# Personalized Service Degradation Policies on OTT Applications Based on the Consumption Behavior of Users

Juan Sebastián Rojas(✉), Álvaro Rendón Gallón, and Juan Carlos Corrales

Universidad del Cauca, Calle 5 Nº 4-70, Popayán, Colombia
{jsrojas, arendon, jcorral}@unicauca.edu.co

**Abstract.** The proliferation of IP-based telecommunication networks has facilitated the decoupling of application and network layers. This kind of systems allows that Over the Top (OTT) providers deliver their content and applications directly to end users, but at the same time, the OTT applications have generated a growing impact on mobile data traffic and data revenues. In the mobile network's scope, where the Telcos offer users data plans with limited consumption, service degradation is a measure implemented in a generalized way to apply limits to the amount of data that can be transferred by the users over a period. Currently, when a user exceeds his/her established consumption limit, the Telcos, to save resources and ensure the correct performance of the network, restrict the bandwidth according to user consumption. The vast majority of approaches have not considered the consumption behavior of users to propose a set of personalized service degradation policies that benefit the Telcos but take into consideration the users' behavior. This paper proposes personalized service degradation policies, from the identification of different OTT services applying statistical analysis and deep packet inspection, and a classification of users, according to their consumption behavior and machine learning algorithms.

**Keywords:** OTT applications · Service degradation · Machine learning
Classification · Dataset · DPI

## 1 Introduction

The Information and Communications Technologies (ICT) market is undergoing extremely rapid changes. The current generation of service and application companies that use an Over-the-Top (OTT) business model, as a platform for their new products, has begun to generate a major change in the traditional business model used by Internet Service Providers (ISP). Companies and applications such as Skype, YouTube, WhatsApp, Netflix, among many others, have emerged to tackle the new needs in communications and functionalities that users demand [1].

Due to this change the ISPs have found themselves in a scenario that represents great difficulties, where they are no longer the sole competitors in the market and through the scheme proposed by OTT services have become an intermediary that only

O. Gervasi et al. (Eds.): ICCSA 2018, LNCS 10962, pp. 543–557, 2018.
https://doi.org/10.1007/978-3-319-95168-3_37

carries information between OTT applications and the different users who have hired their Internet connection services. For this reason, their traditional business model where the user hired access to an internet connection and different applications deployed through their infrastructure is being remodeled for a more flexible one that considers OTT service providers as allies. This way, ISPs can generate revenue through from the high consumption users of this type of applications. On the other hand, OTT service providers obtain benefits by complying with a service level agreement (SLA) that guarantees the correct operation of their applications.

However, although this type of agreement between the ISP and OTT service providers holds advantages for both parties, there is a situation that has not been considered especially in the mobile networks: the service degradation.

OTT applications are known by their large consumption of network resources for their correct operation and in the mobile networks scope, where mobile operators offer users data plans with limited consumption, service degradation is a mechanism implemented in order to apply limits to the amount of information that can be transferred by the users over a period of time [2–4]. It is usually applied when a user exceeds his/her established consumption limit, in order to save resources and ensure the correct performance of the network. Nevertheless, this degradation is applied in a generalized way, i.e., it affects the performance of all the applications that the user can use. Therefore, the behavior and preferences presented by the user in the consumption of OTT applications is not considered and furthermore it is a breach of the service level agreements that the ISP could have established with certain OTT service providers.

Considering the previous statements, this paper introduces a proposal of personalized service degradation policies based on user's consumption behavior. First a testbed is implemented to build a dataset that enables the identification of different OTT applications from the internet traffic flows generated by users in a network section from Universidad del Cauca. Then, such identification enables the clustering of 1581 users, based on their consumption behavior, into three groups: Low Consumption, Medium Consumption and High Consumption. After the clustering process, a set of personalized policies are proposed for each group following the PCC (Policy and Charging Control) architecture of a LTE network [5]. Furthermore, a classification model capable of classifying a new user in one of the three identified clusters is obtained through machine learning algorithms.

This paper is arranged as follows: Sect. 2 presents a brief background of the most relevant concepts to the proposal; Sect. 3 presents the related works found through a literature review following a systematic mapping methodology [6]; Sect. 4 introduces the proposed scenario; Sect. 5 illustrates the personalized service degradation policies and Sect. 6 shows the conclusions and future works.

## 2 Background

### 2.1 Data Caps

It is a measure implemented by Internet service providers, where limits are applied to the amount of information that can be transferred by network users over a period of time that varies depending on the type of network. Normally it is applied when a user exceeds his/her established consumption limit, in order to save resources and ensure the correct performance of the network. Furthermore it aims at obtaining income by applying surcharges on the excess consumption by the user [2, 3].

