Advanced 5G Network Slicing Isolation Using Enhanced VPN+ for Healthcare Verticals

Bruno Dzogovic[1(✉)], Tariq Mahmood[2], Bernardo Santos[1], Boning Feng[1], Van Thuan Do[3,1], Niels Jacot[3], and Thanh Van Do[4,1]

[1] Oslo Metropolitan Univeristy, Pilestredet 35, 0167 Oslo, Norway
{bruno.dzogovic,bersan,boning.feng}@oslomet.no
[2] University of Oslo, Gaustadalléen 23B, 0373 Oslo, Norway
tariqmah@ifi.uio.no
[3] Wolffia AS, Haugerudvn. 40, 0673 Oslo, Norway
{vt.do,n.jacot}@wolffia.net
[4] Telenor ASA., Snarøyveien 30, 1331 Fornebu, Norway
thanh-van.do@telenor.com

Abstract. Alongside enabling connectivity for people and societies, the fifth-Generation networks (5G) aimed towards establishing an all-inclusive ecosystem for Internet of Things to sustain variety of industrial verticals such as e-health, smart home, smart city, etc. With the successful implementation of 5G infrastructure, it is understood that the traditional security approaches incorporated in the previous 4th generation networks (4G) may not suffice to protect users and industries from adversaries that develop more advanced attack vectors. This is mostly attributed the vulnerabilities imposed by softwareization (Softwareization of networks, clouds, and internet of things https://onlinelibrary.wiley.com/doi/pdf/10.1002/nem.1967.) and virtualization of the network which compromise the isolation and protection of the 5G network slices essential for the support of IoT verticals. In this work, we propose an innovative approach to enhance the isolation of network slices by employing the Enhanced Virtual Private Network+ (VPN+) technology. Furthermore, we demonstrate the impact of an encrypted communication at the transport backhaul network in 5G scenario in terms of defensive success against virtualization layer attacks in the cloud.

Keywords: 5G · Enhanced VPN+ · Network slicing · IoT security · OpenStack

1 Introduction

Many service providers rely on open infrastructures and the open-source model to provide 5G services and connectivity for customers [1]. However, there are many limitations to consider, including cybersecurity-related ramifications and risks that make the 5G network slicing not sufficiently secure, i.e., for the digital elderly care solution we proposed at the secure 5G4IoT lab [2]. 5G is known to inherit most of the proven security practices from the 4G Long-Term Evolution (LTE), but as the network and infrastructure become

I. M. Pires et al. (Eds.): GOODTECHS 2021, LNICST 401, pp. 121–135, 2021.
https://doi.org/10.1007/978-3-030-91421-9_10

softwareized and deployed in public clouds to support the additional industry verticals (like smart infrastructure, smart homes, Internet of Things, automated transportation etc.), these may be insufficient to secure mission-critical applications and even the average user [3]. To handle issues that emerge because of isolation insufficiency between tenants in the provider's infrastructure, the 3rd Generation Partnership Project (3GPP) introduces the concept of network slicing that aims towards segregation of network resources into logical segments, to provide diverse Quality of Service (QoS) and Quality of Experience (QoE) for the end users or industry verticals. Most vulnerabilities from the cloud can shift into the 5G infrastructure, and these are characterized within a Common Vulnerabilities and Exposure list of records within the MITRE project, initiated by MIT university [4]. Network slicing by itself is not sufficient to provide satisfactory levels of isolation and therefore additional methods are needed to avoid certain vulnerabilities. Some of those involve:

- policy-based networking,
- traffic engineering and autonomous smart dynamic routing,
- hardware-level isolation (if applicable),
- anomaly detection as part of Intrusion Detection/Prevention systems (IDS/IPS)
- other techniques that involve fine-grained dynamic and automated threat intelligence.

This research work investigates the virtualization plane of the communication between the 5G and 4G core networks and the radio frontend; namely, what is sufficient to provide an isolation between network slices in the backhaul of a Network Function Virtualization (NFV)-enabled cloud. To deliver network slicing, currently there is no standardized consensus about the methodology and which approach is to be used, as virtualization of network functions can be achieved in various ways. This suggests that it is required to be stringent in terms of security and isolation. To achieve that, we experiment with the enhanced VPN framework [5] in a cloud environment, while using an open-source methodology to deliver security augmentation of the 5G infrastructure.

The paper begins with an introduction to the background topics and technologies and their role in healthcare. Subsequently, we proceed with elucidating details about the 5G infrastructure as well as the concept of network slicing and its isolation. To finalize, the methodology of implementation is described followed by an evaluation that is comprised of performance assessment and demonstrates the network slices isolation. As a conclusion, we cover the lessons learned and provide details about future possibilities for researching topics related to this question.

