BGPeep: An IP-Space Centered View for Internet Routing Data

James Shearer[1], Kwan-Liu Ma[1], and Toby Kohlenberg[2]

[1] Visualization and Interaction Design Innovation lab
University of California, Davis, CA 95616
{jjshearer,klma}@ucdavis.edu
http://vidi.cs.ucdavis.edu
[2] Intel Corporation
toby.kohlenberg@intel.com

Abstract. We present BGPeep, a tool for visualizing Border Gateway Protocol traffic at a detailed level, using a novel depiction of IP-space. This new visualization renders the network prefixes involved with such traffic using a method that leverages the peculiarities of BGP traffic to gain insight and highlight potential router misconfigurations. BGPeep utilizes a simple interface and several methods of interaction to allow users to quickly focus on the data of interest. Our tool highlights aspects of BGP data which have received less attention in previous visualization applications, in order to help form a more complete picture of this vital part of the Internet communications infrastructure.

1 Introduction

The Border Gateway Protocol (BGP) is the top-level routing protocol currently utilized to maintain a constantly connected topology for the global Internet. Every day, many thousands of border routers under the ownership of Autonomous Systems (ASes) constantly converse, exchanging information about their own IP-space ownership, distant network reach-ability, and broken peer connections. This ongoing router "chatter" generates a huge amount of multi-variate data, and at any given time governs the current state of the amorphous, global routing table. This ephemeral data exists exclusively in the rarely-glimpsed world of the BGP speakers - diminutive routers that sit at the topological edge of our networks.

Understanding BGP data is critical given its foundational nature regarding the Internet. This protocol is so deeply entrenched in the communications infrastructure that updating and upgrading is extremely difficult, even though a secure, authenticated version of the protocol is necessary. Router misconfigurations and purposeful attacks can render dark whole swaths of the Internet in a very short period of time. Unsurprisingly, much research exists - both in terms of detection and analysis - to cope with these dangers.

We present BGPeep, a new tool for visualizing BGP update messages using a novel visual encoding of IP-space. Our tool complements the many existing

J.R. Goodall, G. Conti, and K.-L. Ma (Eds.): VizSec 2008, LNCS 5210, pp. 95–110, 2008.

tools for viewing routing data in that it provides a unique picture of the data at lowest-level, rather than focusing on overall AS connectivity. We provide intuitive methods of interaction so that network operators can quickly isolate the data of interest and produce a useful picture for aiding BGP problem diagnosis.

2 Related Work

Given its import and data-intensive nature, it is no surprise that BGP has received given a thorough treatment from the visualization community. Several recent works focus on providing a high-level view of the ever-changing topology amongst autonomous systems, the best known of which is BGPlay [1]. With this work, Colitti et al. allow network operators to monitor or observe the reachability of a specified prefix from the perspective of a given border router. Colitti's colleagues at Roma Tre University extended BGPlay to include the AS "importance" hierarchy in the visualization, drawing inspiration from topographical cartography [2]. Wong, et al described a method [3] of clustering voluminous BGP data - called stemming - in order to present a clear, useful visualization of routing from the perspective on one AS, and demonstrate how their technique can help diagnose BGP anomalies. The described system, like BGPlay, uses animation to show how the routing situation changes over time, allowing network operators to quickly "see" the story rather than crawling through thousands, perhaps millions, of update messages. The LinkRank visualization [4] developed by Lad, Masset, and Zhang, provides a higher level view of AS connectivity in that it simultaneously visualizes the *number* of routes lost or gained between many different ASes. It can help show how the overall topology changes when the link between two ASes fails.

The above cited works all focus on presenting a high-level view of BGP update traffic, aiming to free the network operator from the river of data flowing silently among the many border routers. Other tools deal with the data at a somewhat lower level. Teoh, et al. provide a suite of visualization tools [5] for examining individual update messages with the aim of problem diagnosis and root-cause analysis. They also provide a technique for clustering and picturing these messages as single, categorizable events.

Some visualization applications focus on specific types of BGP misconfiguration or attack. For example, Teoh et al. describe techniques for visualizing Change of Origin AS events [6] [7]. These tools include an encoding of the overall IP-space using a quad-tree. More recently, they have extended their previous work on classification of update messages into BGP events, and provide new tools for showing a more global picture of BGP activity with an application suite called BGPEye [8]. This tool provides several different visualizations of BGP activity from the perspective of one collection point. The different perspectives given by this tools show not only the overall BGP activity, but also how it affects the network connectivity at the data collection point.

Most existing tools focus either on the high-level picture, or specific aspects of the low-level data. BGPeep instead provides a general tool for visually examining

the raw update traffic provided by border routers. The novel IP-space encoding we've developed provides a depiction of announced and withdrawn network prefixes that more clearly conveys the size of the update, and can better show overlapping or conflicting updates. As such, we see it as a useful tool to be used in collaboration with the many existing packages for coping with BGP. Its aim is to provide a tool for general exploration of the traffic generated by peer ASes, a niche not yet filled by existing software.

