Detecting BGP Anomalies with Wavelet

Jianning Mai
ECE Department, UC Davis
jnmai@ece.ucdavis.edu

Lihua Yuan
ECE Department, UC Davis
lyuan@ece.ucdavis.edu

Chen-Nee Chuah
ECE Department, UC Davis
chuah@ece.ucdavis.edu

***Abstract*—In this paper, we propose a BGP anomaly detection framework called *BAlet* that delivers both temporal and spatial localization of the potential anomalies. It requires only a simple count of BGP update messages collected over a certain period. We first investigate the self-similarity in BGP update traffic and present a quantitative validation. The strength of wavelet analysis in handling signals with scaling property and earlier success in applying it for network anomaly detection motivate us to apply the same technique on BGP routing traffic. Later by clustering the anomalies detected at different locations, BAlet is capable of identifying possible network-wide anomalous events. Our method does not rely on any information within the BGP messages, and serves as a complementary tool to reduce the candidate data set for further detailed root cause analysis. We evaluate BAlet on real BGP data sets that are known to contain anomalies. Results show that it is capable of detecting network-wide events such as message volume surges caused by slammer worm attack, and separating affected ASes from the rest.**

I. Introduction

As the *de facto* inter-domain routing protocol, Border Gateway Protocol (BGP)'s routing dynamics can have a widespread global impact on the Internet. Anomalous BGP behavior could result in delayed path convergence, unstable routes, and in the worst case, disruption of network connectivity. Therefore, an in-depth understanding of BGP's dynamics not only help administrators manage the network more efficiently, but also provide valuable insights for a better routing protocol design.

BGP irregularities could be triggered by a variety of events such as link failures, session resets, routers crashing, and misconfiguration. Many studies [1–10] have contributed towards better understanding of various root causes of BGP anomalies. However, given the tremendous volume of BGP routing updates, it is still extremely challenging to manually pinpoint BGP anomalies and their root causes in real time. In general, network administrators need to know "when" and "where" the anomaly happened to start an investigation. Therefore, tools that can provide *temporal* and *spatial* localization of anomalies will be very useful. The ideal anomaly detection mechanism should also be easy to deploy, requiring minimum processing time, capable of detecting anomalies as accurate and indicative as possible.

In this paper, we propose a framework called **B**GP **A**nomaly detection with wave**let** (BAlet) to characterize BGP updates as the first step in building such a tool. BAlet targets at identifying and grouping BGP updates based on different prefixes or ASes that are likely triggered by the same underlying events along the time line. It takes a 2-dimensional matrix of localized update counts as input and works in two phases, as shown in Fig. 1. Phase one involves wavelet analysis on each row of the matrix, while phase two clusters correlated row vectors based on anomaly patterns identified in the phase one. By detecting anomalies in the BGP update time series, as well as clustering them into groups by location, BAlet is notably expressive toward understanding *when* and *where* BGP anomalies happened, thus achieving temporal and spatial localization of the anomalies. This is however not an easy task at all. It requires extensive processing on collected routing data, and hence is performed off-line currently.

The main contributions of BAlet are as follows.

- First, it is a black-box statistical approach that does not rely on the information contained in the BGP updates. Instead, anomalies detected based on the key observation that most anomalies corresponds to increases in the volume of BGP update messages. Temporal and spacial correlations among the anomalies also grant us the opportunity of better localization.
- Second, the incremental nature of BGP updates and data from multiple vantage points ensure this is "network-wide" anomaly detection. BAlet is very effective and scalable at detecting anomalies that are spread over multiple routing domains. Therefore, it serves to complement the existing body of root cause analysis work.

Evaluating our framework on arbitrary BGP routing data is hard because of the difficulty in establishing "ground truth" to compare to. We instead apply the proposed detection methods on BGP data from RIPE NCC [11] and RouteViews [12] that contains well-known network-wide events. BGP update messages are parsed using the Python Routing Toolkit [13] and time series are generated from counting the number of messages. Our results show that in most cases, there are other possible anomalies detected in addition to the reported events. This highlights the goal of BAlet to provide an efficient technique to locate potential BGP anomalies, in order to shorten the overall response time. We do not intend to perform root cause analysis of certain BGP anomalies, nor to detect specific announcement patterns. Instead, BAlet complements existing approaches by locating a smaller set of BGP data (through temporal and spatial localization) that can later be processed by other signature-based sophisticated root cause analysis algorithms.

This work was supported in part by the National Science Foundation under Grant CAREER Award ANI-0238348 and CyberTrust CNS-0716831.

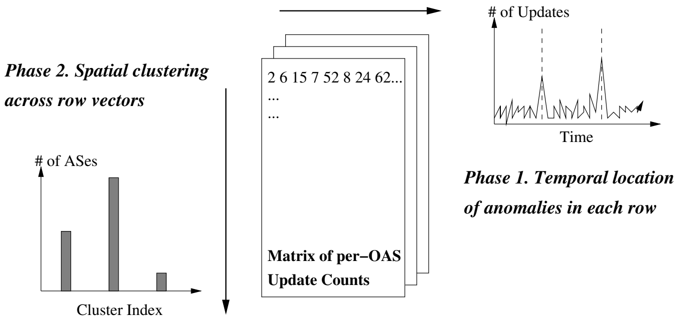

Phase 2. Spatial clustering across row vectors
# of ASes
Cluster Index
2 6 15 7 52 8 24 62...
...
...
Matrix of per−OAS Update Counts
# of Updates
Time
Phase 1. Temporal location of anomalies in each row

Fig. 1. Tow phases of BAlet: temporal detection of anomalies in phase 1, and clustering for network-wide events in phase 2.

