Traffic Offloading Improvements in Mobile Networks

Tao Zheng, Daqing Gu
Orange Labs International Center
Beijing, China
e-mail: {tao.zheng; daqing.gu}@orange.com

Abstract – **The exponential increase in mobile IP data usage causes a shortage in the mobile bandwidth. Traffic offloading is regarded as a solution to the exploding growth of mobile broadband data traffic in the mobile networks. In this paper, a content aware traffic offload scheme is proposed to implement using multiple access paths simultaneously. Moreover, the process flow based-on the scheme in Long Term Evolution (LTE) and other traffic offloading improvements are also presented. This scheme utilizes Content Centric Networking (CCN) concept and Digital Fountain Codes to handle the multi-path control and reduce the complexity of traffic offload implementation.**

Keywords- Traffic offloading, CCN, Fountain Codes, LTE

I. INTRODUCTION

Mobile broadband devices such as smart phones, tablets, wireless dongles and some data-intensive apps have resulted in an exponential increase in mobile IP data usage, which is expected to cause a shortage in the mobile bandwidth. According to the Cisco Visual Networking Index Global Mobile Data Forecast[1], the global mobile data usage tripled in 2010 as compared to 2009. Further, the Cisco forecast predicts that by 2015, there is going to be a 26 fold increase as compared to 2010 levels.

To anticipate this problem, operators have deployed or are deploying “mobile data offloading” solutions to alleviate network congestion quickly. Traffic offloading refers to the ability to move mobile data traffic from cellular to alternative network such as WiFi. So, the data traffic management will be an important issue in traffic offloading.

The 3rd Generation Partnership Project (3GPP) has defined and is defining some traffic offloading mechanisms in various releases. For example, Local IP Access[2] in Release 9, Selected IP Traffic Offload[2], IP Flow Mobility[3], Access Network Discovery and Selection enhancements[4][5][6] and Multiple Access PDN Connectivity[6][7] in Release 10, Broadband Access Interworking using WLAN/H(e)NB and Broadband Access Interworking using H(e)NB[8] in Release 11, WLAN Network Selection for 3GPP Terminals[9], LIPA Mobility and Selected IP Traffic Offload at the Local Network[10], S2a mobility based on General packet radio service (GPRS) Tunneling Protocol (GTP) and WLAN Access[11] and IP Flow Mobility support for S2a and S2b Interfaces[12] in Release 12. Traffic management in these mechanisms focuses on networks and terminals.

The objective of the paper is to study and compare the IP traffic offloading and management solutions in 3GPP. A proposal based on content aware traffic offloading is finally presented.

This paper is organized as follows. In Section 2, we study and compare the IP traffic offloading and management solutions in 3GPP. In Section 3, a content aware traffic offload scheme and its verification are presented. In Section 4, potential extensions in the proposed scheme and other improved points in multi-attachment network are studied. Finally, Section 5 summarizes the conclusions.

II. TRAFFIC OFFLOADING IN 3GPP

Traffic offloading is regarded as a solution to the exploding growth of mobile broadband data traffic in the deployed 3GPP mobile networks. The reason why traffic offloading by WiFi is considered to be a viable solution for mobile data traffic explosion is that there is a lot of available WiFi spectrum with a very large number of compatible devices. And it simplifies the complexity as well as cost of managing and deploying a Cellular network. In 3GPP, from Release 9 to 12, some traffic offloading mechanisms are defined.

A. Release 9

- Local IP Access (LIPA)

LIPA was introduced in 3GPP Release 9, with the discussion on architecture options and impacts to procedures being continued in 3GPP Release-10 and 3GPP Release-11 actively.

LIPA is a mechanism by which a User Equipment (UE) connected to a Home NodeB or Home eNodeB (H(e)NB), is able to transfer data to a local data network connected to the same H(e)NB system directly, without the data traversing the cellular network, and accordingly reduce the load on the mobile core network. LIPA also allows the User Equipment (UE) to access any external network that is connected to the local network.

