Groupe de travail Réseau
Request for Comments : 2330
Catégorie : Information
Traduction Claude Brière de L'Isle

V. Paxson, Lawrence Berkeley National Lab
G. Almes, Advanced Network & Services
J. Mahdavi & M. Mathis, Pittsburgh Supercomputer Center
mai 1998

Cadre pour les métriques de performances IP

1. Statut de ce mémoire

Le présent mémoire apporte des informations pour la communauté de l'Internet. Il ne spécifie aucune forme de norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction

2. Notice de copyright

Table des matières

3. Introduction

L'objet du présent mémoire est de définir un cadre général pour les métriques particulières à développer par l'initiative pour les métriques de performances IP de l'IETF, commencée par le groupe de travail Méthodologie de recherche des meilleures pratiques (BMWG, *Benchmarking Methodology Working Group*) de la zone Exigences de fonctionnement, et poursuivie par le groupe de travail Métriques des performances IP (IPPM, *IP Performance Metrics*) de la zone Transport.

On commence par poser plusieurs critères pour les métriques qu'on adopte. Ces critères sont conçus pour promouvoir une

initiative IPPM qui va maximiser une compréhension commune précise par les usagers de l'Internet et les fournisseurs de l'Internet des performances et de la fiabilité à la fois des chemins de bout en bout à travers l'Internet et des "nuages IP" spécifiques qui comportent des portions de ces chemins.

On définit ensuite du vocabulaire Internet qui nous permettra de parler avec clarté des composants Internet tels que les routeurs, les chemins, et les nuages.

Nous définirons ensuite les concepts fondamentaux de la 'métrique' et de la 'méthodologie de mesure', qui nous permettront de parler avec clarté des questions de mesures. Compte tenu de ces concepts, nous poursuivrons l'exposé par l'importante question des incertitudes et erreurs de mesure, et développerons la notion clé assez subtile de la façon dont elles se rapportent au cadre analytique partagé par de nombreux aspects de la discipline d'ingénierie de l'Internet. On introduira alors la notion de métrique définie empiriquement, et finirons cette partie du document par un exposé général sur la façon dont les métriques peuvent être 'composées'.

Le reste du document traite de diverses questions qui se rapportent à la définition de métriques et méthodologies adaptées : comment s'accommoder d'horloges imparfaites, la notion d'une 'heure du réseau' distincte de 'l'heure de l'hôte', comment agréger des ensembles de métriques de singletons en échantillons et déduire des statistiques sensées de ces échantillons, pourquoi il est recommandé d'éviter de voir les propriétés de l'Internet en termes de probabilités (comme la probabilité d'abandon d'un paquet) car ces termes incluent souvent une hypothèse implicite sur le comportement du réseau, l'utilité de définir des métriques en termes de paquets d'un type générique, les avantages de préférer les adresses IP aux noms d'hôte du DNS, et la notion de paquets 'en forme standard'. Un appendice expose le test de Anderson-Darling pour jauger si un ensemble de valeurs correspond à une certaine distribution statistique, et donne le code C pour la mise en œuvre de l'essai.

Dans certains paragraphes du présent mémoire, on a entouré certains commentaires d'accolades {Commentaire : ... }. On souligne que ces commentaires ne sont que des commentaires, et ne font pas, par eux-mêmes partie du document cadre ni d'une proposition de métrique particulière. Dans certains cas, ce commentaire va exposer certaines des propriétés de métriques qui pourraient être envisagées, mais le lecteur devrait supposer que ce type d'exposé n'est destiné qu'à éclairer des points du document cadre, et non pas à suggérer une métrique spécifique.

4. Critères pour les métriques de performances IP

Le but majeur de l'initiative pour les métriques de performances IP est de réaliser une situation dans laquelle les usagers et les fournisseurs de service de transport Internet aient une compréhension précise communes des performances et de la fiabilité des "nuages" de composants Internet qu'ils utilisent/fournissent.

Pour réalise cela, des métriques de performances et de fiabilité pour les chemins à travers l'Internet doivent être développées. Des critères pour ces métriques ont été spécifiés dans plusieurs réunions de l'IETF :

+ les métriques doivent être concrètes et bien définies,
+ une méthodologie pour une métrique devrait avoir la propriété d'être répétable : si la méthodologie est utilisée plusieurs fois dans des conditions identiques, les mêmes mesures devraient résulter en les mêmes mesures,
+ les métriques ne doivent pas présenter de biais pour les nuages IP mis en œuvre avec des technologies identiques,
+ les métriques doivent présenter des biais compris et équitables pour les nuages IP mis en œuvre avec des technologies non identiques,
+ les métriques doivent être utiles pour que les usagers et les fournisseurs comprennent les performances qu'ils subissent ou fournissent,
+ les métriques doivent éviter d'induire des objectifs de performances artificiels.

5. Terminologie pour chemins et nuages

La liste suivante définit des termes qui doivent être précisés pour le développement des métriques de chemins. On commence par les notions basiques de 'hôte', 'routeur', et 'liaison', puis on passe à la définition des notions de 'chemin', de 'nuage IP', et de 'commutateur' qui nous permettent de segmenter un chemin en ses composantes pertinentes.

hôte : ordinateur capable de communiquer en utilisant les protocoles Internet ; cela inclut les "routeurs".

liaison : connexion au niveau d'une seule liaison entre deux hôtes (ou plus) ; cela inclut des liaisons louées, des ethernets, des nuages en relais de trame, etc.

routeur : hôte qui facilite la communication de niveau réseau entre des hôtes en transmettant les paquets IP.

chemin : séquence de la forme < h0, l1, h1, ..., ln, hn >, où n ≥ 0, chaque hi est un hôte, chaque li est une liaison entre hi-1 et hi, chaque h1...hn-1 est un routeur. Une paire <li, hi> est appelée un 'bond'. Dans une configuration de fonctionnement appropriée, les liaisons et les routeurs dans le chemin facilitent la communication de niveau réseau des paquets qui vont de h0 à hn. Noter que le concept de chemin est unidirectionnel.

sous-chemin : sur un certain chemin, un sous-chemin est toute sous-séquence de ce chemin qui est elle-même un chemin. (Donc, le premier et le dernier élément d'un sous-chemin est un hôte.)

nuage : c'est un graphe non dirigé (éventuellement cyclique) dont les sommets sont les routeurs et les bords sont des liaisons qui connectent des paires de routeurs. Formellement, les ethernets, les nuages de relais de trame, et les autres liaisons qui connectent plus de deux routeurs sont modélisés comme des maillages pleinement connectés de bords de graphes. Noter que se connecter à un nuage signifie se connecter à un routeur de ce nuage par une liaison ; cette liaison ne fait pas par elle-même partie du nuage.

commutateur : cas particulier de liaison, un commutateur connecte directement un hôte à un nuage et/ou un nuage à un autre nuage.

sous-chemin de nuage : c'est un sous-chemin d'un certain chemin, dont tous les hôtes sont les routeurs d'un certain nuage.

résumé de chemin : séquence de la forme < h0, e1, C1, ..., en, hn >, où n ≥ 0, h0 et hn sont des hôtes, chaque e1 ... en est un commutateur, et chaque C1 ... Cn-1 est un sous chemin de nuage.

6. Concepts fondamentaux

6.1 Métriques

Dans le fonctionnement de l'Internet, plusieurs quantités se rapportent aux performances et à la fiabilité de l'Internet, et on aimerait en connaître la valeur. Lorsque une telle quantité est spécifiée avec soin, on appelle cette quantité une métrique. On prévoit qu'il y aura des RFC différentes pour chaque métrique (ou pour chaque groupe de métriques étroitement apparentées).

Dans certains cas, il pourrait n'y avoir pas de moyen évident de mesurer efficacement la métrique ; cela est permis, et même compris comme très utile dans certains cas. Il est cependant exigé que la spécification de la métrique soit aussi claire que possible quant à la quantité qui est spécifiée. Donc, la difficulté de la mesure pratique est parfois permise, mais l'ambiguïté dans la signification ne l'est pas.

Chaque métrique sera définie en termes d'unités de mesure standard. La métrique internationale sera utilisée, et on souligne les points particulier suivants :

+ Lorsque une unité est exprimée en simples mètres (pour les distances/longueurs) ou secondes (pour les durées) les unités en rapport appropriées fondées sur les milliers ou les millièmes des unités acceptables sont acceptables. Donc, les distances exprimées en kilomètres (km), les durées exprimées en millisecondes (ms), ou microsecondes (µs) sont permises, mais pas les centimètres (parce que le préfixe n'est pas exprimé en termes de milliers ou de millièmes).
+ Lorsque une unité est exprimée dans une combinaison d'unités, les unités appropriées qui s'y rapportent sur la base de milliers ou millièmes d'unités acceptables sont acceptables, mais tous ces milliers/millièmes doivent être groupés au début. Donc, les kilomètres par seconde (km/s) sont permis, mais les mètres par milliseconde ne le sont pas.
+ l'unité d'information est le bit.
+ Lorsque des préfixes de métrique sont utilisés avec des bits ou avec des combinaisons qui incluent des bits, ces préfixes auront leur signification métrique (par rapport au 1000 décimal) et non la signification conventionnelle de la mémorisation informatique (qui se rapporte au décimal 1024). Dans toute RFC qui définit une métrique dont les unités comportent des bits, cette convention devra être suivie et sera répétée pour être claire pour le lecteur.
+ Lorsque une heure sera donnée, elles sera exprimée en UTC.

Noter que ces points s'appliquent aux spécifications des métriques et non, par exemple, aux formats de paquets où des octets seront probablement utilisés de préférence ou en plus des bits.

Finalement, on note que certaines métriques peuvent être définies purement en termes d'autres métriques ; de telles métriques sont appelées des 'métriques dérivées'.

6.2 Méthodologie des mesures

Pour un certain ensemble de métriques bien définies, il peut exister des méthodologies de mesure distinctes. Une liste partielle inclut :

+ Des mesures directes d'une métrique des performances utilisant du trafic d'essai injecté. Par exemple, des mesures du délai d'aller-retour d'un paquet IP d'une certaine taille sur un certain chemin à un moment donné.
+ La projection d'une métrique à partir de mesures à un niveau inférieur. Par exemple; étant données des mesures précises du délai de propagation et de la bande passante pour chaque étape le long d'un chemin, la projection du délai complet pour le chemin pour un paquet IP d'une certaine taille.
+ L'estimation d'une métrique constitutive à partir d'un ensemble de mesures plus agrégées. Par exemple, étant données des mesures précises du délai pour un certain chemin d'un seul bond pour des paquets IP de différentes tailles, l'estimation du délai de propagation pour la liaison de ce chemin à un bond.
+ L'estimation d'une certaine métrique à un moment donnés à partir d'un ensemble de métriques en rapport à d'autres moments. Par exemple, étant donnés des mesures précises d'une capacité de flux dans le passé, ainsi qu'un ensemble de mesures de délai précises pour ce temps passé et pour le présent, et en fonction d'un modèle de dynamique de flux, estimer la capacité de flux qui serait observé à présent.

