Scalable Approach to Data Collection in Broadband Access Networks

Tiago Cruz[1], Thiago Leite[1], Patrício Batista[1], Rui Vilão[1],
Paulo Simões[1], Fernando Bastos[2], Edmundo Monteiro[1]
[1]CISUC – DEI, Universidade de Coimbra, Dep. Eng. Informática, Portugal
[2]PT Inovação SA, Aveiro, Portugal

Keywords: monitoring architecture for broadband services, trend inference, home networks

From the operator perspective, reliable data gathered from strategic network locations make all the difference for a number of applications, such as quality and SLA monitoring, network planning or security purposes (threat identification and profiling, violation of *terms of use*, etc.).

Operators still follow classic approaches based on a limited number of standalone probes and filters positioned along strategic places on their own core network, that gather information about specific trends and patterns [1]. However, this model is not scaling properly with the sheer increase of traffic flow volume and diversity [2] – a consequence of access technologies such as DSL and optical fiber and applications such as IPTV, video-on-demand, voice and P2P.

In order to solve this, we suggest moving the monitoring probes to the edges of the access network. More specifically, we propose to place monitoring probes in the borderline between the operator access network and the home network of each subscriber. By massively distributing the monitoring process (from a limited number of probes in the core network to thousands of probes) each probe deals with a much smaller traffic flow, making it possible to apply fine-grained processing techniques. It also becomes possible to use already available network equipment: the broadband routers the subscribers already installed and paid for. The advantages of such an approach relate, therefore, with location, scalability, granularity and equipment cost.

In this paper we present a scalable, massively distributed monitoring architecture that integrates the broadband routers of domestic subscribers into the monitoring platform of the operators. Extending a number of technologies already available, these routers cooperate with the provider in the collection and processing of valuable monitoring data. Each router – remotely managed by the operator – works in a automated way, possessing inference and filtering abilities of its own and being capable of selecting specific data to be sent to the central coordination point. This coordinated operation model allows the monitoring system to access and infer information at two distinct infrastructure levels: microscopic (subscriber) level and macroscopic (operator) level, making it capable of detecting trends otherwise impossible for a device operating autonomously (like standalone probes, in the classic model).

This paper will also address issues such as the correlation of data gathered from each probe, in order to produce the macroscopic view of the network, ethical issues (such as subscriber privacy), system performance – when compared with classic approaches – and manageability.

References

[1] B. Greene et al., *Sink Holes – A swiss army knife ISP security tool – tutorial*, NANOG28, North American Operators' Group, June 2003

[2] C. Fraleigh et al., *Packet-level traffic measurements from the Sprint IP backbone*, IEEE Network, Vol. 17, 2003