Characterization of Network-Wide Anomalies in Traffic Flows

Anukool Lakhina, Mark Crovella, and Christophe Diot *

May 19, 2004

BUCS-TR-2004-020

Abstract

Detecting and understanding anomalies in IP networks is an open and ill-defined problem. Toward this end, we have recently proposed the subspace method for anomaly diagnosis. In this paper we present the first large-scale exploration of the power of the subspace method when applied to flow traffic. An important aspect of this approach is that it fuses information from flow measurements taken throughout a network. We apply the subspace method to three different types of sampled flow traffic in a large academic network: multivariate timeseries of byte counts, packet counts, and IP-flow counts. We show that each traffic type brings into focus a different set of anomalies via the subspace method. We illustrate and classify the set of anomalies detected. We find that almost all of the anomalies detected represent events of interest to network operators. Furthermore, the anomalies span a remarkably wide spectrum of event types, including denial of service attacks (single-source and distributed), flash crowds, port scanning, downstream traffic engineering, high-rate flows, worm propagation, and network outage.

*Anukool Lakhina and Mark Crovella are with the Department of Computer Science, Boston University; email: {anukool,crovella}@cs.bu.edu. Christophe Diot is with Intel Research, Cambridge, UK; email: christophe.diot@intel.com. This work was performed while Mark Crovella was at Laboratoire d'Informatique de Paris 6 (LIP6), with support from Centre National de la Recherche Scientifique (CNRS) France. This work was supported in part by a grant from Sprint Labs, and by NSF grants ANI-9986397 and CCR-0325701.

1 Introduction

A general method for detecting anomalies in network traffic is an important, unsolved problem. In principal, it should be possible to observe most anomaly types by inspecting traffic flows. However, to date, there has been little progress on extracting the range of information present in the complete set of traffic flows in a network. There are many good reasons for this: traffic flows present many possible types of network traffic; the set of all flows occupies a very high-dimensional space; and collecting all traffic flows is very resource-intensive. Nonetheless, the increasingly widespread use of tools such as NetFlow [4] by ISPs make it realistic to contemplate methods for efficiently collecting and effectively analyzing traffic flows.

We make three contributions in this paper. First, we show that when traffic flows are aggregated at the Origin-Destination (OD) level, they can provide a wealth of insight into network-wide anomalies. This suggests a strategy for data reduction that can make flow collection for anomaly detection easier. Second, we apply the subspace method [15] to multivariate timeseries of OD flow traffic defined as # bytes, # packets, and # of IP-level flows. We show that each of these traffic types reveals a different (sometimes overlapping) class of anomalies and so all three types together are important for anomaly detection. Finally, we analyze anomalous events from these high-dimensional timeseries. We show that nearly all the anomalies detected by the subspace method are of interest to network operators. The range of anomalies detected is remarkably broad. For example, by analyzing four weeks of flow traffic from the Abilene network, we have been able to identify occurrences of flash crowds, changes in routing policy, worms, Denial of Service attacks, and massive data transfers. We describe the anomalies found and show the features that they tend to exhibit.

This paper represents a first step toward a broadly applicable system for anomaly diagnosis in networks, one which provides detection (stating that an anomaly is present) and identification (stating the type of the anomaly). The paper illustrates the power of the subspace method for detection when applied to traffic flow data. The paper does not propose an anomaly identification method (all our anomalies were identified through manual inspection) but we believe that, given accurate detection, automated methods for anomaly identification will follow.

This paper builds in part on investigations begun by papers [16] and [15]. In [16] we showed basic characteristics of the byte counts in OD flows, without examining packet or flow counts, and without concentrating on anomalies per se. In [15] we introduced the subspace method, but applied it to a different problem (link data). The current paper represents the next step, and goes well beyond the previous two. It shows that OD flow data is a very rich source of information (much richer than the link data examined in [15]). Furthermore, this paper shows that the subspace method can easily extend to a larger and more diverse set of data than [16] and can reveal a surprisingly wide range of anomalies.

This paper is organized as follows. In Section 2, we describe the Abilene flow data we use. A brief review of and necessary extensions to the subspace method are also presented in this section. In Section 3, we demonstrate that the subspace method can successfully extract anomalies from traffic timeseries of bytes, packets and IP-flows collected on the Abilene backbone network. We characterize and classify these anomalies Section 4. In Section 5, we discuss related work. Finally, concluding remarks and future work are presented in Section 6.

