Real-Time BGP Anomaly Detection Tool (RTBADT) v0.1

Bahaa Al-Musawi, Philip Branch, Grenville Armitage
Internet for Things (I4T) Research Group, Technical Report 180129A
Swinburne University of Technology
Melbourne, Australia
balmusawi@swin.edu.au, pbranch@swin.edu.au, garmitage@swin.edu.au

***Abstract*—This technical report describes the operation of Real-Time BGP Anomaly Detection Tool (RTBADT), a tool to detect BGP anomalies in near real-time. It uses Recurrence Quantification Analysis (RQA) technique, an advanced non-linear statistical technique based on the concepts of phase plane trajectory. RTBADT shows its ability to detect BGP anomalies in near real-time. It also can detect hidden anomalous behaviour in the underlying BGP traffic that may pass without detection. The evaluation of the detection tool has been made through replaying BGP traffic related to well-known BGP incidents within a controlled testbed.**

***Index Terms*—BGP, tools, emulation, anomaly detection, testbed, RQA.**

I. Introduction

The Border Gateway Protocol (BGP) is the Internet's default inter-domain routing protocol. It enables the exchange and maintenance of Network Reachability Information (NRI) between Autonomous Systems (ASes) where an AS represents a large organisation or an Internet Service Provider (ISP). BGP was developed at a time when information provided by a network operator was assumed to be accurate. Consequently, it includes few security mechanisms and so is vulnerable to different types of events such as hijacking, misconfiguration, and link failure. These events have threatened Internet performance and reliability [1].

In the years since it was deployed, many types of anomalies have threatened BGP stability such as TTNet misconfiguration, Nimda, and Moscow blackout. The consequences of BGP anomalies can range from a single to thousands of anomalous BGP updates. Anomalous BGP updates can affect business relationships between individual ISPs or even global routing system. Rapid detection of BGP anomalies helps ISPs protect their networks and mitigate the propagation of anomalous BGP traffic. Identifying anomalous BGP updates within a stream of BGP traffic is a challenge where BGP traffic is voluminous and noisy, around 3 million BGP updates collected on a vantage point per day [2].

Recent statistics on BGP performance show approximately 20% of the hijacking and misconfigurations lasted less than 10 minutes but were able to pollute 90% of the Internet in less than 2 minutes [3]. These statistics demonstrate the need for a new tool that can detect BGP anomalies in real-time where ISPs operators need to react quickly by tuning their BGP configuration to eliminate the propagation of anomalous BGP traffic or notify other ISPs about serious reachability issues. Unfortunately, identifying BGP anomalies is a much harder problem than it seems as a first glance where BGP traffic has been identified as a complex and noisy [4]. Furthermore, there is a set of ASes that send a significant volume of BGP messages consisting of an announcement followed soon by another announcement for their prefixes but with a different path [5].

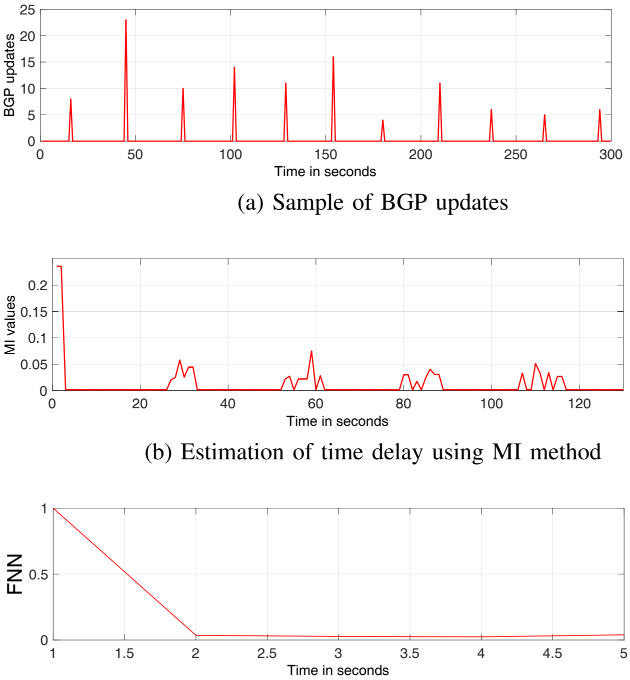
We show in [5] that individual unstable ASes periodically send unstable BGP traffic but they are unsynchronised. The unsynchronised periodic BGP traffic leads to a recurrent behaviour which can be identified using Recurrence Plot (RP). We also show in [6] that Recurrence Quantification Analysis (RQA), an advanced non-linear statistical analysis technique, can be used to detect unstable behaviour of BGP traffic that identify anomalies. In this technical report, we introduce Real-Time BGP Anomaly Detection Tool (RTBADT), a tool to detect BGP anomalies, based on RQA approach described in [6]. RTBADT shows its ability to rapidly (in seconds) detect BGP anomalies as well as other hidden anomalous behaviour that may pass without detection.

The rest of this technical report is organised as follows: In section II, we introduce RQA approach used by RTBADT tool. Section III describe the system design of RTBADT tool. Section IV shows the operation of the BGP anomaly detection tool and configuration setup to run RTBADT. Section V represents the evaluation of RTBADT through replayign one of the most recent well-known BGP events. In section VI, we conclude our work and outline future directions.

