Performance of Flow-Aware Networking in LTE backbone

Sniady, Aleksander; Soler, José

Published in:
Proceedings of OPNETWORK2012

Publication date:
2012

Performance of Flow-Aware Networking in LTE backbone

Aleksander Sniady and Jose Soler
Networks Technology and Service Platforms
DTU Fotonik
Technical University of Denmark
2800 Kgs. Lyngby, Denmark
E-mail: {alesn, joss}@fotonik.dtu.dk

Abstract
According to traffic predictions, the growth in data networks usage will be increasing in the coming years, what will be especially visible in the mobile access networks. This brings new challenges in terms of traffic differentiation and network resource sharing, which need to be faced by wireless technologies, such as Long Term Evolution (LTE).

This paper proposes usage of a modified Flow Aware Networking (FAN) technique for enhancing Quality of Service (QoS) in the all-IP transport networks underlying LTE backbone. The results obtained with OPNET Modeler show that FAN, in spite of being relatively simple, provides good protection against congestion and decreases the need of over-provisioning.

Introduction
The amount of traffic transmitted in data networks grows extremely fast. According to Cisco, it has grown eight times during the last five years and will grow four times more until 2015 [1], mainly because of an increase in mobile traffic, which will grow 26 times between 2010 and 2015 [1].

An answer for the rapidly increasing demand for mobile traffic is the development of new wireless technologies that can provide more throughput and lower delays. The first widely used packet based mobile access was General Packet Radio Service (GPRS), which was the first in a series of continuously developed 3GPP technologies eventually reaching Long Term Evolution (LTE) [2], which is now introduced commercially to customers.

In contrast to the past, when every service had its dedicated distribution network, currently there is a trend to provide everything over a common infrastructure. That is why, LTE networks need not only to provide high throughput, but also need to successfully fulfil different delay and bandwidth requirements set by heterogeneous services operating within these networks [3]. Some of these requirements cannot be realized by the classical IP architecture, because some types of traffic are more sensitive to delay or bandwidth fluctuations. In order to provide usable services to the end customers, transport networks must include some traffic differentiation and quality guarantees mechanisms [4].

In this paper we show that after adaptations to LTE specifics, a simple FAN mechanism can bring an effective QoS mechanism in the transport network underlying the LTE backbone. This allows for providing high-quality real-time services, such as VoIP, which is crucial for mobile operators due to economical profits.

Long-Term Evolution backbone
The introduction of System Architecture Evolution (SAE), which is the name of the new backbone network in LTE, has been the biggest change within the mobile network backbone since the introduction of GPRS and IP Multimedia Subsystem (IMS) [2].

One of the goals of SAE is to provide an efficient backbone network that can support the improvements in the LTE radio part. SAE introduces a simplified, more cost-effective architecture with a flat structure [5]. As a result, packet delay in the backbone is minimized. This allows running modern real-time services such as interactive games, video conferencing or machine-to-machine exchange [3]. A basic overview of the data-plane in the simplified SAE architecture is shown in Figure 1.

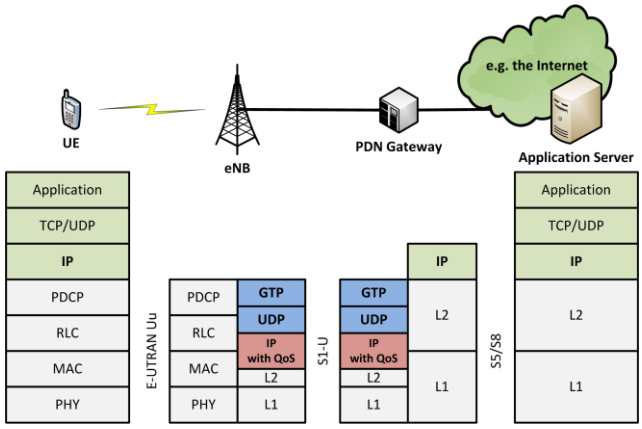

Figure 1: The simplified architecture and the protocol stack used in the data-plane in LTE [2, 4]

The major change in the SAE backbone is an abandonment of the circuit-switched part, which was used for telephony service in GSM and UMTS. Now all the services are delivered based on packet-switched IP technology [2], but LTE still needs to provide telephony service at least of the same quality as GSM and UMTS networks did [6]. Therefore, strict QoS provisioning is needed.