3 BGPeep

BGPeep uses four linked views to present BGP update messages and allow users to manipulate the visualization. Figure 1 shows the main application window, which contains the *prefix visualizer*, the *timeline*, and the low-level *data view*. Figure 2 depicts the *AS tag cloud* and corresponding user-interface controls, which provide the means for initial data retrieval, filtering, and AS subset selection. The typical data browsing scenario is as follows. The user selects and loads a specific data set, and then runs one of the pre-defined queries against the data. This action populates the tag cloud with matching ASes, which can be restricted temporally using the timeline if desired. The user then interacts directly with the tag cloud to select a subset of the ASes for examination in the prefix visualizer. The following sections describe each component's design and interaction abilities in more detail.

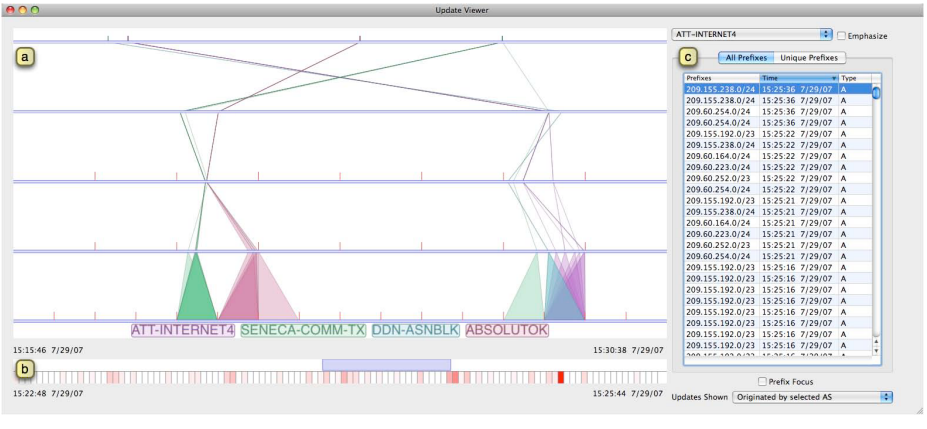


Fig. 1. The update view is the visual center of BGPeep and contains three linked views. The prefix visualizer (**a**) depicts the selected BGP update messages. The timeline (**b**) provides an intuitive means for time-based restriction and provides a visualization of the relative message traffic throughout the selected time. The data view (**c**) is a more traditional tabular view of the BGP data for inspecting specific details of an update message. It provides controls for filtering and focusing in on specific ASes or prefixes.

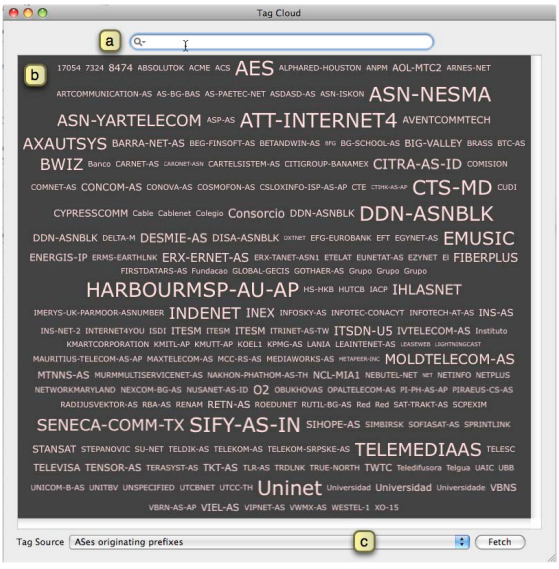


Fig. 2. The AS tag cloud displays (**b**) the ASes matching the search criteria, specified using the selection popup (**c**). Tag sizes are proportional to the relative number of update messages sent in the selected time by the associated AS. Users can filter and search the presented AS subset using the search field (**a**), select ASes for display by clicking the tag, or obtain additional AS information using the detail viewer.

3.1 The Data

BGPeep currently supports ASCII dumps in MRT 'machine' format, such as those provided by the University of Oregon RouteViews project [9]. These dumps are collections of all BGP update messages sent by peer ASes to border routers participating in the RouteViews project. Each record in a given dump is either a BGP update or withdrawal message, with contents as specified in IETF RFC 4271 [10]. For the purposes of our discussion, it is sufficient to know that a message contains at least the follow parts:

Peer AS. This is the topologically neighboring border router which sent the update message to the collection router.

Announcement/Withdrawal. An announcement message is when an AS claims a certain portion of IP-space is reachable through it, and a withdrawal is when it revokes this claim.

A Prefix. The portion of IP-space for which this message applies. Essentially, this is an IP address with a set number of bits marked as fixed. The remainder - the variable bits - represent the range of address the prefix covers. For example, 192.168.1.0/24 represents the range of addresses starting at 192.168.1.0 with the first 24 bits fixed. The remaining 8 bits are variable, covering 256 unique IP addresses. IETF RFC 4632 [11] contains a detailed description of CIDR addressing.

