Traffic Classification – Packet-, Flow-, and Application-based Approaches

Sasan Adibi

ECE Department, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada

***Abstract* — Traffic classification is a very important mathematical and statistical tool in communications and computer networking, which is used to find average and statistical information of the traffic passing through certain pipe or hub. The results achieved from a proper deployment of a traffic analysis method provide valuable insights, including: how busy a link is, the average end-to-end delays, and the average packet size. These valuable information bits will help engineers to design robust networks, avoid possible congestions, and foresee future growth.**

This paper is designed to capture the essence of traffic classification methods and consider them in packet-, flow-, and application-based contexts.

***Keywords* — Traffic Classification, Packet, Flow, Applications, Delay, Payload Size.**

I. INTRODUCTION

Traffic classification techniques are used to categorize traffic flows into tangible selections. These selections may be in two major forms; packet information (e.g., packet size, flow duration, etc) and packet representing the application in use.

There are numerous selections of packet classifications, which are based on how they are observed and analyzed. An observation can be at the packet level, including the consideration of; packet size, duration, burstiness and patterns of transmission. Another observation is to consider the context of which the packets are used in. This can include the application by which the packets are created for, performance measures, and different underlying protocols stacks in use. These will be discussed in later sections.

The management of this paper is as followed: Section II will discuss traffic classification parameters. Sections III and IV are dedicated to flow-based and Quality of Service (QoS)-application-specific traffic classifications respectively, followed by conclusion and references.

A. Traffic analysis in the literature

In the traffic classification literature, the classical method of identifying flows is based on various parameters observations, such as IP addresses, ports, etc. Reference [1] proposes a method for relying on the first five TCP packets observation to identify the application in use. The proposed classification technique works around two phases: an online traffic classification phase and an offline learning phase. The learning phase uses the training data, which checks the TCP flows to extract common behaviors. The traffic classification phase is used to extract the applications running above the TCP layer.

BLINC [2] discusses a new approach in traffic classification where applications and devices hosting the applications are associated. BLINC considers flow activities of hosts instead of considering every individual TCP/UDP flows. The limitation about BLINC is that it is capable of analyzing the statistics only after the connection is terminated. Therefore BLINC is incapable of analyzing the flows on the fly.

Reference [3] presents a framework for traffic classification while packet payload is present. The scheme utilizes several building blocks that are used to create sufficient confidence for application identity. This is done by collecting packets with payloads on the Internet backbone and sorting the TCP/UDP flows based on their port numbers. The results show that a classification based on simple port numbers will provide approximately 70% accuracy for the traffic classification.

Reference [4] is based on NBAR (Network-Based Application Recognition), which is counted as a traffic classification based on Internet applications (e.g., web-based), TCP/UDP port assignments, and other difficult-to-classify applications.

A few studies [5,6] have shown that there are orthogonal correlations between four main traffic classification dimensions; rate, duration, burstiness, and size. These correlations are more accurate for heavy-hitters (e.g., long lasting connections), which contain DNS (Domain Name System) traffic.

Reference [7] presents a security-based application classification technology called App-ID, which operates by establishing application sessions. App-ID identifies different traffic using one of the following approaches: a). Protocol and Port Numbers, b). SSL (Secure Socket Layer) Decryption, c). Application Decoders, and d). Application Signatures.

In the study of traffic classifications, Peer-to-Peer (P2P) networks are also important to consider where

both TCP and UDP on top of IPv4 are used to convey file sharing data between individual users [8,9,10,11]. Reference [8] emphasizes on two main issues, first is P2P applications have matured over the past few years and their usage will be on the rise. The other issue mentioned is that since P2P applications use non-standard and random port numbers, the conventional flow classification techniques are not adequate for proper classifications. Reference [9] demonstrates the accuracy, feasibility and robustness of high speed P2P application signature-based traffic. It discusses a number of P2P application protocols, such as eDonkey, BitTorrent, DirectConnet, Gnutella, and Kazaa protocols. The measurements show that using application-level signature technique, less than 5% false position/negative ratios can be achieved.

A few studies [10,11] offer comparative approaches for studying P2P traffic behaviors. Reference [11] offers three such approaches for P2P application classifications; port-based, application-layer signature, and transport-layer longitudinal approaches using empirical network traces over a two-year period. The results show that classic port-based analysis is not accurate, which is inline with the results achieved in reference [8]. Application-layer signature approach, on the other hand, yield more accurate results, agreeing on the results achieved in reference [9].

Reference [12] uses Naïve Bayesian estimator for Internet traffic classification analysis. With fine-tuning this estimator's variants, the results show 65% accuracy on per-flow traffic classification. The accuracy was increased to 95% when data from the same period was analyzed in addition to the usage of techniques, such as Bayes based kernel-estimator was combined with FCBF (Fast Correlation-Based Filter).

Reference [13] uses a supervised Naïve Bayesian estimator algorithm, which features building statistical models, which described the classes based on training data (machine learned classification). The results show an accuracy of better than 83 % on both per-byte and per-packet classifications.

Reference [14] provides an accuracy of 82-100% based on an empirical evaluation technique, which models both host-specific- and aggregate-protocol behaviors. Such an accurate classification is independent of port label, which opposes the traditional classification methods.

If certain traffic attributes are not considered effectively, the performance of a traffic classifier can be greatly affected. An example of such traffic attributes include flow sizes (mice/elephant), which will contribute to degradation of traffic classification accuracy. [15]. Another attribute is the QoS measures and identifiers, which requires CoS (Class of Service) measurement classifications [16].

