network

MDPI

Article

5G Network Slice Isolation

Stan Wong [1,*], Bin Han [2] and Hans D. Schotten [2,3]

[1] Hong Kong Telecommunication Limited, Hong Kong SAR 999077, China
[2] Division of Wireless Communications and Radio Positioning, University of Kaiserslautern, 67663 Kaiserslautern, Germany; bin.han@eit.uni-kl.de (B.H.); schotten@uni-kl.de or hans_dieter.schotten@dfki.de (H.D.S.)
[3] German Research Center of Artificial Intelligence (DFKI GmbH), 67663 Kaiserslautern, Germany
* Correspondence: jedistan@gmail.com

Abstract: This article reveals an adequate comprehension of basic defense, security challenges, and attack vectors in deploying multi-network slicing. Network slicing is a revolutionary concept of providing mobile network on-demand and expanding mobile networking business and services to a new era. The new business paradigm and service opportunities are encouraging vertical industries to join and develop their own mobile network capabilities for enhanced performances that are coherent with their applications. However, a number of security concerns are also raised in this new era. In this article, we focus on the deployment of multi-network slicing with multi-tenancy. We identify the security concerns and discuss the defense approaches such as network slice isolation and insulation in a multi-layer network slicing security model. Furthermore, we identify the importance to appropriately select the network slice isolation points and propose a generic framework to optimize the isolation policy regarding the implementation cost while guaranteeing the security and performance requirements.

Keywords: 5G; network slicing; security; isolation; insulation

check for updates

Citation: Wong, S.; Han, B.; Schotten, H.D. 5G Network Slice Isolation. *Network* **2022**, *2*, 153–167. https://doi.org/10.3390/network2010011

Academic Editor: Youn-Hee Han

Received: 28 January 2022
Accepted: 3 March 2022
Published: 8 March 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Network slicing [1] is a revolutionary concept of enabling mobile networks on-demand. It extends the business model of the mobile networking from the traditional tariff subscription to the new cloud computing paradigm: network slice as a service (NSaaS). The basic principle of network security, such as authentication, authorization, confidentiality, integrity and availability, can be found in [2]. The new business model and service opportunities are motivating vertical industries to join and develop their own mobile networks and specify the network infrastructure capabilities and performance to align with their business and application characteristics. To achieve this aim, it requires adequately defining the defense mechanisms that protect all deployed network slices of various types with different network performance and security requirements [3]. In particular, these defending mechanisms have to be considered not only for the traditional physical network infrastructures but also in a nested virtualized network environment.

Formerly, the traditional network infrastructure had been considered as a secure environment because it was operated under a single administrative domain and fully maintained by an operator. However, this has been changed in NSaaS, where the mobile network operator (MNO) or network slicing service provider offers network slices of various types for leashes, which coexist over a shared physical infrastructure [4]. José María Jorquera Valero et al. [5] pointed out that multi-tenancy requires a multi-domain security and risk management embedded into the design. Furthermore, the current trust models and existing defense methodologies might not be appropriate to the operation of NSaaS. Those network slices may have different levels of security demands and various specifications of tailored network protection measures. In such an emerging network

environment, the defending and attacking surfaces become much wider than those in legacy systems, and the security problem becomes more complex than the mobile industry had anticipated. Therefore, it calls for an effective isolation mechanism and policy approaches that can protect the network from attacks and infections over these new wide surfaces. For example, Tomasz Wichary et al. [6] discussed security control and policies to protect those network perimeters, and Chun-I Fan et al. [7] developed a scheme for cross-network slice authentication to protect against attackers who aim to impersonate users, network operators or network slices by providing a secure session key exchange.

For developing security solutions to protect the complex network environment when deploying NSaaS, it is seriously important to identify the possible attacking vectors, the adequate defending mechanisms and the appropriate security technologies. This identification process also helps us gain practical security knowledge and increase the security awareness.

Basically, NSaaS shall provide various levels of isolation, e.g., application segmentation isolation, virtual machine isolation, network segmentation isolation and resource isolation, to secure the infrastructure of the mobile network operator (MNO) and to protect the tenant's privacy as well as their services. On the other hand, a typical network slice tenant generally expects its network slice to run as a standalone and fully independent mobile network. Neither a network slice nor the data of its tenant shall be accessed by other unauthorized tenants. Unfortunately, a network slice is based on virtualization, containerization and software-defined network technologies; therefore, faults and mistakes can be propagated to other network slices via the virtualized environment, and attackers may cross network slices to misuse the networks for their desired purposes. This is the main reason resolving network slice isolation has become the primary goal of the mobile industry in order to deploy a secure NSaaS.In their survey in 2018 [8], Luis Suárez et al. have identified network slice isolation as the core concept that impacts the network slice security. Since the traditional approaches, such as traffic isolation, encryption and firewalls, are not providing sufficiently satisfactory performance in countering the related cyber threats, they have envisioned some possible artificial intelligence mechanisms to enhance the network slice security. Unfortunately, little progress has been reported in the suggested approaches. One of the main reasons for this lack of achievement can be the absence of a deep and thorough understanding of the security model in slice isolation.

The goal of this article is to demystify the appropriate defense mechanisms and provide an adequate isolation approach in different points of a network slice. The isolation point must be selected based on the characteristics of the network slice and the MNO's network infrastructure strategy. The main novel contributions of our work are: (1) identified security challenges in deploying NSaaS, (2) proposed a multi-layer model to decompose the network slicing security complexity, (3) analyzed the impact of network slice isolation point selection and (4) proposed a framework to optimize the selection of network slice isolation points.

This article is organized as follows: Section 2 provides the principles of network slicing and network slice types of characteristics. Section 3 discusses the challenges of network slicing security when deploying an NSaaS platform. We use a multi-layer approach to explain the complexity layer-by-layer, then identify that the precision of the network slice isolation would affect the defense and performance of the network slice. Subsequently, we develop a mathematical model of network slice isolation relating to the level of control that the MNO and tenant would apply to the cost of deployment network slice relationships in Section 4. Finally, we conclude the paper in Section 5.

2. The Principles of Network Slicing and Network Slice Types

Network slicing is a logical network representation, composed with a specific mobile network infrastructure configuration, which consists of various levels and types of isolation in a physical infrastructure. It is basically enabled by virtualization, containerization, software-defined network (SDN), virtual network function (VNF) service chain, network function virtualization (NFV) [9] and flexible transport network technologies. The MNO

is expected to utilize those technologies to provide a secure network environment across the radio access network, transport network and core network. This secure network environment shall be fully optimized with the coexistence of multiple network slices and their different service characteristics and requirements. On the other hand, the tenant expects their network slices' structure to be a standalone and fully independent mobile network. Moreover, other tenants shall not have unauthorized access to their network slices nor unauthorized interception with the other tenants' data.