2 Background and Related Work

2.1 5G in Healthcare

To retain the confidentiality of information between a healthcare provider and patients, there must be an end-to-end secure communication. Various healthcare management systems rely on the assumption that the healthcare providers should ensure the safety and reliability of patient information. However, it has been shown that in majority of

incidents involving threats to healthcare systems like the THIS (Total Hospital Information System), are vastly attributed to human error [6]. Despite efforts of governments to establish protection standards and regulation about EHRs (Electronic Health Records) information, nonetheless they are greatly targeted by cyber-criminals because of flaws in personal and organizational management [7]. One of the key areas of our society that benefits significantly from 5G is exactly the healthcare. Amalgamating together the Internet of Things (IoT), big data and Machine Learning/Artificial Intelligence (AI/ML), 5G brings the smart infrastructure aspect to the healthcare verticals. This indicates that there will be a high requirement for automation of handling patient data, as well as real-time monitoring practices of patients that are outside of the hospital premises (i.e., in their own homes). Consequently, the probability of human errors will increase, allowing for additional cyber threats to emerge and put at risk the private information of patients [8].

2.2 5G Reference Architecture

The general architecture of the 4G and 5G networks established at the Oslo Metropolitan University are following the 3GPP, European Telecommunication Standards Institute (ETSI) and the International Telecommunications Union (ITU) specifications, designated in the corresponding technical specification TS 23.501 (v15.8.0) [9]. As described in Fig. 1, the virtualized functions of the 4G and 5G Core Networks are deployed in the OpenStack cloud [10], provisioned within containerized environment using the Docker containerization technology [11]. Containers enable a lightweight immutable infrastructure and when paired with orchestrators such as Kubernetes, resilience, self-healing, and certain level of autonomy [12]. The 4G and 5G infrastructure is achieved by instantiating the vNFs of the Core Networks in containers forming a virtual 4G EPC core (vEPC) and a 5G Core (5GC), tightly integrated within a default Docker runtime environment as a base for controlled experimental conditions.

Containers communicate in a mesh network structure, which is a simple and efficient approach but also a security liability as they share the same kernel of the operating system and thus the networking stack. Therein the requirement for more rigorous isolation and securing the communication between the containerized Core Networks and the virtualized Radio Access Network (vRAN) [13]. As indicated in Fig. 1, the mobile network is deployed according to the Radio Access Network model, where the User-Plane (UP) is separated from the Control-Plane (CP) into different functions, i.e., UPF (User Plane Function) and a C-function group that contains the AMF (Access and Mobility Function) and the other 5GC virtual functions, forming a container cluster. The Next-Generation 5G Radio Access Network communicates with the Control Plane via the UPF and this is referred to as "functional split" to achieve more refined control over the radio frontend, for the sake of optimal resource utilization planning [14].

The split of functionalities for the vRAN is regulated according to 3GPP specification TR 38.801 [15] and relates to the decisions of the operator that deploys the infrastructure including the hardware requirements, topology of the transport network, logical organization etc. (see Fig. 2).

To realize a 4G LTE vEPC, we utilize the OpenAirInterface core network and Remote Radio Unit (RRU) [16], while maintaining a Centralized Unit/Distributed Unit (CU/DU)

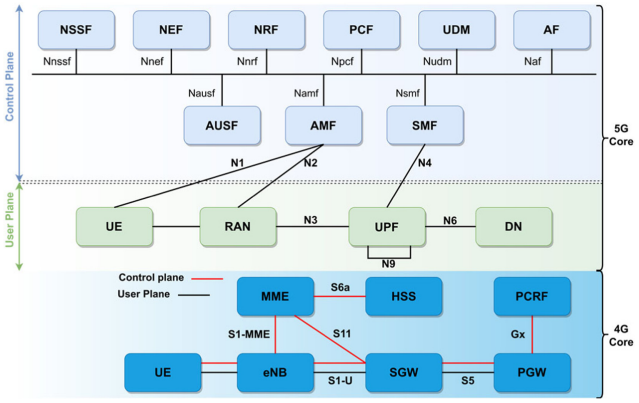

Fig. 1. 4G and 5G Core Networks architecture. 5G decouples the user and control-plane functions unlike the 4G core [14]

split on option 7 according to 3GPP [17]. The 5G next generation RAN and core functions are deployed using the Open5GS core network [18].

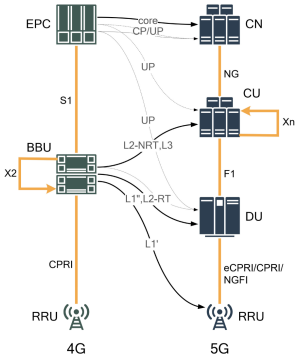

Fig. 2. 4G and 5G functional splits for the transport network. One of many ways 5G moves computationally intensive tasks away from the radio frontend into the cloud and splits the functionality into Centralized and Distributed units.

2.3 Container Virtualization

Containers can deploy various software in a lightweight and immutable manner. Therefore, the Software-Defined Networking (SDN) and slicing controllers, software modems for the evolved Node-B/next-generation Node-B (eNB/gNB) radio frontend for 4G/5G correspondingly, as well as network functions of the 5GC/EPC are provisioned within container environments; that is particularly suitable for Multi-Access Edge and Fog computing scenarios (MEC). The cloud requires support for NFV and a possibility to deliver virtual network functions on-demand or automatically. For that purpose, we utilize the

Tacker module from OpenStack that follows the TOSCA model for NFV. The fundamental advantage of this approach is the possibility to perform service function chaining (SFC), which enables integration of service functions with the SDN controller (O-RAN and OpenDaylight). The traffic is then managed through a VNFFG (VNF Forwarding Graph). The SFC consists of an ordered list of VNFs for traffic to traverse, while the classifier decides which traffic should go through them [19].

