Visual Analytics for BGP Monitoring and Prefix Hijacking Identification

Ernst Biersack[1], Quentin Jacquemart[1],
Fabian Fischer[3], Johannes Fuchs[3], Olivier Thonnard[2],
Georgios Theodoridis[4], Dimitrios Tzovaras[4], and Pierre-Antoine Vervier[1,2]

Abstract—The control plane of the Internet relies entirely on BGP as inter-domain routing protocol to maintain and exchange routing information between large network providers and their customers. However, an intrinsic vulnerability of the protocol is its inability to validate the integrity and correctness of routing information exchanged between peer routers. As a result, it is relatively easy for people with malicious intent to steal legitimate IP blocks through an attack known as *prefix hijacking*, which essentially consists in injecting bogus routing information into the system to redirect or subvert network traffic.

In this paper, we give a short survey of visualization methods that have been developed for BGP monitoring, in particular for the identification of prefix hijacks. Our goal is to illustrate how network visualization has the potential to assist an analyst in detecting abnormal routing patterns in massive amounts of BGP data. Finally, we present an analysis of a real validated case of prefix hijacking, which took place between April and August 2011. We use this hijack case study to illustrate the ongoing work carried out in VIS-SENSE, a European research project that leverages *visual analytics* to develop more effective tools for BGP monitoring and prefix hijack detection.

Index Terms—Network Visualization Methods, Prefix Hijacking, BGP Monitoring.

1 INTRODUCTION

THE Internet is partitioned into tens of thousands of independently administered routing domains called *Autonomous Systems* (ASes), belonging to different organisations. The *Border Gateway Protocol* (BGP) is the de facto inter-domain routing protocol that maintains and exchanges routing information between ASes.

BGP was designed based on the implicit trust between all participants. The protocol by itself does not provide any built-in mechanism to authenticate or validate the routes propagated through the system. Therefore, any AS can potentially announce *bogus* routes into the system, which can eventually trigger large-scale Internet anomalies, such as the *YouTube Hijack* incident [1]. This intrinsic weakness of the protocol can lead to *prefix hijacking* incidents, which consist in redirecting Internet traffic by tampering with the control plane itself.

This paper gives a brief survey of visualization tools that were specifically designed for BGP monitoring and prefix hijack detection (Section 2). Then, Section 3, presents the ongoing work done in VIS-SENSE, a European research project that aims at developing *visual analytics* tools to improve the efficiency of BGP monitoring and prefix hijacking detection. To this end, the analysis is focused on the Link Telecom hijack that took place between April and August 2011 and which comprises one of the very few validated cases of prefix hijacking.

For the sake of completeness, a short overview of BGP concepts and prefix hijacking is initially provided in the remainder of this introductory Section.

1.1 BGP Overview

Interconnected ASes need to be able to exchange network reachability information. Unlike intra-domain routing protocols that route packets through the shortest possible network path, BGP lets each AS define its *routing policy*, which is

- [1] *Eurecom, Sophia Antipolis, France*
- [2] *Symantec Research Labs, Sophia Antipolis, France*
- [3] *University of Konstanz, Germany*
- [4] *Centre for Research and Technology Hellas,Information Technologies Institute (CERTH-ITI), Greece*

Manuscript received ...

then enforced on each BGP router by filtering on incoming and outgoing update messages [2].

BGP updates are exchanged between BGP-enabled routers to announce or withdraw network addresses reachable through them. A BGP update mainly contains the destination network address, the AS path to the destination, and preference indicators. The *AS path* is a sequence of AS identifiers $a_{n-1}, \ldots, a_1, a_0$ that includes all ASes between the source AS (a_0) of the prefix (called *origin AS*) and the recipient AS (a_n) of the update message. The AS path is built sequentially: when a router exports a route to a neighbour, it *prepends* its unique AS number to the path it has received.

Due to the application of the routing policy, BGP uses a particular mechanism to select the preferred route. When multiple prefixes overlap, BGP uses the *longest prefix match* rule, *i.e.*, the most specific announcement matching the destination address is the one to be used for forwarding. For same-length prefixes, BGP uses a route selection process of many variables. They include the length of the AS path, which can be influenced by factors external to the router's configuration.

1.2 Prefix Hijacking

Prefix hijacking is the act of absorbing (part of) the traffic destined to another network through the propagation of erroneous BGP routes.

By hijacking the traffic of another AS, an attacker may black-hole the victim's network (DoS attack), impersonate the victim by stealing its network identity or eavesdrop on the victim's traffic [3].

Prefix hijacking can be performed in several ways. The attacks are usually based on the following key elements [4]. The hijacking AS *claims ownership* of a prefix and starts announcing it. If the victim is also announcing the same prefix, a *Multiple Origin AS* (MOAS) conflict becomes the side effect of the attack because different ASes are announcing the same prefix. Some routers will prefer the hijacked route to forward the traffic because they are topologically closer (and thus, the AS path is shorter, which is favoured by BGP). The attacker can avoid this MOAS conflict by tampering with the AS path. The victim's AS remains as the origin, and the attacker's AS is further down in the AS path. This effectively creates a fake link in the network. Furthermore, a very efficient way of hijacking a network is to announce subnets of the victim's prefix. Because of the longest prefix match rule, the traffic is immediately forwarded to the attacker. Alternatively, by announcing a less specific prefix, the attacker can take ownership of IPs that are left unannounced by the AS that they have been assigned to. Finally, private or unassigned prefixes can be also announced.

