A network application availability assessment method for cloud virtualized network based on network evolution

Juxing Zhu, Ning Huang, Sitong Caihuang, and Junliang Wang,

***Abstract*—Application availability assessment is an important method to ensure the operation of cloud virtualized network. Due to the adaption of network functions virtualization (NFV) based on virtualized technology, the application of cloud virtualized network is not a chain of certain physical devices, but a chain of VNF dynamically depolyed in servers, i.e., the service function chain (SFC). The current availability evaluation methods for SFC can be mainly summarized as methods based on the tradition reliability evaluation method, system-state based methods, component-state based methods and the comprehensive method that integrate these methods hierarchically. Although these methods could evaluate the reliability of the application through certain physical devices, it would be very hard to use these methods to evaluate the availability of these dynamical virtualized VNFs for these methods do not describe the dynamic mapping of VNFs and physical devices. Therefore, a network application availability assessment algorithm based on network evolution is proposed in this paper. The network state is described by the attributes of nodes, links, VNFs and applications in the network evolution object modelling. The state points in a period of time which cause the changing of the system state are found in the network evolution condition. The state of application is changed according to the network evolution rule when after the system state changed and the application availability is calculated by the proposed algorithm. We have analyzed the complexity and convergence of the algorithm, and the results show that the calculation results of the algorithm in this paper are convergent, and the calculation complexity is O (to be determined), which solves the combination explosion problem of the existing evaluation model. Then, a comparison based on the RBD method is used to verify the correctness of the calculation results of the method proposed in this paper through a small network case.**

***Index Terms*—Cloud virtualized network, Network function virtualization, Application reliability, Network evolution model, Service function chain**

I. Introduction

WITH the increasing demand of network in different scenarios, the VNF technology that enable the Network Functions (NFs) to be deployed in generic servers give out a solution to design and deploy different kinds of network application. At this time, the network application is no longer the static route (like when we dial the phone to a friend, the route is our closet base station, then the certain device in the call center, then the closet base station to the friend, and finally his/her phone). The NF of that device in the call center is now dynamically depolyed in the data center network for a better resource utilization, and the network operators could combine different VNF together to form a SFC easily.

In order to provide a better Service Level Agreement (SLA) for the user and make more profit, the network operators need to specify the Service Level Indicators (SLI)[**?**]. Even though there are lots of SLIs (such as the time delay, bandwidth and jitters), the availability is one of the most important indicators. According to 3GPP, some application in 5G network requires five 9s to seven 9s(i.e., 99.999% to 99.9999%). Therefore, different kinds of optimized SFC placement and orchestration methods are proposed[**?**], [**?**], [**?**], [**?**].

Though the placement and orchestration method for SFC has been expensively studied, the availability assessment method has not been systematically studied. At present, the researchers mainly use three kinds of method:

1.The traditional reliability based method. This kinds of methods mainly include the Reliability Block Diagram (RBD) and Fault Tree Analysis (FTA) method.In [**?**], the author uses a two-level hierarchical approach to build two host system models, non-virtualized and virtualized. The fault tree is used at a higher level, and CTMC is used to represent a lower level sub-model. In [**?**] , the authors studied the reliability assessment of a series of network nodes implementing SFC managed by virtualization infrastructure manager (VIM). The authors use a two-layer model. The upper model is RBD, the RBD describes the dependencies between the architecture components. The lower model uses the random reward network (SRN), which simulates the behavior of each component, including repair and migration, failure, etc. The steady-state reliability analysis is used to characterize the minimum configuration of the entire system. In these studies, fault trees and RBD are used as upper-level modeling. These reliability analysis methods are convenient to analyze the logical relationship between system components. However, these method can only describe the simple system that each subsystem is not highly correlate with each other.

2.The system-state based method. This kinds of methods mainly include the Markovian-Chain-based method. In [**?**], the authors model both the failure of the base station (BS) and the transition time of the system state as an exponential distribution. On the basis of this assumption, a CTMC model is established for BS reliability analysis. In [**?**], the authors

Juxing Zhu, Ning Huang and Junliang Wang are with the School of Reliability and System Engineering, Beihang University, Beijing 100191, China, also with the Key Laboratory of Science & Technology on Reliability & Environmental Engineering, Beihang University, Beijing 100191, China(email:zhujuxing@foxmail.com

Sitong Caihuang is with

Manuscript received April 19, 2005; revised August 26, 2015.

use a multi-state system (MSS) to evaluate the availability of multi-tenant SFC infrastructures. They established Universal Generating Function (UGF) by analyzing continuous-time Markov chains. This kind of method can describe the system state transition process of the system and solve the probability distribution of each state. But the scale and complexity of the model will increase with the increase of the system topological relationship , and the difficulty of solving high-order systems will be greatly increased.

