RDTD: A Tool for Detecting Internet Routing Disruptions at AS-Level

Bahaa Al-Musawi
Faculty of Engineering, University of Kufa, Iraq

Mohammed Falih Hassan
Faculty of Engineering, University of Kufa, Iraq

Sabah M. Alturfi
Faculty of Law, University of Kerbala, Iraq

Abstract: Anomalous events such as link failure, misconfiguration, and Denial of Service attacks can affect the Internet inter-domain routing protocol. This effect can range from small to large-scale impact. While large-scale events can be detected using one or multiple global monitoring points, small-scale events need monitoring at the Autonomous System (AS) level. This paper presents a Real-time Detection Tool for Internet routing protocol Disruptions (RDTD) at AS-level. RDTD is a black-box statistical approach that detects disruptions based on observing changes in the underlying behaviour of a series of inter-domain routing updates rather than information contained in inter-domain routing updates. The RDTD can be connected to a designated AS to detect disruptions at that AS or to one of the collectors at public vantage points to detect the Internet routing disruptions from the public vantage-point's view. The evaluation of the detection tool has been made through replaying route traffic related to one of the most well-known events within a controlled testbed. Our evaluation shows the ability of the detection tool to detect route leak in near real-time without requiring a long history of data. RDTD can also detect hidden anomalous behaviour in the underlying traffic that may pass without detection.

Keywords: Inter-domain routing, route leak, emulation, anomaly detection, testbed.

1. Introduction

The Internet is a decentralized global network that consists of tens of thousands of Autonomous Systems (ASes); an Internet Service Provider (ISP) is an example of an AS. ASes use inter-domain routing protocols such as Border Gateway Protocol (BGP) to communicate with other ASes and intra-domain routing protocols such as Open Shortest Path First (OSPF) to communicate between routers within an AS (Al-Musawi, Branch, & Armitage, 2017). ISP

http://doi.org/10.18080/jtde.v8n2.244

operators need to monitor their networks including the exchange of information between routers within their domain (intra-domain) and with other ASes (inter-domain). In this paper, our interest is in the latter. In particular, we are interested in the rapid detection of inter-domain routing disruptions at the AS-level.

BGP is the de-facto Internet routing protocol responsible for exchanging Network Reachability Information (NRI) between ASes. Although many attempts have been made to improve its security, it is still vulnerable to different types of disruptions that threaten its stability. ISPs increasingly suffer from large-scale or small-scale route disruptions in recent years. Recent statistics on the Internet inter-domain routing protocol performance show approximately 20% of the hijackings and misconfigurations lasted less than 10 minutes but were able to pollute 90% of the Internet within 2 minutes (Shi *et al.*, 2012). These statistics demonstrate the need for a new tool that can detect different types of inter-domain routing disruptions in real-time. ISP operators need to react quickly by tuning their configuration to eliminate the propagation of anomalous inter-domain routing traffic or notify other ISPs about serious reachability issues. In this paper, we introduce a Real-time Detection Tool for Internet routing protocol Disruptions (RDTD) at AS-level. RDTD is a black-box statistical approach that does not rely on the information contained in inter-domain routing updates. Alternatively, it detects disruptions based on the key observation that most disruptions correspond to changes in the underlying behaviour of a series of inter-domain routing updates. RDTD is based on using Recurrence Quantification Analysis (RQA), an advanced non-linear statistical analysis technique based on the concept of phase plane trajectory (Trulla *et al.*, 1996; Webber & Zbilut, 2005). Detecting Internet routing disruption at AS-level helps to mitigate the effect of disruptions from propagating to other ASes. In this paper, we do not mainly focus on the concept of RQA: Al-Musawi (2018) provides such a study. Instead, we focus on how to integrate this technique into a tool that can be used by network operators.

Inter-domain routing disruptions can result from different sources, such as hijacking, Denial of Service (DoS) attacks, hardware failure, software bugs, faulty equipment, and misconfiguration by operators. Many types of inter-domain routing disruptions have been noticed, such as TMnet route leak (Toonk, 2015) and Moscow blackout (Roudnev, 2005). Although these events have been noticed as a result of their size and effect on the inter-domain routing traffic and the business relationship among many ASes, other types of events remain unreported or even unnoticed. The RDTD was designed to be applied at AS-level so it can help ISP operators to detect different types of disruptions before their effect spreads to other ASes.

