Security-Oriented Network Slice Backup Method

Ke Chen, Ying Wang, Peng Yu, Naling Li
State Key Laboratory of Networking and Switching Technology
Beijing University of Posts and Telecommunications
Beijing,China
Email:{chen_ke, wangy, yupeng, linaling}@bupt.edu.cn

***Abstract*—5G realizes flexible networking by building network slices, and its realization depends on network function virtualization (NFV) technology, which combines different types of virtual network functions (VNFs) to provide network services. The reliability of VNFs is lower than that of traditional hardware due to the risk of both software and hardware failure, and redundant backup is an effective solution. Meanwhile, from the security point of view, because the 5G network is based on the unified and standardized hardware of the industry, the need for isolation is put forward. Current research on VNF reliability assurance has not considered the special isolation requirements of 5G. In this paper, aiming to guarantee the safety demand as well as minimize backup resource to meet the reliability target, we formalize the safety-oriented backup problem for 5G core network slices and propose a backup algorithm based on isolation (BABI). Simulation results show that the introduction of isolation can double the security of slices. The comparison with the existing backup methods shows that under the same isolation constraint, the proposed approach can achieve a less resource consumption by 60% - 80% and a improvement of the proportion of effective resources by 40% - 80%.**

***Index Terms*—5G slice, reliability, safety, backup.**

I. INTRODUCTION

THE innovation driving force of 5G core network comes from the requirements of 5G business scenarios and new ICT enabling technologies, aiming to provide high-performance, flexible and adaptable network services and comprehensively improve the future-oriented network operation capacity [1]. 5G core network utilizes network function virtualization (NFV)/software-defined network (SDN) and other virtualization technologies to construct different network slices to meet the needs of different business scenarios. At the same time, the flexibility of network and the utilization efficiency of resources are improved [2].

Network slices are constructed through VNFs combination to provide network services, and the flexibility and expansibility of the network are realized. However, compared to highly reliable hardware network devices, the risk of failure of both hardware and software can cause VNFs to fail [3]. Failure of any VNF will result in an interruption of the network slice service. The VNFs' highly reliable is usually insured by providing redundant backup instances, which can be replaced immediately when the primary VNF fails. It should be noted that compared with the privacy and closure of traditional networks, network slices are virtualized private networks built on public infrastructure, which makes the network more vulnerable to attack. Moreover, centralized deployment accelerates the spread speed and expands the spread range of network threats. Therefore, 5G needs to provide a network isolation mechanism [4]. On the one hand, it can avoid the resource competition between slices and ensure the normal deployment and operation of slices. On the other hand, it can prevent the abnormality of one slice or VNF from affecting other slices or VNFS, and effectively prevent the spread of attacks and other security threats.

At present, VNF reliability assurance mainly adopts three methods: Dedicated Protection (DP), Joint Protection (JP) and Shared Protection (SP). Most of the researches [5]–[10] focus on random failures with the aim of minimizing backup resources and improving backup efficiency. Researches on security attacks [11]–[13] improve security defense by mapping VNF or backup instances to more reliable physical nodes. No studies on backup have been conducted to consider the need for secure isolation of 5G slices.

In view of the lack of security isolation in the current researches, this paper studies the backup method of 5G core network slices for security isolation. Isolation means the independence of resources, and there is a certain contradiction between security isolation and resource conservation. A backup algorithm based on isolation (BABI) is proposed to achieve a lower cost backup and a balance between isolation and resource utilization. The main contributions of this paper are as follows:

- A resource-aware backup problem model based on safety isolation is proposed, which introduces the 5G specific isolation requirement of slices while achieving reliability goals;
- The VNFs' differentiated security requirements are introduced. Multi-level isolation is used for fine-grained partition to save resources.
- A backup algorithm based on isolation (BABI) is proposed, which can improve the backup efficiency and reduce backup resource consumption. The BABI achieves a balance between security isolation and resource conservation;

The rest of this paper is organized as follows. Section II reviews the related work. Section III describes the slice reliability guarantee problem model. Section IV presents our proposed BABI algorithm. Section V presents the simulation results. Finally, Section VI summarizes the paper.

