Quality Estimation Framework for Encrypted Traffic (Q2ET)

Lamine Amour*, Van TONG*, Sami SOUIHI*, Hai Anh TRAN† and Abdelhamid MELLOUK*
*LISSI-TincNET Research Team, UPEC, France
Email: van-van.tong@univ-paris-est.fr, sami.souihi@u-pec.fr, mellouk@u-pec.fr
†Bach Khoa Cybersecurity Centre, SOICT, HUST, Vietnam
Email: anhth@soict.hust.edu.vn

***Abstract*—In the coming years, the development of the Internet of Things (IoT) will have relevance for transport, environment, health care, smart cities and also multimedia services (Multimedia Internet of Things (MIoT)). Nowadays, many services including those of the IoT and MIoT encrypt the data to make it secure during the transmission. However, it imposes some obstacles for the ISP (Internet Service Provider) because of the lack of visibility for operators into network traffic. To resolve these issues, we proposed the Quality Estimation Framework for Encrypted Traffic (Q2ET) containing a classification module and a QoE assessment module. The first module inherited from our previous research works to classify the encrypted network traffic using CNN (Convolutional Neural Network). The second one applies the objective and subjective methods based on the statistical analysis and machine learning methods that combine application and network parameters to calculate user's QoE (Quality of Experience) in terms of MOS (Mean Opinion Score). The Q2ET allows the ISP to monitor the user's QoE, detect the decrease of the user's QoE in order to make the appropriate decisions when the problems happen in the network systems.**

***Index Terms*—Quality of experience (QoE), Traffic classification, QUIC, Machine learning, Internet of Things (IoT), Multimedia Internet of Things (MIoT), Video service, VoIP, File transfer.**

I. Introduction

Technological advances in recent centuries have significantly improved people's lives. *Internet of Things (IoT)* paradigm is one of the most promising advances. To present it shortly, it consists of *"a system of connected digital devices or objects uniquely addressable. All of them can communicate independently via a network and without the need for human interaction"* [1]. It can be useful in many fields of activity including health, defense, environment and so on. The *Multimedia IoT (MIoT)* is a part of IoT that can be defined as a *"network of interconnected objects capable of acquiring multimedia contents from the real world and/or present information in a multimedia way"* [9]. In the context of MIoT, ISP traditionally used network management methods based on service quality metrics such as end-to-end delay or available bandwidth. In recent years, the communications industry significantly diversified its offerings, which has resulted in a better opportunity for demanding IoT users. In this context, it is no longer conceivable to design service without integrating the aspects of "*end-user satisfaction*" into the management of the network [22]. For that, ISPs work to estimate the QoE (quality of experience), which is best expressed in MOS (mean opinion score) [8].

Nowadays, many SPs (Service Providers) encrypt the data to make it secure during the transmission and to keep the privacy of the user's data. For example, according to Cisco's report [4], 80 percent of web traffic will be encrypted by 2019. For instance, *Google* has developed *Quick UDP Internet Connection (QUIC)* [17], a new transport layer network protocol on the top of UDP, and applied for some services (e.g., YouTube, Google Driver, etc.). However, it is difficult for ISPs to estimate the QoE of the encrypted traffics that hide application information. Therefore, the possible solutions are to rely on network-based features derived from the encrypted network traffic. Some prior works calculate the QoE using network-based parameters (e.g., bandwidth, delay, packet loss) [6], [27]. Nevertheless, it is not easy for ISPs to identify the flows corresponding to different kinds of services because some previous solutions cannot be applied (e.g., port-based methods, payload-based methods, etc.).

