Seamless LTE-WiFi Architecture for Offloading the Overloaded LTE with Efficient UE Authentication

Ali Saeed Dayem Alfoudi
Department of Computer Science
Liverpool John Moores University
Liverpool, L3 3AF, UK
A.S.Alfoudi@2014.ljmu.ac.uk

Gyu Myoung Lee
Department of Computer Science
Liverpool John Moores University
Liverpool, L3 3AF, UK
G.M.Lee@ljmu.ac.uk

Mohammed Dighriri
Department of Computer Science
Liverpool John Moores University
Liverpool, L3 3AF, UK
M.H.Dighriri@2015.ljmu.ac.uk

Abstract*—Nowadays a cellular network suffers from a data traffic load in a metropolitan area due to the enormous number of mobile devices connectivity. Therefore, the users experience many issues because of a congestion and overload at an access network such as low throughput, long latencies and network outages. Current network operator's solutions, such as capping data usage and throttling a connection speed, have a negative effect on the user satisfaction. Therefore, alternative solutions are needed such as Access Point (AP)-based complementary network. In this paper, we use WiFi as a complementary network to Long-Term Evolution (LTE). We propose a seamless network architecture between LTE and WiFi networks, by utilizing the packet gateway (P-GW) as an IP flow anchor between LTE and WiFi to maintain a seamless connectivity. The proposed architecture has two new components, Access Network Query Protocol-Data Server (ANQP-DS) and Access Zone Control (AZC), to WiFi core network for managing UE authentication and balancing the load of UEs between APs. Finally, we demonstrate and validate the effectiveness of our proposed idea over other prior approaches based on comparison with a current handover and Extensible Authentication Protocol-Authentication and Key Agreement (EAP-AKA) mechanisms in the literature through simulations.

Keywords*—Long-Term Evolution (LTE); WiFi; Extensible Authentication Protocol-Authentication and Key Agreement (EAP-AKA); Access Network Query Protocol-Data Server (ANQP-DS)

I. INTRODUCTION

In a crowded metropolitan environment, during the peak times the users experience many drawbacks such as low throughput, long latencies and network outages due to congestion and overload at an access network [1]. As a first choice, a network operator solved this issue by capping data usage and throttling a connection speed [2]. However, these old approaches have a negative effect on the user satisfaction. Therefore, alternated mechanisms are needed, such as device to device and using Wireless Local Area Networks (WLAN) to offload the overloaded network. The most popular approach that Internet Service Providers (IPS) used to offload is by offloading some traffic into supplementary networks such as WiFi network. For example, some of the companies, such as AT&T, Cisco and Qualcomm, studied new architectures to offload 3G/4G traffic data network to WiFi network [3], [4]. In this approach, there are many challenges that are needed to be solved by researchers, such as the User Equipment (UE) which only monitors the air interface connection, abandoning the backhaul capacity of eNodeB and Access Point (AP) for the core network [5]. Moreover, the dynamic switching between APs when the UE moves to WiFi network coverage area is quite essential [6]. Lastly, verification of a user in the vertical handover procedure is important when the UE switches from LTE to WiFi network [7].

There exist various works and protocol standards, providing offload data between LTE and WiFi networks. The 3rd-Generation Partnership Project (3GPP) radio access networks considers data offloading that is a promising solution to solve the cellular overload problem. They are proposing the Access Network Discovery and Selection Function (ANDSF) mechanism to trigger the handover between various access technologies [8]. Alternative offloading mechanisms are proposed, such as IP Flow Mobility [9], Selected IP Traffic Offload (SIPTO), Local IP Access (LIPA) for data offloading [10], Seamless Internetworking Flow Mobility (SIFM) [11] and multipath transmission protocol (MPTCP) [12]. Most of these techniques suffer from the latency in the UE authentication during the handover procedure [13]. They also have weaknesses in terms of maintaining a mobility management when the UE is switched to the WiFi network it moves in small coverage area of APs, therefore it dynamically changes its AP.

