BLT: A Taxonomy and Classification Tool for Mining BGP Update Messages

Tomoyuki Kitabatake
The University of Tokyo

Romain Fontugne
IIJ Research Lab

Hiroshi Esaki
The University of Tokyo

***Abstract*—The Border Gateway Protocol (BGP) is a key component in Internet routing. Consequently, monitoring BGP messages is essential to identify changes that are detrimental to networks reachability. This is however a complicated task, mainly due to the stateful and noisy nature of BGP. One need to keep track of the entire routing table to really understand the meaning of a single BGP message. And significant bursts of messages may be completely redundant. In this paper, we propose a complete taxonomy of BGP update messages and its corresponding classification tool called BLT. We also introduce a simple anomaly detector based on BLT that pinpoints surge of selected classes of messages. We illustrate the benefits of this detector with five case studies that validate its ability to identify meaningful events.**

I. INTRODUCTION

The Border Gateway Protocol (BGP) is Internet's key protocol for achieving inter-domain routing. Using BGP, Autonomous Systems (ASes) can globally advertise their IP space and the routes they learnt from other ASes. To keep track of routing changes, border routers maintain a local Routing Information Base (RIB) that consists of a set of BGP attributes (e.g. AS path) for each globally routed IP prefix. If the network undergoes changes, routers exchange BGP update messages to inform the new attributes. Depending on a router decision process these new attributes can be reflected in the router's RIB or not.

Monitoring BGP updates is crucial for network operators and researchers trying to track Internet dynamics and identify important changes that can compromise users connectivity. This is however a complicated task because BGP conceals routing process details (e.g. routing policies or complete network topology) and, at the same time, BGP is very noisy for certain network changes and instabilities, sometimes referred as BGP churn [1], [2].

In this paper, our goal is to provide a general framework to assist operators and researchers in monitoring the Internet routing dynamics. Namely, we aim to classify and annotate BGP messages based on their effect on the routing process.

To achieve this goal we identified 17 different changes that update messages cause to routers' RIB. These 17 types of update are organized in a hierarchical taxonomy that provides and increasing level of details. In addition, we provide a classification tool, called BLT, that fetches BGP data and labels each message based on the proposed taxonomy. Since the labels convey detailed functions of the messages, it greatly helps one to filter out superfluous messages and focus only on relevant messages.

We demonstrate the benefits of BLT with a simple application, an anomaly detector that reports surge of messages of a certain class. Using this anomaly detector we present five case studies of BGP route leaks and Internet outages that are easily identified as a surge of one specific type of message.

The main contributions of this paper consist of a complete hierarchical taxonomy of BGP update messages (Section II), an open source classification tool for BGP data (Section III) and an anomaly detector identifying surges of certain types of messages (Section IV).

II. TAXONOMY

Our classification of BGP update messages is based on the effects of messages on routers' RIBs. For example, (1) a BGP message may provide a new path to reach a known IP prefix or (2) signal a new routed prefix to be added in the RIB. For the first case the RIB is updated with a new path whereas for the second case a new entry is added to the RIB.

We have identified 17 different classes of update message and organized them as a tree, with four level of details (see Figure 1). Classes close to the root of the tree are very generic and the leaves stand for the most descriptive classes. These classes are not exclusive, a BGP message may result in multiple changes in the RIB. Therefore, a message may correspond to multiple classes in the taxonomy.

A. Change Size

Starting from the left hand side of our hierarchical taxonomy (Figure 1) the first generic class is *Change Size*. This class represents all update messages that affect the growth of the RIB. These messages are either increasing or decreasing the size of the RIB which are represented by two different subclasses:

Remove Prefix stands for BGP messages that discard entries in the RIB, thus decrease its size. These BGP messages are explicit withdrawals for routes that are registered in the RIB. Withdrawals for IP prefixes that are not registered in the RIB are not classified as *Remove Prefix* (see the description for *Duplicate Withdrawal* below).

New Prefix stands for BGP messages that result in new entries in the RIB, thus increase its size. These BGP messages signal the reachability to a new IP prefix or the fragmentation of known IP prefixes into smaller prefixes [3], [4].

