RFC 5474 : A Framework for Packet Selection and Reporting

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 1 avril 2009

Date de publication du RFC : Mars 2009

https://www.bortzmeyer.org/5474.html

L'échantillonnage est une opération qui consiste à ne sélectionner qu'une partie des objets qu'on mesure. Par exemple, lors de l'étude des paquets passant par un réseau, on ne capture qu'une partie des paquets, afin de ne pas faire exploser le disque et que le temps d'analyse reste raisonnable. Le groupe de travail PSAMP <http://www.ietf.org/html.charters/psamp-charter.html> de l'IETF met au point des normes sur l'échantillonnage de paquets, afin de garantir une certaine cohérence dans les mesures. Ce RFC présente le cadre général de PSAMP.

Les travaux de PSAMP partent dans plusieurs directions, aussi bien la définition des opérations d'échantillonnage que le protocole permettant de transmettre à une autre machine les paquets capturés (de la même façon qu'IPFIX transmet des informations sur les flux). Notre RFC 5474 [1] est le cadre général, le RFC 5475 décrit les mécanismes d'échantillonnage, le RFC 5476 normalise le protocole qui permet d'exporter le résultat de l'échantillonnage et le RFC 5477 décrit le schéma de données utilisé pour cette exportation.

Attaquons cette famille avec la section 3 du RFC, qui décrit les généralités. À un endroit du réseau (par exemple sur le port d'un routeur), on observe les paquets, un processus les sélectionne (c'est l'échantillonnage), un autre construit des données en utilisant les paquets sélectionnés et un dernier les exporte vers un point de collecte, où se fera l'analyse finale (selon un mécanisme proche de celui d'IPFIX, RFC 7011). Les paquets sélectionnés n'ont pas forcément quelque chose en commun et c'est pour cela que le RFC utilise pour l'exportation le terme de "*stream*" et pas celui de "*flow*" (RFC 3917).

Je m'intéresse particulièrement ici au processus de sélection, décrit en section 3.3. La sélection peut se faire sur divers critères, et elle peut mettre dépendre d'un état du processus du sélection (le RFC cite plusieurs exemples de tels états comme le numéro d'ordre du paquet, comme l'état d'un générateur pseudo-aléatoire, etc).

Les protocoles qui mettent en œuvre ce système obéissent à des exigences décrites en section 4. Les mécanismes de sélection (section 4.1) doivent être :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5474.txt

— assez simples pour être déployés facilement en des endroits où il faut aller **vite**. L'idée est de pouvoir traiter les paquets au rythme où ils passent ("*line-rate*"). La section 10 revient plus en détail sur cette exigence de performance et sur la complexité des opérations de sélection de paquets. La sous-section 10.2 plaira aux passionnées des couches basses, puisqu'elle décrit les implémentations possibles dans le matériel, notamment les ASIC.
— mais aussi assez riches pour couvrir tous les cas d'usage.
— et extensibles car tout n'aura pas été prévu.

Les sélecteurs obéissant à ces critères figurent en section 5 et surtout dans le RFC 5475.

Il y a aussi des exigences pour le système de mesure (capacité à indiquer que de l'information a été perdue, respect de la vie privée des utilisateurs, selon le RFC 2804, etc), et pour le système d'exportation (proches de celles d'IPFIX, cf. RFC 3917).

Les sélecteurs sont décrits en section 5. Ils sont de deux modèles, ceux qui filtrent et ceux qui échantillonent. Les premiers sélectionnent certains paquets selon les caractéristiques du paquet. Par exemple, si on dit à tcpdump, en langage BPF, `tcp and dst port 443`, il va filtrer selon ce critère et ne garder que les paquets TCP à destination du port 443 (HTTPS). Les seconds, ceux qui échantillonent, sont tous les autres, ceux qui n'utilisent pas uniquement le contenu du paquet mais un critère extérieur, par exemple un tirage aléatoire. Les sélecteurs qui échantillonent se divisent à leur tour en deux sous-groupes, ceux où la sélection ne dépend pas du tout du contenu du paquet et ceux où ce contenu est utilisé, par exemple pour réaliser une distribution non uniforme. Donc, si j'utilise pcapdump <`http://packages.debian.org/pcaputils`> et que je le lance avec l'option `-S`, j'utilise un sélecteur qui n'est pas un filtre, et qui ne dépend pas du tout du contenu du paquet (cette option garde un paquet sur N, où N est l'argument de l'option).

La section 5.2 résume les sélecteurs importants :

— Échantillonnage fondé sur le comptage des paquets. C'est l'option `-S` de pcapdump mentionnée plus haut. À ma connaissance, ni tcpdump, ni Wireshark n'ont une option équivalente.
— Échantillonnage fondé sur le temps. Je ne connais pas de progiciel de capture de paquets qui aie une telle possibilité, il faut le développer soi-même avec la libpcap <`https://www.bortzmeyer.org/capture-paquets.html`>.
— Diverses formes d'échantillonnage aléatoire. Même remarque que ci-dessus quant à la (non-)disponibilité d'une tellee option dans l'offre logicielle actuelle.
— Filtrage sur le contenu, comme avec le langage BPF cité plus haut dont disposent tous les outils de capture sur Unix. Selon le langage disponible, on pourra utiliser plus ou moins de critères (le RFC 7012 en donne une idée).
— Filtrage selon la valeur d'une fonction de hachage du paquet. C'est une technique que les répartiteurs de charge utilisent souvent.

Les sélecteurs peuvent naturellement être combinés (section 5.5), par exemple en faisant un filtrage suivi d'un échantillonnage.

Mais, au fait, quelle est l'utilité de ce travail ? La section 11 donne des exemples d'applications de l'échantillonnage.

Enfin, l'inévitable section sur la sécurité est la numéro 12, qui pointe, entre autres, un problème général de toutes les mesures passives, le risque d'atteintes à la vie privée (section 12.2) et un risque spécifique de l'échantillonnage, celui qu'un méchant tente d'échapper à la détection en se débrouillant pour que ses paquets ne soient pas ceux sélectionnés (section 12.3).