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], Thanh Van Do[4,1]

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

Abstract. Alongside of supporting the human world, 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 multitude of sites, it has come to realization that the traditional security approaches incorporated in the 4th generation networks (LTE) may not suffice to protect 5G users and industries from adversaries that develop more advanced attack vectors. This is mostly due to the vulnerabilities brought by softwareization[1] 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 a progressive approach to enhance the isolation of network slices by employing the Enhanced VPN+ technology. Furthermore, we describe a method for tackling DDoS and flooding attacks on the communication between the 4G/5G core networks and the Cloud-Radio Access Network, as well as the radio frontend.

Keywords: 5G, enhanced VPN+, network slicing, IoT security

[1] Softwareization of networks, clouds, and internet of things <https://onlinelibrary.wiley.com/doi/pdf/10.1002/nem.1967

This is a post-peer-review, pre-copyedit version of a conference proceeding published in GOODTECHS 2021: Smart Objects and Technologies for Social Good, 7th EAI International Conference, Proceedings, which is also part of the Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering book series (volume 401). The final authenticated version is available online at DOI: https://doi.org/10.1007/978-3-030-91421-9_10

1 Introduction

Many startups, organizations and lower-tier operators will rely on open infrastructures and the open-source model to provide 5G services for various customers, including industries and proponents of the same [1]. However, there are various limitations to adhere to in this open approach, including cybersecurity-related ramifications and risks, which make the 5G network slicing not sufficiently secure for the digital elderly care solution proposed at the secure 5G4IoT lab [2]. 5G is known to inherit most of the security practices from the 4G LTE, but as the network and infrastructure become softwareized and deployed in shared environments (clouds) to support the additional industry verticals (like smart infrastructure, smart homes, Internet of Things, automated transportation etc.), the very same traits may be insufficient to provide adequate security for mission-critical applications and even the average user [3]. To handle these issues that emerge because of isolation insufficiency between tenants in the provider's infrastructure, 3GPP introduces the concept of network slicing, which aims towards segregation of network resources into logical segments to provide diverse Quality of Service and Quality of Experience for the end users or industry verticals. Most SDN/NFV vulnerabilities can easily transfer into the 5G ecosystem 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 in order to avoid some of these inherent vulnerabilities. Some of those involve:

- policy-based networking,
- traffic engineering and 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 ample isolation between network slices in the backhaul of an NFV-enabled cloud. To deliver network slicing, at this point there is no clear consensus about the methodology and which approach is the best since 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 absolute open-source methodology to deliver security augmentation of the 5G infrastructure.

To retain the confidentiality of information between a healthcare provider and patients, there must be a secure information transfer amongst the endpoints. Various healthcare management systems rely on the assumption that the providers should ensure the safety and reliability of patient information. However, it has been shown that in majority of cases that incorporate threats to healthcare systems like the THIS (Total Hospital Information System) is attributed to human error [6]. Despite efforts of

governments to establish safeguarding standards and regulation about EHRs (electronic health records) information, still the very same are vastly targeted by cyber-criminals due to flaws in personal and organizational management [6]. One of the prime areas that shall reap the benefits of 5G is exactly the healthcare. Amalgamating together the IoT ecosystem, big data and machine learning / AI, 5G will expand the functionality of the healthcare sector by orders of magnitude. 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). According to that, the aforementioned human error probability will increase, allowing for additional cyber threats to emerge and put at risk the stated private data [8].

This paper begins with an introduction to the background topics and technologies. Consequently, we proceed with elucidating details about the concept of network slicing and isolation of the same. To finalize, the methodology of implementation is described alongside with evaluation that is comprised of performance assessment and demonstrating the network slices isolation. As a conclusion, we discuss the lessons learned and provide details about future possibilities for researching this specific area.

