Enabling QoS-secured Enhanced Non-Public Network Slices for Health Environments

Henrique C. Resende, Joao Paulo B. Gonçalves
University of Antwerp - imec, Belgium
{henrique.carvalhoderesende, joaopaulo.britogoncalves}@uantwerpen.be

Cristiano B. Both
University of Vale do Rio dos Sinos, RS, Brazil
cbboth@unisinos.br

Johann M. Marquez-Barja
University of Antwerp - imec, Belgium
johann.marquez-barja@uantwerpen.be

ABSTRACT

5G networks are envisioned to provide high Quality of Service (QoS) for several use cases that differ on their network requirements and where they should be deployed. Some use cases are deployed in Public Land Mobile Network (PLMN) infrastructures that are managed by mobile network operators. However, for other use cases, devices connect to the services over private networks or Non-Public Network (NPN). The NPN deployment is mostly envisioned by companies that will benefit from Industry 4.0 and also eHealth to enhance QoS and network security. Network slicing is the 5G concept that comes to address the different service requirements over the same network. In this paper, we present an experimental study on deploying a network slicing solution for an NPN in health environments. This solution aims to provide both performance isolation over WiFi networks and privacy isolating the service traffic over the NPN network backhaul on the way to the application server, thus providing data confidentiality.

CCS CONCEPTS

- **Networks** → Network reliability.

KEYWORDS

network slicing, quality of service, 5G network, wireless connection

1 INTRODUCTION

The new 5G networks have the challenge to fulfill the strict requirements of several use cases [5]. For some use cases, low-latency is a critical requirement for the overall service performance, such as Ultra-Reliable Low-Latency Communication (URLLC) services. For others, high network throughput is the fundamental requirement, for instance, for enhanced-Mobile Broadband (eMBB) services. The network infrastructure should be prepared to fulfill such a fruitful variety of requirements, customize the infrastructure, prioritize services, and virtualized resources. Network slicing is the research topic that studies techniques to share resources and provide the expected QoS for connected clients [5].

The shared resources cover from Virtual Network Function (VNF) to radio spectrum. Hence, the Mobile Network Operator (MNO) should provide tools to isolate access and performance among different services. For radio slicing, the MNO applies techniques on the physical and MAC levels of their infrastructure, such as scheduling and resource block allocation [4], to attend latency and throughput requirements. However, some use cases in Industry 4.0 and Health demand that the devices will be connected to a private network, and MNO will not be able to provide the necessary network performance for such services.

The 3rd Generation Partnership Project (3GPP), the organization assessing the requirements for the new network infrastructures in the second phase of 5G networks (3GPP Rel-16 and beyond) [3], classifies the future 5G networks in two: Public Land Mobile Network(PLMN) and Non-Public Network (NPN). The former is the network provided directly by the MNO infrastructure and will be capable of attending several service requirements. The latter is the classification of networks deployed for private reasons, such as providing indoor connectivity for sensors, robots, auto-guided vehicles, and remote worker's AR-enabled tablets [9]. Figure 1 shows the differences between these networks.

Hospitals networks are one example of NPN because they are the medium to transmit indoor, highly sensitive information every day. Furthermore, to provide connectivity to indoor sensors and hospital services, hospitals will need to deploy a private network with-in their infrastructure. This private infrastructure will enable hospitals to prioritize network traffic and secure the information since the edge of the network. However, to deploy an NPN, studies on how to enable network slicing techniques will be needed to assess heterogeneous radio technologies and integration with PLMNs.

ProTego project[1] researches on security measures to be applied in hospital environments. Network slicing was envisioned to provide both performance and privacy isolation for different slices in the network and enable the dynamic allocation and deallocation of slices in NPN. To offer network slicing, ProTego is developing a tool to manage the network parameters and enhance hospital services. This tool should provide prioritization of hospital services over a WiFi network, which is the most common wireless network type for indoor network access and should provide techniques to isolate the access among services inside Intranet until the application server.

In this paper, we present the design and development of a network slicing solution for NPN hospital environments. The solution integrates state-of-the-art technologies to provide WiFi performance isolation, privacy isolation in a hospital intra-network, and also an upper API that maintain the infrastructure synchronized with the QoS rules. ProTego Network Slicing tool contributions are: (*i*) design an architecture for network slicing in hospital environments, (*ii*) assess the limitations and objectives of network slicing for hospital services, (*iii*) provide an open-source prototype and instructions for network slicing in hospital environments. Furthermore, the long-term objective of the ProTego project is to provide an open-source network slicing toolkit to secure data traffic even for low-cost hospitals that cannot afford expensive technologies to ensure its patients' confidential data.

