# Traffic Management in LTE-WiFi Slicing Networks

**Ali Saeed Dayem Alfoudi, Mohammed Dighriri, Gyu Myoung Lee, Rubem Pereira and Fung Po Tso**
Department of Computer Science, Liverpool John Moores University, L3 3AF, UK
A.S.Alfoudi@2014.ljmu.ac.uk, M.H.Dighriri@2015.ljmu.ac.uk, {G.M.Lee, R.Pereira, F.P.Tso}@ljmu.ac.uk

***Abstract*— Proliferation of the number of smart devices and user applications has generated a tremendous volume of data traffic from/to a cellular network. With a traditional cellular network, a user may experience many drawbacks such as low throughput, large latencies and network outages due to overload of data traffic. The software defined networking (SDN) and network function virtualization (NFV) rise as a promising solution to overcome such issues of traditional network architecture. In this paper, we introduce a new network architecture for LTE and WiFi slicing networks taking into account the advantage of SDN and NFV concepts. We propose an IP-Flow management controller in a slicing network to offload and balance the data traffic flow. By utilizing the P-GW and Wireless Access Gateway, we can handle the IP-Flow between LTE and WiFi networks. The P-GW works as an IP-Flow anchor to maintain the flow seamlessly during the offloading and balancing IP-Flow. Within WiFi networks, we leverage the Light Virtual Access Point (LVAP) approach to abstract the WiFi protocol stack for a programming capability of centralized control of WiFi network through the WiFi controller. By creating a client virtual port and assigning a specific Service Set Identifier (SSID), we give a capability to slice an operator's network to control over his clients within a WiFi coverage area network.***

***Keywords—Long-Term Evolution (LTE); WiFi; Software Defined Networking (SDN); Network Function Virtualization (NFV); Light Virtual Access Point (LVAP); IP-Flow; Data offloading.***

## I. INTRODUCTION

With ever-increasing of smart device connectivity and user applications, the traditional cellular network infrastructure and networking protocols are not sufficient to manage this tremendous data traffic, considering a different level of resource allocation and traffic flows in Radio Access Networks (RAN) and core networks. The user may experience many drawbacks such as low throughput, long latencies and network outages due to congestion and overload of data traffic [1]. As one of the cheapest solutions, a cellular network operator solved this issue by either capping data usage or throttling a connection speed [2]. However, these old approaches have a negative effect on the user satisfaction. Therefore, alternative mechanisms are necessary such as device to device communication and using Wireless Local Area Networks (WLAN) to offload and balance the data traffic flow network. The most popular approach that Internet Service Providers (ISP) and some of companies use is by offloading some traffic flows into supplementary networks such as a WiFi network (e.g., AT&T, Cisco and Qualcomm) [3], [4].

In our work, we will consider the approach of a supplementary network to offload and balance the data traffic flow in the Long-Term Evolution (LTE) network. In this regard, we will focus on a WiFi network. First, we need to discuss some limitations of the current networks architecture (LTE and WiFi).

The current LTE network is facing some issues with the architecture in terms of centralized data flow bearers, centralized monitoring and control, and difficulties of base station and infrastructure in terms of upgrade and configuration [5]. Within the centralized data flow, it is very complicated to update because all the bearers pass through the packet data network gateway (P-GW). Furthermore, there are also financial issues when a modification is necessary in the network where any update or upgrade in the infrastructure increases the operational expenditure (OPEX) and capital expenditure (CAPEX) of network costs.

On the other hand, in the WiFi network there is no central control mechanism over user equipment (UEs) association because the UE locally decides on its own which associations are more suitable to connect. Furthermore, the network operator does not have a control scheme over the UE re-association without requiring additional signaling techniques such as Dyson and ECHOS in [6], [7].

The software defined networking (SDN) and network function virtualization (NFV) are a network architecture technology that opens new trends to eliminate the rigidity present in the traditional networks [8]. These network architectural structures make the behavior of the network to be more flexible and adaptable to meet the requirements of each organization, campus, or group of users. Moreover, it has emerged as a promising solution to overcome such issues in traditional networks architecture. While SDN divides the network architecture into two planes, namely control and data planes, it supports the programming capability of the network infrastructure through an open Application Programming Interface (API). In a cellular network, the NFV can virtualize most of current network infrastructure functionalities with a software. Therefore, it reduces the CAPEX/OPEX of the Mobile Network Operators (MNOs).