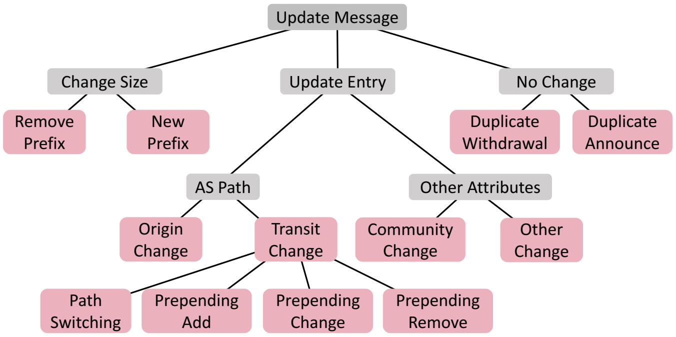

Fig. 1. **Hierarchical taxonomy for BGP update messages.** Classes are based on the differences between a BGP message and the corresponding entry in the RIB. The classes are not mutually exclusive, several classes can be assigned to a single update message. Pink nodes represents labels reported by BLT.

B. *Entry Update*

The second generic class is *Entry Update*. This class represents all update messages that modify BGP attributes stored in the RIB. Since RIBs holds multiple attributes for each IP prefix, this class is further decomposed in multiple sub-classes.

1) AS Path: The AS path is probably the most important attribute in BGP, changes to the AS path have a direct impact on the way traffic is routed. It also discloses a lot of information related to the ASes on the path, for example, AS business relationships [5] and traffic engineering [4].

The *AS Path* class represents any path change observed for IP prefixes registered in the RIB. We further categorize these changes into two sub-classes: *Transit Change* and *Origin Change*.

Transit Change represents any modification made to the AS path except the origin AS, namely the last AS in the path. This class is composed of four sub-classes.

Path Switching represents messages that advertise an AS path that is different from the one registered in the RIB but is the same as the one previously registered in the RIB. These type of messages are mainly revealing route flaps due to hardware or software problems [1].

Prepending Add/Change/Remove exhibit all changes related to AS path prepending. AS path prepending consists in adding multiple times the same AS in the AS path so that the path seems longer hence less preferable in the path selection process. This is a common traffic engineering technique to setup backup links or avoid a certain path.

Origin Change stands for messages that advertise an AS path where the origin AS (i.e. the last AS in the path) is different than the one stored in the RIB. This class of message signals IP prefixes migrating to a different AS. It also can be a sign of unintentional or malicious prefix hijacks [6].

2) Other Attributes: Entry updates that are not changing the AS path are classified as *Other Attributes*. Here we essentially distinguish between BGP communities updates and other changes.

Community Change represents messages with BGP communities that differ from the ones registered in the corresponding RIB entry. BGP communities increase greatly the information carried by an update message. For example, a recent study leverages BGP communities to pinpoint peering facilities traversed by an advertised AS path [7].

Other Change stands for any attribute change except for the AS path and community attribute. We group changes made to attributes other than the AS path and BGP communities because they represent only a very small fraction of observed messages and are usually irrelevant to the analysis of Internet routing.

C. *No Change*

Update messages that advertise the same attributes as the ones found in the corresponding RIB entries are classified in the generic class *No Change*. These superfluous messages are detrimental to routers as they contribute to BGP churn [2]. We further divide this class into two sub-classes:

Duplicate Withdrawal represents messages signaling withdraw for a prefix that is absent from the RIB.

Duplicate Announce represents messages whose attributes are all already registered in the RIB.

III. BLT: BGP-Labeling Tool

Using the above taxonomy we developed a BGP message classification tool, named BLT. It classifies BGP update messages so that network operators, or researchers, can filter irrelevant messages and dedicate their efforts only to a certain type of messages. Our implementation of BLT is made publicly available[1].

BLT is designed as an extension of the BGP framework from CAIDA, BGPstream [8]. It retrieves BGP data using BGPStream and output labeled BGP messages according to the taxonomy presented in Section II.

The classification process consists of four steps illustrated in Figure 2.

1) Initialization: BLT retrieves the RIB data corresponding to the BGP collector and timestamp selected by the user. These RIBs are loaded in memory and will be used to compute BGP messages labels.