In this paper, we propose *Q2ET solution*, a *"Quality Estimation Framework for Encrypted Traffic"* to resolve the challenge of quality estimation in the context of encrypted traffic. First, we implement a classification module inherited from our previous research work [26] to identify and classify encrypted flows. After classifying the network flows into different kinds of services, we apply appropriate QoE modules for each service class to estimate its quality levels using the network-based parameters. If we apply the same QoE modules to different kinds of encrypted flows, the obtained results may be inaccurate which causes inappropriate decisions. The classification module in Q2ET helps to identify types of encrypted flows to estimate the user's QoE more accurately. Q2ET can help the ISPs to monitor the quality level of different services on the fly and make the appropriate decisions to optimize and to enhance the QoE of various services in network systems such as video streaming. When the issues happen in the network systems, there is a reduction of the user's QoE. According to this, ISP can apply some troubleshooting approaches to identify whether the issues result from ISP or Service Provider. If the problems arise from ISP, they can implement some failure recovery methods to avoid its influence. The longer the issues exist, the more serious the problems become.

The remainder of the paper is structured as follows. Section II introduces the related work to the QoE assessment for Internet-based services. Section III presents the Q2ET solution for estimating the quality level of different services in the context of encrypted traffic. In section IV, we describe the experimental results of the Q2ET. Finally, the paper concludes with Section V which highlights some future works.

II. Related work

In the domain of QoE estimation, two aspects are covered. The first one concerns the study of the relationship between network QoS and QoE, where Internet traffic is not encrypted. The second one presents the QoE estimation methods for encrypted Internet traffic.

Many QoE estimation models are designed for non-encrypted traffic. They calculate end-user QoE, mostly in terms of MOS score, from the collected factors. The calculation can be done by objective models, mainly designed for image (SSIM, TMQI), audio (PAQM, PEAQ), and video (VMAF, VQM). Hybrid estimation models can also be used to calculate the end user's QoE. In this kind of method, subjective datasets are collected and are used to drive statistical regression methods or machine learning (ML) approaches.

In [13], Korhonen et al. presented a new QoE estimation method, that concerns video service, using application parameters. This study estimates the user's MOS score using a linear regression model. This method can be enhanced by adding more parameters like network parameters.

In [12], Kim et al. defined a fractional model that predicts user QoE by MOS scores for different multimedia services (VoIP, video on demand, etc.). The model takes into account multiple quality of service (QoS) criteria as well as features of the multimedia service. In contrast to the previous study, this one is based only on network parameters. So, it can be improved by adding some application parameters.

In [23], Aroussi et al. applied the exponential model *(exponential interdependency of quality of experience and quality of service)* to evaluate the video-on-demand service. The network parameters handled are the delay ($IPTD$) and the packet loss ($IPLR$). This study can be improved by adding some specific video parameters like video bit rate and stalls.

In [14], Singh et al. developed a model for estimating video user QoE. In this model, the user's QoE was determined using a five-layer neural network which uses the video parameters. This study showed that QoE usage could be impacted by video compression. One of the ideas to improve this study is also to use network parameters.

In [28], Youssef et al. presented another model to assess the user-perceived video quality using *random forest (RF)*. The application factors such as video frame rate, video bit rate and video quality, were selected using principal component analysis (PCA) for estimating the video QoE.

In [29], Yue et al. proposed a comprehensive data-driven approach using *bagging* technique. An important dataset was extracted to evaluate the video user's QoE using this technique. Using the extracted dataset, the authors conceived an appropriate QoE evaluating model, called "*bagging-based bayesian factorization machine*", to correlate the video features with the user's QoE.

In [3], Chen et al. used *boosting* technique to investigate the QoE assessment for video streaming over *long-term evolution (LTE)* networks. Concretely, they proposed an end-to-end video quality prediction model based on the *GRadient Boosting (GBM)* method using several parameters from the network layer, application layer, video content, and the user device. The proposed QoE assessment model is used to control a bit rate adaptation scheme in order to improve the video quality of the streaming service in LTE networks.

In the last years, for users privacy protection or security reasons, the content is transported encrypted using HTTPS. For example 74% of the cloud internet traffic is encrypted by 2018 according to the *Global Encryption Trends* report [21]. Consequently, estimate the user's QoE for one or different services in such an encrypted scenario is not easy. However, several studies have analyzed the QoE assessment in the encrypted traffic context as illustrated below.

