1-1-2019

Efficient and Secure 5G Core Network Slice Provisioning Based on VIKOR Approach

Xin Li
Wuhan University

Chengcheng Guo
Wuhan University

Lav Gupta
Washington University in St. Louis, lavgupta@missouri.edu

Raj Jain
Washington University in St. Louis

January 1, 2019

Efficient and Secure 5G Core Network Slice Provisioning Based on VIKOR Approach

Xin Li
Chengcheng Guo
Lav Gupta
Raj Jain

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 18, 2019, accepted October 7, 2019, date of publication October 15, 2019, date of current version October 29, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2947454

Efficient and Secure 5G Core Network Slice Provisioning Based on VIKOR Approach

XIN LI[1], CHENGCHENG GUO[1], LAV GUPTA[2], (Senior Member, IEEE), AND RAJ JAIN[2], (Fellow, IEEE)

[1]School of Electronic Information, Wuhan University, Wuhan 430072, China
[2]Department of Computer Science and Engineering, Washington University in St. Louis, St. Louis, MO 63130, USA

Corresponding author: Xin Li (xinli1105@whu.edu.cn)

This work was supported in part by the National Priorities Research Program (NPRP) from the Qatar National Research Fund (a member of The Qatar Foundation) under Grant NPRP 8-634-1-131, in part by the NSF under Grant CNS-1718929 and Grant CNS-1547380, and in part by the Huawei Technologies, and China Scholarship Council under Grant 201506270075. The statements made herein are solely the responsibility of the authors.

ABSTRACT Network slicing in 5G is expected to essentially change the way in which network operators deploy and manage vertical services with different performance requirements. Efficient and secure slice provisioning algorithms are important since network slices share the limited resources of the physical network. In this article, we first analyze the security issues in network slicing and formulate an Integer Linear Programming (ILP) model for secure 5G core network slice provisioning. Then, we propose a heuristic 5G core network slice provisioning algorithm called VIKOR-CNSP based on VIKOR, which is a multi-criteria decision making (MCDM) method. In the slice node provisioning stage, the node importance is ranked with the VIKOR approach by considering the node resource and topology attributes. The slice nodes are then provisioned according to the ranking results. In the slice link provisioning stage, the k shortest path algorithm is implemented to obtain the candidate physical paths for the slice link, and a strategy for selecting a candidate physical path is proposed to increase the slice acceptance ratio. The strategy first calculates the path factor P_f which is the product of the maximum link bandwidth utilization of the candidate physical path and its hop-count, and then chooses the candidate physical path with the smallest P_f to host the slice link. Extensive simulations show that the proposed algorithm can achieve the highest slice acceptance ratio and the largest provisioning revenue-to-cost ratio, satisfying the security constraints of 5G core network slice requests.

INDEX TERMS 5G core network slice, network slicing, slice provisioning, slice security, VIKOR approach.

I. INTRODUCTION

With the emergence of new application scenarios, such as Augmented Reality (AR), Industrial Internet of Things (IIoT), and Vehicle-to-Everything (V2X), 5G networks have very diverse communication requirements, including high throughput, ultra-low latency, and ultra-reliability. Table 1 lists the three main application scenarios and corresponding communication requirements in 5G networks defined by the IMT-2020 Focus Group in the Telecommunication Standardization Sector of the International Telecommunications Union (ITU-T) [1]. The one-size-fits-all architecture of traditional mobile networks is unable to meet the myriad service requirements of the 5G networks. In addition, due to the current distributed and heterogeneous network architecture, any changes to the network architecture need the coordination between vendors and service providers. This is a very difficult process that hinders innovations in network architecture. Therefore, the concept of network slicing has been identified by the Next Generation Mobile Networks (NGMN) Alliance to support vertical applications with different performance requirements and to promote innovation in next-generation network architecture design [2].

Network slicing is considered to be a fundamental feature of 5G networks. It can provide multi-tenancy, multi-service support, and achieve on-demand network services for distinct application scenarios. The 5G system architecture supporting network slicing has already been defined in the first release of 5G normative specifications and has been approved by the 3rd Generation Partnership Project (3GPP) [3]. Specifically speaking, a network slice is a self-contained logical network with its own virtual resources, topology, traffic flow,

The associate editor coordinating the review of this manuscript and approving it for publication was Thanh Ngoc Dinh.

TABLE 1. Three major 5G use cases.

5G Use Case	Examples	Requirements
Enhanced mobile broadband	UHD video, augmented reality	Very high data rate (10 $Gbps$)
Massive machine type communications	Smart city, smart wearables	Ultra-high density (1 $million/km^2$)
Ultra-reliable and low latency communications	Automatic driving, smart grid	Low latency ($1ms$), high reliability

provisioning rules with established quality of service (QoS), security, and measureable performance metrics to provide telecommunication services and network capabilities. For a specific service request, the 5G infrastructure provider initializes the virtual resources and virtual network functions (VNFs) in the resource pool, and they are combined to form a slice instance. Slices are logically isolated and can be deployed with service-specific customized network protocols to host highly differentiated 5G applications and services. There are two types of network slicing: radio access network slicing and core network slicing [4]. In this paper, we focus on core network slicing, where computing and networking resources of the physical network are shared among multiple slice tenants.

The core idea of network slicing is consistent with network virtualization [5], which enables flexible and dynamic network management by allowing multiple heterogeneous and service-specific virtual networks to share one substrate network. One key issue in network virtualization is the virtual network embedding (VNE) [6]. This process allocates physical resources to virtual networks. The same problem needs to be solved in the 5G network slicing. We define this issue as 5G network slice provisioning instead of VNE [1]. Network slice provisioning refers to the process of allocating physical resources to slice requests [7]. In particular, efficient and secure 5G network slice provisioning is a vital challenge. For one thing, the physical resources of the 5G infrastructure are limited. When provisioning slices, efficient utilization of physical resources needs to be considered so that the 5G physical network can receive more slice requests. Concretely, efficient slice provisioning means allocating fewer resources to satisfy a slice request thus reducing provisioning cost. Besides, due to the intrinsic feature of sharing, network slicing introduces new security issues, such as the attacks between slice tenants and slices, mutual attacks between slices, and mutual attacks between slices and the physical network [8], [9]. These security threats may undermine the confidentiality, isolation, and availability of the slices. Thus, it is necessary to design new security mechanisms to deal with the security risks brought by network slicing.

Based on the above considerations, in this paper, we consider the 5G core network slice provisioning problem. Specifically, we solve the problem of the efficient resource allocation in a secure way on the softwarized and virtualized 5G core network supporting heterogeneous services. We refer to this problem as the **E**fficient and **S**ecure 5G **C**ore **N**etwork **S**lice **P**rovisioning (**ES-CNSP**) problem. In order to ensure the security of a 5G core network slice, the slice tenant may request the slice with a specific security requirement. For example, some slice nodes in a slice need to be provisioned on physical nodes with encryption capabilities. Therefore, we introduce resource constraints as well as security constraints to formulate the network slice provisioning into a mathematical programming model. In several VNE studies, ranking nodes is integrated into the node embedding process. Some of them use node computing resources and adjacent link bandwidth resources to rank nodes [10], [11], while some consider the network topology attributes besides resource attributes to rank nodes [12], [13]. However, topology attributes and resource attributes are simply combined as one metric to score and rank nodes in these studies, which cannot comprehensively rank nodes.

To overcome the shortcomings of the existing ranking methods, it is necessary to rank nodes from the perspective of multi-attribute decision making when provisioning slice nodes. Ranking nodes is affected by computing resources, bandwidth resources and topological attributes. We should consider these attributes together instead of combining them as one metric to evaluate each node, and then make decisions according to a certain method, so as to rank the nodes reasonably. This process of ranking nodes based on multiple attributes is a multi-attribute decision problem. The VIKOR method is a commonly used ranking method in multi-attribute decision making. It ranks the alternatives according to the distance between their evaluated value and the ideal solution. It has a strong advantage in obtaining a compromise solution. Therefore, we propose a heuristic 5G core network slice provisioning algorithm called VIKOR-CNSP based on the VIKOR [14] approach. The VIKOR-CNSP algorithm considers the resource attributes and topology attributes of nodes and uses the VIKOR method to rank the nodes with multiple attributes, which can evaluate the contribution of each attribute to the ranking reasonably. The slice nodes are provisioned according to the ranking results. The slice links are provisioned by using the k shortest path algorithm together with our proposed path selecting strategy. Our contributions are summarized as follows:

1) We analyze the security issues in the network slicing environment and formulate the secure 5G core network slice provisioning problem as an integer linear programming (ILP) model.
2) We design a two-stage heuristic slice provisioning algorithm to solve the ES-CNSP problem. In the slice node provisioning stage, we introduce the node importance from the complex network theory to indicate the node provisioning order. We regard the evaluation of node importance using multiple attributes (i.e., resource and topology attributes) of the node as a Multiple Attribute Decision Making (MADM) problem.