Flow-Aware Networking
Flow-Aware Networking (FAN) is a relatively new concept for both avoiding network congestion and ensuring low-delay transmission of certain types of traffic [7]. The idea of FAN is especially interesting due to its simplicity, which fits well the concepts underlying IP networks.

A classical IP router treats every received packet individually, what means that routing decision about one packet

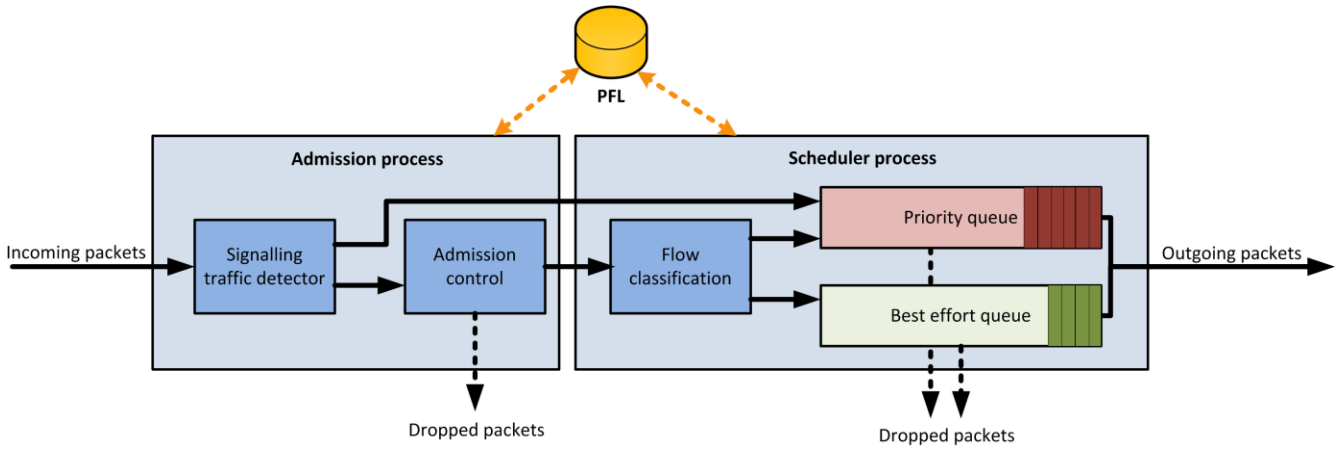

Figure 2: The implemented AFAN model

is independent on the decisions made about other packets belonging to the same IP flow. In contrast to that, when a FAN router receives an IP packet, first it determines to which IP flow the packet belongs. Then the packet is routed in the same way as the other packets of the same IP flow.

FAN is based on a "cross-protect router" [8], which uses an innovative method for flow admission and scheduling. Approximate Flow-Aware Networking (AFAN) has been chosen for LTE. AFAN is a simplified method for implementing FAN that was first proposed by Domzal [11]. AFAN results in simple router design, fast packet processing and greater scalability, what is of big importance in the backbone network. At the same time AFAN is claimed to have performance very similar to other FAN architectures, such as the one proposed by Kortebi [8].

The structure of the AFAN router is shown in Figure 2, while Figure 3 presents its OPNET implementation. AFAN proposed by Domzal [11] has two standard FAN elements:

- admission control,
- scheduler,

while the implemented model described in this paper has been enhanced with:

- flow identification adapted to GPRS Tunnelling Protocol (GTP),
- signalling traffic detector.

The following sections describe all of these elements.