In this paper, we propose a seamless network architecture between LTE and WiFi networks, which overcome the drawbacks of existing architectures to offload the overload cellular network. By utilizing the packet gateway (P-GW) in LTE core and adding two components, Access Network Query Protocol-Data Server (ANQP-DS) and Access Zone Control (AZC), to the WiFi core network, we can handle the UE when it switches from LTE to WiFi. The P-GW works as an IP anchor to maintain the same IP address during mobility between different networks, while in the WiFi network the ANQP-DS and AZC will manage the UE mobility in WiFi network, where the AZC manages APs by balancing the load of UEs between APs and the ANQP-DS holds the information about the UE verification and profile of the WiFi network.

In the pre-performance evaluation of our proposal in the metropolitan environment, we expected that during the handover procedure the time of UE authentication is less than current mechanisms (e.g., Extensible Authentication Protocol-Authentication and Key Agreement (EAP-AKA)), while improving the throughput capacity of WiFi network due to distributed UEs on APs by the AZC.

The rest of the paper is structured as follows. In Section II, we briefly describe the EPC-LTE architecture. In Section III,

we show how the WiFi components can be managed a mobility of UE between APs. LTE and WiFi network integration is presented in Section IV. Performance evaluation is illustrated in Section V. Conclusion follows in Section VI.

II. Evolved Packet Core (EPC) in LTE Networ

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

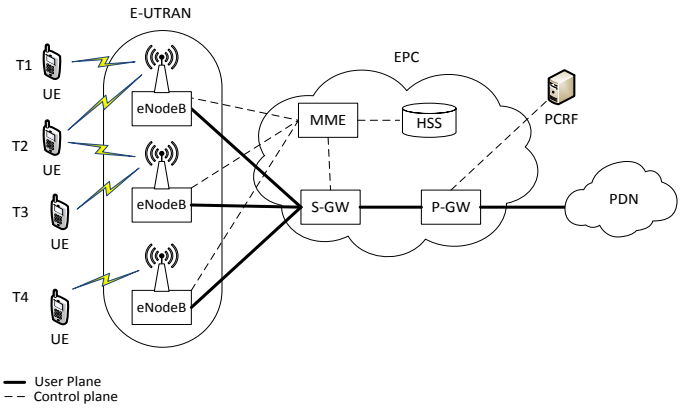

Figure 1: LTE Network

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 HSS, S-GW and P-GW [14]. The MME has a functionality to authenticate and authorize the UE. It's interacting with the Home Subscribe System (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 for 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 the time to setup a bearer the MME is going to tell the S-GW to setup the bearer. The S-GW will pass this indirect on through to the P-GW. These components can manage the data forward and backward through, from the mobile device to the IP flow network.

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

S-GW is only focusing on user plane, it's responsible to forward the data packets from P-GW to eNodeB and maintain the data session, bearer and mobile IP to change in the handover between the different eNodeBs locally. Therefore, it can call as a local or mobility anchor. Moreover, when the mobile device moves from the current eNodeB to another one, the S-GW maintains the session data connectivity for the UE in the handover when switching between various eNodeBs. For example, if the user lives in 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 EPS 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 [15]. 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).

Also 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 for an IMS call or video call, the P-GW and PCRF will interact together to make sure that the right policy has been enforced to that bearer.

4) Home Subscribe System (HSS): This component is a kind of database to store all the information related to the subscriber. HSS is combined of two functions, Home location Register (HLR) and Authentication Centre (AuC), that they already exist in the Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS) networks.

The HSS is responsible of 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.

III. WiFi Network

The UEs with the coverage area of WiFi network were already identified within the LTE network previously. When the UE switches from the LTE to WiFi networks, all the data subscriptions will enquiry from the LTE to WiFi for maintaining the continuity without interrupting connected network.

In this paper as shown in Figure 2, we add two components for the WiFi network to control and manage the WiFi network. The first component Access Zone Control (AZC) is responsible to handle the APs and UE where when UE enters to the WiFi network it can move between the different APs without needing to enquiry about it from the LTE each time. The other component Access Network Query Protocol-Data Server (ANQP-DS) is responsible to collect and store data needed about the UE (subscriber) from the LTE network to stay connected to the WiFi network without interrupted services.

The following describes the functionality of these two components in details.

