

Detecting Traffic Anomalies using an Equilibrium Property

Fernando Silveira^{†*} Christophe Diot[†] Nina Taft[◇] Ramesh Govindan[‡]

[†]Technicolor ^{*}UPMC Paris Universit s
[◇]Intel Labs Berkeley [‡]University of Southern California

ABSTRACT

When many flows are multiplexed on a non-saturated link, their volume changes over short timescales tend to cancel each other out, making the average change across flows close to zero. This equilibrium property holds if the flows are nearly independent, and it is violated by traffic changes caused by several correlated flows. We exploit this empirical property to design a computationally simple anomaly detection method.

Categories and Subject Descriptors: C.2.3
[Computer-Communication Networks]: Network Operations

General Terms: Experimentation, Measurement.

Keywords: Anomaly Detection, Statistical Test.

1. INTRODUCTION

A number of techniques have been proposed that detect traffic anomalies by analyzing network traffic. They all seek to expose anomalies by looking for deviations from some underlying model of normal traffic. Usually, this model has to be learned from days or weeks of anomaly-free traffic traces, which is a practical problem since the training data is never guaranteed to be clean and training should be performed periodically.

In this work, we introduce a new approach to anomaly detection that does not require training a model from historical data. Rather, we use a relatively simple, but surprisingly effective, statistical test to infer strong correlations among flows on a single link. This test is based on a mathematical model of a type of equilibrium which we call ASTUTE (A Short-Timescale Uncorrelated-Traffic Equilibrium).

We validate our detector using traces of real traffic data. First, we study the time scales in which our model’s assumptions are valid. Then, we study the sensitivity of our detector to characteristics of the anomalous traffic. Finally, we use ASTUTE to extract real anomalies from our traces. We manually inspect these anomalies to determine the flows responsible for them and their root cause events. Our results show that ASTUTE detect strongly correlated flow changes, i.e., events where several flows simultaneously increase or decrease their volume. Different types of anomalies (e.g., port scans, link outages, routing shifts) exhibit this type of behavior.

2. ASTUTE ANOMALY DETECTION

We describe our anomaly detection method, ASTUTE, and its underlying assumptions. We use real traffic data to analyze ASTUTE’s sensitivity to its parameters and to characteristics of the anomalous traffic.

2.1 Detection Algorithm

A traffic *flow* is a set of packets that share the same values for a given set of traffic features (e.g., source and destination IP addresses, source and destination ports, and protocol number). Time is divided into fixed sized intervals called *bins*. The *volume* of a flow f during bin i is the number of packets in the flow during the corresponding bin. Our model of normal traffic behavior lies on top of two assumptions:

(A1) **A flow’s properties are independent of other flows’ properties.** Although there are practical reasons for flows to be correlated (e.g., session-level structure, congestion in shared links), previous work has shown that inter-flow dependencies in highly aggregated links are normally very weak [1]. We exploit this observation to detect violations of this flow independence assumption, i.e., time bins where flows become strongly correlated.

(A2) **The distributions of flow properties are time-stationary.** Stationarity depends on the timescale in which we observe flows, i.e., the size of time bins. We investigate the timescales in which this assumption holds analyzing real traffic data (later in this section).

Consider a pair of consecutive bins, i and $i + 1$. Let \mathcal{F} be the set of flows that are active in i or $i + 1$. For $f \in \mathcal{F}$, let $\delta_{f,i}$ be the volume change of f from i to $i + 1$. Finally, let Δ_i be the set of $\delta_{f,i}$ ’s for each $f \in \mathcal{F}$. The following theorem provides the foundation of our anomaly detector.

THEOREM 1. *When both (A1) and (A2) hold, the variables in Δ_i are zero mean i.i.d. random variables.*

PROOF. Please refer to our technical report [2].

Let F be the number of flows in \mathcal{F} . Let $\hat{\delta}_i$ be the sample mean and $\hat{\sigma}_i$ be the sample standard deviation of these volume changes. When Theorem 1 holds, for large F , the score:

$$K(\mathcal{F}) = \hat{\delta}_i \sqrt{F} / \hat{\sigma}_i, \quad (1)$$

follows a standard Gaussian random variable. We call $K(\mathcal{F})$ the *ASTUTE assessment value* (AAV) of a time bin. We flag an alarm if $K(\mathcal{F})$ is larger than a detection threshold K' .

2.2 Timescales of Stationarity

To make sure that ASTUTE anomalies are violations of the flow independence assumption, we need to validate the stationarity assumption. Intuitively, at large timescales, stationarity is violated by daily patterns of link usage. To pinpoint the timescales in which stationarity holds, we run our anomaly detection method in a trace from the GEANT2 network¹ for different bin sizes. We then measure the probability that ASTUTE triggers an anomaly at each given time of the day, averaged over a month.