AS Path. For announcement messages, the AS path is simply an ordered list of ASes that lead to a given prefix. The last AS on the path to a given network prefix is called the *origin AS*. That AS is said to have *originated* that prefix.

3.2 AS Tag Cloud

Tag clouds are an interaction technique that has been popularized recently on the world wide web. A tag cloud is a list of visual elements, typically words, that are assigned different sizes based on some metric. A user can click directly on a tag to instigate some action in the program or browser, often navigating to some other application content. Though little academic research describes tag clouds, Rivadeneira, et al. [12] present recent work which provides an overview and describes evaluation strategies.

The AS tag cloud (Figure 2) is the primary interface element for querying the BGP update data set. Users can select a query to run against the data using the selection popup marked '**c**.' These queries are written in a SQL-like language, and are modifiable by the application designer. BGPeep currently supports queries for returning all ASes which originate prefixes in the current data set, for returning all peer ASes which present updates or withdrawals, and for returning all ASes mentioned in an announced AS path. These queries can be temporally restricted using the timeline, discussed below in Section 3.4.

The query populates the cloud with AS tags, listed alphabetically by AS name, with the sizes assigned based on the relative number of matching updates associated with the given AS. For example, if the user queried 'ASes originating prefixes,' then the tag sizes would be based on the number of prefixes the AS originated in the selected time range. As such, the most active ASes immediately stand out against the background noise of the less active systems. Users can select up to four ASes to display in the prefix viewer at a given time by clicking the appropriate tags. Right-clicking a tag calls up a AS detail view, as depicted in Figure 3(c). This panel, which contains some simple statistics regarding the selected AS for the given dataset, floats above the cloud when requested, and is invisible otherwise. This provides a mechanism for unobtrusively providing information that is not typically useful, but that the user might need to infrequently access.

The tag sizing is meant to help users in their initial encounter with a new data set in order to identify the most active ASes. But for certain tasks, the tag cloud sizing might not be useful. For example, if the user is searching for a particular AS, or activity concerning a particular prefix, then the assigned sizes might simply be distracting. For that reason, BGPeep provides a variety of methods for filtering the cloud. The search field, marked '**a**' in Figure 2, allows the user to select from a list of pre-defined searches such as 'AS name contains...', and 'AS announces prefix...'. When the user enters text, all tags *not* matching the criteria are visually darkened, while matching tags retain their visual impact (Figure 3(b)). As such, a user can quickly locate the AS of interest and select it for display in the other application views.

(a) Unfiltered (b) Filtered (c) Detail display

Fig. 3. Filtering allows BGPeep users to more easily find the ASes of interest. Figure 3(a) shows a normal, unfiltered tag cloud. In Figure 3(b), the cloud is filtered showing thoses ASes with a long description containing the string 'net'. Figure 3(c) shows several selected ASes and one displayed using the AS detail panel, which users can show or hide by right-clicking on a tag.

3.3 Prefix Visualization

The prefix visualization in the main visual element of BGPeep, and provides a novel view of IP-space in a BGP-centric fashion. The view contains five axis, and selectable, colored labels naming the currently visualized ASes. Figure 4 provides a labeled version of the prefix visualization showing only a few updates. The visualization components, rendering technique, and interaction methods are described below.

The Axes. The topmost axis in the display represents the AS associated with the update message, either as peer AS or originating AS, and has values ranging from the lowest AS number in the data set to the highest. For example, if the 'lowest' AS mentioned in the data set was 100, and the highest was 41000, then the midpoint of the first axis would correspond to AS number 20000.

The subsequent axes correspond to the various octets of the prefix's CIDR-style IP address range. For example, for the prefix 192.168.1.0/24, 192 would be plotted on the second axis, 168 on the third, 1 on the fourth, and 0/24 on the fifth. The axis for the second, third, and fourth octets are subdivided to prevent display over-plotting. Using the method described below, a shape is drawn through these axes which shows the viewer which AS(es) announced or withdrew the prefix and what portion of IP-space it covers.

Update Rendering. Each prefix is rendered as a shape that passes through all five axis. There are three situations that contribute to the overall shape of the prefix:

AS to Octet 1. This portion of the shape is a line connecting the AS associated with the update to the location of the first octet, where the Octet axis is valued 0-255 from left to right.