Certain protocols have certain attributes, which can be measured for traffic classifications. One series of protocols that are often noticed on the Internet backbone are routing protocols. There are two types of routing protocols; internetwork and intranetwork routing protocols. Internetwork (aka Internet Autonomic System "AS") routing schemes operate on larger scales, such as BGP (Border Gateway Protocol), whereas interanetwork routing schemes work inside one network's boundaries, such as OSPF (Open Shortest Path First). It is obvious that only internetworking routing schemes are observed on the Internet backbone. Flow classifications based on classifying BGP level prefix flows are one example of routing traffic classifications [17,18]. Reference [17] uses a method based on Dirichlet Mixture Processes, modeling flow histograms with a capability of examining macroscopic flows while distinguishing between various classes of traffic.

An empirical approach to Inter-AS traffic classification [18,19] includes extensive Internet-wide measurements and classifying and ranking them into individual ASs based on the utilities they derive (e.g., residential, business). The scatterplots show that there are correlations between various pairs of utilities.

Machine Learning (ML) methods have also been widely used in traffic classification [20,21], where traffic clusters are created based of various traffic characteristic. Early ML techniques mostly relied on offline and static analysis of traffic batch traces. However recent work is mostly towards real-time ML-based IP traffic classifications.

Traffic classifications with various security measures in mind; have been considered in various literatures [22,23,24]. It is shown [22] that it is possible to classify and categorize Internet traffic flows without proper content analysis. Using statistical signatures, it is possible to classify services even when they are running on non-conventional port numbers [23]. Reference [24] argues that the application of SSL is on the rise and characterization of SSL and a method, which recognizes applications running on encrypted SSL connections based on the first packet size, provide an accurate traffic classification technique with more than 85% accuracy.

Many of the parameters used in the traffic classifications study, exist at the network layer. Therefore several studies [25,26] included deeper attention on the IP protocol, which operates at the network layer in the TCP/IP suite.

II. Traffic Classification Parameters

In this section we introduce a number of network traffic parameters. These parameters are mostly considered in the study of packet and traffic classification techniques.

A. Packet Size

Packet size is one form of traffic classification. Most of the traffic volumes on the Internet can be categorized into either very small (mouse) packets or very large (elephant or heavy tailed) packet sizes. The large packet size is usually associated with higher link usage. Basically 20% of the connections on the Internet are responsible for 80% of the traffic [27,28,29], mostly containing elephant packets.

Zipf's law is a more generalized form of this context. In the packet size scenario, Zipf's law characterizes the frequency of occurrence of certain packet sizes as a function of its rank in the frequency table [30]. This means that there exists an imbalance in the network due to the fact that 20% of the connections carry 80% of the traffic and the rest of the 80% of the connections are for small packet traffic.

Traffic Engineering (TE) [31] is a term applied to a systematic process in which traffic flows are arranged in "classified" groups to simplify their transmission throughout networks and decrease the chance of congestions. TE, by nature, is well positioned to deal with very large volumes through the aggregation of traffics. However TE tends not to perform as efficiently when dealing with mice flows. The drawback of TE in regards to traffic classification is the fact that traffic in a large and random environment (e.g., the Internet) would exhibit volatility in several flow specifications, namely; volume and bandwidth [31]. Fluctuations in these network parameters reduce the efficiency of TE in the process of traffic classifications.

In many cases, flows exhibit inherent bandwidth fluctuations. As mentioned, this creates complications in the traffic classification criteria, leading to frequent reclassification, thus reduction in the classification performance. These fluctuations are due to the following factors [31]:

Connection termination following the link exhaustion - The duration of a connection can be modeled as a stochastic variable dependant on the following parameters [32,33]: The protocol in use, the current (kth) connection arrival time, the current connection (kth) time duration, and client/server performance metrics (e.g., round-trip delay, client delay, server delay, etc) for client/server based applications such as FTP.

The effect of these parameters contributes to the creation of a median time for the flow. This median time for elephant flows (aka heavy-hitters) will be higher since according to reference [34], the longer the connection duration (heavy-hitters), the higher the probability for the link to continue its connection.

Burstiness Effect - Multimedia traffic, especially video data, can be affected by the burstiness of traffic flows, reflected by a number of parameters, such as [34]: Peak-to-average ratio (PAR) and the temporal auto-covariance function (ACF).

Burstiness is a time sensitive parameter and probability-wise, burstiness is more probable to be an issue in heavy-hitter connections compared to mouse flows.

Bandwidth Fluctuations - Bandwidth fluctuations occur relatively frequently in wireless networks compared to wired networks. In wired networks, bandwidth fluctuations may happen due to various reasons, such as, a sudden increase of user demands or a congestion period.

Reasons behind bandwidth fluctuations in wireless networks, mostly related to PHY and MAC layers, include: handoff and handover between Access Points (APs), limitations of available bandwidth in multi-user environments, physical limitations (e.g., reflections, refractions, multipath, etc), vulnerability to various interferences, and dependency of performance to the distance of the client (wireless user) to the server (AP).

A.1 Heavy Hitters (Elephants) versus Mice packets

Heavy hitters can be identified by both their large packet sizes and long duration connections. It has been presented in the literature [35,36] that there's a strong correlation between the rate of a stream and its packet sizes mainly based on the protocol in use.

In wired connections, from a packet size point of view, packets are usually between a few tens of bytes up to 1514 bytes. Depending on the Maximum Transmission Unit (MTU), large files being transmitted are usually broken down into various fragments. Based on captured real traffic, we notice that control packets (packets containing control commands), which do not usually have any data payloads, are less than 200 bytes. Data packets are usually above 200 bytes. Heavy hitter packets, according to the data we have gathered, from packet size point of view, are packets with payloads of 300 to 1514 bytes.