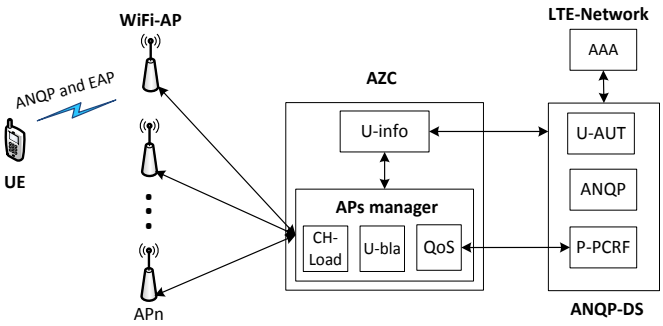

Figure 2: WiFi control components

A. Access Zone Control (AZC)

This element is responsible of managing all UEs and APs in WiFi coverage area zone. It consists of two functional components, these components collaborate each other to manage the seamless mobility, load balance UEs in APs coverage area and maintain the QoS for an individual user in the WiFi network zone.

The following describes details about the components of AZC:

1) U-Info: This element is a kind of cash memory to save the UE identity information. When the UE first successfully joins from the LTE to the WiFi network, it is added to the U-Info. Normally, when the UE switches from one AP to another, it needs to authenticate each time (form the LTE), that may be cost delay in handover process. Therefore, it is added to U-Info after successfully switching to the WiFi AP and completing authentication process; for the UE next switching AP in the WiFi coverage, the authentication process is not needed because the UE moves within the same AZC coverage area.

2) APs manager: The functionality of this element is to handle the APs in the WiFi network zone by channels load balance, user load balance within a specific AP coverage area and maintain QoS for an individual user within a specific application.

B. Access Network Query Protocol-Data Server (ANQP-DS)

We introduce the ANQP-DS as a kind of data server. This server stores data related to a user who was previously connected with the LTE network, such as user profile, subscriber identifier, authentication information and etc., for managing the user seamlessly when switching to the WiFi network. As shown in Figure 2, ANQP-DS consists of three elements:

1) User Authentication (U-AUT): The functionality of this element is to store the information on authentication of user from the HSS in LTE network. When UE requests to join the WiFi network for the first time, the U-AUT collects information authentication about it from HSS and the decision of authentication, if the HSS verifies the UE that means Accepted, otherwise Denied This information is identical to that the operator of LTE is using to allow the user to join to the LTE network such as the EAP security mechanisms for user authentication.

2) ANQP: This element is responsible for storing the information related to the network operator and the network capability such as the current capacity of the throughput, the number of users with an individual AP and the vendor information. Furthermore, in our work the UE will enquiry about the network information that stores in this part before choosing an AP to join to the network. We will give more details about ANQP later.

3) P-PCRF: The functionality of this element is to copy the rule of QoS from the LTE network and save to implement in WiFi network zone. When each UE switches to WiFi network it needs to assign an IP address for the current service (maybe the same IP address previously used or a different IP address). Therefore, when the P-GW assigns an IP address for UE in WiFi network, it is also needed to identify the rules policy of QoS for a service. This rules policy copies form the PCRE in LTE to P-PCRF in case of any changes in status network have a negative impact on network performance for the UE services, the AZC will handle the QoS requirements for the UE current service by enquiring from P-PCRF instead of going again to LTE network.

C. Access Network Query Protocol (ANQP)

The ANQP is a protocol enquiring information which helps the network and UE in order to handle the management of selecting AP to connect the UE to the network. This section describes information that the protocol has to query about it to help the UE connect with the suitable access network in the heterogeneous access environment.

1) Venue Name information: This field marks as a venue name for the network, which may be helpful to a user for network selection (e.g., Costa Coffee Shop, Trafford Centre Free WiFi, etc.).

2) Network Authentication Type Information: From this field, if this is an unsecured network (following the legacy hotspot model), in other words, it can identify the additional information are required to connect to the network such as username and password for the hotspot authentication.

3) NAI Realm list: Each AP has Network Access Identifier (NAI) realm profile available through the BSS (and its service providers) and (optionally) the authentication method of each NAI realm supported are different (optionally amended by the list of EAP Method, which are supported by the BSS).

4) 3GPP Cellular Network information: This field identifies the 3GPP cellular networks available through the AP. Specifically, this field identifies the Public Land Mobile Network (PLMN) ID, comprised of the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the mobile operator. When the client is a mobile device with a cellular subscription (containing a SIM or USIM for cellular authentication), the PLMN ID will be used if the Hotspot provides credential authentication with the subscriber's mobile operator.

