2017-06-02

Challenges of future multimedia QoE monitoring for internet service providers

Robitza, W

10.1007/s11042-017-4870-z
Multimedia Tools and Applications
Springer Science and Business Media LLC

Multimed Tools Appl
DOI 10.1007/s11042-017-4870-z

Challenges of future multimedia QoE monitoring for internet service providers

Werner Robitza[1] · Arslan Ahmad[2] · Peter A. Kara[3] · Luigi Atzori[2] · Maria G. Martini[3] · Alexander Raake[4] · Lingfen Sun[5]

Received: 26 October 2016 / Revised: 20 April 2017 / Accepted: 9 May 2017

Abstract The ever-increasing network traffic and user expectations at reduced cost make the delivery of high Quality of Experience (QoE) for multimedia services more vital than ever in the eyes of Internet Service Providers (ISPs). Real-time quality monitoring, with a

✉ Werner Robitza
werner.robitza@gmail.com; Werner.Robitza@telekom.de

Arslan Ahmad
arslan.ahmad@diee.unica.it

Peter A. Kara
p.kara@kingston.ac.uk

Luigi Atzori
l.atzori@ieee.org

Maria G. Martini
m.martini@kingston.ac.uk

Alexander Raake
alexander.raake@tu-ilmenau.de

Lingfen Sun
l.sun@plymouth.ac.uk

[1] Telekom Innovation Laboratories, Deutsche Telekom AG, Ernst-Reuter-Platz 7, 10587, Berlin, Germany

[2] Department of Electrical and Electronic Engineering, University of Cagliari, Via Università 40, 09124, Cagliari, Italy

[3] WMN Research Group, Kingston University, Penrhyn Road, KT1 2EE, UK

[4] Audiovisual Technology Group, TU Ilmenau, 98693, Ilmenau, Germany

[5] School of Computing, Electronics and Mathematics, University of Plymouth, Drake Circus, Devon, Plymouth, PL4 8AA, UK

Published online: 02 June 2017

focus on the user, has become essential as the first step in cost-effective provisioning of high quality services. With the recent changes in the perception of user privacy, the rising level of application-layer encryption and the introduction and deployment of virtualized networks, QoE monitoring solutions need to be adapted to the fast changing Internet landscape. In this contribution, we provide an overview of state-of-the-art quality monitoring models and probing technologies, and highlight the major challenges ISPs have to face when they want to ensure high service quality for their customers.

Keywords Telecommunications · Network monitoring · Quality of experience · Quality of service · Service monitoring · Encryption · Service defined networks · Network function virtualization

1 Introduction

In our world of rapidly evolving multimedia services, requirements on networks are growing every day. Services become more and more real-time and require higher bandwidth (e.g., Ultra-HD (UHD) video, telepresence, Virtual Reality (VR), gaming and the Internet of Things (IoT)), putting the network performance of Internet Service Providers (ISPs) under critical highlight. This holds true especially for ISPs delivering third party content from Over-the-Top (OTT) providers (e.g., *YouTube* or *Netflix*). In this ecosystem, all stakeholders aim to provide great experience for their customers — defined as Quality of Experience (QoE). QoE is the "degree of delight or annoyance of the user of an application or service. It results from the fulfillment of his or her expectations with respect to the utility and / or enjoyment of the application or service in the light of the user's personality and current state." [25] While this definition is commonly accepted and used in the research domain, traditionally, Quality of Service (QoS) approaches and their associated Key Performance Indicators (KPIs) (e.g., delay or jitter) are the core of monitoring solutions, which are deployed by the industry. Research has shown that raw QoS measurements and the associated KPIs are not necessarily a reliable predictor of QoE [6, 13], which is why modern QoE models focusing on perceptual characteristics of the monitored systems can help at providing a user perspective, based on measurements from the network.

Quality monitoring is one of the first steps in a "quality engineering" process that ISPs implement to ensure the best experienced quality for their customers. The values obtained from measurements are used for getting insight on the current state of the network, but also for managing traffic and providing input for economic decisions. It must therefore be ensured that the acquired data is valid in the sense of providing the ISPs with a representative view of customer-experienced quality. At the same time — in addition to quality — ISPs monitor other parameters in the network, for example related to security and billing. In this paper however, we want to exclusively focus on the quality monitoring step as an input to other important business processes. Figure 1 shows the most important network-related monitoring and management processes for an ISP and highlights the concepts under study in this paper, namely QoS and QoE monitoring and the respective interfaces to ISP traffic management.

In our perspective — despite the advent of new "killer applications" such as cloud gaming and VR — there are still challenges that need to be addressed by ISPs with regard to the monitoring of "classic" services like video and speech. As researchers and practicioners in the domain of quality monitoring, we still observe a discrepancy between ongoing research

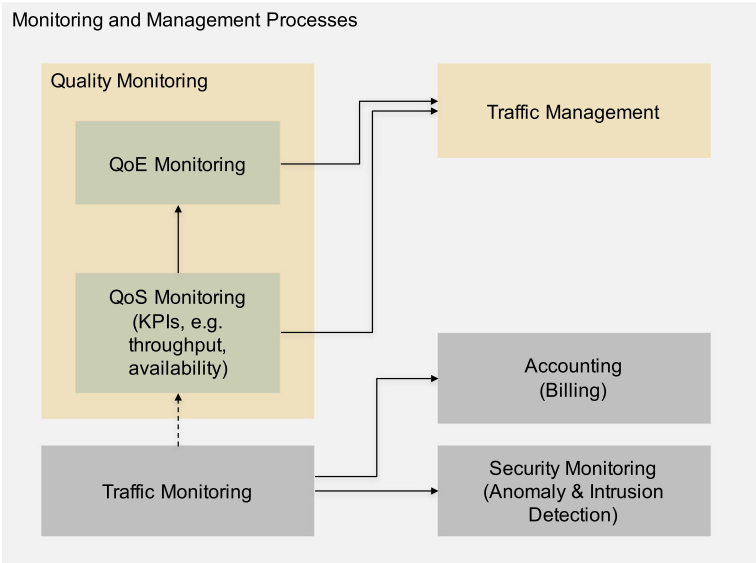

Fig. 1 Concepts related to ISP monitoring and management

and the practical implementation of monitoring solutions, where operators still often take a network-centric perspective, not fully taking into account user factors and QoE.

In this paper, our first presented challenge is based on asking ourselves what ISPs should optimize a network for: should it still be just best-effort bandwidth, or can a new and more comprehensive focus on tailoring services to user QoE increase the satisfaction level for all users? This calls for new monitoring approaches to ensure that the required user-centric QoE data is accessible for later traffic management steps.

High-performance probing systems may allow ISPs to monitor thousands of connections simultaneously and provide diagnostic analyses as well as QoE estimations. However, peeking into all media streams transmitted over a network, capturing user-specific information touches the critical subject of customer privacy. Here, OTTs have reacted by encrypting their streams; the increased amount of application-level encryption however prevents the ISPs from accessing the same data that their monitoring systems relied on for precise quality measurements. Instead, ISPs will see less information, from which they have to estimate QoE. This paradigm shift presents a big challenge for ISPs and calls for new measurement approaches and redesigns of monitoring systems.

Another set of challenges that we will discuss are rooted in fundamental devleopments in Internet architecture; they relate to how the Internet has evolved over the last years and will continue to change in the near future: the rise of Software-Defined Networks (SDNs) and Network Function Virtualization (NFV) will allow for more diverse and scalable monitoring solutions, but can come with drawbacks due to the increased complexity and abstraction of the system architectures.

Softwarization and virtualization technologies also bring other advantages. In such a scenario, network components are equipped with embedded software procedures; these allow for an easier introduction of new quality models, which is required in monitoring procedures to follow the fast evolution of the deployed applications. Another category of new

applications is related to the Internet of Things (IoT). Here, physical (multimedia) sensing devices are being deployed for collecting information about our physical world. These sensors are often virtualized through agents which act as their representatives. All the sensed data is conveyed through them while being processed and cached if needed. These *virtual objects* are promising candidates for the monitoring of the perceived quality.