Wireless traffic starts from 14 bytes (e.g., ACKs, CTS, etc) with no data payloads, up to 1530 bytes, which is a limit by which fragmentation occurs. Based on our real traffic analysis, we label packets with over 400 bytes in lengths as heavy hitters.

B. Duration

Duration of packet streams is another form of packet classification. Depending on the application, a short lived packet can last from a few milliseconds up to a few minutes. Long-lived packets, on the other hand, can last from a few minutes up to several hours. Statistics [35,36] show that there are direct links between larger packet sizes and longer durations. Based on captured real traffic from multimedia-rich connections, most control packets,

such as beacons, ACKs, CTSs, etc, are light connections (tortoises) and other packets forming connections (connection requests, confirmations, data transmission, acknowledgement transmission, teardowns, etc), are considered heavy hitters (dragonflies).

C. Confidence Interval (CI)

CI is a population-related parameter, which is an interval estimator [38,43,46]. Confidence intervals are used give an estimate on how reliable a sample is. For an extreme diverse sample space, such as the traffic patterns on the Internet backbone, either one has to monitor the lines for a long period of time (e.g., months or years) and then run traffic classification techniques over the saved traces, or use small sample space with an aid of a confidence interval estimator. A confidence interval of higher than 95% is a relatively good estimation. Bayesian and Gaussian interval estimations are examples, by which confidence intervals can be estimated.

III. Flow-based Traffic Classification

A flow is defined as a unidirectional series of IP packets with unique source/destination addresses, port numbers (assuming TCP or UDP to be the transport layer protocol) and protocol number [40,41,42].

The main focus of this section is to discuss application specific classes of traffic. However it is important to talk about a few basic and fundamental definitions first.

Four main parameters associated to every flow are: size, duration, rate, and burstiness. Correlation between size and rate is protocol-based. In regards to small/medium flow sizes, due to different timeout mechanisms, the strong correlation between size and rate is more likely a pervasive artifact. Such an argument might require the use of a larger packet size or the deployment of a larger initial window to improve TCP performance. This will increase the chance that more data is sent in one round trip time "RTT" before the timeout occurs. There is a strong correlation among flow size and rate. Size can be chosen based on bandwidth availability [42].

A. Flow-Level Metrics

Reference [40] classifies flows according to their *sizes, durations,* and *inter-arrival times*. These are defined as followed [40]:

A.1 Flow Size

Flow size is the total number of bytes transferred between a server and a wireless client during a connection. From the client point of view, it does not matter if a new server giving service (handover happens with a new IP address) while the connection is still ongoing. However this measurement is usually done per server/client pair [42,43,45,46].

Mice Flows - Mice flows are those with relatively low sizes transmitting for a short duration. The duration limit is less than the time required for the accumulation of 10 KB data and the packet sizes are usually less than 500 Bytes each.

P *Elephant Flows* - Elephant flows on the other hand are flows, which usually last more than an hour carrying relatively large packet sizes (often larger than 1 KB each). Therefore for a typically elephant flow (on average) more than 3 MB of data is accumulated compared to 10 KB in the mice flow case.

Peer-to-Peer (P2P) networking has gained much popularity in the recent years. The statistical flows for both P2P and Internet have been well modeled and bounded between Pareto and Weibull distributions [40] and their probability density functions (pdf) can be derived from the following two Equations (f_{WEB} and f_{P2P}):

$$f_{WEB}(S) = \begin{cases} 0.26S^{-0.62}e^{-\left(\frac{S}{2.7}\right)^{0.38}} & : S \le 30KB \\ \frac{3.33}{S^{2.05}} & : 30KB \le S \le 5MB \\ \frac{600466}{S^{3.35}} & : S \ge 5MB \end{cases}$$

$$f_{P2P}(S) = \begin{cases} 0.63S^{-0.19}e^{-\left(\frac{S}{1.36}\right)^{0.81}} & : S \le 4KB \\ \frac{0.0548}{S^{0.35}} & : 4KB \le S \le 10MB \\ \frac{7034}{S^{2.42}} & : S \ge 10MB \end{cases}$$

Fig. 1 shows the comparison between web and P2P distribution functions across the 4 kB flow size space.

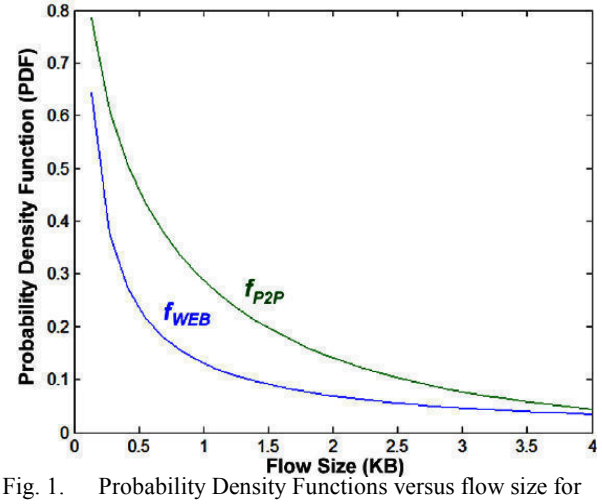

Fig. 1. Probability Density Functions versus flow size for WEB versus P2P activities

The distribution for the web-flow size includes a long-tailed distribution. A probability distribution is called long-tailed (aka heavy-tailed) when high probability regions are far from the median or mean.