In [19], Mangla et al. introduced an eMIMIC methodology to estimate video QoE metrics in the context of encrypted HTTP-based Adaptive Streaming (HAS) sessions. This methodology uses passive network measurements (packet headers from network traffic) to model a HAS session and estimate some video QoE metrics (re-buffering ratio, average bitrate, etc.). Despite the good results of this approach, it may be interesting to consider other parameters from the application layer or the network layer to try to improve the performance of the proposed methodology.

In [20], Orsolic et al. proposed the ViQMon monitoring tool to estimate the perceived video YouTube quality in the encrypted traffic context. This tool worked on the client-side and can be used on various devices and platforms (Android, iOS). It operates by extracting YouTube performance data from the official app's Stats for Nerds window. This study shows that a significant difference exists in buffering and application behavior when the video is embedded and when the video is played directly in the official YouTube application.

In [7], Dimopoulos et al. developed a new methodology for detecting video streaming QoE issues in the context of encrypted traffic. They propose predictive models for calculating different levels of QoE degradation. These models are achieved by using three key influence factors: the average video quality, the stalling numbers, and the quality variations. The proposed methodology can attempt 90% prediction accuracy.

In [11], Gring et al. built a framework for video quality by storing service information (client information, decrypted network traffic, and encrypted messages). They used a man-in-the-middle proxy to store all the data that concern video bitstream, active probing and traffic shaping. Based on these data, they accurately estimated the perceived video QoE using the ITU-T Rec. P.1203.

III. MAIN PROPOSAL: QUALITY ESTIMATION FOR ENCRYPTED TRAFFIC (Q2ET)

In this paper, we proposed a new solution, called Q2ET, to assess the QoE of users in the context of encrypted Internet traffic (Fig. 1).

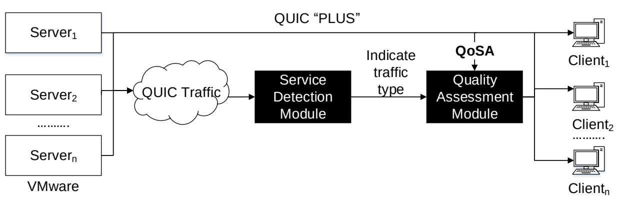

Fig. 1. Overview of the proposed architecture

The experimental platform is composed of several servers to generate Internet traffic. Q2ET solution is composed of two modules named "service detection module" and "quality assessment module". In our work, the term "module" indicates a set of operations that are being carried out for encrypted traffic detection (service detection module) and QoE assessment (quality assessment module).

The platform works as follows: Each server is in charge of one tested service: voice over IP (VoIP), streaming video, and file transfer. Each service generates its encrypted traffic. When the classification module identifies the specific service, the user's QoE estimation model is calculated for this service using the appropriate estimation model. A generic QoE model is implemented to give an overview of the overall network effectiveness.

The main objective of the Q2ET solution is to allow the ISPs to monitor the user's QoE in the context of encrypted data and to make the appropriate decisions when the QoE degradation occurs in the network systems.

A. *Traffic classification module*

Traffic classification plays an essential role in network management. It can help ISP to identify the flows and make appropriate decisions. For example, we can classify the network traffic into different kinds of services, and then implement the relevant QoE modules for these services. When we detect the user's QoE degradation in the network systems, we can apply specific solutions (e.g., routing algorithms, etc.) corresponding to the different kinds of services. These solutions will reduce the influence of the issues and make the user's QoE better.

Many research works concentrate on traffic classification, in particular in encrypted network traffic. Bashir et al. [2] proposed a flow-based method to identify the *BitTorrent* flows with the accuracy of over 90%. Zeng at al. [30] proposed a light-weight framework using deep-full-range (DFR) for encrypted traffic classification including Chat, Email, File, P2P and VoIP of VPN and non-VPN services. Artificial neural network (ANN) is a kind of machine learning algorithm inspired by the biological neural networks. However, ANN incurs two main drawbacks related to high input size and the weight matrix. However, *Convolutional Neural Network (CNN)* comprises some characteristics [10] (e.g. spare connectivity,parameter sharing, equivariant representations, etc.) that can overcome these drawbacks. Consequently, in this paper, we propose the CNN-based traffic classification method for encrypted network traffic (some QUIC-based services).

