Network architecture supporting seamless flow mobility between LTE and WiFi networks

Dhathri R. Purohith, Aditya Hegde and Krishna M. Sivalingam
Department of Computer Science and Engineering, Indian Institute of Technology Madras, Chennai India
India-UK Advanced Technology Centre of Excellence in Next Generation Networks, Systems and Services (IU-ATC)
prdhathri@gmail.com, hegde.aditya@gmail.com, krishna.sivalingam@gmail.com, skrishnam@iitm.ac.in

***Abstract*—Recently, there has been a tremendous growth in mobile network traffic. Network providers are looking for techniques that selectively offload the mobile data traffic onto WiFi (IEEE 802.11) networks to balance the load and improve network performance. Several architectures based on Proxy Mobile IPv6 (PMIPv6) have been proposed to support seamless data offloading. The demerits of PMIPv6 include lack of flow mobility and single point of failure. There exist architectures that extend PMIPv6 to support flow mobility, but still face the problem of overhead at the gateway and single point of failure. In this paper, we propose Seamless Internetwork Flow Mobility (SIFM), a new architecture that overcomes these drawbacks and provides seamless data offload supporting flow mobility. Both the PMIPv6 and the SIFM architectures have been implemented and evaluated incorporating salient LTE and WiFi network features in the ns-3 simulator. The performance studies validate that seamless mobility can be achieved for clients in both of these architectures. The results show that for the best possible (scenario dependent) offload value, the SIFM architecture shows an improvement of 13.86%, 29.05% and 11.33% whereas the PMIPv6 architecture shows an improvement of 7.96%, 19.52% and 7.83% in terms of delay, packet loss and throughput respectively compared to no offload scenario in each architecture. Further, we also show that the support for flow mobility in the SIFM architecture provides the flexibility to move selective flows to another network. This helps in achieving better performance gain compared to moving all the flows of the user as done in the PMIPv6 architecture.**

I. Introduction

There has been a tremendous growth in the number of mobile devices connecting to the Internet. The network traffic is shifting from text-only data to audio/video data that require high bandwidth. Since the mobile network traffic has increased enormously, Internet Service Providers (ISP) tend to offload some traffic onto other networks to improve performance. IEEE 802.11 (WiFi), a cost effective and widely deployed wireless technology, is the most popular network for traffic offload. Many ISPs such as AT&T and networking companies like Cisco and Qualcomm have studied architectures to offload the 3G/4G traffic to the WiFi [1], [2]. In data offloading, maintaining the user sessions and offloading of selective flows provides the best user experience in addition to balancing the load on the networks.

The main challenge faced in maintaining the user sessions across networks is that connecting to a different network changes the IP address of the user, resulting in loss of the IP session. This is because the IP address acts as a locator and an identifier at the same time. On the other hand, seamless user session mobility expects the locator and the identifier properties of the IP to be decoupled which is achieved by IP mobility. Thus, to facilitate seamless data offload, we require the network to efficiently support IP mobility.

IP mobility provides an option to move either all or no flows of a given user across the networks. To better balance the load, we need an option to move selective flows of a given user, i.e. to enable *flow mobility*. Flow mobility provides the user with the flexibility of choosing the most suitable network for a given application. For example, consider a user on a heavily loaded LTE network who is watching a video and also downloading a file. Moving the video traffic to WiFi is not good since it increases the delay and thus QoS constraints cannot be met. Instead, only the file download can be moved to the WiFi network. If some other user is running a non-delay sensitive application, then only such flows can be moved to better balance the load on the network. This level of freedom in choosing the flows to be moved across the networks cannot be provided only by IP mobility. Thus, flow mobility becomes important in achieving a better distribution of load on the networks along with providing better quality of experience to the users.

There exist various protocol standards for providing IP mobility, namely, Mobile IP (MIP) [3], Dual Stack Mobile IP (DSMIPv6) [4] and Proxy Mobile IPv6 (PMIPv6) [5]. Proxy Mobile IPv6 is a Network-Based Localized Mobility Management Solution (NetLMM) [6]. MIP and DSMIPv6 are host based protocols where the user initiates the mobility and hence require significant changes on the mobile node. In PMIPv6, all the mobility related implementations are done at the network and do not require many changes at the mobile node. The 3GPP standard TS 23.261 v12.0.0 [7] proposes a DSMIPv6 based interface for IP flow mobility (IFOM) and seamless Wireless Local Area Network (WLAN) offload. The 3GPP standard TS 24.327 v12.0.0 [8] describes General Packet Radio System (GPRS) and WLAN internetworking aspects. The 3GPP TS standard 23.402 v13.1.0 [9] proposes architecture enhancements for non 3GPP access. The specification defines interfaces to support network based mobility using PMIPv6.

This paper proposes a novel architecture named Seamless Internetwork Flow Mobility (SIFM), that overcomes the

978-1-4799-8461-9/15/$31.00 © 2015 IEEE

drawbacks of existing architectures by utilizing the concepts of PMIPv6 and Software Defined Networking (SDN) [10]. The SDN architecture is based on decoupling the data plane from the control plane. It introduces two components, namely Controller and Switches. The controller and the switch communicate using the OpenFlow [11] protocol. When a switch receives a packet it has never seen before, it forwards it to the controller. The controller takes the routing decision, and instructs the switch on how to forward similar packets by adding entries in the switch's flow table.

The proposed SIFM architecture defines a Flow Controller (FC) similar to an OpenFlow controller [11]. The FC only carries out the mobility related functionality. The Packet Data Network Gateway (PGW) in the LTE network and the Wireless Access Gateway (WAG) in the WiFi network act as OpenFlow-hybrid switches [11] that carry out mobility related signalling on behalf of the User Equipment (UE). They follow the instructions of the FC when a mobile node moves from an LTE network to a WiFi network in order to provide seamless transition.

The SIFM architecture and the PMIPv6 architecture have been implemented in the ns-3 simulator specifically for studying data offloading between the LTE and the WiFi networks. These architectures can be used for traffic offloading between any two access technologies such as 2G and 3G by implementing the functionalities required for seamless mobility at the corresponding entities defined in the respective standards. For the SIFM architecture, the entities that perform the functionality of the MAG must be OpenFlow complaint in order to communicate with the FC. Performance studies show that with the best possible (scenario dependent) offload value, both SIFM and PMIPv6 architectures improve performance when offloading the data compared to the no offload scenario.