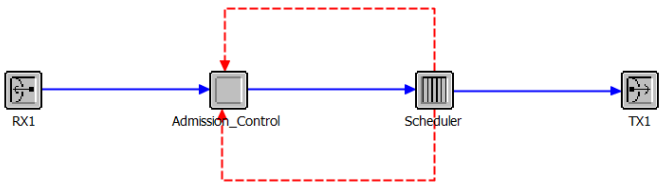

Figure 3: OPNET model of the AFAN module

Flow Identification adapted to GTP

In a pure IP network flows may be easily identified using the IP header fields: destination and source addresses, protocol ID; together with the UDP/TCP header fields: source and destination port numbers. Thus, this five element tuple is a desired way of identifying an IP flow.

However, the packet transport among nodes within SAE is based on a tunnelling mechanism using GTP [2] [14]. Original IP packets sent by a User Equipment (UE) or packets incoming from an external network, are firstly encapsulated within a GTP packet and then encapsulated within an outer IP packet. Due to this double encapsulation, individual flows are more difficult to identify, as the information about the final destination and the true point of origin are hidden deeper in the packet structure. Therefore, the mechanism of flow identification in FAN needs to be specifically designed to support the GTP protocol. In the model herein presented, a FAN router looks for an internal IP packet encapsulated within an outer IP packet. If the internal packet is found, then the header fields of the outer packet are ignored and the flow is identified using the information carried in the internal packet.

Admission Control

Whenever a new packet arrives to a FAN router, the first thing is to determine whether its flow is already registered in the Protected Flow List (PFL) which is a register of all active flows currently transmitting through the router. If the flow, to which the packet belongs, is present in the PFL, then the packet is accepted and it is passed to the scheduler (regardless of the state of an outgoing link).

If the arriving packet belongs to a new flow (not registered in the PFL) then the packet is accepted (and the flow information is added to the PFL) only if there is no congestion state on the outgoing link. State of the link (congested or non-congested) is determined by the scheduler block.

New flows are blocked during the congestion state. The purpose of this is to ensure that active flows receive good network performance and that they can provide users with the expected service experience. When a flow is blocked its admission time increases significantly, but in return, once it is accepted it receives very stable and reliable service from the network.

If a flow is inactive for a given time period then it is removed from the PFL.

A state diagram of the Admission Control process implemented in OPNET is shown in Figure 4.

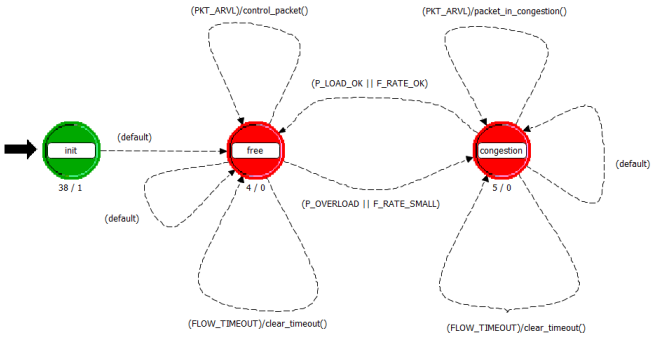

Figure 4: Admission Control process

Signalling detector adapted to SAE

The described admission control mechanism has been enhanced with the signalling traffic detector that adapts FAN specifically to a SAE network. Apart from user traffic, SAE transmits a lot of internal signalling traffic, which is used to exchange information and requests between SAE nodes. The signalling traffic requires little resources from the network, but on the other hand, it is very important for the network operation. Signalling packets need to receive low delay service in the network. A good example can be a handover operation, when it is important that a connection is quickly established through a new eNB. Thus, the signalling traffic must be transmitted rapidly to minimize interruption time [6].

With the FAN mechanism enabled, during a congestion state, the signalling could be blocked what would make FAN useless, regardless of how well it improves the data-plane transmissions. Thus, the signalling traffic cannot be treated in the same way as the user data and cannot compete for the network resources. It needs a special procedure to get the highest priority in the network. In order to achieve that, a new element has been added to the AFAN model - the signalling traffic detector. The signalling packets bypass the FAN admission control and the flow classification and are put directly in the priority queue (described later). This mechanism is based on the solution by Jajszczyk [15].