2) Attributes comparison: BLT retrieves BGP update messages for a selected time frame. The messages are handled in sequential order, the attributes of a message are compared to the attributes of the corresponding entry in a RIB. The differences between the message and the entry are then sent to update the RIB and to the classification step.

3) RIB update: The differences obtained in the previous step represent a change propagated by the routing infrastructure. To classify subsequent BGP messages we update the loaded RIBs with this new piece of information.

4) Classification: The differences between the last update message and the RIBs are also used to classify that message. This step is essentially traversing the taxonomy tree (Figure 1) and finding nodes that match the observed differences. Only

[1] https://github.com/romain-fontugne/BLT

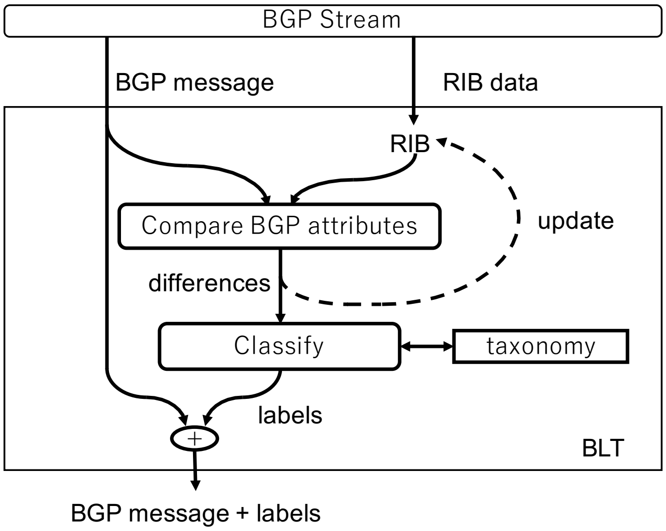

Fig. 2. **BLT overview.** Obtain BGP data from BGPStream, classify BGP update messages based on their differences with the local RIBs, and output both BGP messages and labels.

the most specific nodes are reported (i.e. pink nodes in Figure 1). For example, if a message signal a prefix advertised from a new origin AS then only the label *Origin Change* is reported (not *AS path* nor *Update Entry*).

Finally, BLT outputs the original BGP update messages retrieved from BGPStream along with the computed labels.

IV. Anomaly detection

To illustrate the benefits of BLT for monitoring the Internet routing infrastructure, we developed a routing anomaly detection method based on BLT results. This application demonstrates the relevance of BLT labels to Internet routing activities and the practical use of BLT for network operators.

This application monitors the proportion of message labels and reports periods of time when the number of messages for a certain class is abnormally high. The cause of the detected anomalies differ depending on the reported label. For example, an excessive number of messages labeled as *Duplicate Announce* might reveals noisy BGP messages that might be due to BGP session resets, whereas the surge of messages classified as *New Prefix* might reveal an accidental leak of internal prefixes and more specific prefixes [9].

The principles of the proposed anomaly detector are fairly simple. First, we use BLT to retrieve BGP messages and corresponding labels for a selected time frame and BGP collector. Second, for each message class we model the usual number of messages and report time periods when the data significantly deviates from this computed reference. The reference is obtained from the median number of messages and the median absolute deviation (MAD). These two operators are robust to outlier values [10] and have been extensively employed for anomaly detection [11], [12].

Formally, let $X_l(t)$ be the number of messages classified with label l at the time bin t. Then we define as anomalous a time bin t that satisfies the following equation:

$$X_l(t) > median(X_l) + \tau MAD(X_l)$$

where τ is the sensitivity parameter, and, $median(X_l)$ and $MAD(X_l)$ are, respectively, the median and MAD values for all time bins. In our experiments we set the bin size to ten minutes and the sensitivity parameter $\tau = 10$.

We also make the source code of this anomaly detector publicly available[2].

V. Results

In this section we present several case studies that demonstrate the values of BLT and the proposed anomaly detector to monitor different types of routing anomalies. Section V-B illustrates results obtained by monitoring BGP update messages for all ASes on the Internet therefore large-scale routing anomalies. In Section V-C we monitor only small sets of prefixes and events that affect these prefixes.