In this article, to provide a suitable context for the challenges later described, we first give an overview of the history and current state of QoS/QoE monitoring solutions. Then, we discuss the above-mentioned challenges from a perspective of researchers and practitioners in the field of QoE monitoring. Our contribution is a discussion of all these aspects with links to current research, as we believe there is a need to raise awareness of those challenges.

2 From quality models to probes and monitoring systems

In this section, we describe the components of typical monitoring systems. We first focus on monitoring approaches from a historical perspective, then describe types of quality models, which are typically integrated in probes. These are devices that are placed in the network with the purpose of measuring its performance and delivering data to characterize the quality of services running on that network. Finally, we talk about different ways to organize monitoring systems.

2.1 From KPIs to modern quality models

From a historical perspective, we can observe different developments in the approaches for network and service quality monitoring. As mentioned before, early generations of performance monitoring were technology-centric rather than user-centric, with the main focus on defining and monitoring KPIs, usually at the lower layers of the Internet protocol stack (e.g., IP layer). In this regard, the metrics defined by the IETF IPPM working group assume a key role even today. They focus on the measurement of quality, performance and reliability of protocols and services that operate on top of the IP layer [7]. Standards by the International Telecommunication Union (ITU-T) also play a role here: ITU-T Rec. Y.1540 defines parameters used for assessing the speed, accuracy, dependability, and availability of IP packet transfer services. ITU-T Rec. Y.1541 specifies performance objectives to be achieved. Finally, to implement monitoring systems, NetFlow and IPFIX are protocols that are often used to capture flows in selected points of the network [21]. While this kind of monitoring is still of great importance and widespread use today, the results obtained from IP-level measurement cannot be directly used for a precise prediction of application-level QoE. Hence, we will focus on the latter aspect in more detail.

In order to find out how certain KPIs relate to user-perceived QoE, starting with the beginning of the last decade, *QoS–QoE relationship models* have become more frequently used. Here, certain QoS parameters are mathematically related to QoE values, usually now taking into account more application-level related parameters. For example, instead of just investigating IP packet statistics to quantify the level of quality for an IPTV stream, RTP traffic can be taken into consideration too. These QoS–QoE models were mainly built for voice and video services, which means that they are lacking universal applicability for other services [6]. We will talk about these models in detail in the next section.

In the recent years, a shift from traditional technology-centric QoS models to more holistic user-centric QoE models could be observed [8], although QoS–QoE mapping models

are still used. A common approach for such QoE models is to predict QoE from a multi-dimensional space. These models differ from QoS–QoE relationship models: several other parameters — which are not measurable by traditional KPIs — are taken into account. This category is referred to as "context-aware", since the (user) context has become essential in the modeling of the user-perceived quality. Algorithms based on machine learning and artificial intelligence are gaining interest in this scenario due to their potential for higher adaptability, reliability and robustness over statistical and parametric/probabilistic models [15].

2.2 Quality models

Quality models automatically provide a value of quality based on a certain input, much like if we asked a human observer to rate a given stimulus (e.g., a ten-second video clip). While researchers may use them in the lab to conduct experiments "offline", they are typically implemented in network probing devices in order to allow for automated QoE calculations. We can classify QoE models based on the information they use, according to [35]: as shown in Fig. 2, we can define *No-Reference* (NR), *Reduced-Reference* (RR), and *Full-Reference* (FR) models, depending on whether they have no, partial, or full access to a source signal. FR models compare the source signal with the received one, for example, an automated telephone call that was recorded both at the source and the receiving end. Since both signals are required for quality calculation, data transfer of the signals is often required. This makes it impractical to use these models at remote ends, especially when large video traffic has to be inspected. In order to reduce the amount of information needed, RR and NR models typically operate on the client side only. RR models receive an auxiliary channel of information, whereas NR models only inspect received signals. They therefore require less data, which typically comes at the cost of lower accuracy [38].

Another form of QoE model classification is visualized in Fig. 3: *Signal-based models* (or *media-based models*) work on the levels of pixels and samples only; they assume full access to data and decoding capabilities. *Hybrid models* combine signal information with bitstream-level information, such as packet headers. *Parametric models* only operate on transmitted packet-level or bitstream-level information, or — in the case of so-called *planning models* — assume no actual transmission, but can be used for designing networks with a certain service in mind. Naturally, a model with access to more information (e.g.,

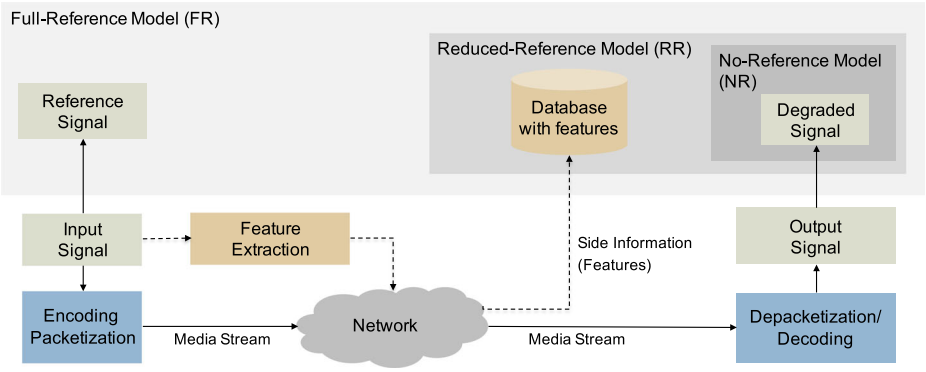

Fig. 2 Model classification according to information available from source

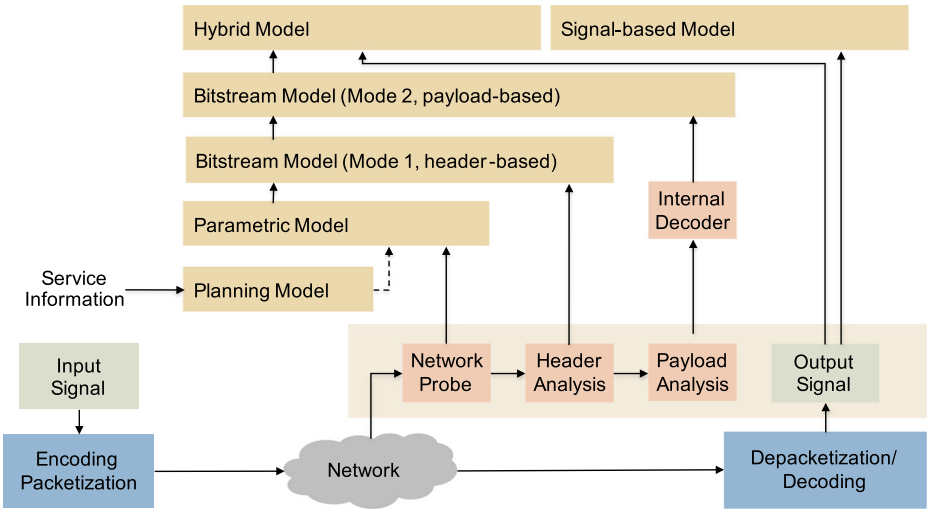

Fig. 3 Model classification according to information extracted from the transmission, based on [35]

decoded video frames instead of just packet headers) should provide a more accurate estimation of the quality, but in practice — and as we will see later — the amount of information accessible is often influenced by several extrinsic factors beyond control of the ISP.

The International Telecommunication Union (ITU) has standardized a number of quality models for different services. A comprehensive overview of these models was already given by Raake et al. in 2011 [35], however, since then, several new models have been standardized. ITU-T Rec. G.1011 provides a reference of all ITU models for quality estimation and compares their application areas, which helps practitioners in choosing the right model for a given service. Among the most notable models for speech quality evaluation are the Full-Reference ITU-T P.862 (PESQ) and ITU-T P.863 (POLQA) and the parametric ITU-T G.107 ("E-Model"). For video quality estimation, we highlight ITU-T J.144/J.247/J.341 as FR models, and ITU-T P.1201/P.1202 as parametric models for IPTV-type transmissions. An important recent ITU development for media quality assessment is the ITU-T P.1203 family of recommendations, which describes a comprehensive, parametric bitstream-based quality model for HTTP adaptive streaming services. This model consists of an audio and video quality prediction component and a temporal integration component, the latter of which takes into account player-level indicators such as stalling events and audiovisual quality variations.