We show in Section III that time-series generated from the count of BGP update messages exhibits self-similarity. This motivates us to apply wavelet analysis techniques due to its strength in exposing scale dependent properties in self-similar signals [14]. Our wavelet-based algorithm for the temporal localization of anomalies requires only minimum processing, and is scalable and suitable for online, real-time monitoring. In Section IV, we present our clustering algorithm which achieves the spatial localization. We illustrate that BAlet is effective in detecting and understanding various BGP anomalies by performing the two-dimensional analysis.

II. Related Work

Generally BGP updates can be attributed to two types of transactions, table exchange and incremental updates. Whenever a BGP peering session is established, all exportable routes in the routing tables are exchanged between the peers. Otherwise, under normal operations, a router only sends out incremental route changes. Link failures, router glitches, and misconfiguration can all cause a BGP session to be reset, which will in turn provoke unusual upsurge in updates. Wang *et al.* [4] and Lad *et al.* [8] analyzed the BGP log data collected from various monitoring points to understand the causes of the high surge in BGP update messages during the Code Red/Nimda and SQL Slammer attacks, respectively. It shows that local connectivity dynamics actually propagate globally in current BGP routing protocol. As a result, a small number of overloaded edge networks links to the Internet potentially cause global routing anomaly. Zhang *et al.* [15] present an algorithm called Minimum Collection Time (MCT) to accurately detects the start and duration of table exchanges from a stream of BGP updates.

Another well-studied BGP anomaly is the Multiple Origin AS (MOAS) conflict first coined by Zhao *et al.* [16]. A prefix is usually originated by a single AS. MOAS appears when multiple origin ASes announce the same prefix. Its causes span from legitimate cases such as multihoming, route aggregations, and IP Anycast, to anomalous cases like misconfiguration and hijacking attacks. Instead of attempting an accurate route hijacking detection, PHAS [17] notifies of the origin AS changes to the original prefix owners in a timely and reliable way. Recent work by Qiu *et al.* [18] uses cooperation among ASes for detection. Built on previous works, Hu *et al.* [19] significantly improves the detection accuracy of IP prefix hijacking by combining passive analysis of BGP routing updates with active data plane fingerprints of suspicious prefixes. The novel algorithm demonstrates the ability to distinguish between legitimate routing changes and actual attacks.

Visualization-based tools are also devised to analyze BGP updates [20] and to detect MOAS events [21]. Zhang *et al.* [22] applied both signatures (a pre-defined pattern of events) and statistic methods for anomaly detection. These tools need extensive processing on the content of the collected routing data, and are therefore more appropriate for off-line post-processing.

Several previous work are close to our proposed framework in terms of methodology. An instance-learning framework [23] is proposed to identifies anomalies based on deviations from the normal BGP-update dynamics for a given destination prefix and across prefixes. In their scheme, wavelet transform is employed to extract update dynamic features, which are then clustered into normal and abnormal groups. Xu *et al.* [24] also suggests that updates triggered by distinct underlying events can be separated. Specifically, Principal Components Analysis (PCA) techniques is applied to achieve this goal. It is shown that the method based on PCA is able to obtain a set of clusters corresponding to a set of prefixes or ASes which are affected by the same underlying event. Note that BAlet, on the other hand, first detects anomalies for each AS or prefix. The detected volume surges are then clustered into correlated events both in time and space dimensions.

Recently, a Generalized Likelihood Ratio (GLR) based hypothesis test is designed to extract features [25] in the change patterns of BGP message volume and AS path length. Temporal correlations amongst features are used to effectively minimize the number of false alarms in the detection. Huang *et al.* [26] apply the same PCA subspace technique to detect BGP disruptions. Details in the dynamic routing updates are then combined with network-wide static configurations to identify the root cause of the disruptions. Our emphasis and approach are different in that BAlet achieves the network-wide events detection based on BGP updates received at a single vantage point, as demonstrated in the paper. It can also adapt to multi-points event correlation by combining the data set. Therefore, it is much simpler and more suitable for online adoption.

Network traffic has been shown to exhibit self-similarity [27, 28]. Yuan *et al.* [29] and Huston [30] demonstrated the same property with the BGP traffic. Fourier analysis can be adapted to detect drift, trends and abrupt changes in a signal. For instance, the Short-Time Fourier Transform (STFT) analyzes a small window of signal at a time to map it into both time and frequency domain. However, once the time window is chosen in STFT, the window remains the same for all frequencies. Given the nature of self-similarity in BGP update traffic, wavelet analysis has proved to be more effective on change detection at multiple scales. Previous work [31–33] applied wavelet-based algorithms to detecting traffic anomalies and network attacks. We adopt a procedure based on the maximal overlap discrete wavelet transform to locate BGP anomalies in the time domain.

III. Detecting Anomalies with Wavelet

In network anomaly detection, anomalies are generally manifested as *abrupt changes*, and generally caused by either network failures and performance problems, or security-related problems [34]. The same argument applies to BGP as well. Anomaly detection methods usually include rule-based approach, finite state machines, pattern matching, and statistical analysis. It is shown that the first three approaches have limitations in that they require substantial knowledge about the protocols as well as enormous processing power. However the auto-regressive model used in [34] are only suitable for data with fixed scale in time and frequency. Section III-A unveils the self-similarity in BGP routing data, which motivates our wavelet-based method. We introduce the wavelet transform briefly in Section III-B followed by a summary of existing network anomaly detection algorithms using wavelet in Section III-C. Our detection results are presented in Section III-D.