The main issue of this solution [15] is that FAN routers need to be statically configured to detect the signalling packets. This is because the authors suggest using IP addresses to detect these packets. This could be done e.g. by checking if a header of an incoming packet carries the IP address of Mobility Management Entity (MME), which is the main control node in SAE.

However, using IP addresses is both impractical, as IP address of MME would have to be set in all FAN routers, and inefficient, because the signalling traffic which is exchanged between other network nodes than MME would be still impossible to distinguish from the data traffic.

This is why it is herein suggested to access the header fields of GTP packets. Basing on the message-type field in the GTP header it is possible to easily detect the signalling packets.

Traffic classes

In general, as it is claimed by Bonald [9], there are two major classes of packet data flows: “signal conservation” or “throughput conservation”.

The signal conservation flows are generated by real-time and streaming applications. These applications are affected by packet loss and delay, and there are certain acceptance limits on those two parameters depending on application (e.g. due to different codecs) [9] [10]. As long as these limits are not exceeded, then a delivered packet flow allows an application to perform well. The signal conservation flows are called “priority flows” in the following sections, because in FAN their packets are scheduled with priority over other packets in order to stay within delay limits.

The throughput conservation flows transfer data that is not directly affected by packet loss or delay. The quality perceived by end-users depends on the overall transmission time. This type of flow is elastic, as flows may easily adapt to the available network bandwidth, without effect on the quality perceived by the end-users [9] [10]. The throughput conservation flows are called “best-effort”, as they are served by FAN routers using resources not consumed by the priority flows.

Flow Classification in FAN

FAN exploits this division and classifies each packet flow into one of the two classes. The flow classification method is implicit what is new compared with IntServ or DiffServ [9]. There is no marking system, there is no signalling exchanged between FAN routers. The only information which can be used for flow classification is the size of the buffer memory of a router occupied by packets of a given flow [9]. If the packet arrival rate of a flow is smaller than an average service rate, then such a flow does not accumulate packets in the buffer. Thus, basing on the buffer occupation it is possible to detect and prioritize flows that transmit with rate below the average. It applies to most of the signal conservation flows [7]. Hence, the flows which packets do not exceed certain bit-limit in the buffer are classified as priority.

By default all new flows are classified as priority flows, but if some flow exceeds the bit limit, then its classification changes to the best-effort class. The classification may be changed in the opposite direction as well, and the flow may be promoted back to the priority class.

While this simple, implicit division into the two classes gives much less control over network behaviour, it saves a lot of network resources.

Scheduler process

A goal of the scheduler is to create a queuing system, which will prioritize packets belonging to the priority flows.

The scheduler contains two queues, one for each of the two flow classes. Packets from the priority queue are always sent in the

first place, so packets in the best-effort queue wait as long as the other queue is not empty.

Apart from that, the scheduler block calculates congestion indicators, which determine whether an outgoing link is congested. The indicators' values are passed to the admission block, which decides if the limits are exceeded.

A state diagram of the scheduler process implemented in OPNET is shown in Figure 5. It has been based on the acb_fifo standard OPNET model, but it is enhanced with additional functions and transitions.

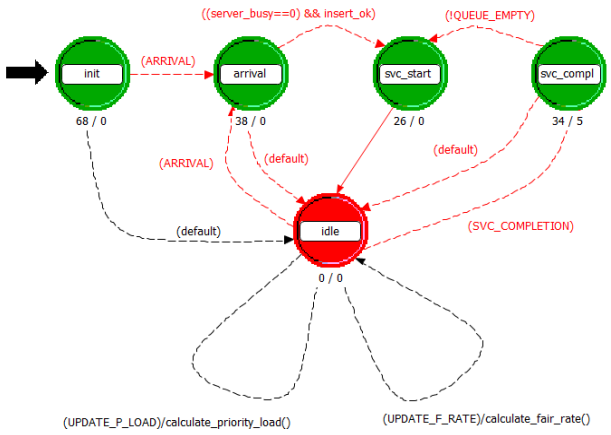

Figure 5: Scheduler process

Congestion detection

There are two indicators, which are calculated periodically, which define the congestion state. These are *priority load* and *fair rate* [11].