A.2 Inter-Arrival Time between Flows

This is the time between any two consecutive flow arrivals. Inter-arrival times in flows are practically independent from each other and are distributed exponentially according to Poisson process. IP traffic on top of TCP and UDP, also has uncorrelated inter-arrival flow times (also true in regards to the flow lengths), therefore it can be modeled by a combination of algorithmic scaled normal distributions [47].

A.3 Flow Duration

This is calculated from the start of the initial handshake of the flow until the last data packet and tear-down of the link related to the flow. At this level we also have mice flow and elephant flow concepts.

To quantify these two concepts, Internet traffic measurements have shown that 80% of total traffic on the backbone is caused by 20% of the traffic flows with relatively long flow durations.

In the Flow Size section a simple math was carried out to calculate a time range for both mouse and elephant flows. According to the definition a typical mouse flow can be as short as a few micro-seconds (based on current 802.11 bandwidth limit of 54 Mbps) up to several minutes. A typical elephant flow lasts from an hour to several days and could transmit up to several thousand terabits of data in a single flow.

A.4 Flow Fluctuation Patterns

In general, one can categorize flow fluctuation patterns as: *Slowly varying continuous data flow, a fast varying continuous data flow, traffic with common periodic trends, short-lived bursts,* and *noise*.

Slowly varying continuous data flows are long-lived connections generated from a steady source with relatively high correlation among successive data. Therefore, only small variations are observed in a short period of time. An example would be the data transmitted from thermal sensors.

Fast varying data flows are long-lived flows where the volume of data generates fluctuates rapidly over a relatively short period of time. In these types of flows, high variations are observed with low correlation indexes among successive data. An example of this would be data transmission across a busy LAN.

Common periodic trends are long-lived traffic patterns which are observed to be periodic in nature, such as web server traffic and scheduled backup data.

Short-lived bursts are also part of most data network traffic. As mentioned before, a long established busy LAN connection may exhibit fast varying data flow, however over a short period of time, such a connection may include short-lived bursts resulting from rapidly fluctuating traffic levels. A burst can be characterized as a fluctuating data stream over a relatively short period of time.

Background noise is an inevitable part of any network traffic. A high SNR (Signal-to-Noise Ration) value ensures relatively high level of signal and low level of noise.

The network traffic categories mentioned can be applied to almost all aggregated network traffic. Thus, proper analysis of these flow types is of great importance.

B. Traffic Control

Depending on the nature of the flows, either majority being mice, elephant, or a combination of both, network will deal with various conditions differently. For instance if the majority of the flows are mice and the network has undergone congestion periods, dropping packets will do little in dealing with congestion control. In general, such a network will pose random behavior with high adaptability to sudden changes, which can be a favorable issue for time-sensitive applications. Telnet and HTTP transfer streams tend to be of mice flow type [41].

For a network where majority of the flows are elephant, depending on the protocol in use, it can be tolerant against congestion, in particular if the majority of the traffic is based on TCP, as TCP features a built in congestion avoidance mechanism. TCP (FTP applications) and UDP (video applications) flows are examples of elephant flows [41].

Flow duration increase may increase the Long Range Dependence (LRD) (aka long memory, measured by Hurst parameter) as well. LRD is an autocorrelation value of a data stream, which approaches a constant value (normalized to 1) as the number of data bits increases. If the limit in equation 3.1 exists for a real number of r, then α (s) is the autocorrelation function and X_t is the LRD stationary process (Fig. 2 [adapted from [48], Equation 3).

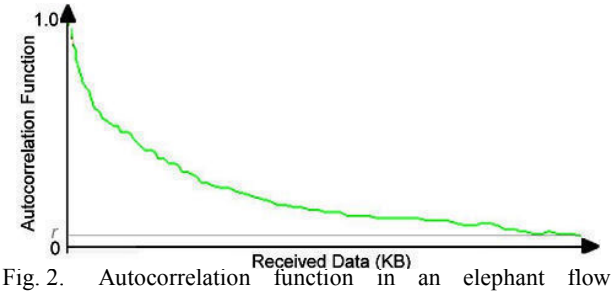

Fig. 2. Autocorrelation function in an elephant flow merging to the value r

Thus for a typical elephant flow, equation 1 should hold. The following definitions are related to LRD:

Hurst parameter - is an indicator parameter, which increases when traffic volume and burstiness increase.

Self similarity - is a statistical property, fractal-like, to examine produced data for similar patterns over a scale of time. A few of its properties are: slow decaying variance, long-range dependence, and Hurst effect.

IV. QoS-Application-Specific Traffic Classification

The purpose of this section is to study traffic classifications from different QoS requirement perspectives. These types of classifications can be layered-based, such as: application, network, and lower layers (MAC and PHY), which makes it a fairly complex task to configure. Therefore in this section we try to break down different aspects of QoS from traffic classification point of views and discuss the details for each part.

A. QoS Traffic Classes

QoS is an essential part of a non-best-effort traffic classification, which is important to ensure priority data, in particular; multimedia applications running on stringent wireless links are handled with proper priority in a timely manner (upper limits on delay values). These multimedia applications (data containing both audio and video), based on the delay tolerability, can be grouped in the following categories [49,50]:

Streaming - Clients request audio/video files from servers and pipeline reception over the network and display. Streaming data can be interactive, that is the user can control some operations (e.g., pause, resume, fast forward, rewind, etc.).

Unidirectional Real-Time (Half-Duplex): Functioning similar to existing TV and radio devices (e.g., mobile-TV), however data delivery direction is from the network to the device. It is a non-interactive service, only listen and/or view.