In general, there are two approaches for enabling a client to connect to a physical AP in a WiFi network, namely active and passive approaches. The active approach is when the UE itself scans for available APs, while in the passive approach the UE listens to the AP. The UE sends probe messages to all available APs in the active approach and the AP who replies with the probe message will be the candidate of UE, then the UE will select which one is more appropriate to connect. For instance, the association process is determined between the UE MAC address

and the Basic Service Set Identifier (BSSID) of the AP. The BSSID of an AP is defined as an AP MAC address and it is different from the Service Set Identifier (SSID), which is known as a network name [9], [10].

In this work, we use the Light Virtual Access Point (LVAP) approach for abstracting the IEEE 802.11 protocol stack to overcome such ordinary difficulties between UEs and the infrastructure. With this approach, no modification is required on UEs side, where each UE receives a unique BSSID to connect to an access network.

In this paper, we introduce a new network architecture for LTE and WiFi networks taking into account the advantage of SDN and NFV concepts. We propose an IP-Flow management controller in a slicing network to offload and balance the data traffic flow. By utilizing the P-GW and Wireless Access Gateway (WAG), we can handle the IP-Flow between LTE and WiFi networks. The P-GW works as an IP-Flow anchor to maintain the flow seamlessly during the offloading and balancing IP-Flow. Within WiFi networks, we leverage the LVAP approach to abstract the WiFi protocol stack for a programming capability of centralized control of WiFi networks through the WiFi controller.

The rest of the paper is organized as follows. In Section II, we briefly describe the Evolved Packet Core (EPC)-LTE architecture. Section III shows how we can virtualize the EPC. Virtual WiFi AP migration and an UE virtual port are presented in Section IV. Slicing technology is applied in both LTE and WiFi networks in Section V. Section VI presents the seamless slicing between LTE and WiFi based on IP-Flow mobility. Conclusion follows in Section VII.

## II. Evolved Packet Core (EPC) in LTE network

As shown in the Figure 1, there are four components of EPC in the LTE network.

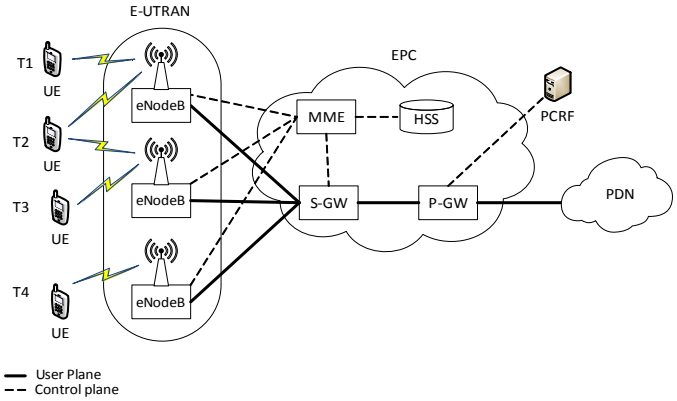


Figure 1: LTE Network

1) *Mobility Management Entity (MME):* this element controls most of the operations that occur in the EPC. We can say it is the brain of the operation in EPC. The major responsibility of MME is managing a tracking area location when the UE moves in different eNodeB coverage areas. MME interacts with other elements in EPC, such as Home Subscribe System (HSS), S-GW and P-GW [11]. The MME has a functionality to authenticate and authorize the UE. It's interacting with the HSS to implement these operations because the HSS kind of databases store all data that are related to those two functionalities of MME. For example, to answer the question of authentication (e.g., the *IMSI (International Mobile Subscriber Identity)* of UE (the process of verifying)) and for authorization (e.g., *roaming authorization*). Among its duties, it also gives the key instructions to other node elements in EPC (S-GW and P-GW). For example, MME gives the instruction directly to the S-GW and indirectly to the P-GW, when it is time to setup a bearer the MME tells the S-GW to setup the bearer. The S-GW will pass this indirect instruction on to the P-GW. These components can manage the data forward and backward flows from the mobile device to the IP flow network.

2) *Serving GateWay (S-GW):* It is the gateway which connects the interface between the EPC and E-UTARN. For each mobile device linked with the EPC, there is a single S-GW at a given point of time.