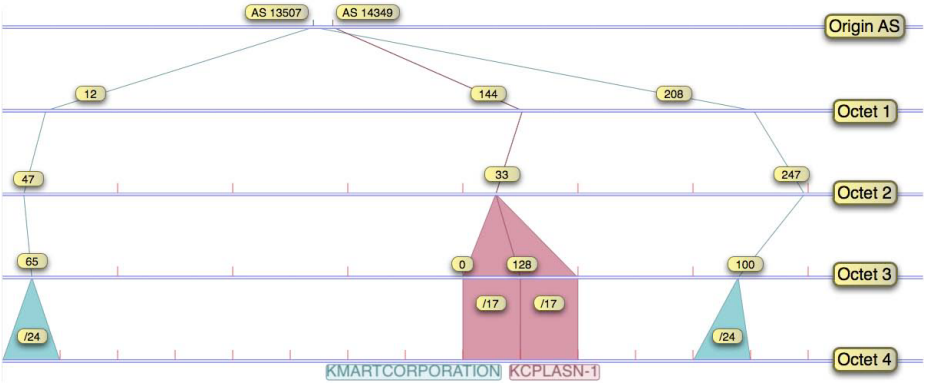
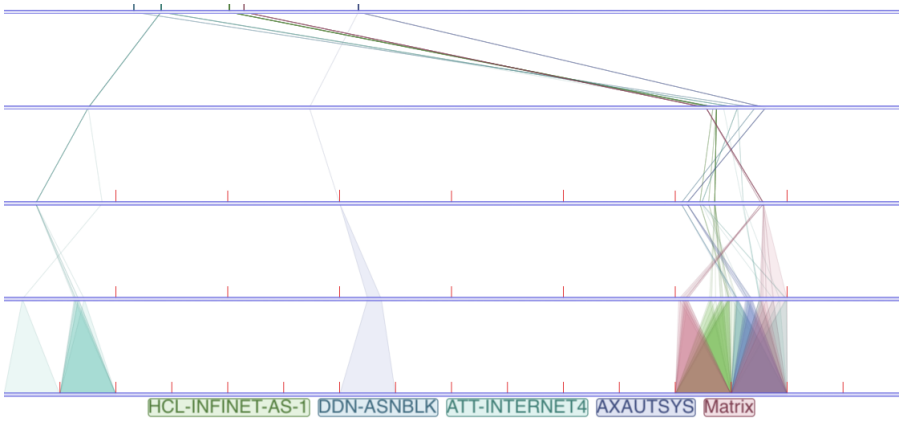


Fig. 4. The prefix visualization, labeled for explanation, showing four prefix announcements from two ASes. The top axes denotes the AS associated with the update message, and the subsequent four axes represent the four IP address octets. Each axis is subdivided as detailed in section 3.3 to avoid extensive display over-plotting and allow easier visual decoding of the prefix. Variable portions of the CIDR address are draw as polygons that extend across the addresses in the range. Note that in this particular image, we also see a potential inefficiency in the announcements for AS 14349. Instead of announcing two /17 prefixes, it could instead announce one /16 and handle the de-aggregation internally.

Octet to Octet. Octet 2, and later axes are subdivided into a set number of sections, demarcated with small hash marks. Each section on the axis corresponds to the entire 0-255 octet range *for prefixes whose first octet falls above it.* This is evident from Figure 4. Prefix 12.47.65.0/24 flows down the left side of the display due to this subdivision. This allows many more prefixes to be shown simultaneously without overlapping.

Ranges. Almost all BGP updates involve a range of addresses, usually 256 unique IPs or more in size. Ranges are depicted using a triangle which covers all the addresses contained in the update. Because most updates are /24 or greater in size, the shape between axes 4 and 5 are usually a triangle or a rectangle. This depicting of ranges means that larger ranges are fuller, larger shapes. Also, prefixes announcing less than 256 addresses - usually indicative of a misconfiguration - clearly show up as skinny shapes between the final two axes.

All updates for the selected ASes are rendered simultaneously in the display to allow intra- and inter-AS comparison. Each prefix is rendered with a user-modifiable base opacity. This allows the user to see - at a glance - very chatty ASes. If the base opacity is set very low, yet the prefix visualizer shows a relatively solid-colored prefix, then this prefix was announced many times in the selected time period. The user can then examine the specific timing details in the data view table.

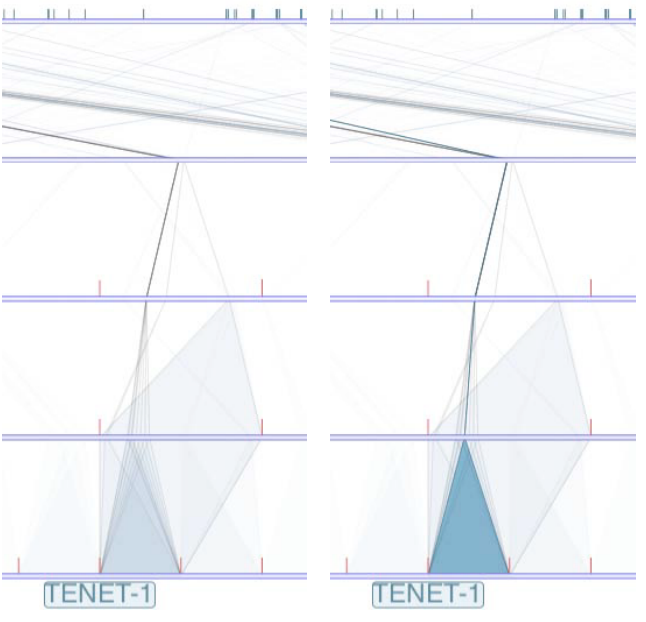


(a) No emphasis

(b) AS *Matrix* emphasized

Fig. 5. AS emphasis can help isolate a particular AS for closer examination, or compare/contrast two similar ASes. In the top image, three displayed ASes announce prefixes in the same octect range, leading to some cluttering on subsequent axes. In the bottom image, the unselected ASes are assigned 10% opacity, so that the selected AS is highlighted, but all context is not lost.

