This is a postprint version of the following published document:

Julian Andres Caicedo-Muñoz, Agapito Ledezma Espino, Juan Carlos Corrales, Alvaro Rendón: QoS-Classifier for VPN and Non-VPN traffic based on time-related features, Computer Networks, Volume 144, 2018, Pages 271-279, ISSN 1389-1286

DOI: [10.1016/j.comnet.2018.08.008](https://doi.org/10.1016/j.comnet.2018.08.008)

© 2018 Elsevier B.V. All rights reserved.

This work is licensed under a [Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License](https://creativecommons.org/licenses/by-nc-nd/4.0/).

QoS-Classifer for VPN and Non-VPN traffic based on time-related features

Julian Andres Caicedo-Muñoz^{a,*}, Agapito Iedezma Espino^b, Juan Carlos Corrales Muñoz^a, Alvaro Rendon Gallon^a

^aTelematics Engineering Group (GIT), Universidad del Cauca, Campus Tulcan, Cauca-Popayan, Colombia

^bDepartment of Computer Science and Engineering, Universidad Carlos III de Madrid, Avenida de la Universidad 30, 28911, Leganes-Madrid, España

Abstract

The Quality of Service (QoS) is a continue challenging issue in the telecommunication industry, manly having an impact over telco services provision. Traffic classification, traffic marking and policing are general stages to QoS managing. Different approaches have focused on traffic classification, being machine learning algorithms the promising ones. However, traffic marking over time-related features is not widely explored, especially for VPN traffic. Hence, a specific QoS classifier for VPN traffic base on per-hob Behavior (PHB) over a specific domain was proposed. To this end, a baseline QoS-Marked dataset was generated as from 3: characterized VPN traffic one, besides some machine learning algorithms were compared and T-Tester was performed. As a result, 42: Bagging has the best behavior for all scenarios applied and its higher value is 94,42% of accuracy. Hence, a QoS classifier is an 43: effective approach for traffic treatment over DiffServ networks.

Keywords: QoS classifier, per-hob Behavior, VPN Traffic Characterization

1. Introduction

The Quality of Service (QoS) is a continue challenging issue in the telecommunication industry, manly having an impact over telco services provision. In that sense, ITU-T has defined QoS as "Totality of characteristics of a telecommunications service that bear on its ability to satisfy stated and implied needs of the user of the service" [1]. In a narrow sense, QoS has a tight relationship with network performance, particularly, jitter, bandwidth, delay, and throughput which are a few quantitative parameters in the network management, but also, QoS is concerned of how managing any congestion in the network. Hence, traffic classification, traffic marking and policing are the general stages for controlling traffic and preventing any network collapse.

Some works as [2] [3] [4] are promising approaches for Traffic Classification base on machine learning algorithms, but these are not considering neither QoS managing nor implementation of any method of marking. Marking and policing process were considered by [5] [6], wherein each packet is marked base on customer preferences and payload. Payload checking for marking is an effective manner to determinate the type of traffic, but is not an efficient solution, specifically for marking VPN traffic wherein user data is protected. To solve this, classification and marking processes base on some time-related features for VPN and Non-VPN traffic were proposed. Two initial QoS classifier tasks were defined for treatment of traffic and a QoS-

marked dataset was generated for being routed over a DiffServ network.

A Weka experiment was configured for testing and training some machine learning algorithms over baseline QoS-Marked dataset and replicated over an original characterization VPN and Non-VPN traffic dataset [7]. Finally, a T-Tester was performed for algorithms comparison taking account their statistical significance.

The rest of this paper is structured as follows. Section 2 presents methods and original dataset used as support elements in this work. Besides, a QoS classifier approach for labeling of characterization VPN and Non-VPN traffic base on PHB method is described. Section 3 outlines the results obtained after having performed some machine learning algorithms. Section 4 discusses the results obtained. Finally, section 5 conclusion and future works are presented.

2. Materials and Methods

According to QoS managing the traffic classification, traffic marking and policing are general stages for controlling network flows and maintaining an acceptable performance in the telco service provision (See Figure 1).

