# Detecting BGP Anomalies Using Recurrence Quantification Analysis

**Bahaa Al-Musawi**

School of Software and Electrical Engineering

Swinburne University of Technology

This dissertation is submitted for the degree of

*Doctor of Philosophy*

January 2018

I would like to dedicate this thesis to my greatest supporters my parents, my brothers and sisters, my beloved wife Zahraa, my sons Mahdi and Baqer, and my little lovely daughter Fatima.

# Declaration

I hereby declare that except where specific reference is made to the work of others, the contents of this dissertation are original and have not been submitted in whole or in part for consideration of any other degree or qualification in this, or any other University. This dissertation is the result of my own work and includes nothing which is the outcome of work done in collaboration, except where specifically indicated in the text. The content of the thesis is the result of work which has been carried out since the beginning of my candidature on October 2013.

Bahaa Al-Musawi
January 2018

# Preface

The Border Gateway Protocol (BGP) is the de-facto inter-domain routing protocol responsible for exchanging Network Reachability Information (NRI) between Autonomous Systems (ASes). Unfortunately, BGP was developed at a time when the information exchanged between its participants could be assumed to be accurate and therefore it is vulnerable to different types of attacks. Detecting BGP anomalies has attracted many researchers to identify and/or mitigate anomalous BGP traffic that can affect business relationships between Internet Service Providers (ISPs) as well as its effect on the Internet stability and reliability. However, the characteristics of BGP traffic have not well understood. For example, what are the characteristics of normal and anomalous BGP traffic? What are the characteristics of BGP routers when forwarding normal traffic and when forwarding anomalous BGP traffic?

The research of this thesis arose from the above questions. In this thesis, I introduce a novel scheme that can differentiate between normal background BGP traffic and anomalous traffic. My scheme is based on using Recurrence Quantification Analysis (RQA), an advanced non-linear statistical analysis technique which uses the concepts of phase plane trajectory. This scheme can rapidly detect BGP anomalies as well as other hidden anomalous periods in the underlying system behaviour.

The research described in this thesis has attracted considerable industry support:

- I was awarded a grant of $AUD 28,518 from Information Society Innovation Fund (ISIF) under the category of the Asia-Pacific Network Information Center (APNIC) Internet Operations Research Grants for the project titled “Rapid detection of BGP anomalies” [1]. The selection process was very competitive where only 10 projects were selected from more than 300 submissions. The grant is being used for the development of a new version of the BGP Replay Tool (BRT) v0.1 [2], a tool to replay past BGP updates with time stamps, and software that makes use of my RQA scheme. The BRT v0.2 is available on [3] and the software is available on [4].

- I was awarded a Student Travel Grant (STG) for 5th PhD School on Traffic Monitoring and Analysis 2015 (TMA2015) in Barcelona, Spain during April 21-22, 2015.

- I have been granted access to Virtual Internet Routing Lab (VIRL) under academic license [5]. I used this extensively for my experimental work and development of the software for the ISIF funded project.

- Cisco Systems have supported my research work with a substantial grant to support me during my candidature which I gratefully acknowledge.

- I have been granted all registration and travel costs, under an ISIF grant, to introduce the RQA scheme and BRT v0.2 at APNIC 44, technical operations II session, that was held in Taichung, Taiwan 12-14 September 2017 [6].

Much of the material of the thesis has been published in a refereed journal and presented at refereed conferences:

- The material in Chapter 2 is based on the IEEE COMST article (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, First quarter 2017) [7] where we[1] introduce our definition of anomalous BGP traffic and unstable BGP traffic. This paper discusses and classifies BGP anomalies and reviews the 20 most significant techniques used to identify them. Our classification is based on the broad category of approaches, BGP features used to identify the anomaly, effectiveness in identifying the anomaly and effectiveness in identifying which AS was the location of the event that caused the anomaly. We also discuss a number of key requirements for the next generation of BGP anomaly detection techniques.

- A paper based on modelling BGP speakers as a dynamic system and introducing the RQA approach to detecting BGP anomalies forms the basis of Chapter 4. This work was presented at the IEEE International Performance Computing and Communications Conference (IPCCC) in Nanjing, China 2015 (B. Al-Musawi, P. Branch, and G. Armitage, "Detecting BGP instability using Recurrence Quantification Analysis (RQA)) [8]. We were delighted when one of the founders of RQA (Dr. Norbert Marwan) requested a copy of this paper whose comment on it was "Great! Thank you very much for this interesting paper! Nice work!".

- A paper based on using linear and non-linear statistical analysis showing that BGP traffic has recurrent behaviour caused by unsynchronised periodic behaviour from a set of ASes. This paper was presented at International Telecommunication Networks and

[1] Although the author uses "we" and "our" rather than "I" and "my", the work described is the author's own except where noted.

Applications Conference ITNAC 2017, Melbourne, Australia 2017 (B. Al-Musawi, P. Branch, and G. Armitage, “Recurrence Behaviour of BGP Traffic”) [9].

During the research work for this thesis and as part of the concurrent ISIF supported project I have developed or contributed the following open source software:

- BRT v0.1, a tool to replay past BGP updates and events. BRT v0.1 is described in the technical report (B. Al-Musawi, P. Branch, and G. Armitage, “BGP Replay Tool (BRT) v0.1,” Centre for Advanced Internet Architectures, Swinburne University of Technology, Melbourne, Australia, Tech. Rep. 160304A, 04 March 2016.) [2].

- BRT v0.2 was developed using the ISIF grant to support peering with different BGP speakers operating systems such as Quagga and real Cisco routers. BRT v0.2 also supports IPV6 [10].

- The material of Appendix A is based on the content of the technical report that describes BRT v0.2 (B. Al-Musawi, R. Al-Saadi, P. Branch, and G. Armitage, "BGP Replay Tool (BRT) v0.2", I4TRL Technical report 170606A, 06 June 2017).

The contributions of this thesis can be summarised as:

- Define unstable BGP traffic and anomalous BGP traffic;

- Classify BGP anomalies into four main categories, these being direct intended anomaly, direct unintended anomaly, indirect anomaly, and link failure;

- Discuss key requirements for the next generation of BGP anomaly detection techniques;

- Demonstrate that unstable BGP traffic from a single BGP speaker has the characteristics of a periodic behaviour;

- Show that BGP routers generate traffic that has the characteristics of being non-linear, determinism, and stable;

- Show that the aggregate BGP traffic for a set of unstable ASes has the characteristic of a recurrence behaviour;

- Demonstrate that the RQA approach is able to differentiate between normal but unstable BGP traffic and anomalous BGP traffic;

- Introduce BRT, a new tool that can help researchers and operators replay past BGP updates with time stamp;

# Acknowledgements

I would like to express my sincere gratitude and appreciation to my supervisors, Ass. Prof. Philip Branch and Prof. Grenville Armitage, for their excellent advice and support through my Ph.D. studies. They have been and always will be a source of inspiration and my role model as a researcher. I would also like to thank Dr. Jason But, Dr. Antonio Cricenti and my colleagues for their support and advice when needed.

I am thankful to Joel Obstfeld, Simon Knight and all other VIRL team at Cisco for providing free license and support.

Special thanks to Simon Forsayeth from ITS/Swinburne University for setting up the physical rack of hosts on which I ran VIRL.

# Abstract

The Border Gateway Protocol (BGP) is the Internet's default inter-domain routing protocol that manages connectivity among Autonomous Systems (ASes). BGP is an incremental protocol where, after the initial transfer of a full routing table, BGP traffic to peers should only reflect underlying topology or traffic engineering changes. Unfortunately, most BGP traffic consists of announcements, updates and withdrawals unrelated to any underlying network management goals. We define such BGP traffic as unstable BGP traffic as long as it does not disseminate the business relationship between Internet Service Providers (ISPs) or threaten BGP operation. We define ASes that originate unstable BGP traffic as unstable ASes.

BGP was developed at a time when information provided by an AS was assumed to be accurate. Although many attempts have been made to improve its security, BGP is still vulnerable to different types of anomalous events. BGP anomalies are rare but can cause great damage when they occur. The consequences of these anomalies can range from a single to thousands of anomalous BGP updates. These consequences have threatened Internet performance and reliability. Identifying BGP anomalies is a challenging task where BGP traffic has been characterised to be noisy, voluminous, and complex. Furthermore, unstable BGP traffic has the effect of masking anomalous traffic.

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. These statistics demonstrate the need for rapid detection of BGP anomalies. Early detection of BGP anomalies enables network operators to protect their network from the worst consequence of the anomalous behaviour and helps to improve Internet stability. Current approaches tend to be slow and require substantial historical data.

To overcome these challenges, this thesis proposes a novel scheme to detect BGP anomalies based on Recurrence Quantification Analysis (RQA). RQA is an advanced non-linear statistical analysis technique using phase space concepts. RQA can identify BGP anomalies rapidly. RQA can also identify abnormal hidden behaviour in the underlying BGP traffic that may otherwise pass without observation. Using the past and emulated BGP anomalies, we demonstrate that RQA can detect BGP anomalies within 62 seconds using 1200 seconds of historical BGP updates.

The main contribution of this thesis is to demonstrate that RQA can be used to detect anomalous BGP events rapidly. We apply RQA to well known BGP events and also to controlled experiments which we carried out on our network testbed.

We also demonstrate that background BGP traffic can be well described as the aggregation of unsynchronised periodic traffic with different frequencies. This behaviour is widespread and can last for months or even years.

Finally, we model BGP speakers (a router or a device that runs BGP) as dynamic systems using the concepts of phase space trajectory. Our modelling shows that BGP speakers generate traffic that have the characteristics of being non-linear, deterministic, and stable.

g

# Contents

# List of Figures

# List of Tables

# Abbreviations

| | |
|---|---|
| ACF | Auto-correlation Function |
| AfriNIC | African Network Information Center |
| APNIC | Asia-Pacific Network Information Center |
| ARIMA | Autoregressive Integrated Moving Average |
| ARIN | American Registry for Internet Numbers |
| AS | Autonomous System |
| ASes | Autonomous Systems |
| BGP | Border Gateway Protocol |
| BRT | BGP Replay Tool |
| CIDR | Classless Inter-Domain Routing |
| DDoS | Distributed Denial of Service |
| DET | Measure for recurrence quantification:Determinism |
| DoS | Denial of Service |
| DVV | Delay Vector Variance |
| EBGP | External BGP |
| EGP | Exterior Gateway Protocol |
| ENT | Measure for recurrence quantification:Shannon entropy |
| EWMA | Exponentially Weighted Moving Average |

| | |
|---|---|
| FFT | Fast Fourier Transform |
| FN | False Negative |
| FNN | False Nearest Neighbor |
| FP | False Positive |
| GLRT | Generalized Likelihood Ratio Test |
| HMMs | Hidden Markov Models |
| HOPA | Higher-order Path Analysis |
| HVP | High-visibility prefix |
| IANA | Internet Assigned Number Authority |
| IBGP | Internal BGP |
| ICMP | Internet Control Message Protocol |
| IETF | Internet Engineering Task Force |
| IRF | Internet Routing Forensic framework |
| IRR | Internet Routing Registry |
| IXP | Internet Exchange Point |
| L-MAX | Measure for recurrence quantification: length of the longest diagonal line |
| L-MEAN | Measure for recurrence quantification:mean of the diagonal line length |
| LACNIC | Latin America and Caribbean Network Information Centre |
| LAM | Measure for recurrence quantification:Laminarity |
| LOI | Line of Identity |
| LVP | Limited-Visibility Prefix |
| MDFMT | MRT Dump File Manipulation Toolkit |
| MED | Multi Exit Discriminator |
| MI | Mutual Information |

| | |
|---|---|
| MOAS | Multiple Origin AS |
| MRAI | Minimum Route Advertisement Interval |
| mRMR | minimum Redundancy Maximum Relevance |
| MRT | Multi-Threaded Routing Toolkit |
| NANOG | North American Network Operator’s Group |
| NIR | National Internet Registries |
| NLRI | Network Layer Reachability Information |
| NRI | Network Reachability Information |
| OSPF | Open Shortest Path First |
| PCA | Principal Component Analysis |
| PGBGP | Pretty Good BGP |
| PKI | Public Key Infrastructure |
| RFD | Route Flap Damping |
| RIB | Routing Information Base |
| RIP | Routing Information Protocol |
| RIPE | Réseaux IP Européens |
| RIPE NCC | Réseaux IP Européens Network Coordinate Centre |
| RIRs | Regional Internet Registries |
| RP | Recurrence Plot |
| RPSL | Routing Policy Specification Language |
| RQA | Recurrence Quantification Analysis |
| RR | Measure for recurrence quantification:Recurrence Rate |
| RRC | Remote Route Collector |
| SVM | Support Vector Machine |

| | |
|---|---|
| T2 | Measure for recurrence quantification:recurrence time of 2nd type |
| TCP | Transmission Control Protocol |
| TN | True Negative |
| TP | True Positive |
| TT | Measure for recurrence quantification:Trapping Time |
| VIRL | Virtual Internet Routing Lab |
| XML | Extensible Markup Language |

# Chapter 1

# Introduction

Today the Internet provides the communication infrastructure for modern commerce, education, entertainment and health services. Because of society's increasing reliance on the Internet, its reliability and security are of critical concern. The Internet has been subjected to many types of attacks such as Denial of Service (DoS), hijacking of hosts and servers, and threats to routing protocols [11]. Internet routing is divided into two levels. These are intra-domain routing and inter-domain routing. Intra-domain routing protocols refer to Interior Gateway Protocols (IGP) such as Open Shortest Path First (OSPF) to ensure traffic exchange within an Autonomous System (AS), a set of routers under a single technical administration unit. Inter-domain routing protocols include Exterior Gateway Protocols (EGPs) such as Border Gateway Protocol (BGP) to ensure Network Reachability Information (NRI) between Autonomous Systems (ASes).

BGP is the Internet's default inter-domain routing protocol that manages connectivity among ASes. It was developed at a time when information provided by an AS could be assumed to be accurate. Consequently, BGP did not provide any authentication measures for advertising routes [12–14]. Several methods and proposals have since been introduced to improve the security of BGP. These can be classified into four broad categories: cryptographic based prevention, anomaly mitigation, mitigation of unstable route propagation, and anomaly detection. Cryptographic approaches [15, 16] use Public Key Infrastructure (PKI) to ensure the authentication of routing announcements to minimise the risk of hijacking. Anomaly mitigation approaches [17, 18] propose ignoring or delaying suspicious route updates by the operators after detecting them. None of these approaches, however, offer a combination of suitable performance, adequate security, and deployable support infrastructure [14]. Moreover, these proposals are not able to mitigate BGP misconfiguration and some forms of BGP hijacking [19, 20]. Mitigating propagation of unstable routes such as described in [21] and [22] has been proposed as a way of limiting the propagation of unstable BGP routing information. Finally, anomaly detection approaches such as [8, 23, 24] aim to discover anomalous information or behaviour in BGP traffic and raise an alarm or take other action. Rapid detection of BGP anomalies is the topic of this thesis.

BGP is vulnerable to anomalies such as hijacking, misconfiguration and 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 [8]. 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 [23]. 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. In this thesis, we introduce a new detection scheme that can detect BGP anomalies quickly. It can also detect hidden anomalous behaviour in the underlying system behaviour that may pass without observation.

The rest of this chapter is organised as follows. In Section 1.1, we discuss the challenges of detecting BGP anomalies and introduce our definitions of unstable BGP traffic and anomalous BGP traffic. In Section 1.2, we discuss the need for a technique that can differentiate between unstable and anomalous BGP traffic. We also discuss our contributions in more details. Finally, we present the organisation of this thesis in Section 1.3.

## 1.1 Research motivations and objectives

BGP is a path vector protocol responsible for managing NRI between ASes with guarantees of avoiding routing loops [25]. ASes are not bound by physical relationships but reflect business and organizational relationships. BGP is a routing policy protocol where ISPs configure their BGP routers to apply business relationships. ISPs may also apply traffic engineering to control the direction and load balance of traffic through path prepending [26]. In this environment, it can be difficult to define what is meant by an anomaly. To obtain a satisfactory definition, it is necessary to consider the purpose of BGP and how specific BGP activity does or does not contribute to that purpose. BGP's purpose is to further the business goals of an organisation in providing its NRI to other organisations. Any BGP activity that does not contribute to those business goals or undermines them can be considered anomalous. Unfortunately, It can be very difficult to determine whether or not a particular activity is or is not furthering those goals. For example, BGP updates that do not reflect underlying topology changes may be anomalous. They might be the consequence of route flapping where routes are repeatedly announced and then soon after withdrawn. Such activity is anomalous. However, changes that do not reflect underlying topology changes might also be a consequence of traffic engineering where some routes are preferred over others because they use under-utilized link capacity. Such activity is not anomalous even though it may not reflect underlying topology changes.

Even when BGP activity does not contribute to the business goals of the AS not all such activity can be regarded as being of equal significance. There is a spectrum of anomalous behaviour from relatively harmless to highly harmful. For example, route flapping, although it consumes router and link resources, is relatively harmless. Further along the harm spectrum might be path announcements that add unnecessary delay to routed packets. Further still might be path announcements whose purpose is directing traffic via nodes where it can be collected and exploited for surveillance or intelligence purposes. At the far end of the spectrum might be where routes are announced that direct the traffic to a destination where it is dropped ("blackhole-ing").

We differentiate between anomalous behaviour that does not threaten BGP's ability to disseminate accurate NRI and harmful anomalies that do. We define BGP traffic generated by the first type as an instability. We refer to the second type as an anomaly and its consequences of BGP traffic as anomalous traffic. For example, route flapping may cause long term instabilities while traffic engineering may result in short term instabilities. Neither is a direct threat to the ability of BGP to communicate reachability information. However, a misconfiguration by BGP router operators can result in announcing used and/or unused prefixes which is a threat. The process of differentiating between unstable and anomalous BGP traffic is a challenge.

In the years since it was widely deployed, many types of anomalies have been recorded, including hijacking, misconfiguration by operators, link failure and DoS attacks. It is worth noting that it is not just direct attacks on BGP that can cause anomalies and instability. Although malware such as Nimda and Slammer were directed at web servers, BGP routing was also affected during these attacks [27, 28]. An example of misconfiguration is the Pakistan Telecom incident. 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 [29]. The panix.com domain incident is an example of hijacking. On 22 January 2006 AS27506 hijacked the panix.com domain causing loss of connectivity for several hours [30]. Other hijacks have continued for long periods without detection. An example is the Link Telecom incident when an attacker obtained control of the company's prefixes for approximately 6 months and used them to send spam e-mails [31].

In addition to reported events, many events are unreported or even unnoticed [32]. A recent statistical analysis on BGP performance for a period of 10 years beginning from 2001 shows that the huge growth in the size of the Internet was leading towards increased instability [33]. Shi et al. [23] presented statistics and trends of bogus routes in the Internet over a period of 1 year from May 2012. During this period, around 40k bogus routes (routes that should not appear on the Internet) were detected. Among the causes of these bogus routes, there were 193 BGP hijacks and 27 misconfigurations. These statistics demonstrate the need for rapid (within seconds) detection of anomalous BGP traffic caused by different types of BGP anomalies. Rapid detection of BGP anomalies helps ISPs protect their networks and mitigate the propagation of anomalous BGP traffic. In the next section, we introduce our contributions into BGP anomaly detection research.

## 1.2 Contributions

Although unstable BGP traffic is relatively harmless, it has the effect of masking anomalous traffic that indicates potentially harmful accidental or deliberate anomalies. A technique is needed that can rapidly distinguish between normal background and potentially harmful BGP traffic. For that purpose, we focus on finding the characteristics of normal-but-unstable BGP traffic and the characteristics of anomalous BGP traffic. We also focus on finding the characteristics of BGP speakers when forwarding normal-but-unstable traffic and when forwarding anomalous BGP traffic. Identifying these characteristics helps to choose a suitable technique that can differentiate between anomalous and unstable BGP traffic. These characteristics help, in addition, to understand BGP behaviour over time. In this thesis, we provide the following contributions:

First, we show that the complex and noisy BGP traffic can be understood as an aggregation of oscillations of different frequencies from different ASes. Using linear statistical analysis, we show that unstable ASes show a significant level of periodic behaviour in terms of sending BGP updates. We also investigate BGP traffic related to unstable ASes and show that although some unstable AS behaviour lasted for many years and others for a short time, the characteristic of periodicity in BGP traffic is persistent and can be seen in BGP traffic at least since 2005. However, although BGP traffic related to individual unstable ASes shows reasonably periodic behaviour, the aggregated BGP traffic for a set of unstable ASes does not show a structure of periodicity.

Second, we model a BGP speaker as a dynamic system sending BGP updates and path lengths depending on BGP messages received from neighbours and local routing policies. Our modelling is based on using phase plane trajectory. Modelling BGP speakers as dynamic systems helps to understand and predict BGP speaker behaviour over time. The outcome of our modelling shows that BGP traffic sent by BGP speakers has the characteristics of being stable, deterministic, and non-linear.

Third, using the outcome of our modelling we use Recurrence Plot (RP), an advanced non-linear statistical analysis technique. RP is used to visualise the time-dependent behaviour of the dynamics of a system as a square matrix where each element corresponds to a point in time states. Using RPs enables us to identify the structure of the aggregated BGP traffic. By using RPs, we can see that the aggregated BGP traffic has the characteristic of recurrent behaviour. The source of this characteristic is the unsynchronised periodic traffic sent by unstable ASes.

Fourth, we introduce a novel scheme to detect BGP anomalies based on Recurrence Quantification Analysis (RQA), a non-linear data analysis method to quantify the number and duration of recurrent behaviour in dynamic systems. We show that RQA is able to differentiate between normal-but-unstable BGP traffic and anomalous traffic that identifies anomalies. In addition to the ability of RQA to rapidly (within 62 seconds) detect BGP anomalies, RQA scheme can also identify hidden anomalous behaviour that may pass without detection. Using well-known and emulated BGP events, our RQA scheme can detect all well-known BGP anomalies as well as hidden unobserved anomalies.

Figure 1.1 shows the design of RQA scheme for detecting BGP anomalies. The input of our scheme is BGP traffic sent by a BGP speaker which is intended to be monitored while the output is an alarm identifying detection of BGP anomalies. This RQA scheme is comprised of four stages. The first stage is simply extracting BGP features from the input BGP traffic. The second stage represents the process of calculating RQA measurements for each BGP feature. At the third stage, we identify significant changes in RQA measurements, which reflect behaviour changes in the underlying BGP traffic, based on past RQA measurements. The output of this stage is an alarm for each RQA measurement. The last stage of RQA scheme is a logical OR for all RQA measurements alarms.

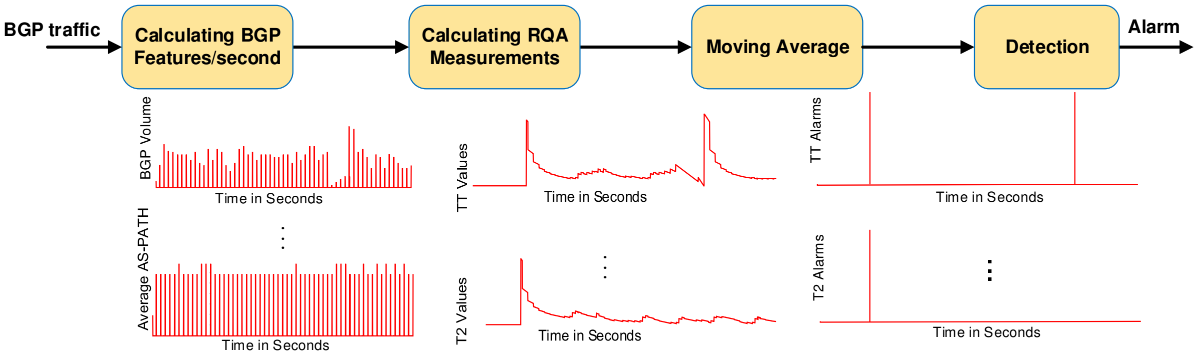


Figure 1.1: RQA scheme design for detecting BGP anomalies

## 1.3 Thesis organisation

This thesis is organised into six chapters. In Chapter 2, we provide an overview of BGP, BGP anomalies, BGP data sources, and discuss the most significant techniques used to identify BGP anomalies. We classify BGP anomalies into four main categories, these being direct intended anomaly, direct unintended anomaly, indirect anomaly, and link failure. We also classify BGP data sources for detecting BGP anomalies into three main categories: BGP raw data and route registry database as well as other less commonly used sources. We then explore BGP anomaly detection techniques in terms of their approaches, type of BGP data and features used, ability to identify different types of anomalies and their source causes, the network from which the anomaly originated. Finally, we discuss a number of key requirements for the next generation of BGP anomaly detection techniques, these being real-time (in seconds) detection, differentiation between types of BGP anomalies, and identification of the source network of the BGP anomaly.

In Chapter 3, we present the concepts of phase plane trajectory, RPs and RQA. Interpreting phase trajectories and RPs is explored and discussed. We also explore RQA measurements and how these measurements change to reflect changes in the input data. To understand how RQA measurements change based on the input data and determine the most suitable RQA measurements to detect anomalous behaviour, we do an experimental analysis of RQA measurements. Finally, we summarise the effectiveness of each RQA measurements ability to detect anomalies.

In Chapter 4, we make three contributions. Firstly, we investigate the characteristics of unstable BGP traffic using linear statistical analysis. We show that BGP traffic is dominated by unsynchronised periodic updates. The characteristic of periodicity in BGP traffic is part of underlying BGP traffic. Our statistics for ten years of BGP traffic shows that although for some active ASes instability lasted for many years and others lasted for a short time, we still can see the periodic behaviour for BGP traffic sent by these ASes. Secondly, we use the concepts of phase plane trajectory to model BGP speakers as dynamic systems sending BGP traffic based on local routing policies and receiving BGP traffic from neighbours. Modelling BGP speakers as dynamical systems helps to understand their behaviour over time. The outcomes of our investigations show that BGP traffic sent by BGP speakers has the characteristics of stability, determinism, and non-linearity. Third, built on the characteristics obtained from our modelling, we use RP to investigate the characteristics of the aggregated BGP traffic. Here we see that the aggregated BGP traffic has the characteristic of recurrent behaviour. We also show that RQA is able to differentiate between unstable and anomalous BGP traffic during TMnet event, one of the most recent well-known BGP events.

In Chapter 5, we introduce our novel scheme to detect BGP anomalies and describe its design in detail. As a result of a lack of ground truth time stamps for the BGP events, we introduce our control testbed where we synthesize unstable BGP traffic and introduce anomalies. Then, we use BGP traffic from our control testbed to select optimal values of our scheme's parameters and choose the most effective RQA measurements to detect BGP anomalies. The evaluation of our scheme is based on using past well-known BGP events as well as BGP traffic collected from our testbed. RQA scheme is able to detect all BGP anomalies as well as other periods of anomalous behaviour that have not been observed before.

Finally, we present our conclusions and outline possible future research work in Chapter 6.

# Chapter 2

# BGP anomalies

## 2.1 Introduction

BGP is the Internet's default inter-domain routing protocol. It enables the exchange and maintenance of NRI between ASes which are organized in a hierarchical fashion. It was developed at a time when information provided by an AS 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.

In this chapter, we provide an overview of BGP. This includes BGP architecture, BGP messages, BGP attributes and BGP policies. We also overview prior research works on BGP anomalies in four areas. Firstly, we classify BGP data sources for detection BGP anomaly into three main categories: BGP raw data and route registry database as well as other less commonly used sources. Secondly, we classify BGP anomalies into four main categories, these being direct intended anomaly, direct unintended anomaly, indirect anomaly, and link failure. Thirdly, we explore BGP anomaly detection techniques in term of their approaches, type of BGP data and features used, ability to identify different types of anomalies, and their ability to identify network from which the anomaly originated. Finally, we discuss a number of key requirements for a next generation of BGP anomaly detection techniques, these being real-time (in seconds) detection, differentiation between types of BGP anomalies, and identification of the source network of the BGP anomaly.

The rest of this chapter is organized as follows. Section 2.2 presents a brief overview of BGP, BGP messages, BGP policies, and BGP attributes. We also explore different data sources and BGP features that can be used as an input to detect BGP anomalies. Section 2.3 provides a detailed summary of different types of BGP anomalies while section 2.4 reviews the major approaches to detecting BGP anomalies. In section 2.5, we discuss a number of key requirements for the next generation of BGP anomaly detection techniques and summarise strengths and weakness of current BGP anomaly detection techniques. The chapter concludes with section 2.6.

## 2.2 BGP overview

### 2.2.1 Introduction to BGP

The Internet is a decentralized global network comprised of tens of thousands of ASes. An AS is a set of routers under a single technical administration using an IGP such as OSPF to communicate with other routers within the AS and an EGP such as BGP to communicate with other ASes. Routing protocols are classified into three main types based on their algorithm: link state such as OSPF, distance vector such as Routing Information Protocol (RIP), and path vector such as BGP. BGP has two forms: Internal BGP (IBGP), running between BGP routers within an AS and External BGP (EBGP), running between BGP routers within different ASes. ASes are often peered together through a dedicated connection between peers or by a third party such as an Internet Exchange Point (IXP). BGP has undergone a number of revisions and refinements over the years, starting with RFC1105 [34] (version 1), RFC1163 [35] (version 2), RFC1267 [36] (version 3) and the current BGP version 4 (BGP-4) documented in RFC4271 [25].

BGP is the Internet's default EGP. It maintains and exchanges NRI between ASes which are organized in a hierarchical fashion. As with IP addresses, each AS has a unique identifier called the AS number, taken from either public or private AS number space [37]. Original AS numbers were 2-bytes and ranged from 0 to 65535. Due to growth in demand, 4-byte AS numbers were subsequently introduced ranging from 0 to 4294967295 [38]. The Internet Assigned Number Authority (IANA) has reserved, for private use, the last 1023 numbers of 2-byte AS numbers, namely 64512-65534, and the last 94967295 numbers of 4-byte AS numbers, namely 4200000000-4294967294 [39]. Each AS has a range of IP addresses identified by a prefix. For example, the IPv4 address prefix 192.2.2.0/24 refers to all addresses in the range 192.2.2.0-192.2.2.255 while the IPv6 address prefix 2001::/19 refers to all addresses in the range 2001:: to 2001:1fff:ffff:ffff:ffff:ffff:ffff:ffff. BGP provides a set of mechanisms for supporting Classless Inter-Domain Routing (CIDR) described in RFC4632 [40]. These mechanisms include aggregation support of routes with their AS-PATH (a BGP's attribute described later in Section 2.2.4) and advertising support for a set of destinations as a prefix. Aggregation is the process of combining the characteristics of several routes with common addresses into a single route. This helps reduce the number of routing messages as well as the number of

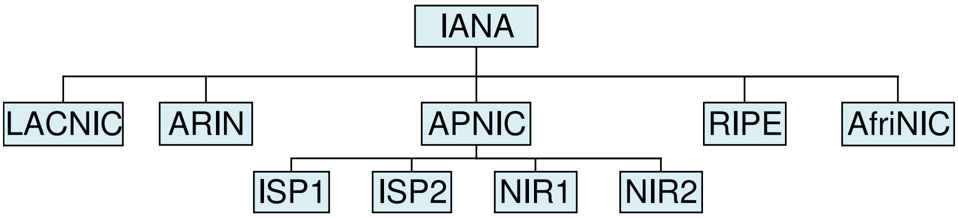


Figure 2.1: Address distribution hierarchy for the Internet

advertised routes.

IANA manages a variety of activities such as domain names, prefixes and AS numbers. IANA delegates allocation of prefixes and AS numbers to five Regional Internet Registries (RIRs). These are Réseaux IP Européens (RIPE) for assigning prefixes and AS numbers for Europe, the American Registry for Internet Numbers (ARIN) manages the IP addresses assignments for North America, the Asia-Pacific Network Information Center (APNIC) assigns IP addresses in Asia and the Pacific Rim, Latin America and Caribbean Network Information Centre (LACNIC) manages address space through the Latin American and Caribbean regions, and the African Network Information Center (AfriNIC) serves the African region. In some cases, RIRs provide services such as domain names, prefixes, and AS numbers through National Internet Registries (NIR). Figure 2.1 shows the structure of IANA where RIR such as APNIC assigns blocks of IP addresses and AS numbers to NIRs and ISPs.

### 2.2.2 BGP messages

BGP is an incremental protocol where after a complete exchange of routing table or Routing Information Base (RIB), only changes to the routing table information are exchanged through announcement messages, withdrawal messages or an update of existing route attributes. RIB for a BGP speaker (a router or a device that runs BGP) consists of Adj-RIBs-In, Adj-RIBs-Out, and Loc-RIB. Adj-RIBs-In refers to routing information that is learned from (adjacent) neighbours. Adj-RIBs-Out refers to routing information that is ready for advertisement to (adjacent) peers while Loc-RIB refers to the routes that will be used by the local BGP speaker based on its local policies and Adj-RIBs-In received [25].

BGP uses the Transmission Control Protocol (TCP) with TCP port number 179 [25]. Using TCP as a transport protocol avoids the need for BGP to manage message delivery and flow control between its peers and eliminates extra data used to confirm connection reliability. The size of BGP messages ranges from 19 octets, containing only a BGP header, to 4096 octets. Regardless of type, each message has a fixed size header as shown in Figure 2.2.

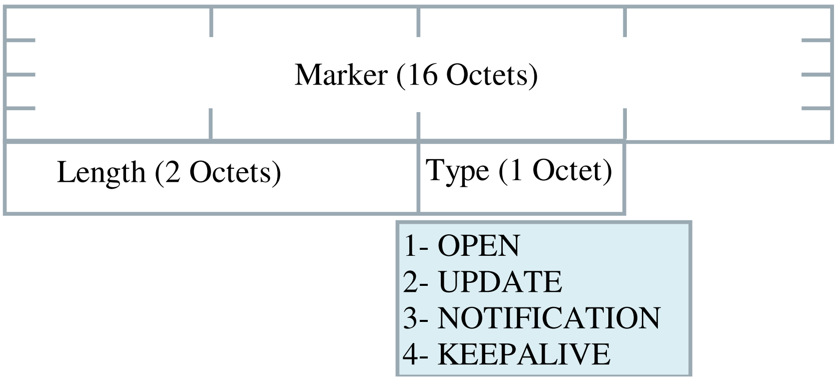


Figure 2.2: BGP common message header format

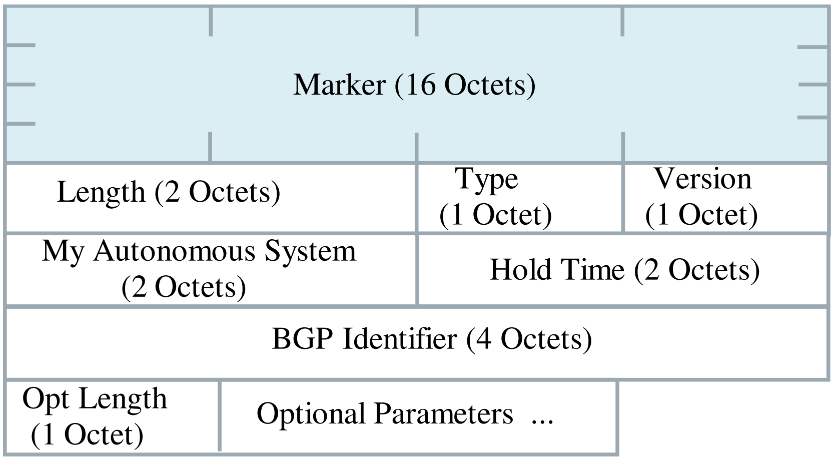


Figure 2.3: BGP open message format

The first 16 octets are all ones to mark the start of a message. While the length field represents the total message length, the type field refers to one of four possibilities: OPEN, UPDATE, NOTIFICATION, and KEEPALIVE. OPEN message is the first message sent after establishing a TCP connection between two peers. When the other side accepts this message, KEEPALIVEs are periodically transmitted to confirm the connection. Figure 2.3 shows BGP OPEN message format for a 2-byte AS number. A NOTIFICATION message supplies information regarding a terminated session.

The most important message is the UPDATE message which is used to announce a new route, withdraw a route that was advertised previously, or update an existing route with new parameters. An AS can withdraw an announced route if and only if that AS previously advertised it. Also, an AS can announce or withdraw multiple routes that have the same path attributes.

Two identities for BGP speaker are represented in the OPEN message: "My Autonomous System" refers to AS number of the sender and BGP identifier described in [41], a unique identifier within an AS where its value is determined on startup and is the same for every local interface and BGP peer.

### 2.2.3 BGP policies

Routing policy can be defined as how routing decisions are made. It is the exchange of routing information between ASes, where ASes are the unit of routing policy in BGP as stated in RFC1930 [42]. ASes interconnect with each other by different relationships. In general, there are three types of relationships: customer-provider, peer-to-peer, and sibling-to-sibling [43, 44]. In customer-provider relationships customers pay a fee to their providers for transiting traffic. ASes in peer-to-peer relationships exchange traffic without paying each other. Nevertheless, only traffic originating to or from the peered AS or their downstream customers is accepted. Traffic from their providers or other peers is not accepted. The sibling-to-sibling relationships, which is a rare case, refers to the relationship between two ASes belonging to the same organization. None of these three relationships are restricted by a physical relationship; they are business and organizational relationships.

BGP routing policies are classified into four main classes: business relationship, traffic engineering, scalability, and security-related policies [45]. ISP operators need to configure their BGP routers taking into consideration the four types of policies to enforce their relationships with other ASes. For example, an AS may need to configure its policy so that it does not provide transit services between its providers.

BGP routing policies are based on different BGP attributes; where there is no BGP policy specified, BGP will select a route with a minimum AS-PATH length. 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 [46]. A fault in configuration of a BGP router could produce a local impact or even a global impact. For example, TTNet, an ISP in Turkey, announced more than 100,000 incorrect routes to its peers causing a large number of Internet users to lose connectivity to a large number of domains for several hours [47].

Changing BGP policies can lead to route flapping [48], the situation in which BGP speaker sends an excessive number of BGP updates related to a single prefix or a set of prefixes [49]. To improve Internet stability at Internet edges, Minimum Route Advertisement Interval (MRAI) and Route Flap Damping (RFD) mechanisms have been developed to limit propagation of unstable routes. MRAI specifies a minimum time between which the speaker can send successive update messages. If an announcement is withdrawn within the MRAI neither is forwarded. RFD works on the receiving side using a larger time scale than MRAI. For each peer, RFD monitors the frequency of BGP updates for a given prefix. When the update rate between two BGP peers exceeds a set threshold, the update related to this prefix is suppressed. RFD was introduced in [49] and [50] to improve Internet stability by reducing sustained routing oscillation on network edges. RFD is a technique that has been widely implemented. However, in 2006 RIPE's routing working group recommended against using RFD [51]. Recently there are recommendations to use it but with adjustments to algorithm constants [52, 53]. It is worth noting that between the dates of RFD being introduced and it being mostly deactivated (1998-2006), RFD was not able to mitigate the propagation of unstable routes caused by indirect anomalies (described in Section 2.3.3).

### 2.2.4 BGP attributes

BGP attributes are a set of properties carried in a BGP update and used to determine the best route among many possible paths to a specific destination. These attributes are mainly classified into four types: well-known mandatory (should be included in all BGP updates and all BGP speakers can recognise them), well-known discretionary (could be included in a BGP update and all BGP speakers can recognise them), optional transitive (can be recognised by some BGP speakers. They should be accepted and sent to peers even if it is not recognized by BGP peers) and optional non-transitive attributes (can be recognised by some BGP speakers. They can be ignored and not advertised to peers). The most well-known and widely used attributes are: Origin, AS-PATH, LOCAL-PREF, AGGREGATOR, and Multi Exit Discriminator (MED) [25, 54].

Origin is a well-known mandatory attribute created by the BGP speaker that generates the related routing information. It refers to the type of an originated update with three possibilities: 0 refers to an update originating from IGP, 1 refers to an update originating from EGP, and 2 for INCOMPLETE, when a route originates from another routing protocol instead of BGP such as static route.

AS-PATH is a well-known mandatory attribute which identifies a list of ASes that have had an update message passing through their prefixes. The components of this list can be AS-SETs or AS-SEQUENCEs. AS-SET refers to an unordered set of ASes while AS-SEQUENCE refers to an ordered set of ASes. BGP is a path vector protocol where each BGP speaker adds its own AS number in the path of a BGP update before passing it to an EBGP peer. This attribute prevents routing loops between BGP speakers. Figure 2.4 shows an example of how the AS-PATH attribute works. When AS1000 sends a route to AS4000, it adds its own AS number to the beginning of the path. AS2000 receives the update and appends its AS number before passing it to AS3000. Finally, AS3000 receives the update, and inserts its own AS number to send it to AS4000. BGP is a path vector protocol where [3000,2000,1000] shows

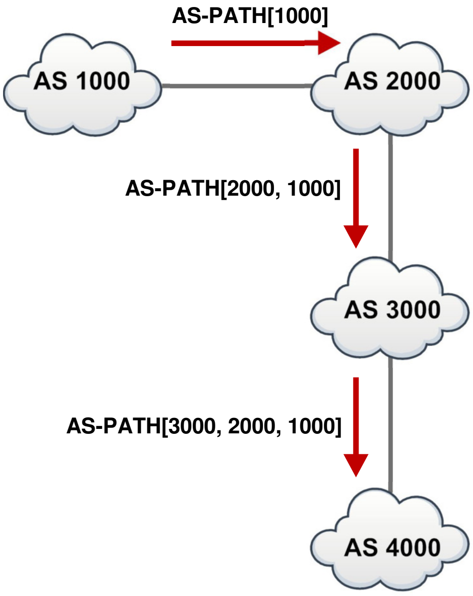


Figure 2.4: An example of BGP AS-PATH attribute

the full path for an update sent by AS1000 to AS4000.

LOCAL-PREF is a well-known discretionary attribute. LOCAL-PREF represents a degree of preference on a scale of 0 to 4294967295 for a network operator for a route between multiple routes within an AS. A high value of this attribute shows a strong preference for a particular route. For example, in a business relationship ISPs will usually prefer routes learned from their customers over routes learned from a peer; therefore, a value of LOCAL-PREF in range 99-90 could be assigned for customers, 89-80 for peers, and 79-70 for providers [45]. This attribute was used by PGBGP [18] to mitigate the propagation of suspicious routes through assigning them with low LOCAL-PREF. This attribute, however, should not be used with external peers except for the BGP confederation case described in RFC5065 [55].

AGGREGATOR is an optional transitive attribute. It contains information about the BGP speaker that aggregates the route. Although the aggregation helps to reduce the number of advertising routes, it can hide AS-PATH and other attributes of the aggregated prefixes. Figure 2.5 shows an example for route aggregation. In this example, AS1 and AS2 advertise 10.10.3.0/24 and 10.10.4.0/24 respectively to AS3. AS3 aggregates these prefixes by sending the single prefix 10.10.2.0/23. The value of AS-PATH for the single prefix is based on the aggregation configuration at AS3. AS3 can hide the paths to AS1 and AS2 and send the prefix 10.10.2.0/23 with AS-PATH=[3], this can cause a blackhole if any of the advertised prefix by AS1 or AS2 withdrawal. AS3 can also configure the aggregation to include both of the originating ASes as AS-SET, in this case AS4 will receive the prefix 10.10.2.0/23 with

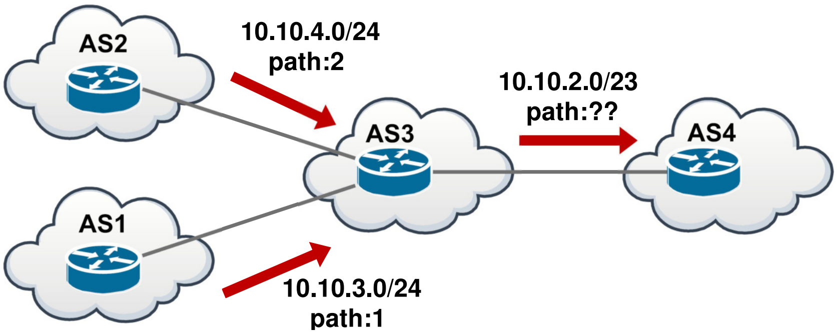


Figure 2.5: An example of BGP route aggregation

Table 2.1: BGP path selection priority

| Priority | Policy Attribute |
|---|---|
| 1. | Highest LOCAL-PREF value |
| 2. | Lowest AS-PATH length |
| 3. | Lowest Origin Type |
| 4. | Lowest MED value |
| 5. | EBGP learned over IBGP learned |
| 6. | Lowest IGP cost |
| 7. | Lowest Router ID |

AS-PATH=[3,{1,2}].

MED is an optional non-transitive attribute which provides a mechanism to influence external neighbours about the preferred path into an AS that has multiple entry points. The MED with the lower metric is preferred as an exit point.

Among these attributes, a BGP router follows a sequence of comparisons to find its best route among various routes based on their attributes. Table 2.1 shows the sequence of comparisons.

BGP messages are sent to reflect changes in ASes topology and policy. When a BGP router receives a BGP message that changes its routing table it will propagate that message to all or a group of its neighbours based on its local policies. Otherwise, the message will be terminated. Figure 2.6 shows the stages of convergence to a new prefix announced by AS1. Firstly, AS1 announces the new prefix with its AS number (10.10.0.0/16 and path:1). When AS2 receives the new announcement, it will check the announcement with its entire RIB table and because this entry is new, AS2 will add and send it to all its neighbours[1]. Secondly, AS3 and AS4 will receive the new announcement with path [2,1] and add it to their RIB as it does

[1] Routes are chosen based on the AS-PATH attribute only where other attributes such as MED and LOCAL-PREF are not considered in our examples.

not exist in their RIB. In this stage, AS3 and AS4 will propagate the new announcements to their neighbours. BGP can guarantee routes are loop free. Therefore, any BGP updates received by an AS which contains its own AS number will be ignored.

At the third stage, AS5 will receive the full path to the new prefix from AS4. Meanwhile, AS4 and AS3 receive new updates from AS3 and AS4 for the new prefix with paths [3,2,1] and [4,2,1] respectively but these updates will not be forwarded because they are not the best routes. The highlighted path [2,1] at AS3 and AS4 represents the best route.

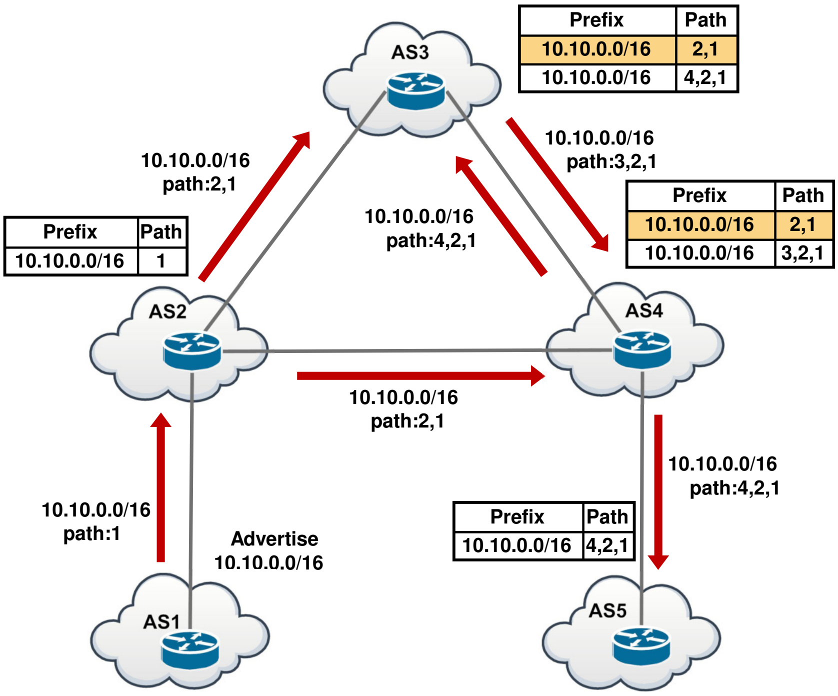


Figure 2.6: Announcing a new prefix

### 2.2.5 BGP data sources

BGP anomaly detection techniques use various sources of BGP data for detection of BGP anomalies. Usually, extracting significant information from BGP data is done during a preliminary stage of anomaly detection. These data sources include BGP raw data, route registries database as well as other types of BGP data sources [56]. Below, we describe each of these types of data.

#### 2.2.5.1 BGP raw data

There are two types of BGP raw data: control plane, which refers to RIB and/or BGP update messages exchanged between BGP speakers, and data plane, based on the routes that packets use between an observer and the source [57].

**Control plane** Control plane data can be obtained from free download repositories such as RouteViews project [58] and Réseaux IP Européens Network Coordinate Centre (RIPE NCC) [59] or monitored in a real-time from BGP speakers such as BGPmon [60] in the RouteViews project. The RouteViews and RIPE NCC are the most well-known repositories that provide free download for BGP updates and RIB. RouteViews peers with many sites in north America and had provided BGP data since 2001, while RIPE peers with many sites in Europe and provides BGP data since 1999. The total numbers of collectors and peers change over time as a result of adding/removing some vantage points[2]. The RouteViews repository provides BGP updates every 15 minutes and BGP routing tables every 2 hours. Until June 2003, RIPE was providing offline BGP updates every 15 minutes with BGP routing tables every eight hours. From 2003 it offers BGP updates every 5 minutes. The RouteViews and RIPE have been used in many research efforts such as [24, 61] and [62]. These two well-known repositories provide data in Multi-Threaded Routing Toolkit (MRT) format described in [63]. The MRT format is not a human readable. Software such as bgpdump [64] and pybgpdump [65] are used to convert it to a readable format.

The BGP speakers generate up to a gigabyte of control plane data a day [66]. Unfortunately, as well as being large, there is no direct information to identify the network that triggered the BGP messages [67]. Many tools have been introduced to extract significant information such as [68], speed up processing such as [69], and replay past BGP events such as [2]. A first step in building a scalable BGP tool that enables users querying BGP archived data with some simple analysis and statistics for a given period of time was presented in BGP-Inspect [70]. Although this tool provides much significant information such as shortest and longest path, it does not provide necessary information for operators and researchers such as the cause of shortest and longest path. Other tools with a visualization capability were presented to help diagnosis BGP anomalies such as BGPlay [71] and VisTracer [72]. Biersack et al. presented a short survey of BGP visualization tools for monitoring BGP messages and particularly for the identification of prefix hijacks [57].

In contrast to the two offline BGP repositories, BGPmon represents the next step for the RouteViews Project in term of real-time data [58]. The capability of the new monitoring

[2] For example, as at the 18th of January 2016 there are 18 collectors for the RouteViews project with 588 peers in different locations around the world while RIPE peers with 14 collectors around the world with 566 peers.

system is not limited to providing real-time monitoring but also uses Extensible Markup Language (XML) format, which is supported by many applications and is human readable [60]. BGPmon, however, does not provide data processing. Where this processing is needed, tools such as Cyclops [73] can be used for this purpose.

**Data plane** Data plane is based on the way that packets actually flow between two nodes. This data can be obtained through active probing of available live hosts in the monitored networks. Different techniques of obtaining BGP data plane have been introduced. For example, Schlamp et al. used archived netflow data of Munich's Scientific network [31]. Biersack et at. developed a tool called Spamtracer to monitor routes toward malicious hosts [57]. Others used different types of fingerprints such as host OS properties, IP identifier, TCP time stamp, and the Internet Control Message Protocol (ICMP) time stamp as an indicator to detect suspicious prefixes [74].

Control plane and data plane sources each have advantages and drawbacks. In general, techniques that use the control plane such as [75] and [73] are easy to deploy, but can be inaccurate while techniques that use the data plane such as [76], [72], and [77] have a better detection accuracy, but suffer from vantage point limitations [23, 76, 77]. Techniques that use a combination of control and data plane can be both accurate and have good vantage points, but their deployment is not easy [23, 31, 57].

#### 2.2.5.2 Route registries database

To ensure stability and consistency of Internet-wide routing, the Internet Routing Registry (IRR) was established to share information between network operators [78]. The IRR is a distributed routing database where ASes store their routing policies expressed in the Routing Policy Specification Language (RPSL) described in [79]. This data may be used by anyone worldwide to help debug routing problems, configure backbone routers, and engineer Internet routing and addressing. It also enables validation of linkage between a BGP speaker and the networks it announces, such as APNIC's whois database [80]. Each RIR has its own network information database, part of which is used for routing information. IRR has been used by many researchers to test whether BGP updates originated from valid BGP speakers. For example, Nemecis [81] is a tool to extract and infer information from an IRR database and validate it against a BGP routing table. In addition to IRR databases, there are other sources that provide IP to AS number mapping such as team Cymru [82].

Unfortunately IRR information is incomplete because of lack of maintenance [44, 83]. Siganos and Faloutsos in [81] show that just 28% of IRR information is consistent. Furthermore, using this information is limited to detecting the two direct types of anomalies, described in Section 2.3. In spite of these limitations, route registries database can be used with BGP raw data sources to produce quite robust anomaly detection [23, 56].

#### 2.2.5.3 Other sources of BGP data

In addition to the first two types of BGP data sources, there are other sources such as bogon prefixes, the mailing list archive of North American Network Operator's Group (NANOG), and IP geolocation databases. Bogon prefixes are IP addresses that should not appear on the Internet. These are either within private address space [84], in a range of space reserved by IANA, or not allocated by any RIRs [85]. Bogon prefixes are not a static list where IP addresses are regularly added/removed from bogon lists. These lists are regularly updated and published by different sources. For example, CIDR report offers a daily list of bogon prefixes based on the IANA registry files, the RIR stats files, and the RIR whois data [86]. The team Cymru also offers a list of bogon prefixes [87] which is periodically updated. ISP operators do not need only to filter these prefixes and mitigate their propagation, they need a plan for keeping their filters up-to-date. Observation of bogon prefixes may be used as an indicator to detect BGP anomaly [12]. For example, BGP misconfiguration can produce large number of bogus routes (unused prefixes) as well as used prefixes [83]. Bogon prefixes may also be used as an identifier to differentiate hijacking toward intended prefix from misconfiguration [76].

The archives of NANOG mailing list have also been used as a source of BGP data in BGP anomaly detection techniques. The NANOG contains technical information, discussion, operational issues exchanged by network operators. Feamster and Balakrishnan in [46] use the archive of NANOG to identify challenges and common problems of configuring a BGP router to build rrc, a tool that detect BGP configuration faults based on static analysis. However, the archives of NANOG mailing list cannot be used for automated detection or real-time analysis.

IP geolocation databases map an IP address to its geographical location such as MaxMind's and IP2location [88, 89]. MaxMind and IRR databases were used in [90] map prefixes to a particular country. In addition to the described sources, looking glass has also been used [23]. Looking glass are computers on the Internet that provide information relative to backbone routing and network efficiency.

Adoption of different types of BGP data can produce a more reliable BGP anomaly detection approach. For example, various types of data such as RouteViews and RIPE NCC, public route servers, looking glass, and routing registry databases have been used to detect BGP anomalies in [23]. In [90], control plane, data plane, IRR, MaxMind, and active traceroute probing from Ark [91] were used to analyse episodes of BGP anomalies in Egypt and Libya caused by service providers implementing government censorship orders.

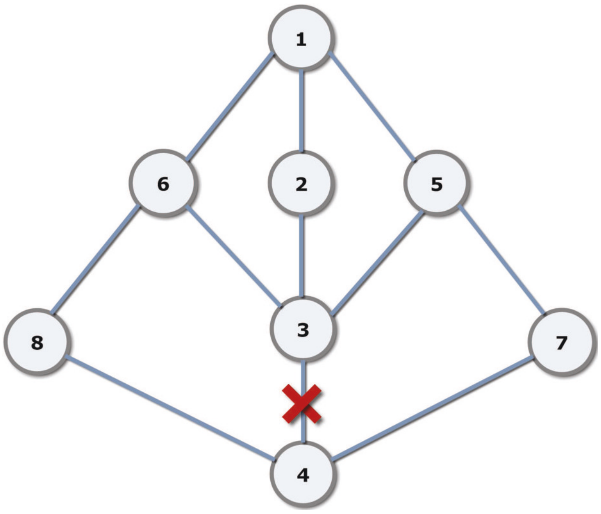


Figure 2.7: An example for the effect of a link failure

### 2.2.6 BGP features

Extracting relevant information from BGP data source produces different numbers and types of BGP features which are then used as an input to a BGP anomaly detection technique. In general, these features can be classified into two types related to deviations in number of BGP updates and in the path data contained within the update field AS-PATH.

BGP messages are complex structures and detecting abnormal data in a series of BGP messages is a challenge [92]. Although individual BGP messages that constitute an anomaly provide no direct indication of why and where they originated, analysing a series of BGP messages can give such information. Some researchers have successfully used a single BGP feature to detect BGP anomalies such as [62], where BGP message volume was used as a single BGP feature. BGP message volume refers to the number of announcements and withdrawals sent from an AS or a prefix during a selected time interval. Other researchers have used more than a single BGP feature. For example, [93] and [24] used BGP volume, AS-PATH length, and observation of rare ASes in the AS-PATH to detect BGP anomalies. During instability periods caused by anomalies such as hardware or link failure, BGP path exploration attempts to find possible alternative paths for the unreachable destination. As a result, a large number of long and rare AS-PATHs appear. The topology in Figure 2.7 explains the effect of link failure on AS-PATH length and how different lengths of AS-PATH and rare ASes appear in alternative paths. In this topology, each node represents a different AS with a single BGP router. When the path between AS3 and AS4 fails, AS3 will send a withdrawal message to its neighbours. AS1 receives notification of alternative paths from its neighbours as a result of lose the connection between AS3 and AS4 such as (2,3,5,7,4) and (2,3,6,8,4). Observ-

Table 2.2: Possible BGP features from number of BGP update

| ID | Features |
|---|---|
| 1 | Total number of announcements/withdrawals/updates per AS |
| 2 | Number of announcements/withdrawals/updates per prefix |
| 3 | Maximum/Average announcements per prefix |
| 4 | Number of duplicate announcements/withdrawals |
| 5 | Number of new announcements |
| 6 | Number of IGP, EGP, and INCOMPLETE in the Origin attribute |
| 7 | Number of re-announcements after a withdrawal |
| 8 | Number of withdrawals transmitted to unreachable prefix |
| 9 | Number of withdrawals after announcing the same path |
| 10 | Number of unique prefixes originated by an AS |
| 11 | Concentration ratio (first, second, and third) |

ing different AS-PATH lengths and rare AS numbers can help to detect such types of BGP anomalies.

Other researchers have used more specific features extracted from the two main features (deviation in number of BGP updates and AS-PATH) such as number of announced and withdrawn prefixes, average AS-PATH length, and maximum AS-PATH length, and then adopted an algorithm or a technique to find the most-important features which produce highest detection performance. Al-Rousan and Trajkovic extracted 37 features from BGP updates calculated on a 1 minute sliding window [61], then used Fisher score [94] and minimum Redundancy Maximum Relevance (mRMR) [95] to select the most-important features for detection. For this they identified 10 features that they adopted as input for detecting BGP anomaly. de Urbina Cazenave et al. presented new features related to BGP volume called concentration ratios. These features refer to the observation that the update volume is not equally distributed between all ASes and prefixes [96]. Table 2.2 and Table 2.3 show possible features used by different BGP anomaly detection techniques related to number of BGP updates and AS-PATH respectively. We will discuss these in more detail later in the next section.

## 2.3 BGP anomalies

In our survey paper [7] and this thesis, we define BGP updates that threaten BGP operation or undermines business relationships between ISPs as anomalies. The consequences of BGP anomalies can range from single to thousands of anomalous BGP updates. A single BGP update is classified as an anomaly if it contains an invalid AS number, invalid or reserved IP prefixes, a prefix announced by an illegitimate AS, AS-PATH without a physical equivalent or

Table 2.3: Possible BGP features from AS-PATH attribute

| ID | Feature |
|---|---|
| 1 | AS-PATH length |
| 2 | Maximum/Average AS-PATH length |
| 3 | Maximum/Average unique AS-PATH length |
| 4 | Announcement to longer/shorter path |
| 5 | Observation of rare ASes in the path |
| 6 | Maximum/Average of rare ASes in the path |
| 7 | AS-PATH change according to geographic location |
| 8 | Prefix origin change |
| 9 | Number of new paths announced after withdrawing an old path |
| 10 | Number of new-path announcements |

which does not match a common routing policy [97]. A set of BGP updates can be classified as an anomaly if its characteristics show a rapid change in the number of BGP updates, containing longest and shortest paths, or changes in the behaviour of total BGP traffic over time [8, 24].