### 2.2 Quality of Service (QoS)

From the perspective of network operators, Quality of Service (QoS) can be considered as a performance measurement of the network which focus on operation parameters only. In RFC 2386 from IETF (Internet Engineering Task Force) it is defined as “The set of service requirements that the network must meet in the transport of a flow”, while for ITU (International Telecommunications Union) it is defined as “all the characteristics of a telecommunication service that determine Its ability to meet the explicit and implicit needs of the service user” [7–10].

### 2.3 PCC Rule

A PCC rule is an element of the PCC Architecture (Policy and Charging Control) of an LTE network. The purpose of the PCC rule is to detect a packet belonging to an IP flow or SDF (Service Data Flow), identify the service or application the SDF contributes to, provide applicable charging parameters for the SDF, and provide policy control for the SDF [5].

### 2.4 Traffic Classification

It is an automated process that, according to different parameters, categorizes traffic within a network into different classes. Each class can be treated in a different way in order to differentiate the services consumed by a user [11, 12]. Traffic classification in IP networks is usually done in three ways: Port Number Classification, Deep Packet Inspection (DPI) and Statistical Classification. A combination of the last two methods is implemented in this paper.

**Statistical Classification.** The strategy developed by this approach is to perform the classification using behavioral or statistical patterns based on flow-level data or generic properties from the packets such as addresses, ports, packet size, and interarrival times and so on. The main advantage of the statistical classification is the ability to identify a protocol without having to examine the payload carried by the packet [12].

**Deep Packet Inspection.** DPI approaches have been intensively deployed in traffic classification approaches as well as Network Intrusion Detection Systems (NIDS). Through DPI it is possible to compare the contents of captured packets against a set of rules which are usually written in string format. The most common tools to implement are nDPI (through ntopng), libprotoident, JnetPcap, among others [12].

## 3 State of the Art

An extensive literature review following the systematic mapping methodology proposed in [6] was carried out in order to obtain an overview of the research area and determine the quantity and type of related works. The topics of interest were: Service degradation aiming at identifying how this resource control mechanism is managed within ISPs and mobile networks; Quality of service (QoS) aiming at identifying which are the parameters related to service degradation; Traffic classification focusing on identifying the most popular techniques used for this process; OTT services aiming at knowing how this topic has been developed in the research field and at finding datasets that enabled the development of a classification model; Categorization of Users in a mobile network in order to know how operators classify the users inside the network.

Following the systematic mapping methodology the following related works are highlighted: In [13] Agababov et al., present "Flywheel" a proxy service for HTTP that aims to extend the life of user data plans in mobile networks, by reducing the size of the packets that are exchanged between servers and user devices. "Flywheel" integrates with Chrome browser and on average reduces by 50% the consumption in the data plans generated by the navigation and loading of web pages. In [2, 3] Chetty et al., presented results from a qualitative study of households living with bandwidth caps and the design and implementation of a tool, called "uCap", to help home users manage Internet data.

In [4] the US Company Ixia, presents in a white paper an analysis of the QoS policies (dynamic allocation of network resources, priority control, limitation of traffic rates) that are usually implemented in a LTE (Long Term Evolution) mobile network. Furthermore, they present the QoS parameters that significantly affect the performance of the different services offered in the network (video, voice, gaming, internet, etc.) and highlight the importance of categorizing users for a mobile operator in order to efficiently manage network resources. In [14] Williams et al., present a preliminary comparison of the performance of 5 machine learning algorithms (Naive Bayes, C4.5, Bayesian Network, Naive Bayes Tree) for the classification of IP traffic, concluding that the algorithm of decision tree C4.5 is the most accurate and efficient. In [15] Yang et al., present an analysis of the behavior of users in the consumption of mobile internet within a 3G. Through the analysis, they proposed three types of characterization for the users: Consumption of the data plan, which focuses on the rate of consumption generated by the user and classifies them into two profiles: normal user and heavy user; Mobility pattern where they focus on identifying the movement patterns of users within the network and Application consumption that focuses on what type of applications are mostly used through the mobile internet link. Finally, it is worth mentioning that most of the works related to OTT services [16–19] only presented different analysis on ISPs business models and the sudden changes provoked by the OTT service providers.

The previous related works show that there is a trend related with OTT services, data caps and service degradation that aims at helping the user to avoid being affected by such mechanism especially in mobile networks. However, to the best of our knowledge there are no works that presented a dataset related with traffic from OTT applications or a model aimed at the identification of the user consumption behavior in order to perform a personalization of the service degradation policies applied to each user by the network operators.

## 4 Proposed Scenario

With the aim of proposing a set of personalized service degradation policies considering the user's consumption behavior around OTT applications, three main sections have been established: the dataset description, showing its attributes and structure; the dataset preprocessing describing all the activities performed before the modeling; the classification modeling describing the obtained results in the tests performed with 8 machine learning algorithms.