5) Domain Name list: This field identifies the UE with the home or visited hotspot.

IV. LTE AND WIFI CORE NETWORK INTEGRATION

Figure 3 represents the proposed architecture for LTE and WiFi networks. The top part of Figure shows the components of the LTE EPC and the bottom part of Figure shows the WiFi network. As we can see from the Figure, the P-GW works as a mobility agent. P-GW maintains the IP flow for the UE when it moves from the LTE to WiFi network.

There are many scenarios when the UE moves from the LTE to WiFi networks. In the first scenario, when the network operator wants to offload the data load of the LTE network, it will offload some of the active UEs from the LTE to WiFi, and will be done for the UEs with the non-delay applications, such as FTP files and web pages [16]. In the second scenario, when the UE moves towards from LTE to the WiFi coverage network, the handover will take place in order to switch the UE to the WiFi network. In the first scenario in charge of the whole process, firstly the IPS sends control message to the UE enquiry about the available WiFi APs, then it will choose the best available AP to join within the AZC controlling. While in the second scenario the UE sends a request message to switch to another AP that has enough capacity and best RSS.

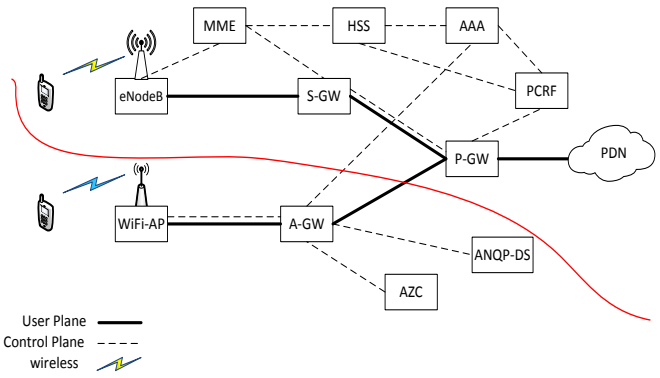

Figure 3. LTE and WiFi network

In this paper we mainly focus on the WiFi network after the UE moves from LTE network to it. We assumed that UE was previously with the LTE network. Firstly, the UE scans for available WiFi APs as shown in Figure 4. For the detected AP the UE will send a request message to connect with it, this message asks the AP to respond with ANQP information, each AP has its own ANQP with AP profile. Then the UE will match an ANQP-UE with an ANQP-AP. If they are not matched, then the UE will search for another AP. Else, UE sends an acknowledge message with the information about authorization to AP. The AP will forward this message to ANQP-DS server for authenticating the UE. One of ANQP-DS servers is to authenticate a UE by applying one of EAP models that the UE use, in our case we apply the same LTE network authentication method. Because UE for the first time joins to WiFi network, the ANQP-DS will ask the Authentication, Authorization and Accounting (AAA) server in the LTE network for authorizing a current UE. If the AAA is not recognized a UE, then it will respond ANQP-DS with a message that the UE is not authorized to join WiFi network and then ANQP-DS sends a reject message to AP in order to forward to UE. On the other hand, if the AAA acknowledges the UE, then AAA aggregates additional information about the UE when it was with LTE network and then will send to ANQP-DS in WiFi network such as the previous PCRF policy service (it is used in case of the UE currently with the same service or application that was within LTE network). As shown in Figure 4, when the AAA sends an accepting message to ANQP-DS, the ANQP-DS will add the UE to the U-Info in AZC, to mark that the UE is authenticated, in the future this UE will not need to be re-authenticated when it moves between WiFi APs in handover process, because the AZC just checks the U-Info for enquiry about the UE authentication status. As a results, it will decrease the delay time for re-authentication of UE in the handover process between APs.