Interactive Real-Time (Full-Duplex) - Two-way traffic, similar to a phone conversation and videoconferencing (e.g.., talking/listening broadcasting/ viewing at the same time). This class has a more stringent delay requirement compared to real-time streaming and unidirectional, requires normally less than 150 msec of delay for both audio and video applications (in each direction).

B. Wireless QoS Requirements

QoS in general falls into two categories; user perspective (application interaction) and network perspective. Application perspective QoS refers to the quality of the high-level applications as perceived by the user, including multimedia (e.g., video, audio, streaming, text, file transfer, etc) presentation subjective quality. We already discussed delay, bandwidth, round-trip (end-to-end) delay, and jitter as part of the QoS-related parameters. Other user perspective parameters in regards to QoS include:

Connection Drop – When the delay or jitter figures increase passed certain limits, the link quality either becomes unbearable to the user or the underlying application drops the connection, causing a link failure. In either case, it will affect the user profoundly.

Depending on the application in use (e.g., audio, video, voice messaging, audio streaming, etc), the requirements for the subjective QoS (user perception) figures may change. For instance, if the end-to-end audio delay becomes more than 150 msec, the user level of discomfort starts to increase dramatically.

In regards to network perspective QoS, the QoS-related parameters for multimedia applications include: Bandwidth or Throughput, Round-Trip Time (RTT), End-to-End Delay (E2ED), Bite error rate (BER), Packet Loss Ratio (PLR), Packet drop ratio (PDR), and Jitter [51,52,53,54]. A few of these parameters were introduced earlier in this section and the rest are defined as followed:

Bit Error Rate – BER is the measure of the number of errors bit-wise; 1 is sent, however 0 is received, or 0 is sent and 1 is received. Channel conditions contribute to the value of BER, so when noise and/or interference levels rise, BER value rises too.

Packet Loss Ratio – PLR is a parameter that represents the ratio of the number of lost packets to the total number of packets sent. The performance of the link and the intermediate nodes has direct impacts on PLR. The higher the PLR value, the less efficient the communication path between the source and the receiver is.

Packet Drop Ratio – PDR is a performance measure that is mostly affected by the receiver's input buffer. When the input buffer starts to get full, a mechanism starts discarding (dropping) the packets. The lower the PDR value, the better the quality of these buffers.

B.1 Bandwidth Requirements

Based on the multimedia application in use, bandwidth constraints are different. Table I (adapted from [52,59,60,61]) shows bandwidth requirements for various MPEG formats (combination of video and audio).

B.2 Voice over IP (VoIP) Bandwidth Requirements

Voice over IP is an important multimedia application, which has become a dominant engine of transporting voice across IP networks (Internet).

TABLE I
DIFFERENT DATA RATES FOR DIFFERENT VIDEO APPLICATIONS

Algorithm	Format	Format Specific Properties	Data Rate (kbps)
DPCM	H.120	625-line-50 field, 525-line-60 field	1544 (NTSC) 2048 (PAL)
DPCM, DCT, MC	H.261	88x72, 176x144, 352x288, 704x576 Comparable to MPEG-1	20, 2048
8x8 DCT, CIF, SIF	MPEG-1	352x288, 352x240, 25 fps (PAL), CBR, MPEG-1, Audio, Layer 2 VCD	32 (audio) – 1,536 (video)
8x8 DCTVLC	H.262	Similar to MPEG-2	60-2,048
8x8 DCT, CIF, SIF	MPEG-2	MPEG-1, Low (352x288), Main (720x476), SD (1440x1152), HD (1920x1152), SVCD, DVD	32-80,920
OBMC, DCT, SQCIF, QCIF, CIF, 4CIF, 16CIF	H.263	12bx96, 176x144, 352x288, 704x576, 1408x1152 – up to 72 fps	10-64 (audio) 1,024-20,480
4x4 DCT, 8x8 DCT	H.264	Similar to MPEG-4	64-983,040
DCT, VBSMC	MPEG-4	Level 4, 720x1280 progressive 1080x1920 interlace	24-24,5760

VoIP systems deploy specific codec to packetize voice messages. Each of these codecs has specific characteristics with unique bandwidth and delay requirements. The bandwidth requirements of a number of codecs are mentioned in Table II (adapted from [55,56,57,58]). The qualities of these codecs have direct effects on both user-perception (voice/video), as well as network perspective QoS (e.g., overall delays).

B.3 End-to-End Delay

In a VoIP system, the transmission of voice data packets is not instantaneous and latency is the term used to describe the time durations for the needed time that a packet of voice data to be packetized, encoded, moved across the network to an endpoint, decoded and de-packetized, de-jittered, and decoded at the receiving end.

As mentioned, the end-to-end delay has to be minimized for real-time and interactive applications. End-to-end delay reduction directly improves throughput figures. A thorough end-to-end delay analysis is needed for precise throughput calculations.

Total latency is so-called end-to-end latency, mouth-to-ear latency, round-trip-delay (RTD), or round-trip time (RTT) [56].

In VoIP, real conversations usually involve "turn-taking" with 200 msec breaks. When the latency of a network approaches the 200 msec limit, the conversation flow becomes distorted. The two end parties may interrupt each other by starting to talk simultaneously or remain silent at the same time. Degradations for delays over 150 msec (300 msec two-ways) will affect any signal greatly [62]. For video codecs there are also limits for the delay, for instance H.261 and H.263 are typically within the 200 msec to 400 msec limit.

Multimedia applications often require bounded delay figures to offer seamless QoS. An end-to-end delay is comprised of the following delay figure combinations [63]: Packet loss, packet processing delay (codec, serialization, queuing, and propagation delays), and network jitter.