Of course, apart from standardization efforts, the scientific community and video providers have also released a plethora of quality models; their listing is beyond the scope of this paper. Further models for video quality assessment can be found in [13]. Another recent example is Video Multi-Method Assessment Fusion (VMAF) by Netflix [1]. Still, we believe that the use of standardized models for monitoring — rather than internally developed or proprietary tools — allows for a better understanding of the obtained quality estimations; it also allows different technologies and the monitoring results of different ISPs to be compared.

Current models often assume transmission via long-established Internet protocol standards such as UDP and TCP at the transport layer, RTP, and HTTP at the application layer.

However, major developments such as HTTP/2 will challenge existing models that, for example, try to predict video buffer states and web page loading times (for websites) to adapt to new transmission techniques. New protocols such as Google's proprietary Quick UDP Internet Connections (QUIC), submitted for standardization to the IETF, will require completely different approaches to modeling web traffic.

2.3 Probes

Probes are devices that extract and process information sent over a network (e.g., counting and forwarding packets). They may implement quality models as described above, but they can also be exclusively used for simple network traffic monitoring. We can categorize probes into *active* and *passive* ones. Active probes initiate data transfer. For example, they could start a telephone call to another probe, or request a video from a remote server using a browser running on a PC. Passive probes inspect traffic that passes through them without interfering. This distinction becomes very important in terms of how much and which kind of information can be captured, and how much control an operator has over that information. Active probes typically provide more detailed and reliable information from a user perspective, but they just capture a small sample from an entire network or a network branch. Passive probes typically provide more coarse quality predictions, but offer a better overview of the quality across a whole network or network branch. Passive probes also have the advantage of not generating additional media traffic, whereas active probes may deteriorate already bad network quality by putting additional load on the network paths they operate in. However, comparing the amount of data generated by a single probe in a certain location to the possible traffic requirements of a larger population of real customers, this impact is typically neglected in practice.

By analyzing the major Internet performance monitoring platforms, we concluded that there is not a strong preference between software and hardware probes. SamKnows, BISmark, and RIPE Atlas are examples of platforms that deploy dedicated hardware-based probes, whereas Dasu, Netradar, Portolan and perfSONAR rely on software installations for some hardware systems [7]. (It should be added that these probe systems do not implement higher-level QoE models, but are more typically used for QoS assessment.)

Hardware probes are able to gather round-the-clock measurements, whereas software measurements are more susceptible to resource contention from other applications and are harder to calibrate, but on the other hand have lower distribution costs. Performance is also an issue: surveying the market, one can find a number of offers for probes that monitor network performance on lower levels (e.g., IP). However, for estimating QoE for multimedia systems, higher processing power (e.g., for decoding UHD video streams and performing signal-based analysis) will be necessary. Here, hardware solutions are still more prevalent and practical.

2.4 QoS/QoE monitoring systems

A complete QoS/QoE monitoring system consists of one or multiple probes, placed in specific locations in a transmission chain, with the purpose of determining the quality of a service at a given point in time, for a certain location. Since probes may just forward captured information, with the quality calculation happening at a central location, we identify two distinct points [8]: 1) the monitoring point, at which information is collected, and 2) the quality estimation point, at which the information is used to calculate a quality indicator.

In Fig. 4, we give an overview of a typical situation in which an OTT provides content to a customer. The OTT ingests content to a Content Distribution Network (CDN), which again is peered to an ISP's core network. The ISP provides access to the customer via an access network. Generally, we refer to client-side and network-centric monitoring. In case of client-side monitoring, the probe is placed in the customers' premises, as suggested by the name. However, network-centric monitoring is not so self-explanatory: it refers to placing the probe either in an access network, or in the core ISP network.

Figure 4 also shows the tunnels that may exist in case of end-to-end encryption between an OTT and a customer. Content encryption — such as video bitstreams protected by Digital Rights Management (DRM) — has its server-side endpoint at the OTT. CDNs are typically the endpoint for application-layer (e.g., TLS-based HTTPS) encryption. We will later refer to the challenges that ISPs face because of these data tunnels when it comes to QoE monitoring.

What are the advantages and disadvantages of the network- and client-centric approaches? The client-centric method places a probe either at a real customer's location or at a representative access point. For example, a probe may be set up behind the router at users' homes, if they agree to be surveyed. Such a probe is able to capture detailed information, taking into account events happening beyond the access network (e.g., low WiFi performance or faulty routers, wrongly configured DNS settings). However, a large drawback is the much lower number of streams that can be measured when compared to a network-centric probe. For each location, a new device has to be placed (although with virtualization, as we will see later, this issue can be mitigated). Setting up a probe at a real user's location however raises privacy concerns.

The network-centric approach is very efficient: with the respective equipment, multiple network streams can be analyzed in parallel. The challenge here lies in dissecting the data streams and choosing the type of information to monitor. In such a case, it is not always obvious how to take into account degradations that happen beyond the monitoring point. For example, it is more difficult to diagnose end-user equipment problems (such as the ones stated above). Here, the fact that most traffic is connection-oriented helps in troubleshooting, but more detailed traffic inspection (Deep Packet Inspection, DPI) is needed to reveal more information.

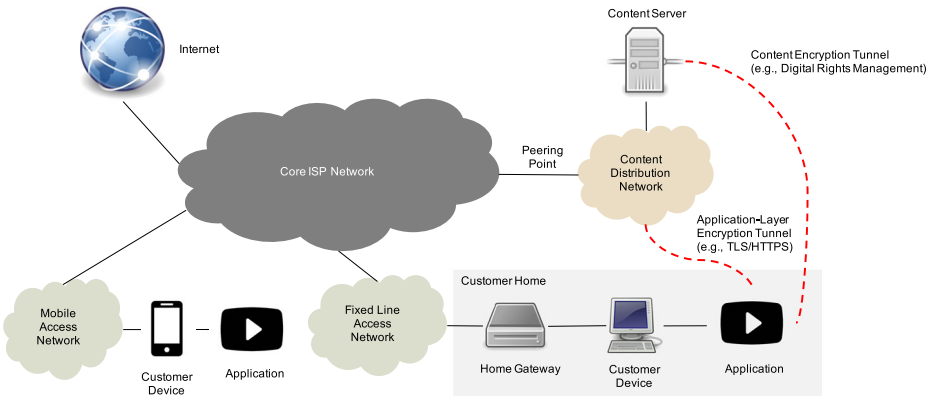

Fig. 4 Simplified network topology for OTT media services delivered to fixed/mobile-network consumer. *Dashed lines* indicate encrypted payload

Futhermore, network-centric monitoring does not consider the multi-dimensional aspects of QoE. Beyond the network attributes, these aspects include the application, the system, the context and the user behavior itself [36]. This consideration is particularly highlighted in [39], where QoE is represented as a multi-layered vector. This concept is called the *ARCU Model*, and each influencing factor is looked at as a set of measurable KPIs. DPI is not applicable in this scenario because it can only classify QoE-relevant traffic characteristics if the traffic is not encrypted. We will later discuss how encryption can be handled for QoE monitoring, however, the factors of context and user behavior will be still missing in that information [22]. The state-of-the-art therefore asks for monitoring QoE by placing the probes not only at the client side, but *in* the user terminal [2, 3, 11, 12, 42].

Although the work in [2, 11, 42] includes application-level KPIs in QoE monitoring — highlighting that application-level monitoring is indeed important — these approaches do not consider the context, system, and user factors. The work in [12] considers battery usage as well as application- and network- level KPIs for QoE monitoring. The work in [3] proposes a multi-layered approach for QoE monitoring by considering the application- and network-level KPIs in combination with system-level resources, user location (for the context) and user profile. The authors achieve this through a probe at the user terminal. The major challenge in this regard is the monitoring of the context. Moreover, the selection of optimal operating frequency of a user-end passive probe remains an open issue: the monitoring application at the terminal may require system-level resources which can also affect the performance of the other application [3]. Therefore it is sensible to combine both client-side and network-centric probes for a more accurate and more holistic quality estimation.