II. Detection Approach

The detection approach used in the RTBADT tool is based on using Recurrence Quantification Analysis (RQA), an advanced non-linear statistical analysis technique which uses the concepts of phase plane trajectory. RQA provides quantitative measures of the Recurrence Plot (RP), a tool to visualise the time-dependent behaviour of the dynamics of a system using the concepts of phase plane trajectory, and simplifies interpretation of recurrent data. We have shown in [5] that BGP traffic has the characteristic of recurrence behaviour. The source of this behaviour is unsynchronised periodic traffic by unstable ASes. We have also shown in [6] that RQA is able to distinguish between recurrent normal behaviour and other behaviour that identify anomalies. RQA can rapidly detect BGP anomalies as well as other hidden anomalous periods that may otherwise pass without detection [6]. The strength of RQA applied to this approach is in its ability to rapidly distinguish between the recurrence behaviour that is a part of normal BGP behavior and behaviours that indicate anomalies. Furthermore, RQA is able to detect behaviour that cannot be detected with other techniques.

RQA provides several measures of complexity such as Recurrence Rate (RR), Determinism (DET), Trapping Time (TT), and the recurrence time of second type (T2). These measurements demonstrate the characteristics of systems at different times. For example, RR refers to the probability that a system recurs after a number of time states. DET can be interpreted as the predictability of a system. TT can be used to measure how long the system remains in a specific state while T2 is a measure of time taken to move from one state to another [7].



(a) Sample of BGP updates

(b) Estimation of time delay using MI method

(c) Estimation of embedding dimension using FNN method

Figure 1. Estimation of time delay and embedding dimension

RQA needs three parameters that they have to be carefully selected. These are time delay (τ), embedding dimension (m), and the recurrence threshold (ε). The Auto-correlation function (ACF) and Mutual Information (MI) are the most well-known methods to determine time delay. Unlike ACF which measures linear correlation, MI measures both linear and non-linear correlation. Therefore, we will use the MI method to determine the time delay parameter. The first minimum value of MI represents the value of time delay. For a periodic data, the value of periodicity can be used as the value of time delay. While calculating the value of periodicity can be easily found if the value of MRAI set to > 0, the default value of MRAI in Cisco routers is in a range of 28 to 32 seconds, it needs more attention when the MRAI set to 0 like in Juniper and Quagga routers. To estimate the embedding dimension parameter, False Nearest Neighbour (FNN), a tool for determining the proper embedding dimension in dynamic systems, can be used. The FNN requires the value of time delay which should be calculated first. Once again, the first minimum value of FNN represents the value embedding dimension. Although there is not a well-established method to determine the optimal values of the threshold, the value of threshold has to be selected to be as small as possible. Generally, optimal selection of recurrence threshold depends on the application and experiment. In classification and signal detection, for example, a better choice of the threshold ranges (20-40)% of the signal's standard deviation while a recommendation from [8] suggests that the threshold has to be selected less than 10% of the maximum phase space diameter. Our analysis for the value of RQA threshold in BGP domain shows that the threshold value should be less than 10% of the maximum phase space diameter. We use pss, a Matlab command within Cross Recurrence Plot (CRP) Toolbox for Matlab available online on [9], to compute the maximum phase space diameter. CRP also provide a tool to create RP. These tools are also available within RTBADT package [10].

Selecting non-optimal values for RQA's parameters can produce different structures for the same input data and then might result different detection accuracy. For example, the estimated value of time delay for a sample of BGP updates shown in Figure 1a using MI method shows value of 1 second as the first minimum value but it also shows a periodicity of value 28 seconds as shown in Figure 1b. Whatever the selected value of time delay 1 or 28 seconds, the estimation value of embedding dimension is 2, as shown in Figure 1c, and the threshold value is 3. However, the representation of RP shows different structure as shown in Figures 2b and 2c. Our recommendation for choosing RQA parameters is to choose the value of time delay equal to the periodicity and there should not be an intersection to the main diagonal line in RP. It is also recommended not to use a high value of threshold that results a black matrix[1]. Figure 2d shows an example of choosing a high value to the threshold.