The rest of this paper is organised as follows: Section 2 explores related work in the detection of inter-domain routing disruptions. In section 3, we introduce the structure and design of the RDTD tool. Section 4 shows the operation and configuration setup to run RDTD. Section 5

http://doi.org/10.18080/jtde.v8n2.244

presents the evaluation of RDTD through replaying one of the most recent well-known BGP events and compares its performance with other techniques. In section 6, we conclude our work and outline future directions.

2. Related Work

One of the earliest efforts of identifying inter-domain routing disruptions was by Labovitz, Malan & Jahanian (1998). To detect Internet routing disruptions, the authors applied the Fast Fourier Transform (FFT) to a series of BGP updates. Although the technique did not provide a way to identify the cause or source of routing disruptions, it demonstrated that rapid changes in the routing traffic are correlated with disruptions. Following the work by Labovitz, other techniques were applied to the problem of inter-domain routing identification. These included using statistical analysis techniques (Deshpande *et al.*, 2009; Huang *et al.*, 2007), validation of Internet routing traffic based on historical routing data sets (Haeberlen *et al.*, 2009; Shi *et al.*, 2012), and tools to detect Internet routing disruptions (Luckie, 2010; Lutu, Bagnulo & Maennel, 2013).

Huang *et al.* (2007) introduced a technique based on using Principal Component Analysis (PCA) and subspace method to detect AS node, link, and peer failure. They used inter-domain routing volume as a single feature extracted every 10 minutes with a window size of 200 minutes. Although the technique can detect and identify the three types of failure, it requires information about router configurations. Their technique cannot work in real-time, detecting the three types of failures in a range of 9-96 minutes.

The Generalized Likelihood Ratio Test (GLRT) is a standard statistical technique used in hypothesis testing. Deshpande *et al.* (2009) adopted it as an instability detection technique. Their approach used statistical pattern recognition, which incorporated the technique. The approach was able to detect different types of inter-domain disruptions such as the Moscow blackout, Nimda, and Panix domain hijack. However, it is slow, typically requiring around one hour to detect instability.

Haeberlen *et al.* (2009) presented a prototype to detect inter-domain routing faults at the AS-level called NetReview. This prototype uses 1 year of routing data to detect inter-domain disruptions, where inter-domain disruptions include node and link failure, misconfiguration, policy violations, and attacks. Although NetReview can detect in near real-time different types of inter-domain disruptions and identify their source cause, it requires each AS to reveal information related to its policy configuration. In addition, it has a scalability problem because of the need to store large log files, a particular issue for ISPs.

http://doi.org/10.18080/jtde.v8n2.244

Argus (Shi *et al.*, 2012) is a system to detect prefix hijacking and identify the attacker in real-time. Argus uses the control plane to detect bogus routes and the data plane to verify anomalies through checking their reachability. This system uses more than 2 months of historical inter-domain routing data to classify new data as normal or suspicious, then checks the reachability of prefixes to verify the suspicious updates through using tools such as CAIDA's Ark. Although Argus can detect hijacking and identify the source in near real-time, it cannot detect other types of disruptions such as misconfiguration and DoS attacks.

Scamper (Luckie, 2010) is a packet prober designed to support large-scale Internet measurements. It is a tool that implements most of the classical Internet measurement tools such as ping and traceroute that supports IPv4 and IPv6 probing. It was mainly designed to help researchers for scientific experiments rather than building accurate instrumentation. However, Scamper was not designed to detect Internet route disruptions.

BGP Visibility Scanner (Lutu, Bagnulo & Maennel, 2013) is a tool that can help ISP operators to validate the correct implementation of their routing policies through monitoring their routes from multiple observation points. However, this tool is not able to detect different types of disruptions such as Internet route leaks. Furthermore, it requires using multiple monitoring points.

Cyclops (Chi, Oliveira & Zhang, 2008) is a system that displays AS-level connectivity and changes as inferred from Public-View. Cyclops collects data related to AS-level topology from different sources such as looking glasses, inter-domain routing tables and updates of hundreds of ASes across the Internet. It helps the network operators to view their AS connectivity as seen from other ASes, which can provide a comparison between the observed connectivity and the intended connectivity.

Unlike different inter-domain routing disruptions tools, we introduce RDTD, a real-time detection tool to detect Internet inter-domain disruptions at AS-level. RDTD is based on using non-linear statistical analysis calculations that utilise calculations of hidden information occurring in the inter-domain routing traffic to detect disruptions. This information represents recurrence features in a series of Internet routing traffic. Our work differs from others in that we overcome their drawbacks by detecting disruptions in real-time and without requiring a long history of data: our tool requires 1200 seconds of historical data to detect disruptions in a range of 1-200 seconds.