Codec delay is the combination of frame processing and lookahead delays, which are defined as:

- Frame processing delay is a delay of processing a single voice data frame.
- Lookahead delay is the next frame processing delay, which is needed for algorithms with correlation schemes (e.g., ADPC)

The rest of the delays are from: BER, PLR, PDR, PRDeR, echo, and Jitter. Jitter is one of the most important phenomena affecting the quality of a VoIP system.

Jitter happens due to the fact that there is not delivery guarantees for the voice packets across IP networks, therefore there are possibilities that not all voice data packets travel the same path, causing variation in the packet arrival times. This may happen because some packets may chose paths with more hops than other packets. Therefore packets arrive at the destination node with variable delays causing much higher latency effect, called *jitter*, which is calculated per seconds. Table III (adapted from [64,65,66] shows a few audio codecs delay figures.

Too many packets being processed at the intermediate gateways/routers may overwhelm the processing duties momentarily. Both of these circumstances cause latency to become irregular and this irregular delay, as mentioned, is called jitter. To lessen the effects of jitter, packets are gathered in a jitter buffers in the intermediate transmission devices and at the receiving-end device. Table IV (adapted from [52]) shows the acceptable VoIP jitter figures for Cisco-based systems, which should be below the 70 msec level and for inter-frame delay (frame delay jitter) in video, it should be less than 0.15 msec (for H.261).

The combination of end-to-end delay, jitter, noise-levels, and other factors are used to calculate a subjective measure for VoIP system, which is called; the Means Square Opinion (MOS) value. MOS values vary from 5 (highest) to 1 (lowest).

TABLE II
VOIP CODEC BANDWIDTH REQUIREMENTS

Codec	Data Rate (kbps)	Coding Technique	Bandwidth (kbps)
G.711 (A-, μ-law)	64	PCM	68-96
G.722	48, 56, 64	ADPCM	88
G.722.1	24, 32	ACELP	42, 52
G.723.1	5.3, 6.4	ACELP/MPC-MLQ	26, 27
G.726	24, 32	ADPCM	48, 64
G.728	16	LD-CELP	78
G.729	6. 4, 8, 11.8	CS-ACELP	31.2
G.729a	8	CS-CELP	40
AMR-WB (G.722.2)	6.6-23.85	ACELP	36-49
AMR-WB+	5.2-48	ACELP	7.2-50
AMR-NB	4.75-12.2	ACELP	36-44
GSM EFR	12.2	ACLEP	30
GSM FR	13.3	RPE-LTP	31
iLBC	13.3, 15.2	FB-LPC	24, 32

The quality of the audio codec has a direct impact on the MOS score (Table V). Table VI (adapted from [67]) shows a few codecs and their upper MOS limits.

TABLE III
AUDIO CODEC DELAYS

Codec	Codec Delays
G.711	0.25 msec
G.722	1.25 msec
G.722.1	60 msec
G.723.1	97.5 msec
G.726	0.25 msec
G.728	1.25 msec
G.729	25 msec
G.729a	35 msec
AMR	45 msec
GSM EFR	40 msec
iLBC	45 / 70 msec

TABLE IV
JITTER FIGURES IN VOIP (CISCO-BASED) SYSTEMS

Jitter	Quality
Less than 40 ms	Excellent *(unnoticeable jitter)*
40-75 ms	Acceptable *(noticeable jitter)*
Larger than 75 ms	Unacceptable

TABLE V
COMPARISON OF R-VALUES AND MOS SCORES

Characterization	MOS Value
Very Satisfied	4.3+
Satisfied	4.0-4.3
Some Users Dissatisfied	3.6-4.0
Many Users Dissatisfied	3.1-3.6
Nearly All Users Dissatisfied	2.6-3.1
Not Recommended	1.0-2.6

TABLE VI
UPPER LIMITS OF CODEC'S MOS VALUES

Codecs	MOS
G.711	4.3
iLBC	4.14
AMR (12.2 kbps)	4.14
G.729 (8 kbps)	3.92
G.723.1 (6.3 kbps)	3.9
GSM EFR (12.2 kbps)	3.8
G.726 ADPCM (32 kbps)	3.8
G.729a (8 kbps)	3.7
G.723.1 (5.3 kbps)	3.65
GSM FR (12.2 kbps)	3.5

III. CONCLUSIONS

This paper summarizes various criteria for traffic classification purposes, including packet-, flow-, and application-based aspects. We studied different parameters under each category, numerated the parameters considered for each section, and identified the QoS measures and parameters.

REFERENCES

[1] L. Bernaille, R. Teuxeira, I. Akodkenou, A. Soule, K. Salamatian, "Traffic Classification on the Fly", ACM SIGCOMM Computer Communication Review, vol. 36, no. 2, April 2006.

[2] T. Karagiannis, K. Papagiannaki, and M. Faloutsos, "BLINC: Multilevel Traffic Classification in the Dark", ACM Sigcomm 2005, Philadelphia, PA, USA, August 2005.

[3] Andrew W. Moore and Konstantina Papagiannaki, "Toward the Accurate Identification of Network Applications", Passive and Active Measurements Workshop, Boston, MA, USA, March 31 - April 1, 2005.