Detecting BGP anomalies enables network operators to protect their network from the worst consequence of the anomalous behaviour. We construct a taxonomy of BGP anomalies with four main categories as follows [7]:

1. Direct intended anomaly.
2. Direct unintended anomaly.
3. Indirect anomaly.
4. Link failure.

These categories can be further classified into subcategories as shown in Figure 2.8 and discussed in the next section. Each type of anomaly can produce different consequences. For example, a misconfiguration by an ISP can result in announcement of used and/or unused prefixes with a consequent significant increase in BGP volume and a significant change in number of hops in paths to specific prefixes. Table 2.4 shows possible consequences for different types of BGP anomalies.

### 2.3.1 Direct intended BGP anomaly

This type of anomaly refers to all types of BGP hijacking which can appear in different scenarios such as prefix hijack and sub-prefix hijack. Hijacking occurs when an attacker claims

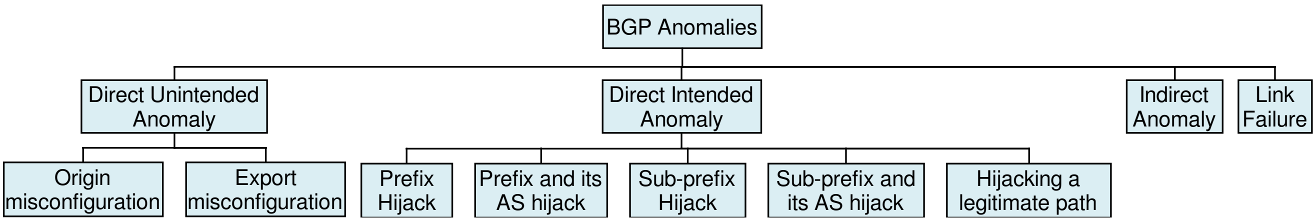


Figure 2.8: Taxonomy of BGP anomalies

Table 2.4: Possible consequences of BGP anomalies

| ID | Observed Case | Possible BGP Anomaly |
|---|---|---|
| 1 | A significant change in volume of BGP updates | All types of anomaly except direct intended |
| 2 | Observing rare ASes and long paths in the AS-PATH | Link failure |
| 3 | A significant change in number of hops between attended prefixes and monitoring points | Direct intended and unintended anomaly |
| 4 | Geographic deviation of intermediate ASes between attended prefixes and monitoring points | Direct intended and unintended anomaly |
| 5 | Reachability issues to attended prefixes | All types of anomaly |

to own a prefix or sub-prefix that belongs to another AS causing redirection of routes from the AS to the attacker. Attackers hijack prefixes to produce different malicious activities. For example, the hijacker can blackhole all traffic to the victim causing a DoS for that network. In another scenario, the attacker becomes a man-in-the-middle, intercepting the traffic without affecting victim reachability. Phishing attacks can also be done by hijacking a prefix through redirecting traffic to an incorrect destination. Additionally, the attacker can use stolen IP addresses to send spam [98].

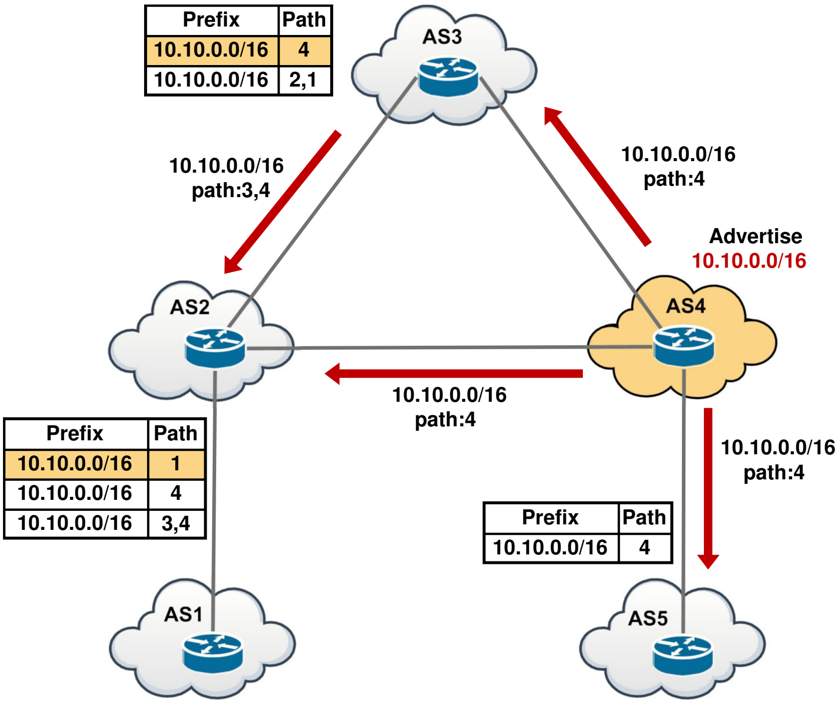
Since BGP was created, many hijacking events have been observed. Notable examples include the following. On the seventh of May 2005 AS174 hijacked one of Google's prefixes causing it to lose connectivity to the google.com domain for nearly an hour [99]. Other events have continued for longer periods of time. For example, in the Link Telecom (AS12812) incident an attacker obtained control of the company's prefixes and AS ownership for approximately 6 months and used them to send spam e-mails. The attacker took advantage of a financial crisis experienced by Link Telecom to send a forged letter of authorization for the AS12812, then started to advertise routes with the hijacked AS and its prefixes [31]. While these incidents are notable as a result of their size and scale, many similar but smaller scale incidents are unreported or not even noticed [32].

In addition to illegitimate announcements, some Distributed Denial of Service (DDoS) mitigation services will legitimately advertise sub-prefixes of a particular AS for short periods of time in order to redirect, clean (remove suspicious traffic) and reinject traffic heading towards their customer such as in [100].

The direct intended anomalies are classified into five subtypes: hijacking a prefix, a prefix and its AS, a sub-prefix, a sub-prefix and its AS, and hijacking a legitimate path [74]. To demonstrate these types of hijacking, we use the topology shown in Figure 2.6.

#### 2.3.1.1 Prefix hijack

In this type of hijack, an attacker configures its BGP router to announce a prefix belonging to another AS. BGP allows any BGP speaker to announce any route regardless of whether the route actually exists or not [19]; therefore, the attacker's neighbours will adopt it as a new route. Figure 2.9 shows an example of prefix hijacking. AS4 hijacks the prefix 10.10.0.0/16 belonging to AS1 causing a Multiple Origin AS (MOAS) conflict for other ASes. A MOAS conflict occurs when a particular prefix appears to originate from more than one AS. MOAS conflicts occur legitimately in many cases such as IXP, multi-homing, and anycast. However, identifying a valid MOAS from an attack is difficult [101].



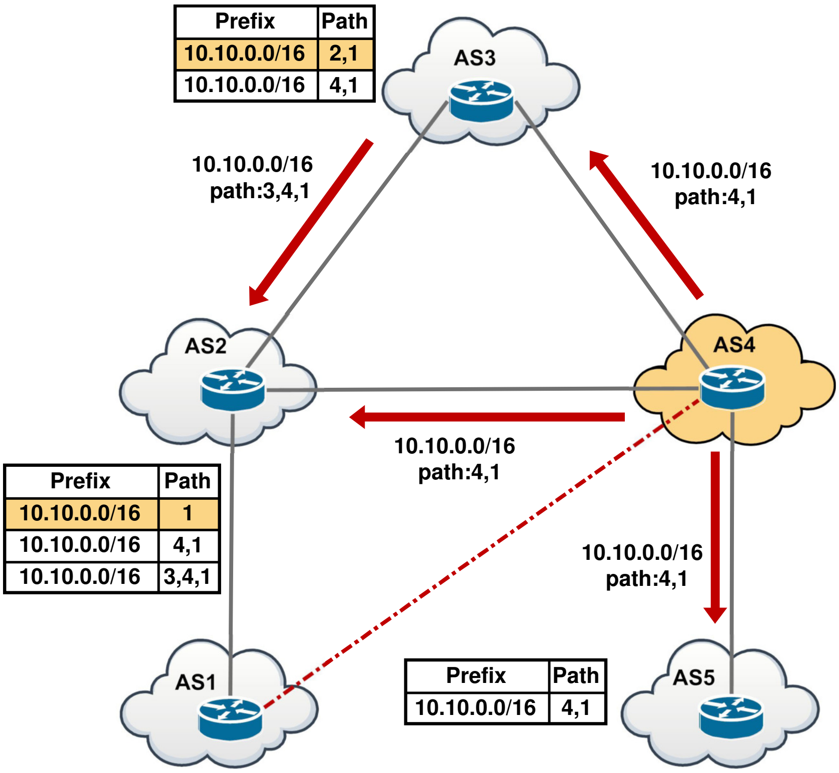
| Prefix | Path |
|---|---|
| 10.10.0.0/16 | 4 |
| 10.10.0.0/16 | 2,1 |

| Prefix | Path |
|---|---|
| 10.10.0.0/16 | 1 |
| 10.10.0.0/16 | 4 |
| 10.10.0.0/16 | 3,4 |

| Prefix | Path |
|---|---|
| 10.10.0.0/16 | 4 |

Figure 2.9: Prefix hijacking

When AS2, AS3 and AS5 receive the AS4 advertisement, they compare the new prefix with their RIB. While AS3 and AS5 update the entry (10.10.0.0/16 with path 4,2,1) to



| Prefix | Path |
|---|---|
| 10.10.0.0/16 | 2,1 |
| 10.10.0.0/16 | 4,1 |

| Prefix | Path |
|---|---|
| 10.10.0.0/16 | 1 |
| 10.10.0.0/16 | 4,1 |
| 10.10.0.0/16 | 3,4,1 |

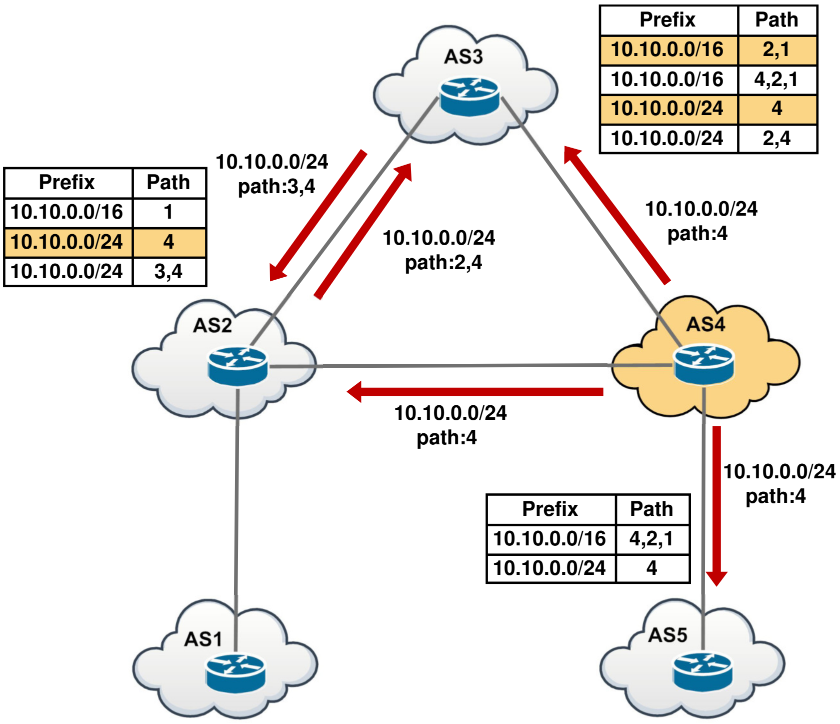
| Prefix | Path |
|---|---|
| 10.10.0.0/16 | 4,1 |

Figure 2.10: Prefix and its AS hijacking

(10.10.0.0/16 with path 4) as they previously received this prefix by AS4 (as discussed in Figure 2.6), AS2 will add it as a new entry. AS2 will not use it as a best route as it has the same path length. However, in this example, AS5 and AS3 will send all packets that relate to prefix 10.10.0.0/16 to AS4 instead of AS1.

#### 2.3.1.2 Prefix and its AS hijack

In this scenario an attacker announces that there is a direct connection between its AS and a victim AS causing redirection of routes from the AS to the attacker instead. The attacker tries to avoid a MOAS conflict by sending a fake path with the hijacked prefix. Figure 2.10 shows an example of hijacking an AS and its prefix. AS4 sends an announcement that it has a connection with AS1. AS2, AS3 and AS5 will receive this update and compare it with their RIB table. While AS5 will use the new announcement as a best route, AS2 and AS3 will not. In this example, only AS5 is affected by the hijack of AS4. AS4 can now carry out malicious activities such as DoS against AS1 and tampering with packets that are sent from AS5 to AS1.



| Prefix | Path |
|---|---|
| 10.10.0.0/16 | 2,1 |
| 10.10.0.0/16 | 4,2,1 |
| 10.10.0.0/24 | 4 |
| 10.10.0.0/24 | 2,4 |

| Prefix | Path |
|---|---|
| 10.10.0.0/16 | 1 |
| 10.10.0.0/24 | 4 |
| 10.10.0.0/24 | 3,4 |

| Prefix | Path |
|---|---|
| 10.10.0.0/16 | 4,2,1 |
| 10.10.0.0/24 | 4 |

Figure 2.11: Sub-prefix hijacking

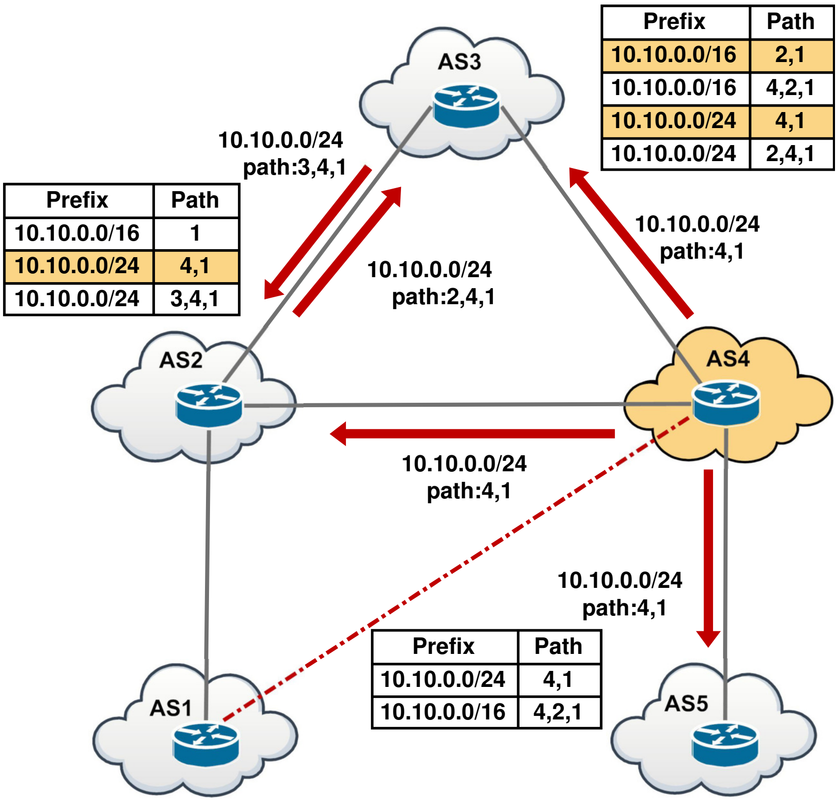
#### 2.3.1.3 Sub-prefix hijack

In this scenario an attacker announces a sub-prefix that belongs to a victim AS. BGP selects the most specific address or longest address match. For example, a BGP router will select a specific address such as 10.10.0.0/24 over a more general address such as 10.10.0.0/16. Figure 2.11 shows an example of this type of hijack where AS4 announces a prefix 10.10.0.0/24 which is a part of the prefix 10.10.0.0/16 owned by AS1. AS2, AS3 and AS5 receive this update and add it as a new entry. Although there is a direct connection between AS1 and AS2, AS2 will send all packets that belong to the prefix 10.10.0.0/24 toward AS4 instead of AS1. This is the most widely propagated type of hijacking since all ASes between the attacker and the victim are affected. Moreover, this type of hijacking can be globally propagated when there is no other advertisement or filtering for this route [74].

#### 2.3.1.4 Sub-prefix and its AS hijack

In this scenario, the attacker announces a fake path to a subnet of a target prefix. Using a fake path with sub-prefix hijack represents a critical challenge for detection as the attacker does not claim to own a full prefix length which can be detected using control plane data [77]. Hu and

Mao in [74] claim that this type of hijacking is the most difficult to detect.



| Prefix | Path |
|---|---|
| 10.10.0.0/16 | 2,1 |
| 10.10.0.0/16 | 4,2,1 |
| 10.10.0.0/24 | 4,1 |
| 10.10.0.0/24 | 2,4,1 |

| Prefix | Path |
|---|---|
| 10.10.0.0/16 | 1 |
| 10.10.0.0/24 | 4,1 |
| 10.10.0.0/24 | 3,4,1 |

| Prefix | Path |
|---|---|
| 10.10.0.0/24 | 4,1 |
| 10.10.0.0/16 | 4,2,1 |

Figure 2.12: Sub-prefix and its AS hijacking

Figure 2.12 shows an example of this type of hijacking. AS4 announces it has a path to the prefix 10.10.0.0/24 which is a part of 10.10.0.0/16 owned by AS1. AS2, AS3, and AS5 will add it as a new entry. Although the path length to the address 10.10.0.10 at AS2 is just 1, AS2 uses the longer path [4,1] as the prefix 10.10.0.0/24 is more specific than 10.10.0.0/16.

#### 2.3.1.5 Hijack a legitimate path

This type of hijacking does not require any announcements by the attacker. The attacker simply manipulates received updates before propagating them. Figure 2.13 shows how to accomplish this type of hijacking. AS4 received the update 10.10.0.0/16 with the path [2,1]. It will propagate the update 10.10.0.0/16 with the path [4,1] instead of the full path [4,2,1]. In this example, only AS5 adopts the manipulated route as a default route. This hijack is similar to the prefix and its AS hijacks but the attacker violates propagation instead of announcing an attractive path. This type of hijacking is one of the key security issues considered by the

Internet Engineering Task Force (IETF) [102], but it has received little research attention [23].

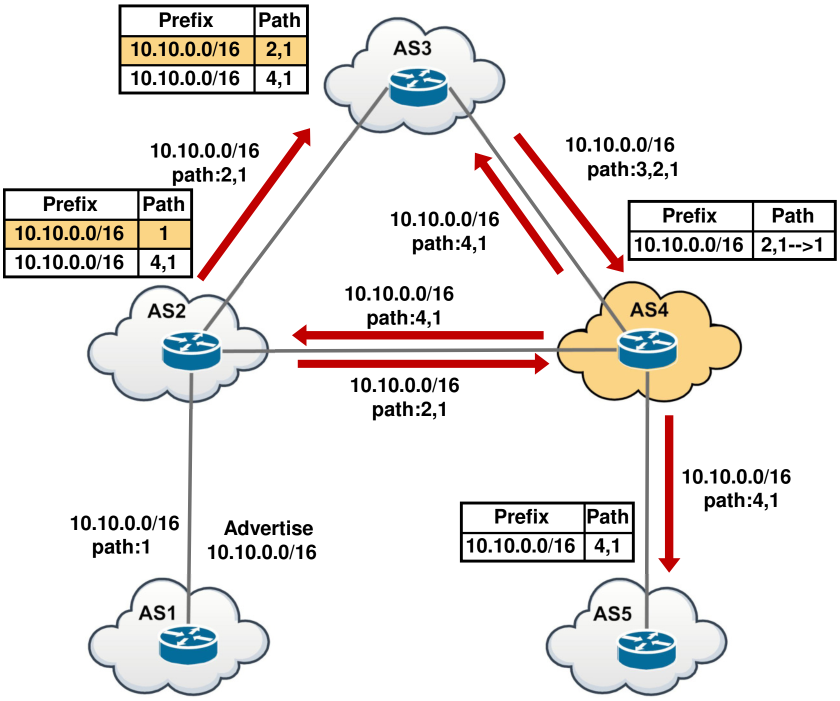


Figure 2.13: Hijacking a legitimate path

## 2.3.2 Direct unintended BGP anomaly

This type of anomaly refers to BGP misconfiguration by BGP router operators. Faulty configuration of BGP routers can result in announcing used and/or unused prefixes. While announcing used prefixes causes hijacking since the prefixes belong to other ASes, unused prefixes cause leaked routes which may result in an overload or blackhole to other ASes. The effect of announcing used prefixes is similar to 'Prefix Hijack' described earlier but is unintended and can be corrected as soon as the operator discovers it. However, the misconfiguration may cause packet loss, unintended paths between hosts, and forwarding loops [46].

Configuring BGP policies is not an easy task as there are many factors that need to be considered such as business relationships, traffic engineering, scalability, and security-related policy [45]. Consequently, this type of anomaly can occur easily. An example is a route leak incident by Dodo, an ISP in Australia, on 23 February 2012. One of Dodo's routers accidentally announced all its internal routes to Telstra, one of the major ISPs in Australia.

As Dodo is a Telstra customer, Telstra used the announced routes as its best routes causing loss of internet connectivity in most of Australia for around 45 minutes [103]. Although some tools have been developed to help operators eliminate faults, such as router configuration checker [46], rancid [104], and BGP Visibility Scanner [105], faults in BGP configuration are still frequently seen. Some of these faults have global effects such as two recent incidents observed on March 2014 by Indosat and Turk Telecom. Indosat, an Indonesian ISP, propagated over 320,000 incorrect routes for more than two hours [106]. Turk Telekom, the major ISP in Turkey, in response to instructions from the government of Turkey to censor twitter.com, accidentally hijacked IP addresses of popular DNS such as 8.8.8.8 and 4.2.2.2 [107].

BGP misconfiguration can be classified into origin misconfiguration and export misconfiguration. Origin misconfiguration occurs when the operator accidentally announces prefix/prefixes that they do not own or fail to filter private ASes. Export misconfiguration occurs when the operators accidentally configure BGP policies, for example, by blocking some authorized routes causing DoS to the blocked prefixes [83, 93]. Each type of misconfigurations has different effects. Deshpande et al. in [93] show that origin misconfiguration causes dangerous fluctuations in BGP routes while export misconfiguration threatens BGP routing convergence.

Direct unintended anomaly also refers to AS number space attribution overlaps between RIRs. In November 2009, it was noted that AS1712 has been used by both Twilight Communications (an organization in Texas assigned by ARIN) and Ecole Nationale Superieure des Telecommunications (an organization in Paris assigned by RIPE) [108]. According to IANA, AS1712 should be assigned by ARIN, not RIPE. This overlap occurred because AS numbers in the 1700's were assigned by RIPE in 1993, before the existence of ARIN, and consequently AS1712 was used by both RIPE and ARIN [109].

### 2.3.3 Indirect anomaly

This type of anomaly refers to malicious activities directed at Internet components such as web servers. Although BGP is a routing protocol for managing Internet reachability information between ASes, it experienced periods of instability during the Nimda, Code Red II, and Slammer worm attacks. These attacks caused routing overload to the entire Internet through causing some ASes to send significant numbers of BGP messages [27, 28, 110].

Nimda and Code Red II, two well-known computer worm attacks observed during 2001, were directed at hosts and servers running Microsoft Operating Systems [111]. However, large spikes of BGP messages were also observed during these attacks. During the Nimda attack around 30 times the normal number of BGP updates were observed [28]. Another example of indirect attacks is the Slammer worm attack. Slammer is the fastest computer worm yet seen, infecting more than 90% of vulnerable hosts in around 10 minutes. Although it was not directed at any routing protocol, BGP experienced critical instability during this attack. Lad et al. in [27] show the effect of the Slammer attack on BGP stability. They show a dramatic increasing in BGP update announcements during the attack. The average BGP announcement on some ASes exceeded 4500 updates per prefix compared to an average of 47 updates per prefix on the day before of the Slammer event. The problem was that no differentiation of BGP routing traffic and normal data traffic was made so that a congested data path led to BGP peer failures since KEEPALIVEs were choked. Today providers usually differentiate between routing/control/management traffic and data traffic to reduce the impact of this class of problem.

### 2.3.4 Link failure

ASes are peered together by either a private peering, through a dedicated connection between peers, or a public peering by a third party such as an IXP. Failure in one of these connection links (private or public) or one of the Internet core ASes could cause national or global instability for many ASes. The last twenty years have recorded many BGP events caused by link failure. For example, on 25 May 2005 there was a blackout in Moscow causing the MSK-IX, an organization operating Internet Exchange and providing Internet businesses in Moscow and many Russian cities, to be shutdown for several hours. This blackout affected many ISPs in Russia [112]. Other failures have a global effect. For example, in January 2008 a Mediterranean cable break incident caused thousands of networks in more than 20 countries to be unreachable. This outage caused BGP rerouting[3] as a result of losing reachability to these networks [114]. Consequently, thousands of networks were in the situation of sending a high volume of BGP updates to find alternative paths.

## 2.4 A review of BGP anomaly detection approaches

Many methods, systems, and approaches have been presented to detect BGP anomalies such as in [74] and [23] or locate the source cause of anomaly after detection such as in [92] and [115]. To simplify the comparison between BGP anomaly detection approaches and techniques, we build a taxonomy of algorithms, methods, and techniques into five main classes. These classes are: time series analysis, machine learning, statistical pattern recognition, validation of BGP updates based on historical BGP data, and reachability checks. Figure 2.14 shows our taxonomy of BGP anomaly detection in term of approaches, BGP data sources and features.

[3] Rerouting can be triggered by different causes such as network faults, misconfiguration, and hijack [113].

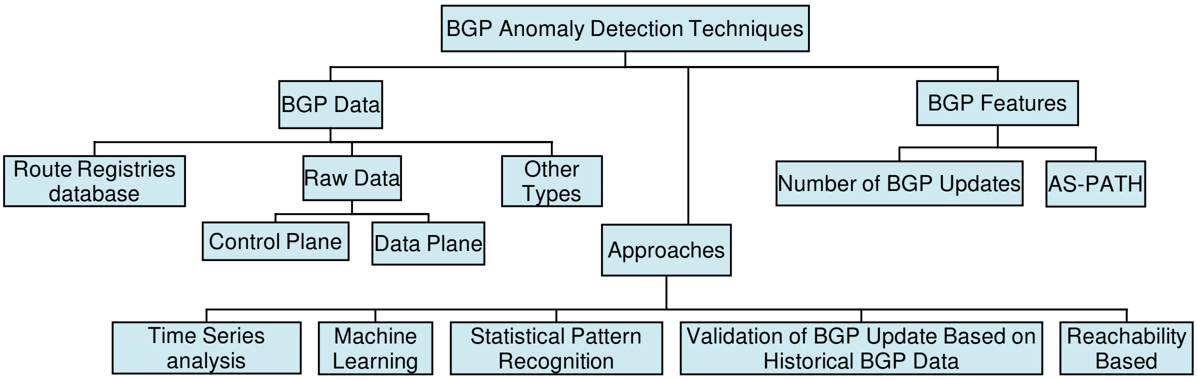


Figure 2.14: Taxonomy of BGP anomaly detection

In this section, we explore approaches of BGP anomaly detection based on five aspects.

1. Technique used for detection.
2. Ability to identify different types of anomalies.
3. Used data sources.
4. Observed BGP features.
5. Ability to identify the source cause of anomalies.

We now discuss BGP anomaly detection approaches in more detail.

### 2.4.1 Time series analysis approaches

One of the earliest efforts of identifying BGP anomalies was by Labovitz et al. [116]. The authors applied the Fast Fourier Transform (FFT) [117] to routing update rates. They used BGP data collected from five IXPs in the USA for a period of 9 months. The authors adopted five BGP features to detect BGP instability as listed in Table 2.5. Although the technique did not provide a way to identify the cause or source of routing instability, it demonstrated that rapid changes in routing updates are correlated with instability.

Another time series analysis method to detect BGP anomalies made use of the Wavelet Transform [118]. Mai et al. introduced a new framework to detect BGP anomalies called BAlet [62], an extension to the work described in [119]. The BAlet uses Daubchies5 (db5) Wavelet transform to detect BGP anomaly and Single-Linkage [120] as a clustering algorithm to identify possible networks that originate anomaly. The BAlet is based on the BGP control plane where RouteViews and RIPE NCC is used to extract BGP message volume as a single BGP feature. To evaluate the BAlet, BGP traffic during the Slammer attack and 6 months of monitoring BGP log files at the AS12 were used to detect BGP anomalies. Although the BAlet is able to identify possible location from which the anomaly originated, it is slow, typically requiring 20 minutes of data.

The Wavelet transform was also adopted in the BGP-lens [121], a tool to analyze BGP data and detect anomalies. The BGP-lens is based on using the Haar Wavelet transform and median filtering approach [122]. Its goal was to identify what characterized normal BGP data and how to detect BGP anomalies. This tool was evaluated with Abilene data (an academic research network) for a period of two years through investigation of BGP updates (announcements and withdrawals) per prefix. The BGP-lens offers three levels of alarm and a range of periods to check. However, this work did not address detection delay and appears unable to detect anomalies in real-time (in seconds).

Al-Musawi et al. in [8] showed that BGP updates sent from BGP routers have the characteristics of determinism, recurrence, and non-linearity. We used these characteristics to present an approach to BGP anomaly detection based on RQA. RQA is an advanced non-linear analysis technique based on a phase plane trajectory [123]. The approach uses BGP volume and average length of AS-PATH as BGP features extracted every second. We evaluated our approach using one of the recent BGP incidents caused by Telekom Malaysia (TMnet) which caused significant network problems for the global routing system [124]. RQA is able to rapidly detect BGP anomalies caused by a high volume of BGP updates as well as hidden abnormal behaviour that may otherwise pass without observation. Further evaluation of different types of BGP anomalies will be discussed in Chapter 5.

Table 2.5 shows a summary of BGP anomaly detection techniques based on time series analysis. It is noted that all approaches based on time series analysis in [62, 116, 121] and [8] has not been tested to detect direct intended anomalies.

### 2.4.2 Machine learning based approaches

Li et al. presented an Internet Routing Forensic (IRF) framework to detect BGP anomalies based on using a machine learning algorithm [66]. The IRF framework was based on the control plane where the RouteViews and RIPE NCC were used to extract 35 features every 1 minute. The framework applies the C4.5 algorithm [125] to build a decision tree. The authors evaluated their framework by using two different cases: worm attacks (indirect BGP anomalies), comprising the CodeRed and Nimda, and electricity failure, East Coast and Florida blackout [126]. The IRF is able to detect BGP events based on learned rules of past BGP events. For example, using the rules learned from CodeRed and Nimda worms attack to detect Slammer. However, the framework did not address the problem of identifying the location which caused the anomaly and appears not capable of doing so. The IRF, furthermore, was

Table 2.5: Summary of approaches based on time series analysis

N1= Addressed and capable, N2= Addressed but not capable, N3= Not addressed but possibly capable, N4= Not addressed and appears not capable

| Work | Used Data Source | Observed BGP Features | Technique | Types of Anomaly | Identify Source Cause |
|---|---|---|---|---|---|
| Labovitz et al. [116] | Control plane | Number of new paths announced after withdrawing an old path; Number of new-path announcements; Number of re-announcements after withdrawing the same path; Number of duplicate announcements; Number of withdrawals transmitted to unreachable prefix | FFT | Tested with 9 months of BGP data | N2 |
| Mai et al. [62] | Control plane | BGP message volume | db5 Wavelet transform and Single-Linkage | Tested with indirect anomaly and 6 months of BGP data | N1 |
| Prakash et al. [121] | Control plane | Number of announcements and withdrawals per a prefix | Haar Wavelet transform and Median filtering | Tested with 2 years of BGP data | N1 |
| Al-Musawi et al. [8] | Control plane | BGP volume and average length of AS-PATH | RQA | Tested with direct unintended anomaly | N3 |

not evaluated to detect direct types of BGP anomalies. A similar approach to IRF framework was introduced by de Urbina Cazenave et al. [96]. This framework has the ability of using different data mining algorithms such as decision tree, Naive Bayes, and Support Vector Machine (SVM) [125]. This framework consists of two main parts: an advanced feature extraction for 15 BGP features extracted every 30 seconds from BGP raw data downloaded from the Route-Views and RIPE NCC and data mining algorithms to classify BGP events. The authors show that SVM produces better performance than decision tree and Naive Bayes. Although the new proposal shows its ability to detect a wide range of BGP anomalies such as misconfiguration, blackout, and worm attacks, it was not tested to detect direct intended anomalies and did not address the problem of identifying the location that caused the anomalies and appears not capable of doing so.

Al-Rousan et al. presented another example of using machine learning to detect BGP anomalies is [61]. This mechanism consists of two main phases, an advanced feature extraction from BGP updates and a classifier to classify BGP updates as normal or abnormal. In the first phase, 37 features are extracted every 1 minute from BGP raw data downloaded from the two well-known BGP control plane repositories, then Fisher [94] and mRMR [95] scoring algorithms are used to select the 10 most-important features that have highest performance for detection. However, the authors show that volume features are more effective in detecting anomaly behavior than AS-PATH features. The second phase uses the SVM and Hidden Markov Models (HMMs) [127] to detect BGP anomalies. The suggested mechanism was evaluated using three indirect anomaly events: Slammer, Nimda, and Code Red I. Other types of BGP anomalies such as direct and indirect anomalies have also been tested. This mechanism, however, did not address how to identify the location which caused the anomalies and appears not capable of doing so.

Lutu et al. in [128] presented a system to detect BGP anomalies at an early stage based on prefix visibility at the inter-domain level. Prefix visibility is the occurrence of a prefix in the global routing table at every sampling moment. They classified prefix visibility into Limited-Visibility Prefix (LVP) and High-visibility prefix (HVP), where LVP is a stable long-lived internet route with a prefix visibility less than 95% of all routing table extracted from the RouteViews and RIPE NCC. HVP refers to prefix visibility with more than 95% of all the extracted routing table. The authors used the BGP Visibility Scanner [105], a tool for identifying limited visibility for stable prefixes in the Internet, to detect LVP and HVP. They also used a machine learning winnowing algorithm to classify whether LVP resulted from a misconfiguration by a BGP router operator or was a natural expression of global routing policies in the Internet. "Winnowing" is based on boosted classification trees described in [129]. Among 9 features based on visibility of prefixes, the 7 most important features were selected using classification and regression trees [125]. Although the proposal is able to detect anomalies which are still undetected by many other tools, it is limited to detect direct unintended anomaly. In addition, it does not show its ability to identify the location which caused the anomaly and appears not capable of doing so.

Table 2.6 shows a summary of BGP anomaly detection techniques based on machine learning. It is noted that none of these approaches [61, 66, 96, 128] address detecting BGP hijacking (direct intended anomaly) or are able to identify the source cause of anomaly.

### 2.4.3 Statistical pattern recognition based approaches

Huang et al. [130] introduced a technique to detect BGP node, link, and peer failure. This technique uses a Principal Component Analysis (PCA) based subspace method [125] to detect and differentiate between the three failures. They used three types of data source: BGP updates, operational mailing list, and routing configuration for the Abilene network, where BGP update volume was used as a single BGP feature extracted every 10 minutes with window size of 200 minutes. The authors used the NANOG operational mailing list to validate the ground truth of detection. Although the approach is able to detect, identify, and differentiate between BGP node, link, and peer failure, it requires information of router configuration and is unsuitable for real-time detection since it takes from 9-96 minutes.

Deshpande et al. in [24] presented a BGP anomaly detection approach based on the Generalized Likelihood Ratio Test (GLRT), a standard statistical technique used in hypothesis testing, deployed on a single BGP router. Three BGP features (BGP volume, AS-PATH length, and rare ASes) were extracted every 5 minutes from BGP updates downloaded from the RIPE NCC. The most relevant features among the three features were selected using Fisher score [94]. The authors showed that using AS-PATH and rare AS in AS-PATH features with message volume improved the False Positive (FP) rate compared with using message volume alone. FP refers to normal events that are classified as anomalous while False Negative (FN) refers to anomalous events that are classified as normal. The authors compared their proposal with the adaptive Exponentially Weighted Moving Average (EWMA) scheme in [131], PCA based scheme used in [130], and Wavelet based scheme used in [119]. The new approach was evaluated with ten well-known events (such as worm attacks, misconfiguration, equipment failure, and hijacking) and produced a high level of detection accuracy and low computation cost compared with the other mechanisms. However, this detection system is slow, typically needing around an hour to detect anomalies.

Ganiz et al. [132] presented a Higher-order Path Analysis (HOPA) to detect BGP anomalies and able to differentiate between indirect BGP anomaly and link failure. HOPA is a

Table 2.6: Summary of approaches based on machine learning

N1= Addressed and capable, N2= Addressed but not capable, N3= Not addressed but possibly capable, N4= Not addressed and appears not capable

| Work | Used Data Source | Observed BGP Features | Technique | Types of Anomaly | Identify Source Cause |
|---|---|---|---|---|---|
| Li et al. [66] | Control plane | Number of announcements and updates for an AS and prefix; Number of new-path announcements; Re-announcements after withdrawing the same path; Number of paths announced after withdrawing an old path; Number of withdrawals after announcing the same path<br>Selected from 35 features extracted every 1 minute | C4.5 | Tested with indirect anomaly and link failure | N4 |
| de Urbina Cazenave et al. [96] | Control plane | Number of announcements, withdrawals, and updates for an AS and prefix; Maximum and average announcements for a prefix; Maximum and average AS-PATH length; Maximum and average unique AS-PATH length; Announcements to longer and shorter path; Concentration ratio (first, second, and third) order<br>Extracted every 30 and 60 seconds | Decision tree, Naive Bayes, and SVM (best results) | Tested with direct unintended anomaly, indirect anomaly, and link failure | N4 |
| Al-Rousan and Trajkovic [61] | Control plane | Average rare ASes in an AS-PATH; Maximum AS-PATH length; Number of duplicate withdrawals<br>Number of withdrawals, incomplete packets and duplicate announcements; Packet size<br>Selected from 37 features extracted every 1 minute using Fisher and mRMR | SVM and HMMs | Tested with indirect anomaly | N4 |
| Lutu et al. [128] | Control plane | Average number and its standard deviation for LVP generated by same origin AS; Average proportion and its standard deviation of active monitors detecting the LVP; Average and standard deviation of absolute visibility degree for the LVP; Prefix length of the LVP<br>Selected from 9 features extracted every two weeks using classification and regression trees | Winnowing algorithm | Tested with direct unintended anomaly | N4 |

data-mining approach used to produce relevant information from BGP updates, downloaded from the RouteViews project, every 6 minutes, then classify them using Student's t-test [125], a statistical hypothesis analysis. Although their approach is able to differentiate between two types of BGP anomalies in 360 seconds, it was not evaluated with the most common types of BGP anomalies (the two direct anomalies). In addition, HOPA did not address how to identify the location which caused the anomalies but it is possibly capable of doing so.

Theodoridis et al. [133] introduced an unsupervised learning mechanism to detect BGP hijacking using control plane BGP raw data. This mechanism is based on observing the geographic changes of intermediate AS in the AS-PATH between the competing routes. Frequency of AS appearance in the path and geographic deviation of intermediate AS were introduced as a two BGP features. These two features have also been used by BGPfuse [134], a visualization tool to detect BGP hijacking. The unsupervised proposal uses Z-score calculation, a statistical measure for a particular value of the number of standard deviations [125], to rank how much the intermediate AS are suspicious. The authors assumed that the attackers usually carried out their activity on remote locations to avoid any legal actions and reduce the possibility of identification. This mechanism was evaluated using the Link Telecom incident and showed it was able to detect the deviation of intermediate AS during the hijack. This mechanism did not address how to identify the location which caused the anomaly nor real time detection but it is possibly capable of doing so. However, the authors did not evaluate the ability of their mechanism to detect other types of BGP anomalies such as direct unintended and indirect anomalies.

Table 2.7 shows a summary of techniques based on statistical pattern recognition to detect BGP anomalies. It is noted that approaches based on statistical pattern recognition show their ability to detect different types of BGP anomaly and identify the source cause.

### 2.4.4 Validation of BGP updates based on historical BGP data

This approach to BGP anomaly detection uses a history of RIB table and/or BGP updates to validate new BGP updates, assuming that Internet topology does not frequently change. Pretty Good BGP (PGBGP) is a detection and mitigation system against BGP attacks [18]. PGBGP uses history of both RIB and BGP updates downloaded from the RouteViews project to validate new updates. It uses a prefix and origin AS pair (prefix origin change feature) from both RIB and update history over the previous 10 days. It also eliminates routes that are no longer active and older than 10 days. When a new route is received and its pair (prefix and origin AS) is not recorded in the history period, it considers the update suspicious and will be propagated with a low LOCAL-PREF. PGBGP did not address the problem of identifying the

Table 2.7: Summary of approaches based on statistical pattern recognition

N1= Addressed and capable, N2= Addressed but not capable, N3= Not addressed but possibly capable, N4= Not addressed and appears not capable

| Work | Used Data Source | Observed BGP Features | Technique | Types of Anomaly | Identify Source Cause |
|---|---|---|---|---|---|
| Huang et al. [130] | Control plane, operational mailing list, and routing configuration | BGP volume extracted every 10 minutes with a window size of 200 minutes | PCA-based on subspace method | Tested with link failure | N1 |
| Deshpande et al. [24] | Control plane | BGP volume; AS-PATH length; Rare AS in a path Extracted every 5 minutes | EWMA, PCA, and GLRT (better performance) | Tested with all types of anomalies | N1 |
| Ganiz et al. [132] | Control plane | Number of announcements, withdrawals, and updates for an AS and prefix | HOPA | Tested with indirect anomaly and link failure | N3 |
| Theodoridis et al. [133] | Control plane | Frequency of AS appearance in the path; Geographic deviation of intermediate AS | Z-score calculation | Tested with direct intended anomaly | N3 |

location which caused the anomaly but it possibly capable of doing so. Although PGBGP is able to detect prefix and sub-prefix hijacking, it has some limitation related to using the history period (10 days). For example, MOAS may last for a few days and may not be observed for months. An enhanced history-based algorithm was introduced by Sriram et al. [56] that successfully overcame PGBGP drawbacks through using a longer period (e.g, months).

Lad et al. [75] presented PHAS, a prefix hijacking detecting system with the capability of sending alarms to the real prefix owners. PHAS analyzes BGP data in real-time to detect when a prefix hijacking event occurred or was resolved. PHAS requires a registration process from prefix owners who want to use it. The registration is used as a base point to monitor origin changes of that prefix. The system uses an adaptive window scheme with 1 hour as the initial size window. The adaptive scheme increases the window size when there are many changes in the origin of a prefix and decreases it in case of a small number of changes. The authors believe that only the prefix owners can distinguish between legitimate changes and hijacking changes for their prefixes; therefore, this approach offers a filter facility to prefix owners to add which AS may use a specified prefix. PHAS uses the RouteViews repository as a BGP control plane and prefix origin changes as a single BGP feature. Although the system does not require any router reconfiguration, it requires registration and has consequent issues related to authenticating legitimate ownership as there is no secure mechanism to differentiate between a legitimate owner and an attacker.

Haeberlen et al. [19] presented a prototype to detect BGP faults at the AS level called NetReview. This prototype uses a tamper-evident log, containing BGP messages to and from AS neighbours, to detect BGP faults, where BGP faults include BGP router and link failure, misconfiguration, policy violations, and attacks. NetReview requires each BGP speaker to maintain a history log file of around one year of data and a set of rules that describe its best practices and routing polices, then other ASes can use this information to audit how the rules are followed. NetReview requires each AS to log a public pledge to show its ownership of AS numbers and prefixes. NetReview has been tested under a control testbed to detect different types of BGP anomalies. Although NetReview can detect in real-time different types of BGP anomalies and identify their source cause, it requires each AS to reveal information related to its policy configuration and suffers from scalability problems related to the size of storing log files especially for large ISPs.

Argus [23, 135] 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 BGP data to classify new BGP updates as normal or suspicious, then checks the reachability of prefixes to verify the suspicious updates through using tools such as iplane [136] and CAIDA's

Ark [91]. In addition, the IRR data is also used to improve the false positive rate. Although Argus can detect BGP hijacking and identify the source cause in real-time, it cannot detect sub-prefix hijacking nor other types of anomalies such as indirect anomaly and link failure.

Table 2.8 shows a summary of work in detecting BGP anomalies based on historical RIB and/or BGP updates. It is noted that all approaches based on historical BGP data use prefix origin change as a single BGP feature.

Table 2.8: Summary of approaches based on using historical BGP data

N1= Addressed and capable, N2= Addressed but not capable, N3= Not addressed but possibly capable, N4= Not addressed and appears not capable

| Work | Used Data Source | Observed BGP Features | Technique | Types of Anomaly | Identify Source Cause |
|---|---|---|---|---|---|
| Karlin et al. [18] | control plane | Prefix origin change | Validate new BGP update based on 10 days of BGP history | Tested with direct intended anomaly | N3 |
| Lad et al. [75] | control plane | Prefix origin change | Validate new BGP updates based on prefix registration by owners | Tested with direct intended anomaly | N3 |
| Haeberlen et al. [19] | control plane | Prefix origin change | Validate new BGP updates based on 1 years of BGP and set of rules | Tested with a control testbed | N1 |
| Shi et al. [23] | control plane, data plane, and IRR | Prefix origin change | Classify new BGP updates based on 2 months of BGP history | Tested with direct intended and unintended anomalies | N1 |

### 2.4.5 Reachability check

This type of technique uses the BGP data plane to check reachability to a certain prefix using different types of tools such as hping [137], Nmap [138], traceroute [139], iTraceroute [140], and Paris traceroute [141]. One of the earliest works to detect BGP hijacking based on data plane was by Zheng et al. [76]. The authors assumed that the network location for a prefix remains unchanged over time so a significant change in network distance (hop count between source and destination) from a selected vantage point to a certain IP may be used as an indicator of hijacking. They used a combination of ping, traceroute, and iplane [136] to count the number of hops towards a certain prefix. This proposal can detect prefix hijacking in real-time, but it is not able to detect sub-prefix hijacking. Furthermore, it was not tested to detect other types of anomalies.

In [74], the control plane is used to detect suspicious BGP messages, then data plane probing is launched to verify if the suspicious data is an anomaly or not. In general, attackers use dissimilar OS or configure OS to open some ports when compared with legitimate users; thus, tools such as Nmap [138] can identify the OS fingerprint of the attacker. The authors used a set of fingerprints such as host OS properties, IP identifier, TCP time stamp, and ICMP time stamp to identify the attackers. For example, the IP identifier is designed to be unique for each IP datagram to help IP fragment reassembly. The identifier is incremented for every outgoing packet regardless of its destination. The authors used this identifier to send probe packets simultaneously to the same suspicious IP from two locations to check if they arrived at the same destination. The authors did not address the problem of identifying the location which caused the anomaly but it is possibly capable of doing so. However, this system is difficult to deploy as it relies on complicated probing and requires installation of customized software at its vantage points [23].

Tahara et al. [142] proposed a method to detect prefix hijacking based on data plane by using a ping test. When an attacker hijacks a prefix, packets traverse toward the attacker instead of the real prefix owner. However, during a hijacking attack, not all AS experience the effect of the attackers (as shown in Figure 2.9); therefore, checking reachability to a suspicious prefix from different vantage points can be used by an observer to detect a prefix hijack. The authors, however, did not address detection delay nor identification of the location which caused the anomalies but the method is possibly capable of doing so.

Zhang et al. presented iSPY [77], a tool for detecting prefix hijack in real-time based on the observation that connectivity to victim hosts is lost during hijacking attempts. iSPY is able to distinguish between a real attack and a link failure or network congestion. It uses the BGP data plane where a combination of iTraceroute, ping, and TCP ping, a ping over TCP port such as that available in Nmap [138], are used to check the reachability to a certain prefix. Deploying iSPY on a network requires collecting in advance a set of live IPs using active probing, an IP-to-AS mapping, and a continuous update to its database. However, iSPY's ability is limited to detecting regular prefix hijacking only. Other types of hijacking such as sub-prefix hijacking cannot be detected.

Table 2.9 shows a summary of work for detecting BGP anomalies based on reachability check. This table shows that all approached based on reachability check use data plane to detect or verify the exist of anomaly. However, none of these approaches were tested to detect indirect BGP anomaly.

Table 2.9: Summary of approaches based on reachability check

N1= Addressed and capable, N2= Addressed but not capable, N3= Not addressed but possibly capable, N4= Not addressed and appears not capable

| Work | Used Data Source | Observed BGP Features | Technique | Types of Anomaly | Identify Source Cause |
|---|---|---|---|---|---|
| Zheng et al. [76] | Data plane | Number of hops toward a suspicious prefix | Combination of ping, traceroute, and iplane | Tested with direct intended anomaly | N1 |
| Hu and Mao [74] | Control plane and data plane | Set of fingerprints such as OS properties, IP identifier, TCP time stamp, and ICMP time stamp | Combination of hping and Nmap | Tested with direct intended anomaly | N3 |
| Tahara et al. [142] | Data plane | Reachability from different vantage points | Ping test | Tested with direct intended anomaly | N3 |
| Zhang et al. [77] | Data plane | Reachability of a prefix from transit ASes | Combination of iTraceroute, ping, and TCP ping | Tested with direct intended anomaly and link failure | N2 |

## 2.5 Key requirements for next generation of BGP anomaly detection

We have presented many systems, approaches, and tools with different capabilities for detecting BGP anomalies. A summary comparison between BGP anomalies detection techniques in term of real-time detection, ability to detect different types of BGP anomalies, differentiate between types of BGP anomalies, and identify the location which caused the anomaly is shown in Table 2.10. This table shows that none of these works offers a combination of adequate real-time detection and identification for all types of anomalies as well as locating the cause of anomalies. A recent analysis [23] shows that some hijackings proceed in less than ten minutes and can affect 90% of the Internet within less than two minutes. Thus, detection of BGP anomalies in real-time (less than two minutes) is required to mitigate their propagation between BGP speakers. However, detecting BGP anomaly in real-time is not enough to stop propagation of anomalies without requiring action from the operators. To accomplish that, the operators need extra information to ensure that an alarm is raised by serious threats. This

Table 2.10: Reviewed works in light of four characteristics properties

C1=Has not been tested with a specific type of anomaly, C2= Direct intended anomaly, C3=Direct unintended anomaly, C4= Indirect anomaly, C5=Link failure, N1= Addressed and capable, N2= Addressed but not capable, N3= Not addressed but possibly capable, N4= Not addressed and appears not capable

| Work | Real-time Detection | BGP Detected Anomalies | Differentiate Between Anomalies | Identify Source Cause |
|---|---|---|---|---|
| Labovitz et al. [116] | N4 | C1 | N4 | N2 |
| Mai et al. [62] | N2 | C4 | N4 | N1 |
| Prakash et al. [121] | N4 | C1 | N4 | N1 |
| Al-Musawi et al. [8] | N1 | C3 | N4 | N3 |
| Li et al. [66] | N2 | C4 and C5 | N4 | N4 |
| de Urbina Cazenave et al. [96] | N1 | C3, C4, and C5 | N4 | N4 |
| Al-Rousan and Trajkovic [61] | N4 | C4 | N4 | N4 |
| Lutu et al. [128] | N4 | C3 | N4 | N4 |
| Huang et al. [130] | N2 | C5 | N4 | N1 |
| Deshpande et al. in [24] | N2 | C2, C3, C4, and C5 | N4 | N1 |
| Ganiz et al. [132] | N1 | C4 and C5 | between C4 and C5 | N3 |
| Theodoridis et al. [133] | N3 | C2 | N4 | N3 |
| Karlin et al. [18] | N2 | C2 | N4 | N3 |
| Lad et al. [75] | N2 | C2 | N4 | N3 |
| Haeberlen et al. [19] | N1 | C1 | N4 | N1 |
| Shi et al. [23] | N1 | C2 and C3 | N4 | N1 |
| Zheng et al. [76] | N1 | C2 | N4 | N1 |
| Hu and Mao [74] | N1 | C2 | N4 | N3 |
| Tahara et al. [142] | N3 | C2 | N4 | N3 |
| Zhang et al. [77] | N1 | C2 and C5 | between C2 and C5 | N2 |

can be done through identifying the type of anomaly as well as the location which caused the anomaly. For example, the action taken by an operator when dealing with a direct intended anomaly is different from that taken when dealing with direct unintended anomaly, where the unintended anomaly may stop as soon as the operator discovers the fault or is informed of it by its neighbours. However, distinguishing direct and intended from unintended anomaly has not been resolved [32]. The ability to locate the attackers is critical for mitigating anomaly effects through introducing an early recognition mechanism to stop the propagation of attacks.

## 2.6 Conclusions

BGP is the Internet's default inter-domain routing protocol. It was developed at a time when information provided by an AS could be assumed to be accurate. BGP has been threatened by different types of anomalies that affect its stability and performance. During the past twenty years many different types of anomalies have affected BGP stability and performance. These can be mainly classified into four main categories: direct intended anomaly, direct unintended anomaly, indirect anomaly, and link failure. We also classify BGP data sources into three main categories: raw data (control plane and data plane) and route registry database as well as other types of BGP data sources.

This chapter surveys 20 significant works in the field of BGP anomaly detection during the period of 1998 to late 2015. It examines these works in terms of BGP data sources and features, detection technique, ability to detect different type of BGP anomalies and locate the source cause of anomalies. Time series analysis, machine learning, statistical pattern recognition, validation of BGP updates based on history log, and reachability check are the main techniques that have been used to detect BGP anomalies.

There is still much to be done in the field. None of these significant works offers a combination of detecting in real-time for all types of anomalies, differentiating between them, and identifying the source cause of the anomaly. This combination is needed to enable operators to mitigate the propagation of anomalies, protect their network, and help to understand the inter-domain routing protocol.

# Chapter 3

# Recurrence quantification analysis

## 3.1 Introduction

We are familiar with many situations in daily life where we can predict with reasonable certainty, how they will evolve. For example, parents can predict if their children are straying into danger if they are playing too near a road. We can predict that a thunderstorm is likely by observing the sky on a hot and humid summer's day. These types of predictions are not based on complex analysis but on having seen the progression evolve in the past. The prediction makes use of the fact that many situations evolve in a similar way. In other words, they exhibit some degree of determinism.

Deterministic systems have attracted much attention in recent decades [123]. Many systems that in the past were thought to be random are now thought to be chaotic. That is, they are deterministic but very sensitive to small changes in initial conditions. Many systems may not be strictly deterministic, but the progress of some sequence of behavior may well be deterministic. We cannot predict the weather more than a few days ahead, but when we see a particular sequence of weather events we can be confident (as in the example above) that a thunderstorm is in the offing.

We describe such systems as recurrent. The system may exhibit some predictable sequence of behavior for a period of time, before switching to another sequence of predictable behavior. Each sequence is broadly predictable but transitions from one sequence to another may not be. These systems were originally analysed using a graphical method called a RP. RPs enable the visualization of the evolution of potentially non-stationary dynamical systems [143]. The essential idea is that the system has a trajectory within an m-dimensional phase space. A phase space is constructed by mapping the system behavior against a time shifted version of itself. An RP is a two dimensional representation of the phase space trajectory. The power of such analysis is that it uncovers time correlations between data regardless of whether the system is linear or non-linear, stationary or non-stationary[1]. Thus it is able to uncover patterns that may not be apparent from simply analysing a one dimensional series of values. RP has been used in many disciplines such as astrophysics and geosciences to characterize time series behavior [123].

Although it is a powerful tool for visualizing system behavior, RPs are essentially qualitative and require considerable expertise to interpret. RQA was introduced to deal with these shortcomings. It provides quantitative measures of recurrence from the RP and simplifies interpretation of recurrent data. In RQA the density of recurrence points, histograms of the lengths of diagonal and vertical lines and other characteristics of the RP are quantified to provide useful measures of complexity. RQA has been used to detect anomalous behavior in network traffic [144] and computer programs [145].

In this chapter we introduce the concepts of the phase space trajectory, RPs and RQA. We also demonstrate how RQA measurements are related to typical time series. Furthermore, we show how RQA can be used to detect anomalies within the underlying time series that may not be apparent using conventional techniques.

This chapter is organized as follows: Section 3.2 introduces the phase space trajectory of a system, estimates type of motion, identifies determinism and linearity for dynamic systems. Section 3.3 illustrates how RP can be used to visualize the time dependent behavior of the dynamic behavior of a system. Section 3.4 introduces RQA and shows how RQA can be used to simplify interpretation of an RP through the introduction of a number of recurrence measures. In Section 3.5, we demonstrate how RQA measurements change when there is a change in the underlying time series. Finally, in Section 3.6 we summarise the chapter.

## 3.2 Phase space trajectory

The states of systems in nature and engineering typically change over time. The study of transitions of these states is an important task in many disciplines. It provides a way of understanding these systems and predicting their behaviour [123, 146]. Such systems can be defined as dynamical systems consisting of a set of variables that describes their current state and a law that describes how their state changes with time. Formally, a dynamical system is defined by a phase space, a time evolution law and continuous or discrete time.

In phase space, each point corresponds to a definite system state and as the system propagates through time a trajectory is formed. The state of a system at time $t$ can be specified by $d$ variables to form a vector $x(t)$ in $d$ -dimensional phase space. That is

[1] Stationary time series is a characteristic of having a distribution that is independent of time shifts. Most often, the values of mean, variance and auto-correlation structure are constant over time.

$$\vec{x}(t) = (x_1(t), x_2(t), \ldots, x_d(t))^T. \tag{3.1}$$

The time evolution law allows determination of the system at time $t$ based on previous states. In a continuous time system this can be described by a set of differential equations.

$$\dot{\vec{x}}(t) = \frac{d\vec{x}(t)}{dt} = \vec{F}(\vec{x}(t)), \qquad F : \mathbb{R}^d \to \mathbb{R}^d, \tag{3.2}$$

where vector $x(t)$ is a trajectory in phase space.

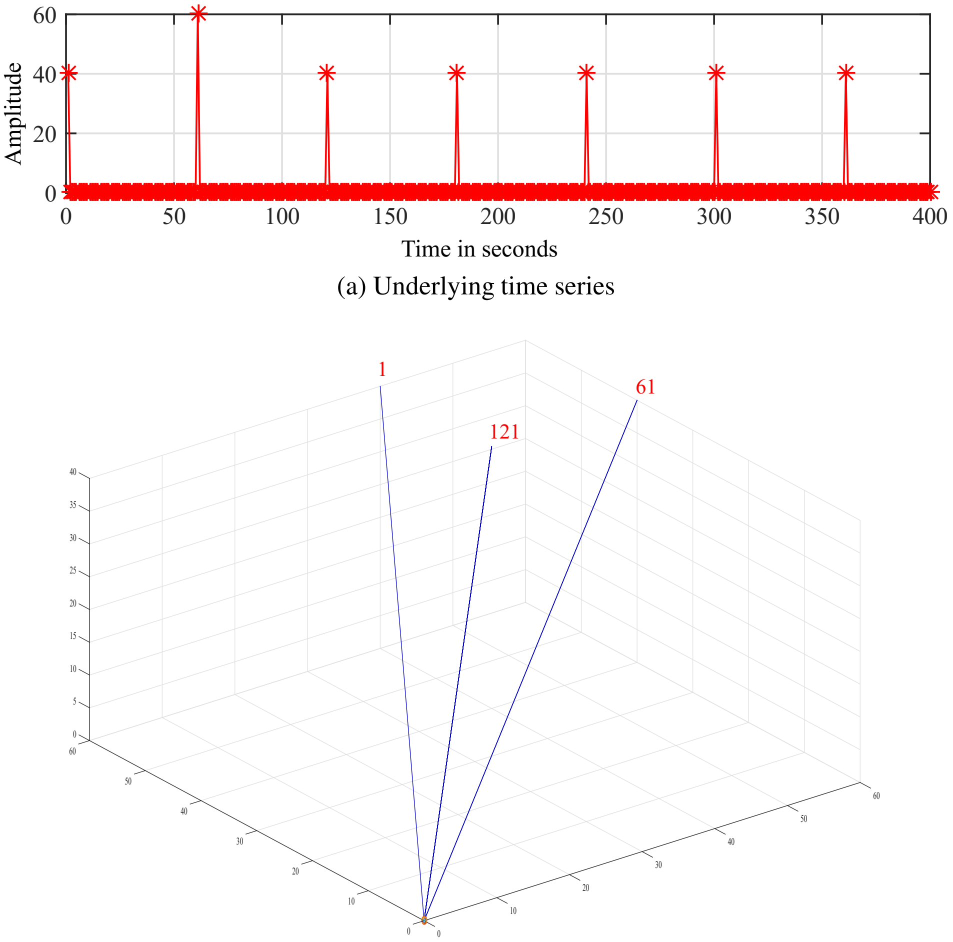
The time evolution of the trajectory describes the dynamics of the system. In particular the trajectory shape can indicate whether the system is periodic, chaotic, stochastic or some combination of all three. However, in practice not all components can be measured. More commonly we have a scalar and discrete time series $(u_i)$ where $u_i = u(i\triangle t)$, $i = 1, \ldots, N$ and $\triangle t$ is a sample interval. A frequently used technique for reconstructing phase space from a time series is the time delay embedding method. This is used to determine the time delay and dimension of the phase space. From the time series, the phase space trajectory can be then reconstructed by

$$\hat{\vec{x}}_i = \sum_{j=1}^{m} u_{i+(j-1)\tau} \vec{e}_j, \tag{3.3}$$

where $m$ is the embedding dimension, $\tau$ is the time delay, $\vec{e}_j$ are the unit vectors.

