An Integration of Slicing, NFV and SDN for Mobility Management in Corporate Environments

Flavio Meneses* | Rui Silva | David Santos | Daniel Corujo | Rui L. Aguiar

Instituto de Telecomunicações and Universidade de Aveiro, Aveiro, Portugal
*Correspondence: flaviomeneses@av.it.pt

Abstract

On-line access to information while on the move has conferred businesses with the capability to be constantly accessible and in operation, independently of geographical area or timezone. There are situations, however, that demand technical solutions for specific scenarios, such as controlled access to corporate-based content. Virtual Private Networks (VPNs) allow controlled remote access to content, supporting scenarios such as teleworking. Nonetheless, such mechanisms are not commonly associated with the highly mobile users of today, which can traverse different types of access networks, while still keeping access to content restricted to corporate network usage. In addition, as VPN mechanisms are disassociated from mobility procedures, service disruption can happen or specific mechanisms and clients can be required in end-user's equipment.

This paper proposes a framework that leverages Network Slicing, enabled by Software Defined Networking and Network Function Virtualisation, to provide seamless and isolated access to corporate-based content, while moving through heterogeneous networks. This solution allows Mobile Network Operators to dynamically instantiate isolated network slices for corporate users, and handover them between 3GPP and non-3GPP networks while users move away from the corporate network. In this way, they are able to keep access to corporate-based content in a transparent way, while maintaining access requirements for the service being used. The framework was implemented and validated over an experimental testbed composed by mobile and Wi-Fi accesses, with results presenting improvements in terms of overhead signaling and data redirection without downtime nor stream reconnection.

Keywords: *Network Slicing, SDN, NFV, Mobility, Remote working*

I. Introduction

Since its beginning, the Internet has been evolving along with its usage traffic patterns. Initially designed for information sharing (e.g., world wide web and e-mail), nowadays the Internet is a prime communication tool used not only to share multimedia (i.e., videos and photos) for social interactions (e.g., social networks), but also for an increasingly wide range of other information exchange scenarios [1]. In parallel, the 3GPP architecture followed such traffic evolutions, evolving its communications core from a voice-based system (i.e., 2G) towards a data-based system, namely the mobile packet core (MPC) found in 4G [2]. User

equipment (UE) not only followed, but actually helped pushing such evolution. Nowadays, current smartphones are equipped with multiple wireless interfaces (e.g., Wi-Fi and LTE), enabling the use of their multimedia features (e.g., live stream video) while on the move. Nevertheless, despite efforts from 3GPP and other standardisation bodies, mechanisms allowing full-integration between 3GPP and non-3GPP networks are still not widespread.

Current mobile architectures are being challenged to face the hugely increasing number of connected devices [1], with the next generation of mobile networks (i.e., 5G) already under study and close to deployment. In this context, 5G does not focus solely in enhanced data rates. Instead, operators are seeking for a sustainable and dynamic network with heterogeneous interoperability. This led network operators to look into technologies such as Software Defined Networking (SDN), Network Function Virtualisation (NFV) and, more recently, Network Slicing. Despite being independent, SDN and NFV complement each other, and their joint integration provides networks with a greater degree of flexibility. NFV decouples the software capabilities from the specifics of the hardware, moving them into data-centers as virtualised network functions (VNF), and SDN dynamically (re)configures the network paths that support the communication among VNFs [2]. Recently, Network Slicing has been gaining a lot of attention by promising the partition of the network in "slices" adapted (in terms of security, isolation and traffic requirements) to different use cases and verticals [3]. Here, VNFs can be seen as the building blocks that can be dynamically instantiated and chained together to form an adapted slice, to satisfy the individual needs of specific scenarios while sharing existing resources. Thus, SDN and NFV have been in the center of the slicing evolution, promising to provide enhanced mechanisms for optimized network operations.

In the meantime, architectural evolutions allied with globalization triggered new ways for collaboration, in an era where remote or teleworking is gaining followers [4]. Currently, remote working is supported by virtual private networks (VPN), which allow enterprises to provide access to internal services (via, e.g., enterprise portals) to collaborators from remote places (e.g., home). This paper proposes a framework that enables network operators to create network slices for better serving remote working, by leveraging the enabling tools for 5G (i.e., SDN, NFV and Network Slicing) over the currently existing architecture. In the proposed concept, the operator provides a slice to the tenant enterprise (or corporation) which can be accessed from heterogeneous networks. The mobile packet core (i.e., the evolved packet core (EPC) in 4G networks) is sliced in specific virtual EPCs (vEPC) instantiated with the VNFs established in the Service Level Agreements (SLAs). Moreover, the framework enables the operator to re-instantiate the slice as the user leaves the enterprise and crosses different networks, maintaining corporate based communications. To do so, the solution not only provides traffic offloading from the licensed LTE to the unlicensed Wi-Fi spectrum (leveraging Wi-Fi APs existing everywhere), but also allows the network service operator to dynamically instantiate a non-3GPP slice that is used to carry and maintain corporate based communications, avoiding the need of VPN services on end-users' equipment. To further enhance this solution, the UEs of enterprise users are virtualised (i.e., vUE) in the enterprise slice, allowing the management and monitoring of enterprise's UEs (e.g., type of traffic allowed, QoS and security level) to be enhanced with SDN-based flow mobility mechanisms.

An experimental assessment was conducted using an open-source EPC deployed in a cloud environment, coupled with a radio cell using SDN and several Wi-Fi APs. Results shown improvements in terms of overhead signalling and data redirection without downtime nor stream reconnection.

The remainder of the article is structured as follows: Section II presents the related work in SDN, NFV and network slicing when applied to mobile and wireless networks. Section III de-

scribes the system architecture, presenting the network entities and their control signalling. A proof-of-concept implementation is presented in Section IV, followed by its assessment in Section V. The article concludes in Section VI.

II. Background and Related Work

This section presents the related work for future network architectures. In this line, after providing an overview of current remote access to corporate networks, SDN and NFV applied to mobile networks and wireless environments are presented, followed by an analysis of existing Network Slicing initiatives. Finally, the related work in MPC softwarization and virtualisation is presented.

i. Remote access to corporate networks

VPNs are the traditional approach for an end-to-end secure connection between two endpoints [5]. A VPN extends a private network across a public network allowing users to access services (or hosts) of the private network. When used in corporate scenarios, the VPN allows out of office secure access by the collaborators to internal services of the corporation. However, most VPN solutions are designed for wired networks with high-speed, highly reliable connections, which hinder its use in mobile scenarios, since mobile devices are susceptible to intermittent connection loss while switching from one network to another [5]. As such, it is important to look for mobile VPN solutions that can provide an experience that does not require the user to reset and reconfigure the VPN session upon switching between networks [5].

In this line, solutions such as virtual private LAN services (VPLS) [6] allow multipoint-to-multipoint communication over the Internet Protocol (IP). Here, the local area network (LAN) at each site is extended to the edge of the provider network, but disregarding the wireless hop and the possibility of private services use over public places.

ii. Software Defined Networking (SDN)

SDN aims to decouple the control decisions from the data plane (or user plane). Thus, as network equipments become simple forwarding devices, control decisions are logically centralised in a high-level entity (i.e., the SDN controller). In this context, the SDN controller exposes Northbound (NB) APIs to communicate with SDN applications for control and managment of the forwarding devices via Southbound (SB) APIs. Despite encompassing several protocols, the SB API OpenFlow [7] represents the de-facto open-source SDN implementation. Also, Open Network Foundation (ONF) is making efforts to continuously standardize and update the OpenFlow protocol [8].

