptom. Based on this, the steps of the optimization method for the probability of positive symptoms adopted in this paper include three sub-processes: calculating the alternative probability of each node, sorting according to the alternative probability, and symptom optimization.

According to the operation process of the dynamic routing protocol, if a node fails, the dynamic routing protocol will use the available nodes near the failed node to replace it. In order to evaluate whether a node has a substitute node, this paper uses the two-hop distance correlation of the node for evaluation. Assuming that there are nodes n_j and n_k, formula (2) can be used to calculate the two-hop distance correlation between these two nodes. $Q(n_j)$ represents the set of nodes connected to the network node n_j. It can be seen from formula (2) that the more similar the adjacent network topology of nodes n_j and n_k, the higher the possibility that nodes n_j and n_k will replace each other.

$$J(n_j, n_k) = \begin{cases} \frac{|Q(n_j) \cap Q(n_k)|}{|Q(n_j) \cup Q(n_k)|} & n_j \text{ and } n_k \text{ are not directly connected} \\ 1 & n_j \text{ and } n_k \text{ are directly connected} \end{cases} \tag{2}$$

Based on the probability of mutual substitution between network nodes, formula (3) is used to calculate the alternative probability of a node. Formula (3) is used to solve

the alternative probability of network node n_j in the network topology, where n_j^a and n_j^b represents the neighboring point of network node n_j.

$$S(n_j) = \sum_{n_j^a, n_j^b \in Q(n_j)} \left(1 - J\left(n_j^a, n_j^b\right)\right) \tag{3}$$

From the analysis of dynamic routing protocol characteristics and the calculation process of node substitution probability, it can be seen that the higher the substitutability of the node, the lower the credibility of the positive symptoms. The lower the substitutability, the higher the credibility of the positive symptoms. Therefore, according to the ascending order of the alternative probability of the network nodes, the network node set N_S^{rep} is obtained. The credibility of the positive symptoms related to the nodes ranked first in the network node set N_S^{rep} is higher. In the fault diagnosis model, the optimization method for the positive symptom connected to node n_j is formula (4). Among them, $S_{n_j}^o$ represents the o-th positive symptom node connected to the network node n_j.

$$\xi_{n_j}^o = S(n_j)^* \mathrm{p}\left(\mathrm{s}_{n_j}^o\right) \tag{4}$$

For the convenience of analysis, $\xi_{n_j}^0$ is normalized using formula (5), and the result is $\xi_{n_j}^{0-nor}$, where ξ represents the set formed by $\xi_{n_j}^0$, $\max_\xi$ represents the maximum value in the set, and $\min_\xi$ represents the minimum value in the set.

$$\xi_{n_j}^{o-nor} = \frac{\max_\xi - \xi_{n_j}^o}{\max_\xi - \min_\xi} \tag{5}$$

By calculating the credibility of the positive symptoms, the credibility of the latest positive symptoms can be obtained as formula (6). Among them, $N_{s_{n_j}^o}$ represents the set of all faulty nodes connected to $S_{n_j}^o$ in the fault propagation model. $|*|$ is used to calculate the number of elements contained in the set.

$$\mathrm{p}^{opt}\left(\mathrm{s}_{n_j}^o\right) = \frac{\sum_{\mathrm{n_j} \in N_{s_{n_j}^o}} \xi_{n_j}^{o-nor}}{\left|N_{s_{n_j}^o}\right|} \tag{6}$$

3.2 Failure Sequencing

Generally speaking, the greater the centrality of a network node and the number of links, the more times the node will be used by various services. Therefore, if an important node fails, there will be more negative symptoms. If an important node fails, but the number of related negative symptoms is small, it means that some negative symptoms are missing or the failure is a false failure. Based on this, the failure model can be optimized based on the importance of the node and the number of negative symptoms of related services.

Through the analysis of the relevant characteristics of the network nodes, it is known that the main factors related to the number of bearer services on the network nodes are the centrality of the nodes and the number of links. The centrality of a node indicates the

degree to which the node is in the center of the network. Generally speaking, the more a network node is in the center of the network, the more likely it is that the node will become a key resource of the network, thereby carrying more services. The number of node links refers to the number of edges of the node. Generally speaking, the greater the number of edges of a node, the greater the possibility of passing through the node, and thus the greater the number of services carried.