The Container Networking Functions are managed and automated with Kubernetes and by using the Tacker module in OpenStack and is not the focus of this current work [20]. Another important module that allows segregation of network resources into virtual and subsequent physical network functions, is the SR-IOV (Single-Input/Output Virtualization) developed by Intel. A rather older approach, the SR-IOV maps and assigns virtual network functions to physical functions [21]. In OpenStack, the SR-IOV runs as an agent on the compute/controller nodes as an element of the Neutron OvS (Open vSwitch) networking component. The agent provides connectivity of instances to the corresponding network infrastructure for VMs via the Intel's VT-d virtualization (that also needs to be supported at a hardware level) [22].

There are various security concerns from running containers in an open infrastructure. Containers suffer of inherent lack of visibility. Most of the underlying infrastructure vulnerabilities that translate into containers are overlooked and this renders many deployments substantially insecure. By using insecure images that do not undergo strict vulnerability analysis practices, an accepting policy can have detrimental consequences to the security of the infrastructure. Containers share the kernel of the host's operating system and cross-talk between namespaces of processes and threads can become a problem.

2.4 Enhanced VPN (VPN+) as Part of the SDN Controller

The 4G/5G infrastructure follows a flat network model, which transports traffic of different types such as the communication between eNBs/gNBs, MME/AMF (Mobility Management Entity/Access and Mobility Function) and cross-handover traffic on the X2-U and X2-C interfaces between the base stations, etc. Furthermore, in 4G the flat IP architecture distributed Radio Network Controller (RNC) functions with eNBs, MME, S-GW and were directly connected to the core network [23]. This led to challenges to provide a secure traffic in the mobile backhaul networks [24].

The enhanced VPN+ facilitates a hard isolation, or specifically an overall separation of underlying network between different network slices with different traffic flows [25]. To resolve this, we refer to the ACTN (Abstraction and Control of Traffic Engineered Networks) framework [25] provided in the realization of a transport network slice, where a vertical industry customers assign the input of their requirements (see Fig. 3). Presumably, the UHD slice is given with MTNC ID = 1, the slice for phone access as MTNC ID = 2, Massive IoT slice with MTNC ID = 3 and URLLC slice MTNC ID = 4. These ID numbers will be appended in TPM (CNC controller) and communicated with the MDSC.

Since the SDN-C has an abstraction of traffic-engineered network topology, it will assign the path to these slices. This same SDN-C has the logical abstraction of the topology in case the vertical industry does not want hard isolation and can build a

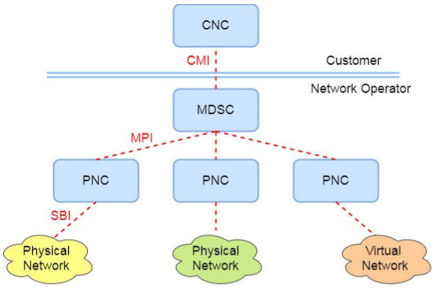

Fig. 3. ACTN architecture components. The network operator controls the infrastructure based on the CNC requests the customers initiate [25]

tunnel based on MPLS or VxLAN VPN. Nevertheless, since we focus on hard isolation, the vertical industry can choose their private tunnel between the two endpoints, which enables for a complete protection of their data without concerns about the interference of other slices' traffic and whether it shall consume the available network resources. In case of a vertical industry requiring an instance of a slice, they can distinguish the slice with a concept of "differentiator", that is an insertion of an additional parameter of MTNC sub-differentiator i.e., MTNC ID 1.1 (where this case represents another instance of slice MTNC 1).

2.5 Network Slicing

Network slicing (or *netslicing*) is defined as a method for delivering customized virtual networks, segmented into logical divisions and according to the requirements of the end users or industry verticals in terms of performance and quality of service. That subdivision is a product of multitude of conditions for connectivity to specific 5G Public Land Mobile Networks (PLMN). 5G defines three major use-cases of connectivity: Ultra Reliable Low-Latency Communication (URLLC), enhanced Mobile Broadband (eMBB) and Machine-to-Machine communications (M2M), also referred to as MIoT (Massive IoT) [26]. The 5G Infrastructure Public Private Partnership Project (5GPPP) has proposed network slicing architecture comprising of four layers, such as infrastructure layer, orchestration layer, business function layer and network function layer (see Fig. 4) [29].

A rather complex set of structures and methods, network slicing enriches service continuity through advanced roaming across networks. A slicing controller administers a virtual network segment that runs on physical infrastructure (cloud), with traffic that traverses multiple local or national PLMN networks. Another way is to allow the host network to create an optimized virtual network that reproduces the one presented by a roaming device's home network [30, 31]. While service function chaining is an excellent paradigm and can deliver great Quality of Experience for the end users, there are numerous security aspects to ponder, mainly when international traffic roaming considered.