We also show that selective offloading helps in achieving better performance gain by considering a simple scenario and using static flow table rules. Mechanisms that dynamically determine flow table rules play an important role in achieving better performance. The 3GPP standard TS 24.312 v12.8.0 [12] defines Access Network Discovery and Selection Function (ANDSF) to assist the UE to discover non-3GPP access networks and provide the UE with rules policing the connection to these networks. Dynamic modification of flow table rules based on the data provided by ANDSF on the current network conditions are a part of our future work and are not presented in this paper.

II. Related Work

3GPP Release 8 [7], proposed an architecture for seamless mobility between 3G and WiFi networks based on DSMIPv6 [4]. The solution does not require any support from WLAN accesses. The changes are required only at the UE and the PGW. The Home Agent functionality as defined in [3] can be implemented in the PGW or as a stand alone box. The S2c interface is defined between the UE and the PGW for all the DSMIPv6 related communications. Cisco [1] and Qualcomm [2] have proposed architectures based on DSMIPv6 for mobility between the 3GPP and the non-3GPP (WiFi) networks. This approach requires significant changes at the UE since UE initiates the binding related communications, which is the major drawback of the approach.

In UE-initiated procedures, mobile nodes must signal themselves to the network when their location changes and must update routing states in the Foreign Agent, in the local Home Agent, or in both. This requires changes to the UE stack, and also raises the problem of complex security configurations to authenticate the signalling exchanges and modifications of routing states. Therefore, the Internet Engineering Task Force (IETF) defined a network-based local mobility management protocol, where local IP mobility is handled without any involvement from the mobile node. As a part of the first phase of efforts in this working group, Proxy Mobile IPv6 (PMIPv6) [5], a network-based local mobility management protocol was developed.

PMIPv6 mainly defines two components to achieve network-based local mobility management namely the Local Mobility Anchor (LMA) and the Mobile Access Gateway (MAG). The MAG performs the mobility related signalling on behalf of the mobile nodes. The LMA keeps track of the users and issues the same IP address to the users when they move across different networks. The LMA and the MAG communicate over the tunnel that is established between the two. Fig. 1 shows the PMIPv6 architecture.

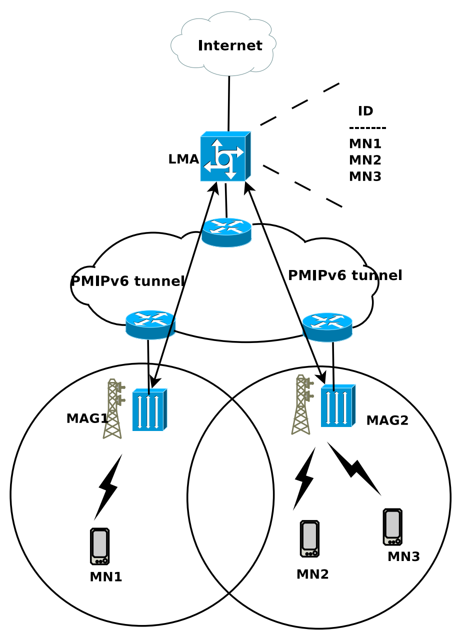

Fig. 1: PMIPv6 architecture

3GPP release 8 [9] defines the S2a interface based on the PMIPv6 architecture between the PGW and the Wireless Access Gateway (WAG) for mobility between the 3GPP networks (e.g., LTE) and the non-3GPP networks (e.g., WiFi). Cisco has proposed an architecture for mobility between the 3GPP and the non-3GPP networks based on PMIPv6 [1].

PMIPv6 solves the problem of user session mobility but does not provide the flexibility to move selected flows of a user. Various architectures adding flow mobility support to PMIPv6 have been proposed in [13] and [14]. In all these architectures, LMA still remains a single point of failure. Architectures using PMIPv6 for mobility between the LTE and the WiFi networks can implement LMA functionality at the PGW or in a separate box placed in the LTE core network. If LMA functionality is implemented at the PGW, it increases the complexity of the PGW. If LMA is implemented as a separate entity, then there is an extra tunnelling overhead between the LMA and the PGW. A unified protocol stack that includes all the original functions of both LTE and WLAN systems is proposed in [15]. An SDN [10] based RAN architecture that provides higher programmability and an easier vertical handover process is proposed in [16]. However, this poses scalability issues. To overcome these problems, we propose a new architecture called SIFM that takes the best of both PMIPv6 and SDN based architectures.

III. Seamless Internetwork Flow Mobility (SIFM)

This section presents the design, the components and the working of the proposed Seamless Internetwork Flow Mobility (SIFM) architecture.

In this paper, we define a flow as having five attributes: the source and the destination IP address, the source and the destination port and the transport protocol used. A set of packets with common attribute values within a given time period is considered as one flow. The definition of flows can be extended as needed.

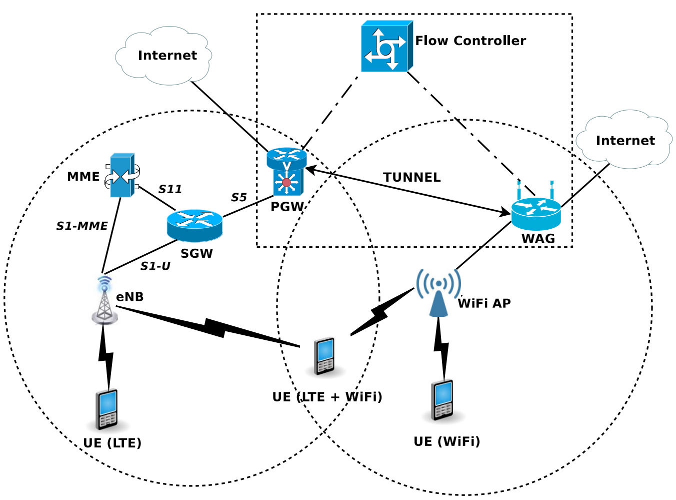

Fig. 2: SIFM architecture for LTE and WiFi networks.