III. System Design

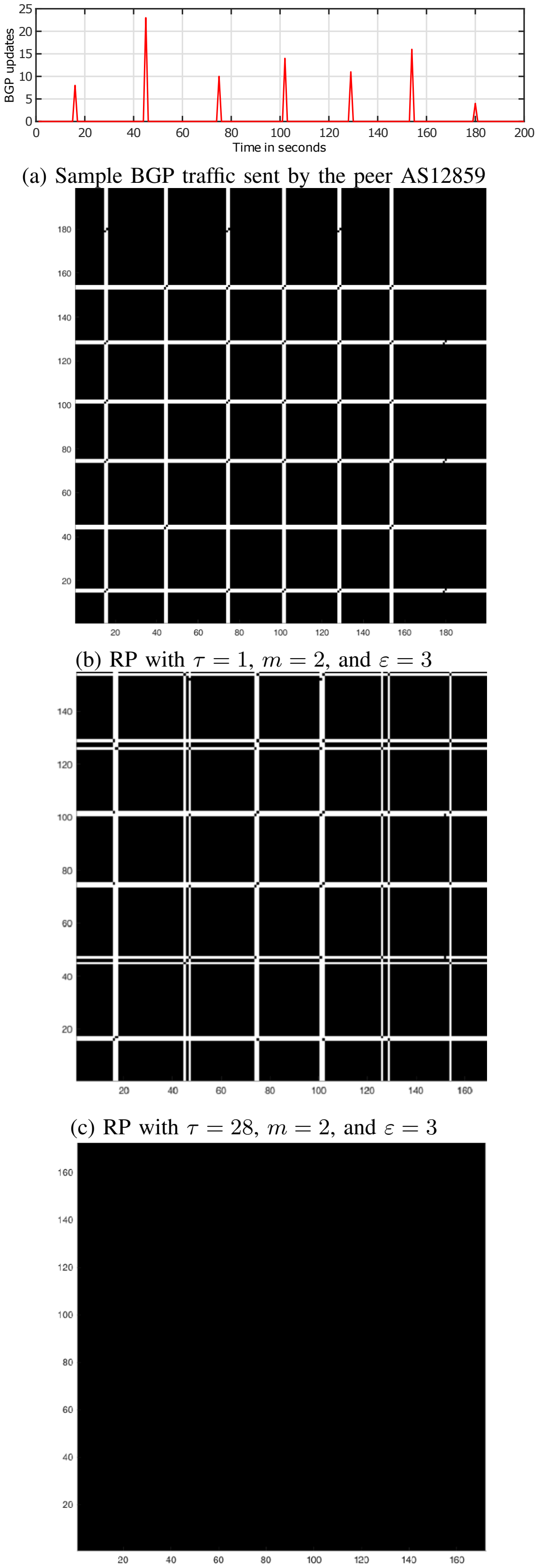
In this section, we describe our detection scheme to detecting BGP anomalies. Our scheme comprised of four stages as shown in Figure 3. RTBADT can be connected to the monitored BGP speaker as a peer.

A. BGP Collector

The purpose of this stage is to provide real-time collecting of BGP traffic. Unlike Quagga [11] which is an open source routing software suite can be used to establish BGP peering and store BGP traffic in MRT format [12], our BGP collector collects BGP traffic in a human readable format. It also calculates a number of BGP features each second. These features avoid the need for converting MRT and calculating BGP features. The output of our collector are BGP volume (V) (total number of announcements and withdrawals) and average length of AS-PATH (AV) calculated every second. The AV feature is calculated as follows:

$$AV = \left[\frac{TA}{A}\right], \tag{1}$$

where TA is total AS-PATH lengths for the announcements, A is total number of announcements , and [ ]



(a) Sample BGP traffic sent by the peer AS12859

(b) RP with $\tau = 1$, $m = 2$, and $\varepsilon = 3$

(c) RP with $\tau = 28$, $m = 2$, and $\varepsilon = 3$

(d) RP with $\tau = 28$, $m = 2$, and $\varepsilon = 10$

Figure 2. Effect of changing RQA parameters on RP

[1] We are more than happy to estimate the RQA parameters for RTBADT's users.

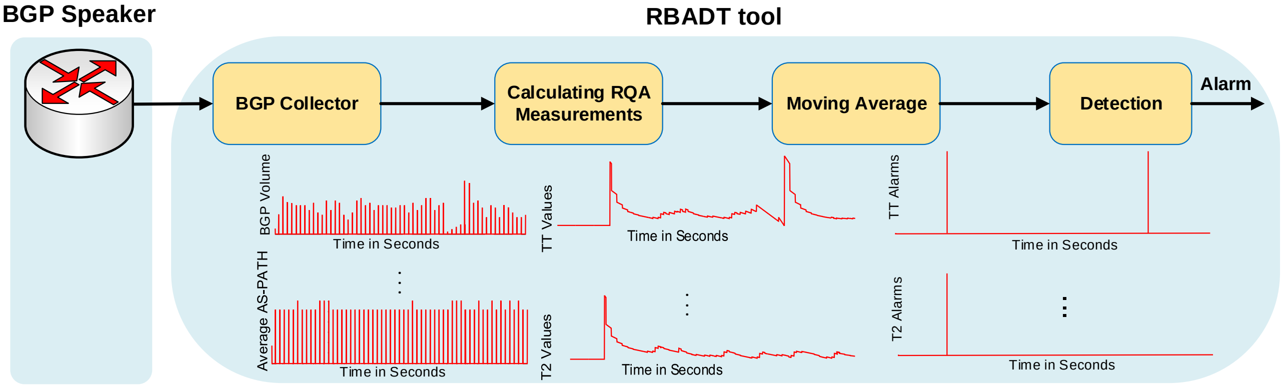
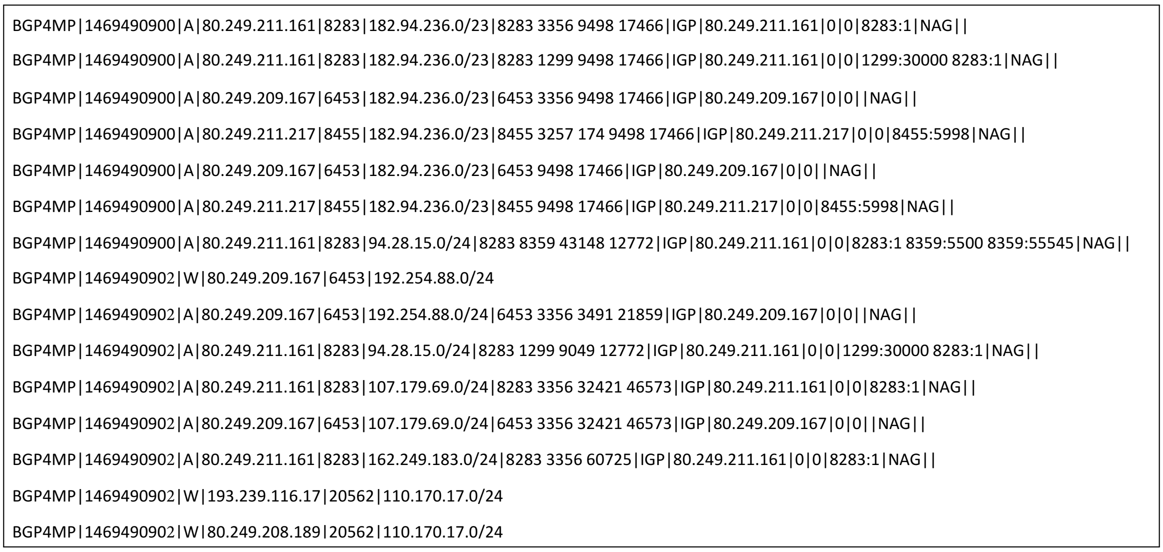