### 4.1 Dataset Description

The data presented on this paper was collected in a network section from Universidad Del Cauca performing packet captures at different hours, during morning and afternoon, over six days (April 26, 27, 28 and May 9, 11 and 15) of 2017. A total of 16.545.768 instances were collected (1.405.590 for April 26, 5.037.080 for April 27, 927.987 for April 28, 2.308.883 for May 9, 3.709.524 for May 11 and 3.156.704 for May 15) and are currently stored in CSV (Comma Separated Values) files, one per day. The dataset presented in this paper is available at [20].

As can be seen in the provided link, three different datasets are available:

**Dataset Version 1.** This dataset contains the 16.545.768 instances with 87 attributes captured over the six days. Considering its size, the dataset was divided in six CSV files (one per day). Each instance holds the information of an IP flow generated by a network device i.e., source and destination IP addresses, ports, interarrival times, layer 7 protocol (application) used on that flow as the class, among others that are illustrated on Table 1. Most of the attributes are numeric type but there are also nominal types and a date type due to the Timestamp. Furthermore, this version of the dataset holds all the application labels (79 different applications) that were found during the DPI process that will be described in a following section.

**Dataset Version 2.** This dataset contains 3.577.296 instances on single CSV file. It has the same structure as the first version, however all the instances that had Unknown, Flow_Not_Found and SSL as class label were removed since most of them were network control flows or applications that could not be recognized with the DPI processing due to payload encryption and did not contribute to the subsequent analysis.

**Users Groups Dataset.** This dataset contains 1581 instances on a single ARFF file. It is the resulting dataset after the clustering process that is described in a subsequent section. Each instance represents a user and holds a summarized information obtained from the second version of the dataset about the consumption behavior related to 29 OTT applications identified in the DPI process. It has 131 attributes including user IP address, total of IP flows generated per application, mean flow duration per application, average packet size of the flows per application, average bytes per second per application and the user group as class label. It is the dataset that allows the proposal of personalized service degradation policies for the users of each group.

**Table 1.** Dataset attributes and description.

| Groups of attributes | Attributes | Description |
|---|---|---|
| Network identifiers (7 attributes) | FlowID; Source IP; Source Port; Destination IP; Destination Port; Protocol; Timestamp | These attributes hold all the information related to the source and destination of an Internet flow, i.e., IP addresses, transport layer protocol and ports |
| Flow descriptors (36 attributes) | Total Fwd Packets; Total Bwd Packets; Total Length of Fwd Packets; Total Length of Bwd Packets; Fwd Packet Length Max; Fwd Packet Length Max; Fwd Packet Length Min; Fwd Packet Length Mean; Fwd Packet Length Std; Bwd Packet Length Max; Bwd Packet Length Min; Bwd Packet Length Mean; Bwd Packet Length Std; Flow Bytes S; Flow Packets S; Min Packet Length; Max Packet Length; Packet Length Mean; Packet Length Std; Packet Length Variance; Down Up Ratio; Avg Fwd Segment Size; Avg Bwd Segment Size; Fwd Avg Bytes Bulk; Fwd Avg Packets Bulk; Fwd Avg Bulk Rate; Bwd Avg Bytes Bulk; Bwd Avg Packets Bulk; Bwd Avg Bulk Rate; Init Win bytes forward; Init Win bytes backward; act data pkt fwd; min seg size forward; Label; L7Protocol; ProtocolName | These attributes hold all the information related to the internet flow, i.e., number of packets, volume and standard deviation among others in the forward and backward direction |
| Interarrival times (15 attributes) | Flow Duration; Flow IAT Mean; Flow IAT std; Flow IAT Max; Flow IAT Min; Fwd IAT Total; Fwd IAT Mean; Fwd IAT Std; Fwd IAT Max; Fwd IAT Min; Bwd IAT Total; Bwd IAT Mean; Bwd IAT Std; Bwd IAT Max; Bwd IAT Min | These attributes hold all the information related to the interarrival times in the forward and backward direction |
| Flag features (12 attributes) | Fwd PSH flags; Bwd PSH flags; Fwd URG flags; Bwd URG flags; FIN Flag Count; SYN Flag Count; RST Flag Count; PSH Flag Count; ACK Flag Count; URG Flag Count; CWE Flag Count; ECE Flag Count | These attributes show the information related to all the flags contained in the header of the packets, i.e., Push flags, Urgent flags, Finish flags, among others |
| Subflow descriptors (4 attributes) | Subflow Fwd Packets; Subflow Fwd Bytes; Subflow Bwd Packets; Subflow Bwd Bytes | If there were subflows, these attributes present all the information related to their number of packets per flow and volume in the forward and backward direction |

(*continued*)

**Table 1.** (*continued*)

| Groups of attributes | Attributes | Description |
|---|---|---|
| Header descriptors (5 attributes) | Fwd Header Length; Bwd Header Length; Average Packet Size; Fwd Header Length 1 | Among these attributes the information related to the header is stored |
| Flow timers (8 attributes) | Active Mean; Active Std; Active max; Active min; Idle Mean; Idle std; Idle max; Idle min | These attributes store the information related with the time each flow was active and inactive |

### 4.2 Dataset Preprocessing

This section presents all the previous procedures performed on the dataset in order to generate a classification model capable of assigning a user on a cluster based on his/her consumption behavior with machine learning algorithms. The preprocessing procedures include: the DPI processing aimed labeling each flow with their respective application and the clustering analysis aimed at identifying different clusters of users based on their consumption behavior.