S-GW focuses only on the user plane, it is responsible to forward the data packets from P-GW to eNodeB and to maintain the data session (e.g., the bearer and the mobile IP) in order to change and handover between the different eNodeBs locally. Therefore, it is sometimes called a local or mobility anchor. Moreover, when the mobile device moves from the current eNodeB to another one, the S-GW maintains the data session connectivity for the UE in the handover when switching between various eNodeBs [12]. For example, if the user works in a city (like Liverpool) he will be the Liverpool subscriber and he is connected to eNodeB LTE network close to his office. When he drives his car to go back home he will switch from one eNodeB to another; The S-GW will switch the connection of UE to the nearest eNodeB on his path to home. As a result, the S-GW is also located in Liverpool. S-GW maintains the data session from P-GW to eNodeB through the General Packet Radio Service (GPRS) Tunnelling Protocol (GTP).

*3) Packets Data Network GateWay (P-GW):* It is the gateway connected to the EPC with external IP network, such as Internet, IP Multimedia Subsystem (IMS), emails and special network services. P-GW is responsible for connecting the UE with IP network by assigning an IP address (IPv4, IPv6) to UE to connect to a specific network [13]. It works as an IP anchor to maintain the same IP address during mobility between 3GPP and non-3GPP services, it acts like a Home Agent (HA).

In addition, the P-GW is responsible to enforce Quality of Service (QoS) policy set by Policy and Charging Rules Functions (PCRF) of QoS components in IMS. When a mobile device requests a bearer or when a bearer needs to setup an IMS call or video call, the P-GW and PCRF will interact together to make sure that the right policy has been enforced for that bearer.

*4) Home Subscribe System (HSS):* This component is a kind of database to store all the information related to the subscriber. HSS has two functions, the Home Location Register (HLR) and the Authentication Centre (AuC) that are already existing in the Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS) networks [13].

The HSS is responsible for storing and updating data related to user subscription such as:

- User addressing and identification numbers.
- User profile.
- Network authentication and authorization information such as path ciphering and integrity protection.

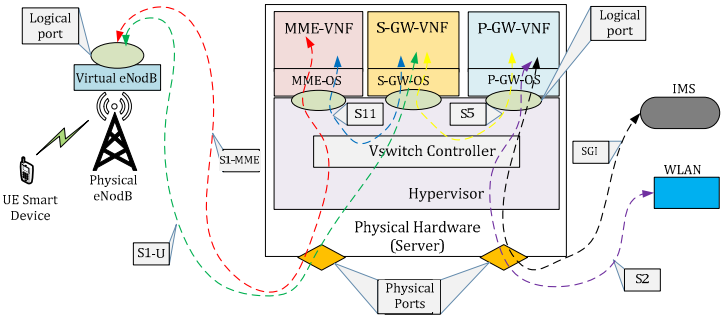


Figure 2: SDN and Virtualize Core LTE network

## III. LTE Network Virtualization

This section describes how we can virtualize the function of the EPC elements that was mentioned in Section II. Let us take three basic elements (MME, S-GW and P-GW) of EPC and put them in the same physical hardware platforms and logically softwarize them. Therefore, in our context, the EPC Function Virtualization (EFV) is a process of virtualizing network function (VNF). As shown in the Figure 2, the MME-VNF, S-GW-VNF and P-GW-VNF all of them sit in the same physical server [14], [15]. The hypervisor places the rules of which device should be placed logically in the platform. Moreover, the hypervisor in our context has a virtual switch (VSwitch) with which it can handle the traffic between different logical ports of VNFs and physical ports of hardware server. For example, in the Figure 2, the interface (S11) connects between the MME-VNF and S-GW-VNF through logical ports by VSwitch, Also, the S1-MME interface connects MME with the eNodeB through the MME-VNF logical port and server physical port by VSwitch. In the same context, other interfaces represent a logical connection of different elements in the LTE network. In addition, if the P-GW intends to forward a message outside the core LTE network via the SGI interface. The logical port of P-GW-VNF sends the message through the SGI interface to the VSwitch Controller, and the latter recognizes the direction of the message outside the core network, then it forwards the message to the server physical port to send outside LTE via SGI interface.