3.The component-state based method. This kinds of methods mainly include the Petri-Network-based method. M.Di Mauro et al. formally model the dynamic behavior of a VNF based on the Stochastic Reward Network[**?**], [**?**]. Subsequently, Besmir Tola and others based on the Stochastic Activity Network (Stochastic Activity Network), described the behavior of the three main nodes in the cloud virtualized network: Virtualization Technology Facility (NVFI), VNF, and Management Controller (MANO). The reliability evaluation model [**?**], [**?**] is given. This Petri net-based model has good applicability when describing a single event (a node failure or repair) in the network. However, this type of model assumes that the various events and states of different nodes are independent of each other, which is not true in the case of multiple failures in the network. Therefore, when this type of model further evaluates large-scale cloud-based virtualized networks that may have multiple points of failure, the problem of high reliability of their services will also arise.

In the NFV architecture proposed by the European Telecommunications Standards Institute (ETSI) [**?**], [**?**], a cloud-based virtualized network includes the resource pool that provides computing, storage, and transmission functions, as well as The Network Cloud Control Engine (NCE), which controls the status of various virtual machines and the deployment of services in the entire network, is implemented through the relevant processes of the corresponding virtual machines deployed on standard server nodes [7]. Therefore, whether it is the hardware failure of the server itself, or various software failures that cause the failure of the VNF deployment process, it will affect the reliability of network services. Current evaluation methods mostly ignore the impact of software faults on the reliability of VNFs in cloud-based networks, and directly correspond to the physical components and VNFs one-to-one; some studies believe that each VNF component is independent of each other, All VNFs can be modeled separately and independently through formal language, ignoring the impact of multi-point failures of different attributes on the entire network, and then there will be a certain deviation in the evaluation value of the entire network reliability of the cloud virtualized network .

In order to solve the above problems, this article will propose an availability assessment method of cloud virtualized network, and calculate the availability value of all application. Due to limited space, the reliability of the business considered in this article is mainly considered at the level of whether the business is connected. The main contributions of this paper can be summarized as follows:

1) The network application availability assessment method for cloud virtualized network based on network evolution is proposed. This network evolution method describe the dynamic behavior of the cloud virtualized network and could be used to analyze the other characteristic (for example, failure propagation) of this kind of dynamic virtualized network. The system state is generated by the program according to the network evolution condition and rule, so that the complete system state space is not needed to be analyzed by people before calculating the availability of application. Thus the complexity of this method is relatively low. And we can assess multiple application deployed on the same network at the same time, which to the best of our knowledge, is hardly done by the other method.

2) The convergence and the correctness of the availability result calculated by this method is validated. The result shows that if the parameter is correctly chosen, the availability value converge below a certain error, and is in accordance with the availability calculated by RBD.

The rest of this article is organized as follow.

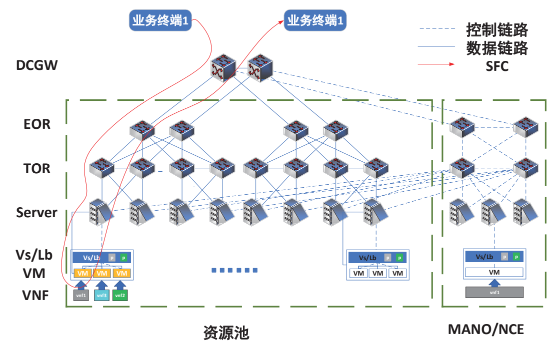

Fig. 1. Schematic diagram of cloud virtualization network structure

II. Network Evolution Modelling

A schematic diagram of the structure of a typical cloud-based virtualized network is shown in Fig. 1. The network structure is a fat tree structure. The network terminal sends requests and receives data through two multiplexed data center gateways (DCGW). There are two layers of switches in the network, inter-rack switches (EOR) and top-of-rack switches (TOR), which receive and send data and control information between blade servers. Each server is virtualized to form several virtual machines (VM) and a virtual switch/responsible splitter (Vs/Lb). The VM carries a special virtual network function (VNF), and Vs/Lb is responsible for acting as a switch between different VMs. A service (or SFC) is a path between several VNFs. All servers are divided into resource pools and MANO/NCE. The servers in the resource pool are responsible for carrying different VNFs and realizing service interruption requests. The server on MANO/NCE is responsible for VM management.