To reconstruct phase space trajectories using time embedding method, embedding dimension and time delay parameters need to be selected carefully. 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. Although the estimation of time delay needs careful attention [123], Webber and Zbilut in [147] argue there is no need to find the optimal time delay. They show that it is not necessary to find the optimal value as system features tend to be stable over different time delays but they recommend choosing a large enough value so that each trajectory in the phase plane adds new information to the phase plane trajectories. 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.

We now illustrate these concepts with some simple examples. Figure 3.1b shows phase space representation for a simple discrete time series input data shown in Figure 3.1a with time delay=60 ($\tau = 60$) and embedding dimension=3 ($m$=3) calculated by MI and FNN respectively. In this figure, we can see that phase space can detect the changes in the input data at times 1, 61, and 121 seconds. These three changes reflect the transition of the system represented in its underlying time series shown in Figure 3.1a. The first change represents the first state of the system at time 1 second, then a new state appears at time 61 seconds and finally the system returns to its initial state at time 121 seconds.

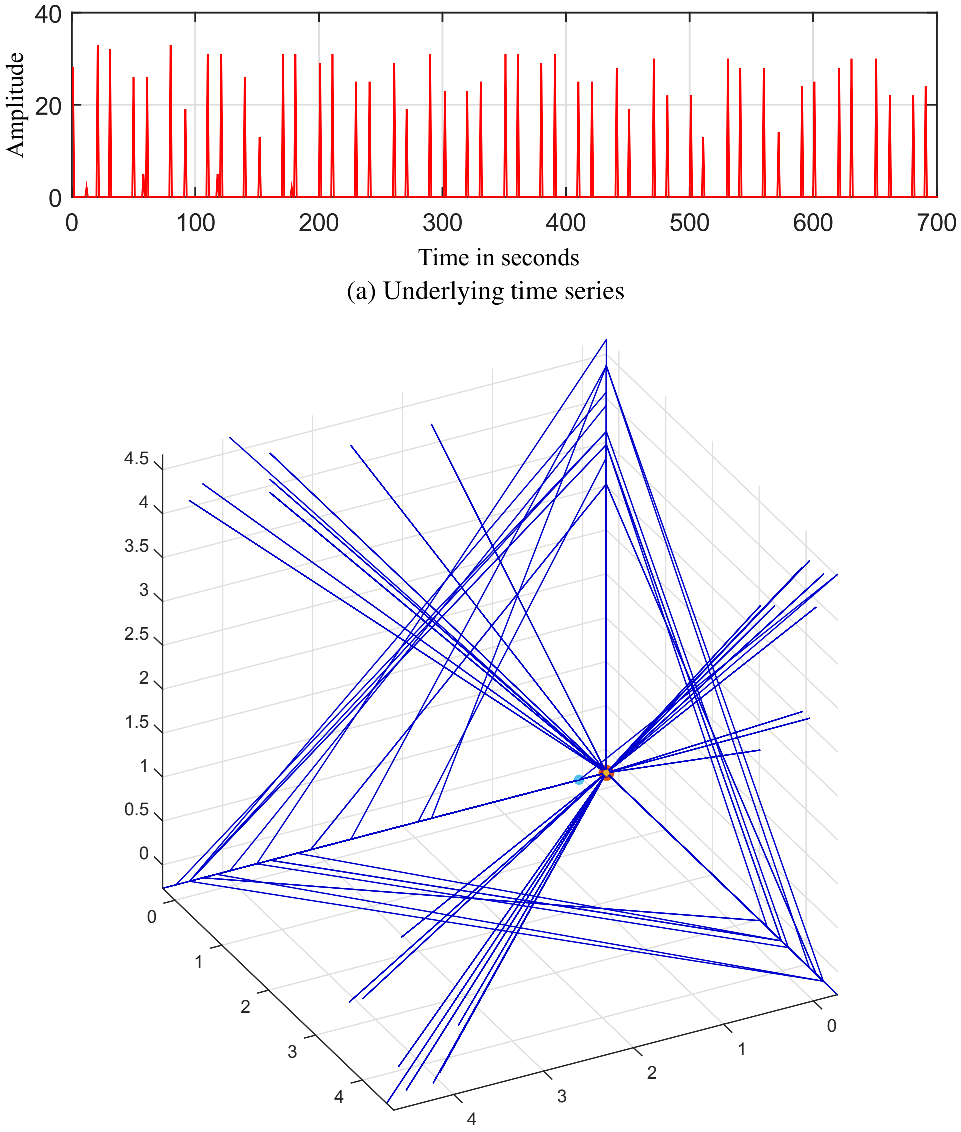


(a) Underlying time series

(b) Phase space representation with $\tau$ =60 and $m$=3

Figure 3.1: Simple example of underlying time series and its corresponding representation of phase space

Figure 3.2 demonstrates how the characteristics of a more complex system can be determined. The time series in Figure 3.2a shows a periodic discrete time series input data while its corresponding phase space representation shown in Figure 3.2b where we can see multiple triangles parallel to each other. Within phase space, periodic behaviour typically appears as cycles.



(a) Underlying time series

(b) Phase space representation with $\tau$ =10 and $m$=3

Figure 3.2: An example of a periodic data and its corresponding representation of phase space

However, identifying the type of motion in dynamic systems using phase plane trajectories is difficult. Different techniques have been introduced to estimate the type of motion in dynamic systems which will be discussed in the next subsection.

### 3.2.1 Type of motion

In dynamical systems, there are different types of motion such as stable, where a system's behaviour appears stable around a point in the phase space, and noisy, where the behaviour is fully random. Identifying the type of motion for a dynamical system can help us understand system behaviour.

While estimating the type of motion in a dynamical system is comparatively easy if the equation of motion in the phase space is available, it is a difficult task when only a series of data is available. With a lack of knowledge about the underlying dynamics, the maximal Lyapunov exponent is a good measure to estimate the type of motion in dynamical systems [148, 149].

The Lyapunov exponent is a measure of the speed with which two points in close proximity separate as the system evolves. To identify type of motion in dynamic systems, maximal Lyapunov exponents is used. The maximal Lyapunov exponents refers to the slope of Lyapunov exponents where a positive slope indicate a chaotic system, a zero slope indicate a possible stable limit cycle system, and an infinite slope indicates a noisy system.

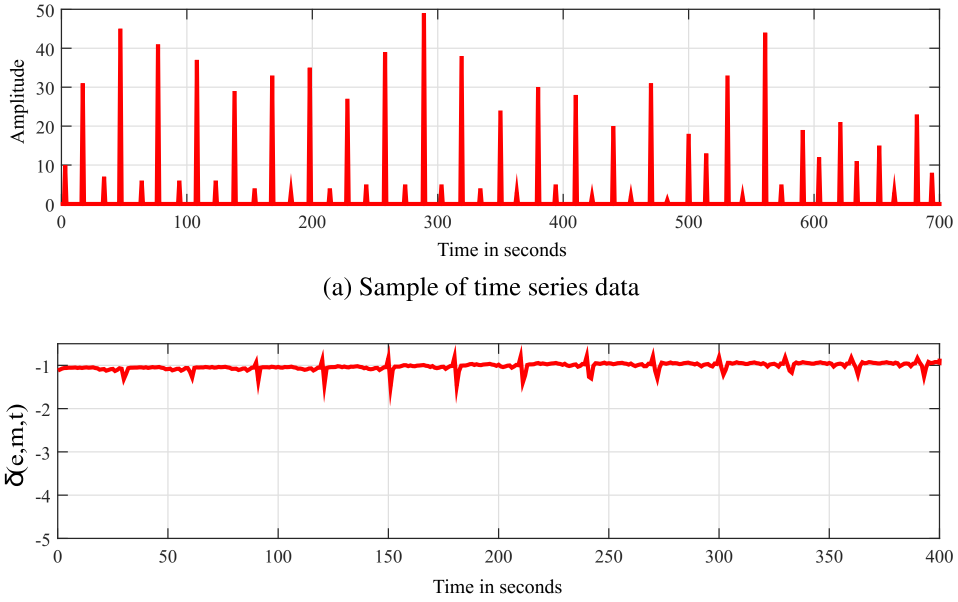
Different methods have been proposed to find the maximum Lyapunov exponents. The most well-known methods are described in [148] and [149]. While the method described in [149] does not depend on the correct embedding dimension, the method in [148] does. TISEAN [150], a software package for analysis of time series with methods based on the theory of nonlinear deterministic dynamical systems, can be used to estimate maximum Lyapunov exponents based on methods described in [148] and [149] respectively. If $s_{n1}$ and $s_{n2}$ are two points in phase space with distance $s_{n1} - s_{n2} = \triangle_0 \ll 1$, distance after a time $\Delta l$ is $\delta_{\Delta l} = s_{n1+\Delta l} - s_{n2+\Delta l}$. The maximal Lyapunov exponents represents the slope of the equation defined in (3.4), where a positive value is an indication of a chaotic system and a zero slope corresponds to a possible stable system.

$$\delta\left(e,m,\tau\right) = \left\langle \ln\left(\frac{1}{\mid \upsilon_n \mid} \sum_{s_{n2} \in \upsilon_n} \mid s_{n1+\tau} - s_{n2+\tau} \mid\right)\right\rangle_n \quad , \tag{3.4}$$

where $m$ is the embedding dimension, $\tau$ is time delay, $\upsilon_n$ is the $e-neighborhood$ of $s_n$ [150].

Figure 3.3 shows an example for an input time series and its corresponding Lyapunov exponents where we can see that Lyapunov exponent exhibits a flat line which indicates possible stable behaviour.

In addition to identifying types of motion in dynamic systems, identifying determinism and linearity helps to select an appropriate method to predict system behaviour. In the next subsection, we discuss different techniques to identify the properties of determinism and linearity in dynamic systems.



(a) Sample of time series data

(b) Lyapunov exponents estimation indicating a stable system behaviour

Figure 3.3: Sample of time series data and its corresponding Lyapunov exponents indicating a stable system behaviour

### 3.2.2 Determinism and linearity

Different methods for detecting the existence of determinism and/or non-linearity in time series are available such as Kaplan's test [151] and Delay Vector Variance (DVV) [152]. Kaplan's test [151] is a technique that uses the linearised versions of the original data which is called surrogate data (or surrogate for short) to examine linearity for an input time series. DVV is a method based on the concepts of FNN and Kaplan's test [151] to examine an input data for determinism and non-linearity. DVV uses an approach for comparing the characteristics of time series based on its predictability against surrogate data. We use DVV to estimate determinism and linearity of dynamic systems.

DVV requires the proper selection of time delay and embedding dimension. The examination of determinism and non-linearity can be interpreted using a DVV plot and DVV scatter diagram respectively. The examination of determinism can be observed in a DVV plot by observing DVV plots converging to unity while non-linearity can be examined in DVV scatter by deviation from the bisector line.

For example, the corresponding DVV plot and DVV scatter diagram for the input data of Figure 3.3a are shown in Figures 3.4a and 3.4b respectively. In this example, we can see the variance converges to a value of 1 in the first diagram which indicates determinism while there is a deviation from the bisector line indicating non-linearity in the second diagram.

In this section, we have discussed the concept of phase space and shown how it can be used for modelling deterministic systems. For a purely deterministic system, all future states can be determined when its current state is known. But phase space is also useful for understanding non-deterministic systems when they are described as a set of states that specify system transitions. However, investigating dynamics of systems in phase space trajectory is a complex task particularly for an $m$-dimensional phase space trajectory (when $m \geq 3$) as shown in Figure 3.2. RPs enable users to investigate $m$-dimensional phase space trajectory using a two-dimensional representation of its recurrences. In the next section, we introduce RPs and show how to interpret their structure.

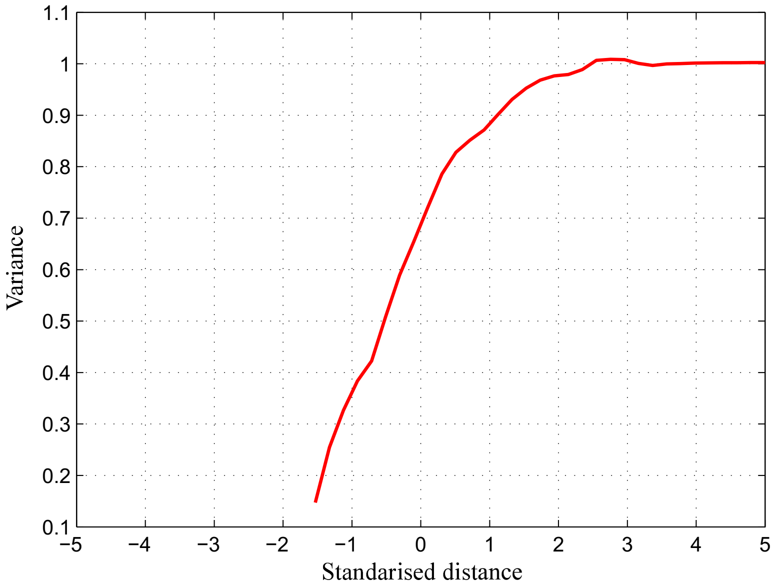
## 3.3 Recurrence plot

Recurrence Plot (RP) is an advanced nonlinear analysis technique introduced by Eckmann et al. [143]. The RP was initially produced to graphically display recurring patterns and non-stationarity in time series. RP was introduced as a tool to visualise the time-dependent behaviour of the dynamics of a system as a square matrix where each element corresponds to a point in time states. With enough data, structural patterns in the RP can reveal information about the time evolution of the phase space. RP is not limited to long data sets. It can be used for short, noisy, and non-stationary data sets [153]. RPs can be formally expressed by the matrix $R$

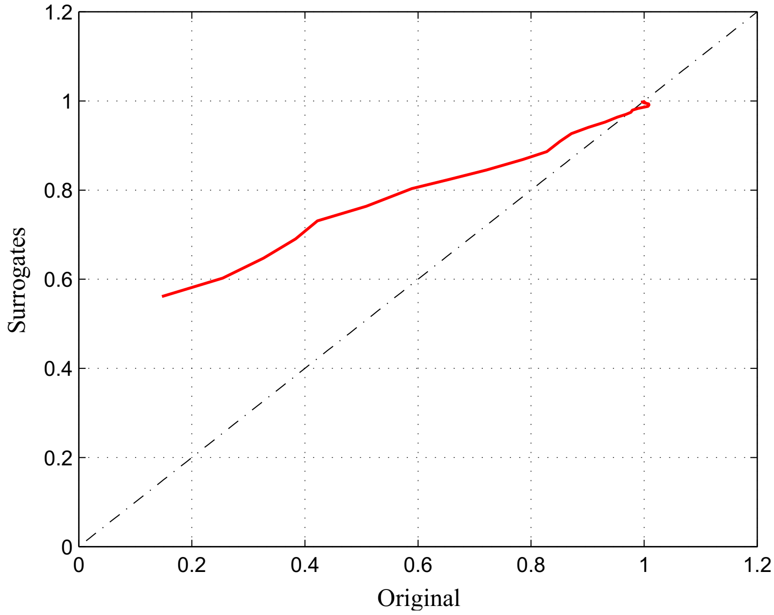
$$\mathrm{R_{i,j}}\left(\varepsilon\right) \quad = \quad \Theta\left(\varepsilon - \|\vec{x_i} - \vec{x_j}\|\right), \qquad i,j = 1,\ldots,N, \tag{3.5}$$

where $R_{i,j}$ is an element of the recurrence matrix $R$, N is the number of measure points, ε is a threshold distance, $\Theta\left(\cdot\right)$ the Heaviside function and $(\|\cdot\|)$ is a normalization operation.

To construct an RP, three parameters have to be carefully selected. These are the two used in reconstructing phase space: time delay $(\tau)$ and embedding dimension $(m)$, and a new one, the threshold $(\varepsilon)$ which refers to the distance between a pair of states in the phase plane. If a pair of states fulfils the threshold condition, their corresponding value of recurrence point is assigned with the value 1; otherwise, the pair is considered dissimilar and assigned with the value of 0. Selecting non-optimal values for RP's parameters can produce different structures for the same input data. For example, non-optimal values of embedding parameters can cause many interruptions to the Line of Identity (LOI), a black main diagonal line with an angle $\frac{\pi}{4}$ in the RP. As noted in our discussion on phase space reconstruction, time delay and embedding dimension can be estimated using the MI and FNN algorithms. 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



(a) Example of DVV plot for a deterministic system



(b) Example of DVV scatter diagram for a non-linear system

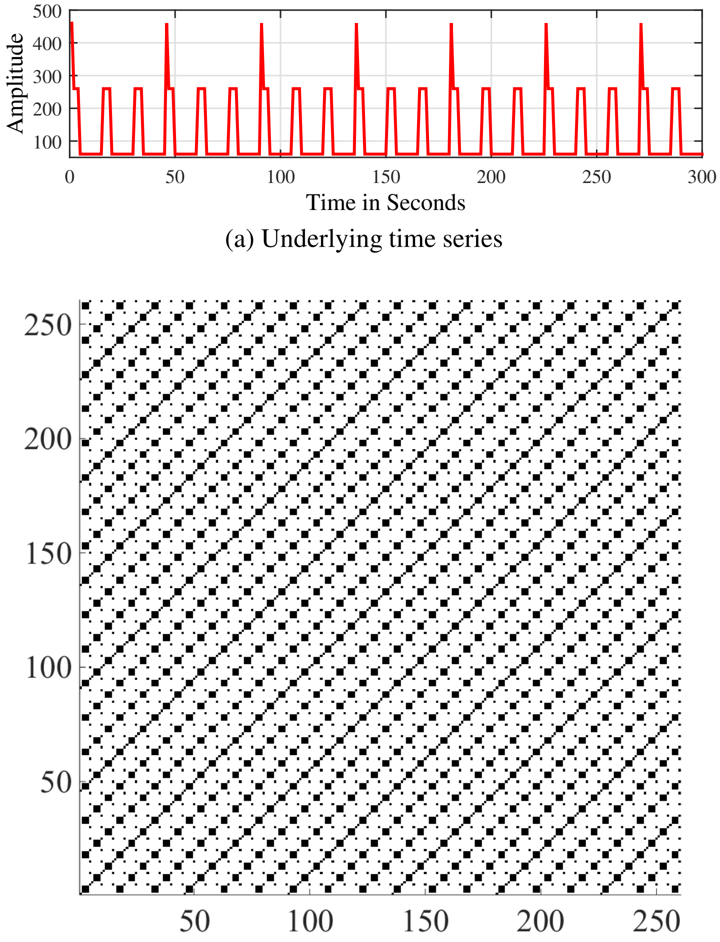
Figure 3.4: Estimation of determinism and non-linearity using DVV method

depends on the application and experiment. In classification and signal detection, for example, a good choice of the threshold ranges is 20-40% of the signal's standard deviation while a recommendation from [123] suggests that the threshold has to be selected less than 10% of the maximum phase space diameter.

From the RP structure, we can infer system characteristics from large and small scale patterns. In large scale patterns, we can infer the characteristics of a system such as whether it is periodic, homogeneous or disrupted. For example, diagonal lines are long for periodic systems and short for chaotic systems. Small scale patterns consist of a combination of isolated dots and dots that form diagonal and vertical lines. These points are structured in different forms reflecting the behaviour of the system at that time. For example, periodic patterns in the small scale structure of an RP are characteristic of a system that is cyclical with periods corresponding to the time distance between periodic structures. Single isolation points in an RP refer to heavy fluctuations. Diagonal lines which are parallel to the LOI indicate a deterministic process while lines that are orthogonal to LOI indicate to the evolution of a system states is similar but they move in the opposite time direction. An example of a periodic time series data and its corresponding RP representation are shown in Figure 3.5. The most striking feature in Figure 3.5b is the long diagonal lines structures parallel to LOI identifying the characteristics of deterministic and periodic behaviour. In this example, we can see two types of diagonal lines. The discontinuous lines related to the amplitude values of 260 with periodicity of 15 seconds and continuous diagonal lines related to the amplitude of 460 with periodicity of 45 seconds.

Changing values of amplitude are reflected in the structure of RP. For example, modifying the amplitude of time 46 seconds from 460 to 5500 shows a notable change in the structure of RP as shown in Figure 3.6. The RP in Figure 3.6 shows a small banding disruption causing discontinues for the diagonal lines which refers to some states that are rare or that some transitions may have occurred. In this case, it refers to a transition state resulting from a large amplitude at time 46 seconds. RP can indicate the time of this transition. In addition to detecting amplitude change, the RP also shows a notable change when there is a change in the signal periodicity. For example, when the value of 460 occurs at times 44, 45, and 46 seconds instead of only 46 seconds the RP shows a noteworthy alteration in its structure as depicted in Figure 3.7. Although it is quite difficult to distinguish periodicity changes in the underlying time series shown in Figure 3.7a, it is obvious to distinguish it in RP as shown in Figure 3.7b where the diagonal lines discontinuous indicate periodicity change.

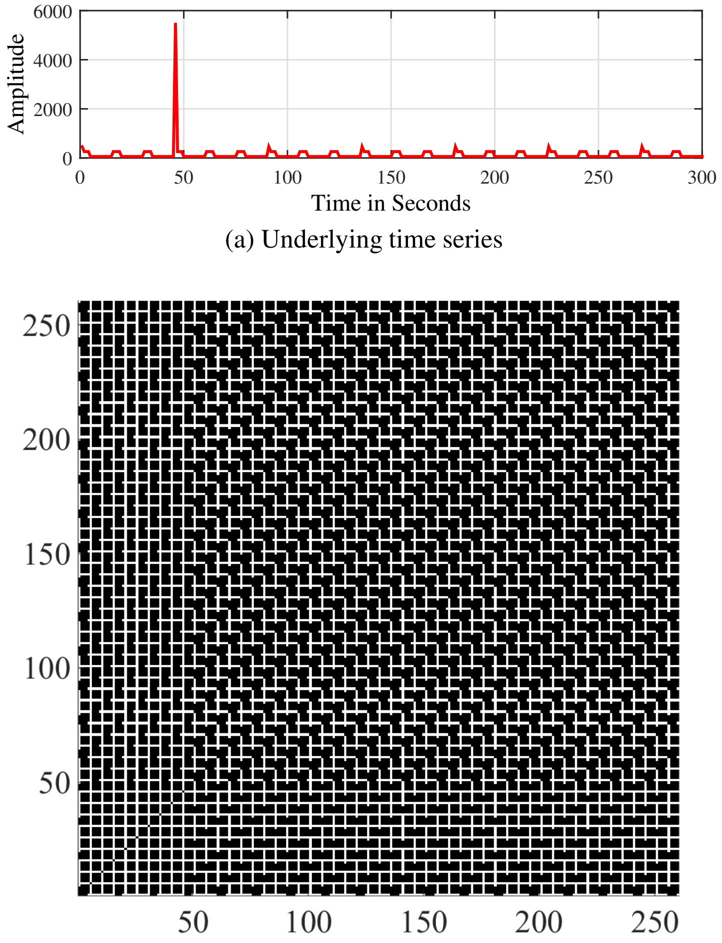
However, interpreting an RP requires a high level of experience especially for complex data. To reduce the difficulty of RP interpretation, RQA has been introduced. In addition,



(a) Underlying time series

(b) RP with time $\tau$ =5 and $m$=9

Figure 3.5: An Example of RP to identify periodicity in the underlying time series

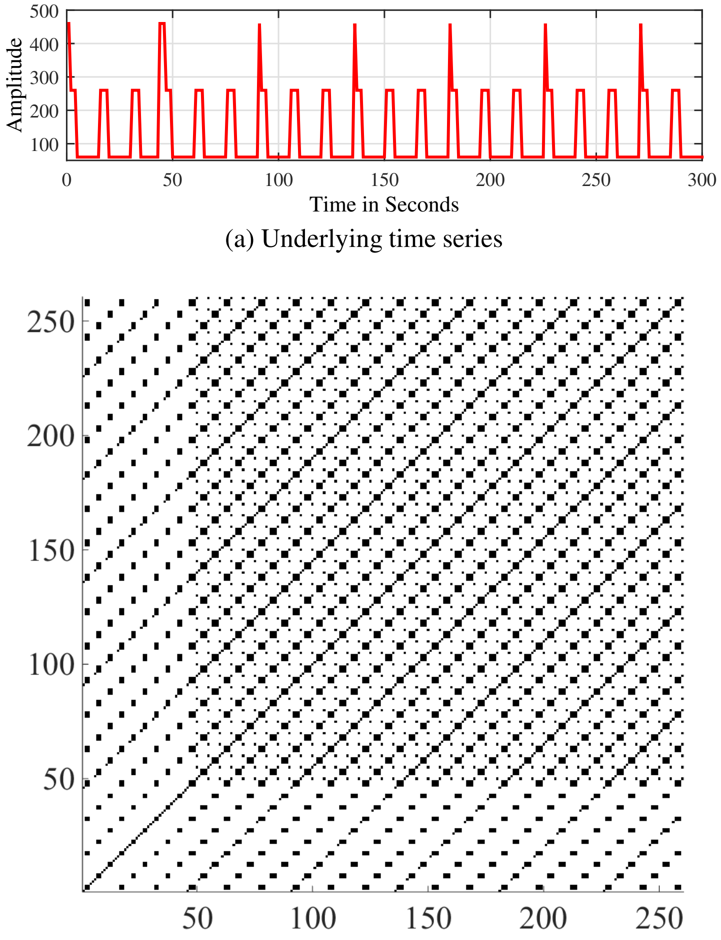


(a) Underlying time series

(b) RP with $\tau$ =5 and $m$=9

Figure 3.6: An example of RP to detect a high amplitude transition in the input data

RP cannot be directly used for automated detection of system behaviour changes or real-time anomaly detection. In the next section, we discuss RQA in detail.



(a) Underlying time series

(b) Recurrence plot with $\tau$ =5 and $m$=9

Figure 3.7: An example of RP to detect periodicity changes

## 3.4 Recurrence quantification analysis

Recurrence Quantification Analysis (RQA) was introduced by Zbilut and Webber [154] to provide several measures of complexity which quantify the small scale structures in RPs. These measurements are called RQA measurements. They introduced five measurements based on diagonal line structure of RPs including Recurrence Rate (RR), Determinism (DET), and the Shannon entropy (ENT) of the frequency distribution of the LOI. These RQA measurements are mainly based on the number, lengths and distribution of the diagonal lines in RPs. However, additional measurements have been presented by Marwan et al. [153]. These additional measurements are mainly based on both vertical and horizontal elements in RPs. In total, there are eight well-known RQA measurements. These measurements can be classified into three types: based on the recurrence density, based on diagonal lines, and measurements based on vertical lines. Now, we discuss the eight most useful measurements in more detail.

Recurrence Rate (RR) refers to the probability that a system recurs after a number of time states. RR is based on the recurrence density in the RP. It measures the density of recurrence points in the RP which simply counts the number of black dots in the RP excluding the LOI. RR can be calculated as

$$RR = \frac{1}{N^2} \sum_{i,j=1}^{N} R_{i,j}, \tag{3.6}$$

where $R_{i,j}$ is an element of the recurrence matrix $R$.

Determinism (DET) can be interpreted as the predictability of a system. DET is a measure based on diagonal lines of the RP. The length of the diagonal lines differ from one system to another. They are long for periodic signals, short for chaotic signals, and absent for stochastic signals. DET can be calculated as the ratio of recurrence points that form diagonal structures to all recurrence points.

$$DET = \frac{\sum_{l=lmin}^{N} lP(l)}{\sum_{i,j}^{N} R_{i,j}}, \tag{3.7}$$

where $lmin$ is a threshold which excludes the diagonal lines formed by the tangential motion of the phase space trajectory, $lmin$ is typically set to two. Setting $lmin$ to one will result in DET and RR being identical. $P(l)$ is the histogram of the lengths $l$ of the diagonal lines [123].

Laminarity (LAM) is a measure of whether the system is in a stable state or if it is transitioning from one state to another. LAM refers to the percentage of recurrence points which form vertical lines in the RP. LAM can be calculated as

$$LAM = \frac{\sum_{v=vmin}^{N} vP(v)}{\sum_{v=1}^{N} vP(v)}, \tag{3.8}$$

where $P(v)$ is the histogram of the lengths $v$ of the vertical lines and the typical value for $vmin$ is set to two.

Trapping Time (TT) can be used to measure how long the system remains in a specific state. It contains information about the vertical structures in the RP. The computation of TT uses the minimal length $vmin$ as in Theorem 3.8 [123].

$$TT = \frac{\sum_{v=vmin}^{N} vP(v)}{\sum_{v=vmin}^{N} P(v)} \tag{3.9}$$

T2 is a measure of time taken to move from one state to another. It is the mean of transit time between stable states. For example, T2 can be used to estimate periodicity for a periodic signal. It represents the average lengths of the white vertical lines in the RP. T2 can be calculated as

$$T_j^2 = |\left\{i,j : \vec{x}_i,\vec{x}_j \in \mathscr{R}_i ; \vec{x}_{j-1} \notin \mathscr{R}_i\right\}|. \tag{3.10}$$

Entropy (ENTR) can be used to measure system's predictability. For example, the value of ENTR is small for uncorrelated data. It is the Shannon entropy of the frequency distribution of the diagonal line lengths. ENTR reflects RP complexity in term of the diagonal lines. ENTR can be calculated as

$$ENTR = \sum_{l=lmin}^{N} p(l) ln\, p(l). \tag{3.11}$$

This measurement has been extended to L-entr, W-entr, and V-entr that refer to entropy of diagonal line length distribution, entropy of the distribution of line lengths, and entropy of vertical line length distribution respectively.

L-MAX is a RQA measurement that is based on diagonal lines of the RP. L-MAX refers to the longest diagonal line found in the RP which can be calculated as

$$L - MAX = max\left(\{l_i; i = 1\} ...N_l\right). \tag{3.12}$$

L-MEAN is the average diagonal line length in the RP which represents the mean prediction time. It is the average time that two segments of the trajectory are close to each other. L-MEAN is calculated as

$$L - MEAN = \frac{\sum_{l=lmin}^{N} lP(l)}{\sum_{l=lmin}^{N} P(l)}. \tag{3.13}$$

To provide a better understanding of RQA measurements, we show how RQA measurements change based on changes of the input data. Doing this enables us to identify the most suitable RQA measurements for detecting system transitions. In particular, what are the most-significant RQA measurements for detection anomalous behaviour in the input data? For example, which RQA measurements change when there is a small change in the input data and which RQA measurements change when there is a large change in the input data?

## 3.5 Effect of amplitude and periodicity changes on RQA measurements

In this section, we demonstrate the effect of changes in amplitude and periodicity within a time series on RQA measurements. We first change amplitude, then periodicity then both and show how RQA measurements are affected. For all cases, we use an input signal with a periodicity equal to 31 seconds and the amplitude value of 10 as an illustrative example. The values of amplitude and periodicity have been chosen to reflect the average value of BGP updates per second and periodicity respectively. For example, the average value of the total number of BGP updates per second during the period 19th to 25th of July 2016 is 10 updates per second. Further discussion about analysing BGP traffic during this period will be covered later in Section 4.3. The value of 31 seconds has been chosen based on the MRAI timer, the default value of MRAI in Cisco routers is 28-32 seconds. The input data and its corresponding RQA measurements are shown in Figure 3.8 where all RQA measurements show similar behaviour over time. Second, we show the effect of changing behaviour for a non-periodic input data but which has the characteristic of recurrence and show the effectiveness of RQA measurements in detecting recurrence changes. In all our calculation of RQA measurements, RQA measurements are calculated every second using the past 300 seconds of data as a window size[2].

### 3.5.1 Changing amplitude

In this subsection, we investigate the effect of changing the amplitude of the input data on RQA measurements. RQA measurements show different behaviour based on changing the value of the amplitude. For example, in Figure 3.9 when we change the amplitude at time 992 seconds from 10 to 20, a notable change in values of L-MAX and W-entr measurements can be seen. The value of L-MAX measurement starts to decrease after one second and this change continues during the window size (300 seconds).

We continue changing the value of the amplitude at time 992 seconds by increasing its value 10 as a step (20, 30, ..., 260) and note that many extra RQA measurements (in addition to L-MAX and W-entr) start to change. Figure 3.10 shows RQA measurements when the amplitude is 260 where we can see that the values of RQA measurements W-entr, V-entr, and T2 drop to zero after one second of the significant change in the amplitude. This behaviour can be used to identify different levels of amplitude change. This change can visually be identified

[2] The window size has the effect on the values of FP and FN as well as its effect to avoid missing the detection of multiple anomalies within a short time. Further investigation for the effect of the window size will be covered in chapter 5.

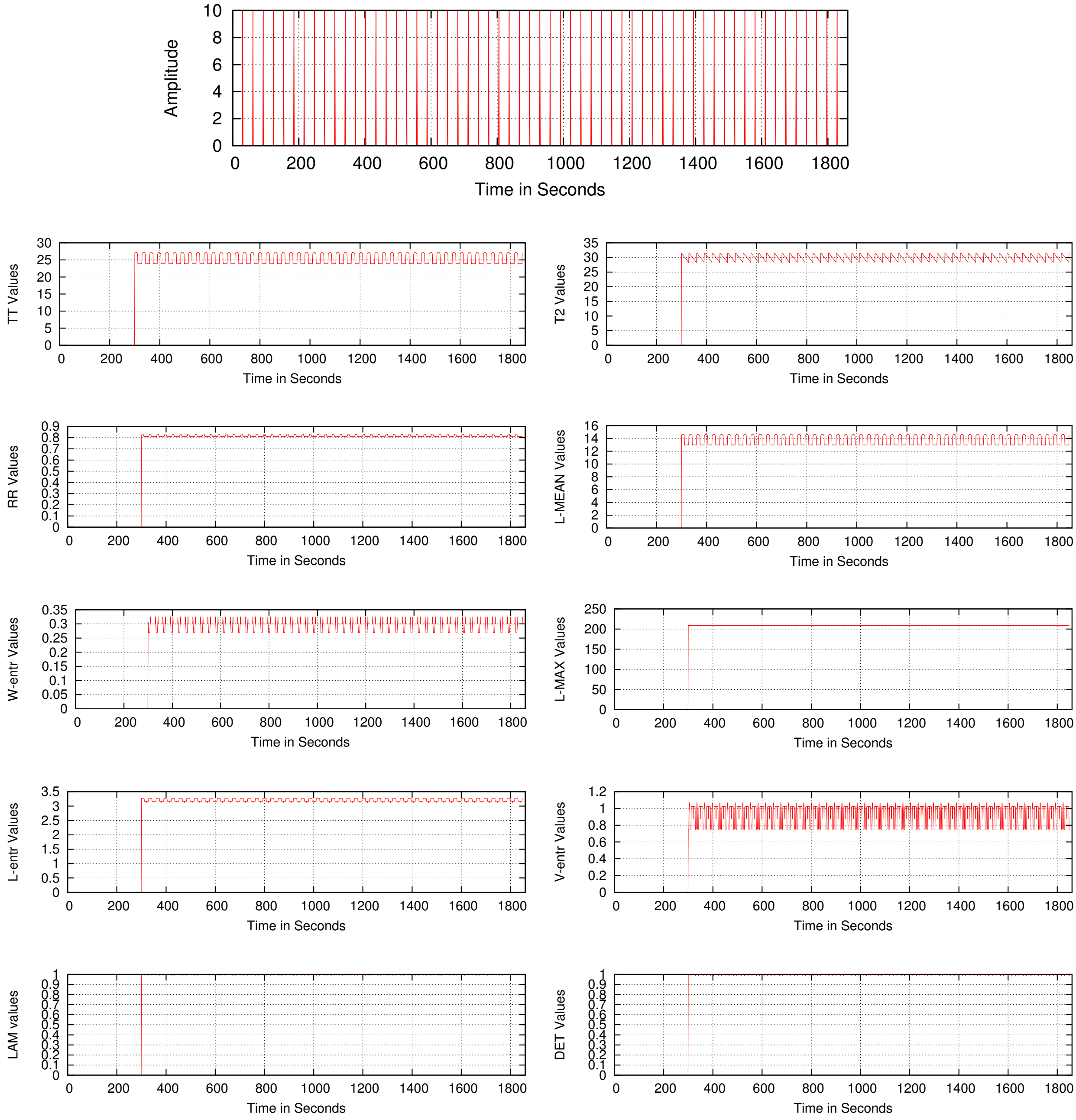


Figure 3.8: An example of periodic time series input data and its corresponding RQA measurements

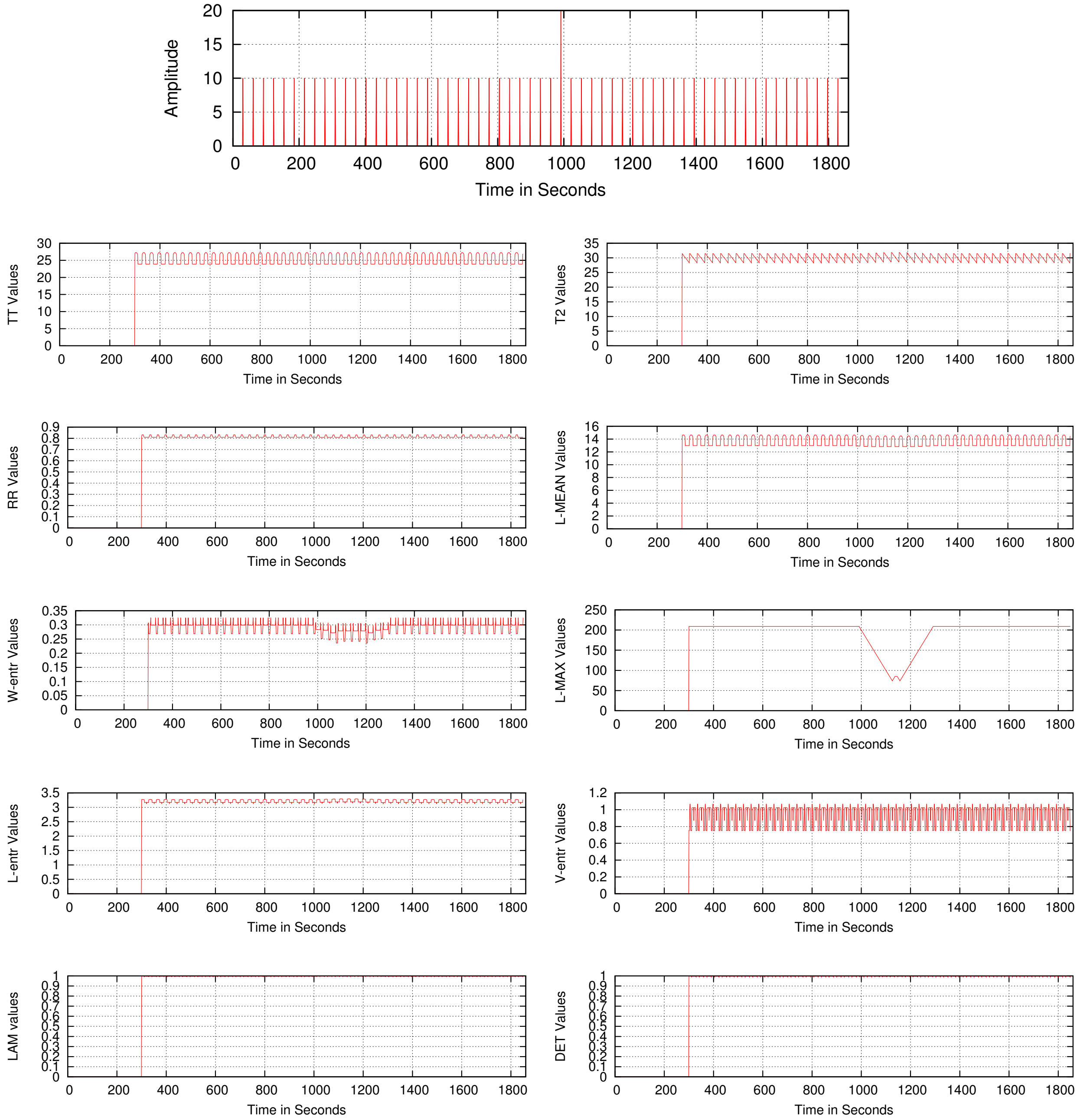


Figure 3.9: The effect of changing the amplitude at time 992 seconds from 10 to 20 on RQA measurements

Table 3.1: Summary for the effect of increasing the amplitude on RQA measurements

| Amplitude | TT | T2 | RR | DET | L-entr | W-entr | V-entr | L-MEAN | L-MAX | LAM |
|---|---|---|---|---|---|---|---|---|---|---|
| 20 | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ |
| 60 | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ |
| 100 | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ |
| 140 | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ |
| 180 | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| 200 | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| 260 | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |

using phase space representation and RP (as discussed before and shown in Figure 3.6) and qualitatively identified using RQA.

Table 3.1 shows a summary of the effect of increasing the value of amplitude on RQA measurements. RQA measurements show different behaviours in response to amplitude changes. For example, W-entr and L-MAX show a notable change when there are small or large changes in the amplitude. On the other hand, RQA measurements such as TT and T2 can detect only large changes in the amplitude, when the amplitude jumps to >17 times relative to the long term average (change from 10 to 170). However, the effect of amplitude change on RQA measurements shows that LAM and DET do not show a notable change in response to amplitude changes.

We also investigate RQA measurements when the amplitude decreases instead of increases. Figure 3.11 shows RQA measurements when the amplitude decreases from 260 to 10. Although the TT measurement shows a notable change when there is a large increase in the amplitude of the input data, it does not show any changes to reflect a corresponding decrease in the amplitude. Table 3.2 shows a summary of the effect of decreasing the amplitude values on the RQA measurements. Once again, W-entr and L-MAX respond to a high and a small decrease in the amplitude while LAM and DET do not respond to amplitude decrease.

In a summary, we can classify RQA measurements based on their response to amplitude changes of the input data into four categories. First, RQA measurements that are not able to detect amplitude changes are LAM and DET. Second, RQA measurements that are able to detect a small increase/decrease in the amplitudes change are L-MAX and W-entr. W-entr is also able to detect different levels of amplitude change as shown in Figure 3.10 which can be used to measure fluctuations of the amplitude of the input data. Third, RQA measurements that are able to detect amplitude spikes are TT, L-MEAN, and L-entr. Finally, RQA measurements T2, RR, V-entr are able to detect spikes and dips in the amplitude.

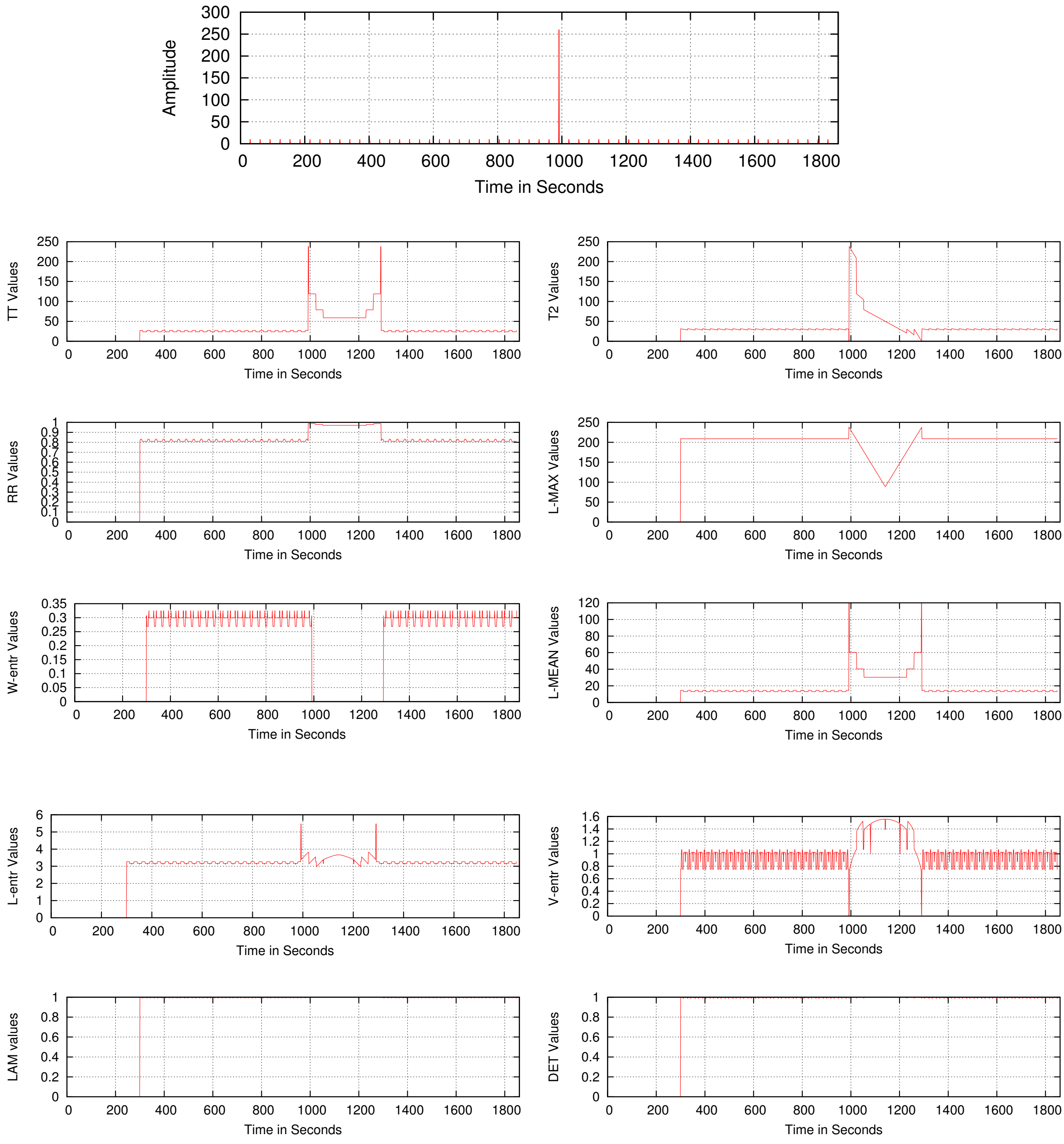


Figure 3.10: The effect of changing the amplitude at time 992 seconds from 10 to 260 on RQA measurements

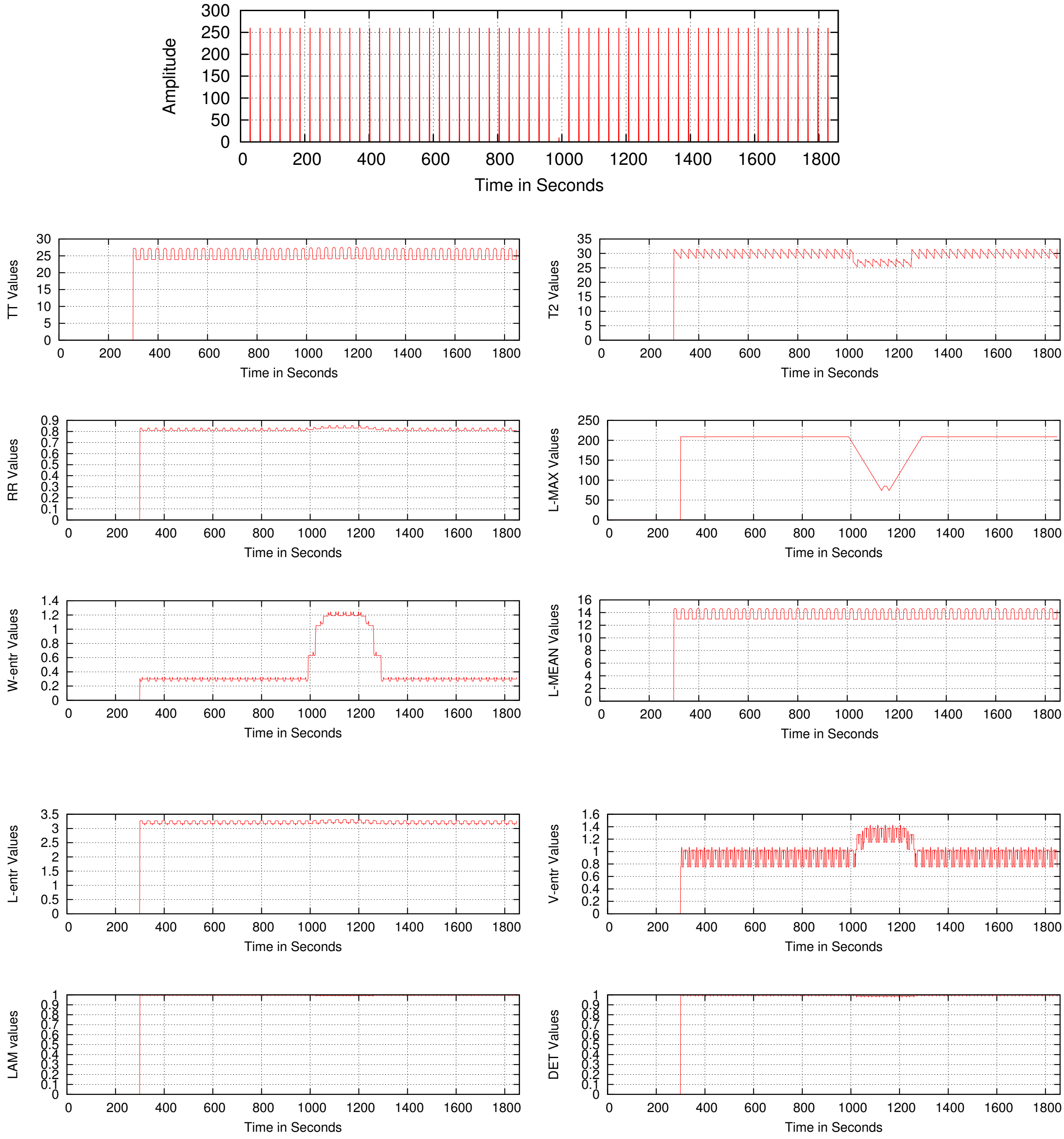


Figure 3.11: The effect of changing the amplitude at time 992 seconds from 260 to 10 on RQA measurements

Table 3.2: Summary for the effect of decreasing the amplitude on RQA measurements

| Amplitude | TT | T2 | RR | DET | L-entr | W-entr | V-entr | L-MEAN | L-MAX | LAM |
|---|---|---|---|---|---|---|---|---|---|---|
| 240 | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ |
| 200 | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ |
| 160 | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ |
| 120 | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ |
| 80 | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ |
| 40 | ✗ | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ | ✗ | ✓ | ✗ |
| 10 | ✗ | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ | ✗ | ✓ | ✗ |

### 3.5.2 Changing periodicity

We now demonstrate the effect of changing periodicity on RQA measurements. In this analysis, we phase shift the signal at time 930 by ±10 seconds as an illustrative example to investigate the effect of periodicity shift on RQA measurements. In other words, we shift the time that we should see the amplitude at 930 seconds by ±10 seconds to see different cases from 920-940 seconds. We see a notable change in the values of RQA measurements of TT, T2, entropy measurements, L-MAX, and L-MEAN. However, other RQA measurements DET and LAM do not show a notable change in term of periodicity shift; therefore, we eliminate these two RQA measurements in our figures. Figure 3.12 shows the effect of shifting the periodicity with value -2 seconds (the amplitude occurs at time 928 seconds instead of 930 seconds) on RQA measurements while Figure 3.13 shows the effect of shifting the periodicity +10 seconds (the amplitude occurs at time 940 seconds instead of 930 seconds) on RQA measurements. In these two figures, RQA measurements respond to phase shift with different values. For example, the value of TT is 21.42 when the phase shift is -2 seconds and 17.83 when the phase shift is +10 seconds. Table 3.3 shows a summary of RQA measurements in term of periodicity shift.

We also show the effect of higher frequency impulses superimposed on a lower frequency signal. In Figure 3.14, there are seven consecutive amplitudes around time 929 seconds. This figure describes a system that changes its behaviour of sending an output every 31 seconds to seven consecutive outputs every one second during the period 926-932 seconds. Figure 3.14 and Figure 3.15 show changing RQA measurements when seven and nine consecutive amplitudes (three and four extra amplitudes on each side) around time 929 seconds respectively. As a result of changing the behaviour of the input data around the time 929 seconds, RQA measurements TT, RR, and V-entr show a change in their value during this period. However,

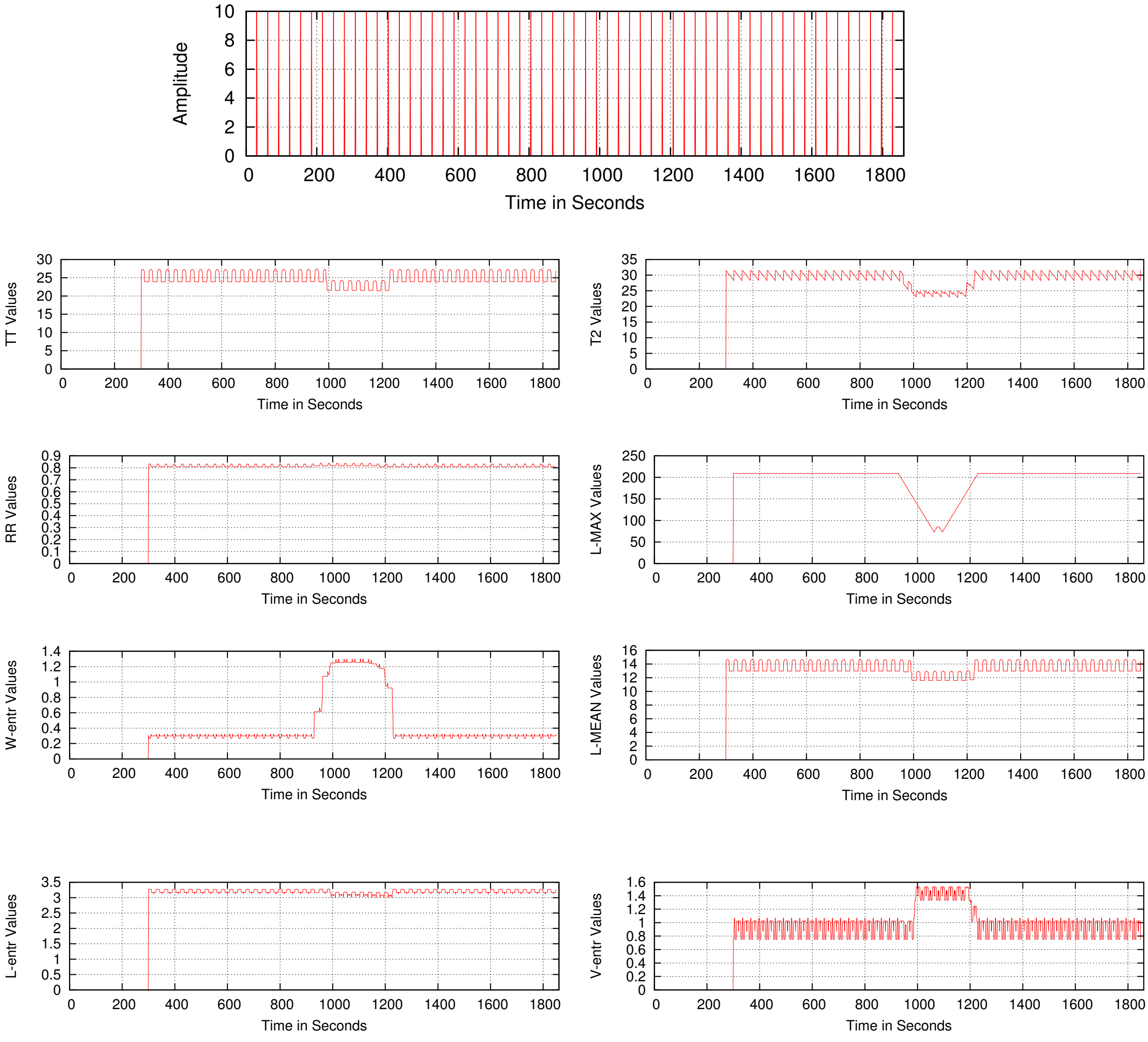


Figure 3.12: The effect of phase shift -2 seconds on RQA measurements

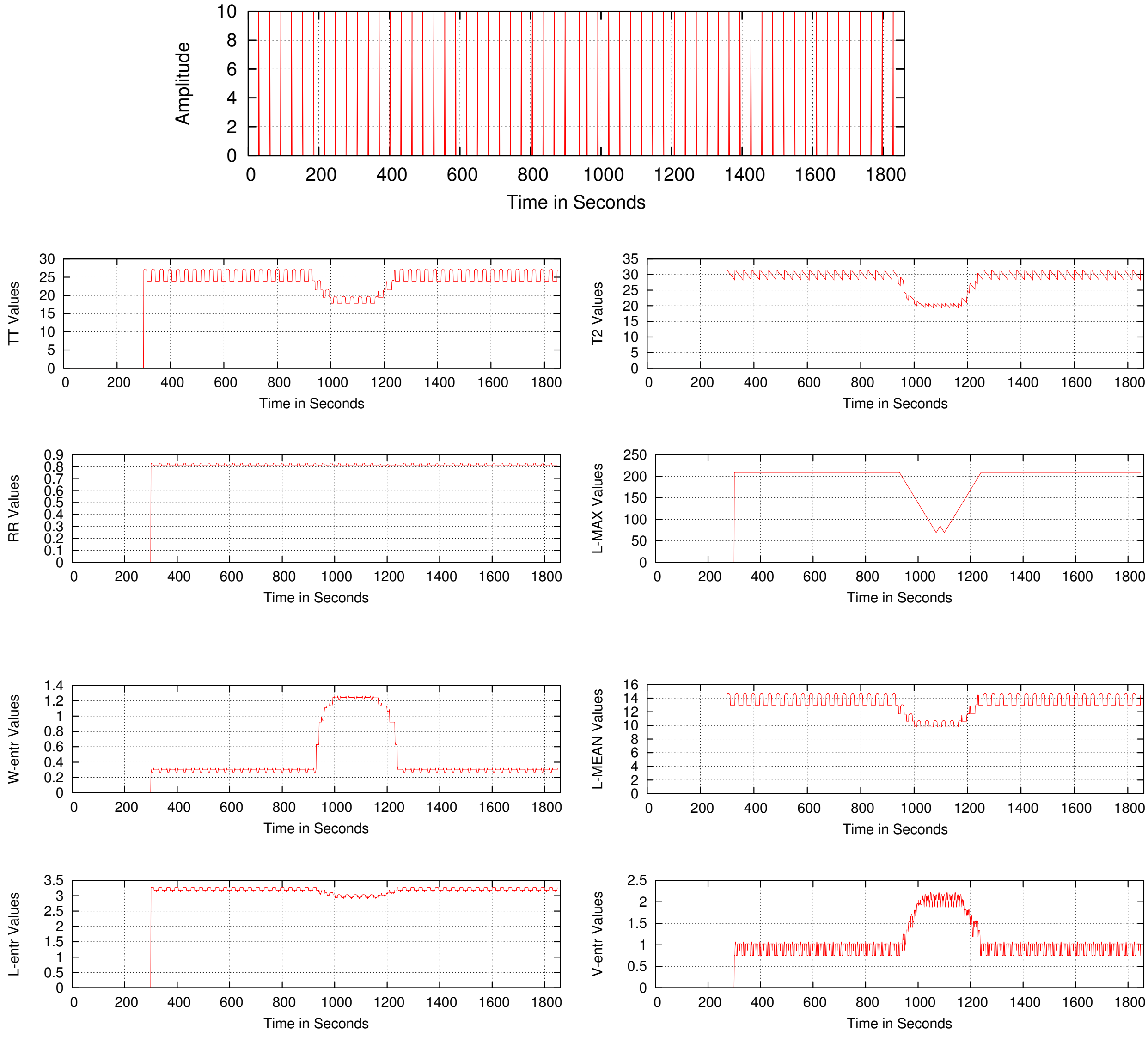


Figure 3.13: The effect of phase shifts +10 seconds on RQA measurements

Table 3.3: Summary for the effect of phase shifts on RQA measurements

| Amplitude | TT | T2 | RR | DET | L-entr | W-entr | V-entr | L-MEAN | L-MAX | LAM |
|---|---|---|---|---|---|---|---|---|---|---|
| 920 | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| 923 | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| 925 | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| 927 | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| 929 | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✓ | ✗ | ✓ | ✗ |
| 930 | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| 933 | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| 937 | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| 940 | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |

among all RQA measurements, a significant change in RR values can be used as an identifier to detect periodicity changes. The minimum value of RR measurements occurs after 61 seconds of last amplitude in the abnormal behaviour for the above three cases. In the next subsection, we investigate the effect of changing both the amplitude and periodicity for the periodic input data on RQA measurements.

