applied sciences

MDPI

Review

How to Isolate Non-Public Networks in B5G: A Review

Qian Sun [1,2], Ning Hui [1,3], Yiqing Zhou [1,2,3,*], Lin Tian [1,2], Jie Zeng [4] and Xiaohu Ge [5]

[1] Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China
[2] Beijing Key Laboratory of Mobile Computing and Pervasive Device, Beijing 100190, China
[3] University of Chinese Academy of Sciences, Beijing 100049, China
[4] School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing 100081, China
[5] School of Electronic Information and Communications, Huazhong University of Science and Technology, Wuhan 430074, China
* Correspondence: zhouyiqing@ict.ac.cn

Featured Application: B5G non-public networks will serve various vertical industries, which are developing rapidly in the era of the Internet of Things. It is forecasted that eight key industries will unlock $1.4 tn in 2030. Since it has been proposed for non-public networks (NPNs) to share the B5G system in part or totally, isolation technologies must be applied to establish customized NPNs without mutual influences between them.

Abstract: Non-public networks (NPNs) have drawn much attention due to their flexibility and efficiency with B5G. According to the requirements of various application scenarios, NPNs can be tailored to a number of deployments, sharing the B5G system totally or in part. The isolation of NPNs is a critical issue. This paper provides a survey of isolation schemes for B5G NPNs. First, we present an overview of various deployments and the corresponding isolation demands for B5G NPNs. To meet these isolation demands, three kinds of NPN isolation—i.e., spectrum isolation, RAN isolation and CN isolation—are discussed. Then, the corresponding isolation technologies are introduced and analyzed. Finally, open research challenges, such as wireless throughput capacity with spectrum isolation, operation with isolation requirements and data isolation of software-defined CN for B5G NPNs, are discussed.

Keywords: NPN; isolation; B5G

check for updates

Citation: Sun, Q.; Hui, N.; Zhou, Y.; Tian, L.; Zeng, J.; Ge, X. How to Isolate Non-Public Networks in B5G: A Review. *Appl. Sci.* **2022**, *12*, 9771. https://doi.org/10.3390/app12199771

Academic Editor: Amalia Miliou

Received: 15 July 2022
Accepted: 15 September 2022
Published: 28 September 2022

1. Introduction

With the development of wireless communication technologies [1–5], one main target of Beyond 5G (B5G) is to serve various vertical industries, which are developing rapidly in the era of the Internet of Things [6]. With the capacities of the network-as-a-service, multiple logical networks will be able to be deployed with the same resources and infrastructures in the B5G era [7]. Thus, it has been proposed for non-public networks (NPNs) to share the B5G system in part or totally to provide customized communication services. Although NPNs are flexible and efficient, there are two problems. The first is how to configure the network parameters to achieve customized service, and the other is that the dynamic factors of one NPN may deteriorate the performance metrics of other NPNs due to the sharing of resources and infrastructures [8]. Therefore, isolation among NPNs has become a big challenge for the establishment of customized NPNs without mutual influence among them. To achieve this, isolation needs to guarantee that each NPN can be configured with its own attributes and stable performance, where "stable performance" means that any change in the network state of one NPN does not violate the qualities of service (QoS) of other NPNs [8]. Since the QoS performance metrics are mainly determined by the resources one NPN can use, isolation of the computing resources and of the spectrum are significant. The own attributes can then be configured with parameters and schemes. Related research on isolation mainly focuses on computing resources isolation, spectrum isolation and customized configuration of protocol parameters, as shown in Figure 1.

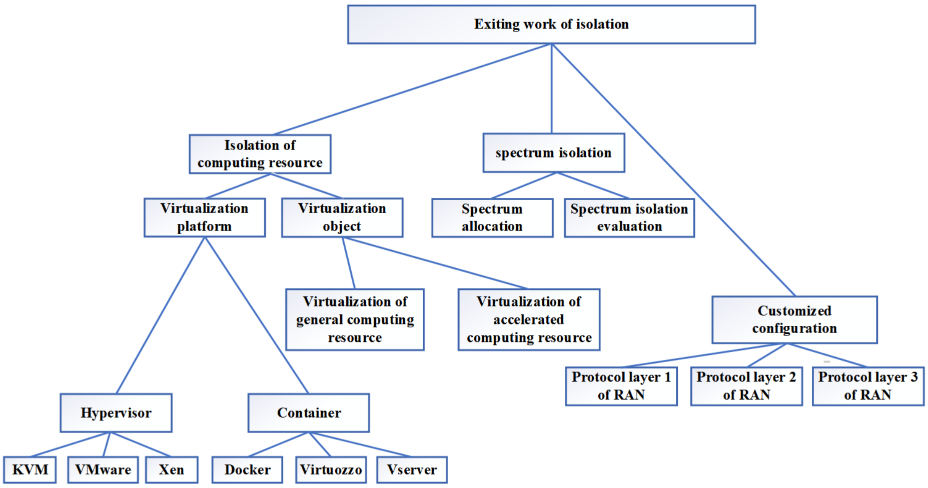

Figure 1. Existing work of NPN isolation.

For computing resources isolation, virtualization technology has been designed, which divides and maps physical resources into logical resources to realize resources isolation [9–11]. This virtualization technology can be summarized with two concepts: the platform of virtualization and the object of virtualization. There are two main types of platforms of virtualization in the computer field, which are hypervisors and containers. The main difference between them is the level of abstraction in terms of virtualization and isolation. A hypervisor, called a virtual machine monitor (VMM), provides the abstraction of physical hardware, while a container implements isolation of processes at the operating system (OS) level [12–14]. The container enables applications to run on the same OS kernel so that the guest OS is not required. Therefore, the container acts as a lightweight alternative to the hypervisor by excluding the execution of the guest OS, hardware virtualization, etc. However, the hypervisor has better performances in isolation, security and supporting different guest OSs because each virtual machine is standalone and independent of the host kernel. Common hypervisors include VMware's ESX, Microsoft's Hyper-V, the open source Xen, KVM, etc. Representatives of containers are Docker and LXC. With regard to the objects of virtualization technology, these include general computing resources, such as CPU, and accelerated computing resources, such as FPGA and DSP. The virtualization of general computing resources is undertaken by the hypervisor and container platforms, while the virtualization of accelerated computing resources is usually undertaken at the task level. Differently from hypervisors and containers, accelerated computing resources can be scheduled directly without the interruption of operating systems in task-level virtualization [15]; thus, the processing delay brought by virtualization is minimized to guarantee real-time performance metrics [12], but the scheduling scheme has to be designed case by case. For NPNs, the proposed virtualization technologies can be used to achieve computing resources isolation. However, more aspects of the spectrum and the protocol configuration still need to be considered to achieve isolation among NPNs.