Network slicing dynamically gives an MNO flexibility in organizing, coordinating and orchestrating any available resources in the wireless and wired network environment. Those resources can be differentiated into a specific service in a particular location. For example, a manufacturer customer would like to have a network slice with a particular location within a few cell sites only. A utility company would like to have a smart grip network slice in some remote sites. Another case would be a hospital authority customer that would like to have a network slice within a hospital area. Those three typical cases illustrate network slice services that can be dynamically deployed and provisioned in a unique geolocation. Furthermore, these individual network slices can port to other network slice service providers or MNO network slice platforms. The GSM Association (GSMA) has provided an introduction of network slice [10] and has proposed the Network Slice Generic Template to formulate a menu for selecting the network slice's perimeters. This GST model can be converted into a network provisioning data model for deploying the network slice [11].

3. Network Slice Isolation As a Security Measure

NSaaS is set to deliver an on-demand mobile network. It encourages the vertical industry to design and develop their mobile network infrastructures and mobile network services. These mobile network infrastructures and services utilize virtualization, containerization and SDN technologies to increase the flexibility of network provision, deployment and operational models and the business transformation and service agility across multiple mobile networks. In particular, these mobile network infrastructures or services provide network independence and network seclusion, which has been demonstrated with multiple points-of-presence slice segment stitching to construct a network slice and also various resources being flexibly manipulated for a network slice [12]. Traditionally, the MNO only has a single administrative domain (AD) to manage, a network element and subscriber to protect, an impersonation of a subscriber to prevent, static attack vectors to identify, etc. However, when the NSaaS is deployed, the network flexibility and service agility will lead to a number of new security challenges. In this paper, we provide a comprehensive study of security challenges in four aspects, from identifying the protection assets, preventing attacks and human errors and identifying the right selection of isolation points and different assets required to manage, for ensuring the understanding of NSaaS' new security challenges and applying the right NSaaS operation protection measures without affecting the network slice service performance requirements that are vitally important in a multi-network slicing environment. It is also critical that the NSaaS security perimeters are adequately defined throughout the entire NSaaS security chain and in the operational level from the radio access network to the transport network and from the transport network to the core network.

3.1. Challenges in Network Slicing Security

In this subsection, the key network slice security challenges are defined in four aspects, which are protection, prevention, identification and management, as summarized in Table 1.

The protection challenges are raised by concerns about the network infrastructure to support NSaaS, where it shall begin to consider the protection of network infrastructure from static-resource to dynamic-resource network environments. Typically, static resources can be referred to as hardware assets, and dynamic resources can be considered software assets. Furthermore, these software assets can be created at runtime when the network

elasticity is triggered by traffic and network services on-demand. Since these runtime software assets can be network slices, virtual network functions and SDN properties that may overload the network and affect the network services availability, we have to protect the network availability, service reliability and company liabilities at all times. In particular, other network services might have a functional error or be compromised, which can possibly affect any other network services' availability. All these protections shall be considered from the network resilience to the risk assessment of network services.

Table 1. Identified challenges in network slicing security.

Aspect	Subject	Objective
Protection	network infrastructure	network resilience and service availability
Prevention	unauthorized access and inappropriate use	cross-AD resource isolation and robustness to insider threat
Identification	security threats	establishing appropriate security control policies
Management	ADs, virtual environment visibility, subscribers of tenants	increased virtual environment visibility and reduced network risk

The prevention challenges are the unauthorized access and inappropriate use of network infrastructure resources, which can be considered the access or usage from the same AD or from other ADs. Traditionally, the MNO only manages a single AD and never has experience managing and authorizing third parties that access various levels of resources based on the service's level agreement with the tenant. Therefore, preventing cross-ADs resource access is another challenge the MNO is required to manage. In particular, under the virtualized network environment, co-resident attacks may trigger unauthorized access to another virtual machine co-existing under the same bare-metal. Furthermore, the MNO also requires preventing another serious issue in all kinds of systems within the infrastructure, including insider threats. In order to prevent insider threats under such fast evolving and changing network environments, a proper management process and control process has to be applied on top of traditional approaches. For example, ISO/IEC 27001 has a series of control processes to ensure the information security management in securing the system. We often face an unknown threat when network automation is applied to a virtualized network infrastructure environment because there is a possibility that an attacker may be inappropriately manipulating network resources via auto-optimization and auto-reconfiguration. Therefore, we shall apply zero trust to prevent auto-manipulation of network resources.

The identification of security threat challenges is typically an essential task for the MNO before network deployment. Usually, the MNO will establish security control policies appropriately, which is not just based on the local regulations' requirements and international benchmark approaches [13] but also the demand for adapting the best practice from the industry. Therefore, identifying the security control policies for deploying NSaaS requires considering the security policies under the flexible network and dynamic network runtime environments. It cannot simply apply black-box approaches that will eventually expose various unidentified attack vectors and vulnerable loopholes since the common practice of identifying the attack vectors or conducting the risk assessments requires an existing network environment. In particular, attack vectors will not be straightforward without an existing network infrastructure and services environment. Even though the flexible network infrastructure is unpredictable for managing the resources, we shall clearly state the security policies when applying network elasticity. Furthermore, we also have to identify the adequate physical and logical isolation points for each of the network slices to protect the service's availability, set the security perimeters and provide appropriate security measures in the future.

In terms of the network management challenges, we have a number of items that must be seriously considered. The MNO shall provide policies to manage the unknown ADs and the virtual environment visibility. In particular, the virtual environment visibility can be managed by different technological techniques, e.g., microsegmentation, hypervisor firewall, etc. These techniques can increase the visibility but also require a substantial amount of knowledge to manage them. On the other hand, under NSaaS, we have many tenants that need to be managed. For example, a tenant's identity, access and privacy need to be properly managed. Furthermore, the MNO shall provide a privacy scheme or guideline for tenants to manage their subscribers in order to reduce the risk of the network.

The above four aspects can assist the MNO in securely operating the NSaaS. Therefore, we propose to plan and provide a precise policy of control to fulfill these aspects as the basic requirements.