1.3 The Link Telecom Hijack Case

On August 20th, 2011, the network administrator of Russian telecommunication company Link Telecom complained to the North American Network Operators' Group (NANOG) mailing list [5] that his network had been hijacked by a spammer. After investigation, it turned out that a spammer had indeed been hijacking AS31733 (Linktel) for five months from April to August 2011. While this network was hijacked, the stolen IP addresses were apparently used to send spam emails, as observed by spamtraps maintained by Symantec.cloud which provides email, web and instant messaging security services. The spammer carried out the hijack by providing the US ISP Internap (AS12182) with a fake proof of ownership of the Linktel network, which then allowed them to advertise the victim's prefixes using the same origin ASN. It is noteworthy that by the time the network was stolen, the victim company had suspended its activity, thus leaving its blocks of IP addresses *unused* and making them a target of choice for the hijacker.

A more detailed analysis of this hijack case is provided in Section 3.

1.4 Detecting Prefix Hijacking

Techniques for detecting prefix hijacking can be divided into two distinct categories: those based on the *control plane*, *i.e.*, the detection signature depends on information found in a router's routing table and/or messages exchanged with this router; and those based on the *data plane*, *i.e.*, the detection signature is based on the way packets actually flow between an observer and the source. RIPE RIS[1], among others, offers binary dumps of BGP messages exchanged by their routers, as well as snapshots of their routing tables to perform control plane analysis.

Detection techniques from the control plane involve the creation of a model that represents the normal, expected behaviour of a network. Whenever the current view of the network differs from

[1] http://www.ripe.net/ris

the model, an alert is raised. The complexity and accuracy of the model is then the key element to a good detection scheme.

Detection techniques from the data plane involve active probing of the network topology and/or available live hosts in the monitored network. The core idea is that when a hijacking takes place, significant topology changes should be observed, while the victim network is different from the hijacking network. The way these elements are measured, as well as their diversity, ensures a good detection.

For an external observer (*i.e.*, who does not own the monitored network), the main problem in detecting prefix hijacking is to validate the attack. Indeed, while very peculiar activity can sometimes be observed, only the network's owner knows the ground-truth. As a result, it can be tricky to differentiate a hijack from a legitimate traffic engineering practice. Moreover, the number of different networks on the Internet, as well as the time and network resources necessary to analyze them, prohibits systematic use of detection techniques based on the control plane.

2 Visualization of BGP Data

Visualization helps in many fields related to network security to get more and better insights. For example, much research has been successfully conducted in the area of visualizing network traffic. Surprisingly, only few prototypes were developed for the analysis of BGP related data or prefix hijacking events. However, visual analysis tools can support an analyst in finding, understanding, and confirming BGP hijacks and other anomalies in routing data, which cannot always be identified or confirmed by fully-automated algorithms.

In Table 1 an overview of popular visualization systems for BGP-related analysis tasks is presented, including mainly two different groups of systems. *BGPlay* [6], [7], [8], *BGPviz*[2], *Link-Rank* [9], *VAST* [11], *TAMP* [10] and *Event Shrub* [12] focus on a high-level AS view, while *ELISHA* [13] and *PGPeep* [14] provide low-level IP views. Some other tools, like *BGP Eye* [15] and *RIPEstat*[3] have multiple views to address specific aspects of the data.

2.1 Systems with High-Level AS Overviews

BGPlay and RIPE's *BGPviz* use a node link diagram to present an intuitive high-level AS view to show the autonomous systems and their connections with each other. *BGPlay* was improved by integrating a topological map [7] to represent hierarchies. Both tools provide timelines, which can be used to focus on interesting time intervals. Animation helps to present routing changes and route flappings. Fig. 1 shows the situation for one of the hijacked prefixes from Link Telecom before and during the hijack using *BGPlay*. Several colored lines describe the advertised routes to the selected prefix, which originated in the red-colored circle representing AS31733. This shows that all the routes to AS31733 go through AS12182 during the hijack.

While this interactive *animated* visualization is quite intuitive for the visual exploration of historic events in BGP data, the analyst must have a clear idea of which time span and which prefix is relevant for the analysis. Compared to static representations, animation is time-consuming and the analyst needs to focus on many changing aspects of the graph. The main benefit of such an animated view is to present a known case, but not necessarily to identify a suspicious event.

Link-Rank is a similar system, because it also uses a graph based representation of the ASes. Additionally, the edges are weighted according to the number of routes and changes between the different AS links. With this supplementary information the analyst can observe routing changes and link instabilities. Activity plots further help to focus on the most suspicious update bursts, which might indicate prefix hijacking resulting in major route changes.

Another tool, focusing on animated node link diagrams, is *TAMP*. It displays a pruned graph for the network topology, an animated clock with controls to show and manipulate the time of the current state of the graph and another detailed chart to present the events belonging to a selected edge. Compared to other tools, strong statistics are included to detect correlations between BGP events at any time scale. The algorithms can be enriched with additional data sources like traffic flows or router configuration files to improve the diagnosis of BGP anomalies. The combination of statistical methods, data enrichment and visualizations helps to detect prefix hijacking, route flapping and anomalies in long time periods.

[2] http://www.ris.ripe.net/bgpviz/
[3] https://stat.ripe.net/

Tool	Level of Detail	Visualization Techniques	Additional Features	Use Cases
BGPlay [6] [7] [8]	high-level AS view	node link diagram	animation, timeline, open for public usage	route flapping, routing changes, presenting suspicious events
Link-Rank [9]	high-level AS view	rank-change graph	activity bar	observing routing changes, link instabilities, prefix hijacking
TAMP [10]	high-level AS view	node link diagram, animated clock, timeline, charts	animation, novel correlation technique, combination with statistics	anomalies in long time periods, route flappings
VAST [11]	high-level AS view	3D display, quad-tree, octo-tree topology visualizations	filtering techniques	explore AS connectivity, identify critical infrastructures, prefix hijacking
Event Shrub [12]	high-level AS view	timelines with glyphs	integrated combination of automated data analysis	anomaly detection based on historic data
ELISHA [13]	low-level IP view	2D quad-tree prefix visualization, 3D view for details	animation, event classification	BGP Origin AS changes, MOAS conflicts
PGPeep [14]	low-level IP view	prefix visualizer using line-based visualization	timeline, tag cloud	reveal potential router misconfiguration, route flapping, prefix hijacking
BGP Eye [15]	multiple views	node link diagram, 3D display, matrix, charts	event classification, clustering, alternative graph layouts	routing change detection, prefix hijacking
RIPEstat	multiple views	charts, timelines, maps	web-based, open for public usage	getting historic details for AS or specific IP prefixes

TABLE 1: Overview of popular visualization systems for BGP-related analysis tasks.