Figure 3. System Design



```
BGP4MP|1469490900|A|80.249.211.161|8283|182.94.236.0/23|8283 3356 9498 17466|IGP|80.249.211.161|0|0|8283:1|NAG||
BGP4MP|1469490900|A|80.249.211.161|8283|182.94.236.0/23|8283 1299 9498 17466|IGP|80.249.211.161|0|0|1299:30000 8283:1|NAG||
BGP4MP|1469490900|A|80.249.209.167|6453|182.94.236.0/23|6453 3356 9498 17466|IGP|80.249.209.167|0|0||NAG||
BGP4MP|1469490900|A|80.249.211.217|8455|182.94.236.0/23|8455 3257 174 9498 17466|IGP|80.249.211.217|0|0|8455:5998|NAG||
BGP4MP|1469490900|A|80.249.209.167|6453|182.94.236.0/23|6453 9498 17466|IGP|80.249.209.167|0|0||NAG||
BGP4MP|1469490900|A|80.249.211.217|8455|182.94.236.0/23|8455 9498 17466|IGP|80.249.211.217|0|0|8455:5998|NAG||
BGP4MP|1469490900|A|80.249.211.161|8283|94.28.15.0/24|8283 8359 43148 12772|IGP|80.249.211.161|0|0|8283:1 8359:5500 8359:55545|NAG||
BGP4MP|1469490902|W|80.249.209.167|6453|192.254.88.0/24
BGP4MP|1469490902|A|80.249.209.167|6453|192.254.88.0/24|6453 3356 3491 21859|IGP|80.249.209.167|0|0||NAG||
BGP4MP|1469490902|A|80.249.211.161|8283|94.28.15.0/24|8283 1299 9049 12772|IGP|80.249.211.161|0|0|1299:30000 8283:1|NAG||
BGP4MP|1469490902|A|80.249.211.161|8283|107.179.69.0/24|8283 3356 32421 46573|IGP|80.249.211.161|0|0|8283:1|NAG||
BGP4MP|1469490902|A|80.249.209.167|6453|107.179.69.0/24|6453 3356 32421 46573|IGP|80.249.209.167|0|0||NAG||
BGP4MP|1469490902|A|80.249.211.161|8283|162.249.183.0/24|8283 3356 60725|IGP|80.249.211.161|0|0|8283:1|NAG||
BGP4MP|1469490902|W|193.239.116.17|20562|110.170.17.0/24
BGP4MP|1469490902|W|80.249.208.189|20562|110.170.17.0/24
```

Figure 4. Example of BGP updates in a human readable format

is the nearest integer function. These BGP features are calculated every second based on time stamp of BGP updates. For example, there are 5 announcements and 3 withdrawals at time stamp 1469490900 in Unix format for BGP updates shown in Figure 4. In this time stamp, the value of TA is 19, A is 5, and then the value of AV is 4 (the nearest integer value of $\left[\frac{19}{5}\right]$ is 4). The calculation of the two BGP features for the whole BGP updates of Figures 4 is:

$$V = [7, 0, 8]$$
$$AV = [4, 0, 4]$$

Our BGP collector uses Net::BGP [13], a module of Perl software, to implement BGP. Net::BGP provides the required functionality to establish BGP peering and exchanging BGP updates. Officially, Net::BGP v0.16 does not support IPv6 BGP updates neither IPv6 BGP peer connection. CAIDA [14] has developed a patch for Net::BGP that allows BGP speaker to send IPv6 announcements through Multi-protocol Reachable NLRI, an optional attribute supported as part of Multi-protocol Extensions for BGP described in [15]. However, this patch does not support IPv6 prefix withdrawn and required BGP speakers with ADD-PATH capability, an extension to BGP protocol described in [16] to allow advertisement of multiple paths for the same prefix. Therefore, we implemented IPv6 route withdrawn through Multi-protocol Unreachable NLRI optional attribute, and removed ADD-PATH BGP capability for compatibility purposes.