[4] Cisco IOS Documentation, "Network-Based Application Recognition and Distributed Network-Based Application Recognition", (as of February 2005).
[5] K. Lan, J. Heidemann, "On the correlation of Internet flow characteristics", Technical Report ISI-TR-574, USC/Information Sciences Institute, July, 2003.
[6] Laurent Bernaille, Renata Teixeira, "Implementation Issues of Early Application Identification", AINTEC 2007
[7] App-ID™ Application Classification, Technology Overview, Paloalto Networks, June, 2007
[8] Thomas Karagiannis, Andre Broido, Nevil Brownlee, kc claffy, "Is P2P dying or just hiding?", Proceedings of Globecom 2004, November/December 2004.
[9] S. Sen, O. Spatscheck, D. Wang, "Accurate, Scalable In¬Network Identification of P2P Traffic Using Application Signatures", WWW 2004, New York, USA, May 2004.
[10] "Peer-to-Peer Traffic Classification", iCore - Research Report, Alberta Informatics Circle of Research Excellence Networks and Wireless Communications New Architectures, Intelligent Software Systems, An Inspiring Circle of Research Excellence, April 2005 - March 2006 Volume 5
[11] Alok Madhukar, Carey L. Williamson, "A Longitudinal Study of P2P Traffic Classification", MASCOTS 2006
[12] Denis Zuev, Andrew Moore, "Internet traffic classification using bayesian analysis techniques", ACM SIGMETRICS 2005, Banff, Canada, June, 2005.
[13] Denis Zuev, Andrew Moore, "Traffic Classification using a Statistical Approach", Passive & Active Measurement Workshop, Boston, U.S.A, April 2005.
[14] James P. Early, Carla E. Brodley, and Catherine Rosenburg, "Behavioral Athentication of Server Flows", Proceedings of the 19th Annual Computer Security Applications Conference, Las Vegas, NV, USA, December 2003.
[15] Jefferey Erman, Anirban Mahanti and Martin Arlitt, "Byte Me: A Case for Byte Accuracy in Traffic Classification", Proceeding of MineNet 2007
[16] M. Roughan, S. Sen, O. Spatscheck, N. Duffield, "Class-of-Service Mapping for QoS: A statistical signature-based approach to IP traffic classification", ACM SIGCOMM Internet Measurement Workshop 2004, Taormina, Sicily, Italy, 2004.
[17] A. Soule, K. Salamatian, N. Taft, R. Emilion, and K. Papagiannaki, "Flow Classification by Histograms or How to Go on Safari in the Internet", In ACM Sigmetrics, New York, U.S.A., June, 2004.
[18] PA-4000 Series Feature Overview, Paloalto Networks, Jan 2008
[19] H. Chang, S. Jamin, Z. Mao, and W. Willinger, "An Empirical Approach to Modeling Inter-AS Traffic Matrices", Proceedings of ACM Internet Measurement Conference (IMC) 2005
[20] A. McGregor, M. Hall, P. Lorier, J. Brunskill, "Flow Clustering Using Machine Learning Techniques", Passive & Active Measurement Workshop 2004 (PAM 2004), France, April 19-20, 2004.
[21] Thuy T.T. Nguyen, Grenville Armitage, "A Survey of Techniques for Internet Traffic Classification using Machine Learning", to appear on IEEE Communications Surveys & Tutorials, 2008
[22] T. Dunnigan, G. Ostrouchov, "Flow Characterization for Intrusion Detection", Oak Ridge National Laboratory, Technical Report, November 2000
[23] Eamonn Linehan, "Internet Worm Detection as part of a Distributed Network Inspection System", Master of Science degree thesis, University of Dublin
[24] Laurent Bernaille, Renata Teixeira, "Early Recognition of Encrypted Applications", Passive and Active Measurement Conference (PAM), April, 2007, Louvain-la-neuve, Belgium
[25] S. McCreary and k. claffy, "Trends in wide area IP traffic patterns - A view from Ames Internet Exchange", in ITC Specialist Seminar, Monterey, CA, 18-20 Sep 2000.
[26] Alessandro Amirante, "Robust and Efficient traffic Classification in IP nEtworks", December 2007, http://www.comics.unina.it/index.php?option=com_content&task=view&id=115&Itemid=164
[27] Jörg Wallerich, Holger Dreger, Anja Feldmann, Balachander Krishnamurthy, Walter Willinger. A methodology for studying persistency aspects of internet flows. SIGCOMM Computer Communications Review (CCR), 35(2):23-36, 2005
[28] Jörg Wallerich, "Capturing the Variability of Internet Flows in a Workload Generator for Network Simulators", Ph.D. Dissertation, University of Munich, 2007
[29] Andre Broido, Young Hyun, Ruomei Gao, and kc claffy, "Their share: diversity and disparity in ip traffic". In The 5th anuual Passive & Active Measurement Workshop, PAM2004 (LNCS3015), 2004.
[30] Wentian Li. References on zipf's law, http://linkage.rockefeller.edu/wli/zipf/, 2003
[31] Konstantina Papagiannaki, Nina Taft, Christophe Diot, "Impact of Flow Dynamics on Traffic Engineering Design Principles", INFOCOM 2004, 7-11 March 2004, Vol. 4, Page(s): 2295- 2306
[32] J. Cao, W.S. Cleveland, Y. Gao, K. Jeffay, F.D. Smith, and M.C. Weigle, Stochastic Models for Generating Synthetic HTTP Source Traffic, IEEE INFOCOM, March 2004
[33] IX SYMPOSIUM ON PROBABILITY AND STOCHASTIC PROCESSES, November 20-24, 2006 CIMAT, Guanajuato Gto
[34] J. P. Dubois, Burstiness Reduction of a Doubly Stochastic AR-Modeled Uniform Activity VBR Video, Proc. WASET, 23-45
[35] Kun-Chan Lan, John Heidemann, "A measurement study of correlations of Internet flow characteristics", USC Information Sciences Institute, ISI-TR-574
[36] Yin Zhang, Lee Breslau, Vern Paxson, and Scott Shenker, "On the characteristics and origins of internet flow rates. In SIGCOMM, Pittsburgh, PA, USA, August 2002
[37] Scatter Plot Tool, Mathcracker, http://www.mathcracker.com/scatter_plot.php
[38] IEEE 802.11, http://en.wikipedia.org/wiki/IEEE_802.11
[39] List of WLAN channels, http://en.wikipedia.org/wiki/List_of_WLAN_channels
[40] Naimul Basher, Aniket Mahanti, Anirban Mahanti, Carey Williamson, and Martin Arlitt, "A Comparative Analysis of Web and P2P Traffic", WWW2008, Performance and Scalability, April 21-25, 2008. Beijing, China
[41] A. L. Narasimha Reddy, "Network Elements based on Partial State", Dept. of Electrical Engineering, Texas A & M University, reddy@ee.tamu.edu, http://ee.tamu.edu/~reddy/