II. RELATED WORK

5G core network applies SDN/NFV technology to realize on-demand networking [14]. Network service is flexibly arranged by dragging and dropping combinations of various VNFs into required network slices [15]. Therefore, the backup of virtual network functions is an effective method to guarantee the reliability of slice.

Current studies on VNF backup are mainly based on three backup strategies: dedicated protection (DP), joint protection (JP) and shared protection (SP). Dedicated protection is one-to-one backup, and Rahul Potharaju et al [16] proved that this backup strategy has low efficiency. In order to improve resource efficiency, Defang Li et al. [9] proposed a deployment and backup scheme utilizing shared redundancy, in which a physical node can be used as a backup node for multiple VNFs and the node has the maximum resource required by VNFs. In [6], aiming to consume the least number of backup resources, the difference in resource requirements of different VNFs is considered and a resource-aware backup model is established. In [7], a cost-aware importance metric (CIM) backup scheme is proposed. Jingyuan Fan et al. [5] proposed JP on the basis of SP. Different from shared backup, physical nodes have the sum of all the resources required by VNFs, which further improves the reliability under limited resources. In their subsequent work [8], they apply JP and propose an online algorithm which significantly improves the acceptance rate of service requests. Prabhu et al. [10] proposed a eREVR solution, which establishes the 5G communication services as a queuing theory model, and enhances the reliability by adding sub-chains.

In terms of security attacks, in the work of [11], [12], the authors establish the network attack and defence process as the game theory model, and believe that network attacker would break the "known" instances at a fast speed. By establishing heterogeneous backup pool for VNFs, the security and defense ability of VNFs are improved. Shuiqing Gong et al. [13] mapped virtual network nodes to physical nodes with certain data encryption level and firewall level, so as to protect nodes from potential network attacks. 5G slices brings slice data leakage, resource competition and other challenges, thus, it is necessary to provide security isolation [17]. Slice isolation is a non-negligible part of guaranteeing the security of 5G network, but the above researches did not introduce isolation mechanism in solving the network security problems.

The focus of this paper is on the balance between safety isolation and resource consumption. Under the reliability target and the safety constraint, this paper proposes a backup strategy based on fine-grained isolation and considering node cost.

III. PROBLEM FORMULATION

In this section, we describe and model the problem of slice backup.

A. 5G Core Network Slice Model

A network slice is composed of sequential virtual network functions (VNFs), which can be modeled as $\boldsymbol{S}_i = \left\{\boldsymbol{v}_j^i | j = 1, ..., N_i\right\}$, where $N_i = |\boldsymbol{S}_i|$ is the VNF number in $\boldsymbol{S}_i$. For each VNF $\boldsymbol{v}_j^i \in \boldsymbol{S}_i$, it can be expressed as a 2-tuple $\boldsymbol{v}_j^i = (c_j^i, a_j^i, l_j^i)$. c_j^i and a_j^i respectively represent the resource requirements and the reliability of the function. $l_j^i \in \{0, 1, 2\}$ represents three isolation levels, i.e., inter-slice sharing, in-slice sharing and in-slice non-sharing, respectively. In this paper, we assume that the VNF type in each slice is not repeated, and j represents the type. $\mathcal{S} = \{\boldsymbol{S}_i | i = 1, ..., N_S\}$ represents the slice set, where $N_S = |\mathcal{S}|$ is the number of slices.

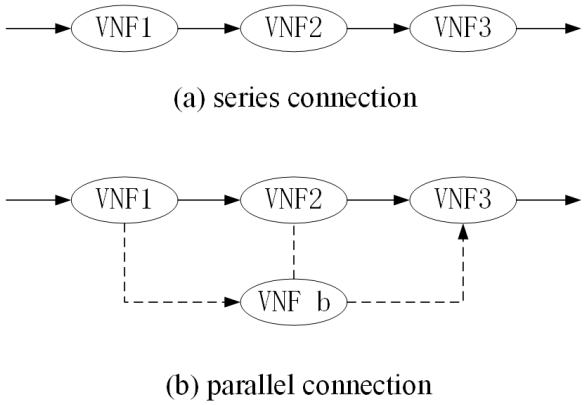

Fig. 1: Two basic types of VNF connections

B. Reliability Model

1) reliability of a single VNF: reliability reflects the probability that a VNF can work normally, and the status of a VNF can be divided into Uptime and Downtime. The reliability of a VNF can be expressed as the percentage of Uptime over the entire time. Uptime and Downtime are usually represented by the mean time between failures (MTBF) and mean time to repair (MTTR), respectively [18]. Therefore, the reliability of a VNF can be expressed as:

$$A = \frac{Uptime}{Uptime + Downtime} = \frac{MTBF}{MTBF + MTTR} \tag{1}$$

2) reliability of components: There are two basic types of VNF connections, i.e., series and parallel, as shown in Fig. 1. Assuming that the failure of each VNF is independent and the failure of any VNF will cause failure of the service, the serial reliability in Fig. 1 (a) can be expressed by Eq. (2).

$$A_s = a_1 \cdot a_2 \cdot a_3 \tag{2}$$

In Fig. 1 (b), VNF 2 and VNF b are connected in parallel and then connected with VNF 1 and VNF 3 in series. The reliability can be calculated by Eq. (3), where $a_2^{'}$ represents the reliability of the part of VNF 2 and b. This part fails when both VNF 2 and VNF b fail, which can be expressed as Eq. (4). In the example of Fig. 1 (b), we can suppose that VNF b is a backup instance of VNF 2.

$$A_p = a_1 \cdot a_2^{'} \cdot a_3 \tag{3}$$

$$a_2^{'} = 1 - (1 - a_2)(1 - a_b) = a_b + a_2 - a_2 a_b \tag{4}$$

TABLE I: Notations

Parameter	Description
Network Slice	
$\mathcal{S} = \{\boldsymbol{S}_i \mid i = 1, ..., N_S\}$	the slice set; $N_S = \lvert\mathcal{S}\rvert$ is the number of slices
$\boldsymbol{S}_i = \left\{\boldsymbol{v}_j^i \mid j = 1, ..., N_i\right\}$	network slice; $N_i = \lvert\boldsymbol{S}_i\rvert$ is the number of VNFs in $\boldsymbol{S}_i$
$\boldsymbol{v}_j^i = (c_j^i, a_j^i, l_j^i)$	the j-th VNF in slice $\boldsymbol{S}_i$
A_i	the reliability of $\boldsymbol{S}_i$
c_j^i	the resource requirements of $\boldsymbol{v}_j^i$
a_j^i	the reliability of $\boldsymbol{v}_j^i$
$l_j^i \in \{0, 1, 2\}$	the isolation level of $\boldsymbol{v}_j^i$
Backup	
A_q	the reliability target for each slice
$\boldsymbol{B}_i = \left\{\boldsymbol{b}_j^i \mid j = 1, ..., N_i^B\right\}$	the backup set of $\boldsymbol{S}_i$, $N_i^B = N_i$
$\boldsymbol{b}_j^i = (\bar{c}_j^i, \bar{a}_j^i)$	the backup instance type corresponding to $\boldsymbol{v}_j^i$
$\bar{c}_j^i$	the resources $\boldsymbol{b}_j^i$ can provide
$\bar{a}_j^i$	the reliability of $\boldsymbol{b}_j^i$
Decision variables	
$k_j^i \geq 0$	the number of $\boldsymbol{b}_j^i$
$x_{pq}^i \in \{0, 1\}$	binary variable indicating if $\boldsymbol{b}_q^i$ provides protection for $\boldsymbol{v}_p^i$

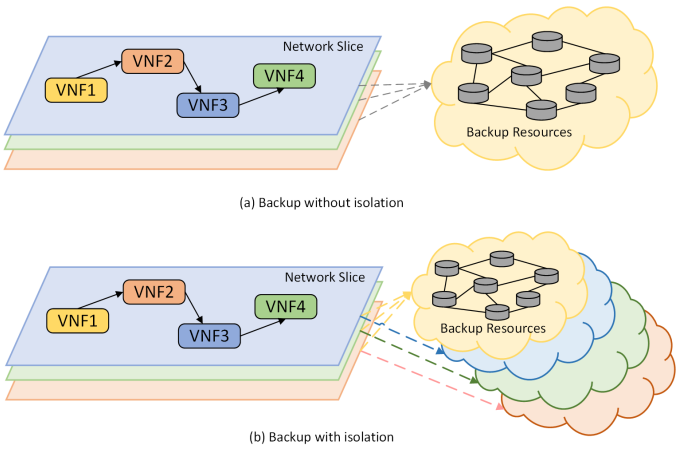

Fig. 2: Safety isolation.