[1]The virtual network embedding (VNE) problem is renamed to network slice provisioning problem in network slicing.

The node attributes taken into account are node CPU, its adjacent link bandwidth, its degree centrality, and its closeness centrality. The VIKOR method is used to comprehensively evaluate the node importance and to rank nodes. The slice nodes are then provisioned in a heuristic manner based on the ranking results.

3) In the slice link provisioning stage, the k shortest path algorithm is implemented to obtain the candidate physical paths for the slice link, and a strategy for selecting a candidate physical path is proposed to increase the slice acceptance ratio. The strategy first calculates the path factor P_f which is the product of the maximum link bandwidth utilization of the candidate physical path and its hop-count, and then chooses the candidate physical path with the smallest P_f to host the slice link.
4) We have developed a simulator to perform extensive simulations. The results show that our proposed algorithm can increase the slice acceptance ratio and provisioning revenue.

The rest of the paper is organized as follows. We introduce the related work in Section II. Section III presents the secure 5G core network slice provisioning model. The node importance ranking based on VIKOR approach is detailed in Section IV. We present the two-stage heuristic 5G core slice provisioning algorithms based on VIKOR in section V. In Section VI, we describe the simulation experiments and analyze the experimental results. Finally, we conclude the paper in Section VII.

II. RELATED WORK

In this section, we first summarize the latest work related to the resource allocation in network slicing. Then, we discuss the latest work related to the security in network slicing. We next present several representative solutions to the traditional virtual network embedding (VNE) problem.

A. RESOURCE ALLOCATION IN NETWORK SLICING

The research in [15] focused on the resource allocation problem of radio access network (RAN) slicing. The authors studied how to allocate baseband resources and radio resources under the heterogeneous cloud radio access network (H-CRAN) architecture. The problem was formulated as a non-convex mixed integer linear programming (MILP) model and solved by the Lagrangian dual method. The proposed resource allocation strategy can achieve higher throughput and better fairness for heterogeneous services. The radio resource allocation problem in Fog Radio Access Network (F-RAN) slicing was investigated in [16]. Under a hierarchical resource allocation architecture, the problem was modeled as a Stackelberg game model, where the global radio resource manager acts as the leader and local radio resource managers act as followers. Since this problem is NP-hard, the authors proposed a process based on an exhaustive search to achieve the Stackelberg equilibrium. The authors in [17] formulated a MILP model for offline network slice embedding problem. The proposed model considered resource constraints, latency as well as reliability. An exact solution to the model verified its feasibility, but it cannot efficiently solve large-scale problem instances. Delgado *et al.* [18] studied the resource allocation problem of sensor network slices. They proposed a joint optimization framework for application admission control and slice resource allocation. A heuristic algorithm was designed to solve the joint optimization problem. The authors in [19] modeled the resource allocation problem cross slices based on service requests and available resources, and proposed the Markov decision framework to obtain the optimal resource allocation strategy for network slices. Simulation experiments showed that their proposed methods not only allocate resources efficiently but also improve the profit of physical network providers. Ye *et al.* [20] proposed a network slicing architecture for end-to-end QoS services in 5G networks. Under this architecture, the resource allocation for RAN slicing and core network slicing was considered. For the RAN slicing, a dynamic spectrum slicing mechanism was proposed for the heterogeneous base stations, which dynamically adjusts the spectrum resources of each base station according to the real-time network load. For the core network slicing, bottleneck-resource generalized processor sharing (BR-GPS) was used as a biresource slicing scheme in multiple traffic flows traversing in an network function virtualization (NFV) node.

In the above-mentioned studies, either the RAN slice resource allocation or the core network slice resource allocation was investigated. However, the security requirements of slices were not taken into account in all of these studies.

B. SECURITY IN NETWORK SLICING

Since slice tenants share the physical network, security and trust are key concerns of network slicing technology. NGMN lists several key security issues in network slicing [21], such as side channel attacks across slices, denial of service to other slices, etc. The authors in [22] discussed the essential enabler of 5G network slice security: slice isolation. They presented some methods to achieve host resource isolation and network communication isolation. This work was the very first one that mitigated the Distributed Denial of Service (DDoS) attack in the 5G core network slicing by resource isolation. Schneider *et al.* [23] stated that sensitive service slices required strong slice isolation. They analyzed the trust relationships between stakeholders in the 5G network slicing system such as infrastructure providers, hardware and software vendors. They introduced some network architecture models to ensure slice security but did not analyze the performance of these models. A method for proactively mitigating DDoS attacks in 5G core network slicing was proposed by using slice isolation in [24]. The authors considered both the inter-slice and intra-slice isolation to create a mathematical optimization model using slice isolation as security constraints. Through simulation and testbed evaluation, they verified that complete slice isolation mitigates DDoS attacks.

TABLE 2. System model notations.

Notation	Description
G^I	5G core infrastructure topological graph.
V^I	Set of physical nodes.
E^I	Set of physical links.
$c_0(v^I)$	Initial total CPU capacity of the physical node v^I.
$c_a(v^I)$	Available CPU capacity of the physical node v^I.
$sr(v^I)$	Security requirement of the physical node v^I.
$sl(v^I)$	Security level of the physical node v^I.
$b_0(e^I)$	Initial total bandwidth of the physical link e^I.
$b_a(e^I)$	Available bandwidth of the physical link e^I.
$P^I(v_i^I, v_j^I)$	Set of loop-free physical paths between v_i^I and v_j^I.
$L(p^I(v_i^I, v_j^I))$	Set of links in $p^I(v_i^I, v_j^I)$.
G^S	5G core network slice request topological graph.
V^S	Set of slice nodes.
E^S	Set of slice links.
$c(v^S)$	CPU capability required by the slice node v^S.
$sr(v^S)$	Security requirement of the slice node v^S.
$sl(v^S)$	Security level of the slice node v^S.
$b(e^S)$	Bandwidth required by the slice link e^S.

The authors in [25] proposed an effective and secure service-oriented authentication framework for 5G IoT services. The proposed framework guaranteed the secure access and selection of slices.

C. VNE SOLUTIONS

The virtual network embedding process involves mapping virtual nodes to physical nodes and virtual links to physical links or paths. The VNE problem has been proven to be an NP-hard problem [26]. Therefore, for large-scale problem instances, heuristic algorithms or meta-heuristic algorithms are used to solve the VNE problem. A representative heuristic algorithm was described in [10]. In this work, the authors used node computing resources and adjacent link bandwidth resources to rank nodes to heuristically map virtual nodes, and implemented the shortest path algorithm to map virtual links. The authors in [27] considered the network topology attributes to rank nodes. The virtual nodes are mapped according to the ranking results. After the node mapping is completed, the shortest path algorithm is also used to solve the link mapping. Authors in [12], [13] simply combined topology attributes and resource attributes as one metric to score and rank nodes. However, these studies did not comprehensively research the impact of both resource and topology attributes on node mapping. The ant colony algorithm and particle swarm optimization algorithm were proposed in the literature [28] and [29] respectively, to solve the VNE problem.

III. SECURE 5G CORE NETWORK SLICE PROVISIONING MODEL

In this section, we first describe the security issues in 5G core network slicing and then present the system model. The used notations are summarized in Table 2.

A. SECURITY ISSUES IN 5G CORE NETWORK SLICING

Network slicing allows multiple logical virtual slices to share a physical network. It brings flexibility and scalability to the 5G network architecture. Fig. 1 illustrates a three-layer system model of the 5G core network slicing. It shows three entities in network slicing: the network infrastructure provider, the slice provider, and the slice tenants. Although network slicing brings many benefits, the operations of the three entities are relatively independent. Therefore, they may not be able to collaborate to ensure that network slices run securely. Conversely, each entity may operate in a malicious manner to gain benefits. Thus, hosting multiple logical slices on a shared physical network presents new security challenges [4].