As a last thought on monitoring systems, it needs to be stated that QoS and QoE monitoring are merely subsets of general network monitoring practices. This inclusion also particularly applies to the tools and applications of such activities. However, their primary challenges — especially in case of QoE monitoring — fundamentally differ, whether we consider present or future challenges. The following section of this paper focuses on the discussion of such QoS- and QoE-related challenges.

3 Future challenges and discussion

Today's Internet is constantly changing its shape: new media services are created, bandwidth availability and requirements are becoming higher and higher by the day, and customers' expectations are changing, adapting to these newly emerging services and novel end-user applications. In this process, ISPs will reach certain limitations and thus face challenges, examples of which we will address in this section.

3.1 Optimizing user satisfaction

Currently the majority of ISPs handle Customer Experience Management (CEM) on the consumer side as a set of KPIs [34], which they consider to be sufficiently reliable representations of actual user experience. For instance, although the perception of service quality indeed correlates to some extent with the number and duration of rebuffering events, these are not the only factors affecting it. From a business perspective, ISPs still primarily focus on these KPIs, since the notion of QoE and its monitoring have just recently appeared as a determining factor among ISP goals. We expect that in the future, monitoring will (and has to) become much more user-centric.

One application of quality monitoring is to measure the compliance of the provided service with a Service Level Agreements (SLAs). These are often set up with customers such as peering partners. In this context, traditional QoS monitoring is prevalent, since in those SLAs only KPIs of the offered services are considered, such as throughput, delay, and packet loss. The ISP's paying customers at the end of the delivery chain often only see a "light" version of such agreements, stating, for example, a maximum available bandwidth. It will be interesting to observe whether an equally important but more user-oriented quality level agreement will become adopted by ISPs. For example, a "Satisfaction Level Agreement" or "Experience Level Agreement (ELA)" [41] would tailor services to the consumers, ensuring a certain level of QoE. A new form of SLAs has already appeared, known as "Next-Generation SLAs" (NG-SLA), metrics of which relate to user satisfaction via business process efficiency [34]. An exciting future trend may also be the personalization of QoE based on individual needs, and optimization considering the interaction between the users of the service.

Current and future QoE optimization goals of ISPs can be approached in several different ways. The most basic approach for optimizing would be simply maximizing mean QoE values while considering financial investments and limitations to maximize the obtainable profit. This might sound general enough to apply to all ISPs, however, optimization does not necessarily happen in this manner. A more specific goal could be to minimize the %POW (percent of Poor Or Worse, see ITU-T Rec. P.910) value in order to maximize the number of service subscribers who do not reject the provisioned quality. By doing so, ISPs reach out for a greater expected number of service subscribers and compensate potential (investment) losses during their quest for improved quality. Similarly, ISPs could aim for maximizing %GOB (percent of Good Or Better, see ITU-T Rec. P.910). However, such a form of optimization — integrated into the business model — rather applies to the future than to the present, as ISPs currently still optimize for KPIs and for best-effort service provisioning rather than a measure of QoE.

Of course the business-driven, QoE-centric optimization of user satisfaction at first sight does not seem like a network monitoring challenge per se. The above considerations reach nearly every element of the value chain. Also, QoE-based customer agreements would necessitate high-level monetary decisions. Yet it needs to be noted that it is indeed a monitoring challenge in the sense of the required data, which must be collected from networks in order to comply with service agreements and to satisfy user requirements. The potential future trend of service personalization — and generally the involvement of individual needs in optimization — however raises the question of privacy, since such solutions rely on information implicitly or explicitly provided by the users. At the time of writing this paper, there is already an ongoing debate on the trade-offs between enhanced user experience through personalization and the protection of user data. This, on its own, is a considerable challenge for the present and the future.

3.2 Encryption and privacy aspects

The recent years have seen a rise in public awareness of privacy matters on the Internet. Since the leak of classified documents of the NSA in 2013, alleged "spying" by governments and ISPs has become a topic of public concern.[1] The IETF's RFC 7258 says, "Pervasive monitoring is a technical attack that should be mitigated in the design of [...] protocols,

[1]For more information, see the documents posted on http://www.theguardian.com/us-news/the-nsa-files.

where possible." In other words, we will see an increasing protection of all traffic on the Internet. Content providers realized the importance of protecting their user data: in the past years, therefore, OTT providers have switched to application-level encryption in order to offer better privacy to their users, such as with the use of SSL/TLS for HTTP or RTP. For example, *YouTube* force-redirects most of its users to a HTTPS version of their portal. Their mobile transmissions are mostly encrypted, too.

Since the raw payload of encrypted traffic is not visible except for the end points of the connection, such an encryption scheme offers tremendously increased user privacy. To ISPs, the transmission could now only be analyzed at the TCP or UDP layer. This makes it much more challenging to apply any quality model that depends on being able to operate on a level where typically, the send and receive times of application-layer packets has to be known. For example, a model for video streaming portals that estimates buffer levels and predicts video rebuffering events based on the transmitted HTTP chunks — such as proposed in [37] — will cease to operate. Similar situations can be envisioned for VoIP or IPTV transmissions using Secure RTP (SRTP). Models that use parameters from the transmitted audio and video codecs (such as resolution or bitrate) would be impossible to use, too. The ISP would only be able to see TCP/IP traffic patterns from a certain Autonomous System (AS) or a CDN to their customer and vice-versa. ISPs will have to find alternatives for monitoring, while still retaining user privacy.

In the last years, researchers have therefore studied how to estimate the user-perceived QoE from low-level parameters rather than relying on application-layer indicators and models. A prime example of a change necessitating a new view is *YouTube*, which, due to its switch to HTTPS, prevented ISPs from using existing passive monitoring tools that could directly estimate video quality by inspecting HTTP headers. As an example for new approaches based on more low-level data, Orsolic et al. [31] have presented a machine-learning–based architecture that estimates *YouTube* QoE from features derived from packet sizes, inter-arrival times, and throughput. They created a testbed to obtain network captures under different traffic conditions as well as ground-truth data against which their models were optimized. The authors succeeded in classifying video QoE, but only resorted to coarse prediction classes ("high", "medium", and "low"). A similar approach was shown by Dimopoulos et al. [14], who instead used real network data to predict typical QoE indicators for streaming services (e.g., played resolutions, stalling events), based on features such as round-trip times, packet loss and chunk sizes. Here, the authors also used machine learning as a promising technique for large-scale quality monitoring and prediction. Similar approaches to the two mentioned above can be envisioned for all kinds of service classes. However, changes to network architecture (e.g., the introduction of protocols like QUIC or new techniques such as HTTP/2 connection multiplexing) make it necessary to constantly adapt and re-train such models. Furthermore, the diversity of system architectures and subtle details in media player implementations mean that these models may have to be re-engineered for different service providers. Ultimately, predictions from such models may never reach the precision of bitstream-based or signal-based models that have access to the real bitstream.

3.2.1 Countermeasures

While we have seen that an estimation of QoE is possible via passive probing in encrypted networks, the accuracy of such models cannot reach that of models operating on the actual video payload. Also, the use-case of above-mentioned models is a network-centric monitoring scenario. Thus, encryption only hinders ISPs from passively monitoring (OTT) services

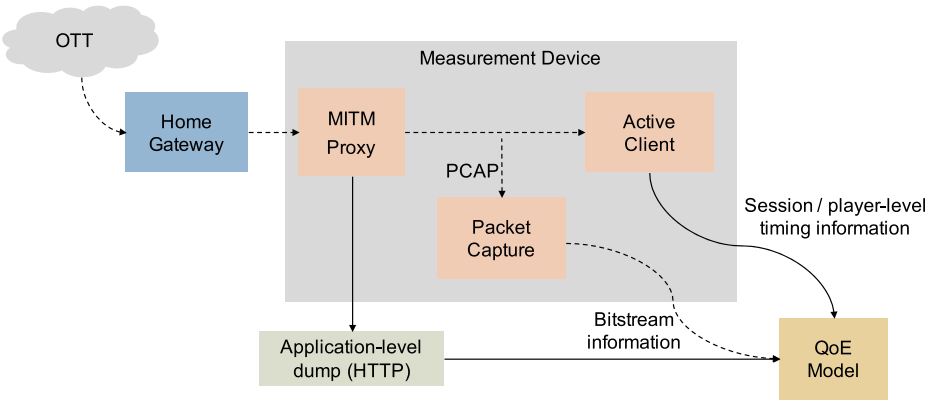

Fig. 5 Man-in-the-middle scheme for measuring QoE of HTTPS-encrypted transmissions. *Dashed lines* indicated encrypted payload

that are not under their control — services like VoIP or IPTV may still be monitored from end to end; an ISP could then either monitor a subset or all of their customer's media sessions. In the case where this is not possible, an active probing scenario based on a client-side measurement may still yield KPIs and KQIs to be used for a quality model (e.g., rebuffering events in video streaming). Here, the ISP would simply simulate a customer using a service according to a representative usage pattern. However, in such a case, an underlying encrypted transmission would still prevent the ISP from extracting the cleartext payload of media streams.