C. Problem Formulation

For the slices that do not meet the reliability target, backup instances are provided for the VNFs based on security isolation until all of the slices reach the target. The optimization goal is to reduce the resource consumption caused by backup. The main notations are provided in Table I.

The network slice provides service by connecting VNFs, which can be regarded as a series of VNFs. Before backup instances are provided for a slice, the reliability of the slice can be expressed by Eq. (5).

$$A_i = \prod_{\boldsymbol{v}_j^i \in \boldsymbol{S}_i} a_j^i \tag{5}$$

The slice reliability requirement is A_q. When the reliability A_i of the slice $\boldsymbol{S}_i$ is lower than A_q, the backup instances need to be allocated for $\boldsymbol{S}_i$. Considering the different isolation requirements of different VNFs, we use l_j^i to represent the isolation level of $\boldsymbol{v}_j^i$ and adopt the corresponding backup strategy for it, as shown in Fig. 2. The set of backup instance types is represented as $\boldsymbol{B}_i = \left\{\boldsymbol{b}_j^i\right\}$. Each backup instance can be represented by a 2-tuple $\boldsymbol{b}_j^i = (\bar{c}_j^i, \bar{a}_j^i)$, where $\bar{c}_j^i$ and $\bar{a}_j^i$ respectively represent the resources $\boldsymbol{b}_j^i$ can provide and its reliability. In this paper, we assume that there is a one-to-one correspondence between the backup instance type and the VNF type, that is, $\bar{a}_j^i = a_j^i$ and $\bar{c}_j^i = c_j^i$. Moreover, we use k_j^i to represent the number of backup instances of this type. Our goal is to determine the number of backup instances of each type in each slice to ensure that the reliability of all slices meets the requirement and to minimize the backup resource consumption. The following two decision variables need to be determined to complete the backup process.

$k_j^i \geq 0$: Number of $\boldsymbol{b}_j^i$. $k_j^i = 0$ means that this type of backup instance is not provided;

$x_{pq}^i \in \{0, 1\}$: Corresponding relationship between the primary VNF and backup instance. $x_{pq}^i = 1$ means that backup instance $\boldsymbol{b}_q^i$ provides protection for $\boldsymbol{v}_p^i$.

The objective functions and constraints of the problem are as follows:

Objective:

$$\min \sum_{i=0}^{N_S} \left(\sum_{j=0}^{N_i} k_j^i \cdot \bar{c}_j^i \right) \tag{6}$$

Subject to:

$$\forall i, A_i \geq A_q \tag{7}$$

$$x_{pq}^i = \begin{cases} 1 & if \;\; \bar{a}_q^i \geq a_p^i \; and \; \bar{c}_q^i \geq c_p^i \; and \; l_p^i = l_q^i \neq 2 \\ 0 & else \end{cases} \tag{8}$$

Eq. (6) is our objective function, which optimizes the resources consumed by the backup instances. Eq. (7) presents the reliability constraint, which means that after backup, all of the slices must meet the reliability requirement. Eq. (8) provides three conditions for the backup instance to provide protection for the VNF. First, the reliability of backup instances cannot be lower than the reliability of VNFs, which can ensure a higher backup efficiency. Second, the resource capacity of the backup instance must not be lower than the VNF requirement for resources; otherwise, the backup will not succeed. The last one is the constraint of security isolation. Except for VNFs with an isolation level of 2 using proprietary backup, only VNFs with the same isolation level can share backup instances (between slices or within slices).

IV. PROPOSED RELIABILITY GUARANTEE METHOD

In this section, we describe the resource-aware slice reliability guarantee method based on multi-level isolation. Our goal is to meet the reliability target and achieve a balance between security isolation and resource conservation.