SDN and OpenFlow provide a greater degree of flexibility and simplicity to the network by enabling its dynamic reconfiguration. As such, OpenFlow has been used not only in data-centres [9][10], but its contribution potential has also started to be assessed in wireless environments [11]. SDN has been also used in mobility management for future networks [12][13], presenting benefits such as the independence of underlying technologies and per-flow mobility support, while streamlining the mobility management operation. However, such approaches do not consider network slicing, thus disregarding handover enhancements in inter-slice mobility scenarios.

The use of SDN and OpenFlow simplified the managment of the network, with works such as [14][15][16] using OpenFlow to create a multi-domain and multipoint-to-multipoint VPN on-demand service (more specifically, VPLS). However, the VPNs stop at the edge of the network.

iii. Network Function Virtualisation (NFV)

NFV implies the use of cloud-like infrastructures and cloud-like life cycle management. Despite that SDN and NFV can be implemented independently of each other, they are comple-

mentary. In this context, while NFV decouples network functions from specific hardware and moves them to data-centres, SDN flexibly (re)configures the network.

Proposals such as Odin [17] and CloudMac [18] apply NFV principles to wireless environments by migrating AP management services to the data-centres. On one hand, Odin [17] builds on a light virtual AP to virtualise the association state, facilitating mobility management by allowing the infrastructure to handoff clients without triggering the reassociation mechanism. On the other hand, CloudMac [18] decoupled medium access control (MAC) services from the AP hardware, such as authentication and association, allowing them to be performed in data-centres. More recently, a virtual entity was instantiated for visualization of the UE elements involved in the network mobility process[19]. This entity, named as a virtual mobile node (vMN), is not only capable of operating as an anchor for the physical UE (or mobile node (MN)) traffic, but also maps the UE in the network, supporting the network controller (i.e., an SDN controller) in enhanced mobility management decisions.

iv. Network Slicing

Network Slicing (or slicing hereafter) aims at partitioning the network to better fit specific services purposes, while maintaining isolation. Slicing initiatives can be mainly divided into three groups [3]: (i) spectrum-level slicing; (ii) infrastructure-level slicing; and (iii) network-level slicing. Also, slicing implies the allocation of the required resources for independent services[3]. However, in wireless environments, the slice isolation of the wireless access medium adds particular challenges, especially when ensuring quality of service (QoS) and SLAs. In this context, not only SDN and NFV are seen as key enablers for resource slicing in wireless networks, but also for wireless network virtualisation (WNV) [3]. Towards a slicing per service, user or application, WNV aims not only the sharing of the infrastructure, but also the radio spectrum.

In the literature, different solutions are proposed depending on the wireless medium access technology. In LTE, solutions such as [20, 21] propose an architecture for LTE base stations (i.e., eNodeB (eNB)) virtualisation with the objective of enabling infrastructure sharing among several operators. Also, [22] proposes an algorithm to dynamically allocate resource blocks depending on the slice demand. Considering the IEEE 802.11 (i.e., Wi-Fi) technology, in [23] the authors state that the use of virtual APs with different service set identifiers (SSIDs) and security configurations allow a single AP to be shared among operators when deployed in popular locations (e.g., airports and hotels). Solutions such as [23] and [24], propose to configure EDCA parameters to improve throughput of the slices.

v. Mobile Packet Core (MPC)

Currently the most recent MPC is the evolved packet core (EPC), which is used in LTE systems [25]. LTE systems assume a flat architecture over a IP network dedicated to support packet-switched connectivity. Figure 1a) illustrates the 3GPP architecture. The EPC includes five main functional entities: Mobility Management Entity (MME), Serving Gateway (SGW), Packet Data Gateway (PGW), Home Subscriber Server (HSS) and the Policy control and Chanrging Rules Function (PCRF) [2]. Another element also present in the EPC is the Access Network Discovery and Selection Function (ANDSF) [26], which is able to provide inter-3GPP connectivity opportunities information in regard to aspects such as geographical location, user profile, speed, amongst others, in combination with HotSpot 2.0 [27]. However, such information is typically pre-defined and static in nature, not contemplating dynamic changes in the network usage by devices and services, such as the ones perceived by flexible network slicing instantiation.

Despite being deployed worldwide, in addition to the above mentioned, EPC faces as well issues related with inflexibility [28, 29], complexity [30, 31], centralised user [31] and

control [32] planes and inefficient resource provisioning and allocation. This led to the use of SDN and NFV in mobile network where the EPC is virtualised in data-centers (i.e., the vEPC). Here, SDN allows greater flexibility in the flow distribution over the infrastructure, thus providing enhanced UE mobility management[2]. Also, with control and data planes decoupled from each other, VNFs can be flexibly deployed around the network, such as in the case where their placement is done closer to the edge, thus shortening network latency[2].

Architectures such as CellSDN [33] and SoftCell [34] introduced SDN to mobile networks for design and management simplification by centralizing the control plane. Also, MobileFlow [35] advocates that SDN improves flow-based forwarding in mobile networks. SoftAir [36] and SoftNet [37] progress from such architectures and, while the former presents indicators for a scalable, flexible and resilient network architecture, the latter proposes a decentralized mobile architecture, with a distributed data forwarding. Focused on virtualising the Evolved Packet Core, SoftEPC [38] addresses the dynamic instantiation of network functions and services at appropriate locations in response to the actual traffic demand.

Figure 1b) presents the EPC where SDN/NFV are used to decouple the user from the control plane. In this context, the usage of OpenFlow (both as a replacement or integrated with) for mobile network mobility management and connectivity control, has been explored in the past. The authors in [39] have replaced the PGW with a SDN-managed box, with packet classification being handled in the edge, and the SDN controller taking care of the LTE signalling protocols needed. Specific to the handover mechanisms, in [40] the SDN controller is used to manage mobility procedures, by controlling eNBs as if they were SDN switches, supported by information collected from the UEs. This concept was extended in [41], with the controller actually managing the SGW and PGW, maintaining an overall perspective of the eNBs to where each UE is connected to, and allowing optimization scenarios. However, all these solutions focus on mobile network aspects, neglecting offloading capabilities with other access networks such as Wi-Fi, or the support of network slicing.

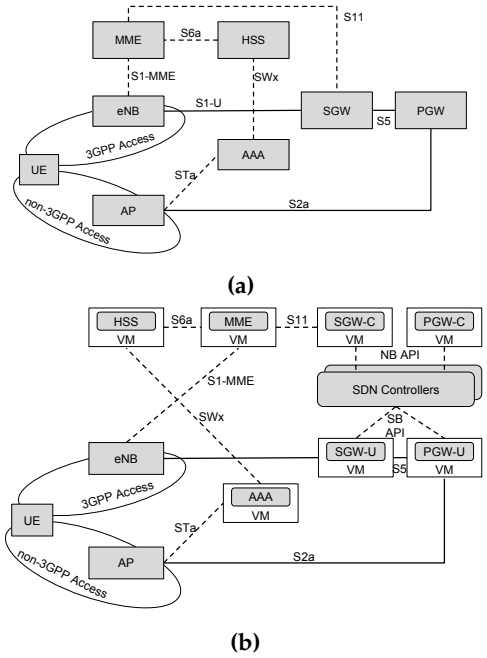

Figure 1: *3GPP and non-3GPP network integration in a: (a) current EPC architecture. (b) SDN/NFV EPC architecture.*

III. System Architecture

Our framework extends existing remote network access proposals, by dynamically instantiating dedicated slices for the corporate UEs, over the current network to which they are connected to, allowing physical resource sharing (i.e., the AP) among different corporations and/or operators in public places (e.g., shopping centre). We argue that such extension facilitates the access to a corporation's internal services by its remote collaborators, since the VPN configuration (through a VPN client) in the UE becomes unnecessary as it is transparent to the terminal. Also, overhead of over the air signalling is reduced, since VPN tunnels finish at the network edge (i.e., AP and

eNB). For this, we explore SDN, NFV and MPC virtualisation techniques, to manage the network in a SDN-based manner, allocating VPN tunnels between servers and PoAs, in support of enhanced corporate-based communications, but extend it by dynamically instantiating a new SSID, allowing 5G-enhanced access to a corporate network, via public networks.