A. Architectural Design

Fig. 2 represents the SIFM architecture for LTE and WiFi networks. The left part of the figure shows the components of the LTE Evolved Packet Core (EPC) and the right part of the figure shows the WiFi network. The main components of SIFM are: (i) Flow Controller (FC); (ii) Mobility Agents (MA); and (iii) User Equipment (UE). In Fig. 2, the EPC Packet Gateway (PGW) and the Wireless Access Gateway (WAG) act as the MAs. They connect the UE to the Internet and also communicate with the FC. Based on the flow instructions given by the FC, the mobile data flow either takes the path along the LTE network or is offloaded through the tunnel between the PGW and the WAG to reach the UE through the WiFi network.

We choose to implement the new functionality of mobility using a concept similar to that of SDN in the SIFM architecture. Since the Flow Controller is centralized, it has the complete view of both LTE and WiFi networks. Hence, better algorithms can be developed to dynamically move the flows between LTE and WiFi networks based on the current network conditions, user's charging profile, priorities etc. Problems related to scalability in SDN will not pose much issues in the SIFM architecture, since mobility is considered only in a local domain. The SIFM architecture is easy to integrate since it does not require major changes to the existing architecture, unlike PMIPv6. This can serve as an intermediate step to move cellular networks towards SDN based architectures. It is assumed that if a user requests mobility as a feature, then the LTE operators providing the feature will have a service level agreement with the other WiFi operators and hence there is a network infrastructure between the two to move the flows. Authentication between the two networks is an important aspect in data offloading: it is a problem on its own and is not discussed in this paper. The 3GPP standard TS 24.234 v12.2.0 [17] proposes EAP SIM and EAP AKA based authentication mechanisms that can be used for authentication.

1) Flow Controller: The Flow Controller (FC) is responsible for assigning flows to the MAs. The FC is a new component defined in the SIFM architecture and has to be added to the current LTE EPC in order to facilitate flow mobility. The FC works similar to an OpenFlow controller [11] but only performs the flow mobility related actions in this architecture. It is aware of all the MAs to which the UE is connected to and as to which of them are active. Based on the information obtained from the MAs, the FC sets up the flow rules and communicates the same to the MAs. When a UE moves from one network to another, the FC instructs the MAs involved to create a tunnel through which active connections are transmitted to the UE without any disruption.

2) Mobility Agents: The Mobility Agent (MA) is a router that provides Internet services to the UE and is responsible for detecting the movement of the UE between the access technologies (e.g., LTE and WiFi). The MA's functionality is similar to that of the MAG in PMIPv6 [5]. In the OpenFlow context, it behaves similar to an OpenFlow-hybrid switch [11]. Whenever a UE comes within a MA's access network, the MA assigns an IP address to the UE and informs the FC about its binding. The MA gets the flow information from the FC and forwards the data packets based on the obtained information. The MA can provide more information about the UE's binding such as access technology, link bandwidth information, packet and port statistics to the FC. Based on these information, the FC can run several algorithms to assign flows between the MAs. Only Control Messages are exchanged between the MAs and the FC. There is no actual data transfer between the two. A messaging protocol, similar to OpenFlow, is used to communicate between the FC and the MAs. In the current infrastructure, functionality of the MA is added at the PGW for the LTE and at the WAG for the WiFi network.

3) User Equipment: The UE is a user or a mobile node (MN) that requests for the service. User, UE and MN mean the same and are used interchangeably in this paper. Since the SIFM architecture supports flow mobility, the UE should be able to receive packets destined to multiple IP addresses at the same time. Also, the IP address cannot be bound to a network interface, in case of the flows which are being moved from LTE to WiFi or vice-versa. To support this, either the UE should support a weak host model [18] or have a logical interface [19]. The logical interface abstracts the underlying physical interfaces called the sub-interfaces and may be attached to multiple access technologies (e.g., LTE and WiFi). Only the logical interface is exposed to the higher layers at the UE and the physical interfaces are hidden. The Transmit/Receive functions of the logical interface are mapped to the Transmit/Receive services exposed by the sub-interfaces. This mapping is dynamic and any change is not visible to the upper layers of the IP stack. Android supports the weak host model, while Windows does not.

B. Data Structures

Two main data structures are defined to support SIFM, as described below: Binding Cache (BC) at the FC and Flow Table (FT) at the MA.

1) Binding Cache (BC): The binding cache (BC) is maintained at the FC and contains the information about all the UEs and the MAs to which they are attached to. Every BC entry contains:

- *MN-ID:* Identifies the Mobile Node uniquely.
- *MA-ID:* Identifies the Mobility Agent uniquely.
- *MN-IP:* IP Address of the Mobile Node within MA's network.
- *MA-IP:* IP Address of the Mobility Agent. This is the tunnel address which is used to communicate with other MAs.
- *PORT-ID:* Physical/Logical port on which the packets destined to the MN are forwarded at the MA.
- *STATUS:* Status of the UE in a MA's network.

2) Flow Table (FT): The Flow Table (FT) is maintained at the MAs and reflects the flow decisions taken by the FC. Entries of the FT determine the path taken by the flow received at the MA. Each FT entry contains:

- *Match-fields:* Fields of the packet header to match against the incoming packets. It might be an ingress port, source/destination IP etc.
- *Priority:* Matching precedence of the flow entry.
- *Counters:* Updated when the packets are matched.
- *Instructions:* Actions to be performed by the MA on the packets matched.
- *Timeout:* Idle time before a flow is expired by the switch.

C. Message Formats

Communication between the FC and the MAs uses messages that comply with the OpenFlow Protocol. Two new message types that follow the experimenter message type as specified in [11] are introduced. The Flow Modification Message and the Port Status update Message defined in OpenFlow are used to meet our requirements.

1) Binding Update: A Binding Update is sent from a MA to the FC when the MA receives a connection request from the UE. The Binding Update message contains MN-ID, MA-ID, MN-IP, MA-IP, PORT-ID and STATUS. MA-IP is the tunnel IP of the MA which is used to communicate with the other MAs. On receiving the Binding Update message, the FC updates its BC and sends a Binding Ack.

