The Bandwidth Balancing Act

Managing QoE as encrypted services change the traffic optimization game

Submitted to the MaRNEW Workshop

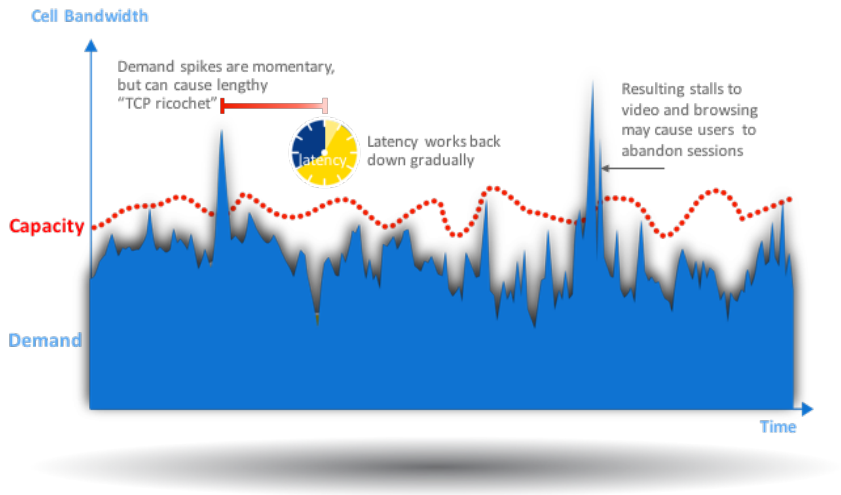
Vijay Devarapalli
August 4, 2015

MOBILE NETWORK QUALITY OF EXPERIENCE (QOE) CHALLENGES

The capacity per cell and the demand placed on each cell (sector-carrier) is not steady. Both change constantly resulting in congestion events at certain instances and under-utilized cell in other instances (see figure below). That means poor customer experiences on one end of the spectrum, and missed revenue opportunity on the other.

Just as operators have begun to deploy solutions for better managing traffic, a surge of encrypted data is appearing on networks, already accounting for 25% of traffic, according to ATIS. In some of Vasona Networks' most recent engagements with operators, we have seen encrypted data comprise the majority of traffic on networks. This trend demands that operators quickly take action to continue intelligent management of traffic on cell networks, or risk seeing the customer experience degrade considerably.

This paper will outline typical causes of cell congestion, challenges posed by encrypted traffic and strategies for taking back control of networks that are flooded with HTTPS sessions



There are a number of contributing factors to poor cell performance including the following:

1. *Fluctuating bandwidth* – The bandwidth that is shared by the users in a cell is not fixed, and fluctuates moment-to-moment as the users move around within the cell, and switch between cells.
2. *Unknown bandwidth* – The actual shared cell bandwidth is not known until the bits are pushed out by the antenna to the UEs. As a user passes behind a building or into an elevator, it can instantly affect how much bandwidth is available. As the cell struggles to deliver those bits to the user, it is not known how many bits per second can be achieved at that moment.
3. *Uneven bandwidth tradeoffs* – The cell bandwidth cannot be evenly traded off among subscribers and services in a cell due to signal conditions.
4. *Inconsistent members* – The number of users and the identity of users changes constantly. In fact, it can change in the middle of a user's video streaming or browsing session. Therefore, the set of users and services that are contending for resources is not constant.

The key to providing consistent QoE is an in-depth understanding of where users and congestion are in the network in real-time and being able to instantly respond to those changing conditions.

RAN CONGESTION AND TCP

The interaction between dynamic demand and dynamic capacity is a challenge for TCP. Applications continually seek to gain more bandwidth and, additionally, if round-trip times (RTT) rise or packets are dropped, applications may be forced into a "slow start" to recover. This results in applications having a variety of speeds across a congested medium.

The mobile network and TCP will generally ensure that sessions get a "proportional fair share" of bits. However, the underlying fluctuating capacity of the mobile network significantly impacts the efficiency of TCP's coping mechanisms and can cause bandwidth-hungry applications to crowd out other apps. At the cell level, there are moments where the demand exceeds the capacity of the cell causing congestion and a steep drop off soon after as a result of packet drops and TCP congestion avoidance. Although these congestion events may only last seconds, and occur only a few times during a session, the damage to user perception is done. It then again takes many seconds or minutes for the demand to slowly grow, as a result of TCP slow start mechanism. This happens over and over in every cell, network-wide causing poor QoE during congestion and under utilized cells when there is slow start for a number of sessions.

TRADITIONAL OPTIMIZATION TECHNIQUES ARE NO MATCH FOR HTTPS

To deal with the issues described in the previous section, mobile operators have traditionally relied on TCP optimization, compressing video by transcoding to a lower bit rate, compressing images, and etc. But with the growth of HTTPS traffic, these techniques no longer work.

DYNAMIC RATECONTROL WITH FEEDBACK FOR HTTPS TRAFFIC

Vasona's unique Dynamic RateControl with Feedback (DRCF), deployed in the RAN, detects congestion on a per-cell basis and manages traffic going into the congested cell. Vasona's DRCF technology is deployed currently in tier-one mobile operator networks globally, managing significant amount of HTTPS traffic (more than 60% in some networks).

Based on this experience, Vasona Networks has determined that solutions that aim to most efficiently and successfully manage traffic must:

- Be transparent when there is no congestion, taking action ***only*** in congested cells
- Determine the active application types and their real needs to ensure high QoE
- Detect congestion per cell the moment it occurs
- Identify the causes of congestion and which UEs are contending for bandwidth
- Addresses the congestion immediately by shaping traffic going to the cell based on the individual session characteristics.
- Not modify the content – no transcoding or compression

- Stop responding to a congestion event as soon as it is over

With Vasona DRCF, the video QoE improves by 20-30% on an average in the form of improved video start delay, reduced stalls and stall time during congestion. Browsing page download times also improve by 20-30%.

It is also very important to manage both HTTP and HTTPS traffic in a congested cell. A solution that manages only HTTP traffic is not sufficient, because the unmanaged HTTPS traffic will continue to congest the cell leading to poor QoE in the cell. To improve the overall QoE, each session, both HTTP and HTTPS needs to be managed based on their individual QoE requirements. The key to managing HTTPS traffic is to identify the traffic and its characteristics accurately. When a new session is setup, there is a need to know the type of session (video/browsing/downloads/etc) and the QoE requirements for that session. Once identified as a browsing or download session, DRCF uses TCP layer techniques to modify the bit rate (increase or decrease) for each session. A combination of techniques based on DNS response, TLS SNI, and heuristics are used to identify and classify each HTTPS session as browsing, video, downloads, audio, background updates, etc. But these techniques are not sufficient to ensure 100% accuracy – traffic classification of HTTPS traffic needs to somehow get better. Therefore, there is a need for IETF to work with the content providers, mobile operators and the network equipment vendors, to better identify and classify HTTPS traffic.

SUMMARY

Vasona has a unique solution that can manage traffic per cell based on RAN congestion and traffic classification, with the goal of improving the overall QoE for the cell under congestion. The main characteristics of the solution are to take action only when the cell is congested and to maximize the QoE for the most number of sessions in the cell. The key to managing HTTPS traffic is to classify it accurately and use TCP layer techniques to control the bit rate of individual sessions. Further work is needed on identifying and classifying HTTPS traffic to increase the accuracy.