VAST uses 3D visualizations to show topological connectivity between different ASes. Interaction possibilities like rotating, zooming or panning help to explore the 3D space. Furthermore, different filter techniques provide the possibility to focus on certain aspects of the data. The tool allows mainly to visually explore AS connectivity and to identify critical infrastructures. Within the visualization update bursts of specific ASes become visible, which can be an indicator for occurred prefix hijacking.

The last tool for high-level analysis is *Event Shrub*. An automatic anomaly detection algorithm is combined with a tightly coupled visual timeline. Pie charts used as small glyphs are plotted to this timeline to represent the different instability events. This representation helps to identify deviations from normal behavior.

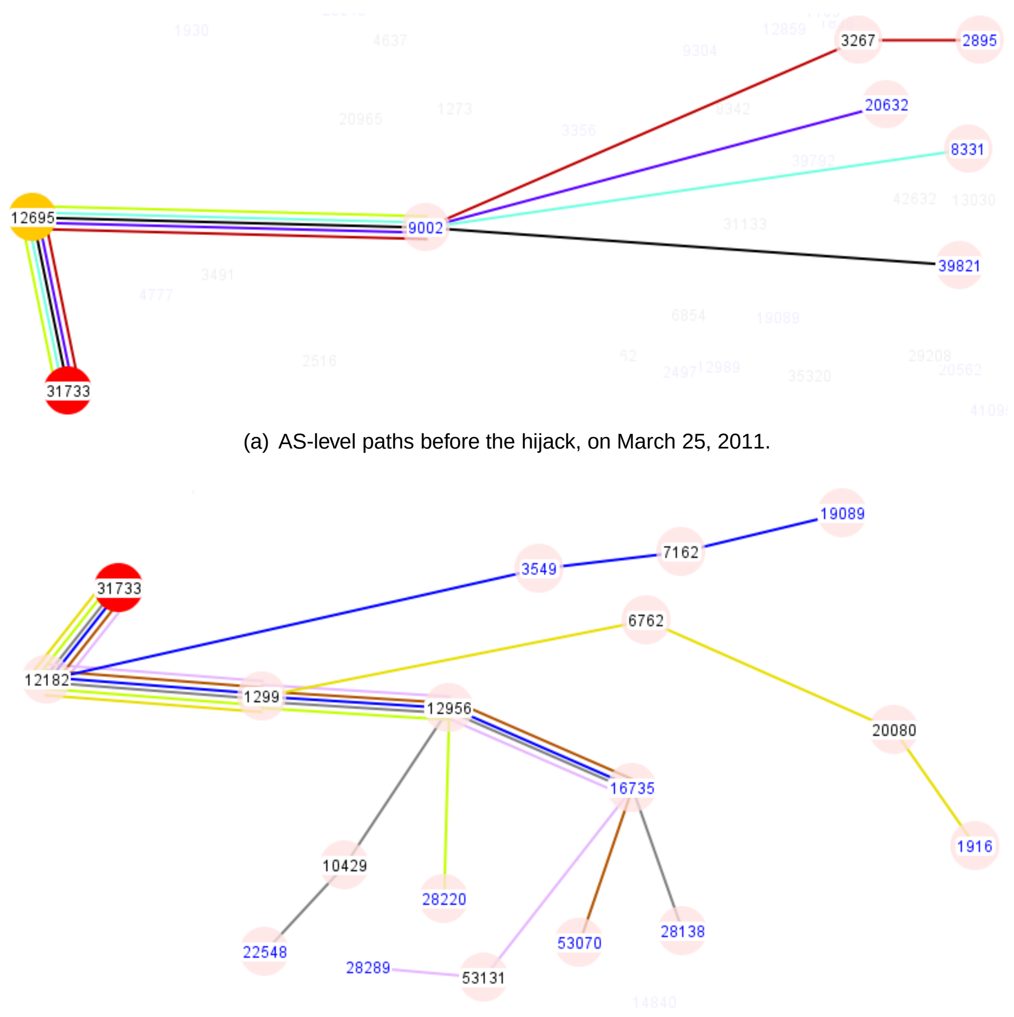
2.2 Systems with Low-Level IP Views

ELISHA makes use of a pixel-based approach. The screen is filled with colored pixels, each representing single IP addresses. They are laid out according to their corresponding IP range. The BGP messages are classified in different event types. Visually mapping this information to color provides a scalable and space-filling overview visualization as seen in Fig. 2. With this animated visualization, analysts are able to detect, explore and visually present routing anomalies and MOASes. Overall, *ELISHA* provides an IP prefix centered approach without representing the overall AS routing paths.

An overview visualization focusing on textual content instead of temporal aspects is tag clouds, which is a key component in *BGPeep*. The different tags represent the names of autonomous systems. The size of the tags depends on the number of update messages for the specific AS. To make use of the hierarchical structure of IP addresses and to provide a more IP-space centered view, horizontal parallel axes are used by *BGPeep*. The first axis represents the AS number; the other four, one byte of an IP address. An update message is represented by a line intersecting the axis at the appropriate positions. Using this visualization technique, it is possible to reveal potential router misconfiguration, route flapping or multiple advertised prefixes.

2.3 Systems with Multiple Views

BGPEye combines data mining techniques and visualizations using multiple views. Update messages are classified and clustered. An overview visualization displays the activity among different ASes in a graph layout. Additionally, a 3D matrix with connecting lines, reveals more detailed information about a single AS. Therefore, prefix hijacking or changes in the overall routing behavior can be detected.