[1]https://protego-project.eu/

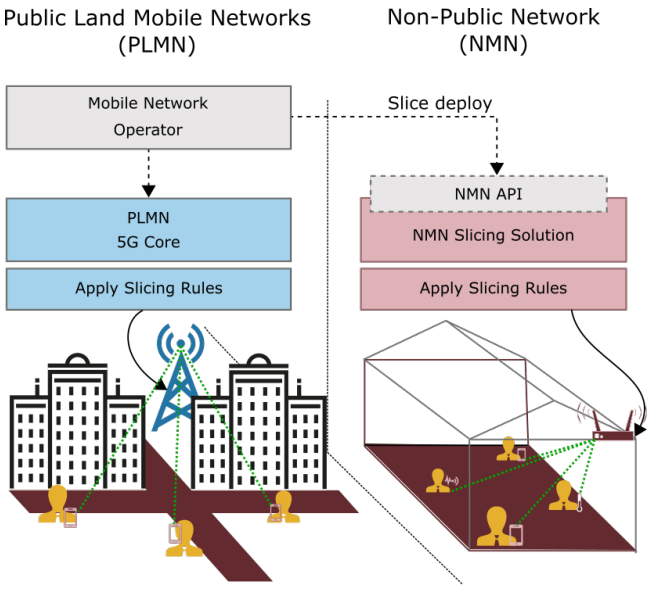

Figure 1: PLMN versus NPN

2 BACKGROUND

Healthcare facilities like hospitals are listed in the top five targets for malware and ransomware, as published by Cylance in [7]. This focus in healthcare facilities is probably because of sellable sensitive data about patients being transmitted through their network and stored in their infrastructure. Hospitals need to provide specialized treatment for critical applications that can support and optimize the health care of patients.

The above couple of characteristics of hospital network infrastructure leads hospitals to choose for NPN deployments, where the network traffic is mostly isolated. However, studies on NPN for hospital environments are still scarce, and it will need more efforts to enable the deployment of such infrastructure. Research projects, like ProTego, are investigating this matter. ProTego assesses security from all perspectives such as encryption key management, encrypted storing and access, continuous authentication on client-side, and network slicing.

A network slice can be described as an expected network behavior for a given service. The network operator of the hospital will manage the network slicing in a hospital environment, and the slices are divided per service. These services in a hospital have different priorities, for instance, a nutrition application, with a low priority, and a hearth-beat monitoring application, with a high-priority. Therefore, the network slicing will use the available tools to prioritize the traffic of one service over another with lower priority.

5G-EmPOWER is an SDN framework for 5G networks that provides slicing techniques [2]. WiFi has proven to be one of the leading technologies to connect users to the network. Therefore, for hospital environments, the feature of the WiFi slicing that 5G-EmPOWER provides serves to isolate the performance of different services at the radio-side. 5G-EmPOWER utilizes techniques and specific hardware to virtualize the WiFi access points and offer different QoS to each of the connected users. QoS is managed by dynamic, creating prioritization queues and steering the data packets to the list that matches with the necessary performance. To identify the service traffic, 5G-EmPOWER uses OvS (Open vSwitch) to tag network packets, which will enable the WiFi scheduler to apply the right prioritization rule for that flow. OvS is a virtual OpenFlow switch that allows the traffic steering and network isolation using OpenFlow rules. Therefore, OvS is an intersection point of performance and privacy isolation.

For the privacy isolation, OvS is used to steer the traffic among different network interfaces that can tunnel the network traffic, apply encryption techniques, or send raw data to the network. These open possibilities enable the dynamic privacy isolation for different levels of sensitive information.

For instance, a service that transmits hearth-beat data for monitoring servers has confidential information about patient health status. Moreover, this service does not require a high network throughput, neither a low latency. Therefore, the network should attend this critical service by prioritizing the service on the radio-side and applying encryption to send the application data through the network. Besides this, there is still research on how to design and what techniques should be used to fill up the requirements for an NPN slicing. Therefore, some features, such as continuous monitoring and automatic adjustments on run-time should be assessed.