### 3.5.3 Changing amplitude and periodicity

In this subsection, we show the effect of changing both the amplitude and periodicity on RQA measurements. Figure 3.16 shows RQA measurements when there are 8 consecutive amplitudes of value 20 around time 929 seconds. The effect of this change is similar to the periodicity change shown in Figure 3.15 where there are seven consecutive amplitudes of value 10. In other words, small changes in amplitude with large change in periodicity has an effect demonstrated by the periodicity change.

By comparison, this behaviour changes when we have a large amplitude change. For example, Figure 3.17 shows the effect of changing the behaviour of the input data when 8 consecutive amplitudes of value 260 occur around time 929 seconds. Here, we can see the behaviour of RQA measurements TT, T2, and L-MEAN is similar to the effect of changing the amplitude only to 260. However, RQA measurements RR and W-entr show different behaviour when there is only change in the amplitude or periodicity and when there are changes in both the amplitude and periodicity. For example, there is a single change in the amplitude or periodicity and when there is a change in both amplitude and periodicity. For example, the value of W-entr when only the amplitude value changed (Figure 3.10) is dropped to zero, increased to 1.19 (Figure 3.14) when only the periodicity change, and increased to 0.92 when both the amplitude and periodicity change (Figure 3.16).

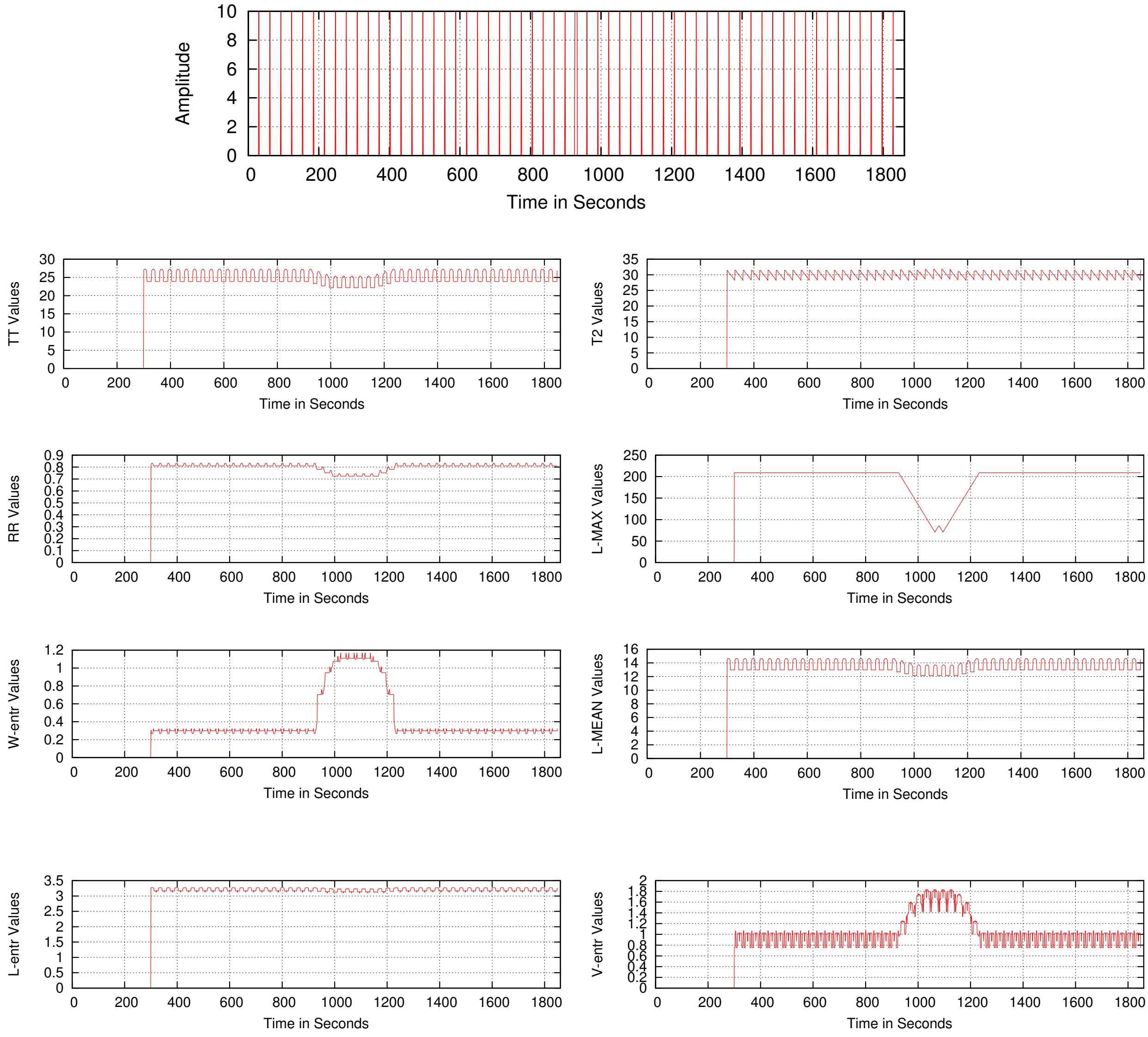


Figure 3.14: The effect of occurring seven consecutive amplitudes around time 929 seconds on RQA measurements

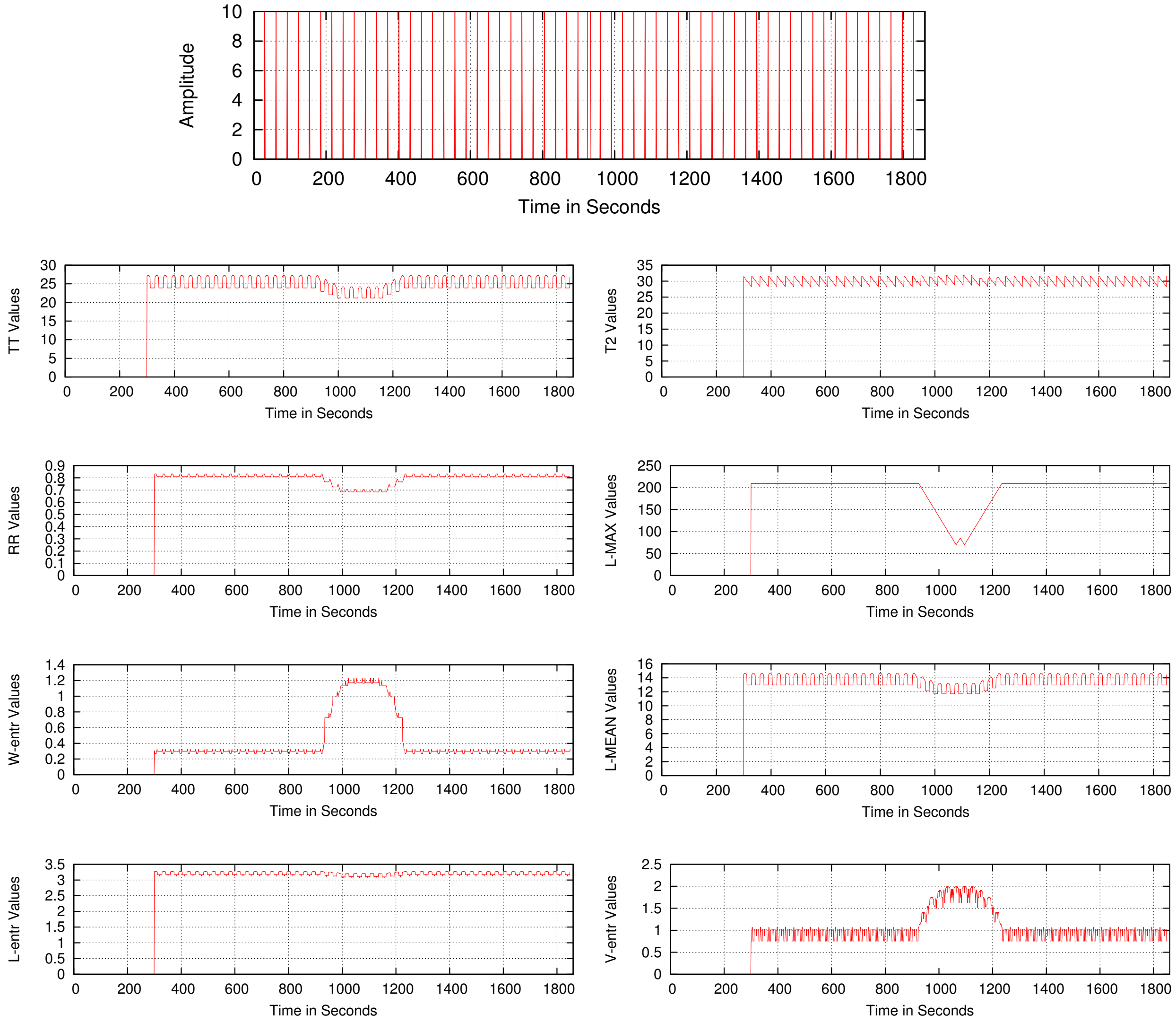


Figure 3.15: The effect of occurring nine consecutive amplitudes around time 929 seconds on RQA measurements

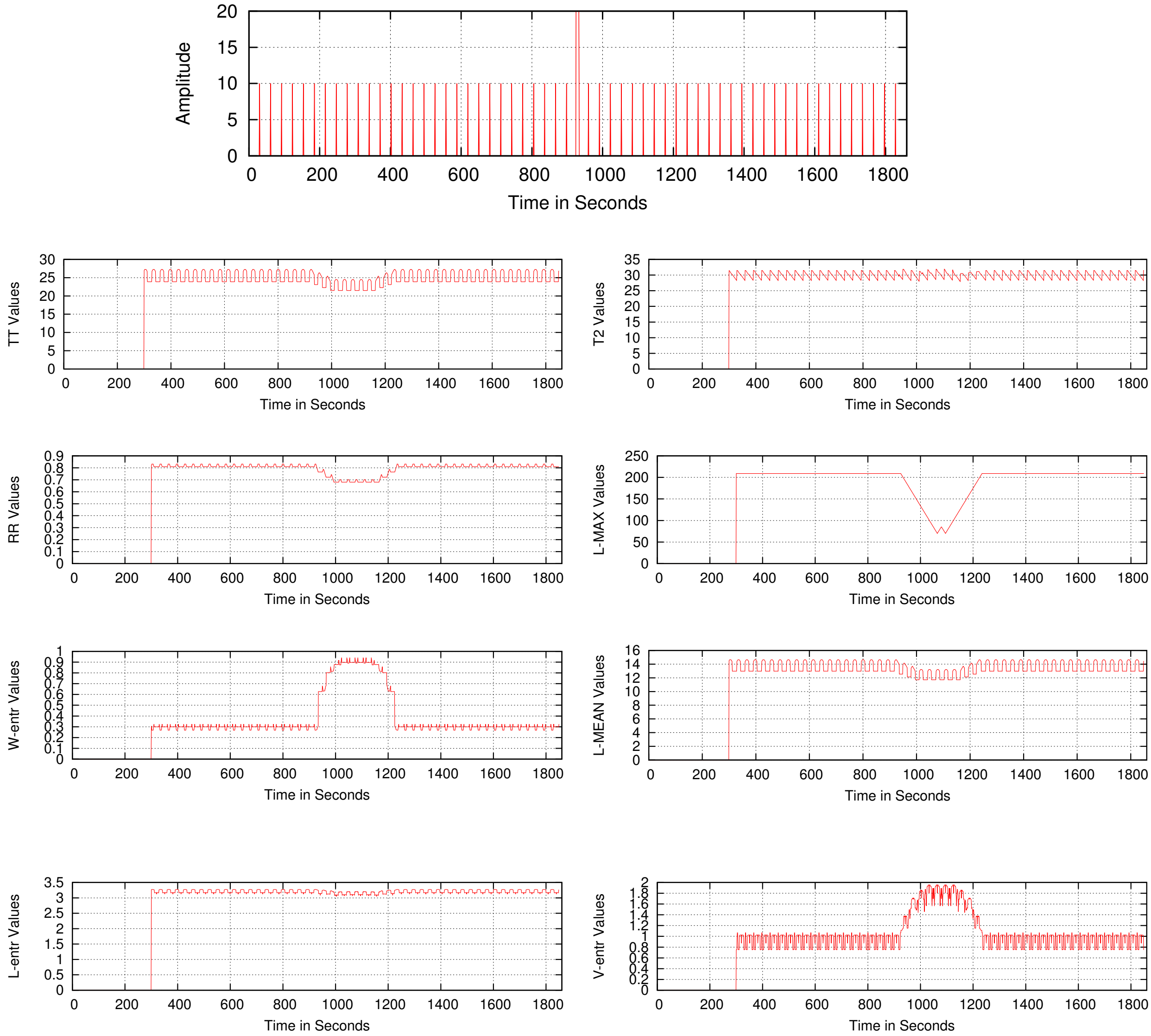


Figure 3.16: The effect of occurring seven consecutive amplitudes of value 20 RQA measurements around time 929 seconds

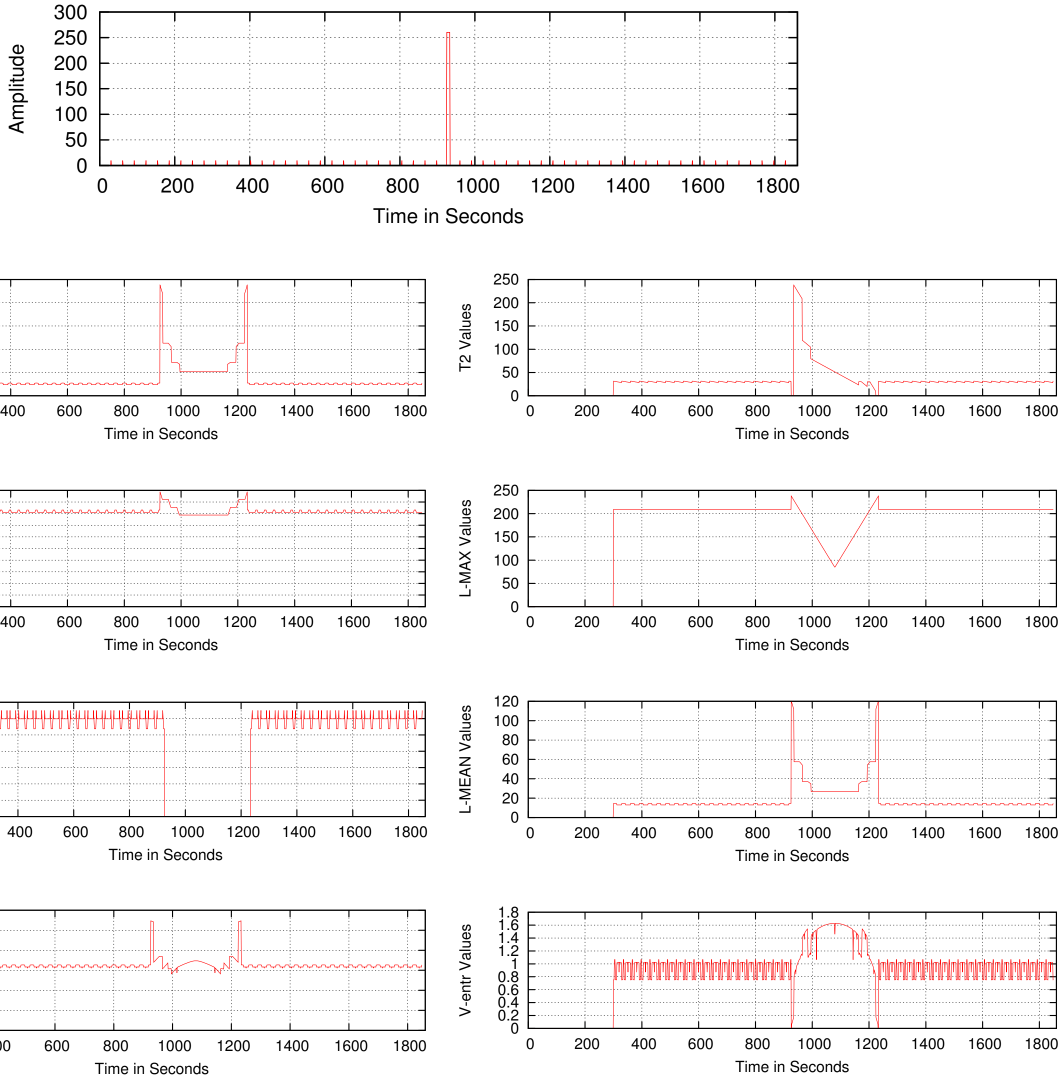


Figure 3.17: The effect of occurring seven consecutive amplitudes of value 260 RQA measurements around time 929 seconds

### 3.5.4 Changing recurrence behaviour

In the previous subsections, we have investigated the impact on RQA measurements of changing amplitude and/or periodicity for a simple periodic time series input. In this subsection, we show the impact of changing recurrence patterns for a recurrent data sequence on RQA measurements. Figure 3.18 shows an example of a recurrent input that exhibit changing of values 1,2,3, and 4 in such a way that recurs over time and its corresponding values of RQA measurements. As before the calculation of RQA measurements is calculated every second based on using the past 300 seconds of data as a window size. The values of RQA measurements do not show a large change during the period of the input data. However, changing the value of amplitude during the period 1012-1017 seconds from 1 to 10 causes many RQA measurements such as TT and T2 to change reflecting the change in the input data as shown in Figure 3.19.

So far, we have demonstrated the ability of RQA to identify changes in behaviour where the change is readily apparent in the underlying time series. Now, we show the power of RQA in identifying changes that are not readily apparent from simple observation of the time series. In this example, we change the recurrent behaviour of data during the period 1040-1060 seconds where we expect to see values of 1 instead of 3 as a recurrent behaviour reflecting on multiple RQA measurements during this period. As shown in Figure 3.20, we see that RR and W-entr respond quickly during the period 1022-1372 seconds. RR values dropped from the range 0.6-0.65 to 0.54-.065 while W-entr increased from the range 1.8-2 to 1.8-2.4 during the period 1022-1372 seconds. This ability to detect recurrence changes is a powerful tool in detecting anomalous behaviour change in deterministic systems using only a short past window of data, 300 seconds in this case.

To summarise our experimental analysis of the effect of changing amplitude and/or periodicity for the input data as well as changes in recurrence behaviour on RQA measurements RQA measurements show different behaviour for the input data changes as follows:

DET and LAM do not show a notable change for amplitude and/or periodicity changes.

RR shows a decrease in value when there is a change in system recurrence behaviour. For example, there is a significant change in RR values when there is a change in periodicity (Figure 3.15) or when there is a change in recurrence patterns for an input data (Figure 3.20). The minimum value of RR measurements occurs after 61 seconds of the last amplitude when there is a change in periodicity or recurrence patterns. However, RR shows a notable increase when a large amplitude change occurs.

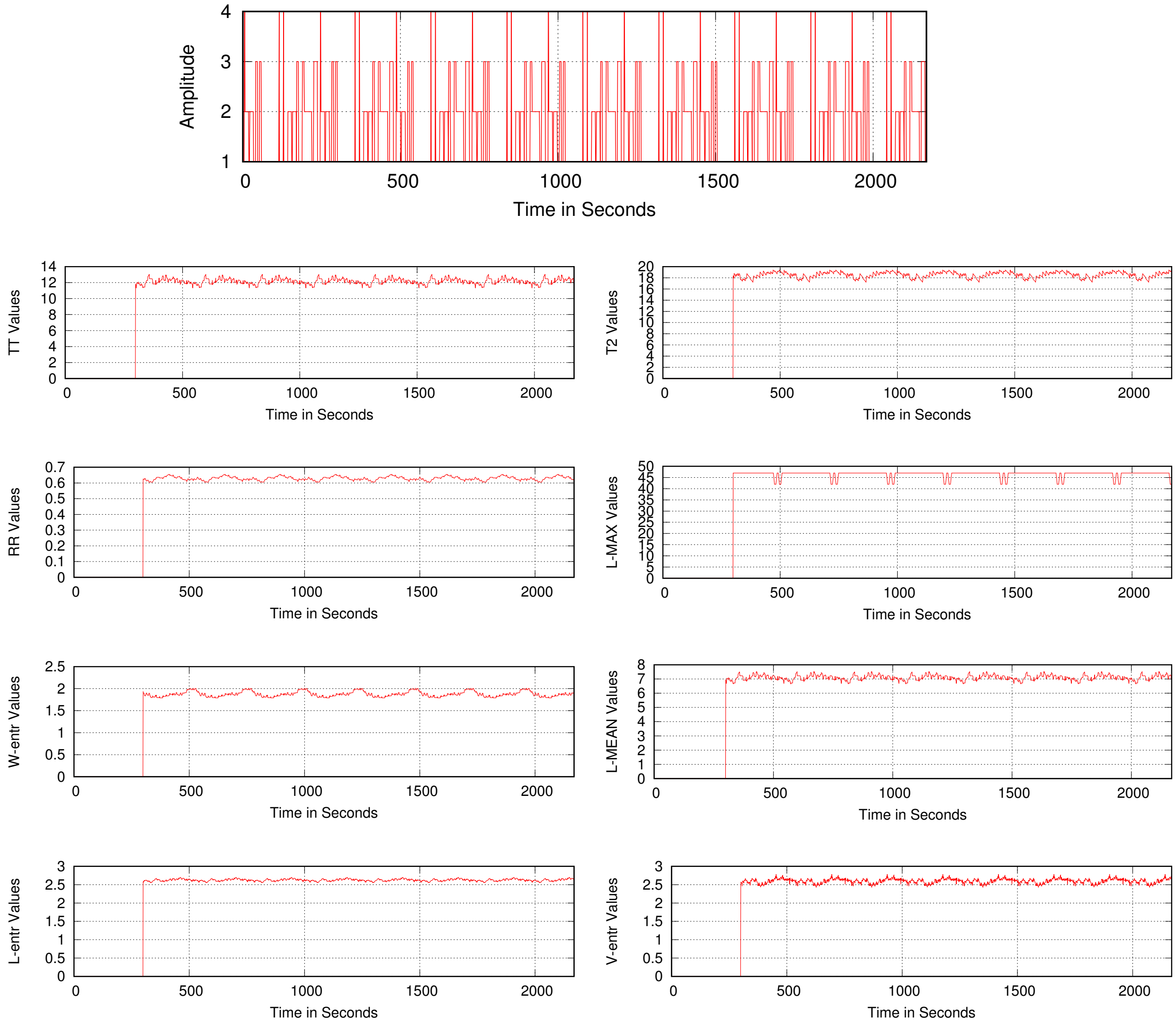


Figure 3.18: An example of a recurrent data and its corresponding RQA measurements

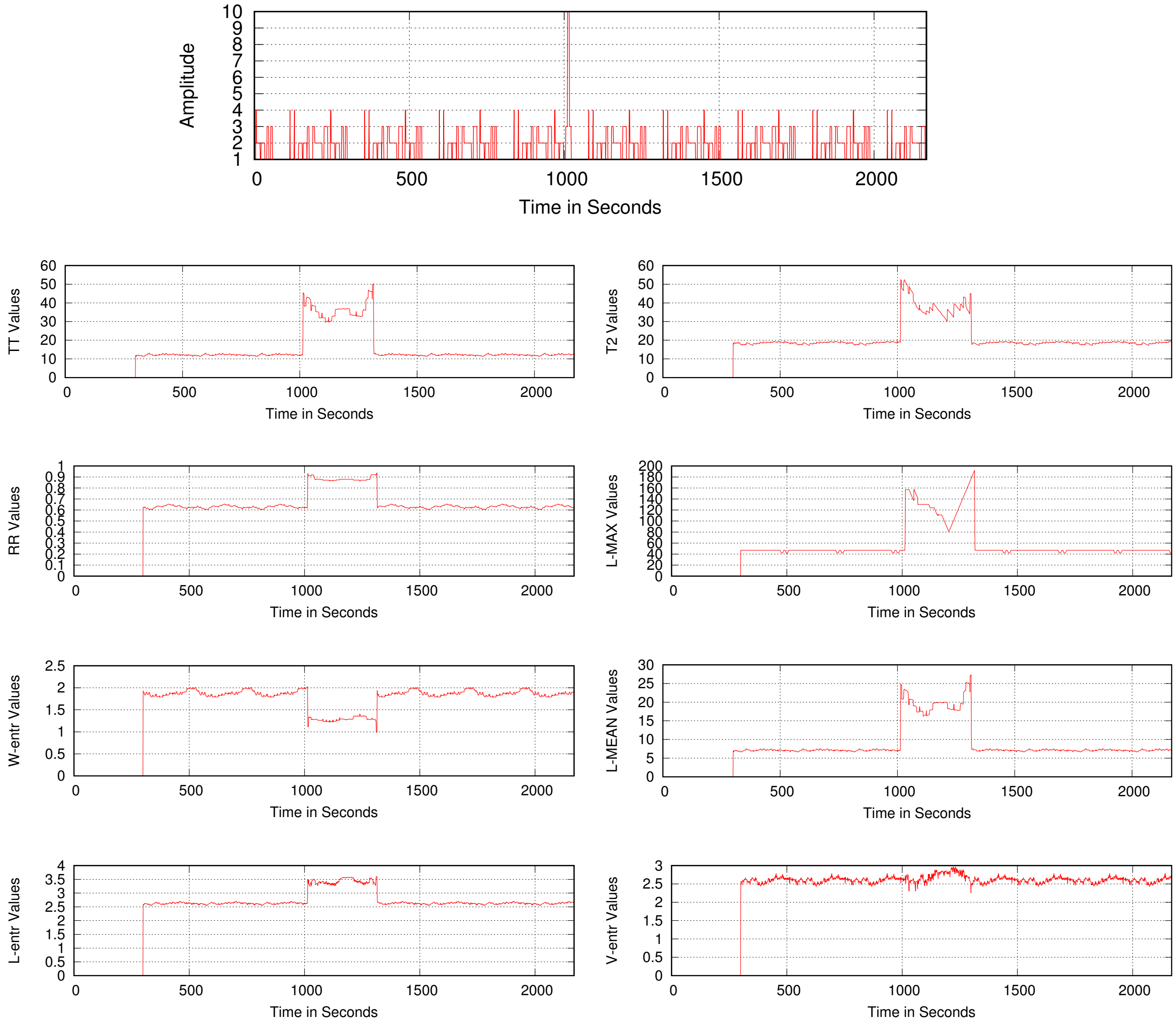


Figure 3.19: The effect of changing the amplitude from 1 to 10 during the period 1012-1017 seconds on RQA measurements

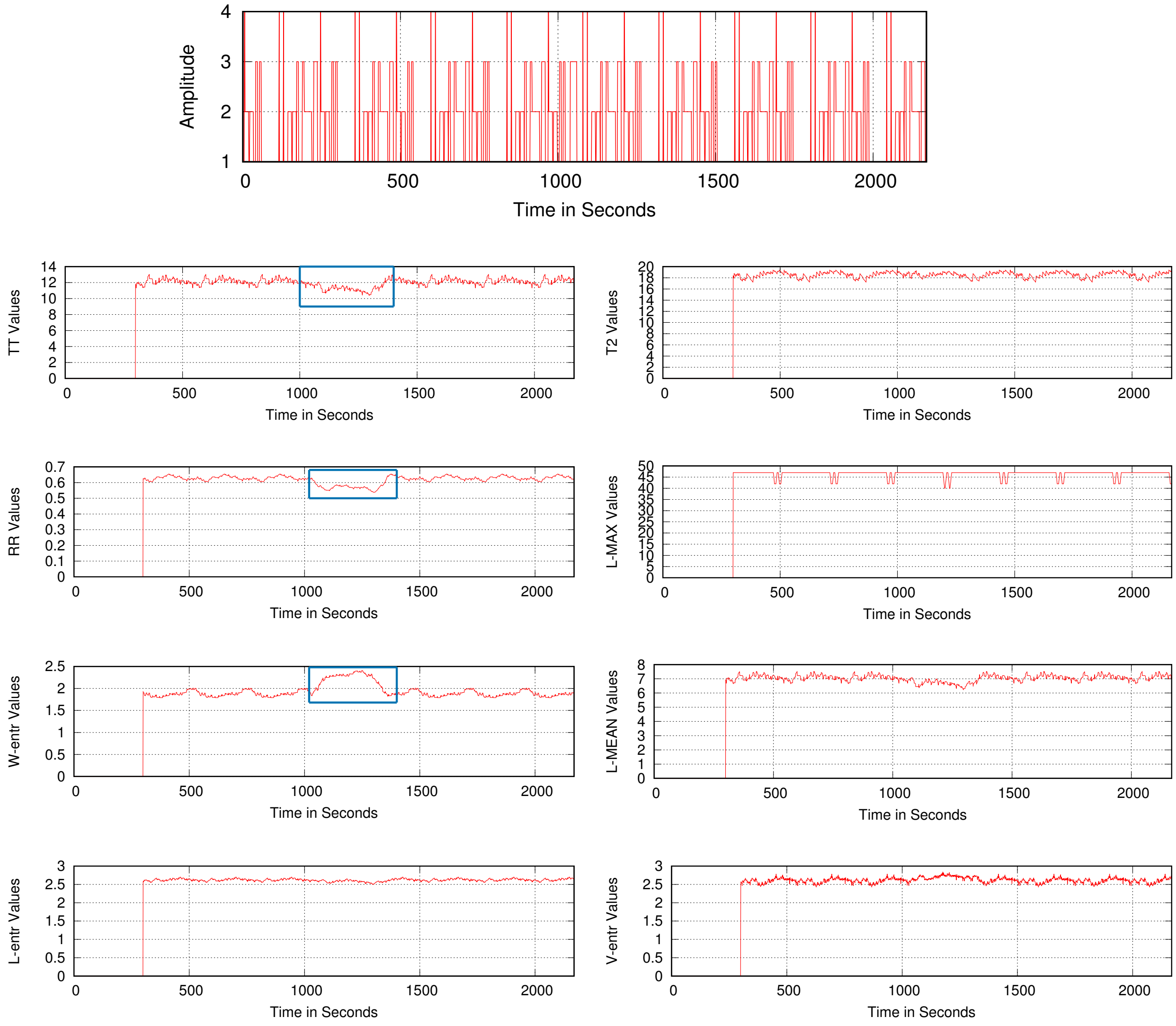


Figure 3.20: The effect of changing recurrence behaviour during the period 1040-1060 seconds on RQA measurements

TT, L-MEAN, and L-entr measurements have shown their ability to rapidly detect a sudden increase in the amplitude values. Although they can detect amplitude change after only one second, TT and L-MEAN are not able to detect small changes in amplitude which help to avoid high FP rates to detect anomalous periods. TT and L-MEAN values change based on variations of amplitude values. For example, maximum value of TT is equal to 141 when the rapid change in amplitude is 180 and it is 238 when the amplitude is 260. These measurements can be used to detect anomalous behaviour based on changing in amplitude of the input data. For example, they can be used to detect BGP anomaly based on BGP features that identify number of BGP updates such as number of BGP announcements, withdrawals, and BGP volume. However, in all our analysis, L-MEAN and TT show similar behaviour for changing amplitude and or periodicity thus we can eliminate one of these measurements to decrease complexity of an anomaly detection technique.

The ability of the T2 measurement is similar to TT and L-MEAN in being able to rapidly detect a sudden increase in the amplitude of the input data. T2 can also rapidly detect a sudden large decrease in the amplitude. This measurement can be used beside TT to measure anomalous behaviour based on amplitude changes.

L-MAX can detect any changes in the input data. Although L-MAX can detect small-/large changes in the amplitude and periodicity of the input data, it shows the same behaviour for all changes. This behaviour can produce high FP rates in a noisy signal thus it is not recommended for anomaly detection.

Like L-MAX, W-entr can detect any changes in the input data. However, the value of W-entr changes based on changing in the input data. For example, there is a small change in the W-entr values when there is a small change in the amplitude (Figure 3.9) and a large change when there is a large change in the amplitude (Figures 3.10). This behaviour can be used to detect different levels of amplitude changes. Furthermore, W-entr can detect periodicity change. This measurement can be used beside TT, T2, L-MEAN, and RR to detect BGP anomalies.

V-entr measurements increase when there is a large change in the amplitude. However, it values shows rapid decrease to zero and sudden increase when there is a very large amplitude change such as when the amplitude value more than 250. This measurement can be used to detect different levels of amplitude change. At the end of this section, five RQA measurements can be used to detect anomalous behaviour. These are: TT, T2, RR, W-entr, and V-entr.

## 3.6 Conclusions

We have presented the concepts of phase plane trajectory, RPs, and RQA. Phase plane is a method of visualising the states of dynamical systems over time, it has been used to measure recurrent behaviour of systems. However, phase plane is very difficult to visualise high-dimensional dynamical systems. RP was introduced to enable the investigation of a high-dimensional phase plane into a two-dimensional representation of its recurrence. The process of quantifying RP structure offers a more objective way for evaluating system under investigation. RQA is a method to quantify RP structure that provides several measures of complexity which quantify RP structure such as TT, T2, RR, and Entropy measurements. RQA measurements changes to reflect changes in system behaviour over time through measuring data read from the system.

We have investigated RQA measurements using a computer-generated time series data and shown how RQA measurements can change based on changing of the input data. RQA measurements show different behaviour in response to changes in the input data. Some RQA measurements such as L-MAX can detect a small change in the input data which can produce many false alarms in a noisy data. Other RQA measurements such as TT, T2, RR, W-entr, and V-entr show their ability to detect significant change in the input. These measurements can be used to detect anomalous behaviour in the input data.

In the next chapter, we use the concepts of phase plane trajectory to model BGP speakers as dynamic systems and characterise BGP traffic sent by BGP speakers. We also use RP to identify recurrence behaviour in the underlying time series BGP traffic.

# Chapter 4

# Modelling BGP Traffic as a Recurrent System

## 4.1 Introduction

BGP is an incremental protocol where, after the initial transfer of a full routing table, traffic between peers should only reflect underlying topology or BGP policies changes. Unfortunately, that is not what we see [8]. Most BGP traffic consists of announcements, updates and withdrawals unrelated to any underlying network management goals [26]. This traffic, although consuming resources, is relatively harmless as long as it does not threaten BGP's ability to disseminate accurate NRI or violate business goals of ISPs. We define this type of BGP traffic as unstable traffic while BGP traffic that does threaten BGP operation or undermines ISPs business goals we define as anomalous traffic.

Unstable BGP traffic is generated by a set of ASes that we define as unstable ASes. There has been some speculation that the source of the unstable traffic is caused by misconfiguration such as prefix overlapping and wide use of the MED attribute [155]. However, locating causes of such routing events is still unknown [67]. Although unstable BGP traffic does not threaten BGP operation or prevent achievement of business goals, it has the effect of masking anomalous traffic that indicates potentially harmful accidental or deliberate anomalies. A technique is needed that can rapidly distinguish between unstable BGP traffic and potentially harmful anomalous traffic.

Although BGP operation has been well described and discussed [25, 156], understanding BGP behaviour over time is still poorly understood. In particular, what are the characteristics of normal-but-unstable BGP traffic and what are the characteristics of anomalous BGP traffic? Does the source of anomalous traffic change rapidly or remain stable? In order to detect anomalous traffic that may indicate a serious event, we need to understand the nature of unstable traffic. To answer these questions, we carry out two investigations. Firstly, we show that apparently complex but voluminous, BGP speakers generate up to a gigabyte of BGP traffic data a day [66], unstable BGP traffic can be understood as an aggregation of oscillations of different frequencies from different ASes. Periodicity can be seen in the most unstable ASes. These ASes show reasonably periodic behaviour in terms of sending BGP updates. We analyse unstable BGP traffic to see how long this periodicity continues. Is it a short or a long term characteristic of normal BGP operation? Secondly, we model a BGP speaker as a dynamic system sending BGP updates based on local routing policies and updates received from neighbours. The goal of the modelling is to study BGP speaker's states over time. For example, what are the characteristics of BGP speakers when forwarding unstable BGP traffic and what are the characteristics of BGP speakers during an anomaly period? Modelling a BGP speaker as a dynamical system helps to understand and predict its behaviour over time. We use the concept of phase plane trajectories to characterise BGP speakers. The outcome of our modelling shows that BGP traffic sent by BGP speakers has the characteristics of being recurrent, non-linear, deterministic, and stable[1].

Building on the outcomes of our investigations, we demonstrate that RQA can distinguish between harmless unstable BGP traffic and harmful anomalous BGP traffic. We show that RQA can indicate anomalous periods in series of unstable BGP traffic using only 200 seconds of past BGP updates. RQA can also indicate hidden anomalous behaviour that may otherwise pass without observation. To illustrate it capability, we apply RQA to one of the most recent BGP events and show it can effectively indicate BGP anomalies as well as some hidden anomalies that have not been observed before. We examine other BGP events in Chapter 5.

The rest of this chapter is organised as follows: Section 4.2 describes BGP datasets that we used in our analysis for BGP periodicity and modelling. In Section 4.3 and 4.4, we analyse BGP traffic volume and BGP route flapping using linear and non-linear statistical analysis. We also model BGP speaker as a dynamic system. Section 4.5 describes our investigation of BGP periodicity and shows that periodic behaviour in BGP traffic can last for at least a decade. In Section 4.6, we evaluate the capability of RQA to detect BGP anomalies using one of the most recent BGP events. We conclude our chapter in Section 4.7.

[1] In this thesis, we use the term "stable" in different contexts. We refer to the dynamic system as stable if its behaviour is stable, not chaotic or random. We also refer to BGP traffic originated by unstable ASes as unstable BGP traffic.

## 4.2 BGP traffic

In this section, we describe data analysis of BGP updates downloaded from publicly available BGP control plane repositories such as [58, 59] which we use to model BGP speakers and investigate the characteristics of periodicity or recurrence in BGP traffic[2]. The RouteViews [58] and RIPE NNC [59] are the most well-known repositories of BGP control plane data. Each of these repositories has multiple Vantage Points (VPs) which run BGP sessions with several routers, referred to as monitors, in many networks.

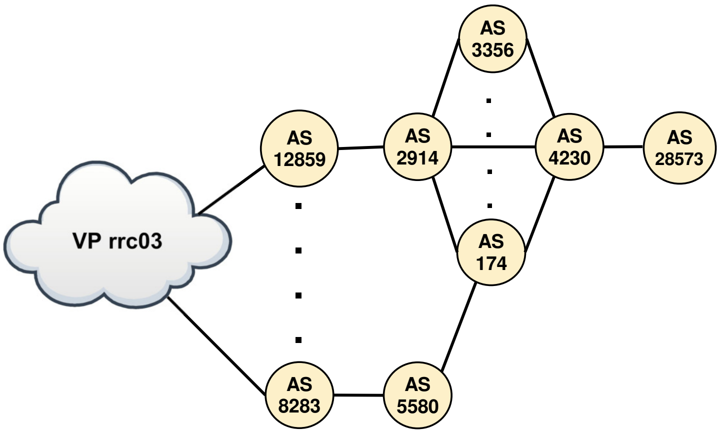


Figure 4.1: Simple BGP topology of the VP rrc03 at RIPE NCC

Figure 4.1 shows an example of BGP topology of the VP rrc03 at RIPE NCC which was peered with 56 peers as observed during the period from 19th to 25th of July 2016. In this example AS12859 and AS8283 represent peers, AS28573 is a source AS, and AS4230, AS174, AS3356, AS2914, and AS5580 are intermediate ASes. When AS28573 sends a BGP update, AS12859 may receive multiple copies of this update via different paths. For example, when AS28573 announces the IPv6 prefix 2804:14d:908a::/48, AS12859 will receive this prefix with three paths [2914, 4230, 28573], [2914, 3356, 4230, 28573], and [2914, 174, 4230, 28573] while the VP rrc03 will receive only one BGP update which is the best route for AS2914 (the path [12859, 2914, 4230, 28573] when no routing policies applied). However, if AS28573 periodically announces then withdraws a prefix every few seconds because of misconfiguration or some other cause, the VP rrc03 may not receive the withdrawn message but update messages with alternative paths. As noted, we have defined these types of BGP updates as unstable traffic [7] which may have the effect of masking anomalous traffic.

[2] We refer to BGP updates traffic as BGP traffic

```
BGP4MP|1468886448|A|2001:7f8:1::a501:2859:2|12859|2804:14d:2a00::/40|12859 2914 4230 28573|IGP|2001:7f8:1::a501:2859:2|0|0|12859:1200|NAG||
BGP4MP|1468886448|A|2001:7f8:1::a501:2859:1|12859|2804:14d:2a00::/40|12859 2914 4230 28573|IGP|2001:7f8:1::a501:2859:1|0|5|12859:1200|NAG||
BGP4MP|1468886448|A|2001:7f8:1::a501:2859:2|12859|2804:14d:90a1::/48|12859 2914 4230 28573|IGP|2001:7f8:1::a501:2859:2|0|0|12859:1200|NAG||
BGP4MP|1468886450|A|2001:7f8:1::a501:2859:2|12859|2804:14d:90a1::/48|12859 2914 3356 4230 28573|IGP|2001:7f8:1::a501:2859:2|0|0|12859:1200|NAG||
BGP4MP|1468886451|A|2001:7f8:1::a501:2859:2|12859|2804:14d:90a1::/48|12859 2914 4230 28573|IGP|2001:7f8:1::a501:2859:2|0|0|12859:1200|NAG||
BGP4MP|1468886452|A|2001:7f8:1::a501:2859:2|12859|2804:14d:9086::/48|12859 2914 3356 4230 28573|IGP|2001:7f8:1::a501:2859:2|0|0|12859:1200|NAG||
BGP4MP|1468886452|A|2001:7f8:1::a501:2859:2|12859|2804:14d:9088::/48|12859 2914 3356 4230 28573|IGP|2001:7f8:1::a501:2859:2|0|0|12859:1200|NAG||
BGP4MP|1468886452|A|80.249.208.200|12859|177.143.0.0/18|12859 2914 4230 28573|IGP|80.249.208.200|0|0|2914:410 2914:1002 2914:2000 12859:1200|NAG||
BGP4MP|1468886455|A|80.249.208.200|12859|179.154.192.0/19|12859 2914 4230 28573|IGP|80.249.208.200|0|0|2914:410 2914:1002 2914:2000 12859:1200|NAG||
BGP4MP|1468886455|A|80.249.208.200|12859|187.66.224.0/20|12859 2914 4230 28573|IGP|80.249.208.200|0|0|2914:410 2914:1002 2914:2000 12859:1200|NAG||
BGP4MP|1468886455|A|2001:7f8:1::a501:2859:2|12859|2804:14d:908d::/48|12859 2914 3356 4230 28573|IGP|2001:7f8:1::a501:2859:2|0|0|12859:1200|NAG||
```

Figure 4.2: An example of BGP updates originated by unstable AS28573 and sent by the peer AS12859

There are two characteristics of BGP update traffic we are interested in. First is BGP traffic volume made up of BGP announcements and withdrawals calculated each second. Second is route flapping measured as BGP update per AS-PATH. Figure 4.2 shows an example of BGP traffic originated by AS28573 and seen by the peer AS12859. In this example, there are 11 BGP updates related to 8 prefixes originated by AS28573. These updates sent during 8 seconds (Unix time stamp 1468886448 to 1468886455) through 2 different AS-PATHs. We represent each path by a number. In this example, the AS-PATH [12859 2914 4230 28573] is assigned with number 1 and the AS-PATH [12859 2914 3356 4230 28573] is assigned with 2. The corresponding representation of BGP traffic volume is [3, 0, 1, 1, 3, 0, 0, 3] while the corresponding representation of BGP route flapping is [1, 1, 1, 2, 1, 2, 2, 1, 1, 1, 2]. In the following sections, we investigate these two characteristics of BGP traffic starting with BGP traffic volume.

## 4.3 BGP traffic volume

In this section, we investigate the characteristics of BGP traffic volume. BGP traffic has been characterised as voluminous, noisy, and bursty [130]. Using linear and non-linear statistical analysis, we show that BGP traffic has a structure of a recurrent behaviour. The source of this behaviour is unsynchronised periodic traffic with different frequencies by a set of unstable ASes.

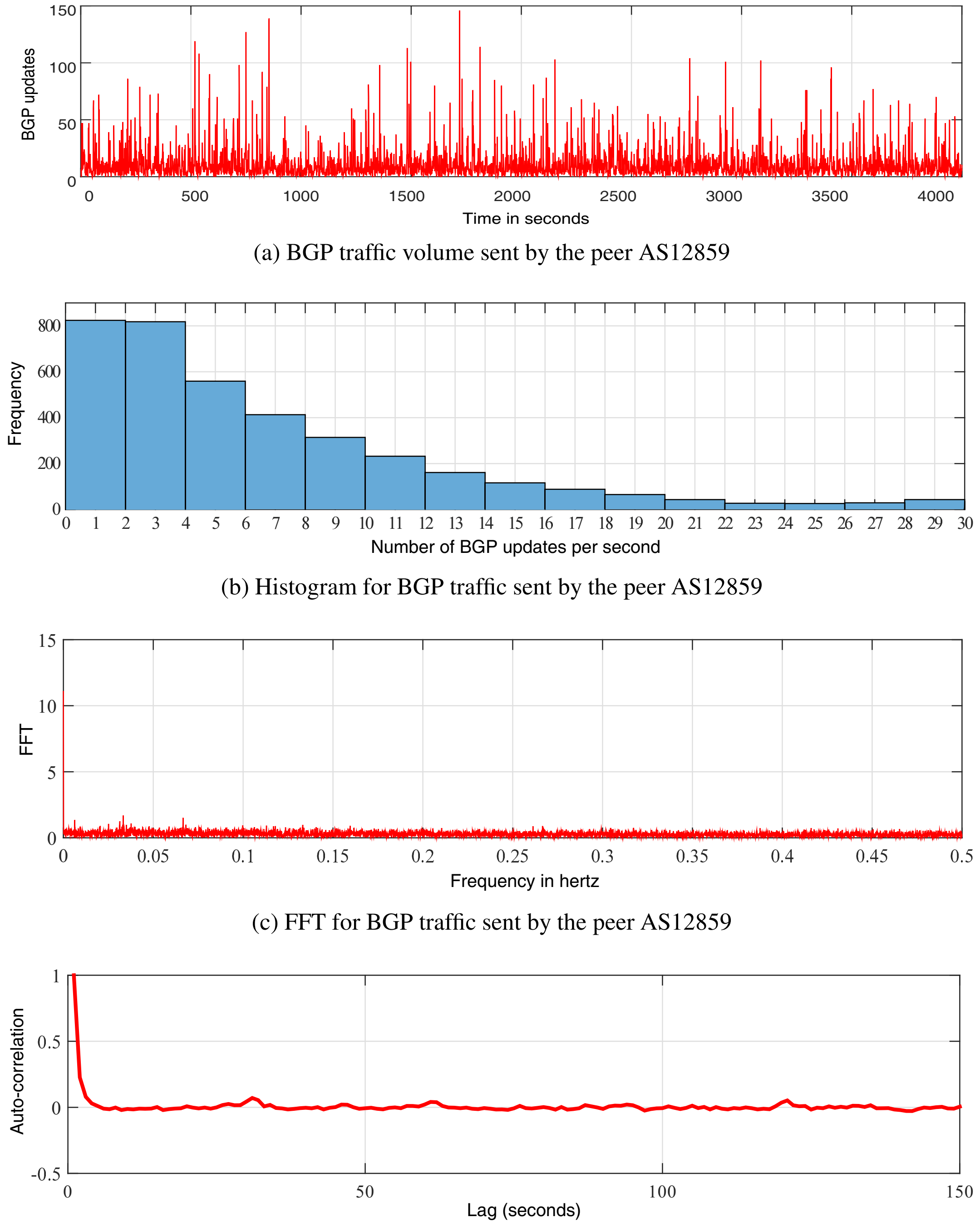
Our investigation includes analysing BGP traffic at different levels. These levels are aggregated BGP traffic originated by a set of unstable ASes and sent by a peer AS, BGP traffic related to individual unstable ASes, and BGP traffic related to individual prefixes associated with a single unstable AS. We also use the concepts of phase space trajectories to model BGP speaker as a dynamic system.

During the period 19th to 25th of July 2016, there were 56 peers connected to the VP rrc03 at RIPE NCC. We use BGP traffic sent by the peer AS1289 in our analysis as it sent the largest number of BGP updates during the period. We start our investigation by exploring the distribution of BGP updates per second sent by AS12859. We also use FFT and ACF, the most well-known techniques to identify periodicity in time series data [157], to explore the characteristics of periodicity in the underlying BGP traffic.

### 4.3.1 Analysis of BGP traffic volume

In this subsection, we explore the characteristics of total BGP updates calculated every second originated by a set of unstable ASes and sent by the peer AS12859. We also analyse BGP traffic related to individual unstable ASes and BGP traffic related to individual prefixes associated with a single unstable AS. Our analysis shows although total BGP traffic sent by BGP speakers does not show a periodic behaviour, it does for BGP traffic originated by individual unstable ASes. These ASes periodically send BGP updates with different frequencies. The periodic behaviour is even more apparent for BGP traffic related to individual prefixes belonging to single unstable ASes. For example, Figure 4.3 shows values of histogram, FFT, and ACF for a sample of BGP traffic sent by the peer AS12859 at VP rrc03 during the period 19th to 25th of July 2016. Although the distribution of the numbers of BGP updates sent by the peer AS12859 shows that most numbers of BGP updates are in a range 0-30 updates per second as shown in Figure 4.3b, the calculations of FFT and ACF do not show a clear indication for periodicity as shown in Figures 4.3c and 4.3d. However, BGP traffic sent by the peer AS12859 represents an aggregation of BGP traffic for a set of unstable ASes. The top-ten unstable ASes during the observation period and seen by the peer AS12859 are AS28573, AS56237, AS45292, AS36943, AS17908, AS16652, AS4755, AS9829, AS55430 and AS198171. We now examine the characteristic of periodicity for BGP traffic sent by some unstable ASes.

The histogram, FFT, and ACF of BGP updates related to a single unstable AS show a better observation for the characteristic of periodicity than the aggregated BGP traffic sent by all unstable ASes. For example, Figure 4.4 shows values of histogram, FFT, and ACF for the total number of BGP updates per second originated by the unstable AS28573 (the most active unstable AS during the observed period) as observed by the peer AS12859. Figure 4.4b shows the occurrence of numbers of BGP updates per second sent by the unstable AS28573 and observed by the peer AS12859. Excluding value of zero which represents no BGP updates sent, we can see that most numbers of BGP updates per second are in ranges 1-6 and 10-12. On the other side, our investigation for detecting periodicity shows there is a periodic behaviour of sending BGP updates by the unstable AS28573 in both time and frequency domains as shown in Figures 4.4c and 4.4d. In these figures, we can see that the unstable AS28573 sends BGP updates with a period of 60 seconds or 0.015 hertz. Periodicity is even clearer when we analyse BGP updates related to a single prefix generated by the unstable AS28573. We see evidence that BGP traffic volume is periodic when considering single prefixes, but it is not synchronised periodic behaviour becomes less obvious.



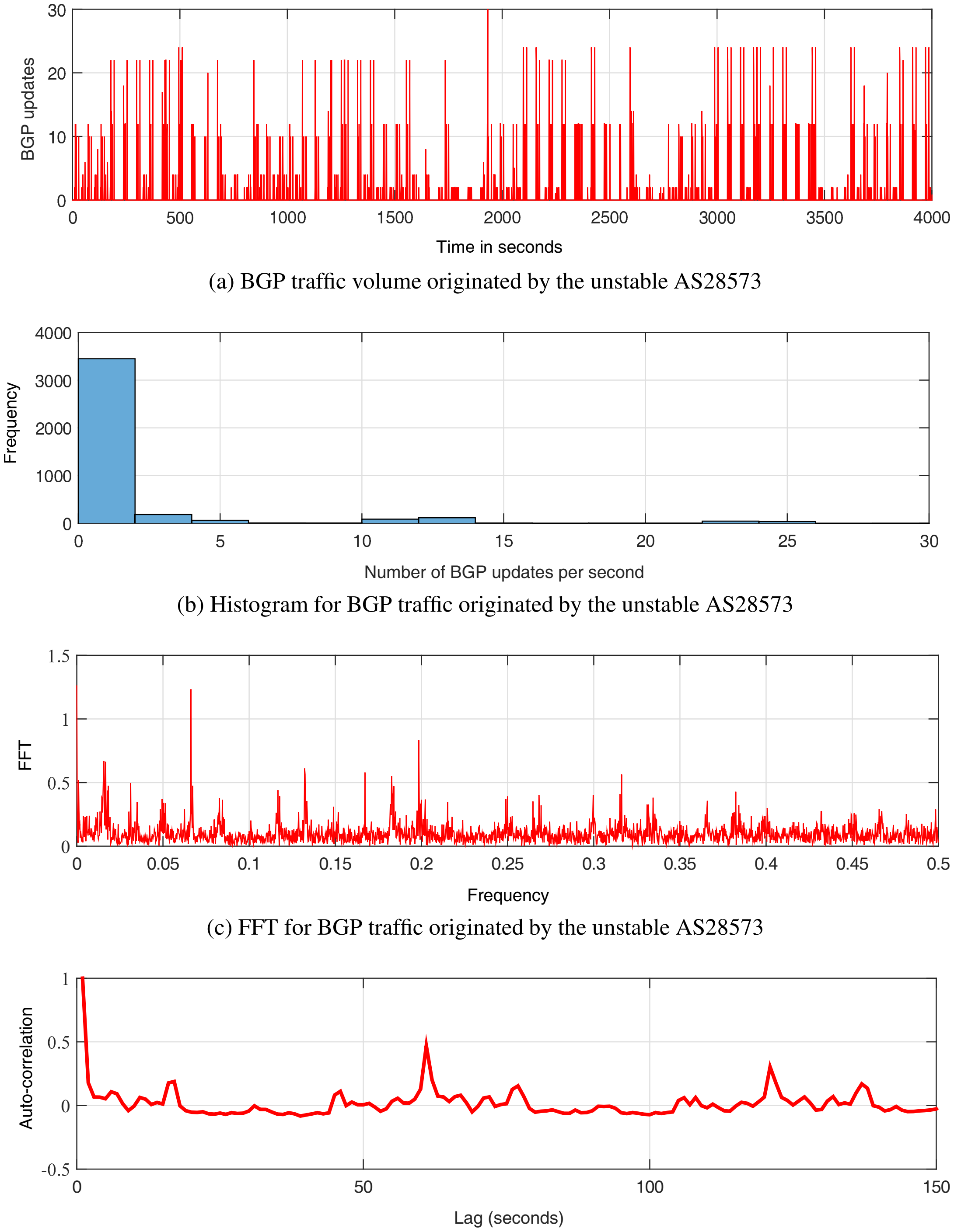
(a) BGP traffic volume sent by the peer AS12859

(b) Histogram for BGP traffic sent by the peer AS12859

(c) FFT for BGP traffic sent by the peer AS12859

(d) ACF for for BGP traffic sent by the peer AS12859

Figure 4.3: Histogram, FFT, and ACF for BGP traffic volume sent by the peer AS12859



(a) BGP traffic volume originated by the unstable AS28573

(b) Histogram for BGP traffic originated by the unstable AS28573

(c) FFT for BGP traffic originated by the unstable AS28573

(d) ACF for BGP traffic originated by the unstable AS28573

Figure 4.4: Histogram, FFT, and ACF for BGP traffic volume originated by the unstable AS28573

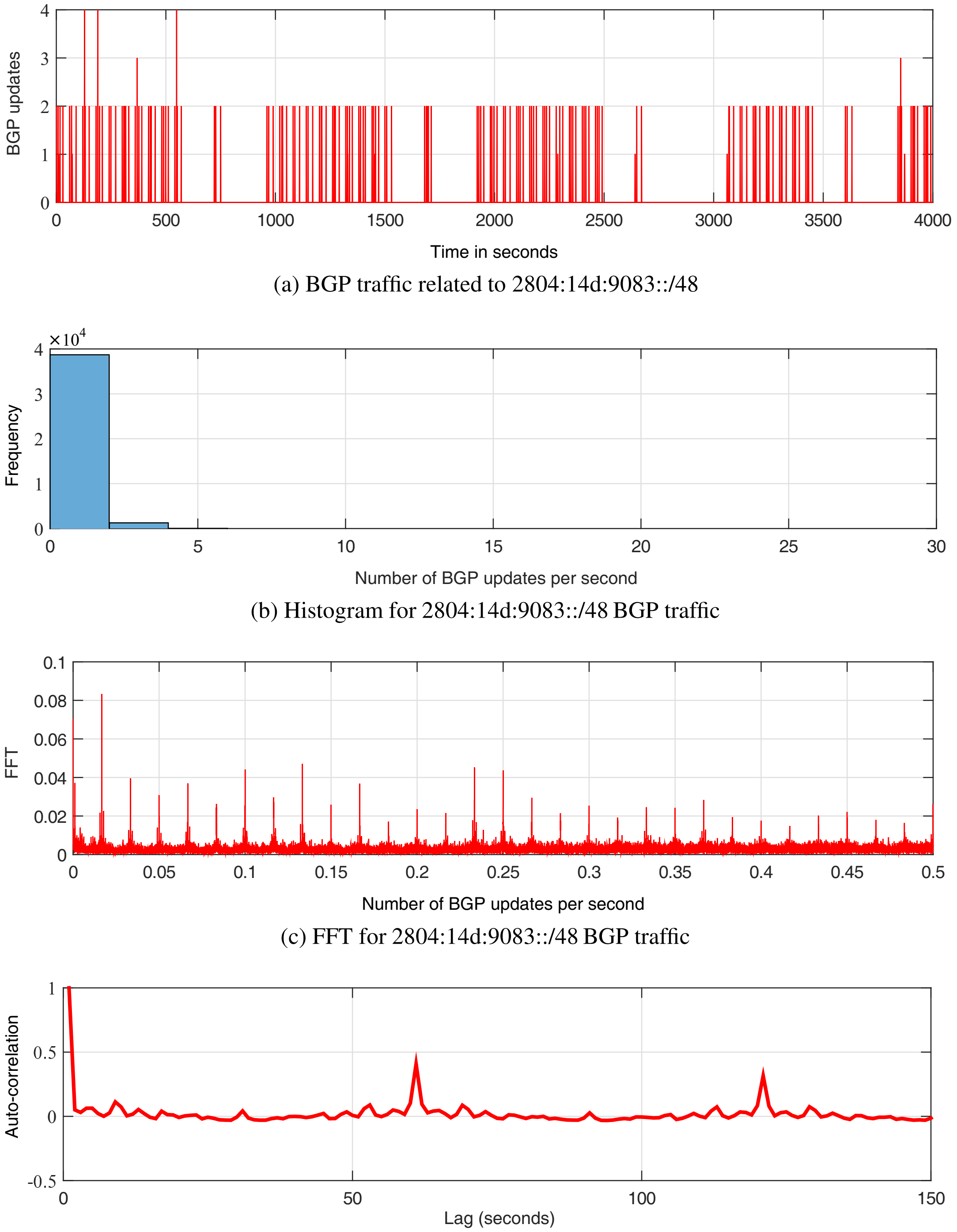
Although BGP traffic related to IPv4 seems to be the prominent part of BGP traffic as a result of the number of IPV4 prefixes used [158], BGP updates related to IPv6 represents an important part of unstable BGP traffic. During the period of analysis, there were 2820997 IPv6 BGP updates and 5083818 IPv4 BGP updates as observed by the peer AS12859. The unstable AS28573 announced 3584258 BGP updates related to 104 IPv6 prefixes and 22121 BGP updates related to 343 IPv4 prefixes. The prefix 2804:14d:9083::/48 was the most unstable prefix announced by the AS28573 during the period of analysis. BGP traffic related to the prefix 2804:14d:9083::/48 shows a notable observation for the distribution of BGP updates and a stronger periodicity than BGP updates related to all prefixes belonged to the AS28573 as shown in Figure 4.5.

Further investigation of BGP traffic shown in Figure 4.5a shows there is consistent behaviour of sending two updates per second for the same prefix and AS-PATH but with different values of the MED attribute. MED is a BGP attribute provides a mechanism to influence neighbours ASes to reach a certain route when there are multiple entry for that AS. This observation supports the analysis by [159] that shows the MED attribute can lead to persistent oscillatory behaviour in BGP traffic.

