Groupe de travail Réseau
Request for Comments : 2680
Catégorie : En cours de normalisation

Traduction Claude Brière de L'Isle

G. Almes
S. Kalidindi
M. Zekauskas
Advanced Network & Services
septembre 1999

Métrique de perte de paquet unidirectionnelle pour IPPM

Statut de ce mémoire

Le présent document spécifie un protocole Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et des suggestions pour son amélioration. Prière de se reporter à l'édition actuelle du STD 1 "Normes des protocoles officiels de l'Internet" pour connaître l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Table des matières

1. Introduction

Le présent mémoire définit une métrique pour la perte de paquet unidirectionnelle à travers les chemins de l'Internet. Elle s'appuie sur les notions introduites et discutées dans le document cadre IPPM, [RFC2330] ; le lecteur est supposé familiarisé avec ce document.

Le présent mémoire est destiné à être parallèle dans sa structure au document qui l'accompagne pou le délai unidirectionnel ("Métrique unidirectionnelle pour IPPM") [RFC2679] ; le lecteur est supposé familiarisé avec ce document.

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" dans ce document, sont à interpréter comme décrit dans la [RFC2119]. Bien que la RFC 2119 ait été écrite en visant les protocoles, les mots clés sont utilisés dans le présent document pour des raisons similaires. Ils sont utilisés pour assurer que les résultats de mesures provenant de deux mises en œuvre différentes sont comparables, et pour noter les instances où une mise en œuvre pourrait perturber le réseau.

La structure du mémoire est la suivante :
+ Une métrique analytique de 'singleton', appelée perte unidirectionnelle de type-P, est introduite pour mesurer une seule observation de transmission ou perte de paquet.
+ En utilisant cette métrique de singleton, un 'échantillon', appelé flux de Poisson de perte unidirectionnelle de type-P, est introduite pour mesurer une séquence de singletons de transmissions et/ou de pertes mesurée à des instants tirés d'un processus de Poisson.
+ En utilisant cet échantillon, plusieurs 'statistiques' de l'échantillon sont définies et discutées.

Cette progression du singleton à l'échantillon et aux statistiques, avec une claire séparation entre eux, est importante.

Chaque fois qu'un terme technique provenant du document cadre IPPM est utilisé pour la première fois dans le présent mémoire, il sera marqué à la fin avec un astérisque. Par exemple, "terme*" indique que "terme" est défini dans la RFC2330.

1.1 Motivation

La compréhension de la perte unidirectionnelle de paquet de type-P* à partir d'un hôte* de source pour un hôte de destination est utile pour plusieurs raisons :
+ Certaines applications ne fonctionnent pas bien (ou pas du tout) si la perte de bout en bout entre les hôtes est grande par rapport à une certaine valeur de seuil.
+ Une perte de paquet excessive peut rendre difficile de prendre en charge certaines applications en temps réel (où le seuil précis de "excessif" dépend de l'application).
+ Plus la valeur de perte de paquet est grande, plus il est difficile aux protocoles de couche transport de soutenir une forte bande passante.
+ La sensibilité à la perte des applications en temps réel et des protocoles de couche transport devient particulièrement importante lorsque des produits à très grand délai/bande passante doivent être pris en charge.

La mesure de la perte unidirectionnelle plutôt que la perte sur l'aller-retour est motivée par les facteurs suivants :
+ Dans l'Internet d'aujourd'hui, le chemin d'une source à une destination peut être différent du chemin de retour de la destination à la source ("chemins asymétriques") de sorte que des séquences de routeurs différentes sont utilisées pour le chemin d'émission et le chemin inverse. Donc, les mesures d'aller-retour mesurent en fait ensemble les performances de deux chemins distincts. Mesurer indépendamment les deux chemins souligne les différences de performances entre les deux chemins qui peuvent traverser des fournisseurs de service Internet différents, et même des types de réseaux radicalement différents (par exemple, des réseaux de recherche par opposition à des réseaux commerciaux, ou ATM par opposition à du paquet-sur-SONET).
+ Même lorsque les deux chemins sont symétriques, ils peuvent avoir des caractéristiques de performances radicalement différentes dues à des mises en file d'attente asymétriques.
+ Les performances d'une application peuvent dépendre principalement des performances dans une direction. Par exemple, un transfert de fichier qui utilise TCP peut dépendre plus des performances dans la direction du flux des données que de celles de la direction dans laquelle voyagent les accusés de réception.
+ Dans les réseaux à qualité de service (QS) l'approvisionnement dans une direction peut être radicalement différent de celui de la direction inverse, et donc, la garantie de QS diffère. Mesurer les chemins de façon indépendante permet la vérification des deux garanties.