A. Method Overview

As we mentioned before, the 5G core network applies NFV/SDN to construct network slices to meet various business needs. In a virtualized environment, network services are realized through an orderly combination of VNFs. VNF failure will cause interruption of the service; thus, VNF backup is required to guarantee reliability for slices. Among these VNFs, some are dedicated to slices, and some are shared among multiple slices. Each VNF has different reliability and resource requirements.

Step 1: This step uses Eq. (5) to evaluate whether all slices meet the reliability requirements. Then, we perform the following step to back up slices that do not meet the reliability requirement.

Step 2: This step determines the number of each type of backup instance. Different isolation levels (from high to low) correspond to the strategies of dedicated backup, shared backup within slices and shared backup between slices. To improve backup efficiency and consume as few backup resources as possible, in our proposed algorithm, we select the VNF that contributes the most to the reliability improvement of the slice for backup every time until the slice reliability meets the target.

The above two steps take into account the security isolation requirements of 5G core network slices and the goal of improving resource utilization while meeting the reliability requirement.

B. Backup Algorithm Based on Isolation

We propose a backup algorithm based on multi-level isolation to protect VNFs in the logical security domain. The backup instances are gradually increased until the slice meets the reliability requirement. The goal of the algorithm is to achieve the target reliability with the least number of required resources. We first give the reliability calculation method to judge whether the target is achieved.

1) reliability calculation method

In a dedicated backup, each backup instance protects only one primary VNF, that is, k_j^i backup instances are connected in parallel with $\boldsymbol{v}_j^i$. In Section III, we assumed that the backup instance is of the same type as the original VNF; thus, k_j^i backup instances meet the constraints in Eq. (8), and a_j^i after backup can be expressed by Eq. (9).

$$a_j^{i'} = 1 - (1 - a_j^i)^{(k_j^i + 1)} \tag{9}$$

As for the VNF that adopt the shared backup strategy within its logical security domain, each backup instance backs up all VNFs that meet the resource and reliability constraints. This can maximize the overall reliability [6]. [8] proves that calculating the overall accuracy and reliability in the case of shared backup is a PP-complete problem. We use Monte Carlo Method to get the approximate value of reliability after backup [19]. When all the backup types are calculated, A_T is the reliability of the security domain after backup.

2) Multi-level isolated backup algorithm

Our proposed backup algorithm based on isolation(BABI) is shown in Algorithm 1. The basic idea of the algorithm is to maximize the improvement rate of the overall reliability with minimal resources when adding a backup instance each time. The number of backup instances is gradually increased until the slice meets the reliability requirement.

Algorithm 1 Multi-level isolated backup algorithm

Input: $\boldsymbol{S}_i$, $\boldsymbol{T}_h^i$, $\boldsymbol{T}_m^i$, $\boldsymbol{T}_l$, A_q
Output: $\left\{k_j^i\right\}$

```
Initialize k_j^i = 0;
Initialize A_i by Eq. (5);
Initialize T_h^i, T_m^i, T_l as null;
for each j do
    Get l_j^i using the security assessment model;
    if l_j^i = 0 then
        Put v_j^i in T_l
    else if l_j^i = 1 then
        Put v_j^i in T_m^i
    else
        Put v_j^i in T_h^i
    end if
end for
while A_i < A_q do
    for each j < N_i do
        Compute the reliability of each VNF in S_i when the
        number of backup instances is {k_1^i, ..., k_{j+1}^i, ...}
        Compute the reliability of S_i by Eq. (5) and record
        it as A_i^*;
        Compute ρ_j by Eq. (10);
    end for
    Choose the j corresponding to the maximum ρ_j;
    k_j^i = k_j^i + 1
    A_i = A_i^*
end while
return {k_j^i}
```