According to the white paper of Cisco [5], video streaming and file sharing comprise over 80 percent of global IP traffic by 2022. Therefore, in this paper, we concentrate on some popular services including VoIP, video streaming and file transfer. Other services are out of the scope of this paper. The Fig. 2 represents the classification module.

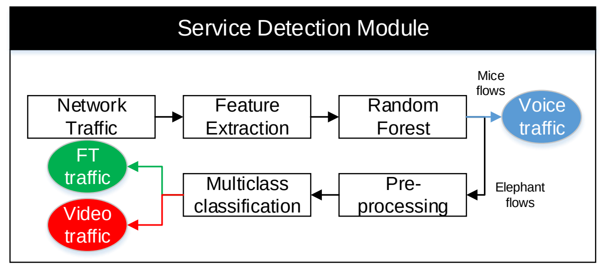

Fig. 2. Overview of the service detection module

This module, which is inherited from our previous work [26] with some modifications, contains two main stages. The first one is to classify the flows into the *elephant-flows* (video streaming and file transfer) and the *mice-flows* (VoIP) using the flow-based features. The second stage is used to identify the flows using the packet-based features. The elephant-flows are enormous (in total bytes) continuous flows while the mice-flows have only small packet length size. To detect the mice flows, we extract 8 flow-based features of the first 200 packets in each flow in the feature extraction phase and then apply a random forest algorithm as a classifier to identify these flows. The flow-based features include the average payload length, the percentage of the small, medium, and large packets in the flows in both directions between client and server.

After identifying the mice-flows, the elephant-flows will be processed in the CNN-based second stage of classification to classify the flows into video streaming and file transfer. First, each packet will be processed in the pre-processing phase to extract the 1400 packet-based features. Next, the multiclass classification takes into account these features using CNN. In each elephant flow, we process the first 10 packets and apply the majority rule to identify the class of these packets.

B. *QoE assessment module*

The second Q2ET module, called "quality assessment", is used to calculate Internet user's QoE in the context of end-to-end encrypted traffic based on the information (the type of service) given by the "service detection" module. Fig. 3 presents an overview of this module.

This module implements several existing QoE estimation models. The first one is to calculate the voice quality (MOS_{Voice}), when mice-flow (VoIP) is detected. The second one is to assess the perceived video quality (MOS_{Video}) for

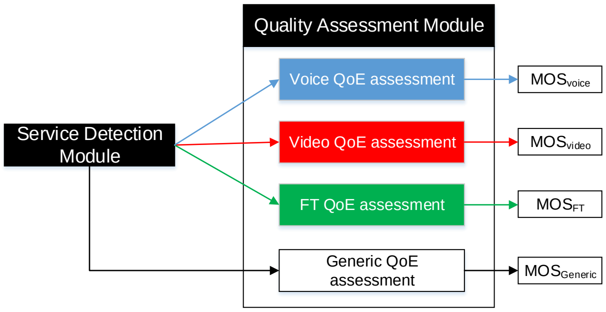

Fig. 3. Overview of the quality assessment module

streaming video users. The third one is to evaluate the quality of file transfer service (MOS_{FT}) when this service is detected. The fourth one consists of a "generic QoE estimation model" that calculates the instantaneous efficiency of the network ($MOS_{Generic}$). It is implemented using the instantaneous network parameters (bandwidth, delay and packet loss rate). This latter allows quantifying the quality of the network immediately, through these immediate conditions.

IV. Evaluation

A. Description

In the achieved experiment, we implement a real testbed using a specific server (virtual machine (VM)) for each tested service as illustrated in Fig. 4.

