Network Path and Quality Validation in the Evolved Packet Core

Yahya Al-Hazmi*, Julius Mueller*, Hakan Coskun* and Thomas Magedanz†
*Chair of Next Generation Networks, Technical University Berlin, Berlin, Germany
Email: {yahya.al-hazmi, julius.mueller, hakan.coskun}@tu-berlin.de
†Next Generation Network Infrastructure, Fraunhofer FOKUS Institute, Berlin, Germany
Email: thomas.magedanz@fokus.fraunhofer.de

I. Introduction

The Internet nowadays plays an imperative role in critical domains such as finance, health, security, entertainment and military where real-time services with guaranteed resources become necessary. Services residing within the application layer in today's fixed and mobile network environments are abstracting from the underlying network layer, and therefore, assuming pure IP connectivity without taking into consideration the in-network services as Quality-of-Service (QoS) guarantees, security and mobility, and routing decisions. These services assuming best-effort data transport without demanding specific QoS, routing schemes (e.g. shortest, most reliable path, etc.). In comparison to the best-effort data transport, real-time services require reliable transport of packet data flows starting at the device going through the access and core networks into autonomous networks towards a service.

End-to-end monitoring provides QoS information along the entire data path. Analyzing all or most parts of a specific packet data flow through fragmented heterogeneous network domains is more complex and requires distributed monitoring techniques. Furthermore, end-to-end monitoring provides only an overall performance measurement, but doesn't expose QoS information on a per-hop basis through the network. However, these measurements are required to optimize individual network parts through the identification of loops, significant delays or packet loss due to overload situations.

This article focuses on the validation of data flows in fixed and mobile networks through the individual network parts, i.e. QoS per hop validation. In particular, the focus is only on the core network part of the Evolved Packet System (EPS) and not on the radio network part (LTE), because the latter one utilizes the shared medium radio and negatively effects the measurement due to packet loss and additional delays.

The Packet-Tracking monitoring tool [4] developed within the G-Lab DEEP project[1], is presented as a software solution for network path and quality monitoring. It utilizes distributed hash based sampling technique to keep up with increasing data rates.

[1]The German-Lab-DEEP project funded by the German Federal Ministry of Education and Research (BMBF) under the grant number 01BK0901

II. Validation Approach

This section represents an approach for monitoring the network traffic flows. The packet tracking as a passive monitoring approach is used for this purpose. It allows pursuing packets on the network path and providing various types of packet related information. Thus, it enables an end-to-end monitoring that provides QoS information along the entire data path. The OpenEPC toolkit is used in this work as an applicable environment for the mobile networks. It connects heterogeneous accesses networks such as 3GPP LTE, UMTS and GPRS and non-3GPP IEEE WiFi and WiMAX, offering a platform for research in the area of mobile networks. The following sections describe the evolved packet core, which reflects the basic design of the OpenEPC toolkit, and the packet tracking monitoring tool.

A. Evolved Packet Core

3GPP standardizes with the All-IP Evolved Packet Core in Release 12 a counterpart to the radio access network technology Long-Term-Evolution (LTE) and its evolution LTE-Advanced (LTE-A). EPC provides network mobility between heterogeneous 3GPP [1] and non-3GPP [2] access network technologies, provides QoS through Policy and Charging Control, pure IP connectivity and security.

Fraunhofer FOKUS and TU Berlin developed the OpenEPC toolkit that adopts large parts of the 3GPP technical standards and represents an all-IP architecture enabling the research, development and fast prototyping of different core networks and application domains within the next generation wireless environment. For this matter, OpenEPC includes the mechanisms of connecting end-user devices to different access networks and supporting communication interfaces to the various service platforms, offering the most suitable connection for the various services in terms of access network selection and of resource adaptation to the current network conditions [3].

Due to its modular structure, the OpenEPC toolkit enables the fast deployment of test network architectures in various combinations coming to meet the requests from the research community. Through its policy and charging control architecture, the subscriber and mobility management mechanisms and through the easy interconnection with various access networks and application platforms, OpenEPC encompasses the complete spectrum of the wireless research enabling the further prototyping of core network enhancements.

B. Packet Tracking

The emerging of traffic engineering due to the rapid growth of the Internet traffic led to have many measurement tools and techniques that have been introduced, reaching from active measurements like ICMP ping and traceroute to passive measurements like pcap and flow measurement. However, most of them introduce various disadvantaged and limitations reaching from the active technique like significant processing overhead and lower accuracy issue affected by injecting additional probe traffic into the network to the passive technique like data flood generated by large amount of measurement traffic.