Il sort du domaine d'application du présent document de dire précisément comment les métriques de perte seront appliquées à des problèmes spécifiques.

1.2 Problèmes généraux concernant l'heure

{Commentaire : La terminologie ci-dessous diffère de celle définie par les documents de l'UIT-T (par exemple, G.810, "Définitions et terminologie pour la synchronisation des réseaux" et I.356, "Performances de transfert de cellule ATM en RNIS-LB") mais elle est cohérente avec celle du document cadre IPPM. En général, ces différences découlent d'arrière-plans différents ; les documents de l'UIT-T ont historiquement une origine téléphonique, alors que les auteurs du présent document (ainsi que du Cadre) se fondent sur les systèmes informatiques. Bien que les termes définis ci-dessous n'aient pas d'équivalent direct dans les définitions de l'UIT-T, nous donnerons après nos définitions une transposition approchante. On notera cependant une confusion potentielle : notre définition de "horloge" est celle des systèmes d'exploitation

informatique qui notent une horloge qui donne l'heure du jour, alors que la définition de l'horloge de l'UIT-T note une référence de fréquence.}

Chaque fois qu'une heure (c'est-à-dire un moment dans l'histoire) est mentionné ici, il doit être compris qu'elle est mesurée en secondes (et ses fractions) par rapport à l'UTC.

Comme c'est décrit plus complètement dans le document cadre, il y a quatre notions distinctes, mais en rapport, d'incertitude d'horloge :

synchronisation*
C'est la mesure dans laquelle deux horloges s'accordent sur l'heure qu'il est. Par exemple, l'horloge sur un hôte pourrait être de 5,4 µs en avance de l'horloge du second hôte. {Commentaire : à peu près l'équivalent UIT-T de "erreur horaire".}

précision*
C'est la mesure dans laquelle une certaine horloge s'accorde à l'UTC. Par exemple, l'horloge d'un hôte pourrait être de 27,1 µs en retard sur l'UTC. {Commentaire : à peu près l'équivalent UIT-T de "erreur horaire sur l'UTC".}

résolution*
Mesure la précision d'une certaine horloge. Par exemple, l'horloge sur un vieil hôte Unix pourrait battre seulement toutes les 10 ms, et donc avoir une résolution de seulement 10 ms. {Commentaire : à peu près l'équivalent UIT-T de "période d'échantillonnage".}

biais*
Mesure le changement de précision, ou de synchronisation, avec le temps. Par exemple, l'horloge d'un certain hôte pourrait gagner 1,3 ms par heure et donc être 27,1 ms en retard de l'UTC à un moment et seulement de 25,8 ms une heure plus tard. Dans ce cas, on dit que l'horloge de cet hôte a un biais de 1,3 ms par heure par rapport à l'UTC, ce qui menace la précision. On peut aussi parler du biais d'une horloge par rapport à une autre horloge, ce qui menace la synchronisation. {Commentaire : à peu près l'équivalent UIT-T de "dérive horaire".}

2. Définition de singleton pour la perte de paquet unidirectionnelle

2.1 Nom de la métrique

Perte unidirectionnelle de paquet de type P *(Type-P-One-way-Packet-Loss)*

2.2 Paramètres de la métrique

+ Src, adresse IP d'un hôte
+ Dst, adresse IP d'un hôte
+ T, une heure

2.3 Unités de la métrique

La valeur d'une perte unidirectionnelle de paquet de type P est soit zéro (ce qui signifie la transmission réussie du paquet) soit un (qui signifie la perte).

2.4 Définition

>>La *Perte unidirectionnelle de paquet de type P* de Src à Dst à l'instant T est 0<< signifie que Src a envoyé le premier bit d'un paquet de type-P à Dst à l'heure du réseau* T et que Dst a reçu ce paquet.

>>La *Perte unidirectionnelle de paquet de type P* de Src à Dst à l'instant T est 1 << signifie que Src a envoyé le premier bit d'un paquet de type-P à Dst à l'heure du réseau T et que Dst n'a pas reçu ce paquet.