The network evolution model of the cloud-based virtualized network is shown in Fig. 2. At the initial moment, all components in the network are normal. At time t_1, a VM node fails, and the VNF carried on the VM node has a backup node. At this time, the service path will be transferred to the standby

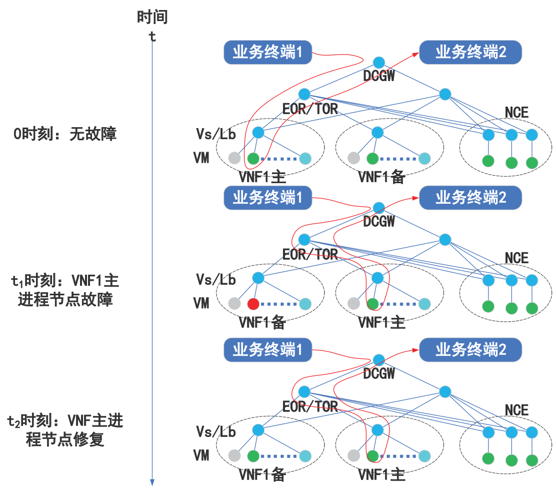

Fig. 2. Network evolution model of cloud-based virtualized network

node, and the original node will wait for repair until the repair is completed at t_2.

The network evolution model needs to describe the object of the network evolution. This object not only needs to describe the infrastructure resources of the network physical layer, but also the basic attributes of the network service.

A. Modeling of Cloud and Virtualized Network Evolutionary Objects

1) Infrastructure layer modeling: For cloud-based virtualized networks, the infrastructure layer modeling mainly includes three aspects, namely, network node information, network link information, and network failure mode information.

Network node information refers to the basic components of the network composed of hardware devices such as Server, VMM, VM, and processes or virtualized software units in the network. In a cloud-based virtualized network, the node types of each network node are heterogeneous, so different network node types need to be described. Here, we divide the network node types into 4 categories: Server nodes, VMM nodes, VM nodes, and Proc nodes (specifically, Proc1, Proc2, and Proc3 nodes correspond to the three different types of services loaded on them). At the same time, the state of the node is used to characterize whether the current state of the node is faulty. Examples of node information are shown in I, and the red part is an example of table content. For cloud-based virtualized networks, we found through research on relevant information provided by Huawei that network failures mainly occurred on network nodes. At the same time, a network node may have multiple independent failure modes, which will affect the design of subsequent network evolution conditions.

Network link information refers to the flow path between different nodes in the network. There are two links here, one is the north-south link for sending data from the upper node to the lower node, and the other is the east-west link for mutual control of time and data transfer between nodes of the same kind (for example, for Nway services). That is, the VM node of its business deployment needs to exchange information

TABLE I
CLOUD VIRTUALIZATION NETWORK NODE INFORMATION

Symbol	Discription
NodeID	Describe the unique identifier of the node
NodeType	Describe the type of node
NodeFailType	The failure mode type of the node
NodeFailMTBF	Mean time to failure of the failure type (h)
NodeFailFDR	Detection rate after failure
NodeFailFDT	Fault detection time (h)
NodeFailAFRR	Probability of automatic repair for software faults
NodeFailAFRT	Automatic repair time for software faults (h)
NodeFailMTTR	Mean time to repair
NodeFailSR	Switch Probability
NodeFailST	Switch Time
NodeState	Indicates whether the node has failed.
NodeIdle	Indicates whether the node is idle
Tasp	Time of calling for check(h)
Tchk	Check time(h)

TABLE II
CLOUD VIRTUALIZATION NETWORK LINK INFORMATION

Symbol	Discription
EdgeID	Describe link unique identifier
EdgeSourceNode	The source node of the link
EdgeDestinationNode	The sink node of the link
EdgeCapacity	Link capacity (GBp/s)
EdgeTraffice	Link flow (GBp/s)

TABLE III
CLOUD VIRTUALIZATION NETWORK APPLICATION INFORMATION

Symbol	Discription
ApplicationID	Unique identifier describing the business
ApplicaitonVNFs	Describe the SFC called by the application
ApplicationWorkPath	Describe the current application link
ApplicationAvail	The availability of the application
ApplicationDownTime	Cumulative unavailable time of business
ApplicationStatus	Describe whether the current business is normal
ApplicationInitTraffic	Record initial traffic
ApplicationTraffic	Describe the relative value of current traffic
ApplicationThreshold	Describe the minimum flow threshold

with the VM node of the flow balancer). For each link, the information of its source and sink nodes is required. At the same time, information about its link capacity and flow is needed. The data dictionary of the link information is shown in II.

2) Network Application layer modeling: In a cloud-based virtualized network, different network elements (Network Function, NF) are combined to form a network service (Netwrok Service, NS), and the network service is a service chain formed by a network service used by two end users (Service Function Chain, SFC). In order to solve the availability of the service, it is necessary to model the network services invoked by the service and the basic network elements occupied by each network service. The business information of the NFV network can be represented by IV.