2.1 ProTego Network Slicing

The ProTego network slicing provides performance and privacy isolation of NPN hospital networks. Hospital services will be prioritized over generic network traffic using the radio access networks, performance, and private network isolation. Furthermore, avoiding unauthorized access to sensitive data. Therefore, we design the ProTego network slicing to receive input from external actuators such as MNOs or the hospital network operators and setup the network to achieve the necessary Key Performance Indicatorss (KPIs).

The ProTego network slicing is composed of three layers, as can be seen in Figure 2. The first layer is to process input from external actuators. This input could be direct tweaking network parameters or providing a network slice type file, as specified by GSM Association[1]. This file or command is processed by the Slice Processor and generates performance and privacy rules, which are sent to the Performance Isolation Engine and the Privacy Isolation Engine. The engines can map the requirements to API calls to the available software, *i.e.*, Software-defined Radio (SDR) controller, Software-Defined Networking (SDN) controller, and the Secure Interface Setup. The SDR controller is responsible for configuring the radio parameters and prioritization queues to reach the necessary performance for the specified service. It will set the available SDN network to steer the traffic securely and without performance degradation inside the hospital infrastructure.

The Secure Interface Setup will provide secure network interfaces with encryption techniques to enable the confidentiality control of sensitive data. These secure network interfaces will be available for the SDN switches to steer the critical service flow through them and perform an extra and customized security layer for hospital services.

3 TESTBED SETUP

Network slicing in the ProTego context is the logical isolation of the network flow per service. It provides an extra security layer for ProTego services and prioritize the traffic in the radio link. To validate the NPN slicing, we design a testbed with radio access, gateway, and processing nodes to emulate a real NPN infrastructure.

Our testbed includes an IEEE 802.11 wireless network using an access point and a client device to emulate an NPN infrastructure for hospital environments. This IEEE 802.11 access point needs to support specialized requirements for slicing. For example, exposing the access point Basic Service Set Identifier (BSSID) register so that can be changed on-demand following the service requirements of QoS and handover [6]. By customizing the BSSID register, it enables a centralized controller to manage the handover for IEEE 802.11 networks, directly affecting the QoS.

Following the ProTego network slicing architecture aforementioned, a privacy gateway and a processing node were deployed. The privacy gateway acts like a middle-box that applies security methods for service flows accessing hospital services or even services outside the hospital infrastructure. Moreover, the processing node serves as a host to hospital services being the end-point of the communication.

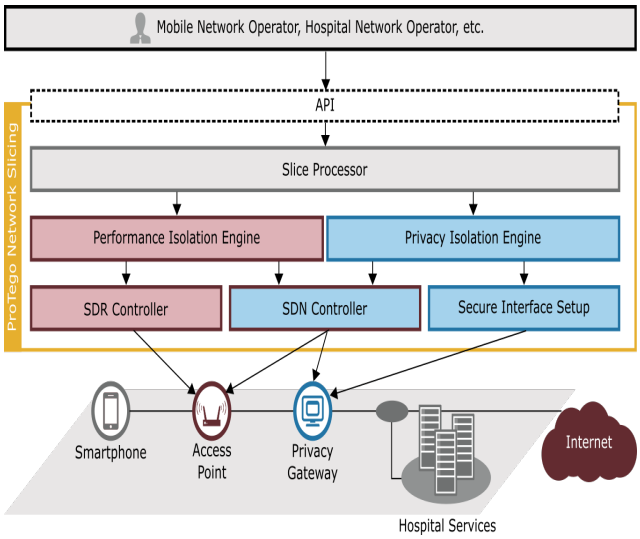

Figure 2: ProTego architecture

3.1 Slicing enablers

Slicing enablers are the frameworks and tools that apply slicing techniques to virtualize, isolate, and prioritize the services' network traffic. Therefore, we chose a set of tools to compose our ProTego network slicing solution to provide performance and privacy isolation for NPN hospital environments.

Performance Isolation. The slicing enabler for performance isolation is 5G-EmPOWER. It performs downlink network traffic prioritization for 802.11 networks and can isolate the traffic by service using OpenFlow (OF) rules. The

5G-EmPOWER components are (*i*) controller, (*ii*) Backhaul controller, and (*iii*) the Wireless Termination Point (WTP). The controller is the component responsible for the management of the Radio Access Network (RAN) by deploying the necessary configuration in WTP, prioritizing the network traffic.

The Backhaul controller manages SDN switches, which identify and tag the network packets that need to be prioritized. These tagged network packets will be identified by a packet processor responsible for prioritizing the wireless network traffic. Both controllers are deployed in the Intel NUC wrapped up in docker containers and accessible by the access points. WTPs is deployed in the WiFi access points where the clients connect, and the network bandwidth is monitored and managed. For the more in-depth research on the functioning of 5G-EmPOWER, see [6, 8].

