A Platform for Home Network Traffic Monitoring

Abdesselem Kortebi[1], Zied Aouini[1, 2], Christophe Delahaye[1], Jean-Philippe Javaudin[1], Yacine Ghamri-Doudane[2]
[1]Orange, France; Email: {abdesselem.kortebi, christophe.delahaye, jeanphilippe.javaudin}@orange.com
[2]L3i lab, University of La Rochelle, France; Email: zied.aouini@etudiant.univ-lr.fr, yacine.ghamri@univ-lr.fr

***Abstract*— In this demo, we present a home network traffic monitoring platform. Our solution is based on two main software components using standard IPFIX flow export architecture: a probe and a collector. The probe role is to capture flows in progress and to perform real time traffic classification. We implemented the probe on an actual home gateway prototype showing its feasibility on hardware constrained devices currently used by the consumers. Furthermore, we addressed hardware accelerators issue inherent to this kind of devices. The collector analyzes the records exported by the probe allowing to visualize various network monitoring data including flow rates, volumes and corresponding applications. Our collector is built upon an open source tool, namely nTopng.**

I. INTRODUCTION

Home network complexity is increasing with the multiplication and diversification of devices (laptops, TVs, smartphones, sensors, etc.), services and connectivity technologies (mainly Ethernet, Wi-Fi, power line communication and multimedia over coax). Moreover, various application types are consumed: Facebook, Youtube, Skype, Bittorrent, etc. In this context, when service degradation occurs, it is difficult for both the end user and the ISP help-desk to easily tackle the issue. In fact, usually, the customer tends to call the ISP help-desk even if the problem is outside the home network. On the other hand, ISPs control all segments of their networks (core, access, etc.) but not the home network (i.e. the portion between the home gateway and the end device). Therefore, relying on efficient traffic monitoring tools allowing to observe and to identify home network flows is a key aspect for diagnostic enhancement and network performance improvement [1] [2].

Actually, home network traffic monitoring would allow among other functions:

- Having better insight on network usage (e.g. devices consuming the highest bandwidth, flow rates, etc.)
- Applying advanced parental control (e.g. blocking access to a specific application from a given device)
- Deploying of QoS mechanisms (e.g. application-based prioritization)
- Detecting anomalies (e.g. botnets attacks)

However, home network traffic monitoring raises many challenges –especially in terms of feasibility– which we address in this demo.

This paper is organized as follows. In the next section, we describe our proposed platform architecture focusing on the involved software components. Then, in section III, we describe the demo setup and the scenarios highlighting the benefits of our solution. Finally, we conclude and cite future work.

II. PLATTFORM ARCHITECTURE

Various traffic monitoring approaches exist. We advocate to rely on a home gateway flows-export-based approach. Indeed, end hosts solutions (e.g. HostView) are not viable in our context where multiple devices and many OSs are being used, not to mention the fact that they are not controlled by the ISP. Furthermore, the full-packet-capture approach applied by some tools, such as Snort and Bro, is not compatible with hardware constrained devices in the home network. On the other hand, flow export is a flexible, standardized and efficient method.

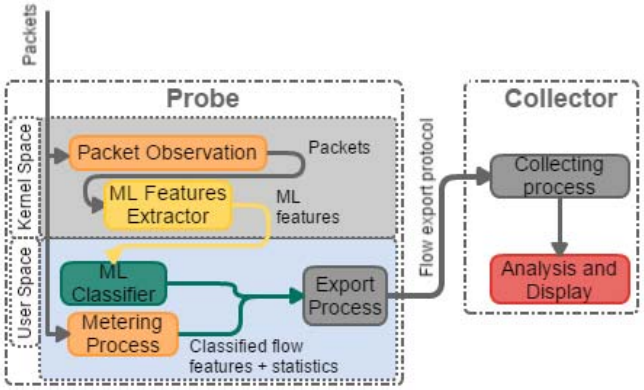

Fig.1. Home network traffic monitoring platform: software components architecture

More specifically, our solution is based on the following software components as illustrated in Fig.1. We implemented a probe on a home gateway prototype (having the same chipset and hardware characteristics as a home gateway commercially deployed at customer premises) whose role is to capture the traffic and export statistics. The probe performs also real time traffic classification using machine learning (ML). The classifier allows flows' applications to be identified based on the statistical features of the very first packet only (payload size, port number, inter packet delays and protocol). One of the main advantages of machine learning techniques is that it does not rely on packet payloads and is consequently agnostic to encrypted traffic. We

computed the training phase of our algorithm based on real residential Internet traces presented in [3]. Finally, as we rely on the standard IPFIX export protocol, we are able to use an open source collector, nTopng[1], to analyze, store and display exported data by the probe. The collector can be run locally, as shown in this demo, or in the cloud.

III. DEMO DESCRIPTION

As mentioned in the previous section, we implemented our probe on a home gateway prototype as it is the central element of the home network where most traffic passes through, in addition to the fact that it is an ISP controlled device. To do so, we had to overcome hardware accelerators issue. Indeed, hardware accelerators are used to perform high speed packets routing, typically at Gigabit/s rate, which prevents the OS from seeing the actual packets and their features. We achieved to interact with those hardware accelerators to get the information we needed.

