Groupe de travail Réseau
Request for Comments : 5560
Catégorie : Sur la voie de la normalisation

H. Uijterwaal, RIPE NCC
mai 2009
Traduction Claude Brière de L'Isle

Métrique unidirectionnelle de duplication de paquet

Résumé
Quand a paquet est envoyé d'un hôte à un autre, on s'attend normalement à ce que exactement une copie du paquet envoyé arrive à la destination. Il est cependant possible qu'un paquet soit perdu ou que plusieurs copies arrivent.

Une métriquc pour la perte de paquet a été définie dans un travail antérieur. Cette métrique quantifie le cas où un paquet qui est envoyé n'arrive pas à sa destination dans un délai raisonnable. Dans le présent mémoire, une métrique pour un autre cas est définie : un paquet est envoyé, mais plusieurs copies arrivent. Le document discute aussi des flux et des méthodes pour résumer le résultat des flux.

Table des matières

1. Introduction

Le présent document définit une métrique pour la duplication unidirectionnelle de paquet à travers les chemins de l'Internet. Il s'appuie sur le document de cadre des métriques de performances IP (IPPM, *IP Performance Metrics*) [RFC2330] ; le lecteur est supposé être familier avec ce document.

Le présent document suit la même structure que le document pour la perte unidirectionnelle de [RFC2680] ; le lecteur est aussi supposé être familier avec ce document.

La structure du présent mémoire est comme suit :

- D'abord, une métrique de singleton, appelée Type-P-one-way-packet-arrival-count *(compte d'arrivée unidirectionnelle de paquet de type P)* est introduite pour mesurer le nombre de paquets arrivant pour chaque paquet envoyé.

- Ensuite, une métrique de singleton, appelée Type-P-one-way-packet-duplication *(duplication de paquet unidirectionnel de type P)* est définie pour décrire une seule instance de duplication de paquet.

- Ensuite, cette métrique de singleton est utilisée pour définir des échantillons, Type-P-one-way-Packet-Duplication-Poisson-Stream *(flux de Poisson de duplication de paquet unidirectionnel de type P)* et Type-P-one-way-Packet-Duplication-Periodic-Stream *(flux périodique de duplication de paquet unidirectionnel de type P)*. Ceux-ci sont introduits pour mesurer la duplication dans une série de paquets envoyés avec des intervalles à distribution de Poisson [RFC2680] ou périodique [RFC3432] entre les paquets.

- Finalement sont introduites des statistiques qui résument les propriétés de ces échantillons.

1.1 Notation des exigences

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

Bien que la RFC 2119 ait été écrite en visant des protocoles, les mots clés sont utilisés dans le présent document pour des raisons similaires. Ils sont utilisés pour assurer que les résultats des mesures provenant de différentes mises en œuvre sont comparables et pour noter les instances où une mise en œuvre pourrait perturber le réseau.

1.2 Motivation

Quand un paquet est envoyé d'un hôte à l'autre, on s'attend normalement à ce qu'exactement une copie du paquet envoyé arrive à la destination. Il est cependant possible qu'un paquet soit perdu ou que plusieurs copies arrivent.

La [RFC2680] définissait une métrique pour la perte de paquet. Cette métrique distingue les cas où le paquet arrive et ceux où le paquet n'arrive pas dans un délai raisonnable. Dans le présent mémoire, une métrique pour un troisième résultat est définie : un seul paquet est envoyé, mais plusieurs copies arrivent.

Comme le présent document décrit un cas similaire à celui discuté dans la [RFC2680], toutes les considérations provenant

de ce document sur le temps et la précision s'appliquent.

2. Définition d'un singleton pour le compte d'arrivée de paquet unidirectionnelle

2.1 Nom de la métrique

Type-P-one-way-packet-arrival-count *(compte d'arrivée unidirectionnelle de paquet de type P)*

2.2 Paramètres de la métrique

- src *(source)* : l'adresse IP d'un hôte
- dst *(destination)* : l'adresse IP d'un hôte
- T, heure du réseau d'un paquet à la source
- T0, temps maximum d'attente qu'un paquet arrive à la destination.

