BGPfuse: Using visual feature fusion for the detection and attribution of BGP anomalies [*]

Stavros Papadopoulos
Department of Electrical and Electronic Engineering
Imperial College London
s.papadopoulos11@imperial.ac.uk

Georgios Theodoridis
Information Technologies Institute
Centre for Research and Technology Hellas
gtheo@iti.gr

Dimitrios Tzovaras
Information Technologies Institute
Centre for Research and Technology Hellas
tzovaras@iti.gr

ABSTRACT

This paper presents BGPfuse, a scheme for visualizing and exploring BGP (Border Gateway Protocol) path change anomalies. BGPfuse uses a set of BGP features that are capable of quantifying the degree of anomaly of each path change event. Moreover, visual methods are introduced for performing the efficient fusion of these multiple features. The exploitation of the human perception, allows to overcome the static-nature of the existing weight-based fusion approaches. A Parallel Coordinates approach is used to visualize these features, which is further enhanced with filtering capabilities, so as to discriminate between normal and abnormal events. BGPfuse uses multiple linked graph views so as to represent in depth the relationships among the involved Autonomous Systems (ASes), as well as a combined graph view to highlight structural similarities between all the individual feature graphs. The structural similarities as well as the filtering capabilities provided by BGPfuse, enable the analyst to perform visual fusion of the BGP features, so as to detect any suspicious behavior and focus only in the most interesting cases. Experimental demonstration of BGPfuse, shows the analytical potential of the proposed approach by decisively capturing malicious BGP hijacking events.

1. INTRODUCTION

Feature fusion deals the appropriate combination of a selected set of features in order to provide a classifier and classify the input dataset into multiple labeled groups. Generally, feature fusion has a wide range of application in many disciplines such as remote sensing[1], face recognition[2], and speech processing and video classification and retrieval[3].

Although there are many well known techniques for algorithmic fusion [4], the disadvantage is that the result of the fusion is static and it fails to follow the dynamic nature of the modern multivariate systems and the corresponding alterations of the features' cross-correlations. Thus, on the basis of obsolete weighting factors, alarming events may be erroneously suppressed or false positives may unjustifiably arise, decreasing the effectiveness of the detection mechanism. For this reason, visualization techniques can be utilized for the purpose of performing the feature fusion, and allow the user to incorporate his experience and knowledge into the analysis.

In this respect, this paper introduces a novel visual feature fusion method for the purpose of combining different BGP features, so as to detect BGP path hijacking events. In order to achieve this, BGPfuse uses a Parallel Coordinates view which is enhanced with filtering capabilities, combined with graph visualizations so as to represent the path change events on per AS (Autonomous System) level.

The rest of the paper is organized as follows: Section 2 presents the related work. Section 3 presents the BGP features that are used by BGPfuse, while Section 4 presents the visual feature fusion technique utilized by BGPfuse. In Section 5 the analytical potential of BGPfuse is illustrated, in a real life hijacking event. Finally, the paper concludes in Section 6.

2. RELATED WORK

BGP (Border Gateway Protocol) is the defacto protocol used in the Internet today for the exchange of routing information between ASes (Autonomous Systems). Each AS is a collection of routing prefixes under the control of one network operator. The lack of security mechanisms on the existing applications of BGP, render it vulnerable to various types of attacks, such as prefix hijacks or Man- In-the-Middle attacks [5]. As a matter of fact, such events can have rather destructive effects on the Internet normal operation, due to their direct impact on the ASes' connectivity [6][7].

To this end, many researchers have focused their efforts on the development of methods that could lead to the detection of anomalies in the BGP infrastructure.

Data mining techniques have been used vastly today for the detection of BGP attacks. In Deshpande et al. [8], multiple features are introduced in order to represent the BGP update messages in a more abstract level. For each feature,

[*]This work has been partially supported by the European Commission through projects FP7-ICT-257495-VIS-SENSE and FP7-ICT-317888-NEMESYS funded by the 7th framework program. The opinions expressed in this paper are those of the authors and do not necessarily reflect the views of the European Commission.

VizSec '13 October 14 2013, Atlanta, GA, USA
Copyright 2013 ACM 978-1-4503-2173-0/13/10 ...$15.00.

a Generalized Likelihood Ratio (GLR) based hypothesis test is utilized so as to detect time periods of instabilities. The detected instability periods are correlated across all the individual features using a majority voting, and alerts are generated for the periods in which more of the half features indicate an anomaly. The disadvantage of this approach unlike the proposed BGPfuse method, is that the analyst is left out of the detection procedure and as a result it is not possible to change the parameters of the anomaly detection algorithm and redefine the results.

Li et al. [9] propose a signature based method, in which the classifier is trained to recognize certain types of behaviors that characterize each BGP anomaly, as for example worm attacks or router misconfigurations. Multiple features are introduced in order to represent the BGP activity on a specified time window. Using a collection of IF-THEN threshold based rules onto these features, the authors were able to classify and detect abnormal BGP events. As with the aforementioned approach the anomaly results are also static, as the analyst is left out of the detection procedure.