2 Methodology

We first introduce the raw traffic data that we collected. Then, we outline the procedure to aggregate this raw data at the level of Origin-Destination flows. We also review the main ideas of the subspace method and show how to extend it to diagnose anomalies in OD flow traffic.

2.1 Network-Wide Traffic Flow Data

Our source of data is IP-level traffic flow measurements collected from the Abilene Internet2 backbone network. Abilene is a major academic network, connecting over 200 US universities and peering with research networks in Europe and Asia. Abilene has 11 points of presence (PoPs) and spans the continental US.[1] The academic and experimental nature of the traffic on Abilene make it an attractive candidate for developing methods to understand anomalies.

We collected sampled flow data from every router of Abilene for a period of four weeks, the week of April 7 to 13, 2003 and the three weeks from December 8 to 28, 2003. Sampling is random, capturing 1% of all packets entering every router. Sampled packets are then aggregated at the 5-tuple IP-flow level (IP address and port number for both source and destination, along with protocol type), every minute using Juniper's Traffic Sampling [13]. The number of bytes and packets in each sampled IP flow are also recorded. This allows us examine three distinct representations of sampled flow traffic, as timeseries of the # of bytes, # of packets and # of IP-flows, all indexed by the 5-tuple headers. Finally, to avoid synchronization issues that could have arisen in the data collection procedure, we aggregated these measurements into 5 minute bins.

The traffic exchanged between an origin-destination pair consists of IP-level flows that enter the network at a given ingress PoP and exit at another egress PoP. We aggregated the IP-level traffic into OD flows. An important advantage of this aggregation is that it dramatically reduces the data volume involved. In order to construct OD flows from the raw traffic collected on all network links, we have to identify the ingress and egress PoPs of each flow. The ingress PoP can be identified by inspecting the router configuration files for interfaces connecting Abilene's customers and peers. For egress PoP resolution, we use BGP and ISIS routing tables as detailed in [8]. We augmented the routing tables with configuration files in order to resolve customer IP addresses that do not appear in the BGP tables. For privacy reasons, Abilene anonymizes the last 11 bits of the destination IP address. This is not a significant concern for egress PoP resolution because there are few prefixes less than 11 bits in the Abilene routing tables. In fact, using this procedure, we were able to successfully obtain the ingress and egress PoPs for more than 93% of all IP flows measured (accounting for more than 90% of the total byte traffic).

Note that our routing tables are computed once a day and stay unchanged for that day. We believe that this does not significantly impact our results since previous studies have found that the impact of routing events on the traffic inside an AS is limited [2, 22]. However, one potential impact is that it becomes more difficult to explain the cause of an anomaly if it is caused by an internal routing change.

To summarize: the data on which we apply the subspace method is OD flow traffic timeseries, defined as the # of bytes, # of packets and # of IP-flows, aggregated at 5 minute intervals for a period of 4 weeks.

In order to faciliate subsequent discussion of this data, we introduce the relevant notation now. We let $\mathbf{X}$ denote the $n \times p$ OD flow traffic multivariate timeseries where $p = 121$ is the number of OD pairs and n is the number of 5-minute bins in the time period being studied. Typically we will study periods of one week and so $n > p$. Thus column i of $\mathbf{X}$ corresponds to the timeseries of OD flow i traffic. Note that we will use $\mathbf{X}$ to refer to either of the three types of traffic (i.e. # bytes, # packets and # IP-flows) and clarify the actual traffic type wherever needed.

[1] The Abilene topology can be found at `www.abilene.iu.edu`.

2.2 The Subspace Method and Extensions

The central ideas behind the subspace method are drawn from the literature on multivariate statistical process control [7, 12]. In [15], we applied the subspace method to detect anomalies in link traffic byte counts. However, anomaly diagnosis using the subspace method is not limited to link traffic alone and can be extended to other multivariate traffic data, such as the three OD flow traffic types. In this section, we briefly review the subspace method and show how to extend it to diagnose anomalies in OD flow traffic.

The subspace method works by examining the timeseries of traffic in all OD flows (*i.e.*, $\mathbf{X}$) simultaneously. It then separates this multivariate timerseries into normal and anomalous attributes. Normal traffic behavior is determined directly from the data, as the temporal patterns that are most common to the ensemble of OD flows. This extraction of common trends is achieved by Principal Component Analysis (PCA). As shown in [16], PCA can be used to decompose the set of OD flows into their constituent eigenflows, or common temporal patterns. A useful property of this decomposition is that the set of eigenflows, $\{\mathbf{u}\}_{i=1}^{p}$, are ordered by the amount of variance they capture in the original data. Thus the first eigenflow, $\mathbf{u}_1$, captures the temporal trend common to all the OD flows, $\mathbf{u}_2$ is the next strongest temporal trend, and so on.

