isif asia

Project factsheet information

Project title	Rapid detection of BGP anomalies
Grant recipient	Centre for Advanced Internet Architectures (CAIA) Swinburne University of Technology PO Box 218, Hawthorn, Vic 3122, Australia +61-3-9214 5847 http://www.caia.swin.edu.au/
Dates covered by this report	01 – 09 – 2016 / 15 – 12 – 2017
Report submission date	01– 05 – 2017
Country where project was implemented	Australia
Project leader name	Bahaa Al-Musawi, balmusawi@swin.edu.au
Team members (list)	Associate Professor Philip Branch, pbranch@swin.edu.au Professor Grenville Armitage, garmitage@swin.edu.au
Partner organizations	None
Total budget approved	AUD 28,518
Project summary	The Border Gateway Protocol (BGP) is the Internet's default inter-domain routing protocol. BGP is vulnerable to different types of attacks such as hijacking, misconfiguration, and Denial of Service (DoS) attacks. Although they happen rarely, these attacks have threatened BGP's stability. Instability affects performance, processing load, and distribution balance of traffic load for BGP speakers. Recent statistics show approximately 20% of hijacking and misconfigurations lasted less than 10 minutes, but with the ability to pollute 90% of the Internet in less than 2 minutes. These statistics demonstrate the need for a real-time detection of BGP anomalies. Rapid detection of BGP anomalies helps Internet Service Providers (ISPs) to protect their networks and mitigate the propagation of anomalous BGP traffic. This project aimed to explore a new technique that quickly detects different BGP anomalies. The approach is based on the use of Recurrence Quantification Analysis (RQA), a non-linear analysis technique based on phase plane trajectories, to detect BGP anomalies. RQA is a way of extracting hidden information from statistics of dynamic systems. We have successfully used RQA to detect BGP instability caused by a high volume of BGP updates as well as hidden abnormal behaviour that may otherwise have passed without observation. However, in this project we developed software that makes use of our research. We produced two software tools. These are Real-Time BGP Anomaly Detection Tool (RTBADT), a tool that can be used by ISP's operator to rapidly (in seconds) detect BGP anomalies and a new version of the BGP Replay Tool (BRT) v0.1, a tool developed by team members to replay past BGP events using public BGP repositories such as Route Views project and RIPE or local log file. BRT will enable researchers to replay past BGP events in controlled testbeds and so gain an understanding of the behaviour of the BGP event. It also helps to understanding BGP behaviour using different types of router's operating system such as Quagga and Cisco. RTBADT will help ISPs mitigate the propagation of BGP anomalies which will lead to improved Internet reliability. The evaluation of the RTBADT is based on using the Virtual Internet Routing Lab (VIRL), a powerful network emulation platform developed by Cisco, and BRT as a control testbed. These tools and their technical reports are available on http://caia.swin.edu.au/tools/brt/.

Table of Contents

This work has been developed with the support provided by the Information Society Innovation Fund (ISIF Asia) – 2015, licensed under the Creative Commons Attribution-ShareAlike 4.0 International.

Background and Justification

The Border Gateway Protocol (BGP) is the Internet's default inter-domain routing protocol. It is responsible for managing network reachability information between Autonomous Systems (ASes), a set of routers under a single technical administration unit, with guarantees of avoiding routing loops. BGP was developed at a time when information provided by an AS could be assumed to be accurate. Consequently, it includes few security mechanisms and so is vulnerable to different types of events such as hijacking, misconfiguration, and Denial of Service (DoS) attacks. The consequences of these anomalies can range from a single to thousands of anomalous BGP updates. These consequences have threatened Internet performance and reliability [1]. 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 [2]. These statistics demonstrate the need for a new technique that can detect BGP anomalies in real-time. Real-time detection of BGP anomalies enables network operators to protect their network from the worst consequence of the anomalous behaviour and mitigates the propagation of BGP anomalies that threaten Internet stability.

BGP is a routing policy protocol where Internet Service Providers (ISPs) configure their BGP routers to enforce their business relationships, traffic engineering, and security-related policies. However, configuring BGP policies is not an easy task since the number of configuration lines in a single BGP router can range from hundreds to thousands [3]. A fault in configuration of a BGP router could produce a local impact or even a global impact. For example, the Pakistan Telecom incident is an example of BGP misconfiguration. In response to a censorship order from its government, the major ISP in Pakistan advertised an unauthorised YouTube prefix causing many ASes to lose access to the site [4]. Another example of BGP misconfiguration was recently caused by Telekom Malaysia (TMnet) which caused significant network problems for the global routing system. TMnet (AS4788) accidentally announced approximately 179,000 prefixes to Level3, the global crossing AS, leading to significant packet loss and slow Internet service around the world [5]. In addition to many reported events, other types of events remain unreported or even unnoticed [6].