(a) AS-level paths before the hijack, on March 25, 2011.

(b) AS-level paths during the hijack, on May 28, 2011.

Fig. 1: Visual exploration of the Link Telecom hijack event with BGPlay. Colored lines show the different route advertisements. Animation is used to interactively show the path changes.

RIPEstat is a web interface, which is continuously improved, with a variety of different charts to show historic activities or different distributions related to the selected AS or IP prefix (see Fig. 3). These visualizations do not present a general overview to detect anomalies, but help to investigate individual cases.

Overall most visualization tools show the routing changes mainly as animation, which is appropriate for visually presenting a particular known event. For exploratory analysis, animation is not entirely satisfying. Therefore, other techniques have to be investigated in order to improve the temporal analysis of MOASes and path changes. To combine the strengths of scalable and informative approaches for long-term analysis, the tight coupling of different techniques seems to be promising. This is a direction being explored in the VIS-SENSE project.

3 Case Study: Visual Analysis of the Link Telecom Hijack

In recent years, some reports have described an emerging threat referred to as the *fly-by spammers* phenomenon. In this attack scenario, spammers hijack blocks of IP addresses to send spam from non-blacklisted IP space in an effort to avoid current spam filters. This Section shows how visualization

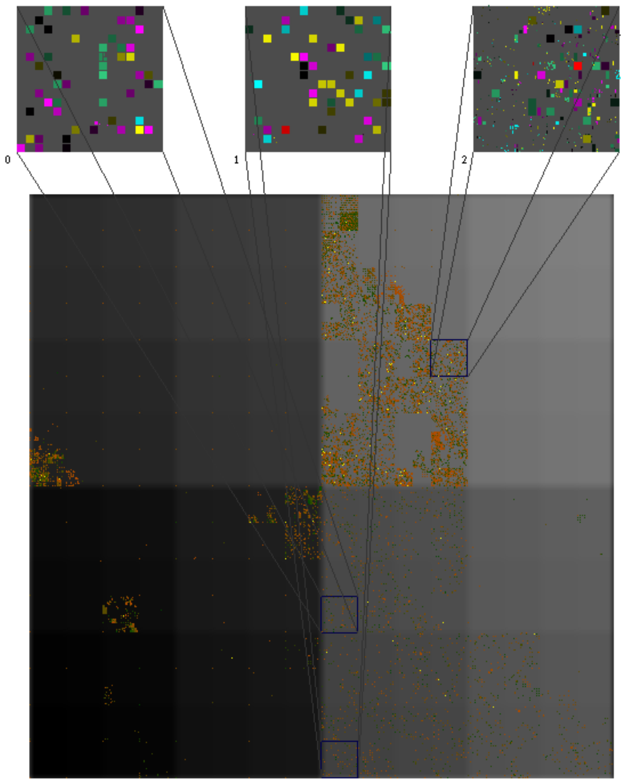
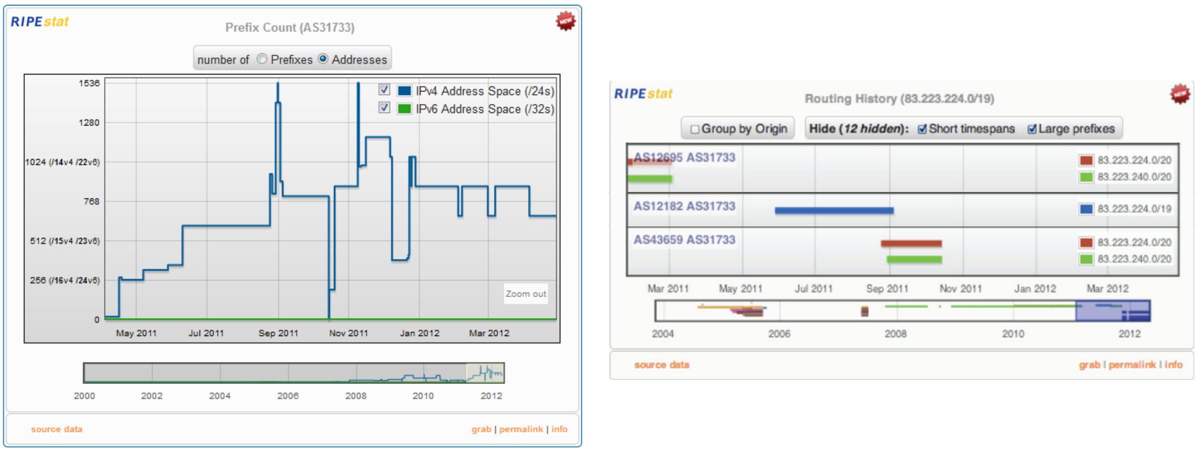


Fig. 2: Elisha: The main visualization consists of a scalable pixel-based approach to display BGP data. Each pixel represents an IP address with a color encoding according to the corresponding BGP event. The three detailed windows at the top enlarge areas of interest to better analyze single IP addresses.



(a) One widget uses a line chart to visualize the number of prefixes or amount of address space announced by a predefined AS (e.g., the AS31733) over time. Peaks represent a high amount of announced address space like *e.g.*, at the end of August.

(b) Another widget shows the routing history of a given IP prefix or AS, *i.e.*, the history of the exact IP prefixes advertised, the origin ASes as well as the direct upstream providers. This example shows the routing state of prefix 83.223.224.0/19 from Link Telecom before (row 1), during (row 2) and after (row 3) the hijack event.