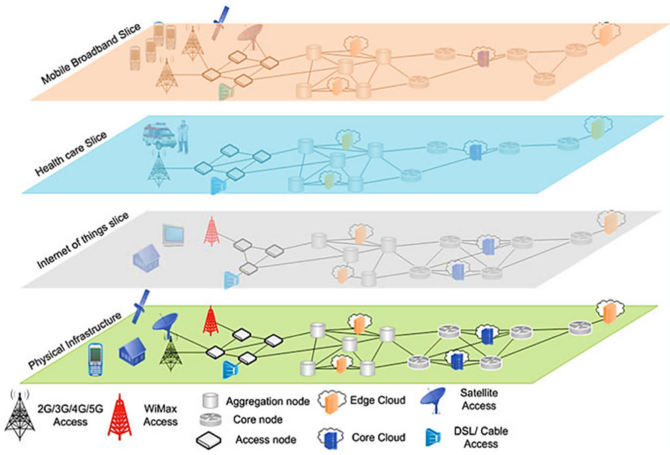

Fig. 4. A 4-layer network slicing architecture. Each slice represents an industry vertical or service chain. Network slicing begins from radio resource scheduling and up to application layer control (courtesy of 5GPPP) [29]

2.6 Isolation of Network Slices

Network slicing can be studied as a 4-phase process, or explicitly:

- Preparation,
- Commissioning,
- Operation and
- Decommissioning.

Considerable amount of focus on network slicing can be attributed to the management and orchestration layer in 5G, which tightly integrates within SDN controllers [26]. However, many security aspects are still deficient and there is no clear indication of isolation of network slices beyond the said policy enforcement and network segregation on lower layers. The major efforts on securing a 5G network is done on the core-network side, where each virtualized network function is secured with corresponding cryptographic procedures and keys (i.e., gNB Access Stratum keys vs. 5GC Non-Access Stratum keys). This continues with the introduction of similar practices to 4G for utilization of cryptographic algorithms in the user-plane and control-plane traffic, as well as the NAS signaling and RRC signaling separately. These security principles are exceptionally important during state transitions and mobility of User Equipment (UE) [30].

Security Threats in 5G and IoT

Various applications of 5G have different requirements in terms of performance, quality of service and security. An example of related work is the healthcare and ensuring a safe ecosystem for providers to reach the patients in a secure manner. Furthermore, availability of this network slice is of paramount importance because a smart healthcare infrastructure shall provide emergency services uninterruptedly [2]. Meanwhile,

the patients need protection of their information, as well as the doctor-patient confidentiality ensured at high levels [14]. The immense amounts of data that shall flow through the adjacent 5G slices is expected to increase by orders of magnitude compared to the 4G networks [13]. 3GPP defines a model for lawful interception of traffic, provided that an adversary is detected, and the details delivered to the LEMF (Law Enforcement Monitoring Facility). However, this is a proactive approach and cannot prevent the adversary from finalizing the attack [32].

Network Slicing as a Service (NSaaS)
Network slicing can be delivered as a service. This way, the Communication Service Customers (CSCs) can manage the slice themselves and decide on parameters via a management interface exposed by the Communication Service Providers (CSPs). In turn, a CSC can play the role of CSP and offer their own services (e.g., communication services) on top of the network slice obtained from the CSP (Fig. 5). For example, a network slice customer can also play the role of Network Operator (NOP) and could build their own network containing the slice(s) obtained from the CSP as a "building block". In this model, both CSP offering NSaaS and CSC consuming NSaaS have the knowledge of the existence of network slices [26].

Network Slicing as NOP Internals
In the "network slices as NOP internals" model, network slices are not part of the NOP service offered and hence are not visible to customers. However, the NOP, to provide support to communication services, may decide to deploy network slices, e.g., for internal network optimization purposes. This model allows CSC to use the network as the end user or optionally allows CSC to monitor the service status (as an assurance of the SLA associated with the internally offered network slice) [26].

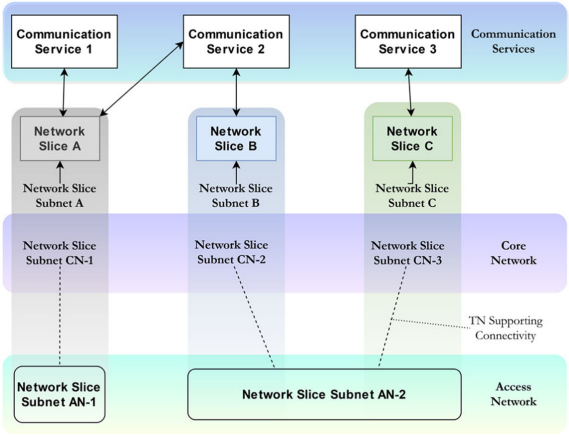

Fig. 5. A variety of communication services provided by multiple network slices. Each slice can be separated at the transport layer and its subnets restricted communication, unless required otherwise [26]

3 Methodology and Implementation

To experiment with enhanced VPN isolation of network slices beyond the hard isolation and using the hardware-level segmentation and virtual network functions, we designed a testbed that is comprised of a communication between the 4G/5G radio frontend and the core network. The core functions are provisioned in the OpenStack cloud and Edge hosting a portion of the vRAN (see Fig. 6).