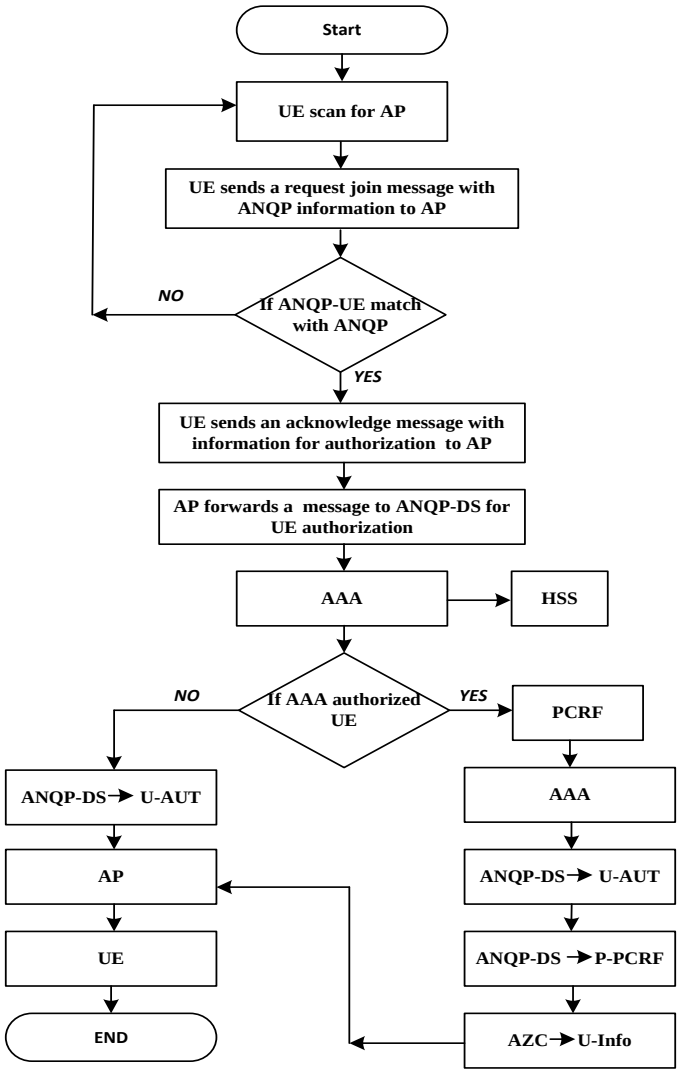

Figure 4: The workflow between LTE and WiFi components

V. PERFORMANCE EVALUATION

This section presents the comparison of performance evaluation of our proposal with existing EAP-AKA standard. The comparison is based on the throughput and authentication delay of UE during the handover procedure.

The simulation parameters in Table I represent the network topology of our simulator. The capacity for uplink and down link in LTE network is 100Mbps and similarly for Wifi network is 54Mbps. All the UEs either connect to LTE or WiFi networks. We assume that the traffic data at each UE is maximum 1Mbps and the maximum number of UEs in LTE without congestion is 25 UEs. From [16] the recommended offloading IP-Flows for applications like Web and FTF are not sensitive to latency. These are called non-delay sensitive applications. Therefore, in our work voice or video traffic will be highly recommended to stick with LTE network because it is very sensitive to latency. Otherwise, the offload will be for IP-Flows with non-delay sensitive applications.

TABLE I: Simulation Parameters

Connection to Internet	1Gbps
LTE Capacity (Uplink / Downlink)	100Mbps
WiFi Network Capacity	54Mbps
Traffic data at each UE	1Mbps per-application

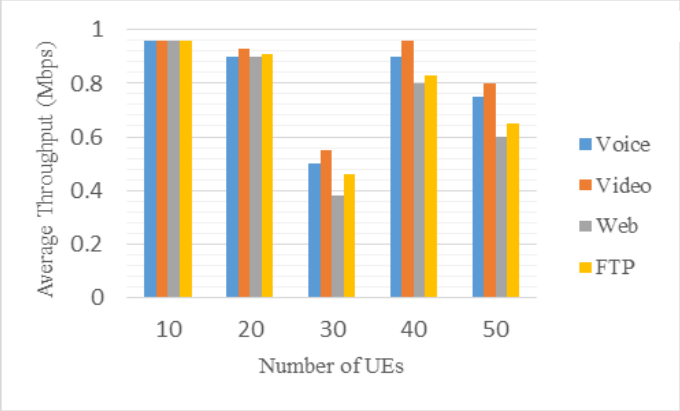

Figure 5: Average Throughput Per-Application

Figure 5 shows the average throughput per-application by UE for various offload values. The throughput is almost the same from 10 up to 20 UEs at 1Mbps per-application. In the scenario of no offload, when the number of UEs increases, the throughput could be decreased sharply, as illustrated at 30 the number of UEs exceeded the threshold value of UEs in LTE causes congestion in the network. On the other hand, when the LTE network is congested, the effectiveness of the offloading increases the average of throughput significantly at 40 UEs. Moreover, when the number of offloading IP-Flows increases from the LTE to WiFi network that may lead to a congestion in the WiFi network, the percentage of offload IP-Flows reached to 45% at 50 UEs.