The unstable AS17908 is another example of unstable ASes that shows periodic behaviour. During the period of the analysis, the unstable AS17908 announced 409499 BGP updates related to 48 IPv4 prefixes and 1 IPv6 prefix. Figure 4.6 shows values of the histogram, FFT, and ACF for BGP updates originated by the unstable AS17908 as seen by the peer AS12859 where we can see clear periodic behaviour with value of 10 seconds as shown in Figure 4.6d. Almost all BGP updates originated by the unstable AS17908, 409447 updates out of 409499 BGP updates, belong to IPv4 prefixes 61.11.80.0/21 and 61.11.90.0/24. Figure 4.7 shows values of the histogram, FFT, and ACF for BGP updates related to IPv4 prefix 61.11.90.0/24 where can see, once again, periodic BGP updates with period of 10 seconds. Nevertheless, not all unstable ASes exhibit such clear periodic behaviour. Among the top-ten unstable ASes during the observation period, 19th to 25th of July 2016, the unstable AS9829 and AS198171 do not shows a clear observation of periodicity.

Using linear statistical analysis we can find that although BGP traffic has been characterised as a complex, noisy, and bursty [130], it can be understood as an aggregation of unsynchronised periodic traffic with different frequencies with additional noise. For example, Figure 4.8 shows a sample of the aggregated BGP traffic related to unstable AS28573, AS56237, AS36943, and AS45292 where we can see periodic change in volume at different frequencies and unsynchronised. In this example, the periodicity of AS45292 and AS56237 is 15 seconds and 60 seconds for AS36943 and AS28573.

Identifying the characteristic of periodicity for unstable prefixes is a step toward identifying BGP anomalies. For example, a sudden change in the characteristic of periodicity for



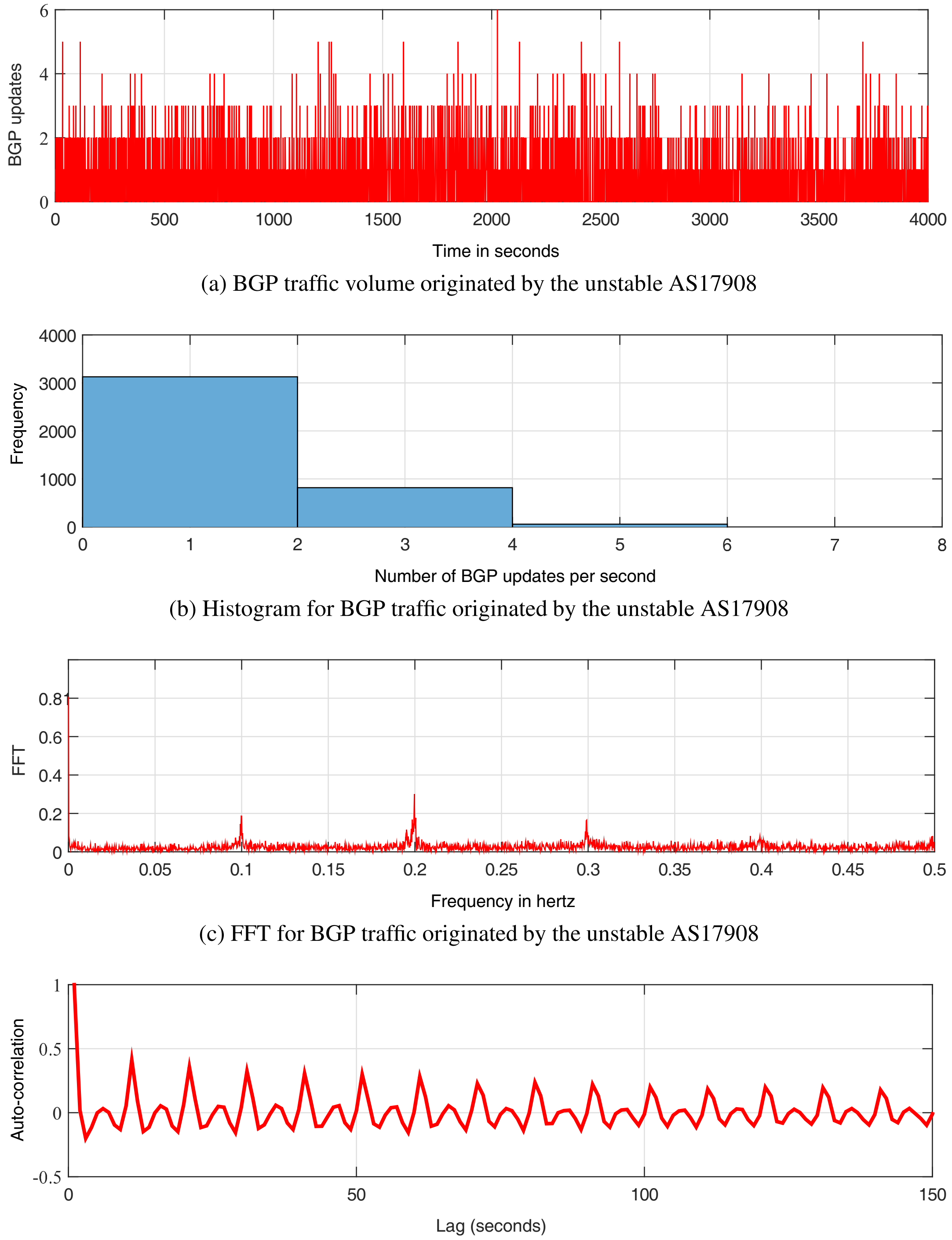
(a) BGP traffic related to 2804:14d:9083::/48

(b) Histogram for 2804:14d:9083::/48 BGP traffic

(c) FFT for 2804:14d:9083::/48 BGP traffic

(d) ACF for 2804:14d:9083::/48 BGP traffic

Figure 4.5: Histogram, FFT, and ACF for BGP traffic volume related to 2804:14d:9083::/48



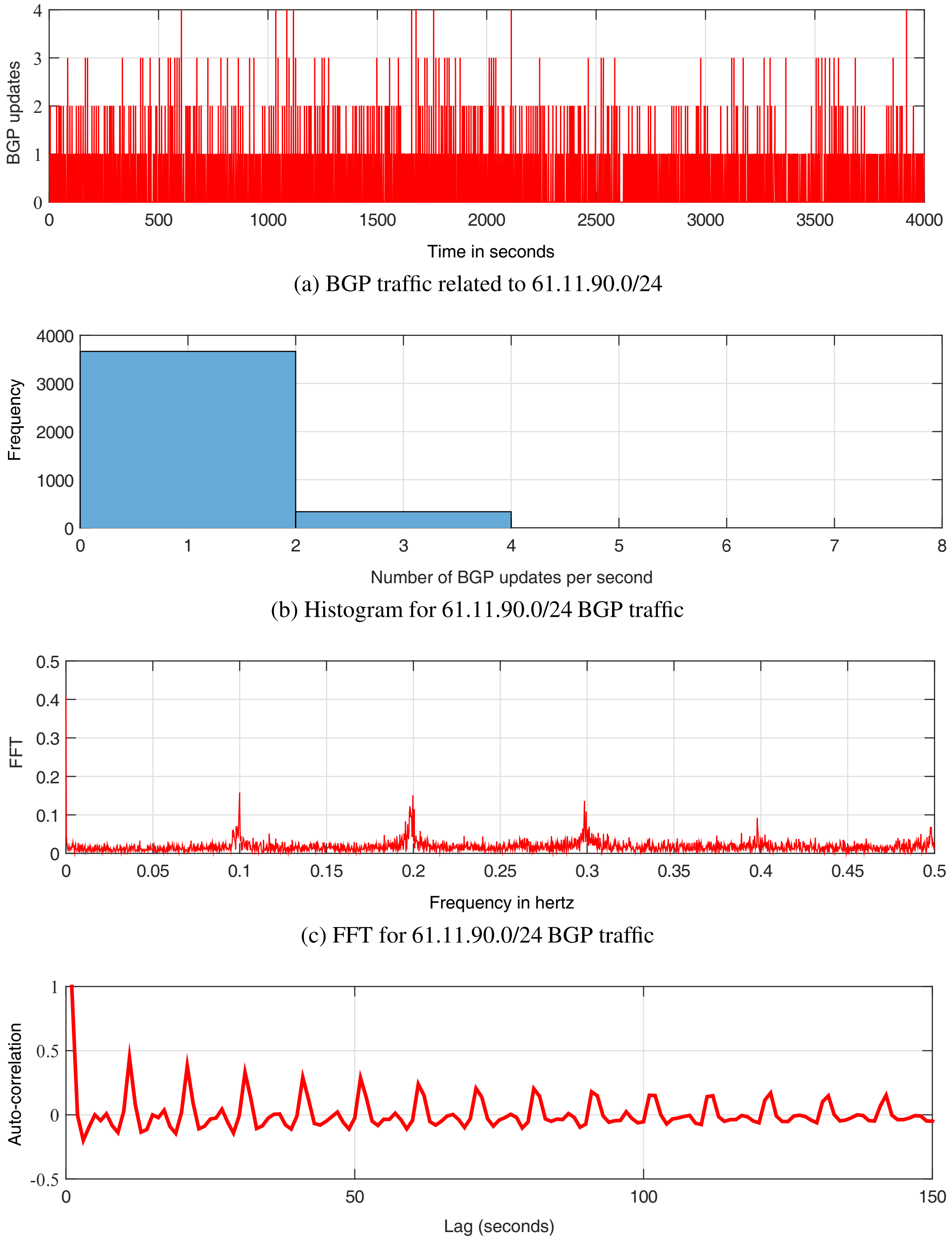
(a) BGP traffic volume originated by the unstable AS17908

(b) Histogram for BGP traffic originated by the unstable AS17908

(c) FFT for BGP traffic originated by the unstable AS17908

(d) ACF for BGP traffic originated by the unstable AS17908

Figure 4.6: Histogram, FFT, and ACF for BGP traffic volume originated by the unstable AS17908



(a) BGP traffic related to 61.11.90.0/24

(b) Histogram for 61.11.90.0/24 BGP traffic

(c) FFT for 61.11.90.0/24 BGP traffic

(d) ACF for 61.11.90.0/24 BGP traffic

Figure 4.7: Histogram, FFT, and ACF for BGP traffic volume related to 61.11.90.0/24

individual unstable prefixes might be an indication to detect anomalies for unstable ASes. However, this indication cannot be used easily to detect anomalies for peer ASes. This is due to the number of BGP updates related to a single unstable prefix represents only a small portion of the total number of BGP updates sent by a peer AS. For example, BGP updates related to unstable prefix 2804:14d:9083::/48 represents only 1.6% of the total number of BGP updates sent by the peer AS12859.

Linear statistical analysis cannot easily identify an apparent structure for the aggregate BGP traffic of a set of unstable ASes as we saw in Figure 4.3. Our next step is to identify the characteristic of the aggregated BGP traffic using non-linear statistical techniques. Furthermore, we identify the characteristic of BGP speakers through modelling BGP speakers as dynamic systems.

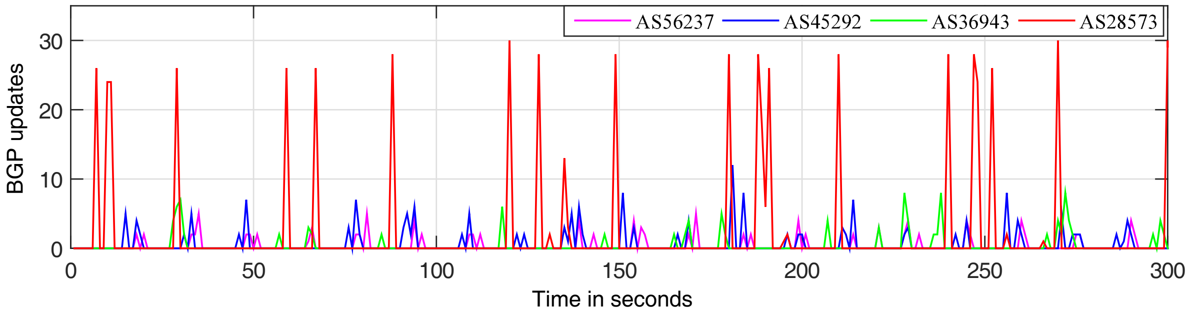
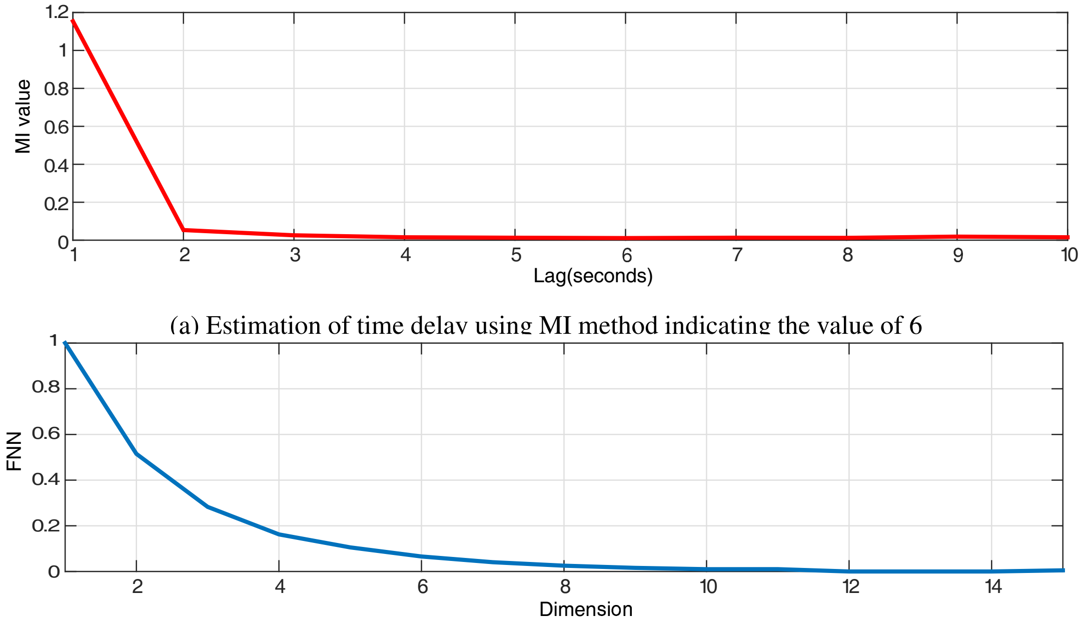


Figure 4.8: Sample of unsynchronised periodic behaviour for the unstable AS28573, AS56237, AS36943, and AS45292

### 4.3.2 Recurrence modelling of BGP update volume

We have shown in the previous subsection that although BGP traffic originated by individual unstable ASes shows approximately periodic behaviour, the aggregated BGP traffic for multiple unstable ASes does not. In this section, we use non-linear statistical analysis to show that the aggregated BGP traffic has the characteristic of recurrent behaviour. Furthermore, we show that BGP speakers have the characteristics of determinism, stability, and non-linear.

To determine the characteristics of traffic generated by BGP speakers over time, we model BGP speakers as dynamic systems using BGP traffic per second sent by BGP speakers. Our modelling is based on the concept of phase space trajectory described in Section 3.2. BGP speakers send BGP updates and path lengths depending on BGP messages received from neighbours and local routing policies. When a BGP speaker receives a BGP message that changes its routing table it will propagate that message to all or a group of its neighbours based on its local policies. Otherwise, the message will be terminated. The properties of the phase space are used to categorise dynamical systems. For example, a system can be categorised as a deterministic if its future states are uniquely determined by its current states.



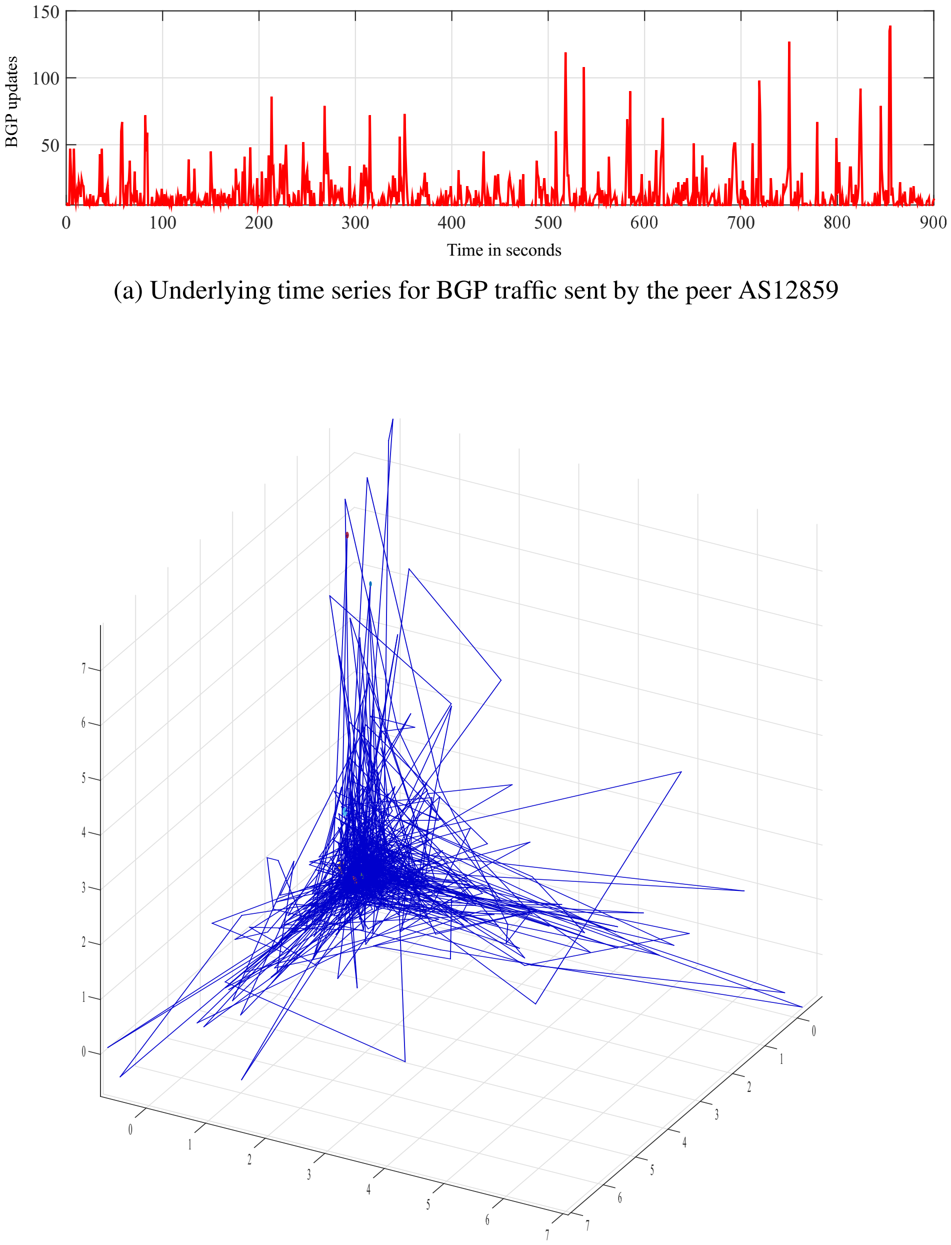
(a) Estimation of time delay using MI method indicating the value of 6

(b) Estimation of embedding dimension using FNN method indicating the value of 12

Figure 4.9: Estimation of time delay and embedding dimension for BGP traffic sent by the peer AS12859

As discussed in Chapter 3, the best-known method for reconstructing phase space trajectories from a time series is the time delay embedding reconstruction method. We use MI and FNN to estimate the value of time delay and embedding dimension respectively. For example, Figures 4.9 shows the calculation of MI and FNN for BGP traffic sent by the peer AS12859 (shown in Figure 4.3a). In this example, the estimation values of time delay and embedding dimension are 6 and 12 respectively which represent the first minimum values of MI and FNN.

Figure 4.10 shows the underlying time series for the total number of BGP updates per second sent by peer AS12859 and collected at VP rrc03 in the RIPE NCC and its corresponding representation of phase space. Although there are some trajectories that deviate from the origin point as a result of some high BGP volume such as at time 525 seconds, most of the phase plane information shows that the BGP speaker (the BGP router that sent BGP traffic,



(a) Underlying time series for BGP traffic sent by the peer AS12859

(b) Phase space representation for BGP traffic sent by the peer AS12859 with time delay=6

Figure 4.10: Underlying time series for BGP traffic sent by AS12859 and its corresponding representation of phase space identifying stable system behaviour

AS12859 in this case) has the characteristics of a stable system. However, as discussed before in Chapter 3, identifying the type of motion in dynamic systems using phase plane trajectories is difficult. We use the concept of maximal Lyapunov exponents [150] to identify the type of motion and DVV [152] method to estimate the properties of determinism and non-linearity.

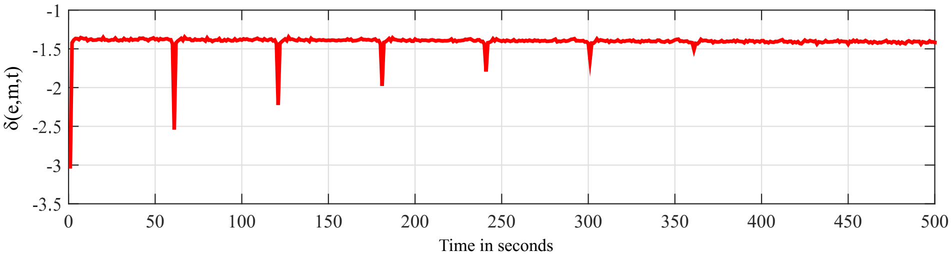
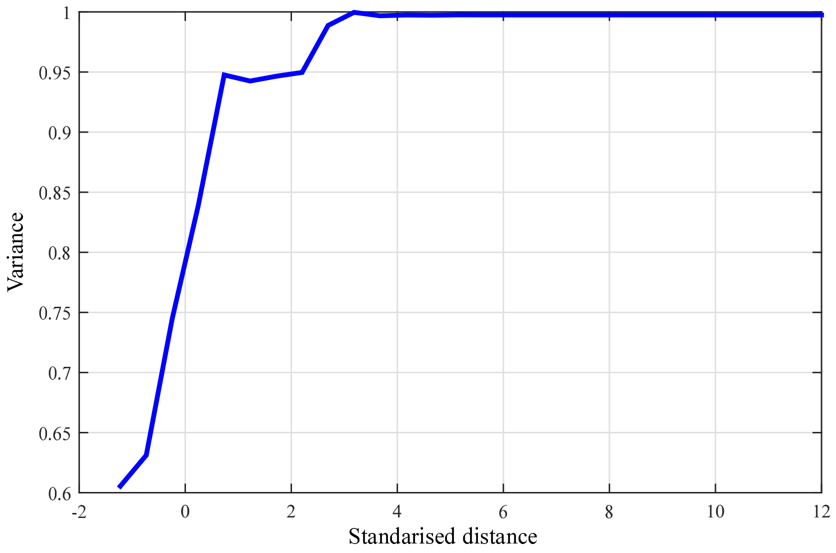


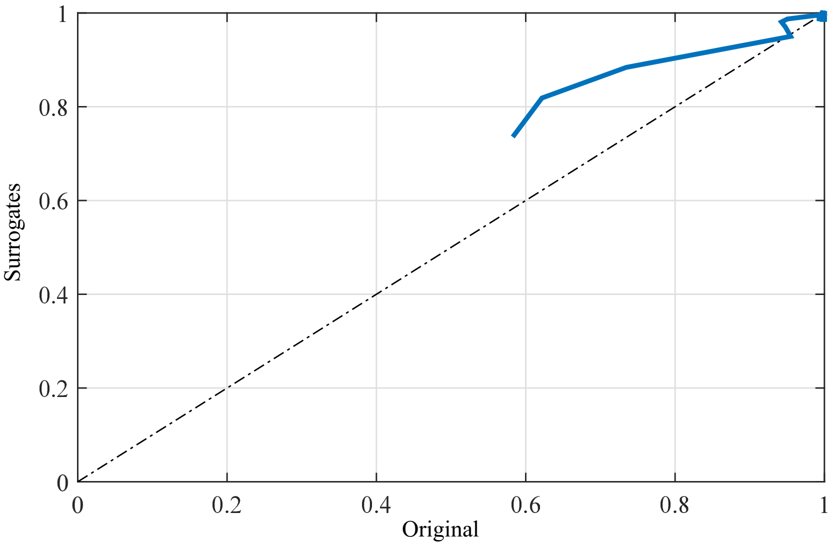
Figure 4.11: Lyapunov exponents for BGP traffic volume sent by the peer AS12859 indicating stable system behaviour

The value of maximal Lyapunov exponent can be estimated through calculating the slope of Lyapunov exponents while determinism and non-linearity can be estimated through DVV plot and scatter diagram respectively. Figure 4.11 shows Lyapunov exponents for BGP traffic sent by the peer AS12859 where we can see the slope value of Lyapunov exponents equal to zero indicating possible stable behaviour. In terms of determinism and non-linearity, the values of variance shown in Figure 4.12a converge to one indicating possible deterministic system behaviour. Figure 4.12b shows a scatter diagram for BGP traffic volume per second sent by the peer AS12859 where we can see a deviation from the bisector line indicating possible non-linear system behaviour. The outcome of our modelling suggests that BGP speakers have the characteristics of being non-linear, stable, and deterministic. These characteristics are important properties to select an appropriate technique to differentiate between unstable and anomalous BGP traffic. For example, there are limitations for analysing BGP traffic using the Autoregressive Integrated Moving Average (ARIMA) model. The ARIMA model has two significant limitations: (1) future values are assumed to be a linear function of past values and (2) a large amount of historical data is required to obtain reliable predictions. We have characterised BGP traffic as non-linear which motivates us to look for another approach [8].

Based on our analysis, we use an RP to visualize the time dependent behaviour of BGP traffic volume. Figure 4.13 shows RP and underlying BGP updates per second sent by the peer AS12859. In the large scale of the RP we can see long diagonal lines that indicate long range periodicity in the underlying system behaviour. The source of this periodicity is caused by unstable ASes that periodically send BGP updates with different frequencies. In addition, there are orthogonal lines to the LOI indicating that the evolution of the BGP speaker

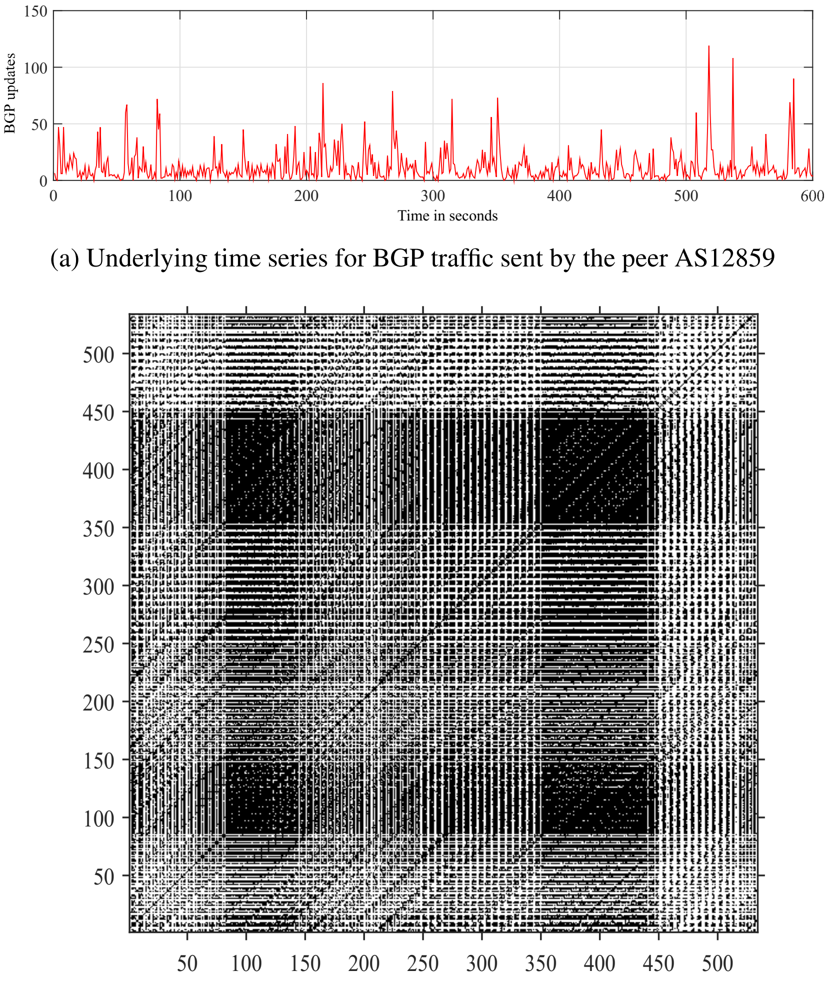


(a) DVV plot indicating deterministic system behaviour



(b) Scatter diagram indicating non-linear system behaviour

Figure 4.12: Estimation of determinism and linearity for BGP traffic sent by the peer AS12859



(a) Underlying time series for BGP traffic sent by the peer AS12859

(b) RP representation for BGP traffic sent by the peer AS12859

Figure 4.13: Identifying recurrence behaviour for BGP traffic sent by the peer AS12859

states is similar at different times but they move in the opposite time direction [147]. At the small scale, single isolated points indicate a fluctuation of system behaviour while vertical and horizontal lines forming rectangles indicate some states that do not change or change slowly. This behaviour is expected as BGP speakers do not continually send BGP updates. Most BGP speakers send updates based on the MRAI timer, the minimum amount of time to wait before sending an advertisement to a particular destination.

To summarise our RP demonstration, the aggregated BGP traffic has the characteristic of recurrent behaviour where the rectangular boxes (constructed by vertical and horizontal lines) are repeated at different time scales.

We can summarise our analysis and modelling for BGP traffic volume sent by BGP speakers as follows. Although BGP traffic generated by individual unstable ASes shows a notable behaviour of periodicity with different frequencies, the aggregated BGP traffic does not show a clear observation of periodic behaviour. However, it shows recurrent behaviour. We have also shown that aggregated BGP traffic has the characteristics of determinism and non-linearity. In the next chapter we show how these characteristics can be used to detect BGP anomalies. In the next section, we carry out a similar analysis to model BGP route flapping.

## 4.4 BGP route flapping

In this section, we analyse BGP route flapping generated by unstable ASes. Using linear statistical analysis such as ACF and FFT we show although the aggregated BGP route flapping of all prefixes related to unstable AS does not show an observation of periodicity, it does for individual prefixes related to a single unstable AS. However, using non-linear statistical analysis, we now show that the aggregated BGP route flapping of unstable ASes has recurrent behaviour. It also has the characteristic of determinism and non-linearity. We start our analysis for BGP route flapping by demonstrating that traditional techniques suggest route flapping is random. We then show that it appears to have recurrent behaviour. We present the histogram, FFT, and ACF for aggregated BGP traffic originated by an unstable AS and for BGP route flapping related to individual prefixes of an unstable AS.

### 4.4.1 Analysis of BGP route flapping

Analysing BGP route flapping for all BGP updates sent by a peer AS and related to all unstable ASes is a challenge. For example, there were 99668 AS-PATHs for 7904815 BGP updates during the period 19th to 25th July 2016. This large number of AS-PATHs leads to an uncorrelated relationship among these AS-PATHs. For example, some AS-PATHs may appear every 5000 updates while other AS-PATHs appear every 200 updates which may lead to uncorrelated sequence of data. Therefore, we do our analysis on BGP route flapping associated with an unstable AS and per individual prefixes related to the unstable AS.

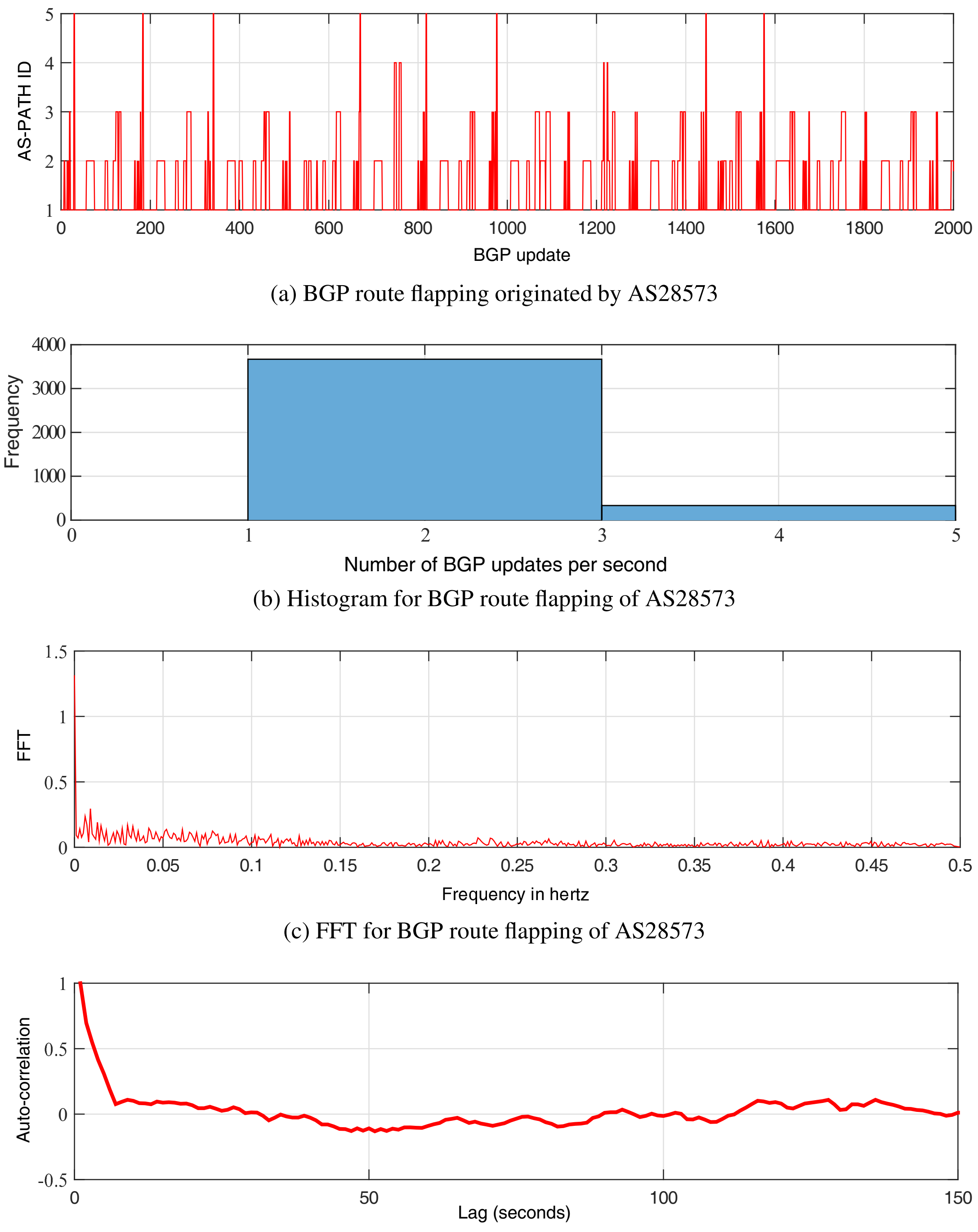
During the period of the analysis, 19th to 25th July 2016, there were 603243 BGP updates originated by the unstable AS28573, the most active unstable AS, as observed by the peer AS12859 in the VP rrc03 through 32 AS-PATHs. Figure 4.14 shows a sample of BGP updates versus top five AS-PATHs between the unstable AS28573 and the peer AS12859. These are AS-PATH1=[12859, 2914, 4230, 28573], AS-PATH2=[12859, 6939, 4230, 28573], AS-PATH3=[12859, 6939, 3356, 4230, 28573], AS-PATH4=[12859, 2914, 3356, 4230, 28573], and AS-PATH5=[12859, 6939, 6453, 4230, 28573]. Although distribution of BGP updates per AS-PATHs shows most updates were passed through AS-PATH1 as shown in Figure 4.14b, BGP updates versus top five AS-PATHs, once again, does not show a structure of a periodic behaviour as shown in Figures 4.14c and 4.14d. However, going beyond total BGP traffic versus AS-PATHs to BGP updates belonging to one prefix per AS-PATH we can see periodicity for BGP path updates.

The unstable AS28573 announced 447 prefixes (104 IPv6 prefixes and 343 IPv4 prefixes) during the period of the analysis. Although these prefixes were generated by one AS (AS28573) and collected by one peer (AS12859), there are different AS-PATHs for these prefixes. For example, BGP traffic related to 2804:14d:9083::/48 (the most unstable prefix announced by AS28573) was passed through three different AS-PATHs while BGP traffic related to 2804:14d:908b::/48 was passed through 12 different AS-PATHs. A probable explanation for this variety of AS-PATHs is because they reflected different business relationship policies between ASes. However, our analysis for BGP traffic related to the most active five prefixes shows there is a periodic behaviour. For example, BGP traffic belonging to the prefix 2804:14d:9083::/48 was sent via three AS-PATHs. Analysing this traffic shows there is periodic behaviour with period of 8 updates as shown in Figure 4.15.

These statistics suggest that periodicity is characteristic of BGP traffic behaviour related to individual prefixes of unstable ASes. Whatever the representation of BGP traffic per second or per AS-PATH, we still see a strong periodic behaviour as shown in Figures 4.5 and 4.15. In the next subsection, we show, once again, although the aggregated BGP route flapping associated with an unstable AS does not show a periodic behaviour, it has a recurrent behaviour.

### 4.4.2 Recurrence modelling of BGP route flapping

We have shown in the previous subsection using linear statistical analysis that BGP route flapping does not show a clear structure of periodicity for total BGP routes belonging to all prefixes of an unstable AS. In this subsection, we investigate BGP route flapping through



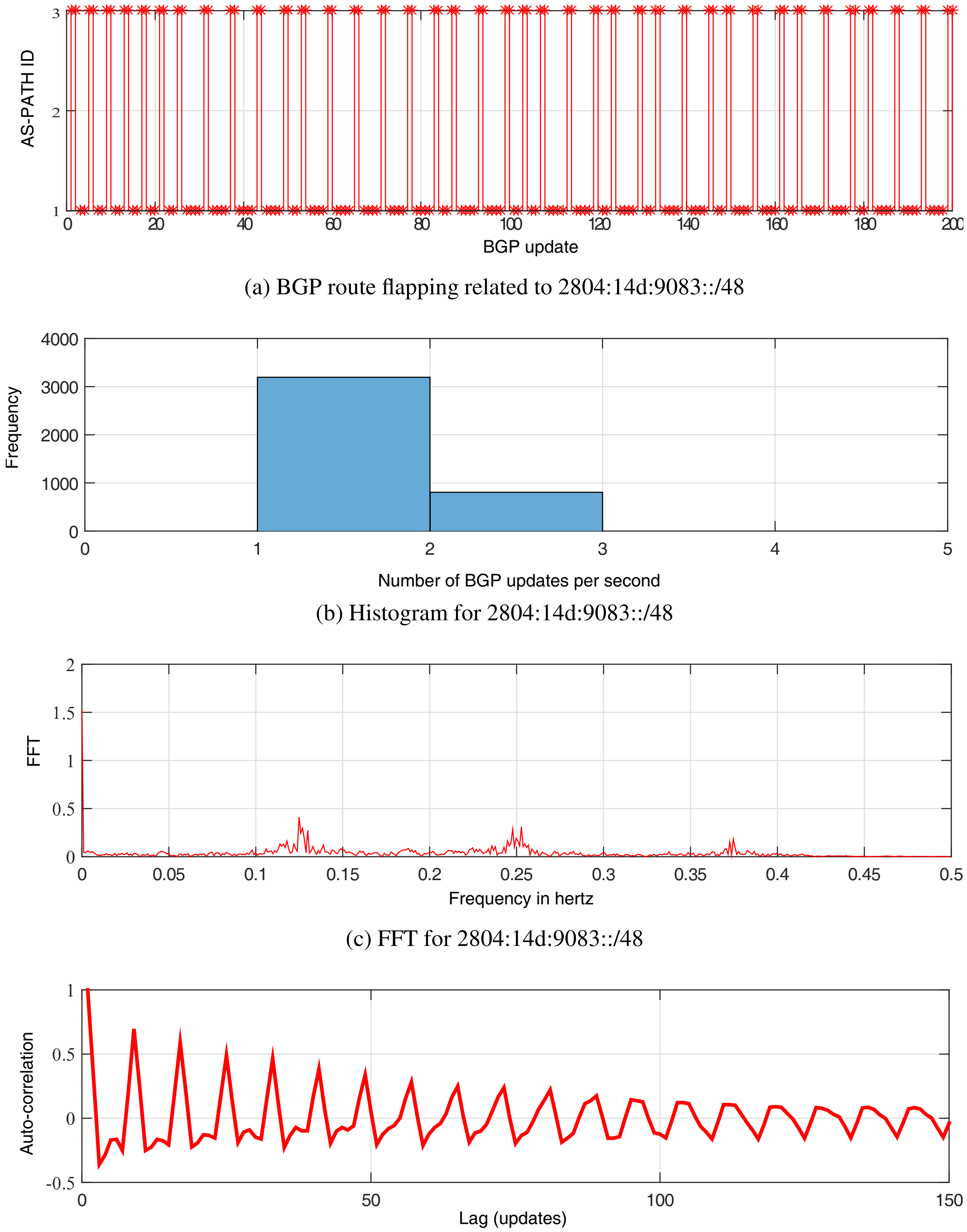
(a) BGP route flapping originated by AS28573

(b) Histogram for BGP route flapping of AS28573

(c) FFT for BGP route flapping of AS28573

(d) ACF for BGP route flapping of AS28573

Figure 4.14: Histogram, FFT, and ACF for BGP route flapping originated by AS28573



(a) BGP route flapping related to 2804:14d:9083::/48

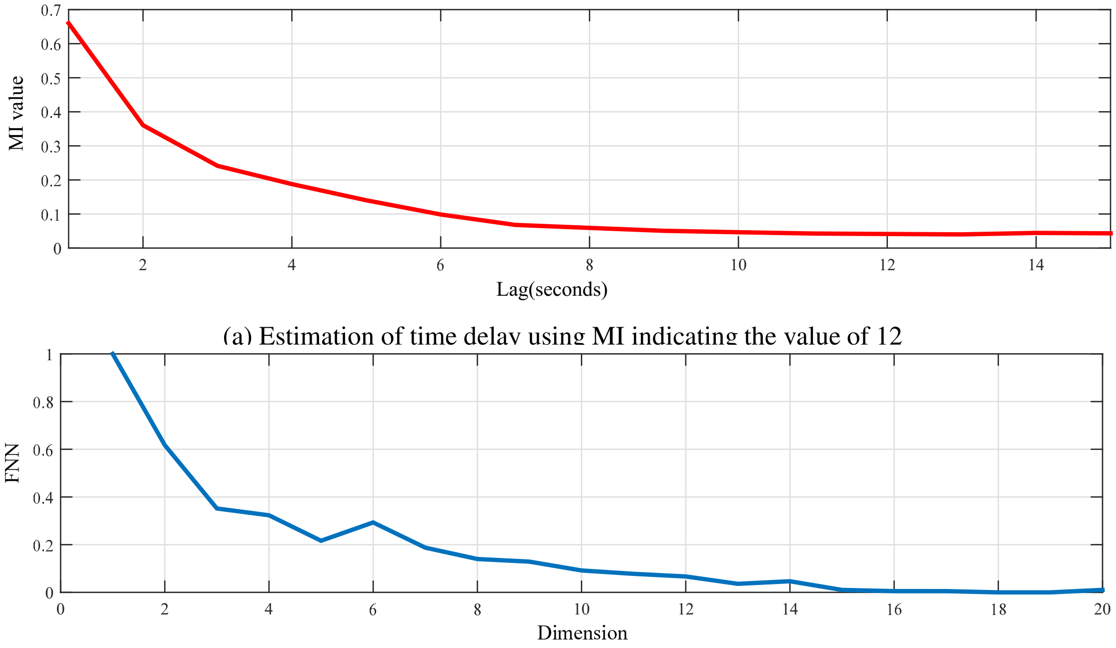
(b) Histogram for 2804:14d:9083::/48

(c) FFT for 2804:14d:9083::/48

(d) ACF for 2804:14d:9083::/48

Figure 4.15: Histogram, FFT, and ACF for 2804:14d:9083::/48

modelling BGP speaker as a dynamic system based on phase space trajectory. As before we use the underlying time series to calculate time delay and embedding dimension. Based on values of MI and FNN shown in Figure 4.16, we use the value of 12 and 3, the first minimum values of MI and FNN, for time delay and embedding dimension respectively.



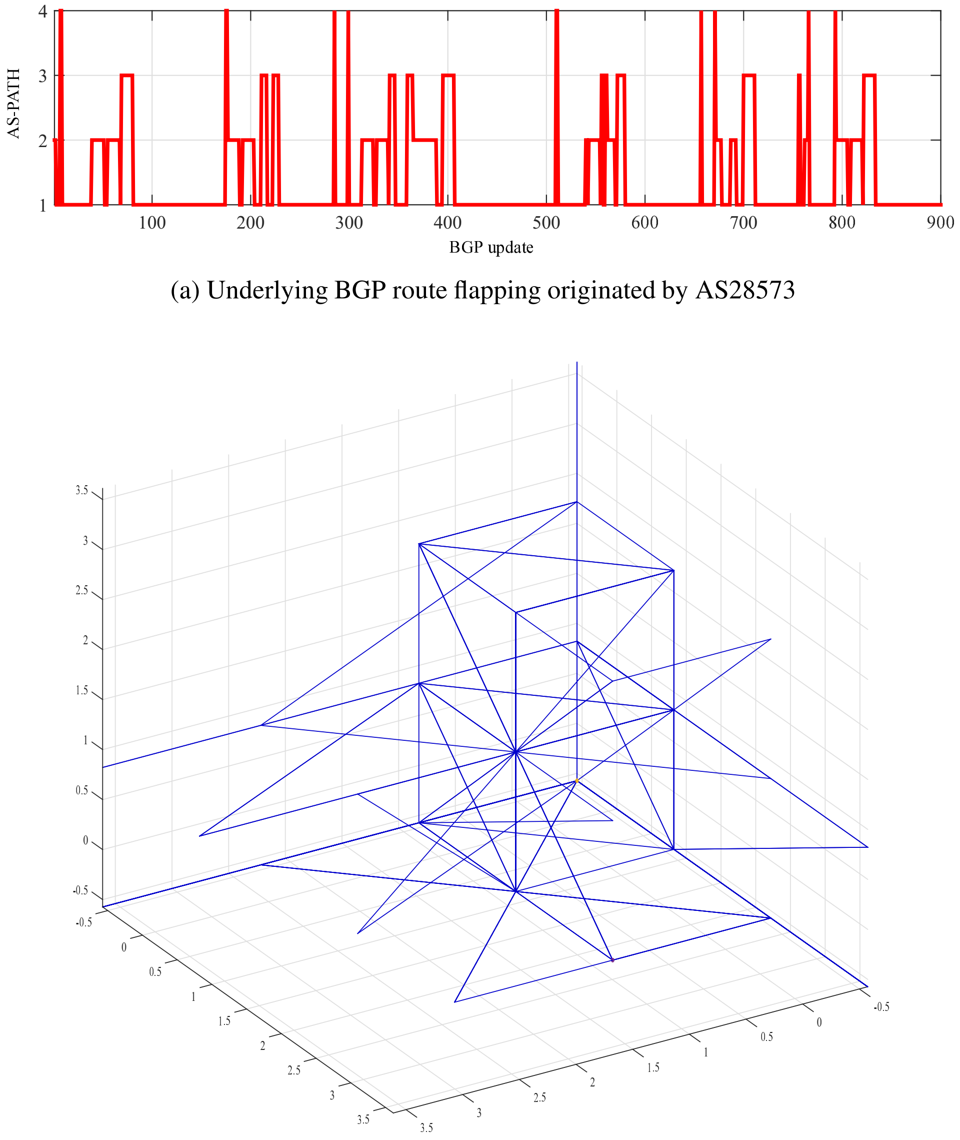
(a) Estimation of time delay using MI indicating the value of 12

(b) Estimation of embedding dimension using FNN indicating the value of 3

Figure 4.16: Time delay and embedding dimension for BGP route flapping of AS28573

The phase space trajectories for BGP route flapping originated by unstable AS28573 and collected from the peer AS12859 are shown in Figure 4.17 where we can see the system exhibits different cycles that recur repeatedly. Once again, we use Lyapunov exponents to estimate type of motion. Figure 4.18 shows Lyapunov exponents for BGP route flapping originated by the unstable AS28573 where the slope value around zero indicates a stable system. In addition to characterising the behaviour of stability for BGP route flapping, we estimate the characteristics of determinism and non-linearity using DVV as shown in Figure 4.19. The interpretation of scatter diagram and DVV plot shows the system has, once again, the characteristics of determinism and non-linearity.

We have shown that BGP route flapping sent by a BGP speaker appears to have the characteristics of stability, determinism, and non-linearity. Based on these observations, we can use an RP to visualise the time-dependent behaviour of the route flapping. Figure 4.20 shows a sample of BGP route flapping originated by the BGP speaker AS28573 and its corresponding representation of RP.



(a) Underlying BGP route flapping originated by AS28573

(b) Phase plane representation for BGP route flapping by AS28573 using time delay=12

Figure 4.17: BGP route flapping originated by AS28573 and its corresponding representation of phase space

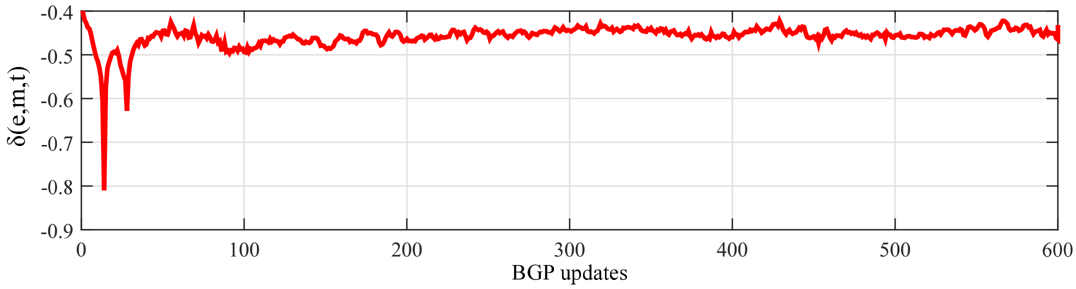
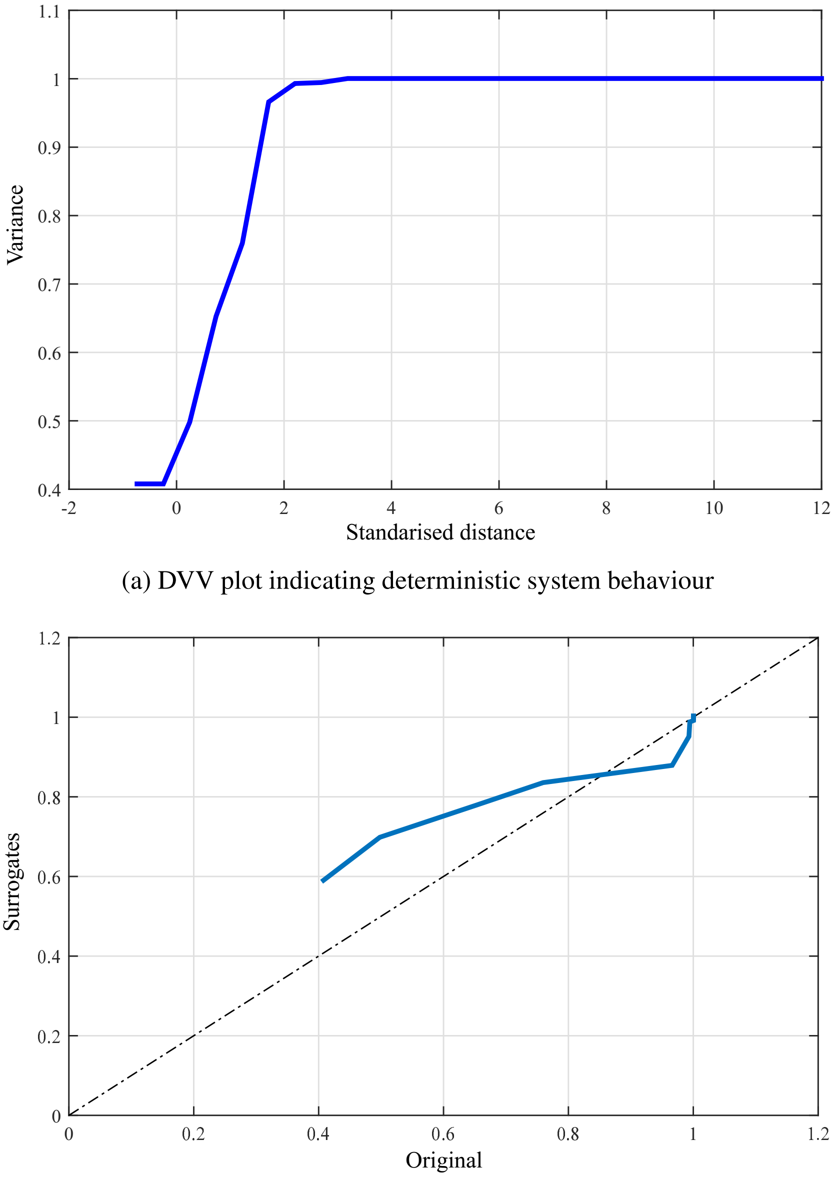


Figure 4.18: Lyapunov exponents for BGP route flapping originated by AS28573

In the RP shown in Figure 4.20b we can see short diagonal lines indicating brief or transient periodicity. This representation supports our analysis of a periodic behaviour for BGP route flapping associated with individual prefixes of unstable ASes. Rectangular boxes formed by vertical and horizontal lines recur with different scales. For example, looking at rectangular highlighted boxes along the LOI in Figure 4.21 we can see how recurrence behaviour is exhibited with time. In this example, the highlighted boxes represent RP for BGP updates 0-200 and 330-530 for the underlying BGP route flapping shown in Figure 4.20a. The outcome of our demonstration for RP representation of BGP route flapping shows, once again, although BGP route flapping appears random, it has the characteristics of recurrent behaviour. This behaviour was not apparent using linear statistical analysis such as ACF and FFT.

Our analysis shows that much of the background traffic of BGP sent by the peer AS which collected that largest volume of BGP traffic, whether it is calculated per second or per AS-PATH, is made of unsynchronised oscillations from different ASes of different frequencies. Our analysis shows unstable ASes generate approximately periodic updates but with different frequencies. The unsynchronised aggregation of different periodic updates leads to recurrent behaviour in the underlying system.

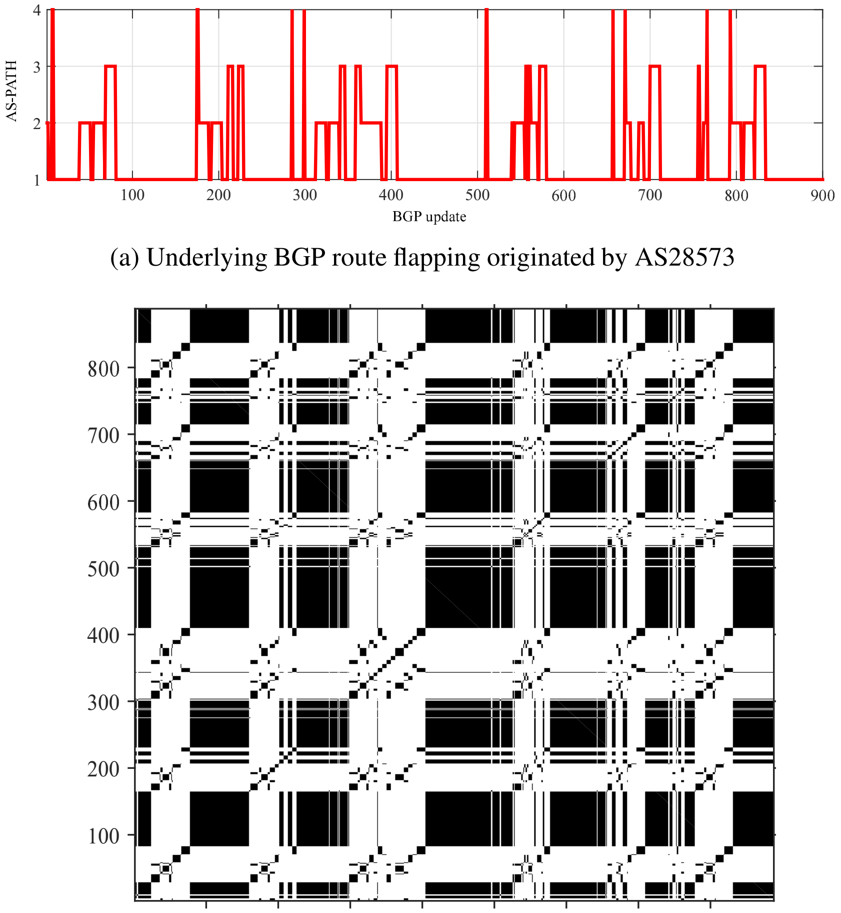
In addition to the recurrent behaviour, the volume of data to be analysed in BGP updates per AS-PATH form is very large compared to total number of BGP updates per second. For example, for the same BGP updates sent by the peer AS12859 during the period 18th to 25th of July 2016, the length of the data in BGP update per AS-PATH is 7904815 updates while it is 604800 seconds in the BGP updates per second form, more than 13 times larger. Therefore, we will use the form of BGP updates calculated every second as a default representation for our analysis on BGP traffic. In the next section, we will explore the characteristic of periodicity for BGP traffic calculated each second in more detail. This includes examining BGP traffic for multiple unstable ASes on different dates and discussing different sources of periodicity. Our interest is the characteristic of periodicity due to a small number of specific unstable ASes or is it a persistent behaviour for all unstable ASes?



(a) DVV plot indicating deterministic system behaviour

(b) Scatter diagram indicating non-linear system behaviour

Figure 4.19: Estimation of determinism and linearity for BGP route flapping originated by AS28573



(a) Underlying BGP route flapping originated by AS28573

(b) RP representation for BGP route flapping originated by AS28573

Figure 4.20: Identifying recurrence behaviour for BGP route flapping originated by AS28573

## 4.5 Persistence of BGP activity

We have shown in Section 4.3.1 and [8] that BGP traffic for unstable ASes is approximately periodic with unsynchronised oscillations as seen from the peer AS that sent the largest volume of traffic in one VP. In this section, we go further to investigate if we can still see this behaviour from multiple VPs, how long this periodicity continues, is this behaviour persistent as a part of BGP behaviour or has it appeared recently for some reasons? To answer these questions, we analyse BGP traffic collected from different VPs at different times as will be discussed in the next subsections.