Cette liste n'est en aucun cas exhaustive. Son objet est de souligner la diversité des techniques de mesure.

Lorsque une certaine métrique est spécifiée, on peut noter et discuter une certaine approche de mesure. Cette approche ne fait cependant pas partie de la présente spécification.

Une méthodologie pour une métrique devrait avoir pour propriété d'être répétable : si la méthodologie est utilisée de multiples fois dans des conditions identiques, elle devrait résulter en des mesures cohérentes.

En revenant un peu sur le mot 'identique' dans le paragraphe précèdent, on pourrait utiliser plus précisément le mot 'continuité' pour décrire une propriété d'une certaine méthodologie : une méthodologie pour une certaine métrique fait preuve de continuité si, pour de faibles variations des conditions, elle résulte en faibles variations des mesures résultantes. Un petit peu plus précisément, pour chaque epsilon positif, il existe un delta positif, tel que si deux ensembles de conditions présentent une différence l'un envers l'autre, les mesures résultantes seront dans un écart d'epsilon l'une par rapport à l'autre. À ce point, cela devrait être pris comme une heuristique guidant notre intuition vers une propriété de robustesse plutôt qu'une notion précise.

Une métrique qui a au moins une méthodologie qui fait preuve de continuité est dite elle-même faire preuve de continuité.

Noter que certaines métriques, telles que le compte de bonds le long d'un chemin, sont des valeurs d'entier et ne peuvent donc pas faire preuve de continuité dans le sens donné ci-dessus.

Noter de plus que, en pratique, il peut n'être pas facile de savoir (ou d'être capable de quantifier) les conditions pertinentes pour une mesure à un moment donné. Par exemple, dans la mesure où la charge instantanée (en paquets à servir) sur un certain routeur dans un réseau de grande zone à débit élevé peut varier considérablement sur des périodes relativement brèves et qu'il sera très difficile à un observateur externe de la quantifier, diverses statistiques d'une certaine métrique peuvent être plus répétables, ou faire mieux preuve de continuité. Dans ce cas, ces statistiques particulières devraient être spécifiées lorsque la métrique est spécifiée.

Finalement, certaines méthodologies de mesure peuvent être 'prudentes' en ce sens que l'acte de mesure ne modifie pas, ou ne modifie que peu, la valeur de la métrique de performances que la méthodologie tente de mesurer. {Commentaire : par exemple, dans un réseau de large zone à haut débit sous une charge modeste, un essai utilisant plusieurs petits paquets de 'ping' pour mesurer le délai ne va vraisemblablement pas interférer (beaucoup) avec les propriétés de débit de ce réseau, telles qu'observées par un observateur extérieur. La déclaration équivalente concernant des essais qui utiliseraient de gros flux pour mesurer une capacité de flux serait probablement fausse.}

6.3 Mesures, incertitudes, et erreurs

Même les meilleures méthodologies de mesure pour les métriques du meilleur comportement peuvent présenter des erreurs. Ceux qui développent de telles méthodologies de mesure devraient cependant s'efforcer de :
+ minimiser leurs incertitudes/erreurs,
+ comprendre et documenter les sources d'incertitude/erreur, et
+ de quantifier le nombre des incertitudes/erreurs.

Par exemple, lorsque on développe une méthode de mesure de délai, comprendre comment toute erreur d'horloge introduit des erreurs de la mesure de délai, et quantifier cet effet autant qu'on le peut. Dans certains cas, il va en résulter une exigence d'une horloge d'au moins une certaine qualité si elle doit être utilisée pour faire une certaine mesure.

Comme second exemple, considérons l'erreur temporelle due à des redondances de mesure au sein de l'ordinateur qui fait la mesure, par opposition aux délais du composant Internet mesuré. La première est une erreur de mesure, alors que la

seconde reflète la métrique qui nous intéresse. Noter qu'une technique qui peut aider à éviter cette redondance est d'utiliser un filtre/renifleur de paquet, fonctionnant sur un ordinateur distinct qui enregistre les paquets du réseau et les horodate avec précision (voir ci-dessous l'exposé sur l'heure du réseau). La trace résultante peut alors être analysée pour assurer le trafic d'essai, minimisant l'effet des délais de l'hôte de mesure, ou permettant au moins de tenir compte de ces délais. On note que cette technique peut se révéler bénéfique même si le filtre/renifleur de paquet fonctionne sur la même machine, parce que de telles mesures donnent généralement un horodatage "au niveau du noyau", par opposition à l'horodatage moins précis du "niveau application".

Finalement, on note que les métriques dérivées (définies plus haut) ou les métriques qui affichent des composants spatiaux ou temporels (définis plus loin) offrent une occasion particulière pour l'analyse des incertitudes de mesure, à savoir comment se propagent les incertitudes (au niveau conceptuel) du fait de la dérivation ou de la composition.

7. Métriques et cadre analytique

Comme l'Internet a évolué depuis les premières études sur la commutation de paquets des années 1960, la communauté de l'ingénierie de l'Internet a fait évoluer le cadre analytique commun des concepts. Ce cadre analytique, ou trame A, utilisé par les concepteurs et les développeurs de protocoles, par ceux qui sont impliqués dans les mesures, et par ceux qui étudient les performances des réseaux informatiques en utilisant les outils de simulation et d'analyse, a grandement facilité notre travail. Un objectif majeur est ici de générer des caractérisations de réseau qui soient cohérentes à la fois dans les réglages analytiques et pratiques, car cela va maximiser les chances que les études de réseau non empiriques puissent être mieux corrélées, et utilisées, pour notre meilleure compréhension du comportement réel du réseau.

Chaque fois que possible, nous aimerions donc développer et nous appuyer sur la trame A. Donc, chaque fois qu'une métrique à spécifier est comprise comme se rapportant étroitement à des concepts inclus dans la trame A, nous allons tenter de spécifier la métrique dans les termes de la trame A. Dans une telle spécification, nous allons développer la trame A en définissant précisément les concepts nécessaires pour la métrique, puis s'appuyer sur la trame A en définissant la métrique dans les termes de ces concepts.

Une telle métrique est appelée "métrique spécifiée analytiquement" ou, plus simplement, une métrique analytique.

{Commentaire : des exemples de telles métriques analytiques pourraient inclure :
- le temps de propagation d'une liaison
  C'est le temps, en secondes, requis par un seul bit pour voyager de l'accès de sortie d'un hôte Internet à travers une seule liaison à un autre hôte Internet.
- la bande passante d'une liaison pour des paquets de taille k
  C'est la capacité, en bit/s, où seuls les bits du paquet IP sont comptés, pour les paquets de taille k octets.
- le chemin
  C'est le chemin, comme défini à la Section 5, de A à B à un moment donné.
- le compte de bonds d'un chemin
  C'est la valeur 'n' du chemin.}

Noter qu'on ne fait pas une liste à priori des concepts de trame A qui vont apparaître dans ces spécifications, mais on encourage à leur utilisation en insistant pour qu'ils soient spécifiés avec soin afin que lorsque se développera notre ensemble de métriques, se développe aussi un ensemble de concepts de trame A spécifié de façon techniquement cohérente les uns avec les autres et en harmonie avec la compréhension courante de ces concepts au sein de la communauté générale de l'Internet.

Ces concepts de trame A seront destinés à s'abstraire des composants réels de l'Internet de telle façon que :
+ la fonction essentielle du composant soit conservée,
+ les propriétés du composant pertinentes pour les métriques dont la création est visée soient conservées,
+ un sous-ensemble de ces propriétés de composant soient potentiellement définies comme des métriques analytiques, et
+ que soient écartées les propriétés des composants réels de l'Internet qui ne sont pas pertinentes pour la définition des métriques dont la création est visée.

Par exemple, lorsque on considère un routeur dans le contexte de la transmission de paquets, on peut modéliser le routeur comme un composant qui reçoit des paquets sur une liaison entrante, les met en file d'attente selon le principe FIFO dans une file d'attente de taille finie, emploie l'abandon des paquets de queue lorsque la file d'attente est pleine, et les transmet sur une liaison de sortie. La vitesse de transmission (en bit/s) des liaisons d'entrée et de sortie, la latence dans le routeur (en secondes) et la taille maximum de la file d'attente des paquets (en bits) sont des métriques analytiques pertinentes.

Dans certains cas, de telles métriques analytiques utilisées en relation avec un routeur vont être en relation très étroite avec des métriques spécifiques des performances des chemins de l'Internet. Par exemple, une formule (L + P/B) évidente qui

implique la latence dans le routeur (L), la taille de paquet (en bits) (P) et la vitesse de transmission de la liaison sortante (B) peuvent approximer de près l'augmentation du délai des paquets due à l'insertion d'un certain routeur dans le chemin.

On souligne cependant que des concepts de trame A bien choisis et bien spécifiés et leurs métriques analytiques vont prendre en charge des initiatives de création de métriques plus générales de façons moins évidentes.

{Commentaire : par exemple, lorsque on considère la capacité de flux d'un chemin, il peut être très intéressant d'être capable de modéliser chacun des routeurs le long du chemin comme transmetteur de paquets comme ci-dessus. Les techniques pour estimer la capacité de flux d'un chemin peuvent utiliser la taille maximum de file d'attente des paquets comme paramètre par des moyens incontestablement non évidents. Par exemple, lorsque la taille maximum de file d'attente augmente, ainsi fait la capacité du routeur à faire passer de façon continue le trafic le long d'une liaison sortante en dépit des fluctuations du trafic provenant d'une liaison entrante. Estimer cette augmentation reste cependant un sujet de recherches.}

Noter que, lorsque on spécifie des concepts de trame A et des métriques analytiques, on va inévitablement simplifier les hypothèses. Le rôle clé de ces concepts est d'abstraire des composants Internet les propriétés qui sont pertinentes pour une certaine métrique. Il faut faire attention d'éviter de faire des hypothèses qui biaisent la modélisation et l'essai de métrique en faveur d'un type de conception.

{Commentaire : par exemple, les routeurs pourraient ne pas utiliser l'abandon de la queue de la file d'attente, bien que cela soit plus facile à modéliser analytiquement.}

Finalement, on notera que différents éléments de la trame A pourraient bien faire différentes hypothèses simplificatrices. Par exemple, l'abstraction d'un routeur utilisée pour approfondir la définition du délai de chemin pourrait traiter la file d'attente de paquets du routeur comme une seule file d'attente FIFO, mais l'abstraction d'un routeur utilisée pour approfondir la définition du traitement d'un paquet à capacité RSVP pourrait traiter la file d'attente de paquets du routeur comme subissant des délais bornés – ce qui est une hypothèse contradictoire. Ce n'est pas pour dire de faire des hypothèses contradictoires au même moment, mais que deux parties différentes de notre travail peuvent pousser le plus simple concept de base dans des voies divergentes pour des objets différents.