2.3 Unités de la métrique

Un nombre entier.

2.4 Définition

Deux paquets sont considérés être identiques si et seulement si :

- Tous deux contiennent des champs d'information identiques (voir le paragraphe 2.5). Le receveur pourrait donc prendre un paquet ou l'autre et utiliser les données dans une application. L'autre paquet ne contient aucune information supplémentaire.
- Les deux paquets apparaissent avoir été envoyés par un seul et même hôte, à une et même destination. Les hôtes sont identifiés par leur adresse IP.

La valeur d'un Type-P-one-way-packet-arrival-count est un nombre entier positif indiquant le nombre de copies (non corrompues et identiques) reçues par dst dans l'intervalle [T, T+T0] pour un paquet envoyé par src à l'instant T.

Si un paquet est envoyé, mais est perdu ou n'arrive pas dans l'intervalle [T, T+T0], alors la métrique est indéfinie. Les applications PEUVENT rapporter une valeur "impossible" (par exemple, -1) pour indiquer cette condition au lieu de "indéfinie".

Si un paquet est fragmenté durant le transport et si, pour une raison quelconque, le réassemblage ne se produit pas, alors le paquet va être réputé perdu. Il n'est donc pas inclus dans le Type-P-one-way-packet-arrival-count.

2.5 Discussion

Cette métrique compte le nombre de paquets arrivants pour chaque paquet envoyé. La valeur de temporisation T0 DEVRAIT être réglée à une valeur quand l'application pourrait potentiellement encore utiliser le paquet et ne l'éliminerait pas automatiquement.

Si cette métrique est utilisée en parallèle avec la métrique de perte de paquet [RFC2680], la valeur de T0 DOIT être la même pour les deux cas afin que les résultats soient comparables.

La métrique compte seulement les paquets qui ne sont pas corrompus durant la transmission et peuvent avoir été renvoyés automatiquement par les couches inférieures ou des appareils intermédiaires. Les paquets qui ont été corrompus durant la transmission mais sont, néanmoins, arrivés à destination ne sont pas comptés.

Les horloges doivent être synchronisées entre la source et la destination afin qu'il soit possible de déterminer de façon univoque et précise l'intervalle [T, T+T0] des deux côtés.

Si cette métrique est utilisée dans un système de mesure active, le système NE DOIT PAS envoyer plusieurs paquets avec des champs d'information identiques afin d'éviter que tous les paquets soient déclarés être des dupliqués. Cette métrique peut aussi être utilisée dans un système de mesure passive, en utilisant les paquets générés par une autre source. Cependant, si la source peut envoyer deux paquets identiques dans l'intervalle [T, T+T0], cela va être incorrectement étiqueté comme un dupliqué, résultant en un faux positif. Il appartient à la mise en œuvre d'estimer si ce scénario a une chance de se produire et si le taux de faux positifs est acceptable.

La définition des champs d'information identiques est telle que deux paquets sont considérés comme identiques si ils sont envoyés de la même source et contiennent les mêmes informations. Cela ne signifie pas nécessairement que tous les bits dans le paquet sont les mêmes. Par exemple, quand un paquet est dupliqué et que les copies sont transférées sur des chemins différents, la durée de vie (TTL, *Time to Live*) peut être différente. La mise en œuvre DOIT spécifier quels champs sont comparés quand elle décide si deux paquets sont identiques ou non.

Dans le cas de IPv4, cela va généralement être : version, ihl, identification, src, dst, protocole, certaines ou toutes les données de protocole de couche supérieure.

Dans IPv6, cela va généralement être : version, prochain en-tête, source, destination, certaines ou toutes les données de protocole de couche supérieure.

Noter que l'utilisation du champ Identification n'est pas présente dans les paquets IPv6 non fragmentés et ne peut pas être suffisante pour distinguer les paquets les uns des autres, même dans IPv4, en particulier à des vitesses de transmission élévées

2.6 Méthodologie

La technique de base pour mesurer cette métrique suit la méthodologie décrite au paragraphe 2.6 de la [RFC2680] avec une exception.