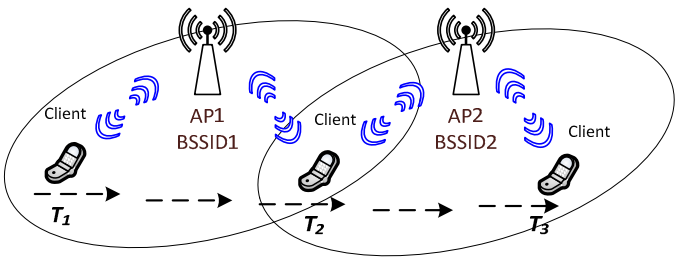


Figure 3. Traditional WiFi Architecture

## IV. WiFi Network

### A. *Virtual WiFi AP migration*

The traditional way of designing WLAN is to follow up a micro cell architecture. The Figure 3 shows how the micro cell works. As depicted in the figure, each AP has its own coverage region and its own BSSID. When the client tries to start the establishment of a new connection to an AP, it sends a probe request message to see which BSSIDs are available (APs) so that it can decide the appropriate one to connect with [16]. For instance, let us assume that there are two APs and each one has its own unique BSSID (BSSID1 and BSSID2). As shown in Figure 3, when the client enters into AP1 coverage area at T1 it sends a probe request message and there is just AP1 with BSSID1, the AP1 can hear the message and respond to the client allowing the client to connect with it. As the client moves to T2, it starts to see the AP2, and at T3 the client notices that the radio signal strength (RSS) for BSSID1 becomes weak, therefore the client will make its own decision to figure out whether to continue with the current BSSID (in this case BSSID1) or to look for another one. It then starts to send a probe request message to the available APs and the both BSSIDs for AP1 and AP2 will hear the probe message and respond. At this point, the client will choose which AP is appropriate to connect with (here AP2 is chosen).

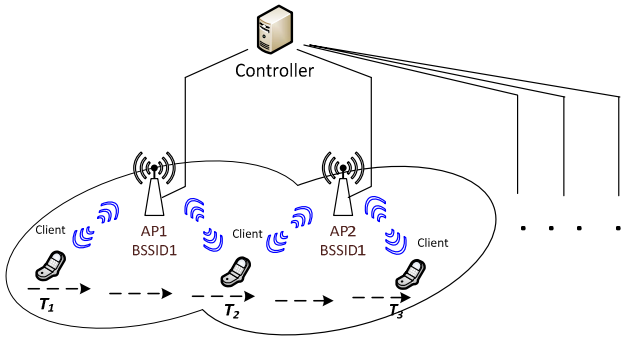


Figure 4. Virtual WiFi-APs Architecture

From this scenario, we can notice a couple of things. Firstly, when an AP advertises its presence by BSSID, the responsibility of the client is to make a decision on whether to join the AP or not. Secondly, as a client moves the decision of where the handover occurs is the client's choice. As the key point here, we want to take off the decision of initiating a network connectivity from a client because one client can affect the behavior of other clients in the network. To take the decision out of a client, both APs should have the same BSSID from the client perspectives. As shown in the Figure 4, when both APs advertise the same BSSID, it does not matter whether the client's position is at T1, T2 or T3 because it will hear just BSSID1. Furthermore, when the client sends a probe message to connect to an AP, it may hear the response from one AP or multiple APs, all of them having the same BSSID1 from the client view point (in such a case it takes a decision away from the client). In addition, as the client moves, it is up to the infrastructure to figure out which AP is in a better position to serve the client (AP1 or AP2) and from the client side there is no handover.

Let us explain the handover from a client perspective. As shown in the Figure 4, both APs are connecting to the controller and periodically APs compose a message digest of all devices (e.g., frame rate, number of transmissions, RSS, etc.) that receive

the BSSID to the controller, so the controller has a global view of network status. Therefore, the controller can manage all the topology and assign which AP has a better link for the client to connect. In this case, the client does not experience any handover process because all the APs have the same BSSID resulting in what is called virtual AP.

### *B. Clients (UE) Virtual Port*

Each device has its own personalized BSSID, if there are two devices within same AP, each one has a unique BSSID [17]. Let us assume that there are two clients (UE1 and UE2) assigned to the same AP1 but each one has a different BSSID (we assume that BSSID1 for UE1 and BSSID2 for UE2). As the UE1 moves over from AP1 to AP2, at some point the controller decides that the AP2 is better to serve UE1; at that point, depending on the topology design, the controller will send the BSSID1 from AP1 over to AP2. This process will continue in the same context as long as the client is migrating from AP to another. Note that the BSSID associated with a client has all corresponding information related to a client (e.g., all the packets, all the sequence numbers, all the corresponding security state, etc.).