AS Emphasis. Very active ASes can sometimes present many update announcements, which makes comparison with other ASes difficult. As a remedy, BGPeep allows the user to select a specific AS for *emphasis*. When selected, the rendered prefixes for that AS retain their opacity, while all other updates and their corresponding labels are rendered with significantly reduced opacity. The user can select another AS for emphasis either by selecting it from the selection popup in the data view, or by clicking its label in the prefix visualizer. Figure 5



(a) No focus (b) Focused

Fig. 6. Individual prefix focus visually isolates the selected prefixes in a potentially crowded display. The selected prefixes are rendered with full opacity, regardless of the set base opacity, and are rendered on top of the other, non-focused prefixes. This allows the user to highlight the prefix of interest without losing the context of the selected AS' overall announcement activity.

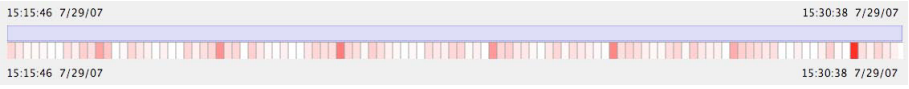
shows AS emphasis in action. Note that the other ASes are not entirely removed - simply faded - so as to retain context for comparison.

Prefix Focusing. Similarly, the user might see a specific prefix in the data view that she wants to highlight in a visually busy mass of updates. In this case, the user can enable prefix focusing by clicking the associated check box in the data view and then selecting one or more prefixes in the table. When focused, a prefix is rendered last - and therefore on top of the other prefixes - with full opacity.

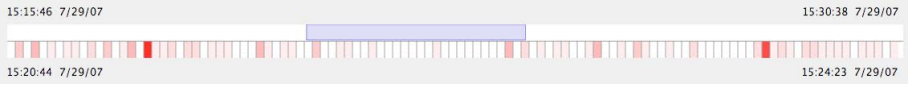
3.4 Timeline

The timeline allows the BGPeep user to temporally restrict queries in the other views, including the initial tag cloud query. When the application starts, the entire time range for the loaded data set is pre-selected, as depicted in Figure 7(a). By clicking and dragging in the upper portion of the timeline, the user can intuitively select only a portion of the time range for display, Figure 7(b).

The bottom half of the timeline is the update frequency visualization, which provides the user with a quick overview of update 'hot spots' for the selected



(a) Timeline



(b) Timeline with selection

Fig. 7. The timeline view allows BGPeep users to temporally restrict both the rendered messages and the initial AS cloud search. The top portion of the timeline is a simple rectangle which represents the portion of the loaded data set currently selected. The bottom portion divides the currently selected time range into equally-sized rectangles and colors each region based on the number of updates in the corresponding time slice. The more saturated the color, the greater the number of updates.

AS. This portion of the display is sub-divided into equally sized rectangles. Each rectangle corresponds to an equal slice of time in the already selected time range. BGPeep colors each rectangle based on the *relative* number of associated updates that occur in that time. The more saturated the color, the greater the number of updates in that time slice, relative to the whole selected range. By alternating the selection between two ASes, the user can compare and contrast when the main activity occurred for each system, which might be important for cases such as that detailed in Section 4.2.

3.5 Data View

The data view provides controls for filtering the displayed update messages in the prefix visualizer, and also provides a more traditional, table-based view of the update messages. The various interface elements are described in Figure 8. The topmost selection popup, labeled '**a**,' allows the user to choose which AS' data is shown in the table, marked '**b**'.

As previously noted, the data view contains interface elements for highlighting specific ASes or prefixes.

The table view contains two distinct presentations of the update messages for the currently selected AS. In the first, *all* update messages - including duplicates - for the selected AS are listed in the table. For each update, the time, the type, the prefix, the AS path, and other data are given. Users can sort on any column in order to arrange the data in the most convenient manner. If an update is a withdrawal, the text for that update is colored red. This allows the user to quick spot flapping routes, as described in section 4.1.

The second table view shows only unique prefixes - filtering out repeat announcements - which can be more useful for initial data exploration. Often an AS will make repeated announcements regarding the same prefix, with the same information. A user can combine all of these updates into a single table line which

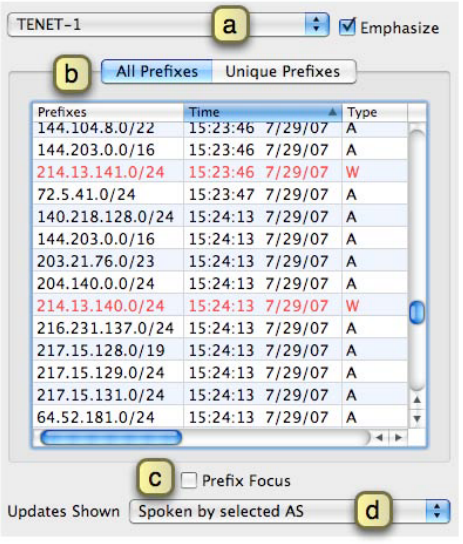


Fig. 8. The data view provides controls for visually isolating specific ASes (**a**), specific prefixes (**c**), examining low-level details of individual update messages (**b**), and varying the type of visualized update messages (**d**). Note that the table view assigns a distinct color to the text of withdrawal messages, which helps to identify cases of route flapping.