Figure 1: General stages for QoS Managing - Adapted from [8]

*Corresponding author. Tel.: +57 3004930101; E-mail: jacaicedo@unicauca.edu.co

Email addresses: jacaicedo@unicauca.edu.co (Julian Andres Caicedo-Muñoz), ledezma@inf.uc3m.es (Agapito Iedezma Espino), jcorral@unicauca.edu.co (Juan Carlos Corrales Muñoz), arendon@unicauca.edu.co (Alvaro Rendon Gallon)

Traffic Classification stage is the procedure to identify different applications and protocols that exist in a network [9]. Michael Finsterbusch et.al [10] has split out the traffic classification techniques in four categories: Port-Based, Statistical approach, Protocol decoding and Pattern-based; Both Port-Based and Statistical use techniques not intrusive as protocol decoding and pattern-based approaches. However, Port-Based depends on the well-known ports for protocols assigned by IANA [11]. In fact, some applications that are not registered can be bypassing censorship using other protocols or can be using random ports to send data. As such, statistical approach is increasing attention during last decade, especially, the machine learning algorithms are promising alternatives.

Marking stage is a procedure to modify the QoS fields of the incoming and outgoing packets base on service policies [8]. Marking can be done in layer 2 (CoS, Class of Service) or in layer 3 (IP Precedence or DSCP) of any packet, particularly, Differentiated Service Code Point (DSCP) is used for managing traffic classes in a Differentiated Services (DiffServ) networks in a proper manner [12]. Besides, having a well-defined DSCP as proposed by RFC-2474 [13], allowing an effective mapping to EXP field in MPLS networks [14].

Policing stage is a procedure to monitoring of data rates for a particular traffic class [8]. Policing allows to having a threshold for re-marking or dropping of packets. Increasing of traffic as regards policing data gathered is taken account to define new QoS policies for controlling and structure the network.

In this paper we focused on traffic classification and marking stages, principally over encrypted VPN traffic. The Characterization VPN traffic is a challenging issue due to being a protocol encapsulation method for maintaining the privacy of data over network. Recently, a work is showed an encrypted VPN traffic dataset based on time-related features [7]. The authors proposed a flow-based classification method and compared only two classifier algorithms. Next is briefly described the dataset, selected algorithms and scenarios.

2.1. Dataset

The dataset contains real traffic generated by traditional applications over regular session and VPN session (Firefox, SMPTS, Skype, Facebook, among others). As result, the authors in [7] have labeled a dataset with 14 different traffic classes split out in 7 VPN and 7 Non-VPN traffic classes separately. The type of traffic is showed in Table 1.

Table 1: Traffic by applications [7]

Traffic	Application
Web Browsing (BRW)	Firefox and Chrome
Email (Mail)	SMTPS, POP3S and IMAPS
Chat	ICQ, AIM, Skype, Facebook and Hangouts
Streaming (STR)	Vimeo and Youtube
File Transfer (FT)	Skype, FTPS and FTP using Filezilla
VoIP	Facebook, Skype and Hangouts
P2P	uTorrent and Transmission (Bittorrent)

2.2. Machine Learning Algorithms

Arash Habibi et.al [7] have only chosen C4.5 and KNN to evaluate the quality of classification processes based on two common metrics: Precision and Recall. As a result, C4.5 algorithm presents best behavior in two scenarios.

Finally, two scenarios were implemented to obtain the traffic classes as depicted in Figure 2. First one (A), distinguishes between only a Non-VPN and VPN traffic, later a specific characterization is realized for labeling each class according to Non-VPN and VPN Traffic (A2). Second one (B), mixed dataset is obtained in one step and all VPN and Non-VPN traffic is labeled.

Figure 2: Scenarios [7] - A2 and B were analyzed

2.3. QoS Classifier approach

The approach proposed was focused on the two early stages for QoS managing, Traffic Classification and Marking. Figure 3 is depicted a general approach.

Figure 3: QoS Classifier general approach

QoS classifier has two inputs. First, traffic with statistical time-related features. Principally, time-related features are obtained in simple manner through analyzing of flow-based data and computationally efficient [7]. Besides, statistical time-related features have a good results by applying some machine learning algorithms techniques [15]. Second, a policies coming from any application domain. An application domain depends on which context a network administrator provides QoS

for different services. Indeed, QoS policies in the education domain differ from normal subscriber domain (i.e., in the education context can prevail VoIP and File transfer services over Chat or P2P services, meanwhile in the subscriber domain, services can be attended indistinctly or giving a bit more value to Streaming service base on recently consumer trends).

QoS Classifier output is a Marked Traffic in order to QoS managing over the network. Marking process depends on policies established by particular domain.

QoS Classifier contains two tasks to combining the inputs and generating a QoS marked traffic. Analyzing Policies task was defined for mapping any specific domain traffic rule to a specific QoS field (e.g. DSCP in DiffServ Architectures, EXP in MPLS). Labeling task was defined to changing the type traffic characterized to a well-known label in the network (e.g. AF/EF in DiffServ or E-LSP/L-LSP in MPLS).