Considerable research has been carried out into BGP anomaly. Generally, it can be classified as security improvements using cryptographic approaches or anomaly detection and mitigation [1]. Although cryptographic approaches can improve BGP security through mitigating BGP hijacking, they are not able to mitigate or identify BGP misconfiguration. Our interest is in this project is in the latter. The process of detecting real-time BGP anomalies is much harder than it seems at a first glance where BGP traffic has been identified as complex, voluminous, and noisy [7]. Furthermore, there is a lack of ground truth time stamps for BGP events. For example, what time in seconds did an event start?

In this project, we introduce two tools. These are Real-Time BGP Anomaly Detection Tool (RTBADT) and BGP Replay Tool (BRT). These tools are available on [8]. RTBADT is a tool that can be used by ISP operator to monitor and detect BGP anomalies through peering it with the intended peer AS. RTBADT uses techniques from Recurrence Quantification Analysis (RQA), an advance non-linear statistical analysis technique based on the concepts of phase plane trajectory [9], to determine if BGP traffic has changed behavior. RQA has successfully been used to detect anomalous behaviour in the underlying BGP traffic [10]. BRT is a tool to replay past BGP updates with time-stamps [11]. We use BRT to replay BGP traffic related to past BGP events within a controlled testbed where our controlled testbed is based on using Virtual Internet Routing Lab (VIRL) [12].

Project Narrative

The objective of this project is to produce techniques for the real-time detection of different types of BGP anomalies and replay past events so that they can be analysed within a controlled testbed. This will involve producing two new tools. These are Real-Time BGP Anomaly Detection Tool (RTBADT), a tool that can be used by ISPs operators to detect within a very short period of time different types of BGP anomalies, and a new version of BGP Replay Tool (BRT), a tool to replay past BGP events. BRT v0.2 overcomes the limitation of BRT v0.1 in term of supporting IPv6, connecting with different routers operating systems such as Quagga and real

This work has been developed with the support provided by the Information Society Innovation Fund (ISIF Asia) – 2015, licensed under the Creative Commons Attribution-ShareAlike 4.0 International.

Cisco routers, and peering multiple BGP peers. In this section, we describe the operation of BRT and RTBADT in some details. Further details are available on [8].

BGP Replay Tool (BRT)

BGP Replay Tool (BRT v0.2) is a tool for UNIX and Windows operating systems providing the ability to replay previously captured BGP updates downloaded from the public route repositories such as Route Views project [13] and RIPE [14] or local log file to test a variety of operations. These repositories provide BGP updates in MRT (Multi-Threaded Routing Toolkit) format described in [15]. The MRT format is not a human readable. Software such as bgpdump [16] and pybgpdump [17] are used to convert it to a readable format. Replying past BGP incidents into a control testbed helps to classify BGP traffic, understand BGP behaviour at BGP speaker level and investigating BGP behaviour with different routers operating systems (OSs) such as Cisco, Juniper, and Quagga.

BRT v0.2 extends the ability of BRT v0.1 [18] to peer with different BGP speakers operating systems such as Quagga and real Cisco routers. It also supports IPv6 and connecting to multiple peers. This tool can help researchers and operators to understand BGP behaviour in different circumstances.

BRT v0.2 uses Net::BGP [19], 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 [20] 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 Multiprotocol Extensions for BGP described in [21]. However, this patch does not support IPv6 prefix withdrawn and required BGP speakers with ADD-PATH capability, an extension to BGP protocol described in [22] 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. The BRT v0.2 and the patch are tested on Perl 5.20.2 and Net::BGP 0.16, and it is publicly available on [23].

The input of the BRT v0.2 tool is a human readable BGP updates with Unix time stamps, bgpdump with [-m] can be used for this purpose. BRT v0.2 provides and option to check that none of the AS numbers in the implemented topology are existing in any AS-PATHs of announced routes for the injected file. This is important to ensure that all injected BGP updates are forwarded between ASes as BGP guarantees of avoiding routing loops through preventing routes that contain its local AS number in the AS-PATH.

BRT v0.2 tool has optional and mandatory command line arguments as shown in Table 1. It is worth noting that IPv6 options should be specified if bgpdump update files contains IPv6 prefixes or when the BGP connection is made over IPv6 protocol.