Fig. 3: Visual routing analysis of an hijack event of AS31733 using Prefix Count and Routing History widgets from RIPEstat.

can be leveraged in the analysis of routing data for a recent validated fly-by spammer case study. We analyze this hijack case from a dual perspective – from both the data and control planes – and we illustrate how such an attack can be detected by combining various visualization techniques that leverage data collected from the two planes. This ongoing work illustrates the research carried out in VIS-SENSE, a European research project that uses visual analytics to develop more effective tools for BGP monitoring and prefix hijack detection.

3.1 Hijack Detection from the Data Plane

Hijacking an IP prefix automatically modifies the route taken by data packets so that they reach the physical network of the attacker. Based on this assumption a tool called *Spamtracer* 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 also translated into AS-level routes using live BGP feeds. Routing anomalies can then be extracted from the routes and analyzed using the different features available, *e.g.*, the ASes owner, the IP hops country, the length of the traced routes, etc.

Spamtracer monitored several IP prefixes belonging to Link Telecom while they were hijacked by the spammer as well as after the legitimate owner regained control over them. Actually, visualizing a series of traceroutes towards a single network as a graph, possibly on top of a map, *e.g.*, a world map or treemap, is particularly suited for the detection of significant changes in the routes. Fig. 4 illustrates the BGP routes to the victim network from a vantage point in France and highlights the AS originating the prefixes and the direct upstream provider during and after the hijack.

In this case study, we observe that during the hijack traffic from the vantage point in France and destined to AS31733 Link Telecom goes to the hijacker network (Fig. 4: route $VP \xrightarrow{A} 1 \xrightarrow{B} 2$) through the direct provider AS12182 Internap (Fig. 4: node 1). By providing a fake proof of ownership of AS31733 prefixes to Internap, a tier-2 US ISP, the spammer managed to peer with this ISP, hence establishing a customer-provider relationship. 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: node 2).

After the hijack traffic goes towards Russia (Fig. 4: route $VP \xrightarrow{D} 3 \xrightarrow{E} 4$) where the legitimate owner of AS31733 resides (Fig. 4: node 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. We also observed that just after the hijack, we did not receive any reply for traceroute probe packets sent to the destination network, neither for ASes located a few hops before the destination network, probably due to strong ICMP filtering or rate limiting rules in those networks. On the contrary, traceroute paths collected during the hijack regularly reached the destination hosts successfully. This sudden change in the network and host reachability also suggests that a major routing change occurred in BGP, which significantly changed the networks paths for reaching the destination.

In this particular hijack case, we see that relevant routing anomalies can be extracted from traceroutes and their visualization. However, studying traceroute anomalies is usually insufficient to detect IP prefix hijacking without raising too many false positives. Combining network topologies inferred from data-plane and control-plane routes, and correlating the anomalies uncovered from both planes, allows to perform much more accurate IP prefix hijacking detection.

3.2 Hijack Detection from the Control Plane

This section focuses on the analysis of the Link Telecom hijack from the control plane. In this respect, it is stressed that the primary routing decision criteria in BGP mostly results from economic agreements between ASes. However, these contracts also reflect geographical constraints. Hence, there is no apparent operational reason for selecting paths that significantly deviate from the ideal direct route. In order to exploit this inherent spatial consistency of the routing procedures, the following methodology is introduced:

- All ASes announced as any prefix's owner are grouped on per hosting-country basis.
- For each one of these hosting-countries (C), the set of intermediate-countries is defined as the set of all the different countries that have to be traversed by any IP traffic that originates from the vantage point of choice (V) and is addressed to prefixes hosted by C.
- For each intermediate-country (I), the probability of its appearance (P_I) along a route towards the hosting-country (C) is calculated

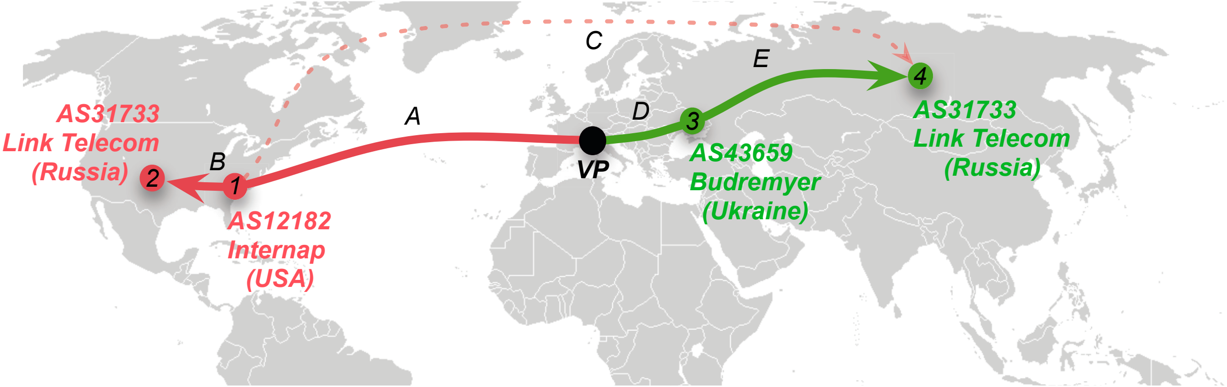


Fig. 4: **Link Telecom (AS31733) Hijack**: visualization of the BGP routes from a vantage point (VP) in France *during* (AB) and *after* (DE) the hijack. The labels (2) and (4) indicate the location of Link Telecom during and after the hijack respectively, whereas (1) and (3) indicate the direct upstream provider during and after the hijack respectively.

