Visual Analytic Representation of Large Datasets for Enhancing Network Security

**D3.2 Correlation analysis and abnormal event detection module**

Contract No. FP7-ICT-257495-VIS-SENSE

---

Workpackage  
Author  
Version  
Date of delivery  
Actual Date of Delivery  
Dissemination level  
Responsible  
Data included from  

The research leading to these results has received funding from the European Community’s Seventh Framework Programme (FP7/2007-2013) under grant agreement n°257495.
The VIS-SENSE Consortium consists of:

<table>
<thead>
<tr>
<th>Institution</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraunhofer IGD</td>
<td>Project coordinator</td>
</tr>
<tr>
<td>Institut Eurecom</td>
<td>Germany</td>
</tr>
<tr>
<td>Institut Telecom</td>
<td>France</td>
</tr>
<tr>
<td>Centre for Research and Technology Hellas</td>
<td>Greece</td>
</tr>
<tr>
<td>Symantec Ltd.</td>
<td>Ireland</td>
</tr>
<tr>
<td>Universität Konstanz</td>
<td>Germany</td>
</tr>
</tbody>
</table>

Contact information:
Dr Jörn Kohlhammer
Fraunhofer IGD
Fraunhoferstraße 5
64283 Darmstadt
Germany

e-mail: joern.kohlhammer@igd.fraunhofer.de
Phone: +49 6151 155 646
Contents

1 Introduction ................................................. 6

2 Feature Correlation Analysis and Definition of Proximity Measures .......................... 9
   2.1 Feature analysis and definition of proximity measures ............................... 10
       2.1.1 Evolution of the routing status over time ................................. 10
       2.1.2 Anomaly introduced by each AS along a prefix’s route ..................... 12

3 Anomaly Detection for Network and Threat Monitoring ..................................... 14
   3.1 The static case ............................................................................. 15
       3.1.1 Problem Definition .................................................................. 15
       3.1.2 Building the \( k \)-partite graph .............................................. 16
       3.1.3 The methodology for Anomaly Detection ..................................... 18
       3.1.4 Reducing memory requirements .............................................. 20
       3.1.5 Downweighting hub nodes ..................................................... 21
       3.1.6 The algorithm for Anomaly Detection ......................................... 22
       3.1.7 Results ............................................................................... 23
   3.2 The dynamic case ............................................................................ 26
       3.2.1 Problem definition ................................................................. 26
       3.2.2 Methodology .......................................................................... 27
       3.2.3 Results ............................................................................... 32

4 BGP Anomaly Detection .................................................................................. 37
   4.1 Background work ............................................................................. 38
   4.2 BGP anomaly detection on the basis of control-plane information analysis .... 39
       4.2.1 Detection and attribution of large scale BGP disturbances on the basis of spatiotemporal correlations ................................................. 40
       4.2.2 Analysis of BGP hijacks: Types and mechanisms ............................ 54
       4.2.3 BGP hijack detection and attribution on the basis of geospatial correlations ................................................................. 60
       4.2.4 BGP hijack detection and attribution on the basis of inferred inter-AS relationships ................................................................. 93
4.3 BGP hijack detection on the basis of data-plane information analysis

4.3.1 Extracting routing anomalies from BGP hijacking scenarios

4.3.2 Extracting suspicious patterns in forwarding paths

4.3.3 Investigating routing anomalies

4.3.4 Analysis of Suspicious BGP Anomaly

4.3.5 Link Telecom BGP Hijack

4.4 Exploitation of heterogeneous sources of information for the BGP activity

5 Conclusions
Abstract

The goal of this deliverable is to describe the research work conducted in the framework of Task 3.1 of WP3. Task 3.1 aims at developing novel algorithms for abnormal event detection from spatiotemporal network information. Therefore, Deliverable 3.2 describes the anomaly detection algorithms for network and threat monitoring, as well as for BGP hijack detection. It should be noted that, the data collected by VIS-SENSE refer to attack events and, thus, should be all considered as “abnormal”. However, among all these attack events, we refer as “abnormal” only to those that have distinctively different patterns from the rest. The anomaly detection algorithms developed within VIS-SENSE are both distance-metric based and non distance-metric based. Moreover, a variety of expressive features have been extracted from raw network trajectory data and defined in Deliverable 3.1. This set of features is enhanced with some new features, which are the result of a feature extraction process and are described in this deliverable. Therefore, an important part of the work carried out in this activity is the definition of appropriate proximity measures that can be used to characterize the similarity of the newly defined features. Furthermore, a feature correlation analysis is conducted to select the most appropriate features for anomaly detection.
1 Introduction

In this deliverable, several aspects of the VIS-SENSE semantic analysis framework are defined. Specifically, within Task 3.1 a semantic analysis of the available information is performed that detects potential abnormal events like irregular patterns of network and routing traffic. Moreover, we perform a correlation analysis of the set of descriptive features that correspond to the data that are collected by the VIS-SENSE data collection infrastructure. The developed techniques are adapted to fit our purposes and generate output to be usable by the advanced data mining techniques for attack attribution developed within Task T3.2, but also for the visualization tools developed within WP4, e.g. by extracting a set of descriptive features and the corresponding anomalies in the dataset that will be fed to the visualization tools developed in WP4. This deliverable is organized as follows.

Chapter 2 presents and analyses a set of relevant descriptive features for BGP analysis, which augments the set of features presented in Deliverable 3.1 - Specifications of the Network Analytics Algorithms and discusses the fundamental issue of feature correlation analysis which is strongly coupled with the performance and efficiency of almost any algorithm developed at the network analytics layer. By removing irrelevant features from the data, feature correlation analysis helps improve the performance of the developed algorithms, improve their interpretability and enhance generalization capability. VIS-SENSE will combine analytical methods for feature correlation analysis with visual ones to help the security analysts to acquire better understanding about the underlying structure of their data by telling them which features are important and how they relate to each other.

Chapter 3 and Chapter 4 analyse the anomaly detection algorithms developed within VIS-SENSE with respect to both network and threat monitoring and BGP hijack detection. By identifying deviation in reference to some “normal behavior”, anomaly detection techniques will reveal significant and often critical actionable information to the analyst and, eventually, they will highlight the occurrence of new phenomena or changes in the modus operandi of malicious actors. Anomalies might be induced in the data for a variety of reasons, such as malicious activity (e.g., BGP hijack, cyber-intrusion, etc.), breakdown of a system, misconfiguration of a system or even errors caused by human intervention. It should be noted that, the data collected by VIS-SENSE refer to attack events and, thus, should be all considered as “abnormal”. However, among all
these attack events, we refer as “abnormal” only to those that have patterns that are distinctively different from the rest.

The developed algorithms are based both on the definition of appropriate proximity measures that can be used to characterise the similarity of different aspects of spatio-temporal data and on non distance-metric based analysis methods. The key challenge for the anomaly detection algorithms to be developed is the huge volume of data and, thus, have to be computationally efficient to handle these large sized inputs. Moreover, the data have to be manipulated in a near real-time manner, thereby requiring algorithms with relatively low time complexity. Another issue related to the large sized input is the false alarm rate. Since the data amounts to millions of data objects, a few percent of false alarms can make analysis overwhelming for an analyst.

In Chapter 3, we emphasize on anomaly detection algorithm for network and threat monitoring. The developed algorithms search for contextual anomalies in the structure of data and are based on graphs. Therefore, the structure in the data set is induced by the edges connecting different nodes and the anomalies are related to the structural properties of the graph. By using graph-based anomaly detections for network and threat monitoring, two different but equally important problems will be addressed. The first one, which is referred to as the static case, is related to the detection of structural anomalies in a given graph. The second one, which is referred to as the dynamic case, is related to detecting anomalies in a time-series of graphs.

In Chapter 4 a detailed description of novel BGP anomaly detection and attribution methodologies is presented and evaluated on the basis of existing real-life scenarios. More concisely, two different as well as complimentary approaches are primarily identified, i.e. control-plane and data-plane analysis, which take into consideration the raw BGP data and the actual IP routing respectively. The control-plane techniques initially focus on the aggregation of the BGP activity on a per country basis, so as to exploit the inherent geospatial consistency of the Internet infrastructure, while a graph-based methodology is also developed by exploiting the inter-AS relationships that are inferred through the processing of the BGP messages. Furthermore, the detection mechanism that is developed on the basis of the data-plane information exploits the fact that malicious routing disturbances (BGP hijacks) are usually executed within the framework of other cyber crimes, such as spam campaigns.

Finally, Chapter 5 concludes the Deliverable.

At this point, it must be mentioned that part of the work included in this deliverable is also described in the paper “A Novel Unsupervised Method for Securing BGP against Routing Hijacks”, which has been accepted for publication in the Proceedings of the “27th International Symposium on Computer and Information Sciences (ISCIS 2012)” 22, as well as in the paper “Visual Analytics for BGP Monitoring and Prefix Hijacking
Identification”, which has been accepted for publication in the “IEEE Network Magazine - Special Issue on Computer Network Visualization” [9]. Moreover, additional papers regarding the work of D3.2 have already been submitted and they are in the review process.
2 Feature Correlation Analysis and Definition of Proximity Measures

The network analytics algorithms developed with the framework of the VIS-SENSE project will provide the means for a semantic analysis of the available information that will enable the extraction of specific patterns of activity and the detection of abnormal events like irregular patterns of network traffic. Therefore, a variety of expressive features have to be defined and extracted from raw network trajectory data collected by the data collection infrastructure. In Deliverable 3.1 - Specifications of the network analytics algorithms, a set of relevant features were described for each of the use case scenarios we have considered in the VIS-SENSE project and which were further described in the Deliverable 1.2 - Use case analysis and user requirements. This set is augmented with some new features that are presented in this chapter. For these newly defined features, appropriate proximity measures are proposed. Finally, this chapter discusses the issue of feature correlation analysis.

Feature selection is accomplished on the basis of correlation between features. In particular, the developed methodologies investigate the following hypothesis: A good feature subset is one that contains features highly correlated with (predictive of) the class, yet uncorrelated with (not predictive of) each other. The evaluation of the above hypothesis is accomplished by creating a feature selection algorithm that evaluates the worth of feature sets. The developed method measures the correlation between features based on their inter-relationships. The general concept of correlation-based feature selection does not depend on any particular data transformation. All that must be supplied is a means of measuring the correlation between any two features. The developed method will be a fully automatic algorithm and it will not require the user to specify any thresholds or the number of features to be selected, although both will be simple to incorporate if desired. Lastly, the developed method will operate on the original feature space, meaning that any knowledge induced by the network analytics algorithms, using features selected by the proposed mechanism, can be interpreted in terms of the original features, not in terms of a transformed space.

Additionally, particular emphasis must be laid on the fact that, within the integrated visual analytics framework of VIS-SENSE, the developed analytical method for feature correlation analysis is combined with visual methods for feature correlation analysis,
so that the security analyst can select the optimum subset of features for each task (e.g. anomaly detection, attack attribution, etc.) and use case. As a consequence, underlying feature correlations that cannot be tracked down via traditional mathematical approaches, are successfully explored and identified through the implementation of adequate interactive visualization modules that are capable of exploiting the human background knowledge and which are extensively described in the deliverables of WP4.

### 2.1 Feature analysis and definition of proximity measures

In order to acquire an as thorough as possible insight into the profoundly volatile as well as multi-dimensional BGP activity, it is of primary importance to proceed with the extraction of novel features that shall be capable of capturing different aspects of the whole range of the abnormal events that are encountered within the BGP functionality. Furthermore, it is equally important, along with the novel features, also to define the most appropriate proximity measures that shall succeed in tracing the features’ dynamics on the basis of the unique inherent characteristics of the corresponding macroscopic phenomena that are described by each feature.

#### 2.1.1 Evolution of the routing status over time

The ultimate result of the exchanged BGP data, i.e. primarily prefix announcements and withdrawals, is the formulation of the routing directives according to the continuously altering conditions of the Internet infrastructure. Hence, the monitoring and the analysis of the ongoing BGP activity along with the corresponding routing status as it alters in time is expected to allow for the detection and attribution of any anomalous routing phenomena. In this respect, it would be highly beneficial to be able to numerically compare successive imprints of the routing tables, so as to be able to trace any significant infrastructural alterations.

To this end, let $A$ be the set of all the $Q$ active ASes that are announced as a prefix’s either owners or intermediate hops; then the vector $V$ is introduced in order to represent the number of an AS’s appearances within the routing table:

$$
V = \begin{bmatrix}
N(A_1) \\
\vdots \\
N(A_Q)
\end{bmatrix}
$$

(2.1)

where $N(A_q)$ is the number of occurrences of AS $A_q$ in the routing table under investigation, $\forall q \in \{1, \ldots, Q\}$. Assuming stable BGP operation, $V$ should retain a consistent
2.1 Feature analysis and definition of proximity measures

behavior across time. Thus, the analysis of the evolution of \( \mathbf{V} \) can provide the necessary means for facilitating the deduction of useful as well as safe conclusions regarding the existence of BGP anomalies within the respective time windows. In this context, the matrix \( \mathbf{R} \) is introduced, comprising multiple sequential vectors \( \mathbf{V} \) acquired at different time instants with period \( \tau \).

\[
\mathbf{R} = [\mathbf{V}_{t_1}, \ldots, \mathbf{V}_{t_I}] = \begin{bmatrix}
N(A_1, t_1) & \ldots & N(A_1, t_I) \\
\vdots & \ddots & \vdots \\
N(A_Q, t_1) & \ldots & N(A_Q, t_I)
\end{bmatrix}
\]  

(2.2)

where \( \mathbf{V}_{t_i} \) is the vector \( \mathbf{V} \) estimated at time instant \( t_i \) (\( t_i - t_{i-1} = \tau \)), \( \forall i \in \{1, \ldots I\} \)

\[\mathbf{V}_{t_i} = \begin{bmatrix}
N(A_1, t_i) \\
\vdots \\
N(A_Q, t_i)
\end{bmatrix}, \forall i \in \{1, \ldots I\} \]  

(2.3)

and \( N(A_q, t_i) \) is the number of appearances of AS \( A_q \) in the routing table imprint taken at time instant \( t_i \).

Based on \( \mathbf{R} \), the Pearson Coefficient matrix against time (\( \rho^T \)) is computed.

\[\rho^T = \begin{bmatrix}
\rho(\mathbf{V}_{t_1}, \mathbf{V}_{t_1}) & \ldots & \rho(\mathbf{V}_{t_1}, \mathbf{V}_{t_I}) \\
\vdots & \ddots & \vdots \\
\rho(\mathbf{V}_{t_I}, \mathbf{V}_{t_1}) & \ldots & \rho(\mathbf{V}_{t_I}, \mathbf{V}_{t_I})
\end{bmatrix} \]  

(2.4)

where \( \rho(\mathbf{V}_{t_i}, \mathbf{V}_{t_j}) \) is the Pearson Coefficient between vectors \( \mathbf{V}_{t_i} \) and \( \mathbf{V}_{t_j} \), i.e. between the routing tables estimated at time instants \( t_i \) and \( t_j \), \( \forall i, j \in \{1, \ldots I\} \), and \( \rho^T \) is of dimensions \( I \times I \). The notion behind the definition of \( \rho^T \) is to quantify the correlation of the different routing table instances and therefore to pinpoint the time window (intermediate time between any two of the compared time instants) when the time consistency of the routing table is distorted.

Moreover, utilizing \( \mathbf{R} \), the Pearson Coefficient matrix against AS (\( \rho^A \)) can also be calculated. More precisely, for ease of reference, the vector \( \mathbf{V}^A \) is introduced, where \( \mathbf{V}^A_q \) is built upon the row \( q \) of \( \mathbf{R} \), i.e. \( \mathbf{V}^A_q \) comprises all the different number of occurrences for AS \( A_q \) throughout the whole set of the consecutive monitored routing table instances.

\[\mathbf{V}^A_q = \begin{bmatrix}
N(A_q, t_1) \\
\vdots \\
N(A_q, t_I)
\end{bmatrix}, \forall q \in \{1, \ldots Q\} \]  

(2.5)
Then, $\rho^A$ is computed from

$$
\rho^A = \begin{bmatrix}
\rho(V_1^A, V_1^A) & \cdots & \rho(V_1^A, V_I^A) \\
\vdots & \ddots & \vdots \\
\rho(V_I^A, V_1^A) & \cdots & \rho(V_I^A, V_I^A)
\end{bmatrix}
$$

(2.6)

The Pearson Coefficient matrix against AS allows the analyst to perform clustering of the ASes that present similar behavior during the BGP anomaly event that is detected with the use of the Pearson Coefficient matrix against time ($\rho^T$) and hence to significantly enhance the attribution of the BGP disturbance phenomena with a peer insight into the perceived activity at AS level.

### 2.1.2 Anomaly introduced by each AS along a prefix’s route

Under conditions of normal equipment/link operation, Internet routing paths are formulated on the basis of:

- Inter-AS agreements and policies, e.g. client-provider relationships.
- Prioritization rules for maximizing the efficiency of the end-to-end communication, e.g. path selection for minimum delay.
- Unforeseeable and usually temporal congestion phenomena, i.e. detours for avoiding traffic bottlenecks.

Thus, it is expected that, throughout the whole monitoring period, only a finite set of ASes is traversed along each prefix’s path. In this respect, calculating the probability of an AS’s appearance along a prefix’s route, shall provide a solid evidence of the legitimacy of a potential new BGP announcement containing the specific AS for the prefix under investigation.

In this context, let $A^p$ be the set of all the $K$ different ASes that have been recorded as intermediate hops towards prefix $p$, according to the exchanged BGP data. Then, similarly to (2.1), the vector $V^p$ is defined for representing the number of an AS’s occurrences along the paths of prefix $p$.

$$
V^p = \begin{bmatrix}
N(A_1^p) \\
\vdots \\
N(A_K^p)
\end{bmatrix}
$$

(2.7)

where $N(A_k^p)$ ($\forall k \in \{1, \ldots, K\}$) is the number of BGP announcements for prefix $p$ that included $A_k^p$ as an intermediate hop. Exploiting the calculation of $V^p$, the corresponding
probability of appearance $\forall A^p_k \in \mathbf{A}^p$ is estimated.

$$B(A^p_k) = \frac{N(A^p_k)}{\sum_{k=1}^{K} \{N(A^p_k)\}}$$

(2.8)

$B(A^p_k)$ provides a quantitative metric of how common is the existence of the AS $A^p_k$ within a path of prefix $p$. The lower the value of $B(A^p_k)$ is, the more suspicious the appearance of $A^p_k$ is considered to be.

Moreover, by calculating the Z-Score of $B(A^p_k)$, an additional metric is acquired that allows for studying the behavior of each AS in conjunction with the overall activity perceived for prefix $p$.

$$S^B(A^p_k) = \frac{N(A^p_k) - E[\mathbf{V}^p]}{\sigma[\mathbf{V}^p]}$$

(2.9)

where $E[\mathbf{V}^p]$ and $\sigma[\mathbf{V}^p]$ are respectively the mean value and the standard deviation of the $\mathbf{V}^p$ elements.

At this point it must be underlined that the aforementioned approach forms the generic cornerstone for the specific feature analysis and proximity measures definition that is performed within the framework of the BGP anomaly detection and attribution methodology and which is presented and evaluated in full detail in Chapter 4. In particular, in Chapter 4 the concepts introduced hereby are adequately elaborated in order to efficiently address the characteristics of two of the most prominent cases of BGP anomalies.
3 Anomaly Detection for Network and Threat Monitoring

The anomaly detection algorithms developed within VIS-SENSE for network and threat monitoring aim at detecting contextual anomalies, which are also referred to as conditional anomalies. In this case, data instances (attack events) are considered anomalous in a specific context. The notion of a context is induced by the structure in the data set and is specified as a part of the problem formulation for each use case scenario. Each data instance is defined using following two sets of attributes: i) contextual attributes are used to determine the context (or neighborhood) for that instance. For example, in spatial data sets, the longitude and latitude of a location are the contextual attributes. In time-series data, time is a contextual attribute which determines the position of an instance on the entire sequence, ii) behavioral attributes define the non-contextual characteristics of an instance. In the specific case of the anomaly detection algorithms developed within VIS-SENSE, which make use of graphs, the structure in the data set is induced by the edges connecting different nodes.

The data collected by the data collection infrastructure of VIS-SENSE can be represented by graphs by considering timestamped pairs of attributes (e.g., source-destination pairs from attack events, email messages, BGP update messages, etc.). Moreover, the output of various algorithms operating at the network analytics layer will be represented by an edge-weighted graph. Specifically, having computed the distances between attack feature vectors, an edge-weighted graph $G_k$ can be built in which the vertices (or nodes) are mapped to the feature vectors $x(k)$ and the edges (or links) reflect the similarity between data objects regarding the considered feature. As customary, the undirected edge-weighted graph (with no self-loops) obtained for a given feature $F_k$ can be represented by its corresponding weighted adjacency matrix (or dissimilarity matrix), which is the $m \times m$ symmetric matrix $A_k(i,j)$. Furthermore, the per-feature computed graphs can be fused to produce a single graph that describes the network state at a given time.

The network analytics algorithms developed within the VIS-SENSE project for anomaly detection in graphs aim at modeling and enhancing the analyst’s understanding of complex global phenomena that arise due to local interactions between graph entities. By using graph-based anomaly detections for network and threat monitoring, two different but equally important problems will be addressed.
3.1 The static case

The first problem is the detection of structural anomalies in a given graph, which is referred to as the static case. Detecting regions of a graph that are anomalous with respect to the rest of the graph can reveal attack strategies that significantly differ from commonly used ones (e.g., malware that exhibits different strategies to propagate or cyber-criminals that develop different methods to launch attacks). Detecting new strategies may indicate a significant shift in the modus operandi of attackers or the rising of new phenomena.

The second problem to be tackled by anomaly detection techniques is the detection of anomalies in a graph either in comparison with a subsequent graph or within a time-series of graphs, which is referred to as the dynamic case. Detecting anomalies in a time-series of graphs can highlight the occurrence of new phenomena and changes in the modus operandi of malicious actors by revealing how they change and adapt their strategies over time to launch more sophisticated attacks.

3.1 The static case

The security problems that are examined by VIS-SENSE and pertain to network and threat monitoring involve data objects of multiple types that are related to each other, which can be naturally formulated as a \( k \)-partite graph. For example, attack events recorded by the honeypot collection infrastructure are related to malware types, geolocation of attackers, ports used to communicate with the honeypot, IP address of the attacker, etc. However, the research on mining the hidden structures from a \( k \)-partite graph and particularly on detecting anomalies of the underlying structure is still limited and preliminary. Therefore, the research work conducted in the framework of the VIS-SENSE project aims at proposing a general model, to find the hidden anomalies in a \( k \)-partite graph. The model provides a principal framework for unsupervised anomaly detection on \( k \)-partite graphs of various structures. Under this model, we derive a novel algorithm to identify the hidden anomalies of a \( k \)-partite graph by identifying abnormal nodes, using neighborhood information. The novelty and strength of our approach resides in its ability to incorporate multiple features, searching for anomalies in the multi-dimensional space. Consequently, the developed scheme searches for contextual anomalies in the specific context formulated by taking all features into account.

3.1.1 Problem Definition

A \( k \)-partite graph is a graph where nodes can be divided in \( k \) disjoint groups \( (V_0, \ldots, V_{k-1}) \), such that no edge connects the vertices in the same group. More formally, a \( k \)-partite
The subgraph $G_l$ formulated by considering nodes only in $V_0$ and $V_l$, $l \in [1, k - 1]$, can be conceptually stored in a $N_0$-by-$N_l$ matrix $M_l$, where $M_l(i, j)$ is the weight of the edge $\langle i, j \rangle$. The value can be 0/1 for an unweighted graph, or any non-negative value for a weighted graph.

The nodes in $V_0(V_l)$ are called row (column) nodes. Note that a column node links to a row node if the corresponding matrix element is not zero. Moreover, row node $n_i$ connects to another row node $n_j$ if there is a column node $c$ linking to both $n_i$ and $n_j$. We call that path a connection between $n_i$ and $n_j$ through $c$. Nodes $n_i$ and $n_j$ can have multiple connections via different column nodes.

For each subgraph $G_l$, $l \in [1, k - 1]$, we can construct the adjacency matrix $A_l$ of $G_l$.
3.1 The static case

Figure 3.1: A 6-partite graph. White circle nodes in the middle represent rogue websites monitored by HARMUR. The nodes corresponding to the feature values of 5 different features (Geolocation, ASN, CreationDate, Registrant and Name-Server) are placed on the sides of a pentagon using different coloring schemes. Feature values can be connected only to rogue websites and not with each other.
3 Anomaly Detection for Network and Threat Monitoring

using $M_l$:

$$A_l = \begin{pmatrix} 0 & M_l \\ M_l^T & 0 \end{pmatrix}$$

In particular, $A_l(i, j)$ denotes the element at $i$-th row and $j$-th column in $A_l$. Suppose we want to traverse the subgraph starting from the row node $n_i$. Then, we have to transform matrix $A_l$ into a transition matrix $P_l$, such that the sum of the probabilities of taking and edge $\langle i, j \rangle$, starting from the row node $n_i$, does not exceed 1. Therefore, the most common approach is to make, for each row node $n_i$, the normalization of the edge weight over all the outgoing edges from $n_i$ proportional to the edge weight.

More formally:

$$P_l(i, j) = \frac{A_l(i, j)}{\sum_{k=1}^{N_l} A_l(i, k)}$$

and

$$P_l = \begin{pmatrix} 0 & M_l^T \\ M_l & 0 \end{pmatrix}$$

Then, by considering the transition matrices $P_l$ corresponding to each subgraph $G_l$, we can construct the transition matrix $P$ of $G$ as follows:

$$P = \begin{pmatrix} 0 & w_1 \cdot M_1^T & w_2 \cdot M_2^T & \cdots & w_{k-1} \cdot M_{k-1}^T \\ M_1^T & 0 & 0 & \cdots & 0 \\ M_2^T & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ M_{k-1}^T & 0 & 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} 0 & M \\ M_1^T & 0 \\ M_2^T & 0 \\ \vdots & \vdots \\ M_{k-1}^T & 0 \end{pmatrix}, \quad (3.1)$$

where $w_l$ is the weight assigned to Feature $l$ and $\sum_{l=1}^{k-1} w_l = 1$.

3.1.3 The methodology for Anomaly Detection

Given a row node $n_i \in V_0$, we want to compute a relevance score for each row node $n_j \neq i \in V_0$. The final result is a 1-by-$N_0$ vector consisting of all the relevance scores to $n_i$.

Our intuition is as follows. We do multiple random walks starting from $n_i$, and count the number of times that we visit each $n_j \in V_0$. These counts reflect the relevance of
3.1 The static case

Figure 3.2: Many connections between \( n_i \) and \( n_j \)

those nodes to \( n_i \). The probability of visiting \( n_j \in V_0 \) from \( n_i \) is the relevance score we want to obtain. In the following, we list some scenarios in which the row nodes have high relevance scores.

- \( n_j \) usually has a high relevance score to \( n_i \) if (1) \( n_j \) has many connections to \( n_i \) as shown in Figure 3.2 or (2) the connections only involve \( n_i \) and \( n_j \) as shown in Figure 3.3. Scenario (1) is obvious because the row nodes \( n_j \) and \( n_i \) have many connections through the columns nodes, which indicates the strong relevance between \( n_j \) and \( n_i \). Scenario (2) is less obvious. The intuition is that the connection that only links \( n_i \) and \( n_j \) brings more relevance between \( n_i \) and \( n_j \) than the connections linking \( n_i \), \( n_j \) and other nodes. The relevance score is not only related to the number of connections but also to the number of nodes involved in the connections. One observation is that the node \( n_j \) with the highest relevance score is not necessarily the one with most connections to \( n_i \). The reason is that those connections link to nodes other than \( n_i \) and \( n_j \) as well. Thus, the relevance is spread out among many different nodes. Nevertheless, both the scenarios above are well captured by our algorithm in spite of its simplicity.