La [RFC2680] ne spécifie pas que l'hôte receveur devrait être capable de recevoir plusieurs copies d'un seul paquet, car il a seulement besoin d'une copie pour déterminer les métriques. Les mises en œuvre de cette métrique devraient évidemment être capables de recevoir plusieurs copies.

2.7 Erreurs et incertitudes

Voir le paragraphe 2.7 de la [RFC2680].

2.8 Rapport de métrique

Voir le paragraphe 2.8 de la [RFC2680].

3. Définition de singleton pour duplication de paquet unidirectionnelle

3.1 Nom de métrique

Type-P-one-way-packet-duplication

3.2 Paramètres de métrique

- src *(source)* : l'adresse IP d'un hôte
- dst *(destination)* : l'adresse IP d'un hôte
- T, heure du réseau d'un paquet à la source
- T0, temps maximum d'attente qu'un paquet arrive à la destination.

3.3 Unités de métrique

Un nombre entier.

3.4 Définition

La valeur d'un Type-P-one-way-packet-duplication est un nombre entier positif indiquant le nombre de copies (non corrompues et identiques) supplémentaires d'un paquet individuel reçu par la destination dans l'intervalle [T, T+T0] comme envoyé par la source à l'instant T.

Si un paquet est envoyé et si seulement une copie arrive dans l'intervalle [T, T+T0], alors la métrique est 0. Si aucune copie

n'arrive dans cets intervalle, alors la métrique est indéfinie. Les applications PEUVENT rapporter une valeur "impossible" (par exemple, -1) pour indiquer cette condition.

3.5 Discussion

Cette métrique est égale à : Type-P-one-way-packet-arrival-count - 1

Cette métrique est supposée être utilisée pour des applications qui ont besoin de connaître la duplication pour un paquet individuel. Toutes les considérations concernant la méthodologie, les erreurs, et le repport de la section précédante s'appliquent.

4. Définition des échantillons pour la duplication de paquet unidirectionnelle

4.1 Flux de Poisson

4.1.1 Nom de métriquue

Type-P-one-way-Packet-Duplication-Poisson-Stream

4.1.2 Paramètres de métrique

- src *(source)* : l'adresse IP d'un hôte
- dst *(destination)* : l'adresse IP d'un hôte
- Ts, un instant.
- Tf, un instant. Ts et Tf spécifient l'intervalle de temps où les paquets peuvent être envoyés pour ce flux.
- T0, temps d'attente maximum pour qu'un paquet arrive à destination.
- lambda, taux en secondes réciproques.

4.1.3 Unités de métrique

Séquence de paires ; les éléments de chaque paire sont :
- T, un instant.
- Type-P-one-way-packet-arrival-count pour le paquet envoyé à T.

4.1.4 Définition

Étant donnés Ts, Tf, et lambda, on calcule un processus de Poisson pseudo-aléatoire commençant à ou avant Ts, avec un taux moyen lambda, et se terminant à ou après Tf. Des valeurs de temps supérieures ou égales à Ts, et inférieures ou égales à Tf sont alors choisies. À chaque instant de ce processus, on obtient la valeur de Type-P-one-way-packet-arrival-count. La valeur de l'échantillon est la séquence constituée des paires résultantes {instant, duplication}. Si il n'y a pas de telles paires, la séquence est de longueur zéro, et l'échantillon est dit être vide.

4.1.5 Méthodologie

Voir le paragraphe 3.6 de la [RFC2680].

4.1.6 Erreurs et incertitudes

Voir le paragraphe 3.7 de la [RFC2680].

4.1.7 Rapport de la métrique

Voir le paragraphe 3.8 de la [RFC2680].

4.2 Flux périodiques

4.2.1 Nom de métrique

Type-P-one-way-Packet-Duplication-Periodic-Stream

4.2.2 Paramètres de métrique

- src *(source)* : l'adresse IP d'un hôte
- dst *(destination)* : l'adresse IP d'un hôte
- Ts, un instant.
- Tf, un instant. Ts et Tf spécifient l'intervalle de temps où les paquets peuvent être envoyés pour ce flux.
- T0, temps d'attente maximum pour qu'un paquet arrive à destination.
- lambda, taux en secondes réciproques.