2 Background and Related Work

2.1 5G Reference Architecture

The general architecture of the 4G and 5G networks established at the Oslo Metropolitan University are following the 3GPP, ETSI and ITU descriptions, designated in the adjacent technical specification TS 23.501 (v15.8.0) [9]. As described in Figure 1, the functions of the 4G and 5G Core Networks reside in the OpenStack cloud [10] and the corresponding Virtual Network Functions (vNFs) are provisioned within containerized environment using the Docker containerization technology [11]. Container runtimes allow for lightweight immutable infrastructure and when paired with orchestrators such as Kubernetes, also resilience, self-healing and automation [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.

Initially, these define basic networking in a mesh structure, which is a simple and efficient approach but also a security liability. Therein the requirement for more rigorous isolation attitude and securing the communication between the Core Networks and the vRAN segments that are provisioned in containers [13]. As indicated in

Figure **1**, one of the key architectural principles that 5G follows is the Cloud-Radio Access Network paradigm, where the User-Plane (UP) is separated from the Control-Plane (CP) within different functions, i.e., UPF (User Plane Function) and a C-function group that contains the AMF (Access and Mobility Function), SMF, NEF, NRF, UDM, AUSF, PCF, AF etc. The Next-Generation 5G Radio Access Network is connecting to 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].

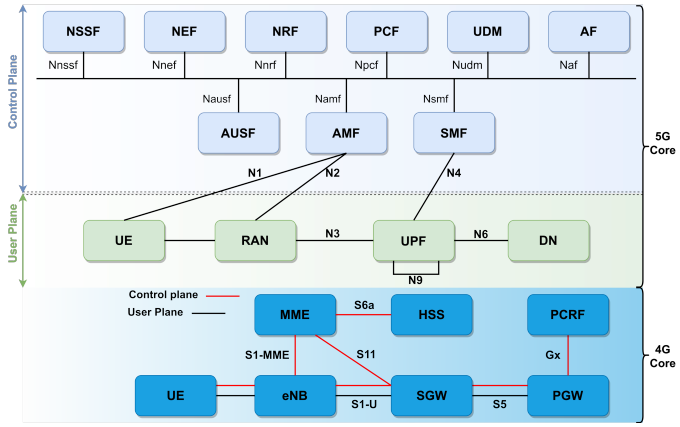

Figure 1. 4G and 5G Core Networks architecture [14]

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

To realize a 4G LTE vEPC, we utilize the OpenAirInterface core network and RRU [16], while maintaining a CU/DU split on option 7 according to 3GPP [17]. The 5G next generation RAN and core functions are deployed using the Open5GS core network [18].

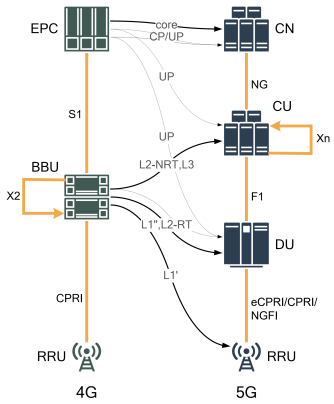

Figure 2. 4G and 5G functional splits for the transport network

2.2 Container Virtualization

The reason why containers are the virtualization choice is because of their light-weighted approach to seamless deployment of various software. Therefore, the software-defined networks and complete virtual network functions of the OpenAirInterface are provisioned within container environments, which is extremely suitable for Multi-

Access Edge and Fog computing models (MEC). The cloud needs to support a NFV enabled environment, which is 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 definition using YAML language. The absolute advantage of this approach is the possibility to perform service function chaining (SFC), where via pluggable infrastructure it is possible to integrate the SFC with the OpenDaylight SDN controller. 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].

Although in early stages, the Container Networking Functions are delivered through Kubernetes by using the Tacker module in OpenStack. This will allow for automation and orchestration of virtual network functions and is not the main focus of this current work [20]. One key technology 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 returns as a divider of physical network interfaces into diverse functions that can map multiple virtual network 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 module. 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 and enabled in the BIOS of the host) [22].