Table 1- BRT v0.2 tool command line arguments

Argument	Value	Optional	Description
-brtas	<AS number>	No	BRT AS number
-brtip	<IPv6 address>	No	BRT IPv4 address
-brtipv6	<IP address>	Yes	BRT IPv6 address
-peeras	<AS number>	No	Peer AS number
-peerip	<IP address>	No	Peer IPv4 address

This work has been developed with the support provided by the Information Society Innovation Fund (ISIF Asia) – 2015, licensed under the Creative Commons Attribution-ShareAlike 4.0 International.

Argument	Value	Optional	Description
-peeripv6	<IPv6 address>	Yes	Peer IPv6 address
-ipv6	Yes		Connect to a peer using IPv6. This is necessary if the connection via IPv6 not IPV4; otherwise, it can be ignored
-f	<filename>	No	BGP update file in human readable with Unix format
-m	<filename>	Yes	Connect to multiple peers specified in <filename>
-s	<filename>	Yes	Check that none of the ASes in the implemented topology are existing in any AS-PATHs of announced routes for the injected file
-v		Yes	Verbose mode
-help		Yes	Display BRT tool help

An example for using the BRT for a simple BGP topology shown in Figure 1 is:
$ perl brt-0.2.pl -brtas 65001 -brtip 172.16.2.2 -peeras 65002 -peerip 172.16.2.1 -f BGP_updates

Figure 1 –Simple topology for connecting BRT

The evaluation of the BRT v0.2 has been made using three different types of testbeds. These include real Cisco routers, Virtual Internet Routing Lab (VIRL) [12], an emulation platform by Cisco, and Quagga using generated BGP updates and past BGP instability incidents. Figure 2 shows number of IPv6 announcements for BGP traffic related to TMnet event, downloaded by route-views4 in the Routeviews project, sent by BRT and collected by Quagga.

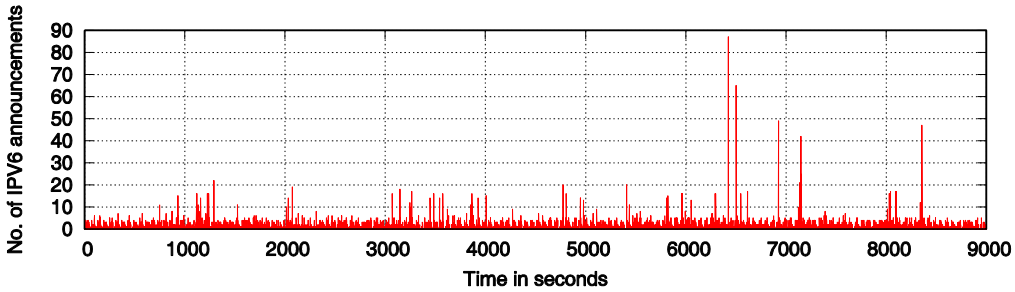

Figure 2-A – Sample of IPv6 announcement for the injected BGP traffic

This work has been developed with the support provided by the Information Society Innovation Fund (ISIF Asia) – 2015, licensed under the Creative Commons Attribution-ShareAlike 4.0 International.

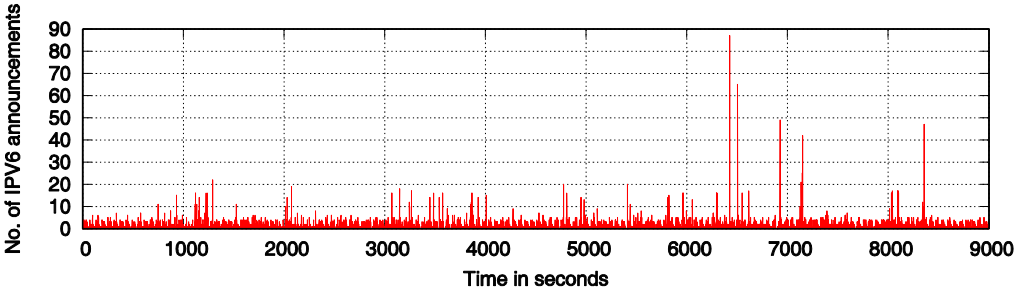

Figure 2-B – Sample of IPv6 announcement for the collected BGP traffic

Figure 2 – Sample of BGP features for the injected and collected for the TMnet incident

Figure 3 shows Mr. Bahaa Al-Musawi, the project leader, evaluates the operation of BRT v0.2, while Figure 4 shows Mr. Rasool Al-Saadi, the developer of BRT v0.2, to replay BGP traffic into VIRL control testbed.

Figure 3 – Evaluating BGP Replay Tool (BRT) using generated BGP updates and past BGP events

Figure 4 - Using Cisco Virtual Internet Routing Lab (VIRL) and BRT to evaluate detection of BGP anomaly.

