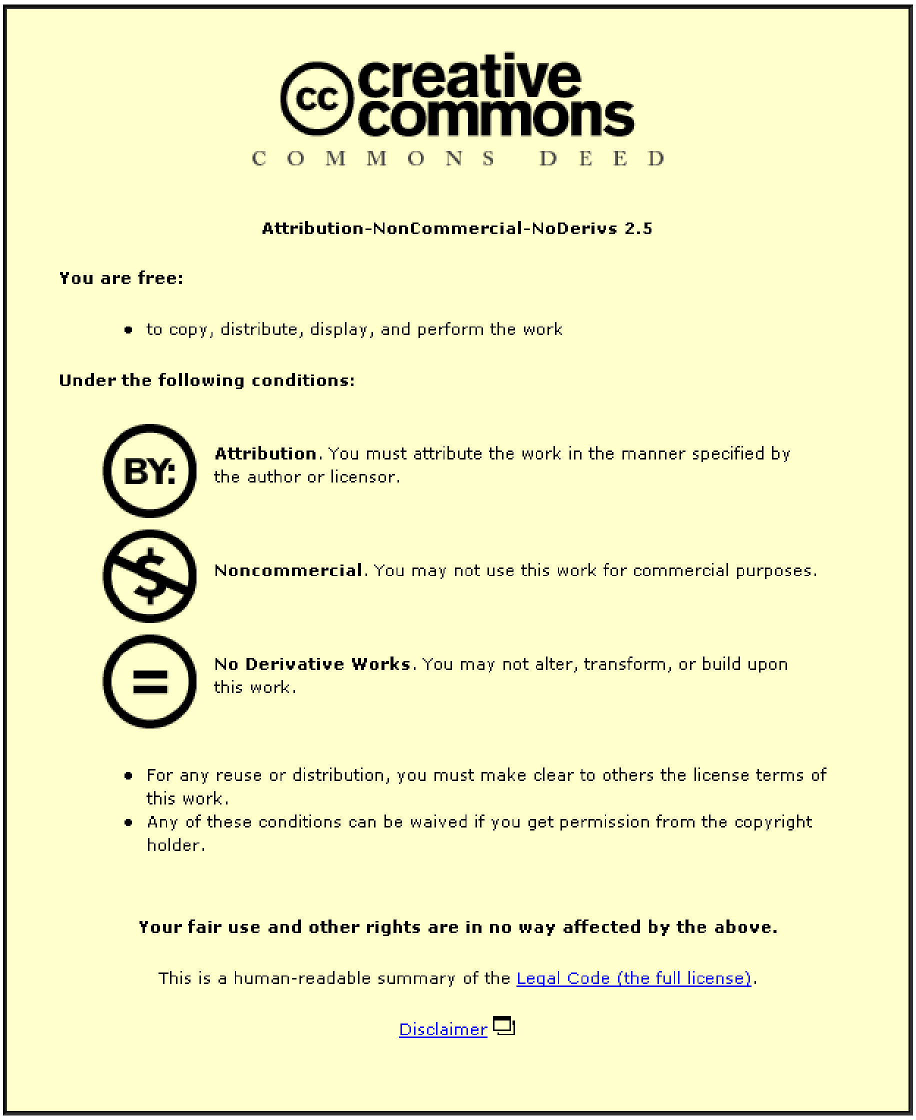

Processing Network Delay Measurements into Network Events

Iain Phillips
Department of Computer Science
Loughborough University,
Leics, LE11 3TU, UK.
I.W.Phillips@lboro.ac.uk

Mark Sandford, David Parish
Department of Electronic Engineering,
Loughborough University,
Leics, LE11 3TU, UK.
J.M.Sandford, D.J.Parish@lboro.ac.uk

1. Introduction

Network Performance Monitoring is an ongoing process as networks and their users are constantly changing. Networks are subject to various changes, some of which are controlled by the network providers (such as upgrades or re-routes) and some are not (equipment failure, usage). Network monitoring may include the detecting of such changes. These changes can be referred to as network *events*. Note that these events can be good or bad.