Considering an IP based corporate wireless network with multiple devices such as laptops, tablets, printers, servers, video conferencing units and IP based telephones which all need to connect to each other and also connect to the internet. The network is implemented using a femto cell gateway and a private gateway to which all these devices connect. If a user needs to print from a laptop, LIPA helps in routing the print request internally, without routing it through the femto cell gateway. Also, email could be sent directly through the private gateway.

ISBN: 978-1-61208-330-8

LIPA is a simple architecture well suited to local networks. LIPA is applicable only to H(e)NB access, not for macro cell access. It needs the additional Local Gateway function in H(e)NB.

B. Release 10

- Selected IP Traffic Offload (SIPTO)

SIPTO is a mechanism where portions of the IP traffic on a H(e)NB access or cellular network are offloaded to a local network, in order to reduce the load on the core network. SIPTO is applicable to H(e)NB access or another gateway in the cellular network that is closer to the UE. SIPTO can be triggered by events like UE mobility, special occasions that lead to concentration of traffic or other network rules.

Compared to LIPA, SIPTO is applicable in both femto and macro networks use cases. However, SIPTO doesn’t help radio congestion.

- IP Flow Mobility (IFOM)

IFOM is a mechanism where the terminal has data sessions with the same Packet Data Network (PDN) connection simultaneously over a 3GPP and a WLAN access network. Under this situation, the UE could add or delete data sessions over either of the access methods, effectively offloading data. Unlike LIPA and SIPTO, where the data offload is largely transparent to the UE, the logic of data offloading in IFOM is more UE centric and largely transparent to the Radio Access Network (RAN).

IFOM helps in both radio and core network congestion. However, compared to LIPA and SIPTO, IFOM needs support of Dual Stack Mobile IPv6 (DSMIPv6) and WiFi or other non 3GPP access network and is more complicated to be implemented.

- Access Network Discovery and Selection (ANDSF) enhancements in Release10

ANDSF is a module within an Evolved Packet Core (EPC) of the System Architecture Evolution for 3GPP mobile networks. ANDSF enables consumer-side devices such as notebooks, modems and mobile phones to discover and communicate with non-3GPP networks such as WiFi or WiMAX and enforce network policy controls. Standards Related to ANDSF in 3GPP are TS 24.312[4], TS 22.278[5] and TS 23.402[6].

- Multiple Access PDN Connectivity (MAPCON)

MAPCON provides the capability for terminals to establish multiple connections to different PDNs via different access methods and a selective transfer of PDN connections between accesses. MAPCON feature is characterized by multiple packet core IP addresses at the UE, any of which may be moved (but unchanged) between 3GPP cellular and WiFi access without impacting the 3GPP access connectivity of the other IP addresses. This allows IP traffic to multiple PDNs through the use of separate PDN-GateWays (PDN-GWs) or a single PDN-GW. The usage of multiple PDNs is typically controlled by network policies and defined in the user subscription of TS 23.401[7].

Multiple PDN connections would need to be supported when the UE is using LTE for part of data connection and WiFi for other part. In fact these two (or multiple) connections should be under the control of the same EPC core that can help support seamless mobility once the terminal moves out of the WiFi hotspot.

C. Release 11

The main problems of the interworking between a 3GPP system and a fixed broadband access arose from the different methods of policy control. 3GPP TS 23.139[8] specifies the interworking between a 3GPP system and a fixed broadband access network defined by Broadband Forum (BBF) to provide the IP connectivity to a 3GPP UE using a WLAN and a H(e)NB connected to a fixed broadband access network. It covers the system description including mobility, policy, Quality of Service/Quality of Experience (QoS/QoE) aspects between a 3GPP system and a fixed broadband access network as well as the respective interactions with the Policy and Charging Control (PCC) frameworks.

3GPP identified the initial use cases for Fixed-Mobile Convergence (FMC) in Release 9 and finalized the work on phases 1 and 2 within Release 11, and phase 3 will be addressed in Release 12 and later releases.

- Broadband Access Interworking using WLAN/H(e)NB

When WLAN is being used for interworking with a fixed broadband access network, 3GPP Evolved Packet System (EPS) considers both EPC routed traffic and non-seamless WLAN offloaded traffic; both traffic types can coexist during network operation. That is, UE can simultaneously have a connection to both the EPC and the non-seamless WLAN offloaded traffic.