Zhang et al. [10] use two types of BGP anomaly detection, a signature based and a statistical based. The signature based method is comprised of a set of standard behaviors that characterize each type of anomaly. Moreover, using the statistical based method on multiple BGP features, the authors were able to acquire a score for each feature that represents the degree of anomaly of the time period under investigation. Furthermore, a linear sum of the scores of each feature is also utilized so as to fuse the features and acquire a single anomaly score. An extension of this work was presented by Teoh et al. [11], where the scores of each feature as well as the global score for all the features are visualized along the BGP update messages selected by the analyst. Using this visualization approach the analyst is able to adjust the parameters of the statistical and signature based methods and come up with better results. However, the adjustable parameters do not refer to the feature fusion procedure but rather to the definitions of anomalous BGP events and the threshold of the fused anomaly metric. The approach of using the visualization to change the parameters of the anomaly detection methods is related to the present work, which also utilizes visual methods to aid the analysis procedure. But unlike [11], the present work utilizes the visualization to aid the visual feature fusion procedure.

Al-Rousan et al. [12] presented multiple features that characterize the BGP activity. The authors used feature selection to reduce the number of features, combined with Naive Bayes classifiers for detecting BGP anomalies, including worm attacks and router misconfiguration. In comparison with the proposed approach the user is not able to change the parameters of the classification in order to find alternative or better results.

BGP-lens [13] examines a given time-series of BGP updates in the temporal and frequency space to discover interesting phenomena, such as periodic behaviors, and anomalies. The authors use a signature based detection algorithm.

Zhang et al. [14] propose the use of wavelets applied on feature vectors that represent BGP update dynamics. Using this approach outliers are detected, which represent possible BGP anomalies.

Biersack et al. [15] present an overview of the visualization tools used for anomaly detection in BGP, mainly based on the visualization of BGP raw data (announcements). The proposed approach, however, uses multiple features and provides a novel visual feature fusion method for their effective combination.

BGPeep [16] is a tool that visualizes the prefixes of the BGP announcements, as well as the origin ASes of these prefixes in an intuitive view. Using this approach, router misconfigurations and route flappings stand out in the visual display and are easily detected.

Compared with the aforementioned approaches, the proposed method focuses on visual feature fusion, so as to allow the analyst to combine all the available data and interactively perform hijack detection and attribution. The use of the graphs in combination with the introduced *Parallel Coordinates User Interface*, provides the actual feature values and feature correlations, as well as additional semantic information, e.g. the geolocation of the ASes, and the relationships between the different events. All the provided views are combined using linking and brushing [17]. But the novelty does not lay in the use of linking and brushing, but in the introduction of a visual scheme that enables feature fusion and allows the analyst to interactively change the parameters of the fusion according to his/her intentions.

3. BGP FEATURES DEFINITION

As it was noted earlier, BGPfuse provides a method for visually enhancing the investigation of BGP path-change events for potential evidence of malicious activity. A path-change event is caused by the circulation of two or more conflicting BGP announcements, which refer to the same prefix and have the same origin-AS, while at least one intermediate AS is different, e.g. Man-in-the-Middle attacks. Due to the high complexity and variability of the inter-AS relations, for evaluating the legitimacy of BGP path-changes, several features can be introduced that quantify the degree of anomaly of each path-change from different perspectives. Hence, in order to acquire a spherical view of the monitored phenomena, these multiple features are visually combined by BGPfuse for achieving the robust detection of any abnormal behavior.

Although the general BGPfuse framework can be applied in any set of relevant BGP features, for the purpose of the present paper the BGP features introduced in [18] have been chosen, since they present different, yet interdependent, attributes of the BGP operation and thus the need for an advanced method of fusing is more than important. The basic notion for the work in [18] lies within the fact that external Internet routing holds extensive geographic characteristics, i.e., the sequence of the traversed ASes is highly dependent on their geographic presence. Thus, according to [18], the AS-path in every BGP announcement is transformed into a country-path, by assigning each AS to the country that it is hosted. For this purpose, two sets need to be defined, the set of ASes:

$$A = \{a_i \mid i \in \{1, D_A\}\} \tag{1}$$

and the set of Countries:

$$C = \{c_i \mid i \in \{1, D_C\} \ and \ c_i \subseteq A\} \tag{2}$$

where D_A is the number of ASes in the Internet, and D_C the number of country domains in the Internet. Furthermore, each country has a specific number of ASes $c_i \subseteq A$ that are hosted in this country (*Origin-Country*).

At this point it should be noted that the higher-tier ASes operate at an international level, having routers in multiple countries. Thus, despite the fact that higher-tier ASes are uniquely identified by a sole country of origin, the attribution of such ASes in one country is not trivial. Furthermore, since these ASes participate in the majority of the announced BGP paths, this procedure also degrades the efficiency of the BGP hijack detection mechanism described here for two reasons: 1) announcements that include higher-tier ASes with distant countries of origin, would be erroneously considered as suspicious due to the high geographic deviation that they induce, and 2) hijacks executed by ASes located in countries that host higher-tier ASes will be lost, since they would be considered as usual-normal behavior. To overcome this limitation, the higher-tier ASes are not taken into account in the calculation procedure. Moreover, it must be underlined that the exclusion of the higher-tier ASes does not affect the efficiency of the proposed approach, since higher-tier ASes are not expected to participate in criminal activities.