Examples of events include network elements coming online or going offline, faults such as broken cables, and changes in delay due to user traffic. Each of these will have an effect on delays measured on routes through the network.

Many other workers have considered the measurement of service levels, for example the time for an email transmission, the time to download a newsgroup or web page, the availability of a server [1,2,3]. This work concentrates on the use of low-level measurements of single-way and round-trip delay and loss usually measured from the network edges to generate network events. In this work we refer to such events as *Data Exceptions*. This method of monitoring is particularly relevant when access to the inside of a network is restricted, e.g., for confidentiality or regulatory conditions, or simply practicality.

2. Data Exceptions

A Data Exception is an instance of unusual performance data that indicates some kind of network event has occurred. As there can be many sources of performance data all relating to the same network, one network event may give rise to numerous data exceptions. In plotting a graph of percentile of delay against time several exceptions can often be seen. Those referred to as step changes, spikes and changes in time-of-day-delay variation are considered here.

A frequently observed data exception, known as a *Step Change*, occurs when the average delays either increase or decrease in such a way that all test packets are affected. That is to say that delay is altered by a constant amount for each packet.

Spikes are sharp increases in delay that last for a relatively short period of time. The increase need not affect all the test packets although the more test packets it affects the more significant it is likely to be. Spikes can be of any size, although to be classified as spike it must be clearly observable above fluctuation in delay caused by load.

0-7803-5864-3 © 2000 IEEE

It is expected that delays increase during those times when usage is higher, for example working hours. This change in delay is called *time-of-day-delay variation.* Changes in this can be significant, for example, a time of day variation change could be due to an increase or decrease in load due to client activity. Changes in time of day variation can also result from reconfiguration of the network, and it is not uncommon for step changes and changes in time of day variation to occur together.

Data Exception types can be defined for other forms of performance data. For instance, lost packet exceptions might include Loss of Service and High Proportion of Loss.

3. Event Generation

The interpretation of measurements is potentially complex. The work in this paper refers to part of a developed rule-based system that is currently monitoring real networks. To generate exceptions measurement data are analysed historically, a day at a time. Three hourly percentile values are calculated and then these are used to generate parameters (called features) that summarise the data. Examples of features are mean and standard deviation.

Collectively the features form a *feature set* that characterises the data. A new feature set is created for each day. Each feature set is used in conjunction with the current, or previous feature set to form a set of *indicators.* Indicators are values that indicate whether or not a significant change in the data has taken place. Examples of indicators are: the ratio of the maximum to the minimum feature and the ratio of consecutive standard deviation. These indicators are tested against thresholds. The thresholds can be altered depending on the network being monitored.

We expect the fastest packets to be carried with the same delay every day. A step change is therefore detected by comparing the quickest packets on successive days. If this change is significant (around 500 microseconds) then a step change can be reported.

Comparing the slowest of say, the 95th, percentile delays in a day with the next slowest and the fastest allows generation of a *spike* exception.

The standard deviation of the percentile values compared day-to-day indicates a *time-of-day-delay variation.*

All the data is searched for data exceptions. Individually these exceptions only give a partial view of a network event, not a complete picture. Collectively however, data exceptions allow us to understand the impact of a network event and provide a diagnostic opportunity.

4. References

[1] M.A.Oliver, I.W.Phillips, D.J.Parish, K.Bharadia, "Determining application sensitivity to network loading conditions", Irish Signals and Systems Conference, ISSC '98, Dublin Institute of Technology, pp 117 - 124, June 1998.

[2] HP Fire Hunter Product – www.firehunter.com

[3] G. Liu, A. K. Mok, E. J. Yang, "Composite Events for Network Event Correlation", in M.Sloman, S.Mazemdar, Emil Lupu, Integrated Network Management VI, pp 247-260, Boston 1999