Previous work on slicing technology has discussed spectrum isolation and protocol configuration [16]. Virtual networks are formed in 5G systems by network slicing, and spectrum isolation refers to virtual networks sharing wireless spectrum resources without deteriorating others' QoS performance metrics. Customized configuration means that virtual networks can be configured with differentiated parameters for network functions [17]. With regard to spectrum isolation, the performance is represented by the satisfaction of QoS performance metrics (such as resource utilization, the throughput, the mean bit rate, etc.) and focuses on the optimization of these performance metrics. For example, improving the QoS performance metrics [16], maximizing the throughputs [18], trading off the terminal throughputs and the signal-to-noise ratio of the slices [19], as well as minimizing the latency [20], are treated as the requirements of slice isolation [21]. Then, to meet the requirements, methods such as game theory and convex optimization, as well as some other methods, are used to allocate wireless resources among the slices. However, there is no quantitative requirement for or index of isolation. Thus, it is hard to judge whether the isolation requirements have been achieved or not. To evaluate the isolation performance, an isolation index, representing the isolation performance of the spectrum, can be defined and calculated with the QoS performance metrics or the spectrum resource assignment parameters [22]. QoS requirements are treated with or mapped onto the isolation requirement. By comparing the isolation index and the isolation requirement, whether the spectrum isolation of one virtual network has been achieved or not can be evaluated. The system tries its best to fulfill the isolation requirements when assigning spectrum resources among virtual networks, and the main ideas that these methods use to achieve spectrum isolation are given in Section 3.

For the differentiated configuration, various control parameters are configured in protocol layers 3 and 2 of the radio access network (RAN) to achieve customized scheduling and access control functions of QoS guaranteed and non-guaranteed services [23]. Furthermore, various ratios of uplink and downlink subframes in protocol layer 1 can be configured to obtain different wireless throughputs for the virtual networks. More descriptions of the customized configuration are given in Section 4. Using slicing technology, researchers have attempted to achieve network isolation at full steam [24]. However, NPNs require guaranteed isolation rather than isolation as best as the system can achieve. One NPN can be deployed by the resource and the infrastructures, which are partly occupied by the NPN and partly by the others sharing the system. However, there has been no analysis or summary of the isolation required by various deployments and isolation technologies to achieve guaranteed isolation. This is important for the application of NPNs.

Therefore, this paper provides a review of isolation aspects for B5G NPNs, and the contributions are as follows. Firstly, we present an overview of NPNs' deployments and compare the performance metrics of the deployments. We conclude that sharing parts of resources and infrastructures is a promising way to establish NPNs, but it will bring great challenges in form of three kinds of isolation. Subsequently, for the three kinds of isolation—i.e., spectrum isolation, radio access network isolation and core network isolation—the main idea necessary to achieve the guaranteed isolation is described using the present isolation technologies, and the advantages, disadvantages and limitations are summarized. Finally, the open research challenges of B5G NPN isolation are discussed.

The isolation technologies for NPNs in the B5G era are discussed in this article. To achieve this, the article is organized as follows. In the following section, deployments of NPNs are described and the isolation demands are analyzed. Then, the technologies to achieve isolation of the spectrum, isolation of the RAN and isolation of the CN for NPNs are summarized in the following three sections. Thus, the decisions about whether the spectrum, the RAN and the CN should be shared or not when deploying NPNs can be made according to the performance metrics of the isolation technologies. The following section describes open issues. Finally, conclusions are drawn.

2. Deployments of NPNs

A B5G NPN provides refined differentiation of communication services to meet the multifarious demands of vertical industries, and this can be established with resources and infrastructures owned by the NPN itself and by the public system. The resources and infrastructures occupied by a particular NPN are called private parts and the others shared among multiple NPNs are called shared parts.

The B5G system employs a modularized architecture, which can meet the various QoS requirements of applications flexibly [25]. With this architecture, the B5G system is composed of a radio access network (RAN) and core network (CN), and the CN mainly consists of the user plane function (UPF) and the control plane (CP). As shown in Figure 2, two kinds of B5G NPNs can be formed with seven deployments. One kind of NPN is the standalone NPN (S-NPN), where none of the B5G system, or only the spectrum, is shared. The two deployments are the isolated S-NPN and the shared spectrum-only S-NPN (see Figure 2a,b), and they are suitable for the application scenarios involving dependent networks with requirements for high isolation, data privacy and low latency, such as the control information transmission of a high-speed train.

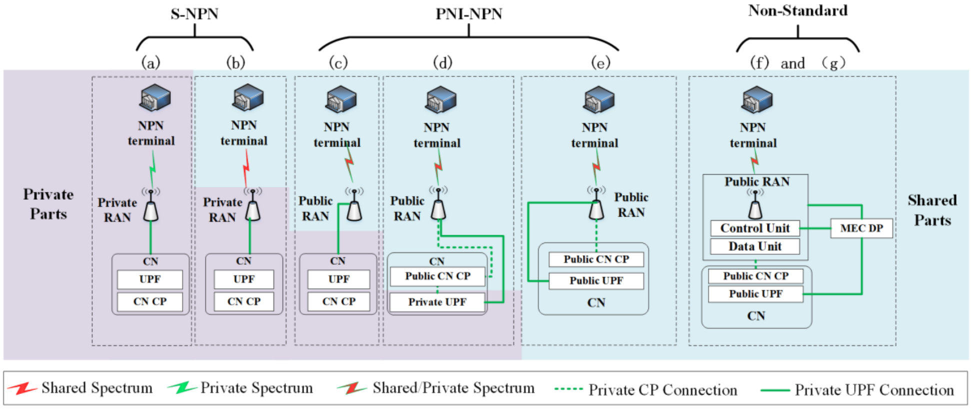

Figure 2. Deployments of NPNs. (**a**) Isolated NPN (**b**) Shared spectrum-only NPN (**c**) Shared RAN NPN (**d**) Shared RAN and CP NPN (**e**) Shared RAN and CN NPN (**f**) N3 LBO NPN (**g**) F1 LBO NPN.