Taking into account the AS-to-Country mapping, all the BGP announcements that are collected by the monitoring BGP router, are analyzed, so as to track down the respective Country-paths that result from the actual AS-paths. For each Country-path, the *Intermediate-Countries* that are traversed to reach the *Origin-Country* (from the specific *Monitoring-Country*, which is constant for each analysis) are identified and they are adequately characterized, in order to allow for quantifying the legitimacy/anomaly of the advertised route. To this end, four descriptive features are extracted and assigned to every *Intermediate-Country* of each BGP announcement:

1. CAP: The probability of appearance of the *Intermediate-Country* within the AS-path towards the specific *Origin-Country.*

2. CAPZ: The Z-score of the aforementioned probability.

3. CGL: The geographic deviation introduced by the *Intermediate-Country* within the AS-path towards the specific *Origin-Country.* It is defined as the ratio of the aggregate geographic distance between the *Monitoring-Country* and the *Origin-Country* when the route traverses the *Intermediate-Country* against the ideal direct path between the *Monitoring* and the *Origin Countries.*

4. CGLZ: The Z-score of the aforementioned CGL feature.

Taking into account the values of the above features for each *Intermediate-Country* within the AS-paths of the conflicting BGP announcements, a total score for the BGP path-change event is calculated, equal to the "worst" score of all the involved *Intermediate-Countries.* Being more specific, since, a normal BGP behavior regards AS-paths that follow common routes with low deviations from the direct line, the most suspicious BGP events concern low values of CAP and CAPZ as well as high values of CGL and CGLZ. Hence, the values of the overall BGP path-change event are equal to the corresponding values of the less probable and more deviating *Intermediate-Country.* In this respect, the most suspicious ASes in the path are the ones that are hosted in this outlying *Intermediate-Country.* Thus, the aforementioned features can be eventually defined on per *Intermediate-AS* basis, for each *Origin-Country* appearing in the BGP announcements.

The extreme values of interest for each feature along with their semantic cross-correlations are described in Tables 1 and 2. As it becomes apparent from this analysis, it is completely impractical to build a weight-based scheme for fusing these multiple features, since the significance of each metric is evaluated within the context of the rest attributes, as well as within the context of the overall state and trends of the system. Hence, in order to facilitate the creative combinational analysis of multiple information instances and perspectives towards solid conclusions, it is mandatory to go beyond mere algorithmic computations and exploit the power of visual analytics. Additionally, besides the filtering of the most suspicious cases, it is necessary to deploy a mechanism for deeper investigating the BGP topology, so as to infer any hidden inter-AS relationships.

4. BGPFUSE VISUALIZATION APPROACH

This section presents the visualization approach of BGPfuse, which is used so as to provide a visual fusion method of the BGP features defined in Section 3, for the purpose of detecting BGP path hijacking events. Once again, it must be underlined that the applicability of BGPfuse is not limited to the specific set of BGP features, but the proposed methodology can be easily extended to provide solution for visual fusion of BGP-related data.

BGPfuse is comprised of three visualization components: 1) Parallel Coordinates User Interface, 2) Feature Graph view, and 3) Combined Graph view. Each one of these components will be described in detail in the subsections that follow.

4.1 Parallel Coordinates User Interface

The *Parallel Coordinates User Interface* uses the Parallel Coordinates visualization approach [19] to visualize the interrelationships between the different features, which is further enhanced with filtering capabilities. Using this view and combined with the graph views, the analyst can perform visual fusion of the aforementioned features for the purpose of BGP path-hijacking detection.

Each Parallel Coordinate represents an individual feature, while the red lines that run across the Parallel Coordinates represent the values of each individual BGP event. The average value of each feature is depicted onto the respective parallel coordinate using a small blue horizontal line. It should be noted that the direction of each parallel coordinate is such that the extreme values of interest, according to Tables 1 and 2, are positioned at the upper part of the Parallel Coordinates User Interface, i.e, low values of the CAP and CAPZ features and high values of the CGL and CGLZ features are positioned at the upper part of the view. Fig. 1(a) depicts the described approach. Using this view, the analyst can immediately gain an understanding of the distribution that each feature follows, as well as possible correlations that may exist between them. Furthermore, the outlier values of each feature, which are of particular importance in BGPfuse, are easy to detect.

As it was mentioned in Section 3, the analyst is interested in events that have extreme values in all the available fea-

Table 1: Relationship between the probability (CAP), Z-score of probability (CAPZ) and the evidence of anomalous events. ↓ represents low and ↑ high values.

CAP	CAPZ	Description
↓	< 0 AND ↓	Very rare intermediate-country while only few rare alternative intermediate-countries exist. Strong evidence of anomaly.
↓	> 0	Very rare intermediate-country, yet more probable than the average. Other rare alternative hops exist. Light evidence of anomaly
↑	< 0	Common intermediate-country, yet there still exist more common routes. No evidence of anomaly
↑	> 0	One of the most common intermediate-countries. No evidence of anomaly.

Table 2: Relationship between the geographic deviation (CGL), Z-score of geographic deviation (CGLZ) and the evidence of anomalous events. ↓ represents low, ↑ high, and ⇑ extremely high values.

CGL	CGLZ	Description
-	$\rightarrow 0$	Close to the average geographic length. No evidence of length anomaly.
-	$\|\| < 1$	Distant from the average geographic length, yet comparable to the standard deviation. No strong evidence of length anomaly
↑	< 0	Noticeably more distant than the shortest path, but closer than the average one. Longer and thus more suspicious routes exist.
↓	↓	Close to both the minimum and the mean route in terms of length. Not only does not the existence of the specific country raise any alarm, but also the vast majority of the countries present a normal geographical distribution (low σ).
-	⇑	High distance from the mean rate, while the majority of the alternative paths are close to the average length. Strong evidence of length anomaly.