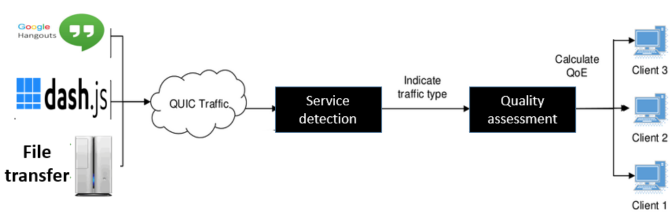

Fig. 4. Description of the achieved experiment

On the server-side, the first service is VoIP where *Google Hangout* is used to generate the voice traffic. The second service (video streaming) is performed by the *Dash server*. The third service for file transferring aimed to transfer large files from server to client. To transfer several files from server to client, we use *quic-go* [18], a QUIC implementation in pure Go language. To capture the network traffic, *Selenium WebDriver* in Google Chrome and Wireshark has been used.

In the service detection module, the Convolutional Neural Network (CNN) method and Random Forest (RF) method are implemented. Both these two methods are used to detect different kinds of QUIC-based services with high accuracy.

Two specific QoE estimation methods (linear regression-based method (noted "LM") and ML-based method (Random Forest) noted "RF") are tested for each kind of QUIC-based service. So, three subjective datasets are used to learn the specific models that concern each detected service. In the case of VoIP service, we use the dataset presented in [25], where network parameters are used to assess VoIP service quality in terms of MOS. Concerning the video service, our subjective dataset, which we built using the ACR method, is used. All the information details that concern this video MOS dataset can be found in [16]. In the case of the file transfer service, the dataset published by Schatz et al. in [24] is used. Figure (5) presents the overall view of the tests.

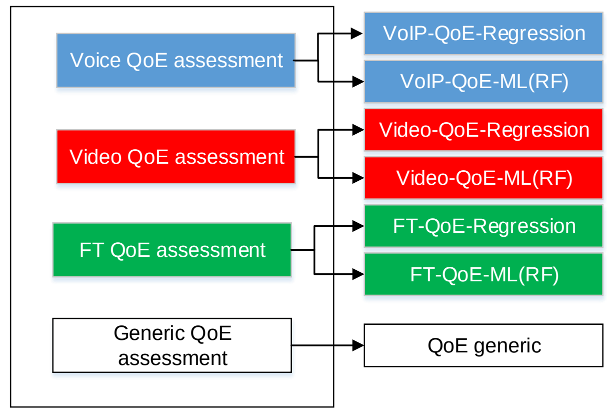

Fig. 5. Experiments description

In summary, 7 MOS values can be calculated within the QoE assessment module: Two predicted values ("LM" and "RF") for each specific service (voice, video and file transfer) and a generic value is given by a generic estimation model (noted $Generic$). To build the specific ML models (RF), we use 3 datasets [16], [24], [25] to build on a controlled laboratory context. $2/3$ of each dataset is used in the learning step and $1/3$ is used to test.

To evaluate the added value of the Q2ET solution, we compare the performance of the generic estimation method to the specific QoE estimation models ("LM" and "RF"). For this, we can calculate the *root mean squared error (RMSE)* (Eq. 1).

$$RMSE = \sqrt{\frac{\sum_1^n (MOS_i - y_i)^2}{n}} \tag{1}$$

where MOS_i are the predicted MOS values, y_i is the real MOS value, and n is the total number of samples considered.

B. Results

According to Fig. 6, we observe that the generic QoE estimation method gives worse results compared to the specific estimation models, where it achieves 0.77 of RMSE error rate. We also show that the RF-base method is the best estimation with 0.27 of the RMSE error rate. This method improves the performance of the generic model by more than 62%.