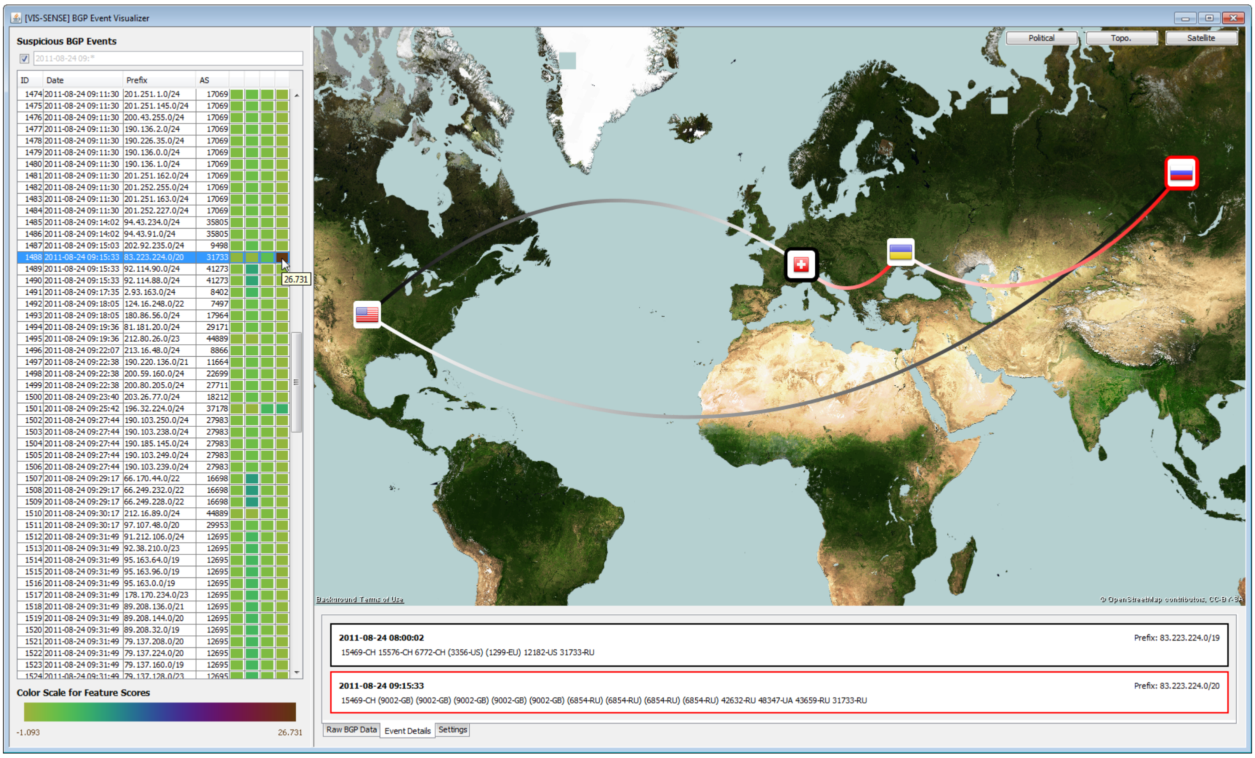
as the fraction of the number of BGP announcements including country I as an intermediate hop towards country C against the total number of BGP announcements that regard prefixes hosted in country C. The aim of P_I, is to provide a quantitative metric of how common is the choice of the respective ASes that are hosted in I as intermediate hops for reaching C.

- The geographic length L_I that is introduced by I is computed as the ratio of the length of the path $C_V \to I \to C$ against the ideal direct path $C_V \to C$, where C_V is the country hosting the vantage point V. Subsequently, besides the $L(I)$, the Z-Score (Z_I) of L_I is also estimated for all the intermediate-countries of C, in order to incorporate the overall routing behavior (distribution of L_I) into the process of assessing the potentially malicious nature of a path's announcement.

Specifically, for the case under investigation, AS31733 (Link Telecom) is officially declared to be located in Russia. Moreover, according to the BGP announcements, the path towards AS31733 appears to traverse AS12182 (Fig. 4: route $VP \xrightarrow{A} 1 \xrightarrow{C} 4$). Hence, regardless of the actual physical location of the hijacking network that forged the AS31733 identity, USA, which hosts AS12182, is considered to act as an intermediate-country (I) towards Russia, which is the legitimate hosting-country (C) of Link Telecom.

Nevertheless, checking the overall BGP announcements that concern Russian ASes and which are collected from monitoring routers (Vantage Points - VPs) situated in central Europe, it is calculated that only for 0.11% of the prefixes hosted in Russia it is necessary for the Internet traffic to traverse USA ($P_{USA} = 0.11\%$ for C=Russia). Furthermore, exploiting the same BGP statistics and taking into account the geographical location of USA in juxtaposition with the direct path between the VP and Russia (Fig. 4: route $VP \xrightarrow{D} 3 \xrightarrow{E} 4$), the Z-Score of the geographic length introduced by USA into a path towards Russia reaches the extreme value of 26.74. Therefore, the existence of AS12182 hosted in USA along the route to AS31733 raises serious alarm for potential malicious behavior.

The proposed BGP hijack detection and attribution mechanism is enhanced with a visualization tool (Fig. 5) developed for efficiently exploiting the novel abnormality assessment metrics. Two different kinds of visualizations are shown to investigate interesting BGP routings. A pixel visualization is used to get an overview of the geographic length of several BGP routes. The coloring of the pixels communicates the Z-Score of the geographic length for a target AS. Additional other metrics are visualized in the same way to easily recognize patterns of different combinations. To visually explore the details and underlying connection suspicious events can be selected. The obsolete and the newly announced paths are drawn with gray and red color respectively along with all the traversed countries. The VP-node as well as the target AS-node are highlighted with a colored border to quickly spot the start and end point of the path. This helps to investigate the suspicious event through visually