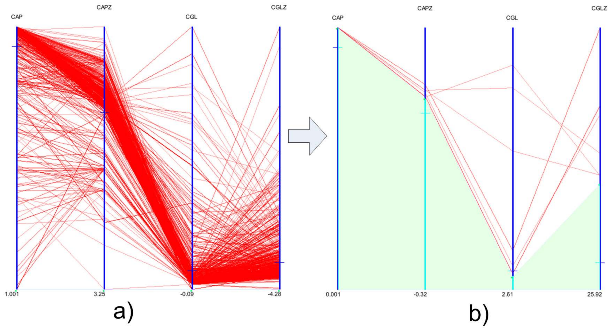


Figure 1: Parallel Coordinates User Interface. (a) The Parallel Coordinates visualization of the available feature values. (b) Using the sliders to adjust each individual feature threshold and visualize only the events that remain across all the features.

tures at the same time. The disadvantage of the Parallel Coordinates visualization, is that due to high cluttering, it does not facilitate the means necessary to accomplish this goal. In order to enhance the Parallel Coordinates approach, filtering is employed. More specifically, sliders are attached onto each parallel coordinate, whose position represents the value of the corresponding threshold. The events whose at least one feature value is below the predefined thresholds are omitted from the visualization. A similar approach was previously presented by Siirtola [20] for creating dynamic queries in parallel coordinates. Thus, by adjusting the position of the thresholds the analyst can perform visual fusion of the available features, so as to focus only on the most interesting events. The definition of the thresholds has a direct impact onto the feature and combined graph views, that directly reflect the remaining events, as well as any relationships between them.

The set of threshold values that are selected in the *Parallel Coordinates User Interface* are defined as follows:

$$T = \{t_i \mid i \in \{CAP, CAPZ, CGL, CGLZ\}\} \qquad (3)$$

where t_i is the selected threshold value of feature $i \in \{CAP, CAPZ, CGL, CGLZ\}$. For the application of the selected thresholds values the following function is introduced, in which if the result is 0, then the corresponding event is filtered out and omitted from the visualization:

$$f_T\left(t_i, e_i^j(w)\right) = \begin{cases} 1 & \begin{cases} e_i^j(w) > t_i, \forall i \in \{CGL, CGLZ\} \\ e_i^j(w) < t_i, \forall i \in \{CAP, CAPZ\} \end{cases} \\ 0 & \text{, for all the other cases} \end{cases} \qquad (4)$$

where $t_i \in T$ is the threshold value of feature $i \in \{CAP, CAPZ, CGL, CGLZ\}$, e_i^j is the j_{th} BGP hijacking event for the feature i and $e_i^j(w)$ its corresponding value.

4.2 Feature Graph view

Feature Graph view provides a graph based visualization of each feature. Using this view the analyst can detect which ASes and Countries are involved in suspicious events according to the selected feature, as well as any relationships that may exist between them.

As it was explained in Section 3 the BGP features are

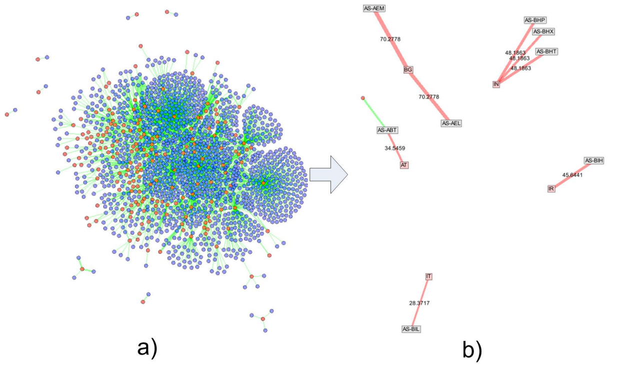


Figure 2: *Feature graph view* of the CGLZ feature, before (a) and after (b) the application of the threshold values. Red color represents the selected edges.

defined on per AS-Country basis, while each pair of AS-Country is characterized by multiple features. Thus, the *Feature Graph view* is comprised of two types of nodes, the country nodes, which are depicted using red color, and the AS nodes, which are depicted using blue color. The existence of an edge between an AS and a Country node, implies the occurrence of a BGP path change event from this intermediate AS to the corresponding destination country. More specifically $G_i = \{V_i, E_i\}$ is the notation used to represent the feature graph of feature $i \in \{CAP, CAPZ, CGL, CGLZ\}$ after the application of filtering:

$$E_i = \left\{ e_i^j \,|\, \forall\, f_T\left(t_i, e_i^j\right) = 1 \right\} \tag{5}$$

$$e_i^j = \{(a_k, c_l) \mid a_k \in \ A \ and \ c_l \ \in \ C\} \tag{6}$$

$$V_i = \left\{ v_i^j \,|\, (\, v_i^j \in A \ or \ v_i^j \in C)\, and \ v_i^j \in e_i^k \ , \forall e_i^k \in E_i \right\} \tag{7}$$

where vertex v_i^j represents either an AS or a Country, and e_i^k is the edge of the k_{th} event that connects an AS vertex and a Country vertex. Furthermore, V_i and E_i represent the set of vertices and edges of the *Feature Graph* G_i for feature $i \in \{CAP, CAPZ, CGL, CGLZ\}$.