3.1.3.0.1 Random Walk. In a random walk with restart one needs to compute the steady probability vector \( \vec{u}_i \) over all the nodes \( n_i \) in \( G \). Then, we can extract the
probabilities of the row nodes as the score vectors. Towards this end, the input row node $n_i$ is transformed into a $(\sum_{i=0}^{k-1} N_i) \times 1$ query vector $\vec{q}_i$ with 1 in the $i$-th row and 0 otherwise. Therefore, if $c$ is the probability of restarting a random walk from the row node $n_i$, then the steady-state probability vector $\vec{u}_i$ can be computed by the following iterative process:

$$\vec{u}_i = (1 - c) P \vec{u}_i + cq_i$$  \hspace{1cm} (3.2)$$

The iterative procedure described by (3.2) is stopped when $\delta(\vec{u}_i) < \epsilon$. The addition of $cq_i$ has actually the effect of adding self-loops to the graph, so that the neighborhood around each node is enforced. This is essential due to the fact that, without self-loops, the random walk for each given node would visit mostly the hub nodes of the graph and this probability would be independent of the starting node $n_i$. A second point worth mentioning is the selection of parameter’s $c$ value. An optimum value of 0.15 is proposed in [36]. However, such a value has the undue effect of strengthening the neighborhood around each node too much, especially in the cases of large graphs where nodes have many outgoing edges. This results in relevance scores, which do not accurately reflect the graph structure around each node. Therefore, we opt for a different strategy, where the value $c_i$ for a given node $n_i$ is dependent on the number of outgoing edges (outdegree) of this node, i.e. the non-zero elements of row $i$ in $P$. Our strategy is analyzed in the following.

### 3.1.4 Reducing memory requirements

A weakness associated with random walks is the large memory requirement and execution time due to matrix multiplication. However, the actual computation of the relevance scores can utilize the $k$-partite structure and the sparsity of the matrix to have more
saving. More specifically, we do not materialize $P$ and modify equation (3.2) as follows:

$$\vec{u}_i = (1 - c) \begin{pmatrix} M \vec{u}_i(N_0 + 1 : N) \\ M_1^T \vec{u}_i(1 : N_0) \\ \vdots \\ M_{k-1}^T \vec{u}_i(1 : N_0) \end{pmatrix} + c \vec{q}_i$$

where $\vec{u}_i(1 : N_0)$ and $\vec{u}_i(N_0 + 1 : N)$ are the vectors of first $N_0$ and last $\sum_{l=1}^{k-1} N_l$ elements of $\vec{u}_i$, respectively. If we compute the relevance scores for all the nodes, we have a similarity matrix $S$.

The saving is significant when the number of nodes in $V_0$ and the number of nodes in every other $V_l, l \neq 0$ differ a lot. Therefore, equation (3.3) is used in practice instead of (3.2).

### 3.1.5 Downweighting hub nodes

Moreover, to alleviate the unnecessarily large impact of hub nodes in the formation of clusters, we apply a weight transformation step to input graphs $A_l$, before normalizing their rows so as to derive each transition matrix $P_l$. Specifically, for a given node $n_i$, the weight of each edge $\langle i, j \rangle$ is downweighted by the outdegree of the target node $n_j$:

$$A_l(i, j) = \frac{A_l(i, j)}{\text{outdegree}(n_j)}$$

The purpose of the above step is to downweight the edges involving high-degree (or hub) nodes, as they can have an undue influence on the calculation of relevance scores.

In the literature, there are also other downweight schemes proposed, as in [18]:

$$A_l(i, j) = \frac{A_l(i, j)}{\text{outdegree}(n_i)} + \frac{A_l(i, j)}{\text{outdegree}(n_j)}$$

This method downweights the weight of each edge $\langle i, j \rangle$ of a given node $n_i$, by the outdegree of both the target node $n_j$ and the source node $n_i$. However, we have noticed that, in building the $k$-partite graph, nodes in $V_0$ have much lower connections than nodes in $V_l, l \in [1, k - 1]$ and, therefore, $\frac{A_l(i, j)}{\text{outdegree}(n_i)}$ becomes the dominant factor, while the effect of $\frac{A_l(i, j)}{\text{outdegree}(n_j)}$ is alleviated. This results in a very slight downgrading of the impact of hub nodes.
3.1.6 The algorithm for Anomaly Detection

Based on the relevance scores for any given node \( n_i \in V_l, 0 \leq l \leq k - 1 \), which are stored in the Similarity Matrix \( S_{N \times N} \), \( N = \sum_{l=0}^{k-1} N_l \), we can compute the normality score for any node. For a given node \( n_i \), the relevance score to any other \( n_j \) stored in \( S(i,j) \) shows the probability of visiting node \( n_j \) while starting a random walk from node \( n_i \). The relevance score should be high for nodes that belong to the same cluster with node \( n_i \) and low or even zero for nodes that share few or no common connections with node \( n_i \). It should be noted that the matrix \( S \) is not symmetric, meaning that \( S(i,j) \neq S(j,i) \).

Given the Similarity Matrix \( S_{N \times N} \), we can derive matrix \( C_{N \times N} \), which will be used for the calculation of the normality score of each node \( n_i \). Each element \( C(i,j) \) of matrix \( C \) is calculated as the Pearson Coefficient of row \( X_i \) of matrix \( S \) with row \( X_j \) of matrix \( S \).

\[
C(i,j) = \rho_{X_i^1X_j^1} = \frac{\text{cov}(X_i^1X_j^1)}{\sigma_{X_i^1}\sigma_{X_j^1}} = \frac{\sum_{k=1}^{N} (X_i^k - \overline{X_i})(X_j^k - \overline{X_j})}{\sqrt{\sum_{k=1}^{N} (X_i^k - \overline{X_i})^2 \sum_{k=1}^{N} (X_j^k - \overline{X_j})^2}} \quad (3.4)
\]

The absolute value of Pearson correlation coefficients are less than or equal to 1, \(-1 \leq \rho_{X_i^1X_j^1} \leq +1\). Moreover, the Pearson correlation coefficient is symmetric: \( \rho_{X_i^1X_j^1} = \rho_{X_j^1X_i^1} \). Correlations equal to 1 correspond to data points that are absolutely correlated. Therefore, whenever nodes \( n_i \) and \( n_j \) belong to the same cluster, meaning that they share many common connections, the value of \( C(i,j) \) should be high. On the contrary, nodes that do not have many common structural properties should have a low value of \( C(i,j) \), since the probability of visiting the same set of nodes should be very low.

Based on this observation, we want to compute the normality score of every node in \( V_l, l \in [0, k - 1] \). A node with a low normality score is an anomaly. Given a node \( n_i \) in \( V_l \), we first find the set \( L_i \) of nodes in \( V_m, m \neq l \) to which \( n_i \) links: \( L_i = \{ n_j | (i, j) \in E \} \). Let \( q_i \) be the size of \( L_i \). If \( n_i \) is “normal”, then the Pearson correlation coefficient between any pair of elements in \( L_i \) should be high. The normality score \( NS(n_i) \) of node \( n_i \) is given by the mean of the Pearson correlation coefficient of all nodes in \( L_i \).

\[
NS(n_i) = 2 \sum_{a=1}^{q_i-1} \sum_{b=a+1}^{q_i} C(a,b) \quad \forall n_a \text{ and } n_b \in L_i \quad (3.5)
\]
From Equation (3.5), it is evident that the lower the normality score \( NS(n_i) \) is, the more abnormal node \( n_i \) is.

A computational trade-off of the described methodology is whether or not to pre-compute the relevance score vectors of all the row nodes and the Pearson coefficient for every pair of nodes. It usually depends on the number of nodes involved. For example, if the dataset has a large number of rows and the input queries are skewed, pre-computation is not recommended, because it incurs huge cost and most of that is wasted due to the skewed distribution of the queries.

### 3.1.7 Results

As mentioned in the introductory section of this chapter, the anomaly detection algorithms developed within VIS-SENSE for network and threat monitoring aim at detecting contextual anomalies, which are also referred to as conditional anomalies. The notion of a context is induced by the structure in the data set, which depends on the edges connecting different nodes. Towards this end, we apply the developed anomaly detection method to the HARMUR dataset, by considering both the case of a single and the case of two features.

We first study the graph that is formed by considering rogue websites and their geolocation, shown in Figure 3.4. Rogue websites are represented by white circles, while their geolocation is represented by violet circles. The graph is positioned using a force-directed algorithm, which allows us to have a clear overview of the clusters that are formed. Our anomaly detection algorithm tries to detect those nodes that connect regions of graph that have few structural similarities. In essence, we try to find nodes that connect different clusters of nodes. The abnormal nodes can be either rogue websites, which are connected to countries that are associated with very different websites, or countries which connect rogue websites that do not belong to the same cluster. It should be noted that, there is no need to (pre)calculate the clusters of the graph, since the cluster membership of each node is induced by its position.

Figure 3.4 shows in red the abnormal nodes spotted by our anomaly detection algorithm. The visual representation of the results verifies the accuracy of our algorithm. Indeed, the nodes that are spotted as anomalous connect regions in the graph that have very few common structural properties. In the most common case, an “abnormal” or very few “abnormal” rogue websites are connected both to a small country associated with few rogue websites and to the USA which is associated with a very large number of websites. In a special case, there are few websites that are connected both to China and Germany, which are both associated with a high number of rogue websites. One can see that if the number of rogue websites connecting China and Germany was higher, these
Anomaly Detection for Network and Threat Monitoring

Figure 3.4: Results of the anomaly detection algorithm for feature “Location”. Anomalous nodes are colored in red.

would not be spotted as “abnormal”, since it would be considered as a normal structure in the graph, as happens with the rogue websites connecting the USA and Germany. An “abnormal” node might indicate the rising of a new attack phenomenon. For example, an “abnormal” website connecting the USA with another country may indicate that a rogue organization is transferring its websites from the USA to another country in order to launch new attacks in that specific country.

In Figure 3.5, we have added a second feature, namely the ASN number associated
3.1 The static case

Figure 3.5: Results of the anomaly detection algorithm for features “Location” and “ASN”. Anomalous nodes are colored in red.

with each rogue website. The ASN numbers are represented by yellow nodes. The graph is repositioned using the same force-directed algorithm, allowing the formulation of clusters based on the connections of rogue websites to different features. It is apparent that, by adding a second feature, the context into which we are searching for anomalies has changed. Therefore, some nodes that were considered “abnormal” in the first case are now viewed as “normal”. On the contrary, nodes that were considered as “normal” in the first case are now considered as “abnormal”, since they connect regions of the
3.2 The dynamic case

The second problem to be tackled by anomaly detection techniques for network and threat monitoring is the detection of anomalies either between two subsequent graphs or within a time-series of graphs, which is referred to as the dynamic case. Towards this end, consider the application of both spectral and graph-matching techniques. Given the diversity of the network and threat monitoring problems to be studied by the VIS-SENSE project, the applicability and the effectiveness of these techniques will be dependent to a large extent on the specific use case to be examined.

3.2.1 Problem definition

The basic idea behind the detection of network anomalies over time is to represent each network state by a graph and study the temporal changes of this graph. Let the network graph $G$ be sampled over time using a constant period of time $dt$. Every time instance $t_i$, where $dt = t_{i+1} - t_i$, results into a new graph state, $G_i$. It has been shown that the study of the changes in the properties of the $G_i$ sequence can be used for the detection of abnormal behavior [14].

Each network graph $G_i$ is represented by a set of nodes $V_i = \{v_0, v_1, \ldots, v_n\}$. A node $v$ is the representative unit of an abstract network component or attribute, such as an IP-address, the e-mail spam bot’s id, etc. It is expected that the network graph nodes exchange information with each other and when this happens the two nodes are abstractly connected with an edge. Thus the graph $G_i$ contains also a set of edges $E_i = \{e_0, e_1, \ldots, e_k\}$. There are cases in which an edge $e$ could also be used to assign a specific attribute to a node. For example suppose that a network contains nodes of IP-addresses and nodes that declare country names. An edge that connects an “ip-address” node to a “country” node can be used to declare the origin of that specific IP-address.

The properties of the graph sequence $G_1, G_2, \ldots, G_i, \ldots, G_N$ can be studied by computing the difference between its graph elements. It is easily understandable that a stable, “normal” behavior will result into small differences between the graphs in the time sequence. Abnormal and irregular events can be hypothesized if a graph’s difference exceeds a given threshold. The graph difference distance is based on graph matching techniques.

Finally, in order to visualize the results in a user-friendly manner a very fast method of Multi-Dimensional Scaling (MDS) that plots the sequence’s graphs onto a 2D plane is used [14].
3.2 Methodology

The anomaly detection algorithm of the dynamic case can be summarized into three steps:

i) Create the graph sequence \( G_1, \ldots, G_N \)

ii) Compute distance matrix \( D \) from the sequence elements

iii) Transform the results into a user-friendly representation using Multi-Dimensional Scaling.

The graph sequence is simply created by grouping the available data by their time of retrieval. Various time periods can be chosen for data grouping (per hour, per day, per month, etc.) depending on the network administration needs. After that step the graph nodes are connected to each other and the result is saved into a sparse matrix data structure for memory economy purposes.

The next step is to compute the distance matrix \( D = [d_{ij}] \) of the graph sequence, where \( d_{ij} \) denotes the distance between graphs \( G_i \) and \( G_j \). The distance \( d_{ij} \) contains information regarding the changes that have taken place in both the nodes and the edges of the graphs. Various distance metrics for graphs can be defined.

The simplest distance formula is defined in (3.6).

\[
    d_{ij} = |V_i| + |V_j| - 2|V_i \cap V_j| + |E_i| + |E_j| - 2|E_i \cap E_j| \quad (3.6)
\]

In the above equation \( |V| \) denotes the number of nodes and \( |E| \) denotes the number of edges of a graph. The \( |V_i \cap V_j| \) denotes the number of the common nodes in the two graphs; the same applies for the edges as well. Thus the distance function contains the number of graph operations that have happened through the transition \( G_i \rightarrow G_j \), i.e. the aggregation of all the graph’s node and edge deletions and insertions. It must be mentioned here that the matrix \( D \) is symmetrical, i.e. \( d_{ij} = d_{ji} \) and its diagonal elements are equal to zero, i.e. \( d_{ii} = 0 \). This results in the computation of only the \( d_{ij} \) elements where \( j > i \). Similar graphs which have a lot of nodes and edges in common will result in differences close to zero, while graph transitions with a lot insertions and deletions will result in a suspicious behavior. The dimensionality \( N \) of the \( D \) matrix \( (D_{K \times K}) \) is equal to the number of the graph elements, i.e. equal to the time instances.

One disadvantage of the formula in (3.6) is that it doesn’t model properly the edge weights of the compared graphs. Thus, it will give the same result in graphs which have the same edge connections, but different weights on them. In such cases, it is more appropriate to use a distance formula that embeds the difference of the edge weights. The
Anomaly Detection for Network and Threat Monitoring

The simplest way to do that is by defining a 2d matrix \( H_{k \times k} = [h_{rc}] \), where \( k = \bigcup_{i=1}^{N} V_i \), i.e. a square matrix having each of its dimensions equal to size of the united set of all the nodes that have been met in the graph sequence (of \( N \) graphs). For each graph \( G_i \), an \( H_i \) matrix is constructed and filled with the corresponding weight values. The resulted matrix \( H_i \) is in most of the cases a sparse matrix and for non directional graphs it is also symmetric. Having constructed the \( H_i \) matrices a new distance metric can be defined:

\[
\bar{d}_{ij} = \frac{1}{2} \sum_{r=1}^{k} \sum_{c=1}^{k} |H_i(r,c) - H_j(r,c)| = \sum_{r=1}^{k} \sum_{c=r+1}^{k} |H_i(r,c) - H_j(r,c)|
\]

(3.7)

Compared to (3.6), \( \bar{d}_{ij} \) models the information of the graphs edges more precisely, making it more appropriate for graphs with weighted edges. Moreover the euclidean distance can be used to augment the difference metric quality between the graphs, i.e.:

\[
\hat{d}_{ij} = \sqrt{\sum_{r=1}^{k} \sum_{c=r+1}^{k} (H_i(r,c) - H_j(r,c))^2}
\]

(3.8)

At this point, it must be mentioned that instead of the distance matrix of the sequence, a simpler distance vector could be used to show the progress of the network graph sequence. However a vector element which contains the distance of a graph against a previous one, can not be used to find how irregular the current network state is in comparison with the whole sequence and hence, a manually defined threshold has to be used. This could result into a lot of false alarms events.

The final step includes the projection of the distance matrix \( D \) onto a 2D or 3D space, in order to permit proper visualization for the user and allow better estimation of the situation. The key here is to represent each graph instance as point (either 2D or 3D), so that its distance to the other graph points is proportional to the distances declared in \( D \). The method for performing this is based on Multi-Dimensional Scaling and takes as an input the distance matrix \( D_{N \times N} \) and outputs the matrix \( X_{N \times M} \), where \( M = 2 \) or \( M = 3 \), depending on the 2D or 3D case. The matrix \( X \) contains the coordinates of each graph \( G_i \) for \( i \in [1 \ldots N] \):

\[
X = \begin{bmatrix}
    x_{11} & \cdots & x_{1M} \\
x_{21} & \cdots & x_{2M} \\
    \vdots & \ddots & \vdots \\
x_{N1} & \cdots & x_{NM}
\end{bmatrix} = \begin{bmatrix}
    x_1 \\
x_2 \\
    \vdots \\
x_N
\end{bmatrix}
\]

(3.9)
3.2 The dynamic case

In (3.9) \( x_i \) is a vector that contains the coordinates of the graph point \( i \). The relation between the distance \( d_{ij} \) and the \( x_i, x_j \) vectors is given in (3.10):

\[
d_{ij}^2 = (x_i - x_j)^T(x_i - x_j) = x_i^T x_i - 2x_i^T x_j + x_j^T x_j
\]  

(3.10)

In the above equation \( x^T \) denotes the transpose vector of \( x \). Because of the equation (3.10), a new matrix \( \hat{D} \), which contains the squared distances between the graphs, has to be computed, i.e.:

\[
\hat{D} = \begin{bmatrix}
d_{11}^2 & d_{12}^2 & \cdots & d_{1N}^2 \\
d_{21}^2 & d_{22}^2 & \cdots & d_{2N}^2 \\
\vdots & \vdots & \ddots & \vdots \\
d_{N1}^2 & d_{N2}^2 & \cdots & d_{NN}^2
\end{bmatrix} = \begin{bmatrix}
0 & d_{12}^2 & \cdots & d_{1N}^2 \\
d_{12}^2 & 0 & \cdots & d_{2N}^2 \\
\vdots & \vdots & \ddots & \vdots \\
d_{1N}^2 & d_{2N}^2 & \cdots & 0
\end{bmatrix}
\]  

(3.11)

Now, the matrices \( \hat{D} \) and \( X \) can be related via the following equation:

\[
\hat{D} = cb^T - 2XX^T + bc^T, \text{ where } b = \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}, \text{ and } c = \begin{bmatrix} x_1^T x_1 \\ x_2^T x_2 \\ \vdots \\ x_N^T x_N \end{bmatrix}
\]  

(3.12)

By multiplying (3.12) with \( J = I - \frac{1}{N}bb^T \) from the left and from the right and applying some simplification, we obtain:

\[
XX^T = -\frac{1}{N}J\hat{D}J
\]  

(3.13)

Now the terms in the right part of (3.13) can be factorized by eigen value decomposition, i.e.:

\[
XX^T = -\frac{1}{N}J\hat{D}J = QLQ^T
\]  

(3.14)

The matrix \( L \) in (3.14) is a diagonal matrix containing the eigenvalues \( l_i \) sorted such as that \( l_1 \geq l_2 \geq \ldots \geq l_N \geq 0 \). By selecting the first 2 or 3 largest eigenvalues (for the 2D or 3D projection respectively) and setting the rest to zeros, the requested matrix \( X \) can be obtained via:

\[
XX^T = \left( QL^1 \right) \left( QL^1 \right)^T \Rightarrow
\]  

(3.15)
Figure 3.6: Monthly graph sequence for features “Bot”, “Country” and “Keyword”. For the 2D projection the simplest distance $d_{ij}$ of (3.6) has been used.

\[ X = Q L^{\frac{1}{2}} \Rightarrow \]  

\[ X = Q \begin{bmatrix} \sqrt{l_1} & 0 & \cdots & 0 \\ 0 & \sqrt{l_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sqrt{l_N} \end{bmatrix} \Rightarrow \]  

(3.16)  

(3.17)
3.2 The dynamic case

Figure 3.7: Monthly graph sequence for features “Bot”, “Country” and “Keyword”. The distance $d_{ij}$ of (3.7) has been used.

$$X_{2D} = Q \begin{bmatrix} \sqrt{l_1} & 0 \\ 0 & \sqrt{l_2} \\ 0 & 0 \\ \vdots & \vdots \\ 0 & 0 \end{bmatrix} \text{ or } X_{3D} = Q \begin{bmatrix} \sqrt{l_1} & 0 & 0 \\ 0 & \sqrt{l_2} & 0 \\ 0 & 0 & \sqrt{l_3} \\ \vdots & \vdots & \vdots \\ 0 & 0 & 0 \end{bmatrix}$$

(3.18)

In (3.18), the matrices $X_{2D}$ and $X_{3D}$ contain the 2D and 3D graph sequence points respectively. The projected distance of one graph point to the others is indicative of its graph difference with the rest. Thus, points that are far from the point cloud’s center may indicate an irregularity with respect to the network behavior. The advantage of this...
method is that is free of any definitions of thresholds and results into a very intuitive way of explaining the network traffic behavior over time.

### 3.2.3 Results

In this subsection the results regarding the dynamic case of the proposed anomaly detection algorithm are mentioned. The dataset on which the algorithm has been applied is based on input from the *SpamCloud* data. More precisely, the experiments have been based on the full dataset of month March (2011) of *SpamCloud*. It is known *a priori* that in the time period between the 15th and 17th day an anomaly has been presented in the

![Figure 3.8: Monthly graph sequence for features “Bot”, “Country” and “Keyword”. The distance $d_{ij}$ of (3.8) has been used.](image-url)
network. More precisely a spamming bot had stopped sending e-mails. The experiments have been conducted taking into account the following features: i) the “Bot” feature data, containing bots’ IDs, ii) the “Country” feature data, containing the origin of the e-mail and iii) the “Keyword” feature data, containing the e-mail subject’s keywords.

Two experiments have been performed. One considering data that are organised so that each graph will contain information regarding a specific day of the month and one taking into account the 24 hours of a daily network traffic. For the first experiment, data clustering has been based on the feature “Day” and for the second on the feature “Hour”.

The results of “month” experiment are depicted in Figures 3.6, 3.7 and 3.8. For better...
representation purposes, the projection on the 2D space has been preferred, i.e. $X_{2D}$ of (3.18). Each figure depicts a sequence of graph points along with their transitions. The points are placed in the 2D space, so that their distances resemble as much as possible the distances of the sequence distance matrix $D$.

Figure 3.6 depicts the graph sequence using the simplest distance metric, $d_{ij}$ defined in (3.6). This figure cannot provide any valid information since it discards any information regarding the graphs’ edge weights and can be considered as misleading. Moreover the huge change that occurred in the networks on days 15 to 17 is not depicted at all.

Figure 3.7 is based on the $\hat{d}_{ij}$ distance of (3.7). This representation can model in a more proper way the edge weights information of the graphs and thus, it results into a
3.2 The dynamic case

Figure 3.11: Daily (24h) graph sequence for features “Bot”, “Country” and “Keyword”. The distance $\tilde{d}_{ij}$ of (3.8) has been used.

totally different point sequence. Now it becomes obvious that events that took place on the days 15-17 had permanently changed the state of the network, by transitioning from the initial right point-cloud to the left one.

Finally, Figure 3.8 has been constructed using the $\tilde{d}_{ij}$ distance of (3.8). This representation gives the user an even more precise visualisation of what has happened to the network after the change on days 15-17. More specifically, the left point-cloud seems to have high concentration, meaning that the behaviour of the bots has been stabilised after the anomaly occurrence.

Results regarding the network’s 24h traffic are depicted in Figures 3.9, 3.10 and 3.11. All three figures manage to depict successfully the periodic cyclic nature of the spamming
Figure 3.12: Daily (24h) graph sequence for features “Bot”, “Country” and “Keyword” using 3D projection. The distance $d_{ij}$ of (3.7) has been used.

bots. An example of a projection in 3D space is depicted in Figure 3.12.
4 BGP Anomaly Detection

Given the exponential growth of the Internet, which is now comprised of an astonishingly large number of interconnected regional and national backbones, the robustness and quality of the provided services is highly dependent on the stability of the Internet’s current interdomain routing protocol, namely BGP (Border Gateway Protocol) [33]. BGP is primarily responsible for routing traffic across these different regions of administrative control, commonly called Autonomous Systems (ASes), which must maintain a complete map, or default-free routing table, of all globally visible network-layer addresses reachable throughout the Internet. Moreover, beyond the generally applicable BGP prioritization rules, the ASes usually also have distinct routing policies that determine their connection to one or more remote ASes. In this respect, at the ASes’ boundaries, peer border routers exchange reachability information to destination IP address blocks, or prefixes, for both transit networks, and networks originating in the routing domain.

Although the efficiency of the Internet operation is supposed to be enhanced under stable routing conditions, there still exist several reasons that can cause either short-term or more permanent alterations of the BGP status, such as:

- Hardware failure, e.g. router malfunction
- Link failure, e.g. fiber cable cut
- Equipment misconfiguration
- Power supply outage
- Congestion phenomena, e.g. traffic overload
- New policies between peering ASes, e.g. inter-country or inter-AS relationships
- Alternative Internet Service Providers (ISPs) at different tiers of the Internet hierarchy

Additionally to the above causes of BGP disturbances, a new one has emerged over the last years: cyber attacks against its functionality and its integrity. Motivated by the potential of a high profit underground economy, cyber attackers have spotted BGP as
a lucrative target for their business. Indeed, attacks against BGP have recently been identified as the stepping stone towards launching spam campaigns [32].

Thus, it becomes more than apparent that it is of critical importance to develop the necessary methodology that would allow not only for the prompt detection of any abnormal BGP behaviors, but especially for the effective root cause attribution of such events as well as the evaluation of their impact upon the Internet operation at both macroscopic and lower levels. Nevertheless, in contrast to the mere detection of a BGP instability, which can be straightforwardly achieved through the rather simplistic comparison between any new prefix announcements against the prefix’s existing records, the extraction of the phenomena’s deeper characteristics remains a prodigiously complicated process, since it requires the correlation of various and voluminous spatiotemporal events as well as the incorporation of multi-dimensional semantic information from third-party resources.

4.1 Background work

Due to the key role of BGP in the proper operation of the Internet, the detection of BGP instabilities has attracted a lot of research effort.

In [43] the authors propose a clustering method based on principal component analysis (PCA) to obtain a set of clusters from a BGP update stream, where each of these is a set of entities (either prefixes or ASes) that are affected by the same underlying event. Their approach aims at root cause analysis, since it groups different prefixes or ASes such that all the members in a group are (most likely) affected by the same cause. PCA is also used in [25] as a BGP anomaly detection method.

In [17] an unsupervised method is proposed based on statistical techniques to detect BGP instabilities. For their analysis, the authors make use of features like AS Path Length, AS Path Edit Distance and Volume of update messages, while a similar approach is also presented in [45].