The input of the algorithm is $\boldsymbol{S}_i$, $\boldsymbol{T}_h^i$, $\boldsymbol{T}_m^i$, $\boldsymbol{T}_l$ and A_q, where $\boldsymbol{T}_h^i$, $\boldsymbol{T}_m^i$ and $\boldsymbol{T}_l$ respectively represent three logical security domains with isolation levels from high to low. Different strategies are applied in different domains. The output is the number of each backup type $\left\{k_j^i\right\}$. Before the backup, the number of all backup types is set to 0, and the overall reliability is A_i. After each backup instance is added, the reliability is calculated. When A_i does not reach A_q, one of the backup types is selected to allocate one instance. When selecting the type of backup to be added, we introduce the unit resource reliability improvement rate ρ_j to describe the improvement effect of the added backup instance on the overall reliability. A backup instance that maximizes ρ_j is added each time. The reliability of $\boldsymbol{S}_i$ before the m-th backup is A_{m-1}^i, and the system reliability after this backup is A_m^i. ρ_j is expressed as Eq. (10).

$$\rho_j = \frac{A_m^i - A_{m-1}^i}{A_{m-1}^i \times c_j^i} \tag{10}$$

V. PERFORMANCE EVALUATION

In this section, we evaluate the performance of our proposed BABI backup method.

A. Simulation Environment and Comparison Method

All simulations are run on a 4-core, 1.80 GHz, 16 GB server. The proposed BABI is implemented and run in Python 2.7. The number of slices is set to 10, and the number of VNFs in a slice ranges from 1 to 9. The number of resource units that each VNF requests for ranges from 10 to 90. The reliability of each VNF ranges from 0.85 to 0.99. The reliability requirement of each slice is selected from $\{0.9, 0.95, 0.98, 0.99, 0.999\}$. We compare our BABI with another two algorithms: the Picker and the random algorithm. Picker is based on the joint backup strategy, two VNFs with the lowest reliability are selected for joint backup each time until the reliability requirement is met [5]. The random method is based on the shared backup strategy, a backup instance is randomly added each time until the reliability target is met.

We first compare the performances of these algorithms under the same isolation strategy, and then compare the impact of the isolation strategy. In the end, we compare the complexity. We evaluate the algorithms from the following four aspects:

- Backup resource consumption (unit): the number of resource units occupied by backup instances to achieve the reliability target.
- Robustness (%): the impact on slice reliability when a random backup instance fails, which is expressed as a percentage of reliability decline. Robustness evaluates how steady the system is when facing various attacks and it is a key performance metric in 5G [20].
- Running time of the algorithm (s).

B. Simulation Results and Analysis

1) Backup resource consumption: Fig. 3 shows the average backup resource consumption of several algorithms under different reliability requirements. The required number of backup resources gradually increases as the reliability requirements increase. It can be found that the number of backup resources required for random allocation is the highest, followed by Picker. Compared with the best compared method Picker, our algorithm consumes fewer backup resources, with reductions of 62.5%, 67.5%, 69.0%, 68.4% and 61.1%, respectively. This is because each backup instance can provide backups for at most two VNFs in Picker, and the resources occupied by the backup instances are the sum of the backup VNF resource requirements. Our algorithm adopts the shared backup strategy in the two lower-security domains. A backup instance can back up all VNFs that meet the conditions in its logical security domain. The greater the number of VNFs that a backup instance can guarantee, the greater the improvement of the overall reliability of the slice.

2) Robustness: Backup instances may fail due to external attacks. We compared the impact of a backup instance failure on the overall reliability in different schemes, as shown in Fig. 4. Compared with the other schemes, the scheme proposed in this paper has a relatively large impact on the overall reliability after failure because one backup instance is shared by more VNFs. Picker occupies a large number of resources, and each backup instance guarantees fewer VNF; thus, the impact of a backup node failure is relatively small. To compare the impact