As it was mentioned earlier, BGPfuse is interested only in the extreme values of each feature according to Tables 1 and 2, thus, the width of the edges is proportional to the importance of the value of the corresponding feature. For example, in the possibility feature graph (CAP), high edge widths represent low possibility values, while in the geographic deviation feature graph (CGL), high edge widths represent high feature values.

Each feature graph is comprised of two types of views. The classical graph view which is depicted in Fig. 2 and the world map view which is depicted in Fig. 5. The world map view positions the country nodes in their relative position on the globe, while the ASes are positioned close to their country of origin. Thus, the analysts can perform his/her analysis by also incorporating the geographical aspects of the path change events.

Fig. 2 depicts the *Feature Graph view* of the CGLZ feature. It is apparent that with out the application of filtering (2(a)) it is impossible to discriminate the important events from the bulk of BGP path change events. On the other hand, after the application of filtering (2(b)) the *Feature graph view* is much less cluttered while also visualizing only the most suspicious events. Thus, by utilizing the *Parallel Coordinates User Interface* to filter out irrelevant information and perform visual fusion, the analyst can focus only on its most important events.

4.3 Combined Graph view

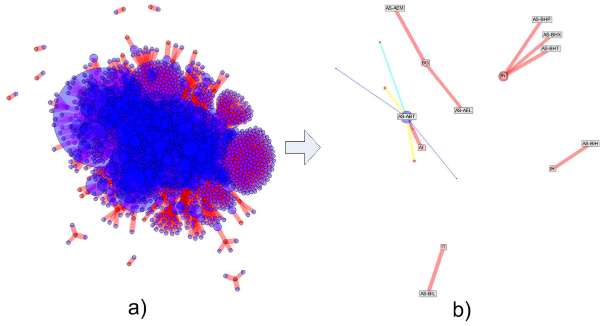


Figure 3: Combined Graph view of all the available features, before (a) and after (b) the application of the threshold values.

The *Combined Graph view* is a fused graph of all the individual feature graphs that is used for the purpose of highlighting their structural similarities. These similarities are used to highlight the suspicious BGP path change events across any number of features, as well as reveal possible participation of an actor in multiple events, visible from multiple features.

The *Combined Graph view* is a graph $GC = \{VC, EC\}$ where the set of edges and vertices are defined respectively as:

$$\begin{gathered} EC = \bigcup_i E_i = \Big\{ ec^k \mid ec^k = e_i^j, \, \forall e_i^j \in E_i, \\ \forall i \in \{\mathrm{CAP}, \mathrm{CAPZ}, \mathrm{CGL}, \mathrm{CGLZ}\} \Big\} \end{gathered} \tag{8}$$

$$VC = \left\{ vc^l |\; vc^l \in ec^k, \, \forall ec^k \in EC \right\} \tag{9}$$

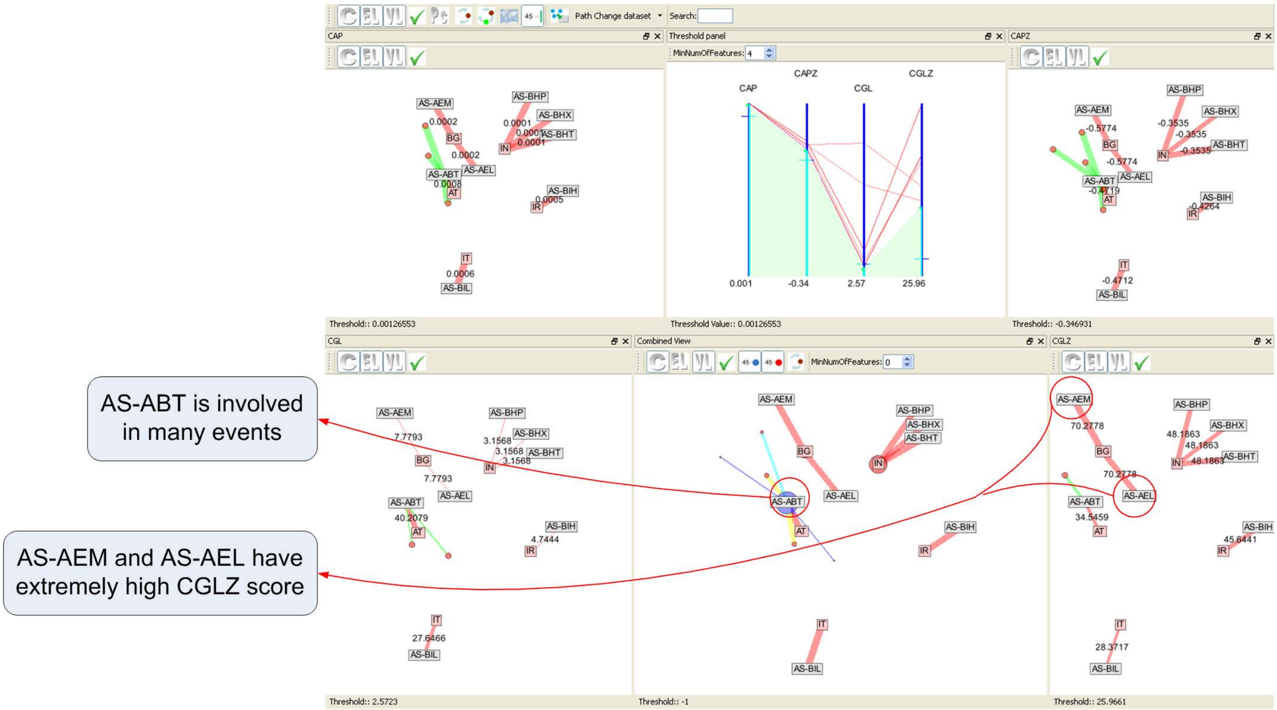
where ec^k is the k_{th} edge of the combined graph, which also exists in at least one other feature graph after the application of filtering.