Next, the motivational scenario is presented, followed by a description of the required mobile network architecture enhancements for its support. Finally, interactions among network entities and flow mobility procedures are discussed.

i. Motivational Scenario

This paper focuses on how network slicing enhances the remote access to private networks while on the move. Keeping this in mind, we propose a framework where the Mobile Network Operator (MNO) instantiates the necessary building blocks to support corporations with remote working communications. Such building blocks may include, for example, mobility management, slice mechanisms and corporation services (e.g., internal portals).

Figure 2 illustrates a simplified scenario, where the MNO provides a slice to the corporate, supporting inter-slice mobility, and with corporation services instantiated in the cloud. Here, the access to the corporation services are ensured via the "vCorp GW " and monitored by the vUEs (along with the "context updater"). The vUE is a virtual representation in the cloud, of the physical UE of the corporations' employees, and readily provides input to the network flow mobility management entities on behalf of its physical counterpart (i.e., the UE). Also, the vUE allows the corporation to dynamically manage the physical UE by setting the requirements for QoS and security level of each collaborator.

When the user leaves the corporate network's Wi-Fi, this movement is perceived by the MNO (i.e., indicated by link events sent by the UE), which triggers the creation of a dedicated slice for the UE over this new network. This slice receives the redirected UE's flows to allow a transparent access the corporate-based services. Whenever the UE changes to another network, the process is repeated, with a new slice being created therein, and the previous slice being released for resources optimization.

In this line, UEs of the corporation are able to remotely access corporation services both from the mobile (e.g., LTE) and the Wi-Fi networks without VPN configuration (through a VPN client). Also, allowing physical resource sharing (i.e., the AP) among different corporations and/or MNOs in public places, we extend such features and dynamically instantiate dedicated slices to be accessed by the specific corporation's collaborators.

Finally, we argue that such extension facilitates the access to a corporation's internal services by its remote collaborators, since the VPN configuration in the UE becomes unnecessary as it is transparent to the terminal. This also reduces the overhead of over the air signalling, since VPN tunnels finish at the network edge.

Next, the required mobile network enhancements for supporting such scenario are described.

ii. Mobile Network Architecture Enhancements

As stated above, the proposed framework aims to inter-operate with 3GPP and non-3GPP networks, by instantiating a 3GPP slice and (when appropriate) dynamically instantiate a non-3GPP (i.e., Wi-Fi) slice for traffic offloading from the licensed to the unlicensed spectrum, while ensuring the traffic requirements

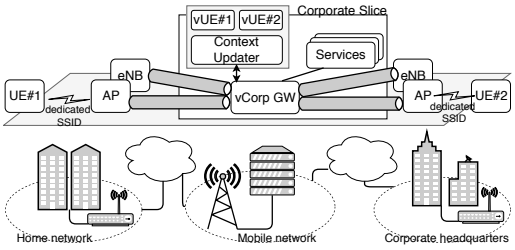

Figure 2: *Use case scenario.*

(in terms of security, isolation and QoS) for corporation's collaborators. For this, we propose the adoption of a SDN/NFV-based 3GPP architecture and the instantiation of new network entities: (i) Slice Creator; (ii) Slice Selector; (iii) Context Updater; and (iv) vUE. As such, Figure 3 presents our proposed mobile network architecture as an enhancement of the architecture presented in Figure 1b) of the related work. For the sake of compatibility, our proposal maintains to the highest possible extent existing interfaces used between 3GPP building blocks, while mapping any new introduced protocol to 3GPP signalling whenever possible.

In the 3GPP standards [25, 42], the interoperability between 3GPP and non-3GPP networks is ensured by the MME and PGW. The MME is responsible for the control of intra-3GPP and inter-3GPP handovers, where the SGW and the PGW are used as data traffic anchors for intra-3GPP and inter-3GPP handovers, respectively. Notwithstanding, with the introduction of new technologies into the network (i.e., slicing, SDN and NFV), we argue that new procedures should be studied, along with the instantiation of new network entities and functions. In fact, for 5G networks, the 3GPP is considering such enhancements, and new network functions are being established under standardisation [43]. In this line, we propose to use the vUE to manage the inter-3GPP mobility of its physical counterpart, alleviating the MME procedures. Note that the MME maintains its standard capabilities, only delegating inter-3GPP handovers to the vUE.

Although our work focuses on the existing EPC, if we followed the current 3GPP standardisation for 5G in [43] the UE's context updater could be integrated in the Access Management Function (AMF), allowing the network to follow the UE and update its context in the virtual instances. The building blocks of our proposal are described next, and depicted in Figure 3 (in blue).

- **Slice Creator:** The slice creator is in charge of dynamically instantiating non-3GPP slices. As such, it communicates with the context updater of each 3GPP slice. Since each slice is specific to each use case, the slice creator chooses the building blocks to be instantiated with the slice. In our proposal, we opted to instantiate the GW for user plane and the Context Updater and vUE for control plane. Note that for proof-of-concept deployment, in our framework we simplified the management and relationship among components. However, in a realistic deployment the slice creator integration in the NFV Management and Orchestration (MANO) system should be considered. In this line, mechanisms to support the communication between the slice creator and NFV orchestrator (NFVO) need to be developed. Alternatively, the slice creator can be integrated in the OSS/BSS and use the Os-Ma-nfvo interface, allowing the MNO to dynamic manage slices by requesting the instantiation of network services and VNFs [44].
- **Slice Selector:** The slice selector maps the UEs to their corresponding slices. For example, while a regular user has its UE connectivity attached to a default slice, corporates may have a dedicated vEPC with different network requirements per UE. Also, the corporate may have dedicated non-3GPP slices for its collaborators to improve the remote working experience.
- **Context Updater:** The context updater communicates with the vUEs, updating its information and requesting the instantiation of non-3GPP slices to the slice creator. Here, the context updater will enhance the capabilities of the SGW and the PGW of the 3GPP by creating and updating the vUEs of the corporation.
- **vUE:** The vUE assumes the MME responsibility of controlling inter-3GPP handovers, but with a finer flow control, since each vUE is responsible for its UEs flows. As such, the vUE maps the UE in the network, keeping the information regarded to the physical UE's wireless link and active flows, and helping the SDN controller in the control decision of the flows regarded

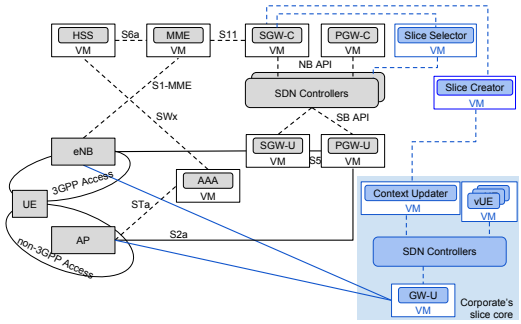

Figure 3: *Proposed mobile network architecture.*

to the UE with updated UE's connectivity context. Also, corporates may define different SLAs per group of users, where each vUE verifies and adapts the QoS of each flow to meet the requirements agreed in the SLAs.