On the contrary, the techniques presented in [27] and [16] are semi-supervised and use data mining algorithms to learn from labeled data (e.g. abnormal event traffic and normal BGP traffic before the event) and apply the learned model to a previously unseen BGP event traffic by using a sliding window approach. If the number of bins matching the model exceeds a certain threshold, an alarm is raised. A learning-based scheme, which makes use of wavelets, is also presented in [44].

The Prefix Hijack Alert System (PHAS) [26] provides alert messages if the update stream is detected to contain any of the following scenarios: i) an origin AS in an update message that is new relative to the set of previously observed set of origin ASes
4.2 BGP anomaly detection on the basis of control-plane information analysis

The term “control-plane” refers to the utilization of the information that lies within the core BGP activity and depicts the set of exchanged routing directives that determine the operational behavior and performance of the Internet infrastructure. The BGP raw data are primarily made available to the analysts through the repositories that are maintained by the Route Views Project (RouteViews) [40] and the Réseaux IP Européens Network Coordination Centre (RIPE NCC) [34], which both operate upon the notion of Vantage Points (VP). More concisely, each VP is an entity capable of peering with multiple fully functional routers that are situated at disparate locations around the globe and which collect, record and eventually communicate back to their parent VPs the BGP activity they perceive throughout their operation. These monitoring routers are called Next-Hops (NH) of the specific VP and each NH peers with only a single VP, while the total NHs that are assigned to the whole range of established VPs comprise the overall set of monitoring ASes (M). Each VP makes available two different types of BGP data files:

- BGP update message files, which are denoted as $F^U$. Each $F^U$ contains all the raw BGP update messages, mainly announcements and withdrawals, that have been received by the peering NHs during the last $T_U$ seconds (for both Route-Views and RIPE, $T_U = 5$ min.). In more detail, a $F^U$ file that is generated at time instant $t$, contains all the BGP update messages that have been received by all

for the same prefix, ii) a new more specific subprefix of an existing announced route is observed, iii) the last-hop AS (i.e., the AS that is one hop away from the origin AS) in an update message is new relative to the set of previously observed last-hop ASes for the same prefix. However, the proposed system fails to detect hijacks that occur without a change in the origin AS and may not always distinguish valid changes from actual hijacks. Alternatively, Argus system [42] focuses solely on the detection of blackholing events (forgery of BGP path with the aim to intercept the IP traffic and blackhole it) and to this end it combines control-plane and data-plane information, so as to trace prefixes that are announced at BGP level (control-plane) but they are practically unreachable (they do not respond to ping).

The analysis presented in [24] is augmented with data plane information in the form of edge network fingerprinting to disambiguate suspected IP hijacking incidences based on routing anomaly detection. Lastly, [39] and [41] rely on the advent of visual analytics technologies and human intervention for the detection of anomalies in BGP update messages.
the VP’s NHs within the time window \((t - T_U, t]\); the \(F_U\) files are made available at regular intervals of \(T_U\) seconds. Special emphasis must be laid on the fact that these BGP update messages included in \(F_U\) files do not necessarily present corresponding alterations of the routing status but solely the traces of the exchanged BGP directives. The reception of a BGP update message for a prefix \(p\) does not straightforwardly obsolete the existing records for \(p\), but on the contrary, the newer messages are rather likely to be ignored or discarded according to either the general BGP or the router-specific prioritization rules. Hence, the simplistic analysis of a BGP announcement or withdrawal in an isolated manner, without the parallel processing of the actual routing records in reference to the current routing records and conditions, cannot lead to solid conclusions regarding the actual operation of the Internet infrastructure.

- BGP router status files, which are commonly known as “dump” files in RouteViews and “bview” files in RIPE and they will be denoted as \(F^B\). In contrast to the \(F^U\) files that merely report on the ongoing BGP activity taking place at different time windows, \(F^B\) files practically provide a snapshot of the existing routing table status at the time instant of the \(F^B\) file’s generation. Thus, \(F^B\) consists of the valid routing records that have been eventually formulated as the aggregated result of the overall BGP activity and routers’ operations until that time instant. Therefore, it can be safely taken for granted that \(F^B\) files present a steady state report of the ASes’ interconnectivity and relationships from each NH’s perspective. In general, \(F^B\) are generated with much lower frequency than \(F^U\) files \((T_B \gg T_U)\); for RouteViews \(T_B = 2hrs\) while for RIPE \(T_B = 8hrs\).

### 4.2.1 Detection and attribution of large scale BGP disturbances on the basis of spatiotemporal correlations

Apart from the BGP anomalies that are related to criminal activity and which can also take place fully sporadically, affecting only specific prefixes and ASes in an isolated manner, the vast majority of the causes of BGP disturbances, as these have been described above, are expected to induce profound impact upon the Internet operation in terms of both the geographical spread of the phenomena and their duration. Therefore, in order to enhance the efficiency of the BGP anomaly detection and attribution mechanisms, the adopted techniques should be capable of extracting the disparate spatiotemporal characteristics of the massive bulk of routing events and adequately cluster them so as to pinpoint their macroscopic features.
4.2 BGP anomaly detection on the basis of control-plane information analysis

4.2.1.1 Problem Formulation

According to the BGP, an AS that wishes to establish the ownership of a prefix, generates a respective BGP update message (prefix announcement) that includes the prefix of interest as well as the origin AS (owner of the prefix) and sends it to all its neighboring ASes, so that their routing tables are adequately updated with the new prefix allocation status (AS-to-prefix matching). Additionally, what is regarded as a primary BGP functionality, every AS receiving the BGP announcement, prepends itself to the original AS path and subsequently forwards the message to all its peering ASes, so that the routing information is spread throughout the Internet infrastructure, while, at the same time, the exact propagation AS-Path towards the announced prefix is recorded. As a result, each BGP announcement received by a monitoring AS \( M \) for a given prefix \( p \) includes two main pieces of information:

- The AS, \( O^p \), that has announced itself as the owner of prefix \( p \). \( O^p \) is also commonly referred to as the origin AS of prefix \( p \), since it is the AS from which the BGP announcement of prefix \( p \) has originated.
- The sequence \( \text{API}^{M,p} \) of \( K \) intermediate ASes that have to be traversed by any Internet traffic originating from (or forwarded by) \( M \) and targeted to an IP address that belongs to the prefix \( p \):

\[
\text{API}^{M,p} = \{A^{M,p}_1, \ldots, A^{M,p}_K\}
\] (4.1)

Hence, to sum up, any prefix \( p \) monitored by \( M \) is uniquely identified by its AS-Path:

\[
\text{AP}^{M,p} = \{M, A^{M,p}_1, \ldots, A^{M,p}_K, O^p\}, p \in \mathbb{P}
\] (4.2)

where \( \mathbb{P} \) is the set of all the active prefixes. According to (4.2), although the owner of each prefix is unambiguously perceived throughout the whole Internet infrastructure, the connecting AS-Path towards a specific prefix is a function of the point of monitoring (source) AS, i.e. different monitoring (source) perspectives result in correspondingly different AS-Paths. Hereafter, the terms source AS and monitor AS will be used interchangeably.

In this respect, any changes taking place concerning the composition of \( \text{API}^{M,p} \), for any monitoring AS \( M \) and any \( p \in \mathbb{P} \), can be regarded as evidence of potential BGP anomaly. Notwithstanding, due to the inherently dynamic nature of IP routing, such phenomena are rather frequent within the Internet infrastructure. Hence, beyond simplistically capturing any AS-Path alterations, it is utterly necessary to provide the effective means for thoroughly attributing such events to a common root cause, so as to be
capable of discriminating among the bulk of the BGP activity and trace any phenomena that present particular interest due to either their root causes or their eventual impact.

4.2.1.2 Proposed methodology

To this end, it is hereafter proposed a novel methodology for the detection and attribution of large scale BGP anomalies, which involves the extraction of new features and proximity measures that make particular use of the spatial characteristics of such large scale phenomena. In detail, the merits of such an approach that captures the ASes’ behavior and activity on a per country basis are threefold:

- It transparently provides common analysis of spatially and semantically correlated AS-Path alterations, i.e. ASes belonging to the same country are by default characterized by high geographical proximity, while they are also expected to share common ISPs at least of the higher Internet tiers.

- It guarantees the availability of sufficiently extensive datasets that facilitate robust statistical analysis, e.g. filtering of sporadic phenomena, capturing larger scale tendencies.

- It smooths out the impact of the monitoring AS choice upon the BGP activity analysis and eases the fusion of anomaly events detected by multiple monitoring routers.

More concisely, let \( C = \{C_1, \ldots, C_D\} \) be the set of the \( D \) different country entities (hosts) that are established within the Internet community in accordance with the international legislation and treaties; for ease of reference, hereafter \( C(X) \) shall denote the country of origin of AS \( X \). Then, for each destination country \( C_d \), we calculate the aggregate set of ASes \( (G^d) \) that provide the interconnection of country \( C_d \) with the rest of the world, i.e. all the ISPs that act as the gateways of country \( C_d \). In this context, exploiting the AS-Path information contained in the BGP update messages, as these have been described in (4.2), \( G^d \) can be easily defined by i) isolating the BGP announcements of prefixes whose owner is located in \( C_d \), where \( C_d = C(O^p) \) and ii) subsequently analyzing the AS-Path sequence (4.1) so as to pinpoint the AS that is the last hop before \( C_d \), i.e. the highest indexed AS within the prefix’s AS-Path with different country of origin from the owner AS.

\[
G^d = \bigcup \{A^{M,p}_k\}, \forall p \in P
\]

\[
A^{M,p}_k \in [API^{M,p}] \text{ such that } C(O^p) = C_d
\]

\[
k = \max\{1, \ldots, K\} \text{ such that } C(A^{M,p}_k) \neq C(O^p)
\]
Interpreting (4.3), $G^d = \{G^d_1, \ldots, G^d_Q\}$ is the union of all the $Q$ different ASes that appear as the immediate neighbors of any AS hosted in country $C_d$ (i.e. union of all the ASes that act as ISPs of country $C_d$) in at least one BGP announcement. At this point, it must be mentioned that, based on the definition of $\text{API}^{M,p}$ in (4.1), $G^d$ and consequently the whole analysis presented hereafter is a function of the monitoring AS $M$ from which the routing paths are viewed. Hence, all the corresponding variables should be adequately annotated with the identity of the monitoring AS, which however is omitted for ease of reading.

Furthermore, in order to quantify the distribution of prefixes among the members of $G^d$, i.e. the contribution of each external AS to a country’s Internet Service Provision, the vector $V^d$ is introduced. $V^d$ presents the number of prefixes forwarded by each one of the ASes comprising the set of $C_d$’s direct ISPs ($G^d$):

$$V^d = \begin{bmatrix}
NAP(G^d_1) \\
\vdots \\
NAP(G^d_Q)
\end{bmatrix} \quad (4.4)$$

where $NAP(G^d_q)$, $\forall q \in \{1, \ldots, Q_d\}$, denotes the number of prefixes that i) are hosted in country $C_d$ and ii) are being announced with the AS $G^d_q$ as the last hop before any AS hosted in $C_d$.

Since the routing records are continuously updated upon the reception of new BGP announcements and withdrawals, which affect both the overall prefix occupancy by country $C_d$ and the distribution of the prefixes’ servicing among the various last hops of $C_d$, it should be underlined that $G^d$ and $V^d$ are functions of time. Hence, in order to follow the evolution of the routing status along the time axis, $V^d$ is computed at various sequential time instants $t_1, \ldots, t_I$ and the corresponding matrix $R^d$ is built:

$$R^d = [V^d_1, \ldots, V^d_I] = \begin{bmatrix}
NAP(G^d_1, t_1) & \ldots & NAP(G^d_1, t_I) \\
\vdots & \ddots & \vdots \\
NAP(G^d_Q, t_1) & \ldots & NAP(G^d_Q, t_I)
\end{bmatrix} \quad (4.5)$$

The dimensions of $R^d$ are equal to $Q \times I$, where $Q$ is the number of different last hop ASes for $C_d$ and $I$ is the number of the studied time instances, and each column corresponds to a $V^d$, i.e. a snapshot of the routing records towards country $C_d$ at time instance $t$. Aiming at acquiring a quantitative insight concerning the consistency of $V^d$ throughout time, the Pearson Coefficient ($\rho$) among all the columns of $R^d$ is calculated and, as a result, the Pearson Coefficient matrix of country $C_d$ against time is formulated with
dimensions $I \times I$. The estimation of $\rho^d$ allows to study the evolution of the routing status and to eventually capture any time-correlated BGP disturbances:

$$\rho^d = \begin{bmatrix}
\rho(V^d(t_1), V^d(t_1)) & \cdots & \rho(V^d(t_1), V^d(t_I)) \\
\vdots & \ddots & \vdots \\
\rho(V^d(t_I), V^d(t_1)) & \cdots & \rho(V^d(t_I), V^d(t_I))
\end{bmatrix}$$

(4.6)

The driving notion behind this analysis lies within the fact that the comparison between two different time instances of $V^d$ is expected to evidently reveal any time windows with substantial alterations regarding the BGP behavior and the corresponding routing operations that are related to country $C_d$. In particular, the Pearson Coefficient ($-1 \leq \rho \leq 1$) is a metric of the linear dependence between two vectors and thus values of $\rho$ much lower than 1 should be safely regarded as strong evidence of substantial deviation between the BGP status at the respective time instants.

In this context, in order to present more evidently the Pearson Coefficient rationale and the contribution of the $\rho^d$ formulation to the detection and analysis of the BGP anomalies, the proposed methodology is studied for the case of two pivotal scenarios:

- **Variation of the routing status at time instant $t_v$** ($t_v \in \{t_1, \ldots, t_I\}$) without further system restoration. In this case, $\forall t_i, t_a \in \{t_1, \ldots, t_I\}$

$$\rho^d(t_i, t_a) = \begin{cases}
1, & t_i = t_a \\
x_{i,a}, & i, a \in [1, v) \text{ OR } i, a \in [v, I] \\
y_{i,a}, & \text{otherwise}
\end{cases}$$

(4.7)

where $y_{i,a}$ should refer to much lower values than $x_{i,a}$ in reference to the maximum Pearson Coefficient value of 1 (absolute linear dependence), since two routing states that both correspond to time windows either before or after the BGP disturbance are expected to present high correlation values ($\rho$ close to 1). On the contrary, the correlation between two routing states that fall with each other at different sides of the BGP incident is expected to be significantly reduced ($\rho$ much lower than 1).

Moreover, $\rho^d$ should be formatted as follows:

$$\rho^d = \begin{bmatrix}
1 & \cdots & x_{1,v-1} & y_{1,v} & \cdots & y_{1,I} \\
& \ddots & \vdots & \vdots & \ddots & \vdots \\
x_{v-1,1} & \cdots & 1 & y_{v-1,v} & \cdots & y_{v-1,I} \\
y_{v,1} & \cdots & y_{v,v-1} & 1 & \cdots & x_{v,I} \\
& \ddots & \vdots & \vdots & \ddots & \vdots \\
y_{I,1} & \cdots & y_{I,v-1} & x_{I,v} & \cdots & 1
\end{bmatrix}$$

(4.8)
4.2 BGP anomaly detection on the basis of control-plane information analysis

- Variation of the routing status at time instance \( t_v \) followed by system restoration at time instance \( t_r > t_v \) \((t_r, t_r \in \{t_1, \ldots, t_L\})\). In this case,

\[
\rho^d(t_i, t_a) = \begin{cases} 
1, & t_i = t_a \\
x_{i,a}, & i, a \in [1, v) \text{ OR } i, a \in [v, I] \\
y_{i,a}, & \text{otherwise}
\end{cases}
\]  

(4.9)

and therefore

\[
\rho^d = \begin{bmatrix}
1 & \ldots & x_{1,v-1} & y_{1,v} & \ldots & y_{1,r-1} & x_{1,r} & \ldots & x_{1,I} \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \ddots & \ddots & \vdots \\
x_{v-1,1} & \ldots & 1 & y_{v-1,v} & \ldots & y_{v-1,r-1} & x_{v-1,r} & \ldots & x_{v-1,I} \\
y_{v,1} & \ldots & y_{v,v-1} & 1 & \ldots & x_{v,r-1} & y_{v,r} & \ldots & y_{v,I} \\
\vdots & \ddots & \vdots & \ddots & \ddots & \ddots & \vdots & \ddots & \vdots \\
y_{r-1,1} & \ldots & y_{r-1,v-1} & x_{r-1,v} & \ldots & 1 & y_{r-1,r} & \ldots & y_{r-1,I} \\
x_{r,1} & \ldots & x_{r,v-1} & y_{r,v} & \ldots & y_{r,r-1} & 1 & \ldots & x_{r,I} \\
\vdots & \ddots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
x_{I,1} & \ldots & x_{I,v-1} & y_{I,v} & \ldots & y_{I,r-1} & x_{I,r} & \ldots & 1
\end{bmatrix}
\]  

(4.10)

Moreover, each row \( i \) of \( \rho^d \) practically presents the correlation between the routing status at time instance \( t_i \) and every other investigated time instance \( t_a \). Thus, in order to ease the imminent detection of the specific time instances of interest when the routing variations (BGP anomalies) occur (e.g. \( t_v \)), there can be defined \( I \) different functions of Pearson Coefficient against time:

\[
\rho^d(t_i, t_a) = \rho(V^d(t_i), V^d(t_a)), \forall i, a \in \{1, \ldots, I\}
\]  

(4.11)

By plotting all the \( I \) functions that are defined in (4.11) together at the same chart, the time instances of BGP inconsistencies will become prominently revealed as the functions’ minima/maxima and junctions points.

4.2.1.3 Real World Implementation

The proposed BGP anomaly detection and attribution mechanism is implemented at two different parallel time scales for achieving maximum granularity with minimum processing overhead. In particular, the exact steps are described below:

- A specific set of NHs (\( M \)) is chosen so as to guarantee the maximum possible geographical distribution of the monitoring ASes and satisfy the urging need for worldwide coverage of the BGP activity.
• For each selected NH $M \in \mathbf{M}$, the vectors $\mathbf{V}^d$ are calculated separately for every peering country $C_d$.

• The routing status matrix $\mathbf{R}^d$ is always computed for the last $I$ $F^B$ files, following a sliding window procedure. The value of $I$ is chosen equal to 7, i.e. a history of the BGP statistics from the last 7 $F_B$ files is always kept, so as to cover a time window of $(7 - 1) \times 6 = 48\text{hrs}$ around any possible BGP anomaly event.

• The Pearson Coefficient matrix $\rho^d$ is calculated for the time instances $\{t^B_1, \ldots, t^B_I\}$, where each time instance coincides with the generation of a $F_B$ file and thus $t^B_i - t^B_{i-1} = T_B$.

• By studying $\rho^d$, $\forall m \in \mathbf{M}$ and $\forall C_d \in \mathbf{C}$, any abnormal BGP behavior (broad alterations of a country’s routing status) that takes place between consecutive BGP router status files, is tracked down.

• The analysis summarized in (4.7) is implemented and $C_d$ be the country towards which the routing status from $M$ has been found to present significant deviations between the routing table reports acquired at time instances $v - 1$ and $v$, i.e. files $F^{B}_{v-1}$ and $F^{B}_{v}$ respectively, on the basis of.

• The instantaneous routing status vector $\mathbf{V}^d$ is estimated for every BGP update message file $F^U_j$ that falls within the time space $[t^B_{v-1}, t^B_v]$. $\mathbf{V}^d$ for file $F^U_j$ depicts the routing status (routing table records) after the processing of the BGP announcements and withdrawals that comprise the $F^U_j$ file. In this respect, let $J = T_B/T_U$ be the number of $F^U$ files between the $F^{B}_{v-1}$ and $F^{B}_{v}$ files and $t^U_j$ be the corresponding time instance of each $F^U_j$ file’s generation. Then, $\forall j \in \{1, \ldots, J\}$, the Pearson Coefficient values between $\mathbf{V}^d(t^U_j)$ and $\mathbf{V}^d(t^B_{v-1})$ as well as between $\mathbf{V}^d(t^U_j)$ and $\mathbf{V}^d(t^B_v)$ are calculated, i.e. the correlation between each one of the consecutive routing states that are formed after incorporating the impact of the BGP activity of the $F^U_j$ file is computed against the previous and the following routing state of reference (contained in $F^{B}_{v-1}$ and $F^{B}_{v}$ files respectively). As a result two different Pearson Coefficient functions are defined for the time window under investigation $[t^B_{v-1}, t^B_v]$:

$$\rho^d_U(t^B_{v-1}, t^U_j) = \rho(\mathbf{V}^d(t^B_{v-1}), \mathbf{V}^d(t^U_j)) \quad (4.12)$$

$$\rho^d_U(t^B_v, t^U_j) = \rho(\mathbf{V}^d(t^B_v), \mathbf{V}^d(t^U_j)) \quad (4.13)$$
Finally, studying the evolution of $\rho_d^U(t_{v-1}^B, t_j^U)$ and $\rho_d^U(t_v^B, t_j^U)$ over time, $\forall j \in \{1, \ldots, J\}$, the exact time windows that the BGP anomalies take place are traced with maximum precision of $T_U \ll T_B = t_v^B - t_{v-1}^B$.

### 4.2.1.4 Use Cases

Before proceeding with the description of the use case scenarios and the acquired evaluation results, it must be mentioned that, within the VIS-SENSE framework, a network analytics software tool has been developed, capable of reproducing the BGP operations and routing decisions by processing the collected BGP messages that become available through the RIPE NCC repository [34]. Apart from accurately emulating the control-plane functionality, the software tool is also equipped with all the necessary modules for achieving both the efficient deployment and the reliable assessment of the proposed BGP anomaly detection-attribution techniques.

As far as the discovery of the large-scale routing disturbances is concerned, in order to provide a more evident and tangible description of the exact implementation of the proposed mechanism as well as to evaluate its efficiency, two major BGP events are chosen to be studied and presented, utilizing the raw BGP data from the RIPE NCC:

**Case A: The East African Marine Systems (TEAMS) cable cut**

On 25 February 2012 at 09:12 UTC, TEAMS undersea fiber cable, which interconnects the Middle East with East Africa, was cut by a ship’s anchor along its segment between the port of Fujairah in the United Arab Emirates and the city of Mombasa, capital of Kenya. This event caused the outage of prefixes hosted in East African countries and especially in Kenya, which was rather effectively and timely faced with adequate redirections of the Internet traffic through alternative physical paths (utilization of other Africa interconnecting links) and ISPs [11].

RIPE NCC BGP router status files (“bview” files) are made available with a period of 8hrs ($T_B = 8\text{hrs}$). Hence, $t_i^B = t_{i-1}^B + 8\text{hrs}, \forall i \in \{1, \ldots, I\}$, where $I = 7$, $t_1^B = 24/02/2012 - 08:00\text{ UTC}$ and $t_I^B = 26/02/2012 - 08:00\text{ UTC}$. In this context, the routing status matrix for $C_d=\text{Kenya(KE)}$ from the $M=\text{AS15469}$ point of monitoring (AS15469 belongs to “Warinet Global Services SA”, situated in Switzerland(CH) and serving as a NH of the rrc00 VP of RIPE NCC) [34] is calculated [14], where all the values are normalized as a percentage (%) of the aggregate number of prefixes serviced.
by all the ISPs of Kenya.

\[
\begin{bmatrix}
(t_1^B) & (t_2^B) & (t_3^B) & (t_4^B) & (t_5^B) & (t_6^B) & (t_7^B) \\
(AS174) & 8.25 & 8.12 & 7.34 & 7.50 & 0.00 & 0.00 & 0.00 \\
(AS3491) & 5.43 & 5.35 & 5.56 & 5.52 & 2.22 & 2.16 & 2.16 \\
(AS3741) & 0.20 & 0.20 & 0.20 & 0.20 & 0.37 & 0.36 & 0.36 \\
(AS5511) & 1.81 & 1.78 & 3.97 & 3.94 & 11.85 & 11.15 & 11.15 \\
(AS6453) & 13.68 & 13.47 & 16.27 & 15.98 & 39.26 & 40.65 & 40.65 \\
(AS5762) & 1.61 & 0.59 & 0.60 & 0.59 & 0.37 & 0.36 & 0.36 \\
(AS8966) & 15.09 & 15.84 & 11.31 & 11.05 & 0.00 & 0.00 & 0.00 \\
(AS9129) & 0.60 & 0.59 & 0.79 & 0.79 & 0.74 & 0.72 & 0.72 \\
(AS9498) & 9.26 & 9.11 & 10.12 & 9.86 & 0.00 & 0.00 & 0.00 \\
(AS15808) & 3.82 & 2.77 & 0.00 & 1.97 & 4.44 & 4.32 & 4.32 \\
(AS22351) & 0.00 & 0.00 & 0.00 & 0.00 & 0.36 & 0.36 & 0.36 \\
(AS27822) & 0.00 & 0.00 & 0.20 & 0.20 & 0.37 & 0.36 & 0.36 \\
(AS36944) & 21.33 & 20.99 & 21.23 & 20.32 & 5.93 & 5.76 & 5.76 \\
(AS37100) & 0.00 & 0.00 & 0.00 & 0.00 & 3.70 & 4.32 & 4.32 \\
(AS37114) & 0.00 & 0.00 & 0.00 & 0.00 & 0.37 & 0.36 & 0.36 \\
(AS37273) & 5.63 & 5.54 & 5.56 & 5.52 & 0.00 & 0.00 & 0.00 \\
(AS38176) & 0.80 & 0.59 & 1.19 & 1.18 & 1.85 & 1.80 & 1.80 \\
(AS44356) & 0.20 & 0.20 & 0.20 & 0.20 & 0.37 & 0.36 & 0.36 \\
\end{bmatrix}
\]

\[R^{KE} = \]

\[\rho^{KE} = \]

\[
\begin{bmatrix}
1 & 0.9945 & 0.9669 & 0.9727 & 0.4511 & 0.4467 & 0.4467 \\
0.9945 & 1 & 0.9734 & 0.9773 & 0.4785 & 0.4716 & 0.4716 \\
0.9669 & 0.9734 & 1 & 0.9976 & 0.5883 & 0.582 & 0.582 \\
0.9727 & 0.9773 & 0.9976 & 1 & 0.5986 & 0.592 & 0.592 \\
0.4511 & 0.4785 & 0.5883 & 0.5986 & 1 & 0.999 & 0.999 \\
0.4467 & 0.4716 & 0.582 & 0.592 & 0.999 & 1 & 1 \\
0.4467 & 0.4716 & 0.582 & 0.592 & 0.999 & 1 & 1 \\
\end{bmatrix}
\]

Subsequently, the corresponding \(7 \times 7\) Pearson Coefficient matrix over time is also computed \((4.15)\).

Furthermore, by plotting together all the rows of \(\rho^{KE}\) \((4.11)\) as separate functions of time, the chart of Figure \(4.1\) is produced. From this figure it is made apparent that significant alterations regarding the routing of Kenya-hosted prefixes have taken place during the time window between \(t_1^B = 25/02/2012 - 08:00\) UTC and \(t_5^B = 25/02/2012 - 16:00\) UTC, i.e. \(t_v^B = t_5^B\) \((4.7)\).
4.2 BGP anomaly detection on the basis of control-plane information analysis

Furthermore, in order to pinpoint more precisely, with a higher time granularity, the exact time windows when the BGP anomaly occurred, the Pearson Coefficient of the routing status that is formulated after the reception of each BGP update message file within \([t_4, t_5]\) against the routing status of \(F^4_B\) and \(F^5_B\) is calculated as described in (4.12)-(4.13), \(\forall j \in \{1, \ldots J\}, J = T_R/T_U = 96, t_U^j = t_U^{j-1} + 5\text{min}\). In this respect, Figure 4.2 presents the plot of \(\rho^{KE}_{B} (t_B^j, t_U^j)\) and \(\rho^{KE}_{U} (t_B^j, t_U^j)\) against \(t_U^j\). According to this chart, it becomes obvious that the routing status regarding Kenya’s interconnection with the rest of the Internet undergoes a period of substantial disturbance, which starts from \(t_U^{15} = 25/02/2012 – 09:15\text{ UTC}\) (i.e. BGP activity for the time space \((t_U^{14}, t_U^{15}) = (09:
10, 09 : 15], since BGP update message file $F_{15}^{U}$ is comprised of all BGP announcements and withdrawals generated after $F_{4}^{U}$ and continues for approximately $35 \times T_{U}$ seconds due to re-routing through alternative ISPs and/or outages of the Kenya’s prefixes, to reach a steady state at $t_{50}^{U} = 25/02/2012$ – 12 : 05 UTC.