**DPI Processing.** As mentioned before the dataset was gathered capturing Internet traffic on a network section from Universidad Del Cauca during six days on 2017. As can be seen in the deployment model, initially all the IP packets were captured using Wireshark a software application that was installed on a computer that was configured to replicate and capture all the traffic that came through the network section core. Such information was stored as PCAP files, obtaining six files (one per day). Later on the PCAP files were processed in two ways: First, using CICFlowmeter [21], a network traffic flow generator which has been written in Java in the University of New Brunswick, 85 statistical flow features (such as Duration, Number of packets, Number of bytes, and Length of packets, among others) were obtained resulting in a total of 16.545.768 instances.

Once CICFlowmeter processing was finished it was necessary to know which application was being used on each flow, however the information obtained with the 85 attributes was insufficient for this task. Therefore a second processing was performed on the PCAP files using ntopng a network traffic software that among many other functions allows the implementation of nDPI, a tool that allows to perform Deep Packet Inspection on the captured flows and obtain the application (Layer 7 protocol) that is being used on that Internet communication [22]. Using Ntopng 79 applications were identified on the flows and were stored on a set of six CSV files. Each instance holds the information of source IP address, source port, destination IP address, destination port and layer 7 protocol of each flow. Then a java application was developed in order to label the 16.545.768 flows with their respective application. On this application a comparison using the network tuple (source and destination IP addresses and ports) was implemented i.e., an instance from the files obtained with CICFlowmeter was compared with all the instances from the files generated with Ntopng. When a match was found two more attributes were added to the file: the layer 7 protocol code (a number between 0 and 226 delivered by Ntopng) and the protocol name (Facebook, Google, etc.). Hence the first version of the dataset holding 87 attributes was obtained with all the flow statistics and their respective application. Then it was noticed that 4 application labels (Unknown, Flow_Not_Found, SSL, and SSL_No_Cert) were not useful since those flows contained network control information (communications between routers and switches) or were flows with encrypted information, hence the application could not be identified, therefore such flows were removed creating the second version of the dataset with 3.577.296 instances and 75 application class labels.

**Clustering Analysis.** After the second version of the dataset was obtained a clustering analysis was performed with the objective of identifying groups that gathered users with similar consumption behavior. As a first attempt a SOM (Self Organized Map) of a sample (3731 instances) of the second version of the dataset was created, following the clustering process presented in [23]. Considering the size of the sample an 18x17 SOM was created following the standard recommendation $5\sqrt{N}$ [24], where N is the number of instances and the result of this operation is the number of nodes of the SOM (306 nodes). With this the U-Matrix, a graph that can be used to identify the clusters within the SOM map, is obtained allowing to observe the distance between each node and its neighbors. By analyzing the U-Matrix it can be seen that there is only one cluster within the dataset with some anomalies. Furthermore, clustering IP flows can provoke that flows of the same user are assigned to different clusters. Besides this version of the dataset holds IP flows generated not only by users but by network devices as well (routers and switches). Therefore and following the dataset used in [23] it is necessary to create a new dataset that can guarantee that all the flows are from user devices and that it summarizes the consumption behavior of each user.

With this in mind a third dataset (Users groups Dataset) is created taking all the flows from a range of IP addresses (192.168.0.0 to 192.168.255.255) that are known to be user devices only. As a result, a set of 1581 users (an instance represents a user) is created focusing on the information of 29 popular OTT applications. The dataset holds 130 attributes which include user IP address, total of IP flows generated per application, mean flow duration per application, average packet size on the flows per application and average bytes per second per application. Subsequently a clustering analysis is performed on the dataset using the average silhouette approach which measures the quality of a clustering by determining how well each instance lies within its assigned cluster. The average silhouette width varies between −1 and 1 and a high value indicates a good clustering. The test is performed varying the number of clusters between 2 and 20 and using a KMeans algorithm. The best number obtained for the clustering of the dataset is between 2 and 3 clusters. Considering that the difference is small, 3 clusters are selected as the number of groups for the dataset. After this conclusion, the clustering is implemented with WEKA using a KMeans algorithm with $K = 3$. With this process, a class label attribute is added to the dataset resulting in 131 attributes.