The benefit of assigning a unique BSSID to each client (UE) is that the infrastructure has an ability to distinguish the service between APs for an individual client. The migration from virtual AP to the virtual UE port technique can create a switch like abstraction when each UE device effectively gets its own virtual port that allows the controller for handling a network topology per-device control in terms of channel access and security parameters.

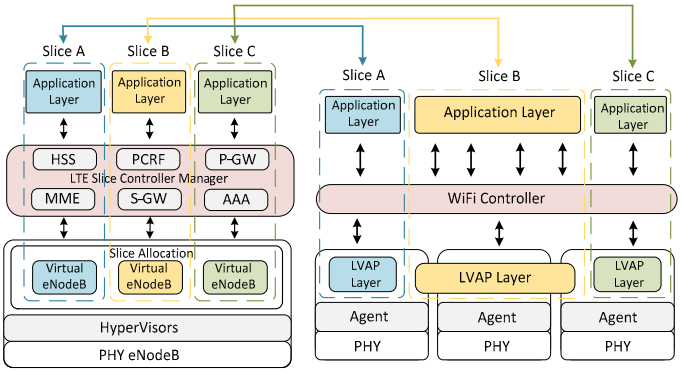


Figure 5. LTE-WiFi Slicing Networks

## V. LTE- WiFi Slicing Network

### *A. Slice Assigning in LTE*

When the service operator asks the LTE Slice Controller Manager (LSCM) and Slice Allocation (SA) to assign a slice for a service (S). There are three possible scenarios for assigning a slice to S. The first scenario is when the LSCM assigns the current slice to S. The second one is when the LSCM decides to expand the current slice to meet the S requirements such as video streaming. Lastly, this scenario is when the LSCM decides to create a newly slice based on the new S technical and QoS requirements such as the remote monitor surgery service [18], [19].

Assigning a slice to a service S depends on the technical requirements $t_s$ (e.g., mobility management, tunneling, etc.) and QoS $q_s$ (e.g., the maximum latency, minimum bandwidth). When the service operator requests to assign a slice to a certain service, it sends S requirements of the slice to the LSCM and SA. Where the LSCM will decide to assign a slice for S according to the following equations (1) and (2).

$$d_t(n) = t_n - t_s \quad \ldots\ldots\ldots \quad (1)$$

$$d_q(n) = q_n - q_s \quad \ldots\ldots\ldots \quad (2)$$

Where $d_t(n)$ and $d_q(n)$ represent the difference of requirements of the required slice $(t_s, q_s)$ and the current slice $(t_n, q_n)$. If one or both parameters have a negative value that means the current slice does not meet the technical or QoS requirements for S. In case of expanding the current slice or creating a new slice, the LSCM's decision will be according to equation (3).

$$d_{ctech}(n) = (C_{en} + C_{oen} + l_{bn}) - (C_c + C_o + l_b) \quad \ldots \quad (3)$$

For any slice $n$ the LSCM calculates $d_{ctech}(n)$, which is the difference between the cost of expanding the current slice and creating a new slice based service. $C_{en}$ is the cost of expanding the current slice, $C_{oen}$ denotes the effective operating cost of current slice after expanding, and $l_{bn}$ represents the cost of losing bandwidth for expanding the current slice. $C_c$ is the cost of creating slice based service, $C_o$ denotes the cost of operation to create a new slice, and $l_b$ represents the cost of losing bandwidth needed to create a new slice. If the value of $d_{ctech}(n)$ is negative that means the cost of expanding the current slice is less than the cost of creating a new slice, therefore the decision of LSCM to assign a slice will have the lowest value (in this case, the expand of the current slice) and vice versa.

### *B. Slicing WiFi network*

When the UE seeks for an AP, the WiFi controller will assign a new Light Virtual Access Point (LVAP). The LVAP abstracts the control logical association and isolation of clients by assigning unique BSSID to each client in order to connect to the AP (virtual AP) as described previously.

Each LVAP is allocated to a client by WiFi controller. Its content contains information that enables the client to logically connect to and isolate from others in the same coverage area. Individual LVAP client contains unique BSSID, one or more SSID, client MAC address, IP address, a set of open flow rules to manage the switch flow tables.