3. Architecture and Design

Real-time Detection Tool for Internet routing Disruptions (RDTD) enables ISP operators to detect different types of Internet routing disruptions in near real-time. Real-time detection

http://doi.org/10.18080/jtde.v8n2.244

enables the operators to mitigate the effect of disruptions to other ASes, which can lead to improving global Internet routing stability. RDTD consists of four stages. These are: collector, calculating the measurements of the non-linear statistical analysis, moving average and detection, as shown in Figure 1.

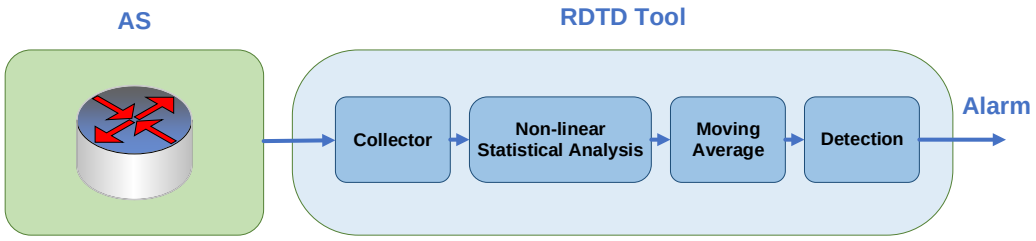

Figure 1. RDTD Structure and Design

3.1 Collector

The purpose of this stage is to provide real-time collection of traffic sent by the monitored AS. Unlike Quagga (Ishiguro, 2018) which is an open-source routing software suite that can be used to establish a connection with the monitored AS and store the inter-domain routing traffic in MRT format (Blunk, Karir & Labovitz, 2011), our collector collects inter-domain routing traffic in a human-readable format. It also calculates several features. These features avoid the need for converting MRT and calculating the features. The outputs of our collector are the total number of announcements and withdrawals (TAW) and the average length of AS-PATH (AVP). These features are calculated every second based on the timestamp of the traffic.

Our collector uses Net::BGP, a module of Perl software, to implement BGP. Net::BGP provides the required functionality to establish AS peering and for exchanging BGP updates. Officially, Net::BGP v0.16 does not support IPv6 BGP updates nor IPv6 BGP peer connection. CAIDA has developed a patch for Net::BGP that allows a BGP router to send IPv6 announcements through Multi-protocol Reachable NLRI, an optional attribute supported as part of Multi-protocol Extensions for BGP (CAIDA, 2016). However, this patch does not support IPv6 prefix withdrawn and requires BGP routers with ADD-PATH capability, an extension to the BGP protocol to allow the advertisement of multiple paths for the same prefix. Therefore, we implemented the IPv6 route withdrawn through the Multi-protocol Unreachable NLRI optional attribute and removed ADD-PATH BGP capability for compatibility purposes (Bates *et al.*, 2007).

3.2 Non-linear Statistical Analysis

Recurrence Quantification Analysis (RQA) is an advanced non-linear statistical analysis technique that uses the concepts of phase plane trajectory, a theoretical space in which every state of a system under study is mapped to a unique spatial location (Trulla *et al.*, 1996). RQA was introduced by Webber and Zbilut (2005) to quantify structures in Recurrence Plots (RPs),

http://doi.org/10.18080/jtde.v8n2.244

an advanced non-linear analysis tool that measures recurrences of a trajectory in the phase plane. RP has been widely used to visualise the time-dependent behaviour of the dynamics of a system as a recurrence matrix R

$$R_{m,n} = \begin{cases} 1: \overrightarrow{x_m} \approx \overrightarrow{x_n}, \\ 0: \overrightarrow{x_m} \not\approx \overrightarrow{x_n}, \end{cases} \quad m, n = 1, \ldots, J, \tag{1}$$

where $\{\overrightarrow{x_m}\}_{m=1}^{J}$ is a trajectory of a system in its phase plane, J represents the number of considered states and $\overrightarrow{x_m} \approx \overrightarrow{x_n}$ means equality up to a distance ε; ε is essential where systems show approximate recurrence to a formerly visited state. In other words, the recurrence matrix compares system states at time m and n. If the difference between these states is within the threshold distance ε, $R_{m,n} = 1$; otherwise, $R_{m,n} = 0$. Consequently, the recurrence matrix tells us when similar states of the underlying system occur (Marwan *et al.*, 2007).