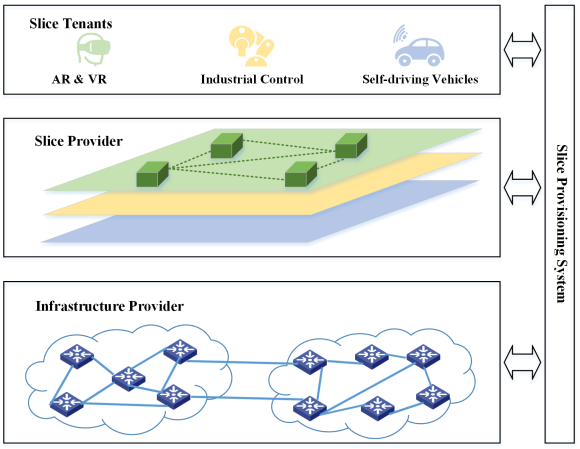


FIGURE 1. Three-layer 5G core network slicing system model.

In our study, we consider the following two security issues in network slicing [9]:

1) The attack on the physical node affecting the slice node: the physical node provides resources for the slice node. When the physical node is maliciously attacked, it can modify the information of the slice node through the virtualization manager, launch the sniffing attack, and block the traffic in the slice.
2) The attack on the slice node affecting the physical node: the malicious slice node attacks a physical node and gains control of it by exploiting the vulnerability of the physical node. For example, the slice node can initiate a DoS attack, continuously inject error information into the physical host in a flooding manner, and finally cause the physical node to reject other slice requests due to lack of physical resources.

In our study, we abstract security issues in the network slicing environment such as information leakage, eavesdropping, DoS attack, etc. into the security requirement and security level instead of delving into specific security issues. Thus, we introduce the node security requirement and security level to model the above two security issues. For the physical node, its security requirement indicates the security level demand for the slice nodes provisioned on it. The higher the security requirement, the higher the security level of slice nodes. Similarly, for the slice node, its security requirement indicates the security level demand for the physical node. The two types

of security constraints corresponding to the above security issues are summarized as follows:

1) The slice node needs to be provisioned on the physical node it trusts, that is, the security level of the physical node cannot be lower than the security requirement of the slice node it hosts.
2) The physical node only hosts the slice nodes it trusts, that is, the security level of the slice node cannot be lower than the security requirement of the physical node that hosts it.

B. SYSTEM MODEL AND PROBLEM FORMULATION

We model the 5G core infrastructure topology as a weighted undirected graph $G^I = (V^I, E^I)$, where V^I is the set of physical nodes and E^I is the set of physical links. For each physical node $v^I \in V^I$, its initial total and available computing capacity are respectively denoted by $c_0(v^I)$ and $c_a(v^I)$. The security requirement and security level of the node v^I are denoted by $sr(v^I)$ and $sl(v^I)$, respectively. Each physical link $e^I \in E^I$ has initial total and available bandwidth represented by $b_0(e^I)$ and $b_a(e^I)$, respectively. P^I denotes the set of all loop-free paths in the infrastructure. The set of loop-free physical paths between v_i^I and v_j^I is denoted by $P^I(v_i^I, v_j^I)$. For each path $p^I(v_i^I, v_j^I) \in P^I(v_i^I, v_j^I)$, $L(p^I(v_i^I, v_j^I))$ is the set of links in $p^I(v_i^I, v_j^I)$. Then the bandwidth of $p^I(v_i^I, v_j^I)$ is defined as $b(p^I(v_i^I, v_j^I)) = \min_{e^I \in L(p^I(v_i^I, v_j^I))} b(e^I)$.

We model the m^{th} slice request as a triplet $SR_m = (G_m^S, t_m^a, t_m^l)$, where G_m^S, t_m^a, and t_m^l represent the topology of the m^{th} slice, its arrival time, and its lifetime, respectively. The slice topology is represented by a weighted undirected graph $G^S = (V^S, E^S)$ where V^S is the set of slice nodes of the request and E^S is the set of slice links. The required computing capability of slice node $v^S \in V^S$ is denoted by $c(v^S)$. The security requirement and security level of v^S are denoted by $sr(v^S)$ and $sl(v^S)$, respectively. Each slice link $e^S \in E^S$ is characterized by the amount of required bandwidth $b(e^S)$.

In order to efficiently utilize physical network resources, we take minimizing slice provisioning cost as our objective to increase the provisioning revenue-to-cost ratio. We formulate ES-CNSP problem into the following integer linear programming (ILP) model by introducing resource and security constraints.

$$\min \sum_{v_k^S \in V^S} \sum_{v_i^I \in V^I} x_i^k (1 + sl(v_i^I)) c(v_k^S) + \sum_{e_{kl}^S \in E^S} \sum_{e_{ij}^I \in E^I} y_{ij}^{kl} b(e_{kl}^S)$$

$$\text{s.t.} \sum_{v_i^I} x_i^k = 1, \quad \forall v_k^S \in V^S \tag{1}$$

$$\sum_{v_k^S} x_i^k \le 1, \quad \forall v_i^I \in V^I \tag{2}$$

$$x_i^k c(v_k^S) \le c_a(v_i^I), \quad \forall v_i^I \in V^I, \ \forall v_k^S \in V^S \tag{3}$$

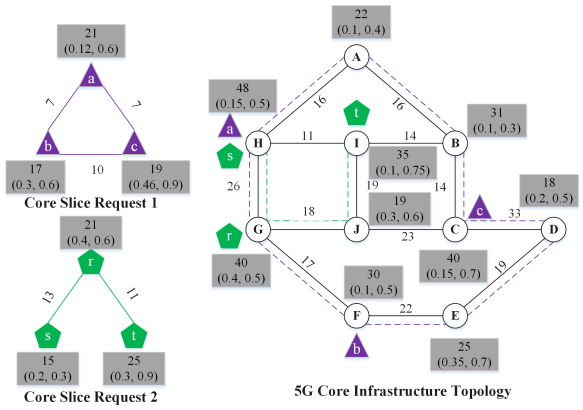


FIGURE 2. An example of 5G core slice resource provisioning.

$$x_i^k sr(v_k^S) \le sl(v_i^I), \quad \forall v_i^I \in V^I, \ \forall v_k^S \in V^S \tag{4}$$

$$x_i^k sr(v_i^I) \le sl(v_k^S), \quad \forall v_i^I \in V^I, \ \forall v_k^S \in V^S \tag{5}$$

$$\sum_{v_j^I} (y_{ij}^{kl} - y_{ji}^{kl}) = x_i^k - x_i^l, \quad \forall e_{kl}^S \in E^S, \ v_i^I \in V^I \tag{6}$$

$$\sum_{e_{kl}^S} y_{ij}^{kl} b(e_{kl}^S) \le b_a(e_{ij}^I), \quad \forall e_{ij}^I \in E^I. \tag{7}$$

x_i^k indicates whether the slice node v_k^S is provisioned onto the physical node v_i^I or not. If v_k^S is provisioned onto v_i^I, x_i^k is 1. Otherwise it is 0. y_{ij}^{kl} indicates whether the physical link e_{ij}^I hosts the slice link e_{kl}^S. If the physical link e_{ij}^I hosts the slice link e_{kl}^S, y_{ij}^{kl} is 1. Otherwise it is 0. Since the network infrastructure provider needs to use additional resources to ensure the security level of physical nodes, for the objective function, we not only consider the cost of provisioning resources, i.e., node CPU capacity cost and link bandwidth cost, but also consider the cost of satisfying security requirement of slice nodes, i.e., security cost. The constraint (1) ensures that each slice node should be provisioned onto one physical node. Eq. (2) guarantees each physical node can only host one slice node from the same slice request. The constraint (3) is the CPU capacity constraint. The constraints (4) and (5) are security constraints as we discussed above. Eq. (6) ensures that each slice link is provisioned onto a physical path and the flow passing through physical nodes on the path except the end nodes is 0. The constraint (7) guarantees that the sum of bandwidth requested by all the slice links that are provisioned onto one physical link cannot exceed its available bandwidth.