- **GW-U:** The GW-U is the gateway of a specific core slice, thus it acts as an anchor for datapath of both intra- and inter-3GPP handovers, replacing the SGW-U and PGW-U. Control decisions are performed by the SDN controller and assisted by the vUE and context updater.

iii. Interaction and Procedures

Our proposal considers different procedures and network entities interaction, depending on the type of access technology used by the UE. Figure 3 depicts the entities involved in the procedures for the 3GPP and non-3GPP attachment, while Figure 4 illustrates the non-3GPP slice instantiation and inter-slice flow mobility procedures. For simplification, in Figure 4 only the involved network entities in the related procedures are presented. The above procedures are described as follows.

iii.1 3GPP attachment and 3GPP slice

When an UE attaches to the network via a 3GPP access the eNB requests credentials to the MME (via the S1-MME interface). The MME validates the IMSI of the UE with the HSS (via the S6a interface), and then replies to the UE. After that, the UE requests a L3 attachment, which is agreed between the MME and the SGW-C (via the S11 interface). Upon attachment completion of the UE, the SGW-C notifies the Slice Selector, which in turn sends the result to the SGW-C and the Context Updater of the correspondent slice. The SGW-C then creates a tunnel between the attached eNB and the GW-U of the respective core slice.

iii.2 non-3GPP attachment and non-3GPP slice instantiation

In Figure 4, when the UE is connected to LTE and detects a non-3GPP access of the operator in its surroundings (i.e., via a known SSID) with link quality above a pre-established threshold, the UE notifies the vUE (messages #2a/#2b) with the identification of the AP[1]. To notify its virtual counterpart, the UE sends an UDP message (#2a) towards the vCorp GW, which in turn redirects to the context updater as an OF *packet_in* message (#2b). The context updater is responsible for updating the vUE information. If this results in an offloading decision by the network, the vUE (along with the context updater) requests a non-3GPP slice (#3) to the Slice creator via an UDP message with the AP and slice identification (i.e., which corporation and/or level of security). Then a dedicated slice (via a unique SSID) for the user (or group of users, depending of the security and mobility policies) is instantiated in the AP (#4).

In Figure 3, when an UE attaches to a non-3GPP access (i.e., Wi-Fi) deployed by the network operator, the AP authenticates the UE in the AAA (interface STa), which in turn verifies the IMSI of the UE with the HSS (interface SWx). DHCP is then requested by the UE, and the SGW-C with slice selector connects (via tunnel) the AP with the respective slice GW. For this we explore wireless virtualisation to deploy multiple SSID with different wireless security encryptions on-demand.

[1]UE SSID detection: To enhance the UE with this capability an application was developed and implemented in the UE. This will be discussed in Section ii.4

iii.3 Inter-slice flow mobility

In our proposal, inter-slice mobility is processed as an inter-3GPP handover scenario. However, we move this responsibility from the MME to our proposed vUE. This allows a greater degree of granularity, since each vUE monitors the flows of its UE. Conversely, current MME implementations do not perform flow-based mobility, instead they offload all traffic, independently of the flow characteristic and the wireless link status of the UE.

In this context, for inter-slice flow mobility, we used the vUE to monitor the wireless link and active flows of its physical counterpart, in order to perform flow-based mobility adapted to each flow, while requesting for non-3GPP slices with the agreed QoS requirements with the tenant corporate. Regarding to intra-3GPP slice mobility, in our proposal the MME continues to be in charge of its management, according with the involved eNB and UE the transmission parameters.

Figure 4 exemplifies the procedures for flow handover between slices, where after a trigger that results in an offloading policy (e.g., UE connected to the Wi-Fi slice) the context updater updates the flow table of the GW (message #5) redirecting the data flow from the licensed LTE to the unlicensed Wi-Fi access network, via an OF *flow_modification* message. Here, the trigger was the UE attachment to the non-3GPP slice, which was notified to the context updater by the MME via a REST message. When the link strength of the Wi-Fi connection crosses a pre-established threshold, the UE reports this to its virtual counterpart (messages #7a/#7b), triggering the redirection from the Wi-Fi to the LTE (message #8), in order to seamlessly keep the data connection (message #9).

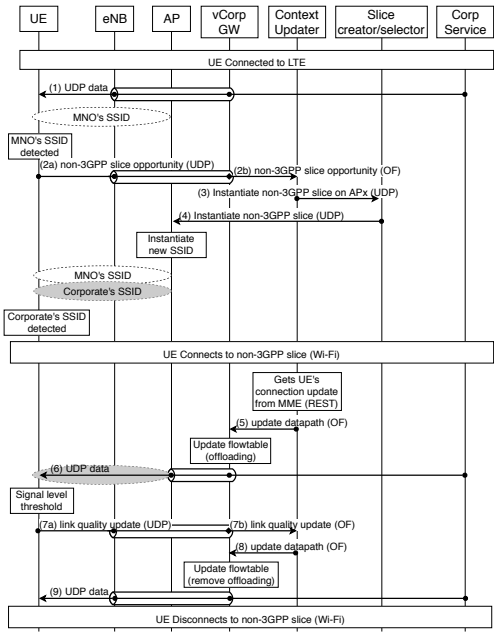

Figure 4: *Simplified signalling for non-3GPP slice instantiation.*

IV. Proof-of-Concept Implementation

This section presents a proof-of-concept implementation of our proposal. For this, we present application models of the proposed framework, followed by an use case description. Finally, implementation details are discussed.

i. Application models

The proposed framework aims to provide the extension of VPN in shared Wi-Fi networks, without requiring VPN clients or procedures to be installed in the UE. For this, the proposed framework instantiates a 3GPP slice for an enterprise and extends the VPN service by dynamically instantiating non-3GPP slices associated to it. As previously discussed, in our proposal, a VPN is defined as a mechanism which enables users to remotely access services from private networks. As such, the proposed framework can be implemented in different business models, depending on where the enterprise services are hosted, the level of virtualisation involved and the contracted services.

Additionally, depending on the network access type (i.e., 3GPP or non-3GPP) and network provider (i.e., MNO or Internet service provider (ISP)) different procedures are taken. When accessing via a 3GPP mobile network,

the user traffic is redirected to the respective 3GPP slice. Otherwise, when accessing via a non-3GPP Wi-Fi, it can be from an ISP or from a LTE and Wi-Fi integration solution (e.g., RAN-Controlled LTE-WLAN Interworking (RCLWI) [45]) of the MNO.