A. Self-Similarity in BGP Routing Data

Self-similarity and long-range dependency (LRD) have been observed in various types of network data traffic. However, similar property has not been established for routing traffic like BGP until recently [29, 30].

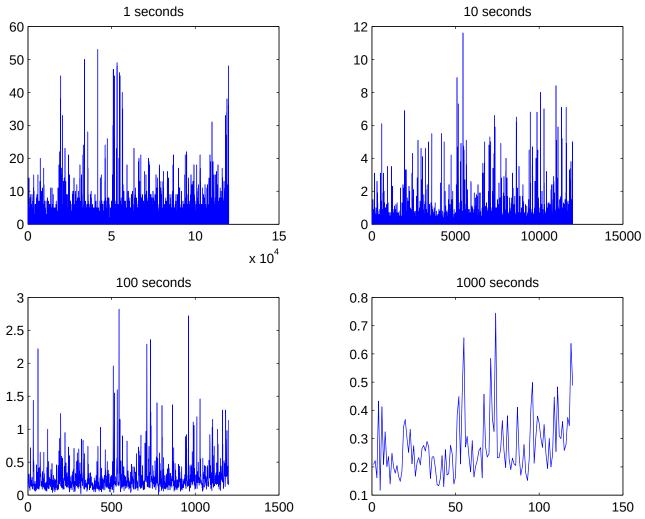
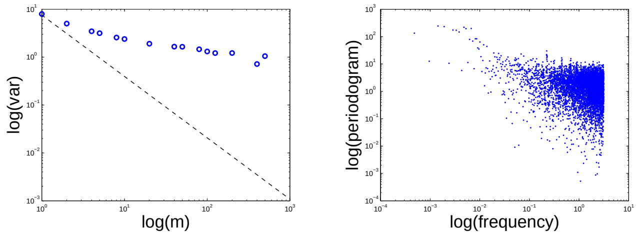


Fig. 2. Burstiness of BGP update counts over various time scales.

We showed in [29] that the volume time series formed by BGP updates exhibits self-similarity and long-range dependence. One of the fundamental properties of self-similarity is the observation of burstiness over a wide range of time scales as discovered in local network and web traffic [27, 28]. Hence simple aggregation on the time scale will not smooth out the burstiness of self-similar traffic. More importantly, the multi-scale nature motivates our choosing of discreet wavelet transforms in detecting anomalies, since simple threshold and correlation are not suitable for differentiating anomalies from normal traffic dynamics.

Figure 2 illustrates BGP updates collected by RIPE RRC08 in Jan 2004. The subplot at upper left corner is a detailed representation of number of updates received every second. The rests are aggregated with bin size of 10, 100, 1000 seconds respectively. These figures show that burstiness appears at different time scales. Similar approach is employed in [28].



(a) Variance Plot

(b) Periodogram

Fig. 3. Quantitative evaluation of the self-similarity using variance plot and periodogram.

Figure 3(a) presents the variance plot which is used to determine the Hurst parameter (H). The circle dots represents the log of normalized variance versus log of m, the aggregation scales. The slope of the variance plot is estimated to be between -0.53 and -0.2. Therefore the estimated Hurst parameter (H) ranges between 0.74 and 0.9, significantly larger than 0.5. In Fig. 3(b), the periodogram plot give us a similar estimation of H.

Huston [30] confirms our finding of self-similar BGP update traffic. Huston [30] discusses the implications of self-similar BGP traffic on the local cache management and securing BGP, while we focus on developing techniques for on-line anomaly detection. Our observation also complements work in [35] towards generating realistic BGP traffic.

B. The Maximal Overlap Discrete Wavelet Transform

Wavelet analysis facilitates multi-resolution analysis (MRA) of traffic time-frequency characteristics, and has proved to be effective at detecting volume anomalies. We focus our detection on a maximal overlap discrete wavelet transform (MODWT) [36] based procedure.

The discrete wavelet transform of signal $\{X[n]\}$ with length N involves the computation of the convolution between the signal and a family of wavelets. Calculating wavelet coefficients at dyadic scales can be treated as filtering operations in which X is passed through a real-valued wavelet filter (high pass) $\{h_l\}$ of even width L. The output is a set of wavelet coefficients $W_{1,t} = X * h_l$ at the original time scale (first level) with length $\frac{N}{2}$. Similarly by filtering the signal with the corresponding scaling filter (low pass) $\{g_l = (-1)^{l+1} h_{L-1-l}\}$, we obtain the first level scaling coefficients $V_{1,t} = X * g_l$ of length $\frac{N}{2}$. Then by applying the inverse DWT on $\{W_{1,t}\}$ and $\{V_{1,t}\}$ independently, we separate the first level detail D_1 from approximation A_1. The decomposition process is repeated using A_1 as an input, which yields D_2 and A_2 at the second level. The maximum level of DWT we can perform is $J \leq \log_2 N$. The MRA thus satisfies

$$X = \sum_{i=1}^{J} D_i + A_J.$$

Each level i represents the strength of a particular frequency in the signal, with a higher value of i indicating a lower frequency.

Although DWT can detect abrupt changes in a time series, it may introduce ambiguities in the time domain. A change in the starting point for a time series can yield quite different results due to the alignment of the time series with the averaging intervals predefined by the DWT. In contrast, MODWT is translation invariant in the sense that it preserves regularity information at each point in time for each scale, and it may be computed for an arbitrary length time series. This translation-invariant property allows alignment of events in a multi-resolution analysis with respect to the original time series. Further details of the MODWT can be found in [36].

C. Abrupt Change Detection

We summarize here the wavelet-based anomaly detection algorithms previously proposed for network traffic in the literature.