{Commentaire : en termes plus mathématiques, on dirait que la trame A prise comme un tout n'est pas nécessairement cohérente, mais que l'ensemble des éléments d'une trame A particulière utilisés pour définir une métrique particulière doit l'être.}

8. Métriques spécifiées de façon empirique

Il y a des métriques de performances et de fiabilité utiles qui ne rentrent pas aussi nettement dans le cadre de la trame A, habituellement parce que la trame A n'a pas le pouvoir ou le degré de détail permettant de les traiter. Par exemple, il serait bon d'être capable de mesurer "la meilleure capacité de flux réalisable le long d'un chemin utilisant un TCP conforme à la RFC-2001", mais on a pas de cadre analytique assez riche pour nous permettre de faire de cette capacité de flux une métrique analytique.

Ces notions peuvent très bien être spécifiées en décrivant plutôt une méthodologie de référence pour les mesurer.

On appellera une telle métrique "métrique spécifiée empiriquement", ou plus simplement, une métrique empirique.

De telle métriques empiriques devraient avoir trois propriétés :
+ on devrait avoir une définition claire pour chacune, en termes de composants Internet,
+ on devrait avoir au moins un moyen efficace de les mesurer, et
+ dans la mesure du possible, on devrait avoir une compréhension (nécessairement incomplète) de cette métrique en termes de trame A, afin qu'on puisse utiliser nos mesures pour raisonner sur les performances et la fiabilité des composants de trame A et des agrégations de composants de trame A.

9. Deux formes de composition

9.1 Composition spatiale des métriques

Dans certains cas, il peut être réaliste et utile de définir des métriques de telle façon qu'elles présentent une composition spatiale.

Par composition spatiale, on entend une caractéristique de certaines métriques de chemins dans lesquelles la métrique telle

qu'appliquée à un chemin (complet) peut aussi être définie pour divers sous-chemins, et dans lesquels les concepts appropriés de trame A pour la métrique suggèrent d'utiles relations entre la métrique appliquée à ces divers sous-chemins (y compris le chemin complet, les divers nuages de sous-chemins d'un certain schéma de chemin, et même de routeurs seuls le long du chemin). La réalité de la composition spatiale dépend :

+ de l'effectivité de l'analyse de ces relations telles qu'appliquées aux composants de trame A pertinents,
+ de l'utilisation pratique des relations correspondantes telles qu'appliquées aux métriques et aux méthodologies de mesure.

{Commentaire : par exemple, considérons certaines métriques pour le délai d'un paquet de 100 octets à travers un chemin P, et considérons de plus un schéma de chemin <h0, e1, C1, ..., en, hn> de P. La définition d'une telle métrique pourrait inclure la conjecture que le délai à travers P est très proche de la somme de la métrique correspondante à travers les commutateurs (ei) et les nuages (Ci) de ce schéma de chemin. La définition inclurait de plus une note sur la façon dont une relation correspondante s'applique aux composants de trame A pertinents, à la fois pour le chemin P et pour les commutateurs et nuages du schéma de chemin.}

Lorsque la définition d'une métrique inclut une conjecture que la métrique à travers le chemin est en rapport avec la métrique à travers les sous-chemins, cette conjecture constitue une preuve que la métrique affiche une composition spatiale. La définition devrait alors inclure :

+ la conjecture spécifique appliquée à la métrique,
+ une justification de l'utilité pratique de la composition en termes de réalisation de mesures précises de la métrique sur le chemin,
+ une justification de l'utilité de la composition en termes de réalisation d'analyse du chemin en utilisant plus efficacement les concepts de trame A, et
+ une analyse de comment la conjecture pourrait être incorrecte.

9.2 Composition temporelle des modèles formels et métriques empiriques

Dans certains cas, il peut être réaliste et utile de définir des métriques de telle façon qu'elles aient une composante temporelle.

Par composante temporelle, on entend une caractéristique de certaines métriques de chemin dans lesquelles la métrique telle qu'appliquée à un certain chemin au moment T est aussi définie pour divers instants $t0 < t1 < ... < tn < T$, et dans lesquels les concepts de trame A appropriés pour la métrique suggèrent des relations utiles entre la métrique appliquée aux instants t0, ..., tn et celle appliquée à l'instant T. L'efficacité de la composante temporelle dépend :

+ de l'utilité de l'analyse de ces relations, telles qu'appliquées aux composantes pertinentes de trame A, et
+ de l'utilisation pratique des relations correspondantes telles qu'appliquées aux métriques et méthodologies de mesure.

{Commentaire : par exemple, considérons une métrique pour la capacité de flux attendue à travers un chemin P durant la période de cinq minutes qui entoure l'instant T, et supposons de plus que nous avons les valeurs correspondantes pour chacune des quatre périodes de cinq minutes précédentes, t0, t1, t2, et t3. La définition d'une telle métrique pourrait inclure une conjecture que la capacité du flux à l'instant T peut être estimée par un certain type d'extrapolation à partir des valeurs de t0, ..., t3. La définition inclurait de plus une note sur la façon dont une relation correspondante s'applique aux composants de trame A pertinents.

Note : Toute composante (spatiale ou temporelle) qui implique une capacité de flux va vraisemblablement être subtile, et les composantes temporelles sont généralement plus subtiles que les spatiales, de sorte que le lecteur devrait comprendre que l'exemple ci-dessus est volontairement très simplifié.}

Lorsque la définition d'une métrique comporte une conjecture que la métrique à travers le chemin à l'instant T se rapporte à la métrique à travers le chemin pour un ensemble d'autres instants, cette conjecture constitue une preuve que cette métrique présente des composantes temporelles. Sa définition devrait alors inclure :

+ la conjecture spécifique qui s'applique à la métrique,
+ une justification de l'utilité pratique de la composante en termes de précision de mesure de la métrique sur le chemin, et
+ une justification de l'utilité de la composante en termes d'analyse plus efficace du chemin avec les concepts de trame A.

10. Questions en rapport avec l'heure

10.1 Problèmes d'horloges

Les mesures d'heure sont au cœur de nombreuses métriques de l'Internet. À cause de cela, elles seront souvent cruciales lors de la conception d'une méthodologie de mesure d'une métrique pour comprendre les différents types d'erreurs et d'incertitudes introduits par des horloges imparfaites. Dans cette section, on définit la terminologie pour discuter des

caractéristiques des horloges et on traite des questions de mesure en rapport qui doivent être abordées par toute méthodologie adaptée.

Le protocole de l'heure du réseau (NTP, *Network Time Protocol*) [RFC1305] définit une nomenclature pour discuter des caractéristiques des horloges qu'on utilisera aussi lorsque approprié [Mi92]. L'objectif principal de NTP est de fournir un moyen de garder une référence horaire précise sur de très longues échelles de temps, comme des minutes ou des jours, alors que pour les besoins des mesures, ce qui est souvent le plus important est la précision à court terme, entre le début de la mesure et sa fin, ou pendant le cours du rassemblement d'un corps de mesures (un échantillon). Cette différence dans les objectifs conduit parfois aussi à des définitions différentes de terminologie, comme on l'expose ci-dessous.

Pour commencer, on définit le "décalage" d'une horloge à un certain moment comme la différence entre l'instant rapporté par l'horloge et l'heure "vraie" telle que définie par l'UTC. Si l'horloge rapporte une heure Tc et que l'heure vraie est Tt, le décalage de l'horloge est alors Tc - Tt.

On dira qu'une horloge est "précise" à un instant particulier si le décalage d'horloge est zéro, et plus généralement la "précision" d'une horloge est la proximité de la valeur absolue du décalage par rapport à zéro. Pour NTP, la précision inclut aussi une notion de fréquence de l'horloge ; pour notre propos, nous incorporons plutôt cette notion dans celle de "biais", parce que nous définissions la précision en fonction d'un seul instant plutôt que sur un intervalle de temps.

Le "biais" d'horloge à un instant particulier est la différence de fréquence (dérivée première de son décalage par rapport à l'heure vraie) entre l'horloge et l'heure vraie.

Comme noté dans la RFC1305, les horloges réelles affichent une certaine variation de biais. C'est-à-dire que la dérivée seconde du décalage d'horloge par rapport à l'heure vraie est généralement différente de zéro. En suivant la RFC1305, on définit cette quantité comme la "dérive" d'horloge.

La "résolution" d'une horloge est la plus petite unité avec laquelle est mise à jour l'heure de l'horloge. Elle donne la limite inférieure de l'incertitude de l'horloge. (Noter que les horloges peuvent avoir de très fines résolutions et donc être très imprécises.) La résolution est définie en termes de secondes. Cependant, la résolution se rapporte à l'heure rapportée par l'horloge et non à l'heure vraie, de sorte que par exemple une résolution de 10 ms signifie seulement que l'horloge met à jour sa notion de l'heure en incréments de 0,01 seconde, et non que c'est la vraie quantité de temps entre les mises à jour.

{Commentaire : Les systèmes diffèrent sur la façon dont une interface d'application de l'horloge rapporte l'heure sur les appels suivants durant lesquels l'horloge n'a pas avancé. Certains systèmes retournent simplement la même heure inchangée comme donnée sur les appels précédents. D'autres peuvent ajouter un petit incrément du temps rapporté pour conserver un accroissement monotone de l'horodatage. Pour les systèmes qui suivent cette dernière méthode, on ne prend *pas* en compte ces petits incréments lorsque on définit la résolution de l'horloge. Ils sont plutôt un obstacle à l'estimation de la résolution de l'horloge, car une méthode naturelle pour le faire est d'interroger de façon répétée l'horloge pour déterminer la plus petite différence positive des heures rapportées.}

On s'attend à ce que la résolution d'une horloge ne change que rarement (par exemple, du fait d'une mise à niveau du matériel).

Il y a un certain nombre de métriques intéressantes pour lesquelles des méthodologies de mesure naturelles impliquent de comparer les heures rapportées par deux horloges différentes. Un exemple en est le délai unidirectionnel de paquet [AK97]. Ici, le temps exigé pour qu'un paquet voyage à travers le réseau est mesuré en comparant l'heure rapportée par une horloge à une extrémité du chemin du paquet, ce qui correspond au moment où le paquet est entré en premier dans le réseau, à l'heure rapportée par une horloge à l'autre extrémité du chemin, ce qui correspond au moment où le paquet a fini de traverser le réseau.