An enhanced VPN+ framework is utilized to establish an encrypted communication between the Centralized Units in the vRAN and the vEPC/5GC core networks in the transport backhaul network. This communication is based on fiber networking on Layer-1, offering a 10 Gbps end-to-end communication bandwidth. For provisioning and maintaining persistent deployment, as well as minimize experimental error, we rely on the immutable infrastructure concept that is delivered by container virtualization and automation tools such as Ansible and Kubernetes. These tools offer seamless automation of the SDN controllers (O-RAN), which serve as network slicing function controllers for orchestrating the three slices represented in Fig. 6 [27].

Within the OpenStack cloud, service layers are defined for provisioning the corresponding vNFs of each slice, allowing traffic to be routed through the Neutron Open vSwitch DPDK networking module [28]. Kubernetes orchestrates the core network infrastructure and ensures immutability and stability in cases when the entire infrastructure needs to be automatically re-deployed due to escalating problems. As described previously, we establish a tunnel between the two endpoints in the cloud, which are the Core Network (5GC) and the Centralized Unit (Baseband Unit). For securing the tunnel, AES-256 encryption is used and its impact on the performance measured. The tunnel should be able to accommodate the virtual functions instantiated by the SDN controller. The Docker containers can communicate with the Neutron service in OpenStack using the Kuryr plugin. To allow this, we set the proper ID of the user and VM instance running the 4G and 5G Core Networks. The container performs authentication through the Kuryr plugin via the OpenStack's Keystone service for handling the authentication procedures of users accessing the core networks in the cloud (CSPs).

3.1 Implementation Stage

Core Network

Conclusively, an enhanced VPN+ deployment is manufactured between the two SR-IOV endpoints in the Docker containers, allowing for encrypted communication without a MPLS-BGP encapsulation. This will provide a clear understanding on the impact of CPU-accelerated encryption using the AES-256 algorithm, and its influence on the performance of the backhaul 4G/5G transport network. As SR-IOV can achieve a hardware-level isolation between endpoints using VLAN segmentation and mapping virtual functions (see Fig. 7), this may prove to be insufficient in a multitenant environment, because additional containers and services can then access the 5G core, which should be isolated. One method for maintaining isolation is by policy enforcement, guiding traffic to the 5GC core from only sources that should access it (i.e., a Centralized Unit or multiple Centralized Units). For operators who desire an additional layer of isolation, despite the underlying policy, a VPN instances are established between the SR-IOV endpoints.

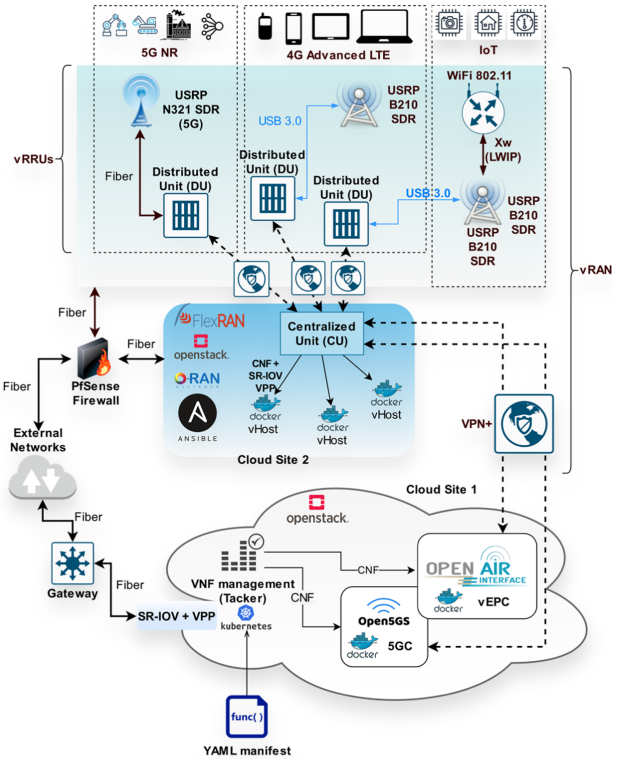

Fig. 6. 4G and 5G hybrid infrastructure at the Secure 5G4IoT Lab within the Oslo Metropolitan University. Each network slice in this case is controlled by a single CU and distinct DUs. In this case, one slice per generation of network (4G and 5G are regarded as different slices)

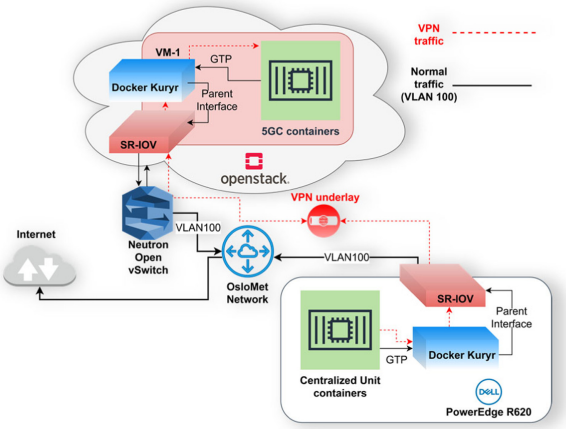

Fig. 7. VLAN segmentation using SR-IOV and VPN instance in the transport network between the Centralized Unit containers and the 5G Core Network in the cloud

3.2 Evaluation

The evaluation stage is comprised of two phases and an initial assumption that an adversary is attempting to demultiplex the transport network stream between the 5G core network containers and the Centralized Unit containers. The attacker hijacks an insecure Docker container running in the same namespace and attempts a Man in the Middle attack, capturing the entire communication and decoupling the control plane Non-Access Stratum (NAS) signaling as well as Packet Data Convergence Protocol (PDCP) packets to obtain information from the UE.