Figure 1 shows this metric for a detection threshold equal to 6. We see that for 5-minute time bins, the probability of detecting an anomaly is uniform throughout the day, indicating it is not sensitive to time-of-day effects. However, for bin sizes larger than 15 minutes, there is a high chance of flagging anomalies when the number of users ramps up in the morning, or drops down in the evening. We have observed the same qualitative result for other traces and different values of the detection threshold. Therefore, in the rest of the paper, we use time bins of 5 minutes.

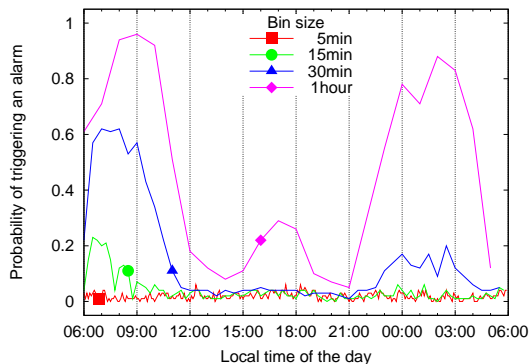


Figure 1: Non-stationarity violates ASTUTE for bins longer than 15 minutes.

2.3 Sensitivity to Anomaly Characteristics

We inject anomalies in the GEANT2 trace to measure ASTUTE’s sensitivity to the number of anomalous flows and the volume in these flows. First, we identify time bins where there are no ASTUTE anomalies. We do this by computing the AAV for each bin, and keeping the bins with an AAV smaller than 2. For each of these bins, we add different amounts of anomalous traffic. We add y anomalous 5-tuples, each with volume change x , for different values of x and y . Then we measure, for each bin, the minimum number of anomalous flows required to trigger an anomaly in ASTUTE. We average this number across all the bins.

Figure 2 shows this metric as a function of the volume per anomalous flow, and for three different values of the detection threshold. The plot shows that given a threshold value, ASTUTE cannot be violated by fewer than a certain number of 5-tuple flows. Note that, for large x values, the minimum number of anomalous flows to trigger an alarm converges approximately to the square of the threshold value. We can generalize this lower bound to all threshold values through a simple mathematical expression (shown in our technical report [2]).

¹GEANT2 - <http://www.geant2.net/>

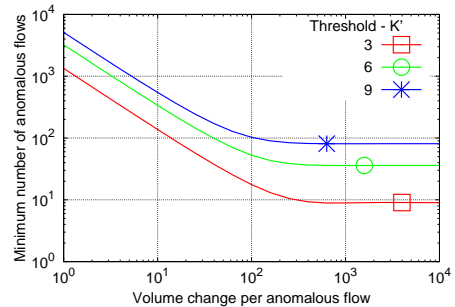


Figure 2: Minimum number of correlated anomalous flows needed to trigger an alarm.

3. EXPERIMENTAL EVALUATION

We extract anomalies from our traces using ASTUTE and we perform manual root cause analysis in order to classify each anomaly according to the type of event that triggered it. This analysis is assisted by information that comes from ASTUTE. Namely, by grouping flows that share features like IP addresses and ports, and checking for ASTUTE in different aggregation levels, we can identify the set of flows causing an anomaly [2]. By analyzing these anomalous flows, we are able to classify the anomalies by type.

Table 3 summarizes the anomalies found in the GEANT2 trace. All of these types of anomalies involves several synchronized flow changes. In port scans, an attacker generates several flows probing ports in a victim. In link failures, all of the flows in the monitored link disappear for one or more time bins. In a prefix outage, the flows to a specific IP prefix disappear, possibly due to a routing change. We also found anomalies caused by measurement gaps, i.e., short periods of no recorded packets. Finally, we were able to discover a legitimate cause for each of these anomalies, i.e., ASTUTE flagged no false alarms.

Anomaly type	# of alarms
Port scan	8
Large file transfer	4
Prefix outage	36
Measurement gap	51
Total	99

Table 1: Anomalies found by ASTUTE in GEANT2.

Our results show that ASTUTE can uncover different types of anomalies, provided they involve several synchronized flows. We have compared ASTUTE to other detectors and used more traces. For all additional results and discussion, we refer the reader to our extended technical report [2].

4. REFERENCES

- [1] N. Hohn, D. Veitch, and P. Abry. Cluster Processes, a Natural Language for Network Traffic. *IEEE Transactions on Networking*, pages 2229–2244, 2003.
- [2] F. Silveira, C. Diot, N. Taft, and R. Govindan. ASTUTE: Detecting a Different Class of Traffic Anomalies. Technical report, Technicolor, 2010. <http://www.thlab.net/~fernando/papers/astute.pdf>.