3.2. Decomposition of Network Slicing Security Complexity

In this subsection, we present a multi-level model of the network slicing security decomposition. Basically, this model also represents a network construction sequence that starts from deciding the type of devices available in the supply chain. Once installed in the network, those devices become physical resources that formulate the infrastructure. In order to be fully utilized, they can be transferred into virtual resources by applying virtualization and containerization technologies. Consequently, those formulated virtual resources should be managed by an information management platform, e.g., NFV. After the physical and virtual infrastructures are fully established, we start to consider the protocol and service chain's protection methodologies and the appropriate isolation points in the network slice. Finally, from the MNO's point of view, it is essential to consider a network slice platform to manage the network slice tenants by means of tenant identities, access rights, services, etc. Note that the above description is simplified regarding the deployment consideration and sequence of architectural design decisions. Furthermore, between every two layers, there is a tight relationship and logical link in the deployment of a network slice. Furthermore, each of the layers and elements has a specific protection method, which we are going to discuss in this subsection.

As illustrated in Figure 1, the lowest three levels in our model are inherited from the traditional network security model, which concerns the fundamental telecommunication equipment supply chain security, physical resource security and physical infrastructure, respectively. The fourth layer to the top layer are the logical and information security concerns, which are considered to deal with a wider attack surface every layer. Furthermore, the complexity of defense in each layer will also increase layer-by-layer from the bottom to the top layer. We further describe each of the layer's characteristics in the following.

Layer I Supply Chain—Usually, it is a first line of defense and is considered a physical active electronic component and passive electronic component. Software components or entities shall be included within the supply chain. Those components' software is often employed with malicious code. Therefore, we have to have certain level of control over the supply chain when deploying NSaaS. ISO 28000 specification has a well-established supply chain security management control framework that can be applied. NIST has also suggested supply chains' life-cycle management [14]. Furthermore, supply chain security management is not just to deliver control and assurance to the overall system, it also requires defining the level of control processes, certifications of the product within the best practice in the current time and the trustworthiness of the protocol applied to test the products. GSMA provides a supply chain toolbox to give a guideline of this first line of defense [15], and NSCS also provides 12 principles to ensure the first line of defense under control within the appropriate stage of the overall supply chain [16].

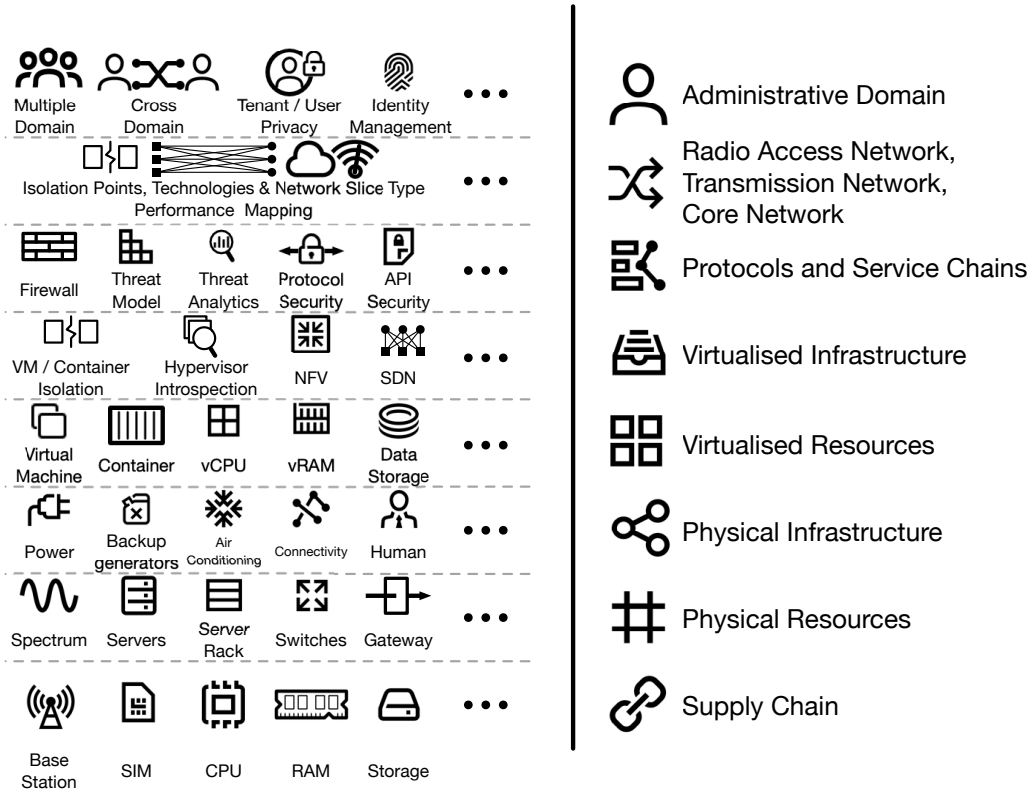


Figure 1. Network slice basic elements.

Layer II Physical Resources—Often, the MNO unifies the physical network elements and license's components as physical resources that will increase the flexibility of the overall mobile network infrastructure and refine the productivity by applying different service management methodologies. Furthermore, the MNO also constantly searches various methods and techniques to fully utilize all available resources in their network infrastructure. Furthermore, by deploying a network slice, the second line of defense is to manage different types of physical resources that apply to a particular network slice. For example, a critical infrastructure network slice can only be deployed in a few specific locations with selected spectrum threats, and the local breakout may also require being deployed with an air-gap isolated server rack, switch and the internet gateway.

Layer III Physical Infrastructure—Facility infrastructure resiliency gives service reliability to the MNO's mobile network infrastructure. There are a number of international data center control frameworks [17] to protect this third line of the network slice's defense service's availability and reliability. For example, a utility smart grid network slice may request a wide area deployment and require a certain level of service availability and reliability. Hence, the MNO may need to pick the right level of the data center for such network slice deployment. Often, the mobile network infrastructure is constructed by different data centers, which different data center management teams and companies are often employed to manage. In maintaining the data center service reliability and ensuring the different levels of data center security, data center security is not only facility security but also includes identity and access management, etc.

Layer IV Virtual Resources—Generally, network slicing is based on virtualization and containerization technologies as its foundation. Network slices can be constructed under virtual machines, containers or a combination of virtual machines and containers, and each network slice can be specifically restricted on the number of vCPU or vRAM and the type of storage. The MNO requires managing its virtual resources so that it does not exceed the maximum level of physical resource limitation and cause service interruptions.

Layer V Virtual Infrastructure—The level of complexity in this layer has been significantly increased. We have to consider the implementation virtual machine and container

isolation techniques to avoid co-residency attack. The typical technique that would be applied is the hypervisor introspections or serverless container isolation technique at the kernel level. The virtualized infrastructure can have an access control list for a particular application to secure the entire network segment using microsegmentation, which automatically applies network segregation. Therefore, the virtualization and containerization network security would be the main consideration in this layer since this layer's defense is across different areas of technology implementation, from application to virtual network segmentation and from infrastructure access control to the CPU firmware trust model. All these techniques are trying to keep network slices isolated from each other.