A. Dataset

The RIBs and BGP update messages analyzed for these case studies are all from the Route Views project [13] which is an archive of BGP data maintained by the University of Oregon. Route Views consists of multiple data sources, in this paper we are only analyzing the data collected at the LINX collector. In 2017 this collector contains data from 25 full-feed BGP peers that provide a good representation of Internet AS paths diversity [14]. For each case study we analyze 24 hours of data, namely BLT retrieves the RIB for each BGP peer and the BGP update messages collected in the following 24 hours.

B. Monitoring Internet-wide events

To monitor the entire Internet routing infrastructure one can fetch all BGP messages from a set of BGP peers and classify these messages with BLT. We illustrate this, by looking at events that had a global impact on the Internet. The three following case studies are BGP route leaks that happened in 2016 and 2017.

1) BGP route leak from Google: On August 25th 2017 around 3:22 UTC, Google (AS15169) advertised over 150k routes for small prefixes that were presumably used for their internal traffic engineering[3]. Because these prefixes were longer than corresponding prefixes found in routing tables, numerous ASes have preferred the leaked paths and routed their traffic towards Google's network. This has affected the reachability to the origin ASes of the leaked prefixes and in particular a major access network in Japan, NTT OCN (AS4713).

Using BLT we retrieved the BGP messages received from the Route Views LINX collector on August 25th. Figure 3 depicts the total number of messages observed on that day (top plot), the number of labels assigned to the messages (middle plot) and the results of the anomaly detector (bottom plot). Usually we observe around 300k BGP messages per 10-minute

[2] https://github.com/romain-fontugne/BLT

[3] https://dyn.com/blog/large-bgp-leak-by-google-disrupts-internet-in-japan/

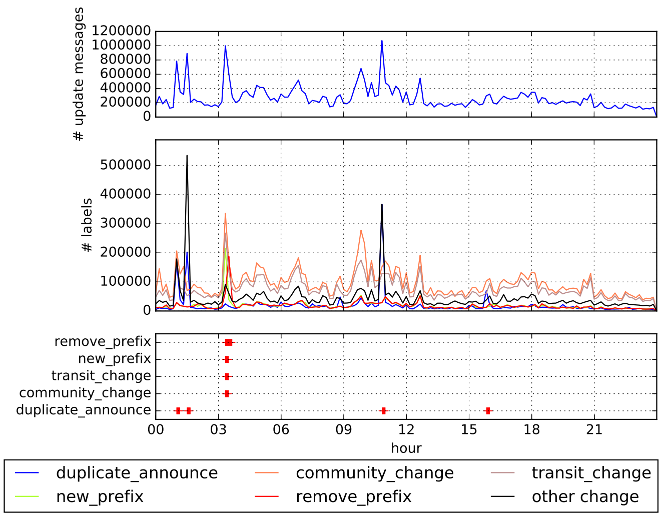

Fig. 3. **BGP route leak from Google.** Number of BGP messages observed on August 25th 2017 (top plot), the number of corresponding labels found by BLT (middle plot), and detected anomalies (bottom plot).

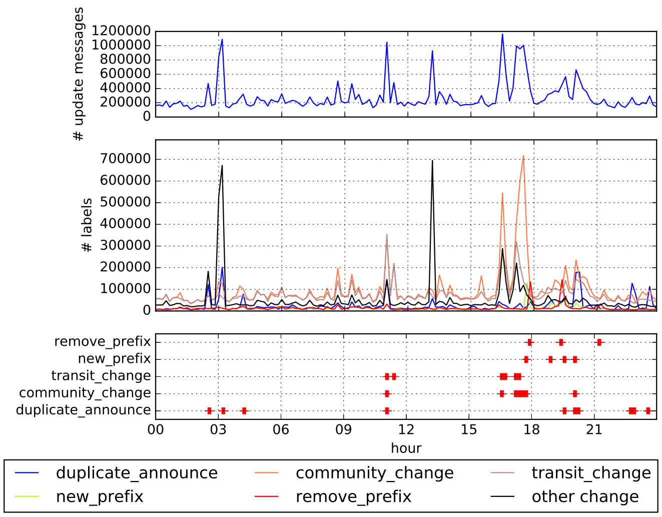

Fig. 4. **BGP route leak from Level(3).** Number of BGP messages observed on November 6th 2017 (top plot), the number of corresponding labels found by BLT (middle plot), and detected anomalies (bottom plot).

bin for this collector, but the average number of BGP messages per bin is markedly over 800k messages three times during the day (Fig. 3 top plot).