**Case B: The 2008 Mediterranean Sea cable cut**

On 19 December 2008 at around 07:30 UTC, three different undersea fiber cables, which interconnect Europe with Africa, the Middle East and Asia: i) ”FLAG Europe-Asia”
In a similar manner to Case A, the routing paths towards Egypt(EG) are monitored from AS12637 (assigned to “Seeweb s.r.l.”, located in Italy(IT) and operating as a NH of the rrc10 VP of RIPE NCC in Milan) \[34\], for \( t_B^1 = 18/12/2008 - 08:00 \) UTC and \( t_B^2 = 20/12/2008 - 08:00 \) UTC. The routing status matrix for \( C_d=\text{Egypt(EG)} \) from the

Figure 4.3: Case B - Egypt: Plot of Pearson Coefficient matrix

(FEA), ii) "South East Asia Middle East Western Europe-3" (SEA-ME-WE-3) and iii) "South East Asia Middle East Western Europe-4" (SEA-ME-WE-4), were cut in the area of the Mediterranean Sea between Italy and Tunisia, along their segments that interconnects Italy with Egypt \[10\].
4 BGP Anomaly Detection

$M = \text{AS12637}$ is presented in (4.16),

$$R^{EG} = \begin{bmatrix}
(t_1^B) & (t_2^B) & (t_3^B) & (t_4^B) & (t_5^B) & (t_6^B) & (t_7^B)
\end{bmatrix}
\begin{bmatrix}
(\text{AS174}) & 0.46 & 0.46 & 0.45 & 0.00 & 0.00 & 0.00 \\
(\text{AS701}) & 0.04 & 0.04 & 0.04 & 0.12 & 0.00 & 0.01 \\
(\text{AS3536}) & 0.10 & 0.14 & 0.14 & 0.00 & 0.00 & 0.00 \\
(\text{AS3491}) & 0.00 & 0.00 & 0.00 & 0.00 & 0.00 & 0.00 \\
(\text{AS3549}) & 0.04 & 0.04 & 0.04 & 0.09 & 0.00 & 0.00 \\
(\text{AS4788}) & 0.00 & 0.00 & 0.00 & 0.00 & 0.00 & 0.00 \\
(\text{AS5511}) & 0.01 & 0.01 & 0.01 & 0.00 & 0.00 & 0.00 \\
(\text{AS6453}) & 0.03 & 0.03 & 0.03 & 0.07 & 0.10 & 0.10 \\
(\text{AS15412}) & 0.32 & 0.29 & 0.28 & 0.72 & 0.90 & 0.85 & 0.83
\end{bmatrix} (4.16)$$

while (4.17) shows the respective $7 \times 7$ Pearson Coefficient matrix over time.

$$\rho^{KE} = \begin{bmatrix}
1 & 0.9935 & 0.9926 & 0.4457 & 0.4759 & 0.4665 & 0.4597 \\
0.9935 & 1 & 0.9999 & 0.3744 & 0.4089 & 0.3987 & 0.3916 \\
0.9926 & 0.9999 & 1 & 0.3668 & 0.3996 & 0.3893 & 0.3821 \\
0.4457 & 0.3744 & 0.3668 & 1 & 0.9778 & 0.9758 & 0.9714 \\
0.4759 & 0.4089 & 0.3996 & 0.9778 & 1 & 0.9991 & 0.9972 \\
0.4665 & 0.3987 & 0.3893 & 0.9758 & 0.9991 & 1 & 0.9995 \\
0.4597 & 0.3916 & 0.3821 & 0.9714 & 0.9972 & 0.9995 & 1
\end{bmatrix} (4.17)$$

The plot of $\rho^d(t_i^B, t_a^B), \forall i, a \in \{1, \ldots, I\}$ (4.11) is presented in Figure 4.3 from which the BGP disturbance is detected between $F_{3}^{B} \equiv t_{3}^{B} = 19/12/2008 - 00:00$ UTC and $F_{4}^{B} \equiv t_{4}^{B} = 19/12/2008 - 08:00$. Additionally, Figure 4.4 shows $\rho^d(t_i^B, t_j^U)$ and $\rho^d(t_a^B, t_j^U)$, $\forall t_j^U \in [t_i^B, t_a^B], j = \{1, \ldots, J\}$ and the exact beginning of the abnormal routing behavior is determined at $t_{0}^{U} = 19/12/2008 - 07:30$ UTC, i.e. the BGP update message file that corresponds to the BGP activity taking place between $t_{0}^{U} = 19/12/2008 - 07:25$ and $t_{0}^{U} = 19/12/2008 - 07:30$.

As far as the time response of the detection mechanism is concerned, emphasis must be laid on the fact that, in the case that the analyst is only interested in the detection of the anomaly and not its subsequent evolution in time, there is no need for choosing such a large sliding window of $I = 7$; on the contrary, computing and comparing $V^d$ for only a few BGP update message files after the beginning of the disturbance, would be sufficient to reveal the instability incident.
4.2 BGP anomaly detection on the basis of control-plane information analysis

4.2.1.5 Conclusions

A near-real time anomaly detection technique has been presented hereby, for detecting the instabilities in BGP and isolating the location and time of their origin, without the need for human intervention. The proposed method can be implemented on a single router without raising issues concerning widespread deployment and modification of standards. Contrary to existing techniques which are mostly signature-based or supervised behavior-based, and mainly rely on features extracted from the volume of update messages, our method introduces two significant novelties. First, it is completely un-
supervised, requiring no a-priori knowledge of the dynamics of BGP instabilities and hence, no specific patterns of BGP activity are assumed or investigated. Second, it manages to efficiently capture and take advantage of the underlying correlation among the spatiotemporal characteristics of the voluminous and macroscopically disparate BGP activity; to this end a new feature is extracted, namely the vector of the last hop ASes that provide Internet connectivity on per country grouping and the variations of these vectors during stable periods and periods of instability.

The presented methodology has been implemented and assessed against two major real-life incidents of BGP disturbance, due to the accidental destruction of international fiber trunks. Being more specific, according to these use case evaluation, it becomes obvious that the proposed technique is capable of precisely defining the exact time instances of the instabilities’ occurrence, the evolution of the BGP abnormal behavior over time as well as the geographical impact and spreading of the detected phenomena.

4.2.2 Analysis of BGP hijacks: Types and mechanisms

The term BGP hijack generally refers to the creation and circulation of illegitimate BGP announcements that override the existing routing directives and cause unsolicited alterations to the nominal BGP status and operation. Through these fraudulent BGP announcements, the malicious ASes manage to gain unauthorized access to IP resources and traffic.

As it has already been thoroughly presented in the previous section, a wide variety of BGP anomalies and especially the ones that are related with infrastructural failures/destructions/misconfigurations can be easily detected by adequately exploiting the spatiotemporal correlation of the corresponding BGP activity. The broad extent of such incidents, in terms of both the magnitude of the related BGP activity and the eventual effect upon the configuration of the Internet physical structure, facilitates the identification of coherent patterns within the bulk and variety of the unceasing routing alterations.

On the contrary, malicious attacks against the BGP integrity are most probably expected to be executed completely sporadically both in time and space. More concisely, it appears rational that the malicious ASes refrain from carrying out massive attacks, so as to avoid raising any alerts and therefore to achieve the maximum prolongation of the impact and benefits of their actions. For this reason, the cyber criminals target at isolated prefixes, while their attacks are executed with sufficiently low repetition frequency. As a result, the malicious BGP activity is highly scattered from both a spatial (IP address and AS space) and a temporal point of view. Therefore, although the resulting routing changes are promptly traced and reported through the regular Internet mechanisms
4.2 BGP anomaly detection on the basis of control-plane information analysis

(monitoring of routers’ tables), they still remain practically undetected, since their abnormal nature is well hidden within the massive volume of ordinary BGP events. Hence, the discovery of BGP hijacks poses a special objective regarding the analysis of BGP anomalies.

In this context, for the actual implementation of an efficient BGP hijack detection system, it is an absolute prerequisite to develop suitable methodologies for discriminating among the whole set of monitored phenomena. In particular, given the aforementioned absence of solid hijacking patterns or correlations between hijacking events, adequate criteria need to be formulated, so as the consistency of each BGP announcement to be separately scrutinized in juxtaposition with the prevailing BGP activity. Additionally, what is of enormous importance, is that the adopted techniques must be capable of both guaranteeing the zero false negative ratio and minimizing the false alarms, so as to ensure that no BGP compromises are erroneously disregarded as legitimate or accidentally unnoticed due to monitoring overhead.

Ideally, in order to successfully carry out such a challenging task, it would be necessary to keep a complete and continuously updated track of all the ASes’ properties and their historical evolution, with particular focus on the complex semantic inter-AS relationships. Nevertheless, it must be underlined that the acquisition of this information requires a substantially time-consuming offline research through a great range of third-party resources and hence such approaches are bound to fail to process even a slight proportion of the aggregate BGP incidents. Moreover, the commercial relationships among the ASes are not publicly available and thus the collection of the necessary semantic information cannot be taken for granted to be always applicable and feasible [23] [20]. Consequently, a realistic hijack detection solution must utilize fully automated methodologies, which would extract added value information regarding the legitimacy of the BGP phenomena also on the basis of the raw BGP data.

The BGP hijacks can be roughly classified into two primary categories, depending on their effect on the reachability of the advertised prefix [7] [24]:

4.2.2.1 Prefix AS-Path hijacks.

The attacking AS maliciously announces itself as an intermediate hop along the path of an already occupied prefix, with the aim to either blackhole or intercept the traffic that falls within the IP space of the specific prefix and which will be thereafter compelled to traverse the hijacking AS. This case of BGP anomaly is usually referred to as AS-Path anomaly or AS-Path hijack, since the new BGP announcement affects solely the sequence of ASes (AS-Path) towards the origin-AS, which remains the same.

More precisely, as described in 4.2.1, let $W^{M,p}$ be the existing AS-Path connecting
the monitoring AS $M$ with the AS $O_p$ that owns prefix $p$.

$$W^{M,p} = \{ M, A^M_p, \ldots, A^{M,p}_{K_p}, O_p \}, \ p \in P$$  \hspace{1cm} (4.18)

The AS-path defines the set of the $K$ successive ASes ($A_k^p \in A, k = \{1, \ldots, K\}$) that have to be traversed, in order for $O_p$ to be reached from $M$ by any IP traffic in the range of prefix $p$. Moreover, $P$ and $A$ are the sets of all the active prefixes and ASes respectively. Since the route that is followed towards a given destination is dependent upon the starting point, $W^{M,p}$ is a function of $M$. However, considering a steady monitoring AS, the notation of $M$ is excluded from the hereafter analysis for reasons of simplicity. Hence, (4.18) can be rewritten as

$$W^p = \{ M, A^p_1, \ldots, A^p_{K_p}, O^p \}, \ p \in P$$  \hspace{1cm} (4.19)

Furthermore, let $W^q$ be an AS-Path announced at a later time instant for prefix $q$ that presents at least partial overlap with prefix $p$ ($p \cap q \neq \emptyset$).

$$W^q = \{ M, A^q_1, \ldots, A^q_{K_q}, O^q \}, \ q \in P$$  \hspace{1cm} (4.20)

In the case that the origin-AS is the same for both BGP announcements ($O^p = O^q$), then, an AS-Path anomaly is defined as the co-existence of two different AS-paths for overlapping prefixes or, equivalently, an AS-Path anomaly is identified if and only if there is at least one non-common intermediate AS between the two available AS-Paths.

$$\begin{cases} W^p \cap W^q \neq \emptyset \\ p \cap q \neq \emptyset \\ O^p = O^q \end{cases}$$  \hspace{1cm} (4.21)

At this point, it should be noted that, according to the routing prioritization rules:

- If $q \supset p$, then the second BGP announcement affects the routing of only the IP addresses that fall in the non-common IP space of prefix $q$, i.e. $q - q \cap p$.
- If $q \subset p$, then the IP traffic that is addressed for $q$ is rerouted through $W^q$, instead of $W^p$. On the contrary, the IP traffic for $p - q \cap p$ is still routed through $W^p$.
- If $q = p$, then the AS-Path that is advertised for $q$ ($W^q$) prevails against the initial AS-Path towards $p$ ($W^p$) if $W^q$ is shorter than $W^p$, i.e. $K^q < K^p$.

Thus, it becomes evident that the routing policies for prefix $p$ are impacted by the alternative BGP announcement if either $q \subset p$ or $q = p$ and $K^q < K^p$. 

56

SEVENTH FRAMEWORK PROGRAMME
4.2 BGP anomaly detection on the basis of control-plane information analysis

Aiming at pinpointing the attacking AS, the $H(p, q)$ is introduced to denote the set of non-common ASes between $W^p$ and $W^q$.

$$F(p, q) = W^p \cup W^q - W^p \cap W^q$$  \hspace{1cm} (4.22)

In case $H(p, q) \neq \emptyset$, each one of these non-common ASes, $A_h \in H(p, q) \equiv \{A_1, \ldots A_H\}$, are suspected of performing BGP hijacking (traffic interception or blackholing) against the origin-AS ($O^p = O^q$). As a matter of fact, if it is assumed that a BGP hijack event has actually been carried out by $A_h \in H(p, q)$, then, the rest of the non-common ASes that comprise $H(p, q)$ are unintentionally exploited for realizing the malicious detour through $A_h$. Moreover, if for the hijacking $A_h$ it is found that $A_h \in W^p$, it can be safely deduced the conclusion that the later announcement is the root cause of the hijacking, while, if $A_h \in W^q$, then the monitored event most probably regards an attempt executed by the owner $O^p$ to restore the normal routing path.

Hence, in order to be able to qualitatively and, eventually, quantitatively evaluate the legitimacy of an AS-Path alteration, it is necessary to respectively assess the legitimacy of each AS’s appearance within the announced AS-Path (High-level requirement for the detection of AS-Path hijacks).

4.2.2.2 Prefix Ownership Hijacks.

The malicious AS circulates a forged BGP announcement, declaring itself as the owner of a prefix $p$, which, however, it has not obtained officially from the IP regulatory authority, i.e. the Internet Routing Registry (IRR). Two main motivations can be identified for performing a prefix ownership hijack:

- The prefix hijack is performed as the necessary step for facilitating the execution of the attacker’s core criminal activities. By masquerading as the owner of legitimate (not blacklisted) IP addresses, the attacker has the opportunity to overcome firewall barriers and proceed with further criminal activities, such as spamming or even compromising selected hosts.

- The attacker gains access to traffic targeted to the victim AS.

Furthermore, incidents of prefix ownership hijacking can be further classified into three subcases, based on the state of the prefix prior to the circulation of the BGP announcement under investigation:

- The claimed prefix has not been allocated to any AS, but remains at the disposal of the corresponding IRR. These prefixes that are still available in the IRRs’ address space...
pool without an assigned owner are referred to as bogus prefixes [31]. The arbitrary acquisition of a bogus prefix is strictly prohibited. On the contrary, according to the legitimate procedure, the interested AS is required to submit an official application to its servicing IRR and subsequently it is allowed to proceed with the advertisement of the granted IP space. This type of prefix hijack is very difficult to be traced by a third party analyst, as no conflict in the routing table records is caused. Nevertheless, the hijacking of bogus prefixes could be very easily and promptly discovered by the IRRs themselves. An IRR could take advantage of its access to the Internet infrastructure, so as to straightforwardly compare any new BGP announcement against the lists of unallocated prefixes that only the IRR possesses updated in full detail.

- Although the claimed prefix has been properly allocated, it still does not appear in the routing tables, since it has not been explicitly announced by its rightful owner so far. Such a phenomenon can be encountered as the result of ASes requesting larger IP ranges than their current needs, so as to cater for probably augmented future requirements. The AS advertises only the IP addresses that cover its current domain size, while the rest of the acquired prefixes are left unattended. Such a hijack is very hard to be captured, since i) neither a routing alteration occurs so as to trigger an alert of third-party surveillance entities ii) nor the network connectivity of the victim AS is affected so as to raise any suspicions.

- The attacking AS announces a prefix that appears in the Internet to be already occupied by another AS. Such occurrences are also known as MOAS (Multiple Origin AS) events, since the claimed prefix appears in the routing tables with two different origin-ASes simultaneously [29]. It would be expected that this type of prefix hijack would be the easiest to be traced, as the Internet connectivity of the victim AS would significantly deteriorate, if not be totally disrupted, and hence the victim AS would be expected to immediately deploy all the necessary countermeasures. Nevertheless the detection of the anomaly and the re-establishment of the normal BGP operation by the victim AS itself cannot be taken for granted, due to two primary reasons:

  - If the attacking AS does not announce a subprefix (smaller IP space) of the already advertised prefix, but a prefix of equal size, then, according to the routing prioritization rules, the new BGP announcement will only be taken into account by the routers that lie in the proximity of the attacker, since the routers opt for the announcement that involves the shortest AS-Path towards the origin-AS. Hence, if the victim and the attacking AS are located far from
4.2 BGP anomaly detection on the basis of control-plane information analysis

each other within the Internet topology, it is most probable that the victim AS will not take notice of the malicious attack imminently, since it will lose connectivity only with remote domains.

– It is a common phenomenon that cyber criminals carefully select their targets so as pursue attacks against idle ASes, i.e. ASes that belong to organizations that have ceased their operation and thus their domains remain practically inactive. As a consequence, the malicious BGP activity remains unnoticed, as the offended domains are actually neglected or even disabled.

Additionally, besides the aforementioned gains that the criminals may profit from prefix hijacking in expense of the regular Internet operation, this particular subcase of prefix hijack entails the highest threat against the Internet infrastructure itself, since it radically affects the connectivity of fully functional domains. Therefore, for reliably safeguarding the ASes’ operation against hijacks of already announced prefixes, it is essential to develop and deploy a detection framework that will be based on the exhaustive analysis of the consistency of the BGP announcements and the evaluation of the routing alterations that are caused by suspicious BGP activity.

In order to formulate the case of MOAS prefix hijack, let $W^p$ be the original AS-Path connecting the monitoring AS $M$ with the owner AS $(O_p)$ of prefix $p$.

$$W^p = \{M, A^p_1, \ldots, A^p_K, O_p\}, \ p \in P$$ (4.23)

Moreover, let $W^q$ be the AS-Path declared in a later BGP announcement for the prefix $q$ that overlaps with $p$ ($q \cap p \neq \emptyset$).

$$W^q = \{M, A^q_1, \ldots, A^q_K, O_q\}, \ q \in P$$ (4.24)

Similarly to the analysis for the AS-Path anomalies, based on the routing prioritization policies, the advertisement of $q$ has an impact on the ownership of prefix $p$, if and only if either $q$ is a subset of $p$ or an alternative shorter AS-Path is declared for the same prefix $p$. Thus, a MOAS event is considered to be triggered by the second BGP announcement, when the following conditions are met:

$$\left\{ O^p \neq O^q \right\} \left\{ q \subset p \text{ OR } \left[q = p \text{ AND } K^q < K^p\right]\right\}$$ (4.25)

Nevertheless, apart from the prefix ownership hijacks, which are rather rare in general, there are plenty of legitimate reasons that can justify the occurrence of MOAS phenomena. More concisely, the vast majority of the MOAS phenomena appear as the result of ordinary prefix reallocation procedures:
4 BGP Anomaly Detection

- Prefix transaction between an ISP (Internet Service Provider) and its customers. It is the most common practice for the customers of an ISP to announce their newly obtained prefixes, without these prefixes having been withdrawn by the ISP first. This way, in case the specific prefix is withdrawn by its new owner (customer of the ISP), the prefix is mapped once again to its initial owner (ISP), without it being necessary for the ISP to re-circulate an adequate BGP announcement of this prefix.

- Prefix transaction between customers of the same ISP. Within the context of the reallocation of an ISP’s IP space, the phenomenon of prefix reassignment between customers of the same ISP without any prior withdrawal of the exchanged prefixes is regularly encountered.

In consequence, in order to decide upon the legitimacy of a prefix ownership hijack, it is mandatory to develop a methodology capable of extracting and quantifying the semantic information that concerns the relationship between the previous and the new owner of the prefix under investigation (**High-level requirement for the detection of prefix ownership hijacks**).

### 4.2.3 BGP hijack detection and attribution on the basis of geospatial correlations

As it becomes apparent from the aforementioned analysis of the two primary types of BGP hijacks (AS-Path and prefix ownership), the cornerstone for establishing an efficient detection and attribution framework of the BGP threats is to define quantitative metrics of the inter-AS relationships at either universal or local level. In this respect, within the framework of the BGP operation and the respective problem formulation that has already been described, a fully unsupervised as well as behavior-based technique is introduced for detecting and characterizing BGP hijacks.

#### 4.2.3.1 Proposed methodology

According to the proposed methodology, evidence of the strength of the potential organizational relationship between two ASes is implicitly derived by exploiting the proximity/disparity of their corresponding countries of origin within the Internet topology. To this end, two primary attributes are extracted, while, different similarity measures and distances are utilized, in order to capture the dynamics of the BGP activity with the highest possible accuracy. The analysis is built upon the definition of two different classes of related-countries for each origin-country, where each one of these classes attempts to
4.2 BGP anomaly detection on the basis of control-plane information analysis

encompass the features of the AS-Paths and prefix ownership change regarding the specific origin-country. The term *origin-country* refers to the country where the origin-AS of a prefix is located. Moreover, it must be underlined that the term *related-countries* refers to the set of countries that present Internet bonds with the origin-country of interest, according to the specific criteria of correlation that are defined below and which incorporate the characteristics of the BGP activity that involves these countries.

In more detail, let $C = \{C_1, \ldots, C_D\}$ be the set of all the separate country-entities identified at Internet level. Then, for each origin-country $C_d \in C$, the following two classes of related-countries are introduced, for mapping the contribution of the rest of the countries to the AS-Path anomalies and MOAS events that originate in country $C_d$:

A $I^d$ is the set of $J$ countries that host all the intermediate ASes that are traversed in order for IP traffic from $C(M)$ to reach $C_d$ for every prefix $p \in P^d$; $P^d$ is the set of all the prefixes hosted by ASes located in $C_d$ and $C(X)$ denotes the location-country of AS $X$.

$$
\begin{align*}
I^d &= \bigcup \{ C(A^p_k) \}, \forall p \in P^d \text{ and } \forall k = \{1, \ldots, K^p\} \\
P^d &= \bigcup \{ p \}, \forall C(O^p) = C_d \\
C(A^p_k) &\neq C(M) \text{ AND } C(A^p_k) \neq C^d
\end{align*}
$$

(4.26)

Interpreting (4.26), for every announced path $W^p$ that is declared for any of the prefixes hosted in country $C_d$ ($p \in P^d$), the countries of all the ASes that lie in-between the last AS of country $C(M)$ and the first AS of country $C^d$ are taken into account for building $I^d = \{I^d_1, \ldots, I^d_J\}$, i.e. $I^d$ is comprised of the $J$ different countries that have been so far recorded as intermediate hops between country $C(M)$ and country $C^d$. Similarly, the vector $I^d$ is estimated, which contains the number of appearances ($NAP(I^d_j)$) of each intermediate-country $I^d_j$ across the all the announced AS-Paths towards hosts of the destination-country $C^d$.

$$
I^d = \begin{bmatrix}
NAP(I^d_1) \\
\vdots \\
NAP(I^d_J)
\end{bmatrix}
$$

(4.27)

B $U^d$ is the set of the $N$ countries that appear as locations of all the ASes that have announced a prefix $q$ that overlapped with a prefix $p$ previously originating in country $C_d$.

$$
\begin{align*}
U^d &= \bigcup \{ C(O^q) \} \\
\forall q \text{ such that } q \cap p \neq \emptyset \text{ AND } O^q \neq O^p \\
C(O^p) &= C^d
\end{align*}
$$

(4.28)
Based on its definition, \( U^d = \{U^d_1, \ldots, U^d_N\} \) involves all the countries (hereafter referred to also as customer-countries of \( C_d \)) that have proceeded with the acquisition of IP addresses from the country \( C_d \). Moreover, the vector \( U^d \) consists of the number of prefixes \( (NAP(U^d_n)) \) that have been claimed by country \( U^d_n \) at the expense of country \( C_d \).

\[
U^d = \begin{bmatrix} NAP(U^d_1) \\ \vdots \\ NAP(U^d_N) \end{bmatrix}
\]  

(4.29)

Ultimately, the union of all the countries that belong to \( I^d \) and \( U^d \) comprise the set of related-countries of the origin-country \( P^d \). The definition of \( I^d \) aims at facilitating the detection of AS-Path anomalies. By exploiting the statistics of the set of countries that participate in the connectivity route of the country under investigation, any inconsistencies in contradiction to the usual pattern shall be revealed. In parallel, the utilization of \( U^d \) allows for evaluating the maliciousness of prefix ownership transactions, by studying the relationship and the common characteristics of the countries that are engaged in the MOAS event, based on their behavior in similar cases in the past.

The driving notion behind the introduction of the set of related-countries (\( P^d \)) resides in the urgent necessity to acquire a solid quantitative metric that would allow the analyst to numerically and thus automatically approach the semantic information that regards the relationship between ASes that are engaged in routing alterations. Taking advantage of this valuable metadata, the normality of the monitored BGP events is ultimately assessed. In this respect, \( P^d \) is further divided into \( I^d \) and \( U^d \), in order to focus on the different attributes that need to be taken into consideration in the case of the AS-Path alterations and MOAS phenomena. Based on \( I^d \) the legitimacy of an AS’s occurrence as an intermediate hop in an alternative AS-Path is judged, while the study of \( U^d \) provides useful insight regarding the announcement of a specific AS as the new owner of an already occupied prefix. Hence, the parallel introduction of \( I^d \) and \( U^d \) provides an holistic tool for dealing with the extremely challenging task of BGP hijack detection and attribution.

Additionally, concerning the pivotal motivation for the definition of \( I^d \) and \( U^d \), it must be underlined that in order to draw safe conclusions about the maliciousness of a BGP announcement, it would be necessary to have access to the complete history of the BGP activity as well as unlimited time for scrutinizing these data. Nevertheless, even in this ideal scenario, the efficient analysis would demand the grouping of the BGP activity in a manner that the necessary statistical depth for solidly comparing every new incident becomes available. For instance, the authors in [45] attempt to calculate the probability of announcing each one of the competing AS-Paths for a specific prefix. However, the
frequency of a route’s announcement cannot be regarded as a safe criterion for judging its malicious nature. In more detail, the same AS-Path is usually repeatedly announced at semi-regular intervals, for ensuring that the routing tables are maintained and updated; thus whenever an alternative route is announced for the first time, it is bound to be labeled as malicious. On the other hand, if the initial route was only announced at its first notice, the detection mechanism will not be able to differentiate between the competing paths, since they shall appear as equally probable.