TABLE IV
CLOUD VIRTUALIZATION NETWORK VNF INFORMATION

Symbol	Discription
VNFID	The unique identifier of the network VNF
VNFBackupType	Service backup types
VNFDeployNode	Master nodes of the VNF
VNFBackupNode	Slayer nodes of the VNF
VNFFailSR	Switch rate
VNFFailST	Switch time
VNFSwitchPath	Switch Path
VNFWait	The state of the VNF

Services will call different VNFs. These VNFs are divided into three different types according to their backup conditions: non-backup services, cold backup services, and hot backup services. They are deployed on different types of VM nodes. For network services, since this project mainly focuses on whether the service is interrupted, the service attributes can be designed as shown in **??**.

B. The evolution conditions of cloud virtualised network

Network evolution conditions are mainly caused by the interruption of top-level network services under different failure modes of different devices. At the same time, the network failure of the top node will cause the failure of the bottom node according to a certain probability. At the same time, network nodes will be repaired due to automatic repair and manual repair. Therefore, the main ideas for the design of network evolution conditions are as follows:

1. For each network node, it is assumed that the time probability distribution of failure, automatic repair, and manual repair are all exponentially distributed. First, according to the different failure modes occurring on it, the node state sequence corresponding to the failure mode is generated respectively. For example, for the H1 node, there are two failure modes. According to the MTBF of failure mode 1, the duration before a failure is generated. Then determine whether the fault is detected. If it is not detected, the fault will exist until the inspection time (168 hours); if it is detected, it will be judged whether it is automatically repaired or manually repaired according to the probability of automatic repair, and the repair time will be given. . Finally, the failure state sequence of failure mode 1 is synthesized.

2. For all failure modes of each node's failure, the failure state sequence of the node is given, that is, the failure state sequence of all failure modes is combined.

3. Give the node that fails at each moment.

C. The evolution rules of cloud virtualised network

1) DCGW/EOR/TOR: When a switch node fails, the service traffic of different services carried by it is interrupted, and the service carried by it experiences a failure with a duration of NodeFailST.

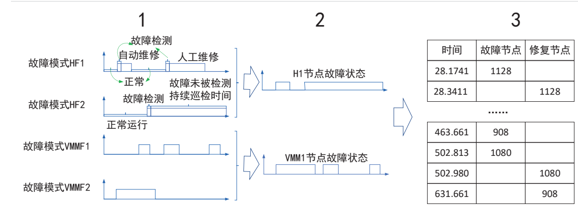

Fig. 3. The evolution conditions of cloud virtualised network

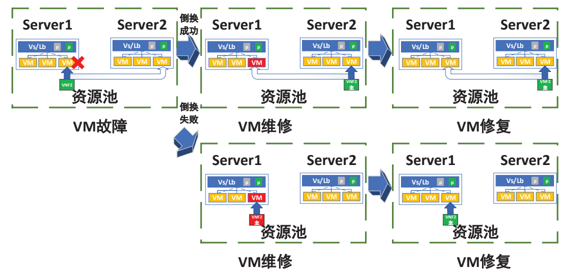

Fig. 4. The cold backup VNF process fails

2) Server: When a Server node fails, all its downstream software nodes fail. At this time, the migration of all VMs and proc nodes hosted on it will be triggered. At this time, if the migration is successful, all nodes and services on it experience a failure of NodeFailST time, and the Server node enters the maintenance state, and becomes an idle Server node after repair. If the migration fails, or there is no idle server, all nodes on it experience a failure time of NodeFailMTTR.

3) Vs/Lb: When a Vs/Lb node fails, the traffic of all VM nodes and services in the server is interrupted. Since Vs/Lb contains forwarding and control functions, all VM nodes and business traffic cannot occur

4) VM: When a VM node fails, different maintenance and protection strategies will be determined according to the type of the node and its subordinate VNF.

For a VNF without backup, it waits for the original fault to be repaired after it fails, and there is no additional rule. At this time, the failure time is the duration of the failure.

For a cold backup VNF, when the main VM node fails, it is judged whether the switchover can be successful. If the backup VM node does not fail and the switchover is successful, the failure time is the switchover time, and the primary node becomes the standby node after the failure is repaired; if the switchover fails or the standby node fails, wait for the failure of the primary node to disappear, and the failure time is the time of the primary node. Fault repair time.

For a hot backup VNF, when any of its working VM nodes fails, it is judged whether the switchover is successful. If the switch is successful, the traffic of the node is switched to the other two nodes, and the switch is performed when the node fails. At this time, the VNF fails with 2 NodeFailST; and when the switch fails, the VNF fails, and the business failure time It is the failure recovery time of the node.

