Middleboxes in Cellular Networks

Szilveszter Nádas, Salvatore Loreto
Ericsson Research,
Szilveszter.Nadas@ericsson.com, Salvatore.Loreto@ericsson.com

November 4, 2014

Abstract

This is a position paper regarding the role of middleboxes and middlebox layer in an evolved protocol stack. The focus of the paper is on the requirement of cellular networks, but the statements are not limited to cellular systems. The paper describes relevant properties of cellular networks and discusses the related roles of the middleboxes. It addresses how a middlebox layer may support these roles. Finally it provides considerations about the incentives of the actors and security questions.

1 Cellular Networks and Mobile Broadband

In cellular networks the congestion level of a single flow is more variable than over fixed access. The two main contributors are the variability of air interface channel quality between the radio base station and the user equipment and the fact the resources of a radio cell are shared among all active users in that cell. Sometimes even the Mobile Backhaul connecting the Radio Base Stations to the rest of the network can be such shared bottleneck. Because of this variability and of the cost of the radio resources, *optimizing resource sharing* among streams is even more important than in case of fixed Internet access. It can be advantageous to optimize resource sharing among the streams of the same user, and also to optimize resource sharing among the streams of different users. We define the term flow as all the packets in both directions an application sends between the same server and client. The flow may contain several streams, which may have different performance demands.

In Cellular Networks the Radio Resource Management algorithms [1] are responsible ensuring the high efficiency of the usage of the radio resources, e.g. by waiting for the right channel quality before transmission and to allocate and release radio channels. To ensure high performance, explicit information about the streams is beneficial, such as *classification of the stream* with respect to packet delay requirement, chattiness of the stream

or the Transport Protocol used. The provided information can be used to find the right optimum between waiting for the right channel quality and minimizing delay for the critical applications.

Cellular networks often implement similar protocol functions as Transport Protocols do. This redundancy may be costly in overhead or processing. It may also cause unwanted interactions between those protocols. When knowledge about both the Transport Protocol and the cellular network is available *this redundancy may be minimized*.

Two examples for optimization:

- Reliable transmission is implemented in Radio Link Control Acknowledged Mode (RLC AM). Some transport protocols (e.g. [2]) also propose Forward Error Correction to ensure timely and reliable delivery. In the RLC AM loop this FEC is unnecessary and can be optimized.
- RLC AM functionality is redundant with TCP reliable transmission. Still, RLC AM reliable transmission is necessary, because even the very small error rate of the lower layer retransmission over the radio channel would cause TCP congestion response and that would make it impossible to reach high enough throughput.

2 Roles of Middleboxes

In order to support the abovementioned features we identified the following middlebox roles. Other important roles, e.g. firewall, NAT and parental control are not discussed here.

Middleboxes can act as *Policy Decision Points*: they select domain specific QoS solution of flows, streams or packets based on traffic identification, flow states and/or packet handling information. Traditionally in case of broadband traffic DPI/SPI boxes perform this role.

Middleboxes can provide *information about the network path* (e.g. maximum achievable bitrate, minimum delay, etc.) to aid path selection, for example to help end-point decide which access to use, when there are several alternatives. This information can be static or dynamic, which also describe the state of the network in addition to the optimal/typical capabilities of the network.

Middleboxes might *send advisory messages* to applications to help adaptation. Examples for such advisory messages are to provide an initial congestion window, to help adaptation in case of adaptive media, or to tailor the service directly, based on of the congestion status of the network.

Middleboxes can also provide *transport protocol enhancement* in several layers. They may optimize FEC and retransmission. They may completely replace the used transport protocol to optimize it to the properties of the local domain.

Middleboxes can provide *application layer optimization*, e.g. HTTP proxy, transcoding, caching. This functionality cooperates with the application layer in an end-host. Middleboxes can act as a gateway and translate between application protocols used in the different domains. For example; translate between HTTP2 used in the cellular network with HTTP1.1 used in the Internet.

3 Role of a Middlebox Layer

There are several ways to support the abovementioned goals. Middleboxes may act on/replace transport and/or application protocols. While this is a very flexible and versatile approach, it also has the largest impact on end-user privacy. We think that in order to get end-host cooperation, a light-weight approach shall also be possible, with keeping the more versatile approach as an option for more cooperating end-hosts.

In order to support the abovementioned goals a middlebox layer may be introduced. A new standalone middlebox layer in the protocol stack has advantages compared to including similar functionalities natively in a Transport Protocol or in the Internet Protocol. The middlebox layer is proposed to be between the IP and Transport Protocol layers. To support deployment in legacy environment it may be over UDP/IP. Because it is a separate layer below the transport protocol it allows the middleboxes to be transport protocol independent and it can be used even for legacy transport protocols.

The middlebox layer may have a middlebox header, which has static fields and may also be extended by extension headers. This header may be between the UDP and the Transport Protocol header.

For some of the middlebox roles exchange of signaling messages is needed either in-band or using a separate signaling connection. The protocol used for this communication and whether it is to be standardized is outside the scope of this paper.

The middlebox layer may use a pre-configuration procedure, which can be executed when a device is connected to a domain. This is especially useful for application layer optimization, because in this case already during the setup of the flow the middlebox can be addressed.

4 End-host Consent, Incentives and Security

Clear incentives are needed for the involved actors (OTTs, Network Operators, End-Users, OS developers) to cooperate thorough middleboxes. We believe that such incentives can be found for the above listed middlebox functionalities. We refer to the paper [3] in this area.

The need to provide security and confidentiality to the end user is driving a considerable usage of (D)TLS to encrypt the Application Protocol traffic. At same time this need has triggered a discussion and also work in IETF on how to provide security natively in a Transport Protocol. Both those trends are reducing the possibilities for the middleboxes to provide transparent optimizations. A newly introduced middlebox layer might allow some transparent optimization possibilities; for example if the protocols allow the middlebox to understand the traffic characteristics, then the middleboxes may provide Policy Decision without explicit consent of the end-points. When there is a signaling exchange with a middlebox it is an intentional action by one of the end-hosts and thus it cannot be transparent.

Information about the network path is also a sensitive data and different network operators may allow different types of information to be communicated towards the end-points. In a collaborative environment, the network operator should also have clear incentives to reveal this information. Therefore middleboxes should have a configurable mechanism in which the middlebox owner decides what type of information that can be exposed outside to internet applications. For example information on the radio network such as congestion level or maximum possible throughput.

The security association of end-to-end protocols shall not be available in the middleboxes, unless those protocols are terminated in the middlebox. Therefore any kind of middlebox communication must have separate security association if any. Middleboxes should be identified with a valid certificate, when possible. Handling encryption for signaling messages is relatively straightforward and should be implemented. Header fields and extension headers may also use encryption or authentication.

5 Conclusion

This paper discusses issues of cellular systems, which can be optimized by the use of middleboxes: the high variability of congestion, finding the optimum between good radio channel and small delay and redundancy in protocol functions. We introduce middlebox roles: providing traffic identification and network information, exchanging advisory messages and optimizing transport and application protocols. We describe middlebox layer, which provides a light-weight approach to provide or support these roles. Finally we discuss the need for incentives of all involved actors and security aspects.

References

[1] Dahlman, Parkvall, Skold, Beming: 3G Evolution: HSPA and LTE for Mobile Broadband, 2nd Edition, pp 286, pp527-528

[2] http://www.chromium.org/quic, checked 2014-10-29

[3] David D. Clark et all, Tussle in Cyberspace: Defining Tomorrows Internet, IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 13, NO. 3, JUNE 2005, https://impact.asu.edu/cse534fa06/reading/p462-clark.pdf