Nous sommes donc aussi intéressés par la terminologie de description de la façon dont deux horloges C1 et C2 se comparent. Pour ce faire, on introduit les termes qui se rapportent à ceux de ci-dessus dans lesquels la notion de "heure vraie" est remplacée par l'heure telle que rapportée par l'horloge C1. Par exemple, le décalage de l'horloge C2 par rapport à C1 à un instant particulier est Tc2 - Tc1, la différence instantanée des heures rapportées par C2 et C1. Pour ôter toute ambiguïté entre l'utilisation des termes pour comparer deux horloges par rapport à l'utilisation des termes pour se comparer à l'heure vraie, on va dans le premier cas utiliser le mot "relatif". Ainsi, le décalage défini plus tôt dans ce paragraphe est le "décalage relatif" entre C2 et C1.

Lorsque on compare les horloges, l'analogue de "résolution" n'est pas "la résolution relative", mais plutôt la "résolution conjointe", qui est la somme de la résolution de C1 et de C2. La résolution conjointe indique alors une borne inférieure prudente de la précision à tout intervalle de temps calculé en soustrayant les horodatages générés par une horloge de ceux générés par l'autre.

Si deux horloges sont "précises" l'une par rapport à l'autre (si leur décalage relatif est zéro) on dira que cette paire d'horloges est "synchronisée". Noter que des horloges peuvent être extrêmement synchronisées tout en étant arbitrairement imprécises en termes de représentation de l'heure vraie. Ce point est important parce que pour de nombreuses mesures de l'Internet, la synchronisation entre deux horloges est plus importante que la précision des horloges. C'est aussi assez vrai des biais, pour autant que le biais absolu ne soit pas trop grand, le biais minimal relatif est plus important, car il peut induire une tendance systématique dans les temps de transit des paquets mesurés par comparaison des horodatages produits par les deux horloges.

Ces distinctions se font jour parce que pour les mesures Internet, ce qui est souvent le plus important sont les différences de temps calculées en comparant le résultat des deux horloges. Le processus de calcul de la différence supprime les erreurs dues à l'imprécision des horloges par rapport à l'heure vraie, mais il est crucial que les différences elles-mêmes reflètent précisément les différences en heure vraie.

Les méthodologies de mesure vont souvent commencer par une étape consistant à s'assurer que deux horloges sont synchronisées et ont un biais et une dérive minimaux. {Commentaire : Une façon efficace de s'assurer de ces conditions (et aussi de la précision des horloges) est d'utiliser des horloges qui déduisent leur notion de l'heure d'une source externe, plutôt que seulement de l'horloge de l'ordinateur de l'hôte. (Ces dernières subissent souvent de grosses erreurs.) Il est de plus préférable que les horloges déduisent directement leur heure, par exemple, en ayant un accès immédiat à une unité de GPS *(Global Positioning System)*.}

Deux problèmes importants surviennent si les horloges déduisent indirectement leur heure en utilisant un protocole de synchronisation de l'heure du réseau tel que NTP :

+ D'abord, la précision de NTP dépend en partie des propriétés (en particulier du délai) des chemins Internet utilisés par les homologues NTP, et ce peut être précisément les propriétés qu'on souhaite mesurer, de sorte qu'il serait malsain d'utiliser NTP pour calibrer de telles mesures.
+ Ensuite, NTP se concentre sur la précision d'horloge, qui peut se faire aux dépens du biais et de la dérive d'horloge à court terme. Par exemple, lorsque l'horloge d'un hôte est indirectement synchronisée à une source horaire, si les intervalles de synchronisation surviennent de façon peu fréquente, l'hôte va alors parfois se trouver faire face au problème de comment ajuster son heure en cours incorrecte, Ti, avec une heure considérablement différente, plus précise, qu'il vient d'apprendre, Ta. Les deux façons générales de le faire sont soit de régler immédiatement l'heure actuelle sur Ta, soit d'ajuster la fréquence de mise à jour de l'horloge locale (donc, son biais) de telle sorte qu'à un certain instant futur, l'heure locale Ti' soit en accord avec l'heure plus précise Ta'. Le premier mécanisme introduit des discontinuités et peut aussi violer les hypothèses courantes d'accroissement monotone des horodatages. Si l'horloge de l'hôte est réglée en arrière dans le temps, cela peut parfois être facilement détecté. Si l'horloge est avancée, cela peut être plus difficile à détecter. Le biais induit par le second mécanisme peut conduire à des imprécisions considérables lors du calcul de différences d'heure, comme exposé plus haut.

Pour illustrer pourquoi le biais est un problème crucial, considérons des échantillons de délais unidirectionnels entre deux hôtes Internet faits à une minute d'intervalle. Le vrai délai de transmission entre les hôtes pourrait plausiblement être de l'ordre de 50 ms pour un chemin transcontinental. Si le biais entre les deux horloges est de 0,01 %, c'est-à-dire, de 1 pour 10 000, alors après 10 minutes d'observation, l'erreur introduite dans la mesure est de 60 ms. Sauf si elle est corrigée, cette erreur est suffisante pour effacer complètement toute précision de la mesure du délai de transmission. Finalement, on note que l'établissement des erreurs de biais entre des horloges réseau non synchronisées est un sujet de recherche ouvert. (Voir dans [Pa97] une discussion sur la détection et la compensation de ces sortes d'erreurs.) Ce défaut rend l'utilisation d'une source d'horloge solide, indépendante, telle que le GPS, particulièrement désirable.

10.2 La notion "d'heure du réseau"

La mesure Internet est souvent compliquée par l'utilisation des hôtes Internet eux-mêmes pour effectuer la mesure. Ces hôtes peuvent introduire des délais, des goulots d'étranglement, et ainsi de suite, qui sont dus à des effets du matériel ou du système d'exploitation et n'ont rien à voir avec le comportement du réseau qu'on voudrait mesurer. Ce problème est particulièrement aigu lorsque l'horodatage des événements du réseau survient au niveau application.

Afin de fournir un moyen général de parler de ces effets, on introduit deux notions "d'heure du réseau". Ces notions ne sont définies qu'en termes d'un hôte Internet H qui observe une liaison Internet L en un endroit particulier :

+ Pour un certain paquet P, l'heure d'arrivée au réseau de P à H sur L est le premier instant T auquel tout bit de P est apparu à sa position d'observation de H sur L.
+ Pour un certain paquet P, l'heure de sortie du réseau de P à H sur L est le premier instant T auquel tous les bits de P sont apparus à la position d'observation de H sur L.

Noter que la localisation du point d'observation sur la liaison est intrinsèque de la définition. Cette distinction est importante parce que pour les liaisons à forte latence, on peut obtenir des temps très différents selon le point exact d'où on

observe la liaison. On pourrait permettre que la position d'observation soit une situation arbitraire sur la liaison ; cependant, on la définit en termes d'hôte Internet parce qu'on prévoit qu'en pratique, pour les métriques IPPM, de telles mesures de rythmes seront contraintes d'être effectuées par des hôtes Internet plutôt que par des matériels spécialisés qui pourraient être capables de surveiller une liaison à des localisations où un hôte ne le peut pas. Cette définition tient aussi compte du problème des liaisons qui sont constituées de multiples canaux physiques. Parce que ces canaux multiples ne sont pas visibles à la couche IP, ils ne peuvent pas être observés individuellement selon les termes des définitions ci-dessus.

Il est possible, bien qu'on l'espère peu courant, qu'un paquet P puisse faire plusieurs trajets sur une certaine liaison L, du fait d'une boucle de transmission. Ces trajets pourraient même se chevaucher, selon la technologie de la liaison. Chaque fois que cela se produit, on définit une heure réseau différente associée à chaque instance de P vue à la position de H sur la liaison. Cette définition vaut la peine qu'on la donne parce qu'elle sert à rappeler que des notions comme *l'heure unique* à laquelle passe un paquet à un point dans l'Internet est par nature glissante.

Le terme d'heure du réseau a été historiquement utilisée pour noter vaguement l'heure à laquelle un paquet apparaît sur une liaison, sans spécifier exactement si cela se réfère au premier bit, au dernier bit, ou à d'autres considérations. Cette définition informelle est généralement déjà très utile, car elle est usuellement utilisée pour faire la distinction entre le moment ou les délais de propagation du paquet commencent à courir et cessent d'être dus au réseau mais aux hôtes des points d'extrémités.

Lorsque c'est approprié, les métriques devraient être définies en termes d'heure du réseau plutôt qu'en heures d'hôte de point d'extrémité, ainsi, la définition de la métrique souligne les problèmes de séparation des délais dus à l'hôte de ceux dus au réseau.

On note qu'une difficulté potentielle du traitement de l'heure du réseau concerne les fragments IP. Il peut être le cas que, du fait de la fragmentation, seule une portion d'un certain paquet passe par la localisation de H. De tels fragments sont eux-mêmes des paquets légitimes et ont des heures réseau bien définies qui leur sont associées ; mais le plus grand paquet IP qui correspond à leur agrégat peut ne pas en avoir.

On note aussi que ces notions n'ont pas, à notre connaissance, été précédemment définies dans ces termes exacts pour le trafic Internet.
Par conséquent, on pourrait trouver à l'expérience que ces définitions exigent quelques ajustements à l'avenir.

{Commentaire : Il peut parfois être difficile de mesurer l'heure du réseau. Une technique est d'utiliser un filtre de paquets pour surveiller le trafic d'une liaison. L'architecture de ces filtres tente souvent d'associer à chaque paquet un horodatage aussi proche que possible de l'heure du réseau. On note cependant qu'une source courante d'erreur est de faire fonctionner le filtre de paquet sur un des hôtes de point d'extrémité. Dans ce cas, il a été observé que certaine filtres de paquets reçoivent pour certains paquets des horodatages qui correspondent au moment où le paquet a été *programmé* pour l'injection dans le réseau, plutôt que lorsque il est réellement *envoyé* sur le réseau (heure du réseau). Il peut y avoir une différence substantielle entre ces deux instants. Une technique pour traiter ce problème est de faire fonctionner le filtre à paquets sur un hôte distinct qui surveille passivement la liaison en question. Cela peut cependant être problématique pour certaines technologies de liaisons. Voir dans [Pa97] un exposé sur les sortes d'erreurs que les filtres à paquet peuvent présenter. Finalement, on note que les filtres à paquets vont souvent seulement capturer le premier fragment d'un paquet IP fragmenté, du fait de l'utilisation du filtrage sur des champs dans les en-têtes IP et de protocole de transport. Comme on désire généralement que nos méthodologies de mesure évitent la complexité de la création de trafic fragmenté, une stratégie pour traiter leur présence telle que détectée par un filtre à paquets est d'étiqueter le trafic mesuré en forme usuelle et d'abandonner d'analyser plus avant l'horodatage du paquet.}

11. Singletons, échantillons et statistiques

Avec l'expérience, nous avons trouvé utile d'introduire une séparation entre trois notions distinctes – quoique en rapport :

+ Par une métrique de 'singleton', on se réfère aux métriques qui sont, dans un sens, atomiques. Par exemple, une seule instance de "capacité de débit en vrac" d'un hôte à un autre pourrait être définie comme une métrique de singleton, même si l'instance implique de mesurer les horaires d'un certain nombre de paquets Internet.
+ Par une métrique 'd'échantillons', on se réfère aux métriques déduites d'une certaine métrique de singleton en prenant ensemble un certain nombre d'instances distinctes. Par exemple, on pourrait définir une métrique d'échantillons de délais unidirectionnels d'un hôte à un autre sur une heure de mesures, chacune faite à des intervalles de Poisson avec un espacement moyen d'une seconde.
+ Par métrique 'statistique', on se réfère aux métriques déduites d'une certaine métrique d'échantillons en calculant des statistiques des valeurs définies par la métrique de singleton sur l'échantillon. Par exemple, la moyenne de toutes les valeurs de délai unidirectionnel sur l'échantillon donné ci-dessus pourrait être définie comme une métrique statistique.