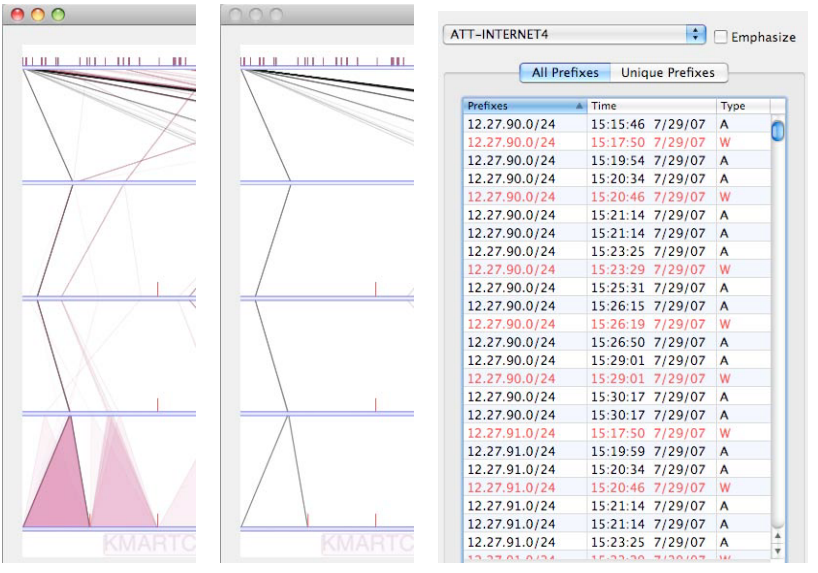
has only the prefix and the count of times it was announced. This is useful if the user wants to quickly focus each individual prefix announced by a particular AS in order to get a sense of the overall IP-space ownership claimed.

4 Results

The primary benefit of BGPeep is the ease by which it allows a user to quickly navigate and visualize the traffic observed at a particular router. However, there are some particular cases of router misconfiguration or mischief for which BGPeep can provide a unique perspective.

4.1 Route Flapping

Route flapping occurs when an AS repeatedly announces and then withdraws a specific network prefix. While flapping usually has little effect on the overall topology of the Internet, it can generate excessive network traffic and can unnecessarily add to the workload of computationally constrained routers. BGPeep provides features to help identify such cases. First, it renders withdrawal messages with a fixed opacity, black outline as detailed in Figure 9. The result is that moderately-to-heavily flapping routes appear very different from those that are simply announced. When the user adjusts the base rendering opacity to zero, the withdrawn routes - even those withdrawn only once - leave behind a visible



(a) Regular (b) Withdrawals (c) Flapping in the table

Fig. 9. Withdrawal messages are rendered slightly differently from prefix announcements. Announcement borders have the same hue and base opacity as the fill color for the given AS. Withdrawal messages, however, are drawn with a black border at a fixed opacity. As a result, a flapping route will have a 'pencil-sketch' look (left) when rendered with non-zero base opacity, and will leave behind a visual residue (center) when the base opacity is set low. Combined with the distinct coloring and sort options available in the data view table (right), it is easy to identify flapping routes.

outline. He or she can then use the data view table to see specific details of the offending update messages by sorting on time and prefix. Withdrawal messages are printed with red text, and the alternating red-black text makes flapping easy to identify.

4.2 Prefix Highjacking

Prefix Highjacking occurs when AS A mistakenly or purposefully announces itself as the owner of AS B's network prefix. If the path announced by A is shorter than that in the current global routing table, or the newly announced prefix is more specific, then many systems will mistakenly route packets truly destined for B to A.

A high-profile case of prefix hijacking occurred on February 24, 2008 when Pakistan Telecom announced itself the origin AS of 208.65.153.0/24, an IP range owned by YouTube. The announcement was mean to block YouTube from within Pakistan, but somehow it mistakenly leaked out to neighboring ASes. As a result, the announcement propagated throughout the Internet and many hosts could no longer properly route packets to YouTube. Eventually, YouTube announced the