The Fig. 1(a), (b) and (c) illustrates the number of flows per application. It can be observed that the most used applications are Browsing and Google followed by YouTube, Gmail, Facebook, Yahoo and Twitter. Furthermore, after analyzing the distribution of the clusters it can be observed that although mostly all the users access the same applications, they vary in the intensity of their consumption. The users of

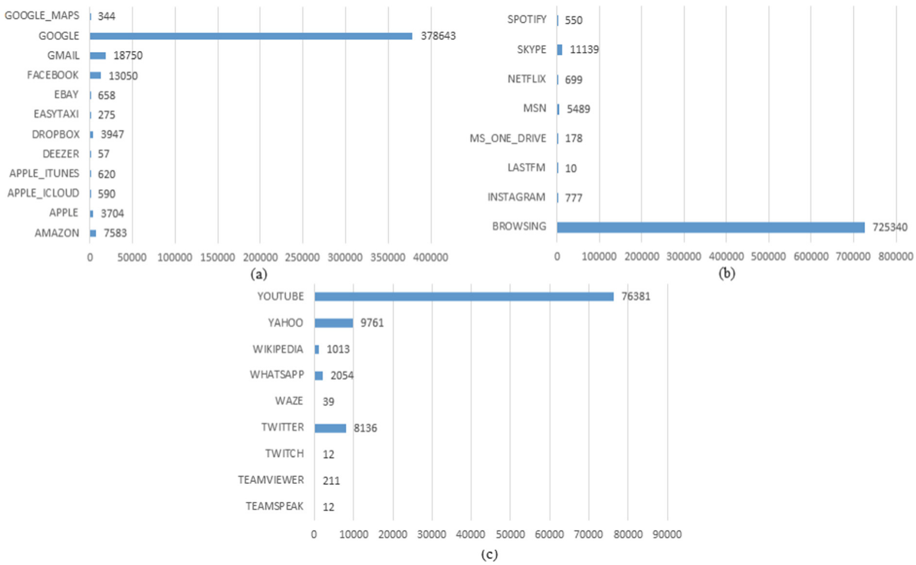

**Fig. 1.** Flows per application divided in three graphs (a), (b) and (c).

cluster 1 consume the higher number of applications (14 applications) for the longest time: Amazon, Apple, Browsing, Dropbox, Facebook, Gmail, Google, MSN, Skype, Twitter, Whatsapp, Wikipedia, Yahoo and YouTube; the users of clusters 2 consume 13 applications for a slightly minor time than cluster 1 and the consumed applications are: Amazon, Apple, Browsing, Dropbox, Ebay, Facebook, Gmail, Google, MSN, Skype, Twiitter, Yahoo, YouTube; Finally cluster 3 contains the users that exhibit the behavior with the least consumption intensity in time and quantity of applications, consuming 5 applications: Amazon, Browsing, Facebook, Google and YouTube. Considering the previous statements cluster 1 was defined as the High consumption users, cluster 2 as the medium consumption users and cluster 3 as the low consumption users. The Fig. 2, divided in (a), (b) and (c), illustrates the average generated flows by application on each cluster.

With the previous clustering analysis, it is possible to proceed with the construction of a classification model and with the proposal of personalized service degradation policies for each cluster which are described on following sections.

### 4.3 Classification Modeling

This section describes the tests performed with 8 machine learning algorithms on the Users Groups Dataset using WEKA in order to obtain the best classification model capable of assigning a user to one of the identified clusters based on the consumption behavior. The tested algorithms are: Random Forest, Boosting with J48, Bagging with J48, Support Vector Machines with LibSVM and SMO (Sequential minimal optimization) algorithms, J48, KNN and Naive Bayes. All the algorithms are evaluated through a corrected T test, the Support Vector Machines are tested with different kernel

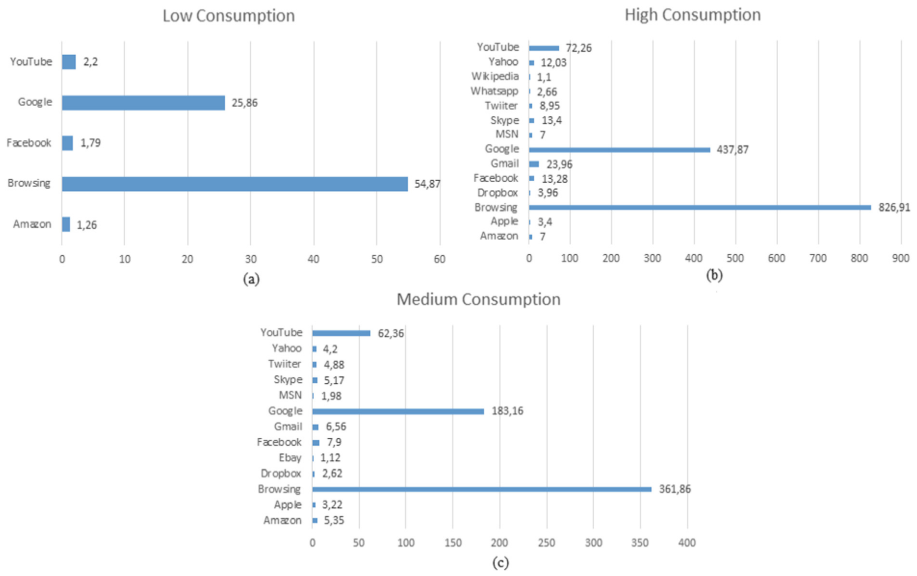

**Fig. 2.** Average flows generated by application on each cluster. (a) Low consumption; (b) High consumption and (c) Medium consumption.