Layer VI Protocol and Service Chain—In this layer, a formulated network slice shall have a specific service to deliver. Usually, the MNO formulates those services that may use a service chain approach. Service chains are often in a sequential manner of network functions that can also split into multi-locations, and the traffic will propagate from one network location to another in a specific sequence. Due to the network service chain's sequential structure, we can collect network intelligence data that can be used to increase the virtual network infrastructure visibility and threat intelligence protection on different levels of the network slice's defense. However, we have to avoid the inappropriate virtual resource manipulations; therefore, we can use the appropriate security protocol and API security to prevent malicious manipulations.

Layer VII Radio Access Network, Transmission Network and Core Network—When deploying a network slice, we need to identify various isolation points as network defense perimeters, where different isolation techniques can be applied. Those isolation points must be carefully selected; otherwise, the service performance can be easily affected. Therefore, mapping the isolation points with adequate technology under different network slice types is an important process in deploying network slices.

Layer VIII Administrative Domain—Consequently, there is a possibility that the tenant may have purchased multiple network slices across different MNOs, and the tenant may share all resources across multiple network slices. Therefore, the MNO or network slice service provider requires protecting each AD's user and tenant privacy and must manage users' and tenants' identities who accesses the appropriate AD.

The above multi-layer approach can assist the network slice's service provider or MNO to distinguish and differentiate the level of managing the NSaaS platform and to protect the overall MNO network service availability. After resolving the network slice complexity in layers, we shall focus on the practical deployment of NSaaS, which focuses on the defense of three domains in the data center: radio access network, transport network and core network.

3.3. Precision of Network Slice Isolation Point

Identifying an adequate network slice isolation point and applying the right network slice isolation mechanism and policy at those isolation points are the main challenges in deploying multi-network slicing to a mobile operator network. Network slices are designed to support the co-existence of multiple tenants on an MNO physical network with independent, isolated and fully secured network services. Furthermore, one tenant would not know another tenants' existence in the network. A similar strategy has been proposed on the Internet to isolate services or applications using a service-oriented architecture [18]. However, it might need abnormal detection to protect the behavior of the network slice from faults, e.g., an inappropriate selection of isolation points. In the case of such faults, the anomaly detection algorithm can also be invoked to obtain the score of isolation points behavior [19], which may be further exploited by machine learning techniques to isolate the faults [20] and to model the slice behavioral patterns under a particular setup of isolation points.

GSMA has defined eight types of network slice use cases, and each of the network slice types could have different network configurations, network performance requirements, traffic criteria and security control, etc. All these characteristics would ultimately lead

to delivering the service experience to the subscriber and fulfilling the network slice's Service Level Agreement (SLA) securely [21]. In particular, multi-network slice deployment involves different network technologies, resource migration and resource optimization at the runtime. Either an inappropriate selection of the isolation points or wrongly applying an isolation mechanism and policy in each of the isolation points can cause network performance degradation or service delivery interruption after resource optimization and migration. Therefore, we shall identify each of the possible isolation points and adequate security mechanisms and policies applied to those isolation points. By appropriately specifying these features, it helps not only by securing the network slice but also by enhancing the network performance without affecting the subscriber's experience or violating the SLA.

Figures 2–5 provide illustrations of some phenomena when deploying a network slice. Figure 2 is divided into three parts: on the right and left sides, two options are illustrated where the tenant requests for a network slice with the most tenant control and minimal influence from the MNO (left) or balanced control shared between the tenant and the MNO (right), respectively. In the earlier case, the MNO only provides physical resources (e.g., spectrum etc.); in the latter case, several layers of the protocol stack and some specific network functions are defined and controlled by the MNO. In the middle, Figure 2 shows how the level of isolation matters to the cost of deployment when considering network slice isolation. In particular, Figure 2 indicates the minimal and maximal cost of isolation that would start on a positive manner due to the physical resources (e.g., spectrum etc.) that belong to the MNO. The graph also indicates the characteristics of the isolation relationship in between the level of control a tenant can gain when deciding to purchase a network slice. Furthermore, the graph indicates that is not directly proportional to each other due to the vast number of isolation techniques that can be applied to deliver similar protection. Figure 3 provides an overview of controlling a network slice by the tenant. When the tenant has minimal control of a network slice, which implies the tenant fully relies on the MNO to manage the network slice, and the MNO has less responsibility to apply isolation in order to protect the network slice. On the other hand, when the tenant has maximal control of the network slice, the MNO is responsible for applying isolation to the network slice for protecting the other tenant's privacy. Figure 4 reflects the control of the MNO, which is correlated to Figure 3. Furthermore, Figure 4 indicates when the MNO has absolute control of the network slice, which is a monolithic network. There would be no NSaaS existing in the network. The network relies on the fourth-generation telecommunications system.Finally, Figure 5 shows the exclusive relationship between the MNO control and tenant control on any certain network slice. It shall be noted that Figures 2–5 show no quantitative results but only qualitative relations among the level of isolation, slicing cost and control levels, which can be straightforwardly derived from the control-sharing mechanism and the cost budget of network slice isolation.

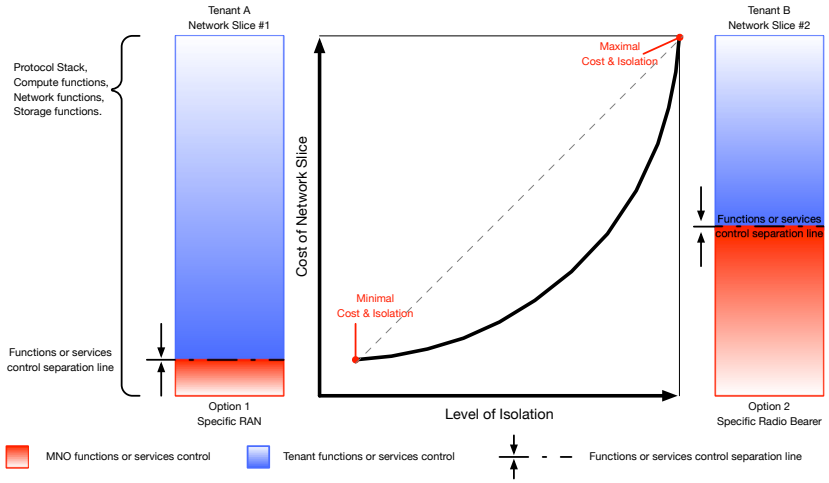


Figure 2. The network slice's cost rises with the isolation level due to the additional implementation of tenant-dedicated functions and service control.