The other kind of NPN is the public network integrated NPN (PNI-NPN). As shown in Figure 2c–e, with different deployments, more and more parts of a B5G NPN can be shared among different NPNs. For the shared RAN PNI-NPN in Figure 2c, the RAN has been shared. Based on this, the CP of the CN is also used in common in the shared RAN and CP PNI-NPN in Figure 2d. These two deployments of the PNI-NPN can meet the requirements for medium isolation, data privacy and latency since the data plane of the CN is dedicated and can be used for application scenarios focusing on data security, such as remote telemedicine, in which the private data of patients is transmitted. Lastly, for the shared RAN and CN PNI-NPN in Figure 2e, the RAN and the CN are both shared, and this deployment can be used in applicable scenarios with non-sensitive isolation and latency, such as an automation warehousing communication network. Furthermore, there are two local breakout (LBO) NPNs that utilize mobile edge computing data plane (MEC DP) equipment to offload the traffic of the NPN locally, with the MEC DP parsing the data stream from the N3 interface or from the F1 interface; these are called the N3 LBO NPN and the F1 LBO NPN, as shown in Figure 2f,g [26]. The two LBO PNI-NPN deployments have already been used in virtual/augmented reality (AR/VR), for which the cost and the transmission delay can be reduced. In spite of this, the interfaces of the MEC DP are non-standard, which results in a negative impact on security and compatibility. The performance metrics and the application scenarios of the seven NPN deployments are summarized in Table 1.

Due to the high cost and scarce spectrum of the S-NPN, the PNI-NPN is well-recognized as the dominant B5G NPN [27]. Taking the city of Rittal in Germany as an example, the cost of an NPN equals EUR 1000 + 5 Bt(6a1 + a2), where B MHz is the allocated frequency bandwidth, 1000 is the number of years the NPN is allowed to use the spectrum and a1 and a2 km^2 are a coverage area with a high density of the population and other areas, respectively. However, the spectrum is always scarce. Although some countries have begun to allocate the spectrum to important industrial users [28], it is impossible for all industrial users to have their own spectrum. Therefore, the PNI-NPN is a promising way to solve the above two problems. By sharing the spectrum, RAN and CN among different NPNs, the transmission capacity of one NPN can be made flexible, and the utilization of resources is improved. However, a serious challenge emerges, which is isolating the different NPNs to achieve customized configuration and stable performance [8]. Therefore, it is important to study isolation technologies to achieve the three kinds of NPN isolation; i.e., spectrum isolation, RAN isolation and CN isolation.

Table 1. Performance metrics and application scenarios of the seven NPN deployments.

Deployment Option	**Performance Metrics**					**Application Scenarios**
	Isolation	**Data Privacy**	**Latency**	**Cost**	**Standardized or not**	
Isolated S-NPN	High	High	Low	High	Yes	High-speed train
Shared spectrum-only S-NPN	High	High	Low	Medium high	Yes	Smart power grid
Shared RAN PNI-NPN	Medium	Medium	Low	Medium	Yes	Remote telemedicine
Shared RAN and CP PNI-NPN	Medium low	Medium low	Medium	Medium	Yes	Internet of Vehicles
Shared RAN and CN PNI-NPN	Low	Low	High	Low	Yes	Automation warehousing
N3 LBO NPN	Low	Low	Medium	Low	No	AR/VR
F1 LBO NPN	Low	Low	Medium	Low	No	AR/VR

3. Spectrum Isolation

Spectrum isolation means that different NPNs share the spectrum in an orthogonal way, and the wireless performance of one NPN does not deteriorate when the dynamic factors of other NPNs, such as wireless traffic and channel conditions, exist. Using spectrum isolation, spectrum resources can be shared among NPNs flexibly; thus, the efficiency of the spectrum resources can be improved greatly. In spite of this, there is a serious challenge, which is that the spectrum isolation performance of NPNs must be expressed quantitatively and meet the requirements. To achieve this, there are two key aspects. One is how to calculate the performance and requirements of spectrum isolation for one NPN quantitatively. The other is assigning spectrum resources among NPNs to meet isolation requirements.

For the first aspect, spectrum isolation can be represented by the QoS parameters of one NPN, which is called spectrum isolation based on QoS parameters. Thus, the QoS requirements can be used as the isolation requirements directly or they can be further mapped onto one isolation requirement, which needs to represent all the QoS requirements or the comprehensive requirement of all the QoS requirements. Then, the isolation indicators of one NPN are defined in accordance with the isolation requirements to represent the corresponding isolation performances [17]. For instance, there is one NPN g with one QoS requirement, q_g. Thus, the isolation requirement denoted by z_g equals q_g. Then, the index of the isolation performance denoted by s_g is defined to reflect whether z_g is met or not. Thus, if z_g is met, s_g equals 1; otherwise, s_g is smaller than 1. s_g can be calculated by $\mathrm{E}\left(\min\left(p_g(t), z_g\right)/z_g\right)$ if NPN g requires its performance to be no smaller than z_g. Otherwise, s_g can be calculated by $\mathrm{E}\left(z_g/\max\left(p_g(t), z_g\right)\right)$, if NPN g requires its performance to be no larger than z_g, where $\mathrm{E}(x)$ means to calculate the expectation of x [17]. $p_g(t)$ is the instantaneous performance corresponding to q_g.