1) Hypothesis testing: An early work [31] proposed an network anomaly detection algorithm based on wavelet and Bayesian analysis. Assume that the wavelet coefficients at detection scale $\{W_j\}$ are zero-mean Gaussian stationary process. The hypothesis to be tested is $H_0 : var(W_{j,1}) = \cdots = var(W_{j,N})$, and the alternative hypothesis $H_0 : var(W_{j,1}) = \cdots = var(W_{j,n-1}) \neq var(W_{j,n}) = \cdots = var(W_{j,N})$. The change point n in the time series can be estimated from the log likelihood ratio defined as:

$$\Delta = \log f(H_0|W_j) / \log f(H_1|W_j).$$

If $\Delta > 1$, we can make the decision to choose H_1, since a change in the process leads to variance change after wavelet decomposition.

The algorithm requires neither auto regression nor thresholds to detect changes. It is shown to be able to detect and locate subtle changes in variance from time series, and performs better than adaptive thresholding techniques and auto-regressive models.

2) Deviation score: Barford *et al.* [32] lay out their anomaly detection algorithm in three steps. First the time-series is decomposed into multiple levels using wavelet. The decomposed signals are then synthesized into High (H), Middle (M) and Low (L) bands. Lower levels contain high frequency fluctuations and higher levels reveal slow-moving general trends. The observation is that the "local deviation" in the high frequency representation exposes the beginning and end of short-lived events, while the local variability in the mid frequency filters expose their duration. Hence surges in the local variances indicates a sharp unpredictable change in the volume of the measured traffic.

Potential anomalies are therefore identified by looking at relative ratio of local variance and global variance defined as *deviation score*. Global variance is the variance calculated over the whole lifespan of the signal and local variance is calculated over a moving window. A thresholding mechanism is then applied for anomaly detection purpose. Employing the method on realistic network traffic data actually exposed a number of true anomalies verified post-mortem by network engineers.

3) Residual signal: Another simple design utilizing residual signal has been employed in [33]. The algorithm starts with constructing a time series signal X, and decomposes X into A_1 and D_1 using wavelet transformation. A_1 represents the baseline, i.e., the long term trend of X. To obtain the residual signal in time interval i, subtracting the trend from the time series $R(i) = X(i) - D(i-1)$. Finally signal an alarm when $R(i)$ exceeds the a predefined threshold. The threshold value has to be selected based on the statistical distribution of the history residual values.

D. Illustration: Temporal Localization of BGP Anomalies

As introduced in Section III-B, wavelet analysis uses windowing techniques to map a signal into a function of time and frequency. Smaller (larger) window size gives us more high (low)-frequency components. By varying window sizes, wavelet analysis can extract multi-resolution properties of the data at different scales. The choice of mother wavelets, or *filters*, determine the quality of *time* and *frequency* localization. In this paper, we use a short, compact filter known as the Daubechies family wavelets with five vanishing moments (db5). A short filter is preferred to avoid excessive blurring in the time domain, which makes it difficult to distinguish strong short-duration change versus milder longer-duration changes.

Figures 4 shows the detection results on BGP data collected from RIPE RRC08 using the deviation score algorithm (Sec. III-C2). The main advantage of the deviation score method is to detect anomalies at different time scales. The signal reconstruction step offers the flexibility of change detections targeting different time scales. We shaded the areas of anomalies identified in the figures. BGP behavior during the shaded time intervals can then be diagnosed for potentially anomalies. Administrators need to investigate only the much-reduced candidate data set for root cause analysis.

Our preliminary root cause analysis reveals that AS 6066 was announcing almost every single block of IP prefixes to AS 12654 on Jan. 21. In most cases, these announcements are without any aggregation. We suspect there is a misconfiguration causing AS 6066 mistakenly announce prefixes without aggregation. The anomaly shown at the left side of Fig. 4 is less severe. The BGP session between AS 2914 and AS 12654 was lost and re-established and AS 2914 started feeding AS 12654 with its huge BGP table.

IV. Time and Space Localization of Anomalies

Applying wavelet based change detection to BGP traffic help us locate potential anomalies temporally, as demonstrated in the previous section. However, time values only comprise a

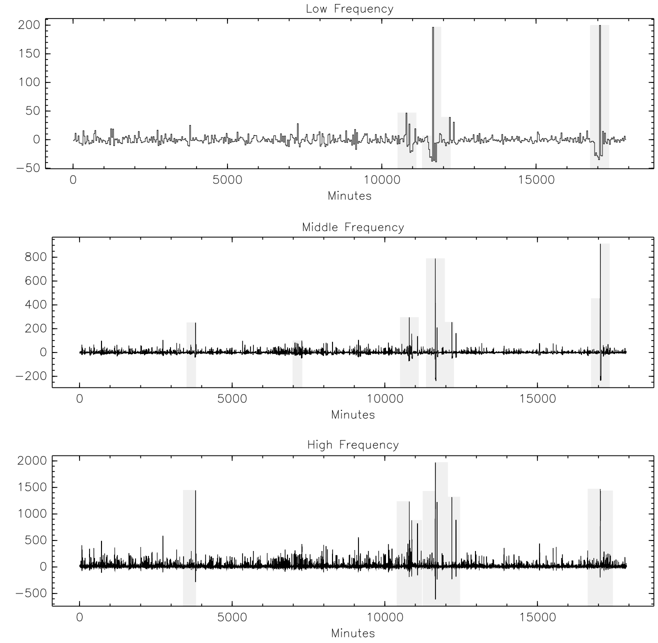


Fig. 4. Temporal localization of BGP anomalies in January 2004 at monitoring point RIPE RRC08.

single dimension in locating the network-wide anomalies. The natural followup question is "where" such misconfigurations, network failures, and worm attacks happened. We would like to decide whether the anomalies have local or global impact, or somewhere in between. In order to achieve both temporal and spatial detections, BAlet performs a 2-dimensional analysis on the BGP data in 3 steps. First, we need to construct an update count matrix with each row representing a time series from a unique origin. Next the wavelet change detection algorithm is applied to mark all the potential anomalies for each row in the matrix. Finally, a clustering mechanism is performed to identify time-correlated anomalies among ASes or prefixes. We may also discover space correlations in the clusters. Since network-wide BGP anomalies propagates to peering ASes across geographic locations, we could even reconstruct the trail of the impact.

