Vivisecting WhatsApp through Large-Scale Measurements in Mobile Networks

Pierdomenico Fiadino, Mirko Schiavone, Pedro Casas
FTW Vienna
surname@ftw.at

ABSTRACT

WhatsApp, the new giant in instant multimedia messaging in mobile networks is rapidly increasing its popularity, taking over the traditional SMS/MMS messaging. In this paper we present the first large-scale characterization of WhatsApp, useful among others to ISPs willing to understand the impacts of this and similar applications on their networks. Through the combined analysis of passive measurements at the core of a national mobile network, worldwide geo-distributed active measurements, and traffic analysis at end devices, we show that: (i) the WhatsApp hosting architecture is highly centralized and exclusively located in the US; (ii) video sharing covers almost 40% of the total WhatsApp traffic volume; (iii) flow characteristics depend on the OS of the end device; (iv) despite the big latencies to US servers, download throughputs are as high as 1.5 Mbps; (v) users react immediately and negatively to service outages through social networks feedbacks.[1]

Categories and Subject Descriptors

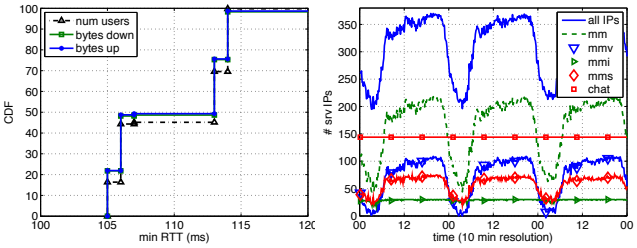
C.2 [**Computer-Communication Networks**]: Miscellaneous; C.4 [**Performance of Systems**]: Measurement Techniques

Keywords

WhatsApp, Large-Scale Measurements, Mobile Networks.

1. MOTIVATION & METHODOLOGY

WhatsApp is doubtlessly the leading instant multimedia messaging service in mobile networks. It handles more than 64B messages per day, including 700M photos and 100M videos. With half a billion of active users, it has become the fastest-growing company in history in terms of users. The goal of this work is to provide the first large-scale characterization of the complete service, highly useful for mobile operators and service providers, both to asses its impact on the network and to understand how to track its usage.



(a) min RTT to WhatsApp IPs. (b) WhatsApp daily active IPs.

Figure 1: Characteristics of WhatsApp servers.

As WhatsApp traffic is encrypted, our study required a complex methodology to discover the traffic flows and the corresponding hosting servers: firstly, by analyzing WhatsApp traffic captures at end devices, and particularly focusing on the DNS requests, we identified the naming scheme used by the servers. Secondly, using this naming scheme on top of the HTTPTag traffic classification tool [1], and following a similar procedure to [2], we collected a week of WhatsApp flows at the core of a European national-wide mobile network (from 18.02 to 25.02), which were then analyzed through the DBStream large-scale analysis system [3]. In a nutshell, every time a user issues a DNS request for the fully qualified domain name `*.whatsapp.net`, HTTPTag creates an entry mapping this user to the server IPs provided in the DNS reply. Each entry is time stamped and expires after a time-out based on the TTL of the DNS reply. Using these mappings, all the subsequent flows between this user and the identified servers are assumed to be WhatsApp flows. To increase the robustness of the approach, the list of IPs is augmented by adding those servers signing the TLS/SSL certificates with the string `*.whatsapp.net`, as observed at the end device captures. Finally, by using the MaxMind GeoIP databases (`http://www.maxmind.com`), combined with geo distributed DNS active measurements using the RIPE Atlas monitoring network (`https://atlas.ripe.net`), we identified and characterized the WhatsApp hosting infrastructure.

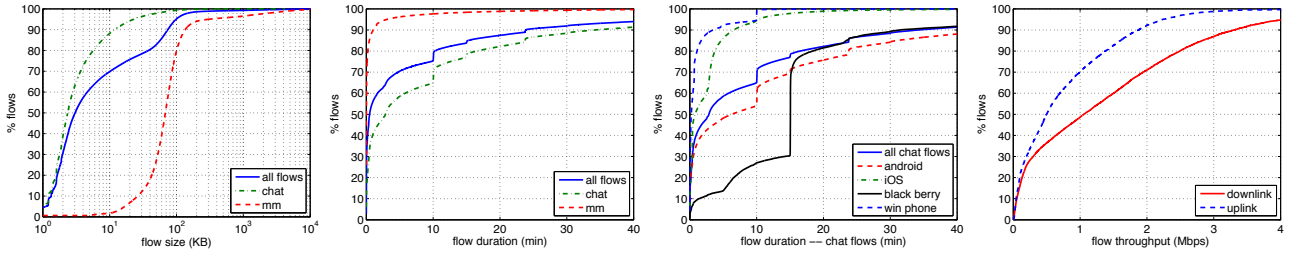
2. ANALYSIS & FINDINGS

The complete dataset consists of more than 140M chat flows, 9M photo/audio content flows, and 5M video flows. Our main findings are the following:

(i) WhatsApp uses a highly structured naming scheme to handle different message types: servers are associated to different third-level domain names, de-

[1]This work has been done in the framework of the EU-IP project mPlane, funded by the EC under grant 318627. The work is partially funded by the DARWIN4 COMET project.

SIGCOMM'14, August 17–22, 2014, Chicago, IL, USA.
ACM 978-1-4503-2836-4/14/08.
http://dx.doi.org/10.1145/2619239.2631461.



(a) Flow size. (b) Flow duration. (c) Flow duration per OS. (d) MM flow throughput.