Although RP is a powerful tool for visualizing system behaviour, it requires considerable expertise to interpret and cannot be used for real-time monitoring. Consequently, RQA was introduced to overcome these challenges through quantifying structures in RPs and provide the corresponding values of measurements (Marwan *et al.*, 2007). RQA provides many measurements that are known as RQA measurements. The most well-known RQA measurements are recurrence rate, determinism, and trapping time. Each of these measurements measures individual characteristics in the RP. For example, the recurrence rate refers to the probability that a system recurs after several time states. It represents the number of black dots in the RP excluding the black main diagonal line in the RP.

$$Recurrence\ rate = \frac{1}{J^2} \sum_{m,n=1}^{J} R_{m,n}, \tag{2}$$

where $R_{m,n}$ is an element in the RP matrix.

RQA has been successfully used in different domains, such as Internet of Things (IoT) (Forkan *et al.*, 2019) and detecting anomalies in intra-domain routing protocols (Al-Musawi *et al.*, 2020). We have shown in Al-Musawi (2018) that RQA can distinguish between recurrent normal behaviour and other behaviours that identify disruptions. RQA can rapidly detect the inter-domain routing disruptions as well as other hidden anomalous periods that may otherwise pass without detection. 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 internet-domain traffic behaviour and behaviours that indicate disruptions. Furthermore, RQA can detect behaviour that cannot be detected with other techniques (Al-Musawi, 2018).

Before calculating RQA measurements for the two features, (TAW) and (AVP), we normalise these features by subtracting the mean value to smooth noisy traces. RQA measurements are based on many parameters. These include time delay (τ), embedding dimension (m) and

http://doi.org/10.18080/jtde.v8n2.244

recurrence threshold (ε). The values of (τ) and (m) can be calculated using mutual information and false nearest neighbour, respectively. The first minimum values of mutual information and false nearest neighbour represent the values of (τ) and (m). The value of (ε) can be calculated using the recommendation from Marwan *et al.* (2007) by choosing the threshold value of less than 10% of the maximum phase plane diameter. We use the TISEAN package to calculate the values of (τ) and (m) and a Matlab toolbox available online on (Marwan, 2015) to calculate the value of (ε), which we provide within the RDTD package. In this paper, we do not provide a heuristic analysis for selecting the most effective RQA measurements: Al-Musawi (2018) provides such a heuristic analysis. Instead, we focus on providing a real-time detection tool for detecting Internet routing disruptions.

3.3 Moving Average

This stage aims to smooth the values of the RQA measurements to enable the detection of notable changes. A notable change in values of the RQA measurements in terms of increment or decrement indicates anomalous behaviour in a series of Internet inter-domain routing traffic. To identify RQA measurement changes that indicate an anomaly, we apply the moving average technique based on the following format:

$$RDTD_{alarm} = \bar{M} \pm \sigma(M) * T, \quad (3)$$

where (M) is the length of the window size for the detection, $\bar{M}$ is the mean value of (M), (σ) is the standard deviation of data with length (M) seconds and (T) is the threshold value, expressed as a multiple of the standard deviation. For example, $T = 5$ 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: for more details, see Al-Musawi (2018). This included $W = 200 \rightarrow 1200$ and $M = 200 \rightarrow 1200$ with an increment of 50 and $T = 1 \rightarrow 10$ with an increment of 1. Our analysis showed that window sizes $W = 200$ seconds and $M = 1200$ seconds, together with a threshold value in the moving average stage of $T = 9$, are optimal values to be used in our detection scheme.

3.4 Detection

In this stage, the detection decision is made. The input to this stage is multiple RQA alarms calculated by the moving average stage, while the output is an alarm that identifies the detection of the inter-domain routing disruptions. We use all logical ORs based on the need to minimise the 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.

http://doi.org/10.18080/jtde.v8n2.244

In this section, we have presented the design of our RDTD tool for detecting the Internet routing disruptions. In the next section, we introduce RDTD and discuss its use.