This work has been developed with the support provided by the Information Society Innovation Fund (ISIF Asia) – 2015, licensed under the Creative Commons Attribution-ShareAlike 4.0 International.

Real-Time BGP Anomaly Detection Tool (RTBADT)

RTBADT is a tool to detect BGP anomalies in near real-time. It uses the technique of Recurrence Quantification Analysis (RQA), is an advanced non-linear statistical analysis technique using phase space concepts, to detect BGP anomalies. 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 [9].

We have shown in [10] and [24] that BGP traffic has the characteristic of recurrence behaviour. RQA has been successfully used to rapidly detect BGP anomalies as well as other hidden anomalous periods that may otherwise pass without detection [10]. 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 behaviour and behaviours that indicate anomalies. Furthermore, RQA is able to detect behaviour that cannot be detected with other techniques.

RQA needs three parameters which they have to be carefully selected. These are time delay (τ), embedding dimension (m), and the recurrence threshold (ε). Selecting non-optimal values for RQA's parameters can produce different structures for the same input data. Different algorithms can be used to determine these parameters. 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. 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 first minimum values of MI and FNN represent the values of time delay and embedding dimension respectively. 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. a recommendation from [9] suggests that the threshold has to be selected less than 10% of the maximum phase space diameter that we use in our tool. We provide a script that calculate these parameters within RTBADT package.

The system design of RTBADT tool comprised of four stages as shown in Figure 5. These are BGP collector, calculating RQA measurements, moving average, and detection.

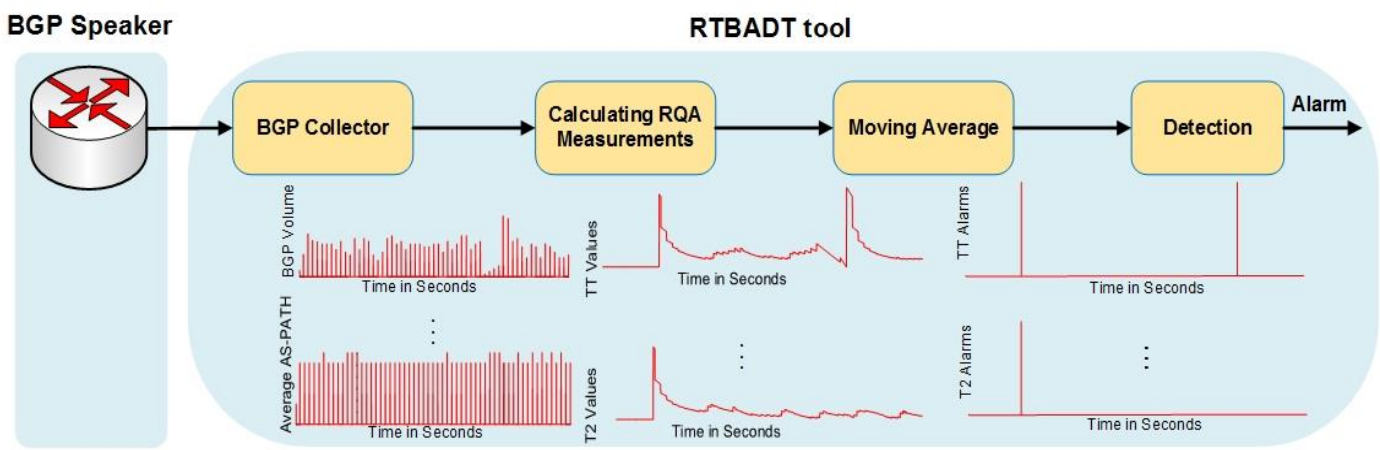

Figure 5 – System Design for RTBADT

The purpose of BGP collector is to provide real-time collecting of BGP traffic. The most widely used technique to collect BGP traffic is using Quagga. Quagga is a routing software package that provides TCP/IP based routing

This work has been developed with the support provided by the Information Society Innovation Fund (ISIF Asia) – 2015, licensed under the Creative Commons Attribution-ShareAlike 4.0 International.

services for different protocols such as OSPF, IS-IS, and BGP [25]. Unlike Quagga which is used to establish BGP peering and store BGP traffic in MRT format, 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 is BGP volume (total number of announcements and withdrawals) and average length of AS-PATH calculated every second.

At the second stage, the calculation of RQA measurements for each BGP features is done. 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 [9]. Our heuristic analysis shows that TT and T2 are the most effective RQA measurements to detect BGP anomalies. The output of this stage is TT and T2 for each BGP feature (BGP volume and average AS-PATH).