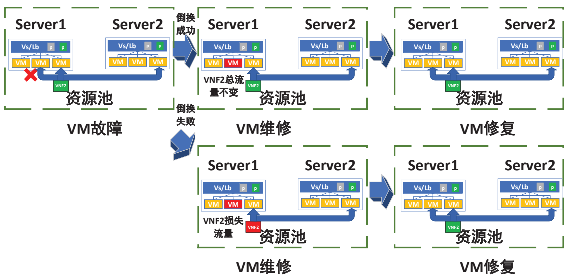

Fig. 5. The hot backup VNF process fails

III. Reliability Evaluation of Cloud Virtualization Network

The algorithm flow of cloud virtualization network reliability evaluation is shown in Figure **??**.

The overall reliability calculation module of the network starts with the input of the cloudized virtual network, business information, calculation times and calculation cycle data from the very beginning. At this time, the software begins to model the evolution object and initialize it, and automatically generate the evolution state of the fault data according to the network information, generate the set of faulty nodes at each time, and the set of restored nodes at each time.

The loop starts at this time, and each loop is a Monte Carlo simulation.

First traverse the set of recovery nodes. For the business involved in each node, if the cumulative failure time of the business is non-zero, the failure occurrence time is added to the cumulative failure occurrence time of the business.

After completing the traversal of the restored node, start traversing the failed node, and according to the type of the node, determine the processing rules after the node failure, and jump to the corresponding program, if the type of the failed node is DCGW/EOR/TOR, etc., then jump to Switch node fault handling module.

After traversing the faulty node, the reliability calculation of all services is started. The reliability of the i-th service is $1-(\sum App\_unavailtime^{i}(t)/T)$, and the reliability of the entire network is $R_{Application}(T)=\sum_{i}^{N_{Application}} w_i R_A^i(T)$ At this time, a simulation cycle is completed, and the cycle counts i+1, and loops until i reaches the expected number of calculations input.

After completing the simulation of the expected number of calculations, the business reliability of the i-th service is $R_A^i(T)/N$, and the reliability of the entire network is $R_{Application}(T)/N$.

IV. Case Analysis and Discussion

In this part, we first constructed a typical cloud-based virtualized network case, in which a certain number of VNFs and network services were randomly deployed, and then selected typical network services to analyze the stability of the results of the calculation model, and use this article The proposed model calculates the reliability of a single network service and the entire network service.

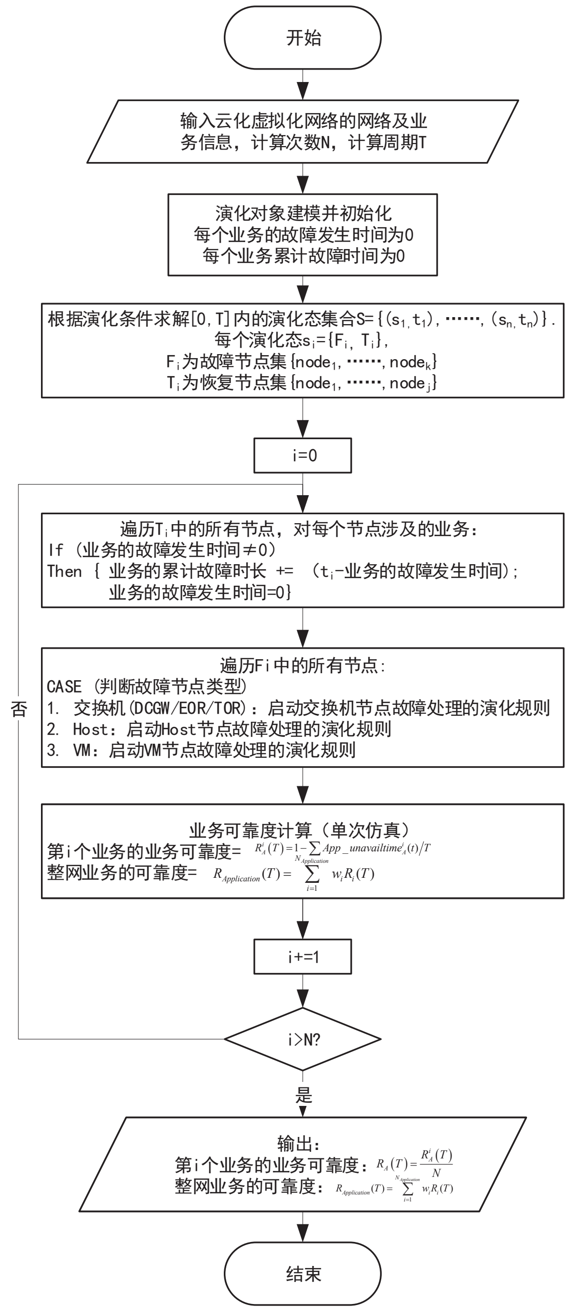

Fig. 6. Reliability evaluation model

In this case, each node sets its node parameters according to its node type. The relevant parameters of each type of node are shown in Table 5.