B. Calculating RQA Measurements

This stage represents the calculation of RQA measurements for each BGP features calculated at previous stage. Before calculating RQA measurements for each BGP feature, we normalise the input time series data (BGP features) by subtracting the mean value to smooth noisy traces. Calculation RQA measurements is based on many parameters. These include time delay (τ), embedding dimension (m), recurrence threshold (ε), and window size (W). The values of (τ) and (m) can be calculated using MI and FNN respectively where the first minimum values of MI and FNN represent the values of (τ) and (m) while the value of (ε) can be calculated using the recommendation from [8] by choosing the threshold value less than 10% of the maximum phase space diameter. We use TISEAN package [17] to calculate the values of (τ) and (m) and [9] to calculate the value of (ε) which we provide it within RTBADT package [10].

C. Moving Average

The aim of this stage is to smooth the values of RQA measurements to enable detection of notable changes. A notable change in values of RQA measurements in term of increment or decrement indicates anomalous behaviour in a series of BGP traffic. To identify RQA measurement's changes that indicate an anomaly, we apply moving average technique based on the following format:

$$RQA_{alarm} = Mean(M) \pm sd(M) * X, \qquad (2)$$

where (M) is the length of the window size for the detection, (sd) is the standard deviation of data with length (M) seconds and (X) is the threshold value which represents number of times for the standard deviation. For example, $X = 5$ represents 5 standard deviations of data with length (M) seconds. We did a heuristic analysis to select the optimal values of the window size (M) and the threshold value(X) as well as (W), the window size for calculating RQA measurements. This includes $W = 200 \rightarrow 1200$ and $M = 200 \rightarrow 1200$ with an increment of 50 and $X = 1 \rightarrow 10$ with an increment of 1. Our analysis shows that windows size $W = 200$ seconds, $M = 1200$ seconds and the threshold value of moving average stage is $X = 9$ as optimal values to be used in our detection scheme.

D. Detection

Finally in this stage, the detection decision is made. The input of this stage are multiple RQA alarms calculated by the moving average stage while the output is an alarm that identifies detection of a BGP anomaly. We use all logical ORs based on the need to minimise False Positives (FPs) rate. FP refers to normal events that are classified as anomalous while False Negative (FN) refers to anomalous events that are classified as normal. We note that only TT measurement is able to detect BGP anomalies with zero value of FN and FP rates. However, in some cases TT measurements can detect BGP anomalies faster than T2. Consequently, we use a logical OR function

In this section, we have presented the design of our RQA scheme for detecting BGP anomalies. In the next section, we introduce RTBADT to detecting BGP anomalies and discussing the required arguments.

IV. Real-Time BGP Anomaly Detection Tool (RTBADT)

Real-Time BGP Anomaly Detection Tool (RTBADT) is a Perl script to detect BGP anomaly in near real-time. It also uses bash scripts to calculate RQA measurements. RTBADT connects to a peer AS that is intended to be monitored. Although RTBADT logs all detected BGP anomalies with their time stamps and the last 1200 seconds of BGP features, it offers the facility of sending an e-mail notification and real-time plot. These options can be activated by enabling -email and -plot command line arguments. The optional and mandatory arguments of the RTBADT tool are listed in Table I. A simple example of using RTBADT to monitor the peer AS65002 is shown in Figure 5 while the necessary command lines argument can be as follows:

```
#perl rtbadt-01.pl -colas 65003 -colip
    10.0.0.49 -peeras 650002 -peerip
    10.0.0.20 -email 1 -plot 1
```

In this example, the user enables the options of sending an e-mail notification when an anomaly is detected and enabling a real-time plot of BGP features and alarm detection.

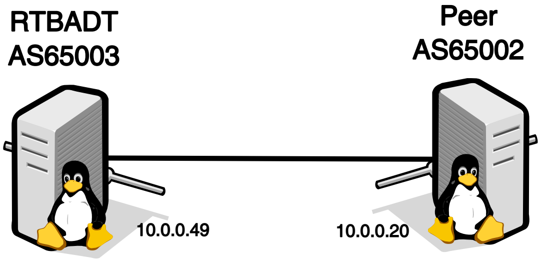


Figure 5. A Simple example to monitor a BGP speaker using RTBADT tool

Table I
BRT v0.2 tool command line arguments

Argument	Value	Optional	Description
-colas	<AS number>	No	RTBADT AS number
-colip	<IP address>	No	RTBADT IPv4 address
-peeras	<AS number>	No	Peer AS number
-peerip	<IP address>	No	Peer IPv4 address
-email	<0,1>	Yes	1=> send email notification, 0=> don't
-plot	<0,1>	Yes	1=> run real-time plot or 0=> don't
-help		Yes	Display RTBADT tool help

Table II
List of necessary Perl modules

Perl module	Purpose
Net::BGP	Provide the required functionality to establish BGP peering and receiving BGP traffic from BGP speaker which intended to monitor
Getopt::Long	Extend processing of command line options
Statistics::Basic	Provide a collection of statistics calculations such as mean and standard deviation that we need them at moving average stage
Mail::Sender	Sending mails with attachments through an SMTP server

To run RTBADT tool, RTBADT needs some Perl modules and other open source packages. The Perl modules are listed in the Table II. These modules can be downloaded and installed using cpan shell. For example, to install Net::BGP the following steps are requires:

```
#perl -MCPAN -e shell
cpan[1]> install Net::BGP
```

To apply IPv6 support patch to Net::BGP module, we provide a patch installation script that simplifies the process. This can be done using the following command:

```
# cd patch
# ./patch.sh
```

In addition to install the necessary modules, enabling e-mail option for sending a notification when an anomaly detected needs extra action. Users need to allow access to less secure apps in their e-mail setting. For example, allowing less secure apps in gmail account can be activated through the following link https://myaccount.google.com/lesssecureapps. It is important for users to send a test e-mail using the provided script name test_email.pl in the RTBADT package.