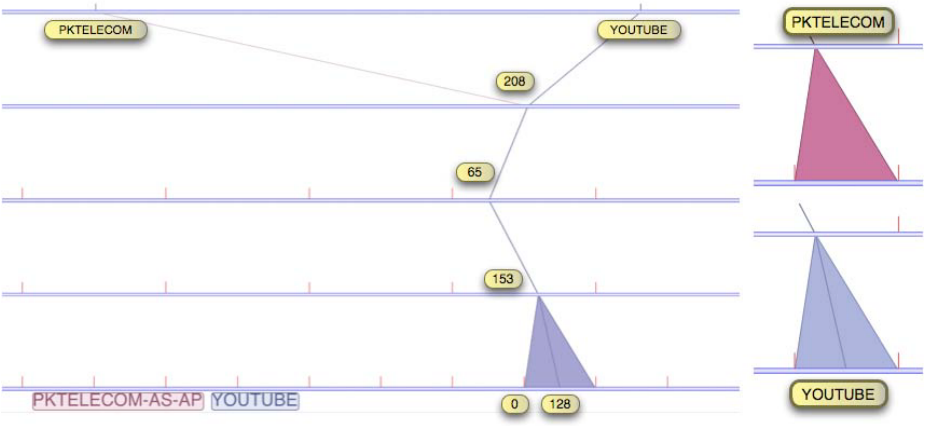


Fig. 10. This shows the prefix hijacking of YouTube's 208.65.153.0/24 by Pakistan Telecom on February 24th, 2008. Note how the AS lines 'funnel' into the same prefix. Also note the later de-aggregation purposefully announced by YouTube to combat the hijacking.

same IP-space as two smaller /25 prefixes, which repaired connectivity for many hosts. The RIPE news archive contains a detailed analysis of this event [13].

Figure 10 shows this event, as rendered in the BGPeep prefix visualizer. The image clearly shows that both Pakistan Telecom and YouTube claim ownership of the same prefix, and that YouTube later announced two consecutive, smaller prefixes. In order to obtain this image, we loaded data from the RouteViews archive for February 24th into BGPeep and searched for ASes involved with prefixes beginning with '208.65.153.0' bounded by the time range of the event. The timeline frequency visualization provided temporal context to the selected announcements.

4.3 Inefficient Announcements

Inefficient prefix announcements, like flapping, can have a negative effect on overall routing performance by generating unnecessary traffic, and by increasing the size of the global routing table. For example, most ASes do not announce or propagate announcements for prefixes smaller than 256 hosts, since almost all ASes deal in chunks of IP-space of size /24 or greater. BGPeep's prefix visualization clearly shows suspiciously small announcements, as depicted in Figure 11. Here the suspicious updates are obvious because they deviate from the typical visual pattern of triangles between the bottom two axes.

Figure 12 shows another example of how BGPeep can highlight potentially bad route announcements. Here an AS has announced three prefixes which are consecutive in IP-space. Consulting the data view, we saw the for all three, the announcement details, including the AS Path, were identical. It is likely that these three prefixes could be collapsed into one announcement.

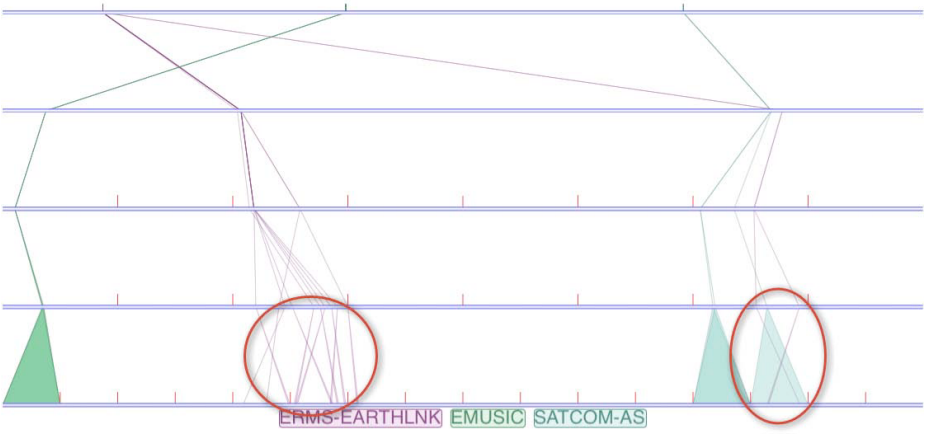


Fig. 11. In this figure, we see that ERMS-EARTHLINK has announced many sub-/24 prefixes, including a few individual IP addresses. Because of the deviation from the normal visual pattern, these 'spikes' on the last axis visually jump out at the user. This could be of particular use in an animated, real-time monitoring application of BGPeep.

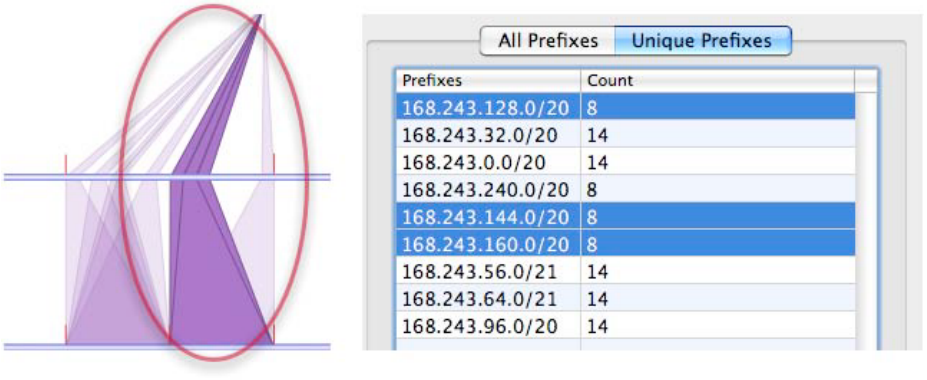


Fig. 12. An example of possibly inefficient route announcements. The focused routes, circled in red, announce consecutive ranges of IP address with the same AS path. Most likely, the originating AS could collapse these announcements into one consecutive IP range and perform and needed de-aggregation internally. This helps keep the global routing table small, which is important given the limited computing power most BGP speakers possess. These kinds of striated patterns are easy to see using BGPeep.