Privacy Isolation. We utilize OvS to steer the traffic based on the service flow among several interfaces to enable access isolation and an extra security layer's appliance. Open vSwitch (OvS) allows the use of OF rules and has modules that implement Virtual Extensible LAN (VXLAN) and Internet Protocol Security (IPsec) encapsulations protocols. VXLAN creates a virtual network and applies different network identifiers to service flows, which helps the isolation of the network traffic. While the IPsec implements the cryptography, adding confidentiality to the data flowing in the network.

The privacy isolation solutions are deployed in the privacy gateway, which provides security per service flow until the hospital's private datacenter. The access points have one-hop connectivity security that protects the data flow from external and internal attacks using the privacy gateway. The encryption of the data needs to take place as near to the edge as possible, encrypting the data on the access point or in a more processing powered unit, the privacy gateway.

3.2 Envisioned scenario

The ProTego network slicing system has its Minimum Viable Product (MVP) with the hardware and slicing enablers being setup. However, the quality of the network connectivity using these solutions should be assessed to understand patterns of behavior and how they affect QoS in the hospital infrastructure. For example, adding an extra security layer affects the service network throughput, and different encryption methods should be considered based on the type of service.

In the envisioned scenario, the wireless client connects to the access point with the 5G-EmPOWER WTP enabled. The client has two services requesting data from a hospital service server located in the processing node. Before getting to the processing node, the service traffic passes through the privacy gateway, which encrypts the traffic for this specific service flow. In our scenario, the controllers were deployed in the privacy gateway, which was already configured with a container engine. The container engine supported the deployment of the 5G-EmPOWER controller, Backhaul controller, and the Secure Interface Setup in different containers, isolating the control services from one another. We could analyze the behavior patterns of NPNs with different QoS requirements with this testbed setup.

4 TESTBED EVALUATION

To validate the actual outcome of our slicing solution, we performed three different experiments, two (*i, ii*) for performance isolation and one (*iii*) for privacy isolation. The performance isolation experimentation assessed the behavior of the software with (*i*) UDP and (*ii*) TCP protocols to analyze the availability of ProTego services given the protocol utilized. Furthermore, (*iii*) the privacy isolation using VXLAN is evaluated regarding the deployment time of a slice and performance degradation.

4.1 Performance isolation

The experiment for performance isolation aims to validate the expected software behavior for different protocols such as TCP and UDP. Validation using both protocols was chosen to analyze how network slicing would behave with services that will be used in the hospital and that use both transport protocols. Due to the distributed characteristic of WiFi, it is already known beforehand that only the client downlink will be sliced. 5G-EmPOWER, the tool used for performance isolation, does not modify the client only the access point.

The experiment is deployed using two iPerf3 flows emulating two different services. These iPerf3 clients connect to different iPerf3 servers accessible in various ports, enabling OvS to detect the unusual traffic generated using OF rules for different source ports. Having two different services, we configured in 5G-EmPOWER one slice for each service enabling the customization of the utilized airtime by them. 5G-EmPOWER identified three slices in total being two for our emulated hospital services and the other for general traffic, as can be seen in Figure 3. For both experiments of UDP and TCP, the bitrate for the iPerf traffic was set to 20Mbps from the processing node to the wireless client (downlink). Moreover, for the UDP, the experiment starts distributing the traffic equally, and at the 90th second, we give only a third of the airtime to the slice 1, as can be seen in Figure 4, indicated by the arrow.

In general, the traffic through the wireless link has a lot of variation due to the interference. In the first half of the UDP experiment, we can see that the traffic for both slices maintains the same throughput, confirming the network's