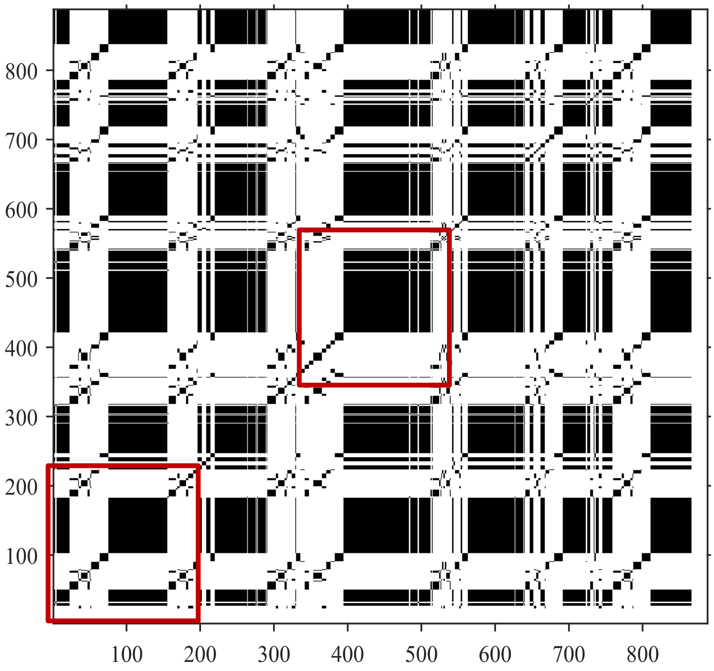


Figure 4.21: Exhibition of recurrence behaviour for BGP route flapping of AS28573

### 4.5.1 Investigating periodicity for one week of BGP traffic

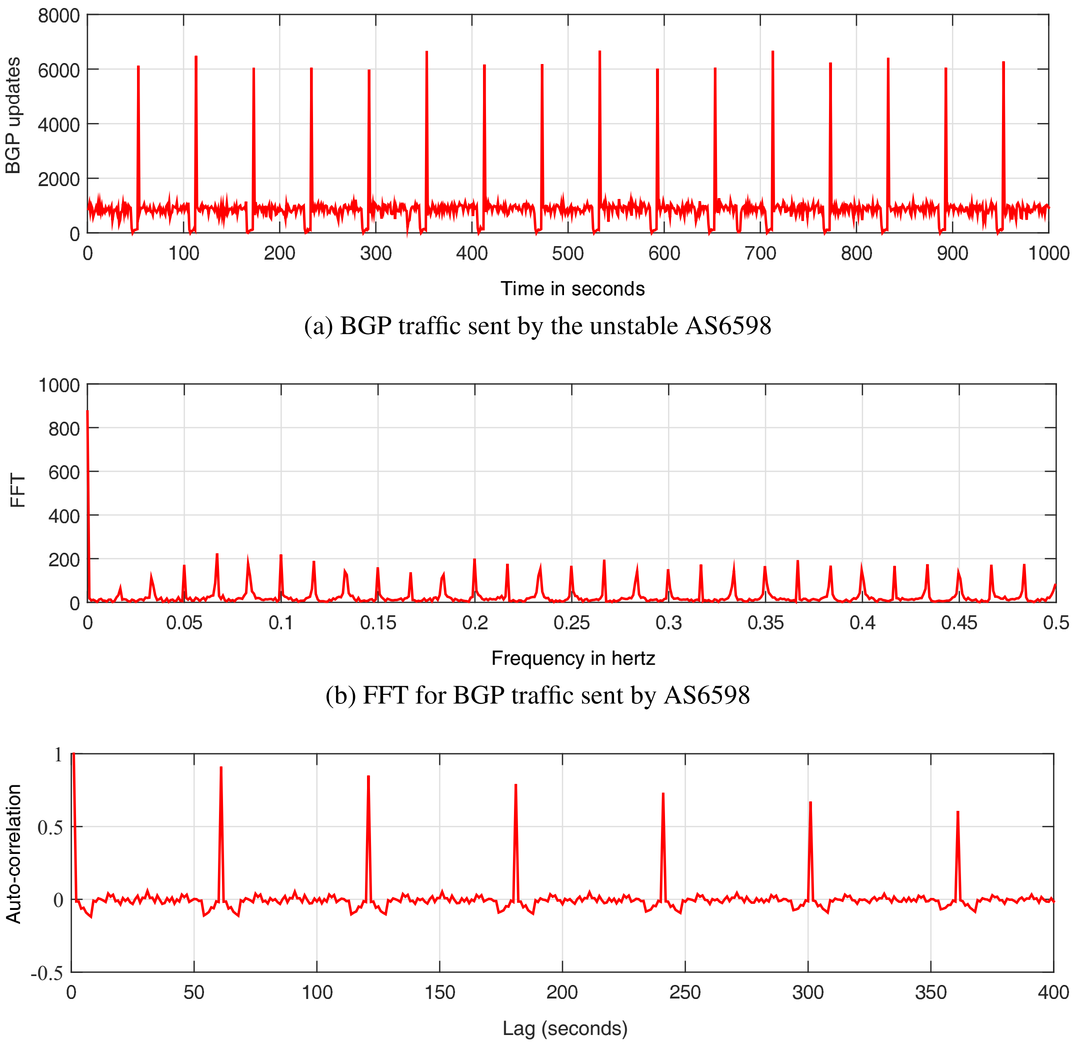
In this subsection, we investigate the periodicity in BGP traffic collected from all VPs at the RIPE NCC during one week. The aim of this analysis is to explore whether we can still see the periodic behaviour at multiple VPs or just limited to the VP rrc03. The RIPE NCC has 14 active VPs as observed during the period of 19-25 July 2016. Each of these VPs has a different number of peers. For example, VP rrc03 had 30 peers on July 19th 2016. Table 4.1 shows the location of VPs, total number of peers, and total number of BGP updates collected per VP between July 19th and 25th 2016. Most BGP updates collected at RIPE NCC VPs share BGP updates sent from the same active ASes as highlighted in the bold font shown in Table 4.1. This outcome supports the conclusions by [67] where the authors show that most of BGP traffic contain BGP updates related to a few number ASes. For example, AS28573 has been seen among the most active ASes in all VPs except the VP rrc15 which is located in Brazil.

Although the VP rrc15 does not have the largest number of peers as shown in Table 4.1, it collected the largest number of BGP updates. The analysis on this VP shows that some active ASes sent a significant volume of BGP messages consisting of an announcement followed soon by another announcement for the prefix but with a different path. For example, AS6598 and AS24427 sent 172814690 (20 GB of BGP updates) and 139360416 (17 GB of

Table 4.1: Top ten active ASes during 19/7/2016 to 25/7/2016 at RIPE NCC

| ID | VP | Location | No. of Peers | No. of Updates | Top Ten Active ASes |
|---|---|---|---|---|---|
| 1 | rrc00 | RIPE NCC, Amsterdam, Netherlands | 117 | 56607624 | **9829**, **28573**, **17908**, **29084**, 38841, **23911**, **56237**, **4755**, 45820, **45292** |
| 2 | rrc01 | LINX, London, UK | 91 | 49691008 | **28573**, 1132, **9829**, **29084**, **4755**, **17908**, **45292**, **56237**, 45271, **23911** |
| 3 | rrc03 | AMS-IX, Amsterdam, Netherlands | 154 | 61387387 | **28573**, **9829**,55430, **56237**, **17908**, **45292**, 46652, **4755**, 198171, 36943 |
| 4 | rrc04 | CIXP, Geneva, Switzerland | 85 | 309426550 | **9829**, **28573**, 11664, 18196, **29084**, 15964, 23487, **23911**, 12252, 19429 |
| 5 | rrc05 | VIX, Vienna, Austria | 118 | 33125632 | **28573**, **9829**, 18403, **56237**, **29084**, **45292**, 198171, 174, 3651, 22394 |
| 6 | rrc06 | JPIX, Otemachi, Japan | 77 | 10537831 | 11139, **28573**, **9829**, **4755**, **29084**, **17908**, **23911**, 52145, 45820, 45194 |
| 7 | rrc07 | NETNOD, Stockholm, Sweden | 80 | 44990945 | **28573**, **17908**, **4755**, **9829**, **56237**, **45292**, 11139, 45820, 38841, 46573 |
| 8 | rrc10 | MIX, Milan, Italy | 85 | 55015019 | **28573**, **9829**, **29084**, 55430, **4755**, **17908**, **45292**, **56237**, **23911**, 45194 |
| 9 | rrc11 | NYIIX, New York, USA | 86 | 63104404 | **28573**, 18403, **17908**, **9829**, **29084**, **56237**, **4755**, 38841, **45292**, 52145 |
| 10 | rrc12 | DE-CIX, Frankfurt, Germany | 127 | 115294534 | **28573**, **9829**, **45292**, **4755**, **56237**, **17908**, 16652, 198171, **23911**, 46044 |
| 11 | rrc13 | MSK-IX, Moscow, Russia | 75 | 53865912 | **28573**, **9829**, **17908**, **4755**, 38841, **45292**, **23911**, **56237**, 45820, 45194 |
| 12 | rrc14 | PAIX, Palo Alto, USA | 102 | 46854297 | **28573**, **4755**, **9829**, **17908**, 18196, 45820, **29084**, **23911**, 46573, 16652 |
| 13 | rrc15 | PTTMetro-SP, Sao Paulo, Brazil | 80 | 714338144 | 6598, 24427, 1118, 29337, 35894, 62638, 45177, 59891, 62943, 35908 |
| 14 | rrc16 | NOTA, Miami, USA | 54 | 23496781 | **28573**, **9829**, 38841, **4755**, **17908**, **29084**, 45820, **56237**, **45292**, 46573 |

BGP updates) of BGP updates respectively during one week. This significant volume of BGP messages is an announcement followed soon by an update message for only 35 prefixes (all IPv4 prefixes) owned by AS6598 and 33 prefixes (all IPV4 prefixes) owned by AS24427. Figure 4.22 shows total number of BGP updates calculated every second sent by AS6598 as observed by peer AS16735 at VP rrc15 and its corresponding values of FFT and ACF where we can see a very strong periodicity in BGP traffic sent by the active noisy AS6598.

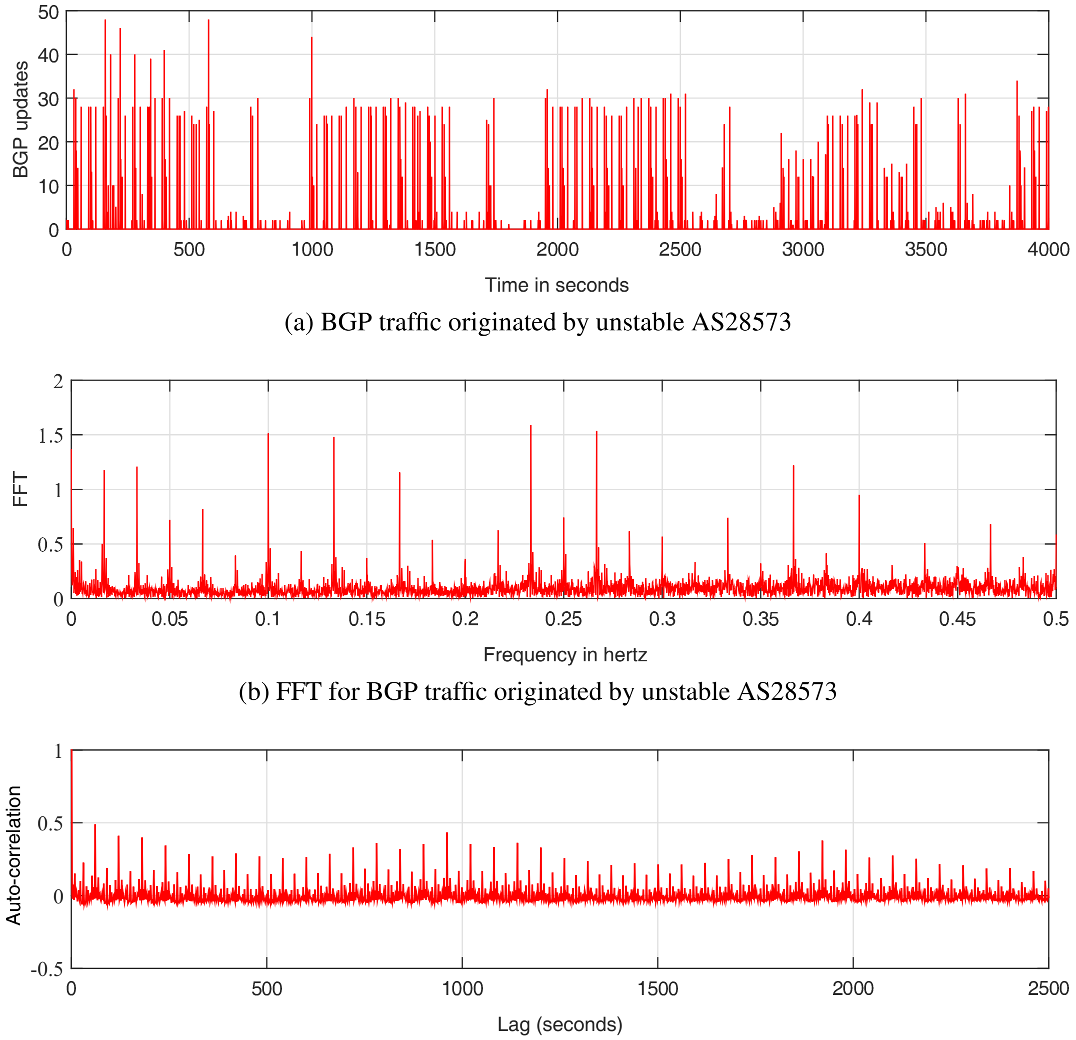


(a) BGP traffic sent by the unstable AS6598

(b) FFT for BGP traffic sent by AS6598

(c) ACF for BGP traffic sent by AS6598

Figure 4.22: BGP traffic volume sent by AS6598 and its corresponding values of FFT and ACF



(a) BGP traffic originated by unstable AS28573

(b) FFT for BGP traffic originated by unstable AS28573

(c) ACF for BGP traffic originated by unstable AS28573

Figure 4.23: BGP traffic originated by AS28573 and its corresponding ACF and FFT

Figure 4.23 shows a sample of BGP traffic originated by the unstable AS28573 and collected by the VP rrc03 and its corresponding of the FFT and ACF. In this figure, we can see multiple scales of periodicity with the smallest period 60 seconds and the largest 960 seconds[3]. In this example, we can see periodicity is less pronounced than what we can see in Figure 4.22. This is due to the number of AS-PATHs between unstable AS and the vantage point. BGP traffic of unstable AS28573 travelled through 32 different AS-PATHs while BGP traffic related to unstable AS6598 traveled through only two AS-PATHs.

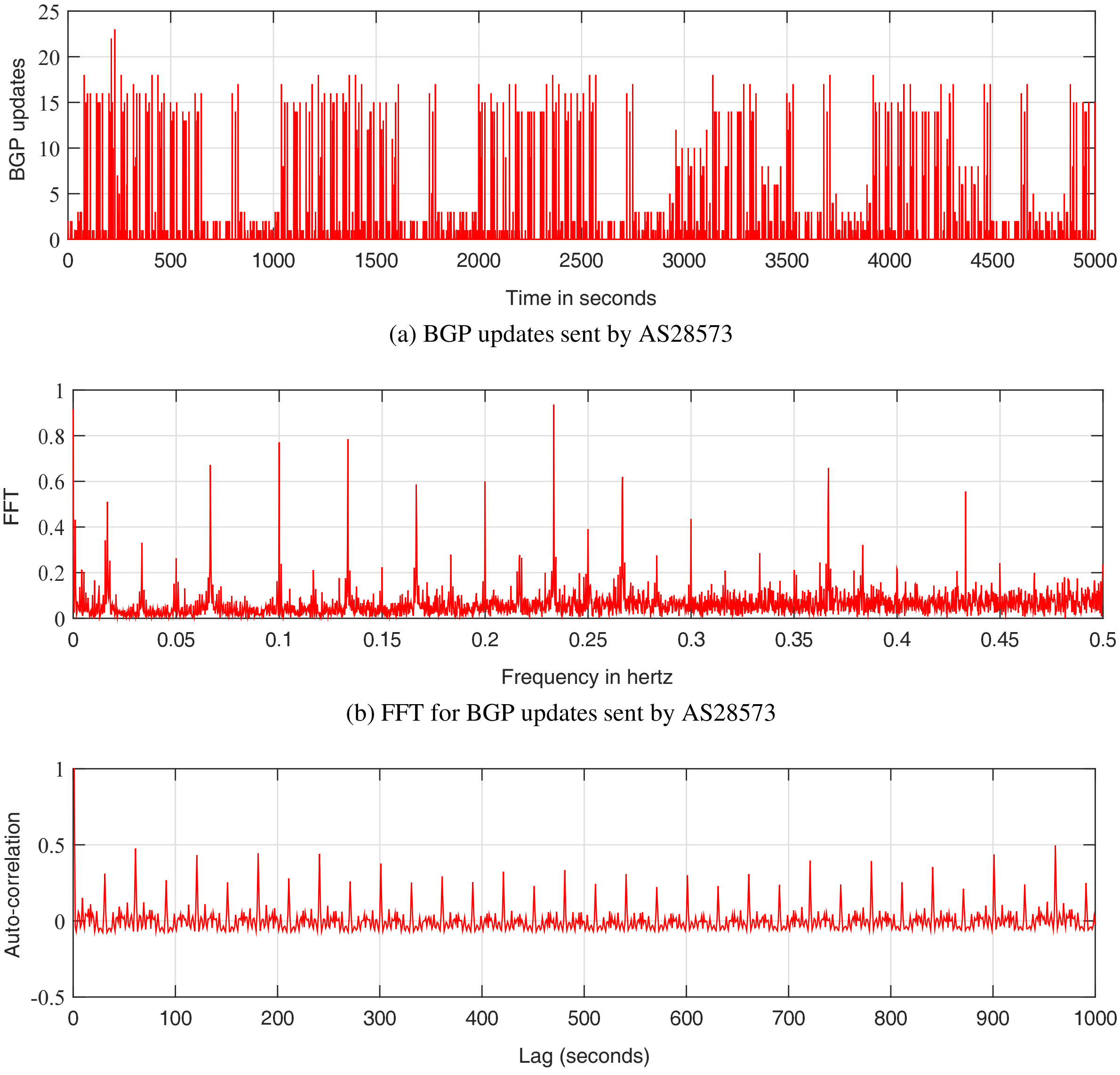
In total, we have analysed 1.638 billion BGP updates collected at all active VPs of RIPE NCC during the period of 19-25 July 2016. During the analysis period, we can still see periodic behaviour at multiple VPs ranging from very strong to weak or unclear depending on the length of paths between the active ASes and the VPs.

### 4.5.2 Investigating active ASes for past ten years

In this subsection, we carry out further investigations on BGP updates by analysing collected BGP traffic for the past ten years. Our interest in this investigation is to explore the active noisy ASes. Are these active ASes continuing with their behaviour or do they stop and other ASes appear? In other words, is the characteristic of periodicity due to a small number of specific unstable ASes or is it a persistent behaviour for all unstable ASes?

We sample data by examining the most active ASes on the 1st of June of every year during the period 2006-2015. The top ten active ASes during this period have been calculated based on VPs that collected the largest number of BGP updates compared to other VPs on that date. For example, the VP rrc03 has been selected as it collected the largest number of BGP updates during the 1st of June 2006 compared to other VPs. Table 4.2 shows the selected VP, the number of collected BGP updates and top ten active ASes during the period 2006-2015. This table shows that some of these active ASes which are highlighted in bold continued for multiple years such as AS9829 and AS8402 while other ASes appeared in a short period of time such as AS15491 and AS9121. Our analysis to the top ten unstable ASes during the period 2006-2015 shows although there are many unstable ASes lasted for a short period of time, many showed a periodic behaviour. For example, BGP traffic sent by the active AS28573 during the 1st of June 2015 shows a clear periodic behaviour as shown in Figure 4.24.

[3] The value of 960 seconds is a result of configuring Route Flap Damping (RFD) mechanisms in one of ASes in the AS-PATH to limit propagation of unstable routes.



(a) BGP updates sent by AS28573

(b) FFT for BGP updates sent by AS28573

(c) ACF BGP updates sent by AS28573

Figure 4.24: BGP updates sent by AS28573 and its corresponding of FFT and ACF

Table 4.2: Top ten active ASes during 2006-2015

| Year | VP | No. of Updates | Top Ten Active ASes |
|---|---|---|---|
| 2006 | rrc03 | 14193568 | 15270, 15105, 4134, 9121, 6983, 20141, 26407, 17785, 25994, and 4193 |
| 2007 | rrc12 | 6495115 | 16322, 9583, 25306, 8151, 2697, 13311, 7018, 23966, 24326, and 5800 |
| 2008 | rrc03 | 8125184 | 6389, 8866, 4323, 9583, 2386, 4755, 9498, 11492, 7018, and 31003 |
| 2009 | rrc12 | 3071880 | 9198, 8103, **9829**, 21491, 47408, 14846, 7753, 1221, 4802, and 17676 |
| 2010 | rrc01 | 5209999 | **9829**, 32528, 8865, 8452, 13193, 35805, 17974, 34337, 37204, and 28052 |
| 2011 | rrc12 | 6445955 | 9430, **9829**, 27738, 11492, 6389, 24560, 19743, 3462, 27065, and 17974 |
| 2012 | rrc13 | 6159786 | 8926, 3549, 8452, 9482, 18101, **9829**, 1257, 29049, **8402**, and 17813 |
| 2013 | rrc01 | 5688131 | 36998, 9304, 33920, 4538, **8402**, 18403, 27738, 31148, 27884, and 24835 |
| 2014 | rrc12 | 7349238 | 7545, **9829**, 23752, 262287, 7579, **8402**, 45899, 28573, 41691, and 9808 |
| 2015 | rrc12 | 12615410 | 28709, 28573, **9829**, 23752, 45899, 61570, 54169, 15491, 39891, and 22059 |

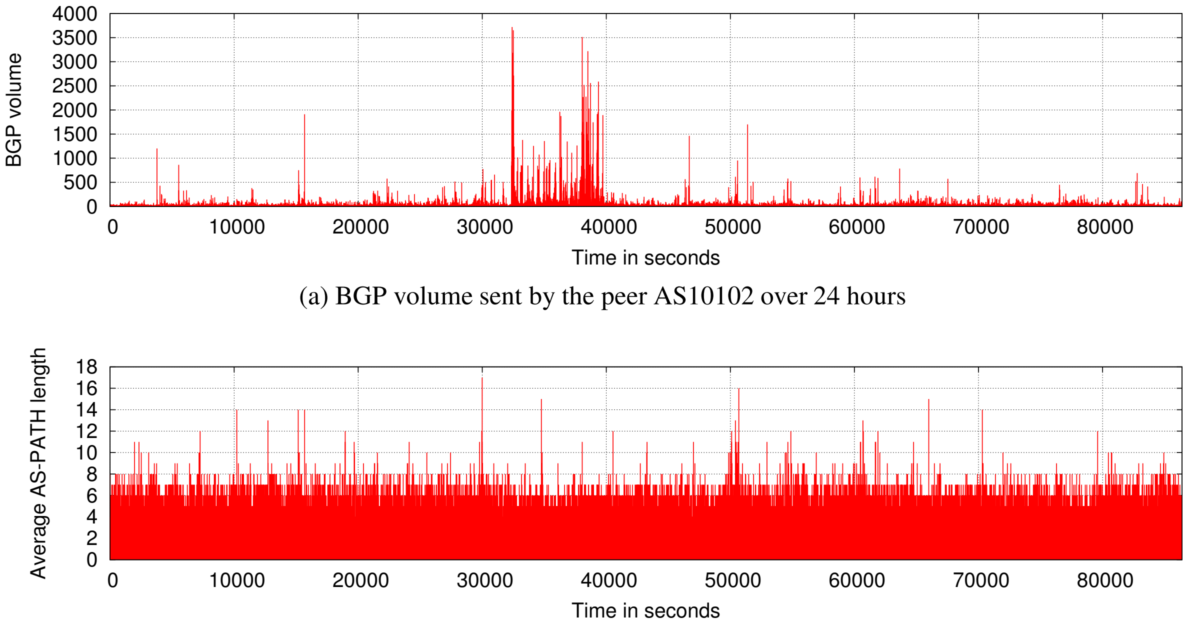
Our statistics for ten years of BGP traffic suggests the characteristic of periodicity in BGP traffic is part of underlying BGP traffic. Although some active noisy ASes persisted for many years and others lasted for a short time, we still can see the periodic behaviour for BGP traffic sent by these ASes. BGP traffic generated by active ASes has the effect of masking anomalous traffic that indicates potentially harmful accidental or deliberate anomalies. A technique is needed that can rapidly distinguish between normal background and potentially harmful traffic. We have shown in Section 4.3.2 that RP can be used to identify the characteristic of recurrence behaviour in the underlying BGP traffic volume. However, as highlighted in Section 3.4 that RP cannot be directly used in real-time anomaly detection. RQA can be used for that purpose. In the next section, we use RQA to detect anomalous periods that identify anomalies in a series of unstable BGP traffic. In the next section, we use RQA to detect anomalous periods that identify anomalies in a series of unstable BGP traffic.

## 4.6 Identifying BGP anomalies during the TMnet incident

In this section, we show how RQA can be used to differentiate between unstable BGP traffic generated by active ASes and anomalous BGP traffic generated by different types of BGP anomalies. Our approach makes use of RQA by first extracting BGP features and then calculating RQA measurements based on those features. Significant variations in the RQA measurements indicate a change in normal behaviour that represents BGP anomaly. As discussed before in Section 2.2.6, there are many BGP features can be extracted from a series of BGP updates. However, we have modelled BGP speakers as dynamic systems send BGP updates and path lengths based on BGP updates received from neighbours and local routing policies.

Changes in BGP speaker behaviour of sending a number of BGP updates and path lengths can be used as an indicator to detect anomalous behaviour. Therefore, we use BGP volume (total number of announcements and withdrawals) and average AS-PATH length calculated every second as BGP features in our approach.

To evaluate RQA capability to indicate BGP anomalies, we use BGP updates related to BGP events. TMnet is one of the most recent incidents of BGP anomalies was observed on the 12th of June 2015 by Telekom Malaysia (TMnet). It is an example of direct unintended BGP anomalies 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 [124]. In the next chapter we look at other events and evaluate the effectiveness of RQA in greater depth.

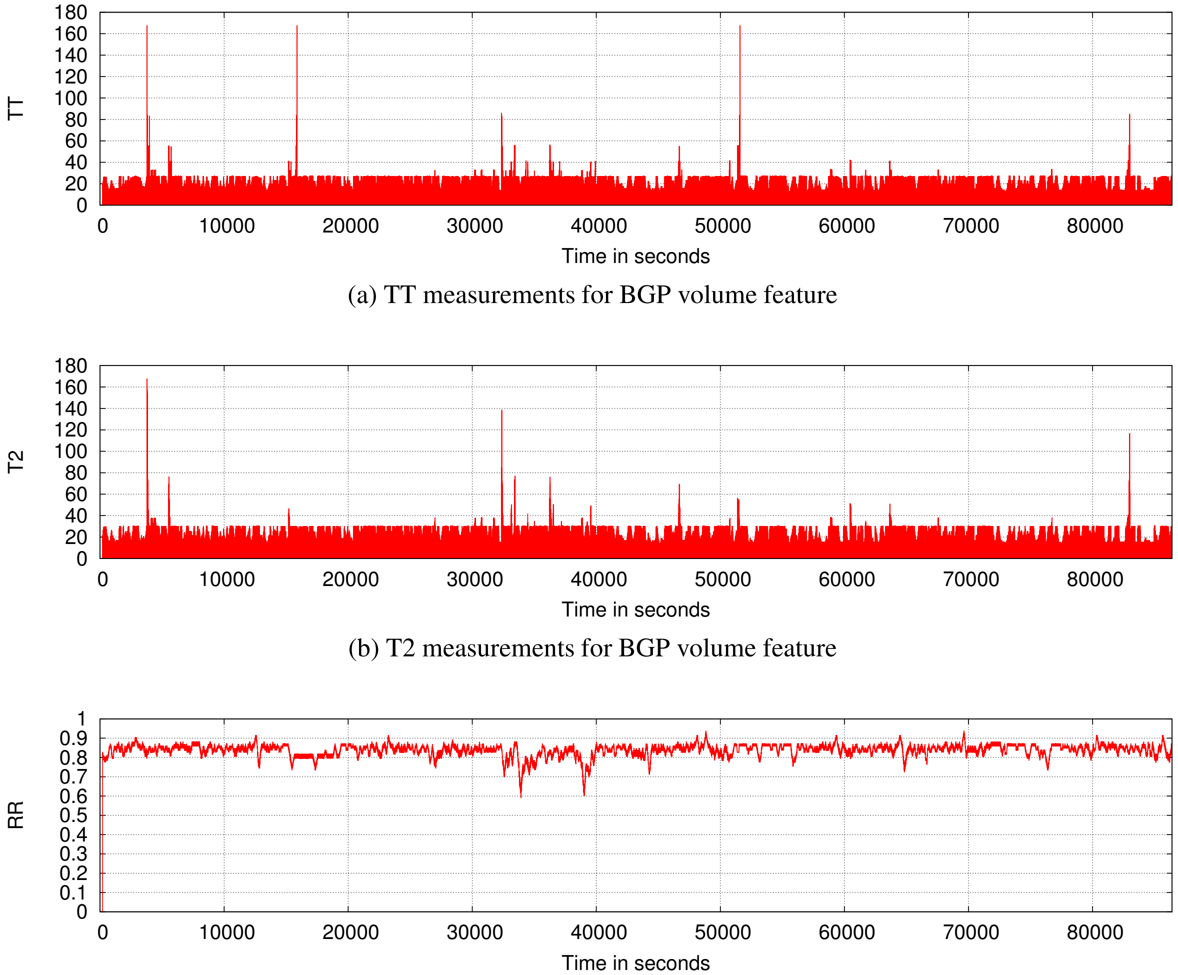


(a) BGP volume sent by the peer AS10102 over 24 hours

(b) Average AS-PATH length for BGP traffic sent by the peer AS10102 over 24 hours

Figure 4.25: BGP features sent by the peer AS10102 during TMnet event

Figure 4.25 shows BGP volume and average AS-PATH length features calculated every second where we can see a significant increase in number of BGP updates during the event. The peer AS10102 sent multiple high volume of BGP updates such as during the periods 3750-5600 seconds and 15100-15700 seconds before continued to sent a significant volume of BGP updates during the period 30000-40000 seconds. TT and T2 measurements can identify these periods of anomalous behaviour in term of BGP volume traffic using only 200 seconds of past BGP updates as shown in Figure 4.26[4]. RQA can also detect other types of anomalous behaviour which cannot be observed from a simple observation. For example, during the period 33700-33900 seconds there is no significant change in the BGP volume neither average AS-PATH length as shown in Figure 4.27 but RQA measurements show a significant change. The source of this change is abnormal behaviour in term of the interval for sending BGP updates or the behaviour of MRAI starting after time 33000 seconds as shown in Figure 4.27a.



(a) TT measurements for BGP volume feature

(b) T2 measurements for BGP volume feature

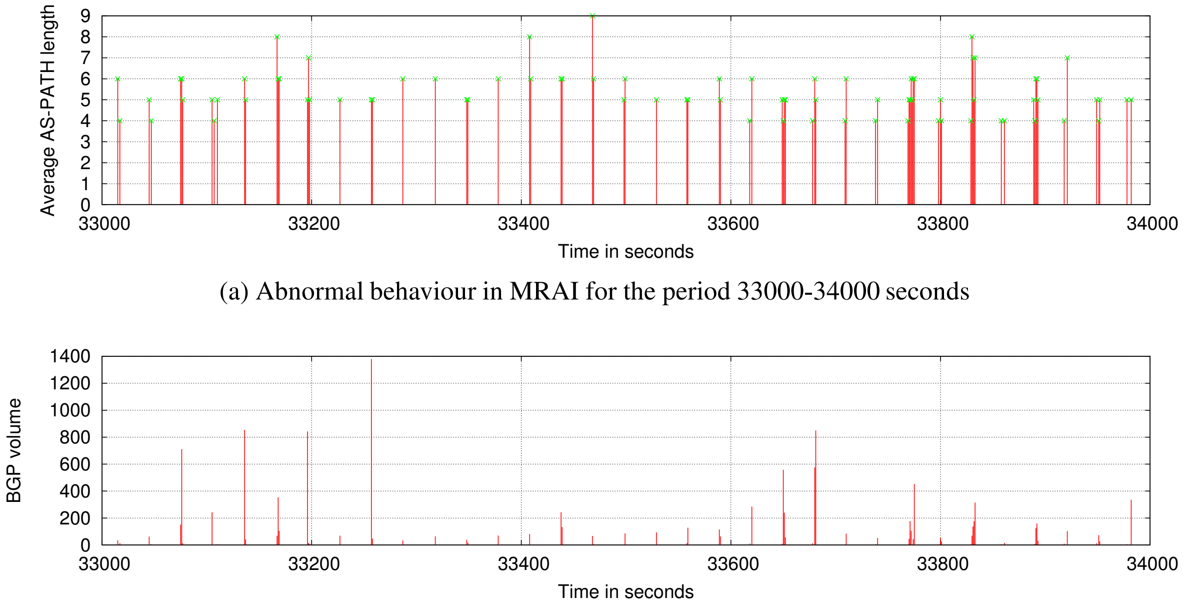
(c) RR measurements for average AS-PATH length feature

Figure 4.26: RQA measurements during TMnet event

In this section, we introduced our RQA approach to indicate BGP anomalies using one of the most recent BGP events. RQA is able to differentiate between unstable BGP traffic and anomalous traffic that identifies anomalies. RQA is also able to disclose otherwise hidden

[4] More analysis for selected the period of past BGP updates and optimal RQA measurements to detect BGP anomlies with low rates of FP and FN will be discussed later in Chapter 5.

information related to the anomaly such as changes in the frequency of updates. Further details about detection delay and FP and FN rates will be discussed in the next chapter.



(a) Abnormal behaviour in MRAI for the period 33000-34000 seconds

(b) BGP volume feature during the period 33000-34000 seconds

Figure 4.27: Hidden anomalous behaviour during TMnet event

## 4.7 Conclusions

BGP updates are sent to reflect changes in network topology or policies change. Any BGP activity that does not contribute to business goals of an organisation or undermines them can be considered anomalous. However, real-world BGP update traffic is of a substantial volume that is much larger than might be expected. There is a set of unstable ASes that send BGP traffic consisting of route announcements followed soon after by withdrawals that do not appear related to underlying network management decisions or events. The process of identifying anomalous BGP traffic in the presence of unstable BGP traffic is difficult because the unstable BGP traffic has the effect of masking anomalous traffic.

In this chapter, we have shown that unstable BGP traffic has the characteristics of a periodic behaviour with different frequencies. The characteristic of periodicity in BGP traffic is part of BGP behaviour. Although some unstable ASes persisted for years and other for months, we still can see this periodicity in BGP traffic. However, the aggregated BGP traffic for all unstable ASes does not show a structure of a periodic behaviour. Using the concepts of phase plane trajectories, we show the aggregated BGP traffic has the characteristics of recurrence, determinism, non-linearity, and stable behaviour. Built on this insight, we demonstrate that RQA, an advanced non-linear analysis technique based on a phase plane trajectory, may be able to differentiate between unstable traffic and anomalous traffic that identifies BGP anomalies. Using one of the most recent BGP anomalies, we showed that RQA is able to detect anomalous behaviour that indicates BGP anomalies as well as hidden anomalous behaviour that may otherwise pass without observation, as shown in Figure 4.27. In the next chapter, we will evaluate RQA's ability to detect BGP anomalies. We will also identify the most effective RQA measurements and investigate the selection of the optimal values of the window size that can produce low rates of FP and FN.

# Chapter 5

# Detecting BGP anomalies using RQA

## 5.1 Introduction

When BGP was developed, trust between its participants was assumed. Consequently, it includes few security mechanisms and so is vulnerable to different types of events. In the years since it was deployed, many types of these have been recorded such as BGP misconfiguration and link or node failure. The consequences of these events can range from a single to thousands of anomalous BGP updates. As highlighted in Section 2.3, a single BGP update is categorised as anomalous if it originated from an illegitimate or invalid AS while a set of BGP updates are categorised as anomalous if there is a significant change in the number of BGP updates, a significant change in the AS-PATH length or changes in the behaviour of total BGP updates over time. Our interest is in the later. In particular, we detect BGP anomaly at BGP speaker level using a series of BGP updates sent by the BGP speaker.

We have shown in the previous chapter that RQA can differentiate between normal but unstable BGP traffic and anomalous traffic. Using one of the most recent well-known BGP events as an example, we showed how RQA can distinguish BGP anomalies from unstable BGP traffic and indicate hidden anomalous behaviour that may otherwise pass without observation. In this chapter, we introduce an RQA based scheme to detect BGP anomalies and we then discuss our scheme's design in detail. We also investigate the most effective RQA measurements and the optimal values for RQA scheme parameters that produce a high detection rate and low detection delay.

In the years since it was deployed, many types of anomalies have threatened BGP stability such as TTNet misconfiguration, Nimda, and the Moscow blackout. Although many researchers have analysed these events such as [62] and [66] using BGP data from the events to evaluate their approaches, there is still a lack of ground truth data for these events. This issue represents a challenge to almost all network anomaly detection work [160]. In BGP, there is a lack of time stamps for these events. For example, what time in seconds did an event start? Furthermore, there might be other BGP anomalies that have not been reported or noticed [32]. Our approach is to use a network testbed in which synthetic anomalies are generated and then confirming against well-known BGP events. Nevertheless, we acknowledge that synthetic events are an approximation only to the ground truth. Our BGP testbed uses the Virtual Internet Routing Lab (VIRL) [5], a powerful network emulation platform developed by Cisco, and BGP Replay Tool (BRT) [2], a tool that we developed to replay past BGP updates. We use the results obtained from the testbed to evaluate and choose our scheme parameters and select the most effective RQA measurements that best identify BGP anomalies.

We run our RQA scheme using 1233790 seconds (14.28 days or 342.72 hours) of BGP traffic collected from our controlled testbed and different types of well-known BGP events. These include Nimda as an example of indirect BGP anomaly, Moscow blackout as an example of link failure, and TTNet and TMnet as examples of direct unintended BGP anomaly. Our detection scheme can detect all the introduced BGP anomalies in our testbed (12 emulated BGP anomalies) and the well-known BGP events as well as hidden anomalous behaviour in the underlying BGP traffic. This hidden anomalous behaviour represents an early stage of BGP anomalies which the RQA scheme can identify. To evaluate our RQA scheme for detecting BGP anomalies, four main metrics have been used. These are True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN). TP refers to numbers of anomalies that are classified as anomalies while TN refers to numbers of normal events that are classified as normal. FP refers to normal events that are classified as anomalous while FN refers to anomalous events that are classified as normal. The evaluation of RQA scheme using 14.28 days of BGP traffic shows its ability to detect 46 TP alarms with 5 FP alarms detected within 62 seconds as a detection delay.

The rest of this chapter is organised as follows: in Section 5.2, we introduce our controlled testbed where we synthesise unstable BGP traffic and introduce anomalies. Section 5.3 describes the design of our RQA based scheme for detecting BGP anomalies. In Section 5.4, we discuss the selection of the optimal values of our detection scheme and the most effective RQA measurements to produce high accuracy detection. We evaluate the accuracy of our scheme using the past and emulated BGP anomalies in Section 5.5. Finally, we conclude our chapter in Section 5.6.

## 5.2 Indicating BGP anomalies using RQA-testbed

In this section, we address the problem of obtaining ground truth of anomalous BGP events. Such information is necessary for an evaluation of our approach to detecting BGP anomalies.

For that purpose, we introduce a controlled BGP testbed using the VIRL [5] and BRT [2]. VIRL is a network emulation system uses Linux KVM hypervisor, OpenStack, and a set of virtual machines running real Cisco network operating systems [5]. BRT is a tool to replay past BGP updates [2], described in Appendix A.

We use the topology shown in Figure 5.1, which has been used in previous work to emulate a small Internet [161], to evaluate our scheme. This topology enables all BGP routers, except as200r1, to receive the injected BGP traffic via different AS-PATHs. For example, as30r1 can receive the injected BGP traffic via as1r1, as300r1, and as20r1. In this topology, each router runs Cisco IOSv 15.2(2)T. We also use two virtual machines running Ubuntu 14.04.2 LTS operating system. The first virtual machine is used to feed BGP updates into as40r1 using BRT while the second virtual machine works as a Remote Route Collector (RRC) to collect BGP data from several VPs. RRC requires Quagga, a routing software package that provides TCP/IP based routing services for different protocols such as OSPF, RIP, and BGP [162]. In the topology shown in Figure 5.1, we do not use any BGP policies except at the collecting points to avoid these collectors from working as a transit between ASes. To collect BGP updates from different VPs, RRC is peered with as20r1, as30r1 and as300r1. RRC also runs our scheme to detect BGP anomalies.

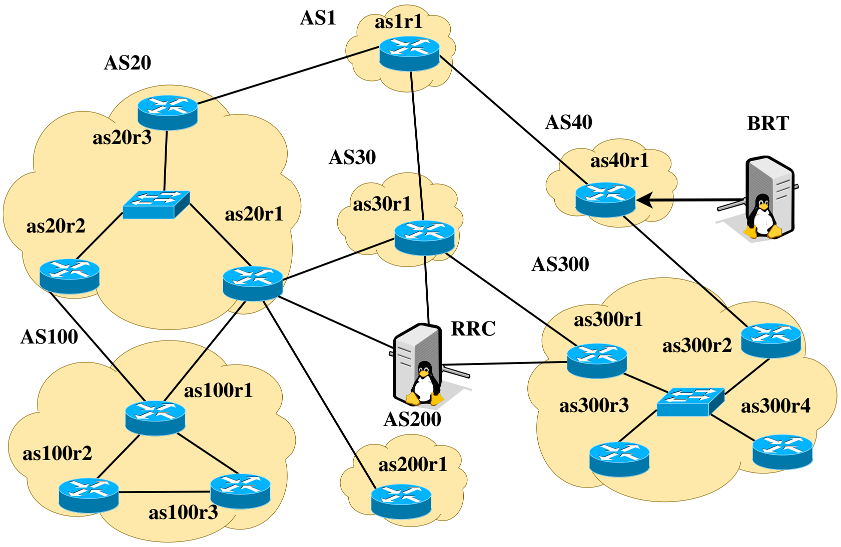


Figure 5.1: Testbed topology

We have shown in Section 4.3 that unstable BGP traffic appears to be an aggregation of oscillations of different frequencies from a set of unstable ASes. In our testbed, we synthesise this traffic by generating a series of prefixes belonging to different ASes that periodically announce then withdraw updates at regular time intervals. We then introduce an anomaly by shutting down an AS as an example of node failure.

We carry out two types of experiments using our controlled testbed. In the first experiment, we start running RRC to collect BGP traffic at different vantage points before injecting a low volume of synthesised BGP traffic then introducing an emulated node failure. In the second experiment, we start running RRC after injecting a high volume of synthesised BGP traffic then introducing multiple emulated node failures at different times. The reason for using different volumes of synthesised BGP traffic is to evaluate the capability of RQA to identify BGP anomalies in a series of low and high volume of unstable BGP traffic. In both experiments, RQA is able to distinguish anomalous behaviour from a series of unstable BGP traffic.

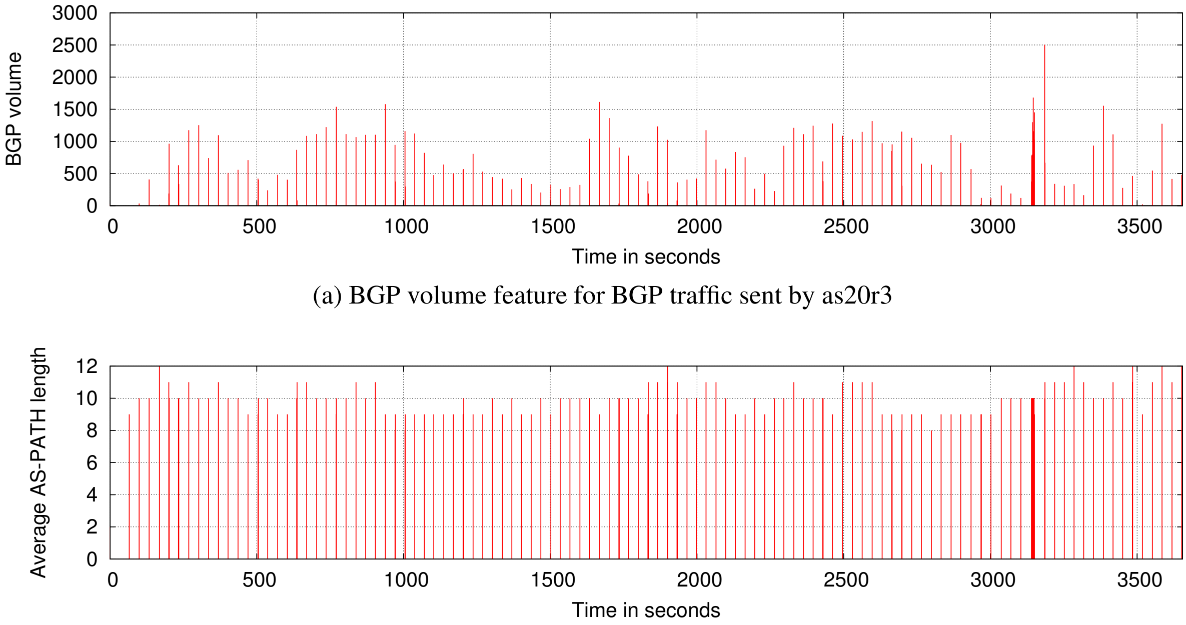
### 5.2.1 Injecting low volume of synthesised BGP traffic

In this experiment we generate a series of prefixes 182.7.x.0/24 to 182.29.x.0/24 that periodically announce then withdraw updates after a specific time. For example, 182.7.x.0/24 includes all prefixes in the range 182.10.1.0/24 to 182.10.20.0/24 that announce then withdraw networks after 10 seconds while 182.15.x.0/24 refers to all prefixes in the range 182.15.1.0/24 to 182.15.20.0/24 that announces then withdraw it after 15 seconds[1].

We inject the generated series of BGP updates using BRT and introduce an emulated node failure by shutting down all interfaces of AS1 after 2950 seconds from the start of the injection. The first 200 seconds of BGP updates represent the start of our experiment during which transient behaviour occurs. Therefore, we will ignore any significant changes in the RQA measurements during this period. As a result of the node failure, there is a notable decrease followed by an increase in the number of BGP updates during the period 2950-3200 seconds. This is because when as1r1 was shut down, its neighbours as40r1, as30r1, and as20r3 do not become aware of this event until the BGP hold timer expires, the default value of which is 180 seconds. Figure 5.2 shows the total number of BGP updates (BGP volume) and the average length of AS-PATH features calculated every second for BGP traffic sent by as20r3 and collected at RRC. The calculation of RQA measurements for BGP volume and average AS-PATH length features shows a significant change in RQA measurements during the node failure as well as at time 201 seconds (the start of our experiment which TT and T2 can identify the start of the injection traffic) as shown in Figure 5.3. In this figure we can see a significant change in the values of TT, T2 and RR values for BGP volume features and RR values for average AS-PATH length feature after the failure, a further discussion for the most effective

[1] We have shown in Section 4.3.1 that 10 and 15 second periods are typical of unstable ASes.

RQA measurements to detecting BGP anomalies will be covered in Section 5.4.



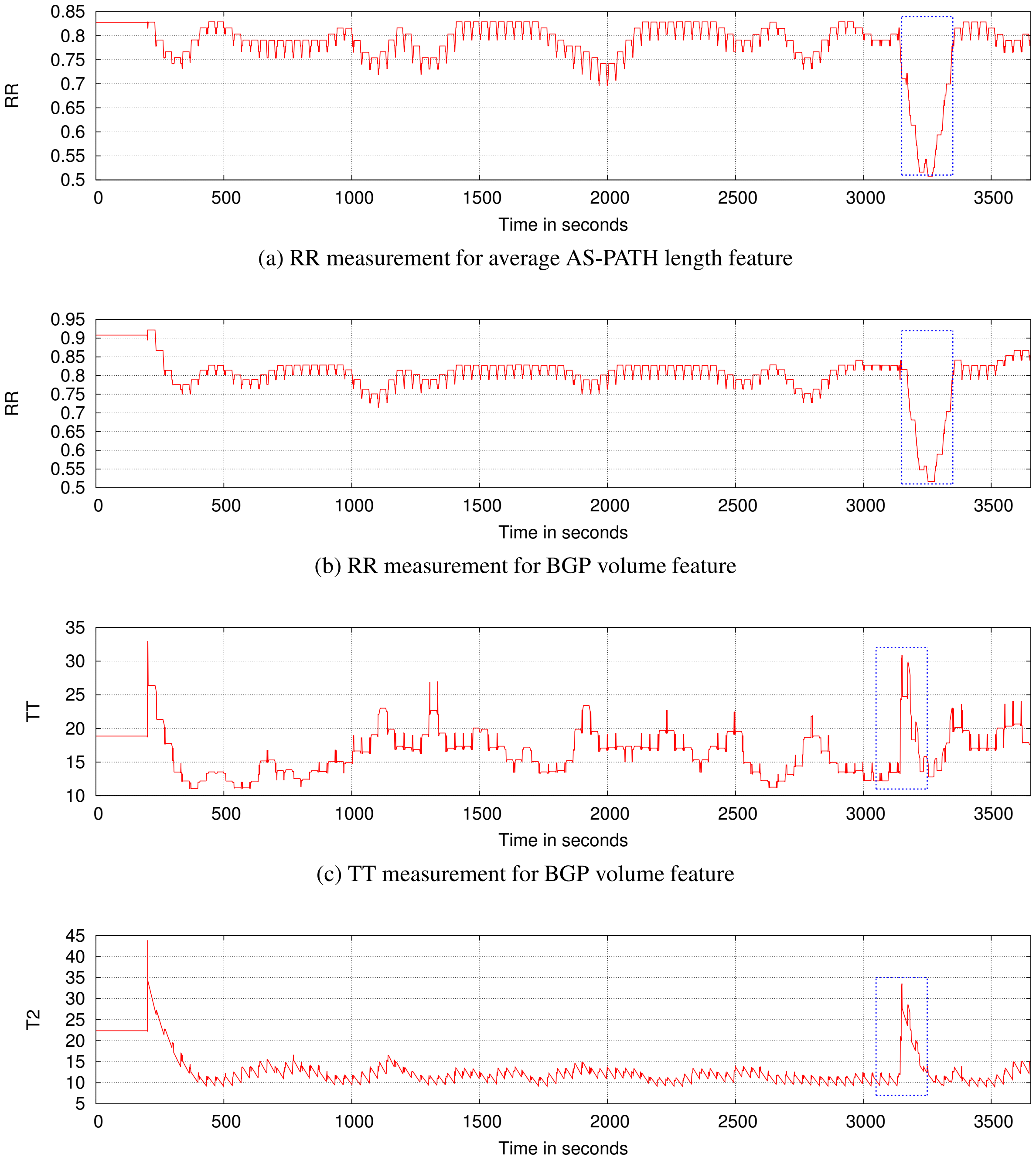
(a) BGP volume feature for BGP traffic sent by as20r3

(b) Average AS-PATH length feature for BGP traffic sent by as20r3

Figure 5.2: Experiment-1 BGP volume and average AS-PATH length features collected by as20r3

The period 2950-3185 seconds represents the start of the node failure followed by the period of the hold time and then the response of the as20r3 to the failure. In other words, the interval 2950-3185 seconds can be described as three periods. First, during the period 2950-3139 seconds, the as20r3 sent small number of BGP updates which did not exceed 500 BGP updates per second. This is because as20r3 did not recognise the node failure where the hold timer was not yet expired. Second, there was an increase in the number of BGP updates during the period 3140-3150 seconds, the hold timer expired, where the as20r3 sent BGP updates with alternative AS-PATHs. Although the maximum number of BGP updates during this period is 1682 BGP updates, it does not represent a high volume increase compared to previous periods such as 938 seconds (1579 BGP updates) and 1667 seconds (1614 BGP updates). Third, the as20r3 sent 2502 BGP updates at time 3185 seconds which represents the highest volume of BGP updates per second sent by as20r3 during the period of the experiment.

Figure 5.4 shows BGP volume and average AS-PATH length features and their corresponding values of TT, T2, and RR measurements during the period 3100-3190 seconds. In this figure, we can see there is a significant change in the values of TT, T2, and RR at time 3145 seconds. In this period, RQA measurements indicate anomalous behaviour in the BGP



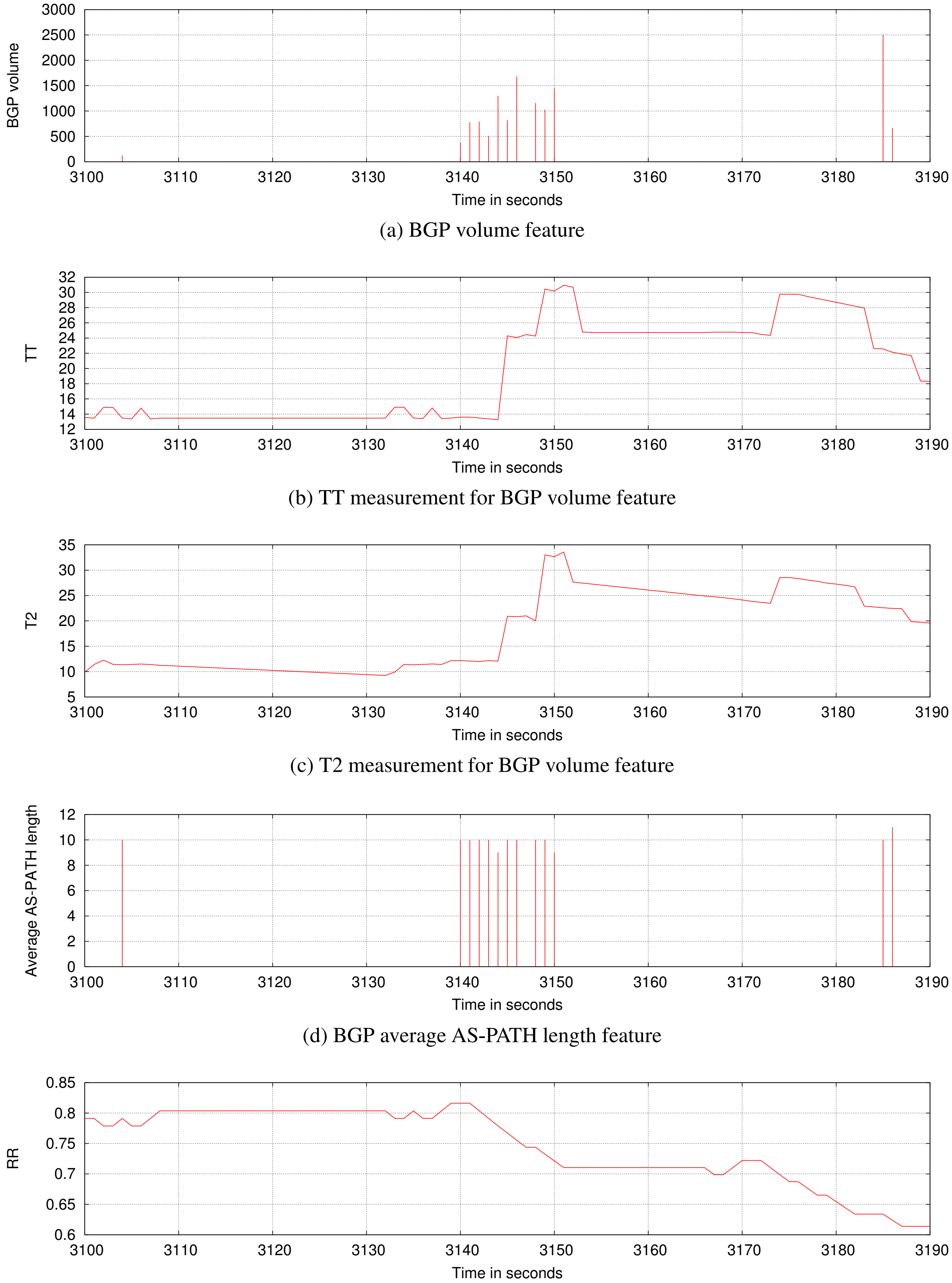
(a) RR measurement for average AS-PATH length feature

(b) RR measurement for BGP volume feature

(c) TT measurement for BGP volume feature

(d) T2 measurement for BGP volume feature

Figure 5.3: Experiment-1 RQA measurements for BGP features



(a) BGP volume feature

(b) TT measurement for BGP volume feature

(c) T2 measurement for BGP volume feature

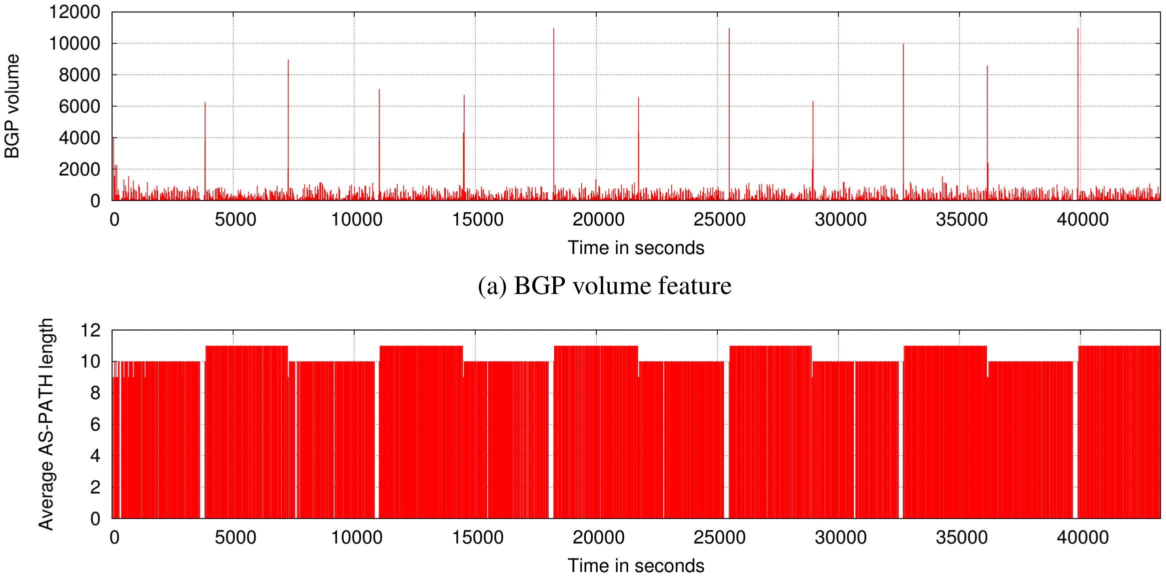
(d) BGP average AS-PATH length feature

(e) RR measurement for average AS-PATH length feature

Figure 5.4: Early indication of anomalous behaviour for experiment-1

speaker as20r3 before a significant volume of BGP updates is sent. The maximum values of TT and T2 measurements can be seen at time 3151 seconds while the minimum value of RR measurement can be seen at time 3220 seconds. It is worth noting that there is a substantial change in the volume around times 600 and 1600 seconds which do not affect RQA measurements at all (Figure 5.2a). RQA measurements are not simply responding to changes in the number of BGP updates per second. Rather RQA measurements are responding to a change in the frequency of updates sent by AS20r3 which sent multiple BGP updates in the period of a few seconds rather the default value (28 to 32 seconds).

The evaluation of our scheme to indicate BGP anomalies using a low volume of synthesised BGP traffic shows that RQA measurements can indicate anomalous but hidden behaviour in BGP traffic, during the period 3140-3340 seconds, which represents an early indication of BGP anomalies before starting to send a significant volume of BGP updates.