Now we discuss the way to construct the update matrix and to perform clustering. The residual signal wavelet algorithm (Sec. III-C3) is selected for the time domain detection in our 2-dimensional analysis due to its simplicity. To efficiently scan through a huge number of rows of time series in the matrix, we prefer a method with single level wavelet transformation and easy threshold comparison.

A. Matrix of BGP Update Counts

One way to achieve spatial localization, for example, is to categorize BGP update messages based on their Original ASes (OAS). Table I illustrates a 2-dimensional matrix $\mathbf{X}$ thus formed on Per-OAS update counts over time. Each row vector $\mathbf{x}_i = [x_{i1}\, x_{i2} \cdots x_{1n}]$ is a time series of update counts for OAS i. The time interval setting of vector $\mathbf{x}_i$ is decided by the size of *detection window*, in which we detect anomalies.

TABLE I
2D MATRIX $\mathbf{X}$ OF PER-OAS UPDATE COUNTS

	t_1	t_2	$\cdots$	t_n
$\mathbf{x}_1$	x_{11}	x_{12}	$\cdots$	x_{1n}
$\mathbf{x}_2$	x_{21}	x_{22}	$\cdots$	x_{2n}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\mathbf{x}_m$	x_{m1}	x_{m2}	$\cdots$	x_{mn}

The Per-OAS matrix $\mathbf{X}$ shown above is not the only way we integrate space information into the time series. We can generate a row vector based on *prefix* – the very index into routing table entries. Also the transpose of $\mathbf{X}$ can be formed with each row vector represents the update counts from every OAS or prefix in the same time interval. We will specify the construct of the matrices for the experiments in the following sections.

Our purpose is on observing temporal correlations among anomalies detected at different locations. The correlation can be gauged by the distances among vectors. There are several options when it comes to measure the distance. The simplest is Euclidean distance, however, it takes no account of any patterns of covariance that exist in the data. We choose Mahalanobis distance defined as following:

$$D_{ij}^2 = (\mathbf{x}_i - \mathbf{x}_j)\mathbf{C}_{\boldsymbol{X}}^{-1}(\mathbf{x}_i - \mathbf{x}_j)^T \tag{1}$$

where $\mathbf{C}_{\boldsymbol{X}} = E[(\mathbf{X} - E[\mathbf{X}])(\mathbf{X} - E[\mathbf{X}])^T]$ is the covariance matrix of $\mathbf{X}$.

B. Cluster Analysis

1) Methodology: There are a lot noise in the matrix of update counts along both temporal and spatial dimensions. After applying residual signal wavelet anomaly detection progressively on each time series in the matrix, those locations with no obvious abrupt changes can be discarded. Furthermore, since we correlate update counts across multiple OASes and prefixes, we are interested in only those anomalies detected at more than two different locations or for at least two prefixes. Anomalies found from only one single OAS or prefix are more likely to be just isolated aberrations rather than network-wide events. By decreasing the order of the matrix, we are also able to reduce the complexity of the correlation and clustering process. We call a time series obtained after order reduction a feature vector.

Once we obtain a list of feature vectors using the above selection, we cluster the vectors based on the distance between every pair of them. There are many existing algorithms for clustering such as *K-means* and *Single-Linkage* hierarchical clustering. We adopt a simple iterative algorithm [33], which is an alternative to K-means without predetermined number of clusters. The algorithm assumes each cluster has a centroid. A vector belongs to the cluster whose centroid is closest to it compared with the distances from itself to other centroids.

The algorithm starts with one cluster whose centroid is randomly chosen. Then, it iteratively selects a vector that has the largest distance to it as a new hub, and re-clusters all the vectors based on their distances to all the selected hubs. This process continues until there is no vector whose distance to its hub is larger than the half of the average hub-hub distance. We also compare the simple iterative algorithm against vanilla K-means and Single-Linkage, and find out both work equally well. However, Single-Linkage are much faster for us in terms of running time.

Once we detect a new cluster of network-wide anomalies, we generate an alarm before examining further to identify the involved OASes or prefixes from which the cluster shaped. Based on the suspicious spatial and temporal localization, system administrators can decide whether root causes of the anomalies can be identified, or the abnormal events that should be further investigated.

2) Evaluations: To validate BAlet, we perform several detailed analysis on BGP update data collected by RIPE NCC [11].

a) A single origin AS: In the first case study, we randomly picked BGP log files for AS#12 over a 6 month period from October 1, 2002 to March 31, 2003 to analyze. The data is aggregated in one day interval since we are concerned to the volume change on a daily bases.