2) Binding Ack: On receiving the Binding Update, the FC sends a Binding Ack to the MA to acknowledge the reception of the Binding Update. In addition to this, if the FC already has a BC entry for the UE, it sends the information about the IP of the UE corresponding to the old MA, to the new MA. This is required by the new MA to map the flows corresponding to the old IP, to the new IP.

3) Flow Modification Message: A Flow Modification Message is sent from the FC to a MA to inform the MA about all the flow mobility related decisions taken by the FC. The Flow Modification Message mainly contains information about the match fields which is used to match the incoming flow at the MA and the instructions which define the actions to be performed on the matched flows. In addition to this, it also contains auxiliary fields such as priority and timeout values. On receiving the Flow Modification Message, the MA updates its Flow Table.

4) Port Status Update: The Port Status Update is sent from a MA to the FC to inform the FC about any change in the UE's port status with respect to the MA. It contains MN-ID, MA-ID, PORT-ID and STATUS. On receiving the Port Status Update, the FC updates the status of the port as per the received message in the appropriate BC entry.

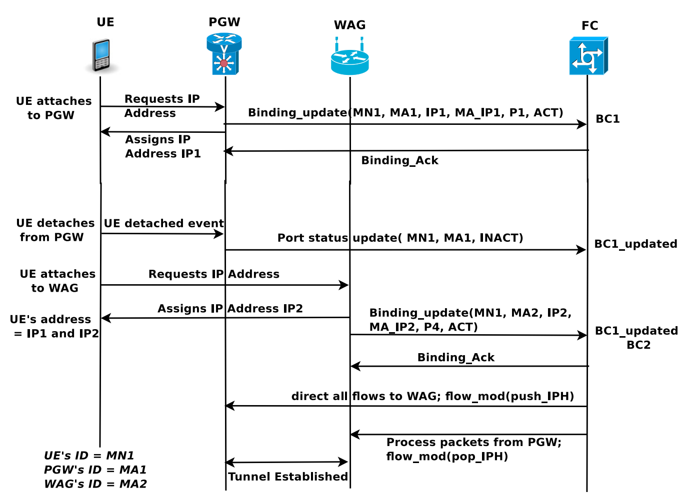

Fig. 3: SIFM architecture operation details.

D. Protocol Operation

Fig. 3 explains the working of the SIFM architecture with the LTE and the WiFi networks. The steps are detailed below.

1) The UE connects to the LTE network. The PGW receives the connection request, assigns an IP to the UE, sets up default bearers and sends the Binding Update to the FC. The FC responds with a Binding Ack.
2) After sometime, the UE disconnects from the LTE network. The PGW, on detecting the movement of the UE, sends a Port Status Update to the FC. The FC updates the BC entry as inactive.
3) When the UE comes in the range of a WiFi network, the WAG receives a connection request from the UE. The WAG assigns a new IP to the UE and sends a binding update to the FC. Both the IP addresses are now configured on the UE's logical interface.
4) Since the FC already has an entry corresponding to the UE, it makes a new entry for the WAG and sends a Binding Ack to the WAG. The FC also sends Flow Modification Messages to the PGW and the WAG based on its decision.
5) In case of complete handover, the FC instructs the PGW to move all the existing flows corresponding to the UE over the tunnel. It also instructs the WAG to decapsulate the packets received on the tunnel from the PGW and forward it to the UE on the appropriate port. The new connections from the UE are established over the new network (i.e, WiFi in this case), there by reducing the tunnelling overhead.
6) In case of dual network connectivity, the FC can run several algorithms based on the link bandwidth information, packet and port statistics, etc. and assign flows between the PGW and the WAG based on the algorithm's output. Algorithms should be aimed at balancing the load on both the networks and provide better quality of experience to the user.

The support for flow mobility in SIFM architecture is the main advantage over other architectures. The data provided by ANDSF [12] can be used to develop algorithms that run in the FC of the SIFM architecture to dynamically determine when a handover should occur and which flows can be moved based on the current network conditions.

IV. Performance Study

This section explains the implementation, topology and the network parameters used to evaluate the PMIPv6 and the SIFM architectures for LTE and WiFi networks. Comparative analysis of the metrics for both the architectures are presented.

The PMIPv6 based architecture and the SIFM based architecture for LTE-WiFi network mobility have been implemented in the ns-3 network simulator [20] (version 3.20). The ns-3 network simulator does not support IPv6 with LTE. To implement PMIPv6, we have extended the LTE module of the simulator (LENA) to support IPv6. PMIPv6 messages i.e, proxy binding updates and acknowledgements are implemented as per RFC 5213 [5]. LMA is implemented as a different node which is connected to PGW/SGW node and WAG by point-to-point links. Communication between the LMA and the access gateways happen via PMIPv6 tunnel that is established at the start of the simulation.

To implement the SIFM architecture for LTE and WiFi networks, we have added a new module to ns-3 simulator called "openflow-hybrid". This implements the functionalities of the FC, OpenFlow-hybrid switch [11] and the messaging between the FC and the MA. The PGW/SGW and the WAG are modified to support the MA functionalities. To support the logical interface at the UE, a new UeLogicalNetDevice class that abstracts the LTE and the WiFi interfaces at the UE is implemented.

A. Network Topology and Simulation Parameters

The network topology for PMIPv6 architecture is as shown in Fig. 4. Both the PGW and the WAG (MAGs) are connected to LMA via a point-to-point link and communicate over the PMIPv6 tunnel. The LMA is connected to the Remote Host.

The network topology for the SIFM architecture is as shown in Fig. 5. In the SIFM architecture, both the PGW and the WAG are directly connected to the Internet. The PGW and the WAG (MAs) are connected to the FC via a point-to-point link and a TCP connection is established between the FC and the MAs for all mobility related communications. A simple IP-in-IP tunnel is established between the PGW and the WAG to offload the traffic. In all our simulations, we create the tunnel proactively at the start of the simulation. This can also be dynamically created (reactive approach) when there is a need to offload. But this approach is not considered since it might increase the overhead of the handover process.