The priority load is an amount of priority traffic transmitted as a percentage of the total link capacity. The priority load is calculated as a number of transmitted priority bits over a time period divided by the length of this period and a bit rate of the link:

$$priority\_load = \frac{priority\_bits}{(t_2 - t_1) \cdot service\_rate} \quad (1)$$

If the priority load exceeds a set limit (e.g. 60%) then a FAN router changes to the congested state.

The second indicator – the fair rate estimates a maximum transmission rate achieved by best-effort flows. The fair rate is calculated, as the bigger of the following two cases:

- a bit rate of the link multiplied by a total inactivity time (time when no packets are processed) during a time period, divided by the length of this period, or
- a number of transmitted best-effort bits over a time period, divided by the length of this period and a number of best-effort flows in the PFL:

$$fair\_rate = MAX\left\{ \frac{inactivity\_time \cdot service\_rate}{(t_2 - t_1)}, \frac{b.effort\_bits / no\_of\_b.effort\_flows}{(t_2 - t_1)} \right. \quad (2)$$

The fair rate being below a certain threshold (e.g. 5%) also defines the congestion state.

Additional implementation considerations

FAN functionality has been implemented within separated network nodes, what made interfacing easier, but kept all advantages of using built-in models. This solution is shown in Figure 6.

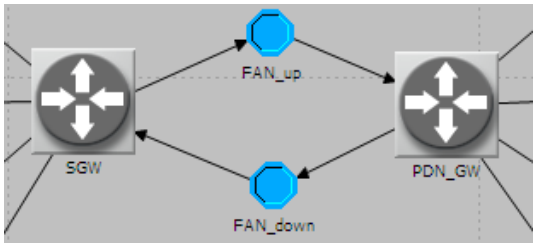

Figure 6: FAN nodes connecting two routers

FAN nodes accept and send IP packets (with encapsulated GTP/UDP/IP packets inside) over PPP links. In this way it is not required to make interfaces with internal OPNET modules and functions.

The whole model could have been build from scratch. However, then some benefits of the standard built-in models would be lost:

- the ability to use predefined traffic models, which being in accordance to commonly used application profiles (e.g. FTP usage, VoIP) reflect real-life users' behaviour
- modelled GTP mechanism, which adds overhead to transmitted data
- modelled SAE signalling

Application profiles

Effort has been taken to create a simulation scenario with realistic traffic models, meaning:

- In the network there should exist all typical application types used over IP networks.
- The network traffic should model real applications. This includes packet size, overhead, packet rate and tunnelling mechanisms.
- The proportion between traffic generated by different application types should agree with the predictions of mobile traffic demands for year 2015 [1] [16]. A mix of traffic used in the simulations is shown in Table 1. Moreover, a ratio between uplink and downlink traffic should follow the findings of [16].

Table 1. Proportion of the transmitted traffic

Application	Ratio of transmitted data
Voice	10 %
FTP	8 %
HTTP	22 %
Video/Gaming	57 %
M2M/Database access	1 %

Performance measures

In order to verify if there are any noticeable improvements that could be perceived by the end-users, especially regarding the

