Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: October 3, 2007

H. Uijterwaal
RIPE NCC

April 2007

A One-Way Packet Duplication Metric for IPPM
draft-ietf-ippm-duplicate-01.txt

Status of this Memo

Copyright Notice

Abstract

The IETF IPPM working group has defined a metric for packet loss. The packet loss metric quantifies the case where a packet that is sent, never arrives at its destination. However, the opposite is also possible: a packet is sent and arrives more than once. This document defines a metric to quantify these kinds of events.

Table of Contents

1. Introduction

This document defines a metric for one-way packet duplication across Internet paths. It builds on the IPPM Framework document [RFC2330]; the reader is assumed to be familiar with that document.

This document follows the same structure as the document for One-way Packet Loss [RFC2680]; the reader is assumed to be familiar with that document as well.

The structure of this memo is as follows:

- First, a singleton metric, called Type-P-One-way-packet-duplication, is introduced to describe a single instance of packet duplication.
- Then, this singleton metric is used to define a sample, Type-P-One-way-Packet-Duplication-Poisson-Stream, is introduced to measure duplication in a series of packets sent.
- Finally, a method to summarise the properties of this sample is introduced.

1.1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

1.2. Motivation

The IETF IPPM working group has defined a metric for packet loss [RFC2680]. The packet loss metric quantifies the case where a packet that is sent, never arrives at its destination. However, the opposite is also possible: a packet is sent and arrives more than once. This document defines a metric to quantify these kinds of events.

As this document describes a case similar to the one discussed in

[RFC2680], all considerations from that document on timing and accuracy apply.

2. A Singleton Definition for One-Way Packet Duplication

2.1. Metric Name

Type-P-One-way-Packet-Duplication

2.2. Metrics Parameters

- Src, the IP address of a host
- Dst, the IP address of a host
- T, a time
- T0, a time

2.3. Metric Units

A positive integer number

2.4. Definition

The value of a Type-P-One-way-Packet-Duplication is a positive integer number indicating the number of (uncorrupted and identical) copies received by dst in the interval [T, T+T0] for a packet sent by src at time T.

If a packet is sent, but it is lost or does not arrive in the interval [T, T+T0], then the metric is undefined.

2.5. Discussion

This metric counts the number of packets arriving for each packet sent. The time-out value T0 SHOULD be set to a value when the application could potentially still use the packet and not discard it automatically.

The metric only counts packets that are not corrupted during

transmission and may have been resent automatically by lower layers or intermediate devices. Packets that were corrupted during transmission but nevertheless still arrived at dst are not counted.

If a packet is fragmented and one of the fragments arrives more than once, then the packet is counted as duplicated.

2.6. Methodology

Refer to section 2.6 of [RFC2680] (We may cut and paste relevant text into this document later).

2.7. Errors and uncertainties

Refer to section 2.7 of [RFC2680] (We may cut and paste relevant text into this document later).

2.8. Reporting the metric

Refer to section 2.8 of [RFC2680] (We may cut and paste relevant text into this document later).

3. A definition for Samples of One-way Packet Duplication

3.1. Metric Name

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

3.2. Metric Parameters

- Src, the IP address of a host
- Dst, the IP address of a host
- Ts, a time
- T0, a time
- Tf, a time
- lamba, a rate in reciprocal seconds

3.3. Metric Units

A sequence of pairs; the elements of each pair are:
o T, a time
o Type-P-One-way-Packet-Duplication for the packet sent at T.

3.4. Definition

Given Ts, Tf and lambda, we compute a pseudo-random Poisson process beginning at or before Ts, with average rate lambda and ending at or after Tf. Those time values greater than or equal to Ts, and less than or equal to Tf are then selected. At each of the times in this process, we obtain the value of Type-P-One-way-Packet-Duplication. the value of the sample is the sequence made up of the resulting {time, duplication} pairs. If there are no such pairs, the sequence is of length zero and the sample is said to be empty.

3.5. Methodology

Refer to [RFC2680]

3.6. Errors and uncertainties

Refer to [RFC2680]

3.7. Reporting the metric

Refer to [RFC2680]

4. Some statistics definitions for One-way Duplication

4.1. Type-P-one-way-packet-duplication-average

This statistics gives an estimate of the fraction of additional packets that arrived in a stream.

Given a Type-P-One-way-Packet-Duplication-Poisson-Stream, one first removes all values of Type-P-One-way-Packet-Duplication which are undefined. For the remaining pairs in the stream, one calculates:

(Sum Type-P-One-Way-Packet-Duplication/Number of pairs left) - 1 (In other words, #packets received/(#sent and not lost).)