Besides the QoS parameters, spectrum isolation can also be expressed by the degree of sharing of the spectrum resource among NPNs, which is called spectrum isolation based on resource sharing. This means that each NPN is assigned a part of the spectrum resource, and one NPN can use other NPNs' spectrum resources temporarily [22]. Thus, the isolation requirement and indicator of one NPN can be the amount of time that the NPN uses the wireless resources of other NPNs. For example, there is one NPN g that has already obtained r_g bits of the spectrum resource. At the same time, in time window i, NPN g shares its spectrum resource with other NPNs, denoted by $\alpha_{g,i}$, and it obtains spectrum resources from other NPNs, denoted by $\beta_{g,i}$, temporarily. $d_{g,i}$ is the data that needs to be transmitted in time window i. Then, the requirement for spectrum isolation is denoted by z_g. It is calculated by dividing the amount of time during which the QoS requirement is met t_g by the total observation time T_g; i.e., $z_g = t_g/T_g$. Then, the index of spectrum isolation performance for NPN g denoted by $s_{g,i}$ is defined to represent the dependence on the resources provided by other NPNs. Thus, s_g can be calculated by dividing the amount of resources it owns and uses by the amount of resources it uses; i.e., $(r_g - \alpha_{g,i})/(r_g - \alpha_{g,I} + \beta_{g,i})$.

Spectrum assignment among NPNs is designed to meet quantized isolation requirements. For spectrum isolation based on QoS parameters, the isolation indicators can be used to decide whether to reallocate spectrum among NPNs or not, since isolation indicators can reflect whether QoS requirements are met or missed intuitively. The spectrum assignment of NPNs can converge gradually to the minimum amount of resources when the isolation requirements are met [17]. For spectrum isolation based on resource sharing, the isolation indicators can be used to guide the sharing of the spectrum among NPNs, since they reveal the impact of resource sharing on QoS performance metrics. According to the guidance, more or less spectrum will be shared among NPNs, aiming to meet their QoS requirements as best as possible [22]. However, the spectrum shared among NPNs should fulfill the spectrum isolation requirements. After adjusting the spectrum allocation, if the QoS requirements or the isolation requirements are still not fulfilled, the QoS requirements and/or the number of NPNs served by the system should be reduced. The advantages, challenges and solutions for spectrum isolation are summarized in Table 2.

Table 2. Advantages, challenges and solutions for spectrum isolation, RAN isolation and CN isolation.

Items	Advantages	Challenges	Solutions
Spectrum isolation	High-efficiency and flexibility for the spectrum resources	Expressing isolation performance of NPNs quantitatively Meeting the corresponding isolation requirements	Formulating the performance and requirements for spectrum isolation quantitatively Introducing quantitative spectrum isolation when assigning spectrum resources among NPNs to meet the isolation requirements
RAN isolation	Customized performance metrics for air interface in one economical way	Mapping the customized performance metrics of the air interface to the parameters of the RAN Sharing computing resources with latency requirements	Configuring the RAN protocol diversely Adopting task-level virtualization and designing a RAN task scheduling scheme
CN isolation	Multiple logical standalone links for CNs in one economical way	Distinguishing data from different NPNS and their terminals Assigning the minimum computing resources to meet the QoS requirements of CNs	Identifying the NPN and its subscribers Calculating the minimum resource demand of one CN, considering the coupled QoS requirements jointly, then assigning the minimum computing resources using virtualization technologies, such as KVM, VMware and Docker

4. RAN Isolation

RAN isolation means that different NPNs sharing the infrastructures have customized access schemes and run the software of their RANs with logical-isolation computing resources. With RAN isolation, customized performance metrics for an air interface can be provided economically. In spite of this, there are two big challenges: mapping the customized performance metrics of the air interface to the parameters of the RAN and sharing computing resources with latency requirements. To achieve this, when deploying one NPN, the RAN protocol is first configured diversely, and then the RAN software where the computing resource needs to be virtualized at the task level is set up and run.

For customized configuration of the RAN protocol, network slicing is an important technology used to set the parameters of RAN slices flexibly [24]. For the radio resource control (RRC) protocol of radio protocol layer 3, attention must be paid to the usage of the resource assigned to guaranteed QoS services (GSs). For a particular NPN, part of these resources need to be reserved for the GSs being served by the NPN. Thus, various resource reservation ratios [19] can be set for the NPNs. In two NPNs with the same assigned and occupied GSs resources, one new GS can be forbidden in one NPN and can be allowed in the other NPN, since the reservation ratios of the GSs in the two NPNs are different. The medium access control (MAC) sub-layer of radio protocol layer 2 focuses on the amounts of resources assigned to GSs and non-guaranteed QoS services (non-GSs), which can be set in the admission control methods according to the resource demand of the NPNs [23]. For radio protocol layer 1, the parameters in the NPNs can also be configured differentially; for example, the uplink and the downlink subframe ratios can be configured based on the corresponding data rate requirements of NPNs. With these methods, a customized configuration for the RAN protocol can be achieved, as shown in Figure 3.

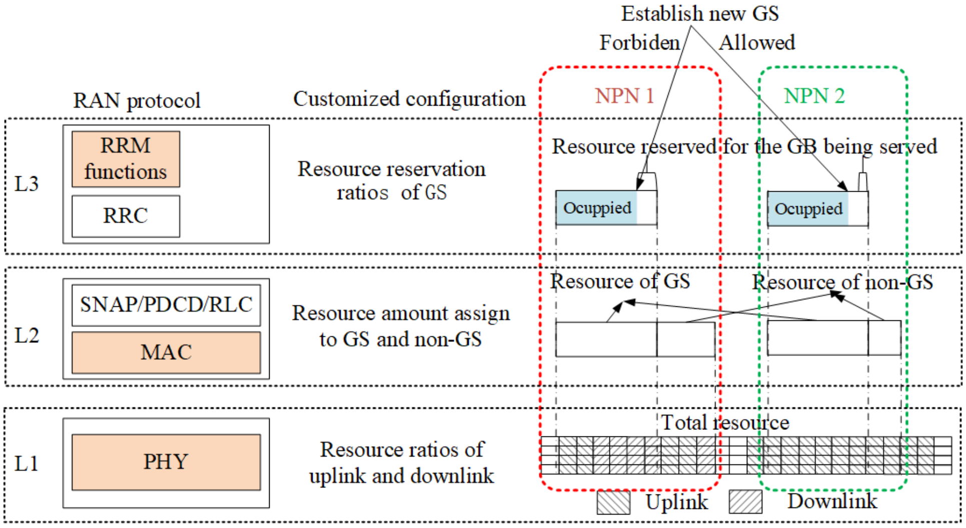

Figure 3. Protocol isolation for RAN.