3 :

2.4. General Approach Implementation

To verify general approach, some particular policies over specific VPN traffic were implemented in order to having a QoS Marked traffic (Figure 4).

46 "

47 "

48 "

49 "

4 :

4 ;

52 "

53 "

54 "

55 "

56 "

57 "

58 "

59 "

5 :

5 ;

62 "

63 "

64 "

65 "

66 "

67 "

68 "

69 "

6 :

6 ;

72 "

73 "

74 "

75 "

76 "

77 "

78 "

79 "

7 :

7 ;

82 "

Figure 4: QoS Classifier Implementation

2.4.1. Subscriber domain

Regular consumers require all services work well over the network (e.g home user). Today consumer trends are focused on streaming video as reported by Internet.org [16]. On the other hand, VPN applications are being more popular because of protecting user personal data [17] [18].

2.4.2. VPN/NonVPN-Traffic

This traffic needs to be processed before getting into QoS classifier. To this end, the normal VPN and NonVPN traffic generated by some application (e.g Skype, Hangouts, Chrome, Facebook) and conveyed over the network are collected and processed as depicted by [7]. As result, a VPN and Non-VPN traffic with some time features are generated as a network traffic flows. Actually, VPN traffic is an important issue due to increasing of users are going online using VPN applications for avoiding internet restrictions [19].

2.4.3. QoS Classifier

An analyzing policies task was implemented taking account services class definition by RFC-4594 [20] and per-hop behavior (PHB) as defined by RFC2474 [13]. This task is network administrator knowledge dependent and manual process. A labeling task was realized by changing type VPN traffic (Traffic-Labels) to PHB-Labels using a weka filter algorithm. As a result, Table 2 shows the relationship between Traffic-Labels implemented by Arash Habibi, et.al. [7] and PHB-Labels base on subscriber domain rules for representing services classes and dropping.

Table 2: Labels Mapping

Scenario	Traffic-Labels	PHB-Labels ¹
NonVPN	Mail	
	Chat	AF12
	FT	
	BRW	AF22
	STR	
	P2P	AF32
A2/B	VoIP	EF
	VPN-Mail	
	VPN-Chat	AF11
VPN	VPN-FT	
	VPN-BRW	AF21
	VPN-STR	
	VPN-P2P	AF31
	VPN-VoIP	EF

2.4.4. QoS PHB Marked

A specific baseline Dataset is the outcome of QoS Classifier. An Input dataset with statistical time-related features was modified taking account a network administrator rules for specific domain and the PHB concept [21].

3. Experiments

Two baseline dataset were obtained (QoS-Marked Traffic). A2 dataset has PHB-Labels ranging from AF12 to AF32 for Non-VPN and AF11 to AF31 for VPN traffic. VoIP traffic was labeled with EF for both. B dataset is a mixed of all PHB-labels ranging from AF11 to AF32 and its priorities numbers (Table 2). As suggest Arash Habibi, et.al. in [7], different flow timeout (ftm) values were selected for testing (15s, 30s, 60s, 120s).

Table 3 presents the setup for experiment. WEKA experimenter for testing each scenario was used. Both scenarios have the same cross validation settings and machine learning algorithms but different datasets. A2 scenario has VPN and Non-VPN for PHB-labels (AF11 to AF31 and AF12 to AF32, respectively). B scenario has all-in one PHB-Labels. The experiment was replicated in original dataset as well (Traffic-Labels). Finally, a T-Tester was performed in the algorithms for each dataset in order to getting a trustworthy statistical result.

¹Drop probabilities: VPN Traffic has lower drop probability than NonVPN Traffic. (i.e AFx1 has lower drop probability than AFx2)

Table 3: Experiment setup				
Approach	Machine Learning Algorithms/WEKA	Scenario	Cross Validation(Folds)	Run
Traffic/PHB-Labels	C4.5/J48	A2-B	10	10
	KNN (K=1)/IBK			
	Naive Bayes			
	Rule(Part)			
	Neuronal Networks/MLPClassifier			
	Bagging (C4.5)			
	Boosting (C4.5)/AdBoostM1

Figure 5: Percent Correct for Traffic-Labels and PHB-Labels approaches in Scenario A2