RTBADT tool is also required Gnuplot package to be installed. This is necessary if the user enable the optional argument of real-time plot. Gnuplot is an open source package for data visualization. It has the advantages of less resource requirements and easy-to-use. It can be installed in Ubuntu OS as follows:

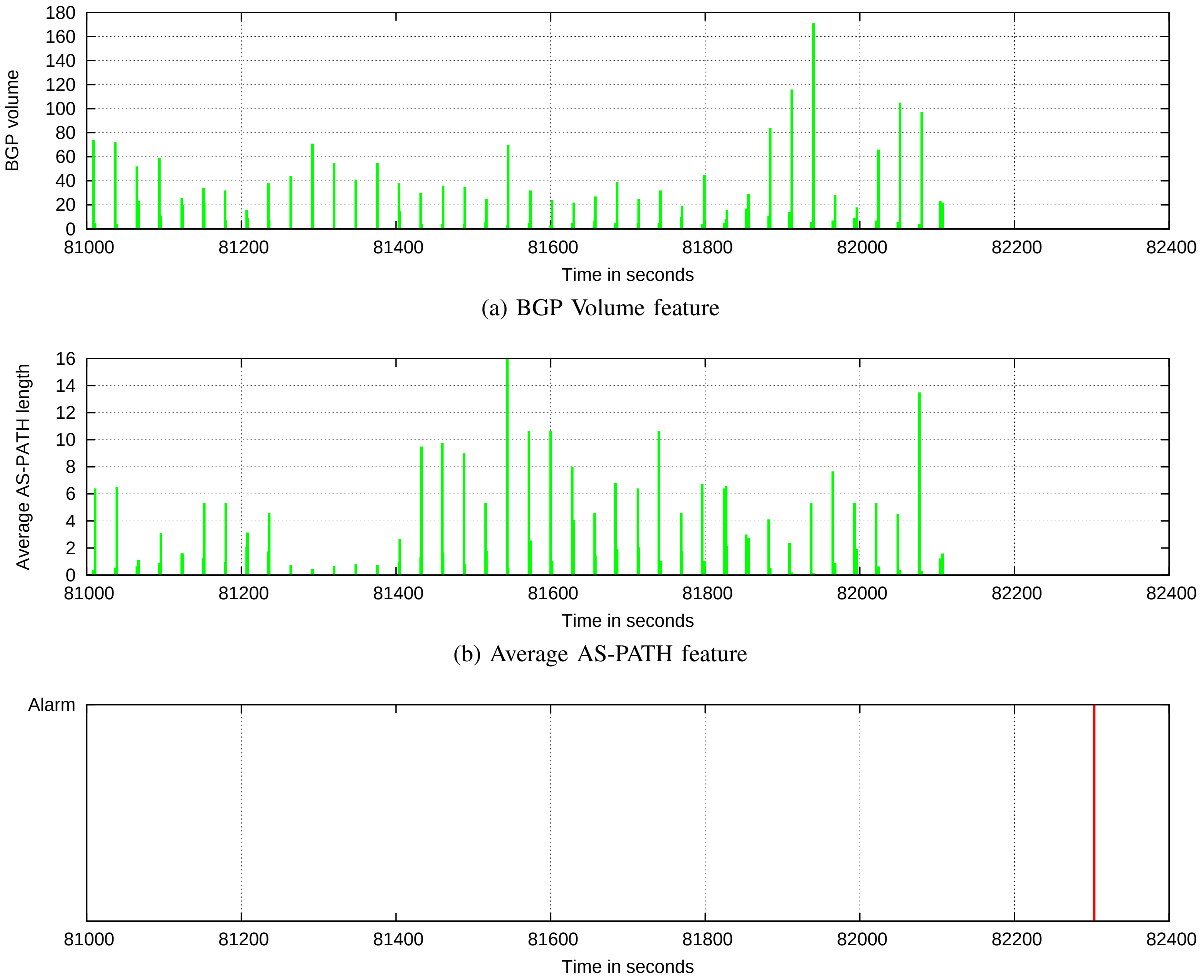
```
#apt-get install gnuplot-x11
```

V. Evaluation

To evaluate our RTBADT detection tool, we replay BGP traffic related to BGP events using BGP Replay Tool (BRT) [18]. BRT is a tool to replay past BGP updates with time stamps available online on [19]. We use the simple topology shown in Figure 5 to monitor BGP traffic sent by BRT speaker that sent BGP traffic related to BGP events.