4. Real-time Detection Tool for Internet routing protocol Disruptions (RDTD)

Real-time Detection Tool for Internet routing protocol Disruptions (RDTD) is a Perl script to detect Internet inter-domain routing disruptions in near real-time. RDTD connects to a peer AS that is intended to be monitored. Although RDTD logs all detected inter-domain disruptions at AS-level with their time stamps and the last 1200 seconds of the traffic 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 RDTD tool are listed in Table 1. A simple example of using RDTD to monitor the peer AS65002 is shown in Figure 2, while the necessary command-line arguments can be as follows:

```
# perl RDTD.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 a route leak is detected and enabling a real-time plot of BGP features and alarm detection.

Table 1. RDTD tool command-line arguments

Argument	Value	Optional	Description
-colas	<AS number>	No	RDTD AS number
-colip	<IP address>	No	RDTD 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 RDTD tool help

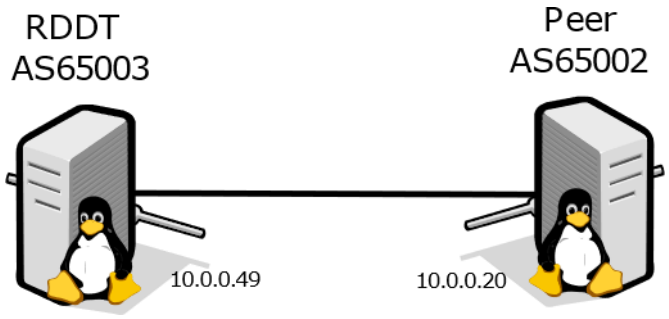

Figure 2. A simple example to monitor an AS using RDTD tool

To run the RDTD tool, RDTD needs some Perl modules and other open-source packages. The Perl modules are listed in Table 2. These modules can be downloaded and installed using cpan shell. For example, to install Net::BGP the following steps are required:

http://doi.org/10.18080/jtde.v8n2.244

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

Table 2. List of necessary Perl modules

Perl module	Purpose
Net::BGP	Provide the required functionality to establish AS peering and receiving inter-domain routing traffic from AS 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 apply the IPv6 support patch to the 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 installing the necessary modules, enabling the e-mail option for sending a notification when an anomaly is detected needs extra action. Users need to allow access to less secure apps in their e-mail settings. (For example, allowing less secure apps in a 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 script named test_email.pl in the RDTD package. The RDTD package is available online at https://github.com/Bahaaqm/RDDT.

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

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

5. Evaluation

To evaluate our RDTD detection tool, we replay inter-domain routing traffic related to the TMnet event, one of the well-known Internet inter-domain routing disruption events, using the BGP Replay Tool (BRT) (Al-Musawi *et al.*, 2017), a tool that we built to replay past Internet routing traffic with time stamps. We use the simple topology shown in Figure 2 to monitor inter-domain routing traffic sent by a BRT speaker sending route traffic related to the events.

http://doi.org/10.18080/jtde.v8n2.244

