Properties of Network Faults *

Marina Thottan
Bell Laboratories, Holmdel, NJ
marinat@lucent.com
Chuanyi Ji
Department of ECSE, RPI, Troy, NY
chuanyi@ecse.rpi.edu

Abstract

Network fault management is a difficult task due to the lack of accurate definitions for the different types of faults. In this work we attempt to characterize network faults by studying their effects on the statistics of network traffic. The evolution of networks in terms of size and variety of network components and services makes it difficult to understand the dynamics of the traffic. Instead, by describing network fault behavior in terms of the changes they effect on the statistics of network traffic, we can develop algorithms to detect or predict network faults. The advantage is the independence of fault descriptions from symptom specific feature vectors and the availability of historical data.

It is observed that predictable faults produce a transient performance degradation before causing a full blown failure. These transient fault signatures are considered as short range correlated signals that are embedded in normal network traffic. In this work, network traffic is measured in terms of the MIB variables. We focus on traffic related faults that affect the network layer devices. Hence the relevant MIB variables are *ipInReceives*, *ipInDelivers*, and *ipOutRequests*. The transient changes of each variable can indicate some problematic behavior. In fault instances however, the transient changes associated with the MIB variables are correlated. This phenomenon is attributed to the dependencies that are inherent in the MIB data. Therefore predictable faults are defined as follows: *Before or during the occurrence of a network fault, traffic related MIB variables undergo transient changes in a correlated fashion.* A typical example of the presence of correlated transient changes in the different MIB variables before the occurrence of a fault is shown in Figure 1. The trace corresponds to a 4 hour period. The fault region is denoted using asterisks. The magnitude of the changes observed in the MIB variables are shown. A value of 0 indicates the absence of transient changes and a value of 1 corresponds to maximum magnitude of change. Note from the lower three plots that the magni-

*Work done while M. Thottan was at RPI. Authors acknowledge DARPA (contract: F30602-97-C-0274)

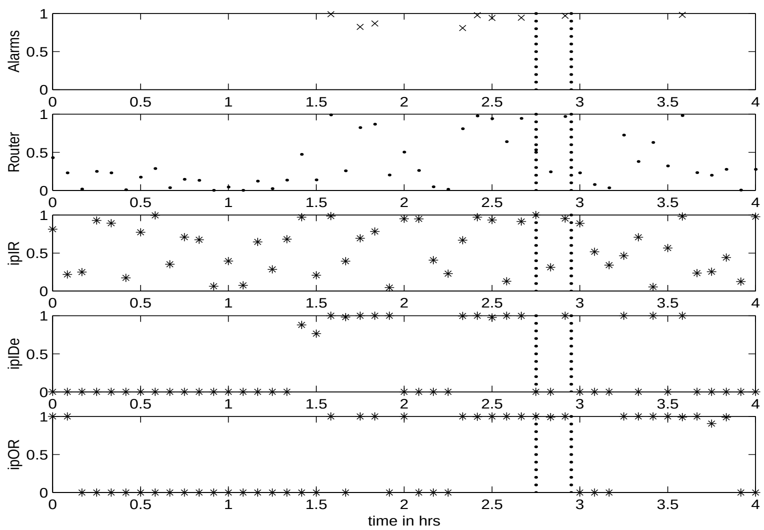

Figure 1: Correlated Abrupt Changes Observed in the *ip* Level MIB Variables

tude of changes in all the three variables increases prior to the occurrence of the fault. Thus showing that the changes in the MIB variables occur in a correlated fashion before fault events. This correlation property is used to obtain router health. Persistence of the correlated transient changes is another property of network faults. Note that prior to fault situations the correlated changes (see router) exhibited a persistent high value over a time period. The persistence criteria is used to declare alarms corresponding to network fault situations.

Understanding the statistical behavior of network faults helps obtain a general classification scheme for network faults as shown in Figure 2. Classification

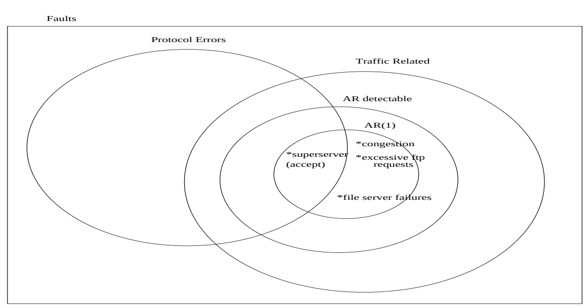

Figure 2: Fault Classification

is based on the statistical order of the AR process used to characterize the transient changes. Continued data collection and increasing number of fault cases available will yield new insights into the nature of network faults.