En appliquant ces notions de singleton, d'échantillon, et de statistique d'une façon cohérente, on sera capable de réutiliser les enseignement tirés de la façon de définir échantillons et statistiques sur diverses métriques. L'orthogonalité *(au sens de statistiquement indépendant)* de ces trois notions va donc rendre notre travail plus efficace et plus intelligible par la communauté.

Dans le reste de cette section, nous allons traiter certains sujets en échantillonnage et en statistiques dont nous pensons qu'ils sont importants pour diverses définitions de métriques et systèmes de mesures.

11.1 Méthodes de collecte d'échantillons

La principale raison de collecter des échantillons est de voir quelle sortes de variations et de cohérences sont présentes dans la métrique mesurée. Ces variations peuvent être par rapport à des points différents dans l'Internet, ou des heures de mesure différentes. Lorsque on établit des variations sur la base d'un échantillon, on fait généralement l'hypothèse que l'échantillon n'est pas "biaisé", ce qui signifie que le processus de collecte des mesures dans l'échantillon n'a pas biaisé l'échantillon de telle sorte qu'il ne reflète plus précisément les variations et la cohérence de la métrique.

Une façon courante de collecter des échantillons est de faire des mesures séparées d'un intervalle de temps fixe : c'est l'échantillonnage périodique. L'échantillonnage périodique est particulièrement intéressant à cause de sa simplicité, mais il souffre de deux problèmes potentiels :

+ Si la métrique mesurée affiche elle-même un comportement périodique, il y a une possibilité que l'échantillon n'observe qu'une partie du comportement périodique si les périodes se trouvent en phase (soit directement, soit si l'une est un multiple de l'autre). En rapport avec ce problème est la notion que l'échantillonnage périodique peut être facilement anticipé. Un échantillonnage prévisible est susceptible de manipulation si il y a des mécanismes par lesquels le comportement d'un composant de réseau peut être temporairement changé de telle sorte que l'échantillon ne voit que le comportement modifié.
+ L'acte de mesure peut perturber ce qui est mesuré (par exemple, injecter du trafic de mesure dans un réseau altère le niveau d'encombrement du réseau, et des perturbations périodiques répétées peuvent amener un réseau dans un état de synchronisation (cf. [FJ94]) magnifiant considérablement ce qui individuellement serait d'un effet mineur.

Une approche se fonde sur "l'échantillonnage additif aléatoire" : les échantillons sont séparés par des intervalles aléatoires indépendants qui ont une distribution statistique commune G(t) [BM92]. La qualité de cet échantillon dépend de la distribution G(t). Par exemple, si G(t) génère une valeur constante g avec une probabilité de un, l'échantillon se réduit alors à un échantillonnage périodique avec une période de g.

L'échantillonnage additif aléatoire présente des avantages significatifs. En général, il évite les effets de synchronisation et donne une estimation non biaisée de la propriété échantillonnée. Ses seuls inconvénients significatifs sont :

+ qu'il complique les analyses de fréquence de domaine, parce que les échantillons ne surviennent pas à des intervalles fixes tels que supposés par les techniques de transformation de Fourier ;
+ que sauf si G(t) est la distribution exponentielle (voir ci-dessous) l'échantillon reste toujours assez prévisible, comme on l'a expliqué pour l'échantillonnage périodique.

11.1.1 Échantillonnage de Poisson

On prouver que si G(t) est une distribution exponentielle avec un taux de lambda, c'est-à-dire G(t) = 1 - exp(-lambda * t) alors l'arrivée de nouveaux échantillons *ne peut pas* être prédite (et là aussi, l'échantillon n'est pas biaisé). De plus, l'échantillon est non biaisé asymptotiquement même si l'action d'échantillonnage affecte l'état du réseau. Un tel échantillon est appelé un "échantillon de Poisson". Il n'est pas enclin à induire la synchronisation, il peut être utilisé pour collecter avec précision des mesures de comportement périodique, et il n'est pas enclin aux manipulations par anticipation des instants où vont survenir de nouveaux échantillons.

À cause de ces propriétés précieuses, on préfère en général que l'échantillonnage des mesures de l'Internet soit collecté en utilisant l'échantillon de Poisson. {Commentaire : On note cependant qu'il peut y avoir des circonstances en faveur de l'utilisation d'un G(t) différent. Par exemple, la distribution exponentielle n'est pas bornée, de sorte que son utilisation va à l'occasion générer de longs espaces entre les heures des échantillons. On peut désirer plutôt borner le plus long de ces intervalles à une valeur maximum dT, pour accélérer la convergence de l'estimation déduite de l'échantillon. Cela pourrait être fait un utilisant G(t) = Unif(0, dT), c'est-à-dire, la distribution uniforme entre 0 et dT. Bien sûr, cet échantillon devient hautement prévisible si un intervalle de longueur proche de dT s'est écoulé sans que soit pris un échantillon.}

Dans sa forme la plus pure, l'échantillon de Poisson se fait en générant des intervalles indépendants, exponentiellement distribués, et en collectant une seule mesure après que chaque intervalle soit écoulé. On peut montrer que si on effectue en commençant à l'instant T un échantillon de Poisson sur un intervalle dT, durant lequel un total de N mesures se trouvent être faites, alors ces mesures seront uniformément distribuées sur l'intervalle [T, T+dT]. De sorte qu'une autre façon

d'effectuer un échantillon de Poisson est de choisir dT et N et de générer N fois l'échantillonnage aléatoire uniformément sur l'intervalle [T, T+dT]. Les deux approches sont équivalentes, sauf si N et dT sont connus en externe. Dans ce cas, la propriété de n'être pas capable de prédire les heures de mesure est affaiblie (les autres propriétés tiennent). L'approche N/dT qui a l'avantage de traiter avec des valeurs fixes de N et dT peut être plus simple que de traiter avec un lambda fixe mais des nombres variables de mesures sur des intervalles de taille variable.

11.1.2 Échantillonnage géométrique

En étroite relation avec l'échantillon de Poisson, on a "l'échantillon géométrique", dans lequel des événements externes sont mesurés avec une probabilité fixe de p. Par exemple, on peut capturer tous les paquets sur une liaison mais seulement enregistrer les paquet dans un fichier de collecte si un nombre généré au hasard à distribution uniforme entre 0 et 1 est inférieur à un p donné. L'échantillonnage géométrique a les mêmes propriétés d'être non biaisé et non prévisible à l'avance que l'échantillon de Poisson, de sorte que si il convient pour une tâche particulière de mesure de l'Internet, il est aussi adapté. Voir plus de détails dans [CPB93].

11.1.3 Génération d'intervalles d'échantillon de Poisson

Pour générer des intervalles d'échantillon de Poisson, on détermine le taux lambda auquel seront faites en moyenne les mesures de singleton (par exemple, pour un intervalle d'échantillonnage moyen de 30 secondes, on a lambda = 1/30, si l'unité de temps est la seconde). On génère alors une série de nombres aléatoires (ou pseudo-aléatoires) à distribution exponentielle E1, E2, ..., En. La première mesure est faite à l'instant E1, la suivante à l'instant E1+E2, et ainsi de suite.

Une technique pour générer des nombres aléatoires (ou pseudo-aléatoires) à distribution exponentielle se fonde sur la capacité à générer U1, U2, ..., Un, nombres (pseudo) aléatoires qui sont uniformément distribués entre 0 et 1. De nombreux ordinateurs ont des bibliothèques qui peuvent faire cela.

Étant donné un tel Ui, pour générer Ei on utilise Ei = -log(Ui) / lambda, où log(Ui) est le logarithme naturel de Ui. {Commentaire : Cette technique est une instance de la méthode plus générale de "transformation inverse" pour générer des nombres aléatoires avec une certaine distribution.}

Détails de mise en œuvre :
Il y a au moins trois méthodes différentes d'approximation de l'échantillonnage de Poisson que l'on décrit ici comme les méthodes de 1 à 3. La méthode 1 est la plus facile à mettre en œuvre et a le plus d'erreurs, et la méthode 3 est la plus difficile à mettre en œuvre et a le moins d'erreurs (potentiellement aucune).

La méthode 1 est traitée comme suit :
1. Générer E1 et attendre cette durée.
2. Effectuer une mesure.
3. Générer E2 et attendre cette durée.
4. Effectuer une mesure.
5. Générer E3 et attendre cette durée.
6. Effectuer une mesure. ...

Le problème avec cette approche est que l'étape "Effectuer une mesure" prend elle-même du temps, de sorte que l'échantillonnage n'est pas fait aux instants E1, E1+E2, etc., mais plutôt à E1, E1+M1+E2, etc., où Mi est la durée nécessaire pour la $i^{ème}$ mesure. Si Mi est très petit par rapport à 1/lambda alors l'erreur potentielle introduite par cette technique est aussi petite. Lorsque Mi devient une fraction non négligeable de 1/lambda, l'erreur potentielle croît.

La méthode 2 tente de corriger cette erreur en tenant compte de la durée exigée par les mesures (c'est-à-dire, le Mi) et en ajustant les intervalles d'attente en conséquence :
1. Générer E1 et attendre cette durée.
2. Effectuer une mesure et mesurer M1, le temps que prend cette mesure.
3. Générer E2 et attendre pendant E2-M1.
4. Effectuer une mesure et mesurer M2 ...

Cette approche fonctionne bien tant que $E\{i+1\} \geq Mi$. Mais si $E\{i+1\} < Mi$ il est alors impossible d'attendre pendant la durée appropriée. (Noter que ce cas correspond à avoir besoin d'effectuer deux mesures simultanées.)

La méthode 3 génère un programme d'instants de mesure E1, E1+E2, etc., et s'y tient :
1. Générer E1, E2, ..., En.
2. Calculer les instants de mesure T1, T2, ..., Tn, comme Ti = E1 + ... + Ei.
3. S'arranger pour qu'aux instants T1, T2, ..., Tn, une mesure soit faite.

En permettant des mesures simultanées, la méthode 3 évite les inconvénients des méthodes 1 et 2. Si, cependant, les mesures simultanées interfèrent les unes avec les autres, alors la méthode 3 n'a aucun avantage et peut en fait se révéler pire que les méthodes 1 ou 2.