The TMnet event is an example of an Internet route leak that was observed on 12 June 2015 by TMnet, an ISP owned by Telekom Malaysia. TMnet (AS4788) accidentally advertised 179,000 prefixes with preferable paths to Level 3, which in turn accepted and propagated them, causing significant instability to the global routing system (Al-Musawi, Branch & Armitage, 2015). We use BRT to replay inter-domain routing traffic sent by AS10102, a peer of the route-views4 collector (Routeviews, 2000), during the TMnet event. As a result of the route leak, AS10102 sent a significant amount of inter-domain routing traffic during the event.

In addition to its ability to rapidly detect the Internet routing disruption caused by a high volume of inter-domain routing traffic, RDTD also raises an alarm when AS10102 stops sending inter-domain routing traffic. Figure 3 shows that RDTD raised an alarm 196 seconds after BRT stopped sending any inter-domain routing traffic; this alarm is not as a result of a lost connection. In total, the RDTD tool detected 8 inter-domain routing disruptions during the events, as shown in Figure 4. RDTD detected 8 disruptions during the day of the TMnet event with a time delay ranging between 1 second and 196 seconds. The first two alarms represent an early detection of the TMnet event, before AS10102 was sending a high volume of Internet routing updates.

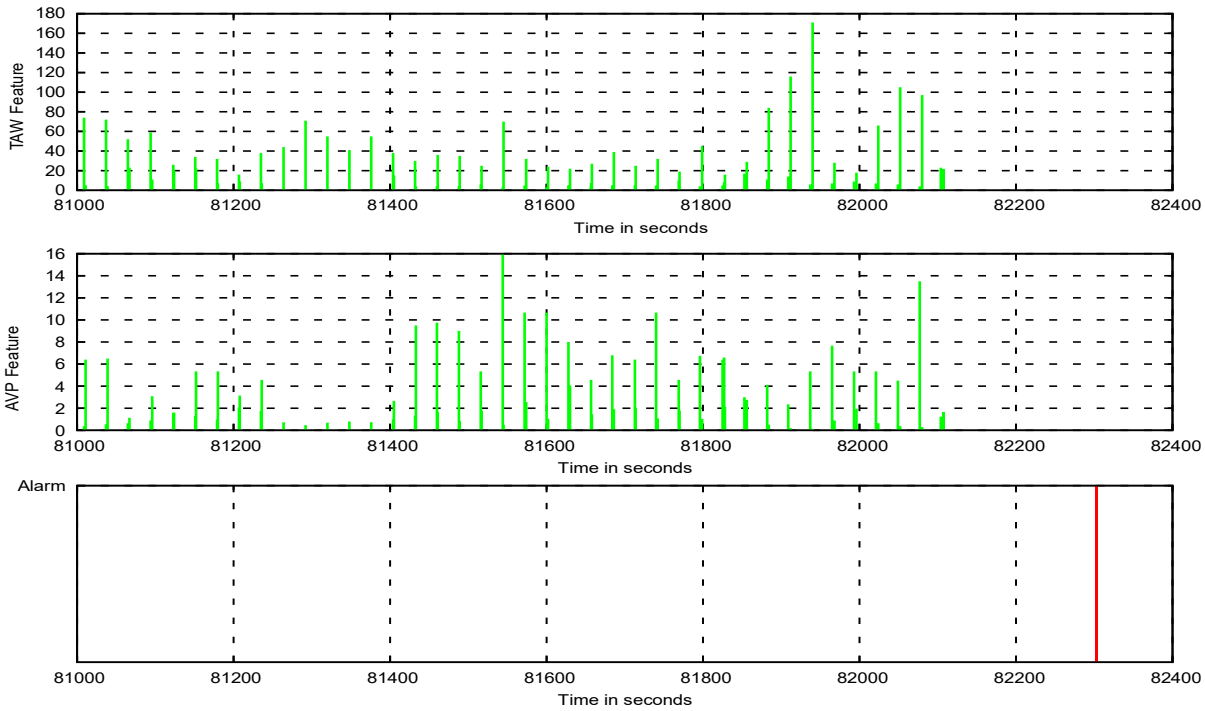

Figure 3. RDTD raised an alarm when the monitored AS stopped sending inter-domain routing traffic

http://doi.org/10.18080/jtde.v8n2.244

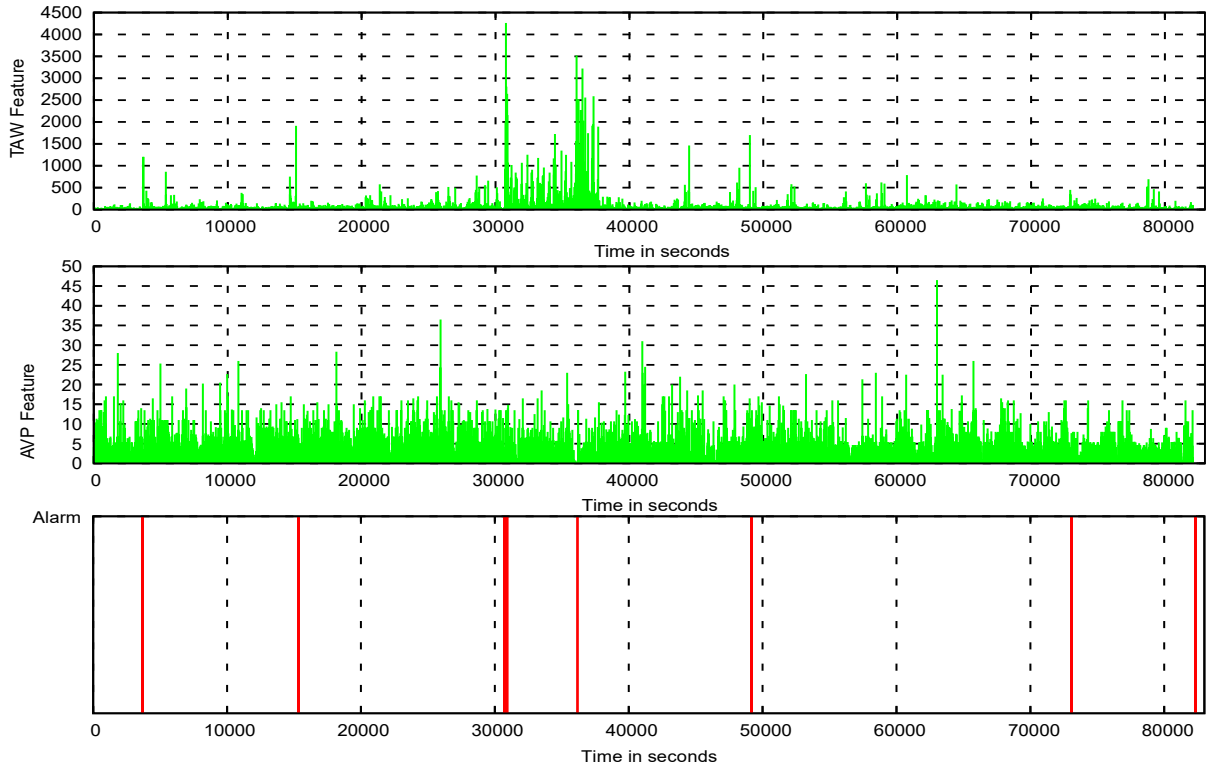

Figure 4. Detected inter-domain routing disruptions using RDTD

Table 3 shows a comparison of techniques described in three papers (Ortiz de Urbina Cazenave, Köşlük & Ganiz, 2011; Deshpande *et al.*, 2009; Haeberlen *et al.*, 2009) as well as our approach used in the RDTD tool. In Deshpande *et al.* (2009), the detection mechanism is based on an adaptive sequential segmentation which uses GLRT to detect the boundary of abnormal behaviours. This mechanism requires 100 minutes of Internet routing history updates and can detect anomalies within an hour. NetReview is a prototype that detects Internet routing disruptions at the AS level (Haeberlen *et al.*, 2009). This prototype requires one year of Internet routing history data to detect BGP disruptions. The framework in Ortiz de Urbina Cazenave, Köşlük & Ganiz (2011) uses machine learning algorithms to detect Internet routing disruptions. It requires data of past events to detect similar types of events. This framework also takes around an hour to detect the disruptions. In contrast, RDTD requires only 20 minutes of BGP history updates and can detect Internet routing disruptions within 200 seconds.

Table 3. Comparison among BGP disruption techniques

Technique	Time Detection	History of Internet routing traffic
Statistical Analysis (Deshpande *et al.*, 2009)	Around 1 hour	100 minutes
History of BGP Data (Haeberlen *et al.*, 2009)	Near real-time	1 year