The computing resources shared among the RAN software need to be virtualized with the aim that the computing tasks of the NPNs' RANs can proceed within their lifetimes. Accelerated computing resources are focused on since most computing tasks for RAN are delay-sensitive. Although general computing resources are also used to process the delay-insensitive tasks of a RAN, its isolation will be considered in Section 5 on CN isolation, which is also applicable to RANs. Generally speaking, accelerated computing resources can be a digital signal processor (DSP) or a field programmable gate array (FPGA). The virtualization of a DSP or FPGA is usually realized by a scheduling scheme designed according to the computing tasks' execution time and lifetimes. To achieve this, the scheduling scheme can be modeled as a directed acyclic graph (DAG), where the computing tasks of RANs can be modeled as the nodes of the DAG, called task nodes, as shown in Figure 4. For the task nodes, lifetimes can be obtained according to the scheduling periods of the wireless subframe, and execution time can be estimated using their software algorithms [15]. Then, the task nodes of the same RAN need to be connected in order since they are usually serial tasks. In accordance with the DAGs, a scheduling list can be obtained to try to calculate the tasks within their lifetimes. To this end, the system will decide whether the accelerated computing resources of the RAN are shared with other NPNs' RANs or not, in accordance with the scheduling list. If the time-sensitive tasks can be processed within their lifetimes, the accelerated computing resource can be shared with the RANs of other NPNs; otherwise, the sharing will be forbidden. Then, more private or sharing infrastructures need to be deployed and turned on to serve the NPNs' RANs. If there are no more infrastructures, the system needs to reject the request to serve some of the NPNs until all the tasks of the RANs can be processed within their lifetime. The advantages, challenges and solutions for RAN isolation are summarized in Table 2.

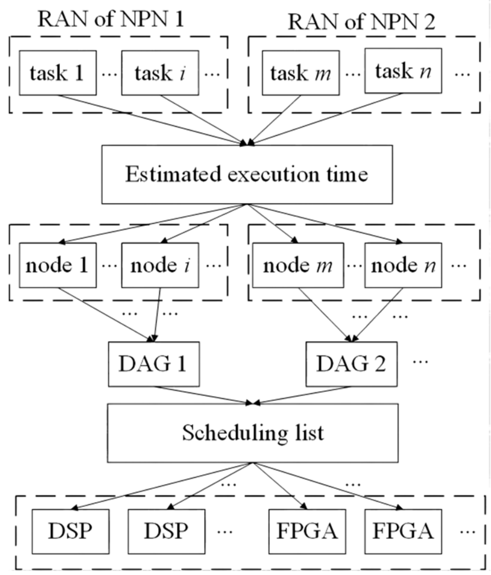

Figure 4. Virtualization of RAN based on DAG model.

5. CN Isolation

CN isolation means that an NPN should not set up signal and data sessions for the subscribers of other NPNs, and it runs the software of its CN with logical-isolated computing resources, where the infrastructures are shared among multiple NPNs. With CN isolation, multiple logical standalone links between the CNs can be established and operated economically. In spite of this, there are two serious challenges: distinguishing data from different NPNs and their terminals and assigning the minimum computing resources to meet the QoS requirements of the CNs. To achieve this, there are two key aspects. One is to identify the NPN and its subscribers. The other is calculating the minimum resource demand of one CN, then assigning the minimum computing resources using virtualization technologies, such as KVM, VMware and Docker.

For the first aspect, 3GPP defines a new identifier for each S-NPN, which can be a combination of a public land mobile network identity (PLMN ID) and a network identifier (NID). Then, the identifications of subscribers and S-NPNs are configured and stored in both the terminal and the CN sides. Thus, an S-NPN can recognize the subscribers and vice versa. Furthermore, a cell access group (CAG) can also be designed for PNI-NPNs, where the CAG represents a group of subscribers that can access one or more CAG cells, and the CAG cell is one kind of cell that only its subscribers can access. Then, one CAG can be identified by the combination of the PLMN ID and CAG ID, and the CAG information is stored at the CN side to recognize the subscribers of each PNI-NPN. At the same time, each terminal also stores one list of CAG cells it can access. Thus, one PNI-NPN can recognize its subscribers and vice versa. Using the identifier of the S-NPN and the CAG of the PNI-NPN, the terminals will only be served by the subscribed NPNs.

Then, virtualization of general computing resources, such as the CPU, is undertaken to run the tasks of CNs, which are usually time-insensitive. Virtualization technologies, such as KVM, VMware and Docker, can be used to map physical resources into logical resources [9]. Then, the CNs of different NPNs can own dedicated virtualized computing resources, which are assigned according to the resource demands and the virtualization overheads [9]. Thus, the resource demand of one CN needs to be calculated, and this equals the sum of the resources needed by all the function modules of this CN. To calculate the minimal resource demand of one function modularly, the QoS requirements should be considered jointly since they are independent [29]. We can use the calculation of a

UPF's resource demand as an example, where two QoS requirements—i.e., forwarding throughput and delay—are considered. Since higher forwarding throughput is helpful to decrease delay, part of the resource demanded by a UPF to meet the forwarding throughput requirement can be used to fulfill the delay requirement, which is called redundant resource, as shown in Figure 5. To remove the redundancy, two weights for the resource demands corresponding to the two QoS requirements are derived using the method of the Person correlation coefficient [30], and these are smaller than one. Then, the resource demand of the UPF can calculated as the weighted sum of the two resource demands. Thus, the resource demand of an NPN's CN can be obtained. Then, the system decides whether the CN resources for one NPN should be shared with others according to the available resources after virtualization. If there are enough resources to meet the resource demands of the multiple CNs of the NPNs, the resource will be shared among the CNs; otherwise, more private or sharing infrastructures need to be deployed and turned on to serve the NPNs' CNs. If there is no more infrastructure, the system needs to deny requests to serve some of the NPNs until the available resources are enough for all the CNs. In addition, isolation of the computing resources for CNs can also be applicable for general computing resources running time-insensitive tasks in RANs. The advantages, challenges and solutions for CN isolation are summarized in Table 2.