A key result of [16] was that only a handful of eigenflows are sufficient to capture the dominant temporal patterns that are common to the hundreds of OD flows. The subspace method exploits this result by designating the trends in these top k eigenflows, $\{\mathbf{u}\}_1^k$, as normal, and the temporal patterns in the remaining eigenflows as anomalous (we use $k = 4$ throughout). We can then use this separation to reconstruct each OD flow as a sum of normal and anomalous components. In particular, we can write, $\mathbf{x} = \hat{\mathbf{x}} + \tilde{\mathbf{x}}$, where $\mathbf{x}$ denotes the traffic of all the OD flows at a specific point in time, $\hat{\mathbf{x}}$ is the reconstruction of $\mathbf{x}$ using only the top 4 trends and $\tilde{\mathbf{x}}$ contains the residual traffic.

To detect the time of the anomaly, we inspect the residual traffic, $\tilde{\mathbf{x}}$, over time for large changes. As in [15], we can use the squared prediction error, $\|\tilde{\mathbf{x}}\|^2$, to detect such abnormal changes. Specifically, at the time of an anomaly, $\|\tilde{\mathbf{x}}\|^2 > \delta_\alpha$, where δ_α denotes the Q-statistic threshold for the squared prediction error at the 1-α confidence level and is given in [12, 15].

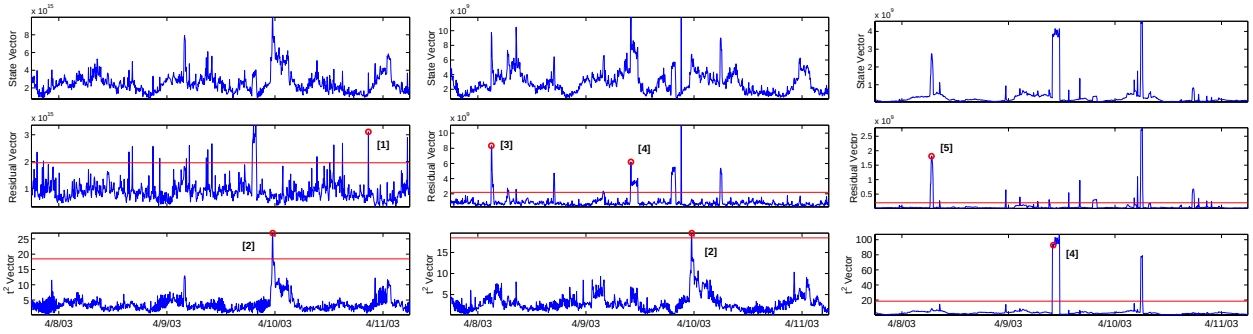
In the context of OD flow traffic (and the new traffic types), we found that the Q-statistic alone is insufficient to detect all anomaly times. Consider the scenario where an unusually large anomaly, or an anomaly that is common to several OD flows, is extracted by PCA in a top eigenflow. If we include this eigenflow in the normal subspace, we cannot detect the anomaly. A common technique used in the statistical process control literature to overcome this problem is to use the T^2 statistic to detect anomalous values in the normal subspace. The T^2 statistic measures how far the modeled data is from its multivariate mean (which, for eigenflows, is equal to zero by construction). To do this, it calculates the sum of squares at each timepoint j of the eigenflows in the normal subspace, as follows:

$$t_j^2 = \sum_{i=1}^{k} u_{ij}^2 \quad j = 1, ..., n.$$

where k is the number of eigenflows in the normal subspace and u_{ij} is the value of the i-th eigenflow at timebin j. For notational convenience, we collect the t_j^2 values at each timebin j in a single timeseries vector $\mathbf{t}^2$. Extremely large values in $\mathbf{t}^2$ are sharp deviations from its mean and hence correspond to anomaly times. These can be detected using the T^2 threshold statistic, which is given as:

$$T_{k,t,\alpha}^2 = \frac{k(n-1)}{n-k} F_{k,n-k,\alpha}$$

where n is the number of samples (timebins), and $F_{k,n-k,\alpha}$ denotes the value of the F distribution with k



(a) # of Bytes (b) # of Packets (c) # of IP-Flows

Figure 1: An illustration of the subspace method on the three types of OD flow traffic. Top row: timeseries of state vector squared magnitude ($\|\mathbf{x}\|^2$); middle row: timeseries of the residual vector squared magnitude ($\|\tilde{\mathbf{x}}\|^2$); bottom row: $\mathbf{t}^2$ vector.

and $n - k$ degrees of freedom at the 1-α the confidence level [11]. An anomaly time is an entry in $\mathbf{t}^2$ that exceeds this threshold value.