Notwithstanding, the deployment of such mechanisms imposes challenges not only related to management domains, and relationship established among different network components, but also the management of dynamically instantiated SSIDs in APs of different providers or the hosting of corporate cloud's services out of the domain of the MNO. In this way, in order to assess our framework, our work considered two key simplification aspects, described as follows. Firstly, the capability to allow multiple MNOs to dynamically instantiate radio slices is still under heavy research, and addresses not only core network aspects but also access network capabilities. In this way, in our proof-of-concept, we used SSIDs to slice the Wi-Fi and provide separated attachment points to users at the same access point. In a downside, such mechanism does not fully isolate the medium access, since it allows UDP upstream traffic to exceed its pre-established bandwidth. Nonetheless, besides allowing us to assess our proof of concept (as the scope of our paper is not on the radio access), proposals in the literature to enhance MAC parameters, at a cost of flexibility, where highlighted in section II. In this line, we developed an API to allow the MNO to dynamically instantiate SSIDs, however both the API and slicing mechanism (i.e., SSID) require enhancements to support multiple MNOs and fully isolate the medium access, respectively. Secondly, in our proof-of-concept both the Wi-Fi APs and the cloud's services hosting belong to the same MNO's domain. This considers that a single MNO has to have all the necessary infrastructure up to the user's end location, which is typically handled by different providers. Such realization would require further inter-operator and/or inter-domain interactions, which also fall out of scope of this work. Next, different models achieving this behaviour are presented.

Partially virtualised corporation Figure 5a presents an overview of this model where the enterprise's services are hosted in in-house servers. Thus, implying a VPN towards enterprise's perimeter. The MNO tunnels the traffic towards the enterprise's network edge, and extends the enterprise VPN up to the cloud by virtualising their UEs. When remotely accessing via Wi-Fi, the MNO requires management capabilities in the corresponding AP, in order to dynamically instantiate a non-3GPP slice there. Here, the AP may be shared among multiple MNOs or it can be a dedicated one deployed by the MNO. Either way, an application programming interface (API) is used to coordinate the slice instantiation request from allowed MNOs.

Fully virtualised corporation Represented in Figure 5b, this model virtualises the enterprise's services in the cloud. Thus, the enterprise's services are remotely accessible from the enterprise's perimeter as well as from the home networks. Here, the MNO and ISP of the enterprise are the same entity, facilitating the management of the deployed APs in the corporate's building, which are directly connected to the cloud. Otherwise, in the home networks, the users may have different ISPs, however management permissions should be given to the MNO to instantiate Wi-Fi slices on-demand, in order to instantiate the VPN service towards the enterprise's cloud services and end-users.

ii. Implementation details

Our solution is based on the previously presented fully-virtualized model. For implementation simplicity purposes only, our proof-of-concept exploits the fact that the MNO and ISP reside on the same entity and assumes a trustable network underlying the framework, with GRE tunnels being used without encryption. Nevertheless, our framework's architecture is designed to support secured tunneling protocols. In fact, Open vSwitch (OvS) supports IPsec tunneling and there are associated

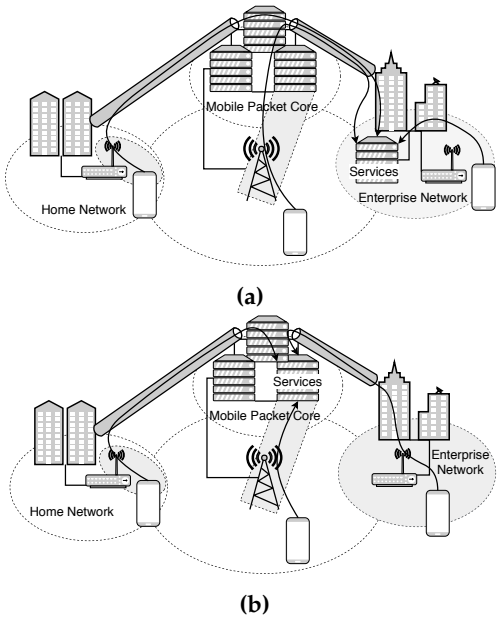

Figure 5: *Application models for a corporate network deployment in a: (a) Partially virtualised corporation. (b) Fully virtualised corporation.*

software patches in order to support GTP[2].

ii.1 3GPP network

The 3GPP network implemented for our proof-of-concept was based on the OpenAirInterface (OAI) [46] framework, which is compliant with the 3GPP standards. The eNB was implemented in a physical machine with the Intel(R) Core(TM) i7-7700K CPU and 32 GB of RAM, the USRP B210 software-defined radio (SDR) board, the LP0965 antenna and a LTE band 7 duplexer. Also, the eNB runs Ubuntu desktop 16.04 LTS OS with the 4.4.0-116-lowlatency kernel version. In addition, mobile core network functions (i.e., HSS/MME, AAA, DHCP, SPGW-C) were implemented in our in-house OpenStack data-center (Ocata) in virtual machines (VMs) with 1 core and 2 GB of RAM, running Ubuntu server 16.04 LTS OS. As discussed previously, control and data paths were decoupled, thus the SPGW-U was implemented in a VM with 2 cores and 4GB RAM, running Ubuntu server 16.04 LTS OS. In the SPGW-U the OvS (version 2.5.5) was used to allow the dynamic data path reconfiguration via OpenFlow flow-based rules, which was patched to enable GTP tunnelling. Finally, the Ryu SDN controller [47] was used for the SPGW-C, allowing the reconfiguration of the network datapath via SDN mechanisms (e.g., OpenFlow and OvSDB).

Regarding to the new proposed network entities, namely the slice creator and the slice selector, both were implemented as a Ryu SDN application. As such, both run along with the SDN controller and interacted with the remaining entities via UDP messages, and when applicable deploying OF messages through the SDN controller.

ii.2 non-3GPP access

In our implementation the non-3GPP access used was Wi-Fi, more specifically, the IEEE 802.11n at 5GHz. The AP was implemented using APU2c4 with wle600vx wireless modules. The Ubuntu 14.04 LTS OS was used with the hostapd v2.1 [48] software for AP capabilities. For the non-3GPP slice instantiation an application was developed, which reconfigures the Linux *hostapd* daemon creating a new SSID with the necessary characteristics (e.g., security, traffic shaping) and implements traffic shaping through Linux traffic control when requested by the network controller. Finally, the new SSID was configured in IEEE 802.11n at 5GHz with EAP-AKA authentication.

ii.3 Enterprise Slice

In our proposal the enterprise slice is defined as the slice of the network where the data traffic of the enterprise's users is managed. In this context, in the enterprise slice, the control and data plane were decoupled and while the vCorp-GW is a VM for data traffic redirection, the SDN controller with the Context Update and the vUE applications manage the user's traffic regarding security and QoS. Both the vCorp-GW and the SDN controller were implemented in a VM with 1 core, 2 GB of RAM and

[2]OvS pacth for GTP: https://patchwork.ozlabs.org/patch/579431/

running Ubuntu desktop 16.04 LTS OS. While the OvS was used in the GW, the Ryu was used as SDN controller.

Regarding to the context updater, it was implemented as an Ryu SDN application that manages the vCorp-GW traffic via OF messages and updates the UE's context in the cloud (i.e., the vUE). As such, it communicates with the remaining network entities via UDP or REST messages.

As presented before, the vUE is the virtual representation of the UE, which maps its physical counterpart in the network. The vUE can be seen as an internal information collection of the UE wireless events in the context updater. When the update of such collection results in an handover policy (e.g., link going down), the vUE (along with the context updater) reconfigures the datapath via OF messages.

Figure 6 presents an overview of the datapath for enterprise's authorised and non-authorised users. Since *UE#1* is an authorised enterprise user, its data traffic is redirected towards the vCorp-GW (i.e., in the 3GPP slice), both from 3GPP and non-3GPP access. Also, the *UE#1* is attached to the AP via a dedicated slice (i.e., unique SSID), allowing the physical resource sharing of the AP with the *UE#2*. The *UE#2* can (eventually) connect to both 3GPP and non-3GPP, but being an unauthorised user, its data traffic is redirected to the default 3GPP slice, with no access to the corporation services.