One caveat that can transpire as a result of running containers in an open infrastructure model is the security. Containers suffer of inherent lack of visibility when security is put into question. Most underlying vulnerabilities that translate also into containers, tend to be 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.

2.3 Enhanced VPN (VPN+) as part of the SDN controller

The 4G LTE architecture is based on flat all-IP backhaul network, which transports traffic of different types such as the ones from Evolved-NodeBs (eNBs), Service Gateways (SGWs), Mobility Management Entities (MME) and cross-handover traffic on the X2-U and X2-C interfaces between the eNB base stations. Furthermore, in LTE the flat IP architecture distributes Radio Network Controller (RNC) functions with eNBs, MME, S-GW and are directly connected to the core network [23]. This leads to challenges to provide a secure traffic in the mobile backhaul networks [24].

With the enhanced VPN feature of isolation, the hard isolation has one advantage by having a complete separation of underlying network so the traffic of particular network slices can use the distinct network resources [25]. To rectify 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 customer provides the input of their requirements (see Figure 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.

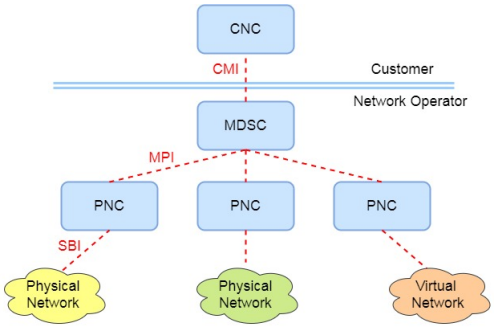

Figure 3. ACTN architecture components [25]

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 tunnel based on MPLS or VxLAN VPN. Nevertheless, since we are focused on hard isolation the vertical industry can choose their private tunnel between the two endpoints, which allows them for a complete protection of their data without concerns regarding the interference of other slices' traffic shall consume their resources or bandwidth. In case if a vertical industry desires an instance of a slice, they can differentiate the slice with a concept of differentiator with introducing an additional parameter of MTNC sub-differentiator i.e., MTNC ID 1.1 (where this case represents another instance of slice MTNC 1).

2.4 Network Slicing

Network slicing (or *netslicing*) is defined as a method for delivering customized virtual networks, segmented into logical portions and according to the requirements of the end users or industry verticals in terms of performance and quality of service. That subdivision is a result to multitude of conditions for connectivity to specific 5G PLMN networks. 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 by Public Private Partnership Project (5GPPP) has proposed network slicing architecture consisting of four layers, such as infrastructure layer, orchestration layer, business function layer and network function layer (see Figure 4) [29].

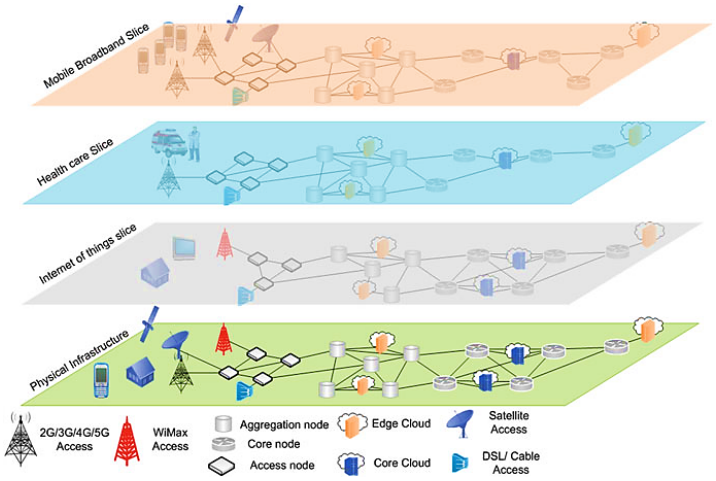

Figure 4. A 4-layer network slicing architecture (courtesy of 5GPPP) [29]

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, especially when international traffic roaming is taken into consideration.