Moreover, in the case that the competing paths are interchangeably announced for the prefix under investigation, the respective routes will be found to present comparable probability values; notwithstanding, such phenomena may correspond to repeated attempts by the owner to re-establish the legitimate status after successful hijack attacks. The same complications would be caused in the case of a MOAS event when either the prefix is announced for the first time by this particular new owner or no transaction had occurred in the past between the old and the new origin-ASes. In consequence, it becomes evident that by studying the BGP activity on a per AS, AS-Path or prefix basis would result to an unacceptably high ratio of false alerts, since every new BGP announcement that would not comply with the previous behavior of the engaged ASes would be easily mistaken as hijack.

On the contrary, by aggregating the BGP activity on per country level, the proposed methodology takes advantage of the inherent spatial correlation that characterizes the Internet infrastructure and the respective routing operations. As a consequence of inter-country and inter-AS agreements, local/Internet-wide policy regulations and the tiered hierarchy of the ISPs, for every country of interest there is a limited number of peer countries \((I_d)\) that support the interconnection of its end-hosts with the rest of the world. There is a finite set of countries \((U^d)\) and \((P^d)\) with which prefix transactions are commonly recorded. Hence, any BGP alterations involving the introduction of countries that are not common for the Internet activity of the specific destination-country is bound to raise significant suspicions of interception. Additionally, considering particularly the scenario of BGP cyber attacks, special emphasis must be laid on the fact that such malicious activity is usually carried out by (or through) remote hosts, in order to decrease the probability of being tracked down as well as to escape any legal actions and countermeasures. Thus, the risk of losing sight of intra-country threats due to the proposed per country aggregation is expected to be rather low.

Moreover, what is of profound importance, since the exhaustive analysis of historical information would be required, an analysis performed at per prefix or AS level would impose substantial memory and processing overhead due to the massive volume of data that would be required to be stored and managed, even for short monitoring time windows. On the other hand, by aggregating the BGP behavior at the country level, the extent of
the maintained database is radically reduced, while at the same time the extraction of the inter-host correlations and dependencies is limited to the finite set (approximately 250) of the Internet country-entities.

In this context, the two features that form the cornerstone of the proposed technique are presented below. Furthermore, for each one of these features, two distinctive distance metrics are defined, in order to provide different statistical perspectives of the feature’s behavior. Ultimately, through the numerical estimation of these features on the basis of the four different metrics, a completely unsupervised technique for detecting and characterizing any isolated BGP anomaly is formulated.

Distribution of the related-countries in terms of frequency of appearance

The vector $I^d$ holds the information of how many times each country has served as an intermediate hop towards the investigated origin-country $C_d$. By analyzing the frequency of appearance of country $C_X$ as an intermediate hop towards $C_d$ in comparison with the frequency of appearance for the rest of the countries, one can evaluate how ordinary it is for a new BGP announcement originating in $C_d$, to advertise an AS-Path that includes $C_X$ ($C_X \in I^d$). Similarly, the vector $U^d$ holds the information of how many times each country has claimed a prefix hosted in $C_d$. Hence, by studying the distribution of the frequency of appearance of the countries comprising $U^d$, one can derive conclusions about how usual it is for a MOAS event against $C_d$ to be triggered by an AS hosted in $C_X$ ($C_X \in U^d$).

In this context, two different metrics are introduced for analyzing the frequency of appearance of the related-countries in $I^d$ and $U^d$.

A. Probability of a country’s appearance

i) along a path towards country $C_d$.

$$B^d_i(I^d_j) = \frac{NAP(I^d_j)}{\sum_{j=1}^{\mid I^d \mid} \{NAP(I^d_j)\}}, \forall I^d_j \in I^d \quad (4.30)$$

From (4.30), it becomes obvious that the requested probability is equal to the conditional probability that an AS $X$ from country $C(X)$ appears within a routing path when the owner AS is hosted in $C_d$

$$B^d_i(I^d_j) = PR[X \in WP|(C(O^p) = C_d \text{ AND } C(X) = I^d_j)] \quad (4.31)$$

which is equal to the fraction of the $C(X)$’s appearances towards country $C_d$ against the sum of the appearances of all the countries that act as intermediate
hops for $C_d$. As far as its physical meaning is concerned, $B_d^I(I^d_j)$ is a measure of how frequently $I^d_j$ serves as an intermediate hop for $C_d$ and therefore, how frequently $I^d_j$ is expected to appear in a BGP announcement that refers to a $C_d$ host.

ii) as a new owner of a prefix hosted in $C_d$.

$$B_d^U(U^d_n) = \frac{\text{NAP}(U^d_n)}{\sum_{n=1}^{N} \{\text{NAP}(U^d_n)\}}, \forall U^d_n \in U^d \quad (4.32)$$

Equation (4.32) calculates the conditional probability that an AS $X$ from country $C(X)$ announces a prefix previously originating in $C_d$ ($B_d^U(U^d_n) = PR[C(X) = U^d_n|(C(O^p) = C_d)]$), which is equal to the fraction of the $C(X)$’s appearances in MOAS events of country $C_d$ against the sum of the appearances of all the countries in MOAS events of $C_d$.

B. Z-Score of the probability of a country’s appearance.

$$Z[B_d^I(I^d_j)] = \frac{\text{NAP}(I^d_j) - E[I^d]}{\sigma[I^d]} \quad (4.33)$$

$$Z[B_d^U(U^d_n)] = \frac{\text{NAP}(U^d_n) - E[U^d]}{\sigma[U^d]} \quad (4.34)$$

where $E[I^d]$ and $E[U^d]$ are the mean values of the elements of vector $I^d$ and $U^d$ correspondingly

$$E[I^d] = \frac{1}{J} \sum_{j=1}^{J} \{\text{NAP}(I^d_j)\} \quad (4.35)$$

$$E[U^d] = \frac{1}{N} \sum_{n=1}^{N} \{\text{NAP}(U^d_n)\} \quad (4.36)$$

and $\sigma[I^d]$ and $\sigma[U^d]$ is the standard deviation of all the elements of vector $I^d$ and $U^d$ correspondingly.

$$\sigma[I^d] = \sqrt{\frac{1}{J} \sum_{j=1}^{J} \{(\text{NAP}(I^d_j) - E[I^d])^2\}} \quad (4.37)$$
In essence, $Z[B^d_d(I^d_j)]$ (or $Z[B^d_d(U^d_n)]$) shows how common is country $I^d_j$ ($U^d_n$), taking into account the distribution of the frequency of appearance for the whole set of countries that belong to $I^d$ ($U^d$), i.e. Z-Score is capable of capturing the role of each related-country, taking into account the role of the other related-countries that service $C_d$. Being more specific,

i) $Z[B^d_d(I^d_j)] < (> ) 0$: $I^d_j$ is less (more) common in comparison with the average probability of an AS’s appearance along a $C_d$ path.

ii) $|Z[B^d_d(I^d_j)]|$: $NAP(I^d_j)$ is far from the mean value and/or $\sigma[I^d]$ is low ($\sigma \downarrow \Leftrightarrow$ tight distribution), which means that the number of $I^d_j$ appearances significantly varies from the average intermediate-country behavior for the case of the destination-country $C_d$, while at the same time there are only few countries that appear along the $C_d$ routes (or at least there are only a few countries that rarely appear along the $C_d$ routes).

iii) $|Z[B^d_d(I^d_j)]|$: $NAP(I^d_j)$ is close to the mean value and/or $\sigma[I^d]$ is high ($\sigma \uparrow \Leftrightarrow$ loose distribution), from which it can be deduced the conclusion that $I^d_j$ behavior is close to the average pattern for $C_d$, while, on the contrary, the values for the frequency of appearance for the rest of the intermediate-countries are rather disparate (multiple alternative countries other that the most common one).

Ultimately, in order to get a more concrete view of the $Z[B^d_d(I^d_j)]$ contribution to the analysis of the BGP hijacks, it would be rather interesting to study the Z-Score by taking into consideration the corresponding appearance probability ($B^d_d(I^d_j)$). For example, a low value of $B^d_d(I^d_j)$ would probably raise an alert for the existence of $I^d_j$ within a BGP announcement; nevertheless, corresponding low value of $|Z[B^d_d(I^d_j)]|$ would lead to more modest conclusions, especially if $Z[B^d_d(I^d_j)] < 0$, since $I^d_j$ seems to approach the average probability of appearance and at the same time the common pattern for $C_d$ includes high deviations. On the other hand, very low negative values of $Z[B^d_d(I^d_j)]$ in conjunction with low $B^d_d(I^d_j)$ would most probably be decisive about a highly suspicious BGP event, since in such a case $I^d_j$ appears as a rather rare instance within a generally normal BGP activity for country $C_d$. The aforementioned analysis is summarized in Table 4.1. In brief, the overall conclusion is that the lower the values of $B^d_d(I^d_j)$ and $Z[B^d_d(I^d_j)]$ are, the more alarming the appearance of intermediate-country $I^d_j$ is.
4.2 BGP anomaly detection on the basis of control-plane information analysis

<table>
<thead>
<tr>
<th>$B^d_I(I^d_J)$</th>
<th>$Z[B^d_I(I^d_J)]$</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>↓</td>
<td>&lt; 0 AND ↓</td>
<td>Very rare intermediate-country while only few rare alternative intermediate-countries exist. Strong evidence of anomaly.</td>
</tr>
<tr>
<td>↓</td>
<td>&gt; 0</td>
<td>Very rare intermediate-country, yet more probable than the average. Other rare alternative hops exist. Light evidence of anomaly</td>
</tr>
<tr>
<td>↑</td>
<td>&lt; 0</td>
<td>Common intermediate-country, yet there still exist more common routes. No evidence of anomaly</td>
</tr>
<tr>
<td>↑</td>
<td>&gt; 0</td>
<td>One of the most common intermediate-countries. No evidence of anomaly</td>
</tr>
</tbody>
</table>

Table 4.1: Common analysis of $B^d_I(I^d_J)$ and $Z[B^d_I(I^d_J)]$

The same analysis is also valid for the pair $B^d_U(U^d_n)$ and $Z[B^d_U(U^d_n)]$ that shall be utilized in the case of assessing the legitimacy of a MOAS event instead of an AS-Path alteration.

Distribution of the related-countries in terms of geographic topology

Routing algorithms generally opt for the shortest path in terms of delay and thus the minimization of the geographic distance of the aggregate end-to-end communication link is one of the most prominent decision criteria for defining the routing primitives. Hence, apart from specific inter-AS and/or inter-country agreements and policies as well as occasional large-scale failures within the Internet infrastructure, there is no apparent operational reason for selecting routes that significantly vary from the direct route. Equivalently, provider-customer relationships are usually established between ASes with close geographical proximity, since there must be a common point of presence in order for the IP-traffic to be implemented. Moreover, the provision of IP connectivity from a remote AS would abuse the aforementioned requirement for shortest path routing.

Furthermore, as it has already been underlined above, the cyber criminal activity is highly anticipated to originate from remote geographic locations and especially from specific countries with favorable legal system and/or relationships with the rest of the international community. Consequently, profound geographic deviations along the routing path (AS-Path hijacks) or prefix transaction between geographically distant ASes (MOAS hijacks) are not just evidence of path anomaly, but they can be safely regarded to be indicative of abnormal Internet functionality due to malicious BGP activity.

In this context, in order to quantitatively evaluate the geographic anomaly imposed
by the existence of an AS in a new BGP announcement (either as intermediate hop or origin-AS), two complementary measures are extracted and defined.

A. Geographic length introduced by a country’s appearance

i) along a path towards country $C_d$.

$$L^d_I(I^d_j) = \frac{G(C(M), I^d_j) + G(I^d_j, C_d)}{G(C(M), C_d)} \quad (4.39)$$

In (4.39), $I^d_j$ is any of the intermediate-countries towards $C_d$, $M$ is the monitoring AS, $C(X)$ is the country of location of AS $X$ and $G(C_x, C_y)$ is the geographic distance between countries $C_x$ and $C_y$ ($C_x, C_y \in C$). From (4.39) it can be seen that $L^d_I(I^d_j)$ is calculated as the geographic length of the $C(M) \rightarrow I^d_j \rightarrow C_d$ path, normalized against the minimum possible geographic path between the source and destination countries, i.e. the ideal direct link. The estimation of $G(I^d_j)$ allows for tracing the countries and thus the corresponding ASes that prominently fail to satisfy the inherent geographic coherence that characterizes the Internet architecture and operation as the result of the ideal shortest path routing policy.

ii) as a new owner of a prefix hosted in $C_d$.

$$L^d_U(U^d_n) = \frac{G(C(M), U^d_n) + G(U^d_n, C_d)}{G(C(M), C_d)} \quad (4.40)$$

In (4.40), $U^d_n$ is any of the countries whose AS has announced IP space previously originating in $C_d$.

The more distant the new and the old owner are in, reference to their relative position from the monitoring point, the more suspicious can the prefix transaction be considered.

B. Z-Score of the geographic length introduced by a country’s appearance. Similarly to the definition of the Z-Score for the probability of each country’s appearance, the Z-Score of the geographic deviation of each related-country against the direct path is computed below.

$$Z[L^d_I(I^d_j)] = \frac{L^d_I(I^d_j) - E[L^d_I(I^d_j)]}{\sigma[L^d_I(I^d_j)]} \quad (4.41)$$

$$Z[L^d_U(U^d_n)] = \frac{L^d_U(U^d_n) - E[L^d_U(U^d_n)]}{\sigma[L^d_U(U^d_n)]} \quad (4.42)$$
where $E[L^d_I(I^d_j)]$ and $E[L^d_U(U^d_n)]$ are the mean values of $L^d_I(I^d_j)$ ($\forall I^d_j \in I^d$) and $L^d_U(U^d_n)$ ($\forall U^d_n \in U^d$) correspondingly

$$E[L^d_I(I^d_j)] = \frac{\sum_{j=1}^{J} \{NAP(I^d_j) \times L^d_I(I^d_j)\}}{\sum_{j=1}^{J} \{NAP(I^d_j)\}}$$ (4.43)

$$E[L^d_U(U^d_n)] = \frac{\sum_{n=1}^{N} \{NAP(U^d_n) \times L^d_U(U^d_n)\}}{\sum_{n=1}^{N} \{NAP(U^d_n)\}}$$ (4.44)

and $\sigma[L^d_I(I^d_j)]$ and $\sigma[L^d_U(U^d_n)]$ are the standard deviations of $L^d_I(I^d_j)$ and $L^d_U(U^d_n)$.

$$\sigma[L^d_I(I^d_j)] = \sqrt{\frac{1}{\sum_{j=1}^{J} \{NAP(I^d_j)\}} \sum_{j=1}^{J} \{NAP(I^d_j) \times (L^d_I(I^d_j) - E[L^d_I(I^d_j)])^2\}}$$ (4.45)

$$\sigma[L^d_U(U^d_n)] = \sqrt{\frac{1}{\sum_{n=1}^{N} \{NAP(U^d_n)\}} \sum_{n=1}^{N} \{NAP(U^d_n) \times (L^d_U(U^d_n) - E[L^d_U(U^d_n)])^2\}}$$ (4.46)

The statistical analysis of potential geographic anomalies on the basis of Z-Score, allows us to acquire a peer view of each related-country’s role in reference to the general BGP pattern that is being formulated for the specific origin-country under investigation. For example, for the AS-Path alterations,

i) $Z[L^d_I(I^d_j)] < (>) 0$: The geographic deviation introduced by $I^d_j$ is lower (higher) than the average distance of all the perceived routing paths between the $C(M)$ and $C_d$.

ii) $|Z[L^d_I(I^d_j)]| \uparrow$: $L^d_I(I^d_j)$ is far from the end-to-end path’s mean geographic distance and/or $\sigma[L^d_I(I^d_j)]$ is low, which can lead to the conclusion that $I^d_j$’s location significantly deviates from the average path, while at the same time there are only a few alternative countries towards $C_d$, or at least there are only a few countries that are located far away from the common $C_d$ routes.
### 4 BGP Anomaly Detection

#### Table 4.2: Common analysis of $L^d_I(I^d_j)$ and $Z[L^d_I(I^d_j)]$

<table>
<thead>
<tr>
<th>$L^d_I(I^d_j)$</th>
<th>$Z[L^d_I(I^d_j)]$</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>$\rightarrow 0$</td>
<td>Close to the average geographic length. No evidence of length anomaly.</td>
</tr>
<tr>
<td>-</td>
<td>$</td>
<td></td>
</tr>
<tr>
<td>$\uparrow$</td>
<td>$&lt; 0$</td>
<td>Noticeably more distant than the shortest path, but closer than the average one. Longer and thus more suspicious routes exist.</td>
</tr>
<tr>
<td>$\downarrow$</td>
<td>$\downarrow$</td>
<td>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 $\sigma$)</td>
</tr>
<tr>
<td>-</td>
<td>$\uparrow\uparrow$</td>
<td>High distance from the mean rate, while the majority of the alternative paths are close to the average length. Strong evidence of length anomaly.</td>
</tr>
</tbody>
</table>

iii) $|Z[L^d_I(I^d_j)]| \downarrow$: $L^d_I(I^d_j)$ is close to the mean value and/or $\sigma[L^d_I(I^d_j)]$ is high; thus $I^d_j$ is geographically close to the average distance of all the intermediate hops of $C_d$, while, at the same time, there are multiple alternative intermediate-countries disparately located.

Finally, by taking into account $L^d_I(I^d_j)$ in parallel with $Z[L^d_I(I^d_j)]$, the analyst can derive fruitful conclusions concerning the semantics of the monitored BGP phenomena. To this end, Table 4.2 presents in brief the correspondence between the most interesting combinations of $L^d_I(I^d_j)$ and $Z[L^d_I(I^d_j)]$ values and the macroscopic attribution of such phenomena as far as the attention they draw regarding their potentially malicious nature. In general, it can be stated that the higher is the value of $L^d_I(I^d_j)$ and $Z[L^d_I(I^d_j)]$, the more suspicious the existence of country $I^d_j$ along the routing path towards country $C_d$ can be considered to be. Following the identical rational, but from the perspective of prefix ownership alterations, the MOAS phenomena are studied through the calculation and comparison of $L^d_U(U^d_n)$ and $Z[L^d_U(U^d_n)]$.

To sum up, according to the pivotal concept of the country-based BGP anomaly detection scheme that has been presented in Section 4.2.3, for each country $C_d$ that is being found to serve as the origin of a prefix (origin-country), two classes of related-countries are defined:
4.2 BGP anomaly detection on the basis of control-plane information analysis

- \( I_d \), i.e. the set of the \( J \) different countries whose ASes have served as intermediate hops towards an origin-AS hosted in \( C_d \).
- \( U_d \), i.e. the set of the \( N \) different countries whose ASes have announced a prefix that was until then owned by an origin-AS hosted in \( C_d \).

For each country \( I_d^i \in I_d \), the metrics \( B_d^i(I_d^i) \), \( Z[B_d^i(I_d^i)] \), \( L_d^i(I_d^i) \) and \( Z[L_d^i(I_d^i)] \) are defined, so as to quantify the regularity of the appearance of an AS \( X \) with \( C_X = I_d^i \) along an AS-Path originating in an AS that is located in \( C_d \). Similarly, for each country \( U_d^j \in U_d \), the metrics \( B_d^j(U_d^j) \), \( Z[B_d^j(U_d^j)] \), \( L_d^j(U_d^j) \) and \( Z[L_d^j(U_d^j)] \) are introduced, so as to quantify the regularity of a MOAS event that involves a prefix hosted in \( C_d \) and announced by an AS \( X \) with \( C_X = U_d^j \). The composition of the sets \( I_d \) and \( U_d \) as well as the values of the corresponding eight metrics are continuously updated upon the reception of new BGP messages.

4.2.3.2 Real-world implementation upon BGP AS-Path hijacks

In this section, the particular technical details for realistically applying the proposed geospatial BGP anomaly detection scheme in the case of AS-Path hijacks will be described. Moreover, the efficiency of this novel detection and attribution methodology will be evaluated against a publicly announced AS-Path hijack.

Implementation Issues.

Despite the solid theoretical background of the aforementioned country-based methodology, its straightforward real-world implementation for the case of AS-Path hijacks should suffer from a severe drawback that would significantly degrade its efficiency. A substantial fraction of the intermediate hops along an announced AS-Path are higher-tier ASes, which, inherently as a result of their high position in the Internet hierarchy, provide the ASes’ connectivity across multiple countries or even continents. Thus, due to their practically worldwide coverage and their functionality as distant gateways, higher-tier ASes are involved in the vast majority of the perceived AS-Paths. However, despite their global presence, higher-tier ASes, like any other AS, are uniquely identified by a sole country of origin, which usually coincides with the location of the enterprise’s headquarters. Therefore, including the higher-tier ASes in the calculation of \( I_d \) is not only impractical for these specific ASes, but it will also contaminate the overall statistical analysis, since it will heavily contribute to the formulation of a radically erroneous and hence misleading estimation of the \( B_d^i(I_d^i) \), \( Z[B_d^i(I_d^i)] \), \( L_d^i(I_d^i) \) and \( Z[L_d^i(I_d^i)] \) values for the whole \( I_d \) set.
In order to make this problem more evident, let us assume the real example of AS-Path 
\{AS15469, AS15576, AS174, AS6762, AS8966, AS36866, AS13224\}, where 
C(AS15469) = CH (Switzerland), C(AS15576) = CH, C(AS174) = US (USA), 
C(AS6762) = IT (Italy), C(AS8966) = AE (United Arabic Emirates), 
C(AS36866) = KE (Kenya) and C(AS13224) = KE. In this case, AS174, AS6762 and AS8966 will be recorded as a subset of the overall 
intermediate hops towards KE and respectively, according to (4.26), US, IT and AE 
will be included in the set of KE’s intermediate countries, i.e. \{US, IT, AE\} \subseteq U^{KE}. 
Nevertheless, taking into account AS174 for the computation of 
\textit{NAP}(I^d_i), I^d_i \equiv US, a very high value for US will be produced and hence, based on such announcements, the false conclusion will be drawn that any IP traffic originating in CH shall have to traverse US to reach KE, which from a geographical perspective is completely incoherent. 
This overestimation of the US involvement in the routing of KE traffic would have two 
major consequences in the efficiency of the AS-Path hijack detection and attribution 
mechanism:

i) Announcements that include higher-tier ASes established in US would be erroneously considered as suspicious due to the high \textit{Ld}(I^d_i) value. This would result to an unacceptably high False Positive Ratio (false alarms).

ii) The \textit{Ld}(I^d_i) distribution would be utterly tampered, since the higher-tier ASes are almost always present in AS-Paths. Thus, BGP hijacks executed by isolated ASes located in remote hosts would remain unobserved, since the numerical values of the corresponding geographical metrics would be comparable to the vast majority of the samples as these would be formulated because of the higher-tier presence.

Therefore, the False Negative Ratio would rise (undetected cyber activity).

In this respect, a subset of \textit{I}^d is defined, \textit{I}'^d, that is comprised of all the \textit{J'} countries that belong to \textit{I}^d but are not classified as higher-tier ASes:

\[
\left\{ \begin{array}{l}
I'^d = \{I'^d_1, \ldots, I'^d_{J'}\}, \ J' \leq J \\
I'^d = I^d \cap [\text{Not-higher-tier ASes}] 
\end{array} \right. 
\] (4.47)

Eventually, \textit{Bd}(I'^d), \textit{Z}[\textit{Bd}(I'^d)], \textit{Ld}(I'^d) and \textit{Z}[\textit{Ld}(I'^d)] are calculated for the set \textit{I}'^d. 
However, for simplicity and consistency of reference, the initial notation will be kept. 
Moreover, before proceeding, it must be underlined that this exclusion of the higher-tier ASes from the geographic-based statistical analysis does not degrade or compromise the reliability of the BGP detection mechanism, since higher-tier ASes are not expected under any circumstances to deploy criminal activity; on the contrary as far as their participation in BGP anomalies is considered, potentially they shall only be engaged in misconfiguration events. Hence, no issue of increasing the false negative ratio is raised.
4.2 BGP anomaly detection on the basis of control-plane information analysis

According to the analysis above, the metrics $B^j_d(I^d_j)$, $Z[B^j_d(I^d_j)]$, $L^j_d(I^d_j)$ and $Z[L^j_d(I^d_j)]$ are defined on a per intermediate-country level. Thus, in order to achieve the ultimate goal of detecting and attributing any BGP attacks against a prefix’s legitimate AS-Path, it is necessary to quantify the legitimacy of the new AS-Path as a whole. Therefore, it is necessary to expand this methodology in a manner that is implemented at AS-Path level.
anomaly level. As a matter of fact, on the basis of the AS-Path anomaly definition that is described in (4.21), it becomes apparent that each AS-Path anomaly is uniquely determined by two competing AS-Paths, while in turn, each AS-Path is respectively identified by a sequence of intermediate-countries. In this context, let once again $H(p, q)$ be the set of non-common ASes that are involved in the AS-Path alteration caused by two BGP announcements of the overlapping prefixes $p$ and $q$, where both $p$ and $q$ originate from the same AS, which is located in country $C_d$ (4.22). Then, considering the fact that suspicions of malicious BGP activity are raised for intermediate-countries with low values of $B_d(I^d_j)$, $Z[B_d(I^d_j)]$ and high values of $L_d(I^d_j)$ and $Z[L_d(I^d_j)]$, for each monitored AS-Path anomaly, the corresponding scores at AS-Path level are defined:

- **Country Appearance Probability per AS-Path anomaly ($CAP_{path}$)**
  \[
  CAP_{path} = \min\{B_d(C(A_h))\}, \forall A_h \in H(p, q) \quad (4.48)
  \]

- **Z-Score of Country Appearance Probability per AS-Path anomaly ($CAPZ_{path}$)**
  \[
  CAPZ_{path} = \min\{Z[B_d(C(A_h))]\}, \forall A_h \in H(p, q) \quad (4.49)
  \]

- **Country Geographic Length per AS-Path anomaly ($CGL_{path}$)**
  \[
  CGL_{path} = \max\{L_d(C(A_h))\}, \forall A_h \in H(p, q) \quad (4.50)
  \]

- **Z-Score of country geographic length per AS-Path anomaly ($CGLZ_{path}$)**
  \[
  CGLZ_{path} = \max\{Z[L_d(C(A_h))]\}, \forall A_h \in H(p, q) \quad (4.51)
  \]

**Use case of AS-Path hijack**

Based on the records of the North American Network Operators Group (NANOG) mailing list, on August 20th 2011, a Russian telecommunication company named “Link Telecom” (AS31733), reported that five of its prefixes, i.e. 46.96.0.0/16, 83.223.224.0/19, 94.250.128,160.0/19 and 188.164.0.0/16, had been hijacked. In more detail, the hijack began approximately in April 2011 and it practically entailed the reactivation of the set of the aforementioned prefixes, which, until that time, had remained idle for a prolonged period of several months, although they were still allocated to (in the possession of) “Link Telecom”.

The malicious BGP announcements did not affect the ownership of the prefixes under investigation, but they involved the circulation of abnormal AS-Paths (AS-Path
4.2 BGP anomaly detection on the basis of control-plane information analysis

Figure 4.6: Distribution of Z-Score of Country Appearance Probability per AS-Path anomaly (CAPZ\textsuperscript{path})

anomaly) which dictated that the IP traffic traverses the hijacking AS for interception purposes. The hijacking AS is located in the US and will be hereafter referred to as AS\textsubscript{hij} for ease of reference. As a countermeasure, following the detection of the hijack, the victim AS (AS31733) generated on August 24th and 29th response announcements of longer subprefixes (e.g. 83.223.224.0/20 and 83.223.240.0/20 against 83.223.224.0/19) so as to overwrite the existing malicious routing records (taking advantage of the higher priority of the longer prefixes) and restore the legitimate BGP operation.
In this respect, the hereby proposed methodology is implemented for the whole day of August 24th 2011, when the countermeasures of AS31733 were first carried out. All AS-Path anomalies taking place on August 24th 2011 are recorded and, for each one of these monitored events, the values of the four novel metrics ($CAP_{path}$, $CAPZ_{path}$, $CGL_{path}$ and $CGLZ_{path}$) that have been introduced for quantifying the potentially malicious nature of routing path alterations are calculated. As a matter of fact, the response of the victim AS is expected to trigger an AS-Path anomaly event as a result of the juxtaposition of the newly circulated legitimate route (rather straight path between the

---

SEVENTH FRAMEWORK PROGRAMME
4.2 BGP anomaly detection on the basis of control-plane information analysis

Figure 4.8: Distribution of Z-Score of Country Geographic Length per AS-Path anomaly (CGLZ$^{path}$)

monitoring point and AS31733) against the forged existing path previously intercepted by AS$H$ (route traversing US). The raw data of the BGP activity that took place on August 24th 2011 are obtained once again through the RIPE NCC repository [34], while the AS15469 (“Warinet Global Services SA”), which is situated in Switzerland(CH) and serves as a NH of the rrc00 VP of RIPE NCC, is chosen as the monitoring point (M).