Use formula (7) to calculate the centrality of the node, and use formula (8) to calculate the number of links of the node. Among them, $n_r \in \psi(n_j)$ represents the network node collection after removing the network node n_j from the network topology. d_{rj} represents the number of links included in the shortest path between network node n_r and network node n_j. $e \in E(n_j)$ represents the edge of network node n_j, and $bw(e)$ represents the bandwidth value of the edge. It can be seen from formula (7) that the larger the value of $CC(n_j)$, the more likely the network node n_j is to be in the center of the network topology, and the greater the number of services carried on it. It can be seen from formula (8) that the larger the value of $DC(n_j)$, the more resources of network node n_j, and the greater the number of services carried on it. Through the normalized formula (9), the total resource Ω_{n_j} of the network node n_j can be obtained.

$$CC(n_j) = \frac{1}{\sum_{n_r \in \psi(n_j)} d_{rj}} \tag{7}$$

$$DC(n_j) = \sum_{e \in E(n_j)} bw(e) \tag{8}$$

$$\Omega_{n_j} = \frac{CC(n_j) - \min_{CC}}{\max_{CC} - \min_{CC}} + \frac{DC(n_j) - \min_{DC}}{\max_{DC} - \min_{DC}} \tag{9}$$

The proportion of the resources of the network node n_j in the total resources is shown in formula (10). Among them, $n_i \in N_s$ represents all network nodes in the network topology. The proportion of negative symptoms related to network node n_j in the total negative symptoms is shown in formula (11). Among them, $S_{n_j}^-$ represents the negative symptoms related to network node n_j, and S^- represents the set of negative symptoms of all network nodes.

$$\eta_{n_j} = \frac{\Omega_{n_j}}{\sum_{n_i \in N_s} \Omega_{n_i}} \tag{10}$$

$$\sigma_{n_j} = \frac{\left|S_{n_j}^-\right|}{\left|S^-\right|} \tag{11}$$

Based on the above analysis, formula (12) can be used to calculate the fault credibility β_{n_j} of network node n_j. Among them, β_{n_j} represents the reliability of the fault. The closer the value is to 1, the higher the reliability.

$$\beta_{n_j} = \frac{\eta_{n_j}}{\sigma_{n_j}} \tag{12}$$

4 Algorithm Description

The fault diagnosis algorithm based on service characteristics under software defined network slicing (FDAoSC) proposed in this paper includes three processes: building an initial fault propagation model, optimizing fault propagation model, and fault set diagnosis. In the step of constructing the initial fault propagation model, the underlying network service provider first receives a collection of abnormal services from the virtual network, and then builds a fault propagation model of the underlying network and abnormal services based on the mapping relationship and the virtual network resources occupied by the abnormal services. In the optimization step of the fault propagation model, the positive symptom values in the fault propagation model are first optimized, and then the fault credibility of the network nodes is calculated and arranged in descending order. In the fault set diagnosis step, first use the sorted fault credibility set to construct a suspected fault propagation model, and secondly determine the fault set based on the maximum coverage algorithm.

The two steps of constructing the initial fault propagation model and optimizing the fault propagation model have been described in the previous section. The following describes the diagnosis steps of the fault collection. Fault set diagnosis includes two subprocesses: constructing fault set and selecting faulty node based on maximum coverage. When constructing the fault set, assume that the number of simultaneous faults is k. Therefore, a set of k suspected faults consisting of 1 to k faulty nodes is constructed at the same time. The set of k suspected failures is denoted by $H = \{n_1, n_2, \ldots, n_k\}$, where the suspected failure nodes are the k suspected failure nodes ranked in the front of the failure credibility set.

In order to evaluate the explanation ability of the suspected fault set $H = \{n_1, n_2, \ldots, n_k\}$ for abnormal services, the explanation ability of the fault set is defined as $EXP(H,S)$, and the calculation is carried out using formula (13). $\prod_{n_j \in H} P(n_j)$ represents the probability that the failures of the suspected failure set $H = \{n_1, n_2, \ldots, n_k\}$ are all failures. $\prod_{s_i \in S} \left(1 - \prod_{n_j \in H} \left(1 - P(s_i|n_j)\right)\right)$ means that any symptom $s_i \in S$ can find at least one failed network node in the suspected failure set $H = \{n_1, n_2, ..., n_k\}$. By calculating the k suspected failure sets, the suspected failure set $H = \{n_1, n_2, ..., n_k\}$ with the largest value of $EXP(H,S)$ is taken as the final failure set.

$$EXP(H, S) = \prod_{n_j \in H} P(n_j) \times \prod_{s_i \in S} \left(1 - \prod_{n_j \in H} \left(1 - P(s_i|n_j)\right)\right) \tag{13}$$

5 Performance Analysis

5.1 Network Environment

The network topology in the experimental environment is generated using GT-ITM [7] tool. The generated network topology includes two types: virtual network and underlying network. The network nodes of the virtual network obey the uniform distribution of (5, 15), and the network nodes of the underlying network increase from 100 to 500. The

resource allocation from the virtual network to the underlying network uses the classic algorithm [8].