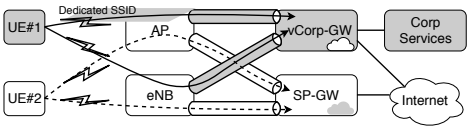

Figure 6: *Deployed datapath simplification, where UE#1 is a registered UE of the corporation and UE#2 is a regular user.*

ii.4 User Equipment (UE)

The UE was deployed using an APU2c4 with the Wi-Fi wle600vx and the LTE Huawei ME909s-120 wireless modules. For EAP-AKA authentication the *wpa_supplicant* [49] software was used. Additionally, an application was developed in order to inform the network of a non-3GPP slice instantiation opportunity. The application uses the *libnl* [50] for gathering Wi-Fi information and events (e.g., neighbour SSIDs and cells, link strength, Wi-Fi connection and disconnection, etc.). Such events are then informed to the network controller.

For requesting the non-3GPP slice the application scans the wireless environments in a periodicity of 9s (similarly to iOS and Android OS [51]). Also, to prevent a *break-before-make*, when connected to an Wi-Fi network, the application monitors the signal strength, alerting the network when a pre-established threshold is crossed.

V. Evaluation and Discussion

In this section we evaluate and discuss the proof-of-concept implementation in terms of handover performance, throughput achieved in a non-3GPP slice, and overhead in over-the-air data traffic. The experiments were run 50 times with the results being presented with a confidence interval of 95%. Next we discuss the overhead introduced by VPN clients (we used OpenVPN as example), and compare it with our framework, focusing on overhead introduced per packet.

i. Packet overhead

Figure 7 depicts the overhead per data packet introduced by our framework in wireless and wired connections, comparing it to use of IPSec instead of GRE and to the use of OpenVPN for remote access.

The use of a client such as OpenVPN in the UE improves communication security on the wireless medium, however increases the over-the-air overhead as a trade-off. For example, using OpenVPN in a TUN-style tunnel over UDP and default TLS options, about 69*bytes* of overhead are increased to each packet.

In our proposal the VPN tunnel stops at the AP and/or eNB, and uses a dedicated slice (i.e., a unique SSID when connected via Wi-

Fi), saving overhead over-the-air. Additionally, our proposal also reduces the overhead in the wired connection, since a GRE tunnel encapsulation increases 24*bytes*. Also, if we desire a security enhancement, IPSec can be used in tunnel mode with an overhead cost of 52*bytes*.

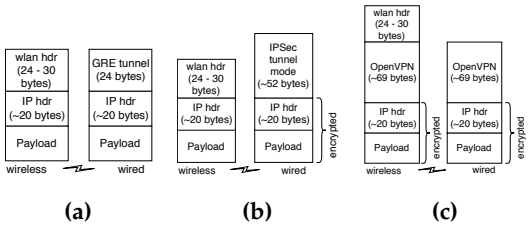

Figure 7: *Packet overhead when considering: (a) GRE tunnel (b) IPSec in tunnel mode. (b) OpenVPN.*

In this context, there is a trade-off between security degree and overhead introduced per packet: despite that the overhead might not seem much, when considering highly scaled networks, this additional overhead can affect network equipments' performance when dealing with multiple VPNs at high speed connections. Nevertheless, our framework ensures VPN's encryption up to the network edge, but it is flexibly enough to extend VPN services through wireless with different levels of security and overhead. In a scenario of residential Wi-Fi networks, where the encryption is usually ensured only by Wi-Fi protocols, our framework reduces the overhead over the air and consequently saves UE's energy, by dynamically instantiating a dedicated SSID accessible for registered corporate's UE (via EAP-AKA using the SIM card).

As final note, when considering shared wireless environments (e.g., home and shopping centre), our framework has the advantage of aggregating users per server avoiding multiple VPN connections to the server, reducing overhead.

ii. non-3GPP slice instantiation delay

In our framework the handover is performed in a make-before-break approach. As such, despite that the handover takes about 10*ms* (from LTE to Wi-Fi and vice-versa), the redirection procedure takes about 26*s* ($\pm$3*s*). As such, the redirection procedure can be divided as following: (1) suitable AP discovery; (2) slice instantiation; (3) UE's connection to the AP; and (4) flow redirection. Figure 8 shows the cumulative distribution function (CDF) of such procure (from 1 to 3).

The (1) suitable AP discovery is regarded to the UE's detection of the MNO's SSID in range and informing it to the network (i.e., to the vUE), which takes 9*s* ($\pm$2*s*). The (2) slice instantiation takes 10*s* and is the delay between the non-3GPP slice request and it being instantiated. Then (3) the UE takes about 7*s* ($\pm$1*s*) to detect and connect to the dynamically instantiated corporation SSID. Finally, (4) the data flow is redirected from the 3GPP to the non-3GPP slice.

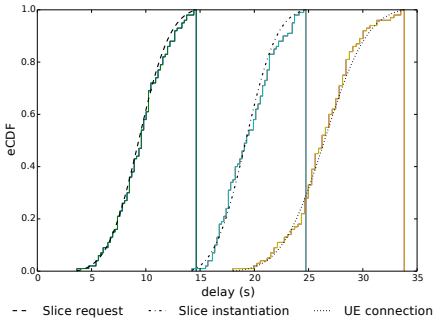

Figure 8: *Instantiation of a non-3GPP slice.*

In this line, while the instantiation of the non-3GPP slice takes 10*s*, the overall procedure takes about 26*s*. When compared to VPN clients (which takes about 5*s* to connect) our framework takes 5 times longer. However, our mechanisms is transparent to the user, as such not requiring his/her intervention. Contrarily, VPN clients requires the configuration and the input from the user, decreasing the QoS and experience of the user.

Finally, our framework can explore location service of current smartphones, and preemptively instantiate the non-3GPP slice, saving 20*s* of delay (i.e., slice request and slice instantiation).

iii. Handover performance

In order to assess our proof-of-concept in terms of handover performance (achieved throughput over time and downtime) we virtualised corporation services in the cloud and accessible through the vCorp-GW. Figure 9 illustrates an UDP stream handover mimicking a scenario with remote working while on the move. The iperf3 [52] application was used in order to generate UDP flows with a pre-established bandwidth, facilitating the visualisation of impact of proposed framework over the QoS. In our tests the UE acts as an UDP client and requests an enterprise service with a bandwidth of 50Mbps.

Initially, the user is in the corporation perimeter and is connected to the corporate services via Wi-Fi with an SSID associated to a specific type of user: guest, premium (e.g., CEOs and CTOs) or staff. On its way home the user is able to telework work via LTE (from 25*s* to 63*s*), and, upon arrival to home (at 63*s*), a dedicated SSID is dynamically instantiated in its home Wi-Fi. This avoids the necessity of a VPN client service in the UE, while saving signalling over-the-air.

As discussed above, the non-3GPP slice takes about 10*s* to be instantiated and the UE takes another 7*s* to detect and to attach the slice. For simplification, in the evaluated scenario, the network pre-emptively instantiated the non-3GPP slice in the user's home network, saving the instantiation delay in the offloading mechanism. For this, the network can exploit localization services of current smartphones or pre-schedule the slice instantiation. In this context, since the vUE works on behalf of the UE for network management decisions, the UE informs the vUE of neighbour cell and/or current location, allowing the network to pre-emptively take procedures to adapt (or instantiate) slices.