One way to overcome this problem is to perform a man-in-the-middle attack (MITM) on the monitoring device itself. Here, any traffic between the OTT and the client player (e.g., a web browser) is intercepted by a proxy installed on the client itself.[2] The proxy thus terminates the HTTPS connection, which gives it access to the cleartext application-level payload. Figure 5 shows the general scheme of a MITM measurement. The proxy captures the payload, which can then be analyzed together with player KPIs (such as video stalling events). Given the understandable concerns about user privacy and the resulting full encryption of services, the MITM approach seems promising and easy to implement. However, it can *only* be used on devices owned by the ISP and *not* on a real customer device. This is because a fake certificate authority (CA) needs to be installed on the monitoring device — something that real customers cannot be forced to do, as it would compromise their privacy and would in fact be illegal in most jurisdictions. Furthermore, the impact of MITM-based approaches on the actual measurements needs to be critically checked. Hence, this solution can only be used in special cases, with active probes, and may not yield a representative picture of QoE.

3.2.2 Future approaches — QoE as a cooperation between OTTs and ISPs

As long as existing monitoring systems are still functional, there may be little incentive to change a running system or invest into new models and frameworks. Standardization bodies also have to first catch up with the rise of encryption, having to define work items for

[2] An example of such a tool can be found under https://mitmproxy.org/.

future studies, which may take years to complete. While commercial tools exist that claim to predict QoE even for encrypted streams, they would have significantly less information about the media available, and thus may be noticeably inferior in their quality predictions when compared to current models.

For a long time, there have been ongoing collaborations among OTTs and ISPs in terms of peering among their Autonomous Systems, either through Public Peering Interconnections (PPI) through Internet eXchange Point (IXPs) or through Private Network Interconnection (PNI). Those collaborations are based on mutual agreements [44], and they often involve payments from one side to another. Some ISPs are also now hosting surrogate servers provided by OTTs in their networks in order to decrease end-to-end latency for the content retrieval as well as to decrease traffic in the core network of the ISP [5, 32]. For example, YouTube and Netflix are providing both peering connections as well as surrogate servers to the collaborating ISPs for their services [18, 30]. As another example, [17] describe a protocol enabling ISP–OTT collaboration. However, these approaches are not primarily QoE-centric and may require incorporation of QoE monitoring and exchange of information among the two entities for a more QoE-oriented service delivery.

One possible solution could be an OTT–ISP collaboration for QoE-aware service delivery. Here, [43] shows an SDN-based ISP–OTT collaboration scheme for video delivery that focuses on video-specific traffic features. Another architecture for ISP–OTT collaboration is proposed in [4]. Here, the OTT monitors quality as delivered to the users on a session basis. They share QoE measurements with an ISP for a joint management of service delivery. The work in [4] shows that this approach could lower user churn.

An OTT–ISP collaboration would therefore consist of OTTs providing the ISPs access to KPIs or KQIs that would otherwise be hidden by encryption. For example, a video provider always knows when their customers experience rebuffering. An interface could be defined in which this kind of information (metadata) is made available to the ISP in an anonymized fashion. Three approaches are possible: 1) The OTT actively sends information to the ISP, 2) the ISP actively requests information from an OTT server, or 3) information is sent along the regular transmissions so that it can be passively monitored. For options 1 and 2, a dedicated server needs to be set up at either location, and a "QoE API" needs to be negotiated between OTT and ISP to exchange information. Another solution for option 1 and 2 could be the extension of the peering API such as PeeringDB API [33] where OTTs can send information as metadata or ISPs can get information related to traffic flows during the peering. Option 3 calls for more fundamental changes in how HTTPS transmissions work. A different solution to this problem [23] would consist in the metadata being carried along the TLS data in an auxiliary channel, but marked as not privacy-sensitive. Also, the data could be sent through ICMP packets in an out-of-band channel at a lower level than TCP.[3]

To give an example of how communication between network operators and OTTs can be achieved, *Server and Network Assisted DASH* (SAND) [40] is an extension of MPEG-DASH (Dynamic Adaptive Streaming over HTTP). DASH has become the de-facto standard for distributing video over the Web, alongside less frequently used solutions like Apple HTTP Live Streaming (HLS). SAND is an example of a system which goes beyond the playback client and the media server communicating over a fully encrypted connection, as typically done today. With SAND, additional network elements are introduced

[3]For further position papers on this topic, the interested reader is pointed to the workshop *Managing Radio Networks in an Encrypted World (MaRNEW)*, hosted by the IETF in September 2015, https://www.iab.org/activities/workshops/marnew/

("DASH-assisting network element"), which enable network operators to receive and signal information on the playback sessions (such as quality metrics), which in turn can be used by the streaming service and clients to optimize quality under the given network operator's constraints.

To summarize, OTT–ISP collaboration is a challenging field of its own, with interesting prospects for users who would gain from improved QoE. However, due to largely political arguments on both sides, realization of the aforementioned concepts is often prevented or slowed in practice.

3.2.3 Net neutrality concerns

All the above-mentioned alternatives have their benefits and drawbacks. On the positive side, in all of the above scenarios, the ISPs could utilize data provided by the OTT not only to monitor the QoE, but also to increase the QoE of that OTT service on their networks, for example by selecting more efficient peering points or routing. However, while not a core issue of network monitoring itself, the topic of net neutrality has to be discussed at this point: recent regulations in the United States and the EU have forced ISPs to treat all traffic equally, no matter from/to whom it is sent. In the lawmakers' perspective, Internet is a "good" that all users should have equal access to. Encryption helps to achieve net neutrality, since it (partly) masks the content of traffic, but ISPs could nonetheless classify it according to its origin and other intrinsic properties.

OTTs may be concerned that after having determined QoS and QoE levels, ISPs throttle their traffic when they have access to QoE-related information. For example, the EU regulation 2015/2120 says that "reasonable traffic management" from ISPs is allowed when it "responds to the objectively different technical quality of service requirements of specific categories of traffic." The directive thus makes it clear that QoS requirements may vary from service to service. However, in addition, it specifies that "any (...) differentiation should, in order to optimise overall quality and user experience, be permitted only on the basis of objectively different technical quality of service requirements (...) of the specific categories of traffic, and not on the basis of commercial considerations." Thus, the EU has adopted a terminology in which QoE is explicitly considered and should be optimized — the requirement for this of course are respective QoE-based monitoring systems.

Business constraints aside, the prospect of optimizing the quality of an OTT service over an ISP's network should incentivize the OTT to supply the necessary information for the ISP to do so. However, customer privacy and net neutrality should in our view never be at stake in such a scenario, and this risk may deter OTTs from engaging in such a collaboration, notwithstanding other financial interests. Ultimately, a partnership between OTTs and ISPs should lead to a more stable or higher QoE for their customers.

How does network neutrality play such a large role in QoE monitoring? A successful collaboration requires ISPs to be able to prove to the OTTs that an efficient provisioning (which may include lowering bandwidth for certain services) does not necessarily lead to reduced QoE. This can only be proven by valid and reliable QoE models or user tests. For example, for a video streaming service, only a well-trained and evaluated QoE model should be the basis for deciding whether a reduction in bandwidth manifests in a significant change in user-perceived QoE. KPIs such as network throughput cannot be employed to drive these decisions alone. It is therefore critical to base any decisions of network management on accurate data. The scenario; however, becomes more complicated when different OTT services or service classes are involved: which ones should be prioritized? Also, different legislations make international collaborations and agreements more complicated.