Note that the confidence limits for the T^2 test were derived based on an assumption of normality in the underlying data. Since we are applying the T^2 on the projected data, i.e. the eigenflows, this requirement translates to normality in the eigenflows. Strictly speaking, normality in eigenflows means that the underlying OD flows must be multivariate normal. While we have not tested the Abilene OD flows for strict normality, we note that since the eigenflows are linear combinations of the OD flows, one can appeal to the central limit theorem and justify approximate normality for the eigenflows, even when the original variables are not normal. Moreover, we find that the T^2 test yields excellent performance in practice when applied to all three types of traffic data over all datasets.

We found that when extended in this manner, the subspace method effectively detected anomalies with a very low false alarm rate. In the section that follows, we illustrate the effectiveness of the subspace method when it is applied on all three types of OD flow traffic.

3 Applying the Subspace Method

In this section, we illustrate how the subspace method detects anomalies in each of the three types of OD flow timeseries.

Figure 1 shows examples results for the three different views of OD flow traffic over a common 3.5 day period. The top row of Figure 1 presents timeseries of total traffic ($\|\mathbf{x}\|^2$). The middle row shows the timeseries of the residual traffic vector, $\|\tilde{\mathbf{x}}\|^2$, along with the corresponding threshold line. Finally, in the bottom row, we present timeseries of the $\mathbf{t}^2$ metric, along with the statistic threshold. The threshold for both the statistics were computed at the 99.9% confidence level.

Figure 1 illustrates a number of properties of whole-network traffic flow data. The top row of the figure shows that the three types of OD flow traffic can differ substantially. This suggests that the three data types present complementary information about the nature of traffic across the network. Furthermore, each of these views is noisy and appears to be nonstationary, showing noticeable diurnal cycles.

The lower two rows of the figure show how effective the subspace method is at isolating and highlighting anomalies (values above the threshold represent anomaly detection). The periodicity in the original traffic is

largely removed, and anomalies appear as distinct "spikes" against a background of noise. The power of the method is also seen in the fact that the $\mathbf{t}^2$ metric for bytes and packets extracts some similar features from the data (*e.g.,* the anomaly (2) occuring on 4/10) despite the fact that the original traffic timeseries (top row) in each case is very different.

The figure also shows that the set of anomalies detected in each traffic type (# bytes, # packets, and # IP-flows) is noticeably different. This shows that each traffic type is important for detecting anomalies, a point which we substantiate quantitively in the next section.

To illustrate the diverse set of anomalies detected in a common 3.5 day period across the traffic types, we have marked selected anomalies from each type along with their likely explanations. Anomaly labeled (1) is a byte anomaly and corresponds to a bandwidth measurement experiment, (2) corresponds to a similar bandwidth measurement experiment but appears in both byte and packet traffic types, (3) is packet anomaly corresponding to a DOS attack on port 110 (smtp), (4) appears in packet and IP-flow traffic types and is a DOS attack on port 113 (identd), and (5) is an IP-flow anomaly that appears to be caused by a port scan. In the next section, we describe how we identified these and all of other detected anomalies.

4 Characterization of Anomalies

Having detected anomalies in each of the three traffic types, we now characterize these anomalies. We seek to understand the type of information that can be extracted from network-wide traffic flows, and the utility of the subspace method in performing the extraction.

The subspace method designates a time instant during which traffic is anomalous. Thus the first step to identifying the nature of the anomaly is to pinpoint the set of OD flows involved. We used a straightforward method: since each anomaly results in a value of the $\|\tilde{\mathbf{x}}\|^2$ or $\mathbf{t}^2$ that exceeds the threshold statistic, we determine the smallest set of OD flows, which if removed from the corresponding statistic, would bring it under threshold. More sophisticated identification methods are possible if one adopts a hypothesis-testing view (as was used in [15]); however since a goal of our study is to characterize anomalies, by definition we do not have an *a priori* set of hypothesized anomalies ready for testing.