For the purpose of interworking with a fixed broadband access network, a 3GPP system has to recognize the local IP address of the UE connected to the fixed broadband access network. The S9a interface session can be established and perform the policy interworking when the local policy of the BBF network indicates that the policy control for non-seamless WLAN offload is allowed for the UE, as well as the 3GPP home operator’s policy.

- Broadband Access Interworking using H(e)NB

In contrast to the interworking scenario using WLAN access, the interworking architecture using H(e)NB supports only EPC-routed traffic. For the purpose of interworking with a fixed broadband access network, this architecture basically uses S9a similar to the architecture using WLAN described above. Then the S9a interface also carries the H(e)NB’s local IP address and User Datagram Protocol (UDP) port number(s), and/or the Fully Qualified Domain Name (FQDN) of the fixed broadband access network to the Broadband Policy Control Framework (BPCF) from the Policy and Charging Rules Function (PCRF).

D. Release 12

- WLAN Network Selection for 3GPP Terminals

3GPP TR 23.865[9] studies WLAN network selection for 3GPP terminals in Release 12. The solutions are based on architectures as specified in TS 23.402[6] and will take into account Hotspot 2.0 specifications developed by the Wi-Fi Alliance (WFA) [13]. 3GPP operator's policies for WLAN network selection will be provisioned on 3GPP terminals via pre-configuration or using the ANDSF server for their delivery.

- LIPA Mobility and SIPTO at the Local Network

3GPP TR 23.859[10] studies on the support of mobility for LIPA between the H(e)NBs located in the local IP network and functionality to support SIPTO requirements at the local network, including mobility. The report is intended to document the analysis of the architectural aspects to achieve these objectives in order to include the solutions in the relevant technical specifications.

- Study on S2a mobility based on GTP and WLAN Access

In 3GPP TR 23.852[11], S2a mobility based on GTP and WLAN Access is studied:

The addition of an S2a based on GTP option. In particular this Study Item will develop the necessary stage 2 message flows to support S2a based on GTP and mobility between GTP-S5/S8 and GTP-S2a; Supporting WLAN access to EPC through S2a via mechanisms; The study item gives some solutions separately for GTP based S2a and WLAN access to EPC through S2a.

- Study of IP Flow Mobility support for S2a and S2b Interfaces

3GPP TR 23.861[12] studies the scenarios, requirements and solutions for UEs with multiple interfaces which will simultaneously connect to 3GPP access and one, and only one, non-3GPP access. Solutions to be studied include the possibility of dynamically routing to specific accesses individual flows generated by the same or different applications belonging to the same PDN connection. The study of solutions to support routing of different PDN connections through different access systems is also in the scope of this item. This study item also investigates the mechanisms for provisioning the UE with operator’s policies for multiple access PDN connectivity and flow mobility.

III. Content Aware Traffic Offload Scheme

This section proposes a content aware traffic offloading scheme in 3GPP. In the scheme, fountain codes [14] are used to transport the information from servers to terminals through different access paths. Fountain codes technique having the slight overhead and impressive codec, is exploited to generate the segments for delivery. The data streams can be transported smoothly in all different access paths simultaneously or part of them when breakdown happens and terminals do not need to handle the breakdown and recovery.

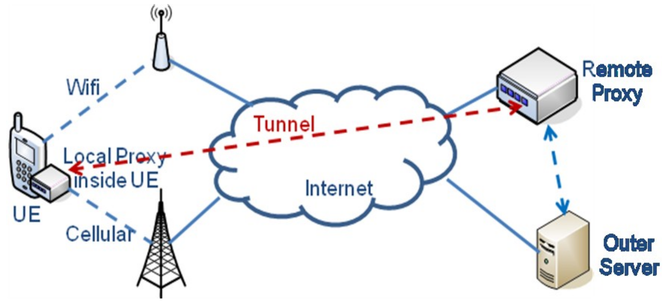

Figure 1. System Overview of the scheme

A. The scheme overview

The system overview is illustrated in Figure 1. It is composed of terminal and remote general Hypertext Transfer Protocol (HTTP) proxies. A local proxy built in the terminal is responsible for the conversion between the HTTP request/response and the Interest/Data packets. The remote proxy exchanges Interest/Data packets with the local HTTP proxy through the Transmission Control Protocol (TCP) or UDP based tunnel established over multiple heterogeneous links in the content centric way. The remote proxy fetches the content from the outer server in the Internet to satisfy the terminal’s request. The main reason for using two proxies is that the tunnel between the two proxies can help Content Centric data stream penetrate the network.