Figure 2: WhatsApp flow characteristics and performance.

pending on the nature of the message (control, chat, media). Chat and control messages are handled by *chat servers* on ports 5222 (XMPP) or 443, identified by the domain names `e|c|dX.whatsapp.net` (`X` is a variable for load balancing). To allow a fast delivery of messages, chat connections are kept up while the application is active or in background. Transfers of photos, videos and audio are instead managed by HTTPS *multimedia servers* identified by `mms|mmi|mmvXYZ.whatsapp.net`, `mms|mmi` for audio and photos, and `mmv` for videos. Each HTTPS connection is dedicated to a single content, and closed on transfer completion.

(ii) Despite its worldwide popularity, WhatsApp is a centralized service hosted by a single provider at servers located in the US: 386 server IPs hosting WhatsApp are observed in the complete dataset, belonging to a single AS owned by the cloud provider SoftLayer (AS36351). To avoid biased conclusions about the set of IPs seen from a single Vantage Point (VP), we performed active measurements using RIPE Atlas: we analyzed which IPs were obtained resolving the same domain names from 600 boxes around the globe during multiple days. These measurements confirmed that the same set of IPs is always replied, regardless of the location of the requester. Using MaxMind, we observed that these IPs are mainly located in Dallas and Houston. We confirmed this through traceroutes and active RTT measurements. Fig. 1(a) plots the distribution of the min. RTT from the VP to the server IPs, weighted by the number of flows and traffic volume. The cdf shows that the service is evenly handled between two different yet potentially close locations at about 106ms and 114ms from the VP, which is compatible with our findings. To understand the dynamics of these IPs, fig. 1(b) shows the number of daily active IPs, split by message type. More than 350 IPs serve flows during peak hours, and 200 IPs are active even in the lowest load hours. Chat servers are constantly active to keep the state of active devices. Note that the `mmi` and `mms` IPs also seem to have a share of always-active IPs.

(iii) Flow characteristics and performance: Tab. 1 reports the downlink/uplink volume and flow shares. While the majority of the flows correspond to chat messages, media messages account for more than 76% of the total up/down traffic, with video covering almost 40%. In terms of flow size/duration, figs. 2(a-b) show that chat flows are small sized (6.7KB avg.) and long lasting (17' avg.), whereas media flows are bigger (225KB avg.) and shorter (2' avg.). The flow duration cdf additionally reveals some steps at exactly 10', 15' and 24', suggesting the usage of Time-Outs (TOs) to terminate idle connections. As shown in fig. 2(c), these values are dictated by the OS of the device. Different TOs are visible for Android at 10', 15' and 24'; iOS uses a TO

features	chat (%)	mm (%)	mmv (%)	mmi (%)	mms (%)
$\text{bytes}_{\text{down/up}}$	17/30	83/70	40/36	13/16	30/18
flows	93.4	6.2	0.3	2.9	2.9

Table 1: Volume and flows per traffic category.

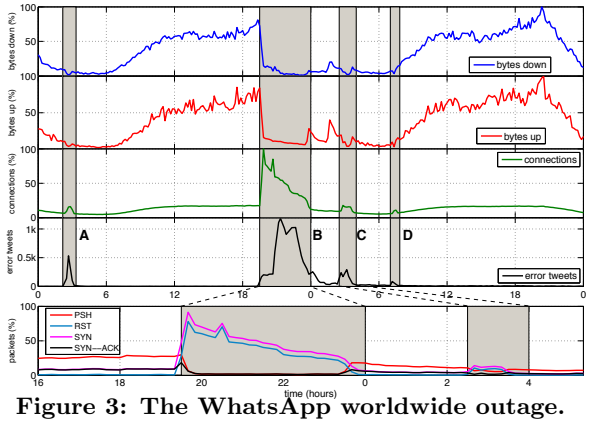


Figure 3: The WhatsApp worldwide outage.

of 3', BlackBerry has 15' TOs, whereas Win phones favors 10' TOs. When it comes to performance, fig. 2(d) indicates that, despite the big latencies to US servers, throughputs for multimedia flows bigger than 1MB are rather high, achieving an avg. down/up flow throughput of 1.5 Mbps/800 kbps.

(iv) User reactions to WhatsApp outages are rapidly observed through social networks feeds: fig. 3 depicts the volume and flow counts time series during 2 days around the major outage occurred in Feb. 22nd '14. The event is not only clearly visible from the traffic measurements, but can also be correlated with the user reactions on social networks. Through the `downdetector.com` application we collected the counts of Twitter feeds containing the keyword "whatsapp", coupled with keywords reflecting service impairments such as "outage", "is down" (i.e. *error tweets*). The main reported outage (event `B`) occurred at around 19:00CEST, but similar outages are observed in the error tweet counts which have the same network traffic signature (`A`, `C` and `D`), i.e., a traffic volume drop and an increase in the flows count. To better drill-down the outage, the figure also depicts a 12-hour-zoom of the TCP flags counters. A steeped increase of the SYN and RST packets indicates that devices were repeatedly trying to reconnect after the servers reset the connections, suggesting that the failure occurred at the application layer.

3. REFERENCES

[1] P. Fiadino, et al., "HTTPTag: A Flexible On-line HTTP Classification System for Operational 3G Networks", in *IEEE INFOCOM*, 2013.

[2] I. Bermudez, et al., "DNS to the rescue: Discerning Content and Services in a Tangled Web", in *ACM IMC*, 2012.

[3] A. Bär, et al., "DBStream: an Online Aggregation, Filtering and Processing System for Network Traffic Monitoring", in *TRAC*, 2014.