A. Replay TMnet event

On the 12th of June 2015, ISP Telekom of Malaysia advertised 179,000 prefixes with preferable paths to the Level 3 which in turn accepted and propagated causing a significant instability to the global routing system [20]. We use BRT to replay BGP traffic sent by AS10102 during 12th of June 2015. As a result of the route leak, the peer AS10102 sent a significant number of BGP updates during the event. In addition to its ability to



(a) BGP Volume feature

(b) Average AS-PATH feature

(c) RTBADT alarm as a result of not receiving any BGP updates

Figure 6. RTBADT raised an alarm when the monitored BGP stopped sending BGP updates

rapidly detect BGP anomaly caused by high volume of BGP traffic, RTBADT also raises an alarm when a BGP speaker stops sending BGP traffic. Figure 6 shows RTBADT raised an alarm as a result of BRT stopped sending any BGP updates 196 seconds, this alarm is not as a result of lost connection. In total, RTBADT tool detected 8 BGP anomalies during the events as shown in Figure 7.

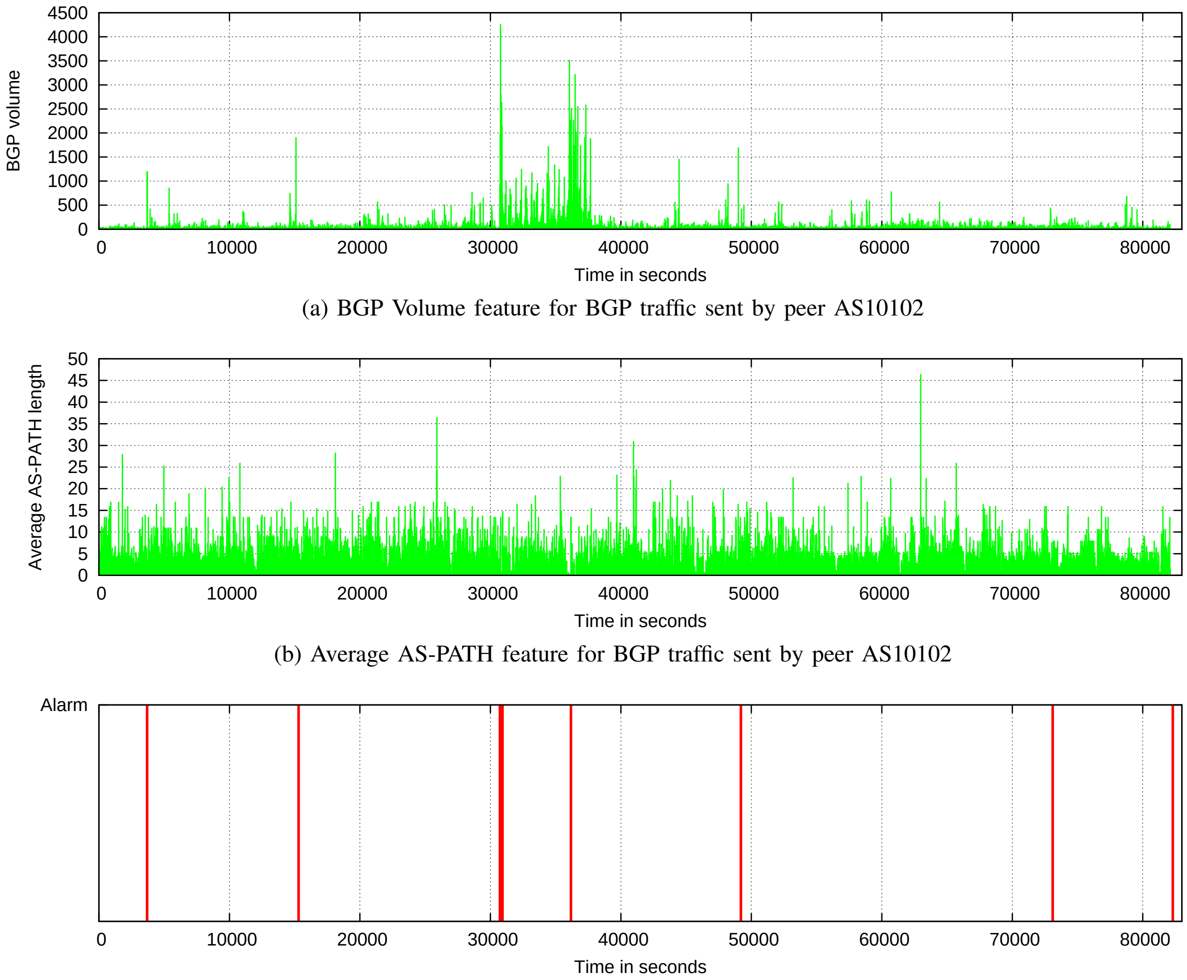
B. Known Issues

RTBADT has been tested on Unix OS such Ubuntu and shows reliable and stable performance. However, in some cases, the real-time plot window might stopped after a while. Users can close the stopped real-time plot window and run only the real-time option as follows:

```
$./realtime &
```

VI. Conclusions

BGP is vulnerable to different types of attacks that could produce a local impact on business relationship between individual ISPs or even a global impact to the Internet routing. Detecting BGP anomalies in real-time helps ISPs operators to prevent the impact of anomalies. In this paper, we introduced Real-Time BGP Anomaly Detection Tool (RTBADT), a tool to detect BGP anomalies in real-time. RTBADT uses Recurrence Quantification Analysis (RQA), an advanced non-linear statistical analysis technique based on the concepts of phase plane trajectory. RTBADT shows its ability to rapidly detect BGP anomalies. The evaluation of RTBADT has been made using a controlled testbed and injecting BGP traffic related to one of the most well-known BGP events. Our future work, will involve connecting RTBADT with a real BGP speaker.