In terms of network node failure simulation, the prior failure probability of the bottom node is set to obey the uniform distribution of [0.001, 0.01]. The state of the network node is updated once at an interval of 20 s to simulate the dynamic characteristics of the underlying network. In terms of algorithm comparison, compare the FDAoSC algorithm in this paper with the fault diagnosis algorithm based on resource bearing relationship (FDAoRBR). Among them, the algorithm FDAoRBR establishes a fault diagnosis model by analyzing the relationship between resource bearers and associating service status with underlying network resources. In terms of algorithm comparison indicators, the analysis is carried out from three aspects: the accuracy rate of fault diagnosis, the false alarm rate, and the diagnosis time. Accuracy refers to the proportion of identified faults in real faults. The larger the value, the more faults identified by algorithm diagnosis. The false alarm rate refers to the proportion of the identified false faults in the identified faults. The smaller the value, the higher the authenticity of the faults diagnosed by the algorithm. Diagnosis duration refers to the duration of the algorithm from receiving the service status to outputting the fault set. The smaller the value, the better the algorithm performance.

5.2 Performance Comparison

The comparison result of the accuracy of the fault diagnosis algorithm is shown in Fig. 2. From the figure, it can be seen that the network size has a small effect on the diagnosis accuracy of the two algorithms, and the accuracy of the algorithm in this paper is higher. It shows that this paper optimizes the symptom set and the fault set, thereby improving the accuracy of the fault diagnosis model.

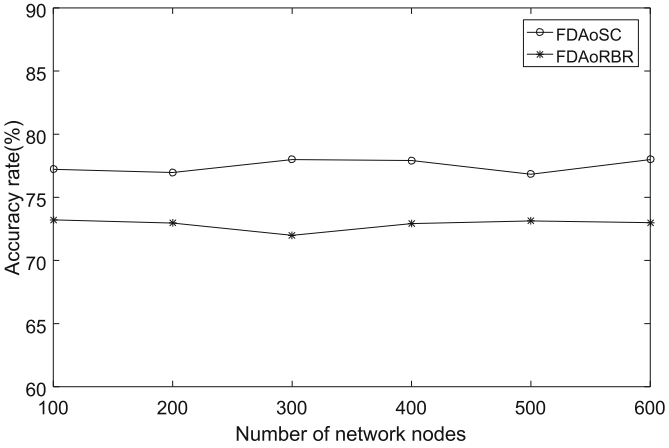

Fig. 2. Comparison of accuracy rate

The comparison result of fault diagnosis false alarm rate is shown in Fig. 3. It can be seen from the figure that the two algorithms have achieved relatively stable diagnosis

results under different network scales. The false alarm rate of the algorithm in this paper is lower than that of the traditional algorithm. This is because the algorithm in this paper evaluates characteristics such as symptom status and fault credibility, and better solves the problem of inaccurate fault propagation model caused by dynamic environment. The algorithm in this paper improves the accuracy of the fault diagnosis model data, thereby reducing the false alarm rate.

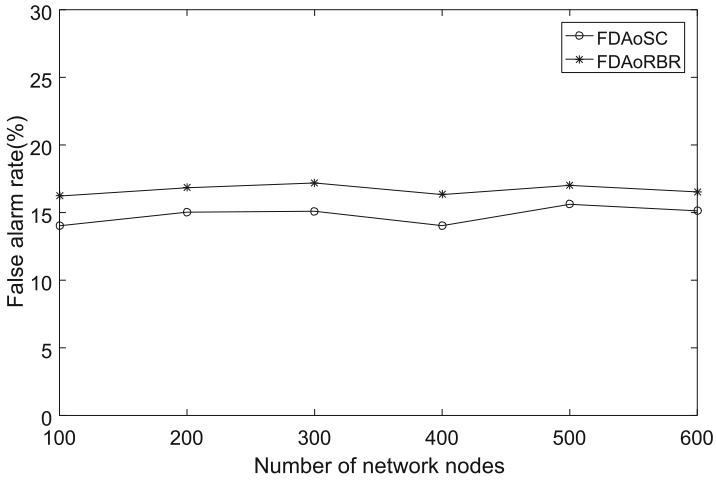

Fig. 3. Comparison of false alarm rate

The result of the comparison of the fault diagnosis duration is shown in Fig. 4. It can be seen from the figure that as the network size increases, the diagnosis time of the two algorithms increases faster. Compared with the existing algorithm, the diagnosis time of the algorithm in this paper has increased slightly. This shows that the algorithm in this paper optimizes faults and symptoms, and there is a certain time overhead. However, the algorithm in this paper constructs a set of suspected faults based on fault credibility, and the time to infer the fault is shorter.