Machine Learning (Ortiz de Urbina Cazenave, Köşlük & Ganiz, 2011)	Around 1 hour	720 minutes per training
RDTD	1-200 seconds	20 minutes

http://doi.org/10.18080/jtde.v8n2.244

6. Conclusion

Inter-domain routing disruptions could produce a local impact on the business relationship between individual ISPs or even a global impact on Internet routing stability. Detecting Internet inter-domain routing disruptions in real-time helps ISP operators to mitigate the impact of disruptions. In this paper, we introduced RDTD, a tool to detect inter-domain routing disruptions in near real-time. RDTD uses an advanced non-linear statistical analysis technique based on the concepts of phase plane trajectory. RDTD has shown its ability to rapidly detect inter-domain routing disruptions without requiring a long history of data. The evaluation of RDTD has been made using a controlled testbed and injecting inter-domain routing traffic related to one of the most well-known Internet route leak events. Our future work will involve connecting RDTD with a real AS.

References

Al-Musawi, B. (2018). *Detecting BGP Anomalies Using Recurrence Quantification Analysis*. Ph.D. dissertation, Swinburne University of Technology. Available at https://researchbank.swinburne.edu.au/file/627b88ea-e0d7-477a-9b64-6317fea582f7/1/bahaa_al_musawi_thesis.pdf

Al-Musawi, B., Al-Saadi, R., Branch, P., & Armitage, G. (2017). *BGP Replay Tool (BRT) v0.2*. Retrieved from http://i4t.swin.edu.au/reports/I4TRL-TR-170606A.pdf

Al-Musawi, B., Branch, P., & Armitage, G. (2015). Detecting BGP instability using recurrence quantification analysis (RQA). *2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC)*, Nanjing, 1-8, doi: 10.1109/PCCC.2015.7410340.

Al-Musawi, B., Branch, P., & Armitage, G. (2017). BGP anomaly detection techniques: A survey. *IEEE Communications Surveys & Tutorials, 19*(1), 377-396.

Al-Musawi, B., Branch, P., Hassan, M. F., & Pokhrel, S. R. (2020). Identifying OSPF LSA falsification attacks through non-linear analysis. *Computer Networks,167*, 107031. https://doi.org/10.1016/j.comnet.2019.107031

Bates, T., Chandra, R., Katz, D., & Rekhter, Y. (2007). Multiprotocol extensions for BGP-4. Retrieved from https://tools.ietf.org/html/rfc4760

Blunk, L., Karir, M., & Labovitz, C. (2011). Multi-Threaded Routing Toolkit (MRT) Routing Information Export Format, October. Retrieved from http://tools.ietf.org/html/rfc6396

CAIDA. (2016). bgp-hackathon. Retrieved from https://github.com/CAIDA/bgp-hackathon/tree/master/bgpd-3

Chi, Y.-J., Oliveira, R., & Zhang, L. (2008). Cyclops: The AS-level Connectivity Observatory. *SIGCOMM Computer Communication Review, 38*(5), 5-16. https://doi.org/10.1145/1452335.1452337

Deshpande, S., Thottan, M., Ho, T. K., & Sikdar, B. (2009). An online mechanism for BGP instability detection and analysis. *IEEE Transactions on Computers*, *58*(11), 1470-1484. doi: 10.1109/TC.2009.91