Pour les phénomènes Internet, on ne sait pas à quel point les imprécisions de ces méthodes sont significatives. Si les Mi sont très inférieurs à 1/lambda, n'importe laquelle des trois devrait suffire. Si les Mi sont inférieurs à 1/lambda mais peut-être pas de beaucoup, alors la méthode 2 est préférable à la méthode 1. Si les mesures simultanées n'interfèrent pas les unes avec les autres, la méthode 3 est alors préférable, bien qu'elle puisse être considérablement plus dure à mettre en œuvre.

11.2 Cohérence interne

Une exigence fondamentale d'une bonne méthodologie de mesures est que celles-ci soient faites en utilisant aussi peu d'hypothèses non confirmées que possible. L'expérience nous a montré à nos dépens combien il est facile de faire des hypothèses (souvent implicites) qui se révèlent incorrectes. Un exemple en est d'incorporer dans une mesure la lecture d'une horloge synchronisée sur une source très précise. Il est facile de supposer que l'horloge est donc précise, mais à cause de bogues du logiciel, d'une perte de puissance à la source, ou d'une perte de communication entre la source et l'horloge, celle-ci peut être en fait assez imprécise.

Ce n'est pas pour dire qu'il ne faut jamais faire *aucune* hypothèse quand on mesure, mais plutôt que dans la mesure de ce qui est praticable, les hypothèses devraient être vérifiées. Un moyen puissant de le faire implique de vérifier la cohérence interne. Une telle vérification s'applique aussi bien aux valeurs observées de la mesure qu'aux *valeurs utilisées par le processus de mesure lui-même*. Un simple exemple de la première est que quand on calcule un délai d'aller-retour, on devrait vérifier qu'il n'est pas négatif. Comme un intervalle de temps négatif n'est pas une grandeur physique, si il s'en trouve un il doit immédiatement signaler une erreur. *Ces sortes d'erreurs devraient alors faire l'objet d'investigations !* Il est crucial de déterminer d'où vient l'erreur, parce que ce n'est qu'en le recherchant avec diligence qu'on peut construire la confiance en la validité fondamentale de la méthodologie. Par exemple, il se pourrait que le délai d'aller-retour soit négatif parce que durant la mesure, l'horloge a été réglée en avance du processus de synchronisation avec une autre source. Mais cela pourrait aussi être parce que le programme de mesure a accédé à une mémoire non initialisée dans un de ses calculs, et seulement très rarement, cela conduit à un calcul erroné. Cette seconde erreur est plus sérieuse, si le même programme est utilisé par d'autres pour effectuer la même mesure, comme eux aussi vont subir les mêmes résultats incorrects. De plus, une fois découverte, elle peut être complètement réparée.

Un exemple plus subtil de vérification de la cohérence interne vient de la collecte des échantillons de délais unidirectionnels sur l'Internet. Si on a un gros échantillon de tels délais, il peut être très instructif d'aligner, par exemple, les paires de (heure de mesure, délai mesuré) pour voir si la droite résultante a une pente nettement différente de zéro. Si c'est le cas, une interprétation possible en est qu'une des horloges utilisées dans les mesures est biaisée par rapport à l'autre. Une autre interprétation est que la pente est en fait due à d'authentiques effets du réseau. Déterminer quel est le cas va souvent être très éclairant. (Voir dans [Pa97] une discussion sur la distinction entre le biais d'horloge relatif et un authentique effet du réseau.) De plus, si cette vérification fait partie de la méthodologie, la découverte que la pente à long terme est très proche de zéro est une preuve positive que les mesures ne sont probablement pas biaisées par une différence de biais.

Un dernier exemple illustre la vérification de la cohérence interne du processus de mesure lui-même. Nous avons présenté ci-dessus les techniques de l'échantillonnage de Poisson, sur la base de la génération d'intervalles à distribution exponentielle. Une bonne méthodologie de mesure inclurait de tester les intervalles générés pour voir si ils sont bien à distribution exponentielle (et aussi pour voir si ils souffrent de corrélation). Dans l'appendice, on discute et donne le code C pour une telle technique, d'objet général, d'essai de bonne tenue, qu'on appelle le test d'Anderson-Darling.

Finalement, on note que ce qui est vraiment pertinent pour l'échantillonnage de Poisson des métriques de l'Internet est souvent non pas quand les mesures commencent mais les heures du réseau qui correspondent au processus de mesure. Elles peuvent très bien être différentes, à cause de complications sur les hôtes utilisés pour effectuer la mesure. Donc, même avec une confiance totale dans les générateurs de nombres pseudo aléatoires et dans les algorithmes qui les suivent, nous vous encourageons à considérer comment ils peuvent vérifier autant que possible les hypothèses de chaque procédure de mesure.

11.3 Définition des distributions statistiques

Une façon de décrire une collection de mesures (un échantillon) est une distribution statistique -- informelle, sous forme de percentiles. Il y a plusieurs façon légèrement différentes de le faire. Dans ce paragraphe, on donne une définition standard pour uniformiser ces descriptions.

La "fonction de distribution empirique" (EDF, *empirical distribution function*) d'un ensemble de mesures scalaires est une

fonction F(x) qui pour tout x donne la fraction des mesures totales qui étaient ≤ x. Si x est inférieur à la valeur minimum observée, alors F(x) est 0. Si il est supérieur ou égal à la valeur maximum observée, alors F(x) est 1.

Par exemple, soient les six mesures -2, 7, 7, 4, 18, -5.

Alors F(-8) = 0, F(-5) = 1/6, F(-5,0001) = 0, F(-4.999) = 1/6, F(7) = 5/6, F(18) = 1, F(239) = 1.

Noter qu'on peut récupérer les différentes valeurs mesurées et combien de fois chacune est survenue à partir de F(x) -- aucune information concernant la gamme des valeurs n'est perdue. D'un autre côté, résumer les mesures en utilisant des histogrammes perd en général des information sur les différentes valeurs observées, de sorte que EDF est préféré.

En utilisant soit EDF, soit un histogramme, on perd cependant des informations concernant l'ordre dans lequel les valeurs ont été observées. Que ces pertes soient potentiellement significatives va dépendre de la métrique mesurée.

On va utiliser le terme "percentile" pour se référer à la plus petite valeur de x pour laquelle F(x) > à un certain pourcentage. De sorte que le 50ème percentile de l'exemple ci-dessus est 4, car F(4) = 3/6 = 50 % ; le 25ème percentile est -2, car F(-5) = 1/6 < 25 %, et F(-2) = 2/6 ≥ 25 % ; le 100ème percentile est 18 ; et le 0ème percentile est –l'infini, comme l'est le 15ème percentile.

Il faut faire attention quand on utilise les percentiles pour résumer un échantillon, parce qu'ils peuvent prendre une apparence non garantie de plus de précision qu'ils n'en ont en réalité. Un tel résumé doit inclure la taille N de l'échantillon, parce que toute différence de percentile plus fine que 1/N est en dessous de la résolution de l'échantillon.

Voir dans [DS86] plus de précisions concernant les EDF.

On terminera par une note sur la notion courante (et importante !) de médiane. En statistiques, la médiane d'une distribution est définie par le point X pour lequel la probabilité d'observer une valeur ≤ X est égale à la probabilité d'observer une valeur > X. Lorsque on estime la médiane d'un ensemble d'observations, l'estimation dépend de si le nombre d'observations, N, est impair ou pair :

+ Si N est impair, le 50ème percentile comme défini ci dessus est alors utilisé comme médiane estimée.
+ Si N est pair, La médiane estimée est alors la moyenne des deux observations centrales ; c'est-à-dire que si les observations sont triées en ordre croissant et numérotées de 1 à N, où N = 2*K, alors la médiane moyenne estimée est la moyenne de la (K)ème et de la (K+1)ème observations.

Usuellement, le terme "estimée" est sauté dans l'expression "médiane estimée" et cette valeur est simplement appelée la "médiane".

11.4 Essais d'adaptabilité

Pour certaines formes de calibration de mesures on a besoin de vérifier si un ensemble de nombres est cohérent avec ceux qui ont été tirés d'une distribution particulière. Un exemple est celui qui applique une vérification de cohérence interne à des mesures faites en utilisant un processus de Poisson, une vérification regarde si l'espacement entre les instants d'échantillonnage reflète bien une distribution exponentielle ; ou si l'approche dT/N présentée plus haut a été utilisée, si les temps sont uniformément distribués sur [T, dT].

{Commentaire : Il y a au moins trois ensembles possibles de valeurs qu'on peut vérifier : les heures programmées de transmission de paquet, comme déterminées en utilisant un générateur de nombres pseudo aléatoires, des horodatages de niveau utilisateur faits juste avant ou après que le système appelle pour transmettre le paquet, et les heures du réseau pour les paquets tels qu'enregistrées en utilisant un filtre à paquets. Tous trois portent des informations potentielles : les échecs des heures programmées à correspondre à une distribution exponentielle indiquent une imprécision de la génération de nombres aléatoires ; les échecs des heures de niveau utilisateur indiquent des imprécisions des temporisateurs utilisés pour programmer la transmission ; et les défaillances de l'heure du réseau indiquent des imprécisions dans la transmission réelle des paquets, peut-être à cause d'un conflit de partage des ressource.}

Il y a un grand nombre de techniques de bonne répartition statistique pour effectuer de telles vérifications. Voir dans [DS86] un exposé complet. Cette référence recommande les test EDF d'Anderson-Darling comme étant un bon test tous usages, ainsi que particulièrement bon pour détecter les déviations d'une certaine distribution dans les parties inférieures et supérieures de l'EDF.

Il est important de comprendre que la nature des vérifications de bonne répartition fait qu'on choisit d'abord un "niveau de confiance", qui est la probabilité que l'essai déclare faussement que l'EDF d'un certain ensemble de mesures échoue à correspondre à une distribution particulière alors que en fait les mesures reflètent bien cette distribution.

Sauf mention contraire, les essais IPPM de bonne répartition sont faits en utilisant un seuil de confiance de 5 %. Cela signifie que si l'essai est appliqué à 100 échantillons et que 5 de ces échantillons sont réputés avoir échoué à l'essai, les échantillons sont tous cohérents avec la distribution qui a fait l'objet de l'essai. Si une partie significativement supérieure de l'échantillon échoue à l'essai, alors l'hypothèse que les échantillons sont cohérents avec la distribution testée doit être rejetée. Si significativement moins d'échantillons échouent à l'essai, on peut soupçonner que les échantillons ont peut-être été biaisés pour coller à la distribution. De même, certains essais de bonne répartition (y compris de Anderson-Darling) peuvent détecter si il est probable qu'un certain échantillon soit biaisé. On utilise aussi un seuil de confiance de 5 % pour ce cas; c'est-à-dire que l'essai va montrer qu'un certain échantillon est "trop bon pour être honnête" 5 % du temps, de sorte que si l'essai rapporte ce fait significativement plus souvent qu'une fois sur vingt, cela indique que quelque chose d'anormal est survenu.