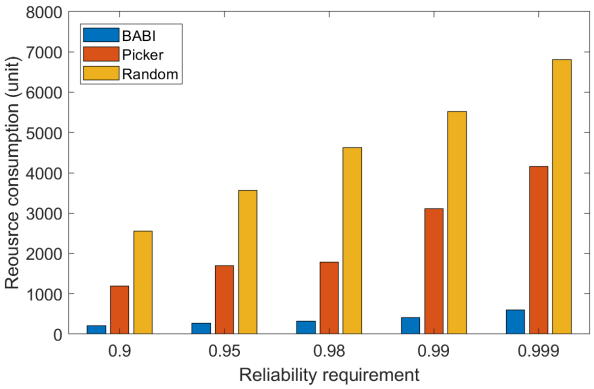

Fig. 3: Backup resource consumption

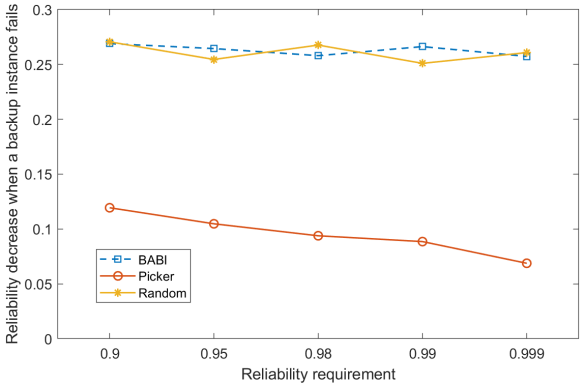

Fig. 4: The robustness of slices.

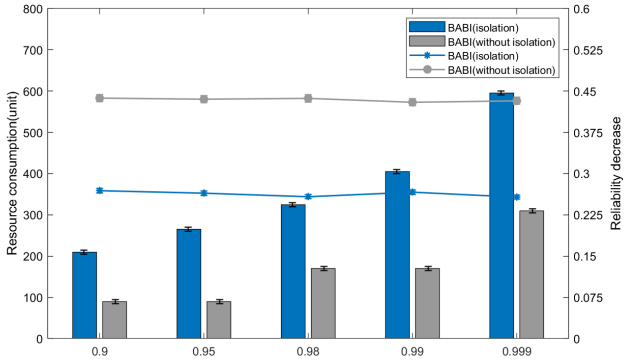

Fig. 5: The impact of isolation.

of multi-level isolation, we removed the multi-level isolation part from this algorithm for simulation and comparison. The results are shown in Fig. 5. The introduction of multi-level isolation reduces the scope of sharing to a certain extent, and increases security in exchange for the consumption of some backup resources. Taking the reliability requirement of 0.9 as an example, compared with the method that does not introduce multi-level isolation, we increased the number of backup resources by 52.7%, and the robustness was approximately doubled.

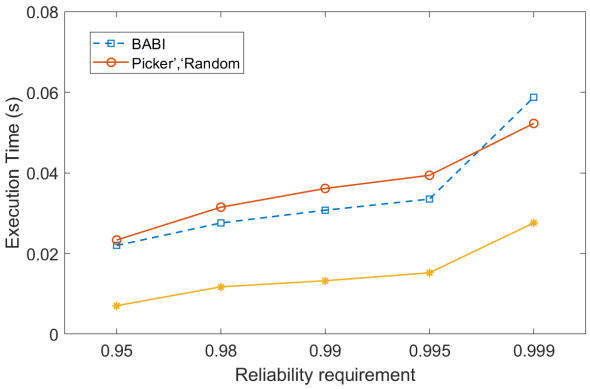

Fig. 6: Execution time.

3) Execution time: We compared the execution times of the four algorithms, and the results are shown in Fig. 6. The Random algorithm has the lowest complexity. The execution time of our algorithm is surpassed only by that of the Random algorithm. Taking the reliability requirement of 0.98 as an example, the Random algorithm has a 56.9% shorter execution time than our algorithm. However, Fig. 3 shows that it consumes 12.8 times more resources than does our algorithm.

Simulation results show that our solution achieves a balance between security isolation and resource consumption. Compared with non-isolated shared backup, the introduction of multi-level isolation has brought a certain increase in the number of backup resources, but it effectively meets the security demand of 5G slices. Under the same isolation strategy, our algorithm can minimize the backup resource consumption, and its complexity is the second best, being inferior only to that of the random algorithm.

VI. CONCLUSIONS

5G slices realize flexible networking, but they also face reliability and security issues. In this paper, we realize the reliability guarantee problem of 5G core network slice through VNF backup. We achieved multi-level isolation to meet the differentiated safety requirements of slices. The solution with the least resource consumption is found through our BABI algorithm. The simulation evaluation in Section V proves that the multi-level isolation strategy in our scheme can effectively improve the security of slices and the advantages of the BABI algorithm in resource saving.