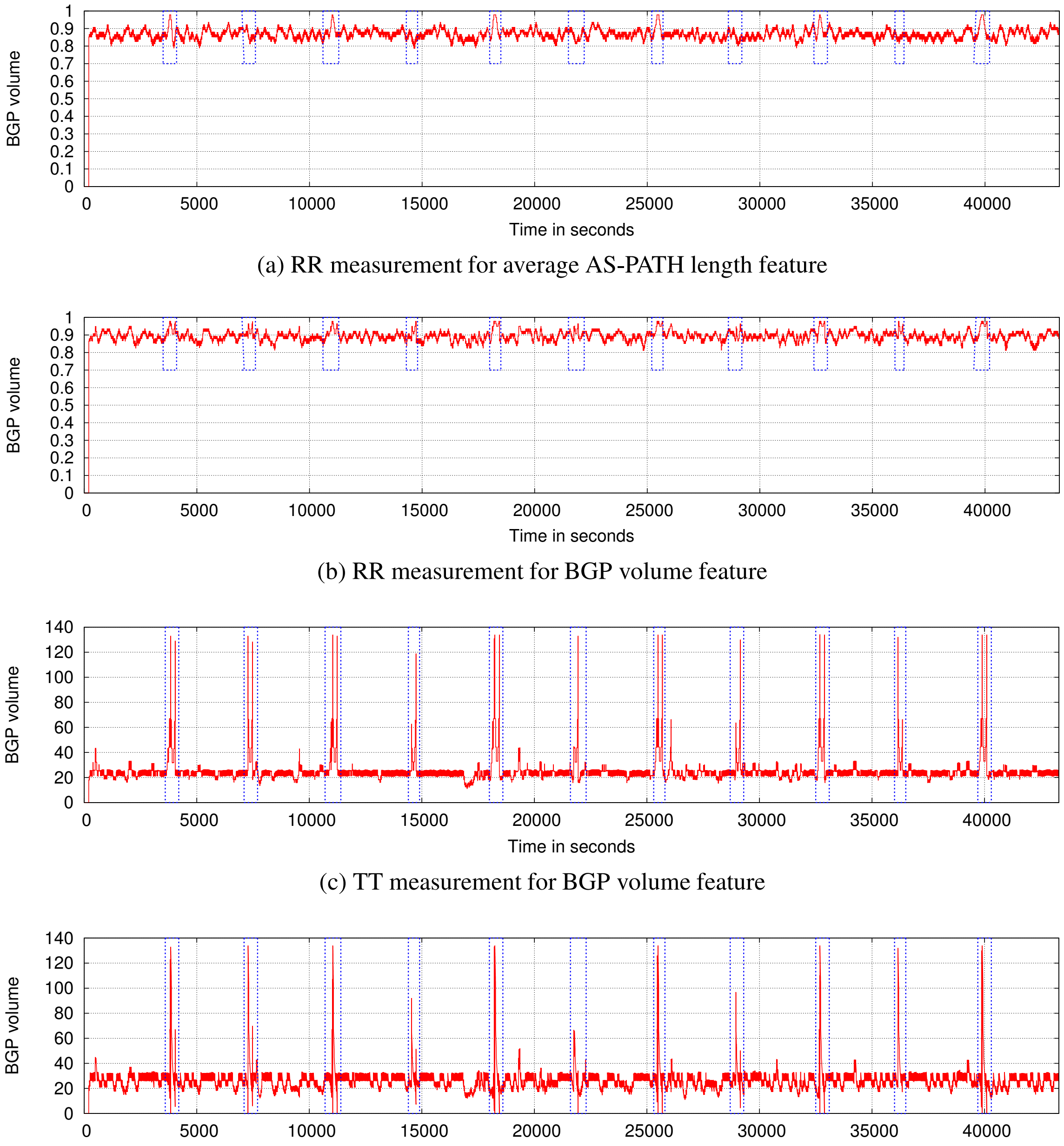
(a) BGP volume feature

(b) Average AS-PATH length feature

Figure 5.5: Experiment-2 BGP features of BGP traffic collected by as20r3

### 5.2.2 Injecting high volume of synthesised BGP traffic

In this experiment, we use our topology shown in Figure 5.1 and inject a high volume of synthesised BGP traffic for a period of 12 hours. We also extend the number of anomalies to six hardware failures, one failure every 2 hours. We introduce a hardware failure after 3600 seconds (1 hour) which is the first failure then reconnect AS1 by enabling all interfaces after another 3600 seconds. We continue in this sequence to obtain, in total, six hardware failures and five re-connections for AS1. In other words, we introduce 11 emulated BGP anomalies



(a) RR measurement for average AS-PATH length feature

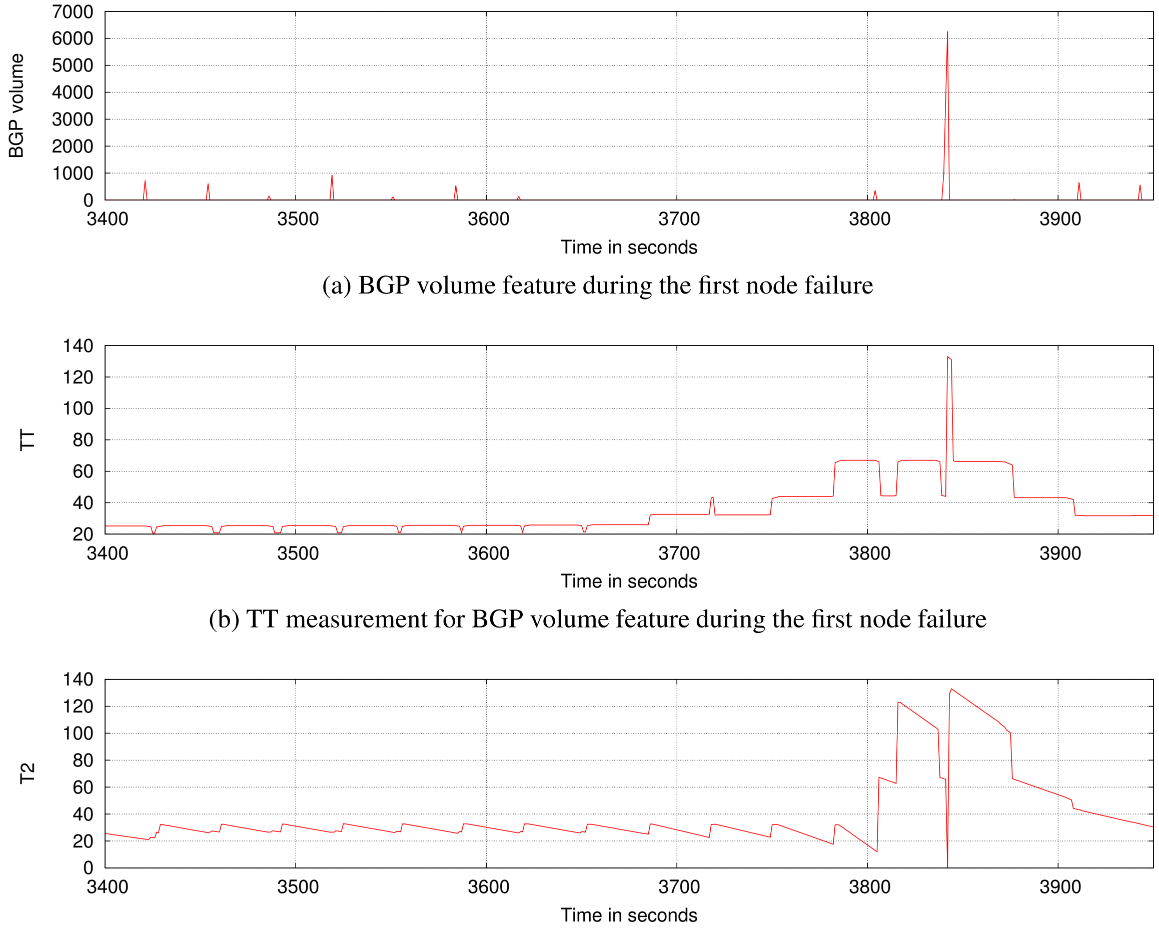
(b) RR measurement for BGP volume feature

(c) TT measurement for BGP volume feature

(d) T2 measurement for BGP volume feature

Figure 5.6: Experiment-2 RQA measurements for BGP features

(6 hardware failures and 5 reconnects) every 3600 seconds. We use 3600 seconds as a period between emulated anomalies to ensure the all routers received the BGP rerouting (as a result of disconnecting and reconnecting AS1) and to avoid overlapping between transient behaviours of emulated BGP anomalies. Figures 5.5 show BGP features for the collected BGP traffic sent by the peer as20r3. Although we use the same injected BGP updates and the same period of time between node failures and reconnects, we can see different values of BGP volume at different times. For example, the value of BGP volume at the first failure 3842 seconds is 6260, 7098 for the second failure at time 11039 seconds, and 10984 for the third failure at time 18243 seconds. The difference in the values of volume depends on the content of RIB and BGP updates received from neighbours at times of the node failures.



(a) BGP volume feature during the first node failure

(b) TT measurement for BGP volume feature during the first node failure

(c) T2 measurement for BGP volume feature during the first node failure

Figure 5.7: Early indication of anomalous BGP behavior during first node failure for experiment-2

Figure 5.6 shows the corresponding values of RQA measurements of the two BGP features. Figure 5.7 shows BGP volume feature during the first node failure and its corresponding values of T2 and TT where we can see that these RQA measurements, once again, indicate an early stage of BGP anomalies. In this example, the peer as20r3 did not send any BGP updates during the period 3617-3804 seconds then sent multiple BGP updates with values 1003, 3729, and 6260 BGP updates during the time stamp 3840, 3841, and 3842 seconds respectively. TT and T2 measurements responded to this hidden anomalous behaviour (stop sending BGP updates during period 3617-3804 seconds) at time 3718 seconds and 3806 seconds respectively, the first notable changes in the values of TT and T2. In this example, TT and T2 measurements can indicate the anomalous behaviour within 122 seconds and 34 seconds respectively before peer as20r3 sent multiple BGP updates.

In this section, we have used our controlled testbed to synthesise low and high volume unstable BGP traffic and then introduce node failures. In both experiments, RQA can differentiate between normal-but-unstable BGP traffic and anomalous BGP traffic that identifies anomalies. In the next section, we will use the results obtained from our controlled testbed as a ground truth data to select optimal values of our scheme parameters.

## 5.3 RQA scheme design

We now describe our RQA based detection scheme for detecting BGP anomalies. Our scheme is comprised of four stages as shown in Figure 5.8. The input of our scheme are BGP updates received from the monitored BGP speaker while the output is an alarm that indicates the detection of BGP anomalies. Now, we describe our scheme in more detail.

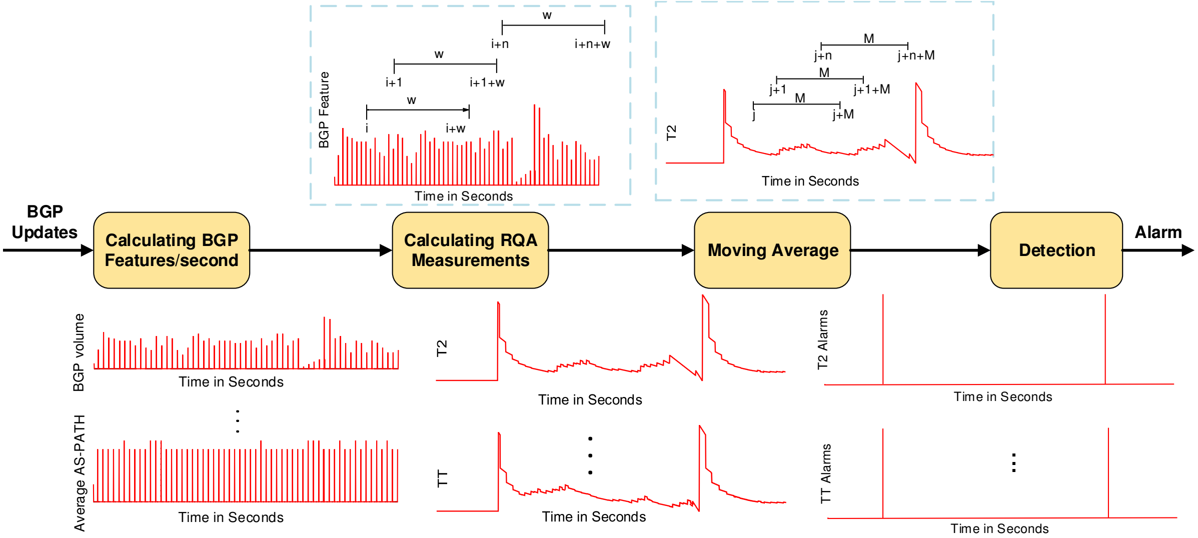


Figure 5.8: Detection process of RQA scheme to detecting BGP anomalies

### 5.3.1 Calculating BGP features

At this first stage, we calculate BGP features from BGP updates sent by the BGP speaker. The output of this stage are BGP features in time series representation as shown in Figure 5.8. There are multiple BGP features that can be used. As discussed in Section 2.2.6 and listed in Table 2.3, BGP features can be mainly classified into deviations in the number of BGP updates and in the path data contained within the update field AS-PATH. We use these two main BGP features to identify behaviour changes of the monitored BGP speaker. In particular, we use BGP volume $(V)$ (total number of announcements and withdrawals) and average length of AS-PATH $(AV)$ in our scheme to detect BGP anomalies. The $AV$ feature is calculated as follows:

$$AV = \left[\frac{TA}{A}\right], \tag{5.1}$$

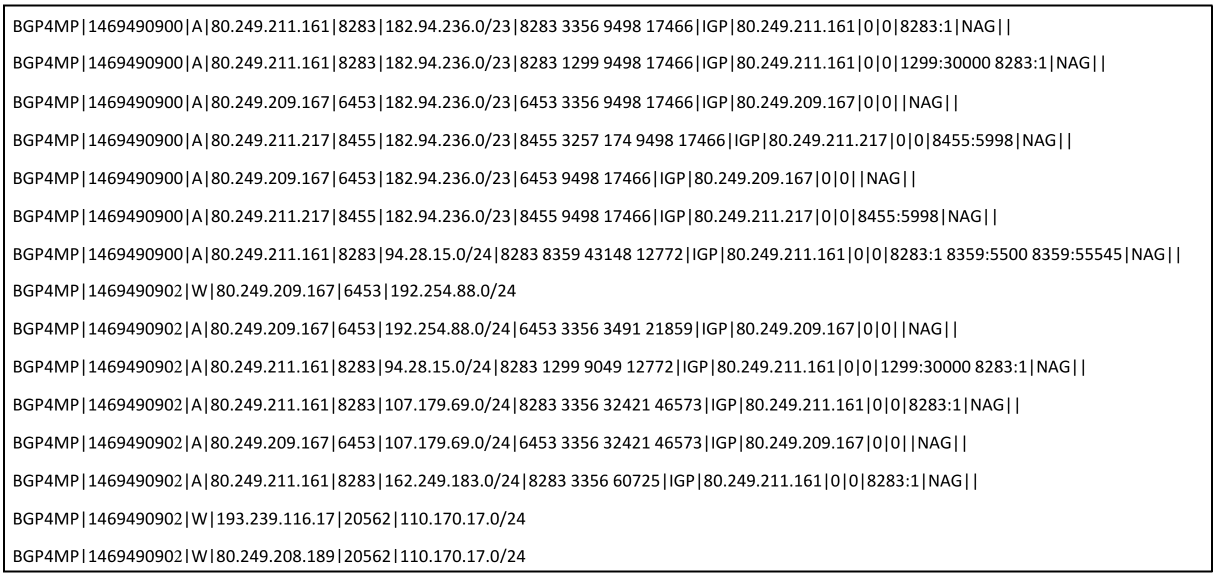
where $TA$ is total AS-PATH lengths for the announcements, $A$ is total number of announcements , and $[]$ is the nearest integer function. These BGP features are calculated every second based on time stamp of BGP updates. For example, there are 5 announcements and 3 withdrawals at time stamp 1469490900 in Unix format for BGP updates shown in Figure 5.9. 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 5.9 is:

$V = [7,0,8]$

$AV = [4,0,4]$

### 5.3.2 Calculating RQA measurements

This stage represents the calculation of RQA measurements for each BGP feature calculated during the previous stage. Before calculating RQA measurements for BGP features, we normalise the input time series data (BGP features) by subtracting the mean value to smooth noisy traces. Calculation of RQA measurements is based on many parameters. These include time delay $(\tau)$, embedding dimension $(m)$, recurrence threshold $(\varepsilon)$, and window size $(W)$. As discussed in Chapter 3, the values of $(\tau)$ and $(m)$ can be calculated using MI and FNN respectively while the value of $(\varepsilon)$ can be calculated using the recommendation from [123] by choosing the threshold value less than 10% of the maximum phase space diameter. We use TISEAN package [150] to calculate the values of $(\tau)$ and $(m)$ and Matlab toolbox available in [163] to calculate the value of $(\varepsilon)$.