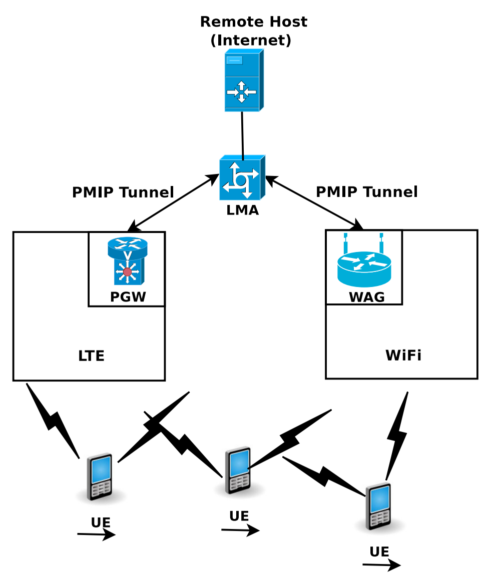

Fig. 4: Network topology for PMIPv6 architecture.

The network parameters used for the simulation are summarized in Table I. The effective capacity of LTE downlink and uplink is ≈ 71 Mbps and that of WiFi network is ≈ 22 Mbps due to signalling overhead. Multiple UEs are connected

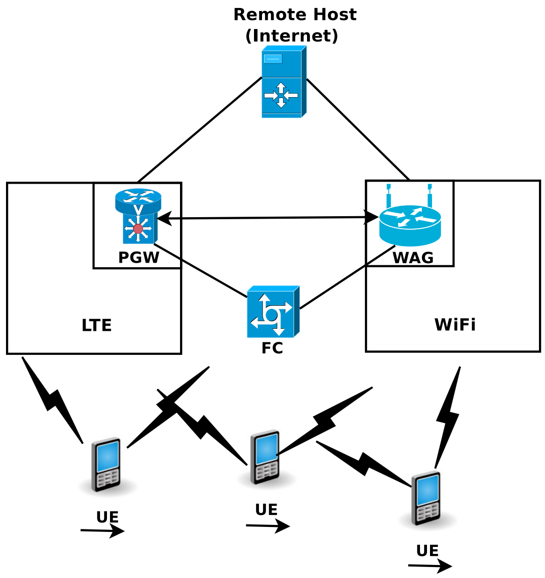

Fig. 5: Network topology for SIFM architecture.

to either the LTE or the WiFi Network. We consider a single eNB to which all the UEs are connected. Both TCP and UDP traffic are running between every UE and the remote host. The details of the traffic are as given in Table I. Some of the UEs are static and others are mobile as determined by the offload value specified in the simulation. The arrow indicates the direction of movement of the UEs. Initially, all the UEs are in the range of the LTE Network. The UEs that are mobile will move towards the WiFi network and their flows are offloaded when they get connected to the WiFi network. The speed of the UE is 1 m/s (1.8 Kmph). A lower speed is considered since WiFi offloading helps only when users are less mobile. In other words, UEs are expected to be connected to WiFi for a sufficient period of time such as at home, at coffee shops, or in the office. The delay, the throughput and the packet loss values are calculated for different offload percentages by varying the number of UEs.

TABLE I: Simulation Parameters

BandWidth of Link Connecting to Internet	1Gbps
LTE Downlink Capacity	100Mbps
LTE Uplink Capacity	100Mbps
Scheduler Used at LTE	Round Robin
WiFi Network Capacity	54Mbps (802.11 a)
No. of users	varies from 10 to 50
Offload value	varies from 0% to 30% of the total traffic
Traffic at each UE	1 UDP app, 1Mbps, CBR 1 TCP app, 1Mbps, CBR

B. Performance Evaluation Results

This section presents a comparative analysis of the metrics such as delay, throughput and packet loss rate for the SIFM architecture and the PMIPv6 architecture considering different offload values.

Fig. 6 shows the average delay experienced by a UE for different offload values for both the architectures. This includes the average delay of both TCP and UDP flows. It can be seen that up to 30 users, LTE successfully handles the load since the total capacity of the LTE eNB is approx. 71 Mbps and the total downlink traffic is 60 Mbps for 30 users. When the number of UEs is further increased, the LTE network experiences congestion and hence the delay increases for the no-offload scenario. For 40 users, offloading up to 30% and for 50 users offloading up to 20% reduces the delay compared to no offload scenario. Further increase in the offload increases the delay since the WiFi network will start to experience congestion. The graph also shows that offloading the traffic when the LTE network is not congested increases the average delay. This is because of the handover delay overhead and congestion at the WiFi network that has a lower capacity, as considered here. As IEEE 802.11ac networks with around 1 Gbps become more prevalent, these values would change.

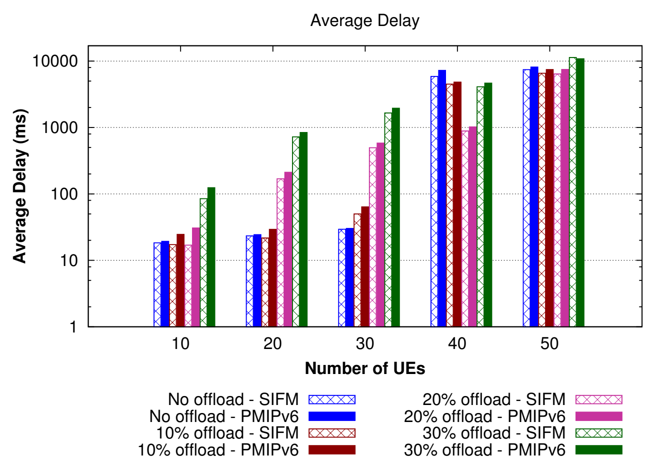

Fig. 6: Delay comparison for SIFM and PMIPv6 architecture

Fig. 7 shows the average per application throughput experienced by a UE for different offload values for both the architectures. It can be seen that the throughput is almost equal to the requested bandwidth (i.e, 1Mbps/application) up to 30 users. Further increase in the number of users decreases the throughput drastically for the no-offload scenario. Offloading the traffic for higher number of users, i.e. when the LTE network is congested, increases the average throughput. Offloading when resources are available at the LTE network and with very high offloads (e.g., 30%), decreases the throughput due to congestion at the WiFi network.