C. AN EXAMPLE OF SLICE PROVISIONING

According to our proposed system model, we give a concrete example of 5G core network slice provisioning shown in Fig. 2. The right side of Fig. 2 shows the 5G core infrastructure topology. The number and the ordered pair in the grey rectangle next to the node indicate the available CPU capacity and security feature of the physical node, respectively. The first element in the ordered pair is the security requirement,

and the other is the security level. In our study, the security level is expressed as a real number between 0 and 1 and security requirement is expressed as a real number between 0 and 0.5 as described in Section VI. The number next to the link indicates available bandwidth of the physical link. The left side of Fig. 2 illustrates two 5G core network slice requests (i.e., in purple triangles and green pentagons). The number in the rectangle next to the node indicates the CPU demand of the slice node and the ordered pair in the rectangle represents the security requirement and security level of the slice node. The number by the link denotes the amount of bandwidth requested by the slice link. The slice provisioning result which satisfies the resource constraints and security constraints is presented on the right side of Fig.2. Slice nodes a, b, and c of the slice request 1 are provisioned onto the physical nodes H, F, and C, respectively. Slice links a-b, b-c, and a-c are provisioned on the physical path H-G-F, F-E-D-C, and H-A-B-C, respectively. Slice nodes r, s, t of slice request 2 are provisioned onto physical nodes G, H and I, respectively. Slice links r-s and r-t are provisioned on physical paths G-H and G-J-I, respectively.

D. PERFORMANCE METRICS

The 5G core network infrastructure provider expects to maximize the operating profit during the long-term operation. Thus, the main objective of the slice provisioning is to maximize provisioning revenue, reduce provisioning cost and accept more slices. In our study, the performance of the slice provisioning algorithm is evaluated by using slice acceptance ratio and provisioning revenue-to-cost ratio. The two metrics are defined as follows.

Slice acceptance ratio (AR)**:** it is defined below.

$$AR = \lim_{T\to+\infty} \frac{\sum_{t=0}^{T} S_m(t)}{\sum_{t=0}^{T} S(t)} \tag{8}$$

where $\sum_{t=0}^{T} S_m(t)$ is the number of slice requests provisioned successfully and $\sum_{t=0}^{T} S(t)$ is the total number of slice requests from time $t = 0$ to T.

Provisioning revenue-to-cost ratio (RC)**:** We assume the unit price of CPU capacity and bandwidth is 1 and also consider the cost or revenue caused by meeting the security requirements. Then we define the provisioning revenue and cost of slice request G^S at time t as follows.

$$Rev(G^S, t) = \sum_{v^S \in V^S} (1 + sr(v^S))c(v^S) + \sum_{e^S \in E^S} b(e^S) \tag{9}$$

$$Cost(G^S, t) = \sum_{v^S \in V^S} (1 + sl(v^I))c(v^S) + \sum_{e^S \in E^S} |L(p^I(e^S))|b(e^S) \tag{10}$$

$p^I(e^S)$ is the physical path hosting the slice link e^S, and $L(p^I(e^S))$ denotes the set of physical links in $p^I(e^S)$. Hence, we define provisioning revenue-to-cost ratio as:

$$RC = \frac{Rev}{Cost} = \lim_{T\to+\infty} \frac{\sum_{t=0}^{T} \sum_{G^S \in S_m(t)} Rev(G^S, t)}{\sum_{t=0}^{T} \sum_{G^S \in S_m(t)} Cost(G^S, t)} \tag{11}$$

IV. NODE IMPORTANCE RANKING BASED ON THE VIKOR APPROACH

In our study, we introduce the concept of node importance from the complex-network theory [30] to indicate the order in which the slice nodes are provisioned. The node importance is affected by many factors. In the traditional virtual network embedding (VNE) problem [6], most studies use the node resource attributes [10] to evaluate the importance of nodes. Several studies consider node topology attributes on the node importance besides resource attributes [12], [13]. However, they simply combine topology attributes and resource attributes as one metric to measure the node importance. Therefore, in this section, we first propose the node attributes related to resource and topology. Then we describe the VIKOR approach to comprehensively evaluate the node importance using the defined attributes.

A. NODE ATTRIBUTES

During the process of slice nodes provisioning, physical nodes with higher available CPU and adjacent link bandwidth should be given higher priority to host slice nodes. Slice nodes with higher requested CPU and adjacent link bandwidth should be provisioned preferentially. However, considering only node resources may cause node load imbalance and inefficient resource utilization issues. Therefore, we also consider the topology attributes (i.e., degree centrality and closeness centrality) to avoid these issues. The node degree centrality characterizes the local connection richness of the node in the network. The larger it is, more chance the physical node has to host slice nodes. The node closeness centrality characterizes the distance from the node to all other nodes from a global perspective. The larger the closeness centrality, the easier it is to obtain a shorter path, thus reducing the use of bandwidth resources. These discussed factors contribute to the node importance. Therefore, we use node computing capability, node's adjacent link bandwidth, local topology attribute, and global topology attribute to evaluate the importance of a node. They are defined below.

1) NODE COMPUTING CAPABILITY

We regard the computing capability of a node as a local resource attribute. For the physical node, the computing capability is its available CPU. The physical node with more available CPU is able to host more slice nodes. For the slice node, the computing capability is its requested CPU. The slice node with more requested CPU should be given

higher priority when slice nodes are provisioned. The node computing capability is defined as follows.

$$NC(v_i) = c(v_i) \tag{12}$$

2) ADJACENT LINK BANDWIDTH

We define the sum of the bandwidth of all adjacent links of a node as another resource attribute. For the physical node, the bandwidth of its adjacent link is the available bandwidth. It is easier to find a physical path to host the slice links which are connected to the slice node provisioned onto the physical node with greater sum of the bandwidth of all adjacent links. For the slice node, the bandwidth of its adjacent slice link refers to the amount of bandwidth it requests. Since the slice node with greater sum of the bandwidth of all adjacent links is more difficult to be provisioned, it should be provisioned preferentially.

$$LB(v_i) = \sum_{e \in E(v_i)} b(e) \tag{13}$$

where $E(v_i)$ is the set of all the adjacent links of v_i.

3) LOCAL TOPOLOGY ATTRIBUTE

The degree centrality [30] of a node is introduced to represent its local topology attribute. It is defined as the number of a node's adjacent links. Degree centrality reflects the local importance of a node. The physical node with larger degree centrality has more adjacent links, therefore, it is easier to find a physical path to host the slice links connected with the slice node provisioned on it.

$$LT(v_i) = \sum_{v_j} a_{ij} \tag{14}$$

where a_{ij} is 1 if the node v_i and the node v_j is connected by a link. Otherwise it is 0.

4) GLOBAL TOPOLOGY ATTRIBUTE

We use the closeness centrality [30] to represent the node global topology attribute. It is calculated as the reciprocal of the sum of the shortest paths of the node to all other nodes. The closeness centrality evaluates the global importance of a node based on the shortest path. Thus, shorter physical path can be obtained for the slice links connected with the slice node which is provisioned onto the physical node with larger closeness centrality. The following is the definition of closeness centrality.

$$GT(v_i) = \frac{1}{\sum_{i \neq j} d(v_i, v_j)} \tag{15}$$

where $d(v_i, v_j)$ is the length of the shortest path between node v_i and node v_j.

B. VIKOR APPROACH

The evaluation of node importance using multiple attributes of the node defined above is a Multiple Attribute Decision Making (MADM) problem [31]. The procedure of solving the MADM problems is shown in Fig. 3. We use the VIKOR method proposed by Opricovic [14] to evaluate node importance. The VIKOR method is a compromise ranking method based on the ideal solution. It ranks the alternatives according to the distance between their attributes and the ideal solution, providing a maximum "group utility" for the "majority" and a minimum of an "individual regret" for the "opponent" to make the decision process more rational. The idea of the evaluation of node importance based on VIKOR is to regard network nodes as alternatives and use the node attributes defined above to comprehensively evaluate the nodes. The VIKOR approach is described in detail below:

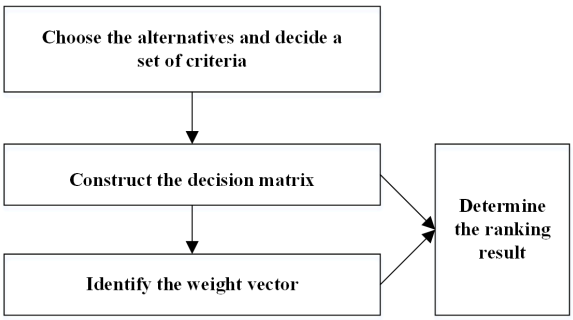


FIGURE 3. Procedure for solving MADM problems.

Step 1: Constructing the decision matrix.