The working environment can be IPv4 or IPv6. In IPv6 network, the remote proxy can be assigned with different IPv6 addresses including unicast address, multicast address and anycast address. Given the unicast address, the terminal establishes the tunnel with the single specific remote proxy. The multicast addressing refers to the configuration where the terminal can set up the tunnels concurrently connecting the collection of remote proxies. The anycast addressing makes the terminal build the tunnel to the nearest remote proxy among several candidates.

Since the service session in the scheme is identified with the Uniform Resource Identifier (URI) that is independent of the IP addresses associated with the different connections to the network, the terminal can keep the ongoing session alive as long as the content identifier is invariant. The dynamics due to the connection switching in the mobile scenario is only visible in the tunnel running over the TCP or UDP sessions managed by the local HTTP proxy and shielded from the perspective of the HTTP session in the normal web-based client of the terminal.

CCN is an alternative approach to the architecture of networks which was proposed by Xerox PARC within the CCNx [15] project. From the network perspective, in CCN, network entities in ordinary network are replayed by data entities.

Unlike state-of-the-art multi-path approaches such as Multi-Path Transmission Control Protocol (MP-TCP), CCN can help us to hide some network control implementing details with the help of the ‘connection-less’ nature of CCN. In the proposed solution, we utilize the CCN concept rather than CCN protocol, thus it's not necessary to consider the change of network access paths through fountain codes to encapsulate data packets.

The service session coupling with the remote proxy avoids the problem of Domain Name System (DNS) resolution potentially confronted with the multi-homed terminal. Since the remote proxy acts as the agent of the terminal for content acquisition, the terminal has no need for DNS resolution except to forward the request message to the remote proxy. The update on the access router is additionally not mandatory any more because the conversion between IP address and URI is executed in the sense of application layer.

B. The scheme in LTE

When the scheme is applied in LTE network, the remote proxy can be deployed within PDN-GW and the local proxy is still in terminals. The architecture is showed in Figure 2. Terminals can retrieve information from outer server through different access system simultaneously and can switch smoothly among them without any breakdown. Multiple data streams can be transported though multiple access systems, such as LTE RAN, trusted non-3GPP access and non-trusted non-3GPP access.

In this scheme, fountain codes are used to transport data packets between two proxies. The reasons of choosing fountain codes as the encapsulation technology are showed as follows. Fountain codes are rateless in the sense that the number of encoded packets that can be generated from the source message is potentially limitless. Regardless of the statistics of the erasure events on the channel, the source data can be decoded from any ser of K' encoded packets, for K' slightly larger than K. Fountain codes can also have very small encoding and decoding complexities and automatically adapt the change of multiple access paths to avoid the implementation of path control details [14].

