



HAL
open science

Vers des mesures haute fréquence d'internet plus éthiques

Matthieu Gouel, Kevin Vermeulen, Hugo Rimlinger, Olivier Fourmaux, Timur Friedman

► **To cite this version:**

Matthieu Gouel, Kevin Vermeulen, Hugo Rimlinger, Olivier Fourmaux, Timur Friedman. Vers des mesures haute fréquence d'internet plus éthiques. 8èmes Rencontres Francophones sur la Conception de protocoles, l'évaluation de performances et l'expérimentation de Réseaux de communication, May 2023, Cargese, France. hal-04090683

HAL Id: hal-04090683

<https://hal.science/hal-04090683>

Submitted on 5 May 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Vers des mesures haute fréquence d'internet plus éthiques

Matthieu Gouel^{1,2}, Kevin Vermeulen³, Hugo Rimlinger^{1,2}, Olivier Fourmaux¹ et Timur Friedman^{1,2}

¹Sorbonne Université, CNRS, LIP6, 4 place Jussieu, 75005 Paris

²LINCS, 23 avenue d'Italie, 75013 Paris

³LAAS-CNRS, 7 avenue du Colonel Roche, 31031 Toulouse

La communauté dispose aujourd'hui d'outils de mesures actives permettant de scanner internet en entier en quelques minutes. Ces outils, bien qu'utiles, peuvent déclencher des mécanismes de défense des routeurs et peuvent pousser les opérateurs à filtrer définitivement ce trafic qui est néanmoins utile à tous les utilisateurs d'internet. Dans cet article, nous poussons la communauté à prendre conscience du problème éthique posé par les mesures haute fréquence et proposons des pistes pour rendre ces mesures plus éthiques.

Mots-clés : mesures actives d'internet; éthique de la mesure

1 Introduction

Aujourd'hui, des techniques de mesures actives peuvent sonder le réseau à très haute fréquence, jusqu'à plusieurs millions de paquets par seconde. Envoyer des pings d'une source vers l'ensemble des adresses IPv4 ($2^{32} - 1$) ou effectuer des traceroutes vers tous les préfixes IPv4 /24 annoncés dans internet est possible en quelques dizaines de minutes [Bev16, VRB⁺20]. Ces avancées permettent d'effectuer des études d'internet avec une résolution temporelle plus élevée.

Mais ces mesures à haute vitesse peuvent également être préjudiciables. En effet, celles-ci peuvent demander des ressources importantes aux routeurs, et potentiellement déclencher des mécanismes de défense contre les dénis de service, comme une limitation du nombre de réponses envoyées aux paquets ping et traceroute (appelé *taux limite* ou *rate limiting* en anglais). Dépasser le taux limite d'un routeur pendant trop longtemps peut avoir des conséquences directes sur les chercheurs qui voient leurs résultats entravés, ou sur les opérateurs qui ne peuvent plus obtenir d'informations sur l'état de leur réseau. Le tableau 1 montre un exemple de deux traceroutes T et T' réalisés à 15 minutes d'intervalle. Une interface est manquante (“*”) dans T' au TTL 7. Cette étoile a pour conséquence de rendre le chemin entre systèmes autonomes (AS) de T' incomplets, ce qui peut être préjudiciable pour un opérateur qui souhaiterait analyser une panne ou pour un chercheur qui voudrait analyser ce chemin. Ce phénomène est typiquement provoqué par un dépassement du taux limite, et nous défendons que cela est évitable si on sait que des mesures trop importantes vont le déclencher. Aussi, de manière indirecte, dépasser le taux limite trop souvent peut inciter les opérateurs à ne plus répondre du tout aux paquets ping et traceroute, et de ce fait les utilisateurs finaux ne bénéficieraient plus des recherches en mesure d'internet qui étudient par exemple les problèmes de performance, de sécurité, ou encore de neutralité d'internet.

Dans un contexte plus global aux technologies de l'information et de la communication (TIC), le rapport Menlo [KD12] définit l'éthique de la recherche sous la forme d'une balance bénéfiques/préjudices, et encourage les chercheurs à maximiser les bénéfiques et minimiser les préjudices, sans pour autant définir de frontière précise pour décider si une recherche est éthique ou non. Partridge et al. [PA16] ont depuis précisé cette ligne directrice aux mesures d'internet, en statuant que “l'envoi d'une seule sonde vers une adresse IP constitue au pire un léger préjudice, alors que l'envoi persistant d'une série de sondes à haute vitesse vers une adresse IP constitue un préjudice grave, car pouvant involontairement bloquer un lien précisément quand celui-ci est nécessaire pour une urgence”. Bien que plus précise, cette définition ne définit

TABLE 1: Deux traceroutes T et T' depuis la même source vers la même destination mesurés dans un intervalle de 15 minutes. Dans T' , le routeur à TTL 7 n'a pas répondu (“*”) à TTL 7, ce qui a pour conséquence qu'un AS est manquant dans le chemin au niveau AS de T' .