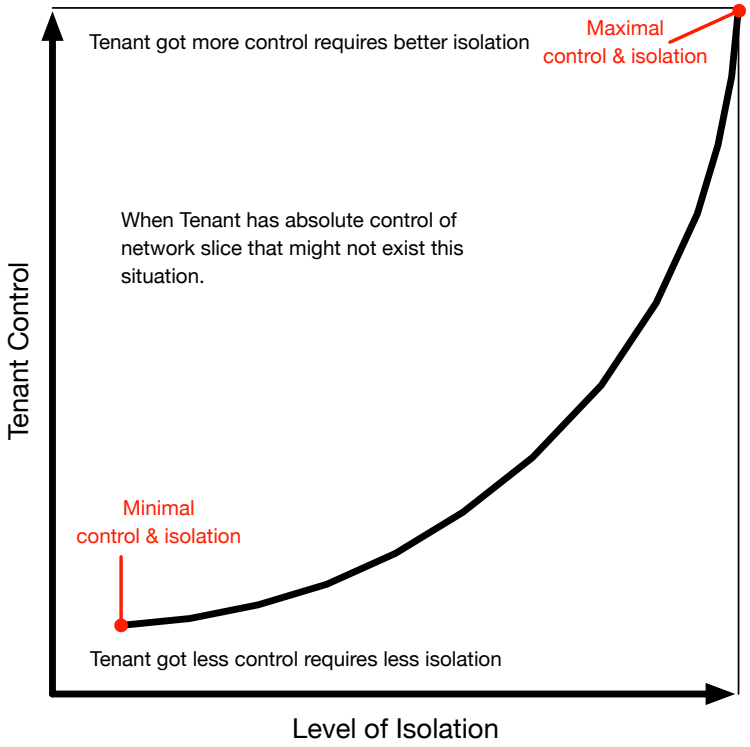


Figure 3. The tenant obtains more control of its slice with a higher isolation level since more shared functions are replaced by dedicated ones.

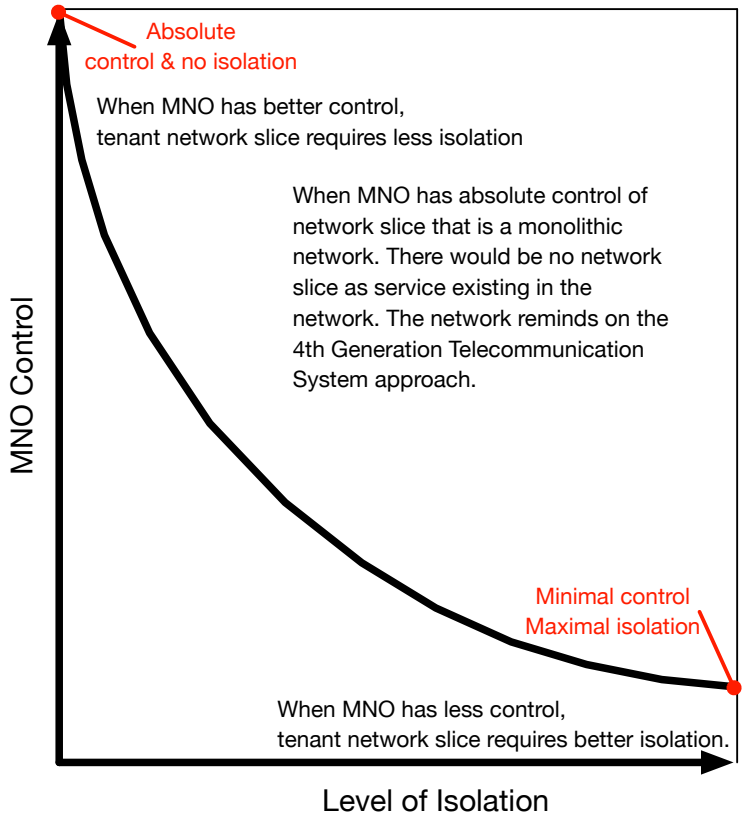


Figure 4. The MNO retains less control on a leased slice with a higher isolation level since more shared functions are replaced by dedicated ones.

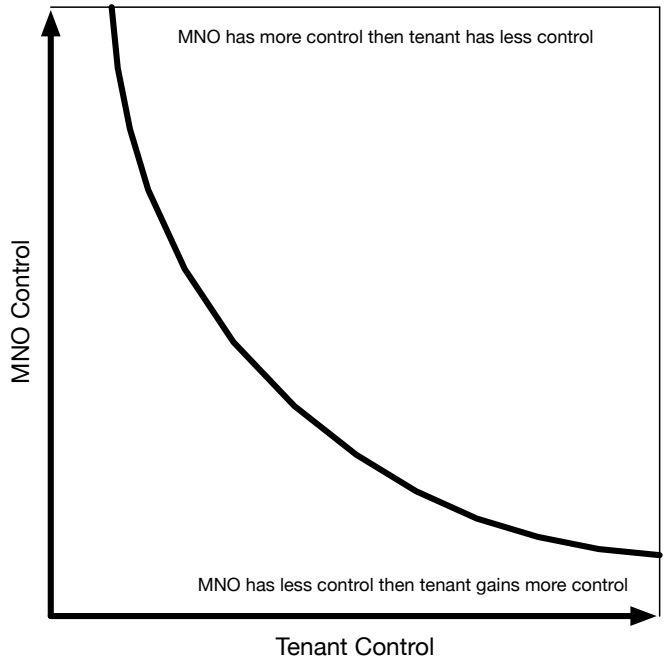


Figure 5. The controls of MNO and tenant are exclusive to each other.