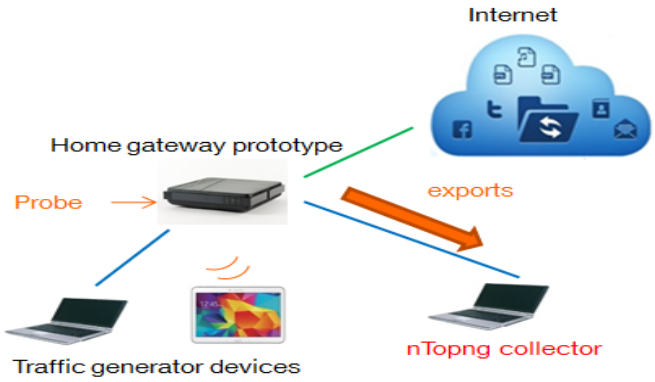

Fig. 2. Demo setup

The setup of our demo is shown in Fig. 2. It is composed of the home gateway, two end devices (PC and tablet) generating Internet traffic and a laptop hosting the nTopng collector. Then, we launch a YouTube video flow using the Chrome browser (relying on the Quic protocol) and a Facebook session.

Figure 3 depicts the information displayed on the nTopng GUI regarding the ongoing flows. As we can see, our probe is able to identify the Quic protocol and the Facebook flows (with 99.9% and 96% confidence levels, respectively). Furthermore, real-time throughput and the volume of each flow are indicated along with other information (IP addresses, duration, etc.). It is also possible to focus on a specific device to check all flows that it generates and the corresponding applications. This kind of information might be useful for the end user and the ISP help-desk for troubleshooting purposes.

IV. CONCLUSION

In this paper, we described a home network traffic monitoring platform. At this aim, we combined a flow export approach and a machine learning method. We implemented a software probe on a home gateway prototype allowing exporting flows statistics and performing real-time traffic classification. We used an open source collector (nTopng) to display the exported information. We showed that our approach is feasible and efficient. The detailed description of the proposed machine learning algorithm will be part of another paper submitted to the IM 2017 conference, special track on "autonomic management".

In our future work, we will conduct an extensive performance evaluation including the probe CPU consumption and memory occupation as well as the traffic classification algorithm accuracy.

REFERENCES

[1] Z. Aouini, A. Kortebi, Y. Ghamri-Doudane, "Traffic monitoring in home networks : enhancing diagnosis and performance tracking", IEEE IWCMC 2015.

[2] A. Kortebi, Z. Aouini, M. Juren, J. Pazdera, "Home network traffic monitoring case study : Anomaly detection", IEEE GIIS 2016.

[3] Z. Aouini, A. Kortebi, Y. Ghamri-Doudane, "Towards understanding residential Internet traffic: from packets to services", IEEE NoF 2016.

Recently Active Flows

10 Applications

Info	ML Application (confidence)	ntopng Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes
Info	Quic (99.99%)	QUIC.Google	UDP	192.168.1.2:44177	173.194.0.199:443	1 min, 19 sec	Server	5.28 Mbit	32.02 MB
Info	Google (83.66%)	Facebook	TCP	192.168.1.2:60259	edge-star-shv-01-cdg...:443	46 sec	Client Server	1.59 Kbit	170.2 KB
Info	Google (83.66%)	Facebook	TCP	192.168.1.2:59428	xx-fbcdn-shv-01-fra3...:443	46 sec	Client Server	16.88 Kbit	16.34 KB
Info	Facebook (96.12%)	Facebook	TCP	192.168.1.2:59426	xx-fbcdn-shv-01-fra3...:443	18 sec	Client Server	69.3 bps	5.06 KB
Info	Facebook (96.12%)	Facebook	TCP	192.168.1.2:59422	xx-fbcdn-shv-01-fra3...:443	18 sec	Client Server	69.3 bps	5.06 KB
Info	Facebook (96.12%)	Facebook	TCP	192.168.1.2:59423	xx-fbcdn-shv-01-fra3...:443	18 sec	Client Server	0 bps	5.06 KB
Info	Facebook (96.12%)	Facebook	TCP	192.168.1.2:59425	xx-fbcdn-shv-01-fra3...:443	18 sec	Client Server	69.3 bps	5 KB
Info	Facebook (96.12%)	Facebook	TCP	192.168.1.2:59427	xx-fbcdn-shv-01-fra3...:443	18 sec	Client Server	0 bps	5 KB
Info	Facebook (96.12%)	Facebook	TCP	192.168.1.2:59424	xx-fbcdn-shv-01-fra3...:443	18 sec	Client Server	69.3 bps	5 KB
Info	Quic (100.00%)	QUIC.Google	UDP	192.168.1.2:33893	par21s05-in-f2.1e100...:443	42 sec	Client Server	0 bps	4.92 KB

Showing 1 to 10 of 20 rows

« < 1 2 > »

Fig. 3. Screenshot of collector GUI, ongoing flow

[1] http://www.ntop.org/ndpi/released-ndpi-1-5-1-and-ntopng-1-2-1/