In order to compare the traditional reliability calculation methods, we have designed a small network case (as shown in Figure 14) for calculation. Two types of VNF are deployed in the figure. VNF1 is a 2 Way backup VNF, and VNF2 is a backup VNF of the active backup type. There are two services in the network.

As shown in Figure **??**, we have constructed a cloud virtualization network model consisting of 1 DCGW node,

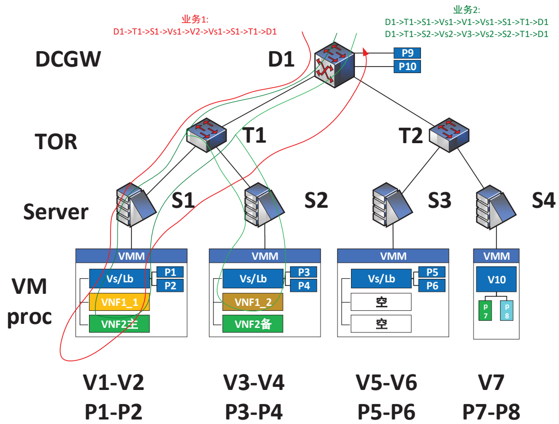

Fig. 7. Small network case topology

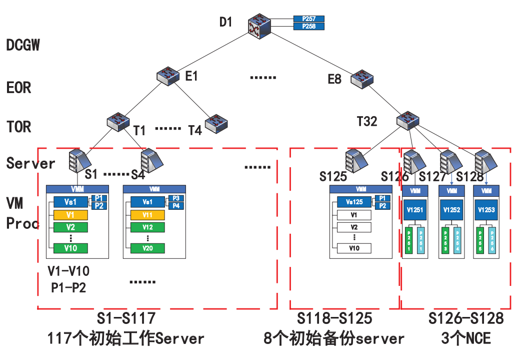

Fig. 8. Large network case topology

TABLE V
CASE PARAMETER SETTING

Type	MTBF	FDR	FDT	AFRR	AFRT	MTTR
DCGW	50	1	0s		2h	
TOR	50	1	0s		2h	
Server	50	1	0s		2h	
Vswitch	2	0.9	0s	0	10min	2h
VM	2	0.9	0s	0	10min	2h
Proc	20	0.9	0s	0	10min	2h

TABLE VI
CASE PARAMETER SETTING

Type	MTBF	FDR	FDT	AFRR	AFRT	MTTR
DCGW	50y	1	15s			2h
TOR	50y	1	15s			2h
Server	50y	1	15s			2h
Vswitch	2y	1	240s	0.9	10m	2h
VM	2y	1	240s	0.9	10m	2h

8 EOR nodes, 32 EOR nodes and 128 Server nodes. Among them, there are 125 service servers, and each server has 10 VMs; 3 servers are used as NCE services.

In this network, 147 VNFs are randomly deployed on 1170

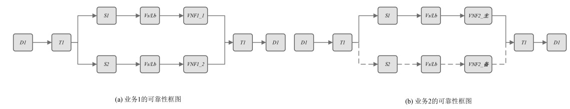

Fig. 9. Reliability block diagram analysis

VMs on S1-S117, which are divided into three categories: 1) 60 mainframe VNFs; 2) 29 active and standby VNFs; 3) 58 2 way type VNF. The specific parameters of VNF are shown in Table 9 in the appendix.

We randomly select VNFs to combine to form 100 businesses. Among them: 1) 30 services including only 1 VNF; 2) 40 services including 2 VNFs; 3) 30 services including 3 VNFs. The specific parameters of the business are shown in Table 10 in the appendix.

A. Algorithm correctness analysis

In the traditional method, the reliability of the virtual network infrastructure (NFVI) and virtual link (Vlink) deployed by the VNF and VNF is often calculated through the RBD method. According to the ETSI report [7], two business reliability block diagrams in two cases can be given as shown in **??**.

At this time, the reliability of the two services can be expressed as:

$$\begin{aligned} R_{app_1} &= R_{D_1} * R_{T_1} * (1-(1-R_{S_1} * R_{Vs} * R_{VNF1\_1}) \\ &\quad *(1-R_{S_2} * R_{Vs} * R_{VNF1\_2})) \qquad (1) \\ R_{app_2} &= R_{D_1} * R_{T_1} * (R_{S_1} * R_{Vs} * R_{VNF} \\ &\quad +(1-R_{S_1} * R_{Vs} * R_{VNF2\_M}) * p_s * R_{S_2} \\ &\quad *R_{Vs} * R_{VNF2\_s}) \qquad (2) \end{aligned}$$