The second stage of the evaluation is the establishment of a VPN+ transport network between the 5GC and the Centralized Unit. In this situation, the adversary shall not be able to decapsulate the traffic due to the inability to decipher an AES-256 encrypted tunnel. This will indicate that in case of virtualization vulnerability exploitation, an adversary will encounter a rather challenging obstacle that will prevent personal information of healthcare patients to be exposed.

4 Results

The total number of captured packets in both scenarios is 1000. By utilizing logistic regression, we measure the classifiers of the attack vectors for attempting a reconnaissance activity on the 5G transport network and capture PDCP information from devices. One such example is the 802.15.4 LR-WPAN IoT device (see Fig. 8), where the traffic can be obtained and the frames from the packet read successfully. Based on the success of the decapsulation outcome, we can predict the difference between the attempts in cases of plain communication, compared to the one that is transmitted through the VPN+ and where the TLS handshake is detected but the content of the communication cannot be viewed without decrypting the traffic with TLS certificates and the private key (sample Wireshark capture in Fig. 9).

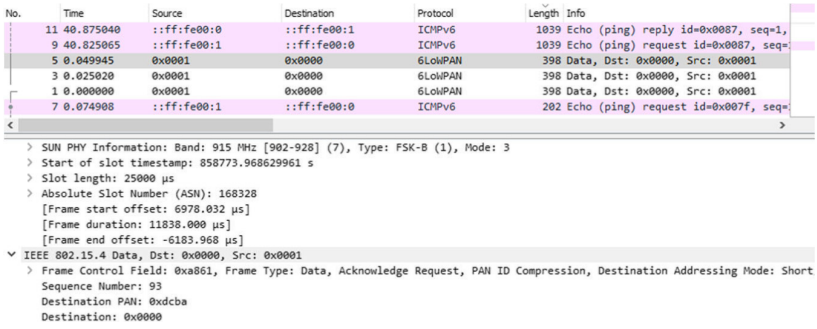

Fig. 8. In case without any encryption, the attacker can target vulnerable devices such as IoT that work on less secure protocols such as 802.15.4 LR-WPAN

The classifiers are defined via a sigmoid function that maps between actions, which allow the attacker to read the communication, compared to actions in which the attacker

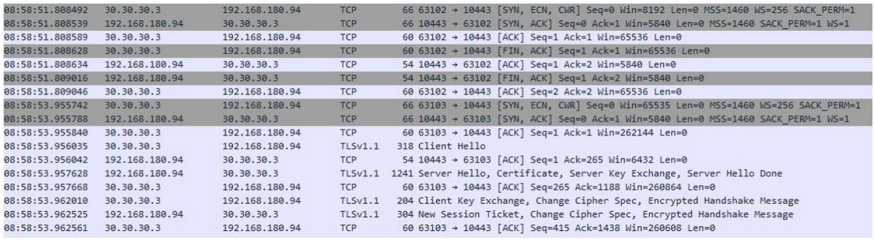

Fig. 9. With the VPN instantiated at the transport network, the attacker can only view the TLS handshake between the cloud core network and the CU

cannot read the communication considering the sample size of 1000 packets. The outcome variable is binary (true or false) and the predictive values are the number of protocols that are encapsulated within PDCP that can be compromised during an attack. The sigmoid function will serve as activation function for the logistic regression and is defined as:

$$f(x) = \frac{1}{1 + e^{-x}} \tag{1}$$

We define a cross-entropy cost function due to the lack of positive second derivative for square error and avoid local optima:

$$J(\theta) = -\frac{1}{m} \sum_{i=1}^{m} [y^{(i)} \cdot \log(h_\theta\left(x^{(i)}\right) + (1 - y^{(i)}) \cdot \log(1 - h_\theta(x^{(i)}))] \tag{2}$$

Where: m is the number of examples, $x^{(i)}$ is the feature vector for the i^{th} example, $y^{(i)}$ is the value for the i^{th} example and θ is the parameters vector.

The results are evident according to the tests that the attacker has a probability of 0.98452 to read the communication from the 1000 packet sample size, including decapsulating the PDCP headers (which is 98% of the entire communication) when there is no VPN tunneling, compared to −0.99442 probability in the other case (Fig. 10 and Fig. 11). The relative error deviation in the logistic regression model is ~0.02 and this can be improved by optimizing the θ gradient descent in the cross-entropy cost function.