A significant change in the values of RQA measurements indicate a BGP anomaly. Therefore, we apply moving average method 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. The output of moving average stage are multiple RQA alarms. The detection stage is simple represents all logical ORs. This been made based on the need to minimise the rate of False Positive (FP), normal events that are classified as anomalous.

RTBADT v0.1 tool has optional and mandatory command line arguments as shown in Table 2. A simple example of using RTBADT to monitor the peer AS65002 is shown in Figure 6 while the necessary command lines argument as follows:

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

Table 2- RTBADT v0.1 tool command line arguments

Argument	Value	Optional	Description
-colas	<AS number>	No	BRT AS number
-colip	<IPv6 address>	No	BRT 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

This work has been developed with the support provided by the Information Society Innovation Fund (ISIF Asia) – 2015, licensed under the Creative Commons Attribution-ShareAlike 4.0 International.

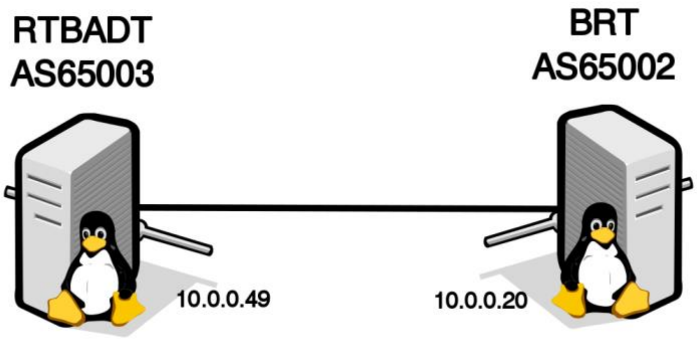

Figure 6 – Simple example to monitor a BGP speaker using RTBADT

To evaluate the performance of RTBADT tool to detect BGP anomalies in real-time, we use BGP traffic related to TMnet event, an example of BGP misconfiguration caused by ISP Telekom of Malaysia. 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 [5]. 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. RTBADT tool detected 7 BGP anomalies during the events as well as raised an alarm when no BGP traffic sent by BRT as shown in Figure 7.