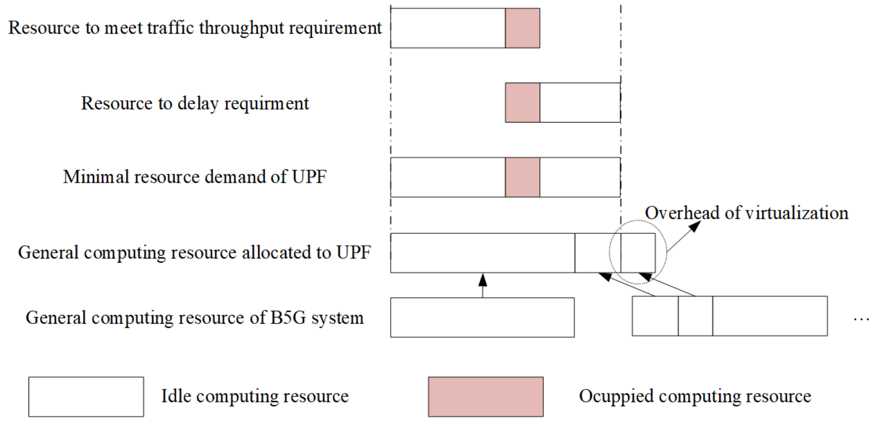
Resource to meet traffic throughput requirement
Resource to delay requirment
Minimal resource demand of UPF
Overhead of virtualization
General computing resource allocated to UPF
General computing resource of B5G system
...
Idle computing resource
Ocuppied computing resource

Figure 5. Virtualization of CN using the UPF as an example.

6. Open Research Challenges

6.1. Wireless Throughput Capacity with Spectrum Isolation

Spectrum isolation should be achieved in the B5G system with NPNs. At present, there is no theory to reveal how spectrum isolation for NPNs affects the wireless throughput capacity in the B5G system. Since the capacity boundary is unknown, the B5G system has to reserve enough spectrum resources to guarantee that the isolation performance can meet the requirements, which leads to wasting valuable spectrum [19,31]. Therefore, it is important to study the wireless capacity of the B5G system with spectrum isolation for NPNs. To achieve this, it may be necessary to define the key parameters determining the performance of the wireless capacity and spectrum isolation [23,32]. Then, the relationships between/among the parameters should be derived, as these can reveal the quantitative decreases in wireless capacity with the corresponding spectrum isolation requirements. Finally, spectrum assignment among NPNs should be undertaken based on the theory of wireless throughput capacity with spectrum isolation [17,33]. The former potential research line would bring great benefits by maximizing the capacity of the B5G system and sharing spectrum among NPNs efficiently.

6.2. Operation of NPNs with Isolation Requirements

Operation becomes an important issue after deploying B5G NPNs to provide communication services to vertical industries, as who operates what part of the B5G NPNs needs to be specified. It should be clarified which entities are responsible for running the network on a day-to-day basis and for managing the resources and services of the B5G NPNs [24,34]. The entities could include enterprises using the NPNs and mobile network operators (MNOs) operating the B5G system. If the enterprise operates its NPN, management is undertaken independently from any other networks and called isolated operation. If the MNO operates a NPN, the management is part of the overall network operations and called a unified operation. For isolated operations, it is easy to configure and reconfigure an NPN according to dynamic states, such as traffic. However, continuous service is difficult when one terminal is out of its NPN's coverage, and the costs are relatively high [34]. For unified operations, continuous service can be provided at a low cost. However, reconfiguring the NPN is complex, and requests must be sent by the enterprise to the MNO based on the dynamic states, which need to be responded to and carried out by the MNO. Due to this, unified operations result in poor network flexibility and low data security [34].

To address these issues, a joint operation between the enterprises and the MNOs is a better method that can ensure flexible and continuous services at a relatively low cost [34]. To achieve this, the demands and results of the operations need to be exchanged between the enterprises and the MNOs, for which data security and privacy are a serious challenge [35]. To solve this problem, federated learning, which contains a local model and a joint model, is a promising technology. Each enterprise or MNO can train its local model with the local data, and the results after training can be exchanged among enterprises and MNOs without sharing the private data [36]. The joint model can act as a global coordinator that is trained to obtain the global optimal management strategies with the received results of local models. With this potential research line, NPNs can be managed efficiently and securely through a joint operation based on federated learning.

6.3. Data Isolation of Software-Defined CNs

The CN of an NPN is software-defined and runs, in general, on a hardware platform, which is the trend in the B5G era. As a result, the physical boundaries among NPNs' CNs are broken, which introduces a great risk for data security [37]. This means that data theft and tampering among the CNs will be possible as there are no physical boundaries. Therefore, data isolation is needed to prevent the data of each CN from being accessed across the CNs. To achieve data isolation, hardware and software security can be improved through research on cloud platforms. Furthermore, protocol security still needs to be further studied [38,39]. Protocols with endogenous security capabilities are a hot topic in the context of sixth-generation mobile communication networks, for which zero trust architecture [40,41], heterogeneous redundancy construction [42] and blockchain are potential technologies [43].

7. Conclusions

In this article, isolation schemes for spectrum isolation, RAN isolation and CN isolation were discussed for seven deployments of B5G NPNs. For spectrum isolation, the indices of isolation performance and requirements were defined and calculated for NPNs quantitatively. Based on the indices, spectrum resources can be assigned among NPNs to meet isolation requirements. For RAN isolation, the customized configuration of the RAN can be achieved by setting the parameters of the RAN protocol properly. Then, RAN software can be run on the accelerated computing resource, which is virtualized using the scheduling scheme of the computing tasks. For CN isolation, with a newly defined identifier and CAG, an NPN can recognize its subscribers, and the subscribers can also recognize their NPN. CN software runs on general computing resources, which can be virtualized with virtualization technologies, such as KVM. When deploying NPNs, the spectrum and computing resources can be shared among the NPNs if the QoS and the isolation requirements of all NPNs can be met. Otherwise, more resources should be added or else the system will only be able to serve fewer NPNs.