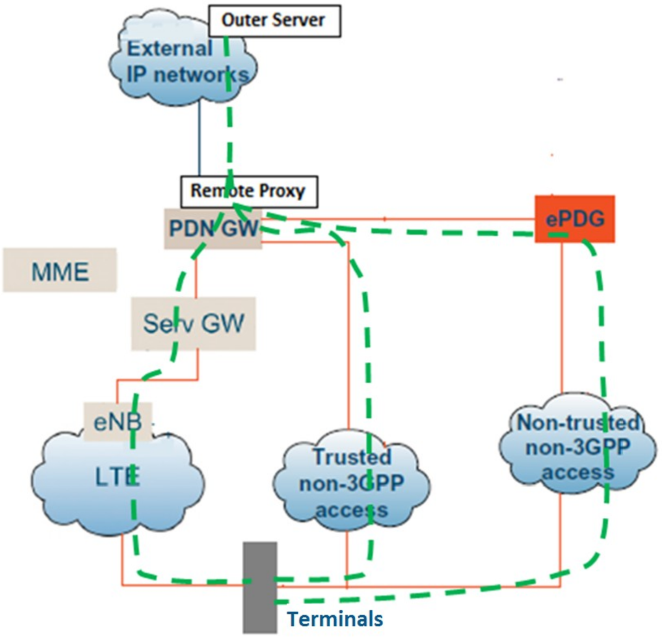

Figure 2. The content aware traffic offload in EPC

The source hosts simply transfer the packets with the different coding schemes as many as possible to the destination hosts without concerns over the reordering induced in various paths. It increases the data throughput and avoids the complicated reconciliation between the multiple paths.

Figure 3 gives the process of the content aware traffic offload.