L'appendice donne un échantillon de code C pour la mise en œuvre de l'essai d'Anderson- Darling, ainsi qu'une discussion de son utilisation.

Voir dans [Pa94] une discussion sur les essais de bonne répartition et proximité de répartition dans le contexte des mesures de réseau.

12. Éviter les métriques stochastiques

Lorsque on définit des métriques qui s'appliquent à un chemin, un sous chemin, un nuage, ou autre élément de réseau, on ne les définit en général pas en termes stochastiques (de probabilités). On préfère plutôt une définition déterministe. Ainsi, par exemple, plutôt que de définir une métrique de "probabilité de perte d'un paquet entre A et B", on va définir une métrique de "taux de perte de paquet entre A et B". (Une mesure donnée par la première définition pourrait être "0,73", et par la seconde, de "73 paquets sur 100".)

On souligne que la distinction ci-dessus concerne les *définitions* des *métriques*. Elle n'est pas destinée à s'appliquer à la sorte de technique qu'on peut utiliser pour analyser le résultat des mesures.

La raison de cette distinction est la suivante. Lorsque les définitions sont faites en termes de probabilités, il y a souvent des hypothèses cachées dans la définition sur le modèle stochastique du comportement à mesurer. Le but fondamental d'éviter les probabilités dans notre définition de métrique est d'éviter de biaiser nos définitions avec ces hypothèses cachées.

Par exemple, une hypothèse cachée facile à faire est que la perte de paquet dans un composant de réseau due au débordement de file d'attente peut être décrite comme quelque chose qui arrive à tout paquet avec une certaine probabilité. Cependant, dans l'Internet d'aujourd'hui, les abandons de file d'attente sont en fait usuellement *déterministes*, et supposer qu'ils devraient être décrits de façon probabiliste peut obscurcir des corrélations cruciales entre abandons dans une file d'attente parmi un ensemble de paquets. De sorte qu'il vaut mieux noter explicitement les hypothèses stochastiques, plutôt que de les voir se glisser implicitement dans nos définitions .

Cela ne signifie *pas* qu'on abandonne les modèles stochastiques pour *comprendre* les performances du réseau ! Cela signifie simplement que lorsque on définit des métriques IP, on doit éviter des termes comme "probabilité" au profit de termes comme "proportion" ou "taux". On va toujours utiliser, par exemple, l'échantillon aléatoire afin d'estimer les probabilités utilisées par les modèles stochastiques qui se rapportent aux métriques IP. On n'exclut pas non plus la possibilité de métriques stochastiques lorsque elles sont vraiment appropriées (par exemple, peut-être pour modéliser les erreurs de transmission causées par certains types de bruit de ligne).

13. Paquets de type P

Une propriété fondamentale de nombreuses métriques de l'Internet est que la valeur de la métrique dépend du type de paquet IP utilisé pour faire la mesure. Considérons une métrique de la connexité IP : on obtient des résultats différents selon qu'on est intéressé par la connexité pour les paquets destinés à des accès TCP bien connus ou à des accès UDP non réservés, ou à ceux qui ont des sommes de contrôle IP invalides, ou à ceux qui ont un TTL de 16, par exemple. Dans certaines circonstances, ces distinctions seront très intéressantes (par exemple, en présence de pare-feu, ou de réservations RSVP).

À cause de cette distinction, on introduit la notion générique de "paquet de type P", où dans certains contextes, P sera explicitement défini (c'est-à-dire, exactement quel type de paquet est visé) partiellement défini (par exemple, "avec une charge utile de B octets") ou laissé générique. Donc, on peut parler de connexité IP de type P générique ou de connexité HTTP d'accès IP plus spécifique. Certaines métriques et méthodologies peuvent avec profit être définies en utilisant des définitions de type P générique qui sont alors rendues spécifiques lorsque on effectue les mesures réelles.

Chaque fois qu'une valeur de métrique dépend du type des paquets impliqués dans la métrique, le nom de la métrique va comporter soit un type spécifique, soit une phrase telle que "type-P". Nous n'allons donc pas définir une métrique de "connexité IP" mais plutôt une métrique de "connexité IP de type P" et/ou peut-être une métrique de "connexité HTTP d'accès IP". Cette convention de dénomination sert à nous rappeler qu'il est important d'être conscient du type exact de trafic qu'on mesure.

Note : il serait très utile de savoir si un certain composant Internet traite équitablement une classe C de différents types de paquets. Si il en est ainsi, alors chacun de ces types de paquets peut être utilisé pour les mesures suivantes du composant. Cela suggère d'imaginer une métrique ou suite de métriques qui tentent de déterminer C.

14. Adresses Internet ou nom d'hôte

Lorsque on considère une métrique pour un chemin à travers l'Internet, il est souvent naturel de la voir comme étant pour le chemin de l'hôte Internet H1 à l'hôte Internet H2. Une définition dans ces termes, peut cependant être ambiguë, parce que les hôtes Internet peuvent être rattachés à plus d'un réseau. Dans ce cas, le résultat de la métrique va dépendre duquel de ces réseaux est réellement utilisé.

À cause de cette ambiguïté, de telles définitions devraient plutôt être définies en termes d'adresses IP de l'Internet. Pour le cas courant de chemin unidirectionnel à travers l'Internet, on utilisera le terme "Src" pour noter l'adresse IP du commencement du chemin, et "Dst" pour noter l'adresse IP de la fin.

15. Paquets de forme standard

Sauf mention contraire, toutes les définitions de métrique qui concernent des paquets IP comportent l'hypothèse implicite que les paquets sont de *forme standard*. Un paquet est de forme standard si il satisfait à tous les critères suivants :

+ Sa longueur donnée dans l'en-tête IP correspond à la taille de l'en-tête IP plus la taille de la charge utile.
+ Il comporte un en-tête IP valide : le champ de version est 4 (ceci sera étendu ultérieurement pour inclure 6) ; la longueur d'en-tête est ≥ 5 ; la somme de contrôle est correcte.
+ Ce n'est pas un fragment IP.
+ Les adresses de source et de destination correspondent aux hôtes en question.
+ Soit le paquet possède un TTL suffisant pour voyager de la source à la destination si le TTL est décrémenté de un à chaque bond, soit il possède le TTL maximum de 255.
+ Il ne contient pas d'options IP sauf notation explicite.
+ Si un en-tête de transport est présent, il contient aussi une somme de contrôle valide et d'autres champs valides.

On exige de plus que si un paquet est décrit comme ayant une "longueur de B octets", alors $0 \leq B \leq 65\ 535$; et si B est la longueur de charge utile en octets, alors $B \leq (65\ 535 -$ taille d'en-tête IP en octets).

Ainsi, par exemple, on pourrait imaginer de définir une métrique de connexité IP comme une "connexité IP de type-P pour les paquets de forme standard avec le champ IP Type de service réglé à 0", ou, plus succinctement, "connexité IP de type-P avec le champ TOS réglé à 0", car de forme standard est déjà impliqué par convention.

Un type particulier de paquet de forme standard qu'il est souvent utile de prendre en compte est le "paquet IP minimal de A à B" – c'est un paquet IP avec les propriétés suivantes :

+ Il est de forme standard.
+ Sa charge utile de données est 0 octets.
+ Il ne contient pas d'options.

(Noter qu'on ne définit pas son champ Protocole, car différentes valeurs peuvent conduire à des traitements différents par le réseau.)

Lorsque on définit des métriques IP, on doit se souvenir qu'aucun paquet plus petit ou plus simple que cela ne peut être transmis sur un réseau IP qui fonctionne correctement.

16. Remerciements

Les commentaires de Brian Carpenter, Bill Cerveny, Padma Krishnaswamy Jeff Sedayao et Howard Stanislevic ont été appréciés.

17. Considérations pour la sécurité

Le présent document concerne les définitions et concepts qui se rapportent aux mesures dans l'Internet. On expose les procédures de mesure en termes très généraux, au niveau des principes qui se prêtent eux-mêmes à de bonnes mesures. À ce titre, les sujets discutés n'affectent pas la sécurité de l'Internet ou des applications qui y fonctionnent.

Ceci dit, on devrait reconnaître qu'effectuer des mesures de l'Internet peut soulever des problèmes aussi bien de sécurité que de confidentialité. Des techniques actives, dans lesquelles le trafic est injecté dans le réseau, peuvent être détournées pour des attaques de déni de service déguisées en activité légitime de mesure. Des techniques passives, dans lesquelles le trafic existant est enregistré et analysé, peuvent exposer les contenus du trafic Internet à des receveurs non prévus. Par conséquent, la définition de chaque métrique et méthodologie doit inclure une discussion correspondante de considérations sur la sécurité.

18. Appendice

On donne ci-dessous les sous-programmes en langage C pour calculer la statistique d'essai Anderson-Darling (A2) pour déterminer si un ensemble de valeurs est cohérent avec une certaine distribution statistique. En externe, les deux principaux sous-programmes intéressants sont :

```
double exp_A2_known_mean(double x[], int n, double mean)
double unif_A2_known_range(double x[], int n, double min_val, double max_val)
```

Tous deux prennent comme premier argument, x, l'ensemble de n valeurs objet de l'essai. (En retour, les éléments de x sont triés.) Les paramètres restants caractérisent la distribution à utiliser : soit le (1/lambda)moyen, pour une distribution exponentielle, soit les bornes inférieure et supérieure, pour une distribution uniforme. Les noms des sous-programmes soulignent que ces valeurs doivent être connues à l'avance, et *non* estimées à partir des données (par exemple, en calculant l'échantillon moyen). L'estimation des paramètres à partir des données *change* le niveau de signification de la statistique de l'essai. Alors que [DS86] donne d'autres tableaux de signification pour certaines instances dans lesquelles les paramètres sont estimés à partir des données, pour nos besoins, on s'attend bien sûr à connaître les paramètres à l'avance, car ce qu'on veut vérifier sont généralement des valeurs comme les heures d'envoi des paquets dont on souhaite vérifier qu'elles suivent une distribution connue.

Les deux sous-programmes retournent un niveau de signification, comme on l'a décrit précédemment C'est une valeur entre 0 et 1. L'utilisation correcte des sous-programmes est de fixer à l'avance le seuil du niveau de signification à vérifier ; généralement, ce sera 0,05, correspondant à 5 %, comme on l'a aussi décrit précédemment. Ensuite, si le sous-programme retourne une valeur strictement inférieure au seuil, les données sont alors réputées être non cohérentes avec la distribution présumée, *sous réserve d'une erreur correspondant au niveau de signification*. C'est-à-dire que, pour un niveau de signification de 5 %, 5 % des données d'heures qui sont bien sûr tirées de la distribution présumée seront faussement réputées incohérentes.