TTL	T hops	T' hops	T AS hops	T' AS hops
1	2001 :67c :6ec :201 :145 :220 :0 :1	2001 :67c :6ec :201 :145 :220 :0 :1	1101	1101
2	2001 :67c :6ec :1101 :192 :12 :54 :241	2001 :67c :6ec :1101 :192 :12 :54 :241	1101	1101
3	2001 :610 :fc7 :0 :145 :145 :2 :218	2001 :610 :fc7 :0 :145 :145 :2 :218	1103	1103
4	*	*	*	*
5	2001 :a60 : :89 :303	2001 :a60 : :89 :303	8767	8767
6	2001 :a60 :0 :217 : :1 :1	2001 :a60 :0 :217 : :1 :1	8767	8767
7	2001 :1578 :0 :ff : :1 :2	*	12657	*
8	2001 :1578 :400 :111 :1 :0 :85 :1	2001 :1578 :400 :111 :1 :0 :85 :1	35003	35003

pas ce qu'est “une série de sondes à haute vitesse”. Dans le cas des mesures de ping et traceroute, nous (la communauté et les opérateurs) disposons d'un signal pour définir une série de sondes non éthique : le taux limite. Dans cet article, nous faisons donc les contributions suivantes : (1) proposer une définition de l'éthique des mesures de ping et traceroute basé sur le taux limite. (2) énoncer les défis pour effectuer des mesures respectant notre définition.

2 Le taux limite comme mesure d'éthique

Le taux limite est le moyen qu'ont les opérateurs de spécifier que mesurer au-delà de ce taux est anormal. Des études précédentes ont montré que mesurer en dessous du taux limite limitait l'utilisation de ressources et n'affectait pas les résultats de mesures externes [VLA⁺20]. Dans ce contexte, nous proposons de définir qu'une mesure ping ou traceroute est éthique si elle minimise les dépassements du taux limite d'un équipement.

Cette définition est sujette à débat, mais a la qualité de définir une valeur mesurable, choisie par chaque opérateur, comme ce qu'il considère être un trafic anormal pour son réseau. Cependant, des études précédentes ont montré qu'une portion significative des opérateurs utilise une valeur de taux limite par défaut, qui ne reflète pas une volonté de limitation du trafic ping et traceroute. Pour aider les opérateurs dans le choix de ce paramètre, des études précédentes ont montré l'impact de séries de sondes à différentes vitesses de sondage sur les ressources consommées par les routeurs [VLA⁺20].

En faveur de notre définition, nous mentionnons que la mise en place d'un taux limite est obligatoire en IPv6 [DH17], et donc que le taux limite sera de plus en plus un facteur à prendre en compte par les différents acteurs qui effectuent des mesures dans internet.

3 Défis pour la construction d'un système de mesure plus éthique

La définition que nous proposons pour le cas particulier des mesures de type ping et traceroute est plus concrète que celles proposées auparavant, mais présente plusieurs défis de taille : (1) à moins que l'opérateur ne divulgue le taux limite configuré sur ses interfaces, celui ou celle qui mesure ne connaît pas le taux limite a priori. Le premier défi est donc de mesurer le taux limite des interfaces. (2) Si l'on connaît le taux limite des interfaces, encore faut-il imaginer des algorithmes de mesure qui respectent ce taux. Le second défi est donc de construire un système qui, avec une connaissance des taux limites, effectuera ses mesures pour essayer de ne jamais dépasser le taux limite.

Nous n'avons pas encore de solutions définitives et évaluées pour répondre à ces défis, mais nous décrivons des pistes pour construire des solutions et les problèmes auxquels elles seront confrontées.

3.1 Comment mesurer le taux limite d'une interface ?

Le taux limite peut grandement varier d'une interface à une autre, de quelques paquets par seconde à des dizaines de milliers [VLA⁺20].

Comme le signal du dépassement du taux limite est une perte (non-réponse à un paquet), des solutions qui semblent intéressantes sont des algorithmes comme le slow start (exponential increase) et/ou le AIMD (additional increase, multiplicative decrease) du protocole TCP.