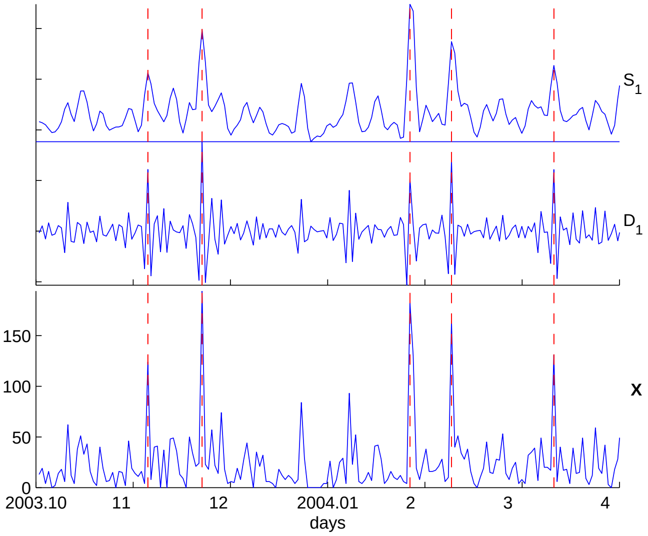
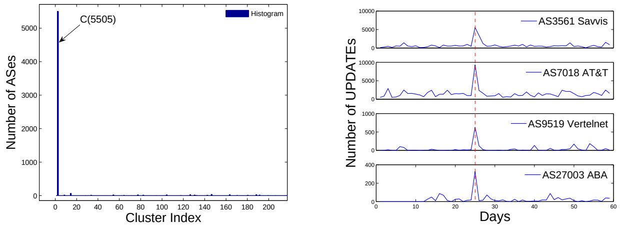


Fig. 5. Time series of BGP update received at RRC00 from original AS 12 between October 1, 2003 and March 31, 2004, five potential anomalies detected on day 35, 52, 117, 130, and 162

Figure 5 shows the time series of update data originated from AS 12. In order to detect abrupt changes in the time series, we calculate the simple residual signal of the long-term trend considering the first level detail D_1 as a wide-sense stationary Gaussian process. When we set the threshold at 2.5σ for random variable D_1, we can detect anomalies with an error rate of 0.5% since:

$$P(\mu - 2.5\sigma \leq D_1 \leq \mu + 2.5\sigma) \approx 99.5\%$$

There are 5 days detected on which the number of updates are likely to be abnormal, as shown in the figure with dotted vertical lines.



(a) Clusters

(b) Typical group pattern

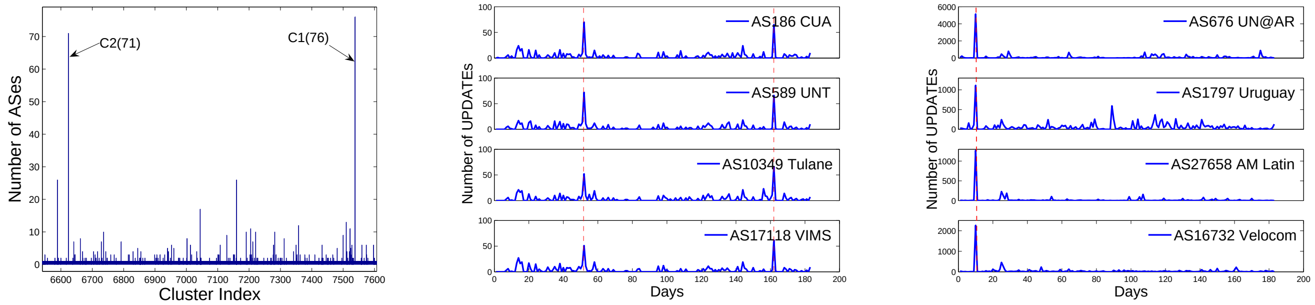
Fig. 6. A global event detected involves over $5,500$ ASes from 01/2003 to 02/2003 with surge on day 23.

b) A global event: January 25, 2003 marked the day slammer worm attacked. As shown in [8], although the worm was not directly targeted at the routing infrastructure, a number of critical AS peering links were overloaded, which caused a globally observed increase in the volume of routing update messages.

We construct the matrix of per-OAS update counts as described in Section IV-A. The time series in each row represent the number of route announcements every day during January and February 2003. After dimension reduction by removing the row vector containing no detected anomalies, BAlet performs the clustering on the matrix and identifies a major cluster, which consists of over $5,500$ ASes from a total of more than $19,000$ active ASes as shown in Fig. 6(a). We find out that almost all of the ASes in this cluster correlates along the events of the slammer day. Typical anomaly pattern from 4 cluster members is illustrated in Fig. 6(b). We confirmed that a surge in the update messages has been detected on January 23, 2003 from all the ASes in the cluster. Therefore BAlet captures this network-wide anomaly and correlates them successfully. Besides the major cluster, small clusters involving around 20 ASes also indicates multiple underlying network-wide surges in much smaller scales.

c) Temporal and spatial correlations: This example proves further that BAlet is effective at pinpointing the time and locations of the possible network anomalies, thus serves as a first step in troubleshooting BGP routing problems. We chose the 6 months time frame from October 2003 to March 2004 at RRC00 to evaluate. It turns out that there are no global events that affects a large portion of ASes in the previous example. However, we do locate several correlated events as shown in Fig. 7. The top 2 clusters are marked in Fig. 7(a), with the number inside the brackets indicating the size of each cluster.