The next step is to aggregate anomalies in space and time. We start with the set of anomalies cast as triples of *(traffic type, time, OD flow)* where "traffic type" is one of Bytes (B), Packets (P), or IP-Flows (F). We first aggregate all triples with the same time value, placing some triples into the new categories BP, BF, FP, and BFP. Thus a BP anomaly is one that is detected in both byte and packet timeseries at the same time. Then we group triples to form anomalies in space (all OD flows corresponding to the same traffic type and time) and time (all triples with consecutive time values, having the same traffic type). This results in our final set of anomalies, in which each anomaly has an associated set of OD flows and potentially spans consecutive time bins.

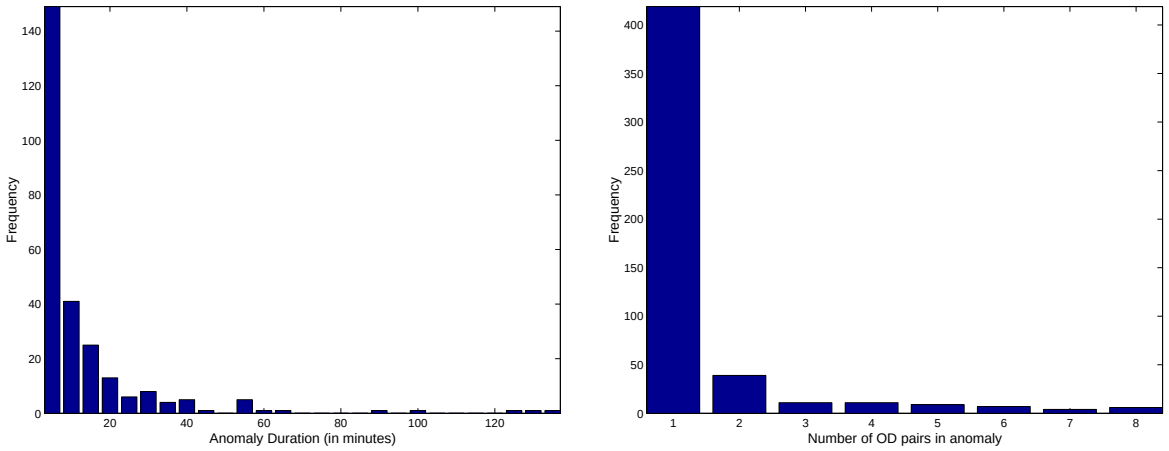
The number of such anomalies found in our four weeks of data is shown in Table 1. This table shows a number of interesting features. First of all, each traffic type (B, F, and P) is important for detecting anomalies, allowing detection of anomalies that are not systematically detected in the other types. Secondly, a relatively small set of anomalies are detected in more than one traffic type. Indeed, there are no anomalies that are detected in just the bytes and flows simultaneously.

Histograms of anomaly duration and size (measured in number of participating OD flows) are shown in Figure 2. The figure shows that most anomalies are small, both in time and space; however a non-negligible number of anomalies can be quite large.

We inspected each of the anomalies identified to determine their root causes. To aid our inspection, we developed a semi-automated procedure that encoded common patterns found in the data, and output a

Traffic	B	F	P	BF	BP	FP	BFP
# Found:	74	142	102	0	27	28	10

Table 1: Number of anomalies found in each traffic type.



(a) Anomaly Duration (b) # of OD Flows responsible

Figure 2: Quantifying the scope of network-wide anomalies by duration and by the number of OD flows involved.

tentative classification for each anomaly. However each classification was checked by hand to ensure its correctness.

In classifying anomalies, an important distiguishing tool is the notion of a *dominant* IP address range and/or port. An address range or port is dominant in a particular OD flow and timebin if it is unusually prevalent. We used a simple threshold test: if the address range or port accounted for more than a fraction p of the total traffic (defined over either of the three types) in the timebin, it was considered dominant. We found that a value of $p = 0.2$ worked well. We used this threshold test to determine, for each anomaly, whether any source address range, destination address range, source port, or destination port was dominant. We emphasize that this heuristic is simply one way to identify and classify anomalies, and other heuristics may also work well.

After inspecting each anomaly, and taking into account the presence of dominant features in the anomaly, we were able to group all anomalies into the categories shown in Table 2. About 10% of the anomalies could not be placed in any category. In addition, about 8% of anomalies after inspection turned out to be false alarms (meaning that visual inspection of traffic timeseries showed no distinctly unusual changes in volume).