In a network with n nodes, each node is an alternative, and it has m attributes. The attributes for each alternative can be expressed in the form of a decision matrix as follow:

$$X_{n\times m} = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1m} \\ x_{21} & x_{22} & \cdots & x_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nm} \end{bmatrix} \tag{16}$$

In the above equation, an element x_{ij} of the decision matrix $X_{n\times m}$ is the value of the i^{th} alternative in terms of the j^{th} attribute.

Step 2: Normalizing the decision matrix.

In order to eliminate the influence caused by the different dimensions of the attributes, the values of the attributes need to be normalized. We use $Z_{n\times m}$ to denote the normalized matrix. Each element x_{ij} in the decision matrix $X_{n\times m}$ is normalized according to the following formula (i.e., L2 normalization).

$$z_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^{n} x_{ij}^2}}, \quad i = 1, 2, \cdots, n;\ j = 1, 2, \cdots, m. \tag{17}$$

Step 3: Evaluating nodes based on the VIKOR approach.

First, the positive ideal solution and the negative ideal solution are determined. The positive ideal solution consists of the maximum value of each attribute, while the negative

ideal solution consists of the minimum value of each attribute.

$$Z^+ = \{\max_i z_{ij}\} = \{z_1^+, z_2^+, \cdots, z_m^+\}. \quad (18)$$

$$Z^- = \{\min_i z_{ij}\} = \{z_1^-, z_2^-, \cdots, z_m^-\}. \quad (19)$$

Next, S_i (i.e., group utility) and R_i (i.e., individual regret) are calculated.

$$S_i = \sum_{j=1}^{m} \omega_j \frac{|z_j^+ - z_{ij}|}{|z_j^+ - z_j^-|}. \quad (20)$$

$$R_i = \max_j \{\omega_j \frac{|z_j^+ - z_{ij}|}{|z_j^+ - z_j^-|}\}. \quad (21)$$

Where $\omega_j = \frac{1}{m}$. Then, the VIKOR index (i.e., node importance here) value Q_i for the i^{th} alternative is calculated:

$$Q_i = \xi \frac{S_i - S^*}{S^- - S^*} + (1-\xi)\frac{R_i - R^*}{R^- - R^*} \quad i = 1, 2, \cdots, n. \quad (22)$$

Where $S^* = \min_i S_i$, $S^- = \max_i S_i$, $R^* = \min_i R_i$, and $R^- = \max_i R_i$. Finally, the alternatives are ranked according to Q_i in the ascending order.

V. HEURISTIC ALGORITHM DESIGN

In this section, we propose a heuristic algorithm named VIKOR-CNSP to solve the efficient and secure 5G core network slice provisioning problem. The algorithm includes two stages: slice node provisioning and slice link provisioning. The slice nodes are provisioned according to the node ranking results obtained through the VIKOR method. The slice links are provisioned by the Yen k shortest path algorithm [32] combined with our proposed path selection strategy. The detailed algorithms are described below.

A. SLICE NODE PROVISIONING BASED ON THE VIKOR APPROACH

When a slice request arrives at the slice provisioning system, the slice node importance is evaluated according to the VIKOR method described above and ranked by the Q value from small to large. The smaller the Q value, more preferentially the slice node is provisioned. The physical node importance is evaluated in the same way. The slice nodes are sequentially provisioned in ascending order of their Q value. First, candidate physical nodes that satisfy the slice node resource constraints and security constraints are obtained. Then, the slice node is hosted on the physical node with the smallest Q value. The slice node provisioning is presented in Algorithm 1.

Algorithm 1 Slice Node Provisioning Based on VIKOR Approach

Input: Infrastructure network G^I and slice request G^S
Output: Slice node provisioning map

for each slice node $v^S \in V^S$ **do**
  Q value is calculated using VIKOR Approach.
end for
Rank slice nodes in ascending order of Q value and put the ranking results into *sliceNodeList*.
for each physical node $v^I \in V^I$ **do**
  Q value is calculated using VIKOR Approach.
end for
for each slice node $v^S \in$ *sliceNodeList* **do**
  Obtain the candidate physical nodes *candidate*(v^S) for v^S satisfying the resource and security constraints.
  if *candidate*(v^S) is not empty **then**
    Provision v^S onto the candidate physical node which has the smallest Q.
    Put the provisioning result of v^S into *sliceNodeProvisioningMap*.
  else
    return *sliceNodeProvisioningFailed*
  end if
end for
return *sliceNodeProvisioningMap*

B. SLICE LINK PROVISIONING USING SMALLEST PATH FACTOR

Slice links are provisioned by implementing the k shortest path algorithm. First, the k shortest path algorithm obtains k candidate physical paths for the slice link. To further improve the slice acceptance ratio and resource utilization, we propose a novel path selection strategy. We define the product of the maximum link bandwidth utilization along the path and its hop-count as the path factor P_f, which is defined as Eq.(23). The strategy selects the path with the smallest P_f from the candidate paths to host the slice link. The reason why we design this strategy is that the physical link with excessive bandwidth utilization in the path is likely to become a bottleneck in the subsequent provisioning process, causing subsequent slice requests to be rejected. In addition, the physical path with fewer hops helps in saving bandwidth, thus increasing the utilization of bandwidth resources. Slice link provisioning is described in Algorithm 2.

$$P_f = (1 - \frac{b_a(e^I)}{b_0(e^I)})_{max} \cdot |L(p^I)|. \quad (23)$$

C. SLICE PROVISIONING PROCEDURES

The two-stage slice provisioning procedures are described in Algorithm 3. In order to provide a clear understanding of the proposed algorithm, the flowchart is shown in Fig. 4.

D. TIME COMPLEXITY OF VIKOR-CNSP

In this section, we analyze the time complexity of the VIKOR-CNSP algorithm. In the node provisioning stage, there are $|V^I|$ alternatives evaluated by VIKOR. For each alternative, the time complexity of calculating attributes is dominated by the calculation of closeness centrality. Its complexity is $O(|V^I||E^I| + |V^I|^2)$. In the slice link provisioning stage, the time complexity is dominated by the k

Algorithm 2 Slice Link Provisioning Using Smallest Path Factor

Input: Infrastructure network G^I, slice request G^S, and slice node provisioning results *sliceNodeProvisioningMap*

Output: Slice link provisioning map

Rank all the slice links in E^S based on bandwidth requirements from large to small and put the ranking results into *sliceLinkList*.
for each slice link $e^S \in$ *sliceLinkList* **do**
  Obtain the candidate substrate paths *substratePathList* for e^S meeting its bandwidth demand by implementing the k shortest path algorithm.
  if *substratePathList* is not empty **then**
    for each substrate path *substratePath* $\in$ *substratePathList* **do**
      Calculate P_f based on Eq.(23).
    end for
    Provision e^S onto the candidate substrate path with the minimum P_f.
  else
    return *sliceLinkProvisioningFailed*
  end if
end for
return *sliceLinkProvisioningMap*

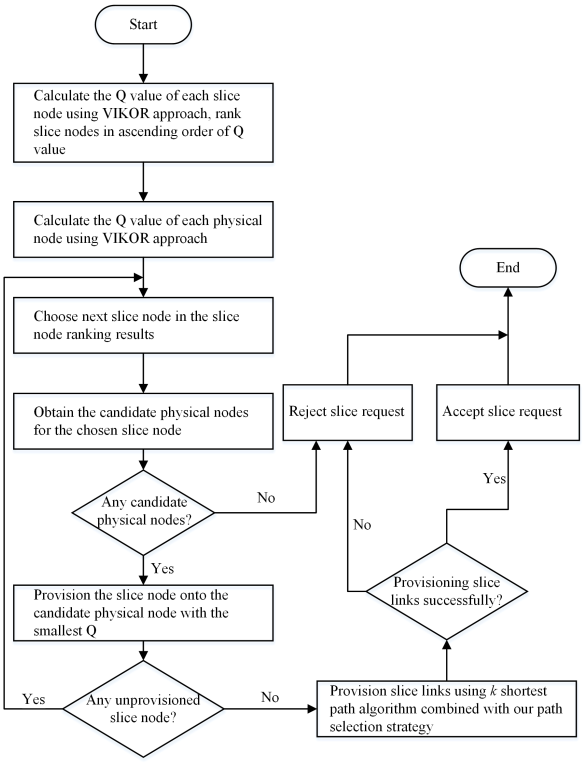


FIGURE 4. Algorithm flowchart.

shortest algorithm, which is $O(k|V^I|(|E^I| + |V^I|log|V^I|))$. Therefore, VIKOR-CNSP has polynomial running time of $O(|V^I|^2|E^I| + |V^I|^3) + O(k|V^I|(|E^I| + |V^I|log|V^I|))$.