As an output, the distributions of $CAP^{path}$, $CAPZ^{path}$, $CGL^{path}$ and $CGLZ^{path}$ are presented in Figures 4.5, 4.6, 4.7, 4.8 respectively, so as to provide a profound perspective of the capability of these metrics to efficiently facilitate the accurate discrimination of
the bulk of daily BGP events and allow for their classification on the basis of their legitimacy.

From Figure 4.5 it becomes apparent that the vast majority of the AS-Path anomalies involve rather common intermediate countries, while only for a very small fraction of approximately 7% the ASes that participate in the path alteration event are hosted in countries that are highly unusual for the specific destination-country.

Moreover, Figure 4.6 shows that a percentage of less than 15% of the overall monitored AS-Path anomalies involve intermediate-countries with probability of appearance lower than the average ($CAP^Z_{path} < 0$) and only approximately 0.1% of the path alterations present noticeably low $CAP_{path}$, i.e. values of $CAP_{path}$ lower than one standard
4.2 BGP anomaly detection on the basis of control-plane information analysis

Figure 4.10: Scatter plot of $CGL^{\text{path}}$ against $CGLZ^{\text{path}}$

deviation of the $CAP^{\text{path}}$ distribution ($CAP^{\text{path}} < -1$).

Furthermore, according to Figure 4.7, almost 98% of the BGP events that are related to the alteration of the announced path involve intermediate countries that do not introduce additional geographic path length more than the direct source-destination distance, i.e. ($CGL^{\text{path}} < 2$).

Finally, Figure 4.8 shows that $CGLZ^{\text{path}}$ is also usually limited to very low values, i.e. $CGLZ^{\text{path}} < 1$ for circa 85% of the cases of path alterations. Summarizing the conclusions from the analysis of Figures 4.5-4.8, it is apparent that only a rather minor ratio of the whole set of BGP path events are expected to present sufficiently extreme (too low or high) values for all the four metrics.
To the same end of evaluating the discriminating capability of the proposed features, Figures 4.9 and 4.10 show the scatter plot of \( CAP \) against \( CAPZ \) as well as the scatter plot of \( CGL_{path} \) against \( CGLZ_{path} \). In particular, from Figure 4.9 it becomes evident that there is a prevailing linearity between \( CAP_{path} \) and \( CAPZ_{path} \) and therefore it is expected to be of limited interest to study in parallel the evolution of both of these metrics, while, on the contrary, the computation of \( CAP_{path} \) should suffice to provide the necessary peer insight to the country appearance probability per AS-Path anomaly. On the other hand, based on Figure 4.10, it can be safely deduced that \( CGL_{path} \) and \( CGLZ_{path} \) are far from being regarded as completely dependent; for example, there are cases of substantially high values of \( CGL_{path} \) that correspond to disproportionately low
4.2 BGP anomaly detection on the basis of control-plane information analysis

![Scatter plot of CAP\textsuperscript{path} against CGLZ\textsuperscript{path} values of CGLZ\textsuperscript{path}, which can be interpreted as follows: Although the particular AS-Path anomaly involves an intermediate country with high geographic deviation from the direct source-destination link, for the case of the specific destination-country there have also been recorded intermediate countries that introduce comparably high geographic deviation.

Finally, Figures 4.11 and 4.12 present the scatter plot of CAP\textsuperscript{path} against CGL\textsuperscript{path} and CGLZ\textsuperscript{path} respectively. With the red triangle the AS-Path anomaly that corresponds to the incident under investigation is marked. As it becomes apparent, taking into account the Country Appearance Probability in conjunction with the Z-Score of the Country Geographic Length (Country Geographic Length of each event in reference to]
the general routing behavior of the specific destination-country) of all the monitored BGP path alterations, the proposed methodology is capable of decisively pinpointing the BGP hijack due to both the low probability of traversing US along a route from CH towards RU and the high geographical deviation introduced by US as an intermediate hop of such a route.

### 4.2.3.3 Real-world implementation upon BGP prefix ownership hijacks

In contrast to the case of AS-Path anomalies, the proposed country-based technique for BGP anomaly detection can be straightforwardly applied to MOAS events, without any considerations for special categories of ASes. The engagement of higher-rank ASes in MOAS phenomena is equally ordinary as any other AS’s and therefore there is no need for such ASes to be excluded from the composition of $U^d$.

As described in (4.25), a MOAS event is defined as the coexistence of two overlapping prefixes $p$ (former announcement) and $q$ (later announcement) with different origin-AS. Thus, making use of the calculation of $U^d$ (4.28) and its describing scores (4.32), (4.34), (4.40), (4.42), the legitimacy of each MOAS event that rises at the BGP level is quantitatively assessed by means of the following metrics:

- **Country Appearance Probability per MOAS event ($CAP_{MOAS}$)**
  \[
  CAP_{MOAS} = B_d^d(U(C(O^q))), \; d = C(O^p)
  \]  
  (4.52)

- **Z-Score of Country Appearance Probability per MOAS event ($CAPZ_{MOAS}$)**
  \[
  CAPZ_{MOAS} = Z[B_d^d(U(C(O^q))], \; d = C(O^p)
  \]  
  (4.53)

- **Country Geographic Length per MOAS event ($CGL_{MOAS}$)**
  \[
  CGL_{MOAS} = L_d^L(U(C(O^p))), \; d = C(O^p)
  \]  
  (4.54)

- **Z-Score of country geographic length per AS-Path anomaly ($CGLZ_{MOAS}$)**
  \[
  CGLZ_{MOAS} = Z[L_d^L(U(C(O^p))], \; d = C(O^p)
  \]  
  (4.55)

where $O^p$ and $O^q$ are the owner ASes of prefixes $p$ and $q$, respectively.
Use case of prefix ownership hijack

The most prominent example of a prefix ownership hijack regards the unauthorized announcement of a portion of the YouTube’s IP space by the Pakistan Telecom and it is broadly known as the YouTube-Pakistan incident [30] [12]. The detailed timeline of the event is provided below:

• Until 24 February 2008.
  There is in effect a BGP announcement that determines AS36561 (YouTube) as the origin-AS for the prefix 208.65.152.0/22. AS36561 is also the owner of other prefixes that are not engaged in the hijack.

• 24 February 2008, at 18:47 (UTC).
  AS17557 (Pakistan Telecom) announces 208.65.153.0/24 to its provider PCCW Global (AS3491). Due to the routing prioritization rule that were previously described, the announcement of Pakistan Telecom prevails against the initial one published by YouTube, as it involves a longer prefix. Hence, instead of being forwarded to the YouTube domain, any IP traffic regarding the 208.65.153.0/24 space is redirected to Pakistan Telecom. Access to the YouTube website is lost, since all the three IPs (208.65.153.238, 208.65.153.251 and 208.65.153.253) that are linked to the YouTube.com domain in the DNS (Domain Name Server) records fall within the 208.65.153.0/24 range.

• 24 February 2008, at 20:07 (UTC).
  AS36561 re-circulates announcements of 208.65.153.0/24. Between two announcements of the same prefix, a router opts for the shortest AS-Path. Thus, YouTube’s later announcement is disregarded by the routers that reside closer to Pakistan and therefore a portion of the YouTube’s IP traffic is still routed to the Pakistan Telecom.

• 24 February 2008, at 20:18 (UTC).
  AS36561 announces 208.65.153.128/25 and 208.65.153.0/25. By breaking 208.65.153.0/24 into two adjacent subprefixes, YouTube exploits the longest prefix policy and regains the possession of the aggregate prefix.

• 24 February 2008, at 21:01 (UTC).
  AS3491 withdraws all prefixes originating from Pakistan Telecom and in this way the hijack of 208.65.153.0/24 is terminated.

Emphasis must be laid on the fact that, although the intervention of the Pakistan Telecom was deliberate, the YouTube-Pakistan incident was not the outcome of a criminal
action, but the result of a misconfiguration. The Pakistan Telecom aimed at blocking the access of its users (and the users of its customer ASes) to the YouTube website. To this end, the plan was to advertize itself within its intranet as the origin-AS of the YouTube.com IPs. By hacking the Internet infrastructure at as low as the BGP level, instead of solely tampering with its DNS registrations, Pakistan Telecom would blackhole any YouTube related traffic even in the case that a user browsed YouTube’s IPs directly. However, due to a misconfiguration, the forged BGP announcement propagated outside the AS17557 intranet, to PCCW Global, and from there it contaminated the routing tables of the whole planet.

Nevertheless, despite its misconfiguration nature, this incident is characterized by all the features that a malicious MOAS hijack is expected to have in terms of the attack’s strategy and execution. Therefore, the YouTube hijack has given rise to profound concerns about the reliability of the BGP infrastructure and its vulnerability against potentially malicious actions that may be executed in the future. Moreover, due to the fact that it was observed at a worldwide extent (massive worldwide access to the YouTube website) as well as because of the extreme rareness of such phenomena (it stands so far as the unique indisputable case of an isolated prefix hijack that has been publicly recorded), the YouTube-Pakistan incident serves as the common reference, if not the inspiration, for the bulk of the BGP hijack research that has been conducted thereafter [13] [8]. Hence, the YouTube hijack is chosen as the most appropriate use case for benchmarking the VIS-SENSE country-based MOAS detection and attribution algorithm.

To this end, the proposed technique is applied to the BGP data that are collected during the whole day of February 24th 2008. In more detail, each BGP announcement circulated on that day is compared against the routing status of the affected prefixes. If a MOAS phenomenon is discovered according to (4.25), the set $U_d$ of the customer-countries of the prefix’s initial origin-country is updated and the values $CAP^{MOAS}$, $CAPZ^{MOAS}$, $CGL^{MOAS}$ and $CGLZ^{MOAS}$ that determine the legitimacy of the MOAS event are calculated. For carrying out this study, the raw BGP data for the date under investigation are acquired from the RIPE NCC repository [34]. Among the available monitoring points, the AS3333 is selected ($M = AS3333$), which belongs to RIPE NCC, is located in Netherlands (registered to the Internet country entity Europe - EU) and pertains to the Vantage Point rrc00 of RIPE NCC.

As a result of the statistical study of the MOAS phenomena encountered on February 24th 2008, the distributions of $CAP^{MOAS}$, $CAPZ^{MOAS}$, $CGL^{MOAS}$ and $CGLZ^{MOAS}$ are computed and presented in Figures 4.13-4.16 in order to acquire a deeper insight into the discriminating capability of each corresponding metric. According to Figure 4.13 only a percentage less than 0.5% of the $CAP^{MOAS}$ measurements fall below the
4.2 BGP anomaly detection on the basis of control-plane information analysis

![Graph showing the distribution of Country Appearance Probability per MOAS event](image)

Figure 4.13: Distribution of Country Appearance Probability per MOAS event ($\text{CAP}^{\text{MOAS}}$)

value of 5% (prefix announcement from an AS that resides in a country that rarely claims prefixes of the previous origin-country), while the bulk of the MOAS events regard the transaction of prefixes between a pair of countries that regularly appears to be involved in such phenomena. Thus, similarly to the conclusions drawn in Section 4.2.3.2 for the case of the BGP AS-Path alterations, it is noted that $\text{CAP}^{\text{MOAS}}$ shows rather high granularity and hence it can be proven as a highly efficient screening criterion for ranking
Figure 4.14: Distribution of Z-Score of Country Appearance Probability per MOAS event (CAPZ\textsuperscript{MOAS})

the suspiciousness of the traced MOAS events. Furthermore, based on Figure 4.14, only a ratio as low as 10% of the aggregate set of discovered prefix ownership alterations are caused by ASes located in countries with a probability of appearance lower than the average (CAP\textsuperscript{MOAS} < 0) for the specific victim origin-country.

Interpreting Figure 4.15, approximately 98% of the MOAS events are triggered by ASes hosted in countries that do not introduce additional geographic length higher than the initial direct path towards the previous origin-AS of the prefix of interest (CGL\textsuperscript{MOAS} < 2). Finally, the vast majority of the CGLZ\textsuperscript{MOAS} measurements (more than 90% of the
4.2 BGP anomaly detection on the basis of control-plane information analysis

Figure 4.15: Distribution of Country Geographic Length per MOAS event ($CGL^{MOAS}$)

total samples) are restricted to values lower than 1, i.e. the distance from the average behavior for the origin-country of reference is lower than 1 standard deviation unit. Hence, such incidents can be regarded to fall within the ordinary statistical pattern of MOAS phenomena. In consequence, carrying out a common analysis of the distributions above, it can be safely deduced the conclusion that only a very limited percentage of the overall prefix ownership events presents a sufficiently extreme scoring of the four metrics introduced and hence, this evaluation framework can be safely applied for filtering the maliciousness of the increasingly numerous MOAS incidents.
Additionally, to further explore the analytical properties of the introduced metrics as well as capturing any redundancy in the acquired information between the two metrics of the same feature, the scatter plots of $\text{CAP}^{\text{MOAS}}$ versus $\text{CAPZ}^{\text{MOAS}}$ and $\text{CGL}^{\text{MOAS}}$ versus $\text{CGLZ}^{\text{MOAS}}$ are depicted in Figures 4.17 and 4.18 respectively. From this perspective, it is observed that a prevailing linear relationship exists between $\text{CAP}^{\text{MOAS}}$ versus $\text{CAPZ}^{\text{MOAS}}$ (green line in Figure 4.17), i.e. events with high $\text{CAP}^{\text{MOAS}}$ are also characterized by high $\text{CAPZ}^{\text{MOAS}}$. Nevertheless, there still exist MOAS events that...
4.2 BGP anomaly detection on the basis of control-plane information analysis

Figure 4.17: Scatter plot of $\text{CAP}^{\text{MOAS}}$ against $\text{CAPZ}^{\text{MOAS}}$

significantly deviate from this linear relationship.

The samples within the cyan ellipse are identified by negative $\text{CAPZ}^{\text{MOAS}}$ (below the average $\text{CAP}^{\text{MOAS}}$) despite the increased $\text{CAP}^{\text{MOAS}}$, which means that there still exist more popular customer-countries for the specific victim-countries that are engaged in these incidents. However, such phenomena can be still neglected, as the value of $\text{CAP}^{\text{MOAS}}$ is still high enough to suppress any suspicions. Moreover, the MOAS events within the green ellipse have zero $\text{CAPZ}^{\text{MOAS}}$ with 100% $\text{CAP}^{\text{MOAS}}$, i.e. they regard incidents where the customer-country is the unique country that has ever claimed prefixes of the initial origin-country. Hence, for minimizing processing overhead and the analysis’ complexity, the computation of $\text{CAPZ}^{\text{MOAS}}$ could possibly be omitted,
Figure 4.18: Scatter plot of $CGL^{MOAS}$ against $CGLZ^{MOAS}$

since the information contributed by $CAPZ^{MOAS}$ can be obtained by the sole study of $CAP^{MOAS}$.

On the contrary, according to 4.18, the scatter plot between $CGL^{MOAS}$ and $CGLZ^{MOAS}$ is built upon two equally important constituents:

- Samples with $CGLZ^{MOAS} \approx 0$ despite the increasing $CGL^{MOAS}$. They depict MOAS events where, although the customer-country introduces excessive geographic length, most of the customer-countries for this origin-country are also geographically dispersed and therefore it can be regarded that such a phenomenon of high $CGL^{MOAS}$ is ordinary for this specific origin-country.
4.2 BGP anomaly detection on the basis of control-plane information analysis

Figure 4.19: Scatter plot of $\text{CAP}^\text{MOAS}$ against $\text{CGL}^\text{MOAS}$

- Samples with proportional $\text{CGLZ}^\text{MOAS}$ and $\text{CGL}^\text{MOAS}$ values. They concern MOAS events that involve BGP announcements from remote countries, while most of the customer-countries that have been so far recorded to claim prefixes of the origin-country reside in its close proximity.

Consequently, there is no standard correlation between $\text{CGLZ}^\text{MOAS}$ and $\text{CGL}^\text{MOAS}$ and hence both of these metrics should be included, so as to acquire a spherical view of the investigated incident.

Following this rational, the scatter plots of $\text{CAP}^\text{MOAS}$ versus $\text{CGL}^\text{MOAS}$ and $\text{CAP}^\text{MOAS}$ versus $\text{CGL}^\text{MOAS}$ are respectively presented in Figures 4.19 and 4.20, where the YouTube-Pakistan incident is denoted with a red triangle. By juxtaposing the quantitative re-
sults of $CAP^{MOAS}$ and $CGLZ^{MOAS}$ the exceptional nature of the YouTube hijack is profoundly revealed among the massive bulk of MOAS phenomena. The proposed country-based technique for BGP hijack detection and attribution captures this incident by exploiting two facts: i) Pakistan is extremely rarely encountered as a customer of USA and ii) Pakistan is located too remotely from USA to be regarded its legitimate customer.
4.2.4 BGP hijack detection and attribution on the basis of inferred inter-AS relationships

The technique that is introduced in Section 4.2.3 for achieving the challenging task of BGP hijack detection and attribution quantifies the inter-AS relations using the correlations between the corresponding countries that the ASes are located in. The purpose of grouping the BGP activity at country level is to create a generic statistical pattern of the BGP operation under normal conditions, so as to manage to evaluate the legitimacy of each BGP anomaly by measuring its distance from the expected behavior.

Nevertheless, despite the coherent theoretical study as well as its proven effectiveness under the most prominent cases of both AS-Path and MOAS hijacks, it becomes apparent that the country-based methodology is inadequate to trace any BGP anomalies that may be generated at intra-country level, i.e. the attacking AS resides in the same country with the victim AS. In this respect, an alternative technique is developed for numerically capturing the coherence among the ASes that are involved in any BGP event, i.e. the ASes along the announced AS-Paths (AS-Path hijack) or the competing origin-ASes (MOAS hijack).

4.2.4.1 Analysis of inter-AS relationships

In spite of the Internet’s mesh architecture as far as the mere physical interconnection of the communicating peers is concerned (data transmission at the physical, data link and network layer), the comprising entities of the Internet (ASes), which carry the burden of deploying and maintaining the necessary infrastructure (links and equipment) as well as managing the IP space for providing data delivery services, are hierarchically organized within a three-tier framework. This hierarchical classification is formatted on the basis of the uni/bidirectional provision of telecommunication services between the involved ASes and it stems from the fact that each AS is dependent upon higher-tier ASes for establishing its required worldwide access.

It must be underlined that the ASes’ categorization is not determined formally by an Internet administrative authority, but it reflects the extent of the IP traffic or equivalently the ratio of the ASes that are eventually serviced (at any hop of the aggregate Internet route) by an AS’s network. The classification of the ASes is mostly carried out arbitrarily, based on the draft rule that i) 1st-tier ASes are Internet Service Providers (ISPs) of end-users or other small 1st-tier ASes, ii) 2nd-tier ASes provide Internet services to 1st-tier ASes and usually operate at either country or continent level and iii) 3rd-tier ASes, offer the universal interconnectivity of 2nd-tier ASes, while they can be also found operational at local level for large customers. Internally, the ASes of every
Figure 4.21: Annotated graph of the Internet infrastructure on the basis of inter-AS relationships

tier also differentiate from each other in terms of magnitude. In general, ASes at lower levels recompense ISPs at higher levels in exchange for access to the rest of the Internet. Thus, the inter-AS relationships from an Internet service perspective are principally semantic, since they derive as the result of enterprise agreements between the engaged ASes. Notwithstanding, despite their semantic nature, the inter-AS relationships also correspond to the ASes’ actual connectivity, as the ASes’ common presence or the existence of a physical link between them is mandatory for the data forwarding to be accomplished.

Acquiring a solid knowledge of the inter-AS relationships can be proven valuable for assessing the maliciousness of BGP anomalies, since the existence of a well-established dependency between two ASes can justify their common participation in an AS-Path alteration or a MOAS event. In this context, three major cases of bilateral AS relationships are defined in the Internet infrastructure [23] [35] [19] [21] [20]:

- Provider-To-Customer (p2c) or Customer-To-Provider (c2p). A Provider offers transit connectivity to IP traffic of its Customers.
Peer-To-Peer (p2p). Two ASes can establish an agreement for mutual exchange of traffic on a quid pro quo basis. The involved peers forward to each other only traffic regarding either themselves or their customers.

Sibling-To-Sibling (s2s). Two ASes that administratively belong to the same organization can be connected through a direct link. Two siblings exchange only IP traffic of their own origin.

Taking into account the aforementioned inter-AS relationships, an annotated graphical representation of the Internet infrastructure is drawn in Figure 4.21, where the green arrows denote the directional p2c link, the orange arrows denote the p2p links and the cyan arrows denote the s2s links. According to the definition of the three possible inter-AS relationships, there are certain restrictions that apply to IP routing among the Internet’s comprising ASes [23]:

- IP traffic arriving at an AS \( X \) from one of \( X \)’s customers can be forwarded to any of \( X \)’s providers, peers and customers.
- IP traffic arriving at an AS \( X \) from one of \( X \)’s providers can be forwarded only to any of \( X \)’s customers.
- IP traffic arriving at an AS \( X \) from one of \( X \)’s peers can be forwarded only to any of \( X \)’s customers.

The following examples of Internet routes at AS level, i.e. BGP AS-Paths, are described in Figure 4.21:

- Path 1-2 (magenta). Traffic between AS1 and AS2 can be straightforwardly exchanged via their s2s link, without any need for transiting through their common ISP.
- Path 4-5 (red). In order to reach AS4, traffic originating from AS5 should i) initially reach the highest-level AS12 through an uphill path of two consecutive p2c links (AS12 → AS9 → AS5) and ii) subsequently follow a downhill path towards the destination AS4 through three consecutive p2c links (AS12 → AS11 → AS8 → AS4). The path AS12 → AS10 → AS7 → AS3 → AS4 (also longer than AS12 → AS11 → AS8 → AS4) would not be feasible since, normally, AS3 does not forward traffic from its ISP through the s2s connection with AS4.
- Path 1-3 (yellow). Traffic between AS1 and AS3 can be exchanged via the p2p link of their ISPs (AS6 and AS7 respectively), so as to avoid the transit fees of AS10, i.e. AS1 ← AS6 ↔ AS7 → AS3 instead of AS1 ← AS6 ← AS10 → AS7 → AS3.
4 BGP Anomaly Detection

- Path 4-7 (purple). Although route AS7 → AS3 ← AS8 → AS4 appears as the shortest sequence of ASes for facilitating the data flow between AS7 and AS4, such a path cannot be realistically applied, since an AS3 cannot transit traffic between AS7 and AS8, i.e. a p2c link cannot be followed by a c2p link.

To sum up, the validity conditions for a BGP AS-Path are described in Lemma 4.1.

**Lemma 4.1.** A BGP AS-Path is valid if and only if it is comprised of the following sequence of sub-routes:

1. Zero or more c2p links, followed by
2. Zero or one p2p link, followed by
3. Zero or more p2c links

Making virtue of these BGP directives that reflect the ASes’ business agreements and dependencies, several methods have been proposed for inferring the inter-AS relationships through the exploitation of the BGP announcements. Pioneering research in this field has been carried by Gao [23], who introduced a set of heuristic rules in order to extract the inter-AS relationships from the BGP messages. To this end, a new metric, the AS’s degree, is utilized, in order to quantify the magnitude of each AS. The degree of AS $X$ is defined as the number of the $X$’s direct neighbors, i.e. the set of ASes that are straightforwardly connected with $X$ via any type of link (p2c, c2p, p2p, s2s), and it is calculated as the aggregate number of different ASes that appear adjacent to $X$ in any announced AS-Path for any prefix and any origin-AS. Subsequently, the global ranking of all the active ASes is performed, according to their degree. Then, for each announced prefix $p$ with AS-Path $W_p$, described in (4.19), the AS with the highest degree is pinpointed $A_{HD}^p$ and the overall AS-Path to be divided into two sequential sub-routes: i) the uphill path from the monitoring AS ($M$) until the highest degree AS ($A_{HD}^p$) and ii) from the highest degree AS ($A_{HD}^p$) until the origin-AS ($O_p$). For every pair of successive ASes $X, Y$ belonging in the uphill sub-route ($X, Y ∈ M, ..., A_{HD}^p$), $X$ is considered as a customer of $Y$ and $Y$ as a provider of $X$, while, for every pair of successive ASes $X, Y$ belonging in the downhill sub-route ($X, Y ∈ A_{HD}^p, ..., O_p$), $X$ is considered as a provider of $Y$ and $Y$ as a customer of $X$. Moreover, let $X$ be the AS with the highest degree between the two ASes that are adjacent to $A_{HD}^p$. Then, $X$ is regarded to have a p2p link with $A_{HD}^p$ under the condition that i) $A_{HD}^p$ does not provide transit services to $X$ in any other prefix announcement monitored so far and ii) the degrees of $X$ and $A_{HD}^p$ are of comparable magnitude, i.e. the degree of $X$ is no lower than a given threshold ratio in comparison with the degree of $A_{HD}^p$. 

96 SEVENTH FRAMEWORK PROGRAMME
4.2 BGP anomaly detection on the basis of control-plane information analysis

Furthermore, the authors in [35] suggest a more solid mathematical formulation for solving the Type-of-Relationship (ToR) problem. Following their approach, an undirected graph of the BGP topology is built, where an edge connects any pair of ASes that appear in adjacent positions in an announced AS-Path. Subsequently, by processing the BGP messages, a directional p2c/c2p/p2p type is assigned to each edge, in a manner that the eventual directed graph maximizes the percentage of valid BGP routes in reference to the actual AS-Paths announced in the BGP messages. In this respect, it is proven that the ToR decision problem is NP-complete, while computational efficient approximations for its solution have also been proposed, focusing solely on the definition of the c2p and p2c relationships [19] [21]. Moreover, particular emphasis has been laid by Dimitropoulos et al. on the solid extraction of the p2p relationships [20], which led to the development of a publicly available repository that holds valuable information about the ASes’ ranking and relationships [15].

Notwithstanding, regardless of the exact chosen method for inferring the AS relationships from the raw BGP data, eventually, as a result of this mapping, a directed graph of the BGP topology is created, where each vertex represents a single AS and each bidirectional/unidirectional edge corresponds to the type of relationship (p2c, c2p, p2p) between the connected ASes.

4.2.4.2 Proposed methodology

As it has already been mentioned, in order to judge upon the malicious nature of a BGP event, it would be of highly beneficial for the analyst to be aware of any available semantic information concerning the business activity of each AS’s proprietor organization as well as the relationships that may exist among the participating ASes. This cognition of the underlying agreements that eventually determine the BGP decisions, allows for the identification of any reasonable cause that can justify the monitored BGP behavior, so as to vote in favor of the event’s legitimacy. Nevertheless, due to the massive volume of the BGP activity and the continuous alterations of the BGP status, it is not feasible to implement such a time-consuming procedure for exhaustively studying each BGP event separately.