Donc, il est important de se souvenir que si ces routines sont utilisées fréquemment, on va bien sûr rencontrer des échecs occasionnels, même si les données sont irréprochables.

Un autre point important concernant les niveaux de signification est qu'il n'est pas correct de les comparer afin de déterminer quel ensemble des valeurs est "meilleur" pour une certaine distribution. Une telle vérification devrait plutôt être faite en utilisant des "métriques d'approximation" telles que la métrique lambda^2 décrite dans [Pa94].

Bien que les routines fournies soient pour les distributions exponentielles et uniformes avec des paramètres connus, il est généralement facile d'écrire des routines comparables pour toute distribution avec paramètres connus. Le cœur des essais A2 réside dans une statistique calculée pour vérifier si un ensemble de valeurs est cohérent avec une distribution uniforme entre 0 et 1, qu'on appelle Unif(0, 1). Si on souhaite vérifier si un ensemble de valeurs, X, est cohérent avec une certaine distribution G(x), on calcule d'abord Y = G_inverse(X)
Si X est bien distribué selon G(x), Y sera alors distribué selon Unif(0, 1) ; de sorte qu'en vérifiant la cohérence de Y par rapport à Unif(0, 1), on vérifie aussi la conformité de X à G(x).

On note, cependant, que le processus de calcul de Y ci-dessus pourrait donner des valeurs de Y en dehors de la gamme (0..1). De telles valeurs ne devraient pas survenir si X est bien distribué selon G(x), mais elle peuvent facilement se produire si il ne l'est pas. Dans ce dernier cas, on doit éviter de calculer la statistique A2 centrale, car des exceptions de virgule flottante peuvent se produire si une des valeurs est en dehors de l'intervalle (0..1). En conséquence, les routines vérifient cette possibilité, et si elle se rencontre, retournent une statistique A2 brute de -1. La routine qui convertit la statistique A2 brute en un niveau de signification propage de même cette valeur, retournant un niveau de signification de -1. Ainsi, toute utilisation de ces routines doit être prête à un possible niveau de signification négatif.

Le dernier point important concernant l'utilisation de la statistique A2 concerne n, le nombre de valeurs à vérifier. Si n < 5

l'essai n'est alors pas significatif, et dans ce cas, un niveau de signification de -1 est retourné.

D'un autre côté, pour des données "réelles" l'essai *gagne* en puissance lorsque n augmente. Il est bien connu dans la communauté des statistiques que les données réelles ne correspondent jamais exactement à une distribution théorique, même dans des cas tels que celui d'un grand nombre de lancers de dés (voir dans [Pa94] une brève discussion et des références). L'essai A2 est assez sensible pour que, pour des ensembles suffisamment grands de données réelles, l'essai échoue presque toujours, parce qu'il va s'arranger pour détecter de légères imperfections dans l'adéquation des données à la distribution.

Par exemple, on a trouvé que lors de l'essai de 8 192 heures du réseau mesurées pour des paquets envoyés à des intervalles de Poisson, les mesures échouent presque toujours au test A2. D'un autre côté, un essai de 128 mesures échoue au seuil de signification de 5 % de seulement environ 5 %, comme prévu. Donc, en général, lorsque l'essai échoue, il faut faire attention à bien comprendre pourquoi il a échoué.

Le reste de cet appendice donne le code C pour les sous-programmes mentionnés ci-dessus.

```
/* Sous-programmes pour calculer la statistique d'essai A2 Anderson-Darling.
* Mis en œuvre sur la base de la description dans "Goodness-of-Fit Techniques," R. D'Agostino and M. Stephens, éditeurs,
* Marcel Dekker, Inc., 1986.
*/

#include <stdio.h>
#include <stdlib.h>
#include <math.h>

/* Retourne la statistique d'essai A^2 brut pour n échantillons triés z[0] .. z[n-1], pour z ~ Unif(0,1).
*/
extern double compute_A2(double z[], int n);

/* Retourne le niveau de signification associé à une valeur de statistique d'essai A^2 de A2, en supposant qu'aucun
* paramètre de la distribution vérifiée n'a été estimé à partir des données.
*/
extern double A2_significance(double A2);

/* Retourne le niveau de signification A^2 pour comparer n observations x[0] .. x[n-1] à une distribution exponentielle
* avec la moyenne donnée.
*
* EFFET COLATÉRAL : Les x[0..n-1] sont triés en sortie.
*/
extern double exp_A2_known_mean(double x[], int n, double mean);

/* Retourne le A^2 niveau de signification pour comparer n observations
* x[0] .. x[n-1] à la distribution uniforme [min_val, max_val].
*
* EFFET COLATÉRAL : Les x[0..n-1] sont triés en sortie.
*/
extern double unif_A2_known_range(double x[], int n, double min_val, double max_val);

/* Retourne un nombre pseudo-aléatoire distribué selon une distribution exponentielle avec la moyenne donnée. */
extern double random_exponential(double mean);

/* Fonction d'aide utilisée par qsort() pour trier les valeurs en virgule flottante en double précision. */
static int
compare_double(const void *v1, const void *v2)
{
   double d1 = *(double *) v1;
   double d2 = *(double *) v2;

   if (d1 < d2)
      return -1;
   else if (d1 > d2)
      return 1;
   else
```

```
        return 0;
}

double
compute_A2(double z[], int n)
{
   int i;
   double sum = 0.0;

   if ( n < 5 )
      /* Trop peu de valeurs. */
    return -1.0;

/* Si une des valeurs est en dehors de la gamme (0, 1) alors
* échec immédiat (et éviter une possible exception de virgule flottante dans le code suivant).
*/
   for (i = 0; i < n; ++i)
      if ( z[i] <= 0.0 || z[i] >= 1.0 )
         return -1.0;

/* Page 101 de D'Agostino and Stephens. */
   for (i = 1; i <= n; ++i) {
      sum += (2 * i - 1) * log(z[i-1]);
      sum += (2 * n + 1 - 2 * i) * log(1.0 - z[i-1]);
   }
   return -n - (1.0 / n) * sum;
}

double
A2_significance(double A2)
{
/* Page 105 de D'Agostino and Stephens. */
   if (A2 < 0.0)
      return A2;    /* Valeur A2 boguée – la propager. */

/* Vérifier de possibles valeurs biaisées. */
   if (A2 <= 0.201)
      return 0.99;
   else if (A2 <= 0.240)
      return 0.975;
   else if (A2 <= 0.283)
      return 0.95;
   else if (A2 <= 0.346)
      return 0.90;
   else if (A2 <= 0.399)
      return 0.85;

/* On vérifie maintenant de possibles incohérences. */
   if (A2 <= 1.248)
      return 0.25;
   else if (A2 <= 1.610)
      return 0.15;
   else if (A2 <= 1.933)
      return 0.10;
   else if (A2 <= 2.492)
      return 0.05;
   else if (A2 <= 3.070)
      return 0.025;
   else if (A2 <= 3.880)
      return 0.01;
   else if (A2 <= 4.500)
      return 0.005;
   else if (A2 <= 6.000)
```

```
        return 0.001;
    else
        return 0.0;
}

double
exp_A2_known_mean(double x[], int n, double mean)
{
    int i;
    double A2;

/* Trier les n premières valeurs. */
    qsort(x, n, sizeof(x[0]), compare_double);

/* En supposant qu'elles correspondent à une distribution exponentielle, les transformer en Unif(0,1).
*/
    for (i = 0; i < n; ++i) {
        x[i] = 1.0 - exp(-x[i] / mean);
    }

/* Maintenant, faire l'essai A^2 pour voir si elles sont vraiment uniformes. */
    A2 = compute_A2(x, n);
    return A2_significance(A2);
}

double
unif_A2_known_range(double x[], int n, double min_val, double max_val)
{
    int i;
    double A2;
    double range = max_val - min_val;

/* Trie les n premières valeurs. */
    qsort(x, n, sizeof(x[0]), compare_double);

/* Transforme Unif(min_val, max_val) en Unif(0,1). */
    for (i = 0; i < n; ++i)
        x[i] = (x[i] - min_val) / range;

/* Faire maintenant l'essai A^2 pour voir si elles sont vraiment uniformes. */
    A2 = compute_A2(x, n);
    return A2_significance(A2);
}

double
random_exponential(double mean)
{
    return -mean * log1p(-drand48());
}
```

19. Références

[AK97] G. Almes, S. Kalidindi, M. Zekauskas, "Métrique de délai unidirectionnel pour IPPM", RFC2679, septembre 1999. *(P.S.)*

[BM92] I. Bilinskis and A. Mikelsons, "Randomized Signal Processing", Prentice Hall International, 1992.

[DS86] R. D'Agostino and M. Stephens, editors, "Goodness-of-Fit Techniques", Marcel Dekker, Inc., 1986.

[CPB93] K. Claffy, G. Polyzos, and H-W. Braun, "Application of Sampling Methodologies to Network Traffic Characterization," Proc. SIGCOMM '93, pp. 194-203, San Francisco, septembre 1993.

[FJ94] S. Floyd and V. Jacobson, "The Synchronization of Periodic Routing Messages," IEEE/ACM Transactions on Networking, 2(2), pp. 122-136, avril 1994.

[Mi92] D. Mills, "Protocole de l'heure du réseau, version 3, spécification, mise en œuvre et analyse", RFC1305, STD 12, mars 1992. *(Remplacée par RFC5905)*

[Pa94] V. Paxson, "Empirically-Derived Analytic Models of Wide-Area TCP Connections", IEEE/ACM Transactions on Networking, 2(4), pp. 316-336, août 1994.

[Pa96] V. Paxson, "Towards a Framework for Defining Internet Performance Metrics", Proceedings of INET '96, ftp://ftp.ee.lbl.gov/papers/metrics-framework-INET96.ps.Z

[Pa97] V. Paxson, "Measurements and Analysis of End-to-End Internet Dynamics", Ph.D. dissertation, U.C. Berkeley, 1997, ftp://ftp.ee.lbl.gov/papers/vp-thesis/dis.ps.gz.

20. Adresse des auteurs

Vern Paxson
MS 50B/2239
Lawrence Berkeley National Laboratory
University of California
Berkeley, CA 94720
USA
téléphone : +1 510/486-7504
mél : vern@ee.lbl.gov

Guy Almes
Advanced Network & Services, Inc.
200 Business Park Drive
Armonk, NY 10504
USA
téléphone : +1 914/765-1120
mél : almes@advanced.org

Jamshid Mahdavi
Pittsburgh Supercomputing Center
4400 5th Avenue
Pittsburgh, PA 15213
USA
téléphone : +1 412/268-6282
mél : mahdavi@psc.edu

Matt Mathis
Pittsburgh Supercomputing Center
4400 5th Avenue
Pittsburgh, PA 15213
USA
téléphone : +1 412/268-3319
mél : mathis@psc.edu

21. Déclaration complète de droits de reproduction