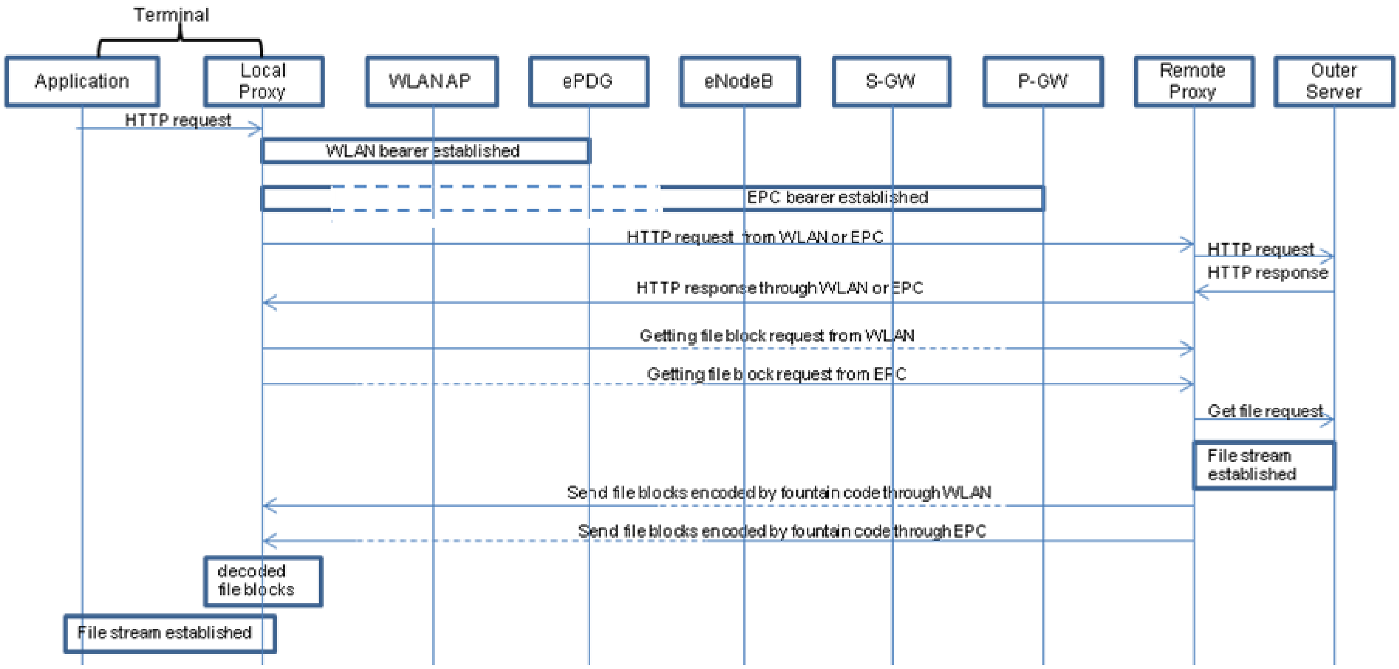

Figure 3. The process flow generating IPv6 flow label

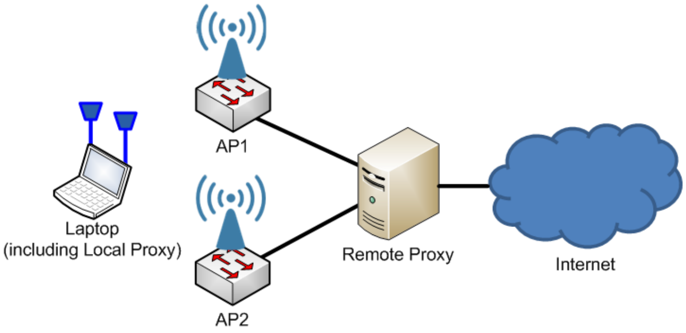

Figure 4. The test-bed topology in lab

In the terminal, the local proxy handles the application's request towards outer server through HTTP. The bearer of WLAN or EPC is established in advance or when the local proxy receives the request. After the local proxy received the response from outer server, it sends the requests getting file blocks to the remote proxy, which acquires the file from outer server, encodes the file blocks by fountain codes and sends them to the local proxy though different access paths. The local proxy decodes the received blocks and sends them to application. During the transportation, the change of paths between the remote proxy and the local proxy will not impact the blocks' decoding due to the fault-tolerance property of fountain codes.

C. The verification of this scheme

According to the traffic offloading scheme mentioned above, a verification test was implemented in our lab. Because there is no mobile data access in the lab, we chose two WiFi interfaces and Access Points (AP) to simulate two access paths. Figure 4 shows the test topology, which is composed of a laptop (including a local HTTP proxy) with two WiFi interfaces, two WiFi APs and a remote proxy connecting to Internet.

The local proxy and remote proxy, fountain encoding and decoding were implemented through programming. On this test-bed, we tested various combinations of two access paths and handover between them. The data delivery between the laptop and Internet cannot be interrupted in these scenarios. The test validated the feasibility and validity of this scheme.

IV. Potential Extensions and Improved Points for Multi-attachment Networks

The proposed scheme in Section 3 can be easily extended in other use cases and there are other improved points for multi-attachment networks.

A. Potential Extensions

The potential extensions of this scheme include mobile content distribution and mobile data offloading in addition to the mobility management.

- Mobile content distribution

It is simple and practicable to implement the content distribution in the IPv6 mobile network with our solution. The remote proxy introduced in our method may take the role of content cache in the Content Distribution Network (CDN). The content centric networking relying on the URI identifier and many-to-many transport enables the tight coupling between request routing and load balancing in the simplified way where the remote proxy can realize the distributed load sharing by simply tuning its transmission rate and forwarding the content request to other proxies.

- Mobile data offloading

Mobile data offloading, also called traffic offloading can be smoothly supported by our solution without interrupting the ongoing session. The session maintenance with URI is able to shield the negative side-effect yielded by the IP address variation due to the link switching triggered by the traffic offloading. Given the single service session, the many-to-many transport implemented with the Digital Fountain coding makes the data delivery through the complementary network independent of the original one in the cellular networks without fearing the packet reordering that may deteriorate the QoS/QoE performance.

B. Improved points for multi-attachment network

- IP aware traffic management

In EPC network, the IP packets are transported in GTP Tunnel. Figure 5 shows the IP packet structure through GTP Tunnel. EPC entities just handle GTP Tunnel instead of IP packet.

The UE and the PDN-GW (for GTP-based S5/S8) or Serving-GW (for Proxy Mobile IP (PMIP)-based S5/S8) use packet filters to map IP traffic onto the different bearers. Some EPC's mechanisms, such as QoS, PCC, are based-on bearers, the packets contained in the same bearer share same QoS profile and be treated in the same way. It's hard to handle IP packets in such mechanisms.

When UE attaches multiple networks, except for EPC, other access methods handle IP packets directly. Therefore in EPC, the transport layer is not able to know and use the information, e.g., QoS related information, hidden in (1) the tunnel header and (2) original IP packet. In the context of this paper, by applying IP aware traffic management, the transport layer will be able to read and use this hidden type of information. So, IP aware traffic management in multi-attachment network will be beneficial to reduce the complex and promote the efficiency of the traffic offloading mechanism.