Most of the entries in Table 2 are fairly easy to distinguish by inspecting the dominant attributes of the raw flows. ALPHA flows are high-rate flows from a single source to a single destination which account for a dominant fraction of byte traffic. These can be distinguished from DOS and DDOS attacks, which feature a dominant fraction of packet or flow traffic, all to a single destination. The distinction between FLASH-CROWD and DOS anomalies can be difficult. We adopted the heuristic in [10] which starts from the assumption that DOS attacks are always spoofed. In that light, traffic emerging from topologically clustered hosts and directed to well known destination ports (*e.g.* port 53 (dns) or 80 (web)) are classified as flash crowd events. As a result, some of the flash crowds we detect may be DOS attacks in reality.

Anomaly	Definition	Features	Examples
ALPHA	Unusually high rate point to point byte transfer [20].	Spike in B, P and BP traffic, attributable to a single dominant pair (source and destination). Short duration (less than 10mins), and limited to single OD flow.	Bandwidth measurement experiments by [21] and [19].
DOS, DDOS	(Distributed) Denial of service attack against a single victim.	Spike in P, F or FP traffic, the dominant fraction of which is destined to a single destination IP, with no dominant source IP. Can involve multiple OD flows and typically last less than 20mins.	Multiple instances where a large number of packets are sent to a single destination IP at ports that are frequent targets of DOS attacks (*e.g.,* port 0)
FLASH CROWD	Unusually large demand for a resource/service [10].	Spike in F or FP traffic towards a dominant destination IP and dominant destination port. Typically short-lived and limited to a single OD flow.	Multiple instances of large number of web requests to single IP (port 80).
SCAN	Scanning a host for a vulnerable port (port scan) or scanning the network for a target port (network scan)	Spike in F traffic, with similar number of packets as flows from a dominant source; no dominant combination of destination IP and port. Can involve multiple OD flows and typically last less than 10mins.	Network scans for port 139 (NetBIOS).
WORM	Self-propogating code that spreads across a network by exploiting security flaws.	Spike in F traffic with no dominant destination, and only a dominant port.	Found flows with dominant port 1433 (known to be used by the MS SQL-Snake worm).
POINT TO MULTI-POINT	Distribution of content from one server to many users.	Spike in P, B or BP traffic from a dominant source to numerous destinations, all at the same (well known) port.	Single server broadcasts at port 119 (news nntp service) to large destination set.
OUTAGE	Events that cause decrease in traffic exchanged between an OD pair.	Decrease in BFP traffic, usually to zero. Can last for long duration (hours) and in all instances, affected multiple OD flows.	Instances of scheduled maintanance downtime (verified by [1]) at LOSA PoP on 4/17, and a measurement failure from CHIN PoP on 12/21.
INGRESS-SHIFT	Customer shifts traffic from one ingress point to another ingress point.	Decrease in F traffic for one OD flow and a spike in F traffic for another. No dominant attribute. Involves multiple OD flows.	Multihomed Abilene customer CALREN shifted its traffic from LOSA to SNVA during LOSA outage.

Table 2: Types of anomalies, with their attributes as seen in sampled network-wide flow measurements. The examples are actual anomalies detected by the subspace method and identified from manual inspection.

We relied on port information to manually verify a large set of our anomaly classifications. For example, we found that most ALPHA traffic was exchanged between dominant ports that ranged from 5000-5050 (used by bandwidth experiments conducted at [21]), port 56117 (used by pathdiag [19]), and port 1412 (used by filesharing applications such as kazaa/morpheus). Most of the DOS anomalies targetted port 0, although we found instances of a large numer of packets targetting a single destination at port 110 (smtp) and in another case, port 113 (identd). Moreover, we uncovered instances of flow traffic that used a dominant port 445 in our April data, which perhaps was caused by the March outbreak of the Deloader worm [5]. Other suspicious worm anomalies featured large spikes in flow traffic with the dominant attribute as port 1433 (sql server); we conjecture that these could be lingering remnants of the MS SQL-Snake worm, which spread using this port.

We also found instances of anomalies with no dominant attribute. Many of these anomalies had sharp dips in traffic volume. By correlating these dips with the Abilene Operations weekly reports [1], we were able to find explanations for most of the traffic dips. One interesting consequence of an outage event that we detected was a surge in traffic that lasted the same duration and occurred elsewhere in the network. Closer inspection revealed that this was an example of a multihomed customer routing traffic around the outage.