4. Model of Network Slice Isolation

In this section, we develop a mathematical model to help MNO identify the cost of deploying the right network slice isolation points. We use the 3GPP protocol stack [22,23] as a network slice logical deployment representation. We begin with the case where the isolation points can be independently selected for every individual slice. Ideally, those isolation points would not have any impact on the performance nor implementation cost of other slices. Therefore, we define a mathematical model to provide a rational representation. We start with the following notations:

We consider the set of all N slices $\mathcal{N} = \{1, 2, 3, \dots, N\}$, where every slice needs to implement a full stack $\mathcal{P} = \{1, 2, 3, \dots, P\}$ of protocol layers. Every individual slice $n \in \mathcal{N}$ can independently and flexibly choose the method to implement each protocol layer, either in a physical way or in a virtual way. This can be formulated with a binary indicator for every pair of network slice n and protocol layer p:

$$v_{n,p} = \begin{cases} 1 & n \text{ virtualizes } p \\ 0 & \text{otherwise} \end{cases}, \quad \forall n \in \mathcal{N}, p \in \mathcal{P}. \tag{1}$$

For each protocol layer p of a specific network slice n, call its isolation level $i_{n,p}$, the tenant control level $t_{n,p}$ can be selected from a finite discrete set $\mathcal{T}_{n,p} \subseteq \mathcal{T}$, where $\min(\mathcal{T}_{n,p}) = 0$ and $\max(\mathcal{T}_{n,p}) = t_{n,p}^{\max} \in (0, 1)$. We also define the MNO control level $m_{n,p} = 1 - t_{n,p}$, the operations cost $c_{n,p}^{\text{op}}$ and the infrastructural cost

$$c_{n,p}^{\text{ifr}} = c_{n,p}^{\text{P}} v_{n,p} + c_{n,p}^{\text{V}} (1 - v_{n,p}), \tag{2}$$

where $c_{n,p}^{\text{P}}$ and $c_{n,p}^{\text{V}}$ are the cost to implement p for n physically and virtually, respectively. Their values in practical systems are determined by the specific hardware and software used by the MNO. Generally, given an arbitrary fixed $i_{n,p}$,

$$c_{n,p}^{\text{P}} > c_{n,p}^{\text{V}}, \quad \forall (n, p) \in \mathcal{N} \times \mathcal{P}. \tag{3}$$

The total isolation cost of slice n is, therefore,

$$c_n = \sum_{p \in \mathcal{P}} \left(c_{n,p}^{\text{ifr}} + c_{n,p}^{\text{op}} \right). \tag{4}$$

For every slice n, we define the quality of service q_n and the security level s_n. We aim at minimizing the isolation cost:

$$\begin{aligned}
\underset{\mathbf{I},\mathbf{T},\mathbf{V}}{\text{minimize}} \quad & \sum_{n \in \mathcal{N}} c_n && \text{(5a)}\\
\text{subject to} \quad & t_{n,p} + m_{n,p} = 1, \forall (n,p) \in \mathcal{N} \times \mathcal{P}, && \text{(5b)}\\
& p_n \geq p_n^{\min}, \forall n \in \mathcal{N}, && \text{(5c)}\\
& s_n \geq s_n^{\min}, \forall n \in \mathcal{N}, && \text{(5d)}
\end{aligned}$$

where $\mathbf{I} = [i_{1,1}, i_{1,2} \ldots, i_{1,P}, i_{2,1}, i_{2,2} \ldots, i_{2,P} \ldots i_{N,P}]$ is the vector of isolation point selection, $\mathbf{T} = [t_{1,1}, t_{1,2} \ldots, t_{1,P}, t_{2,1}, t_{2,2} \ldots, t_{2,P} \ldots t_{N,P}]$ the vector of control level specification and $\mathbf{V} = [v_{1,1}, v_{1,2} \ldots, v_{1,P}, v_{2,1}, v_{2,2} \ldots, v_{2,P} \ldots v_{N,P}]$ the vector of virtualization selection. Here, Equation (5b) implies that the control over each protocol layer p of a leased network slice n is shared between the tenant and the MNO, and their controls are mutually exclusive to each other, which we have illustrated in Figure 5.

Note that $i_1 > i_2$, $m_1 > m_2$, $t_1 > t_2$, and for all (n, p), we have:

$$t_{n,p}^{\max}|_{i_{n,p}=i_1} > t_{n,p}^{\max}|_{i_{n,p}=i_2} \tag{6}$$

$$c_{n,p}^{\text{P}}|_{i_{n,p}=i_1} > c_{n,p}^{\text{P}}|_{i_{n,p}=i_2} \tag{7}$$

$$c_{n,p}^{\text{V}}|_{i_{n,p}=i_1} > c_{n,p}^{\text{V}}|_{i_{n,p}=i_2} \tag{8}$$

$$c_{n,p}^{\text{op}}|_{m_{n,p}=m_1} > c_{n,p}^{\text{op}}|_{m_{n,p}=m_2} \tag{9}$$

$$q_n|_{i_{n,p}=i_1} > q_n|_{i_{n,p}=i_2} \tag{10}$$

$$s_n|_{t_{n,p}=t_1} > s_n|_{t_{n,p}=t_2} \tag{11}$$

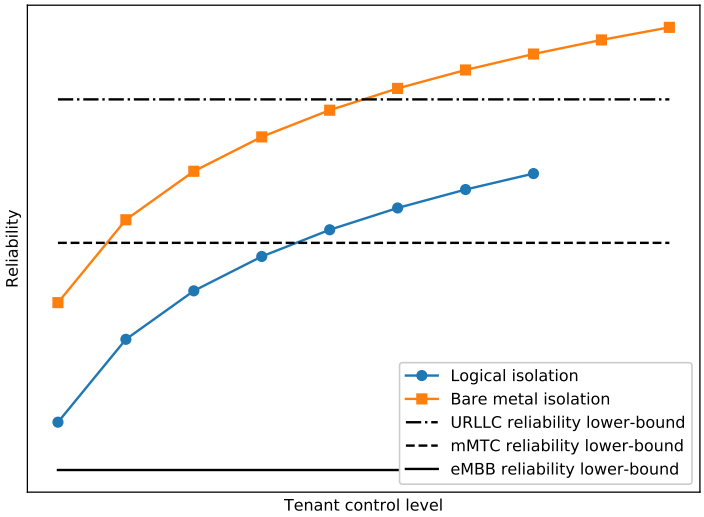
$$s_n|_{i_{n,p}=i_1} > s_n|_{i_{n,p}=i_2} \tag{12}$$