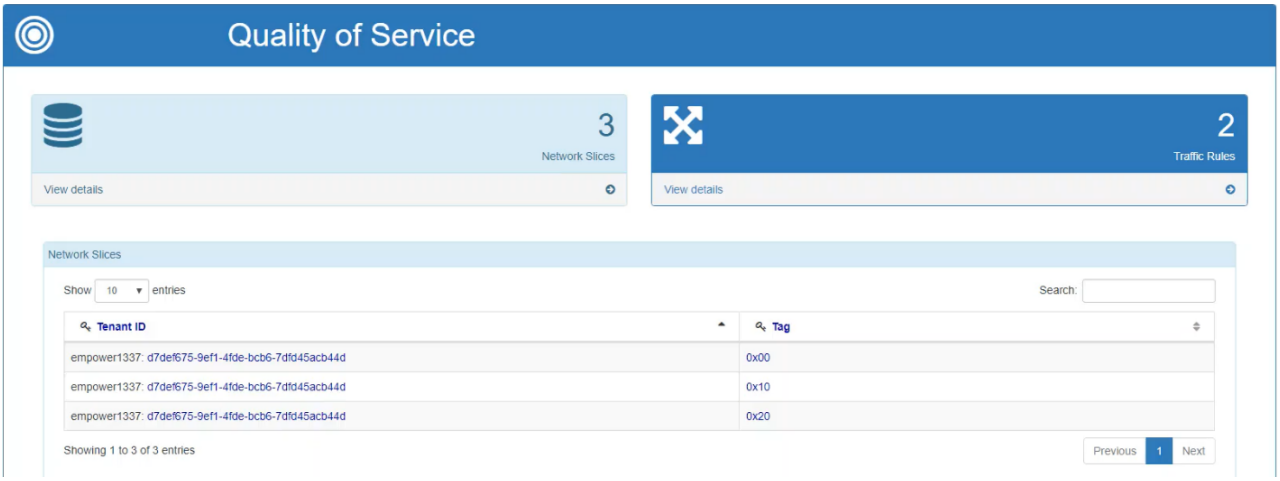

Figure 3: EmPOWER slices

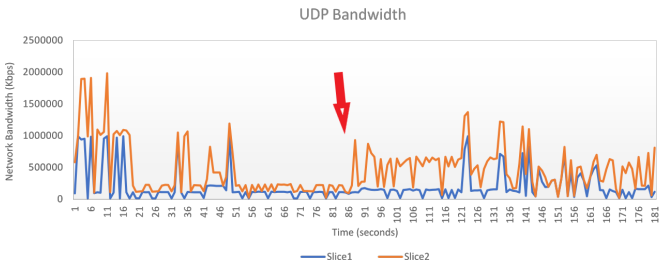

Figure 4: Performance UDP

expected behavior given the airtime configuration. Furthermore, after the second 90, slice 1 was changed to 1/3 of the airtime of slice 2. The result of this change can be explicitly seen in the second half of the chart when the throughput of slice 2 increases. Besides some network spikes due to wireless connectivity variation, slice 1 throughput keeps at 1/3 of the network throughput of slice 2, demonstrating that the UDP downlink for the application can be customized to prioritize hospital services.

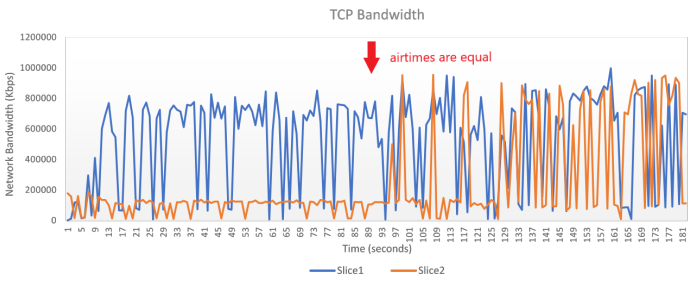

Figure 5: Performance TCP

The experiment for the performance isolation of TCP traffic started with different airtimes for the slices. After the second 90, the airtimes were equally distributed between the slices, as shown in Figure 5. The distribution of airtime started with slice 2 having 1/4 of the airtime of slice 1. After we changed the airtime for slice 2 to the same as slice 1, we can see that the throughput of slice 2 does not adapt immediately, having an adaptation time before consuming the same amount of bandwidth as slice 1. This delay is caused by the normal behavior of the TCP protocol, which increases the amount of data sent gradually. After assessing the outcome of using performance isolation with downlink TCP traffic, we conclude that any Web-based application most of the time the downlink traffic is higher than the uplink traffic will benefit from the performance isolation provided by 5G-EmPOWER and the ProTego network slicing tool.