Isolation of Network Slices

Network slicing can be considered as a 4-phase process, namely:

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

Much of the work regarding network slicing can be attributed to the management and orchestration layer in 5G, which tightly integrates with a given SDN controller [26]. However, many security aspects are still lacking and there is no clear indication of isolation of network slices beyond the said policy enforcement and network segregation on Layer-2. 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 proceeds with the introduction of similar practices like in 4G for utilization of encryption algorithms for the user-plane and control-plane traffic, the NAS

signaling and RRC signaling separately and the AMF function. These security principles are exceptionally important during state transitions and mobility [30].

Security threats in 5G and IoT
Different applications of 5G have different requirements in terms of performance, quality of service and security. An example of related work is the healthcare vertical and ensuring a safe ecosystem for healthcare providers to reach the patients in a secure manner. Furthermore, availability of this network slice is of the utmost importance because a smart healthcare infrastructure shall provide emergency services at any given time [2]. The patients need to have their sensitive personal data protected, as well as the doctor-patient confidentiality ensured at high levels [32]. 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 [33]. 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 hand cannot prevent the adversary from finalizing the attack [34].

Network Slicing as a Service (NSaaS)
Network slicing can be delivered in the model of a service itself. This way, the CSCs can manage the slice themselves and decide on parameters via a management interface exposed by the CSPs. In turn, these 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. For example, a network slice customer can also play the role of NOP and could build their own network containing the network slice 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].

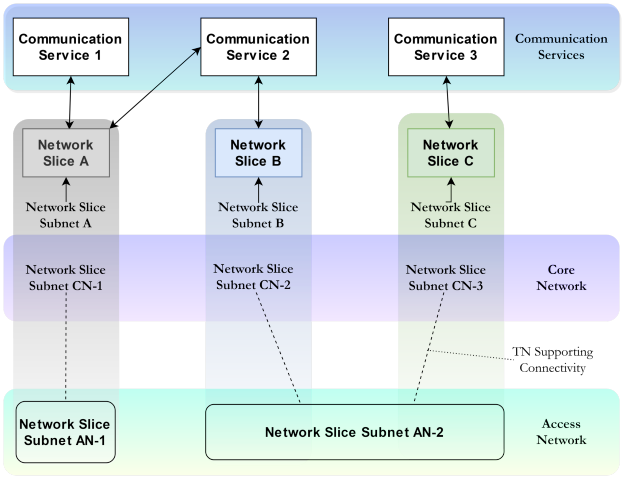

Figure 5. A variety of communication services provided by multiple network slices [26]

Network Slicing as NOP internals
In the "network slices as NOP internals" model, network slices are not part of the NOP service offering and hence are not visible to its 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 (assurance of the SLA associated with the internally offered network slice) [26].

3 Methodology and Implementation

To experiment with enhanced VPN isolation of network slices beyond the hard isolation using the hardware-level segmentation of network functions, as well as virtual Network Functions, we designed a testbed that is comprised of a common communication between the 4G/5G radio frontend and the core network in the private OpenStack cloud (see Figure 6).

An enhanced VPN+ framework is employed to establish a tunneled communication between the Centralized Units in the vRAN and the vEPC / 5GC core networks in the cloud. 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 (Open-RAN), which serve as network slicing function controllers for orchestrating the three slices represented in Figure 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 is used as an orchestrator for running YAML manifests of the core infrastructure and ensure immutability in cases the entire infrastructure needs to be 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 correspond to 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 Core Network. The container performs authentication through the Kuryr plugin via the OpenStack's Keystone service for handling the authentication procedures in the cloud.