More specifically, Equation (6) implies the constrains of the isolation level and the upper bound of the MNO control level. As a result, with more isolation, more layers in the protocol stack can be securely controlled by the MNO. Equations (7) and (8) imply the infrastructural cost of a network slice under a certain level of the protocol layer—regardless of whether the protocol layer is physically or virtually implemented. Furthermore, the cost of network slice would increase along with the isolation. For example, it may cost more to maintain the protocol layer on an air-gap isolation-independent server than to run it on a virtual machine. Equation (9) shows that the cost of operations is related to the protocol layer, which increases along with the MNO control level, since it requires more effort in the VNF MANO module. Equation (10) shows that the performance of a network slice that can be improved by raising the isolation level of its arbitrary protocol layer since less loss will be caused by the resource scheduling among different slices sharing the same infrastructure under bare-metal or virtual machines. Equation (11) demonstrates the fact that a network slice is more secure when more of its control is granted to the tenant rather than the MNO. Equation (12) demonstrates that when a network slice is more secure, it is a better isolation from the other network slices. It is worth remarking that $\mathbf{I}$, $\mathbf{T}$ and $\mathbf{V}$ are all defined on discrete sets, making the problem in Equation (5a)–(5d) non-convex and therefore rejecting conventional convex optimization problem solvers. Nevertheless, their domains are all finite, making it possible to solve Equation (5a)–(5d) with a simple exhaustive search in cases where N, P and $|\mathcal{T}|$ are small. For cases where the dimension is large and an exhaustive search becomes computationally expensive, we can relax Equation (5a)–(5d) into a linear programming (LP) problem by extending the domains of $\mathbf{I}$, $\mathbf{T}$ and $\mathbf{V}$ into continuous spaces

through linear interpolation. Such linear programs are guaranteed to be efficiently solved with polynomial time complexity. Thereafter, the optimal solution to the original problem in Equation (5a)–(5d) can be obtained by rendering the optimum relaxed LP, e.g., with the well-known branch-and-bound or cutting-plane algorithms.

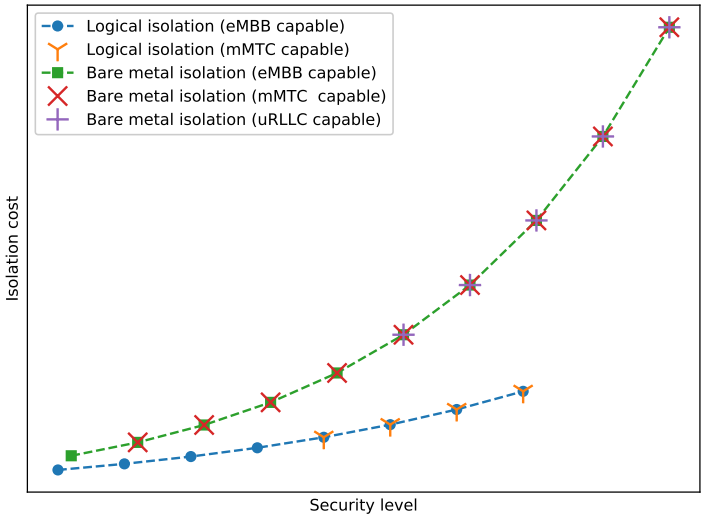
Network Slice Planning Procedures

An overview of network slice deployment planning procedures is provided as follows. We begin with Figure 6a, which gives the network slice isolation plan based on Quality of Service (QoS) satisfaction. Basically, the QoS satisfaction shall be conducted and aggregate individual QoS parameters. We take the reliability as an example, which is shown in Figure 6a. The three horizontal lines on the graph represent the minimal reliability requirements of a specific type of network slice service. More specifically, the level of the service reliability requirement of an enhanced Mobile Broadband (eMBB) network slice is the lowest among the three because eMBB may accept high-latency network QoS and a certain level of packet loss. The level of service reliability of a massive Machine-Type Communications (mMTC) network slice is on a mid-level since mMTC deploys a large number of device connections with short messages transmission and no re-transmission policy characteristics since the duty cycle of mMTC devices may be very short. These features of mMTC are asking for a better service reliability than that of the eMBB network slice. Last but not the least, the highest service reliability is an Ultra-Reliable Low-Latency Communications (URLLC) network slice, which very often applies to deliver critical infrastructure while commonly providing a certain level of defense mechanisms. Figure 6b gives another network slice deployment consideration. We often see the network slice deployment using air-gap isolation, logical isolation or a combination of isolation methods. Obviously, each network slice would have a set of constrains with different protocol stacks that can be controlled by tenant or MNO.From the MNO point of view, when the tenant has more control of the network slice, it is better to apply air-gap isolation because there is better reliability than logical isolation. Figure 6b provides the result of comparing air-gap (bare-metal) isolation and logical isolation. Therefore, in terms of considering isolation, when we have the same isolation level, the reliability increases with the tenant control level. On the other hand, a network slice that has the maximal tenant control level requires the isolation level to be maximal as well. It can use air-gap isolation, which is shown in the Figure 6b.



(**a**)

Figure 6. *Cont.*



(**b**)

Figure 6. How to select the appropriate NS isolation plan: (**a**) check the QoS satisfaction under different isolation plans, and (**b**) select the isolation plan with regards to the trade-off between security and cost.

According to the results, obviously, the tenant can remove some of the isolation options. For example, in general, logical isolation would not be possible for deployment in URLLC services due to performance requirements; the only possible solution would be to apply air-gap isolation with physical resources. We can further to discuss the trade-off, which is shown in Figure 6b. Basically, the tenant can choose from all the available options with regard to its cost of security and defense preference. Typically, the tenant may demand a security-hardening network slice, but the cost of isolation would be directly proportional to security hardening, which is shown in Figure 6a. Figure 6b also indicates the upper bound of the security level related to the upper bound of the tenant control level, i.e., by the isolation level, bare-metal isolation can achieve more than logical isolation. In order to achieve a better level of security, it is always better to use air-gap (bare-metal) isolation rather than logical isolation. However, it may cost more and have less flexibility.

5. Conclusions and Outlooks

When deploying NSaaS, the MNO must resolve various levels of complex deployment and operation issues in order to provide a secure service to the vertical industries (tenants). Although, 3GPP has thoroughly laid out the 5G standalone architecture and provides network slice application functions, it has not yet identified the common practice and security design in operating the NSaaS. With its main functions based on virtualization and containerization technologies, NSaaS provides flexibility and agility for the telecommunication infrastructure; however, it also introduces a number of new risk factors and widens the attack surface simultaneously. In this paper, we have explored and addressed the complexity and challenges of risk factors and the attack surface in eight layers of NSaaS, which allow MNOs and tenants to identify the defense mechanisms on each of the particular network slices. In particular, for an NSaaS platform in operation, each of the network slices should apply a certain level of isolation that reflects the level of protocol stack control from either the MNO or the tenant. Furthermore, these deployed isolation methods are related to the overall protection of the network infrastructure, and defense mechanisms should be embedded within the network architecture, e.g., microsegmentation, etc. We have also developed a mathematical model to represent the relationship between isolation level and the control distribution over the MNO and tenant. This model can be used to guide the MNO and tenant in designing the SLA regarding their control levels and the isolation cost of the deployed network slice. The results show that air-gap isolation

provides the ideal performance of network slice deployment, but it also has the highest cost due to the under-utilization of resources. As a possible research direction for our future work, it is of great interest to evolve the qualitative models we have developed in this article into quantitative ones. To do so, case studies of specific deployment scenarios and practical applications must be carried out.