(a) BGP Volume feature for BGP traffic sent by peer AS10102

(b) Average AS-PATH feature for BGP traffic sent by peer AS10102

(c) Detected BGP anomalies using RTBADT tool

Figure 7. Detected BGP anomalies using RTBADT during TMnet event

ACKNOWLEDGEMENTS

The development of BRT v0.2 has been made possible in part by "APNIC Internet Operations Research Grant" under the ISIF Asia 2016 grant scheme.

REFERENCES

[1] B. Al-Musawi, P. Branch, and G. Armitage, “BGP Anomaly Detection Techniques: A Survey,” *IEEE Communications Surveys Tutorials*, vol. 19, no. 1, pp. 377–396, Firstquarter 2017.

[2] J. Obstfeld, X. Chen, O. Frebourg, and P. Sudheendra, “Towards Near Real-Time BGP Deep Analysis: A Big-Data Approach,” *arXiv preprint arXiv:1705.08666*, 2017.

[3] X. Shi, Y. Xiang, Z. Wang, X. Yin, and J. Wu, “Detecting Prefix Hijackings in the Internet with Argus,” in *Proceedings of the 2012 ACM Conference on Internet Measurement Conference*, ser. IMC ’12. New York, NY, USA: ACM, 2012, pp. 15–28.

[4] Y. Huang, N. Feamster, A. Lakhina, and J. J. Xu, “Diagnosing Network Disruptions with Network-wide Analysis,” *SIGMETRICS Perform. Eval. Rev.*, vol. 35, no. 1, pp. 61–72, Jun. 2007.

[5] B. Al-Musawi, P. Branch, and G. Armitage, “Recurrence behaviour of BGP traffic,” in *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*. IEEE, 2017, pp. 1–7.

[6] B. Al-Musawi, P. Branch, and G. Armitage, “Detecting BGP instability using Recurrence Quantification Analysis (RQA),” in *2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC)*, Dec 2015, pp. 1–8.

[7] N. Marwan and J. Webber, CharlesL., “Mathematical and Computational Foundations of Recurrence Quantifications,” in *Recurrence Quantification Analysis*, ser. Understanding Complex Systems, C. L. Webber, Jr. and N. Marwan, Eds. Springer International Publishing, 2015, pp. 3–43. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-07155-8_1

[8] N. Marwan, M. C. Romano, M. Thiel, and J. Kurths, “Recurrence plots for the analysis of complex systems,” *Physics Reports*, vol. 438, no. 5, pp. 237–329, 2007.

[9] N. Marwan, “CROSS RECURRENCE PLOT TOOLBOX 5.18 (R29.3),” July 2015. [Online]. Available: http://tocsy.pik-potsdam.de/CRPtoolbox/

[10] B. Al-Musawi, “Real-Time BGP Anomaly Detection Tool (RTBADT),” January 2018. [Online]. Available: http://caia.swin.edu.au/tools/bgp/brt/rtbadt-0.1.tgz

[11] K. Ishiguro, “Quagga Routing Suite.” [Online]. Available: http://www.nongnu.org/quagga/

[12] L. Blunk, M. Karir, and C. Labovitz, “Multi-Threaded Routing Toolkit (MRT) Routing Information Export Format,” RFC 6396 (Standards Track), Internet Engineering Task Force, October 2011. [Online]. Available: http://tools.ietf.org/html/rfc6396

[13] S. J. Scheck, “Border Gateway Protocol version 4 speaker/listener librar,” September 2013. [Online]. Available: http://search.cpan.org/~sscheck/Net-BGP-0.16/lib/Net/BGP.pm

[14] CAIDA, “IPv6 announcement support patch for the Net::BGP perl modules,” February 2016. [Online]. Available: https://github.com/CAIDA/bgp-hackathon/tree/master/bgpd-3

[15] T. Bates, R. Chandra, D. Katz, and Y. Rekhter, “Multiprotocol Extensions for BGP-4,” RFC 4760 (Draft Standard), Internet Engineering Task Force, January 2007. [Online]. Available: https://tools.ietf.org/html/rfc4760

[16] D. Walton, E. Chen, and J. Scudder, “Advertisement of Multiple Paths in BGP,” RFC 7911, Internet Engineering Task Force, July 2016. [Online]. Available: http://www.ietf.org/rfc/rfc7911.txt

[17] R. Hegger, H. Kantz, and T. Schreiber, “Practical implementation of nonlinear time series methods: The TISEAN package,” *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 9, no. 2, pp. 413–435, 1999.

[18] B. Al-Musawi, R. Al-Saadi, P. Branch, and G. Armitage, “BGP Replay Tool (BRT) v0.2,” I4T Research Lab, Swinburne University of Technology, Melbourne, Australia, Tech. Rep. 170606A, 06 June 2017. [Online]. Available: http://i4t.swin.edu.au/reports/I4TRL-TR-170606A.pdf

[19] R. Al-Saadi, “BGP Replay Tool (BRT) v0.2,” May 2017. [Online]. Available: http://caia.swin.edu.au/tools/bgp/brt/brt-0.2.tgz

[20] A. Toonk, “Massive route leak causes Internet slowdown,” BGPMON, June 2015. [Online]. Available: http://www.bgpmon.net/massive-route-leak-cause-internet-slowdown/