5 Future Work

This work presents the core visual elements and interaction design for BGPeep. We're currently working on extending our tool to incorporate animation to show the announcements over time. With this feature, the user could place the tool into

a 'monitoring' or 'playback' mode and watch as live prefixes or a selected data subset arrive at their AS' border routers. As each update arrives, it would briefly flash with full opacity, and then slowly fade away. In such an implementation, flapping routes, overly chatty neighbors, and inefficient announcements would be easy to spot. This could be combined with an overlay of the particular ASes own prefix space, so that hijacking and de-aggregation would be immediately evident to a watchful eye.

6 Conclusion

We have presented BGPeep, and interactive system for visualizing BGP update messages at a lower level than most existing applications. Using BGPeep, an network operator can interactively explore the update traffic as seen by her border routers, and better understand the traffic generated by peering ASes. In addition, our unique encoding of IP-space affords the user a fresh perspective on such data sets, and can clearly show IP-space de-aggregation, prefix hijacking, and route flapping. We believe BGPeep to be a useful addition to the already powerful arsenal of visualization tools available for contending with the data avalanche BGP presents.

Acknowledgements

This research was supported in part by Intel Corporation, the U.S. National Science Foundation through grants CCF-0634913, IIS-0552334, CNS-0551727, and OCI-0325934, and the U.S. Department of Energy through the SciDAC program with Agreement No. DE-FC02-06ER25777.

Special thanks to the University of Oregon Route Views Project for providing the data used in the development of BGPeep.

References

1. Colitti, L., Di Battista, G., Mariani, F., Patrignani, M., Pizzonia, M.: Visualizing interdomain routing with bgplay. Journal of Graph Algorithms and Applications 9, 117–148 (2005); Special Issue on the 2003 Symposium on Graph Drawing, GD 2003
2. Cortese, P., Di Battista, G., Moneta, A., Patrignani, M., Pizzonia, M.: Topographic visualization of prefix propagation in the internet. IEEE Transactions on Visualization and Computer Graphics 12(5), 725–732 (2006)
3. Wong, T., Jacobson, V., Alaettinoglu, C.: Internet routing anomaly detection and visualization. In: International Conference on Dependable Systems and Networks, 2005. DSN 2005. Proceedings, 28 June-1 July 2005, pp. 172–181 (2005)
4. Lad, M., Massey, D., Zhang, L.: Visualizing internet routing changes. IEEE Transactions on Visualization and Computer Graphics 12(6), 1450–1460 (2006)
5. Teoh, S.T., Ma, K.L., Wu, S.F.: A visual exploration process for the analysis of internet routing data. In: VIS 2003: Proceedings of the 14th IEEE Visualization 2003 (VIS 2003), Washington, DC, USA, p. 69. IEEE Computer Society, Los Alamitos (2003)

6. Teoh, S.T., Ma, K.L., Wu, S.F., Zhao, X.: Case study: interactive visualization for internet security. In: VIS 2002: Proceedings of the conference on Visualization 2002, Washington, DC, USA, pp. 505–508. IEEE Computer Society, Los Alamitos (2002)
7. Teoh, S.T., Ma, K.L., Wu, S., Jankun-Kelly, T.: Detecting flaws and intruders with visual data analysis. Computer Graphics and Applications 24(5), 27–35 (2004)
8. Teoh, S.T., Ranjan, S., Nucci, A., Chuah, C.N.: Bgp eye: a new visualization tool for real-time detection and analysis of bgp anomalies. In: VizSEC 2006: Proceedings of the 3rd international workshop on Visualization for computer security, pp. 81–90. ACM, New York (2006)
9. University of Oregon RouteViews Project, `http://www.routeviews.org`
10. Rekhter, Y., Li, T., Hares, S.: A Border Gateway Protocol 4 (BGP-4). RFC 4271 (Draft Standard) (2006)
11. Fuller, V., Li, T.: Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan. RFC 4632 (Best Current Practice) (2006)
12. Rivadeneira, A.W., Gruen, D.M., Muller, M.J., Millen, D.R.: Getting our head in the clouds: toward evaluation studies of tagclouds. In: CHI 2007: Proceedings of the SIGCHI conference on Human factors in computing systems, pp. 995–998. ACM, New York (2007)
13. YouTube Hijacking: RIPE Analysis, `http://www.ripe.net/news/study-youtube-hijacking.html`