Suspicious BGP Events

☑ 2011-08-24 09:*

ID	Date	Prefix	AS				
1474	2011-08-24 09:11:30	201.251.1.0/24	17069	🟩	🟩	🟩	🟩
1475	2011-08-24 09:11:30	201.251.145.0/24	17069	🟩	🟩	🟩	🟩
1476	2011-08-24 09:11:30	200.43.255.0/24	17069	🟩	🟩	🟩	🟩
1477	2011-08-24 09:11:30	190.136.2.0/24	17069	🟩	🟩	🟩	🟩
1478	2011-08-24 09:11:30	190.226.35.0/24	17069	🟩	🟩	🟩	🟩
1479	2011-08-24 09:11:30	190.136.0.0/24	17069	🟩	🟩	🟩	🟩
1480	2011-08-24 09:11:30	190.136.1.0/24	17069	🟩	🟩	🟩	🟩
1481	2011-08-24 09:11:30	201.251.162.0/24	17069	🟩	🟩	🟩	🟩
1482	2011-08-24 09:11:30	201.252.255.0/24	17069	🟩	🟩	🟩	🟩
1483	2011-08-24 09:11:30	201.251.163.0/24	17069	🟩	🟩	🟩	🟩
1484	2011-08-24 09:11:30	201.252.227.0/24	17069	🟩	🟩	🟩	🟩
1485	2011-08-24 09:14:02	94.43.234.0/24	35805	🟩	🟩	🟩	🟩
1486	2011-08-24 09:14:02	94.43.91.0/24	35805	🟩	🟩	🟩	🟩
1487	2011-08-24 09:15:03	202.92.235.0/24	9498	🟩	🟩	🟩	🟩
1488	2011-08-24 09:15:33	83.223.224.0/20	31733	🟩	🟩	🟩	🟫
1489	2011-08-24 09:15:33	92.114.90.0/24	41273	🟩	🟩	🟩	🟩
1490	2011-08-24 09:15:33	92.114.88.0/24	41273	🟩	🟩	🟩	🟩
1491	2011-08-24 09:17:35	2.93.163.0/24	8402	🟩	🟩	🟩	🟩
1492	2011-08-24 09:18:05	124.16.248.0/22	7497	🟩	🟩	🟩	🟩
1493	2011-08-24 09:18:05	180.86.56.0/24	17964	🟩	🟩	🟩	🟩
1494	2011-08-24 09:19:36	81.181.20.0/24	29171	🟩	🟩	🟩	🟩
1495	2011-08-24 09:19:36	212.80.26.0/23	44889	🟩	🟩	🟩	🟩
1496	2011-08-24 09:22:07	213.16.48.0/24	8866	🟩	🟩	🟩	🟩
1497	2011-08-24 09:22:38	190.220.136.0/21	11664	🟩	🟩	🟩	🟩
1498	2011-08-24 09:22:38	200.59.160.0/24	22699	🟩	🟩	🟩	🟩
1499	2011-08-24 09:22:38	200.80.205.0/24	27711	🟩	🟩	🟩	🟩
1500	2011-08-24 09:23:40	203.26.77.0/24	18212	🟩	🟩	🟩	🟩
1501	2011-08-24 09:25:42	196.32.224.0/24	37178	🟩	🟩	🟩	🟩
1502	2011-08-24 09:27:44	190.103.250.0/24	27983	🟩	🟩	🟩	🟩
1503	2011-08-24 09:27:44	190.103.238.0/24	27983	🟩	🟩	🟩	🟩
1504	2011-08-24 09:27:44	190.185.145.0/24	27983	🟩	🟩	🟩	🟩
1505	2011-08-24 09:27:44	190.103.249.0/24	27983	🟩	🟩	🟩	🟩
1506	2011-08-24 09:27:44	190.103.239.0/24	27983	🟩	🟩	🟩	🟩
1507	2011-08-24 09:29:17	66.170.44.0/22	16698	🟩	🟩	🟩	🟩
1508	2011-08-24 09:29:17	66.249.232.0/22	16698	🟩	🟩	🟩	🟩
1509	2011-08-24 09:29:17	66.249.228.0/22	16698	🟩	🟩	🟩	🟩
1510	2011-08-24 09:30:17	212.16.89.0/24	44889	🟩	🟩	🟩	🟩
1511	2011-08-24 09:30:17	97.107.48.0/20	29953	🟩	🟩	🟩	🟩
1512	2011-08-24 09:31:49	91.212.106.0/24	12695	🟩	🟩	🟩	🟩
1513	2011-08-24 09:31:49	92.38.210.0/23	12695	🟩	🟩	🟩	🟩
1514	2011-08-24 09:31:49	95.163.64.0/19	12695	🟩	🟩	🟩	🟩
1515	2011-08-24 09:31:49	95.163.96.0/19	12695	🟩	🟩	🟩	🟩
1516	2011-08-24 09:31:49	95.163.0.0/19	12695	🟩	🟩	🟩	🟩
1517	2011-08-24 09:31:49	178.170.234.0/23	12695	🟩	🟩	🟩	🟩
1518	2011-08-24 09:31:49	89.208.136.0/21	12695	🟩	🟩	🟩	🟩
1519	2011-08-24 09:31:49	89.208.144.0/20	12695	🟩	🟩	🟩	🟩
1520	2011-08-24 09:31:49	89.208.32.0/19	12695	🟩	🟩	🟩	🟩
1521	2011-08-24 09:31:49	79.137.208.0/20	12695	🟩	🟩	🟩	🟩
1522	2011-08-24 09:31:49	79.137.224.0/20	12695	🟩	🟩	🟩	🟩
1523	2011-08-24 09:31:49	79.137.160.0/19	12695	🟩	🟩	🟩	🟩
1524	2011-08-24 09:31:49	79.137.128.0/23	12695	🟩	🟩	🟩	🟩

26.731

Color Scale for Feature Scores

-1.093 26.731

2011-08-24 08:00:02 Prefix: 83.223.224.0/19

15469-CH 15576-CH 6772-CH (3356-US) (1299-EU) 12182-US 31733-RU

2011-08-24 09:15:33 Prefix: 83.223.224.0/20

15469-CH (9002-GB) (9002-GB) (9002-GB) (9002-GB) (9002-GB) (6854-RU) (6854-RU) (6854-RU) (6854-RU) 42632-RU 48347-UA 43659-RU 31733-RU

Fig. 5: BGP-Event-Visualization: The pixel visualization on the left acts as an overview to be able to focus on interesting events (*e.g.*, AS31733 with a high Z-Score). The graph visualization with an underlying geographic map reveals details about the selected route. Grey paths are obsolete, red paths are new routings.

compare the route changes .