The evaluated scenario was compared with the throughput for a dual interface UE (Wi-Fi and LTE) where no handover mechanisms is applied. Here, the user is attached to a Wi-Fi and LTE networks simultaneously and is accessing the corporation services through VPN. As such, as the UE changes access network, the VPN requires a reconnection (for evaluation proposes we assumed 3*s*) to the server. In this line, when the UE disconnects from the Wi-Fi (at 25*s*) the VPN tries to reconnect through the LTE, negatively affecting the achieved throughput. Moreover, when the UE connects to a new Wi-Fi network (at 62*s*), another VPN reconnection is required in order to offload the traffic via Wi-Fi. Comparing to our framework, the VPN client scenario originates a throughput loss of 8% between VPN reconnections.

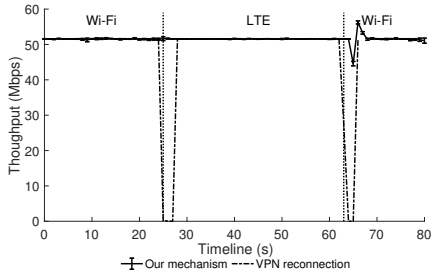

Figure 9: *Proposed framework.*

Finally, we argue that we should look for ways to offload the traffic to non-3GPP access (such as the Wi-Fi) while keeping or enhancing the QoS. This gains more value when considering places of social gathering, since BSs support a limited number of LTE connections due to the finite spectrum that can be used at one physical location, leading to degraded service quality for customers [53]. Also, studies, such as [54], show that Wi-Fi is typically more energy efficient than LTE, pointing out that offloading to Wi-Fi will usually reduce the UE energy consumption.

VI. Conclusion and Future work

This paper takes advantage of network slicing, NFV and SDN mechanisms in order to allow remote working in corporate scenarios. In this context, the proposed framework instantiates a core network slice for a corporation and dynamically re-instantiates it at the target network, as the user moves away from the corporation, whether it is in a 3GPP or non-3GPP

technology. This solution is further supported by creating a virtualised representation of the UE, the vUE, which not only operates as a data anchor, but also provides support for the mobility process. In this way, the configuration of a VPN client in the UE becomes unnecessary as it is transparent to the user. Here, a VPN service is defined as a mechanism that allows the remote access to private networks.

The proposed framework was experimentally evaluated in a physical testbed and results showcased gains in terms of signalling overhead and throughput. This packet overhead is reduced since the VPN tunnel stops at the edge (i.e., AP and/or eNB) and multiple user may share the VPN extension (i.e., dedicated SSID). Additionally, the proposed framework potentially is more energy efficient, since encryption processing does not involve the UE, contrary to current VPN solutions. Finally, more secured methods for SSID instantiation can be explored, such as the use of a hidden SSID, that is randomly generated upon non-3GPP slice request, and further informed to the UE.

Acknowledgments

This work is funded by FCT/MEC through national funds under the project PTDC/EEI-TEL/30685/2017 and by the Integrated Programme of SR&TD "SOCA" (Ref. CENTRO-01-0145-FEDER-000010), co-funded by Centro 2020 program, Portugal 2020, European Union, through the European Regional Development Fund, and when applicable co-funded by FEDER - PT2020 partnership agreement under the project UID/EEA/50008/2019.

References

[1] Cisco. Cisco visual networking index: Global mobile data traffic forecast update, 2016–2021 white paper. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html, 2015. ; Online; accessed 15 May 2018.

[2] Van-Giang Nguyen, Anna Brunstrom, Karl-Johan Grinnemo, and Javid Taheri. Sdn/nfv-based mobile packet core network architectures: a survey. *IEEE Communications Surveys & Tutorials*, 19(3):1567–1602, 2017.

[3] Matías Richart, Javier Baliosian, Joan Serrat, and Juan-Luis Gorricho. Resource slicing in virtual wireless networks: A survey. *IEEE Transactions on Network and Service Management*, 13(3):462–476, 2016.

[4] Graham Sewell and Laurent Taskin. Out of sight, out of mind in a new world of work? autonomy, control, and spatiotemporal scaling in telework. *Organization Studies*, 36(11):1507–1529, 2015.

[5] Abdullah Alshalan, Sandeep Pisharody, and Dijiang Huang. A survey of mobile vpn technologies. *IEEE Communications Surveys & Tutorials*, 18(2):1177–1196, 2016.

[6] Vach Kompella and Marc Lasserre. Virtual private lan service (vpls) using label distribution protocol (ldp) signaling. *RFC 4762*, 2007.

[7] Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, and Jonathan Turner. Openflow: enabling innovation in campus networks. *ACM SIGCOMM Computer Communication Review*, 38(2):69–74, 2008.

[8] Open Network Foundation (ONF). Openflow switch specification: Version 1.5.1. https://www.opennetworking.org/wp-content/uploads/2014/10/openflow-switch-v1.5.1.pdf, 2015. ; Online; accessed 15 May 2018.

[9] Richard Cziva, Simon Jouët, David Stapleton, Fung Po Tso, and Dimitrios P Pezaros. Sdn-based virtual machine management for cloud data centers. *IEEE Transactions on Network and Service Management*, 13(2):212–225, 2016.

[10] Laizhong Cui, F Richard Yu, and Qiao Yan. When big data meets software-defined networking: Sdn for big data and big data for sdn. *IEEE network*, 30(1):58–65, 2016.

[11] Kok-Kiong Yap, Masayoshi Kobayashi, Rob Sherwood, Te-Yuan Huang, Michael Chan, Nikhil Handigol, and Nick McKeown. Openroads: Empowering research in mobile networks. *ACM SIGCOMM Computer Communication Review*, 40(1):125–126, 2010.

[12] Tien-Thinh Nguyen, Christian Bonnet, and Jérôme Harri. Sdn-based distributed mobility management for 5g networks. Wireless Communications and Networking Conference (WCNC), 2016 IEEE, pages 1–7. IEEE, 2016.

[13] Luis M Contreras, Luca Cominardi, Haiyang Qian, and Carlos J Bernardos. Software-defined mobility management: Architecture proposal and future directions. *Mobile Networks and Applications*, 21(2):226–236, 2016.

[14] Michael Scharf, Vijay Gurbani, Thomas Voith, Manuel Stein, W Roome, Greg Soprovich, and Volker Hilt. Dynamic vpn optimization by alto guidance. Software Defined Networks (EWSDN), 2013 Second European Workshop on, pages 13–18. IEEE, 2013.

[15] Madhusanka Liyanage, Mika Ylianttila, and Andrei Gurtov. Improving the tunnel management performance of secure vpls architectures with sdn. Consumer Communications & Networking Conference (CCNC), 2016 13th IEEE Annual, pages 530–536. IEEE, 2016.

[16] Ronald van der Pol, Bart Gijsen, Piotr Zuraniewski, Daniel Filipe Cabaça Romão, and Marijke Kaat. Assessment of sdn technology for an easy-to-use vpn service. *Future Generation Computer Systems*, 56:295–302, 2016.

[17] Lalith Suresh, Julius Schulz-Zander, Ruben Merz, Anja Feldmann, and Teresa Vazao. Towards programmable enterprise wlans with odin. Proceedings of the first workshop on Hot topics in software defined networks, pages 115–120. ACM, 2012.

[18] Peter Dely, Jonathan Vestin, Andreas Kassler, Nico Bayer, Hans Einsiedler, and Christoph Peylo. Cloudmac - an openflow based architecture for 802.11 mac layer processing in the cloud. Globecom Workshops (GC Wkshps), 2012 IEEE, pages 186–191. IEEE, 2012.