Fig. 8 shows the average packet loss rate per UE for different offload values for both the architectures. When the LTE network gets congested i.e, for 40 and 50 users, the packet loss rate increases for the no offload scenario. Offloading will reduce the packet loss rate when the number of users is more than 30. Apart from the bandwidth constraints, the handover process also contributes to the packet loss rate. Hence, offloading when the network is not congested, i.e, less than 30 users results in a certain amount of packet loss. For

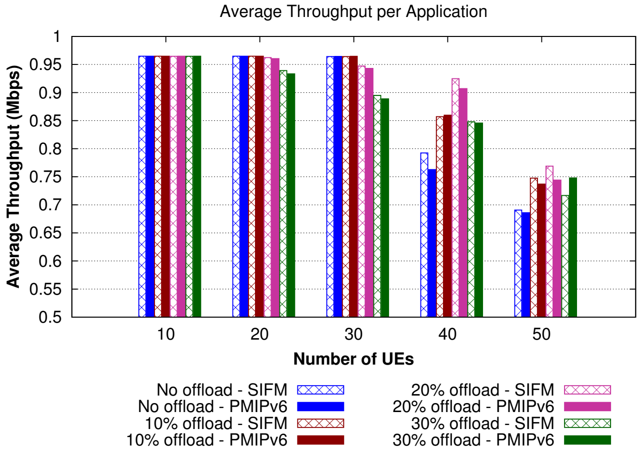

Fig. 7: Throughput comparison for SIFM and PMIPv6 architecture

example, for 20 users and 30% offload case, though there is no congestion in both the networks, packet loss is there due to the handover process.

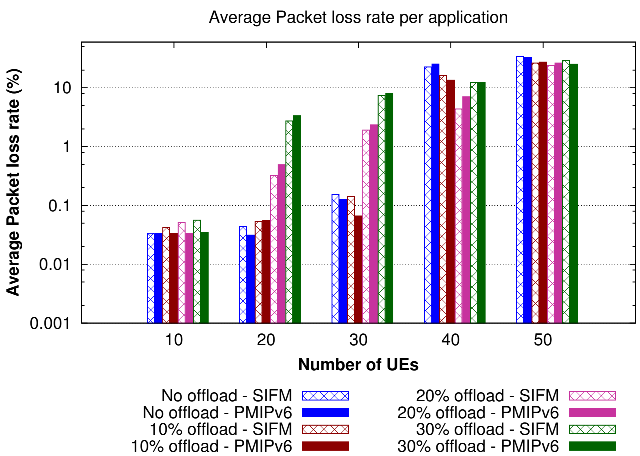

Fig. 8: Packet loss comparison for SIFM and PMIPv6 architecture

For the simulation parameters considered, the total request from all the users is 100 Mbps, LTE network capacity is approx. 71Mbps and WiFi network capacity is approx. 22 Mbps (out of the 54 Mbps channel capacity) due to signalling overhead. The best possible offload value in this scenario is 20% offload for 50 users, which offloads 20Mbps traffic to WiFi. In this case, the SIFM architecture achieves a better gain of 13.86% in terms of delay compared to the gain of 7.96% achieved by the PMIPv6 architecture. This is because of the tunnelling overhead between the LMA and the PGW in the PMIPv6 architecture. The delay with no offload increases in PMIPv6 architecture as shown in Fig. 6 and hence the gain decreases. In terms of throughput and packet loss rate, SIFM achieves a gain of 29.05% and 11.33% where as PMIPv6 achieves a gain of 19.52% and 7.83% respectively.

The average handover (HO) delay for a flow that is moved between the LTE and the WiFi network is shown in Table II. PMIPv6 has a slightly higher handover delay. This is due to the fact that when a UE moves to a different MAG, the IP address configuration takes time since the MAG has to consult the LMA before sending the Router Advertisement.

TABLE II: Handover Delay

No.of flows offloaded	Avg. HO Delay with SIFM (in s)	Avg. HO Delay with PMIPv6 (in s)
5	0.398	0.544
10	0.405	0.552
15	0.418	0.559
20	0.431	0.559
25	0.453	0.560

The main advantage of the SIFM architecture over the PMIPv6 architecture is flow mobility support. Flow mobility is useful when the user is connected to both the networks at the same time. To demonstrate the advantages of flow mobility, we consider the same topology as in Fig. 4 and Fig. 5 but static UEs. All the UEs are connected to both LTE and WiFi networks at the same time. We consider 3 kinds of offloads.

- *Full Mobility*: All the flows of a user is moved.
- *TCP offload*: Only TCP flows of a user is moved.
- *UDP offload*: Only UDP flows of a user is moved.

For example, for the scenario of 20% offload for 50 users, we move both TCP and UDP flows of 10 users in Full Mobility, only TCP flows of 20 users in the TCP offload and only UDP flows of 20 users in the UDP offload scenario. Since PMIPv6 architecture only supports Full Mobility, Full Mobility scenario of PMIPv6 is compared with the TCP offload and the UDP offload scenarios of the SIFM architecture for 20% and 30% offload values. Full Mobility scenario for the SIFM architecture is not shown in the following graphs since the values closely follow the full mobility scenario of the PMIPv6 architecture as shown in Fig. 6, Fig. 7 and Fig. 8.

Fig. 9 shows that the average delay for TCP applications decreases when only UDP flows are moved. This is because the load on the LTE network is reduced and the TCP applications do not experience the handover delay as in the case of full mobility scenario. However, in case of TCP only offload, the average delay for TCP applications increases as compared to full mobility scenario due to handover delay overhead. For similar reasons, the average delay for UDP applications decreases when only TCP flows are offloaded and increases when only UDP flows are offloaded as shown in Fig. 10.