One important aspect of the *Combined Graph view* is that it emphasizes the events that exist across many features. To achieve this, a metric is defined which quantifies the *Degree of existence* of each edge across the all the feature graphs:

$$\begin{gathered} D_e\left(ec^k\right) = \sum_i f_T\left(t_i, e_i^j\right), \, \forall e_i^j = ec^k, \\ i \in \{\mathrm{CAP}, \mathrm{CAPZ}, \mathrm{CGL}, \mathrm{CGLZ}\} \end{gathered} \tag{10}$$

thus the *Degree of existence* metric measures in how many features the corresponding event is visible from, after the application of filtering. This information is mapped onto the *Combined Graph* by changing the color and width of the edge. Table 3 describes this procedure.

Furthermore, another metric is defined that describes the *Degree of anomaly* of a vertex:



AS-ABT is involved in many events

AS-AEM and AS-AEL have extremely high CGLZ score

Figure 4: BGPfuse visualization of all the BGP path change events (W_{all}) that occurred on 24-Aug-2011, after the application of filtering. The set of selected thresholds is $T = \{(t_{CAP}, t_{CAPZ}, t_{CGL}, t_{CGLZ}) = (0.001, -0.347, 2.57, 25.9)\}$

Table 3: The color and the width of each edge according to the *Degree of existence* across all four features.

color	width	Degree of existence
red	4	exists across all 4 features
yellow	3	exists across 3 features
light blue	2	exists across 2 features
dark blue	1	exists only in 1 feature

$$D_v\left(vc^k\right) = \sum_j D_e\left(ec^j\right), where\ vc^k \in ec^j, \quad \forall ec^j \in EC \tag{11}$$

The *Degree of anomaly* metric is the sum of the *Degree of existence* of all the edges that include the corresponding vertex. The higher the *Degree of anomaly* of a vertex the most suspicious this AS or Country is, as it implies that is involved in many BGP path change events visible from many features after the application of filtering. The value of this metric is mapped onto the size of the corresponding vertex. Figure 3 depicts the *Combined Graph view* described here, before (3(a)) and after the application of filtering (3(b)). It should be noted that in Figure 3(a) the *Degree of anomaly* of the country vertices is not mapped onto their size, so as to reduce visual clutter.

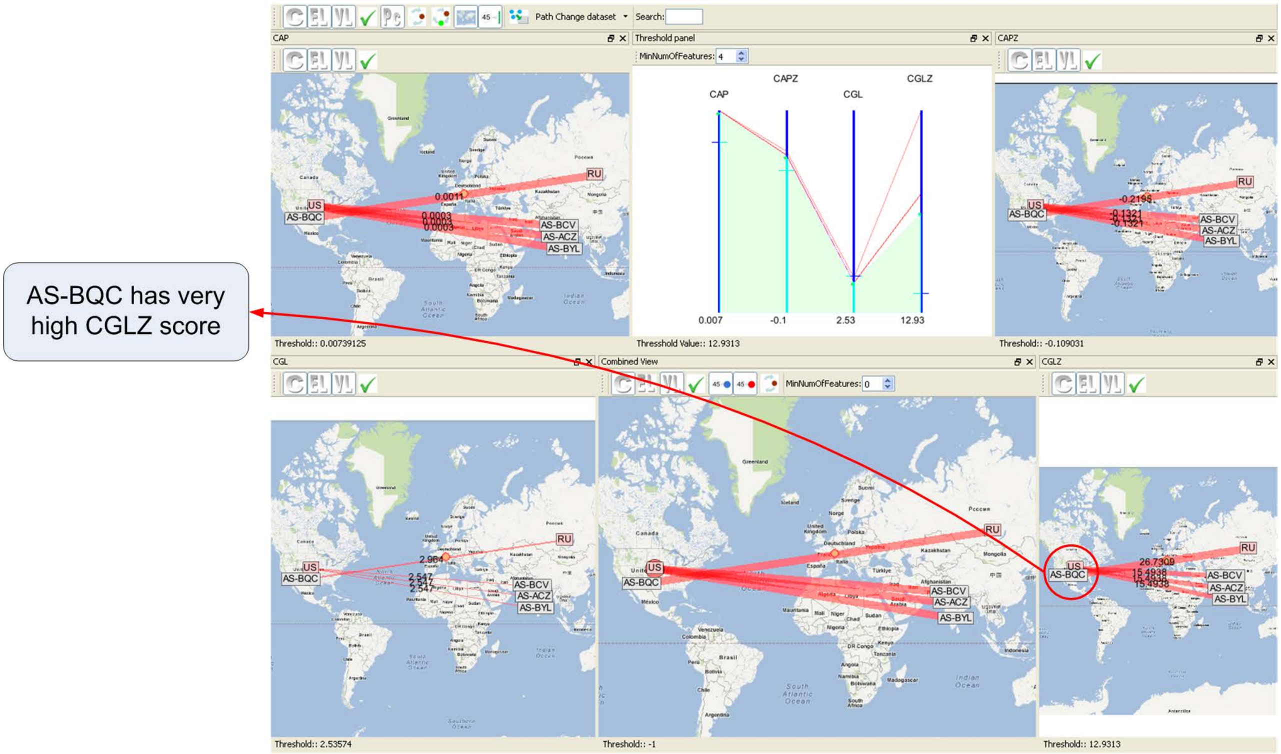
As in the case of feature graphs, the *Combined Graph view* also provides two types of views. The classical graph view, which is depicted in Fig. 3 and the world map view, which is depicted in Fig. 5.