Algorithm 3 Slice Provisioning Algorithm VIKOR-CNSP

Input: Infrastructure network G^I and the i^{th} slice request $SR_i = (G_i^S, t_i^a, t_i^l)$

Output: Slice provisioning result

Release the physical resources occupied by the slice requests ending at t_i^a and update physical resources.
Slice nodes of G_i^S are provisioned using Algorithm 1.
if Slice nodes provisioning failed **then**
  return *sliceProvisioningFailed*
else
  Slice links of G_i^S are provisioned using Algorithm 2.
  if Slice links provisioning failed **then**
    return *sliceProvisioningFailed*
  else
    Allocate physical resources to slice request G_i^S and update physical resources.
    return *sliceProvisioningSucceeded*
  end if
end if

TABLE 3. Algorithms for comparison.

Notation	Description
VIKOR-CNSP	Our proposed provisioning algorithm considering resource and topology attributes based on VIKOR approach
TOPSIS-CNSP	The algorithm considering resource and topology attributes based on TOPSIS approach in [33]
BL	The baseline algorithm only considering local resources in [10]
CC	The algorithm in [34] considering closeness centrality

VI. PERFORMANCE EVALUATION AND RESULTS DISCUSSION

In this section, we describe the simulation settings and experimental scenarios for the evaluation. To verify the performance of our algorithm, we compare our proposed algorithm with the existing VNE algorithms listed in Table 3. The performance metrics focus on the slice acceptance ratio, the slice provisioning revenue-to-cost ratio, the node utilization, and the link utilization.

A. SIMULATION SETTINGS

We have developed a simulator named VIKORSlicePro using JAVA. The Brite tool [35] has been integrated into the simulator to generate the infrastructure network and the 5G core network slice topology based on the Waxman topology model with the parameter $\alpha = 0.15$ and the exponential parameter $\beta = 0.2$ [36]. In order to be able to compare our algorithm, we use parameter settings similar to those in existing VNE studies [10], [12], [37].

The infrastructure network size is set to 100 nodes, and adjacent nodes are connected with a probability of 0.5. The node security level takes a real number uniformly distributed between 0 and 1. The node security requirement is a real number uniformly distributed between 0 and 0.5. The initial node computing capacity and link bandwidth capacity are real

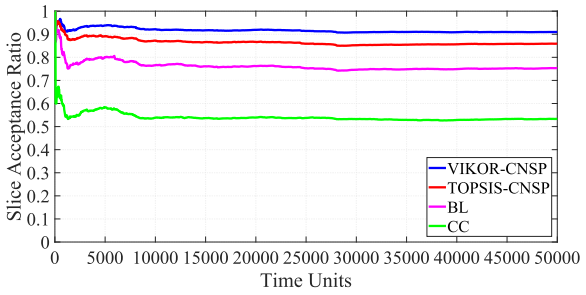


FIGURE 5. Slice acceptance ratio with a slice traffic load of 20 Erlangs.

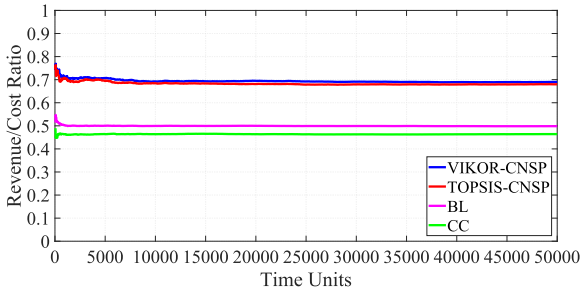


FIGURE 6. Provisioning revenue-to-cost ratio with a slice traffic load of 20 Erlangs.

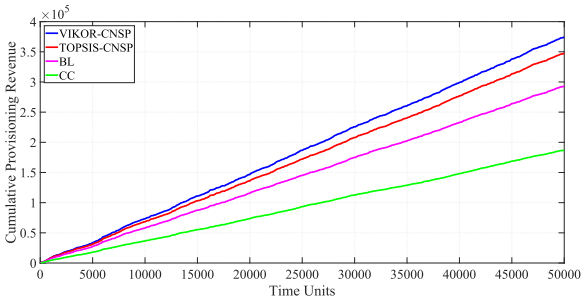


FIGURE 7. Cumulative provisioning revenue with a slice traffic load of 20 Erlangs.

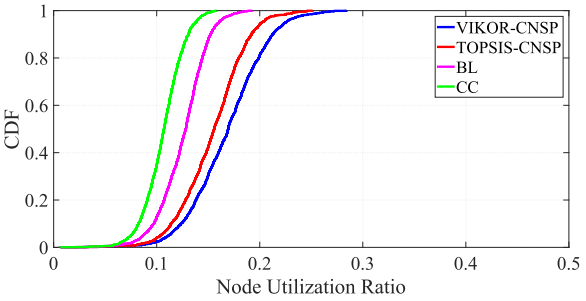


FIGURE 8. Node utilization CDF with a slice traffic load of 20 Erlangs.

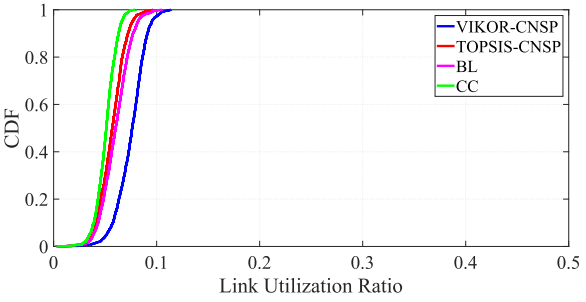


FIGURE 9. Link utilization CDF with a slice traffic load of 20 Erlangs.

numbers uniformly distributed between 50 and 100. Without loss of generality, we set the unit price of the computing and bandwidth resources to 1.

The number of the slice nodes in a slice request is between 3 and 10 and they are connected by a probability of 0.5. The parameters of slice node security level and security requirement are taken the same way as physical node. The CPU capacity requested takes a uniformly distributed real number between 0 and 20. The bandwidth requested is a real number uniformly distributed in the range [0, 50].

Slice requests arrive according to a Poisson process with a mean arrival rate of λ. The lifetime of the slice request follows an exponential distribution with a mean of $\frac{1}{\mu} = 500$ time units yielding to slice traffic of $\lambda \times \frac{1}{\mu}$ Erlangs. We run each simulation scenario for 50,000 time units.

B. RESULTS DISCUSSION

1) SLICE TRAFFIC LOAD OF 20 Erlangs SCENARIO

First, we examine the simulation scenario in which the slice request arrival rate is 4 requests per 100 time units yielding to a slice traffic load of 20 Erlangs. The slice acceptance ratio, slice provisioning revenue-to-cost ratio and cumulative revenue, and resource utilization of the four algorithms are depicted in Fig. 5, Fig. 6, Fig. 7, Fig. 8, and Fig. 9, respectively. We obtain the reported results by averaging the performance metrics from 10 independent simulations.

Fig. 5 shows that our proposed VIKOR-CNSP algorithm has the highest slice acceptance ratio throughout the simulation. The slice acceptance ratio of the four algorithms is relatively high at the beginning of the simulation because the node computing capacity and link bandwidth are sufficient. As the simulation progresses, the resources available are gradually reduced which results in a reduction in the slice acceptance ratio. After about 10, 000 time units, the slice acceptance ratio tends to be stable. The reason is that the arrival and departure of the slices reach a relatively balanced state, and thus the available resources of the physical network are relatively stable. In the stable state, the VIKOR-CNSP performs 5.92%, 20.78%, 70.54% better than TOPSIS-CNSP, BL, and CC, respectively.

Our proposed algorithm has the highest slice acceptance ratio because it can comprehensively evaluate nodes from the perspective of both resource attributes and topology attributes, and the proposed path selection strategy avoids bottleneck paths. In addition, although TOPSIS-CNSP also takes into account resource attributes and topology attributes, TOPSIS does not consider the relative importance of the

"shortest distance" from the ideal solution and the "farthest distance" from the negative-ideal solution while VIKOR does [14]. Thus, VIKOR-CNSP outperforms TOPSIS-CNSP.