Fig. 11 shows that the average throughput for TCP applications increases when only UDP flows are moved. This is because the load on the LTE network is reduced and the available bandwidth for TCP applications increases. However, in case of TCP only offload, the average throughput for TCP applications decreases with increase in the number of users and offload value due to congestion at the WiFi network. Similarly, as shown in Fig. 10, the average throughput for UDP applications increases when only TCP flows are offloaded

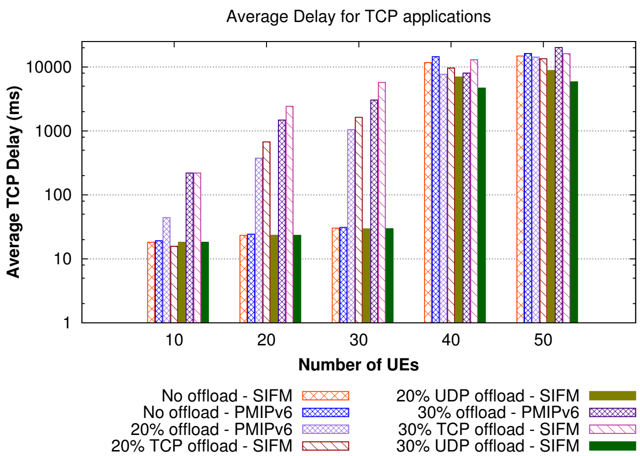

Fig. 9: TCP delay comparison - with and without flow mobility

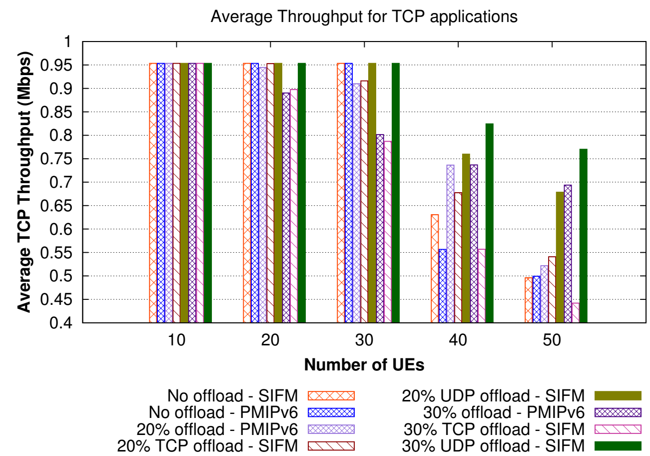

Fig. 11: TCP throughput comparison - with and without flow mobility

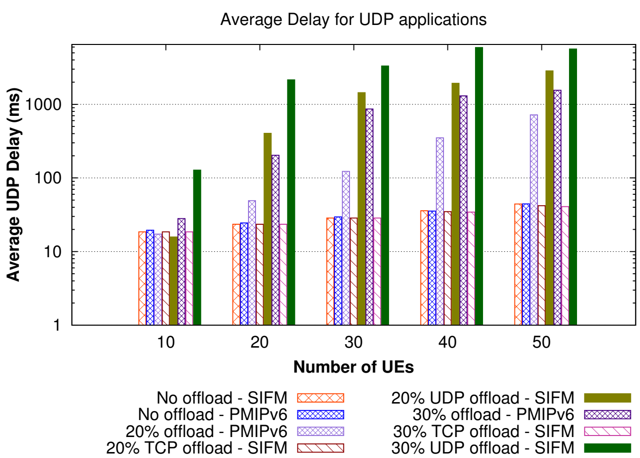

Fig. 10: UDP delay comparison - with and without flow mobility

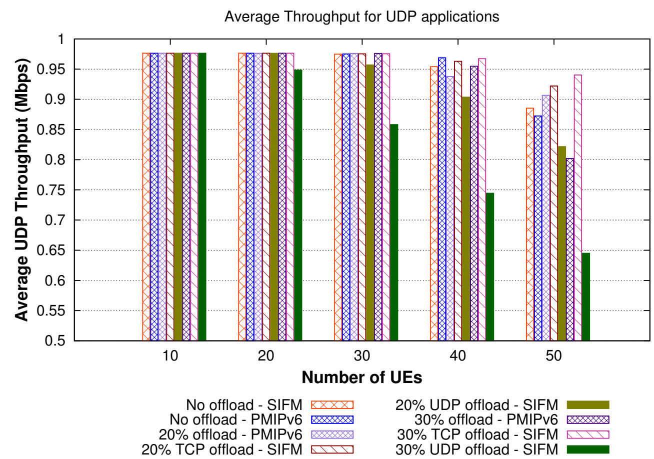

Fig. 12: UDP throughput comparison - with and without flow mobility

due to lower load on the LTE network. The average UDP throughput decreases with increase in the number of users and offload value due to congestion at the WiFi network. In 50 users, 30% TCP offload scenario, WiFi network is overloaded with TCP traffic. Due to re-transmissions of TCP, the congestion is increased and the throughput of TCP traffic is very low. With UDP traffic, even though the throughput decreases, it is not as much affected as TCP traffic.

Fig. 13 shows that the average packet loss rate for TCP applications decreases with UDP only offload compared to the full mobility scenario. This is because the TCP traffic does not experience the handover loss in UDP only offload and also the traffic on the LTE network is reduced. However, in case of TCP only offload, the average packet loss rate for TCP applications is slightly higher compared to full mobility when the number of users are high and for higher offload values. This is due to handover loss and congestion at the WiFi network. The average packet loss rate for UDP applications decreases when only TCP flows are offloaded since UDP flows do not undergo handover loss and the load on the LTE network is reduced as shown in Fig. 14. However, the packet loss rate for UDP applications increases when only UDP flows are offloaded. This loss can be attributed to the handover loss experienced by the UDP traffic and also due to congestion at the WiFi network when the offload value is high for higher number of users.

The experiments show that flow mobility provides more flexibility in offloading the traffic. For example, flows can be given priorities and offloaded based on the priorities. If one user is hogging the network, then only high priority flows of the user can be retained and other flows can be offloaded. In the experiments conducted, if we consider the UDP flows as high priority, then the results show that retaining the UDP flows and offloading only the TCP flows will improve the overall performance of the UDP traffic compared to the complete offload scenario. Similarly, if the TCP traffic is given