functions (linear, polynomial and RBF) obtaining the best results for the linear function and the number of neighbors for KNN are optimized to 23 by WEKA. Table 2 illustrates the results of the corrected T test in terms of precision, recall, true positive rate, false positive rate and the F measure. The tests were conducted using a 10 fold cross validation and a significance level of 0.05. It can be seen in the results that the best classifier is the SMO Support Vector Machine trained with a linear kernel function, however considering the high recall and precision of most of the algorithms, except for Naïve Bayes, it is possible to conclude that any of the tested algorithms would allow to create a good classification model for the Users Group Dataset.

**Table 2.** Classification tests results.

| Algorithms | Precision (%) | Recall (%) | TP rate (%) | FP rate (%) | F measure (%) |
|---|---|---|---|---|---|
| Random forest | 90.8 | 90.7 | 90.7 | 5.2 | 90.5 |
| Boosting with J48 | 94.3 | 94.1 | 94.1 | 2.9 | 94.1 |
| Bagging with J48 | 93.6 | 93.5 | 93.5 | 3.2 | 93.6 |
| LibSVM - linear kernel | 93.7 | 93.7 | 93.7 | 3.2 | 93.7 |
| SMO - linear kernel | 98 | 98 | 98 | 1.1 | 98 |
| J48 | 91.8 | 91.8 | 91.8 | 4 | 91.8 |
| KNN with K = 23 | 94.8 | 94.8 | 94.8 | 2.6 | 94.7 |
| Naive Bayes | 72.6 | 69.6 | 69.6 | 14.1 | 70.1 |

## 5 Service Degradation Policies

In this section the personalized service degradation policies for each cluster are proposed. It is important to mention that the structure of the policies are based on the PCC (Policy and Charging Control) architecture of an LTE network proposed by the ETSI in [5]. Precisely the element that is proposed is a PCC rule which is divided in predefined or dynamic rules as explained in the specification. However considering the context of the service degradation it is only logical that the proposed PCC rules must be dynamic since these type are triggered by the occurrence of an event, that will be the case when a user exceeds his/her consumption limit. The elements in a PCC rule are (Table 3):

**Table 3.** Elements of a PCC rule.

| Element | Definition |
|---|---|
| Policy rule name | Is the name given to the PCC rule in order to be easily identified |
| SDF template | This is the packet filter pre-configured by network operators in accordance with their policy, and each of them typically consists of 5-tuple (Source IP address, Destination IP address, Source port number, Destination port number, and Protocol ID). The Protocol ID is checked with DPI |
| SDF GBR (Guaranteed Bit Rate) | This parameter is used for a GBR type bearer, and indicates the bit rate to be guaranteed by the LTE network. It is not applied to a non-GBR bearer with no guaranteed bandwidth and it must be defined in the upload and download link |
| SDF MBR (Maximum Bit Rate) | This parameter indicates the maximum bit rate allowed in the LTE network. Any packets arriving at the bearer after the specified MBR is exceeded will be discarded |
| QCI (QoS Class Identifier) | It's an integer from 1 to 9 that indicates nine different QoS performance characteristics of each IP packet. QCI values are standardized to reference specific QoS characteristics, and each QCI contains standardized performance characteristics (values), such as resource type (GBR or non-GBR), priority ($1 \sim 9$), Packet Delay Budget (allowed packet delay shown in values ranging from 50 ms to 300 ms), Packet Error Loss Rate (allowed packet loss shown in values from $10^{-2}$ to $10^{-6}$ |
| ARP (Allocation and Retention Priority) | At times of network congestion, the ARP value of a subscriber's bearer will determine whether or not it can replace an existing bearer that has a lower ARP precedence by a new bearer with a higher ARP. It is an integer ranging from 1 to 15, with 1 being the highest level of priority |
| SDF gating status | This parameter defines the gating status for the LTE bearer i.e., if a bearer is permitted to pass through (open) or if it is blocked (closed) |
| SDF charging | This parameter indicates if the charging policies associated to the user equipment is online or offline |

By analyzing the structure of a PCC rule there are only two possibilities for the service degradation policy: degrade the service by affecting the bit rate associated to the SDF (Service Data Flow) or block the service by modifying the gating control parameter since the GBR and ARP are established in the specification by the QCI. Therefore Table 4 illustrates how is recommended to perform the service degradation for each cluster considering the 15 most used applications observed in the consumption behavior.