As described in the client virtual port, the benefit of the unique BSSID in LVAP is that the controller can distinguish a certain UE when moving between different APs. This allows handling the handover of client between varying APs. From a client perspective, there is no handover because APs always have the same BSSID.

As shown in the Figure 5, for slicing the WiFi network, the LVAP will assign a specific slice by defining a set of SSIDs, because these SSIDs are related to the specific slice in the LTE. When a UE is assigned to one of these SSIDs, it is automatically assigned to a certain slice.

### *C. Slicing association between LTE and WiFi networks*

The operator would always like to control his clients in order to introduce the best quality service and user experiences. In this work, we introduce a slicing network architecture in a scenario where a UE moves between different access network interfaces (LTE and WiFi). A UE that is within a certain LTE slice network,

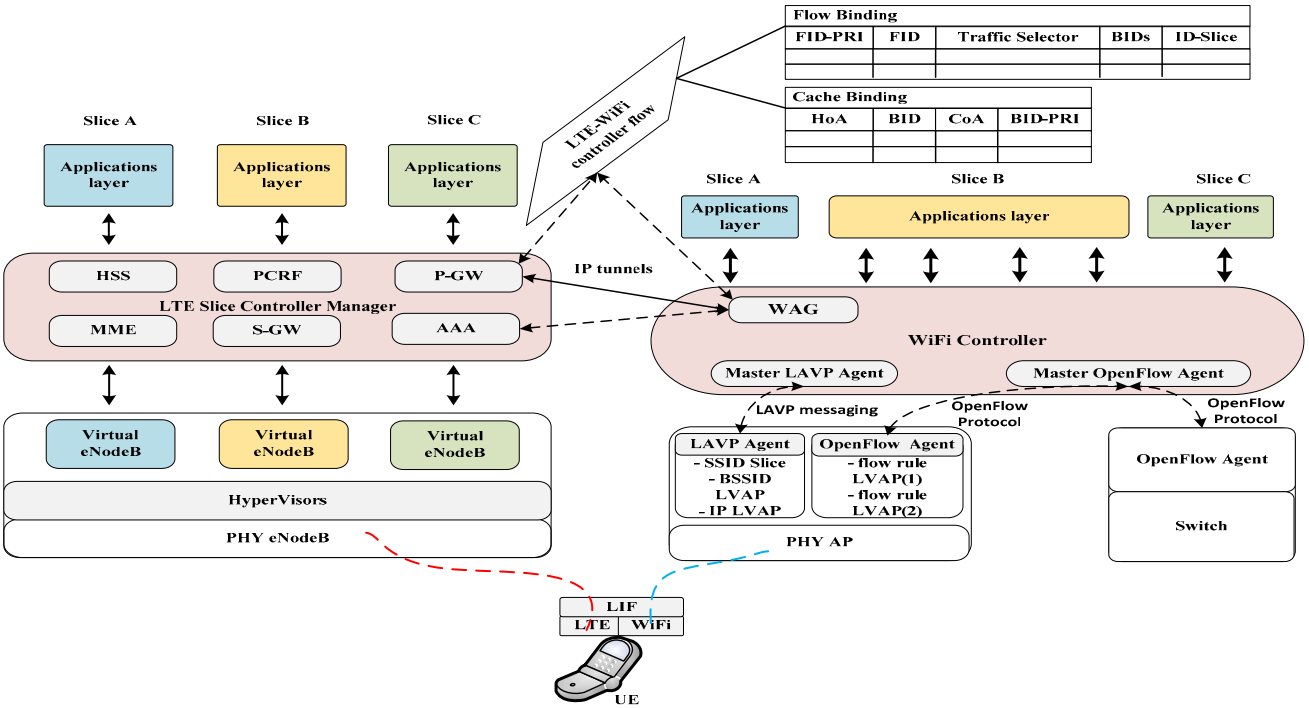


Figure 6: logical Connection LTE-WiFi

and for any other reason such as offloading for better RSS, it triggers the handover process to another access network, in this case a WiFi network. Now, the question is how we can keep the UE under the same slice control after switching to a WiFi network coverage area.