[42] KUN-CHAN LAN JOHN HEIDEMANN, “A measurement study of correlations of Internet flow characteristics”, USC Information Sciences Institute, ISI-TR-574
[43] Yin Zhang, Lee Breslau, Vern Paxson, and Scott Shenker, “On the characteristics and origins of internet flow rates”, In SIGCOMM, Pittsburgh, PA, USA, August 2002. IEEE.
[44] Johannes Krohn, “VoIP Standards and Status”, Cisco Systems
[45] Chih-Hong LIN, “The Paradigm Shift: From Packet Blasting to Application and Service Awareness Testing”, Agilent Technologies, SwiNOG#15, Dec. 4th, 2007 Berne
[46] Aleksej Spenst, ”Quality of Service in Local Area Networks Seminar SS07 Telecommunications Lab, April 25, 2007
[47] Yonatan Levy, F. Huebner, D. Liu, A Hierarchical Multi-Class Traffic Model for Data Networks, Proceedings of ITC-16, Edinburgh, Scotland June, 1999.
[48] Kenny Qing Shao, "Traffic measurement in hybrid satellite-terrestrial network, Communication Network Laboratory, School of Engineering Sciences, Simon Fraser University
[49] E D Puschita, T P Palade, QoS Perspective for Wireless Scenarios. Broadband Europe 2005, Bordeaux, 12-14 December 2005
[50] Cristina Aurrecoechea, Andrew T. Campbell and Linda Hauw, "A Survey of QoS Architectures", Multimedia Systems Journal, Special Issue on QoS Architecture, 1997
[51] Ahsan Habib, Sonia Fahmy, and Bharat Bhargava, "Monitoring and controlling 5QoS network domains", International Journal of Network Management, Int. J. Network Mgmt 2005; 15: 11–29
[52] Prof. Dr.-Ing. Thorsten Herfet, "Quality of Service – Ein Blick über den Tellerrand", Saarland University, January 17, 2006
[53] Aura Ganz, Zvi Ganz, Kitti Wongthavarawat, "Multimedia Wireless Networks: Technologies, Standards, and QoS", Prentice Hall Publisher, September 18, 2003
[54] "Overcoming Barriers to High-Quality Voice over IP Deployments", Intel Whitepaper, 2003
[55] Voice Codecs , Voice over IP - Tested by Uninett AS, http://forskningsnett.uninett.no/voip/codec.html, 2004-01-14
[56] Phil Karn, Craig Partridge, "Improving Round-Trip Time Estimates in Reliable Transport Protocols", Proceedings of ACM SIGCOMM '87 11-13 August 1987, pp2-7
[57] Video Conferencing Standards, TANDBERG, Application Notes, D10740, Rev 2.3, http://www.tandberg.com/collateral/white_papers/white paper_Videoconferencing_standards.pdf
[58] Thomas Wiegand, Video Coding Standards, Digital Image Communication, http://iphome.hhi.de/wiegand/assets/pdfs/DIC_video_coding_standards_07.pdf
[59] Pankaj Topiwala, Munish Jindal, H.264/AVC: Overview and Intro to Fidelity-Range Extensions, FastVDO, 2004, http://www.ti.com/asia/docs/india/tiidevconf2004/analog_symp/munish.pdf
[60] Voice Over IP - Per Call Bandwidth Consumption, Cisco Systems, Document ID: 7934, http://www.cisco.com/en/US/tech/tk652/tk698/technologies_tech_note09186a0080094ae2.shtml
[61] Bandwidth Calculator for VOIP, AsteriskGUIDE, http://blog.asteriskguide.com/bandcalc/bandcalc.php
[62] Sven Wiethoelter, "Virtual Utilization and VoIP Capacity of WLANs Supporting a Mix of Data Rates", Technical University Berlin, Technical Report, September 2005
[63] Networking Technology Applications, Secure Voice over IP, University of Ottawa Course Note, ELG5369, IP-Based Internetworking Technologies, Chap9, http://www.ncct.uottawa.ca/COURSE/ELG5369/ELG5369_Chapter9.ppt
[64] Steve Heath, Multimedia and Communications Technology, Second Edition, Focal Press, August 1999
[65] Jerry D. Gibson, Toby Berger, Tom Lookabaugh, Dave Lindgergh, Richard L. Baker, Digital Compression for Multimedia, Principles & Standards, Morgan Kaufmann, Jan 1998
[66] Eric D. Siegel, Designing Quality of Service Solutions for the Enterprise, John Wiley & Sons, October 1999
[67] Mean Opinion Score, Wikipedia, http://en.wikipedia.org/wiki/Mean_Opinion_Score