What is most striking about Table 2 is the extremely wide range of anomaly types detected. They range from unusual end-user behavior (ALPHA, FLASH CROWD, POINT/MULTIPOINT), to malicious end-user behavior, (either actual DOS, DDOS, WORM or potentially malicious SCANs), to operational events such as equipment outage (OUTAGE) and downstream traffic engineering (INGRESS SHIFT). The fact that all of these events can be detected in a straightforward manner from whole-network traffic data is one of the principal contributions of our work.

The count of each type of anomaly found is shown in Table 3. The most prevalent anomaly type is the ALPHA flow, which is primarily detected in byte and packet traffic. The high prevalence of ALPHA flows is due to the bandwidth-measurement experiments routinely run over Abilene; thus, a commercial network would probably not show a similar pattern. We detected a large amount of network and port scanning, and a similarly large number of flash-crowd events. Operational events (equipment outages and customer traffic shifts) are less frequent.

Table 3 also illustrates the different kind of information that is present in each type of traffic. ALPHA flows tend to be detected as byte or packet anomalies; this makes sense since the root cause of these events is an attempt to move a large amount of data over the network. DOS events tend to be detected as flow or packet anomalies, but not as byte anomalies; this makes sense since the purpose of the attack is to generate interrupts and other per-packet effects on the target, but not to move a large amount of payload data. SCAN events are naturally flow anomalies; each new combination of port and target IP generates a new flow, without trasmitting an unusually large number of packets or bytes. Finally, FLASH events are also naturally flow anomalies because each source IP generates a distinct flow.

Finally, we note that the table illustrates the remarkably low false alarm rate of the subspace method. Only about 8% of the anomalies detected turned out to be false alarms. Thus almost any anomaly detected by this method appears to be of interest to network operators, whether as a case of unusual user behavior, or malicious user activity, or significant operational events. Note however that about 10% of the anomalies detected could not be classified; we believe that this is largely an effect of our less-than-perfect (*i.e.*, manual) anomaly classification methods and that further study would probably uncover important causes of these anomalies as well.

Type	ALPHA	DOS	SCAN	FLASH	PT.-MULT.	WORM	OUTAGE	INGR.-SHIFT	Unknown	False Alarm
B	59	4	1	1	0	0	0	0	4	5
F	5	19	44	50	0	2	1	0	8	13
P	54	18	2	2	2	0	0	1	13	10
BP	19	0	0	0	0	0	0	1	6	1
FP	0	3	8	10	0	0	0	1	5	1
BFP	0	0	1	1	1	0	2	1	3	1
Total	137	44	56	64	3	2	3	4	39	31

Table 3: Range of anomalies found for each traffic type.

5 Related Work

To the best of our knowledge, this is the first work to expose and characterize the breadth of network-wide traffic anomalies that can be detected from sampled flow measurements in an IP network.

The general area of classifying network anomalies (not necessarily traffic anomalies) has received much attention recently. Researchers have characterized Internet intrusion activity [24], failure events in IP networks [17], and also constructed taxonomies for Internet worms [23], denial of service attacks [9] and defenses [18].

Earlier related work has focused on detecting and classifying anomalies from flow measurements taken at a single router or link. Barford *et al* employed a wavelet-based signal analysis of flow traffic to characterize single-link byte anomalies [3]. In [6], Duffield *et al* proposed techniques to infer the population of worm infections from sampled traffic measurements. The authors of [10] provided topological clustering heuristics for a web server to distinguish denial of service attacks from flash crowd behavior. We use a simplified version of their heuristic to distinguish these two anomalies. The authors in [14] devised a number of heuristics to detect specific attack patterns from flow header data, although no evaluation on real data is given. The principal distinguishing feature of our work is that we characterize a wide range of network-wide (as opposed to single-link) traffic anomalies, by aggregating sampled flow measurements at the origin-destination level.

6 Conclusion and Future Work

In this paper, we showed how to harness the wealth of information that is present in sampled traffic flows to detect and understand network-wide anomalies. We showed that whole network anomalies can be accurately detected from aggregating traffic flows at the level of Origin-Destination flows, and by employing the three readily available traffic types: # of bytes, # of packets and # of IP-flows. We illustrated that a remarkable breadth of anomalies, ranging from unusual customer behavior to malicious activity to network failures, can be detected by applying the subspace method to such data. Our work thus forms the first characterization of traffic anomalies that span IP networks.