Fig. 6 presents the slice provisioning revenue-to-cost ratio. As shown in Fig. 6, the VIKOR-CNSP algorithm has the largest slice provisioning revenue-to-cost ratio. The revenue-to-cost ratio decreases rapidly in the early stage of simulation because the physical resources are consumed as the slice arrives, which causes that the subsequent arriving slices are provisioned on the physical path with more hops so that increases the provisioning cost. When the simulation time reaches 10, 000 time units, the revenue-to-cost ratio tends to be stable because the arrival and departure of the slices reach a relatively balanced state.

Fig. 7 presents the cumulative provisioning revenue. As shown, that the VIKOR-CNSP algorithm can obtain the most cumulative provisioning revenue and it has the fastest revenue growth. The reason is that VIKOR-CNSP can reasonably evaluate nodes in the node provisioning stage, and thus can accept more slice requests than other algorithms.

Fig. 8 and 9 show the cumulative distribution function (CDF) of node utilization ratio, and CDF of link utilization ratio, respectively. The VIKOR-CNSP has the highest node and link utilization ratios. The figures indicate that the VIKOR-CNSP allocates more resource to slices than other algorithms. This is consistent with Fig. 5. In addition, we notice that the node utilization has a dependency on the slice acceptance ratio which means that the higher the slice acceptance ratio, the better the node utilization while the link utilization shows a different behavior. The reason is that one slice node is provisioned on one physical node, whereas one slice link could be provisioned in many ways.

2) VARIABLE SLICE TRAFFIC LOAD SCENARIOS

We evaluate our algorithm under the simulation scenarios where the slice arrival rate is 2, 4, 6, 8, and 10 slice requests per 100 time units producing slice traffic loads of 10, 20, 30, 40, and 50 Erlangs. The slice acceptance ratio and the revenue-to-cost ratio of the algorithms are presented in Fig. 10 and Fig. 11, respectively. For all the algorithms, the slice acceptance ratio decreases as the slice traffic load increases. Because the physical network resources get scarce at heavier load, the slice requests are more likely to be rejected. The revenue-to-cost ratio decreases from a load of 20 Erlangs to 40 Erlangs, while after 40 Erlangs it tends to be stable. Because the slice links are provisioned along the shorter physical path under light load scenario and the lower slice acceptance ratio under heavy load scenario makes revenue-to-cost reach a relatively stable state. In all scenarios, the VIKOR-CNSP has the highest slice acceptance ratio while its revenue-to-cost ratio is slightly smaller than TOPSIS-CNSP but very close after slice traffic load reaching 30 Erlangs. VIKOR-CNSP may be still preferred since it has a higher slice acceptance ratio which may bring a better higher slice tenant satisfaction.

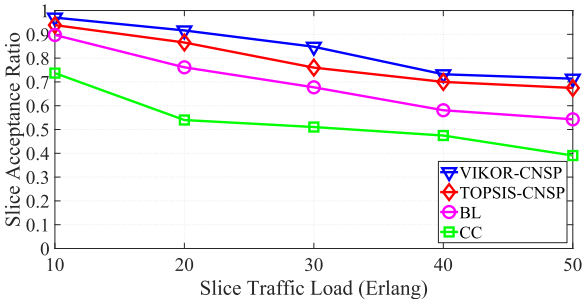


FIGURE 10. Slice acceptance ratio with variable slice traffic load.

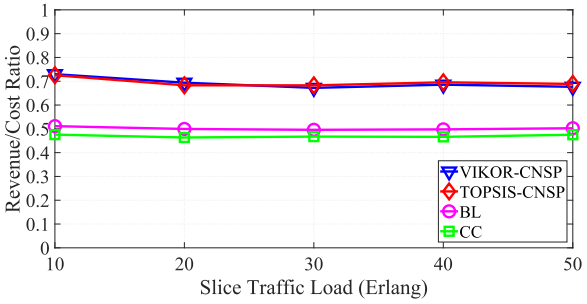


FIGURE 11. Provisioning revenue-to-cost ratio with variable slice traffic load.

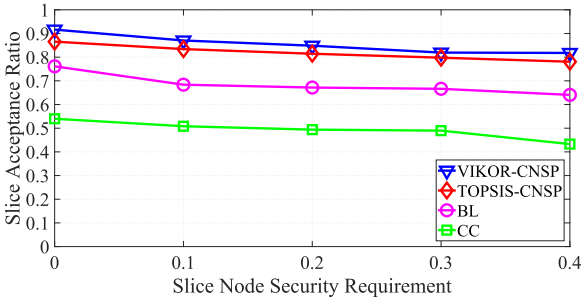


FIGURE 12. Slice acceptance ratio with the variable slice security requirement.

3) VARIABLE SLICE SECURITY REQUIREMENT SCENARIO

In practice, different types of services may have different security requirements. Therefore, we study the efficiency of our slice provisioning algorithm in different slice node security requirements scenarios. In the experiment, the security requirement of the slice node is set to a uniform distribution of $[x, 0.5]$, where x is the minimum value of the slice node security requirement. The slice security requirement increases with the increase of x, which takes the value 0, 0.1, 0.2, 0.3, 0.4. The other parameters in the experiment are the same as slice traffic load of 20 Erlangs scenario. Fig. 12 shows that the slice acceptance ratio decreases as the security requirement of the slice node increases. This is because it is more difficult to find physical nodes satisfying slice security requirements under stricter security requirement, which cause more slices to be rejected. However, our algorithm has the highest slice acceptance ratio throughout the experiments.

VII. CONCLUSION

In this paper, we have formulated the secure 5G core network slice provisioning problem and proposed a heuristic slice provisioning algorithm named VIKOR-CNSP based on the VIKOR approach to enable slices to efficiently share the physical network resources. Our algorithm uses the VIKOR method to comprehensively evaluate nodes importance and to rank nodes considering network resource and topology attributes. The slice nodes are then provisioned according to the ranking results. In the slice link provisioning phase, we implement the k shortest path algorithm and propose a path selection strategy to provision slice links.

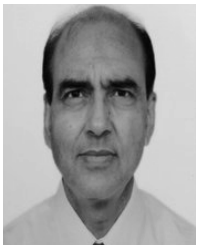
Extensive simulations verify that our proposed algorithm can efficiently utilize network resources to obtain the highest slice acceptance ratio and the best revenue-to-cost ratio performance satisfying the resource and security constraints as compared to other algorithms. Further, we studied the performance of the algorithm under different slice traffic loads and different slice security requirements. The results show that our algorithm can still produce the best performance. In the future, we plan to study the dynamic reprovisioning of slices to further improve slice acceptance ratio and provisioning revenue and cost.