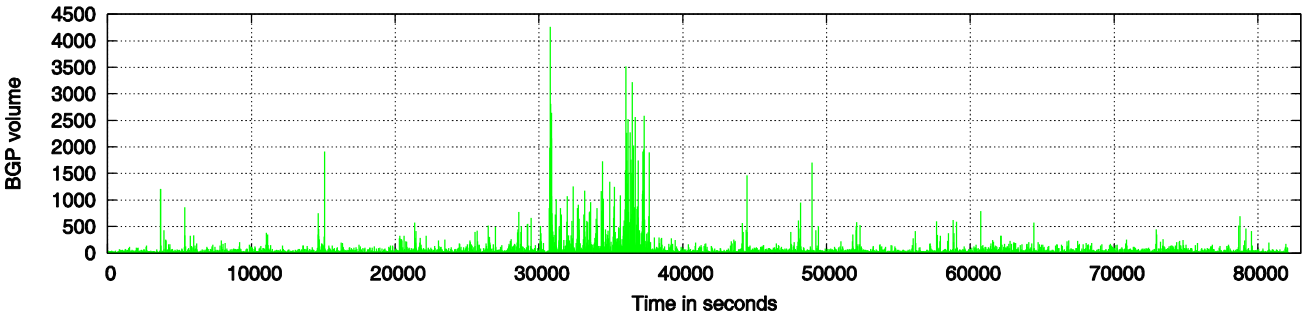

Figure 7-A – BGP Volume feature for BGP traffic sent by peer AS10102

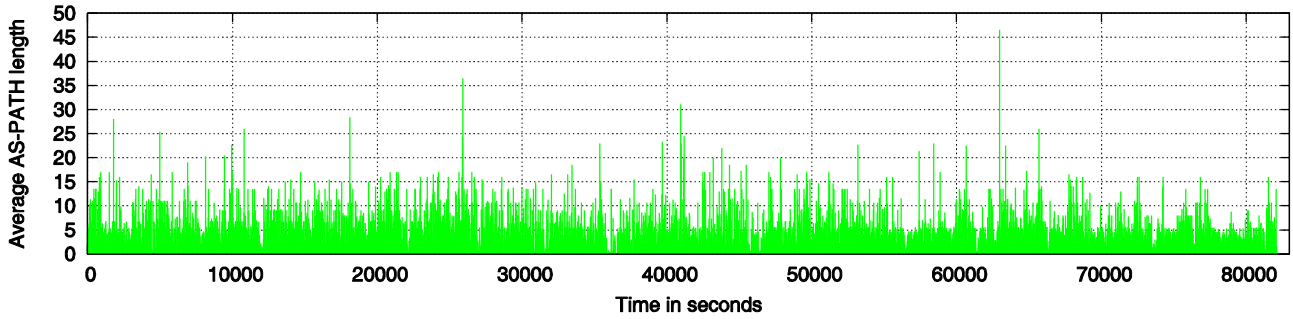

Figure 7-B – Average AS-PATH feature for BGP traffic sent by peer AS10102

This work has been developed with the support provided by the Information Society Innovation Fund (ISIF Asia) – 2015, licensed under the Creative Commons Attribution-ShareAlike 4.0 International.

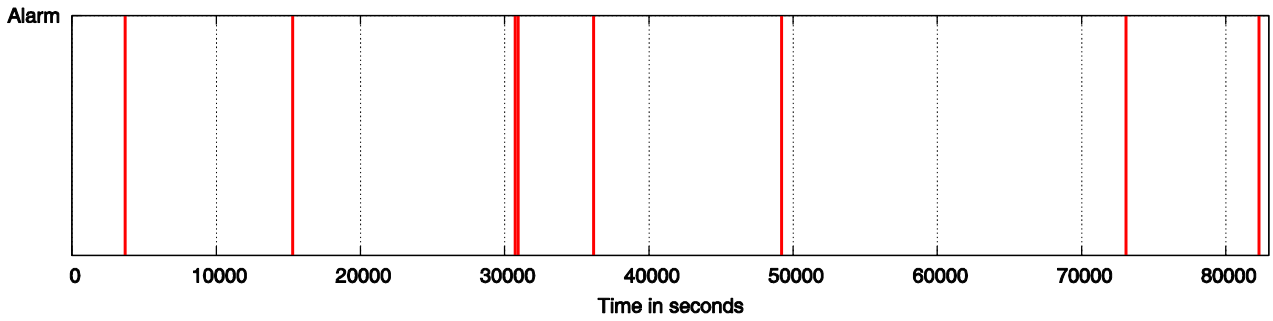

Figure 7-C – Detected BGP anomalies using RTBADT tool

Figure 7 – Detected BGP anomalies using RTBADT during TMnet event

Indicators

Indicators	Baseline	Progress assessment	Course of action
Develop a new version of BGP Replay Tool (BRT) v0.1 [27], a tool to replay past BGP updates. The new version will overcome the limitations of BRT v0.1 such as supporting IPv6 and peering with multiple peers.	BRT v0.1 is currently available on [27]. BRT v0.1 does not support peering with Quagga and real Cisco routers. It also does not support multiple peering.	BRT v0.2 is now available on [23]. BRT v0.2 extends the ability of BRT v0.1 to peer with different BGP speakers operating systems such as Quagga and real Cisco routers. It also supports IPv6 and connecting to multiple peers.	No further action required.
Evaluating the capability of RQA to detect different types of BGP anomalies under a controlled testbed.	RQA approach has successfully used in [10] to detect past BGP events without considering the rate of false positive (FP) and false negative (FN). The evaluation of RQA has been carried out using a controlled testbed to produce low rate of FN and FP.	The evaluation of RQA scheme has been applied using 14.28 days of BGP traffic related to past well-known and synthesised BGP traffic. RQA scheme shows its ability to detect 46 TP alarms and 5 FP alarms detected with 62 seconds as a detection delay.	No further action required.
Integration of Recurrence Quantification Analysis software into a module able to take BGP traffic and identify if it is anomalous.	The modules that carry out the RQA are available but are not integrated.	RTBADT is now available on [27]. The evaluation of RTBADT has been carried out using BRT v0.2 and a controlled testbed.	Use RTBADT tool to connect with real BGP speakers.
Create a website that describes the project and contains all necessary tools.	The website is not available	http://www.caia.swin.edu.au/tools/bgp/brt/ domain is now available. The website provides all necessary background information and tools about the projects.	No further action required.

This work has been developed with the support provided by the Information Society Innovation Fund (ISIF Asia) – 2015, licensed under the Creative Commons Attribution-ShareAlike 4.0 International.