2.5 Discussion

Donc, la perte unidirectionnelle de paquet de type P est 0 exactement lorsque le délai unidirectionnel de type-P est une valeur finie, et elle est 1 exactement lorsque le délai unidirectionnel de type-P est indéfini.

Les questions suivantes vont probablement apparaître en pratique :
+ Une certaine méthodologie devra inclure un moyen de distinguer entre une perte de paquet et un très long délai (mais un

délai fini). Comme noté par Mahdavi et Paxson [RFC2678], on pourrait utiliser de simples bornes supérieures (comme la limite théorique de 255 secondes de la durée de vie des paquets IP [RFC0791]) mais une bonne ingénierie, incluant la compréhension des durées de vie des paquets, sera nécessaire en pratique. {Commentaire : Noter que, pour de nombreuses applications de ces métriques, il peut n'y avoir pas de dommage causé en traitant un long délai comme une perte de paquet. Par exemple, un paquet audio en play-back qui arrive seulement après le point de play-back pourrait aussi bien avoir été perdu.}

+ Si le paquet arrive, mais est corrompu, il est alors compté comme perdu. {Commentaire : On est tenté de compter le paquet comme reçu car la corruption et la perte de paquet sont des phénomènes en rapport, mais distincts. Cependant, si l'en-tête IP est corrompu, on ne peut pas être sûr des adresses IP de source ou de destination et c'est donc sur des bases fragiles qu'on estimerait que le paquet corrompu reçu correspond à un certain paquet d'essai envoyé. De même, si d'autres parties du paquet sont nécessaires pour la méthodologie pour savoir que le paquet corrompu reçu correspond à un certain paquet d'essai envoyé, alors un tel paquet devrait être compté comme perdu. Compter ces paquets comme perdus mais pas les paquets qui ont d'autres parties corrompues serait incohérent.}
+ Si le paquet est dupliqué le long du chemin (ou des chemins) de sorte que plusieurs copies non corrompues arrivent à destination, le paquet est alors compté comme reçu.
+ Si le paquet est fragmenté et si, quelle qu'en soit la raison, le réassemblage ne se fait pas, le paquet sera alors réputé perdu.

2.6 Méthodologies

Comme avec les autres métriques de Type-P-*, la méthodologie détaillée va dépendre du type-P (par exemple, du numéro de protocole, du numéro d'accès UDP/TCP, de la taille, de la préséance).

Généralement, pour un certain type-P, la méthodologie se déroulerait comme suit :

+ S'arranger pour que Src et Dst aient des horloges qui soient synchronisées entre elles. Le degré de synchronisation est un paramètre de la méthodologie, et dépend du seuil utilisé pour déterminer la perte (voir ci-dessous).
+ Chez l'hôte Src, choisir les adresses IP de Src et de Dst, et former un paquet d'essai de type-P avec ces adresses.
+ Chez l'hôte Dst, s'arranger pour recevoir le paquet.
+ Chez l'hôte Src, placer un horodatage dans le paquet de type P préparé, et envoyer le paquet vers Dst.
+ Si le paquet arrive dans un délai raisonnable, la perte de paquet unidirectionnelle prend zéro.
+ Si le paquet ne réussit pas à arriver dans un délai raisonnable, la perte de paquet unidirectionnelle est prise comme étant un . Noter que le seuil de "raisonnable" est ici un paramètre de la méthodologie.

{Commentaire : La définition de raisonnable est intentionnellement vague, et est destinée à indiquer une valeur "Th" si grande que toute valeur dans l'intervalle fermé [Th-delta, Th+delta] soit un seuil équivalent à la perte. Ici, delta renferme toutes les erreur de synchronisation d'horloge le long du chemin mesuré. Si il y a une seule valeur d'après laquelle le paquet doit être compté comme perdu, on réintroduira le besoin d'un degré de synchronisation d'horloge similaire à celui nécessaire pour le délai unidirectionnel. Donc, si une mesure de perte de paquet paramétrée par une valeur spécifique de temporisation "raisonnable" non démesurée est nécessaire, on peut toujours mesurer le délai unidirectionnel et voir quel pourcentage de paquets provenant d'un certain flux excèdent une certaine valeur de temporisation.}

Les questions telles que le format du paquet, les moyens par lesquels Dst sait quand attendre le paquet d'essai, et les moyens par lesquels Src et Dst se synchronisent sortent du domaine d'application du présent document. {Commentaire : On prévoit de documenter ailleurs notre propre travail en décrivant de telles techniques de mise en œuvre plus détaillées, et nous encourageons d'autres à le faire aussi.}

2.7 Erreurs et incertitudes

La description de toute méthode de mesure spécifique devrait inclure une prise en compte et une analyse des diverses sources d'erreur ou d'incertitude. Le document cadre fournit des lignes directrices générales sur ce point.