6 Conclusion

The software defined network slicing technology makes the relationship between faults and symptoms in the fault diagnosis algorithm more complicated, resulting in a decrease in the accuracy of the fault diagnosis model and the performance of the fault diagnosis algorithm. To solve this problem, this paper proposes a fault diagnosis algorithm based on service characteristics under software defined network slicing. The algorithm includes three processes: constructing an initial model of fault propagation, optimizing the fault propagation model, and fault diagnosis. The algorithm receives a collection of abnormal services from the virtual network. Based on the mapping relationship and the virtual network resources occupied by abnormal services, the fault propagation model of the underlying network and abnormal services is constructed. The positive symptom

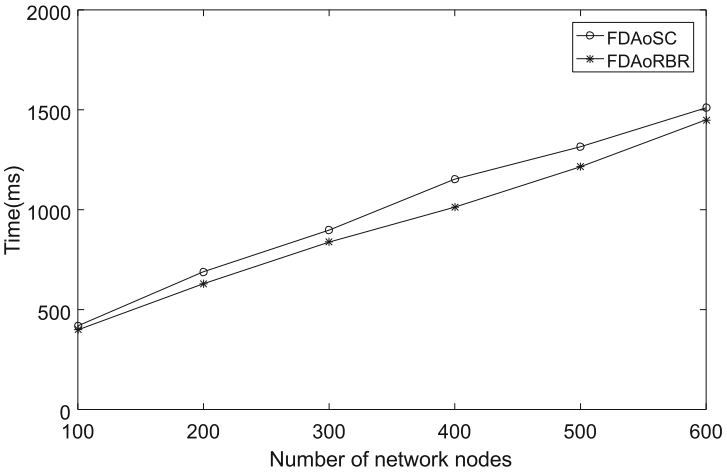

Fig. 4. Comparison of time

value in the fault propagation model of the algorithm team is optimized to improve the fault credibility of the network node. The algorithm uses the sorted fault credibility set to construct a suspected fault propagation model, and uses the maximum coverage algorithm to determine the fault set. The algorithm optimizes the symptom value in the fault propagation model based on the substitutability of the node, establishes a mathematical model of the importance of the node and the number of symptoms of the fault, and optimizes the fault propagation model. The experimental part verifies that the algorithm in this paper improves the accuracy of fault diagnosis.

When evaluating the importance of nodes, this article only considers the centrality of nodes and the number of links. The next step is to enrich this content and analyze the node attributes such as the approximate ideal ranking method and the analytic hierarchy process to better improve the algorithm performance.

Acknowledgement. This work is supported by science and technology project from State Grid Jiangsu Electric Power Co., Ltd: "Technology Research for High-efficiency and Intelligent Cooperative Wide-area Power Data Communication Networks (SGJSXT00DDJS1900168)".

References

1. Kaizhi, H., Qirun, P., Quan, Y., et al.: A virtual node migration method for side channel risk perception. J. Electron. Inf. Sci. **41**(9), 2164–2171 (2019)
2. Wu, B., Ho, P.H., Tapolcai, J., et al.: Optimal allocation of monitoring trails for fast SRLG failure localization in all-optical networks. In: Proceedings of 2010 IEEE Global Telecommunications Conference, Miami, USA, pp. 1–5 (2010)
3. Dusia, A., Sethi, A.S.: Recent advances in fault localization in computer networks. IEEE Commun. Surv. Tutor. **18**(4), 3030–3051 (2016)
4. Rish, I., Brodie, M., Ma, S., et al.: Adaptive diagnosis in distributed systems. IEEE Trans. Neural Netw. **16**(5), 1088–1109 (2005)

5. Jin, R., Wang, B., Wei, W., et al.: Detecting node failures in mobile wireless networks: a probabilistic approach. IEEE Trans. Mob. Comput. **15**(7), 1647–1660 (2016)
6. Yu, Y., et al.: Falcon: differential fault localization for SDN control plane. Comput. Netw. **162**(106851), 1–15 (2019)
7. Zegura, E.W., Calvert, K.L., Bhattacharjee, S.: How to model an internetwork. In: Proceedings of IEEE INFOCOM (1996)
8. Yu, M., Yi, Y., Rexford, J., Chiang, M.: Rethinking virtual network embedding: substrate support for path splitting and migration. ACM SIGCOMM CCR **38**(2), 17–29 (2008)