Cluster 1 is made up of 76 ASes from universities and research institutes that are part of an area educational network. Anomaly detection returns two correlated events for the cluster members: one on November 12, 2003, the other on March 10, 2004, as shown in Fig. 7(b). In both cases, we observe that all the ASes in the cluster kept announcing their prefixes every 5 minutes. Since most ASes were holding only a couple of prefixes and usually not very active (sending just one or two announcements per day), the surge of almost a hundred messages on those two days indicates something unusual. The



(a) Top 2 clusters

(b) Cluster 1 pattern

(c) Cluster 2 pattern

Fig. 7. Two network-wide events identified from 10/2003 to 03/2004 using clustering.

second incident could be related to the short AT&T/Level 3 outage reported on NANOG [37], while possible causes for the first surge detected may be due to misconfigurations or router failures.

Cluster 2 consists of 71 ASes which are mostly geographically located in Latin America. Figure 7(c) shows 4 ASes randomly picked from the cluster: namely, AS676 (United Nation Development Office in Argentina), AS 1797 (Uruguay), AS 27658 (America Express Latin America), and AS16732 (Velocom, an ISP in Argentina). The anomaly detected happens on October 10, 2003. High message counts on the day could be a indication of major hardware failures.

V. Conclusions and Future Work

In this paper, we presented BAlet, a framework to achieve both temporal and spatial localization of BGP anomalies. We first studied the self-similarity of signals generated from BGP update count, and conclude that signals of total BGP traffic is self-similar with H parameter around 0.8. We applied wavelet analysis for temporal localization of the anomalies because of its strength in handling self-similar signal. The deviation score and residual signal based algorithms at different time-granularity are employed and prove to be effective in detecting volume anomalies. BAlet requires only a simple count of BGP update messages, therefore, it is scalable and suitable for online monitoring. Our two-dimensional clustering procedure opens up further possibilities in locating anomalies not only temporally but spatially. In addition to locating the potentially anomalous time span and origin ASes, BAlet helps in understanding the scale of the impact from slammer attack. This step requires to construct a BGP update matrix based on the origin AS or prefixes, and to perform clustering over the anomalies detected.

In the future, we would construct the BGP update matrix based on the prefixes rather than the OASes to detect anomalies such as MOAS conflicts. Furthermore, we need to thoroughly evaluate BAlet's 2-dimensional analysis method in terms of performance and complexity, such as false postives/negatives ratios and processing time benchmarking. This toolkit can also be improved for real-time detection. However the major hurdle lies in the computation time of cluster analysis. Currently it took 10 $\sim$ 20 minutes to finish the clustering. We believe by optimizing the clustering algorithm, the job can be done in sub-minute. The other difficulty is the trade-off between the time interval value for cluster analysis and reducing computation time. Choosing a large time interval means higher probability to detect network-wide anomalies. On the other hand, the dimension of the matrix increases, which also increase the processing time. As part of our future work, we also plan to compare with other statistical techniques, such as likelihood hypothesis test and FFT based time and frequecy analysis tools.

References

[1] C. Labovitz, G. R. Malan, and F. Jahanian, "Internet Routing Instability," in *Proc. ACM SIGCOMM*, Cannel, France, Sep 1997.

[2] K. Varadhan, R. Govindan, and D. Estrin, "Persistent Route Oscillations in Inter-Domain Routing," *IEEE/ACM Transactions on Networking*, vol. 32, no. 1, 1999.

[3] J. Cowie, A. Ogielski, B. Premore, and Y. Yuan, "Global Routing Instabilities during Code Red II and Nimda Worm Propagation , Preliminary Report," Renesys Corporation, Tech. Rep., Sep 2001. [Online]. Available: http://www.renesys.com/projects/bgp_instability

[4] L. Wang, X. Zhao, D. Pei, R. Bush, D. Massey, A. Mankin, S. F. Wu, and L. Zhang, "Observation and Analysis of BGP Behavior under Stress," in *Proc. 2nd Internet Measurement Workshop*, Marseille, France, Nov 2002. [Online]. Available: http://www.icir.org/vern/imw-2002/proceedings.html

[5] A. Basu, C.-H. L. Ong, A. Rasala, F. B. Shepherd, and G. Wilfong, "Route Oscillations in I-BGP with Route Reflection," in *Proc. ACM SIGCOMM*, 2002.

[6] R. Mahajan, D. Wetherall, and T. Anderson, "Understanding BGP Misconfiguration," in *Proc. ACM SIGCOMM*, Pittsburgh, PA, Aug 2002.

[7] T. G. Griffin and G. Wilfong, "An Analysis of the MED Oscillation Problem in BGP," in *ICNP*, 2003.

[8] M. Lad, X. Zhao, B. Zhang, D. Massey, and L. Zhang, "Analysis of BGP Update Burst during Slammer Attack," in *Proceedings of the 5th International Workshop on Distributed Computing*, Dec 2003.

[9] A. Feldmann, O. Maennel, Z. M. Mao, A. Berger, and B. Maggs, "Locating Internet Routing Instabilities," in *Proc. ACM SIGCOMM*, Portland, Oregon, USA, Aug 2004.

[10] J. Wu, Z. M. Mao, J. Rexford, and J. Wang, "Finding a needle in a haystack: pinpointing significant BGP routing changes in an IP network," in *Proc. 2nd conference on Symposium on Networked Systems Design & Implementation (NSDI'05)*, Boston, MA, USA, May 2005.

[11] "RIPE (Reeaux IP Europeens)," http://www.ripe.net/.

[12] D. Meyer, "University of Oregon Route Views Project," http://www.routeviews.org/.

[13] R. Mortier, http://mort.belltower.co.uk/pyrt.html.

[14] P. Abry and D. Veitch, "Wavelet Analysis of Long Range Dependent Traffic," *IEEE Transactions on Information Theory*, vol. 44, no. 1, pp. 2–15, 1998. [Online]. Available: citeseer.nj.nec.com/abry98wavelet.html

[15] B. Zhang, V. Kambhampati, M. Lad, D. Massey, and L. Zhang, "Identifying BGP Routing Table Transfers," in *Sigcomm Workshop on mining network data (MineNet-05)*, Philadelphia, PA, USA, Aug 2005.