According to [17] the round trip time messaging of EAP-AKA standard between the WiFi and LTE network is 150ms, which means that our proposal is approximately 79ms. Because, in the EAP-AKA, the UE needs to reach to the AAA server in LTE for verifying a UE each time when it switches AP. While in our proposal the UE just needs to attach the ANQP-DS server for authenticating a UE. If we apply the EAP-AKA in the fast handover, the time needed for UE authentication procedure is 605ms [13], on the other hand in our proposal the time needed for UE authentication is just 330ms. Therefore, our proposal significantly decreases the re–authentication time by 58% as shown in Table II.

TABLE II: Comparison of Authentication Latency

Authentication mechanisms	**Authentication latency (ms)**
EAP-AKA standard	605
Our proposal	330

VI. Conclusion

In this paper, we have proposed a seamless network architecture between LTE and WiFi to offload the overload LTE network, by utilizing the P-GW as an IP flow anchor between LTE and WiFi to maintain a seamless connectivity. We have added two components (i.e., ANQP-DS and AZC) to WiFi core network for managing UE authentication and balancing the load of UEs between APs. As a result of our proposal, we have shown that it can decrease the latency of UE authentication during the handover procedure between LTE and WiFi networks.

References

[1] P. Taylor, “Data overload threatens mobile networks,” BENTON FOUNDATION. [Online]. Available: https://www.benton.org/node/122825.

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

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

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

[5] J. Ling, S. Kanugovi, S. Vasudevan, and A. K. Pramod, “Enhanced capacity and coverage by Wi-Fi LTE integration,” IEEE Commun. Mag., vol. 53, no. 3, pp. 165–171, 2015.

[6] Z. Zhong, P. Kulkarni, F. Cao, Z. Fan, and S. Armour, “Issues and challenges in dense WiFi networks,” IWCMC 2015 - 11th Int. Wirel. Commun. Mob. Comput. Conf., pp. 947–951, 2015.

[7] J. Cao, M. Ma, and H. Li, “An uniform handover authentication between E-UTRAN and Non-3GPP access networks,” IEEE Trans. Wirel. Commun., vol. 11, no. 10, pp. 3644–3650, 2012.

[8] T. Specification, “Etsi ts 124 615,” vol. 0, no. Im, pp. 0–28, 2012.

[9] T. Specification and G. Services, “3Gpp Tr 23.829,” vol. 1, no. Release 10, pp. 1–43, 2011.

[10] Sheets. R, “Local area network,” Pat. No.US5127067, vol. 0, pp. 0–23, 1985.

[11] D. R. Purohith, A. Hegde, and K. M. Sivalingam, “Network architecture supporting seamless flow mobility between LTE and WiFi networks,” Proc. WoWMoM 2015 A World Wirel. Mob. Multimed. Networks, 2015.

[12] M. A. Patino Gonzalez, T. Higashino, and M. Okada, “Radio access considerations for data offloading with multipath TCP in cellular/WiFi networks,” Int. Conf. Inf. Netw., pp. 680–685, 2013.

[13] Y. El Hajjaji El Idrissi, N. Zahid, and M. Jedra, “A new fast re-authentication method for the 3G-WLAN interworking based on EAP-AKA,” 2013 20th Int. Conf. Telecommun. ICT 2013, 2013.

[14] A. Basta, W. Kellerer, M. Hoffmann, H. J. Morper, and K. Hoffmann, “Applying NFV and SDN to LTE mobile core gateways, the functions placement problem,” Proc. 4th Work. All things Cell. Oper. Appl. challenges - AllThingsCellular ’14, pp. 33–38, 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] “Mobile Data Offload – Wi-Fi Offload,” Telecommun. Eng. Cent., vol. 19, no. 3, 2015.

[17] H. Kwon, K. Cheon, K. Rho, and A Park, “USIM based Authentication Test-bed for UMTS-WLAN Handover,” Infocom, pp. 8–10, 2006.