Author Contributions: Conceptualization, Q.S. and Y.Z.; methodology, Q.S., N.H. and L.T.; formal analysis, Q.S. and Y.Z.; investigation, Q.S. and N.H.; resources, L.T.; writing—original draft preparation, Q.S. and N.H.; writing—review and editing, Q.S., Y.Z., J.Z. and X.G.; visualization, Q.S. and N.H.; supervision, Q.S.; project administration, Q.S.; funding acquisition, L.T. All authors have read and agreed to the published version of the manuscript.

Funding: This paper was funded by national key research and development program grant number 2021YFB2900504.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ge, X.; Yang, B.; Ye, J.; Mao, G.; Wang, C.-X.; Han, T. Spatial Spectrum and Energy Efficiency of Random Cellular Networks. *IEEE Trans. Commun.* **2015**, *63*, 1019–1030. [CrossRef]
2. Xiang, L.; Ge, X.; Wang, C.-X.; Li, F.Y.; Reichert, F. Energy Efficiency Evaluation of Cellular Networks Based on Spatial Distributions of Traffic Load and Power Consumption. *IEEE Trans. Wirel. Commun.* **2013**, *12*, 961–973. [CrossRef]
3. Ge, X.; Ye, J.; Yang, Y.; Li, Q. User Mobility Evaluation for 5G Small Cell Networks Based on Individual Mobility Model. *IEEE J. Sel. Areas Commun.* **2016**, *34*, 528–541. [CrossRef]
4. Zhong, Y.; Quek, T.; Ge, X. Heterogeneous Cellular Networks with Spatio-Temporal Traffic: Delay Analysis and Scheduling. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 1373–1386. [CrossRef]
5. Ge, X.; Huang, K.; Wang, C.-X.; Hong, X.; Yang, X. Capacity Analysis of a Multi-cell Multi-antenna Cooperative Cellular Network with Co-channel Interference. *IEEE Trans. Wirel. Commun.* **2011**, *10*, 3298–3309. [CrossRef]
6. Sun, Q.; Tian, L.; Zhou, Y.; Shi, J.; Wang, Y.; Zhang, Z. A Two-Layered Incentive Scheme for Cooperation in Sliced 5G D2D Networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 13289–13304. [CrossRef]
7. Tilly Gilbert. $1.4TN of Benefits in 2030: 5G's Impact on Industry Verticals [R/OL]. (2019-10). February 2021. Available online: https://carrier.huawei.com/~{}/media/CNBGV2/download/program/Industries-5G/5G-Impact-on-Industry-Verticals.pdf (accessed on 14 July 2022).
8. 5G Non-Public Networks for Industrial Scenarios. 5G-ACIA Whitepaper. March 2019. Available online: https://www.5Gacia.org/index.php?id=6958 (accessed on 14 July 2022).
9. Cao, J.; Ma, M.; Li, H.; Ma, R.; Sun, Y.; Yu, P.; Xiong, L. A Survey on Security Aspects for 3GPP 5G Networks. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 170–195. [CrossRef]
10. Sollfrank, M.; Loch, F.; Denteneer, S.; Vogel-Heuser, B. Evaluating Docker for Lightweight Virtualization of Distributed and Time-Sensitive Applications in Industrial Automation. *IEEE Trans. Ind. Inform.* **2021**, *17*, 3566–3576. [CrossRef]
11. Raveendran, N.; Song, L.; Jiang, C.; Gu, Y.; Han, Z.; Pan, M.; Tran, N.H. Cyclic Three-Sided Matching Game Inspired Wireless Network Virtualization. *IEEE Trans. Mob. Comput.* **2021**, *20*, 416–428. [CrossRef]
12. Xiong, K.; Adolphe, S.S.R.; Boateng, G.O.; Liu, G.; Sun, G. Dynamic Resource Provisioning and Resource Customization for Mixed Traffics in Virtualized Radio Access Network. *IEEE Access* **2019**, *7*, 115440–115453. [CrossRef]
13. Tian, L.; Zhou, Y.; Wang, Y.; Yang, J.; Sun, Q.; Yuan, J.; Yang, B. Evaluation Methodology for Virtual Base Station Platforms in Radio Access Networks. *IEEE Access* **2018**, *6*, 49366–49374. [CrossRef]
14. Choudhury, S.; Maheshwari, S.; Seskar, I.; Raychaudhuri, D. ShareOn: Shared Resource Dynamic Container Migration Framework for Real-Time Support in Mobile Edge Clouds. *IEEE Access* **2022**, *10*, 66045–66060. [CrossRef]
15. Bhaumik, S.; Bansal, R.; Karmakar, R.; Mopur, S.K.; Mukherjee, S.; Chitale, M.J.; Chakraborty, S. NetStor: Network and Storage Traffic Management for Ensuring Application QoS in a Hyperconverged Data-Center. *IEEE Trans. Cloud Comput.* **2022**, *10*, 1287–1300. [CrossRef]
16. Zeng, S.; Dai, G.; Sun, H.; Zhong, K.; Ge, G.; Guo, K.; Wang, Y.; Yang, H. Enabling Efficient and Flexible FPGA Virtualization for Deep Learning in the Cloud. In Proceedings of the IEEE Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM), Fayetteville, AR, USA, 3–6 May 2020; pp. 102–110.
17. Zhang, S.; Luo, H.; Li, J.; Shi, W.; Shen, X. Hierarchical Soft Slicing to Meet Multi-Dimensional QoS Demand in Cache-Enabled Vehicular Networks. *IEEE Trans. Wirel. Commun.* **2020**, *19*, 2150–2162. [CrossRef]
18. Dai, L.; Tian, L.; Sun, Q.; Zhou, Y.; Wang, Y.; Feng, C. Wireless Resource Management in Sliced Networks Based on Isolation Indexes. In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), Nanjing, China, 29 March–1 April 2021; pp. 1–6.
19. Hossain, A.; Ansari, N. 5G Multi-Band Numerology-Based TDD RAN Slicing for Throughput and Latency Sensitive Services. *IEEE Trans. Mob. Comput.* **2020**, 1–12. [CrossRef]
20. D'Oro, S.; Bonati, L.; Restuccia, F.; Melodia, T. Coordinated 5G Network Slicing: How Constructive Interference Can Boost Network Throughput. *IEEE/ACM Trans. Netw.* **2021**, *29*, 1881–1894. [CrossRef]
21. Reyhanian, N.; Maham, B. Statistical Slice Selection in Multi-Tenant Networks with Maximum Isolation of Reserved Resources. In Proceedings of the Asilomar Conference on Signals, Systems, and Computers (ACSSC), Pacific Grove, CA, USA, 1–4 November 2020; pp. 1002–1006.