Author Contributions: Conceptualization, S.W.; methodology, S.W.; formal analysis, B.H.; investigation, S.W., B.H.; resources, S.W. and H.D.S.; writing—original draft preparation, S.W. and B.H.; writing—review and editing, B.H., S.W. and H.D.S.; visualization, S.W. and B.H.; project administration, H.D.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

Abbreviations

The following abbreviations are used in this manuscript:

3GPP	Third-Generation Partnership Project
AD	Administrative Domain
eMBB	enhanced Mobile Broadband
GSMA	GSM Association
ITU	International Telecommunication Union
mMTC	Massive Machine-Type Communications
MNO	Mobile Network Operator
NFV	Network Function Virtualization
NSaaS	Network Slice as a Service
QoS	Quality of Service
SDN	Software-Defined Network
SLA	Service Level Agreement
VNF	Virtual Network Function
URLLC	Ultra-Reliable Low-Latency Communications

References

1. Subedi, P.; Alsadoon, A.; Prasad, P.W.C.; Rehman, S.; Giweli, N.; Imran, M.; Arif, S. Network Slicing: A next generation 5G perspective. *Eurasip J. Wirel. Commun. Netw.* **2021**, *2021*, 102. [CrossRef]
2. Cunha, V.A.; da Silva, E.; de Carvalho, M.B.; Corujo, D.; Barraca, J.P.; Gomes, D.; Granville, L.Z.; Aguiar, R.L. Network slicing security: Challenges and directions. *Wiley Int. Technol. Lett.* **2019**, *2*, e125. [CrossRef]
3. Olimid, R.F.; Nencioni, G. 5G network slicing: A security overview. *IEEE Access* **2020**, *8*, 99999–100009. [CrossRef]
4. Ordonez-Lucena, J.; Ameigeiras, P.; Contreras, L.M.; Folgueira, J.; López, D.R. On the rollout of network slicing in carrier networks: A technology radar. *Sensors* **2021**, *21*, 8094. [CrossRef] [PubMed]
5. Jorquera Valero, J.M.; Sánchez Sánchez, P.M.; Lekidis, A.; Fernandez Hidalgo, J.; Gil Pérez, M.; Siddiqui, M.S.; Huertas Celdrán, A.; Martínez Pérez, G. Design of a security and trust framework for 5G multi-domain scenarios. *J. Netw. Syst. Manag.* **2022**, *30*, 7. [CrossRef]
6. Wichary, T.; Mongay Batalla, J.; Mavromoustakis, C.X.; Żurek, J.; Mastorakis, G. Network slicing security controls and assurance for verticals. *Electronics* **2022**, *11*, 222. [CrossRef]
7. Fan, C.I.; Shih, Y.T.; Huang, J.J.; Chiu, W.R. Cross-network-slice authentication scheme for the 5th Generation mobile communication system. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 701–712. [CrossRef]
8. Suárez, L.; Espes, D.; Le Parc, P.; Cuppens, F.; Bertin, P.; Phan, C.T. Enhancing network slice security via Artificial Intelligence: Challenges and solutions. In Proceedings of the Conference C & ESAR 2018, Rennes, France, 16–17 November 2018.
9. Esmaeily, A.; Kralevska, K. Small-scale 5G testbeds for network slicing deployment: A systematic review. *Wiley Wirel. Commun. Mob. Comput.* **2021**, *2021*, 6655216. [CrossRef]
10. GSM Association. Whitepaper. An Introduction to Network Slicing. 2017. Available online: https://www.gsma.com/futurenetworks/wp-content/uploads/2017/11/GSMA-An-Introduction-to-Network-Slicing.pdf (accessed on 27 January 2022).
11. GSM Association. NG.116. Generic Network Slice Template v6.0. 2021. Available online: https://www.gsma.com/newsroom/wp-content/uploads//NG.116-v6.0.pdf (accessed on 27 January 2022).
12. Valsamas, P.; Papadimitriou, P.; Sakellariou, I.; Petridou, S.; Mamatas, L.; Clayman, S.; Tusa, F.; Galis, A. Multi-PoP network slice deployment: A feasibility study. In Proceedings of the IEEE 8th International Conference on Cloud Networking (CloudNet), Coimbra, Portugal, 4–6 November 2019.

13. Available online: https://www.cisecurity.org/resources/?type=benchmark (accessed on 27 January 2022).
14. NIST. Defending against Software Supply Chain Attacks. April 2021. Available online: https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf (accessed on 27 January 2022).
15. GSM Association. Whitepaper. Mobile Telecommunications Security Landscape. March 2021. Available online: https://www.gsma.com/security/wp-content/uploads/2021/03/id_security_landscape_02_21.pdf (accessed on 27 January 2022).
16. Available online: https://www.ncsc.gov.uk/collection/supply-chain-security (accessed on 27 January 2022).
17. ISO/IEC 22237—1:2021.Information Technology—Data Centre Facilities and Infrastructure—Part I General Concept. Available online: https://www.iso.org/standard/78550.html (accessed on 27 January 2022).
18. Ye, C.; Cheung, S.C.; Chan, W.K. Sifter: A Service Isolation Strategy for Internet Applications. *IEEE Trans. Serv. Comput.* **2021**, *14*, 1545–1557. [CrossRef]
19. Hariri, S.; Kind, M.C.; Brunner, R.J. Extended Isolation Forest. *IEEE Trans. Knowl. Data Eng.* **2021**, *33*, 1479–1489. [CrossRef]
20. Carnes, J.R.; Fisher, D.H. Machine Learning Techniques for Fault Isolation and Sensor Placement. In Proceedings of the 1993 Goddard Conference on Space Applications of Artificial Intelligence, Greenbelt, MD, USA, 10–13 May 1993.
21. Ben Saad, S.; Ksentini, A.; Brik, B. An end-to-end trusted architecture for network slicing in 5G and beyond networks. *Secur. Priv.* **2022**, *5*, e186. [CrossRef]
22. 3GPP, TS 38.300. NR; NR and NG-RAN Overall Description; Stage-2. Release 16. Available online: https://www.3gpp.org/DynaReport/38300.htm (accessed on 27 January 2022).
23. 3GPP, TS 33.501. Security Architecture and Procedures for 5G System. Release 17. Available online: https://www.3gpp.org/DynaReport/33501.htm (accessed on 27 January 2022).