Pour la perte, il y a trois sources d'erreur :

+ La synchronisation entre horloges sur Src et Dst.
+ Le seuil de perte de paquet (qui se rapporte à la synchronisation entre horloges).
+ Les limites des ressources dans l'interface réseau ou le logiciel sur l'instrument récepteur.

Les deux premières sources sont corrélées et pourraient résulter en ce qu'un paquet d'essai avec un délai fini soit rapporté comme perdu. La perte unidirectionnelle de paquet de type-P est 0 si le paquet d'essai n'arrive pas, ou si il arrive et si la différence entre l'horodatage de Src et l'horodatage de Dst est supérieure au "délai raisonnable", ou au seuil de perte. Si les horloges ne sont pas suffisamment synchronisées, le seuil de perte peut n'être pas "raisonnable" - le paquet peut prendre beaucoup moins de temps pour arriver que ce qu'indique son horodatage de Src. De même, si le seuil de perte est réglé trop bas, de nombreux paquets peuvent alors être comptés comme perdus. Le seuil de perte doit être assez élevé, et les horloges

suffisamment bien synchronisées pour qu'un paquet qui arrive soit rarement compté comme perdu. (Voir les discussions dans les deux paragraphes précédents.)

Comme la sensibilité de la mesure de perte de paquet au manque de synchronisation d'horloge est moindre que pour le délai, on renvoie le lecteur au traitement des erreurs de synchronisation dans la métrique de délai unidirectionnel [RFC2679] pour des précisions.

La dernière source d'erreur, les limites de ressources, causent l'abandon du paquet par l'instrument de mesure, et son comptage comme perdu alors qu'en fait le réseau a livré le paquet dans un délai raisonnable.

Les instruments de mesure devraient être calibrés de telle façon que le seuil de perte soit raisonnable pour l'application des métriques, et les horloges devraient être assez synchronisées pour que le seuil de perte reste raisonnable.

De plus, les instruments devraient être vérifiés pour s'assurer de la possibilité qu'un paquet arrive à l'interface réseau, mais que sa perte due à l'encombrement sur l'interface ou pour d'autre épuisement de ressource (par exemple, des mémoires tampon) sur l'instrument soit faible.

2.8 Rapport de la métrique

Le calibrage et le contexte dans lesquels la métrique est mesurée DOIVENT être examinés avec attention, et DEVRAIENT toujours être rapportés avec les résultats de la métrique. On présente maintenant quatre éléments à considérer : Le type-P des paquets d'essai, le seuil de perte, le calibrage de l'instrument, et le chemin traversé par les paquets d'essai. Cette liste n'est pas exhaustive; et toute information supplémentaire qui pourrait être utile pour les applications d'interprétation des métriques devraient aussi être rapportées.

2.8.1 Type-P

Comme noté dans le document cadre [RFC2330], la valeur de la métrique peut dépendre du type de paquets IP, ou "Type-P", utilisés pour faire la mesure. La valeur du délai unidirectionnel de type-P pourrait changer si le protocole (UDP ou TCP) le numéro d'accès, la taille, ou l'arrangement pour un traitement particulier (par exemple, la préséance IP ou RSVP) change. Le type-P exact utilisé pour faire les mesures DOIT être rapporté avec précision.

2.8.2 Seuil de perte

Le seuil (ou la méthodologie pour distinguer) entre un grand délai fini et une perte DOIT être rapporté.

2.8.3 Résultats de calibrage

Le degré de synchronisation entre les horloges de Src et de Dst DOIT être rapporté. Si possible, la possibilité qu'un paquet d'essai qui arrive à l'interface réseau de Dst soit rapporté comme perdu du fait d'un épuisement de ressource chez Dst DEVRAIT être rapportée.