Project implementation

Project activities	Input	Outputs	Timeline	Status
Develop a new version of BRT v0.1 tool	Hire a software developer	BGP Replay Tool (BRT) v0.2 [23] is ready. Evaluation of RQA for low rate of FP and FN has been assessed.	January 2017 – April 2017	Completed
Create RTBADT tool to detect anomalous behaviour of BGP using RQA technique	Hire software developer	RTBADT is now available on [27]. The evaluation had been done using a controlled testbed and BGP traffic related to well-known BGP events.	April 2017 – November 2017	Completed

Communication and dissemination

The website of the project has been created and it is available on www.caia.swin.edu.au/tools/bgp/brt. It provides all necessary background information about the project, testbed, techniques used, links to the technical reports, and tools. The project was presented at internally at Swinburne University of Technology [28]. It was also presented at APNIC 44, technical operations II session, that was held in Taichung, Taiwan 12-14 September 2017 [29]. The project admired some ISPs, for example, Mr. Simon Baroi, the assistance general manager at Fiberathome company, was interested to use RTBADT tool. He suggested to provide a peer connection and monitor his network. This action will be implemented soon. Furthermore, Mr. Shishio Tsuchiya, a senior systems' engineer at Arista company, was very interested to integrate RTBADT tool in their routers products.

Project Management and Sustainability

Project Management Overview

The project had a delayed start because of funds transfer issues. Nevertheless, progress has been good and we completed the project in a good time frame. The management of the project was a big challenge for the project leader, a PhD candidate at his fourth year, as this is the first experiment to manage such a project. Furthermore, the process of managing writing thesis and finalising the project at same time was another challenge. However, the team member and Swinburne management staff provided all necessary support to make this project went smoothly.

Most development effort is on developing a new version of the BGP Replay (BRT) and Real-Time BGP Replay Tool (RTBADT). BRT will be useful for both ISPs and researchers in term of investigating BGP anomalies. RTBADT will help ISPs to detect BGP anomalies in near real-time and mitigate the propagation of anomalous traffic. The widely use of RTBADT will help to improve Internet stability through mitigating the propagation of anomalous BGP traffic at early stage.

Sustainability and Capacity Building

Development of the tools will enable ISPs to capture BGP traffic and determine if it is anomalous. It will enable ISPs and researchers to replay events enabling a forensic analysis of the event. The scheme used within RTBADT has attracted considerable industry support. For example, we have been granted access to Virtual Internet Routing Lab (VIRL) under academic license [12]. We used this extensively for our experimental work and development of the software for the ISIF funded project. In addition, there some ISPs operator and engineers from other industries who show their interest to use the tool.

This work has been developed with the support provided by the Information Society Innovation Fund (ISIF Asia) – 2015, licensed under the Creative Commons Attribution-ShareAlike 4.0 International.

Project Outcomes and Impact

Project Outcomes

The project will have the following outcomes:

- A new tool to replay BGP traffic
- The ability to use the tool to analyse past anomalous BGP events
- A new tool to identify if BGP traffic is anomalous
- The consequent ability for ISPs to identify if they are observing anomalous traffic

Project Impact

Recent statistics and trends of BGP anomalies show approximately 20% of BGP anomalies lasted less than 10 minutes but were able to pollute 90% of the Internet in less than 2 minutes. RTBADT tool shows it ability to detect BGP anomalies in near real-time. Early detection of BGP anomalies mitigate the propagation of anomalous BGP traffic and reduce the impact to pollute the Internet. The widely use of RTBADT tool can contribute to a more robust Internet.

The two tools forming the contribution of the project will enable identification of BGP anomalies as they occur and forensic examination of BGP anomalies after the event. This second tool will be useful to researchers as well as ISPs.

Overall Assessment

The project has thus far been a success. The objectives of the project include producing real-time detection of different types of BGP anomalies and introducing another tool to replay past BGP events have been met. The evaluation of the tools has been made using semi-realistic controlled testbed. The evaluation of our detection tool shows its ability to detect BGP anomalies within 62 seconds.

The outputs from the project has attracted the community to use the tools and get benefits. There has been some communication about when they could use the tools and how which will go further after integrating the RTBADT tool with GUI capability.

A technical report that describes the use of BGP Replay Tool (BRT) v0.2 is now available on [11]. Another technical that describe the operation of Real-Time BGP Anomaly Detection Tool (RTBADT) will be available soon on [28]. Furthermore, an academic paper that describe the RQA scheme and RTBADT tool will be submitted to an academic journal.

We also keen to motivate ISPs to adopt using our detection tool through establishing a peer connection to detect BGP anomaly as a first toward they use it by own.

Recommendations and Use of Findings

The direct users of this project will be ISPs who need a new technique to identify the early stages of a BGP event that can lead to serious compromise of their network services. Researchers can also get a benefit from this project. They can use BRT to replay past BGP events and evaluate their anomaly detection techniques.