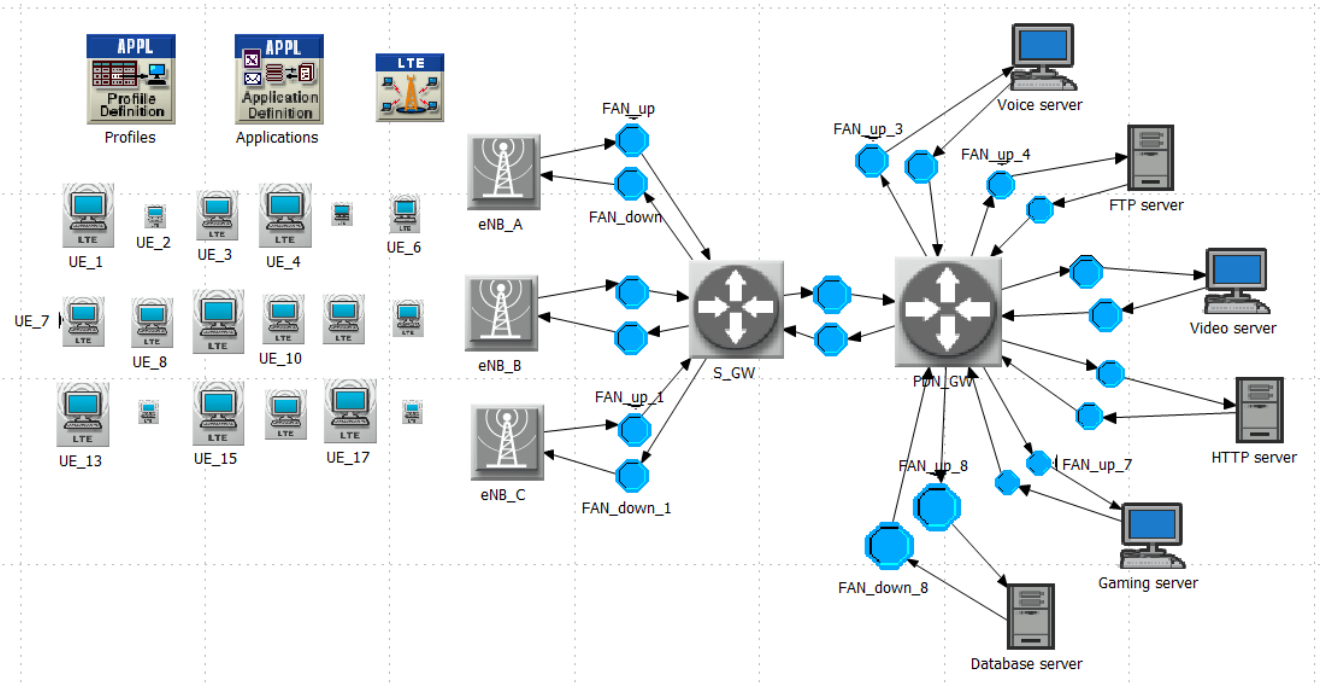

Figure 7: Network topology used in simulations

VoIP service, focus is put on statistics collected by the application layer at connections' end-points.
The performance of each of the five types of applications is assessed in various ways, mainly using time-related statistics:

- The Voice transmission is evaluated using Mean Opinion Score (MOS) value, which grades quality of received voice in range between 1 and 5. The higher the value, the better quality of the sound, with 5 denoting excellent quality [17]. MOS value is estimated by OPNET built-in functions basing on the packets loss and delay.
- The FTP application is evaluated by time (in seconds) it takes to complete a FTP operation (upload or download).
- The HTTP application is evaluated by time it takes to download a complete website with all objects.
- The database access is evaluated using time it takes to complete a given task (database query or entry).
- The gaming and video communication are evaluated by end-to-end packet delay expressed in seconds.

Network topology

The main series of simulations has been run using the topology presented in Figure 7.

There are three eNBs in the network, serving 18 UEs. The eNBs are connected through the Serving Gateway to the Packet Data Network Gateway, which provides access to external network, where 6 application servers are located.

The radio links between the eNBs and the UEs have been configured to use the biggest available LTE bandwidth of 20 MHz. This allows achieving peak rates of 100 Mbit/s in downlink direction and due to that the wireless link should never be a point of bottleneck [3].

Comparison with DiffServ

In order to assess performance of FAN it was confronted with:

- DiffServ using the same network topology and traffic
- pure-IP network (without any QoS mechanism) also using the same topology and traffic.

The results of comparison are shown in Table 2 and Figure 8.

Table 2. Simulation results. The values of bytes sent and received are collected at the application layer.