5. IMPLEMENTATION IN REAL LIFE SCENARIO

In this Section BGPfuse is used to prominently detect and investigate a BGP path-hijacking incident. On August 20, 2011, a Russian telecommunication company, which from now on will be called Victim-AS, reported to the North American Network Operators Group (NANOG) that five of its prefixes had been hijacked. Although, the ownership of the prefixes was not affected, false routes were injected for the purpose of diverting Internet traffic through the Hijacking-AS, thus successfully implementing a Man-in-the-Middle attack. The Hijacking-AS is located in US. As a countermeasure, the Victim-AS responded on August 24, by announcing longer subprefixes with the correct paths.

Before continuing, it must be mentioned that the actual AS-numbers on the figures of BGPfuse are not presented due to privacy concerns. Instead, the corresponding AS-numbers were replaced by a random string of three characters, which from now on will help discriminate between the different ASes.

For the analysis procedure, there are two possibilities: 1) Take into account all the BGP events that refer to different paths, despite the fact that a subset of them might not have caused an actual path change. This set of all the different path events is defined as W_{all}. 2) Filter the events by taking into account only the BGP events that have caused a successful path change event, which represent the set of actual path change events W_{pc}. It is worth noting that $W_{pc} \subseteq W_{all}$.



MinNumOfFeatures: 4

MinNumOfFeatures: 0

Threshold:: 0.00739125

Thresshold Value:: 12.9313

Threshold:: -0.109031

Threshold:: 2.53574

Threshold:: -1

Threshold:: 12.9313

Figure 5: BGPfuse visualization of the successful BGP path change events (W_{pc}) that occurred on 24-Aug-2011, after the application of filtering. The set of selected thresholds is $T = \{(t_{CAP}, t_{CAPZ}, t_{CGL}, t_{CGLZ}) = (0.007, -0.109, 2.53, 12.93)\}$

The BGP announcements utilized in this Section were collected from the RIPE routing monitoring service [21].

5.1 Visualize all the BGP events that refer to different paths

In order to analyze the aforementioned event through BGPfuse, the set of all the BGP path change events W_{all} is firstly selected. The visualization approach of BGPfuse is depicted in Fig. 4, after the application of filtering. It is apparent through the *Combined Graph view* that AS-ABT is involved in many events, which is suspicious. This AS is either performing BGP hijacking attacks, or is a high tier AS. From the CAIDA [22] ranking it is apparent the AS-ABT is within the first 250 ASes, which probably implies that this event does not concern hijacks. Either way, further investigation is needed so as to reach definitive conclusions. Furthermore, from the CGLZ feature graph, it is apparent that two ASes, AS-AEM and AS-AEL have extremely high CGLZ score, which is an indication of anomaly.

After analyzing all the BGP path change events W_{all} a set of suspicious ASes was defined, which is comprised of all the ASes that are visible in Fig. 4. But, due to the nature of BGP it is difficult to discriminate between normal and suspicious behavior. As a result, the findings of BGPfuse need to be further investigated in order to reach safe conclusions. On the other hand, the analyst can focus and investigate only a small set of ASes, which is much easier than investigating all the ASes of the Internet.

5.2 Visualize the successful BGP path change events

To further deepen the analysis of the event in investigation, the set of the actual BGP path change events W_{pc} is selected. The visualization result of BGPfuse is depicted in Fig. 5 using a word map view. After the appropriate selection of thresholds in the Parallel Coordinates User Interface, it is apparent that AS-BQC has very high CGLZ score and very low CAP and CAPZ scores, which according to Tables 1 and 2 indicate an anomaly. In this case however, there is ground truth from the report of the victim AS to NANOG. AS-BQC is the Hijacking-AS which intercepted the Internet traffic towards the Victim-AS, probably for malicious reasons.

As a result of using the proposed approach, the analyst was able to detect many suspicious BGP hijacking events, as well as the aforementioned hijacking incident. BGPfuse achieves this by taking advantage of the computational power of the visualization approach, as well as the undeniable expert judgement, so as to perform a fusion of all the available features and detect any anomalous behaviors.

6. CONCLUSIONS

The present paper proposed BGPfuse, a scheme for visualizing and exploring BGP path change anomalies based on a set of multiple features. These features are able to quantify the degree of anomaly of each BGP hijacking event. BGPfuse provides a method to perform visual fusion of the aforementioned features, so as to help the analyst detect

BGP path hijacking events. An important aspect of these features is that they present complex cross-correlations and they have to be translated within the context of each other, as well as within the context of the other BGP events. To achieve this, a Parallel Coordinates view is proposed which is enhanced with filtering capabilities so as to discriminate between normal and abnormal events. Moreover, even when the most suspicious BGP events are pinpointed, in order to draw a solid conclusion of the events malicious nature, the inter-AS relationships need to be prominently revealed and decoded by exploiting the human perception. Individual feature graphs are proposed so as to represent all the ASes that are involved in path change events, as well as the origin countries of the ASes are being attacked, thus rendering easier to the analyst to detect patterns. Moreover, a combined graph is presented for the purpose of making structural similarities between all the feature graphs salient, and highlighting suspicious events and ASes, as well as possible event relationships. The proposed scheme is applied into a Real-World BGP Hijack Event, which demonstrates the analytics potential of the BGPfuse approach.