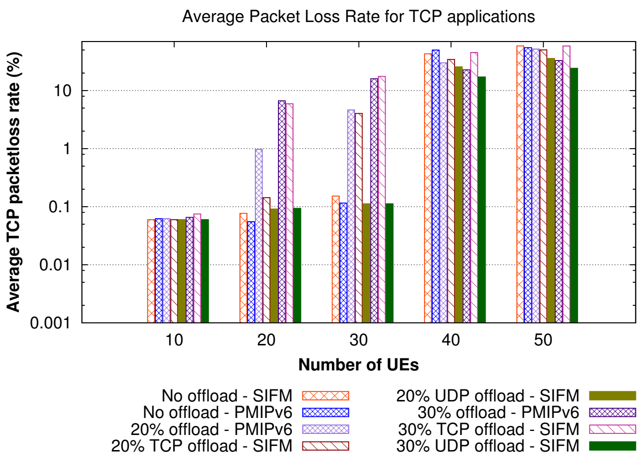

Fig. 13: TCP packet loss comparison - with and without flow mobility

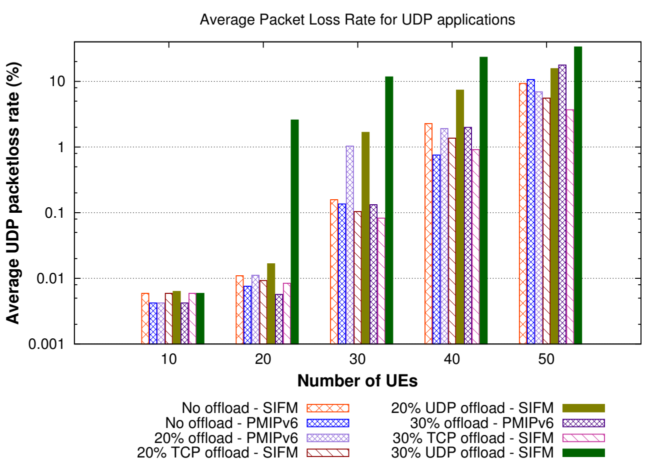

Fig. 14: UDP packet loss comparison - with and without flow mobility

high priority, then offloading only the UDP traffic will improve the performance of the TCP applications. Using algorithms for dynamic flow modification based on user and flow priorities and the current network state, additional performance gain can be achieved.

Only control packets flow between the FC and the MA in the SIFM architecture reducing the chance of failure of the FC. The FC is no more a single point of failure because only the mobility related functionality is affected when the FC fails. Failure of the FC does not have any impact on the functionalities of LTE and WiFi as stand alone networks. Only existing flows pass through the tunnel between the MAs, and the new connections are established over the network to which the UE is currently attached to. Thus, the load on the tunnel is reduced.

V. Conclusions

In this paper, we present a new architecture called Seamless Internetwork Flow Mobility (SIFM) for the network based flow mobility and seamless data offload. The SIFM architecture and the PMIPv6 architecture have been implemented and evaluated for data offloading between the LTE and the WiFi networks. The evaluation results show that the delay, the throughput and the packet loss values are improved by 13.86%, 29.05% and 11.33% respectively for the SIFM architecture and by 7.96%, 19.52% and 7.83% respectively for the PMIPv6 architecture for the best possible (scenario dependent) offload value compared to the no offload scenario. The advantage of flow mobility support with the SIFM architecture over the PMIPv6 architecture is demonstrated for an example network scenario. It is shown that the flow mobility support in the SIFM architecture provides the flexibility to move selective flows which helps in achieving better performance gain compared to moving all the flows of the user as in PMIPv6 architecture. In future work, mechanisms for determining when to switch from LTE to WiFi and dynamically modifying the flow table rules based on the flow priority and current network state can be studied.

References

[1] "Architecture for Mobile Data Offload over Wi-Fi Access Networks," http://www.cisco.com/c/en/us/solutions/collateral/service-provider/service-provider-wi-fi/white_paper_c11-701018.html, Mar. 2014.

[2] "3G LTE Wifi Offload Framework," http://www.qualcomm.com/media/documents/3g-lte-wifi-offload-framework, Mar. 2014.

[3] D. Johnson, C. Perkins, and J. Arkko, "RFC 3775: Mobility Support in IPv6," Jun. 2004.

[4] H. Soliman, "RFC 5555: Mobile IPv6 Support for Dual Stack Hosts and Routers," Jun. 2009.

[5] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "RFC 5213: Proxy Mobile IPv6," Aug. 2008.

[6] J. Kempf, "RFC 4830: Problem Statement for Network-Based Localized Mobility Management (NETLMM)," Apr. 2011.

[7] "3GPP TS 23.261," http://www.3gpp.org/DynaReport/23261.htm.

[8] "3GPP TS 24.327," http://www.3gpp.org/dynareport/24327.htm.

[9] "3GPP TS 23.402," http://www.3gpp.org/DynaReport/23402.htm.

[10] "Software Defined Networks," https://www.opennetworking.org/sdn-resources/sdn-definition, Mar. 2014.

[11] "OpenFlow Specification," https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.4.0.pdf, Oct. 2013.

[12] "3GPP TS 24.312," http://www.3gpp.org/dynareport/24312.htm.

[13] H.-Y. Choi, S.-G. Min, and Y.-H. Han, "Pmipv6-based flow mobility simulation in ns-3," in *5th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, Jun. 2011, pp. 475–480.

[14] T. M. Trung, Y.-H. Han, H.-Y. Choi, and H. Y. Geun, "A design of network-based flow mobility based on Proxy Mobile IPv6," in *3rd IEEE International Workshop on Mobility Management in the Networks of the Future World (INFOCOM WKSHPS)*, Apr. 2011, pp. 373–378.

[15] Q. Cui, Y. Shi, X. Tao, P. Zhang, R. Liu, N. Chen, J. Hamalainen, and A. Dowhuszko, "A unified protocol stack solution for LTE and WLAN in future mobile converged networks," *Wireless Communications, IEEE*, vol. 21, no. 6, pp. 24–33, Dec 2014.

[16] M. Yang, Y. Li, D. Jin, L. Su, S. Ma, and L. Zeng, "OpenRAN: a software-defined ran architecture via virtualization," in *Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM*, Aug. 2013, pp. 549–550.

[17] "3GPP TS 24.234," http://www.3gpp.org/dynareport/24327.htm.

[18] "Host Model," http://en.wikipedia.org/wiki/Host_model, Nov. 2013.

[19] T. Melia and S. Gundavelli, "Logical interface support for multi-mode ip hosts," http://tools.ietf.org/html/draft-ietf-netext-logical-interface-support-09, Mar. 2014.

[20] "ns-3," http://www.nsnam.org/documentation/, Apr. 2014.