Obviously, the questions raised by these topics cannot be answered yet, and it is to be seen whether collaborative approaches manifest as the go-to solution for ISP–OTT relationships. For further details on net neutrality and the associated perspectives, see [19, 27].

3.3 Virtualization

We consider Software Defined Networks (SDN) and Network Function Virtualization (NFV) as key future technologies for network monitoring and management: first of all, they allow for systems to be programmed more dynamically. For example, it is easy to deploy a new model version via software updates and containerized solutions (such as Docker),[4] rather than providing firmware upgrades for hardware probes. This enables more rapid upgrades, higher scalability and lower maintenance costs.

Virtualized monitoring architectures can be built more flexibly and scale more easily. Additionally, virtualization technologies have a significant role in the way physical sensing devices are being deployed for collecting information about our physical world. Since the paradigm of the network monitoring and management is shifting towards virtualization — in combination with drastic growth of high-end IoT-based multimedia applications —, the complexity of monitoring QoE is increasing too. We will address these challenges in this section.

3.3.1 Virtualized probes at the network side

SDN and NFV are becoming more widespread [28], so that core network technologies are shifting towards virtualization. This makes it harder to identify the location in which quality should be monitored and assessed, when those traditional locations do not physically exist anymore. Accordingly, the placement of the virtualized probe remains an important challenge; ISPs should place the Virtual Network Functions (VNFs) by considering effectiveness and cost [20]. For example, in the case of the virtualization of the middle-boxes between two end points, the traffic may follow the indirect paths which may cause potential packet delay hence making the selection of appropriate placement of the probe crucial for delay-sensitive multimedia traffic [20]. While in network data centers, network administrators can perform end-to-end traces of packets, in virtualized data centers, the traffic is invisible to the physical network leading to a significant challenge regarding probe placement and implementation for QoE monitoring. Thus, classic physical probes cannot be used here. Network diagnostics will instead require virtualized probes, which can communicate with both virtual and physical elements of the network for QoE monitoring. Due to a potential high load of the virtual management systems, a trade-off has to be made between accuracy and cost-effective deployment. For example, it needs to be ensured that precise timestamps are collected when needed. Preliminary solutions have been proposed, for instance a CDN architecture in which a virtual manager is used to manage the network based on monitoring probes with the help of utility functions [29].

When it comes to monitoring the QoE, the virtualization technologies bring significant advantages. Indeed, new services are being deployed and the existing ones are changing in the way the functionalities are offered to the final users, which has an impact on the perceived quality. This calls for new models that need to be dynamically realised and instantiated into the network. In this scenario, the use of NFVs technologies allows for adopting

[4] https://www.docker.com/

a plug-and-play approach, so that the collection of new parameters and the new processing operations can be performed without great management burden.

Another important aspect is related to the fact that, an open-loop approach is often used when it comes to the major algorithms and procedures currently embedded in the telecommunication networks. This is the case of some procedures that rely on an off-line estimation of network variables (e.g., quality perceived per user category), rather than on real-time measurements and direct corrective actions. Accordingly, QoE related metrics are usually observed as part of a non-real-time monitoring service as they are just included in offline diagnosis activities for long-term service improvement. This represents a strong obstacle in a scenario characterized by a large variety of supported services and rapid evolutions. In this context the big challenge is the implementation of orchestration functionalities that exploit a closed-loop approach to get the maximum benefits from the available real time feedback information to follow the high dynamicity and unpredictability of the considered scenarios [16]. This objective can be achieved with an extensive use of softwarization and virtualization technologies of the transport services.

3.3.2 Virtualized probes at the client side

ISPs typically monitor the quality at core and access networks. Moreover, some ISPs are also introducing client-centric monitoring procedures through Customer Premises Equipment (CPE), which are in the form of hardware devices. However, replacing CPE with devices with more advanced quality monitoring features may be a huge cost factor for ISPs in a very competitive market, as the number of CPE is in the order of millions or even more, depending on the market share. A more lightweight and client-centered approach to probing would be to offload the measurement into a virtual probe, which runs on traditional, already existing general-purpose hardware. In virtual CPE [10], the probe itself is nothing more than a piece of virtualized software. It does not depend on a specific hardware, and can be instantiated quickly at different locations.

For this reason, the work in [26] puts emphasis on placing the VNFs at the network edge. However, the approach still remains network-centric rather than user-centric. To shift to a more user-oriented perspective, the works in [2, 3, 11, 12, 42] refer to an installation of virtual probes at user-end devices/terminals. Such an approach would not only provide for a cost-effective, robust, and flexible monitoring solution but also can offer additional information related to system, context, and user behavior [3].

However, the placement of virtualized probes for QoE monitoring at user terminals creates new challenges. These include the optimal choice of the monitoring cycle or frequency: a probe installed at the user-end device draws resources available on that device (such as CPU, RAM, and battery) [3]. Hence, continuous monitoring or detailed signal analysis is not possible without consuming users' resources.

A shift towards virtualized probes and virtualized networks will also lead to changes in the way probes are developed and marketed. Vendors of hardware probes rely on business models in which dedicated, highly customized, and costly devices are operated by ISPs, receiving software and hardware support for a longer term. If the ISP wants to expand their traditional monitoring solution, new hardware will have to be bought. Moving to virtualized monitoring architectures, ISPs will have the flexibility to instantiate software-based probes at any time. Vendors of such probing solutions will therefore have to move from one-time payment for physical devices to a subscription- or individual license-based model for the use of virtual probes.

To summarize, this shift to virtualization — no matter if done at the network or client side — may allow ISPs to introduce flexible, cost-effective and hardware-independent monitoring. Still, the implementation and deployment of QoE-centered virtualized probes introduces scalability issues in the required centralized architecture, and challenge security and reliability of the implemented protocols.

3.3.3 Cloud processing — issues of scalability and security

We believe that placing probes in user end devices will become much more widespread. Those probes will then be monitored centrally. Such an approach may have benefits in terms of end-to-end QoE delivery because it provides ISPs with information related to context-, system- and user-influencing factors (including the geographical location) [36], which relates to the principles of context-aware QoE monitoring. Centralized monitoring systems can utilize cloud technologies to reduce network-wide equipment costs and resolve programmability and flexibility issues. However, scalability will remain an open challenge: network overheads will increase with traffic, since a single controller will be computing all routing paths to generate a network-wide globalized routing map [24]. A real-time computation of QoE-based measurements may also result in additional network-wide delays. With respect to network security, a robust and reliable design of SDN controllers will be needed. The above mentioned issues can be addressed by introducing a semi-distributed approach leaving some freedom to SDN software-based switches to take some local traffic management decisions, while still maintaining the overall view of the network services at the control layer.

3.4 Virtual objects

Virtualization technologies are impacting the way many services are being deployed and provided to the final users. This holds true especially in the field of the Internet of Things (IoT). Here, the physical and the virtual worlds merge to realize services that improve users' quality of life. ISPs that offer IoT services must be aware of the future challenges that come along with such a paradigm shift.

One of the major applications of these technologies is the *virtual object*, which is the digital counterpart of any real (human or lifeless, static or mobile, solid or intangible) entity in the IoT. These can be multimedia objects, which are those capable of acquiring multimedia contents from the physical world. They can be equipped with multimedia devices such as cameras and microphones.

Here are two simple application examples: distributed intelligent cameras could tell key facts about the occupancy of a room and/or the behavior of people in the observed environment; speed gauges, positioning systems and cameras can be used to perform remote monitoring and tutoring of practitioners when practicing with a vehicle. These technologies represent important opportunities for ISPs to provide added value services to their customers [9].

As new applications are being deployed based on these technologies, there is a need for novel approaches and models to evaluate their perceived quality. All the sensors in the described scenarios are virtualized through agents. These act as their representatives so that all the sensed data is conveyed through them while being processed and cached if needed. These virtual objects typically run in a cloud / fog computing infrastructures, as the physical devices often have constrained resources. They are then the best candidate for the

monitoring of the contribution of the provided services to the perceived quality. This not only depends on the traditional QoS parameters but also on indicators related to the Quality of Information (to which extent the collected information meets users' needs for a specific time, place and social setting) and Quality of Data (i.e., accuracy of the data).