2.8.4 Chemin

Finalement, le chemin traversé par le paquet DEVRAIT être rapporté, si possible. En général, il est impraticable de savoir le chemin précis que prend un certain paquet à travers le réseau. Le chemin précis peut être connu pour certains types-P sur des chemins courts ou stables. Si le type-P inclut l'option d'enregistrement de chemin (ou le chemin de source lâche) dans l'en-tête IP, et si le chemin est assez court, et si tous les routeurs* sur le chemin prennent en charge l'enregistrement de chemin (ou la source lâche) alors, le chemin sera enregistré avec précision. Cela est impraticable parce que le chemin doit être assez court, que de nombreux routeurs ne prennent pas en charge (ou ne sont pas configurés pour prendre en charge) l'enregistrement de chemin, et que l'utilisation de ce dispositif empirerait souvent artificiellement les performances observées en soustrayant le paquet au processus de traitement ordinaire. Cependant, des informations partielles sont quand même un contexte précieux. Par exemple, si un hôte peut choisir entre deux liaisons* (et donc deux chemins séparés de Src à Dst) alors la liaison initiale utilisée est un contexte précieux. {Commentaire : Par exemple, avec l'établissement de NetNow de Merit, une Src sur un NAP peut atteindre une Dst sur un autre NAP par l'un ou l'autre de plusieurs cœurs de réseau différents.}

3. Définition des échantillons de perte de paquet unidirectionnelle

Étant donnée la métrique de singleton de perte unidirectionnelle de paquet de type-P, on définit maintenant un échantillon particulier de tels singletons. L'idée de l'échantillon est de choisir un lien particulier des paramètres Src, Dst, et type-P, puis de définir un échantillon des valeurs du paramètre T. Le moyen pour définir les valeurs de T est de choisir une heure de début T0, une heure de fin Tf, et un taux moyen lambda, puis de définir un processus pseudo aléatoire de Poisson de taux lambda, dont les valeurs tombent entre T0 et Tf. L'intervalle de temps entre les valeurs successives de T seront en moyenne 1/lambda.

{Commentaire : Noter que l'échantillonnage de Poisson est seulement une des façon de définir un échantillon. Il présente l'avantage de limiter le biais, mais d'autres méthodes d'échantillonnage peuvent être appropriées pour différentes situations. Tous sont encouragés à chercher des cas d'utilisation appropriés de ce cadre général et à soumettre leur méthode d'échantillonnage au processus de normalisation.}

3.1 Nom de la métrique

Flux de Poisson de perte unidirectionnelle de paquet de type P *(Type-P-One-way-Packet-Loss-Poisson-Stream)*

3.2 Paramètres de la métrique

+ Src, l'adresse IP d'un hôte
+ Dst, l'adresse IP d'un hôte
+ T0, une heure
+ Tf, une heure
+ lambda, un taux en secondes réciproques

3.3 Unités de la métrique

Une séquence de paires ; les éléments de chaque paire sont :
+ T, une heure,
+ L, soit zéro, soit un.

Les valeurs de T dans la séquence sont d'accroissement monotone. Noter que T serait un paramètre valide pour la perte unidirectionnelle de paquet de type-P, et que L serait une valeur valide de perte unidirectionnelle de paquet de type-P.

3.4 Définition

Connaissant T0, Tf, et lambda, on calcule un processus de Poisson pseudo-aléatoire commençant à T0 ou avant, avec un taux d'arrivée moyen de lambda, et se terminant à Tf ou après. Les valeurs horaire supérieures ou égales à T0 et inférieures ou égales à Tf sont alors choisies. À chaque instant de ce processus, on obtient la valeur de perte unidirectionnelle de type-P à cet instant. La valeur de l'échantillon est la séquence constituée des paires <heure, perte> résultantes. Si il n'y a pas de telles paires, la séquence est de longueur zéro et l'échantillon est dit vide.

3.5 Discussion

Le lecteur devrait être familiarisé avec l'exposé détaillé sur l'échantillon de Poisson dans le document cadre [RFC2330], qui comporte les méthodes pour calculer et vérifier le processus pseudo-aléatoire de Poisson.

Il n'y a pas de contrainte spécifique sur la valeur de lambda, sauf à noter les extrêmes. Si le taux est trop élevé, le trafic de mesure va alors perturber le réseau, et causer lui-même de l'encombrement. Si le taux est trop faible, on ne peut alors pas capturer un comportement de réseau intéressant. {Commentaire : On prévoit de documenter nos expériences et suggestions sur lambda par ailleurs, pour arriver à un document de "bonnes pratiques actuelles".}

Comme une séquence de nombres pseudo-aléatoires est employée, la séquence des instants, et donc la valeur de l'échantillon, n'est pas pleinement spécifiée. Des générateurs de nombres pseudo-aléatoires de bonne qualité seront nécessaires pour atteindre les qualités désirées.