4.2.3 Unités de métrique

Une séquence de paires ; les éléments de chaque paire sont :
- T, un instant.
- Type-P-one-way-packet-arrival-count pour le paquet envoyé à T.

4.2.4 Définition

À l'instant Ts, on commence à envoyer des paquets avec un taux constant lambda, jusqu'à l'instant Tf. Pour chaque paquet envoyé, on obtient la valeur de Type-P-one-way-packet-arrival-count. La valeur de l'échantillon est la séquence constituée des paires résultantes {instant, duplication}. Si il n'y a pas de telles paires, la séquence est de longueur zéro et l'échantillon est dit être vide.

4.2.5 Méthodologie

Voir le paragraphe 4.5 de la [RFC3432].

4.2.6 Erreurs et incertitudes

Voir le paragraphe 4.6 de la f [RFC3432].

4.2.7 Rapport de la métrique

Voir le paragraphe 4.7 de la [RFC3432].

5. Définitions statistiques pour duplication unidirectionnelle

Note : les statistiques décrites dans cette section peuvent être utilisées pour Type-P-one-way-Packet-Duplication-Poisson-Stream et Type-P-one-way-Packet-Duplication-Periodic-Stream. L'application DEVRAIT rapporter quel échantillon a été utilisé comme entrée.

5.1 Type-P-one-way-paquet-duplication-fraction

Cette statistique donne la fraction des paquets supplémentaires qui sont arrivés dans un flux.

Étant donné un Type-P-one-way-Packet-Duplication-Poisson-Stream, on supprime d'abord toutes les valeurs de Type-P-one-way-Packet-Duplication qui sont indéfinies. Pour les paires restantes dans le flux, on calcule : (Somme de Type-P-one-way-packet-arrival-count/Nombre de paires laissées) - 1 (En d'autres termes, (nombre de paquets reçus)/(nombre de paquets envoyés et non perdus).)

Le nombre peut être exprimé comme un pourcentage.

Note : cette statistique est l'équivalent de l'IPDR [Y.1540].

5.2 Type-P-one-way-replicated-packet-rate

Cette statistique donne la fraction des paquets qui étaient dupliqués (une ou plusieurs fois) dans un flux.

Étant donné un Type-P-one-way-Packet-Duplication-Poisson-Stream, on supprime d'abord toutes les valeurs de Type-P-one-way-packet-arrival-count qui sont indéfinies. Pour les paires restantes dans le flux, on compte le nombre de paires avec Type-P-one-way-packet-arrival-count supérieur à 1. Puis on calcule la fraction des paquets qui satisfont ce critère comme une fraction du total. (En d'autres termes : (nombre de paquets dupliqués)/(nombre de paquets envoyés et non perdus).)

Le nombre peut être exprimé comme un pourcentage.

Note : cette statistique est l'équivalent de RIPR [Y.1540].

5.3 Exemples

Considérons un flux de 4 paquets, envoyés comme : (1, 2, 3, 4)
et arrivant comme :
- Cas 1 : (1, 2, 3, 4)
- Cas 2 : (1, 1, 2, 2, 3, 3, 4, 4)
- Cas 3 : (1, 1, 1, 2, 2, 2, 3, 3, 3, 4, 4, 4)
- Cas 4 : (1, 1, 1, 2, 3, 3, 3, 4)

Cas 1 : aucun paquet n'est dupliqué dans un flux, et Type-P-one-way-packet-duplication-fraction et Type-P-one-way-packet-replicated-paquet-rate sont tous deux 0.

Cas 2 : chaque paquet est dupliqué une fois, et Type-P-one-way-packet-duplication-fraction est 100 %. Le Type-P-one-way-replicated-packet-rate est 100 %, également.

Cas 3 : chaque paquet est dupliqué deux fois, de sorte que Type-P-one-way-packet-duplication-fraction est 200 %. Le Type-P-one-way-replicated-packet-rate est toujours 100 %.