- IPv6 application at multi-attachment radio network

As a network evolution goal, IPv6 is deployed in mobile network, including access network, core network and mobile carrier IP network. IPv6 introduction in mobile network will impact on QoS of mobile services.

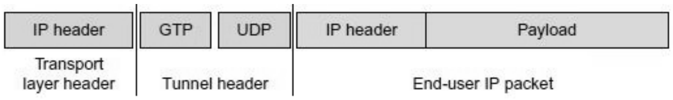

Figure 5. IP packet structure in GTP Tunnel[16]

In EPC, there are two IP headers, which correspond to the transport layer and the end-user IP packet respectively. That is, two IPv6 flow label fields can be handled by mobile network entities and IP carrier network entities respectively.

A sequence of packets sent from a particular source to a particular unicast, anycast, or multicast destination constitute a flow. In IPv4 network, the 5-tuple of the source and destination addresses, ports, and the transport protocol type is able to identify a flow. IPv6 has introduced a field named flow label. The 20-bit flow label in the IPv6 header is used by a node to label packets of a flow. General rules for the flow label field have been documented in RFC 3697 [17].

In multi-attachment radio network, the IPv6 Flow Label can be employed to identify the different access methods and provide traffic management based-on flow for further processing in EPC.

V. Conclusion and Future Work

This paper presents the study on the IP traffic offloading and management in the multi-attachment network in 3GPP, where some mechanisms are investigated and compared. Then a content aware traffic offloading scheme based on CCN and fountain codes is proposed to handle different access systems simultaneously and automatically adapt the change of multiple paths to avoid the implementation of path control details. Tunnel and proxy can help deploy the scheme when CCN is not supported in current networks. Some potential extensions of this scheme and improved points for multi-attachment network are proposed too.

We tested this scheme in our lab. Traffic was able to be transported smoothly among multiple WiFi access paths. The test results verified the feasibility and showed the features of the scheme. In the future work, we consider testing the extension use cases of this scheme and applying other improved points listed in Section 4. In addition, we will focus on the performance of this scheme.

References

[1] http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html, retrieved: February 2014.

[2] 3GPP TS 23.829 Local IP Access and Selected IP Traffic Offload (LIPA-SIPTO) (Release 10), October 2011.

[3] 3GPP TS 23.261 IP flow mobility and seamless Wireless Local Area Network (WLAN) offload (Release 10), March 2012.

[4] 3GPP TS 24.312 Access Network Discovery and Selection Function (ANDSF) Management Object (MO) (Release 10), June 2012.

[5] 3GPP TS 22.278 Service requirements for the Evolved Packet System (EPS) (Release 10), October 2010.

[6] 3GPP TS 23.402 Architecture enhancements for non-3GPP accesses (Release 10), September 2012.

[7] 3GPP TS 23.401 General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 10), March 2013.

[8] 3GPP TS 23.139 3GPP system - fixed broadband access network interworking; Stage 2 (Release 11), March 2013.

[9] 3GPP TR 23.865 WLAN network selection for 3GPP terminals (Release 12), December 2013.

[10] 3GPP TR 23.859 Local IP access (LIPA) mobility and Selected IP Traffic Offload (SIPTO) at the local network (Release 12), April 2013.

[11] 3GPP TR 23.852 Study on S2a Mobility based on GTP & WLAN access to EPC (Release 12), September 2013.

[12] 3GPP TR 23.861 Network based IP flow mobility (Release 12), November 2012.

[13] https://www.wi-fi.org/hotspot-20-technical-specification-v100, retrieved: February 2014.

[14] J. Byers, M. Luby, M. Mitzenmacher, and A. Rege, A digital fountain approach to reliable distribution of bulk data, Proc. ACM SIGCOMM '98, September 1998, pp. 56-67.

[15] http://www.ccnx.org, retrieved: February 2014.

[16] T. Zheng, L. Wang, and D. Gu, A flow label based QoS scheme for end-to-end mobile services, Proc. The Eighth International Conference on Networking and Services (ICNS 2012), March 2012, pp. 169-174.

[17] J. Rajahalme, A. Conta, B. Carpenter, and S. Deering, IPv6 flow label specification, IETF RFC 3697, March 2004.