If the UE were previously under a certain slice control of LTE networks, it would be controlled and managed by the slice operator. In case of the handover, the slice operator will provide the UE with a list of SSIDs that represents the slice in the WiFi network. When the UE moves to WiFi it will be assigned to one of these SSIDs. At this point, the UE will continue within the same slice that was within LTE network. As a result, we give a slice operator the capability to the control over a UE within a different access network (WiFi network).

## VI. Seamless Slicing Networks Based on IP-Flow Mobility

In traditional LTE network, the user service flow setup is held by a network operator. In the same manner, our proposal work encompasses a LSCM that enables a slice operator to setup IP-Flows. Moreover, the LSCM during the setup tags an ID-Slice for each flow. In the same context, we assume that a slice operator is taking care of a flow admission control to ensure that each flow gets enough resource requirement for QoS guarantee.

There are two types of IP mobility: the network based IP mobility and the client based IP mobility. The approach of network based IP mobility is different from the client based IP mobility because the network based IP mobility approach takes care of all steps that are necessary to route the data packets to its destination. Therefore, there is no need for a client to do any signaling to change the network; the network operator does everything.

The network based IP mobility there are two approaches specified, the Proxy Mobile IP version 6 (PMIPv6) by IETF and the GPRS Tunneling Protocol (GTP) by 3GPP. Both have some similarities in the behavior. Nevertheless, the main difference between them is that the GTP is realized on the concept of bearers whereas the PMIPv6 utilizes the IPv6.

The mobility protocols were released in the 3GPP specifications 8 and 9, which specify that it is possible to offload data between the LTE-WiFi and vice versa [20], [21]. However, these specifications are only for complete offloading, it is either possible to communicate to the LTE connection or over the WiFi connection but not over both simultaneously. The reason is, in the architecture, the WiFi is considered as a foreign network. Thus, all the network data packets are forwarded to the WiFi when there is a corresponding entry in the binding cache. To achieve a more efficient data offloading, it is required to send different data flows over different access technologies depending on the traffic types and service requirements.

In our work, we consider that the UE device has a capability to use both interfaces (LTE and WiFi) simultaneously, and create a logical interface (LIF) layer above them in order to hide all the complexity of the connection behind the IP layer. This allows more transparency for the applications in the layers above the IP layer. Figure 6 shows network entities, a P-GW works as an IP anchor, which does all the IP admissions.

Another node called Wireless Access Gateway (WAG) implements the necessary functions in the WiFi network. The routing is done between the P-GW and WAG by the LTE-WiFi Controller Flow (LWCF). It takes care of all the signaling between the P-GW and WAG to tunneling the UE flow mobility from the LTE to the WiFi and vice versa. When a UE changes his network coverage location from LTE to WiFi, the WiFi controller assigns a new LVAP to logically abstract all UE information and status (e.g., IP addresses, port addresses, ID-

Slice (same as SSID) and OpenFlow rules). In case of any change in the UE locations, the LVAP tells the WiFi controller which it in turn will inform the WAG to update the binding tables in the LWCF. One Home Address (HoA) has a number of Care of Address, which may be assigned in the binding cache table. In addition, there is another table called the flow binding table, which specifies the type of traffic route to a corresponding CoAs. Both tables are sorted with respect to the priorities. The highest prioritized entry is at the top. They are linked together over the Binding Identity (BID) fields. If any item is missing in one of the tables, the highest priority binding entry is used by default. Finally, the novelty of the presented architecture is that seamless individual flows can be implemented for any of the interfaces (LTE and WiFi) under a specific slice.

## VII. Conclusion and Future Work

In this paper, we have introduced a new slicing network architecture between LTE and WiFi networks for managing data traffic. Utilizing the concept of SDN and NFV gives a capability to program a network infrastructure and virtualize a network functionality for enabling the network operator to have control over UEs in different access networks. On the one hand, in the LTE network, assigning UE to a certain slice depends on the technical requirements and QoS parameters for a service. On the other hand, the WiFi controller allocates a LVAP for each UE who wants to connect to a WiFi network and assigns an individual BSSID and one or more SSID to give an abstraction information about UE status in order to enable the WiFi controller and a slice operator to handle and manage UE mobility between WiFi-APs.

Several improvements can be made to enhance isolation across flows belong to different slices for the same user by modifying the client LTE drivers. WiFi-APs interference should be resolved when APs are advertising on the same channel. To address these issues, it is essential to design a distribution of APs on network topology through the WiFi controller.