For the Low Consumption group only the most used applications are still functional with their bit rate degraded. For the Medium Consumption group, the 5 most used applications are still functional and the rest are blocked. Finally, for the High Consumption group the 8 most used applications are degraded in the bit rate and the others are blocked. This way the network administrator can save network resources and the degradation process is performed considering the behavior of the users.

As an example, Table 5 illustrates the structure of two PCC rules: The first for Browsing where the bit rate is degraded, considering the speeds that can be offered in a LTE network, and the second for YouTube were all the flows from this application are blocked. The SDF template is defined for the same user and it is worth mentioning that the asterisk means any port or IP address. With this it can be concluded that a set of personalized service degradation policies can be defined for the users on each cluster taking into consideration their consumption behavior.

**Table 4.** Policies recommendation.

| Applications \Clusters | Low consumption | | Medium consumption | | High consumption | |
|---|---|---|---|---|---|---|
| | Degrade service | Block service | Degrade service | Block service | Degrade service | Block service |
| Amazon | | X | | X | | X |
| Apple | | X | | X | | X |
| Browsing | X | | X | | X | |
| Dropbox | | X | | X | | X |
| Ebay | | X | | X | | X |
| Facebook | | X | X | | X | |
| Gmail | | X | X | | X | |
| Google | X | | X | | X | |
| MSN | | X | | X | | X |
| Skype | | X | | X | X | |
| Twitter | | X | | X | X | |
| Whatsapp | | X | | X | X | |
| Wikipedia | | X | | X | | X |
| Yahoo | | X | | X | | X |
| YouTube | | X | X | | X | |

**Table 5.** Policies example.

| Policy rule name | SDF template | SDF GBR | SDF MBR | SDF QCI/ARP | SDF gating status | SDF charging |
|---|---|---|---|---|---|---|
| Browsing degradation | UL:(192.168.10.24, *,*,*, HTTP)<br>DL:(*, 192.168.10.24,*,*, HTTP) | N.A. | UL: 2Mbps<br>DL: 2Mbps | QCI = 9<br>ARP = 9 | Open (permit) | Online |
| YouTube degradation | UL:(192.168.10.24,*,*,*, YouTube) DL:(*,192.168.10.24, *,*,YouTube) | N.A. | UL:Unlimited<br>DL:Unlimited | QCI = 8<br>ARP = 8 | Closed (not permitted) | Online |

## 6 Conclusions and Future Works

This paper presented the description of the creation, preprocessing procedures and classification modeling implemented on a dataset of IP flows generated on a network section from Universidad Del Cauca during six days of 2017, aimed at the analysis of the consumption behavior of users in order to propose a set of personalized service degradation policies that benefit the network operators but take into consideration the users behavior. From the preprocessing procedures it can be concluded that although there are software applications such as CICFlowmeter that allow to obtain the flow statistics such information is not enough to identify the application that is being used on the flow. This problem was solved using DPI which enabled the identification of 79 different applications on the captured flows, however even this process presents some shortcomings since a considerable number of flows were identified as unknown and encrypted applications.

The clustering analysis showed that although a great quantity of OTT applications can be consumed by the users of a network the differences on their behavior are more related to the intensity of consumption than to the number of applications. Furthermore, the applications that were used the most were traditional browsing (HTTP) and Google service suite (search engine, Google+, Google drive, etc.) but this can be related to the fact that the captured sessions were performed on the university campus, therefore the use of social networks applications may not be very common. On the other hand, the analysis identified three different clusters of users that were defined as High Consumption, Medium Consumption and Low Consumption. These groups vary in the quantity and intensity of use of OTT applications. The classification modeling tested 8 different machine learning algorithms obtaining a good precision and recall values in 7 of them. The best algorithm was the SVM (Support Vector Machine) implemented with SMO algorithm enabling the classification of new users in one of the three clusters.

Subsequently a recommendation of a set of personalized service degradation policies were proposed for each cluster taking into consideration the consumption behavior of the users associated to each group and the structure of a PCC rule as it is defined on the ETSI specification [5]. Such recommendation validated that it is possible to consider a personalization of the service degradation procedures.

As future works it is proposed to perform a comparison between the personalized policies with current service degradation policies in terms of efficiency, defining comparison metrics clearly, in order to conclude how good the proposed policies are.

Besides it is necessary to perform a study and implementation of a mechanism that enables the enforcement and implementation of personalized service degradation policies inside a mobile network. Furthermore, the development of a simulation tool that enables the gathering of traffic data from a mobile network would facilitate the construction of future datasets. On the other hand, a mechanism that allows the analysis and classification of users in groups based on their consumption behavior inside the architecture of a mobile network would enable the personalization of the service provisioning in general.