Figure 5 refers to the detection of the Link Telecom hijack incident, where, from both the pixel coloring and the route divergence, it becomes evident that the depicted event regards a rather abnormal path alteration. Additionally, the necessary information is provided for efficiently performing the thorough attribution of the underlying BGP activity.

4 Conclusion

The routing infrastructure of the Internet relies entirely on BGP as inter-domain routing protocol to maintain and exchange routing information between network providers. Because of the vulnerable design of BGP, attackers can easily misuse the routing system through *prefix hijacking* in order to conduct malicious activities, such as spamming and DoS attacks, without worrying about disclosing their identity through their real source IPs.

Efficient network monitoring tools are thus of utmost importance. However, network administrators are challenged today by the sheer volumes of data to analyze, especially when it comes to BGP data collection and monitoring. In this respect, a short survey is given on network visualization methods for BGP, in order to show how visual analysis tools can support an analyst in finding, understanding and confirming BGP hijacks and other anomalies in routing data, in complement to fully-automated analytical methods. Moreover, this paper describes methods and tools that are being developed for BGP monitoring and prefix hijack detection, within the framework of VIS-SENSE, a European research project that focuses on the exploitation of *visual analytics* for enhancing Internet forensics. To this aim, a verified prefix hijacking case that recently occurred is exhaustively analysed by applying the VIS-SENSE methodologies.

Acknowledgments

The research leading to these results has received funding from the European Commission's Seventh Framework Programme (FP7 2007-2013) under grant agreement nr. 257495 (VIS-SENSE).

REFERENCES

[1] RIPE, "YouTube Hijacking: A RIPE NCC RIS case study," http://www.ripe.net/news/study-youtube-hijacking.html, [Online; accessed 13-Jan-2011].

[2] R. Mahajan, D. Wetherall, and T. Anderson, "Understanding BGP Misconfiguration," in *SIGCOMM '02: Proceedings of the 2002 conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*. New York, NY, USA: ACM, 2002, pp. 3–16.

[3] C. Zheng, L. Ji, D. Pei, J. Wang, and P. Francis, "A Light-Weight Distributed Scheme for Detecting IP Prefix Hijacks in Real-Time," *SIGCOMM Comput. Commun. Rev.*, vol. 37, no. 4, pp. 277–288, 2007.

[4] X. Hu and Z. M. Mao, "Accurate Real-time Identification of IP Prefix Hijacking," in *SP '07: Proceedings of the 2007 IEEE Symposium on Security and Privacy*. Washington, DC, USA: IEEE Computer Society, 2007, pp. 3–17.

[5] "IP Prefix hijacking by Michael Lindsay via Internap," http://mailman.nanog.org/pipermail/nanog/2011-August/039379.html, August 2011.

[6] G. Di Battista, F. Mariani, M. Patrignani, and M. Pizzonia, "BGPlay: A System for Visualizing the Interdomain Routing Evolution," in *Graph Drawing (Proc. GD '03)*, ser. Lecture Notes in Computer Science, G. Liotta, Ed., vol. 2912, 2004, pp. 295–306.

[7] P. Cortese, G. Di Battista, A. Moneta, M. Patrignani, and M. Pizzonia, "Topographic visualization of prefix propagation in the internet," *IEEE Transactions on Visualization and Computer Graphics*, pp. 725–732, 2006.

[8] L. Colitti, G. Di Battista, F. Mariani, M. Patrignani, and M. Pizzonia, "Visualizing Interdomain Routing with BGPlay," *Journal of Graph Algorithms and Applications*, vol. 9, no. 1, pp. 117–148, 2005.

[9] M. Lad, D. Massey, and L. Zhang, "Visualizing internet routing changes," *IEEE Transactions on Visualization and Computer Graphics*, pp. 1450–1460, 2006.

[10] T. Wong, V. Jacobson, and C. Alaettinoglu, "Internet routing anomaly detection and visualization." in *DSN*. IEEE Computer Society, 2005, pp. 172–181. [Online]. Available: http://dblp.uni-trier.de/db/conf/dsn/dsn2005.html#WongJA05

[11] J. Oberheide, M. Karir, and D. Blazakis, "VAST: Visualizing Autonomous System Topology," in *Proceedings of the 3rd international workshop on Visualization for computer security*. ACM, 2006, pp. 71–80.

[12] S. T. Teoh, K. Zhang, S.-M. Tseng, K.-L. Ma, and S. F. Wu, "Combining visual and automated data mining for near-real-time anomaly detection and analysis in bgp." in *VizSEC*, C. E. Brodley, P. Chan, R. Lippman, and W. Yurcik, Eds. ACM, 2004, pp. 35–44. [Online]. Available: http://dblp.uni-trier.de/db/conf/vizsec/vizsec2004.html#TeohZTMW04

[13] S. Teoh *et al.*, "Elisha: a visual-based anomaly detection system," in *Int'l. Symp. on Recent Advances in Intrusion Detection (RAID)*, 2002.

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

[15] S. T. Teoh, S. Ranjan, A. Nucci, and C.-N. Chuah, "BGP Eye: A New Visualization Tool for Real-time Detection and Analysis of BGP Anomalies," in *VizSEC*, W. Yurcik, S. Axelsson, K. Lakkaraju, and S. T. Teoh, Eds. ACM, 2006, pp. 81–90. [Online]. Available: http://dblp.uni-trier.de/db/conf/vizsec/vizsec2006.html#TeohRNC06