According to the case parameter settings, because it is difficult to dynamically represent the network link, the initial link of the service is first used to estimate the reliability of the service virtual link. At this time:

$$\begin{aligned} R_{D_1} &= R_{T_1} = R_{S_1} = R_{S_2} = \frac{50*365*24}{50*365*24+2} \\ &= 0.9999954338108045 \qquad (3) \\ R_{Vs/Lb} &= R_{VNF1\_1} = R_{VNF1\_2} = R_{VNF2\_M} = R_{VNF2\_S} \\ &= \frac{2*365*24}{2*365*24+(0.1*2+0.9*(10/60))} \\ &= 0.9999800232301296 \qquad (4) \end{aligned}$$

With the switching probability $p_s = 0.9$, the reliability of the two services can be obtained as:

$$R_{app_1} = 0.9999908667951362, R_{app_2} = 0.9999879560119541 \qquad (5)$$

The two service reliability values calculated using the network evolution method proposed in the article are shown in the table (calculation period $T = 200years$):

TABLE VII
CASE PARAMETER SETTING

N	10	50	100	200	500
App1 Reliability	0.999980	0.999989	0.999990	0.999990	0.999990
App2 Reliability	0.999913	0.999941	0.999933	0.99994	0.99994

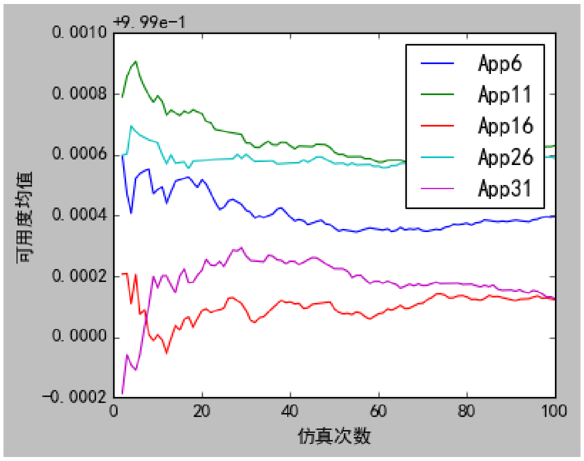

Fig. 10. Variation of the mean availability with the number of simulations

B. Algorithm convergence analysis

Since some parameters of the factors affecting the network evolution conditions in this article are randomly distributed, we take the average value to estimate the subsequent business reliability. According to the central limit law, the mathematical expectation R_i and variance δ^2 of the independent random variable business reliability $\bar{R}_i$ for n simulations, then:

$$\lim_{n\to\infty} P\left\{\frac{\overline{R_i}-R_i}{\sigma-\sqrt{n}}<t_\alpha\right\}=\int_{-\infty}^{t_\alpha}\frac{1}{\sqrt{2\pi}}e^{-t^2/2}dt=\Phi\left(t_\alpha\right) \tag{6}$$

At this time, the absolute error of the simulation is:

$$\varepsilon=\frac{\lambda_\alpha\sigma}{\sqrt{n}} \tag{7}$$

We first analyzed the average availability and simulation errors of the selected five businesses (App6, App11, App16, App26, and App31). Taking T=50 years and a confidence level of 95%, the changes in the business average and the simulation absolute error with the number of simulations are plotted, and the error threshold is $10^{(}-4)$. It can be seen that for these 5 services, as the number of simulations increases, the mean value gradually converges; when the number of simulations is 6, 18, 53, 73, and 77, the results can be satisfied with a confidence level of 95%. Simulation accuracy requirements. It can be seen that the average business reliability calculated by this algorithm gradually converges as the number of calculations increases.

C. Influencing factors of Application reliability

Subsequently, we selected services with different logical path lengths and analyzed the relationship between the simulation error and the number of calculations and the single

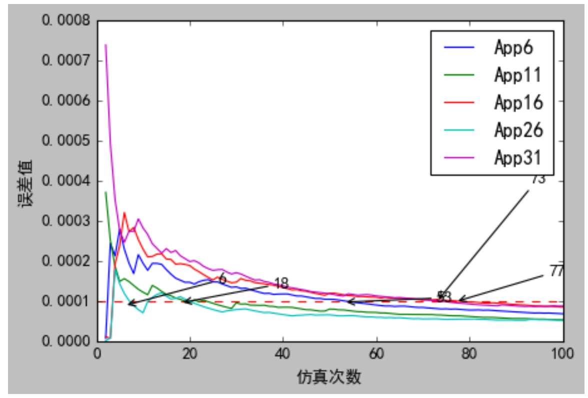

Fig. 11. Variation of error with simulation times

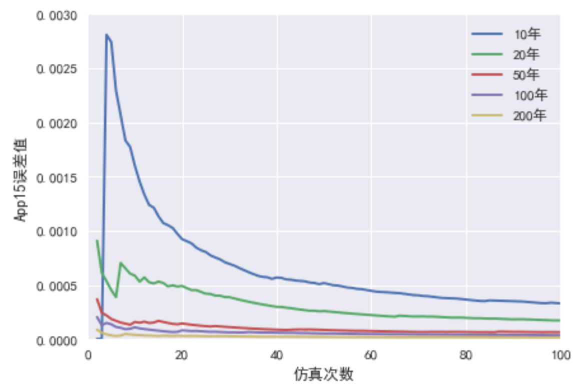

Fig. 12. When the service (App15) uses 1 VNF, the relationship between the error and the number of calculations and the single calculation cycle