Forkan, A. R. M., Branch, P., Jayaraman, P. P., & Ferretto, A. (2019). An Internet-of-Things Solution to Assist Independent Living and Social Connectedness in Elderly. *ACM Transactions on Social Computing, 2*(4), 1-24. https://doi.org/10.1145/3363563

Haeberlen, A., Avramopoulos, I. C., Rexford, J., & Druschel, P. (2009). NetReview: Detecting When Interdomain Routing Goes Wrong. *Proceedings of the 6th USENIX Symposium on Networked Systems Design and Implementation, NSDI 2009*, April, Boston.

Huang, Y., Feamster, N., Lakhina, A., & Xu, J. J. (2007). Diagnosing network disruptions with network-wide analysis. *ACM SIGMETRICS Performance Evaluation Review*, *35*(1), 61-72. http://doi.org/10.1145/1269899.1254890

Ishiguro, K. (2018). Quagga Routing Suite. Retrieved from http://www.nongnu.org/quagga/

Labovitz, C., Malan, G. R., & Jahanian, F. (1998). Internet Routing Instability. *IEEE/ACM Transactions on Networking, 6*(5), 515-528. doi: 10.1109/90.731185

Luckie, M. (2010). Scamper: a scalable and extensible packet prober for active measurement of the internet. *IMC '10: Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*, 239-245. https://doi.org/10.1145/1879141.1879171

Lutu, A., Bagnulo, M., & Maennel, O. (2013). The BGP visibility scanner. *2013 Proceedings IEEE INFOCOM*, Turin, 3243-3248. doi: 10.1109/INFCOM.2013.6567145

Marwan, N. (2015). CROSS RECURRENCE PLOT TOOLBOX 5.18 (R29.3). Retrieved from http://tocsy.pik-potsdam.de/CRPtoolbox/

Marwan, N., Romano, M. C., Thiel, M., & Kurths, J. (2007). Recurrence plots for the analysis of complex systems. *Physics Reports, 438*(5-6), 237-329. http://doi.org/10.1016/j.physrep.2006.11.001

Ortiz de Urbina Cazenave, I. O., Köşlük, E., & Ganiz, M. C. (2011). An anomaly detection framework for BGP. *2011 International Symposium on Innovations in Intelligent Systems and Applications*, Istanbul, 107-111. doi: 10.1109/INISTA.2011.5946083

Roudnev, A. (2005). Re: More on Moscow power failure(was RE: Moscow: global power outage). Retrieved from https://archive.nanog.org/mailinglist/mailarchives/old_archive/2005-05/msg00767.html

Routeviews. (2000). University of Oregon Route Views project. Retrieved from http://www.routeviews.org/

Shi, X., Xiang, Y., Wang, Z., Yin, X., & Wu, J. (2012). Detecting prefix hijackings in the internet with argus. *IMC '12: Proceedings of the 2012 Internet Measurement Conference*, November, 15–28. https://doi.org/10.1145/2398776.2398779

Toonk, A. (2015). *Massive route leak causes Internet slowdown*. June 12. Retrieved from http://www.bgpmon.net/massive-route-leak-cause-internet-slowdown/

Trulla, L. L., Giuliani, A., Zbilut, J. P., & Webber, C. L. (1996). Recurrence quantification analysis of the logistic equation with transients. *Physics Letters A, 223*(4), 255-260. https://doi.org/10.1016/S0375-9601(96)00741-4

Webber, C. L., & Zbilut, J. P. (2005). Recurrence Quantification Analysis of Nonlinear Dynamical Systems. *Tutorials in contemporary nonlinear methods for the behavioral sciences*, 26-94. Retrieved from https://www.nsf.gov/pubs/2005/nsf05057/nmbs/nmbs.pdf