Fig. 7 illustrates the results of testing the video service. In this figure, we also observe that the effectiveness of the generic QoE estimation method is less useful than the specific estimation ones, where it achieves 0.56 of the RMSE error rate. In this figure, we also confirm that using the Random

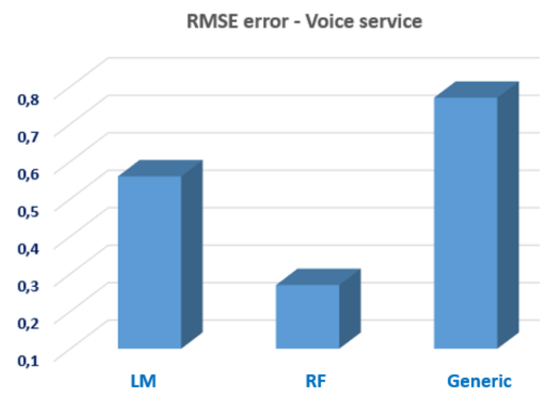

Fig. 6. Estimation performance in terms of RMSE for the VoIP service

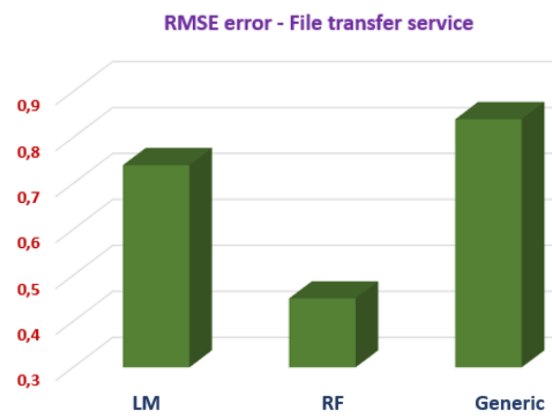

Fig. 8. Estimation performance in terms of RMSE for the Web service

Forest method is the best estimation with 0.24 of RMSE error rate and with 57% improvement over the generic method.

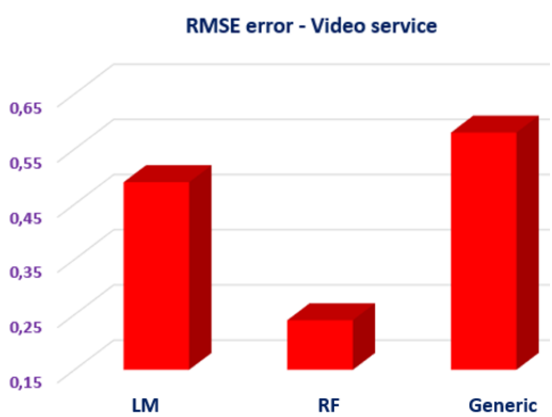

Fig. 7. Estimation performance in terms of RMSE for the Video service

Fig. 8 illustrates the results of testing the web service. It shows that the effectiveness of the Random Forest method and regression method are better than the generic QoE estimation method, which confirms our previous results (VoIP and video results). In this case, we see the specific RF method ensures 46% improvement over the generic approach.

According to our evaluation, the performances confirm the effectiveness of using ML methods to assess different services like video, VoIP and FTP. The results illustrate the added value for ISPs, in the encrypted traffic context, especially when we consider a specific QoE estimation model in the place of the generic estimation model in the QoE assessment process.

C. Perspectives

Our objective in this paper is to propose a new solution that helps ISPs to detect the different kinds of QUIC-based services with high accuracy on the one hand. On the other hand, it estimates the user's QoE for these services. This solution is implemented in a real testbed but can be improved by some additional considerations.

Currently, this work does not consider some specific MIoT application factors like video rebuffering duration or audio bitrate metrics in the QoE estimation model. Also, this work does not consider the codecs of the tested services. For example, SILK codec in the case of voice and H265/VP9 in the case of video service. We note that the used QoE estimations models are built using small experiments, where a reduced number of examples are used for the creation of QoE estimation models. Concerning the future works, a summarization is given below:

- Adding specific MIoT service parameters like codec, bit rate, etc.
- Improving the traffic classification module to detect additional services that use IoT like gaming, virtual reality (VR), mixed reality (MR) and Ultra HD video.
- Investigating various flow-based features to enhance the classification model in time processing and accuracy.
- Enhancing the QoE estimation module by building a large subjective database. Moreover, we can obtain some additional application parameters from the end-user side using PLUS [15], a new "path layer" for network operators on the encrypted protocols, to make the QoE estimation models more accurate.
- Integrating the proposed solution in a network operator infrastructure to study the performance of the Q2ET solution in a real context.