[16] X. Zhao, D. Pei, L. Wang, D. Massey, A. Mankin, S. F. Wu, and L. Zhang, "An Analysis of BGP Multiple Origin AS (MOAS) Conflicts," in *Proc. ACM SIGCOMM Internet Measurement Workshop*, San Francisco, CA, USA, Nov 2001.

[17] M. Lad, D. Massey, D. Pei, Y. Wu, B. Zhang, and L. Zhang, "PHAS: A Prefix Hijack Alert System," in *Proc. 15th USENIX Security Symposium (Security 06)*, Vancouver, B.C., Canada, 2006.

[18] S. Y. Qiu, F. Monrose, A. Terzis, and P. D. McDaniele, "Efficient Techniques for Detecting False Origin Advertisements in Inter-domain Routing," in *Proc. 2nd IEEE Workshop on Secure Network Protocols*, Santa Barbara, CA, USA, Nov 2006.

[19] X. Hu and Z. M. Mao, "Accurate Real-time Identification of IP Prefix Hijacking," in *Proc. 2007 IEEE Symposium on Security and Privacy*, Oakland, California, USA, May 2007.

[20] S. Teoh, K. Ma, S. Wu, and X. Zhao, "Information Visualization for Anomaly Detection," in *Proceedings of 5th IASTED International Conference in Computer Graphics and Imaging (CGIM)*, Hawaii, 2002.

[21] S. Teoh, K. Ma, S. Wu, D. Pei, L. Wang, L. Zhang, D. Massey, and R. Bush, "Visual-Based Anomaly Detection for BGP Origin AS Change (OASC) Events," in *Proceedings of 14th IEEE/IFIP Workshop on Distributed Systems: Operations and Management (DSOM)*, vol. 2867, Heidelberg, Germany, Oct 2003.

[22] K. Zhang, S. F. Wu, A. Yen, X. Zhang, and D. Massey, "On Detection of Anomalous Routing Dynamics in BGP," in *Proc. IFIP Networking*, 2004.

[23] J. Zhang, J. Rexford, and J. Feigenbaum, "Learning-Based Anomaly Detection in BGP Updates," in *Sigcomm Workshop on mining network data (MineNet-05)*, Philadelphia, PA, USA, Aug 2005.

[24] K. Xu, J. Chandrashekar, and Z.-L. Zhang, "A First Step Toward Understanding Inter-Domain Routing Dynamics," in *Sigcomm Workshop on mining network data (MineNet-05)*, Philadelphia, PA, USA, Aug 2005.

[25] S. Deshpande, M. Thottan, T. Ho, and B. Sikdar, "A Statistical Approach to Anomaly Detection in Interdomain Routing," in *Proc. BROADNETS'06*, San Jose, CA, USA, October 2006.

[26] Y. Huang, N. Feamster, A. Lakhina, and J. Xu, "Diagnosing Network Disruptions with Network-Wide Analysis," in *Proc. ACM SIGMETRICS*, San Diego, CA, USA, June 2007.

[27] W. Leland, M. Willinger, and D. Wilson, "On the Self Similar nature of Ethernet Traffic (extended version)," *IEEE/ACM Transactions on Networking*, pp. 1–15, Feb 1994.

[28] M. E. Crovella and A. Bestavros, "Self-Similarity in World Wide Web Traffic: Evidence and Possible Causes," *IEEE/ACM Transactions on Networking*, vol. 5, no. 6, pp. 835–846, Dec 1997.

[29] L. Yuan, J. Mai, and C.-N. Chuah, "BGP Anomaly Detection Using Wavelet Analysis," Technical Report ECE-CE-2004-4, University of California, Davis, Tech. Rep., 2004.

[30] G. Huston, "Measures of Self-Similarity of BGP Updates and Implications for Securing BGP," in *Proc. The 8th Passive and Active Measurement (PAM'07)*, Louvain-la-neuve, Belgium, Apr 2007.

[31] V. Alarcon-Aquino and J. A. Barria, "Anomaly detection in communication networks using wavelets," *IEE Proceedings-Communications*, vol. 148, no. 6, pp. 355–362, Dec 2001.

[32] P. Barford, J. Kline, D. Plonka, and A. Ron, "A Signal Analysis of Network Traffic Anomalies," in *Proc. ACM/SIGCOMM Internet Measurement Workshop*, Marseille, France, Nov 2002.

[33] Y. Xie, H.-A. Kim, D. R. O'Hallaron, M. K. Reiter, and H. Zhang, "Seurat: A Pointillist Approach to Anomaly Detection," in *Proc. 7th International Symposium on Recent Advances in Intrusion Detection (RAID'07)*, Sophia Antipolis, French Riviera, France, Sep.

[34] M. Thottan and C. Ji, "Anomaly Detection in IP Networks," in *IEEE Transaction on Signal Processing, Special Issue of Signal Processing in Networking*, vol. 51, no. 8, Aug 2003, pp. 2191–2204.

[35] O. Maennel and A. Feldmann, "Realistic BGP Traffic for Test Labs," in *Proceedings of ACM SIGCOMM 2002 Conference*, Pittssburgh, PA, Aug 2002.

[36] D. B. Percival and A. T. Walden, *Wavelet Methods for Time Series Analysis*. Cambridge University Press, 2004.

[37] "Nanog mailing list," http://www.nanog.org.