L'échantillon est défini selon les termes d'un processus de Poisson aussi bien pour éviter les effets d'auto-synchronisation que pour capturer un échantillon qui soit statistiquement aussi peu biaisé que possible. Le processus de Poisson est utilisé pour programmer les mesures de délai. Les paquets d'essai ne vont généralement pas arriver à Dst selon une distribution de Poisson, car ils sont influencés par le réseau.

{Commentaire : Il n'est, bien sûr, pas demandé que le trafic Internet réel arrive selon un processus de Poisson.

Il est important de noter que, à l'opposé de cette métrique, les taux de perte observés par les connexions de transport ne reflètent pas des échantillons sans biais. Par exemple, les transmissions TCP (1) surviennent en salves,qui peuvent induire des pertes à cause du volume de salve qui n'aurait pas été observé autrement, et (2) adaptent leur taux de transmission pour tenter de minimiser le taux de perte observé sur la connexion.}

Toute la métrique de singleton de perte unidirectionnelle de paquet de type-P dans la séquence aura les mêmes valeurs de Src, Dst, et Type-P.

Noter aussi que, pour un certain échantillon courant de T0 à Tf, et étant données de nouvelles valeurs horaires T0' et Tf' telles que $T0 \leq T0' \leq Tf' \leq Tf$, la sous-séquence de cet échantillon dont les valeurs horaire tombent entre T0' et Tf' sont aussi un échantillon valide de flux de Poisson de perte unidirectionnelle de paquet de type-P.

3.6 Méthodologies

Les méthodologies découlent directement :
+ du choix des instants spécifiques, en utilisant le processus d'arrivée de Poisson spécifié, et
+ des méthodologies déjà discutées pour la métrique de singleton de perte unidirectionnelle de paquet de type-P.

Il faut faire attention à traiter correctement les arrivées décalées des paquets d'essai ; il est possible que la Src envoie un paquet d'essai à TS[i], puis envoie un second paquet (plus tard) à TS[i+1], alors que Dst pourrait recevoir le second paquet d'essai à TR[i+1], et ensuite recevoir le premier paquet (plus tard) à TR[i].

3.7 Erreurs et incertitudes

En plus des erreurs et incertitudes des source associées aux méthodes employées pour mesurer les valeurs de singleton qui constituent l'échantillon, il faut faire attention à analyser la précision du processus d'arrivée de Poisson de l'heure du réseau de l'envoi des paquets d'essai. Des problèmes avec ce processus pourraient être causés par plusieurs choses, y compris des problèmes avec les techniques de nombre pseudo-aléatoire utilisées pour générer le processus d'arrivée de Poisson. Le document cadre montre utiliser l'essai de Anderson-Darling pour vérifier la précision du processus de Poisson sur de petites trames temporelles. {Commentaire : Le but est de s'assurer que les paquets d'essai sont envoyés "assez près" d'une programmation de Poisson, et d'éviter un comportement périodique.}

3.8 Rapport de la métrique

Le calibrage et le contexte pour le singletons sous-jacents DOIVENT être rapportés avec le flux. (Voir à "Rapporter la métrique" pour la perte unidirectionnelle de paquet de type-P.)

4. Quelques définitions statistiques pour la perte de paquet unidirectionnelle

Étant donnée la métrique d'échantillon de flux de Poisson de perte unidirectionnelle de paquet de type-P, on présente maintenant plusieurs statistiques de cet échantillon. Ces statistiques sont présentées principalement à titre d'illustration de ce qui peut être fait.

4.1 Moyenne de perte unidirectionnelle de paquet de type-P

Étant donné un flux de Poisson de perte unidirectionnelle de paquet de type-P, c'est la moyenne de toutes les valeurs L dans le flux. De plus, la moyenne de perte unidirectionnelle de paquet de type-P est indéfinie si l'échantillon est vide.

Exemple : supposons qu'on prenne un échantillon et que les résultats soient :

Flux1 = <
<T1, 0>
<T2, 0>
<T3, 1>
<T4, 0>
<T5, 0>
>

La moyenne serait alors 0,2.