**Acknowledgements.** The authors would like to thank Universidad Del Cauca for supporting this research and Colciencias for the PhD scholarship granted to MSc(C) Juan Sebastián Rojas.

## References

1. Wesley Clover: Over-The-Top (OTT) a dramatic makeover of global communications (2014)
2. Chetty, M., Banks, R., Brush, A.J., Donner, J., Grinter, R.: You're capped: understanding the effects of bandwidth caps on broadband use in the home. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, New York, NY, USA, pp. 3021–3030 (2012)
3. Chetty, M., Kim, H., Sundaresan, S., Burnett, S., Feamster, N., Edwards, W.K.: uCap: An Internet Data Management Tool for the Home, pp. 3093–3102 (2015)
4. Ixia: Quality of Service (QoS) and Policy Management in Mobile Data Networks (2013)
5. ETSI TS 23.203: Policy and charging control architecture, ITU. http://www.itu.int/itu-t/workprog/wp_a5_out.aspx?isn=6084. Accessed 7 Dec 2017
6. Petersen, K., Feldt, R., Mujtaba, S., Mattsson, M.: Systematic mapping studies in software engineering. In: Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering, Swinton, UK, pp. 68–77 (2008)
7. Crawley, E., Sandick, H., Nair, R., Rajagopalan, B.: A Framework for QoS-Based Routing in the Internet. https://tools.ietf.org/html/rfc2386. Accessed 29 Nov 2016
8. Lakhtaria, K.I.: Enhancing QoS and QoE in IMS enabled next generation networks. In: First International Conference on Networks and Communications, NETCOM 2009, pp. 184–189 (2009)
9. Kritikos, K., et al.: A survey on service quality description. ACM Comput. Surv. **46**(1), 1:1–1:58 (2013)
10. Quality of Service Regulation Manual. https://www.itu.int/pub/D-PREF-BB.QOS_REG01-2017. Accessed 2 Mar 2018
11. Davies, E., Carlson, M.A., Weiss, W., Black, D., Blake, S., Wang, Z.: An Architecture for Differentiated Services. https://tools.ietf.org/html/rfc2475. Accessed 29 Nov 2016
12. Gomes, J.V., Inácio, P.R.M., Pereira, M., Freire, M.M., Monteiro, P.P.: Detection and classification of peer-to-peer traffic: a survey. ACM Comput. Surv. **45**(3), 30:1–30:40 (2013)
13. Agababov, V., et al.: Flywheel: Google's Data Compression Proxy for the Mobile Web (2015)
14. Williams, N., Zander, S., Armitage, G.: A preliminary performance comparison of five machine learning algorithms for practical IP traffic flow classification. SIGCOMM Comput. Commun. Rev. **36**(5), 5–16 (2006)

15. Yang, J., Qiao, Y., Zhang, X., He, H., Liu, F., Cheng, G.: Characterizing user behavior in mobile internet. IEEE Trans. Emerg. Top. Comput. **3**(1), 95–106 (2015)
16. Bertin, E., Crespi, N., L'Hostis, M.: A few myths about telco and OTT models. In: 2011 15th International Conference on Intelligence in Next Generation Networks, pp. 6–10 (2011)
17. Qiao, X., Xue, S., Chen, J., Fensel, A.: A lightweight convergent personal mobile service delivery approach based on phone book. Int. J. Commun. Syst. **28**(1), 49–70 (2015)
18. Mahola, U., Erasmus, L.: Emerging revenue model structure for mobile industry: the case for traditional and OTT service providers in Sub-Sahara. In: 2015 Portland International Conference on Management of Engineering and Technology (PICMET), pp. 1485–1494 (2015)
19. Kibilda, J., Malandrino, F., DaSilva, L.A.: Incentives for infrastructure deployment by over-the-top service providers in a mobile network: a cooperative game theory model. In: 2016 IEEE International Conference on Communications (ICC), pp. 1–6 (2016)
20. Dataset Unicauca - 2018 - Google Drive. https://drive.google.com/drive/folders/1FcnKUlSqRb4q5PkGfAGHz-g7bVKL8jmu?usp=sharing
21. Flowmeter | Datasets | Research | Canadian Institute for Cybersecurity | UNB. http://www.unb.ca/cic/datasets/flowmeter.html. Accessed 30 Nov 2017
22. ntopng: ntop, 4 August 2011
23. Ghnemat, R., Jaser, E.: Classification of mobile customers behavior and usage patterns using self-organizing neural networks. Int. J. Interact. Mob. Technol. IJIM **9**(4), 4–11 (2015)
24. Vesanto, J., Alhoniemi, E.: Clustering of the self-organizing map. IEEE Trans. Neural Netw. **11**(3), 586–600 (2000)