REFERENCES

[1] M. R. Raza, C. Natalino, P. Öhlen, L. Wosinska, and P. Monti, "Reinforcement learning for slicing in a 5g flexible ran," *Journal of Lightwave Technology*, vol. 37, no. 20, pp. 5161–5169, 2019.

[2] A. Ghosh, A. Maeder, M. Baker, and D. Chandramouli, "5g evolution: A view on 5g cellular technology beyond 3gpp release 15," *IEEE Access*, vol. 7, pp. 127 639–127 651, 2019.

[3] V. Nguyen, A. Brunstrom, K. Grinnemo, and J. Taheri, "Sdn/nfv-based mobile packet core network architectures: A survey," *IEEE Communications Surveys Tutorials*, vol. 19, no. 3, pp. 1567–1602, 2017.

[4] P. Popovski, K. F. Trillingsgaard, O. Simeone, and G. Durisi, "5g wireless network slicing for embb, urllc, and mmtc: A communication-theoretic view," *IEEE Access*, vol. 6, pp. 55 765–55 779, 2018.

[5] J. Fan, X. Gao, Z. Ye, K. Ren, C. Guan, and C. Qiao, "Grep: Guaranteeing reliability with enhanced protection in nfv," in *Acm Sigcomm Workshop on Hot Topics in Middleboxes & Network Function Virtualization*, 2015.

[6] J. Zhang, Z. Wang, C. Peng, L. Zhang, T. Huang, and Y. Liu, "Raba: Resource-aware backup allocation for a chain of virtual network functions," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, 2019, pp. 1918–1926.

[7] W. Ding, H. Yu, and S. Luo, "Enhancing the reliability of services in nfv with the cost-efficient redundancy scheme," in *ICC 2017 - 2017 IEEE International Conference on Communications*, 2017.

[8] J. Fan, C. Guan, Y. Zhao, and C. Qiao, "Availability-aware mapping of service function chains," in *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, 2017.

[9] D. Li, P. Hong, K. Xue, and J. Pei, "Availability aware vnf deployment in datacenter through shared redundancy and multi-tenancy," *IEEE Transactions on Network and Service Management*, vol. PP, no. 99, pp. 1–1, 2019.

[10] P. K. Thiruvasagam, V. J. Kotagi, and C. S. R. Murthy, "The more the merrier: Enhancing reliability of 5g communication services with guaranteed delay," *IEEE Networking Letters*, pp. 1–1, 2019.

[11] J. Xie, P. Yi, Z. Zhang, C. Zhang, and Y. Gu, "A service function chain deployment scheme based on heterogeneous backup," in *2018 IEEE 18th International Conference on Communication Technology (ICCT)*, 2018.

[12] S. Xu, X. Ji, and W. Liu, "Enhancing the reliability of nfv with heterogeneous backup," in *Information Technology, Networking, Electronic and Automation Control Conference*.

[13] S. Gong, J. Chen, C. Huang, and Q. Zhu, "Trust-aware secure virtual network embedding algorithm," *Journal on Communications*, vol. 36, no. 011, pp. 180–189, 2015.

[14] S. Kazmi, L. U. Khan, N. Tran, and C. S. Hong, *Network Slicing for 5G and Beyond Networks*, 01 2019.

[15] D. Sattar and A. Matrawy, "Optimal slice allocation in 5g core networks," *IEEE Networking Letters*, vol. 1, no. 2, pp. 48–51, 2019.

[16] R. Potharaju and N. Jain, "Demystifying the dark side of the middle: A field study of middlebox failures in datacenters," in *Proceedings of the 2013 conference on Internet measurement conference*, 2013.

[17] 3GPP, "Security architecture and procedures for 5g system: 3GPP TS 33.501," 2019.

[18] P. Gill, N. Jain, and N. Nagappan, "Understanding network failures in data centers: Measurement, analysis, and implications." New York, NY, USA: Association for Computing Machinery, 2011. [Online]. Available: https://doi.org/10.1145/2018436.2018477

[19] M. Jerrum and A. Sinclair, "The markov chain monte carlo method: An approach to approximate counting and integration," *PWS Publishing Co.*, 1996.

[20] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5g mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2018.