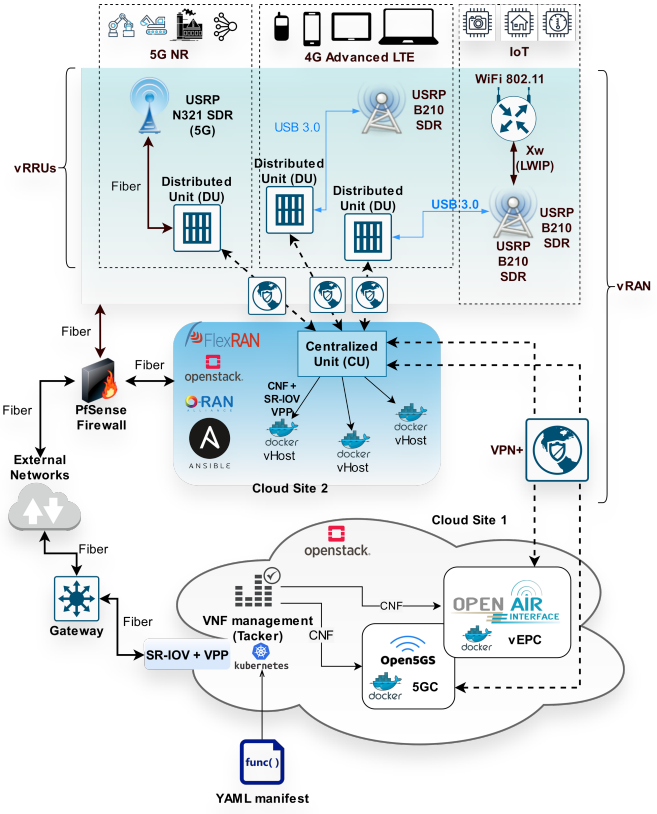

Figure 6. 4G and 5G hybrid infrastructure at the Secure 5G4IoT Lab within the Oslo Metropolitan University

3.1 Implementation stage

Core Network

Conclusively, an enhanced VPN+ deployment is crafted 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 of the impact of CPU-based encryption using the AES-256 algorithm on the performance of the underlying transport network fabrics. As SR-IOV can achieve a hardware-level isolation between endpoints using VLAN segmentation (see Figure 7), this may prove to be insufficient in a multitenant environment, as 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.

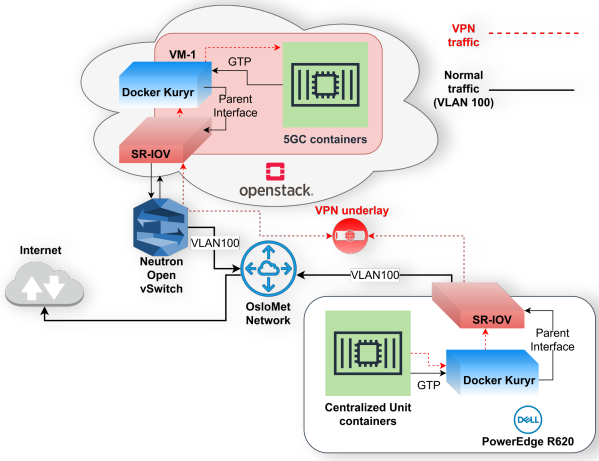

Figure 7. VLAN segmentation using SR-IOV and VPN instance in the transport network between the Centralized Unit containers and the 5G Core Network in the cloud

3.1 Evaluation

The evaluation stage is comprised of two parts. 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 adversary presumably 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 NAS signaling as well as PDCP packets to obtain information from the User Equipment.

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 information from devices that transmit through the PDCP protocol. One such example is the 802.15.4 LR-WPAN IoT device (see Figure 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+, where the TLS handshake is detected but the content of the communication cannot be viewed without decrypting the traffic using the TLS certificates and the private key (sample Wireshark capture in Figure 9).