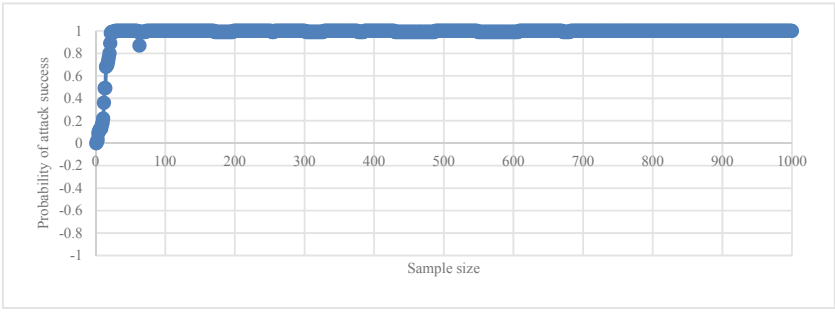

Fig. 10. Logistic regression analysis on the likelihood an attacker will obtain information from the end devices connected in to the 5G core without VPN+ tunneling

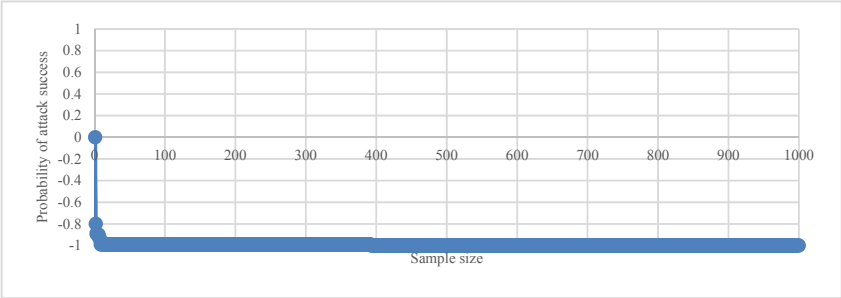

Fig. 11. Logistic regression analysis on the probability an attacker will obtain information from the transport network that is tunneled, and AES-256 encryption enabled

5 Discussion

The logistic regression analysis in this research demonstrates feasibility of an attacker to achieve Man in the Middle attack on a transport network in 5G, compared to when an enhanced VPN+ tunneling is initialized. This use-case however does not consider additional factors that can prove beneficial for the attacker, or supplementary security mechanisms that can influence end-to-end security.

The utilization of enhanced VPN approach for strengthening the isolation of network slices is not sufficient to protect against DDoS/Flooding attacks. This is because the latter requires more stringent mechanism for traffic steering incorporated within the SDN controller, which needs to react based on an input from a threat intelligence system for prevention of flooding attacks. One method to allow for more granular control is the introduction of SR-MPLS (Segment Routing) for IPv6 to enforce dynamic policy shifts in case of flooding and DDoS cyber-attacks.

6 Conclusion

Conclusively to the experimentation, we have demonstrated the successful implementation of an enhanced VPN+ transport network between the Centralized Unit of a 5G C-RAN and the Core Network in the TN. Despite the lack of performance evaluation of the approach, the combination of hardware offloading, isolation using distinct PFs (Physical Functions) and VFs (Virtual Functions) as well as policy enforcement, provides substantial security level that most enterprises deploying 5G will consider. Nevertheless, in some instances where the expense of network performance is not an issue, VPNs may prove a viable possibility to harden the isolation between 5G network slices (i.e., critical infrastructure). For IoT slices that do not require high bandwidth and low latency, the enhanced VPN can introduce great security benefits.

Acknowledgement. This paper is a result of the H2020 Concordia project (https://www.concordia-h2020.eu) which has received funding from the EU H2020 programme under grant agreement No 830927. The CONCORDIA consortium includes 23 partners from industry and other organizations such as Telenor, Telefonica, Telecom Italia, Ericsson, Siemens, Airbus, etc. and 23 partners from academia such as CODE, university of Twente, OsloMet, etc.