The labels obtained with BLT and the results of the anomaly detector (respectively the middle and bottom plot of Figure 3) provide a lot more insights into the collected messages. First, through out the entire day the vast majority of the messages are classified as *Community Change* and *Transit Change*. But the three peaks going over 800k messages are mainly due to different types of messages.

The peak around 1:30 and the one around 11:00 are both due to a surge of messages classified as *Duplicate Announce* and *Other Change*. Both peaks are due to a lots of duplicate and change of the next hop attribute from a single BGP peer, this is likely due to an unstable link in that AS. We found this type of events for all the analyzed case studies. Apart from increasing BGP churn, these events are not particularly appealing. They represent no changes on the inter-domain routing infrastructure and can be easily filter out with BLT.

The peak at 3:20 is composed of different classes of messages. This event is first characterized by the outbreak of numerous new prefixes which is due to Google's BGP route leak. Along with these new prefixes we observe the emergence of multiple BGP messages classified as *Transit Changes* and *Community Changes* that reveal messages exchanged during BGP convergence. These events are then followed by numerous withdrawals that correspond to Google's response to mitigate the route leak.

This example clearly illustrates the small number of alerts reported by our detector and its capacity to pinpoint the BGP leak although we are monitoring millions of messages.

2) BGP route leak from Level(3): The other BGP leak we look at was initiated by Level(3) on November 6th 2017. Around 17:47 UTC, Level(3) advertised numerous routes that were used for Level(3) internal routing. Similar to Google's leak, these prefixes were longer than previously advertised prefixes so numerous ASes have preferred the paths leaked by Level(3). Comcast connectivity was particularly impacted by this event because a lot of their prefixes had been leaked.

Figure 4 illustrates BLT results for the BGP messages gathered by the LINX collector on November 6th 2017. The total number of messages (top plot) shows a few times during the day when the total number of BGP update messages was abnormally high (> 800k messages). BLT labels and the anomaly detector, however, reveal that most of these events are caused by duplicate messages and other changes that are assimilated to BGP noise and flapping routes.

Since the Level(3) BGP leak generated an abnormal number of new prefixes, this event is clearly identified by the anomaly detector (see new_prefix alarms in the bottom plot of Figure 4). We also observe attempts to mitigate the problem afterwards, just before 18:00 UTC numerous prefixes are withdrawn and again around 19:30 when the problem seemed to have been fixed[4]. At 21:15 we also found a lot of withdrawn prefixes but only from a single BGP peer so we suppose that event is not related to the BGP leak. After the Level(3) BGP route leak we also observe numerous ASNs advertising smaller prefixes to mitigate the impact of the outage or circumvent impacted ASNs.

3) Prefix Hijack by Innofield AG: The last Internet-wide case study is a different type of BGP leak. Here the leaking AS is seen as the origin of prefixes that actually belong to other ASes. On April 22nd 2016 at 17:09 a large scale routing incident was caused by the Swiss provider Innofield AG. Innofield usually advertises only one IPv4 and one IPv6 prefix but during the incident this AS and its private sibling AS became the origin of 3431 prefixes that are usually announced