Statistic	QoS	value	Bytes sent	Bytes received
MOS value of voice signal	none	2.12	910 530	821 188
	DiffServ	2.00	910 490	796 602
	FAN	3.52	910 103	900 191
FTP download time (s)	none	failed	1 011 358	247
	DiffServ	failed	1 322 545	322
	FAN	738.27	1 400 341	622 564
HTTP object response time (s)	none	2.05	1 158 137	161 362
	DiffServ	2.68	1 004 744	148 613
	FAN	1.91	11 993 391	1 699 534
Video/Gaming - packet delay (s)	none	0.364	39 050 298	453 081
	DiffServ	0.313	58 183 665	430 999
	FAN	0.233	19 681 253	4 218 227
Database - response time (s)	none	7.439	282 916	5 912
	DiffServ	2.261	228 379	4 226
	FAN	failed	0	0

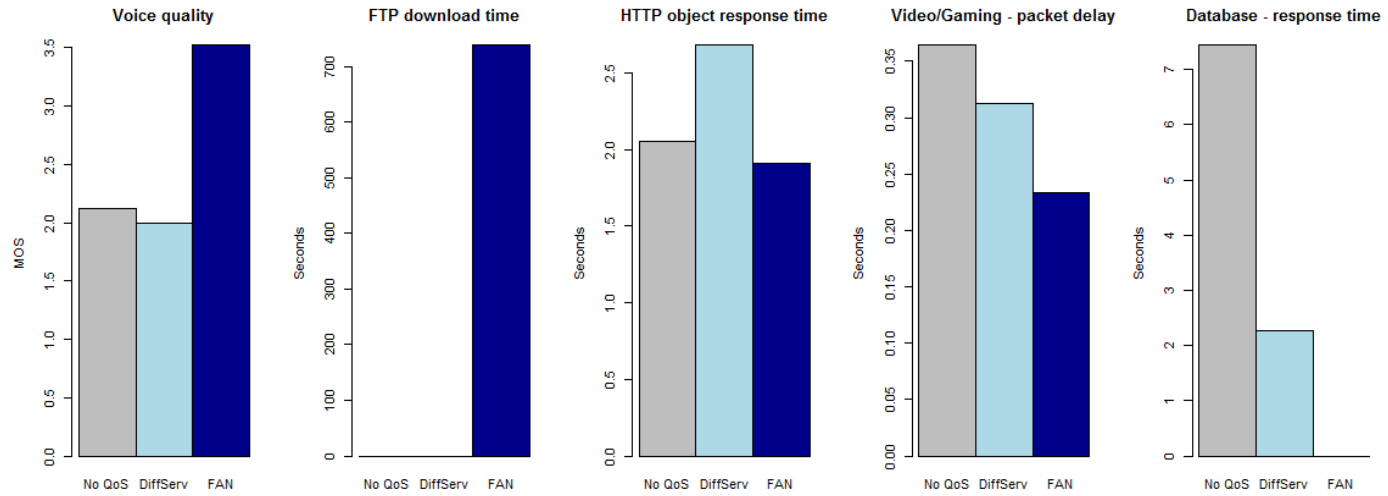

Figure 8. Simulation results.

Note, that the scenarios were supposed to illustrate a heavily overloaded network in order to verify performance during congestion. That is why, in all the scenarios, many of bytes sent by the applications were not delivered and blocked due to the lack of capacity.

DiffServ was configured to classify traffic into three classes depending on the application:

- Expedited Forwarding class for the voice application
- Assured Forwarding class for the gaming & video applications
- Best-Effort class for the remaining applications

The applications in the pure-IP network performed badly due to the overload. Especially, the quality of the received voice was unacceptably low.

Results obtained in the DiffServ scenario were very similar to the pure-IP scenario. The gaming/video applications, which were to be prioritized, were the only applications performing better. They experienced a lower packet delay than in the pure-IP scenario. However, the quality of the received voice, which also was to be prioritized, was even slightly worse than in the pure-IP scenario. The DiffServ-enabled backbone did not provide any admission control what was a reason for poor performance of the applications. The lack of the admission control made the network prone to a large number of incoming requests.