Dans le cas de mesures de type ping, on peut directement appliquer ces algorithmes en sondant les destinations, comme ce sont les destinations elles-mêmes qui répondent aux paquets sondes. Dans le cas de mesures de type traceroute, le problème est différent, car les mesures sont indirectes : l'adresse destination du paquet sonde n'est pas l'adresse qui répond, et sans connaissances a priori, on ne sait pas quelle adresse va répondre. Une solution possible est donc d'effectuer des mesures initiales avec un taux de sondage conservatif (e.g., 100 pps) pour découvrir quelles interfaces correspondent à quelles sondes traceroutes. On pourra ensuite appliquer nos algorithmes inspirés de TCP pour mesurer le taux limite. Remarquons que même si ces algorithmes fonctionnent pour n'importe quel taux limite, il semble évident que mettre un taux de mesures maximum est nécessaire. Il est inutile d'envoyer des dizaines de milliers de paquets par seconde à une interface. Ces techniques semblent faisables, mais soulèvent plusieurs questions.

(1) Peut-on faire passer ces techniques à l'échelle ? Depuis 6 points de mesure, Gouel et al. trouvent que la topologie d'internet observable est composée d'au moins 3.3 millions d'interfaces [GVM⁺22]. Nous proposons l'estimation approximative suivante qui correspond à une infrastructure réaliste : nous avons 6 points de mesures qui peuvent sonder à 100,000 pps. Nous prenons un taux initial de 1 pps, un taux maximum de 128 pps et un facteur de multiplication exponentiel de 2. En faisant l'hypothèse qu'aucune interface n'ait un taux limite inférieur à 128 pps, et en supposant qu'on puisse distribuer équitablement le nombre d'interfaces entre nos 6 nœuds, le nombre de sondes à envoyer par interface est donc de $\sum_{k=1}^7 2^k = 254$, et donc le nombre total est de 838,200,000, soit 1,397 seconde, i.e., environ 23 minutes, un temps qui semble raisonnable.

(2) Comment être confiant qu'une perte correspond à un dépassement du taux limite ? Il se peut qu'une perte soit due à d'autres facteurs, comme la congestion, un changement de chemin vers un routeur qui ne répond pas du tout aux paquets sondes. On pourra sans doute s'aider de signaux correspondant aux deux phénomènes cités précédemment, comme l'augmentation de la variance de RTT pour la congestion, et les messages de mises à jour BGP collectés par les collecteurs publics, les changements de communautés BGP, ou même les changements de chemins dans les traceroutes publiques [GKF⁺20].

(3) Que faire si les mesures initiales deviennent invalides ? Même si les chemins d'internet sont globalement stables, il se peut que nos mesures initiales ne soient plus valides. En effet, avec 10M de préfixes /24 routés, un traceroute par préfixe, et en moyenne un chemin de traceroute qui comporte 15 interfaces, il faut environ 17 jours à 100 pps pour terminer ces mesures initiales. Des travaux récents ont montré que 16% des chemins étaient invalides après 17 jours [GKF⁺20]. Dans notre cas, on peut juste vérifier avant de lancer les mesures de taux limite qu'il existe au moins une sonde traceroute par interface qui est encore valide pour mesurer le taux limite de cette interface.

(4) Que faire lorsque le taux limite est implémenté par les routeurs en termes de bande passante utilisée par le trafic ping et traceroute ? Dans ce cas, tout le trafic ping et/ou traceroute, passé une certaine limite sera perdu sur le chemin au-delà du routeur qui applique cette règle. Nos études préliminaires montrent que ce n'est pas un phénomène courant [VLA⁺20] mais cela peut ajouter du temps aux mesures de taux limite des interfaces sur les chemins après ces routeurs car on ces routeurs représentent des goulots, et cela peut même rendre nos mesures de taux limite impossibles si les interfaces au-delà de ces routeurs ont un taux limite plus grand que ces routeurs.

3.2 Comment adapter la mesure pour ne pas dépasser le taux limite ?

Une fois qu'on aura déterminé le taux limite des interfaces, il faut ensuite adapter la mesure pour qu'elle ne déclenche pas ce taux limite. Pour ce faire, il faut ordonnancer les sondes pour que le taux de sondage d'une interface ne dépasse pas le taux limite, voire une fraction du taux limite pour être encore plus conservatif.