REFERENCES

[1] *Report on Standards Gap Analysis*, document ITU-T SG 13, Dec. 2015.
[2] N. G. Alliance, "Description of network slicing concept," NGMN, Frankfurt, Germany, Tech. Rep. V1.0, Jan. 2016.
[3] *Study on Management and Orchestration of Network Slicing for Next Generation Network (Release 15)*, document TS 28.801, 3GPP, Dec. 2018.
[4] X. Li, M. Samaka, H. A. Chan, D. Bhamare, L. Gupta, C. Guo, and R. Jain, "Network slicing for 5G: Challenges and opportunities," *IEEE Internet Comput.*, vol. 21, no. 5, pp. 20–27, Sep. 2017.
[5] T. Anderson, L. Peterson, S. Shenker, and J. Turner, "Overcoming the Internet impasse through virtualization," *Computer*, vol. 1, no. 4, pp. 34–41, 2005.
[6] A. Fischer, J. F. Botero, M. T. Beck, H. de Meer, and X. Hesselbach, "Virtual network embedding: A survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 1888–1906, 4th Quart., 2013.
[7] M. Leconte, G. S. Paschos, P. Mertikopoulos, and U. C. Kozat, "A resource allocation framework for network slicing," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2018, pp. 2177–2185.
[8] S. Natarajan and T. Wolf, "Security issues in network virtualization for the future Internet," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Jan./Feb. 2012, pp. 537–543.
[9] A. Fischer and H. De Meer, "Position paper: Secure virtual network embedding," *Praxis der Informationsverarbeitung und Kommunikation*, vol. 34, no. 4, pp. 190–193, 2011.
[10] M. Yu, Y. Yi, J. Rexford, and M. Chiang, "Rethinking virtual network embedding: Substrate support for path splitting and migration," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 17–29, Apr. 2008.
[11] P. Zhang, H. Yao, and Y. Liu, "Virtual network embedding based on computing, network, and storage resource constraints," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3298–3304, Oct. 2018.
[12] H. Cao, L. Yang, and H. Zhu, "Novel node-ranking approach and multiple topology attributes-based embedding algorithm for single-domain virtual network embedding," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 108–120, Feb. 2018.
[13] P. Zhang, H. Yao, and Y. Liu, "Virtual network embedding based on the degree and clustering coefficient information," *IEEE Access*, vol. 4, pp. 8572–8580, 2016.
[14] S. Opricovic and G.-H. Tzeng, "Compromise solution by MCDM methods: A comparative analysis of VIKOR and TOPSIS," *Eur. J. Oper. Res.*, vol. 156, no. 2, pp. 445–455, Jul. 2004.
[15] Y. L. Lee, J. Loo, T. C. Chuah, and L.-C. Wang, "Dynamic network slicing for multitenant heterogeneous cloud radio access networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 4, pp. 2146–2161, Apr. 2018.
[16] Y. Sun, M. Peng, S. Mao, and S. Yan, "Hierarchical radio resource allocation for network slicing in fog radio access networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 3866–3881, Apr. 2019.
[17] A. Fendt, C. Mannweiler, L. C. Schmelz, and B. Bauer, "A formal optimization model for 5G mobile network slice resource allocation," in *Proc. IEEE 9th Annu. Inf. Technol., Electron. Mobile Commun. Conf. (IEMCON)*, Nov. 2018, pp. 101–106.
[18] C. Delgado, M. Canales, J. Ortín, J. R. Gállego, A. Redondi, S. Bousnina, and M. Cesana, "Joint application admission control and network slicing in virtual sensor networks," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 28–43, Feb. 2018.
[19] D. T. Hoang, D. Niyato, P. Wang, A. De Domenico, and E. C. Strinati, "Optimal cross slice orchestration for 5G mobile services," in *Proc. IEEE 88th Veh. Technol. Conf. (VTC-Fall)*, Aug. 2018, pp. 1–5.
[20] Q. Ye, J. Li, K. Qu, W. Zhuang, X. S. Shen, and X. Li, "End-to-end quality of service in 5G networks: Examining the effectiveness of a network slicing framework," *IEEE Trans. Veh. Technol.*, vol. 13, no. 2, pp. 65–74, Jun. 2018.
[21] *NGMN Publication 5G Security Recommendations Package #2 : Network Slicing*, N. Alliance, Frankfurt, Germany, 2016.
[22] Z. Kotulski, T. Nowak, M. Sepczuk, M. Tunia, R. Artych, K. Bocianiak, T. Osko, and J.-P. Wary, "On end-to-end approach for slice isolation in 5G networks. Fundamental challenges," in *Proc. Federated Conf. Comput. Sci. Inf. Syst. (FedCSIS)*, Sep. 2017, pp. 783–792.
[23] P. Schneider, C. Mannweiler, and S. Kerboeuf, "Providing strong 5G mobile network slice isolation for highly sensitive third-party services," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2018, pp. 1–6.
[24] D. Sattar and A. Matrawy, "Towards secure slicing: Using slice isolation to mitigate DDoS attacks on 5G core network slices," 2019, *arXiv:1901.01443*. [Online]. Available: https://arxiv.org/abs/1901.01443
[25] J. Ni, X. Lin, and X. S. Shen, "Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 3, pp. 644–657, Mar. 2018.
[26] D. G. Andersen, "Theoretical approaches to node assignment," Dept. Comput. Sci., Carnegie Mellon Univ., Pittsburgh, PA, USA, Tech. Rep., 2002. [Online]. Available: http://repository.cmu.edu/compsci/86/
[27] X. Cheng, S. Su, Z. Zhang, H. Wang, F. Yang, Y. Luo, and J. Wang, "Virtual network embedding through topology-aware node ranking," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 2, pp. 38–47, Apr. 2011.
[28] I. Fajjari, N. Aitsaadi, G. Pujolle, and H. Zimmermann, "VNE-AC: Virtual network embedding algorithm based on ant colony metaheuristic," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2011, pp. 1–6.
[29] Z. Zhang, X. Cheng, S. Su, Y. Wang, K. Shuang, and Y. Luo, "A unified enhanced particle swarm optimization-based virtual network embedding algorithm," *Int. J. Commun. Syst.*, vol. 26, no. 8, pp. 1054–1073, 2013.
[30] M. Newman, *Networks: An Introduction*. Oxford, U.K.: Oxford Univ. Press, 2010.
[31] G.-H. Tzeng and J.-J. Huang, *Multiple Attribute Decision Making: Methods and Applications*. Boca Raton, FL, USA: CRC Press, 2011.
[32] J. Y. Yen, "Finding the K shortest loopless paths in a network," *Manage. Sci.*, vol. 17, pp. 712–716, Jul. 1971.
[33] S. Gong, J. Chen, S. Zhao, and Q. Zhu, "Virtual network embedding with multi-attribute node ranking based on topsis," *Ksii Trans. Internet Inf. Syst.*, vol. 10, no. 2, Feb. 2016.
[34] Z. Wang, Y. Han, T. Lin, H. Tang, and S. Ci, "Virtual network embedding by exploiting topological information," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2012, pp. 2603–2608.
[35] A. Medina, A. Lakhina, I. Matta, and J. Byers, "BRITE: Universal topology generation from a user's perspective," Dept. Comput. Sci., Boston Univ., Boston, MA, USA, Tech. Rep. BU-CS-TR-2001-003, Apr. 2005.
[36] B. M. Waxman, "Routing of multipoint connections," *IEEE J. Sel. Areas Commun.*, vol. SAC-6, no. 9, pp. 1617–1622, Dec. 1988.
[37] M. Chowdhury, M. R. Rahman, and R. Boutaba, "ViNEYard: Virtual network embedding algorithms with coordinated node and link mapping," *IEEE/ACM Trans. Netw.*, vol. 20, no. 1, pp. 206–219, Feb. 2012.

XIN LI received the B.S. degree in electronic and information engineering from Wuhan University, China, where he is currently pursuing the Ph.D. degree in communication and information system with the School of Electronic Information. From September 2015 to September 2017, he was a visiting Ph.D. student with the Professor Raj Jain's Group, Washington University in St. Louis, USA. His research interests include 5G, network slicing, network functions virtualization, and software defined networking.

CHENGCHENG GUO received the B.S. and M.S. degrees from the School of Computer Science, Wuhan University, China, in 1984 and 1997, respectively, and the Ph.D. degree from the School of Electronic and Information, Wuhan University, in 2004, where he is currently a Professor and the Ph.D. Supervisor. His research interests include the Internet and communication technology, wireless mesh networks, industry control networks, and real-time and reliability communications.



LAV GUPTA received the B.S. degree from the Indian Institute of Technology, Roorkee, India, in 1978, and the M.S. degree from the Indian Institute of Technology, Kanpur, India, in 1980. He is currently pursuing the Ph.D. degree in computer science and engineering with Washington University in St. Louis, St. Louis, MO, USA. He has worked for about fifteen years in the area of telecommunications planning, deployment, and regulation. He was a Senior Faculty of computer science and access network planning in India and the UAE for a total of about fifteen years. He is the author of one book, 19 articles, and has been a speaker at many international seminars. His current research interests include virtual network services, multicloud systems, fault and performance management in cloud-based network function virtualization, and application of AI in the management of virtual network services over clouds.

RAJ JAIN (F'93) received the B.S. degree in electrical engineering from APS University, Rewa, India, in 1972, the M.S. degree in computer science and controls from 32 IISc, Bengaluru, India, in 1974, and the Ph.D. degree in applied math/computer science from Harvard University, in 1978. He is currently the Barbara J. and Jerome R. Cox, Jr., Professor of computer science and engineering with Washington University in St. Louis. He was one of the Co-founders of Nayna Networks, Inc.,—a next generation telecommunications systems company, San Jose, CA, USA. He is a Fellow of ACM, AAAS, and the Academy of Science, St. Louis. He was a recipient of the 2017 ACM SIGCOMM Life-Time Achievement Award, the 2015 A. A. Michelson Award, the 2006 ACM SIGCOMM Test of Time Award, the CDAC-ACCS Foundation Award 2009, the IISc Distinguished Alumnus Award 2014, the WiMAX Forum Individual Contribution Award 2008, and ranks among the Most Cited Authors in Computer Science.