3.1. Results and analysis of scenario A2

The accuracy (PercentCorrect) in the A. H. Lashkari et al. work[7] using a single run for cross validation and not T-Tester for Traffic-Labels indicated that C4.5 algorithm has a little better behavior than KNN algorithm. A little decrease in the precision for 15s to 120s was obtained. However, the numerical difference is not strong enough criteria for getting a statistical significance. To solve that, a T-Tester was applied and other machine learning algorithms were performed (See Figure 5 parts a, b). As result, C4.5 is better than KNN and significantly better for all ftm values. This result validates what said by work aforementioned. However, C4.5 has not the best behavior. Indeed, Bagging and Boosting algorithms are significantly better than C4.5 but not significantly different between them (except for 60s ftm value in Non-VPN traffic wherein boosting is worse). Table 4 shows all results obtained by applying a statistical test based on Paired T-Tester (characters '*' and 'v' represent sta-

tistically significant difference; lower scores and higher scores, respectively. Character '-' not represent statistically significant difference).

Our approach has the same behavior. C4.5 is significantly better than KNN for all ftm values, but worse in comparison with Bagging and Boosting (Figure 5 parts c, d). Both Bagging and Boosting are significantly better for all ftm values but not significantly different between them (not exception is presented). Moreover, PHB-Labels has higher scores for all time out values than Traffic-Labels approach (See Figure 5 parts e, f). 15s and 30s ftm are presented as higher results). Table 5 shows all results obtained by applying a statistical test based on Paired T-Tester (characters '*' and 'v' represent statistically significant difference; lower scores and higher scores, respectively. Character - not represent statistically significant difference).

Finally, our approach has better behavior than Traffic-Label approach and continuing with the same trend wherein accuracy

Figure 6: Percent Correct for Traffic-Labels and PHB-Labels approaches in Scenario B

score is lower than PHB-Labels (See figure 6 part a). KNN, Naive Bayes and Multilayer perceptron have worse behavior than C4.5, rules, Bagging and Boosting for all ftm values. C4.5 and Rules are not significantly different but are significantly worse than Bagging and Boosting. Indeed, Bagging is significantly better than boosting and the other ones for all ftm values (See tables 4 and 5). Hence, Bagging is more suitable for Traffic-Labels and PHB-Labels approaches. Again, the best results are presented for shorter ftm value in the overall accuracy and PHB-Labels approach has better scores than Traffic-Labels approach (Figure 6, part d).

Precision and recall by class have a behavior a little different in each ftm for PHB-Labels Precision in AF12 class has high scores for 15s and 120s (See figure 6 part c); bagging is significantly better than others algorithms for all ftm values, excepting for 30s and 60s wherein is not significantly different from boosting (for recall none change was detected). Recall in AF22

Table 4: Statistical Significance by Algorithms in Traffic-Labels Approach

Scenario	ftm (s)	C4.5	KNN	NaiveBayes	Rule	NeuronalNetworks	Bagging	Boosting
A2	NonVPN	15	91.81	87.30*	49.68*	92.48 v	70.59*	93.09 v
		30	89.89	86.48*	44.87*	90.36-	67.66*	91.75 v
		60	88.06	84.05*	31.74*	88.58-	57.31*	90.63 v
		120	89.74	87.20*	39.53*	90.18-	69.17*	91.74 v
	VPN	15	85.91	82.52*	22.49*	86.09-	60.93*	88.28 v
		30	86.50	85.27*	35.18*	86.86-	58.19*	89.03 v
		60	84.15	82.21*	34.35*	84.22-	58.11*	86.66 v
		120	83.62	82.43*	38.86*	84.48-	54.90*	86.43 v
B	VPN-NonVPN	15	81.80	75.00*	27.06*	81.93-	41.89*	84.81 v
		30	80.15	74.82*	24.99*	80.10-	38.50*	83.58 v
		60	77.80	72.75*	20.46*	77.43-	36.11*	81.38 v
		120	77.80	73.25*	22.59*	77.60-	38.16*	81.16 v

Table 5: Statistical Significance by Algorithms in PHB-Labels Approach

Scenario	ftm (s)	C4.5	KNN	NaiveBayes	Rule	NeuronalNetworks	Bagging	Boosting
A2	NonVPN	15	93.23	88.95*	61.14*	93.70-	74.10*	94.42v
		30	91.35	88.18*	59.13*	91.60-	73.11*	92.89 v
		60	91.56	88.26	44.97*	91.89-	67.00*	93.45 v
		120	91.06	89.40*	47.73*	91.03-	72.62*	92.94 v
	VPN	15	90.89	87.69*	37.88*	91.11-	73.91*	92.80 v
		30	91.01	89.11*	44.49*	90.96-	71.72*	92.82 v
		60	87.88	85.87*	48.03*	87.64-	66.72*	90.34 v
		120	87.78	85.02*	48.10*	88.01-	64.75*	89.42 v
B	VPN-NonVPN	15	84.25	77.81*	42.40*	84.65-	53.11*	86.94 v
		30	82.54	77.20*	32.85*	82.32-	48.03*	85.38 v
		60	81.02	76.08*	24.25*	80.92-	47.08*	84.40 v
		120	79.79	75.13*	29.66*	79.60-	42.31*	82.90 v