22. Su, R.; Zhang, D.; Venkatesan, R.; Gong, Z.; Li, C.; Ding, F.; Jiang, F.; Zhu, Z. Resource Allocation for Network Slicing in 5G Telecommunication Networks: A Survey of Principles and Models. *IEEE Netw.* **2019**, *33*, 172–179. [CrossRef]
23. Hui, N.; Sun, Q.; Wang, Y.; Zhang, Z.; Tian, L.; Feng, C.; Guan, Z. Wireless Resource Allocation based on Multiplexing and Isolation in Sliced 5G Networks. In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), Austin, TX, USA, 10–13 April 2022; pp. 1–6.
24. Yang, X.; Liu, Y.; Wong, I.C.; Wang, Y.; Cuthbert, L. Effective Isolation in Dynamic Network Slicing. In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 15–18 April 2019; pp. 1–6.
25. Poe, W.Y.; Ordonez-Lucena, J.; Mahmood, K. Provisioning Private 5G Networks by Means of Network Slicing: Architectures and Challenges. In Proceedings of the IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–6.
26. 3GPP TS 23.501. System Architecture for the 5G System (5GS); Stage 2 (Release 16). August 2020. Available online: https://www.3gpp.org/ftp/Specs/archive/23_series/23.501/23501-h60.zip (accessed on 14 July 2022).
27. Kao, L.; Liao, W. 5G Intelligent A+: A Pioneer Multi-Access Edge Computing Solution for 5G Private Networks. *IEEE Commun. Stand. Mag.* **2021**, *5*, 78–84. [CrossRef]
28. Tehrani, R.H.; Vahid, S.; Triantafyllopoulou, D.; Lee, H.; Moessner, K. Licensed Spectrum Sharing Schemes for Mobile Operators: A Survey and Outlook. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2591–2623. [CrossRef]
29. Ojanen, P.; Yrjölä, S.; Matinmikko-Blue, M. Assessing the Feasibility of the Spectrum Sharing Concepts for Private Industrial Networks Operating above 5 GHz. In Proceedings of the European Conference on Antennas and Propagation (EuCAP), Copenhagen, Denmark, 15–20 March 2020; pp. 1–5.
30. Sun, Q.; Feng, C.; Hui, N.; Tian, L.; Wang, Y. Computing and Storage Resources Allocation of UPF for private 5G networks based on isolation. In Proceedings of the IEEE Vehicular Technology Conference (VTC2022), Helsinki, Finland, 19–22 June 2022; pp. 1–6.
31. Cao, Z.; Zhang, Y.; Guan, J.; Zhou, S.; Chen, G. Link Weight Prediction Using Weight Perturbation and Latent Factor. *IEEE Trans. Cybern.* **2022**, *52*, 1785–1797. [CrossRef]
32. Jenco, J.; Latif, O.A.; Kwasinski, A.; Amer, M. Network Slicing for Wireless Networks Operating in a Shared Spectrum Environment. In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), Austin, TX, USA, 10–13 April 2022; pp. 2435–2440.
33. Korrai, P.; Lagunas, E.; Sharma, S.K.; Chatzinotas, S.; Bandi, A.; Ottersten, B. A RAN Resource Slicing Mechanism for Multiplexing of eMBB and URLLC Services in OFDMA Based 5G Wireless Networks. *IEEE Access* **2020**, *8*, 45674–45688. [CrossRef]
34. Guan, W.; Zhang, H.; Leung, V.C.M. Customized Slicing for 6G: Enforcing Artificial Intelligence on Resource Management. *IEEE Netw.* **2021**, *35*, 264–271. [CrossRef]
35. Rostami, A. Private 5G Networks for Vertical Industries: Deployment and Operation Models. In Proceedings of the IEEE 5G World Forum (5GWF), Dresden, Germany, 30 September–2 October 2019; pp. 433–439.
36. Guo, W.; Xu, J.; Pei, Y.; Yin, L.; Jiang, C.; Ge, N. A Distributed Collaborative Entrance Defense Framework Against DDoS Attacks on Satellite Internet. *IEEE Internet Things J.* **2022**, *9*, 15497–15510. [CrossRef]
37. Ghimire, B.; Rawat, D.B. Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things. *IEEE Internet Things J.* **2022**, *9*, 8229–8249. [CrossRef]
38. Rawat, D.B.; Doku, R.; Garuba, M. Cybersecurity in Big Data Era: From Securing Big Data to Data-Driven Security. *IEEE Trans. Serv. Comput.* **2021**, *14*, 2055–2072. [CrossRef]
39. Gündoğan, C.; Amsüss, C.; Schmidt, T.C.; Wählisch, M. Content Object Security in the Internet of Things: Challenges, Prospects, and Emerging Solutions. *IEEE Trans. Netw. Serv. Manag.* **2022**, *19*, 538–553. [CrossRef]
40. Colombo, P.; Ferrari, E.; Tümer, E.D. Access Control Enforcement in IoT: State of the art and open challenges in the Zero Trust era. In Proceedings of the IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), Atlanta, GA, USA, 13–15 December 2021; pp. 159–166.
41. Syed, N.F.; Shah, S.W.; Shaghaghi, A.; Anwar, A.; Baig, Z.; Doss, R. Zero Trust Architecture (ZTA): A Comprehensive Survey. *IEEE Access* **2022**, *10*, 57143–57179. [CrossRef]
42. Wu, J. Development paradigms of cyberspace endogenous safety and security. *Sci. China-Inf. Sci.* **2022**, *65*, 1–3. [CrossRef]
43. Hu, S.; Liang, Y.C.; Xiong, Z.; Niyato, D. Blockchain and Artificial Intelligence for Dynamic Resource Sharing in 6G and beyond. *IEEE Wirel. Commun.* **2021**, *28*, 145–151. [CrossRef]