[4] https://blog.thousandeyes.com/comcast-outage-level-3-route-leak/

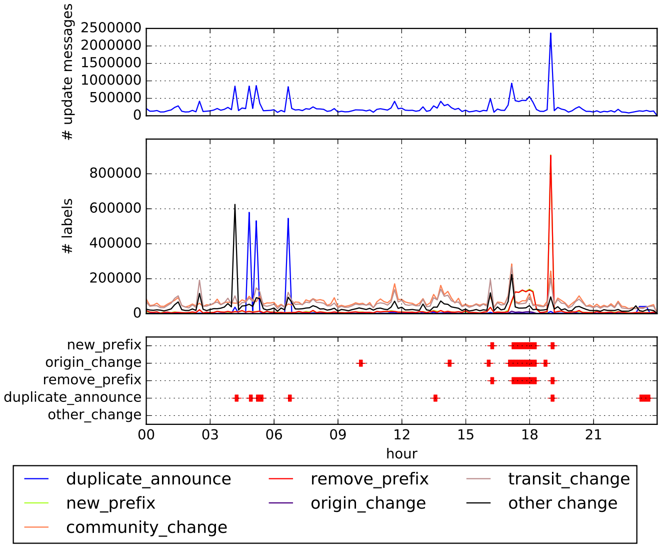

Fig. 5. **BGP Hijack of Innofield AG.** Number of BGP messages observed on April 22nd 2016 (top plot), the number of corresponding labels found by BLT (middle plot), and detected anomalies (bottom plot).

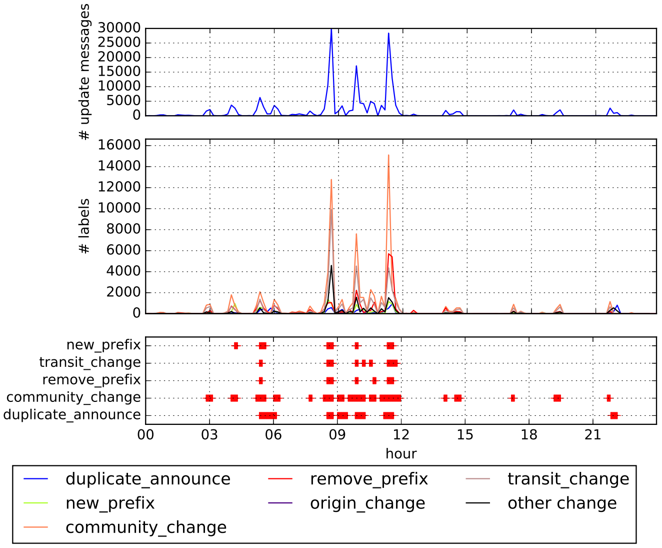

Fig. 6. **Outage in Puerto Rico.** Number of BGP messages observed on September 20th 2017 (top plot), the number of corresponding labels found by BLT (middle plot), and detected anomalies (bottom plot).

by 576 other ASes including popular networks like, Google, Amazon, and Facebook[5].

Figure 5 shows the total number of messages counted on that day (top plot), the number of labels reported by BLT (middle plot) and the results of the anomaly detector (bottom plot). The detector reveals surges of *Origin Change*, *New prefix* and *Remove Prefix* messages from 17:00 to 18:20 and around 18:40. The peak of *Origin Change* is caused by Innofield's BGP route leak. Although this event contains much less prefixes that the two previous case studies, this is easily identified with BLT as a significant surge of *Origin Change*.

On that day, we also observed three other surges of *Origin Change* around 10:00, 14:10 and 16:00. These three events represent IP prefixes that have moved among the numerous ASes own by the United States Department of Defense and we believe these changes are not related to the Innofield issue.

C. Monitoring local routing changes

In this section we look at smaller-scale events. These examples illustrate how an operator can leverage BLT to monitor a certain set of prefixes. The following case studies are two outages in 2017, one in Puerto Rico and one in Syria. For monitoring only networks from these countries we retrieve only the BGP messages corresponding to the prefixes originated by these countries. To find the prefixes of a country we rely on the http://geoinfo.bgpmon.io service [15].

1) Outage in Puerto Rico: Hurricane Maria which is recognized as the worst natural disaster in Puerto Rico was originated from tropical wave and caused massive damage on Dominica and Puerto Rico. When making landfall on Puerto Rico, the hurricane caused significant infrastructure damages and disrupted multiple communication lines. On September 20th 2017 about three-quarters of the prefixes in Puerto Rico became unreachable due to hurricane Maria.

Figure 6 shows the total number of the messages only for Puerto Rican prefixes on September 20th 2017 (top plot), the corresponding labels obtained with BLT (middle plot) and results of the anomaly detector (bottom plot).