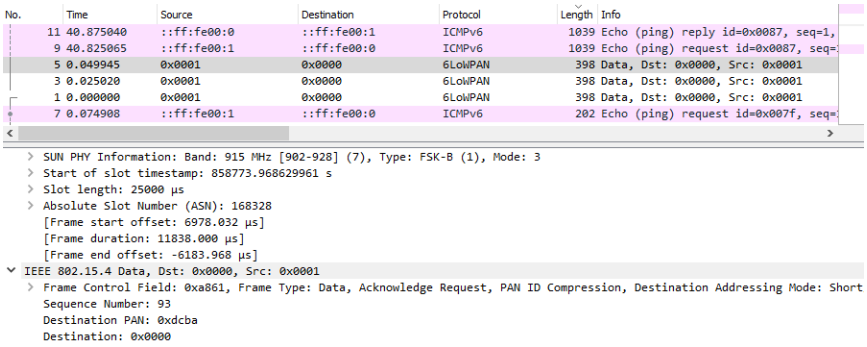

Figure 8. In case without any encryption, the attacker can target vulnerable devices such as IoT that work on less secure protocols such as 802.15.4 LR-WPAN

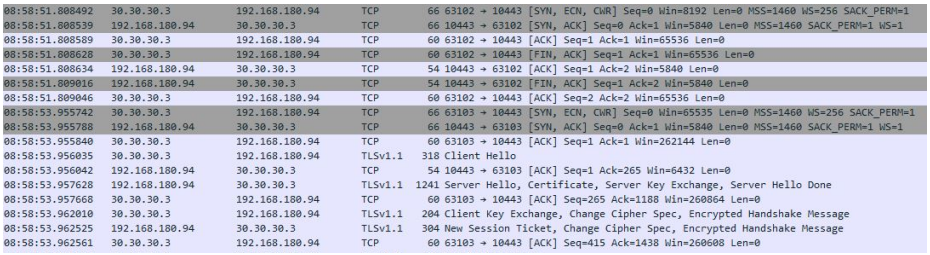

Figure 9. With the VPN instantiated at the transport network, the attacker can only view the TLS handshake between the cloud core network and the CU

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 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:

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

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 tunneling using enhanced VPN+, compared to -0.99442 probability to not be able to in the other case (Figure 10 and Figure 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.

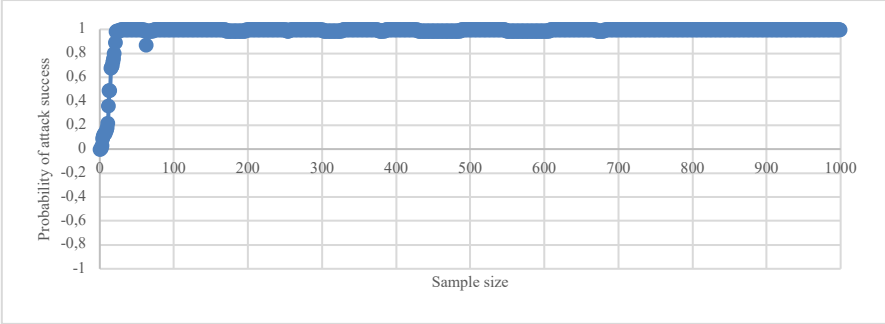

Figure 10. Logistic regression analysis on the likelihood an attacker will obtain information from the end devices connected in to the 5G core without VPN+ tunneling

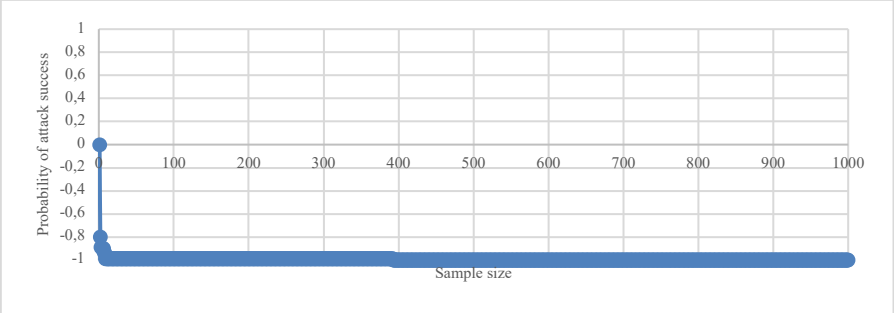

Figure 11. Logistic regression analysis on the probability an attacker will obtain information from the transport network that is tunneled, and AES-256 encryption enabled

5 Discussion

The logistic regression analysis in this research shows a plain 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 take into account additional factors that can prove beneficial for the attacker, or supplementary security mechanisms that can have effect on the end-to-end security. The security term

is very wide and thereby it would be substantially extensive to include every possible use-case scenario.