To tackle these disadvantages and limitations, we introduce a passive measurement tool called Packet Tracking [4]. It provides a possible solution to enhance passive measurement limitations through two mechanisms. First, by deploying hash-based packet sampling which enables the selection of subset of packets to be measured in order to reduce the amount of data from observed traffic and significantly improve the accuracy of network characteristic estimation. Second, by deploying an efficient, flexible, reliable and secure transport method for exporting flow information and selected packet observation data, called IPFIX [5]. Distributed probes measure packet data flows in a single network compartment, a network domain or multiple independent operator networks in parallel by reporting measurements towards a centralized aggregation point. Packet Tracking Netview is used to visualize packet paths and their hop-to-hop characteristics on a worldmap.

Packet tracking enables the following functionalities:

- QoS validation
- Total end-to-end as well as individual network-to-network SLA Validation
- Handover validation, performance evaluation and visualization
- Per hop real-time link quality measurements and security constraints validations
- Flexible measurement granularity adjustment from single packet up to flows

III. Demonstration

This section presents the demo setup and the measurement scenarios. The validation is carried out by monitoring the important QoS parameters, in particular, one-way delay and packet loss. For a demonstration, the OpenEPC toolkit is used as a prototype implementation of the EPC. An end-user is downloading data from an Internet server through any of the available networks provided by the OpenEPC. Monitoring probes are deployed in multiple components along the path between the end-user and the Internet server, in particular, on all OpenEPC components. Hop-by-hop QoS monitoring information is collected from these probes.

In this demo, two setup scenarios are presented. They differ from each other on the network technology used by the end-user as an access network among the available ones provided by the OpenEPC. In the first scenario the LTE is used while the WiFi is used in the second scenario. For having an efficient and effective validation, measurements are taken in two phases: end-to-end measurements, and one-hop measurements between the individual nodes along the entire path.

The environment setup consists of four Eee PC boxes representing the EPC components, one Eee PC notebook as an eNodeB in the case of LTE scenario, and one Eee PC notebook as a client. All components run Ubuntu Linux, with dual core Intel Atom @ 1.60GHz N270 processor, 100MB/s network cards, and 2GB memory. A DLINK fast Ethernet switch Adapter USB 2.0 DUB-E100 provides additional Ethernet interfaces to the Eee PC boxes. A netgear 8 port 100/1000Mbps switch GS608v3 interconnects all scenario components.

It is a critical mechanism to synchronize sampling and perform high precision measurement. Therefore, Network Time Protocol (NTP) is deployed at each EPC component to realize time synchronization.

In both scenarios, one way delay measurements have been conducted while analyzing TCP traffic on each component within the EPC architecture. In particular a file has been downloaded from a server (IP Service) through the EPC towards a UE/device. The setup and the involved network elements are in an isolated network and are therefore have network resources exclusively.

The measurements are captured between the IP services and the specific radio access network controller (ANGw or eNodeB), both involving components on the path and excluding the terminal/UE from the measurements, which would be connected over a wireless link.

In detail we have the following chain of components involved in data traffic routing between the service and the UE:

- LTE: IP Service, PDNGW, SWG, eNodeB
- WiFi/802.11: IP Service, PDNGW, ANGw

As a result of the conducted measurements, the difference between the average end-to-end delay and the sum of the individual one-hop average delays is 0.12 and 0.14 milliseconds in LTE and WiFi, respectively. As expected, the probes do not significantly disturb or change the network property as it is well known in passive measurement tool characteristic.

References

[1] 3GPP. General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access. TS 23.401, 3rd Generation Partnership Project (3GPP), Mar. 2012.

[2] 3GPP. Architecture enhancements for non-3GPP accesses. TS 23.402, 3rd Generation Partnership Project (3GPP), Mar. 2012.

[3] Corici M., Magedanz T., Vingarzan D., Weik P., Prototyping Mobile Broadband Applications with the Open Evolved Packet Core, 2010 14th International Conference on Intelligence in Next Generation Networks (ICIN), Berlin, Germany, ISBN: 978-1-4244-7443-1, DOI 10.1109/ICIN.2010.5640902, Nov 2010.

[4] TUB and FOKUS. Packet tracking. Website, 2012. Available online at www.fokus.fraunhofer.de/go/track, last visited on Mai 25th 2012.

[5] B. Claise, S. Bryant, G. Sadasivan, S. Leinen, T. Dietz, and B. Trammell. Specification of the ip flow information export (ipfix) protocol for the exchange of ip traffic flow information (rfc 5101). Technical report, Technical report, The Internet Engineering Task Force (IETF), January 2008.