The needs and opportunities stemming from this technological change come with important challenges. Current, mostly static services like IPTV and speech do not suffer from the same problems; OTT services like Video on Demand only show a fraction of the issues that we may find with entirely virtualized IoT technologies. Here, it becomes much more difficult to create quality models for the services that we deploy with virtualized technologies. This is due to their fluidity, which contrasts with the classic approach in which we perform lab-based subjective tests with users. As soon as new models will be created in the lab and are deployed in the wild, the relevant services have already changed in the way they are delivered to the final users. Accordingly, the models will not be applicable anymore — new metrics need to be considered, or at least need to be included in a different way.

4 Conclusion

In this article, we gave an introduction to the current state and the future of QoE monitoring, based on the most important challenges we see today. We described the categorization and history of quality models, which are implemented in probes in order to be deployed in QoS/QoE monitoring systems. We also showed examples of recent research into new, user-centric modeling and monitoring approaches.

The major contribution of this article is the discussion of challenges that ISPs need to face when implementing QoE monitoring systems for future networks. One of these challenges stems from the fact that ISPs and OTTs will generally move from a network-centric to a more user-centric perspective. Traditional SLAs are not applicable for negotiating and communicating quality to customers, and it can be imagined that QoE will take a more prominent role here — also in the network optimization goals for ISPs. A question that ISPs must ask themselves is whether there should be a guarantee for something as complex as the level of user experience? We see this as inevitable, as with the advent of more complex and resource-intensive services, users will demand more from their ISP than just a steady Internet connection. Most importantly, calling for more detailed user-centric QoE optimization requires appropriate monitoring solutions, which are still challenging to implement.

Another one of the most important issues is introduced by the increased amount of application-level encryption. How can ISPs monitor application-level data when most OTT traffic is going to be end-to-end encrypted? Here, current works explore machine learning approaches which allow ISPs to predict QoE from lower-level network measurements. Another proposed solution would be a collaboration between OTTs and ISPs. To be more precise, a side-channel could allow OTTs can report certain KPIs and KQIs to ISPs. However, net neutrality concerns play a large role in such a scenario: although net neutrality regulations mostly affect how traffic shaping is being implemented by an ISP, the use of reliable QoE models to quantify the user experience is a precondition for that. We conclude that ISP–OTT collaboration is a highly political topic, but there are technological opportunities that offer ways for both parties to create better services for their users.

Finally, the rise of virtualized networks brings up a number of questions. These include challenges in how new probes have to be designed: they will be developed and marketed in a different manner. Furthermore, in order to allow an ISP to leverage the capabilities of

those new networks, the placement of the (virtualized) probes at either client or network side becomes a critical issue. They will no longer be specific hardware devices at a particular physical location, but instead can be more flexibly scaled, which might draw more resources on nodes. We also explained how implementing probes in customer equipment — as a way to perform client-centric monitoring — is not a silver bullet. As a look into the future of the Internet, IoT technologies will fundamentally change the deployment and monitoring of services. Here, the major challenge lies in developing appropriate quality models.

The future of QoE monitoring is certainly not exclusively determined by the above challenges — and these challenges are also relevant to other areas such as QoE-based traffic management, security, and billing. These issues will be shaped by a broader adoption of new services and technologies such as Virtual Reality and cloud gaming, which are much more demanding in terms of network requirements. However, as we have seen in the paper, even when monitoring the "classic" technologies such as video and speech, ISPs encounter challenges that they need to and will need to face. These developments raise important questions that the research community has to provide answers to, in collaboration with the industry and standardization bodies.

Acknowledgments The work on this paper was funded from the European Union's Horizon 2020 research and innovation program under the Marie Sklodowska-Curie grant agreement No 643072, Network QoE-Net.

References

1. Aaron A, Li Z, Manohara M, Lin JY, Wu ECH, Kuo CCJ (2015) Challenges in cloud based ingest and encoding for high quality streaming media. In: 2015 IEEE International Conference on Image Processing (ICIP). IEEE, vol 2015-Decem, pp 1732–1736, doi:10.1109/ICIP.2015.7351097. http://ieeexplore.ieee.org/document/7351097/
2. Aggarwal V, Halepovic E, Pang J, Venkataraman S, Yan H (2014) Prometheus: Toward quality-of-experience estimation for mobile apps from passive network measurements. In: Proceedings of the 15th workshop on mobile computing systems and applications. ACM, p 18
3. Ahmad A, Atzori L, Martini MG (2017) Qualia: A multilayer solution for QoE passive monitoring at the user terminal. In: IEEE ICC 2017 Communications software, services, and multimedia applications symposium (ICC'17 CSSMA). IEEE, Paris, France
4. Ahmad A, Floris A, Atzori L (2016) QoE-centric service delivery: A collaborative approach among OTTs and ISPs. Comput Netw 110:168–179
5. Ahmad A, Floris A, Atzori L (2017) OTT-ISP Joint service management: a customer lifetime value based approach. In: Accepted for IFIP/IEEE International Symposium on Integrated Network Management. IEEE
6. Alreshoodi M, Woods J (2013) Survey on QoE/QoS correlation models for multimedia services. International Journal of Distributed and Parallel Systems 4(3)
7. Bajpai V, Schönwalder J (2015) A survey on internet performance measurement platforms and related standardization efforts. IEEE Commun Surv Tutorials 17(3):1313–1341
8. Barakovi ć S, Skorin-Kapov L (2013) Survey and challenges of QoE management issues in wireless networks. Journal of Computer Networks and Communications 2013
9. Bruschi R, Lago P, Lamanna G, Lombardo C, Mangialardi S. (2016) Openvolcano: An open-source software platform for fog computing. In: 2016 International Teletraffic Congress. IEEE
10. Carey T, Pattabhiraman R (2016) Management of Virtual CPES. US Patent 20160020962