V. Conclusion

In this article, we propose a new solution, called the Quality Estimation Framework for Encrypted Traffic (Q2ET), which aims to help network operators in improving the quality of their services, including Multimedia IoT (MoIT) services, in the context of encrypted data. Indeed, network operators can no longer estimate the user perception of service in the context of systematic traffic encryption.

Q2ET is composed of two modules. The first module, called service detection module detects three different kinds of QUIC-based services (voice, video and file transfer) with high accuracy. The second module, called quality assessment module, can apply the appropriate quality assessment models for each kind of service to accurately estimate the users perceived qualities. Both of these two modules are implemented in a real testbed, where different QoE estimation methods are tested. The performances confirm the effectiveness of using ML methods to assess different services like video, VoIP and FTP. The results illustrate that the use of a specific QoE estimation model outperforms (by at least 40%) the use of a generic estimation model in the QoE assessment process.

REFERENCES

[1] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer Networks*, 54(15):2787 – 2805, 2010.

[2] Ahmed Bashir, Changcheng Huang, Biswajit Nandy, and Nabil Seddigh. Classifying P2P activity in Netflow records: A case study on BitTorrent. In *2013 IEEE International Conference on Communications (ICC)*, pages 3018–3023. IEEE, 2013.

[3] H. Chen, X. Yu, and L. Xie. End-to-end Quality Adaptation Scheme based on QoE Prediction for Video Streaming Service in LTE networks. In *2013* 11^{th} *International Symposium and Workshops on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt)*, pages 627–633, May 2013.

[4] CISCO. Cisco white paper report: Encrypted traffic analytics. *https://www.cisco.com/c/dam/en/us/solutions/collateral/ enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf*, pages 1–9, April 2019.

[5] VNI Cisco. Cisco visual networking index: Forecast and trends, 2017–2022. *White Paper*, 1, 2018.

[6] Giorgos Dimopoulos, Ilias Leontiadis, Pere Barlet-Ros, and Konstantina Papagiannaki. Measuring video QoE from encrypted traffic. In *Proceedings of the 2016 Internet Measurement Conference*, pages 513–526. ACM, 2016.

[7] Giorgos Dimopoulos, Ilias Leontiadis, Pere Barlet-Ros, and Konstantina Papagiannaki. Measuring video qoe from encrypted traffic. In *Proceedings of the 2016 Internet Measurement Conference*, IMC '16, pages 513–526, New York, NY, USA, 2016. ACM.

[8] Markus Fiedler, Tobias Hossfeld, and Phuoc Tran-Gia. A generic quantitative relationship between quality of experience and quality of service. *IEEE Network*, 24(2):36–41, 2010.

[9] A. Floris and L. Atzori. Quality of experience in the multimedia internet of things: Definition and practical use-cases. In *2015 IEEE International Conference on Communication Workshop (ICCW)*, pages 1747–1752, June 2015.

[10] I Goodfellow. Y. bengio und a. courville,deep learning,, 2016.

[11] S. Gring, A. Raake, and B. Feiten. A framework for qoe analysis of encrypted video streams. In *2017 Ninth International Conference on Quality of Multimedia Experience (QoMEX)*, pages 1–3, May 2017.

[12] H. J. Kim and D. H. Lee and J. M. Lee and K. H. Lee and W. Lyu and S. G. Choi. The QoE Evaluation Method through the QoS-QoE Correlation Model. In *2008 Fourth International Conference on Networked Computing and Advanced Information Management*, volume 2, pages 719–725, September 2008.

[13] J. Korhonen, N. Burini, J. You and E. Nadernejad. How to Evaluate Objective Video Quality Metrics Reliably. In *2012 Fourth International Workshop on Quality of Multimedia Experience*, pages 57–62, July 2012.

[14] K. D. Singh, Y. Hadjadj-Aoul and G. Rubino. Quality of Experience Estimation for Adaptive HTTP/TCP Video Streaming Using H.264/AVC. In *2012 IEEE Consumer Communications and Networking Conference (CCNC)*, pages 127–131, January 2012.