class has high scores for 60s and 120s (See figure 6 part d); bagging is significantly better than others algorithms for all ftm values, excepting for 15s and 30s wherein is not significantly different from boosting. EF and AF31 classes have the same behavior for bagging and boosting in all ftm values, having high scores for both precision and recall (but not significantly different between them). Besides, higher scores are presented for EF class (Figure 6 parts c, d). For the other classes bagging is significantly better than boosting in at least one ftm value both precision and recall.

4. Discussion

A QoS-marked traffic was obtained as from characterized VPN and Non-VPN traffic, wherein PHB-Labels are more suitable for managing the network traffic than Traffic-Labels in [7]. Indeed, PHB-Labels are well-known in Diffserv networks for routing traffic in a proper manner. Moreover, PHB-Labels can be mapped to EXP field as explained in [14] for a MPLS Network.

Statistical significance analysis showed that Bagging and Boosting have the best accuracy in A2 and B scenarios both Traffic-Labels and PHB-Labels approaches. Bagging is significantly better than boosting in B scenario but not significantly

different in A2 scenario, except for 60s-NonVPN wherein bagging is better in Traffic-Labels approach. Hence, bagging is the best classifier for Traffic-Labels and PHB-Labels in two scenarios. Besides, PHB-Labels approach have better results than Traffic-Labels approach for all ftm values in each scenario and for all algorithms analyzed. On the other hand, MLPClassifier has to be tuning in order to achieving higher scores or any domain specific implementation has to be done for improving the accuracy.

QoS-Classifer was proposed as a mechanism for controlling traffic in proper manner and QoS managing through PHB-Labels. To this end, two tasks were defined and implemented. First one, an analyzing policies task taking account the network policies for marking incoming traffic as a well-known network label. However, this task is network administrator knowledge dependent and domain specific. To solve this, a domain ontology would be a good option to having parametrized policies in each domain wherein marking process can be more effective. Second one, a labeling task modifies one traffic label to another one for traffic control in the network. Again, labeling task is policing dependent and manual execution. A recommender system based on traffic behavior can suggest a well-known label for any specific domain policy.

5. Conclusions and future works

In this paper the effectiveness of time-related features for VPN and Non-VPN traffic classification was confirmed. Moreover, we found that bagging and boosting are significantly better than C4.5 in the Traffic-Labels approach. We have proposed a QoS-Classifer with two tasks for traffic treatment over the network. Our proposal took into account the PHB-DiffServ concept and specific domain policies for traffic marking, as the well-known AF and EF labels. Hence, the QoS-Classifer output (QoS-Maked) allows routing all traffic in an effective manner. Finally, bagging has achieved better results for all ftm values in PHB-Label approach, besides our approach has better behavior in overall accuracy than Traffic-Labels approach for all machine learning algorithms in each ftm values both A2 and B scenarios. Higher scores with statistically significant difference were obtained in scenario A2 with 94,42% and 92,82% of accuracy for Non-VPN and VPN traffic, respectively.

As future work a domain ontology can be defined for recommender systems proposals. The ontology will allow to having a labeling recommender system over an incoming network traffic with time-related features. Besides, a mechanism base on incremental learning is suitable for implementing the policing stage in QoS managing process, mainly for being the network traffic so dynamic and requiring differenced treatment for each new telco services. Finally, a Neuronal Network tuning or implementing specific one is necessary for reaching higher scores and better behavior.

6. Acknowledges

The authors would like to thank the Administrative Department of Science, Technology and Innovation -Colciencias- for funding the phd program in which this work was developed. Our sincere thanks go to the CAOS group members for the support provided and the remarkable suggestions.