[19] Flavio Meneses, Daniel Corujo, Carlos Guimaraes, and Rui L Aguiar. An abstraction framework for flow mobility in multitechnology 5g environments using virtualization and sdn. Network Softwarization (NetSoft), 2017 IEEE Conference on, pages 1–5. IEEE, 2017.

[20] Yasir Zaki, Liang Zhao, Carmelita Goerg, and Andreas Timm-Giel. Lte wireless virtualization and spectrum management. Wireless and Mobile Networking Conference (WMNC), 2010 Third Joint IFIP, pages 1–6. IEEE, 2010.

[21] Yasir Zaki, Liang Zhao, Carmelita Goerg, and Andreas Timm-Giel. Lte mobile network virtualization. *Mobile Networks and Applications*, 16(4):424–432, 2011.

[22] Ming Li, Liang Zhao, Xi Li, Xiaona Li, Yasir Zaki, Andreas Timm-Giel, and Carmelita Gorg. Investigation of network virtualization and load balancing techniques in lte networks. Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th, pages 1–5. IEEE, 2012.

[23] Albert Banchs, Pablo Serrano, Paul Patras, and Marek Natkaniec. Providing throughput and fairness guarantees in virtualized wlans through control theory. *Mobile Networks and Applications*, 17(4):435–446, 2012.

[24] Kiyohide Nakauchi, Yozo Shoji, and Nozomu Nishinaga. Airtime-based resource control in wireless lans for wireless network virtualization. Ubiquitous and Future Networks (ICUFN), 2012 Fourth International Conference on, pages 166–169. IEEE, 2012.

[25] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects (3GPP-TS). General packet radio service (gprs) enhancements for evolved universal terrestrial radio access network (e-utran) access (release 16) (3gpp ts 23.401), 2018.

[26] 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals. Access network discovery and selection function (andsf) management object (mo) (release 15) (3gpp ts 24.312), 2018.

[27] Wi-Fi Alliance Technical Committee. Hotspot 2.0 technical task group hotspot 2.0 (release 2) technical specification, 2015.

[28] K. Pentikousis, Y. Wang, and W. Hu. Mobileflow: Toward software-defined mobile networks. *IEEE Communications Magazine*, 51(7):44–53, July 2013.

[29] J. Mwangama, N. Ventura, A. Willner, Y. Al-Hazmi, G. Carella, and T. Magedanz. Towards mobile federated network operators. Proceedings of the 2015 1st IEEE Conference on Network Softwarization (NetSoft), pages 1–6, April 2015.

[30] J. Shin, K. Jung, and A. Park. Design of session and bearer control signaling in 3gpp lte system. 2008 IEEE 68th Vehicular Technology Conference, pages 1–5, Sept 2008.

[31] H. J. Einsiedler, A. Gavras, P. Sellstedt, R. Aguiar, R. Trivisonno, and D. Lavaux. System design for 5g converged networks. 2015 European Conference on Networks and Communications (EuCNC), pages 391–396, June 2015.

[32] Nokia Siemens Networks. Signalling is growing 50% faster than data traffic. white paper, 2012. Online; accessed 10 Jun 2018.

[33] Li Erran Li, Z Morley Mao, and Jennifer Rexford. Toward software-defined cellular networks. Software Defined Networking (EWSDN), 2012 European Workshop on, pages 7–12. IEEE, 2012.

[34] Xin Jin, Li Erran Li, Laurent Vanbever, and Jennifer Rexford. Softcell: Scalable and flexible cellular core network architecture. Proceedings of the ninth ACM conference on Emerging networking experiments and technologies, pages 163–174. ACM, 2013.

[35] Kostas Pentikousis, Yan Wang, and Weihua Hu. Mobileflow: Toward software-defined mobile networks. *IEEE Communications magazine*, 51(7):44–53, 2013.

[36] Ian F Akyildiz, Pu Wang, and Shih-Chun Lin. Softair: A software defined networking architecture for 5g wireless systems. *Computer Networks*, 85:1–18, 2015.

[37] Hucheng Wang, Shanzhi Chen, Hui Xu, Ming Ai, and Yan Shi. Softnet: A software defined decentralized mobile network architecture toward 5g. *IEEE Network*, 29(2):16–22, 2015.

[38] Faqir Zarrar Yousaf, Johannes Lessmann, Paulo Loureiro, and Stefan Schmid. Softepc - dynamic instantiation of mobile core network entities for efficient resource utilization. Communications (ICC), 2013 IEEE International Conference on, pages 3602–3606. IEEE, 2013.

[39] Xin Jin, Li Erran Li, Laurent Vanbever, and Jennifer Rexford. Softcell: Scalable and flexible cellular core network architecture. Proceedings of the Ninth ACM Conference on Emerging Networking Experiments and Technologies, pages 163–174, New York, NY, USA, 2013. ACM.

[40] T. Mahmoodi and S. Seetharaman. Traffic jam: Handling the increasing volume of

mobile data traffic. *IEEE Vehicular Technology Magazine*, 9(3):56–62, Sept 2014.

[41] A. C. Morales, A. Aijaz, and T. Mahmoodi. Taming mobility management functions in 5g: Handover functionality as a service (faas). 2015 IEEE Globecom Workshops (GC Wkshps), pages 1–4, Dec 2015.

[42] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects (3GPP-TS). Architecture enhancements for non-3gpp accesses (release 15) (3gpp ts 23.402), 2018.

[43] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects (3GPP-TS). System architecture for the 5g system, 2018.

[44] ETSI Group Report (GR). Network functions virtualisation (nfv) (release 3) management and orchestration, 2018.

[45] 3GPP TS 36.300. Evolved universal terrestrial radio access (e-utra) and evolved universal terrestrial radio access network (e-utran); overall description; stage 2, 2018.

[46] Navid Nikaein, Raymond Knopp, Florian Kaltenberger, Lionel Gauthier, Christian Bonnet, Dominique Nussbaum, and Riadh Ghaddab. Openairinterface: an open lte network in a pc. Proceedings of the 20th annual international conference on Mobile computing and networking, pages 305–308. ACM, 2014.

[47] RYU project team. Ryu sdn framework. https://osrg.github.io/ryu/, 2014. ; Online; accessed 20 May 2018.

[48] Hostapd. https://w1.fi/hostapd/. ; Online; accessed 15 May 2018.

[49] Linux WPA/WPA2/IEEE 802.1X Supplicant. https://w1.fi/wpa_supplicant/. ; Online; accessed 12 Jun 2018.

[50] Netlink Protocol Library Suite (libnl). https://www.infradead.org/ tgr/libnl/. ; Online; accessed 12 Jun 2018.

[51] M Isabel Sanchez, Antonio de la Oliva, and Carlos J Bernardos. Experimental analysis of connectivity management in mobile operating systems. *Computer Networks*, 94:41–61, 2016.

[52] iperf3. http://software.es.net/iperf/. ; Online; accessed 15 May 2018.

[53] Akshay Baheti. Extensible authentication protocol vulnerabilities and improvements. https://scholarworks.sjsu.edu/etd_projects/425, 2015. ; Online; accessed 1 Jun 2018.

[54] Jose Maria Rodriguez Castillo, Henrik Lundqvist, and Christer Qvarfordt. Energy consumption impact from wi-fi traffic offload. Wireless Communication Systems (ISWCS 2013), Proceedings of the Tenth International Symposium on, pages 1–5. VDE, 2013.