References

1. OpenStack Foundation: Over 60 Global Organizations Join in Establishing 'Open Infrastructure Foundation' to Build the Next Decade of Infrastructure for AI, 5G, Edge. https://www.openstack.org/news/view/463/over-60-global-organizations-join-in-establishing-open-infrastructure-foundation-to-build-the-next-decade-of-infrastructure-for-ai-5g-edge. Accessed 22 Dec 2020
2. Feng, B., et al.: Secure 5G network slicing for elderly care. In: Awan, I., Younas, M., Ünal, P., Aleksy, M. (eds.) MobiWIS 2019. LNCS, vol. 11673, pp. 202–213. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-27192-3_16
3. Ahmad, I., Kumar, T., et al.: Overview of 5G security challenges and solutions. IEEE Commun. Stand. Mag. **2**(1), 36–43 (2018). https://doi.org/10.1109/MCOMSTD.2018.1700063
4. MITRE project: Common Vulnerabilities and Exposures (2021). https://cve.mitre.org/
5. IETF TEAS Working Group: A framework for enhanced virtual private networks (VPN+) service (2020). https://tools.ietf.org/html/draft-ietf-teas-enhanced-vpn-06
6. Narayana Samy, G., Ahmad, R., Ismail, Z.: Security threats categories in healthcare information systems. Health Inf. J. **16**, 201–209 (2010). https://doi.org/10.1177/1460458210377468
7. McDermott, D.S., Kamerer, J.L., Birk, A.T.: Electronic health records - a literature review of cyber threats and security measures. Int. J. Cyber Res. Educ. (IJCRE) **1**, 42–49 (2019). https://doi.org/10.4018/IJCRE.2019070104
8. Latif, S., Qadir, J., Farooq, S., Imran, M.: How 5G wireless (and concomitant technologies) will revolutionize healthcare?. Future Internet **9**(4), 93 (2017). https://doi.org/10.3390/fi9040093
9. ETSI TS.123.501 v15.8.0 technical specification: 5G; System Architecture for the 5G System (5GS) (3GPP TS 23.501 version 15.8.0 Release 15) (2020). https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/15.08.00_60/ts_123501v150800p.pdf
10. OpenStack cloud software: Official documentation. https://www.openstack.org/. Accessed 30 Mar 2021
11. Docker container technology: Official documentation. https://www.docker.com/. Accessed 30 Mar 2021
12. Kubernetes container orchestration platform: Official documentation. https://kubernetes.io/. Accessed 30 Mar 2021
13. Barakabitze, A.A., Ahmad, A., Mijumbi, R., Hines, A.: 5G network slicing using SDN and NFV: a survey of taxonomy, architectures and future challenges. Comput. Netw. **167**, 106984 (2020). https://doi.org/10.1016/j.comnet.2019.106984. ISSN 1389-1286
14. Dzogovic, B., Do, T.V., Santos, B., Jacot, N., Feng, B., Thuan, D.V.: Secure healthcare: 5G-enabled network slicing for elderly care. In: 2020 International Conference on Computer and Communication Systems (ICCCS), Shanghai, China, pp. 864–868 (2020). https://doi.org/10.1109/ICCCS49078.2020.9118583
15. 3GPP Specification TR 38.801: Study on new radio access technology: Radio access architecture and interfaces (2018). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3056
16. Dzogovic, B., Thuan, D.V., Santos, B., Do, T.V., Feng, B., Jacot, N.: Thunderbolt-3 backbone for augmented 5G network slicing in cloud-radio access networks. In: 2019 IEEE 2nd 5G World Forum (5GWF), Dresden, Germany, pp. 415–420 (2019). https://doi.org/10.1109/5GWF.2019.8911710
17. OpenAirInterface5G: OpenAirInterface Software Alliance. https://openairinterface.org/. Accessed 02 Feb 2021

18. Open5GS: Open-source project of 5GC and EPC Release-16. https://open5gs.org/. Accessed 02 Feb 2021
19. OpenStack project Tacker: VNF Forwarding Graphs. https://docs.openstack.org/tacker/latest/user/vnffg_usage_guide.html. Accessed 02 Feb 2021
20. OpenStack project Tacker: ESTI NFV-SOL, Experimenting CNF with Kubernetes VIM. https://docs.openstack.org/tacker/latest/user/index.html. Accessed 02 Feb 2021
21. RedHat OpenShift: About Single Root I/O Virtualization (SR-IOV) hardware networks. https://docs.openshift.com/container-platform/4.4/networking/hardware_networks/about-sriov.html. Accessed 02 Feb 2021
22. OpenStack SR-IOV: OpenStack Neutron SR-IOV functionality. https://docs.openstack.org/neutron/pike/admin/config-sriov.html. Accessed 02 Feb 2021
23. Juniper Networks: LTE Security for Mobile Service Provider Networks (White Paper) (2015). https://www.juniper.net/us/en/local/pdf/whitepapers/2000536-en.pdf
24. Liyanage, M., Gurtov, A.: Secured VPN models for LTE backhaul networks. In: 2012 IEEE Vehicular Technology Conference (VTC Fall), Quebec, Canada, pp. 1–5 (2012). https://doi.org/10.1109/VTCFall.2012.6399037
25. Farrel, A.: What is ACTN framework. Metro-Haul Project. https://metro-haul.eu/2018/08/30/what-is-actn/. Accessed 08 Feb 2021
26. 3GPP specification TS 28.530: management and orchestration; concepts, use cases and requirements, version 16.4.0 (2020). https://www.etsi.org/deliver/etsi_ts/128500_128599/128530/16.04.00_60/ts_128530v160400p.pdf
27. Open-RAN: Alliance for Open Radio Access Networks. https://www.o-ran.org/. Accessed 30 Mar 2021
28. Data Plane Development Kit: Official documentation. https://www.dpdk.org/. Accessed 30 Mar 2021
29. 5G Infrastructure Public Private Partnership (5GPPP): View on 5G Architecture, version 3.0. URL: https://5g-ppp.eu/wp-content/uploads/2019/07/5G-PPP-5G-Architecture-White-Paper_v3.0_PublicConsultation.pdf (2019).
30. 3GPP specification TS 38.300: Technical specification group radio access network; NR; NR and NG-RAN overall description; stage-2, Release 16. Version 16.4.0 (2020). https://www.etsi.org/deliver/etsi_ts/138300_138399/138300/16.04.00_60/ts_138300v160400p.pdf
31. GSMA: An Introduction to Network Slicing, white paper (2017). https://www.gsma.com/futurenetworks/wp-content/uploads/2017/11/GSMA-An-Introduction-to-Network-Slicing.pdf
32. 3GPP specification TS 33.126: Lawful Interception Requirements (Release 16), version 16.3.0 (2021). https://www.etsi.org/deliver/etsi_ts/133100_133199/133126/16.03.00_60/ts_133126v160300p.pdf