References

- [1] ITU-T E.800, Definition of terms related to quality of service, Tech. rep. (2008).
URL <https://www.itu.int/rec/T-REC-E.800/en>
- [2] F. Ertam, E. Avcı, A new approach for internet traffic classification: GA-WK-ELM, Measurement 95 (2017) 135–142. doi:10.1016/j.measurement.2016.10.001.
- [3] N. F. Huang, G. Y. Jai, H. C. Chao, Y. J. Tzang, H. Y. Chang, Application traffic classification at the early stage by characterizing application rounds, Information Sciences 232 (22) (2013) 130–142. doi:10.1016/j.ins.2012.12.039.
URL <http://dx.doi.org/10.1016/j.ins.2012.12.039>
- [4] R.-y. Wang, Z. Liu, L. Zhang, Method of data cleaning for network traffic classification, The Journal of China Universities of Posts and Telecommunications 21 (3) (2014) 35–45. doi:10.1016/S1005-8885(14)60299-5.
- [5] C. J. Liu, Tracking DSCP marking of packets in a QoS enabled triple-play IP network, in: 3rd International Conference on Networking and Services, ICNS 2007, 2007. doi:10.1109/ICNS.2007.121.
- [6] M. Peresse, J. M. Bonnin, Enabling QoS using packet marking and scheduling in a multi-homed NEMO mobile router with GNU/Linux, in: 2009 9th International Conference on Intelligent Transport Systems Telecommunications, ITST 2009, 2009, pp. 58–62. doi:10.1109/ITST.2009.5399382.
- [7] A. H. Lashkari, G. Draper-gil, M. Saiful, A. A. Ghorbani, Characterization of Encrypted and VPN Traffic using Time-related Features, in: O. Camp, S. Furnell, P. Mori (Eds.), In Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP 2016), Rome, 2016, pp. 407–414. doi:10.5220/0005740704070414.
URL <http://www.icissp.org/>
- [8] Cisco Systems, Quality of Service Configuration Guide, Release 4.0(4) SV1 (1), Tech. Rep. 4, Cisco Systems (2009).
- [9] Cisco Systems, WAN and Application Optimization Solution Guide Cisco Validated Design, Tech. Rep. August, San Jose-USA (2008).
- [10] M. Finsterbusch, C. Richter, E. Rocha, J. A. Müller, K. Hänßgen, A survey of payload-based traffic classification approaches, IEEE Communications Surveys and Tutorials 16 (2) (2014) 1135–1156. doi:10.1109/SURV.2013.100613.00161.
- [11] IANA, Service Name and Transport Protocol Port Number Registry (2016).
URL <http://www.iana.org/>
- [12] Cisco Systems, DiffServ - The Scalable End-to-End QoS Model (August) (2005) 1–19.
URL <http://www.cisco.com>
- [13] K. Nichols, S. Blake, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, Tech. rep., IETF-RFC2474 (1998).
URL <https://www.rfc-editor.org/info/rfc2474>
- [14] L. Wu, B. Davie, S. Davari, P. Vaananen, R. Krishnan, P. Cheval, J. Heinanen, Multi-Protocol Label Switching (MPLS) Support of Differentiated Services Status, Tech. rep., IETF-RFC3270 (2002).
URL <https://www.rfc-editor.org/info/rfc3270>
- [15] J. Erman, A. Mahanti, M. Arlitt, Internet Traffic Identification using Machine Learning, Global Telecommunications Conference, 2006. GLOBECOM '06. IEEE (2006) 1–6. doi:10.1109/GLOCOM.2006.443.
- [16] Internet.org, State of Connectivity-A Report on Global Internet Access, Tech. rep., Internet.org (2015). arXiv:arXiv:1011.1669v3, doi:10.1017/CBO9781107415324.004.
- [17] A. Alshalan, S. Pisharody, D. Huang, A Survey of Mobile VPN Technologies, IEEE Communications Surveys and Tutorials 18 (2) (2016) 1177–1196. doi:10.1109/COMST.2015.2496624.
- [18] F. Palmieri, VPN scalability over high performance backbones evaluating MPLS VPN against traditional approaches, in: Proceedings - IEEE Symposium on Computers and Communications, 2003, pp. 975–981. doi:10.1109/ISCC.2003.1214243.
- [19] Global Web Index, The Missing Billion: How Analytics is Wiping The Emerging World Off The Map (2014).
URL <https://www.globalwebindex.net>
- [20] J. Babiarczyk, K. Chan, F. Baker, Configuration Guidelines for DiffServ Service Classes, Tech. rep., IETF-RFC4594 (2006).
URL <https://www.rfc-editor.org/info/rfc4594>
- [21] D. Grossman, New Terminology and Clarifications for Diffserv, Tech. rep., IETF-RFC3260 (2002).
URL <https://www.rfc-editor.org/info/rfc3260>