The number can be expressed as a percentage.

Note: this statistics is the equivalent of the Y.1540 IPDR [Y1540]

4.2. Type-P-one-way-packet-duplication-rate

This statistics gives an estimate of the fraction of packets that was duplicated (one or more times) in a stream.

Given a Type-P-One-way-Packet-Duplication-Poisson-Stream, one first removes all values of Type-P-One-way-Packet-Duplication which are undefined. For the remaining pairs in the stream, one counts the number of pairs with Type-P-One-Way-Packet-Duplication greater than 1. Then one calculates the fraction of packets that meet this criterium as a fraction of the total. (In other words: # with duplication/(#sent and not lost).).

The number can be expressed as a percentage.

Note: this statistics is the equivalent of the Y.1540 RIPR [Y1540]

4.3. Examples

Consider a stream of 4 packets, sent as:

(1, 2, 3, 4)

and arriving as:

- Case 1: (1, 2, 3, 4)
- Case 2: (1, 1, 2, 2, 3, 3, 4, 4)
- Case 3: (1, 1, 1, 2, 2, 2, 3, 3, 3, 4, 4, 4)
- Case 4: (1, 1, 1, 2, 3, 3, 3, 4)

Case 1: No packets are duplicated in a stream and both the Type-P-one-way-packet-duplication-average and the type-P-one-way-packet-duplication-rate are 0.

Case 2: Every packet is duplicated once and the Type-P-one-way-packet-duplication-average is 100%. The type-P-one-way-packet-duplication-rate is 100% too.

Case 3: Every packet is duplicated twice, so the Type-P-one-way-packet-duplication-average is 200%. The type-P-one-way-packet-duplication-rate is still 100%.

Case 4: Half the packets are duplicated twice and the other half are not duplicated. The Type-P-one-way-packet-duplication-average is again 100% and this number does not show the difference with case 2. However, the type-P-one-way-packet-duplication-rate is 50% in this case and 100% in case 2.

However, the type-P-one-way-packet-duplication-rate will not show the difference between case 2 and 3. For this, one has to look at the Type-P-one-way-packet-duplication-average.

5. Security Considerations

Conducting Internet measurements raises both security and privacy concerns. This memo does not specify an implementation of the metrics, so it does not directly affect the security of the Internet nor of applications which run on the Internet. However, implementations of these metrics must be mindful of security and privacy concerns.

There are two types of security concerns: potential harm caused by the measurements, and potential harm to the measurements. The measurements could cause harm because they are active, and inject packets into the network. The measurement parameters MUST be carefully selected so that the measurements inject trivial amounts of additional traffic into the networks they measure. If they inject "too much" traffic, they can skew the results of the measurement, and in extreme cases cause congestion and denial of service.

The measurements themselves could be harmed by routers giving measurement traffic a different priority than "normal" traffic, or by

an attacker injecting artificial measurement traffic. If routers can

recognize measurement traffic and treat it separately, the measurements will not reflect actual user traffic. If an attacker injects artificial traffic that is accepted as legitimate, the loss rate will be artificially lowered. Therefore, the measurement methodologies SHOULD include appropriate techniques to reduce the probability measurement traffic can be distinguished from "normal" traffic. Authentication techniques, such as digital signatures, may be used where appropriate to guard against injected traffic attacks.

The privacy concerns of network measurement are limited by the active measurements described in this memo. Unlike passive measurements, there can be no release of existing user data.

6. Relation with Y.1540

Do we need this?

7. IANA Considerations

This document makes no requests from the IANA. This section can be removed upon publication as a RFC.

8. Acknowledgements

The idea to write this draft came up in a meeting with Al Morton, Stanislav Shalunov, Emile Stephan and the author.

This document relies heavily on [RFC2680] and the author likes to thank the authors of that document for writing it.

Finally, thanks are due to ... for their comments.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

9.2. Informative References

[RFC2330] Paxson, V., Almes, G., Mahdavi, J., and M. Mathis, "Framework for IP Performance Metrics", RFC 2330,

May 1998.

[RFC2680] Almes, G., Kalidindi, S., and M. Zekauskas, "A One-way Packet Loss Metric for IPPM", RFC 2680, September 1999.

[Y1540] A. Morton, "Y.1540", July 2003.

Author's Address

Henk Uijterwaal
RIPE NCC
Singel 258
1016 AB Amsterdam
The Netherlands

Phone: +31 20 535 4444
Email: henk@ripe.net

Full Copyright Statement

Intellectual Property

ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).