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 in order to enforce specially crafted policies in case of flooding and DDoS cyber-attacks, which is a future research candidate for the current use-case.

6 Conclusion

Conclusively to the experimentation, we have demonstrated the successful implementation of a 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 such as critical infrastructure, where the expense of network performance is not an issue, VPNs may prove a viable possibility to harden the isolation between 5G network slices. For IoT slices that do not require high bandwidth and low latency, the enhanced VPN can provide a great solution out of the box.

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. URL: 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, last accessed 2020/12/22.
2. Boning Feng, Thanh Van Do, Niels Jacot, Bernardo Santos, Bruno Dzogovic, Ewout Brandsma, Do Van Thuan, “Secure 5G Network Slicing for Elderly Care”, International Conference on Mobile Web and Intelligent Information Systems MobiWIS. Lecture Notes in Computer Science, vol 11673. Doi: https://doi.org/10.1007/978-3-030-27192-3_16. Springer, Cham (2019).
3. Ijaz Ahmad, Tanesh Kumar, et al.: Overview of 5G Security Challenges and Solutions. IEEE Communications Standards Magazine, Vol. 2, Issue 1, pp. 36-43. Doi: 10.1109/MCOMSTD.2018.1700063 (2018).
4. MITRE project: Common Vulnerabilities and Exposures. URL: https://cve.mitre.org/ (2021).
5. IETF TEAS Working Group: A framework for enhanced virtual private networks (VPN+) service. URL: https://tools.ietf.org/html/draft-ietf-teas-enhanced-vpn-06 (2020).

6. Narayana Samy, G., Ahmad, R., & Ismail, Z.: Security threats categories in healthcare information systems. Health Informatics Journal, pp. 201-209. Doi: 10.1177/1460458210377468 (2010).
7. Donna S. McDermott, Jessica L. Kamerer and Andrew T. Birk: Electronic Health Records - A Literature Review of Cyber Threats and Security Measures. International Journal of Cyber Research and Education (IJCRE). Doi: 10.4018/IJCRE.2019070104 (2019).
8. Latif S, Qadir J, Farooq S, Imran MA.: How 5G Wireless (and Concomitant Technologies) Will Revolutionize Healthcare*?* Future Internet*,* Vol. 9, Issue 4. Doi: 10.3390/fi9040093 (2019).
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). URL: https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/15.08.00_60/ts_123501v150800p.pdf (2020).
10. OpenStack cloud software: Official documentation. URL: https://www.openstack.org/ last accessed 2021/03/30.
11. Docker container technology: Official documentation. URL: https://www.docker.com/ last accessed 2021/03/30.
12. Kubernetes container orchestration platform: Official documentation. URL: https://kubernetes.io/ last accessed 2021/03/30.
13. Alcardo Alex Barakabitze, Arslan Ahmad, Rashid Mijumbi, Andrew Hines: 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges, Computer Networks, Vol. 167, 106984, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2019.106984 (2020).
14. Bruno Dzogovic, Thanh Van Do, Bernardo Santos, Niels Jacot, Boning Feng, Do Van Thuan: Secure Healthcare: 5G-Enabled Network Slicing for Elderly Care*.* 2020 International Conference on Computer and Communication Systems (ICCCS). Doi: http://10.1109/ICCCS49078.2020.9118583 (2020).
15. 3GPP Specification TR 38.801: Study on new radio access technology: Radio access architecture and interfaces*.* URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3056 (2018).
16. Bruno Dzogovic, Do Van Thuan, Bernardo Santos, Thanh Van Do, Boning Feng and Niels Jacot: Thunderbolt-3 Backbone for Augmented 5G Network Slicing in Cloud-Radio Access Networks, 2019 IEEE 2nd 5G World Forum (5GWF). Doi: 10.1109/5GWF.2019.8911710, pp. 415-420. Dresden, Germany (2019).
17. OpenAirInterface5G: OpenAirInterface Software Alliance. URL: https://openairinterface.org/, last accessed 2021/02/02.
18. Open5GS: Open-source project of 5GC and EPC Release-16. URL: https://open5gs.org/, last accessed 2021/02/02.
19. OpenStack project Tacker: VNF Forwarding Graphs. URL: https://docs.openstack.org/tacker/latest/user/vnffg_usage_guide.html, last accessed 2021/02/02.
20. OpenStack project Tacker: ESTI NFV-SOL, Experimenting CNF with Kubernetes VIM, URL: https://docs.openstack.org/tacker/latest/user/index.html, last accessed 2021/02/02.
21. RedHat OpenShift: About Single Root I/O Virtualization (SR-IOV) hardware networks. URL: https://docs.openshift.com/container-platform/4.4/networking/hardware_networks/about-sriov.html, last accessed 2021/02/02.
22. OpenStack SR-IOV: OpenStack Neutron SR-IOV functionality. URL: https://docs.openstack.org/neutron/pike/admin/config-sriov.html, last accessed 2021/02/02.
23. Juniper Networks: LTE Security for Mobile Service Provider Networks (White Paper). URL: https://www.juniper.net/us/en/local/pdf/whitepapers/2000536-en.pdf (2015).