To motivate ISPs operator to use the detection tool starts from asking some of ISPs to have a peer connection and detect anomalies at our side. A weekly or daily report can be provided the operator based on demand shows the state of their network. This report can supply information such as how many detected anomalies, time delay of detection, how many FP alarms raised, and the fluctuation of BGP features during one week.

This work has been developed with the support provided by the Information Society Innovation Fund (ISIF Asia) – 2015, licensed under the Creative Commons Attribution-ShareAlike 4.0 International.

Bibliography

[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] 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.

[3] N. Feamster and H. Balakrishnan, “Detecting BGP Configuration Faults with Static Analysis,” in Proceedings of the 2Nd Conference on Symposium on Networked Systems Design & Implementation - Volume 2, ser. NSDI’05. Berkeley, CA, USA: USENIX Association, 2005, pp. 43–56.

[4] M. A. Brown, “Pakistan Hijacks YouTube,” Renesys Blog, February 2008. [Online]. Available: http://www.renesys.com/2008/02/pakistan-hijacksyoutube-1/

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

[6] M. Wählisch, O. Maennel, and T. C. Schmidt, “Towards Detecting BGP Route Hijacking Using the RPKI,” SIGCOMM Comput. Commun. Rev., vol. 42, no. 4, pp. 103–104, Aug. 2012.

[7] 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.

[8] B. Al-Musawi, “Rapid detection of BGP anomalies,” June 2017. [Online]. Available: http://caia.swin.edu.au/tools/bgp/brt/

[9] 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.

[10] Al-Musawi, B., Branch, P., and Armitage, G. “Detecting BGP Instability Using Recurrence Quantification Analysis (RQA)”. In Proceedings of the IEEE Performance Computing and Communications Conference (2015), IPCCC ’15.

[11] B. Al-Musawi, R. Al-Saadi, P. Branch, and G. Armitage, "BGP Replay Tool (BRT) v0.2", I4TRL Technical report 170606A, 06 June 2017. [Online]. Available: http://i4t.swin.edu.au/reports/I4TRL-TR-170606A.pdf.

[12] J. Obstfeld, S. Knight, E. Kern, Q. S.Wang, T. Bryan, and D. Bourque, “VIRL: the virtual internet routing lab,” in Proceedings of the 2014 ACM conference on SIGCOMM. ACM, 2014, pp. 577–578.

[13] University of Oregon, “University of Oregon Route Views Project.” [Online]. Available: http://www.routeviews.org/

[14] Reseaux IP Europeens Network Coordination Center. [Online]. Available: http://www.ripe.net/

[15] 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

[16] RIPE NCC RIS Projec, “bgpdump.” [Online]. Available: https://bitbucket.org/ripencc/bgpdump/wiki/Home

[17] J. Oberheide, “pybgpdump.” [Online]. Available: https://jon.oberheide.org/pybgpdump/

[18] Al-Musawi, Bahaa, Philip Branch, and Grenville Armitage. "BGP Replay Tool (BRT) v0.1" Centre for Advanced Internet Architectures, Swinburne University of Technology, Melbourne, Australia, Tech. Rep. CAIA-TR-160304A, 04 March 2016. [Online]. Available http://caia.swin.edu.au/reports/160304A/CAIA-TR-160304A.pdf

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

This work has been developed with the support provided by the Information Society Innovation Fund (ISIF Asia) – 2015, licensed under the Creative Commons Attribution-ShareAlike 4.0 International.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] Al-Musawi, B., Branch, P., and Armitage, G. “Recurrence Behaviour of BGP Traffic”. In Proceedings of the International Telecommunication Networks and Applications Conference (ITNAC) 2017, Melbourne, Australia.

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

[26] B. Al-Musawi, “BGP Replay Tool (BRT)v0.1,” March 2016. [Online]. Available: http://caia.swin.edu.au/tools/bgp/brt-0.1.tgz.

[27] B. Al-Musawi, “RTBADT - Real-Time BGP Anomaly Detection Tool v0.1,” December 2017. [Online]. Available: http://caia.swin.edu.au/tools/bgp/brt/rtbadt-0.1.tgz.

[28] B. Al-Musawi, " Rapid Detection of BGP Anomalies", I4TRL Research Lab Seminars, 20 July 2017. [Online]. Available:http://i4t.swin.edu.au/seminars/details/170720A.html.

[29] APNIC 44, “Technical Operations II.” [Online]. Available: https://conference.apnic.net/44/program/schedule/#/day/6/technical-operations-ii.

This work has been developed with the support provided by the Information Society Innovation Fund (ISIF Asia) – 2015, licensed under the Creative Commons Attribution-ShareAlike 4.0 International.