Noter que, comme des chemins Internet en bonne santé devraient fonctionner à des taux de perte inférieurs à 1 % (en particulier si des produits à fort délai/bande passante doivent être assurés) les tailles d'échantillon nécessaire pourraient être plus importantes que ce qu'on aimerait, par exemple, si on veut faire la différence entre diverses fractions de 1 % sur des périodes de une minute, plusieurs centaines d'échantillons par minute pourraient alors être nécessaires. Cela résulterait en plus grandes valeurs de lambda que ce qu'on veut ordinairement.

Noter que bien que le seuil de perte ne devrait pas être établi à un niveau tel que chaque erreurs en perte ne soit pas significative, si la possibilité qu'un paquet qui est arrivé soit compté comme perdu à cause d'un épuisement de ressource est significative comparée au taux de perte qui nous intéresse, la moyenne de perte unidirectionnelle de paquet de type-P sera in signifiante.

5. Considérations pour la sécurité

La pratique de mesures sur l'Internet soulève des problèmes à la fois de sécurité et de confidentialité. Le présent mémoire ne spécifie pas de mise en œuvre des métriques, de sorte qu'il n'affecte pas directement la sécurité de l'Internet ni des applications qui fonctionnent sur l'Internet. Cependant, les mises en œuvre de ces métriques doivent être attentives aux problèmes de sécurité et de confidentialité.

Il y a deux types de problèmes de sécurité : les dommages potentiels causés par les mesures, et les dommages potentiels aux mesures. Les mesures pourraient causer des dommages parce qu'elles sont actives, et elles injectent des paquets dans le réseau. Les paramètres de mesure DOIVENT être choisis avec soin afin que les mesures injectent des quantités triviales de trafic supplémentaire dans les réseaux qu'elles mesurent. Si elles injectent "trop" de trafic, elles peuvent biaiser les résultats des mesures, et dans des cas extrêmes, causer de l'encombrement et des dénis de service.

Les mesures elles-mêmes pourraient être endommagées par des routeurs qui donneraient aux mesures de trafic une priorité différente que celle du trafic "normal", ou par un agresseur qui injecterait des mesures de trafic artificielles. Si des routeurs peuvent reconnaître le trafic de mesure et le traiter séparément, les mesures ne vont pas refléter le trafic réel d'usager. Si un agresseur injecte du trafic artificiel qui est accepté comme légitime, le taux de perte sera artificiellement diminué. Donc, les méthodologies de mesure DEVRAIENT inclure des techniques appropriées pour réduire la probabilité que du trafic de mesures puisse être distingué du trafic "normal". Des techniques d'authentification , telles que les signatures numériques, peuvent être utilisées lorsque approprié pour se garder contre les attaques de trafic injecté.

Les problèmes de confidentialité de mesure de réseau sont limitées par les mesures actives décrites dans le présent mémoire. À la différence des mesures passives, il peut n'y avoir pas de livraison de données d'usager existant.

6. Remerciements

Merci à Matt Mathis pour avoir encouragé ce travail et avoir attiré notre attention en de nombreuses occasions sur la signification de la perte de paquet.

Merci aussi à Vern Paxson pour ses précieux commentaires sur les premiers projets, et à Garry Couch et Will Leland pour plusieurs suggestions utiles

7. Références

[RFC0791] J. Postel, éd., "Protocole Internet - Spécification du protocole du programme Internet", STD 5, septembre 1981.

[RFC2026] S. Bradner, "Le processus de normalisation de l'Internet -- Révision 3", (BCP0009) octobre 1996. (*MàJ par* RFC3667, RFC3668, RFC3932, RFC3979, RFC3978, RFC5378, RFC6410)

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.

[RFC2330] V. Paxson, G. Almes, J. Mahdavi, M. Mathis, "Cadre pour la mesure des performances d'IP", mai 1998. *(Information)*

[RFC2678] J. Mahdavi, V. Paxson, "Métrique IPPM pour la mesure de la connexité", septembre 1999. *(P.S.)*

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

8. Adresse des auteurs

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

Sunil Kalidindi
Advanced Network & Services, Inc.
200 Business Park Drive
Armonk, NY 10504
USA
téléphone : +1 914 765 1128
mél : kalidindi@advanced.org

Matthew J. Zekauskas
Advanced Network & Services, Inc.
200 Business Park Drive
Armonk, NY 10504
USA
téléphone : +1 914 765 1112
mél : matt@advanced.org

9. Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est actuellement fourni par l'Internet Society.