De-anonymizing Encrypted Video Streams

Master's Thesis

7 September 2018

Stefano Peverelli
pstefano@student.ethz.ch

supervised by
Melissa Licciardello

Systems Group
Department of Computer Science
ETH Zürich

Abstract

In the last recent years streaming services such as Netflix, Youtube, Amazon Prime Video, Hulu and others, have become the main source for video content delivery to the public. With the effort of private companies and of the AOM consortium [**?**], various coding formats and streaming techinques have been refined and have gained popularity. *Adaptive Bitrate Streaming*, between others, enables high quality streaming of media content over HTTP, and represents nowadays the industry's standard.

DASH *Dynamic Adaptive Streaming over HTTP* is an instance of Adaptive Bitrate Streaming originally developed by MPEG. In DASH each media file gets encoded at multiple bitrates, which are then partitioned into smaller segments and delivered to the user over HTTP. Netflix's use of DASH services is no mistery, indeed it is already five years that each title on Netflix sits with its own different bitrate copies on a CDN, waiting to be served to clients in a particular area of the planet. [**?**]

Reed et Al. [**?**] have shwon how, despite a recent upgrade in Netflix infrastructure to provide HTTPS encryption to video traffic, it is possible to recover unique fingerprints for each title, due to the adoption throughout the entire Netflix library, of *per-title encoding*. They make use of adudump [**?**] a command-line program that can run on passive TAP device [**?**] or on a live network interface, and uses TCP and ACKS sequences to infer the sizes of application data unit *ADUs* transferred over each TCP connection.

Our approach reiterates parts of Reed et Al.'s work, but cannot rely on their every assumption and discovery, due to constant changes that Netflix is brining to their enconding and streaming algorithms. Moreover our intent is focused on finding out if, by analyzing coarse-grained traffic data, we are able identify a video based on its *bitrate-ladder*.

Contents

1

Introduction

According to the latest Cisco's VNI [**?**], video will account for 82% of all IP traffic in Europe by 2021; in addition, the overall IP traffic per person will triplicate from 13*GB* to 35*GB*. These forecasts clearly picture the growth of the streaming industry, posing, at the same time an important question on the present and future states of the final user's privacy.

As shown by Reed et Al. [**?**] anonimity of user's viewing activity is at risk. Not for the use that Netflix or other streaming services do of user's session data, but because of the risk of a man-in-the-middle attack *MITM* carried by an *evil* party.

In particular, they have shown how the adoption of HTTPS to protect video streams from Netflix *CDN*s to user's end devices, does not hold against passive traffic analysis.

1.1 Motivation

The goal of this project is to replicate part of the work conducted by Reed et Al. and to investigate the possibility of identifying a Netflix stream solely based on the observed average bandwidth. This, follows from the intuition that *per-title encoding* embeds the nature and the complexity of video frames in a unique way, that may reveal the identity of the content being streamed.

1.1.1 Per-Title Encoding

In December 2015 Netflix announced [**?**] that it was introducing a new method to analyze the complexity of each title and find the best encoding recipe based on it. Their goal with the adoption of per-title encoding was to provide users with better quality streams at a lower bandwidth.

Before then, each title was encoded with a *Fixed Bitrate Ladder*; their pipeline returned a list of {*Bitrate, Resolution*} pairs that represented the sufficient bitrate to encode the stream at a certain resolution (**??**), with no visible artificats.

Bitrate (kbps)	Resolution
235	320 × 240
375	384 × 288
560	512 × 384
750	512 × 384
1050	640 × 480
1750	720 × 480
2350	1280 × 720
3000	1280 × 720
4300	1920 × 1080
5800	1920 × 1080

Table 1.1: Netflix original's Fixed Bitrate Ladder

This "one-size-fits-all" ladder, as reported, achieved good results in the encoded video's perceived quality (**PSNR [?]**) given the bitrate constraint, but, would not perform optimally under certain conditions. For instance, high detailed scenes with sudden changes of light, or rapid transitions of camera shots, would require more than $5800 kbps$; in contrast, more static frames, as in animated cartoons, may be encoded at higher resolutions mantaining the same bitrate level.

In summary they noticed how in certain cases, the produced encoding would either present some small artifacts (*e.g.* complex scenes), or waste bandwidth, (*e.g.* static, plain scenes). For this reason, they came up with per-title encoding.

Resolutions	Fixed Bitrate Ladder (kpbs)	Per-Title Bitrate Ladder (kbps)
320 × 240	235	150
384 × 288	375	200
512 × 384	560	290
512 × 384	750	
640 × 480	1050	
720 × 480	1750	440
720 × 480		590
1280 × 720	2350	830
1920 × 1080	3000	1150
1920 × 1080	4300	1470
1920 × 1080	5800	2150
1920 × 1080		3840

Table 1.2: Comparison between the two different approaches for the same title: note how different titles may have different numbers of quality levels. For each movie, the minimum number of quality levels gets computed to produce a JND[1], when switching bitrates during playback.