11. Casas P, Seufert M, Schatz R (2013) YOUQMON: A System for on-line monitoring of YouTube QoE in operational 3G networks. ACM SIGMETRICS Performance Evaluation Review 41(2):44–46
12. Chen QA, Luo H, Rosen S, Mao ZM, Iyer K, Hui J, Sontineni K, Lau K (2014) QoE doctor: Diagnosing mobile app QoE with automated ui control and cross-layer analysis. In: Proceedings of the 2014 Conference On Internet Measurement Conference. ACM, pp 151–164
13. Chen Y, Kaishun W, Qian Z (2014) From QoS to QoE: A survey and tutorial on state of art, evolution and future directions of video quality analysis. IEEE Commun Surv Tutorials
14. Dimopoulos G, Leontiadis I, Barlet-Ros P, Papagiannaki K (2016) Measuring Video QoE from Encrypted Traffic. In: Proceedings of the 2016 ACM on Internet Measurement Conference - IMC '16. ACM Press, New York, pp 513–526, doi:10.1145/2987443.2987459. http://dl.acm.org/citation.cfm?doid=2987443.2987459
15. Feng-Hui H, Wen-An Z, Yu D (2014) Qoe Issues of OTT Services over 5G Network. In: 2014 9th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA). IEEE, pp 267–273
16. Francesco DP, Claudio GG, Salvatore M, Vincenzo S (2016) Future internet architecture: Control-based perspectives related to Quality of Experience (QoE) management. In: 34th Chinese Control Conference. IEEE
17. Frank B, Poese I, Lin Y, Smaragdakis G, Feldmann A, Maggs B, Rake J, Uhlig S, Weber R (2013) Pushing CDN-ISP collaboration to the limit. ACM SIGCOMM Computer Communication Review 43(3):34. doi:10.1145/2500098.2500103. http://dl.acm.org/citation.cfm?doid=2500098.2500103
18. Google Peering. https://peering.google.com/. (Date last accessed 23-March-2017)
19. Habibi Gharakheili H, Vishwanath A, Sivaraman V (2016) Perspectives on Net Neutrality and Internet Fast-Lanes. ACM SIGCOMM Computer Communication Review 46(1):64–69. doi:10.1145/2875951.2875962
20. Han B, Gopalakrishnan V, Ji L, Lee S (2015) Network function virtualization: Challenges and opportunities for innovations. IEEE Commun Mag 53(2):90–97
21. Hofstede R, Celeda P, Trammell B, Drago I, Sadre R, Sperotto A, Pras A (2014) Flow monitoring explained: From packet capture to data analysis with NetFlow and IPFIX. IEEE Commun Surv Tutorials 16(4):2037–2064
22. Hoßfeld T, Skorin-Kapov L, Haddad Y, Pocta P, Siris VA, Zgank A, Melvin H (2015) Can context monitoring improve QoE? A case study of video flash crowds in the Internet of services. In: 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM). IEEE, pp 1274–1277
23. Kasbekar M, Kanitkar V (2015) CDNS, Network Services and Encrypted Traffic. In: Managing Radio Networks in an Encrypted World (MaRNEW) workshop. IAB
24. Kreutz D, Ramos FM, Esteves Verissimo P, Esteve Rothenberg C, Azodolmolky S, Uhlig S (2015) Software-defined networking: a comprehensive survey. Proc IEEE 103(1):14–76
25. Le Callet P, Möller S, Perkis A (2013) Qualinet white paper on definitions of Quality of Experience. Tech. Rep. March, European Network on Quality of Experience in Multimedia Systems and Services (COST Action IC 1003)
26. Manzalini A, Minerva R, Callegati F, Cerroni W, Campi A (2013) Clouds of virtual machines in edge networks. IEEE Commun Mag 51(7):63–70
27. Marsden C (2017) Network Neutrality: From Policy to Law to Regulation. Manchester University Press, UK
28. Mijumbi R, Serrat J, Gorricho JL, Bouten N, De Turck F, Boutaba R (2016) Network function virtualization: State-of-the-art and research challenges. IEEE Commun Surv Tutorials 18(1):236–262
29. Moreira A, Moreira J, Sadok D, Callado A, Rodrigues M, Neves M, Souza V, Karlsson PP (2011) A case for virtualization of content delivery networks. In: Proceedings of the Winter Simulation Conference, pp 3183–3194
30. Netflix Open Connect. https://openconnect.netflix.com. (Date last accessed 23-March-2017)
31. Orsolic I, Pevec D, Suznjevic M, Skorin-Kapov L (2016) Youtube QoE estimation based on the analysis of encrypted network traffic using machine learning. In: 5th IEEE International Workshop on Quality of Experience for Multimedia Communications (QoEMC). Washington
32. Passarella A (2012) A survey on content-centric technologies for the current Internet: CDN and P2P solutions. Comput Commun 35(1):1–32
33. PeeringDB API. https://peeringdb.com/apidocs/. (Date last accessed 23-March-2017)
34. Perkis A, Reichl P, Beker S (2014) Quality of Experience - Advanced Concepts, Applications and Methods, chap. Business Perspectives on Quality of Experience. Springer, pp 97–108
35. Raake A, Gustafsson J, Argyropoulos S, Garcia M, Lindegren D, Heikkila G, Pettersson M, List P, Feiten B et al (2011) IP-Based mobile and fixed network audiovisual media services. IEEE Signal Proc Mag 28(6):68–79

36. Reiter U, Brunnström K, De Moor K, Larabi MC, Pereira M, Pinheiro A, You J, Zgank A (2014) Factors influencing Quality of Experience. In: Quality of Experience: Advanced Concepts, Applications and methods. Springer, pp 55–72
37. Schatz R, Hoßfeld T, Casas P (2012) Passive YouTube QoE Monitoring for ISPs. In: 2012 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS). IEEE, pp 358–364
38. Shahid M, Rossholm A, Lövström B, Zepernick HJ (2014) No-reference image and video quality assessment: a classification and review of recent approaches. EURASIP Journal on Image and Video Processing 2014(1):40. http://jivp.eurasipjournals.com/content/2014/1/40/abstract
39. Skorin-Kapov L, Varela M (2012) A multi-dimensional view of QoE: the ARCU model. In: MIPRO, 2012 Proceedings of the 35th International Convention. IEEE, pp 662–666
40. Thomas E, van Deventer M, Stockhammer T, Begen AC, Famaey J (2015) Enhancing MPEG DASH performance via server and network assistance
41. Varela M, Zwickl P, Reichl P, Xie M, Schulzrinne H (2015) From Service Level Agreements (SLA) to Experience Level Agreements (ELA): The Challenges of Selling QoE to the User. In: 2015 IEEE International conference on communication workshop (ICCW). IEEE, pp 1741–1746
42. Wamser F, Seufert M, Casas P, Irmer R, Tran-Gia P, Schatz R (2015) YoMoApp: A tool for analyzing QoE of YouTube HTTP adaptive streaming in mobile networks. In: Networks and communications (EuCNC), 2015 European conference on. IEEE, pp 239–243
43. Wichtlhuber M, Reinecke R, Hausheer D (2015) An SDN-based CDN/ISP collaboration architecture for managing high-volume flows. IEEE Trans Netw Serv Manag 12(1):48–60. doi:10.1109/TNSM.2015.2404792
44. Yeh CL (2014) Conceptualized framework for regulation of OTT video services: a new battlefield of interconnection and peering. In: 20th ITS Biennial Conference, Rio De Janeiro 2014: The Net and the Internet-Emerging Markets and Policies. International Telecommunications Society (ITS)

Werner Robitza (werner.robitza@telekom.de) is a researcher at the Telekom Innovation Laboratories of Deutsche Telekom AG, working there since 2014 as a fellow of H2020 QoE-Net. He received his diploma degree in computer science from the University of Vienna, where he worked as a researcher from 2009 until 2013. His research interests are Quality of Experience for multimedia applications and user behavior aspects for Web TV services.

Arslan Ahmad (arslan.ahmad@diee.unica.it) is a PhD student at Department of Electrical and Electronics Engineering, University of Cagliari, Italy. He received his engineering degree in Aviation Electronics and Masters degree in Computational Sciences and Engineering from National University of Sciences and Technology, Pakistan. Currently, he is working as early stage researcher in H2020 QoE-NET. His research interests are QoE management in future Internet, image processing and artificial intelligence.

Peter A. Kara (p.kara@kingston.ac.uk) is a research associate at the Wireless Multimedia and Networking Research Group, at Kingston University. He performed his M.Sc. studies in computer engineering at the Department of Networked Systems and Services, at the Budapest University of Technology and Economics. He was involved at FP7 CONCERTO and he is currently a fellow of H2020 QoE-Net. His primary research interests are perceptual QoE and cognitive bias in subjective quality assessment.

Luigi Atzori (l.atzori@ieee.org) is associate professor at the Univesity of Cagliari, Italy, where he leads the laboratory of Multimedia and Communications. He is currently coordinating the H2020 QoE-Net project on innovative quality of experience management in emerging multimedia services.

Maria G. Martini (m.martini@kingston.ac.uk) is professor at Kingston University London, where she also leads the Wireless and Multimedia Networking research group. She has lead the KU team in several EU (e.g., OPTIMIX, CONCERTO, QoE-Net, Qualinet, 3D-ConTourNet), national, and industry-funded projects. She serves as vice-chair of the IEEE Multimedia Communications Technical Committee.

Alexander Raake (alexander.raake@tu-ilmenau.de) was appointed head of the Audiovisual Technology Group at TU Ilmenau in July 2015. Before, he was a Professor at TU Berlin, heading the Assessment of IP-based Applications group at TU Berlin's An-Institut T-Labs, a joint venture between Deutsche Telekom AG and TU Berlin. From 2009 to 2013, he was an Assistant Professor at TU Berlin.

Lingfen Sun (l.sun@plymouth.ac.uk) is an Associate Professor (Reader) on Multimedia Communications and Networks at the University of Plymouth, UK. She has led the UoP team in several EU FP7/H2020 and industry funded projects, including ADAMANTIUM, Author Biographies Click here to download Author Biographies authors.pdf GERYON, Qualinet and QoENet. She was the Chair of Interest Group on QoE for Multimedia Communications for IEEE MMTC (2010-2012).