24. Madhusanka Liyanage & Andrei Gurtov: Secured VPN Models for LTE Backhaul Networks. 2012 IEEE Vehicular Technology Conference (VTC Fall), pp. 1-5. Doi: https://10.1109/VTCFall.2012.6399037. Quebec, Canada (2012).
25. Adrian Farrel: What is ACTN framework. Metro-Haul Project. URL: https://metro-haul.eu/2018/08/30/what-is-actn/, last accessed 2021/02/08.
26. 3GPP specification TS 28.530: Management and Orchestration; Concepts, use cases and requirements, version 16.4.0. URL: https://www.etsi.org/deliver/etsi_ts/128500_128599/128530/16.04.00_60/ts_128530v160400p.pdf (2020).
27. Open-RAN: Alliance for Open Radio Access Networks. URL: https://www.o-ran.org/ last accessed 2021/03/30.
28. Data Plane Development Kit: Official documentation. URL: https://www.dpdk.org/ last accessed 2021/03/30.
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. URL: https://www.etsi.org/deliver/etsi_ts/138300_138399/138300/16.04.00_60/ts_138300v160400p.pdf (2020).
31. GSMA: An Introduction to Network Slicing, white paper. URL: https://www.gsma.com/futurenetworks/wp-content/uploads/2017/11/GSMA-An-Introduction-to-Network-Slicing.pdf (2017).
32. Bruno Dzogovic, Thanh Van Do, Bernardo Santos, Niels Jacot, Boning Feng and Do Van Thuan: Secure Healthcare: 5G-enabled Network Slicing for Elderly Care. 2020 5th International Conference on Computer and Communication Systems (ICCCS), pp. 864-868. Doi: https://10.1109/ICCCS49078.2020.9118583, Shanghai, China (2020).
33. Alcardo AlexBarakabitze, Arslan Ahmad, Rashid Mijumbi and Andrew Hines: 5G network slicing using SDN and NFV - A survey of taxonomy, architectures and future challenges. Computer Networks, Vol. 167, 106984, ISSN 1389-1286. Doi: 10.1016/j.comnet.2019.106984 (2020).
34. 3GPP specification TS 33.126: Lawful Interception Requirements (Release 16), version 16.3.0. URL: https://www.etsi.org/deliver/etsi_ts/133100_133199/133126/16.03.00_60/ts_133126v160300p.pdf (2021).

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.