Our ongoing work is centered on further validating the subspace method and developing extensions for automatic anomaly classification. Thus this paper constitutes a first but promising step towards our broader goal of practical, online diagnosis of network-wide anomalies.

References

[1] Abilene Network Operations Center Weekly Reports. At `http://www.abilene.iu.edu/routages.cgi`.

[2] S. Agarwal, C.-N. Chuah, S. Bhattacharyya, and C. Diot. The Impact of BGP Dynamics on Intra-Domain Traffic. In *ACM SIGMETRICS*, New York, June 2004.

[3] P. Barford, J. Kline, D. Plonka, and A. Ron. A signal analysis of network traffic anomalies. In *Internet Measurement Workshop*, Marseille, November 2002.

[4] Cisco NetFlow. At `www.cisco.com/warp/public/732/Tech/netflow/`.

[5] Deloader Worm Description. At `http://www.f-secure.com/v-descs/deloader.shtml`.

[6] N. Duffield, C. Lund, and M. Thorup. Estimating Flow Distributions from Sampled Flow Statistics. In *ACM SIGCOMM*, Karlsruhe, August 2003.

[7] R. Dunia and S. J. Qin. Multi-dimensional Fault Diagnosis Using a Subspace Approach. In *American Control Conference*, 1997.

[8] A. Feldmann, A. Greenberg, C. Lund, N. Reingold, J. Rexford, and F. True. Deriving traffic demands for operational IP networks: Methodology and experience. In *IEEE/ACM Transactions on Neworking*, pages 265–279, June 2001.

[9] A. Hussain, J. Heidemann, and C. Papadopoulos. A Framework for Classifying Denial of Service Attacks. In *ACM SIGCOMM*, Karlsruhe, August 2003.

[10] J. Jung and B. Krishnamurthy and M. Rabinovich. Flash Crowds and Denial of Service Attacks: Characterization and Implications for CDNs and Web Sites. In *WWW*, Hawaii, May 2002.

[11] J. E. Jackson. *A User's Guide to Principal Components*. John Wiley, New York, NY, 1991.

[12] J. E. Jackson and G. S. Mudholkar. Control procedures for residuals associated with Principal Component Analysis. *Technometrics*, pages 341–349, 1979.

[13] Juniper Traffic Sampling. At `www.juniper.net/techpubs/software/junos/junos60/swconfig60-policy/html/%sampling-overview.html`.

[14] M.-S. Kim, H.-J. Kang, S.-C. Hung, S.-H. Chung, and J. W. Hong. A Flow-based Method for Abnormal Network Traffic Detection. In *IEEE/IFIP Network Operations and Management Symposium*, Seoul, April 2004.

[15] A. Lakhina, M. Crovella, and C. Diot. Diagnosing Network-Wide Traffic Anomalies. In *ACM SIGCOMM*, Portland, August 2004.

[16] A. Lakhina, K. Papagiannaki, M. Crovella, C. Diot, E. D. Kolaczyk, and N. Taft. Structural Analysis of Network Traffic Flows. In *ACM SIGMETRICS*, New York, June 2004.

[17] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C.-N. Chuah, and C. Diot. Characterization of Failures in an IP Backbone. In *IEEE INFOCOM*, Hong Kong, April 2004.

[18] J. Mirkovic and P. Reiher. A Taxonomy of DDoS Attacks and Defense Mechanisms. *ACM CCR*, April 2004.

[19] Pathdiag: Network Path Diagnostic Tools. At `http://www.psc.edu/~web100/pathdiag/`.

[20] S. Sarvotham, R. Riedi, and R. Baraniuk. Network Traffic Analysis and Modeling at the Connection Level. In *Internet Measurement Workshop*, San Francisco, November 2001.

[21] SLAC Internet End-to-end Performance Monitoring (IEPM-BW project). At `http://www-iepm.slac.stanford.edu/bw/`.

[22] R. Teixeira, A. Shaikh, T. Griffin, and J. Rexford. Dynamics of Hot-Potato Routing in IP Networks. In *ACM SIGMETRICS*, New York, June 2004.

[23] N. Weaver, V. Paxson, S. Staniford, and R. Cunningham. A Taxonomy of Computer Worms. In *ACM CCS Workshop on Rapid Malcode (WORM)*, October 2003.

[24] V. Yegneswaran, P. Barford, and J. Ullrich. Internet Intrusions: Global Characteristics and Prevalence. In *ACM SIGMETRICS*, San Diego, June 2003.