It should be noted, that BGPfuse uses a scalable approach, which renders it able to visualize and fuse a relatively large number of features by utilizing the power of Parallel Coordinates and the Combined Graph view.

7. REFERENCES

[1] G. J. Briem, J. A. Benediktsson, and J. R. Sveinsson, “Multiple classifiers applied to multisource remote sensing data,” *Geoscience and Remote Sensing, IEEE Transactions on*, vol. 40, no. 10, pp. 2291–2299, 2002.

[2] Q. Tao and R. Veldhuis, “Threshold-optimized decision-level fusion and its application to biometrics,” *Pattern Recognition*, vol. 42, no. 5, pp. 823–836, 2009.

[3] M. Arevalillo-Herráez, J. Domingo, and F. J. Ferri, “Combining similarity measures in content-based image retrieval,” *Pattern Recognition Letters*, vol. 29, no. 16, pp. 2174–2181, 2008.

[4] P. Chowdhury, S. Das, S. Samanta, and U. Mangai, “A Survey of Decision Fusion and Feature Fusion Strategies for Pattern Classification,” *IETE Technical Review*, vol. 27, no. 4, pp. 293–307, 2010.

[5] H. Ballani, P. Francis, and X. Zhang, “A study of prefix hijacking and interception in the internet,” *ACM SIGCOMM Computer Communication Review*, vol. 37, no. 4, p. 265, 2007.

[6] S. Murphy, “BGP security vulnerabilities analysis,” *RFC 4272*, 2006.

[7] O. Nordström and C. Dovrolis, “Beware of BGP attacks,” *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 1–8, 2004.

[8] S. Deshpande, M. Thottan, T. K. Ho, and B. Sikdar, “An online mechanism for BGP instability detection and analysis,” *Computers, IEEE Transactions on*, vol. 58, no. 11, pp. 1470–1484, 2009.

[9] J. Li, D. Dou, Z. Wu, S. Kim, and V. Agarwal, “An Internet routing forensics framework for discovering rules of abnormal BGP events,” *ACM SIGCOMM Computer Communication Review*, vol. 35, no. 5, pp. 55–66, 2005.

[10] K. Zhang, A. Yen, X. Zhao, D. Massey, S. F. Wu, and L. Zhang, “On detection of anomalous routing dynamics in BGP,” in *NETWORKING 2004. Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications*, pp. 259–270, Springer, 2004.

[11] S. T. Teoh, K. Zhang, S.-M. Tseng, K.-L. Ma, and S. F. Wu, “Combining visual and automated data mining for near-real-time anomaly detection and analysis in BGP,” *Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security VizSECDMSEC 04*, p. 35, 2004.

[12] N. M. Al-Rousan, S. Haeri, and L. Trajkovic, “Feature selection for classification of BGP anomalies using Bayesian models.,” in *ICMLC*, pp. 140–147, 2012.

[13] B. A. Prakash, N. Valler, D. Andersen, M. Faloutsos, and C. Faloutsos, “BGP-lens: Patterns and anomalies in internet routing updates,” in *Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining*, pp. 1315–1324, ACM, 2009.

[14] J. Zhang, J. Rexford, and J. Feigenbaum, “Learning-based anomaly detection in BGP updates,” in *Proceedings of the 2005 ACM SIGCOMM workshop on Mining network data*, pp. 219–220, ACM, 2005.

[15] E. Biersack, Q. Jacquemart, F. Fischer, J. Fuchs, O. Thonnard, G. Theodoridis, D. Tzovaras, and P.-A. Vervier, “Visual analytics for BGP monitoring and prefix hijacking identification,” *Network, IEEE*, vol. 26, no. 6, pp. 33–39, 2012.

[16] J. Shearer, K.-L. Ma, and T. Kohlenberg, “BGPeep: An IP-Space Centered View for Internet Routing Data,” in *Visualization for Computer Security*, pp. 95–110, Springer, 2008.

[17] J. S. Yi, Y. Ah Kang, J. Stasko, and J. Jacko, “Toward a Deeper Understanding of the Role of Interaction in Information Visualization,” *IEEE Transactions on Visualization and Computer Graphics*, vol. 13, no. 6, pp. 1224–1231, 2007.

[18] G. Theodoridis, O. Tsigkas, and D. Tzovaras, “A Novel Unsupervised Method for Securing BGP Against Routing Hijacks,” in *Computer and Information Sciences III*, pp. 21–29, Springer, 2013.

[19] A. Inselberg, *Parallel Coordinates: Visual Multidimensional Geometry and Its Applications.* springer ed., 2009.

[20] H. Siirtola, “Direct manipulation of parallel coordinates,” in *Information Visualization, 2000. Proceedings. IEEE International Conference on*, pp. 373–378, IEEE, 2000.

[21] RIPE Network Coordination Centre (available at http://www.ripe.net), “Routing Information Service project (RIS).”

[22] CAIDA (available at www.caida.org), “The Cooperative Association for Internet Data Analysis.”