[15] Mirja Kühlewind, Tobias Bühler, Brian Trammell, Stephan Neuhaus, Roman Müntener, and Gorry Fairhurst. A path layer for the internet: Enabling network operations on encrypted protocols. In *2017 13th International Conference on Network and Service Management (CNSM)*, pages 1–9. IEEE, 2017.

[16] S. Souihi L. Amour and A. Mellouk. Controlled Laboratory dataset Using Dash.js video player. Access: . https://github.com/Lamyne/Q2ABR-ressources/tree/master/data, October 2017.

[17] Adam Langley, Alistair Riddoch, Alyssa Wilk, Antonio Vicente, Charles Krasic, Dan Zhang, Fan Yang, Fedor Kouranov, Ian Swett, Janardhan Iyengar, et al. The quic transport protocol: Design and internet-scale deployment. In *Proceedings of the Conference of the ACM Special Interest Group on Data Communication*, pages 183–196. ACM, 2017.

[18] lucas clemente. A quic implementation in pure go. *https://github.com/lucas-clemente/quic-go*, April 2019.

[19] T. Mangla, E. Halepovic, M. Ammar, and E. Zegura. emimic: Estimating http-based video qoe metrics from encrypted network traffic. In *2018 Network Traffic Measurement and Analysis Conference (TMA)*, pages 1–8, June 2018.

[20] Irena Orsolic, Mirko Suznjevic, and Lea Skorin-Kapov. Youtube qoe estimation from encrypted traffic: Comparison of test methodologies and machine learning based models. In *2018 Tenth International Conference on Quality of Multimedia Experience (QoMEX)*, pages 1–6. IEEE, 2018.

[21] Ponemon Institute Research. Global encryption trends study for 2018. see : https://www.ncipher.com/2018/global-encryption-trends-study. pages 1–8, April 2013.

[22] W. Robitza, M. Garcia, and A. Raake. A modular http adaptive streaming qoe model candidate for itu-t p.1203 (p.nats). In *2017 Ninth International Conference on Quality of Multimedia Experience (QoMEX)*, pages 1–6, May 2017.

[23] S. Aroussi and T. Bouabana-Tebibel and A. Mellouk. Empirical QoE/QoS Correlation Model based on Multiple Parameters for VoD flows. In *2012 IEEE Global Communications Conference (GLOBECOM)*, pages 1963–1968, December 2012.

[24] R. Schatz and S. Egger. An Annotated Dataset for Web Browsing QoE. 6th International Workshop on Quality of Multimedia Experience (QoMEX). Access: . https://www.schatz.cc/downloads/web-dataset/, September 2014.

[25] Abhishek Soni. Machine Learning classifier for VoIP and RTC Metrics. Access: . https://github.com/lmangani/voip-classifier, November 2017.

[26] Van Tong, Hai Anh Tran, Sami Souihi, and Abdelhamid Mellouk. A novel quic traffic classifier based on convolutional neural networks. In *2018 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2018.

[27] Hai Anh Tran, Said Hoceini, Abdelhamid Mellouk, Julien Perez, and Sherali Zeadally. Qoe-based server selection for content distribution networks. *IEEE Transactions on Computers*, 63(11):2803–2815, 2014.

[28] Y. Ben Youssef, A. Mellouk, M. Afif, and S. Tabbane. Video Quality Assessment Based on Statistical Selection Approach for QoE Factors Dependency. In *2016 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6, December 2016.

[29] T. Yue, A. M. Wei, H. B. Wang, X. D. Deng, and S. D. Cheng. A Comprehensive Data-driven Approach to evaluating Quality of Experience on Large-scale Internet Video Service. In *2016* 12^{th} *International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD)*, pages 1479–1486, August 2016.

[30] Yi Zeng, Huaxi Gu, Wenting Wei, and Yantao Guo. Deep-full-range: a deep learning based network encrypted traffic classification and intrusion detection framework. *IEEE Access*, 2019.