Results obtained in the FAN scenario were much better. Still, there were losses, due to the heavily loaded network, but the FAN mechanism improved transmission quality significantly. Voice communication was the best performing application, as intended. The final MOS of the received voice reached a high score of 3.5. The delay of the gaming application was reduced significantly by over 33% and, what is the most important, considerably less data was lost. The only application, which performed worse, was the database access, which was blocked due to the congestion. However, it did not perform well in the other scenarios either and the small amount of delivered packets in the other scenarios would probably be of no use to the end application.

The results prove that FAN ensures a high-quality voice communication in the LTE backbone, which is carrying heterogeneous applications.

Conclusions

This paper presented Flow-Aware Networking (FAN) as a new method for providing a Quality of Service mechanism in the IP-based transport network underlying the LTE backbone.

It has been proven that FAN may be a valid alternative to DiffServ. It not only performs better in a heavily loaded network, but also it is simpler in implementation and does not require so much configuration effort.

The collected simulation results show that FAN, despite its simplicity, is a very effective way of ensuring stable and low-delay transmission of real-time and streaming traffic. Thus, FAN prioritizes the most profitable communication services, which allow charging customers per usage time, such as the voice calls. This should be of great interest to network operators, because the voice traffic still generates 69% of their revenue [4].

Moreover, FAN allows for effective congestion protection. Combined with an over-provisioning of network capacity, it creates a reliable and efficient system. In FAN no resources are lost due to overbooking or inadequate traffic estimations [9], thanks to the self-managed algorithm that does not require explicit classification or resource reservation.

Finally, the project has shown that OPNET is an efficient tool that provided possibility to simulate SAE network with all its advanced protocols and mechanisms.

References

[1] Cisco Systems, Inc., “Global Mobile Data Traffic Forecast Update, 2010-2015”, *Cisco Visual Networking Index*, 2011.

[2] M. Olsson, S. Sultana, S. Rommer, L. Frid, and C. Mulligan, “SAE and the Evolved Packet Core. Driving the Mobile Broadband Revolution”, *Elsevier Ltd*, 2009.

[3] Alcatel-Lucent, “Long Term Evolution (LTE) Overview”, 2008.

[4] RAD, “LTE Backhaul: Meeting Operator Requirements”, *RAD Data Communications Ltd*, 2009.

[5] K. Bogineni, R. Ludwig, P. Mogensen, V. Nandlall, V. Vucetic, B. K. Yi, and Z. Zvonar, “LTE PART I: Core Network”, *IEEE Communications Magazine*, February 2009.

[6] Rohde and Schwarz, “UMTS Long Term Evolution (LTE) Technology Introduction”, 2008.

[7] S. Oueslati and J. Roberts, “A new direction for quality of service: Flow-aware networking”, *France Telecom R&D*, 2005.

[8] A. Kortebi, S. Oueslati and J. Roberts, “Cross-protect: implicit service differentiation and admission control”, *France Telecom R&D*.

[9] T. Bonald, S. Oueslati-Boulahia, J. Roberts, “IP traffic and QoS control: the need for a flow-aware architecture”, *France Telecom R&D*.

[10] J. W. Roberts, “Internet Traffic, QoS, and Pricing”, *Proceedings of the IEEE*, 2004.

[11] J. Domzal and A. Jajszczyk, “Approximate Flow-Aware Networking”, *IEEE Communications*, 2009.

[12] J. Domzal, R. Wojcik, and A. Jajszczyk, “QoS-Aware Net Neutrality”, *First International Conference on Evolving Internet*, 2009.

[13] E. Mingozzi, L. Lenzini, and G. Stea, “End-to-End Quality of Service Over Heterogeneous Networks”. *Spriner*, 2008.

[14] 3rd Generation Partnership Project, “TS 29.281: General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)”, *Technical Specification Group Core Network and Terminals*, 2011.

[15] A. Jajszczyk and R. Wojcik, “Emergency Calls in Flow-Aware Networks”, *IEEE Communications*, 2007.

[16] Cisco Systems, Inc., “Usage”, *Cisco Visual Networking Index*, 2010.

[17] International Telecommunication Union, “P.800: Methods for subjective determinatio of transmission quality”, *Series P: Telephone Transmission Quality*, 1996.