Cas 4 : la moitié des paquets sont dupliqués deux fois et ceux de l'autre moitié ne sont pas dupliqués. Le Type-P-one-way-packet-duplication-fraction est à nouveau 100 %, et ce nombre ne montre pas la différence avec le cas 2. Cependant, le Type-P-one-way-packet-replicated-paquet-rate est 50 % dans ce cas et 100 % dans le cas 2.

Cependant, le Type-P-one-way-packet-duplication-rate ne va pas montrer la différence entre les cas 2 et 3. Pour cela, on doit regarder le Type-P-one-way-packet-duplication-fraction.

Finalement, on note que l'ordre dans lequel les paquets sont arrivés n'affecte pas le résultat. Par exemple, ces variantes du cas 2 :
- Cas 2a : (1, 1, 2, 2, 3, 3, 4, 4)
- Cas 2b : (1, 2, 3, 4, 1, 2, 3, 4)
- Cas 2c : (1, 2, 3, 4, 4, 3, 2, 1)

(ainsi que toute autre permutation) donnent toutes le même résultat pour Type-P-one-way-packet-duplication-fraction et Type-P-one-way-replicated-packet-rate.

6. Considérations sur la sécurité

Effectuer des mesures sur l'Internet soulève des problèmes à la fois de sécurité et de confidentialité. Le présent mémoire ne spécifie pas une mise en œuvre des métriques, donc il d'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 soucieuses des problèmes de la sécurité et de la confidentialité

Il y a deux types de problèmes de sécurité : le dommage potentiel causé par les mesures et le dommage potentiel aux mesures. Les mesures pourraient causer des dommages parce que elles sont actives, et elles injectent des paquets dans le

réseau. Les paramètres de mesure DOIVENT être choisis avec soin afin que les mesures n'injectent pas des quantités triviales de trafic supplémentaire dans les réseaux qu'elles mesurent. Si elles injectent "trop" de trafic, elles peuvent biaiser le résultat de la mesure, et dans des cas extrêmes, causer de l'encombrement et un déni de service.

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

Les problèmes de confidentialité de mesure du réseau sont limités par les mesures actives décrites dans le présent mémoire. À la différence des mesures passives, il peut ne pas y avoir de livraison des données d'utilisateur existantes.

7. Considérations relatives à l'IANA

L'IANA a enregistré les métriques définies dans le présent document dans le registre des métriques de performances IP (IPPM), voir la [RFC4148].

8. Remerciements

L'idée d'écrire le présent document vient d'une réunion avec Al Morton, Stanislav Shalunov, Emile Stephan, et l'auteur sur le document de rapport IPPM.

Le présent document s'appuie largement sur la [RFC2680], et l'auteur remercie de l'avoir écrit les auteurs de ce document.

Finalement, des remerciements sont dus à Lars Eggert, Al Morton, Martin Swany, et Matt Zekauskas pour leurs commentaires.

9. Références

9.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. DOI 10.17487/RFC2119, *(MàJ par* RFC8174)

[RFC2680] G. Almes, S. Kalidindi, M. Zekauskas, "Métrique de perte de paquet unidirectionnelle pour IPPM", septembre 1999. *P.S. ; Remplacée par* RFC7680)

[RFC3432] V. Raisanen et autres, "Mesure des performances réseau avec des flux périodiques", novembre 2002. *(P.S.)*

9.2 Références pour information

[RFC2330] V. Paxson, G. Almes, J. Mahdavi, M. Mathis, "Cadre pour la mesure des performances d'IP", mai 1998. *(Information ; MàJ par* RFC8468, RFC9198)

[RFC4148] E. Stephan, "Registre des métriques de mesure des performances d'IP (IPPM)", août 2005. BCP0108 *; Obs, voir* RFC6248)

[Y.1540] Recommandation UIT-T Y.1540, "Service de communication de données au protocole Internet – Transfert de paquet IP et paramètre de performances de disponibilité", Union Internationale des Télécommunications, Genève, décembre 2002.

Adresse de l'auteur

Henk Uijterwaal
RIPE NCC
Singel 258
1016 AB Amsterdam
The Netherlands
téléphone : +31 20 535 4444
mél : henk@ripe.net