## References


[1] Paul Taylor, “Data overload threatens mobile networks - Benton Foundation,” 2012. [Online]. Available: https://www.benton.org/node/122825.

[2] S. Curtis, “Can you survive on 4G alone?,” *The Telegraph*, 2013. [Online]. Available: http://www.telegraph.co.uk/technology/internet/10272292/Can-you-survive-on-4G-alone.html.

[3] Qualcomm, “A 3G/LTE Wi-Fi Offload Framework: Connectivity Engine (CnE) to Manage Inter-System Radio Connections and Applications,” no. June, 2011.

[4] Cisco, “Architecture for Mobile Data Offload over Wi-Fi Access Networks,” vol. 8, no. 2008, pp. 1–23, 2012.

[5] M. lsson, S. Sultana, S. Rommer, L. Frid, and C. Mulligan, SAE and the Evolved Packet Core: Driving the Mobile Broadband Revolution, Elsevier, New York, NY, USA, 2009.

[6] R. Murty, J. Padhye, A. Wolman, and M. Welsh, “Dyson: An Architecture for Extensible Wireless LANs,” Proc. 2010 USENIX Annu. Tech. Conf., p. 14, 2010.

[7] A. Vasan, R. Ramjee, and T. Y. C. Woo, “ECHOS – enhanced capacity 802.11 hotspots,” in Proc. IEEE INFOCOM 2005, March 2005, pp. 1562–1572.

[8] Á. L. Valdivieso Caraguay, A. Benito Peral, L. I. Barona López, and L. J. García Villalba, “SDN: Evolution and opportunities in the development IoT applications,” Int. J. Distrib. Sens. Networks, vol. 2014, 2014.

[9] G. Bartlett, J. Heidemann, and C. Papadopoulos, “Understanding passive and active service discovery,” Proc. 7th ACM SIGCOMM Conf. Internet Meas., pp. 57–70, 2007.

[10] N. Rouwers, M. Niga, and K. Langendoen, “Incremental Wi-Fi Scanning for Energy-Efficient Localization,” in Proc. Int’l Conf. Pervasive Computing (PerCom), 2014, pp. 156–162.

[11] P. Beming, L. Frid, G. Hall, P. Malm, T. Noren, M. Olsson, and G. Rune, “LTE-SAE architecture and performance,” Ericsson Rev. (English Ed.), vol. 84, no. 3, pp. 98–104, 2007.

[12] TutorialsPoint, “Lte network architecture.” 2016. [Online]. Available: https://www.tutorialspoint.com/lte/index.htm.

[13] V. G. Nguyen, T. X. Do, and Y. H. Kim, “SDN and Virtualization-Based LTE Mobile Network Architectures: A Comprehensive Survey,” Wirel. Pers. Commun., vol. 86, no. 3, pp. 1401–1438, 2016.

[14] 4G Americas, “Bringing Network Function Virtualization to LTE November 2014 0,” no. November, pp. 0–56, 2014.

[15] Y. Zaki, L. Zhao, C. Goerg, and A. Timm-Giel, “LTE mobile network virtualization Exploiting multiplexing and multi-user diversity gain,” Mob. Networks Appl., vol. 16, no. 4, pp. 424–432, 2011.

[16] Cisco-Reference, “Campus LAN and Wireless LAN Design Guide,” 2015.

[17] L. Suresh, J. Schulz-Zander, R. Merz, A. Feldmann, and T. Vazao, “Towards Programmable Enterprise WLANS with Odin,” *Proc. 1st Work. HotSDN*, pp. 115–120, 2012.

[18] V. G. Nguyen and Y. H. Kim, “Slicing the next mobile packet core network,” 2014 11th Int. Symp. Wirel. Commun. Syst. ISWCS 2014 - Proc., pp. 901–904, 2014.

[19] T. Shimojo, Y. Takano, A. Khan, S. Kaptchouang, M. Tamura, and S. Iwashina, “Future mobile core network for efficient service operation,” 1st IEEE Conf. Netw. Softwarization Software-Defined Infrastructures Networks, Clouds, IoT Serv. NETSOFT 2015, 2015.

[20] 3GPP TS 23.327, “Mobility between 3GPP-Wireless Local Area Network (WLAN) interworking and 3GPP systems.” .

[21] 3GPP TS 24.302, “Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3.” .