Hurricane Maria made landfall in Puerto Rico around 10:15 UTC but we observe first disappearing prefixes from 5:30 UTC, then another set of disappearing prefixes around 8:30, 10:00 and most prefixes around 11:30 (see remove_prefix, Fig. 6 bottom plot). In addition to vanishing prefixes, the damages caused a significant number of network changes identified by the anomaly detector as peaks of *Transit Change*. Our manual inspection of the data validates these results as about 50% of prefixes originated from Puerto Rico at 8:30 disappeared by 12:00.

2) Outage in Syria: The last case study is an outage in Syria that coincides with national examination in that country. There is a few reports on the Syrian government shutting down Internet for the entire country in order to prevent students from cheating[6]. We believe the following event is also related to the national examinations in Syria.

Figure 7 shows the total number of messages on June 1st 2017 (top plot), the number of labels obtained by BLT (middle plot) and the output of the anomaly detector (bottom plot).

We observe only two large peaks of messages, one around 01:00 and another at 5:30. For the first one, a lot of *New Prefix*, *Transit Change*, *Remove Prefix* and *Community Change* messages occur at the same time. This correspond to Syrian prefixes vanishing from routers' RIB (*Remove Prefix*) and

[5] https://bgpmon.net/large-hijack-affects-reachability-of-high-traffic-destinations/

[6] https://motherboard.vice.com/en_us/article/xygv7d/syrian-internet-outages-correspond-exactly-to-national-high-school-test-schedule

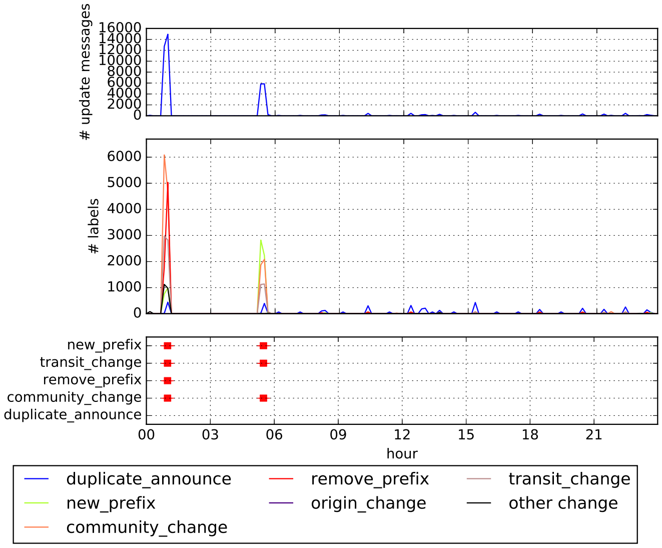

Fig. 7. **outage in Syria** Number of BGP messages observed on June 1^{st} 2017 (top plot), the number of corresponding labels found by BLT (middle plot), and detected anomalies (bottom plot).

corresponding churn caused by path hunting [16].

The second peak, around 5:30, occurs when disappeared prefixes are re-announced on BGP. This peak is composed mainly of *New Prefix*, *Transit Change* and, *Community Change* messages. *New Prefix* messages simply correspond to the first messages announcing the reappearance of the Syrian prefixes. When these prefixes are re-announced, BGP also seeks for the best paths to these prefixes. The convergence phase of BGP is characterized by numerous *Transit Change* and *Community Change* messages appearing synchronously with the emergence of new prefixes.

VI. Related Work

BGP has been widely studied by the research community. The scalability of BGP received a lot of attention, and in particular, the growth of routing tables [3] and BGP churn [1], [2].

BGP data has also been used in various monitoring systems. For example, Argus [6] is a prefix hijack detection system that identifies anomalous changes in BGP data and triggers pings from several vantage points to characterize the detected anomalies. A recent study also uses BGP data to detect Infrastructure outages [7], that approach relies on BGP communities to map AS paths to facilities and BGP update messages to track vanishing facilities. Detected changes are also characterized with extra data plane measurements.

Closer to our work, BGPMon is a service provided by OpenDNS that helps network operators to monitor their IP prefixes. This service relies mainly on BGP data and consists in a set of involved heuristics[7], for example modeling the business relationships between difference ASes. This system mainly focuses on the origin ASes thus it may fails to detect important events where the origin ASes are not changing (e.g. the BGP route leak from Google presented in Section V-B1).