Hence, it is of the utmost importance to develop an unsupervised methodology for implicitly extracting any associations between the ASes of interest, by utilizing the raw BGP data, in order to quantitatively score the legitimacy of the corresponding BGP event. Ultimately, the analyst is capable of isolating only a small subset of the most suspicious BGP phenomena, so as to apply the irreplaceable human background knowledge and intuition for decisively concluding about whether a BGP event is the result of a malicious cyber attack.
In order to satisfy this requirement, a novel metric is introduced for numerically scoring the logical interconnection of two ASes, through measuring the geodesic distance of the corresponding vertices at the graph of the ASes’ BGP topology:

**Definition 4.1.** The geodesic distance between two ASes $X, Y$ of the BGP topology graph $(GD_{BGP}(X, Y))$ is equal to the number of edges of the shortest valid path that connects the two vertices $X, Y$. A valid path is any path that obeys to the conditions described in Lemma 4.1.

In this context, let the occurrence of a MOAS event that is triggered by the announcement of a prefix $q$ from the origin-AS $O^q$ against an overlapping prefix $p$ that is already occupied by the origin-AS $O^p$ (4.25). Then, the coherence between $O^q$ and $O^p$ and, thus, the regularity of the transaction, can be quantified by the calculation of $GD_{BGP}(O^p, O^q)$, $GD_{BGP}(O^p, O^q)$ identifies the graphical proximity between the former and later origin-ASes engaged in a MOAS event and, for ease of reference, it will be hereafter denoted as $(GDO)$. 

$$GDO = GD_{BGP}(O^p, O^q)$$ (4.56)

The basic idea behind the notion of $GDO$ lies within the fact that, based on the BGP announcements and the inferred inter-AS relationships, for each AS a draft neighborhood of ASes is formatted, consisting of its close providers, customers and peers. Hence it is rational that any ordinary MOAS event should entail ASes of the same neighborhood. On the contrary, prefix ownership exchanges between ASes that reside rather remotely within the hierarchical ASes’ topology are expected to raise suspicions of potential BGP hijacks.

Therefore, since the aim of $GD_{BGP}(X, Y)$ is to characterize the proximity of $X$ and $Y$ in reference to the tree-like Internet structure, for the estimation of $GD_{BGP}(X, Y)$, the p2p links are disregarded and solely c2p/p2c links are followed for tracing the shortest valid path between $X$ and $Y$. A p2p link is followed only when a valid path between $X$ and $Y$ cannot be built through the exclusive utilization of c2p/p2c links. In this case that a p2p link is incorporated along the shortest valid path estimation, this p2p link is considered to contribute a double edge to the $GD_{BGP}(X, Y)$ computation, in order to include the transit through a supposed higher-level ISP. This heuristic rule reflects the fact that the proposed approach focuses on extracting the provider-customer or customers-of-the-same-provider association that may exist between the victim and the attacker. Thus, the fact that two ISPs may appear as direct peers does not imply an additional logical interconnection between ASes of each ISP’s cone (Definition 4.2 [20]), since an AS $X$ should present prefix ownership activity involving solely ASes of the same ISP with $X$, i.e. ASes that reside within the same cone with $X$. 

98 SEVENTH FRAMEWORK PROGRAMME
4.2 BGP anomaly detection on the basis of control-plane information analysis

Definition 4.2. The cone of an AS $X$ is the AS $X$ itself plus all the ASs that can be reach following only c2p/p2c and s2s links. In other words, $X$’s cone is equal to $X$ plus $X$’s customers, plus its customers customers etc.

Hence, the shortest valid path between $X$ and $Y$ should traverse the top vertex AS of the smallest cone that contains both $X$ and $Y$. This concept is best presented in Figure 4.22 where, in order to reach AS8 from AS1, the actual path AS1 $\leftarrow$ AS9 $\leftarrow$ AS13 $\leftrightarrow$ AS14 $\rightarrow$ AS12 $\rightarrow$ AS8 is replaced with the route AS1 $\leftarrow$ AS9 $\leftarrow$ AS13 $\leftarrow$ AS? $\rightarrow$ AS14 $\rightarrow$ AS12 $\rightarrow$ AS8 that follows a fully hierarchical structure.

Furthermore, besides estimating the consistency between the victim and the attacker ASes in a MOAS event, a more comprehensive view of the coherence of the new BGP announcement, in reference to the rest of the Internet BGP activity, would be acquired by additionally identifying the logical interconnections of the new origin-AS with the ASes that occupy the neighboring prefixes of the prefix under investigation. Being more specific, let $\mathbf{PN}^p$ be defined as the set of the $2 \times PNR$ prefixes that present the highest
proximity with prefix $p$ as far as their position in the overall IP space is concerned, i.e. Prefix Neighbors of prefix $p$. The definition of $\text{PN}^p$ is given below:

**Definition 4.3.** The set of the Prefix Neighbors of prefix $p$ ($\text{PN}^p$) consists of i) the PNR successive prefixes (Prefix Neighbors Radius) towards higher IP addresses than $p$ plus ii) the PNR successive prefixes towards lower IP addresses than $p$, under the condition that $O^r \neq O^p \forall r \in \text{PN}$.

The Definition 4.3 is schematically represented in Figure 4.23, where the green color marks the $\text{PNR} = 2$ prefixes that comprise $\text{PN}$. Then for the case of a MOAS event, where a prefix $q$ is declared by origin-AS $O^q$ against the announcement of origin-AS $O^p$ for the overlapping prefix $p$, the vector $\text{GD}(O^q, \text{PN}^p)$ is computed by calculating the geodesic distance between the new origin-AS ($O^q$) and each one of the owners of the prefixes comprising the $p$’s Prefix Neighbors

$$\text{GD}(O^q, \text{PN}^p) = \begin{bmatrix} GD_{BGP}(O^q, r_1) \\ \vdots \\ GD_{BGP}(O^q, r_{PNR}) \end{bmatrix}$$ (4.57)

where $\{r_1, \ldots, r_{PNR}\} = \text{PN}^p$.

In graph theory, the maximum geodesic distance of a vertex against any of the vertices of a graph’s subset (subgraph) denotes the *eccentricity* of this vertex in reference to the subgraph. Thus, the greatest value of all the elements of $\text{GD}(O^q, \text{PN}^p)$ measures the *eccentricity* ($\text{ECOPN}$) of the new origin-AS ($O^q$) in juxtaposition with the ASes that are assigned with the adjacent prefixes of $p$ ($\text{PN}^p$):

$$\text{ECOPN} = \text{ECC}(O^q, \text{PN}^p) = \max\{GD_{BGP}(O^q, r)\}, \forall r \in \text{PN}^p$$ (4.58)

The motivation for the introduction and utilization of the Prefix Neighbors notion stems from the fact that prefix allocation is not performed arbitrarily on behalf of the
4.2 BGP anomaly detection on the basis of control-plane information analysis

IRRs. On the contrary, according to the usual approach, large blocks of IP addresses are assigned to high-level ISPs who reallocate them to their customers. Thus, it is generally expected that the ownership of successive IP spaces should present noticeable coherence, without of course excluding the probability of legitimate occurrences of different phenomena. In this context, the minimum as well as the mean value of the elements of $GD(O^q, PN_p)$ can also provide a fruitful insight to the underlying logical interconnection of the involved ASes. Hence, by expanding the definition of eccentricity, the minimum eccentricity ($ECOPN^{\text{min}}$) and mean eccentricity ($ECOPN^{\text{mean}}$) are also introduced.

$$ECOPN^{\text{min}} = ECC^{\text{min}}(O^q, PN_p) = \min \{GD^{BGP}(O^q, r)\}, \forall r \in PN_p \quad (4.59)$$

$$ECOPN^{\text{mean}} = ECC^{\text{mean}}(O^q, PN_p) = \frac{1}{PNR} \sum_{r \in PN_p} \{GD^{BGP}(O^q, r)\} \quad (4.60)$$

Thus, the eccentricity, minimum eccentricity and mean eccentricity of the new origin-AS in comparison with the origin-ASes of the IP space that lies adjacent to the prefix under investigation, provide a numerical insight to any probable relationship that may exist between the suspected malicious AS and the prefix that it announces, regardless of any apparent distance between the two conflicting ASes (former and later owner of the prefix in contention).

To sum up, making virtue of the methodology that has been proposed above for the detection and attribution of BGP hijacks on the basis of inferred inter-AS relationships, each MOAS event can be identified by four metrics:

- Geodesic Distance between the former and the later origin-AS of the prefix in contention ($GDO$) \( (4.56) \)
- Eccentricity between the later origin-AS (suspected attacker) and the set of the origin-ASes of the Prefix Neighbors of the prefix in contention ($ECOPN$) \( (4.58) \)
- Minimum eccentricity between the later origin-AS (suspected attacker) and the set of the origin-ASes of the Prefix Neighbors of the prefix in contention ($ECOPN^{\text{min}}$) \( (4.59) \)
- Mean eccentricity between the later origin-AS (suspected attacker) and the set of the origin-ASes of the Prefix Neighbors of the prefix in contention ($ECOPN^{\text{mean}}$) \( (4.60) \)
4 BGP Anomaly Detection

4.2.4.3 Real-world implementation upon BGP prefix ownership hijacks

The proposed methodology for BGP hijack detection and attribution on the basis of inferred inter-AS relationships is applied to the Youtube-Pakistan MOAS incident, which has been extensively described in 4.2.3.3. In more detail, utilizing once again the raw data that are obtained from the Next Hop AS3333 of the RIPE NCC repository for the whole day of February 24th 2008, all the MOAS events occurring within these 24 hours are recorded according to their definition in 4.25. Subsequently, for each MOAS event, the values of \( GDO \), \( ECOPN \), \( ECOPN^{\text{min}} \) and \( ECOPN^{\text{mean}} \) are calculated and

Figure 4.24: Distribution of \( GDO \) per MOAS event
4.2 BGP anomaly detection on the basis of control-plane information analysis

their distributions are provided in the Figures 4.24 - 4.27. It must be noted that for the Youtube-Pakistan incident, $GDO = 3$, $ECONP = 4$, $ECONP^{mean} = 3.25$ and $ECONP^{min} = 3$

Based on the results shown in Figure 4.24, it becomes apparent that for the vast majority of the monitored MOAS events, the former and the later origin-ASes present high proximity in reference to the inter-AS relationships graph. In more detail, for approximately 60% of the MOAS events, $GDO = 1$, while for approximately 30% of the MOAS events, $GDO = 2$. Taking into account the analysis of the BGP MOAS events in Section 4.2.2.2, these prefix ownership alterations can be safely disregarded, since a value
of \( GDO \) equal to 1, is interpreted as a direct provider-customer relationship between the two engaged origin-ASes and hence the detected prefix transaction can be perfectly justifiable. Furthermore, for \( GDO = 2 \), the MOAS event most probably corresponds to a prefix reallocation between customers of the same provider or to a straightforward prefix announcement from an affiliated AS of a provider’s customer (2 hops distance).

Therefore, making virtue of the estimation of \( GDO \), the analyst is empowered with a reliable quantitative metric of the heuristics rules that are defined in Section [4.2.3.2] as potential legitimate causes of MOAS events. Eventually, the analyst is capable to filter

![Figure 4.26: Distribution of \( \text{ECOPN}^{\text{mean}} \) per MOAS event](image-url)
out the bulk of the monitored BGP activity and scrutinize only the most suspicious security incidents, i.e. the MOAS events with $GDO \geq 3$, which amount to circa 30 cases per 24 hours monitoring window.

Moreover, studying figure, which presents the distribution of $ECOPN$ for the sample of MOAS events gathered on February 24th 2008, it is noticed that the greatest percentage of the announcements of already occupied prefixes is carried out from origin-ASes that have high proximity with even the most distant of the origin-ASes of the neighboring IP space. A similar conclusion is derived also from the analysis of Figure 4.26, which provides an overview of the distribution of the $ECOPN^{mean}$ samples, i.e. of the mean.
eccentricity between the new origin-AS and the origin-ASes of the adjacent prefixes.

The merits from the introduction of the notion of eccentricity become even more evident through the study of Figure 4.27 which shows that for approximately 90% of the MOAS events, the “attacker”-AS present high relationship ($GDP \leq 2$) with at least one of the ASes occupying the prefix’s neighboring IP addresses.

Finally, in order to exploit the merits that can stem from the common analysis of
4.2 BGP anomaly detection on the basis of control-plane information analysis

Figure 4.29: Scatter plot of \( GDO \) against \( ECOPN_{\text{min}} \), with a view of the probability of occurrence for each \( GDO-ECOPN_{\text{min}} \) pair

the aforementioned features, Figure 4.28 plots the pairs of \( GDO \) and \( ECOPN \) values for each MOAS event, while at the same time it presents the probability of occurrence for each \( GDO-ECOPN \) pair, i.e. the distribution of all the monitored \( GDO-ECOPN \) combinations. Focusing on the horizontal plane, it is mentioned that there are cases of MOAS events with disproportional values of \( GDO \) and \( ECOPN \), i.e. there are MOAS events where the “attacker”-AS presents no logical interconnection with the “victim”-AS
while on the contrary it presents high relationship with the origin-ASes of the adjacent prefixes (and vice versa). Additionally, taking into consideration the projection of each \textit{GDO-ECOPN} pair onto the Z-axis it is observed that only the slightest minority of the MOAS events show high values of both \textit{GDO} and \textit{ECOPN}. Similarly, Figure 4.29 shows the scatter plot of \textit{GDO} versus \textit{ECOPN}_{min}.

In contrast to the results obtained through the implementation of the BGP hijack detection and attribution methodology that has been introduced in Section 4.2.3 on the basis of the ASes' geospatial correlations, the hereby detection technique that utilizes the inferred inter-AS relationships does not highlight the Youtube-Pakistan incident as the most prominently suspicious MOAS event of the February 24th 2008. More concisely, according to Figures 4.28 and 4.29, the Youtube-Pakistan incident (marked with the magenta cycle) belongs to the very small set of events that are identified with extreme measurements of \textit{GDO}, \textit{ECOPN} and \textit{ECOPN}_{min}. Hence, it is steadily qualified for further investigation by the network analysts, in order to shed light on the exact causes and mechanism that produced the eventual BGP event.

Nevertheless, there still exist a few MOAS phenomena with even more extreme behavior in terms of \textit{GDO}, \textit{ECOPN} and \textit{ECOPN}_{min}. Such a MOAS event (\textit{GDO} = 5, \textit{ECOPN} = 6 and \textit{ECOPN}_{min} = 5) is triggered by the announcement of prefix 199.247.245.0/24 by AS841 as a subprefix of the prefix 199.247.128.0/17 that had already been announced by AS22573. By thoroughly examining the existing \textit{bview} files, it is found that AS841 and AS22573 (both residing in Canada) had not been previously announced along the same path and therefore no logical proximity of the two ASes could be identified. As a matter of fact, studying also the subsequent BGP activity, it is noticed that the same conditions (no path traversing both AS841 and AS22573) were also valid for several weeks after the aforementioned announcement and only more than a few months later AS841 announced its prefixes through AS22573, so as AS22573 to be ultimately identified as a provider of AS841.

On the contrary, as it has already been discussed in Section 4.2.3.3 the Youtube-Pakistan prefix hijack engages two ASes of high degree and hence it is expected that their geodesic distance does not reaches a rather extreme value. Being more specific, since both AS36561 (Youtube) and AS17557 (Pakistan) lie at the highest levels of the Internet AS hierarchy, it is rational that they can be interconnected within the inter-AS graph through a low number of intermediate hops (transit ASes). Notwithstanding, at the same time, the eccentricity of AS17557 against the origin-ASes of the neighboring IP space of the hijacked prefix is rather high, since AS17557 belongs to a different IRR (AS17557 belongs to the Asia-Pacific IRR, i.e. APNIC - Asia-Pacific Network Information Centre) from the IRR (AS36561 belongs to the American IRR, i.e. ARIN - American Registry for Internet Numbers) that manages the IP range of the hijacked
4.3 BGP hijack detection on the basis of data-plane information analysis

Manipulating the Internet routing infrastructure to hijack a block of IP addresses involves modifying the route taken by data packets so that they reach the physical network of the attacker. A tool called SpamTracer [3] has been developed to monitor the routes towards malicious hosts by performing traceroute measurements repeatedly for a certain period of time. IP-level routes are translated into AS-level routes using live BGP feeds. The motivation for monitoring data plane routes towards specific spamming hosts is to collect the route taken by data packets to reach these hosts as soon as a spam is received from them. By performing multiple measurements on consecutive days for a certain period of time, typically one week, routes towards a given host or network can be compared and analyzed in depth to find evidences of a possible manipulation by an attacker of the routing infrastructure.

Based on the data collected by SpamTracer, we try to analyze the routes to uncover abnormal routing changes and classify them as benign or malicious. First of all, routing anomalies are extracted from the raw traceroutes and BGP data. Routing anomalies are extracted independently for every monitored IP addresses and take into account all the data collected for an IP address during its monitoring time frame. A monitored IP address can also be involved in multiple anomalies. The anomalies can then be further analyzed using various features available, e.g., AS ownership data, IP hop geolocation, the length of the traced routes, etc. The objective of this analysis is to determine if suspicious routing behaviors are in fact benign, i.e., they result from a benign BGP practice [10] or a misconfiguration [28], or if they likely result from a malicious BGP hijack. We explain below why finding the malicious cases is complicated due to the lack of ground truth data to validate anomalies that may also be hijacks.

Below we describe the two approaches that have been developed to discover routing anomalies in the collected routes and identify among those anomalies the ones that possibly result from a malicious BGP hijack. The first approach is referred to as a top-
down approach as we start from known BGP hijacking techniques, i.e., known routing anomalies caused by BGP hijacks, and we attempt to find which set of routes match those symptoms. The second approach is referred to as a bottom-up approach as we start from the forwarding paths and we try to find suspicious routing patterns that might result from malicious routing events.

4.3.1 Extracting routing anomalies from BGP hijacking scenarios

In this approach to identify malicious BGP hijacks, we start from existing scenarios of BGP hijacking [24] for which we know the resulting routing anomalies. It then consists in searching for known anomalies in the collected traces. However, routing anomalies can also result from benign BGP routing practices, e.g., multi-homing of customer ASes by ISPs, aggregation of the announced IP prefixes by ASes, etc, or from non-malicious incidents due to misconfigurations or operational errors.

Every detected routing anomaly is analyzed using some heuristics further described below to determine if it is benign or malicious. However, the lack of ground-truth data which is only available through network owners feedback makes it complicated to determine if a routing anomaly is really benign or not.

Figure 4.30 depicts the classification of considered BGP hijacking scenarios. The different types of anomalies extracted from SPAMTRACER data follows the same classification. Below we describe (i) what the anomalies consist in, and (ii) what techniques are used to investigate them.

Figure 4.30: Top-down approach for analyzing BGP hijack scenarios.
4.3 BGP hijack detection on the basis of data-plane information analysis

4.3.1.1 Prefix Ownership Conflicts

A Prefix Ownership Conflict occurs when a block of IP addresses appear in the Internet routing infrastructure as originated by multiple ASes. This routing behavior can be the result of a hijacker advertising someone else’s IP space in order to attract traffic to or originate traffic from that IP space.

**Same Prefix.**

BGP hijacking can be done by advertising an IP prefix that is already advertised by a different AS. This technique creates a routing anomaly referred to as Multiple Origin AS (MOAS) as a single IP prefix is announced by multiple ASes, which is not expected to happen in the BGP protocol.

While such anomalies can be considered suspicious, they can also result from a benign BGP practice or configuration error in a router. The considered possible benign BGP practices are:

- **multi-homing**: an AS has multiple providers which can provide the Internet with a different view the IP space belonging to the AS;
- **sibling ASes**: ASes belonging to a single administrative entity, e.g., a large company or institution, may announce each other’s prefixes.

The following techniques are used to investigate those anomalies:

- **provider-customer relationship**: an ownership conflict involving ASes having a provider-customer relationship is classified as benign. The reason is that there is no motivation for any of them to hijack the traffic of the other. This scenario can result from multi-homing. The provider-customer relationships are retrieved from BGP AS paths and a third-party Internet topology [1];

- **ASes owner name similarity**: because a single administrative entity may have their ASes registered with slightly different owner names, those scenarios are uncovered by measuring the similarity between the name of the owner of each conflicting AS. When a prefix ownership conflict is analyzed, we use the Levenshtein distance function [2] to measure the similarity between the name of the conflicting ASes. Formally, the similarity between a set $S$ of AS names is defined as follows:

$$ASoSim = \max\{LevenshteinDist(i, j)\}, \forall i, j \in S.$$  

If the maximum value, i.e., the lowest similarity among AS names, is below 0.50, we conclude that the names of the conflicting ASes are similar enough to belong to the same administrative entity.
Different Prefix.
Tampering the ownership of a given IP prefix can also be carried out by advertising a slightly different IP prefix which can be more (resp. longer) or less specific (resp. shorter). This approach to hijack a prefix can be more or less efficient depending, among other things, on the other advertised prefixes close to the targeted one or the configuration of the attacker and the victim networks.

Similar to the MOAS conflicts, the anomalies involving different IP prefixes announced by conflicting ASes to control a given IP space can also result from benign BGP practice or configuration errors. The considered benign BGP practices are the following:

aggregation: an AS may decide to group multiple contiguous IP prefixes into a single IP prefix and advertise it from its own AS instead of advertising all individual IP prefixes. This practice aims at reducing the size of the routing tables at routers in a continuously growing Internet;

sibling ASes: ASes belonging to a single administrative entity, e.g., a large company or institution, may announce each other’s prefixes;

The techniques used to investigate those anomalies are the following:

provider-customer relationship: this technique is the same as the one applied to MOAS conflicts. Benign anomalies resulting from BGP aggregation can be found using the ”provider-customer relationship” technique when the aggregator AS is also a provider of the other AS(es) it conflicts with. This situation is then similar to multi-homing with aggregation performed by one of the providers;

ASes owner name similarity: this technique is the same as the one applied to MOAS conflicts. It is used to investigate anomalies possibly produced by sibling ASes;

4.3.1.2 BGP AS Path Anomalies

When the location of a network changes in the Internet AS topology as a result of a BGP hijack, the sequence of ASes traversed by BGP update messages from two different points is likely to change. While minor changes in the path are considered benign and due to the dynamic aspect of BGP routing, major changes can be considered suspicious and require further investigation to determine if they are indeed benign or if they result from a malicious manipulation of the routing infrastructure.

Next-Hop AS.
This anomaly consists in observing a certain number of different next-hop ASes, i.e.,
4.3 BGP hijack detection on the basis of data-plane information analysis

ASes next to the origin AS in an AS path, for a given origin AS and BGP collector. The detection threshold is currently set to 1 so every origin AS having more than one next-hop ASes triggers an anomaly. Although multi-homed ASes usually shows more than one next-hop AS, we decided to keep this value to be able to detect any change in the next-hop AS as hijackers can hijack an AS by inserting in the AS path their own ASN as the next-hop AS of the victim origin AS. This allows them to keep the correct origin AS and avoid any prefix ownership conflict.

**Complete AS path.**

These anomalies are uncovered by looking for AS paths for a given origin AS and BGP collector which are significantly different. Because changes in the BGP AS paths occur regularly, classifying every change as an anomaly may result in many false alarms. So we compute a similarity measure between AS paths using the Jaccard distance between every pair of AS paths. Usually, the sequence of ASes in an AS path starts from ASes located at or near the edge of the Internet, then traverses ASes in the core of the Internet (backbone ASes) and eventually terminates at ASes at or near the edge of the Internet. In this situation the set of traversed backbone ASes can vary which can result in different though legitimate AS paths. To avoid this situation, tier-1 ASes are removed from AS paths. This action of course makes the assumption that a tier-1 AS is not likely to perform malicious BGP hijacks. Formally, the BGP AS path anomaly can be expressed as follows:

$\text{aspa} = \min \left\{ \frac{|\text{asp}_{i,k} \cap \text{asp}_{j,k}|}{|\text{asp}_{i,k} \cup \text{asp}_{j,k}|} \right\} < t_{\text{aspa}}, \quad \forall i, j \in \{1, \ldots, n\} \quad \forall k \in \{1, \ldots, c\}$

where $\text{asp}_{i,k}$ is the $i^{th}$ AS path collected from the $k^{th}$ BGP collector and $t_{\text{aspa}}$ is the BGP AS path anomaly threshold. The BGP AS path anomaly is thus triggered whenever the set of AS paths from at least one BGP collector sufficiently differs. In the experiments performed so far we have chosen a value of 0.10 for $t_{\text{aspa}}$.

4.3.2 Extracting suspicious patterns in forwarding paths

This approach consists in searching for suspicious patterns in forwarding paths but which are not directly derived from known BGP hijacking scenarios. These suspicious patterns are extracted from (i) the observation of unexpected values in traceroute paths, e.g., a traceroute from a European source to a European destination having intermediate hops in the US, and (ii) metrics already used in previous works to extract routing anomalies from traceroute [47, 38]. These suspicious patterns of features may
not directly indicate that a hijack has occurred so they are meant to be correlated with
the anomalies uncovered using the top-down approach in order to increase our confidence
in the detection of a malicious hijack.

Figure 4.31 illustrates the classification of forwarding paths anomalies which are fur-
ther described here below. The different types of anomalies extracted from SPAMTRACER
data follows this classification.

Figure 4.31: Bottom-up approach to the analysis: traceroute anomalies.

4.3.2.1 Traceroute Destination Anomalies

The traceroute destination anomalies refer to suspicious values in features related to
traceroute metadata. The patterns considered as suspicious are described below.

*Host/AS reachability.*
The destination host/AS of the traceroute paths towards a given IP address is reach-
able (unreachable) for a certain number of days during the monitoring time frame and
suddenly becomes unreachable (reachable) and remains like this until the end of the
monitoring time frame. Note that the host and AS reachability anomaly consists in
two values computed individually for the host and AS levels. Formally, the host/AS
reachability anomaly is expressed as follows:

\[
ra = \begin{cases} 
  True & \text{if } \exists k : r_1 = \ldots = r_{k-1} \neq r_k = \ldots = r_n \\
  False & \text{otherwise}
\end{cases}
\]

where \( n \) is the number of consecutive traceroute instances towards a given host and \( r_i \)
is the host/AS reachability of route \( i \), i.e., \( r_i = true \) if we received replies to traceroute
probes from the destination host/AS, and false otherwise. This reachability anomaly can result from a major routing change in the path from the source to the destination of the traceroute which causes the destination host or AS to become (un)reachable. The AS reachability anomaly can indicate that the destination network has been blackholed as a result of a BGP hijack. This conclusion is reinforced if this anomaly happens with multiple hosts within a single AS.

**Hop count.**
The hop count or the length of a traceroute path is the value of the last TTL for which a reply to our probe IP packets has been received. The hop count anomaly consists in having a significant and sudden change in the hop count. This situation actually suggests that an important enough routing change occurred to permanently change the route taken by packets to reach the destination network. While not always accurate, this anomaly indicates that a routing change, possibly resulting from a BGP hijack, occurred. Formally, the hop count anomaly is expressed as follows:

\[
\text{hca} = \begin{cases} 
\text{True} & \text{if } \exists k : \min\{l_1 \ldots l_{k-1}\} - \max\{l_k \ldots l_n\} > t_{hca} \\
& \text{and } l_{k-1} > l_k \\
\text{True} & \text{if } \exists k : |\max\{l_1 \ldots l_{k-1}\} - \min\{l_k \ldots l_n\}| > t_{hca} \\
& \text{and } l_{k-1} < l_k \\
\text{False} & \text{otherwise}
\end{cases}
\]

where \(n\) is the number of consecutive traceroute instances towards a given host, \(l_i\) is the number of hops in route \(i\) and \(t_{hca}\) is the hop count difference threshold. Considering that most of the traceroute paths have a hop count between 20-25, we have chosen the threshold value of 10 to trigger a hop count anomaly in order to avoid false alarms resulting from highly dynamic though legitimate traceroute paths.