4.2 Privacy isolation

The privacy isolation is characterized by the separation and encryption of given traffic, *i.e.*, service or client. In ProTego, the encryption method must be utilized to protect the confidentiality of patients and staff data. The patient's and staff's service data are encrypted when passing through a virtual secure network interface that utilizes VXLAN to create a virtual network and IPsec as a secure protocol. It is fundamental to understand how security affects the QoS of the network, so a trade-off between security-enabled slices and non-secure slices can be researched. Therefore, to assess the behavior of the proposed privacy isolation tool, we deployed two iPerf3 clients and two iPerf3 servers. The first iPerf3 connection uses the UDP protocol, and the second uses TCP. The traffic in this experiment is separated by protocol, but later can be enhanced to separate by destination port, for example. The default virtual network interface is tagged with VXLAN Network Identifier (VNI) 10, and the secure network slice is

tagged with VNI 20. We highlight that in this experiment, the traffic steering among different virtual interfaces was assessed. However, the encryption of the secure interface is still pending and will require further investigation.

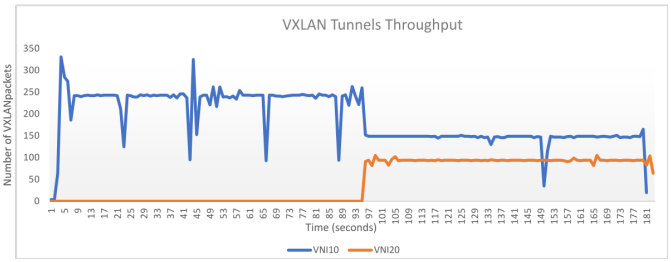

Figure 6: Privacy isolation chart

We started the two traffic generator, as shown in Figure 6, in the second 0. The data were collected by sniffing the physical network interface where both traffic, secure, and not secure, pass-through. At first, the secure network slice was not created, due to all the traffic was passing through the default virtual interface with the VNI 10. After the second 90, the slice was created, and the UDP traffic was redirected to the secure virtual interface, tagged with the VNI 20. The deployment of the OF rule for traffic steering was proven to be useful for our purposes, having less than 5 seconds of delay on changing the traffic from the default interface to the secure interface. Therefore, we will enhance this tool, so it will be possible to create several network slices with different security protocols and techniques.

5 CONCLUSIONS AND FUTURE WORK

This paper presents research on NPN solutions focused on slice characteristics for hospital environments. It was first clarified that studies in such areas of NPN slices are just starting, and basic research is essential at this stage. A simplified NPN architecture to base the studies on experimental NPN slicing was presented in this paper. Up next, to provide precise results for this initial research on NPN slicing, a testbed setup was implemented and described. Having designed and assessed the bases of an NPN infrastructure, the communication and the abstraction infrastructure translation with MNO or hospital network operator should be assessed. Therefore, a study on the main standards for network slicing description will be done together with the translation of the slice requirements to infrastructure configuration.

ACKNOWLEDGEMENTS

This research received partial funding from the European Union's Horizon 2020 Research and innovation program, under grant agreement No. 826284 (ProTego).

REFERENCES

[1] 2018. From Vertical Industry Requirements to Network Slice Characteristics. web site. (2018). https://www.gsma.com/futurenetworks/wp-content/uploads/2018/09/5G-Network-Slicing-Report-From-Vertical-Industry-Requirements.pdf

[2] 2020. 5G-EmPOWER. web site. (march 2020). https://5g-empower.io/

[3] 3GPP. 2019. *Service requirements for the 5G system*. Technical Specification (TS) 22.261. 3rd Generation Partnership Project (3GPP). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3107 Version 16.10.0.

[4] I. Afolabi et al. 2018. Network Slicing and Softwarization: A Survey on Principles, Enabling Technologies, and Solutions. *IEEE Communications Surveys Tutorials* 20, 3 (thirdquarter 2018), 2429–2453.

[5] A.A. Barakabitze et al. 2020. 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges. *Computer Networks* 167 (2020).

[6] E. Coronado et al. 2018. Lasagna: Programming Abstractions for End-to-End Slicing in Software-Defined WLANs. In *2018 IEEE 19th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*. 14–15.

[7] Cylance. 2019. *2019 Threat Report*. Technical Report. Cylance. https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/Cylance-2019-Threat-Report.pdf?_ga=2.194100014.207560192.1557408928-1034628078.1557241850

[8] P. H. Isolani et al. 2019. SDN-based Slice Orchestration and MAC Management for QoS delivery in IEEE 802.11 Networks. In *2019 Sixth International Conference on Software De ned Systems (SDS)*. 260–265.

[9] J. Ordonez-Lucena et al. 2019. The use of 5G Non-Public Networks to support Industry 4.0 scenarios. In *2019 IEEE Conference on Standards for Communications and Networking (CSCN)*. 1–7.