Comme précédemment, ceci est assez directement implémentable pour les sondes ping, mais cela est plus compliqué pour les traceroutes, car on ne sait pas à l'avance quelle interface va répondre à une sonde traceroute. On peut cependant utiliser les résultats des mesures initiales pour obtenir la correspondance entre sondes traceroute et interfaces qui répondent. Ici, on se heurte néanmoins à plusieurs problèmes.

(1) Comme vu précédemment, les chemins d'internet sont dynamiques (bien que globalement stables), ce qui peut perturber notre algorithme. En effet, par exemple, si un chemin change et que la sonde traceroute passe désormais par une interface que l'on sondait précédemment était proche de son taux limite, cette

nouvelle sonde peut déclencher le taux limite. Une approche peu précise, mais simple, consiste à prédire que l'interface qui va répondre est celle qui a répondu précédemment. Étant donné la stabilité des chemins d'internet, si on arrive à obtenir des informations régulières sur des sondes traceroutes depuis la même source vers la même destination (e.g., à une échelle de quelques minutes), on risque de peu se tromper. Une approche plus précise, mais qui demande plus de réflexion, consiste à tenter de prédire quelle interface va répondre à une sonde traceroute. C'est la partie la plus exploratoire de notre travail et nous réfléchissons encore au meilleur moyen d'aborder le problème, mais peut être que des approches à base d'apprentissage sur les changements de chemins est une piste. En effet, on peut restreindre l'ensemble de chemins possibles vers lequel un chemin peut changer à partir de la topologie existante, en supposant que l'on possède une vue assez complète des chemins depuis une source, hypothèse raisonnable étant donné la stabilité des chemins d'internet [GKF⁺20].

(2) Le deuxième problème est le même que pour la mesure du taux limite : comment peut-on être confiant qu'une perte corresponde à un dépassement du taux limite ? La solution réside peut-être dans un modèle statistique basé sur des mesures précédentes vers ces interfaces, qui pourraient dire si un certain taux de perte est probable ou non.

(3) Enfin, que faire lorsque le taux limite est déclenché malgré nos efforts ? Il faut alors diminuer le sondage sur certaines interfaces, qui va soit allonger le temps de mesure, ou alors, si on décide de ne pas envoyer toutes les sondes, réduire la complétude des données. Il faudra alors choisir quelles sondes on décide de ne pas envoyer. Là, on pourra sans doute donner plusieurs cas d'utilisation et choisir les sondes à ne pas envoyer en fonction de ces cas (e.g., maximisation de la découverte de topologie dans certaines parties du réseau, ou maximisation du nombre de chemins complets).

4 Conclusion

Nous avons montré dans cet article la nécessité de se questionner sur l'éthique des mesures d'internet à haute vitesse. Nous proposons que le taux limite d'un routeur devienne partie intégrante de la définition de l'éthique et avons énoncé les défis de recherches et des pistes de solutions pour concevoir des techniques de mesures qui minimiseront les dépassements du taux limite.

Références

- [Bev16] R. Beverly. Yarrp'ing the internet : Randomized high-speed active topology discovery. In *ACM IMC*, 2016.
- [DH17] S. Deering and R. Hinden. Rfc 8200 : internet protocol, version 6 (ipv6) specification, 2017.
- [GKF⁺20] V. Giotsas, T. Koch, E. Fazzion, I. Cunha, M. Calder, H. V Madhyastha, and E. Katz-Bassett. Reduce, reuse, recycle : Repurposing existing measurements to identify stale traceroutes. In *ACM IMC*, 2020.
- [GVM⁺22] M. Gouel, K. Vermeulen, M. Mouchet, J. P Rohrer, O. Fourmaux, and T. Friedman. Zeph & iris map the internet : A resilient reinforcement learning approach to distributed ip route tracing. *ACM SIGCOMM CCR*, 2022.
- [KD12] E. Kenneally and D. Dittrich. The menlo report : Ethical principles guiding information and communication technology research. Available at *SSRN 2445102*, 2012.
- [PA16] C. Partridge and M. Allman. Ethical considerations in network measurement papers. *Communications of the ACM*, 2016.
- [VLA⁺20] K. Vermeulen, B. Ljuma, V. Addanki, M. Gouel, O. Fourmaux, T. Friedman, and R. Rejaie. Alias resolution based on icmp rate limiting. In *PAM*. Springer, 2020.
- [VRB⁺20] K. Vermeulen, J. P Rohrer, R. Beverly, O. Fourmaux, and T. Friedman. Diamond-Miner : Comprehensive Discovery of the internet's Topology Diamonds. In *Usenix NSDI*, 2020.