In order to find the best fitting bitrate ladder for a particular title, there are several criterias that they took into account, the principal ones being:

- How many quality levels should be encoded to obtain a *JND*[2]between each of them.
- Best {*Resolution*, *Bitrate*} pair for each quality level
- Highest bitrate required to achieve the best perceivable quality

As aforementioned, each title's perceived video quality, gets computed as a measure of *Peak signal-to-noise ratio*. The comparison is performed between the produced encode, upsampled to 1080*p*, and the original title in 1080*p*, and the best {*Bitrate*, *Resolution*} pair is assigned to that specific quality level, as depicted in **??**.

In **??**, we can see the impact of per-title encoding on the original bitrate ladder: in order to achieve the same perceivable quality level (point **B** and **C**), it requires a lower bitrate to be encoded to (point **A**). Moreover, with around the same bitrate, one can see how per-title encoding can achieve a higher resolution compared the fixed case (point **A** and **D** respectively). It follows obviously that, holding to a high-quality stream while maintainig or lowering the used bandwidth is key: the end user will get same or better quality then before, at a lower bandwidth.

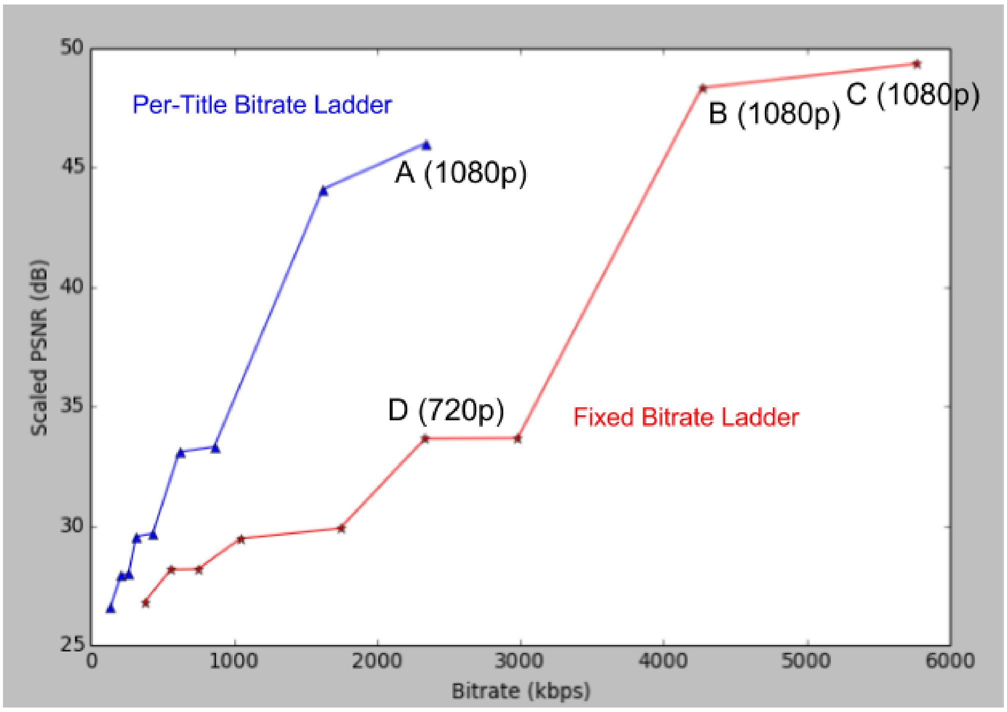

Figure 1.1: Difference between per-title vs. fixed bitrate ladders

[1]just-noticeable-difference

1.1.2 User's Privacy

1.2 Related Work

1.3 Main Objective

1.4 Structure of this Report

ETH

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Declaration of originality

The signed declaration of originality is a component of every semester paper, Bachelor's thesis, Master's thesis and any other degree paper undertaken during the course of studies, including the respective electronic versions.

Lecturers may also require a declaration of originality for other written papers compiled for their courses.

I hereby confirm that I am the sole author of the written work here enclosed and that I have compiled it in my own words. Parts excepted are corrections of form and content by the supervisor.

Title of work (in block letters):

De-anonymizing encrypted video streams

Authored by (in block letters):
For papers written by groups the names of all authors are required.

Name(s):	**First name(s):**
Stefano	Peverelli

With my signature I confirm that

- I have committed none of the forms of plagiarism described in the 'Citation etiquette' information sheet.
- I have documented all methods, data and processes truthfully.
- I have not manipulated any data.
- I have mentioned all persons who were significant facilitators of the work.

I am aware that the work may be screened electronically for plagiarism.

Place, date	**Signature(s)**
Zurich, 07.09.2019	Stefano Peverelli

For papers written by groups the names of all authors are required. Their signatures collectively guarantee the entire content of the written paper.