### 4.3.2.2 Traceroute Path Anomalies

The traceroute path anomalies refer to a suspicious change in the sequence of hops traversed by traceroute paths to a given destination host. More precisely, SPAMTRACER collects IP traceroute paths, map each IP hop to the AS(es) it belongs to and then enrich the path with different other information about each traversed IP hop or AS, e.g., the country of each IP hop and AS, the domain name of each IP hop, the Internet Routing Registry (RIR) of each AS, etc. Those features then allow to consider a traceroute not only as a sequence of IP addresses or ASes but also as a sequence of

---

*FP7-ICT-257495-VIS-SENSE* 115
countries, domain names, RIRs, etc. These alternate paths are leveraged in this detection of suspicious traceroute paths.

**AS-level path.**
The traceroute AS-level path anomalies consist in observing significant differences in traceroute AS paths towards a given host. The similarity between the AS-level paths is computed using the Jaccard distance function between each pair of AS-level paths. Formally, the traceroute AS-level path anomaly is expressed as follows:

$$
aspa = \min \left\{ \frac{|asp_i \cap asp_{i+1}|}{|asp_i \cup asp_{i+1}|} \right\} < t_{aspa}, \; i = 1, \ldots, n - 1
$$

where $asp_i$ is the AS-level path of the $i^{th}$ route and $t_{aspa}$ is the traceroute AS-level path anomaly threshold. The traceroute AS-level path anomaly is thus triggered whenever the set of AS-level paths towards a given IP address sufficiently differs. To cope with the frequently changing backbone ASes traversed, tier-1 ASes are removed from the AS paths. In our experiments we have chosen a value of 0.10 for $t_{aspa}$.

**Country-level path.**
This anomaly consists in extracting traceroute paths towards a given host exhibiting significant discrepancies in the sequence of traversed countries. The country-level path can be extracted from the ASes geolocation. The assumption behind this anomaly is that the countries traversed to reach a given destination from a given source is likely to remain constant even if routing changes occur at the IP or AS levels. Because the country view of a route from a source to a destination is a very high-level view, it does not capture geographically small routing changes and thus only highlights geographically major routing changes. The similarity between country-level paths is assessed using the Jaccard distance function and countries of tier-1 ASes are also removed from the paths. Formally, the traceroute AS-level path anomaly is expressed as follows:

$$
cpa = \min \left\{ \frac{|cp_i \cap cp_{i+1}|}{|cp_i \cup cp_{i+1}|} \right\} < t_{cpa}, \; i = 1, \ldots, n - 1
$$

where $cp_i$ is the country-level path of the $i^{th}$ route and $t_{cpa}$ is the traceroute country-level path anomaly threshold. In the experiments performed so far we have chosen a value of 0.20 for $t_{cpa}$. The traceroute country-level path anomaly is thus triggered whenever the set of country-level paths towards a given IP address sufficiently differs.
4.3 BGP hijack detection on the basis of data-plane information analysis

4.3.3 Investigating routing anomalies

In this section we present the experimental results of the analysis of five months of data, from April 2011 until August 2011, using the methodology described in sections 4.3.1 and 4.3.2. The data set thus consists in the enriched IP/AS traceroute measurements towards malicious hosts and the extracted routing anomalies. The table in Figure 4.32 provides some general information about the SPAMTRACER data set.

<table>
<thead>
<tr>
<th>Traceroute measurements</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td># traceroute paths</td>
<td>848,916</td>
</tr>
<tr>
<td># distinct destination IP addresses</td>
<td>239,907</td>
</tr>
<tr>
<td># distinct destination ASes</td>
<td>5,912</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Routing anomalies</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td># distinct IP addresses having anomalies</td>
<td>41,430 (17.27%)</td>
</tr>
<tr>
<td># distinct IP add. having unsolved Prefix Ownership Conflicts</td>
<td>444 (0.19%)</td>
</tr>
<tr>
<td># distinct IP add. having BGP AS Path Anomalies</td>
<td>22,851 (9.52%)</td>
</tr>
<tr>
<td># distinct IP add. having Traceroute Destination Anomalies</td>
<td>19,145 (7.98%)</td>
</tr>
<tr>
<td># distinct IP add. having Traceroute Path Anomalies</td>
<td>3,574 (1.49%)</td>
</tr>
</tbody>
</table>

Figure 4.32: Statistics about the SPAMTRACER data set.

From Figure 4.32 we can see that in the course of three months we have collected 848,916 traceroutes towards 239,907 distinct IP addresses which corresponds to an average of 5,442 new routes and 1,538 new IP addresses per day. Also we have observed a total of 5,912 distinct destination ASNs in that period. Regarding the anomalies extracted from the traceroute measurements, we can see that 17.27% of all monitored IP addresses are found to have at least one routing anomaly. If we now look at the IP addresses involved in at least one of the four main types of anomalies, we can observe that the Prefix Ownership Conflicts and Traceroute Path Anomalies only involve respectively 0.19% and 1.49% of the monitored IP addresses. BGP AS Path and Traceroute Destination Anomalies involve respectively 9.52% and 7.98% of the IP addresses. These simple statistics highlight the fact that a small subset of the traceroute measurements (17.27%) are involved in at least one routing anomaly.

The Prefix Ownership Conflicts represent the MOAS (multiple origin ASes and a
single prefix) and subMOAS (multiple origin ASes and multiple prefixes) conflicts that could not be solved using the techniques described in section 3. Without these rules, the number of Prefix Ownership Conflicts would be 1,420 (444 + 976). The table in Figure 4.33 shows how the different analysis techniques perform at solving conflicts.

<table>
<thead>
<tr>
<th>Analysis of solved Prefix Ownership Conflicts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solving technique</td>
</tr>
<tr>
<td>-------------------</td>
</tr>
<tr>
<td>Tier-1 (backbone) AS</td>
</tr>
<tr>
<td>Sibling AS</td>
</tr>
<tr>
<td>Provider to Customer (BGP)</td>
</tr>
<tr>
<td>Provider to Customer (Internet Topology)</td>
</tr>
<tr>
<td>Total solved</td>
</tr>
</tbody>
</table>

Figure 4.33: Analysis of Prefix Ownership Conflicts that could be solved using simple heuristics.

From Figure 4.33 we can see that around 95% of conflicts involve ASes with one being a provider of the other. The provider-to-customer relationships inferred from a third-party Internet topology [1] is able is explain most of the prefix ownership conflicts. Actually, due to the low computation cost of checking the inter-AS relationships from this Internet topology, this technique is applied before any other technique. Also, because the Internet topology includes routing information from BGP and from Internet Routing Registries (IRRs), it is able to catch most of the provider-to-customer relationships. Finally, we can see that 1.74% of conflicts involve a tier-1 AS and 2.66% of conflicts involve sibling ASes (by the name of the ASes owner).

Once routing anomalies have been extracted, it is necessary to further investigate them to determine if they result from a benign BGP practice or a possible misconfiguration error at a router. Because the anomalies characterize abnormal patterns at different fields of the data, e.g., BGP AS path, traceroute AS-level path, etc, multiple anomalies can be uncovered for a single monitored IP address. Then, an intuitive way of investigating suspicious cases is to start from those having the highest number of anomalies and progressively investigate cases with fewer anomalies. Figure 4.34(a) plots the CDF of the number of anomalies uncovered per IP address. We can see that if we want to investigate a reasonable number of cases we have to consider only those IP addresses that involve 5 or more anomalies. However, this only accounts for 0.30% of all IP addresses for which a routing anomaly has been extracted. If we assume that cases with
only one anomaly are not strong enough, we still have to look at not less than 9,606 cases having 2 or more anomalies. Thus, this approach does not seem to be the most appropriate one.

Another starting point for the investigation of anomalies is to assume that ASes involving the highest number of anomalies are automatically more suspicious. If we assume that a BGP hijack affects a whole AS, this approach allows to aggregate suspicious cases because we look at the AS level and not at the IP level. Figure 4.34(b) plots the CDF of the number of anomalies uncovered per destination ASN. In this case, we can easily investigate the top anomaly triggering ASNs having more than 50 anomalies. Unfortunately, this only covers 4.50% of all ASNs for which a routing anomaly has been observed. Moreover, there are too many cases having less than 50 anomalies to consider investigating all of them.

Figure 4.34: CDFs of the number of anomalies uncovered per target IP address and destination ASN.

From the plots we can see that investigating every case for which routing anomalies have been uncovered is not feasible. Also some anomalies have synergies with each others, e.g., the BGP AS path and traceroute AS-level path anomalies or the host/AS reachability and the hop count anomaly. Anomalies occurring at the same time also provide a stronger evidence that a major routing change occurred at this point in time. So, it is better to try to correlate anomalies with each others to increase the likelihood that investigated cases actually exhibit a strong abnormal routing behavior. Anomalies can thus be correlated according to (i) their type, e.g., a Prefix Ownership Conflict and (ii) if they occurred on the same day.

The table in Figure 4.35 shows how routing anomalies can be correlated and the resulting number of cases. First of all, we consider cases of IP addresses involved in
## Combining Routing Anomalies

<table>
<thead>
<tr>
<th>Combined anomalies</th>
<th># distinct IP addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix Ownership Conflicts</td>
<td></td>
</tr>
<tr>
<td>BGP AS Path Anomalies</td>
<td>122</td>
</tr>
<tr>
<td>Prefix Ownership Conflicts</td>
<td></td>
</tr>
<tr>
<td>BGP AS Path Anomalies (AS Path Deviation)</td>
<td>85</td>
</tr>
<tr>
<td>Prefix Ownership Conflicts</td>
<td></td>
</tr>
<tr>
<td>BGP AS Path Anomalies (AS Path Deviation)</td>
<td>15</td>
</tr>
<tr>
<td>Traceroute Destination Anomalies</td>
<td></td>
</tr>
<tr>
<td>Prefix Ownership Conflicts</td>
<td></td>
</tr>
<tr>
<td>Traceroute Destination Anomalies</td>
<td>50</td>
</tr>
<tr>
<td>Prefix Ownership Conflicts</td>
<td></td>
</tr>
<tr>
<td>Traceroute Path Anomalies</td>
<td>23</td>
</tr>
<tr>
<td>BGP AS Path Anomalies</td>
<td></td>
</tr>
<tr>
<td>Traceroute Destination Anomalies</td>
<td>2,967</td>
</tr>
<tr>
<td>BGP AS Path Anomalies (AS Path Deviation)</td>
<td></td>
</tr>
<tr>
<td>Traceroute Destination Anomalies</td>
<td>88</td>
</tr>
<tr>
<td>BGP AS Path Anomalies</td>
<td></td>
</tr>
<tr>
<td>Traceroute Path Anomalies</td>
<td>813</td>
</tr>
<tr>
<td>BGP AS Path Anomalies (AS Path Deviation)</td>
<td></td>
</tr>
<tr>
<td>Traceroute Path Anomalies</td>
<td>41</td>
</tr>
<tr>
<td>Traceroute Path Anomalies</td>
<td></td>
</tr>
<tr>
<td>Traceroute Destination Anomalies</td>
<td>867</td>
</tr>
<tr>
<td>Traceroute Path Anomalies</td>
<td></td>
</tr>
<tr>
<td>2 or more Traceroute Destination Anomalies</td>
<td>334</td>
</tr>
<tr>
<td>Traceroute Path Anomalies</td>
<td></td>
</tr>
<tr>
<td>2 or more Traceroute Destination Anomalies on the same day</td>
<td>242</td>
</tr>
</tbody>
</table>

Figure 4.35: Combination of routing anomalies and the number of distinct IP addresses for each combination.

both a Prefix Ownership conflict and a BGP Path Anomaly. Because a change in the origin AS of an IP block likely implies a significant change in the BGP AS path, this combination of the two anomalies makes sense. In this case, we end up with 122...
4.3 BGP hijack detection on the basis of data-plane information analysis

anomalous cases which accounts for about one fourth of all Prefix Ownership Conflicts we had before (444). If we further constraint the set of cases to those having an AS Path Deviation as a BGP AS Path Anomaly, i.e., a significant change in the complete AS path, we end up with 85 cases which have to be investigated. We now consider the situation where the change of the origin AS of an IP block not only modifies the BGP AS path but also significantly modifies the length of the route or the reachability of the monitored hosts within a specific IP block or the complete AS. Namely, we extract cases having a Prefix Ownership Conflict, a BGP AS Path Anomaly and a Traceroute Destination Anomaly. We then end up with 15 cases to investigate. In this situation, the Hop Count anomaly may indicate that the length of the route to the new origin AS has significantly changed from the length of the route to the previous origin AS. The host/AS reachability anomaly also indicates that a change in the destination network or in the traversed networks suddenly modified the host/AS reachability.

When combining the Prefix Ownership Conflicts with the Traceroute Destination Anomalies, 50 cases match the given constraints.

If we now consider cases involving a Prefix Ownership Conflict and a Traceroute Path Anomaly, we have a total of 23 cases to investigate. In fact, the routing behavior characterized by this combination of anomalies is similar to the one involving a Prefix Ownership Conflict and a BGP AS Path Deviation (85) and as a consequence they both share common cases.

When considering cases involving a BGP Path Anomaly we can see if some of them also exhibit a Traceroute Destination Anomaly. In our data set, not less than 2,967 cases match these constraints. If we enforce that cases have at least a BGP AS Path Deviation, i.e., they cannot have only a Next-Hop AS Anomaly, we end up with 88 cases to investigate. These cases describe an interesting routing pattern that correspond to a major change detected in the BGP AS path combined with a significant change observed in the traceroute paths length or in the reachability of the destination host or AS. This routing pattern could very well be the result of a hijacker putting itself as the next-hop AS thus hijacking the complete victim AS without creating any prefix ownership conflict. In section 4.3.5 we describe a validated case of a BGP hijacking spammer that actually exhibits this routing pattern. Finally, this routing pattern could also correspond to a hijacker performing a Man-In-The-Middle attack thus significantly modifying the AS path in order to be able to attract traffic destined to the victim network and forward it back to him. In that case, we would expect to observe a change in the traceroute path length rather than in the host/AS reachability as the objective of the hijacker here is to avoid blackholing the victim network.

Also, we have 813 cases that are found to have both a BGP AS Path Anomaly and a Traceroute Path Anomaly. If we consider only those exhibiting an AS Path Deviation,
we end up with 41 cases.

So far, we have combined anomalies extracted from the data plane and the control plane. We now consider cases having a Traceroute Path Anomaly and a Traceroute Destination Anomaly. Without applying any filtering, 867 cases match the constraints. As the traceroute AS-level paths may suffer from missing hops or may have not reached the destination, we can add another constraint and consider only the cases having two or more Traceroute Destination Anomalies. We then end up with 334 cases. To further reduce the number of cases to analyze, we can keep only the IP addresses for which at least two Traceroute Destination Anomalies occur at the same time. Some of the 242 resulting cases actually belong the validated hijacking spammer case described in section 4.3.5.

Finally, by taking the most constrained sets from each combination of routing anomalies, we are left with 353 different suspicious cases that we have to further investigate to determine if they are benign or malicious. This set of cases is the union of all sets of cases involved in combined anomalies. In the next section we present the analysis of a validated hijacking spammer case study which involves some IP addresses from the set of 353 most suspicious ones.

4.3.4 Analysis of Suspicious BGP Anomaly

In the investigation of the different suspicious cases uncovered by combining multiple routing anomalies, one special case caught our attention. The case involves a network represented by its AS whose traffic appeared to have been hijacked by another AS.

SpamTracer monitored one IP address in the alleged hijacked network during six days in August 2011. From the data collected for this IP address, six routing anomalies were extracted and reveal (i) a Traceroute Destination Anomaly (destination AS reachability), (ii) Traceroute Path Anomalies, (iii) BGP Path Anomalies (AS Path Deviation) and, (iv) a BGP Origin Anomaly (subMOAS conflict). Also, all these anomalies occurred on a single day.

The six routing anomalies uncovered for these traceroutes which occurred on a single day confirm that a major routing change occurred. In this case, a change in the origin AS of the destination IP prefix occurred at the same time as a change in the ASes traversed both in the traceroutes and in the BGP AS paths. The BGP Origin Anomaly has been marked as benign by SpamTracer because the two conflicting ASes include the AS owning the network and the AS of one of its providers. Before the routing change, this provider advertised its customer IP space in a aggregated IP prefix.

The unreachability of the destination AS after the change can be observed on day four and correlated with the Traceroute Destination Anomaly seen on the same day. Also,
4.3 BGP hijack detection on the basis of data-plane information analysis

the last AS that could be reached by traceroutes after the change appears in the BGP AS paths as the direct upstream provider of the new origin AS. This provider-customer relationship could not be officially explained. Also, we now that hijacking a network can be performed by advertising it with a correct origin AS and by putting the attacker AS as the next-hop AS.

After investigation, it turns out that the next-hop AS belongs to a company providing DDoS mitigation as service by sink holing the attacking traffic of their customers. The analysis suggests that either the security company redirected the traffic of their customers AS because they were under attack or the security company may sometimes act as an ISP for some companies AS to easily protect them from undesired traffic. Given the fact that the security company advertised the route in BGP for at least three days, we believe that it actually acted as an ISP for its customer.

Although we have detected abnormal routing changes regarding this network, it is quite difficult to validate these anomalies as a real hijack case without the feedback from the owner of the network.

4.3.5 Link Telecom BGP Hijack

In the investigation of the different suspicious cases uncovered by combining multiple routing anomalies, another special case caught our attention. In more detail, as it has already been discussed in Section 4.2.3.2 on August 20\textsuperscript{th}, the network administrator of the Russian telecommunication company “Link Telecom” complained on the North American Network Operators’ Group (NANOG) mailing list that his network had been hijacked by a spammer \cite{2}. On both August 25\textsuperscript{th} and August 29\textsuperscript{th}, changes were observed in the routes towards AS31733 advertised in BGP. These changes were the result of the owner regaining control over his network. SpamTracer collected data about this event at the same period the owner regained control over his network. The routing anomalies extracted from the traceroutes and BGP routes uncovered an abnormal routing behavior that we describe below.

SpamTracer monitored 135 IP addresses in the AS31733 in the five months of data during August 2011. From the data collected for these IP addresses, 21 of them triggered at least one routing anomaly. The anomalies extracted include (i) Traceroute Destination Anomalies, (ii) Traceroute Path Anomalies and, (iii) BGP AS Path Anomalies.

The investigation of the different cases further indicates that the identified routing behavior is abnormal. To illustrate this, we can look at the following examples of (i) a case exhibiting a combination of Traceroute Destination Anomalies and Traceroute Path Anomalies and, (ii) a case exhibiting a combination of Traceroute Destination Anomalies and BGP AS Path Anomalies (AS Path Deviation).
**Case 1.**

Figure 4.36 illustrates the first case exhibiting Traceroute Destination Anomalies and Traceroute Path Anomalies. There is indeed a significant deviation in the Traceroute AS-level Path between the first traceroute (left) and the six following traceroutes. Also, in the first traceroute the destination host and AS could be reached (node (1)) while the six following traceroutes failed to reach the destination host or AS (nodes (2) and (3)).

Figure 4.36: **Link Telecom (AS31733) Hijack**: example of a suspicious case having Traceroute Destination Anomalies and Traceroute Path Anomalies. The two different paths illustrate the Traceroute Path Anomaly. The colored nodes show the last hop of the traceroutes. In one traceroute, the destination host and AS could be reached (left path and node (1)) while the following traceroutes failed to reach the destination host and AS (right path and nodes (2) and (3)).

**Case 2.**

Figure 4.37 illustrates the second case exhibiting Traceroute Destination Anomalies and BGP AS Path Anomalies. There is really two AS paths trees rooted at AS31733. One branch goes through the next-hop AS12182 and the other one goes through the next-hop
4.3 BGP hijack detection on the basis of data-plane information analysis

AS43659. Similar to case 1, for the first traceroute the destination host and AS could be reached (node (1)) while the six following traceroutes failed to reach the destination host and AS (nodes (2) and (3)).

Figure 4.37: Link Telecom (AS31733) Hijack: example of a suspicious case having Traceroute Destination Anomalies and BGP AS Path Anomalies. The BGP AS paths graph shows two main AS paths trees rooted as AS31733 with one branch going through AS12182 and the branch going through AS43659. The colored nodes show the last hop of the traceroutes. In one traceroute, the destination host and AS could be reached (left path and node (1)) while the following traceroutes failed to reach the destination host and AS (right path and nodes (2) and (3)).

These illustrated cases show that abnormal routing behaviors can indeed be uncovered from the combination of routing anomalies extracted from traceroute and BGP data. The collected traceroutes from a vantage point (VP) in France towards the hijacked network are illustrated in figure 4.38. During the hijack traffic from the vantage point in France and destined to AS31733 Link Telecom goes to the hijacker network (Fig. 4.38: route VP $\rightarrow$ 1 $\rightarrow$ 2) through the direct provider AS12182 Internap (Fig. 4.38: node 1). The last IP hop of the traceroutes, which in this case corresponds to the destination host, is also likely located in the USA (Fig. 4.38: (2)).

After the hijack traffic goes towards Russia (Fig. 4.38: route VP $\rightarrow$ 3 $\rightarrow$ 4) where
the legitimate owner of AS31733 resides (Fig. 4.38 (4)). The paths of IP hops and ASes traversed by the traceroutes are completely different from those during the hijack which suggests a major modification in the routes to AS31733 advertised in BGP. The fact that after the hijack we did not receive any reply for traceroute probe packets sent to the destination network is probably due to ICMP filtering or rate limiting rules in the traversed networks of the new route.

![Link Telecom (AS31733) Hijack](image)

Figure 4.38: **Link Telecom (AS31733) Hijack**: visualization of the traceroutes from a vantage point (VP) in France during (AB) and after (CD) the hijack. Nodes (2) and (4) indicate the location of Link Telecom network during and after the hijack respectively. Node (1) indicates the direct upstream provider of AS31733 during the hijack and node (3) indicates the last hop of traceroutes that could not reach the AS31733 after the hijack.

This hijack case is further described in [37]. We know that the hijack began in April. Although the prefix appeared to be announced by the correct origin AS, i.e., AS31733, it was routed via a US ISP called Internap (AS12182). During the period the network was under the control of the spammer, spam messages were received by Symantec.cloud honeypots and some IP addresses were monitored by SpamTracer. The hijack lasted for five months from April 2011 until August 2011. The hijacking technique employed by the spammer consists in (i) finding a block of IP addresses not currently announced in the public Internet and (ii) have it routed via an ISP possibly using a fake proof of ownership of the network.

This case study presents a validated case of a hijacking spammer that managed to steal someone else’s IP space and sent spam from it. Although we have detected abnormal routing changes regarding this victim network, it is quite difficult to validate
these anomalies as a real hijack case without the feedback from the owner of the victim network.

4.4 Exploitation of heterogeneous sources of information for the BGP activity

As it becomes apparent from the analysis above, control-plane and data-plane methodologies follow two distinct approaches for realizing the ultimate goal of performing the as accurate as possible detection and attribution of BGP anomalies with the massively voluminous set of the overall BGP events. In this respect, instead of competitively implementing control-plane and data-plane analysis, it would be highly beneficial to amalgamate them in a complimentary manner, so as to make virtue of their combined merits. Being more specific, since control-plane and data-plane techniques offer two different as well as totally independent perspectives of the same BGP phenomena, they can be utilized, either in parallel or sequentially, in both the detection and the attribution phase:

- Optimizing the discriminating capability of the BGP anomaly detection mechanism (specificity and sensitivity of the decision support module) for guaranteeing the effective filtering of the BGP activity in terms of its anomalous nature, i.e. minimizing any false alarms (false positives) without disregarding any abnormal cases (elimination of the false negatives).
  - The BGP anomalies that are traced by control-plane monitoring on the sole basis of the raw BGP data can be returned to the data-plane mechanism, so as to acquire a spherical view of the actual impact of the low-level BGP activity upon the real-world Internet operation. Moreover, such a control-plane information would allow the data-plane mechanism to focus solely on prefixes and/or ASes of special interest and thus the in-depth investigation of specific cases is facilitated instead of superficially studying the whole bulk of events.
  - Vice-versa, incidents captured via the data-plane analysis can be enhanced with the results of the control-plane module, since additional evidence of suspicious BGP activity for an AS/prefix that has already caught the attention of the data-plane approach would provide the solid ground for decisively determining the malicious nature of the specific event.

- Control-plane and data-plane methodologies provide information regarding different attributes of the captured BGP disturbances. Hence, the analyst is offered
with a peer insight to the underlying root causes of each phenomenon as well as to its eventual effect upon the Internet operation.

Notwithstanding, detecting suspicious events still indicates only possible instances of prefix hijacking. Unfortunately, attack signatures for prefix hijacking most often also match standard routing practices such as traffic engineering. As a result, the final decision on the hijacked state of a network should always be made after further in-depth analysis of the positive cases coming from the detection techniques.

Unfortunately, BGP data on its own is most often not enough to be able to classify a suspicious routing event as a prefix hijacking attack or as a false positive due to a legitimate-but-peculiar routing practice. Usually a network operator can distinguish between the two with a given certainty, but only the prefix owner knows for sure. Data external to BGP, such as whois records, RIRs’ object lists and routing registries, DNS zone files, ASN to country codes lists etc., are helpful to make a decision: they bring semantic information about the observed network. This semantic information is not easily analyzable by a machine but brings an added dimension of information to a network operator. More importantly, the ability to see the evolution of these external sources of information along with the evolution of the routing state could bring an intrinsic sight on the evolution of a given network. For example, in the particular case of the Link Telecom hijack presented earlier, a view of the whois evolution would show:

1. the expiration of the domain name `link-telecom.biz`

2. the re-registration of that same domain name under a different registrar and registrant.

The RIPE routing registry would show that Internap is not allowed to announce prefixes for Link Telecom. While none of these facts are, on their own, discriminatory, their overall combination, with the peculiar BGP route choice, can only lead to the conclusion that something obscure is going on.
Conclusions

Deliverable 3.2 presents novel methodologies for providing solid solutions to the multi-dimensional problem of the prompt as well as accurate detection and attribution of the anomalies that take place within the whole variety of the topologically and semantically disparate segments of the Internet infrastructure and operation. To this end, initially, the most appropriate features and proximity measures are defined, so as to optimally fit to the characteristics and satisfy the requirements of the most prominent cases of network anomalies. As a matter of fact, besides the elaboration of existing features and proximity measures, novel features are also extracted, so as to acquire the most thorough possible view of the evolution of network status and dynamics in time, along with a profound insight to both the root causes of any disturbance phenomena and their impact upon the normally expected network functionality.

Upon this solid background, an anomaly detection framework for network and threat monitoring is developed. The proposed methodology is based on the graph theory and it allows the efficient analysis of voluminous events of abnormal behavior that are described by multiple cross-correlated features. The research deals with both the investigation of anomalies within a static graph (snapshot of the network status) and the examination of the graph’s evolution in time, i.e. comparison between consecutive snapshots of the network status.

Furthermore, particular emphasis is being laid upon the development of efficient anomaly detection and attribution techniques for the special case of the BGP activity, due to the profound interest it presents regarding the Internet operation. More concisely, the hereby introduced mechanisms deploy both control-plane and data-plane approaches, so as to acquire an holistic perspective of the complicated BGP functionality and hence to optimally discriminate among the overwhelming bulk of the continuous routing alterations. To this end, the control-plane methodology primarily exploits the geospatial correlation of the BGP behavior as well as the inferred inter-AS relationships, while the data-plane technique focuses on the relationships between anomalous BGP events and other cases of malicious cyber activity.
Bibliography