VII. Conclusion

In this paper we presented a general framework to monitor the large number of BGP update messages exchanged by routers. First we introduced a hierarchical taxonomy of BGP messages. Then we developed BLT, a classification tool based on our taxonomy. And finally we proposed a simple anomaly detector to monitor significant events in the data. We illustrated the benefits of this framework with five case studies. The classification of messages allows one to filter out superfluous messages and focus only on relevant ones.

References

[1] Ahmed Elmokashfi, Amund Kvalbein, and Constantine Dovrolis, "Bgp churn evolution: a perspective from the core," *IEEE/ACM Transactions on Networking (ToN)*, vol. 20, no. 2, pp. 571–584, 2012.

[2] Ahmed Elmokashfi and Amogh Dhamdhere, "Revisiting bgp churn growth," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 1, pp. 5–12, 2013.

[3] Luca Cittadini, Wolfgang Muhlbauer, Steve Uhlig, Randy Bush, Pierre François, and Olaf Maennel, "Evolution of internet address space deaggregation: Myths and reality," *IEEE JSAC*, vol. 8, no. 28, pp. 1238–1249, 2010.

[4] Julien Gamba, Romain Fontugne, Cristel Pelsser, Randy Bush, and Emile Aben, "Bgp table fragmentation: what & who?," in *CoRes*, 2017.

[5] Lixin Gao, "On inferring autonomous system relationships in the internet," *IEEE/ACM Transactions on Networking (ToN)*, vol. 9, no. 6, pp. 733–745, 2001.

[6] Xingang Shi, Yang Xiang, Zhiliang Wang, Xia Yin, and Jianping Wu, "Detecting prefix hijackings in the internet with argus," in *Proceedings of the 2012 ACM conference on Internet measurement conference*. ACM, 2012, pp. 15–28.

[7] Vasileios Giotsas, Christoph Dietzel, Georgios Smaragdakis, Anja Feldmann, Arthur Berger, and Emile Aben, "Detecting peering infrastructure outages in the wild," in *ACM SIGCOMM'17*. ACM, 2017, pp. 446–459.

[8] Chiara Orsini, Alistair King, Danilo Giordano, Vasileios Giotsas, and Alberto Dainotti, "Bgpstream: a software framework for live and historical bgp data analysis," in *Proceedings of the 2016 ACM on Internet Measurement Conference*. ACM, 2016, pp. 429–444.

[9] Kotikalapudi Sriram, Doug Montgomery, Danny R. McPherson, Eric Osterweil, and Brian Dickson, "Problem Definition and Classification of BGP Route Leaks," RFC 7908, June 2016.

[10] Rand R Wilcox, *Fundamentals of Modern Statistical Methods: Substantially Improving Power and Accuracy*, Springer Science & Business Media, 2010.

[11] Romain Fontugne, Patrice Abry, Kensuke Fukuda, Pierre Borgnat, Johan Mazel, Herwig Wendt, and Darryl Veitch, "Random projection and multiscale wavelet leader based anomaly detection and address identification in internet traffic," in *Acoustics, Speech and Signal Processing (ICASSP), 2015 IEEE International Conference on*. IEEE, 2015, pp. 5530–5534.

[12] Romain Fontugne, Cristel Pelsser, Emile Aben, and Randy Bush, "Pinpointing delay and forwarding anomalies using large-scale traceroute measurements," in *Proceedings of the 2017 Internet Measurement Conference*, New York, NY, USA, 2017, IMC '17, pp. 15–28, ACM.

[13] "The RouteViews project," *http://www.routeviews.org/*.

[14] Romain Fontugne, Anant Shah, and Emile Aben, "AS hegemony: A robust metric for AS centrality," in *SIGCOMM Posters and Demos*. 2017, pp. 48–50, ACM.

[15] Anant Shah, Romain Fontugne, and Christos Papadopoulos, "Towards characterizing international routing detours," in *Proceedings of the 12th Asian Internet Engineering Conference*. ACM, 2016, pp. 17–24.

[16] Geoff Huston, Mattia Rossi, and Grenville Armitage, "A technique for reducing bgp update announcements through path exploration damping," *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 8, pp. 1271–1286, 2010.

[7] http://www.blackhat.com/us-15/briefings.html#bgp-stream