TABLE VIII
THE CALCULATION RESULT AND CALCULATION TIME OF THE WHOLE NETWORK SERVICE RELIABILITY WHEN N=100, T=[10,20,50,100,200]

T(year)	10	20	50	100	200
Rel	0.996956	0.997944	0.999034	0.999503	0.999741

calculation cycle. It can be seen that as the simulation time increases, the simulation error of different services increases its simulation accuracy as the simulation cycle increases. Will improve. At the same time, comparing the three services, it can be seen that the convergence speed of the calculation results is not that the longer the business logic path, the faster the convergence. The two VNFs in App20 are both active and standby VNFs, so the convergence is the slowest; App60 contains two host-based VNFs, so the convergence speed is relatively fast; App15 includes a 2-way service, so although the logical path is shorter , But the convergence speed is more balanced.

Finally, we give the relationship between the calculation result of the whole network service reliability and the calculation cycle and the number of calculations, as shown in Table 6 and Table 7.

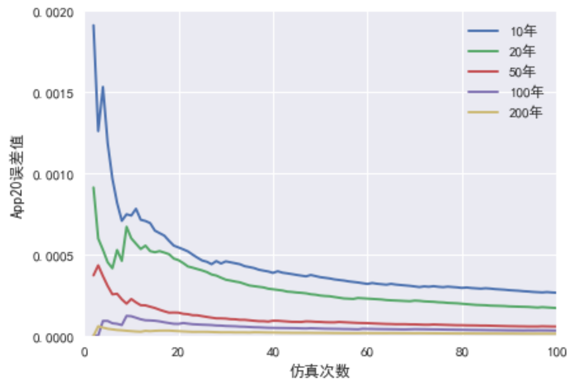

Fig. 13. When the service (App20) uses 2 VNFs, the relationship between the error and the number of calculations and the single calculation cycle

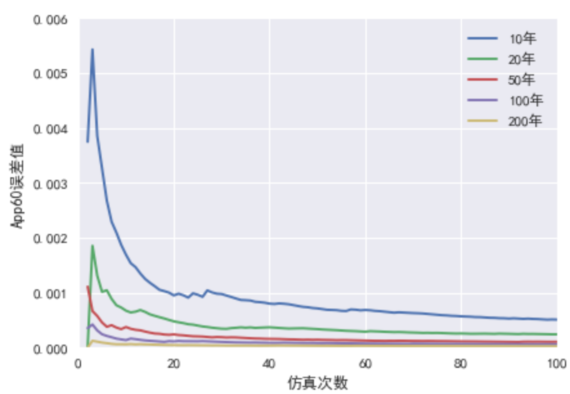

Fig. 14. When the service (App60) uses 3 VNFs, the relationship between the error and the number of calculations and the single calculation cycle

TABLE IX
RELIABILITY CALCULATION RESULTS AND CALCULATION TIME OF THE ENTIRE NETWORK WHEN T=200 AND N=[10,50,100]

N	10	50	100
Rel	0.999725	0.999743	0.999743

V. CONCLUSION

This paper proposes a reliability evaluation model of cloud virtualization based on network evolution. The model includes three parts: network evolution object, network evolution condition and network evolution rule. In the network evolution object modeling part, we established the network infrastructure layer (network nodes and edges) and network business layer (VNF and business) models. In the part of the network evolution condition model, we give out how to generate the relevant algorithms of component state changes over time according to the relevant parameters of the network component. In the part of network evolution rules, we clarified that after the status of each component changes, combined with the current status of the network to affect the status of each service in the network, we finally put forward the reliability evaluation algorithm of the single service and the whole network service of this model. The case verification results show that when the case-related design is simplified, the business reliability results obtained by us and the RBD algorithm are basically the same, and the calculation results of the algorithm converge. On this basis, we calculated and analyzed the service reliability on a large network of 128 servers carrying 100 services, and found that the service reliability is related to the length of the service logic path and the service protection strategy.

ACKNOWLEDGMENT

The authors would like to thank the National Natural Science Foundation of China (No. 61872018).

PLACE PHOTO HERE

Juxing Zhu Biography text here.

PLACE PHOTO HERE

Ning Huang Biography text here.

PLACE PHOTO HERE

Sitong Caihuang Biography text here.

PLACE PHOTO HERE

Junliang Wang Biography text here.