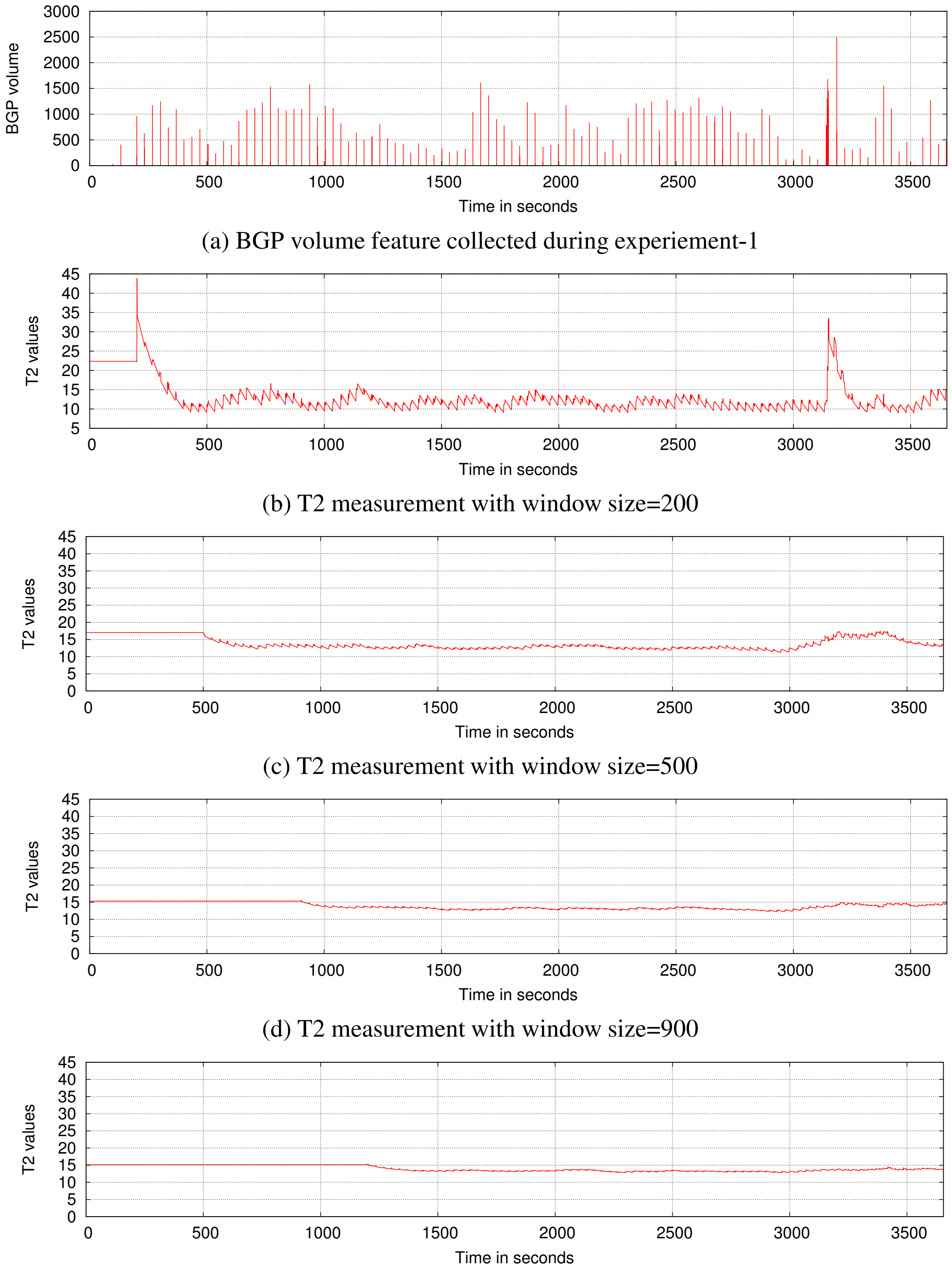
```
BGP4MP|1469490900|A|80.249.211.161|8283|182.94.236.0/23|8283 3356 9498 17466|IGP|80.249.211.161|0|0|8283:1|NAG||
BGP4MP|1469490900|A|80.249.211.161|8283|182.94.236.0/23|8283 1299 9498 17466|IGP|80.249.211.161|0|0|1299:30000 8283:1|NAG||
BGP4MP|1469490900|A|80.249.209.167|6453|182.94.236.0/23|6453 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 5.9: Example of BGP updates in a human readable format

The size of the window $(W)$ needs to be chosen carefully. A large window may fail to identify some transitions in system behaviour while a small window can generate spurious fluctuations in RQA measurements. We use TT and T2 as illustrative examples to show the effect of the window size on RQA measurements. Figures 5.10 and 5.11 show values of T2 and RR calculated with different window sizes for BGP traffic obtained from our experiment described early in Section 5.2.1. For example during the node failure of the first experiment (Section 5.2.1), the maximum T2 value during the failure is 33 when the window size is 200 seconds while it is 17 when the window size is 500 seconds as shown in Figures 5.10b and 5.10c. In addition to the effect of window size on the values of RQA measurements, the window size has an effect on the delay for RQA measurement changes to reflect the change in the input data. For example, the detection period of RR measurements is 500 seconds when the window size is 500 seconds and it is 200 seconds when the window is 200 seconds as shown in Figures 5.11b and 5.11c. The process of selecting the optimal value of the window $(W)$ will be discussed in detail in Section 5.4 where we investigate the accuracy of our detection scheme.

### 5.3.3 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 as discussed in Section 3.5. To identify RQA



(a) BGP volume feature collected during experiement-1

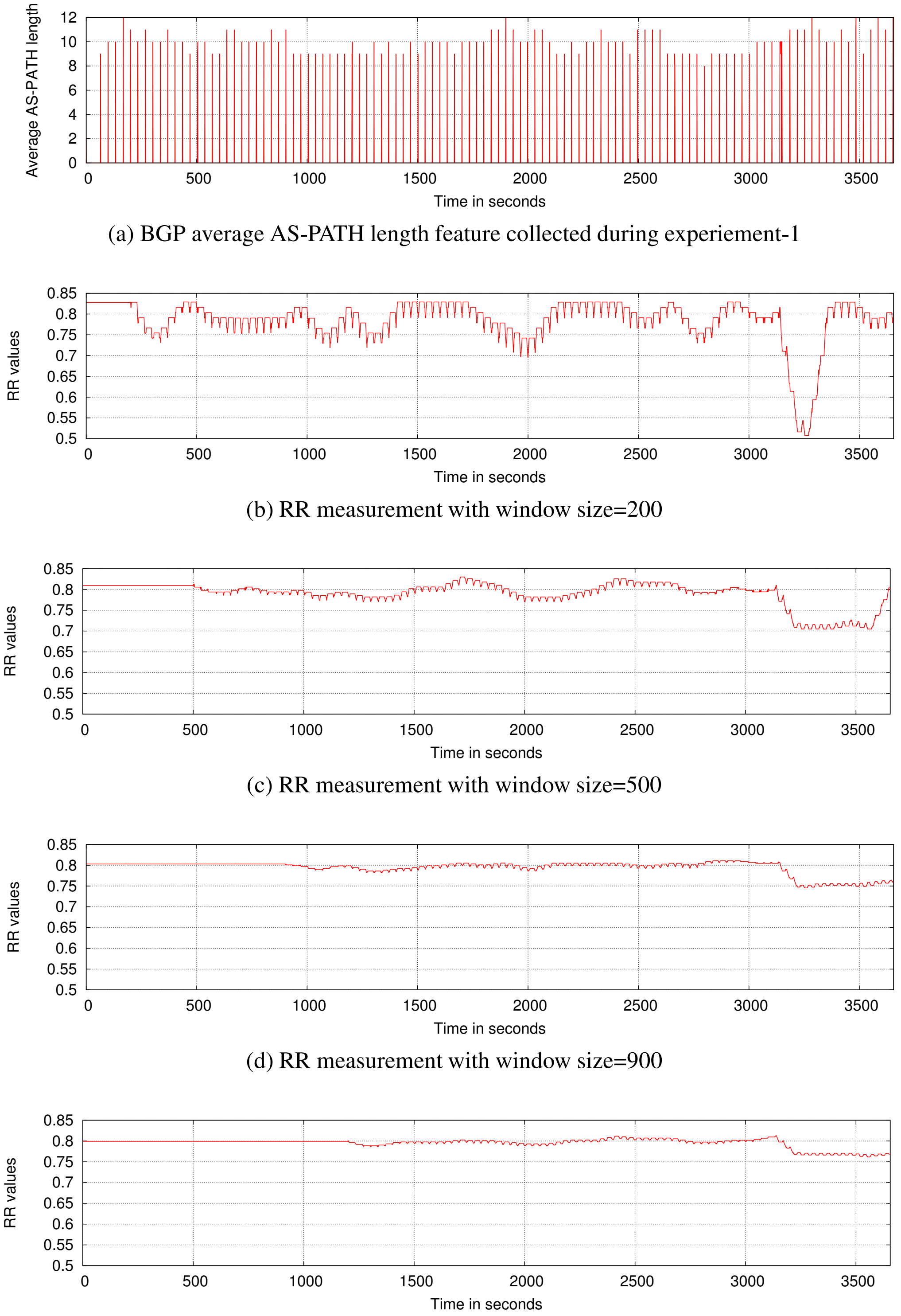
(b) T2 measurement with window size=200

(c) T2 measurement with window size=500

(d) T2 measurement with window size=900

(e) T2 measurement with window size=1200

Figure 5.10: The effect of window size on T2 measurement



(a) BGP average AS-PATH length feature collected during experiement-1

(b) RR measurement with window size=200

(c) RR measurement with window size=500

(d) RR measurement with window size=900

(e) RR measurement with window size=1200

Figure 5.11: The effect of window size on RR measurement

measurement's changes that indicate an anomaly, we apply moving average technique based on the following format:

$$RQA_{alarm} = Mean(M) \pm sd(M) * X, \tag{5.2}$$

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. The process of selecting values of $(M)$ and $(X)$ as well as $(W)$ will also be discussed in detail in Section 5.4 where we adjust the detection parameters for better detection accuracy. The output of this stage is potentially multiple RQA alarms.

### 5.3.4 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. Integration of multiple RQA alarms (from the moving average stage) is an area of further research. But for the purpose of illustration, we use all logical ORs. Our decision is based on the need to minimise FPs. Further discussion of the ability of individual RQA measurements to produce a high detection rate and low detection delay will be introduced in Section 5.4.2[2].

In this section, we have presented the design of our RQA scheme for detecting BGP anomalies. In the next section, we use BGP updates collected from our controlled testbed as ground truth data to select optimal values of our RQA scheme parameters that generate high detection accuracy.

## 5.4 Estimating parameters and selecting measurements

In this section, we discuss the process of selecting optimal values for our RQA scheme's parameters that produce high detection accuracy. These parameters are the window size $(W)$ for calculating RQA measurements, the window size $(M)$ for detecting notable changes of RQA measurements values at moving average stage and the threshold value $(X)$ of moving average stage. We also investigate the selection of the most effective RQA measurements to detect BGP anomalies in term of detection accuracy and detection delay. These measurements and

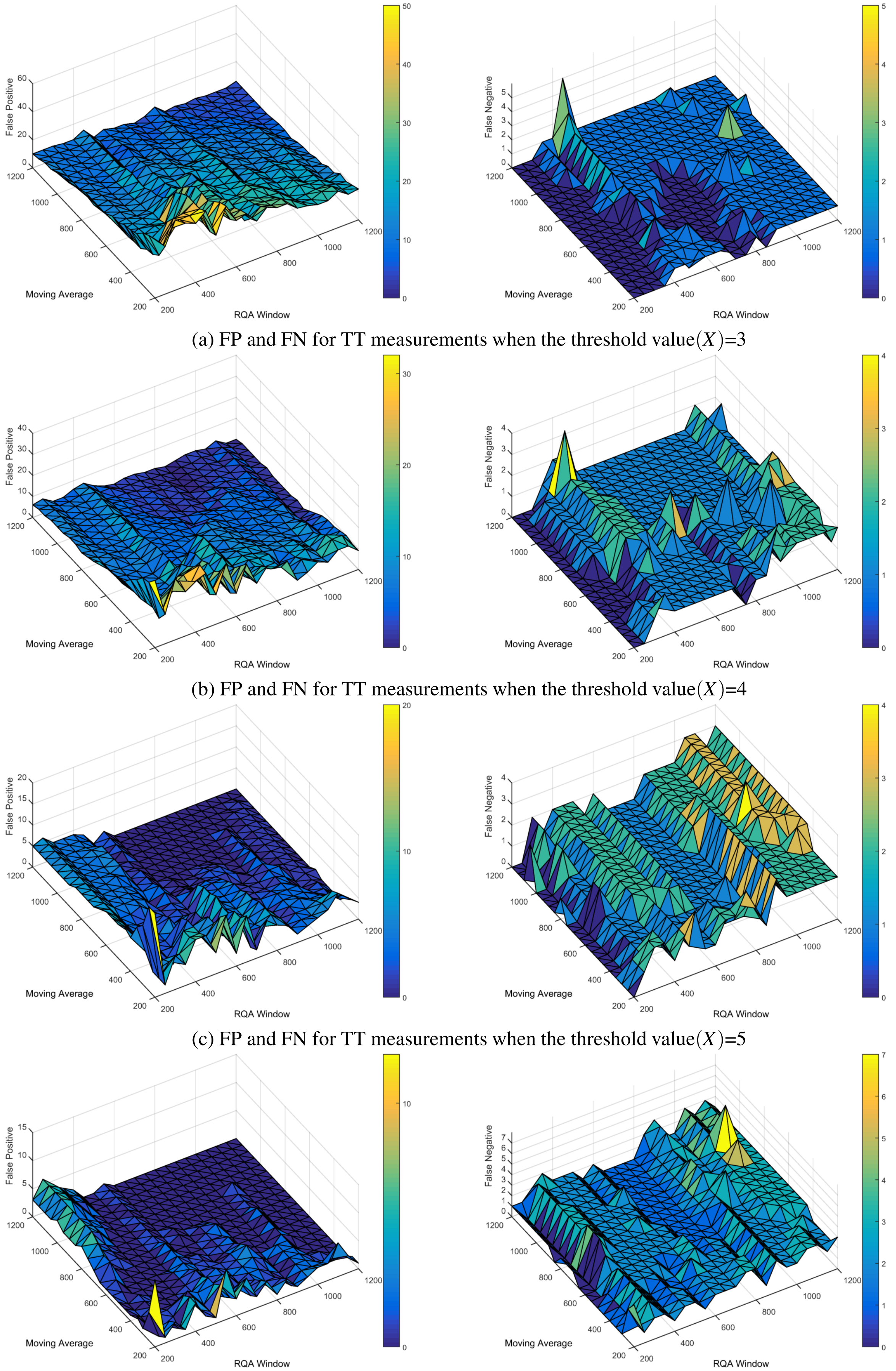
[2] We note that only TT measurement is able to detect BGP anomalies with zero value of FN and FP rates. However, in some cases TT measurements can detect BGP anomalies faster than T2. Consequently, we use a logical OR function

parameters can affect the performance of our detection scheme in term of classifying normal and anomalous events. We use FP and FN to estimate these measurements and parameters. These values are important for network operators. High rates of FN means anomalous events are rarely detected. High FN rates may have a serious consequence on business relationships between ISPs and on Internet stability. However, high rates of FP can overwhelm the network operator since positive results require further investigation to identify whether or not an alarm represents a real anomaly which if it is an FP, means wasted time and hence additional cost.

We start our investigation by selecting the optimal values of windows $(W)$ and $(M)$ that can produce low rates of FN and FP. Based on selected values of these, we investigate the process of selection of the most effective RQA measurements to detect BGP anomalies. For our investigation, we use our results obtained from the two experiments described earlier in Section 5.2 which contains 12 BGP anomalies (1 BGP anomaly from experiment-1 and 11 anomalies from experiment-2) during 46952 seconds (3653 seconds for experiment-1 and 43299 experiment-2).

### 5.4.1 Selecting window size

In this subsection, we explore different sizes of the windows ($W$ and $M$) for calculating RQA measurements and moving average stage and discuss the optimal values that can be used to produce low rates of FP and FN. We evaluate window sizes from 200 seconds to 1200 seconds with an increment of 50 seconds. Figures 5.12 and 5.13 show the effect of changing windows size on FP and FN for RQA measurements TT and T2 calculated for BGP volume feature which we use as examples for RQA measurements. Our selection of the window size is based on low rates of both FP and FN. For example, the window size of 1200 seconds for both $(W)$ and $(M)$ is the best window size in term of FP rates of TT measurement but it is not in terms of FN as shown in Figure 5.12d. Regardless of the value of the threshold which will be discussed later, we can see the lower values of FP and FN are when the value of RQA window $(W)$ is smaller than 300 seconds and the value of moving average window $(M)$ is larger than 1000 seconds. In addition to its effect on FP and FN, the size of the window $(W)$ has to be chosen to be as small as possible to avoid missing the detection of multiple anomalies within a short time. For example, choosing the value of $(W)$ of 1200 seconds leads to missing multiple anomalies that may occur during 1200 seconds as highlighted before in Figure 5.11. Consequently, for successive experiments, we will adopt the values of windows size $W$=200 seconds and $M$=1200 seconds as optimal values to be used in our detection scheme.



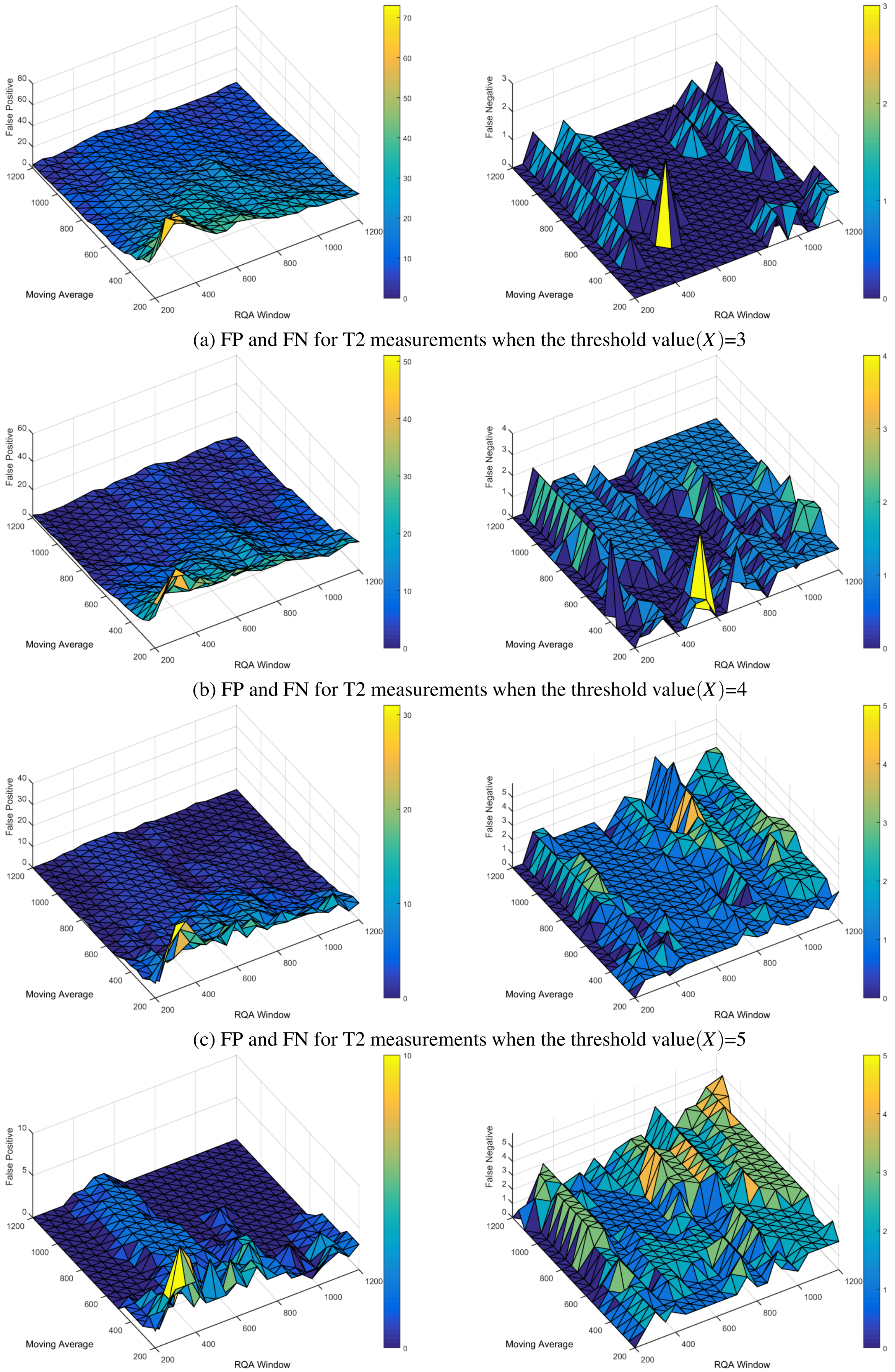
(a) FP and FN for TT measurements when the threshold value($X$)=3

(b) FP and FN for TT measurements when the threshold value($X$)=4

(c) FP and FN for TT measurements when the threshold value($X$)=5

(d) FP and FN for TT measurements when the threshold value($X$)=6

Figure 5.12: Effect of changing windows ($W$ and $M$) on FP and FN rates using TT measurement for BGP volume feature



(a) FP and FN for T2 measurements when the threshold value($X$)=3

(b) FP and FN for T2 measurements when the threshold value($X$)=4

(c) FP and FN for T2 measurements when the threshold value($X$)=5

(d) FP and FN for T2 measurements when the threshold value($X$)=6

Figure 5.13: Effect of changing windows ($W$ and $M$) on FP and FN rates using T2 measurement for BGP volume feature

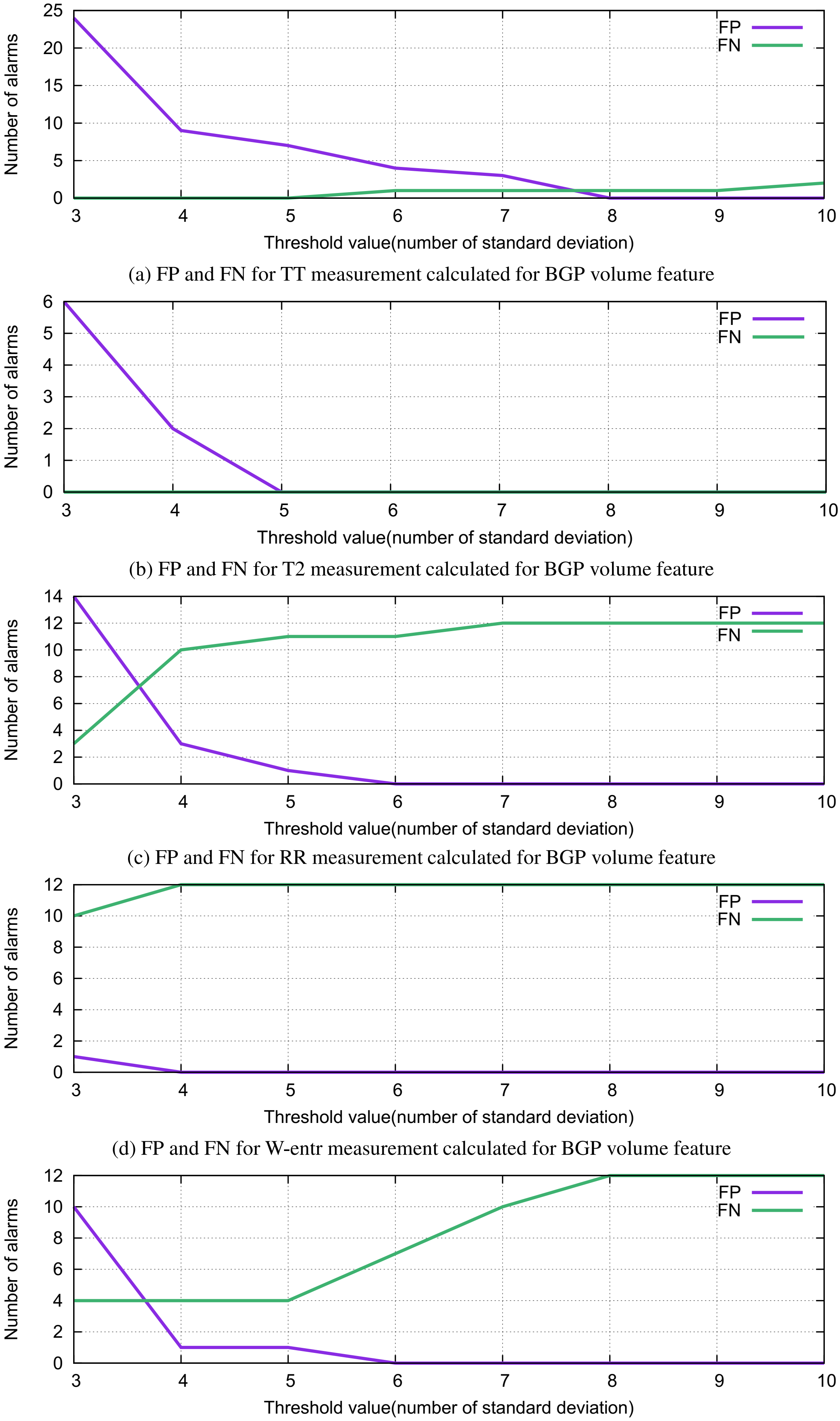
### 5.4.2 Selecting RQA measurements

We have shown in Section 3.5 that RQA measurements TT, T2, RR, W-entr, and V-entr can be used effectively to detect anomalous behaviour of systems. We now use BGP volume and average AS-PATH length features to detect BGP anomalies. Calculating RQA measurements for these two BGP features produces ten RQA measurements (five RQA measurements for each BGP feature). In this subsection, we investigate the selection of the most effective RQA measurements that can detect BGP anomalies. This is necessary to avoid using sparse RQA measurements that can be irrelevant to detect anomalies. Once again, we use our ground truth data obtained from our testbed described in Section 5.2 where we synthesised normal-but-unstable BGP traffic and introduced anomalies.

We use values of $(W = 200)\, seconds$ and $(M = 1200)\, seconds$ that represent optimal values for our detection scheme as discussed earlier. Figures 5.14 and 5.15 show the number of FP and FN with different values of the threshold (number of standard deviations in the moving average stage) for the five RQA measurements (TT, T2, RR, V-entr and W-entr) calculated for both BGP volume and average AS-PATH length features respectively. The calculation of FP and FN shows that all RQA measurements except T2 for BGP volume feature are not able to produce zero values of FP and FN for any value of the threshold. T2 can detect the 12 emulated BGP anomalies with zero values of FP and FN when the threshold value$\geq 5$.

However, in some cases, TT can detect BGP anomalies more quickly than T2. This is based on the patterns changing during an anomalous period. For example, Figure 5.16 shows the detection delay for TT and T2 alarms (outputs of the moving average stage) for BGP traffic related to the first emulated BGP anomaly of experiment-2. Therefore, we carry out more investigation on RQA measurements to determine which RQA measurements can detect BGP anomalies faster than T2 taking into consideration that a zero value of FP and a low value of FN are wanted. We accept that missing some BGP anomalies for other RQA measurements can be used as long as T2 for BGP volume feature can detect all possible BGP anomalies. This can help to detect BGP anomalies as quickly as possible while avoiding high FP rates.

Our further investigation includes detection delay of RQA measurements T2 and TT related to BGP volume and average AS-PATH length features. We eliminate RR, V-entr and W-entr measurements from our investigation for detection delay as those measurements cannot produce a low value of FN when FP=0. For example, RR measurement produces FN=11 when the FP=0 as shown in Figures 5.14c and 5.15c. Although we eliminate RR, V-entr and W-entr measurements from these experiments, we note that they may well be able to be used if more sophisticated techniques were used for integrating RQA measurements. However, that is an area for future research.



(a) FP and FN for TT measurement calculated for BGP volume feature

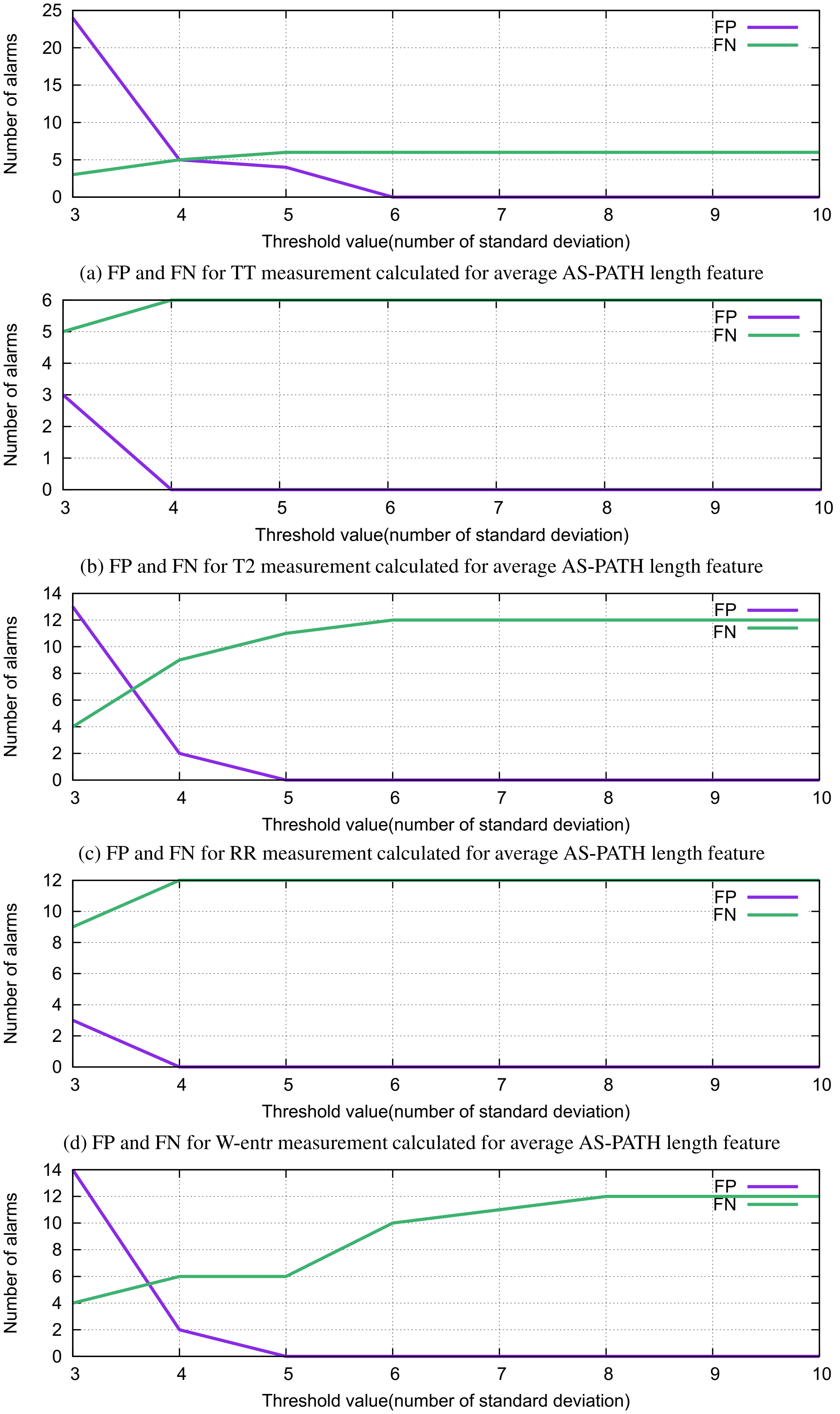
(b) FP and FN for T2 measurement calculated for BGP volume feature

(c) FP and FN for RR measurement calculated for BGP volume feature

(d) FP and FN for W-entr measurement calculated for BGP volume feature

(e) FP and FN for V-entr measurement calculated for BGP volume feature

Figure 5.14: FP and FN of RQA measurements for BGP volume feature



(a) FP and FN for TT measurement calculated for average AS-PATH length feature

(b) FP and FN for T2 measurement calculated for average AS-PATH length feature

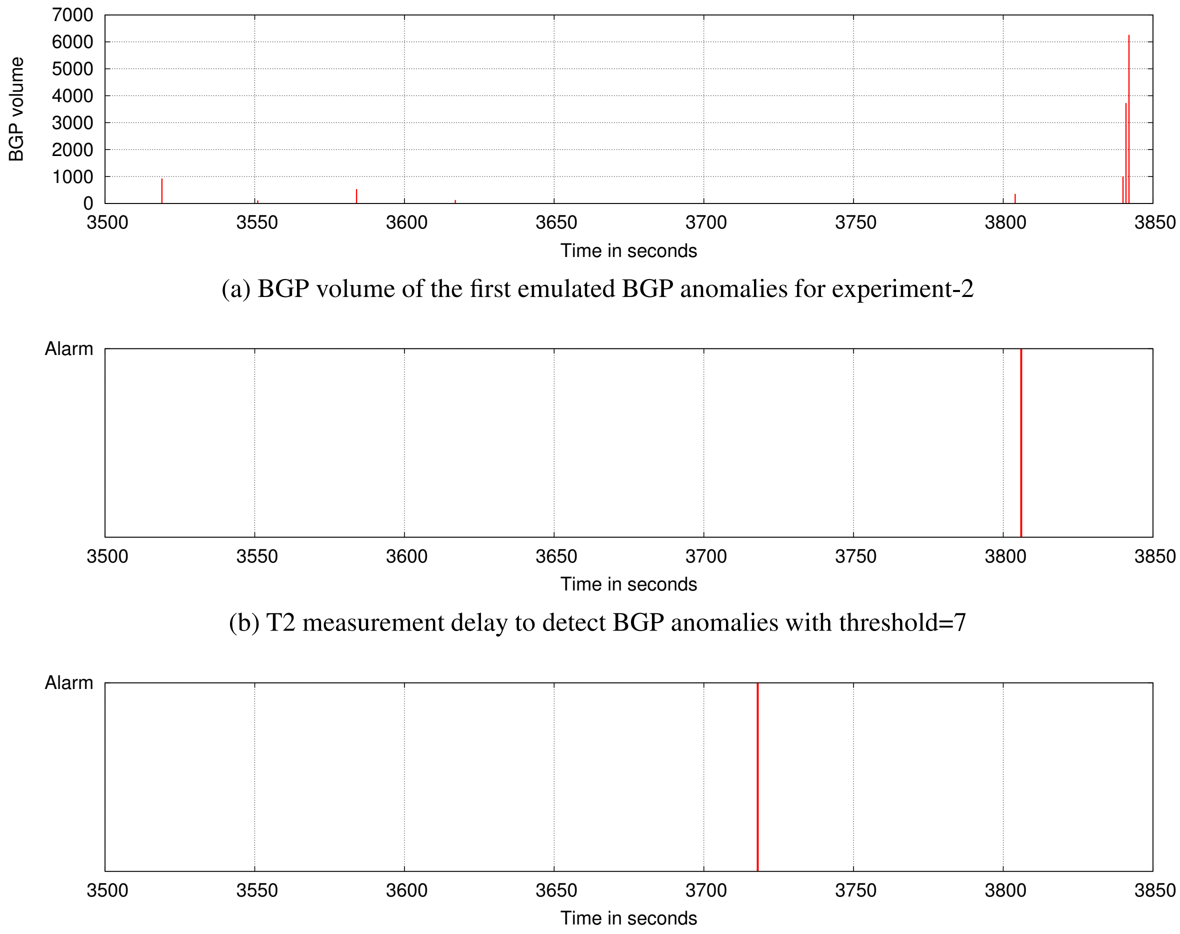
(c) FP and FN for RR measurement calculated for average AS-PATH length feature

(d) FP and FN for W-entr measurement calculated for average AS-PATH length feature

(e) FP and FN for V-entr measurement calculated for average AS-PATH length feature

Figure 5.15: FP and FN of RQA measurements for average AS-PATH length feature

Figures 5.16 and 5.17 show the detection delay in seconds in detecting BGP anomalies for RQA measurements. In these figures we can see that TT detects BGP anomalies more quickly than T2. Our experiments suggest that TT and T2 measurements are the most effective RQA measurements for detecting BGP anomalies.



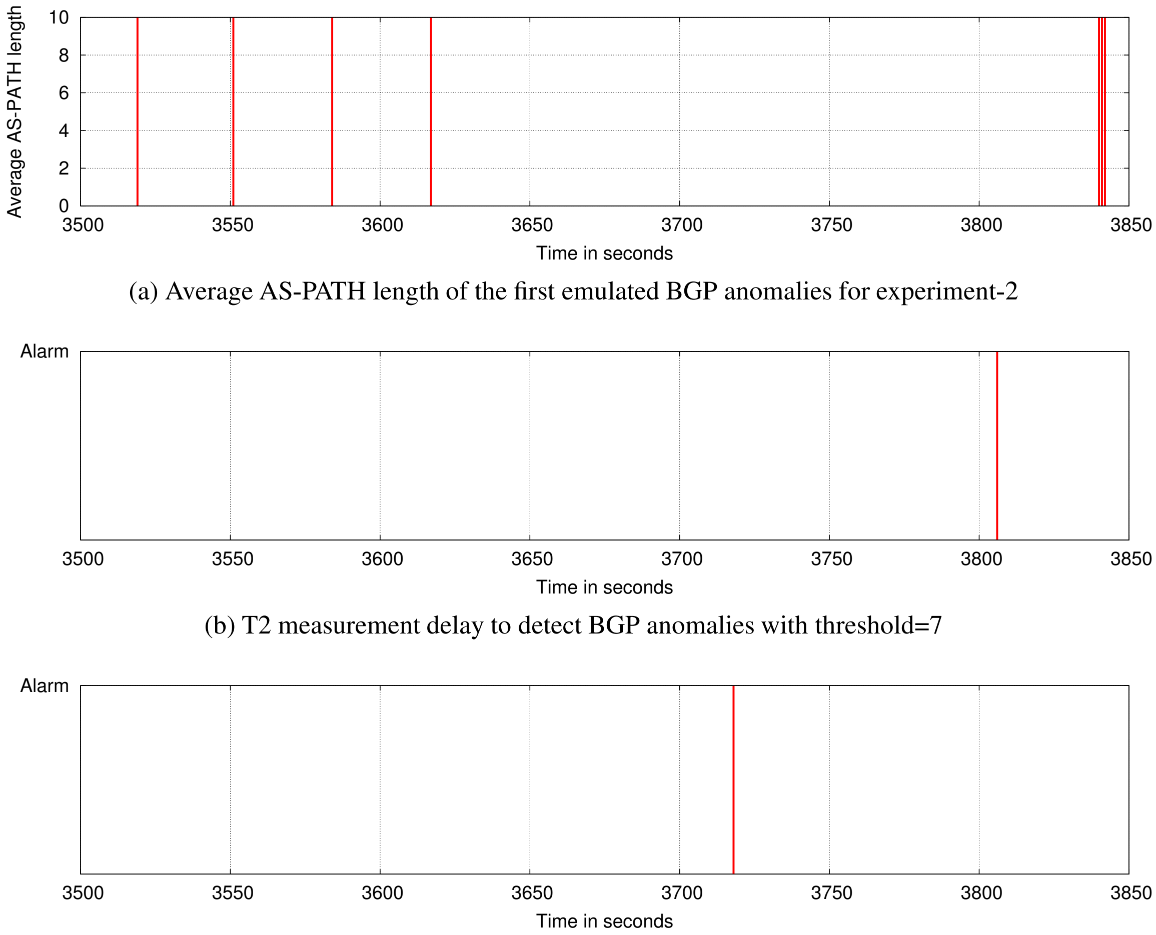
(a) BGP volume of the first emulated BGP anomalies for experiment-2

(b) T2 measurement delay to detect BGP anomalies with threshold=7

(c) TT measurement delay to detect BGP anomalies with threshold=9

Figure 5.16: RQA measurements delay to detect BGP anomalies using BGP volume feature

In this section, we have discussed the process of selecting the optimal values of window sizes and choosing the most effective RQA measurements to detect BGP anomalies. We have shown that RQA window size $W = 200$ and moving average window $M = 1200$ are effective values that can be used in our RQA scheme so our detection scheme requires 1200 seconds of history data. We have also shown that using our simple logical OR for integrating RQA measurements TT and T2 are effective for anomaly detection. In terms of selecting optimal values of threshold, our experiments suggest using T2 threshold value=7 while TT with threshold value=9 for both BGP features gives low FP and FN. In the next section, we will use these



(a) Average AS-PATH length of the first emulated BGP anomalies for experiment-2

(b) T2 measurement delay to detect BGP anomalies with threshold=7

(c) TT measurement delay to detect BGP anomalies with threshold=9

Figure 5.17: RQA measurements delay to detect BGP anomalies using average AS-PATH length feature

values and RQA measurements to evaluate the accuracy and detection delay for our RQA scheme.

## 5.5 Evaluation

The evaluation of our RQA scheme is based on the numbers of TP, TN, FP and FN. The last two parameters (FP and FN) are the most important due to their effect on network operators. However, there are other metrics based on these that can be used to evaluate our RQA scheme. These metrics are accuracy, F-score, precision, and sensitivity which are derived from TP, TN, FP and FN. Accuracy regards normal events as being as important as anomalous events while F-score reflects the success of detecting anomalies rather than detecting both anomalies and normal events. Precision measures the ability of the system to identify classified and unclassified anomalies while sensitivity measures the ability of the system to correctly classify anomalies in the data set. These evaluation metrics are calculated as follows:

$$accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{5.3}$$

$$F-score = 2 \times \frac{precision \times sensitivity}{precision + sensitivity} \tag{5.4}$$

where

$$precision = \frac{TP}{TP+FP} \tag{5.5}$$

$$sensitivity = \frac{TP}{TP+FN} \tag{5.6}$$

In addition to the above metrics, we evaluate the detection delay of our RQA scheme. Our evaluation includes BGP traffic obtained from our controlled testbed discussed in Section 5.2 and different types of well-known BGP events, starting with BGP traffic collected from the controlled testbed.

### 5.5.1 Detecting BGP anomalies using the controlled testbed

In this subsection, we use BGP traffic obtained from our testbed for the two experiments described in Section 5.2 to evaluate the accuracy of our scheme. In total, we analyse 45952 seconds of BGP traffic, 3653 seconds of BGP traffic obtained from experiment-1 and 42299 seconds of BGP traffic obtained from experiment-2. Our detection scheme requires 1200

Table 5.1: Detection accuracy for BGP traffic obtained from our testbed

| Experiment | TP | TN | FP | FN | Precision | Sensitivity | Accuracy | F-score |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 2453 | 0 | 0 | 1 | 1 | 1 | 1 |
| 2 | 11 | 41099 | 0 | 0 | 1 | 1 | 1 | 1 |

seconds of past data so we subtract 1200 seconds from TN values. The values of TP, TN, FP, and FN for both experiments are listed in Table 5.1.

In terms of detection delay, our scheme detects BGP anomalies within 5 seconds. In experiment-1, our scheme raises an alarm at time 3146 seconds so it detects BGP anomalies after 5 seconds since the anomaly started at time 3141 seconds (Figure 5.4). It is worth nothing that the RQA scheme detected BGP anomalies before a BGP speaker started to send a significant volume of BGP traffic. For example, Figure 5.18 shows BGP volume and average AS-PATH length features for BGP updates related to the first node failure of experiment-2 where we can see our scheme can detect BGP anomalies before the as20r3 started to send a significant volume of BGP traffic. It also detects hidden behaviour in the underlying BGP traffic where the as20r3 stopped sending BGP updates for 2 minutes before responding to the hardware failure and sending a significant volume of BGP updates.

### 5.5.2 Applying RQA to notable BGP events

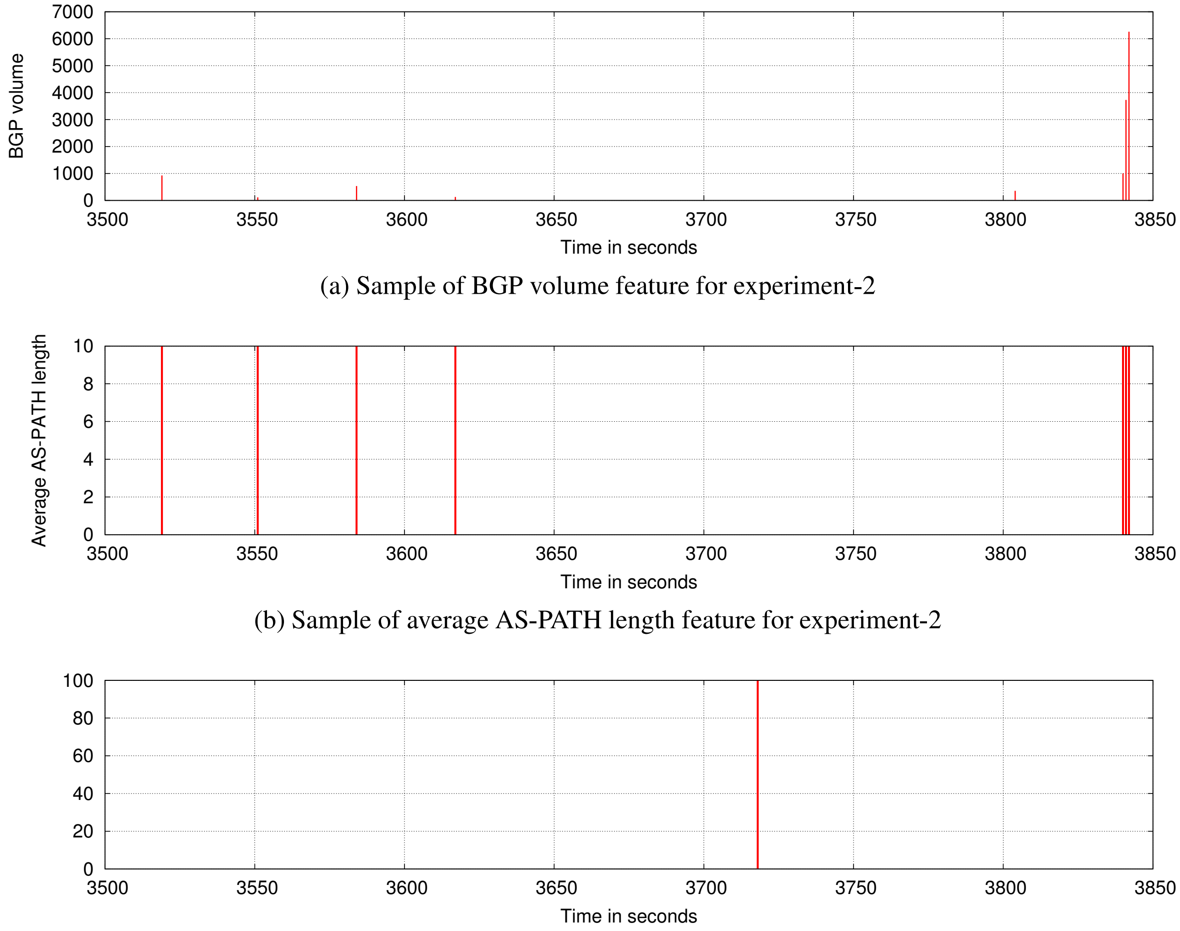
We now apply our scheme to notable BGP events. Table 5.2 shows some well-known BGP events and the selected RRCs that have been chosen based on peers that sent a significant number of BGP updates during the events. Now, we describe each of these events in detail and evaluate the effectiveness of using RQA scheme to detect them.

Table 5.2: List of notable BGP events

| Event | Date | Peers | RRC |
|---|---|---|---|
| Nimda | September 2001 | AS6893, AS513, and AS559 | rrc04, RIPE |
| TTNet | December 2004 | AS13237, AS12793, and AS1853 | rrc05, RIPE |
| Moscow | May 2005 | AS12793, AS13237, and AS1853 | rrc05, RIPE |
| TMnet | June 2015 | AS1299, AS10102, and AS38726 | route-views4 |

#### 5.5.2.1 Nimda event

Nimda is an example of an indirect BGP anomaly. On 18 September 2001, the computer worm "Nimda" attacked a large number of web servers. Although Nimda was directed at web



(a) Sample of BGP volume feature for experiment-2

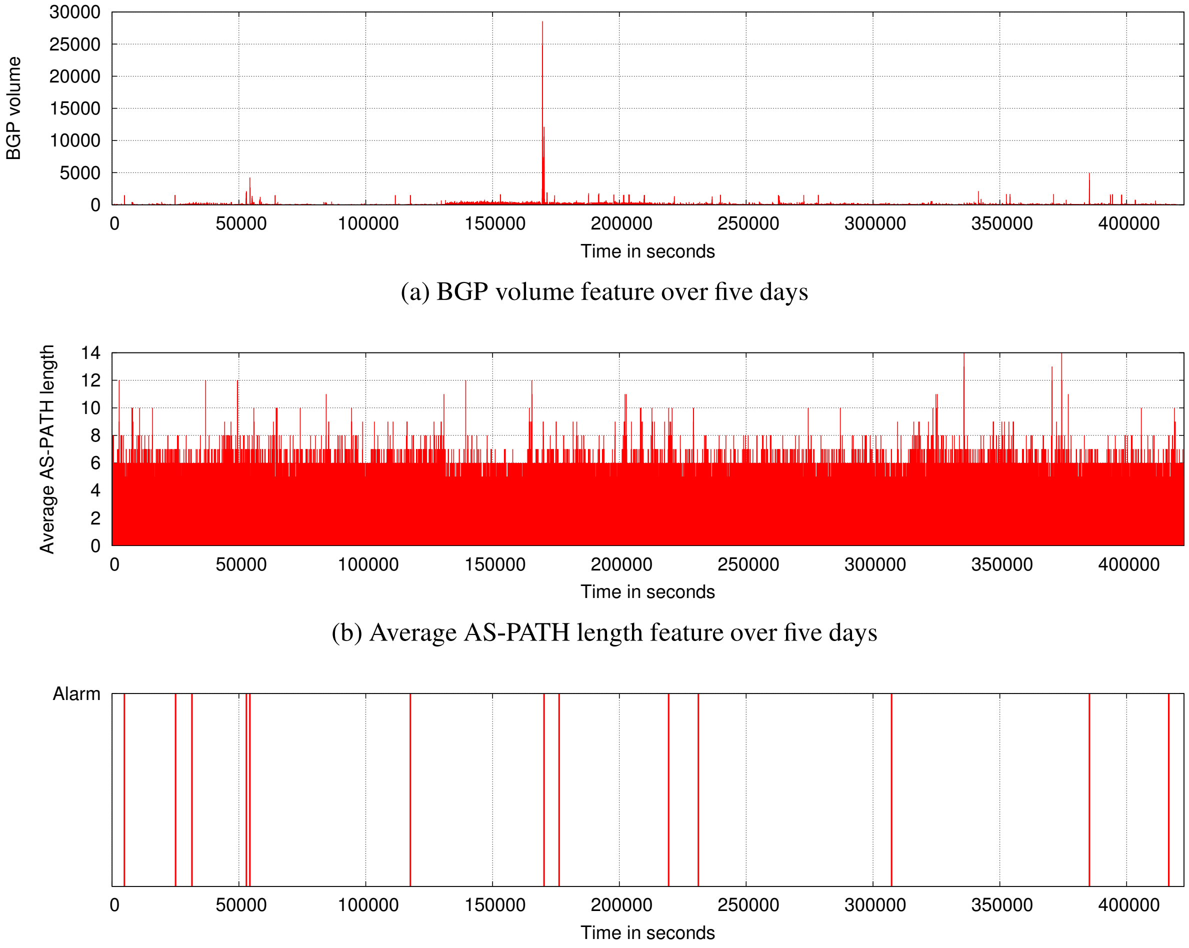
(b) Sample of average AS-PATH length feature for experiment-2

(c) Final detection of BGP anomalies using RQA scheme

Figure 5.18: Early detection of BGP anomalies using RQA scheme

servers, it caused significant instability in BGP behaviour [28]. We download BGP updates from rr04 at RIPE repository during the period 17-22 September 2001.

Figure 5.19 shows BGP volume and average AS-PATH length features for BGP updates sent by the peer AS6893 during the period 17-22 September 2001 and the output or our detection scheme. During the Nimda event 160000-165000 seconds, we can see that BGP volume traffic increased around 30 times from normal of BGP updates which is observed before in [28]. Our RQA scheme can detect anomalous behaviour during Nimda attacks as well as other anomalous periods. In total, there are 13 alarms raised by RQA detection scheme during the period 17-22 September 2001. In particular, there are 2 alarms raised during the event day, 6 alarms before the event, and 5 alarms after the event.



(a) BGP volume feature over five days

(b) Average AS-PATH length feature over five days

(c) Detecting BGP anomalies using RQA scheme

Figure 5.19: BGP features sent by AS6893 during Nimda event and its corresponding detection by RQA scheme

We now do a manual investigation on those 13 alarms to see if they are TP or FP. Determining if an event is an TP or FP is a challenge, nevertheless we believe it a worthwhile exercise. Our investigation includes checking the number of BGP updates and recurrence behaviour change for both BGP features. Our manual investigation for the 13 alarms shows that 10 alarms (including two alarms during the event date) are TP while it is unclear if the remaining 3 alarms represent FP alarms or an early detection for an anomaly. Figure 5.20 shows BGP volume feature for the three possible FP alarms raised by RQA scheme before and after the BGP event. For example, the RQA scheme raised an alarm at time 416615 seconds before the peer AS6893 showed abnormal behaviour in sending BGP updates in some seconds at periods 416732- 416733 seconds, 417271-417282 seconds, 417363-417364 seconds, and 417392-417393 seconds rather than every 28-32 seconds (MRAI timer). Although these possible FP alarms were raised due to changes in the recurrent behaviour, it is not really clear if they represent harmful anomalies or not. However, we consider them as FP alarms as a worst case. The evaluation metrics of our scheme during the period 17-22 September 2001 is shown in the Table 5.3.

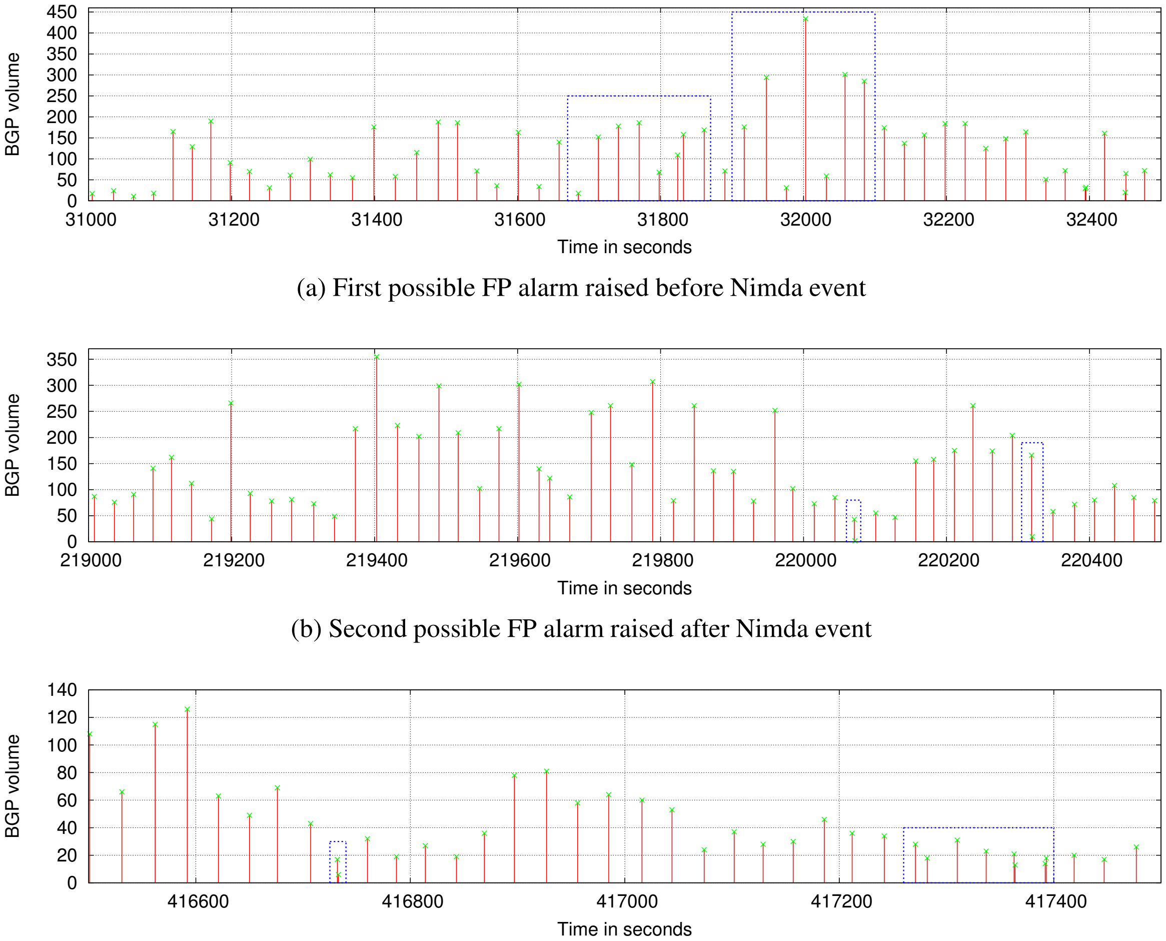
Table 5.3: Detection accuracy for Nimda event

| TP | TN | FP | FN | Precision | Sensitivity | Accuracy | F-score |
|---|---|---|---|---|---|---|---|
| 10 | 421405 | 3 | 0 | 0.7692 | 1 | 0.9999 | 0.8695 |

In term of detection delay, 2 out of 10 alarms require more than 5 seconds as a detection delay. Figure 5.21 shows BGP volume, average AS-PATH length features and RQA scheme's alarm where we can see that our RQA scheme detected BGP anomalies after 62 seconds if we consider the start of the anomaly at time 52891, the longest detection delay among the 8 alarms. In this example, the peer AS6893 started to send a high volume of BGP updates at times 52890-52891 seconds, 52920-52922 seconds and 52948-52952 seconds. RQA scheme raises an alarm at time 52952 seconds, 62 seconds after the start of abnormal behaviour. The evaluation of RQA scheme on the Nimda event shows that RQA generates 10 TP alarms and 3 FP alarms with 62 seconds as the longest detection delay. Once again, this evaluation is a worst cases assuming the 3 early alarms are FP.

### 5.5.2.2 TTNet event

TTNet is an example of a direct unintended BGP anomaly. On Christmas Eve morning 2004, TTNet (an ISP in Turkey) announced more than 100,000 incorrect entries to its peers. As a result, a large number of Internet users were unable to access a large number of domains for several hours [47].

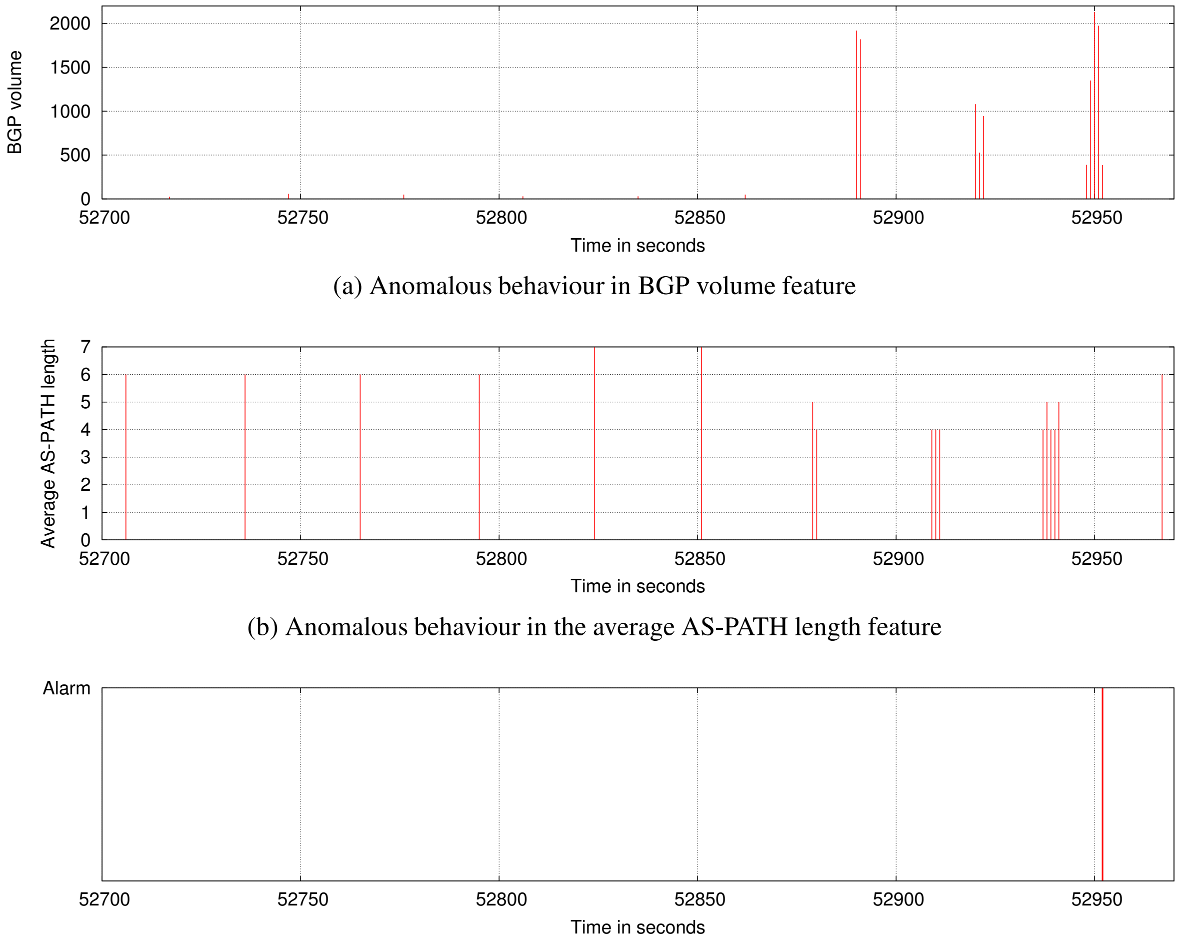


(a) First possible FP alarm raised before Nimda event

(b) Second possible FP alarm raised after Nimda event

(c) Third possible FP alarm raised after Nimda event

Figure 5.20: Three possible FP alarms raised before and after Nimda event



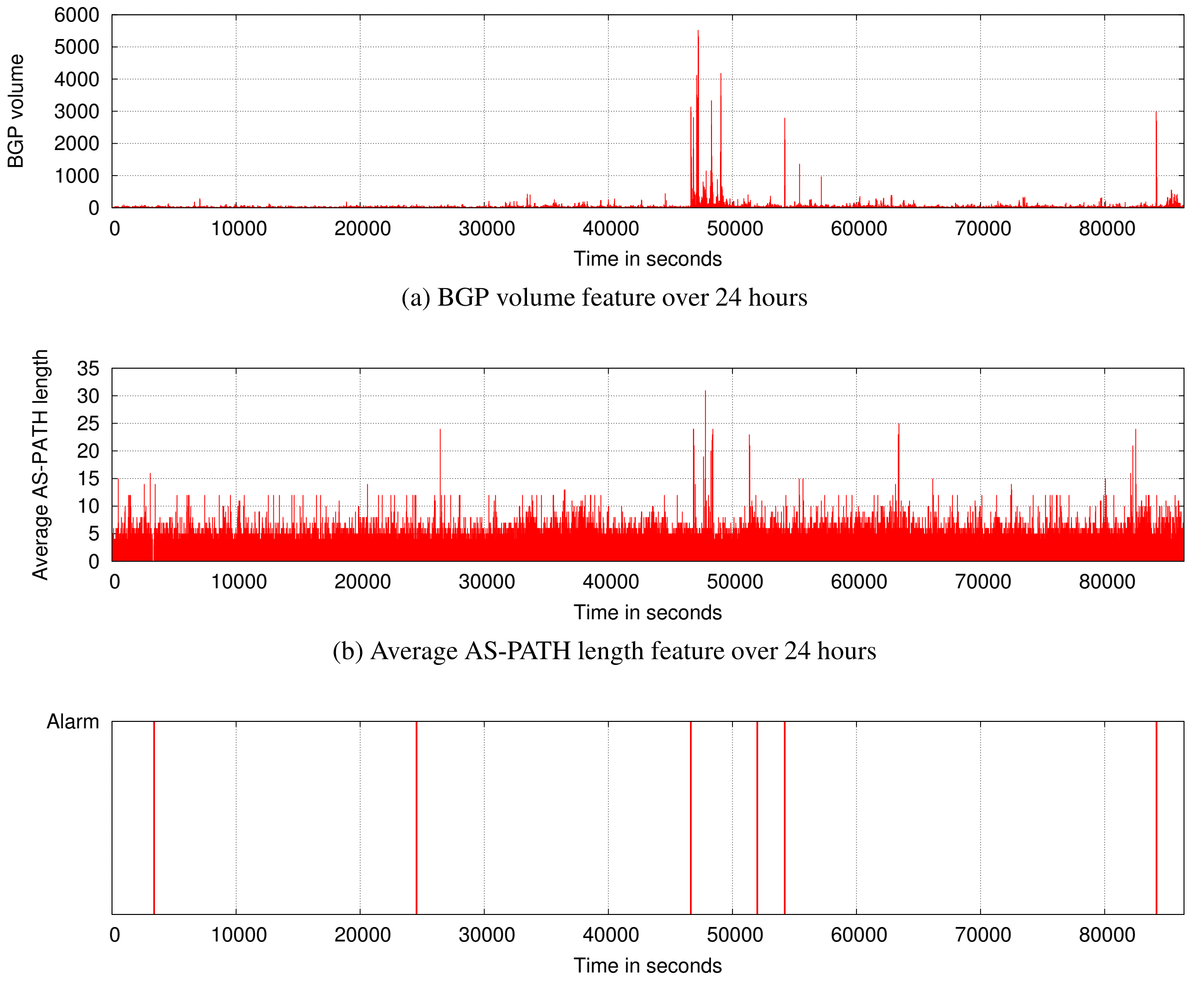
(a) Anomalous behaviour in BGP volume feature

(b) Anomalous behaviour in the average AS-PATH length feature

(c) Detection BGP anomalies after 62 seconds of starting the anomalous behaviour

Figure 5.21: Detecting BGP anomalies within 62 seconds as a longest detection delay

We run our RQA scheme on the day of the TTNet event. Our scheme detects 6 BGP anomalies. Figure 5.22 shows the number of alarms generated by RQA scheme using BGP volume and average length of AS-PATH features calculated every second for BGP traffic sent by the peer AS12793 at rrc05. During this event, AS12793 sent a significant volume of BGP updates during the period 46645-49309 seconds which our RQA scheme rapidly detects. In addition to the high volume detection, RQA scheme detects some hidden anomalies that have not been observed before. For example, during the period 3267-3388 seconds, the peer AS12793 stopped sending any BGP updates as shown in Figure 5.23a which our scheme detect.



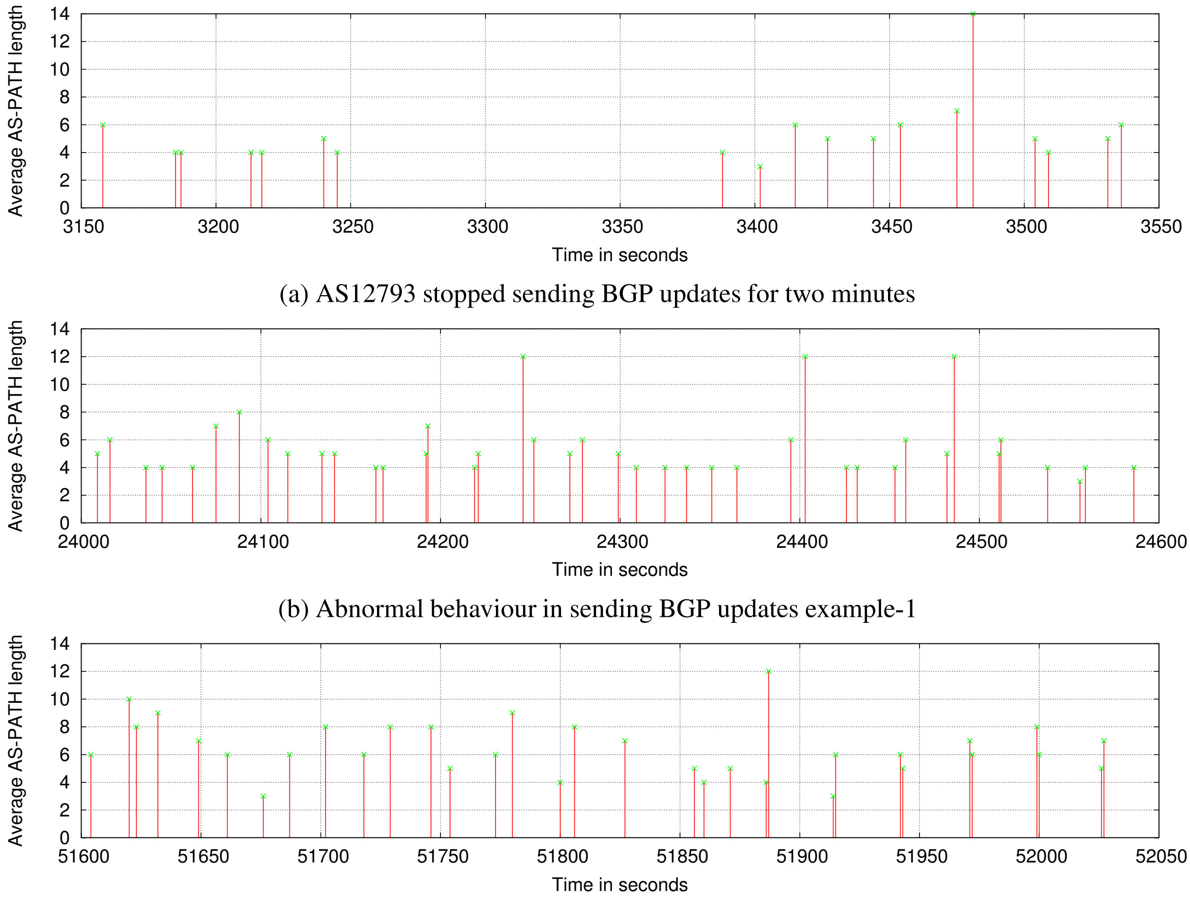
(a) BGP volume feature over 24 hours

(b) Average AS-PATH length feature over 24 hours

(c) Detecting BGP anomalies using RQA scheme

Figure 5.22: BGP features sent by the peer AS12793 during TTNet event and its corresponding detection by RQA scheme

In total, there are 6 alarms raised by RQA scheme during the period of analysis (86401 seconds). Once again, we do a manual investigation to see if the these alarms are TP or FP. Our investigation shows that all alarms are TP. They are either as a result of a significant change in the volume of BGP updates or recurrent change in BGP traffic behaviour. Figure 5.23a shows that the peer AS12793 stopped sending BGP traffic for two minutes while Figures 5.23b and 5.23c shows changing recurrent behaviour in average AS-PATH length feature which our RQA scheme detects them. In particular, there were changes in MRAI timers during these periods. The evaluation metrics of our scheme for TTNet event is shown in the Table 5.4. The longest detection delay for the 6 raised alarms is 31 seconds.



(a) AS12793 stopped sending BGP updates for two minutes

(b) Abnormal behaviour in sending BGP updates example-1

(c) Abnormal behaviour in sending BGP updates example-2

Figure 5.23: Examples of manual investigation for alarms detected before and after TTNet event

Table 5.4: Detection accuracy for TTNet event

| TP | TN | FP | FN | Precision | Sensitivity | Accuracy | F-score |
|---|---|---|---|---|---|---|---|
| 6 | 85201 | 0 | 0 | 1 | 1 | 1 | 1 |

#### 5.5.2.3 Moscow blackout

Around 25 May 2005, there was a power outage that led to the shutdown of the Moscow Internet Exchange Point (MSK-IX) for several hours. Although the shutdown did not produce a global effect on BGP routing stability, many ISPs connected to this exchange point lost their connectivity for several hours [112]. We use BGP updates downloaded from the VP rrc05 at RIPE during the period 22-28 May 2005. Figure 5.24 shows the number of alarms generated by RQA scheme using BGP updates sent by the peer AS12793 (the peer that sent BGP updates). As a result of the event, AS12793 sent a high volume of BGP traffic during the period 273000-283200 seconds. Our scheme flagged 12 alarms over the period of 597376 seconds of BGP updates. Among the 12 raised alarms, the alarm raised at time 272398 seconds is an interesting detection. RQA scheme raised an alarm at time 272398 seconds, 730 seconds before the peer AS12793 started to send a significant volume of BGP traffic at time 273128 seconds and continued sending high volume of BGP traffic for two hours. Figure 5.25 shows an early detection of detecting BGP anomalies. In this case, RQA detected BGP anomalies 730 seconds before the peer AS12793 started to send a significant volume of BGP traffic.

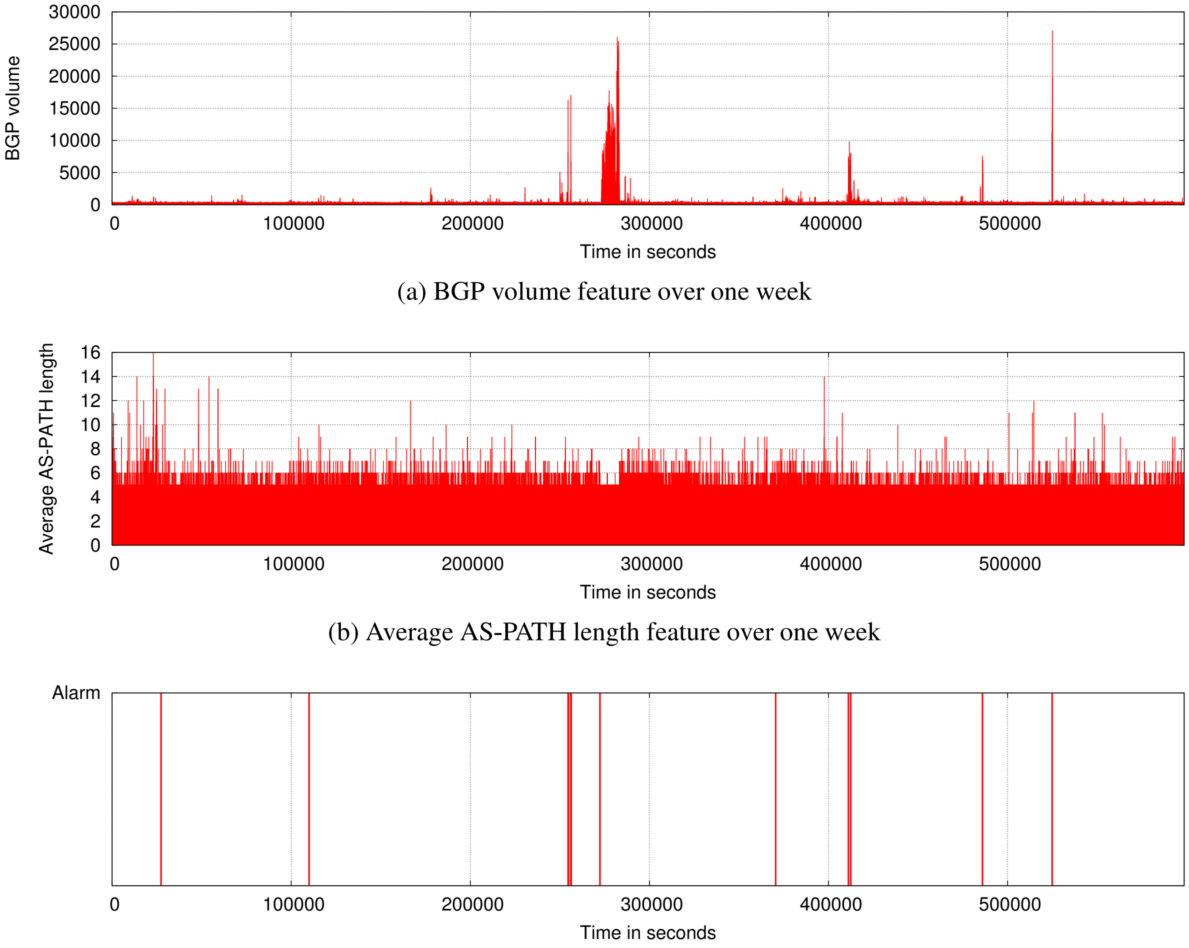
Once again, we do a manual investigation for the 12 raised alarms to see if they represent TP or FP alarms. Among the 12 alarms, 2 alarms there are for which it is not clear if they represent a threat. Although they were raised as a result of changing recurrent behaviour in the underlying BGP traffic sent by the peer AS12793, it is unclear if they represent a threat to BGP operation or not. Consequently, we consider them as FP alarms. Furthermore, the longest detection delay for the 10 raised alarms is 28 seconds. Table 5.5 shows accuracy metrics of our RQA scheme.

Table 5.5: Detection accuracy for Moscow event

| TP | TN | FP | FN | Precision | Sensitivity | Accuracy | F-score |
|---|---|---|---|---|---|---|---|
| 10 | 597376 | 2 | 0 | 0.8333 | 1 | 0.9999 | 0.9090 |

#### 5.5.2.4 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. We run our RQA scheme to detect BGP anomalies during the event. Figure 5.26 shows BGP volume, average AS-PATH length, and number of alarms raised by our scheme using 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.

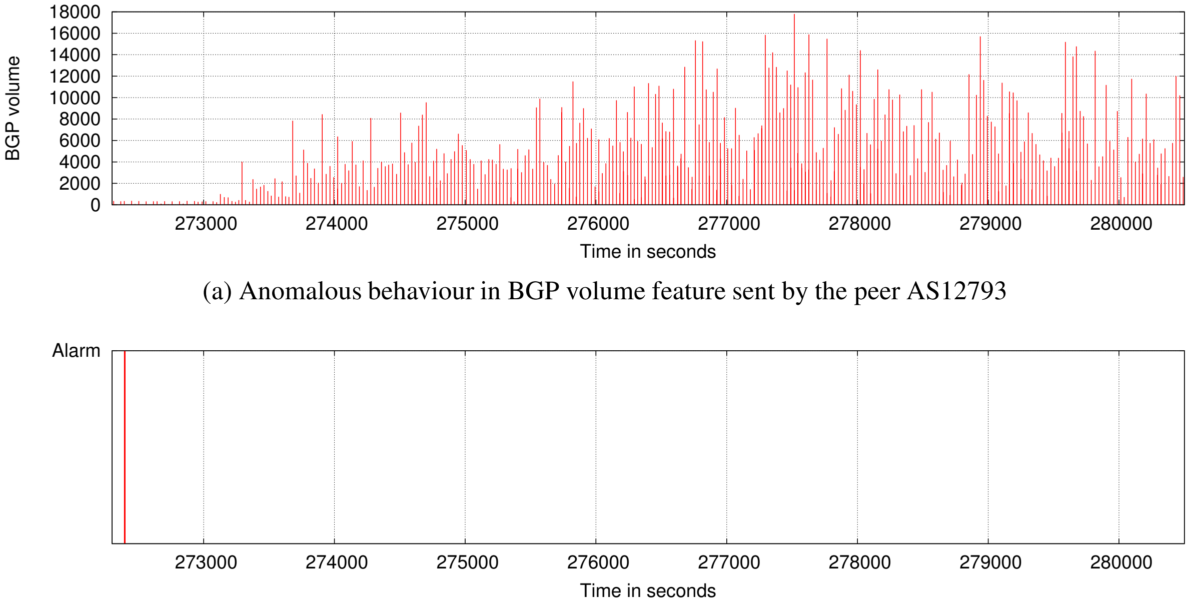


(a) BGP volume feature over one week

(b) Average AS-PATH length feature over one week

(c) Detecting BGP anomalies using RQA scheme

Figure 5.24: BGP features sent by the peer AS12793 during Moscow blackout and its corresponding detection by RQA scheme



(a) Anomalous behaviour in BGP volume feature sent by the peer AS12793

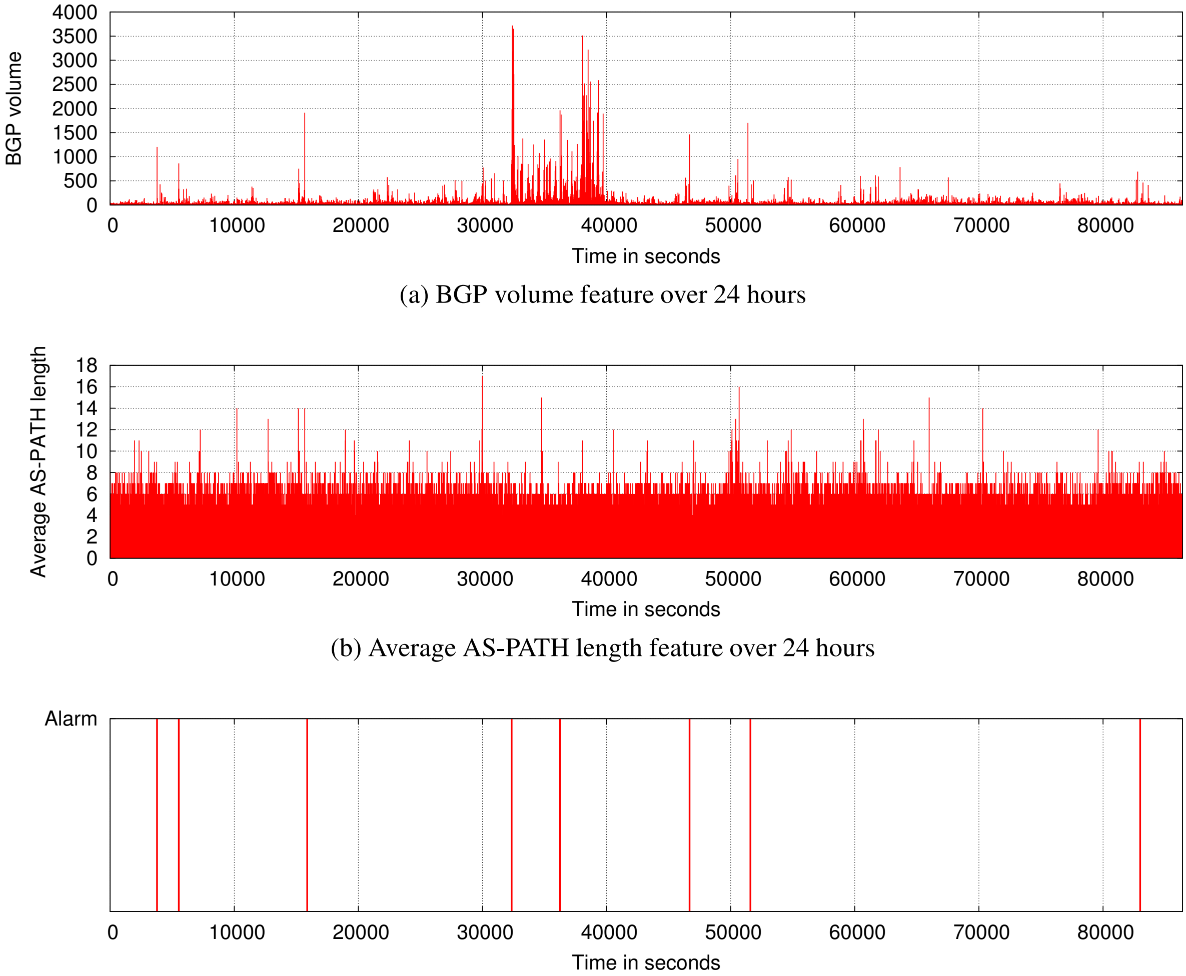
(b) Early detection of BGP anomalies during Moscow blackout

Figure 5.25: Detecting BGP anomaly before 730 seconds of sending high volume of BGP traffic

Our RQA scheme raised 8 alarms during the day of the event. Once again, we do a manual investigation of these alarms, to see if they represent TP or FP alarms, and find they all represent TP alarms. Furthermore, our investigation of delay for the 8 detected alarms shows that although RQA scheme can detect 6 BGP anomalies within 1 second, two anomalies were detected within 199 seconds. Figure 5.27a shows that at time 51388 seconds the peer AS10102 sent a high volume of BGP traffic which RQA scheme does not detect at the start of the window size $(W)$ but can detect at the end of the $W$. Table 5.6 shows the accuracy metrics during TMnet event.

We have used RQA scheme to detect different types of BGP anomalies using our controlled testbed with emulated BGP anomalies and well-known BGP events. RQA scheme demonstrates the ability to detect BGP anomalies including anomalies that have not been recorded before. A summary of our RQA scheme accuracy is shown in Table 5.7 where we can see that RQA scheme detects 46 BGP anomalies with 5 possible FP alarms. Although FPs are often accepted as a fact of life with anomaly detection techniques, identifying FP alarms requires a further investigation by the operators which represents a waste of time and cost[3]. On the other hand, FNs may cause serious consequences to an organisation's reputation and to Internet stability. Dodo [103], Indosat [106], and Turk Telekom [107] events are examples

[3] The average wage rate of supervisory level IT security in the US-based organisations is USD 62.0 per hour [164].

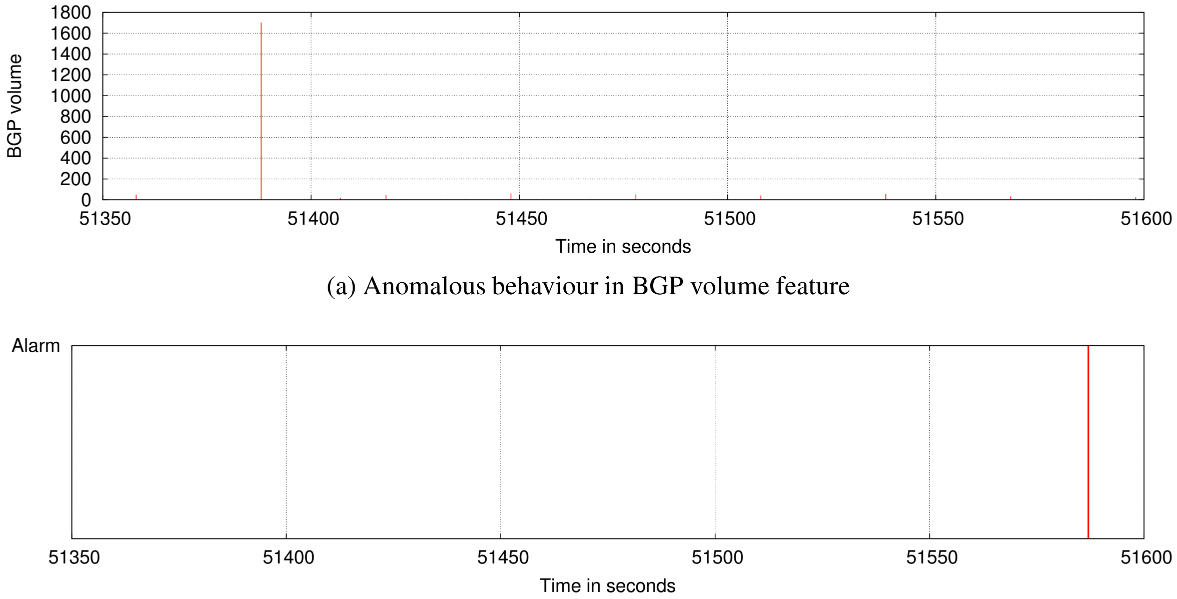


(a) BGP volume feature over 24 hours

(b) Average AS-PATH length feature over 24 hours

(c) Detecting BGP anomalies using RQA scheme

Figure 5.26: BGP features sent by the peer AS10102 during TMnet event and its corresponding detection by RQA scheme



(a) Anomalous behaviour in BGP volume feature

(b) Detection BGP anomalies after 199 seconds of starting the anomalous behaviour

Figure 5.27: Detecting BGP anomalies within 199 seconds as a longest detection delay

of direct unintended BGP anomalies which threatened BGP stability.

In terms of detection delay, RQA scheme detected 46 TP alarms with different delays. RQA scheme detected 22 BGP anomalies within 5 seconds, 18 BGP anomalies within 62 seconds, and only 3 BGP anomalies within 199 seconds as a worst case. Furthermore, RQA can detect hidden anomalous behaviour which may represent an early stage of BGP anomalies as shown in Figures 5.18, 5.23a and 5.25.

Table 5.6: Detection accuracy for TMnet event

| TP | TN | FP | FN | Precision | Sensitivity | Accuracy | F-score |
|---|---|---|---|---|---|---|---|
| 8 | 85205 | 0 | 0 | 1 | 1 | 1 | 1 |

Table 5.7: Summary of detection accuracy of RQA scheme

| TP | TN | FP | FN | Precision | Sensitivity | Accuracy | F-score |
|---|---|---|---|---|---|---|---|
| 46 | 1233739 | 5 | 0 | 0.9012 | 1 | 0.9999 | 0.9484 |

## 5.6 Conclusions

Accidental or deliberate abnormal BGP events such as misconfiguration by ISPs or link failures can affect global routing stability. Recent statistics show some types of BGP anomalies lasted less than 10 minutes but affected 90% of the Internet in less than 2 minutes [23]. These statistics demonstrate the need for real-time BGP anomaly detection that can mitigate the propagation of anomalous BGP traffic. We have introduced our detection scheme to detect BGP anomalies. Our scheme is based on using RQA, an advanced non-linear technique based on using phase plane trajectory, to detect BGP anomalies. RQA scheme is able to differentiate between normal-but-unstable BGP traffic and potentially harmful BGP traffic that can lead to serious BGP events.

We have evaluated our scheme by using BGP traffic collected from our controlled testbed and BGP traffic related to well-know BGP events. RQA scheme can detect these anomalies as well as other hidden anomalous behaviour that has not been observed before. In our experiments, RQA scheme can detect BGP anomalies with 90.12% precision, 99.99% detection accuracy and 94.84% of F-score values. Furthermore, RQA demonstrates an ability to detect early stage anomalous behaviour. In the final chapter, we summarise our research work and outline possible future research directions.

# Chapter 6

# Conclusions and future work

In this thesis we have analysed BGP traffic and have observed that BGP traffic can be understood as an aggregation of oscillations of different frequencies from different ASes. Using linear and nonlinear statistical analysis, we have shown that BGP traffic has recurrent behaviour. The source of this behaviour is unsynchronised periodic behaviour from a set of ASes that we define as unstable ASes. We also define BGP traffic sent by unstable ASes as unstable traffic. Although unstable BGP traffic does not threaten BGP operations, it has the effect of masking anomalous updates that might lead to serious consequences. A technique is required to distinguish between unstable BGP traffic and harmful BGP traffic.

Traffic of this nature is amenable to analysis using recurrence methods. We have applied RQA to notable BGP events and have found that RQA is able to differentiate between normal-but-unstable BGP traffic and potentially harmful BGP traffic that can lead to serious BGP events. As well as examining notable BGP events we have conducted experiments on a controlled testbed to analyse the effectiveness of RQA in detecting BGP anomalies in terms of standard measures of precision, detection accuracy and F-score. We have been able to show that an RQA based scheme can detect BGP anomalies within 62 seconds with 90.12% precision, 99.99% detection accuracy and 94.84% of F-score values.

The research work in this thesis has shown that RQA can give us a better understanding of BGP traffic than has been the case. It allows faster detection of anomalies than other techniques. Nevertheless, there are some weaknesses in the approach. Although RQA detects different types of BGP anomalies within 62 seconds, in some rare cases our RQA scheme requires 199 seconds. Furthermore, RQA scheme requires pre-calculation of RQA parameters (time delay, embedding dimension and RQA threshold) which requires some experience with techniques.

The insight that BGP traffic has recurrent characteristics is perhaps the most important contribution of this thesis. It enables potentially harmful traffic to be identified amongst the large amount of harmless BGP traffic. Future work that this thesis has opened up includes the application of the technique to other protocols. Where a protocol's behaviour has a strong deterministic component RQA may well be of use in detecting anomalous behaviour. In particular other routing protocols and attacks upon them may be detectable using RQA based techniques. Future work may also include fulfilling the remaining requirements for the next generation of BGP anomaly detection discussed in Section 2.5. As well as detecting in real-time for all types of anomalies, it will include differentiating between them, and identifying the source of the anomaly. A further investigation in terms of differentiating between types of BGP anomalies can be done through using other RQA measurements and BGP features and replaying different types of past BGP events under the controlled testbed. The use of RQA for identifying BGP anomalies based on individual unstable prefixes appears to have some potential and is an obvious extension of the work discussed in this thesis.

Other contributions of the thesis include modelling BGP speakers as dynamic systems using the concepts of phase plane trajectories. The outcomes of the modelling show that BGP traffic sent by BGP speakers has the characteristics of being non-linear, deterministic, and stable. We have also classified BGP anomalies into four main categories, direct intended and unintended anomaly, indirect anomaly, and link failure, and have highlighted key requirements for the next generation of BGP anomaly detection techniques.

Ultimately, the purpose of this thesis is to help those responsible for managing networks do so more effectively. Perhaps the most important future work is to translate the insights obtained through this work into software and systems that further that aim.

# References

[1] Information Society Innovation Fund, “ISIF Asia 2016 grant recipients announced!” August 2016. [Online]. Available: https://isif.asia/tag/bgp/

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

[3] 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

[4] B. Al-Musawi, “RTBADT - Real-Time BGP Anomaly Detection Tool V0.1,” January 2018. [Online]. Available: http://caia.swin.edu.au/tools/bgp/brt/rtbadt-0.1.tgz

[5] 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.

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

[7] 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, First quarter 2017.

[8] 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.

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

[10] 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

[11] A. Barbir, S. Murphy, and Y. Yang, "Generic Threats to Routing Protocols," RFC 4593 (Informational), Internet Engineering Task Force, October 2006. [Online]. Available: http://www.ietf.org/rfc/rfc4593

[12] J. Qiu, L. Gao, S. Ranjan, and A. Nucci, "Detecting bogus BGP route information: Going beyond prefix hijacking," in *2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops - SecureComm 2007*, Sept 2007, pp. 381–390.

[13] K. Butler, T. Farley, P. McDaniel, and J. Rexford, "A Survey of BGP Security Issues and Solutions," *Proceedings of the IEEE*, vol. 98, no. 1, pp. 100–122, Jan 2010.

[14] G. Huston, M. Rossi, and G. Armitage, "Securing BGP - A Literature Survey," *Communications Surveys Tutorials, IEEE*, vol. 13, no. 2, pp. 199–222, Second 2011.

[15] S. Kent, C. Lynn, and K. Seo, "Secure Border Gateway Protocol (S-BGP)," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 4, pp. 582–592, April 2000.

[16] G. Huston and G. Michaelson, "Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs)," RFC 6483 (Informational), Internet Engineering Task Force, February 2012. [Online]. Available: http://tools.ietf.org/html/rfc6483

[17] L. Subramanian, V. Roth, I. Stoica, S. Shenker, and R. H. Katz, "Listen and whisper: Security mechanisms for BGP," in *Proceedings of the 1st Conference on Symposium on Networked Systems Design and Implementation - Volume 1*, ser. NSDI'04. Berkeley, CA, USA: USENIX Association, 2004, pp. 10–10.

[18] J. Karlin, S. Forrest, and J. Rexford, "Pretty Good BGP: Improving BGP by Cautiously Adopting Routes," in *Proceedings of the 2006 IEEE International Conference on Network Protocols*, Nov 2006, pp. 290–299.

[19] A. Haeberlen, I. Avramopoulos, J. Rexford, and P. Druschel, "NetReview: Detecting when Interdomain Routing Goes Wrong," in *Proceedings of the 6th USENIX Symposium on Networked Systems Design and Implementation*, ser. NSDI'09. Berkeley, CA, USA: USENIX Association, 2009, pp. 437–452.

[20] S. Goldberg, M. Schapira, P. Hummon, and J. Rexford, “How Secure Are Secure Interdomain Routing Protocols,” *SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 4, pp. 87–98, Aug. 2010.

[21] J. Chandrashekar, Z. Duan, Z.-L. Zhang, and J. Krasky, “Limiting path exploration in BGP,” in *Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies.*, vol. 4, March 2005, pp. 2337–2348 vol. 4.

[22] G. Huston, M. Rossi, and G. Armitage, “A Technique for Reducing BGP Update Announcements through Path Exploration Damping,” *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 8, pp. 1271–1286, October 2010.

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

[24] S. Deshpande, M. Thottan, T. K. Ho, and B. Sikdar, “An Online Mechanism for BGP Instability Detection and Analysis,” *IEEE Transactions on Computers*, vol. 58, no. 11, pp. 1470–1484, Nov 2009.

[25] Y. Rekhter, T. Li, and S. Hares, “A Border Gateway Protocol 4 (BGP-4),” RFC 4271 (Proposed Standard), Internet Engineering Task Force, January 2006. [Online]. Available: http://tools.ietf.org/html/rfc4271

[26] S. Secci, K. Liu, and B. Jabbari, “Efficient inter-domain traffic engineering with transit-edge hierarchical routing,” *Computer Networks*, vol. 57, no. 4, pp. 976–989, 2013.

[27] M. Lad, X. Zhao, B. Zhang, D. Massey, and L. Zhang, “Analysis of BGP Update Surge during Slammer Worm Attack,” in *Distributed Computing - IWDC 2003: 5th International Workshop, Kolkata, India, December 27-30, 2003. Proceedings*, S. R. Das and S. K. Das, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 66–79.

[28] L. Wang, X. Zhao, D. Pei, R. Bush, D. Massey, A. Mankin, S. F. Wu, and L. Zhang, “Observation and Analysis of BGP Behavior Under Stress,” in *Proceedings of the 2Nd ACM SIGCOMM Workshop on Internet Measurment*, ser. IMW ’02. New York, NY, USA: ACM, 2002, pp. 183–195.

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

[30] T. L. Simon, "oof.Panix Sidelined by Incompetence. . . Again," North American Network Operators Group, January 2006. [Online]. Available: https://www.nanog.org/mailinglist/mailarchives/old_archive/2006-01/msg00483.html

[31] J. Schlamp, G. Carle, and E. W. Biersack, "A Forensic Case Study on As Hijacking: The Attacker's Perspective," *SIGCOMM Comput. Commun. Rev.*, vol. 43, no. 2, pp. 5–12, Apr. 2013.

[32] 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.

[33] Y. Zhang and M. Tatipamula, "A Comprehensive Long-Term Evaluation on BGP Performance," in *2011 IEEE International Conference on Communications (ICC)*, June 2011, pp. 1–6.

[34] K. Lougheed and Y. Rekhter, "A Border Gateway Protocol (BGP)," RFC 1105 (Historic), Internet Engineering Task Force, June 1989. [Online]. Available: http://www.ietf.org/rfc/rfc1105.txt

[35] K. Lougheed and Y. Rekhter, "A Border Gateway Protocol (BGP)," RFC 1163 (Historic), Internet Engineering Task Force, June 1990. [Online]. Available: http://www.ietf.org/rfc/rfc1163.txt

[36] K. Lougheed and Y. Rekhter, "A Border Gateway Protocol 3 (BGP-3)," RFC 1267 (Historic), Internet Engineering Task Force, October 1991. [Online]. Available: http://www.ietf.org/rfc/rfc1267.txt

[37] J. Mitchell, "Autonomous System (AS) Reservation for Private Use," RFC 6996 (Best Current Practice), Internet Engineering Task Force, July 2013. [Online]. Available: http://tools.ietf.org/html/rfc6996

[38] Q. Vohra and E. Chen, "BGP Support for Four-Octet Autonomous System (AS) Number Space," RFC 6793 (Proposed Standard), Internet Engineering Task Force, December 2012. [Online]. Available: http://www.ietf.org/rfc/rfc6793.txt

[39] Internet Assinged Number Authority (IANA), "Autonomous System (AS) Numbers," July 2014. [Online]. Available: http://www.iana.org/assignments/as-numbers/as-numbers.xhtml

[40] V. Fuller and T. Li, “Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan,” RFC 4632 (Best Current Practice), Internet Engineering Task Force, August 2006. [Online]. Available: http://tools.ietf.org/html/rfc4632

[41] E. Chen and J. Yuan, “Autonomous-System-Wide Unique BGP Identifier for BGP-4,” RFC 6286 (Proposed Standard), Internet Engineering Task Force, June 2011. [Online]. Available: http://tools.ietf.org/html/rfc6286

[42] J. Hawkinson and T. Bates, “Guidelines for creation, selection, and registration of an Autonomous System (AS),” RFC 1930 (Best Current Practice), Internet Engineering Task Force, March 1996. [Online]. Available: http://tools.ietf.org/html/rfc1930

[43] L. Gao, “On Inferring Autonomous System Relationships in the Internet,” *IEEE/ACM Trans. Netw.*, vol. 9, no. 6, pp. 733–745, Dec. 2001.

[44] R. Oliveira, D. Pei, W. Willinger, B. Zhang, and L. Zhang, “The (In)Completeness of the Observed Internet AS-level Structure,” *IEEE/ACM Transactions on Networking*, vol. 18, no. 1, pp. 109–122, Feb 2010.

[45] M. Caesar and J. Rexford, “BGP routing policies in ISP networks,” *IEEE Network*, vol. 19, no. 6, pp. 5–11, Nov 2005.

[46] 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.

[47] T. Underwood, “Internet-Wide Catastrophe-Last Year,” Renesys Blog, December 2005. [Online]. Available: http://www.renesys.com/2005/12/internetwide-nearcatastrophela/

[48] C. Pelsser, O. Maennel, P. Mohapatra, R. Bush, and K. Patel, “Route Flap Damping Made Usable,” in *Proceedings of the 12th International Conference on Passive and Active Measurement*. Berlin, Heidelberg: Springer, 2011, pp. 143–152.

[49] C. Villamizar, R. Chandra, and R. Govindan, “BGP Route Flap Damping,” RFC 2439 (Standards Track), Internet Engineering Task Force, November 1998. [Online]. Available: http://www.ietf.org/rfc/rfc2439

[50] T. Barber, S. Doran, D. Karrenberg, C. Panigl, and J. Schmitz, “RIPE Routing-WG Recommendation for coordinated route-flap damping parameters,” ripe-178, Februray 1998, obsoleted. [Online]. Available: http://www.ripe.net/ripe/docs/ripe-178

[51] P. Smith and C. Panigl, "RIPE Routing Working Group Recommendations On Route-flap Damping," ripe-378, May 2006, obsoleted. [Online]. Available: http://www.ripe.net/ripe/docs/ripe-378

[52] C. Pelsser, R. Bush, K. Patel, P. Mohapatra, and O. Maennel, "Making Route Flap Damping Usable," RFC 7196 (Proposed Standard), Internet Engineering Task Force, May 2014. [Online]. Available: http://www.ietf.org/rfc/rfc7196

[53] R. Bush, C. Pelsser, M. Kuhne, O. Maennel, P. Mohapatra, K. Patel, R. Evans and Janet, "RIPE Routing Working Group Recommendations On Route-flap Damping," ripe-580, January 2013, obsoletes: ripe-378. [Online]. Available: http://www.ripe.net/ripe/docs/ripe-580

[54] R. White, D. McPherson, and S. Sangli, *Practical BGP*. Redwood City, CA, USA: Addison Wesley Longman Publishing Co., Inc., 2004.

[55] P. Traina, D. McPherson, and J. Scudder, "Autonomous System Confederations for BGP," RFC 5065 (Standards Track), Internet Engineering Task Force, August 2007. [Online]. Available: http://tools.ietf.org/html/rfc5065

[56] K. Sriram, O. Borchert, O. Kim, P. Gleichmann, and D. Montgomery, "A Comparative Analysis of BGP Anomaly Detection and Robustness Algorithms," in *2009 Cybersecurity Applications Technology Conference for Homeland Security*, March 2009, pp. 25–38.

[57] E. Biersack, Q. Jacquemart, F. Fischer, J. Fuchs, O. Thonnard, G. Theodoridis, D. Tzovaras, and P. Vervier, "Visual analytics for BGP monitoring and prefix hijacking identification," *IEEE Network*, vol. 26, no. 6, pp. 33–39, November 2012.

[58] University of Oregon, "University of Oregon Route Views Project." [Online]. Available: http://www.routeviews.org/

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

[60] H. Yan, R. Oliveira, K. Burnett, D. Matthews, L. Zhang, and D. Massey, "BGPmon: A Real-Time, Scalable, Extensible Monitoring System," in *2009 Cybersecurity Applications Technology Conference for Homeland Security*, March 2009, pp. 212–223.

[61] N. M. Al-Rousan and L. Trajkovic, "Machine learning models for classification of BGP anomalies," in *2012 IEEE 13th International Conference on High Performance Switching and Routing*. IEEE, 2012, pp. 103–108.

[62] J. Mai, L. Yuan, and C.-N. Chuah, “Detecting BGP anomalies with wavelet,” in *NOMS 2008 - 2008 IEEE Network Operations and Management Symposium*, April 2008, pp. 465–472.

[63] 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

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

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

[66] J. Li, D. Dou, Z. Wu, S. Kim, and V. Agarwal, “An Internet Routing Forensics Framework for Discovering Rules of Abnormal BGP Events,” *SIGCOMM Comput. Commun. Rev.*, vol. 35, no. 5, pp. 55–66, Oct. 2005.

[67] A. Sapegin and S. Uhlig, “On the Extent of Correlation in BGP Updates in the Internet and What It Tells Us About Locality of BGP Routing Events,” *Computer Communications*, vol. 36, no. 15, pp. 1592–1605, 2013.

[68] J. Wu, Z. M. Mao, J. Rexford, and J. Wang, “Finding a Needle in a Haystack: Pinpointing Significant BGP Routing Changes in an IP Network,” 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. 1–14.

[69] M. Rossi, “MRT dump file manipulation toolkit (MDFMT) - version 0.2,” Centre for Advanced Internet Architectures, Swinburne University of Technology, Melbourne, Australia, Tech. Rep. 090730B, 30 July 2009. [Online]. Available: http://caia.swin.edu.au/reports/090730B/CAIA-TR-090730B.pdf

[70] D. Blazakis, M. Karir, and J. Baras, “BGP-Inspect - Extracting Information from Raw BGP Data,” in *Network Operations and Management Symposium, 2006. NOMS 2006. 10th IEEE/IFIP*, April 2006, pp. 174–185.

[71] G. Di Battista, F. Mariani, M. Patrignani, and M. Pizzonia, “BGPlay: A System for Visualizing the Interdomain Routing Evolution,” in *Graph Drawing: 11th International Symposium, GD 2003 Perugia, Italy, September 21-24, 2003 Revised Papers*, G. Liotta, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 295–306.

[72] F. Fischer, J. Fuchs, P.-A. Vervier, F. Mansmann, and O. Thonnard, “VisTracer: A Visual Analytics Tool to Investigate Routing Anomalies in Traceroutes,” in *Proceedings of the Ninth International Symposium on Visualization for Cyber Security*, ser. VizSec ’12. New York, NY, USA: ACM, 2012, pp. 80–87.

[73] Y.-J. Chi, R. Oliveira, and L. Zhang, “Cyclops: The AS-level Connectivity Observatory,” *SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 5, pp. 5–16, Sep. 2008.

[74] X. Hu and Z. Mao, “Accurate Real-time Identification of IP Prefix Hijacking,” in *2007 IEEE Symposium on Security and Privacy (SP ’07)*, May 2007, pp. 3–17.

[75] M. Lad, D. Massey, D. Pei, Y. Wu, B. Zhang, and L. Zhang, “PHAS: A Prefix Hijack Alert System,” in *Proceedings of the 15th Conference on USENIX Security Symposium - Volume 15*, ser. USENIX-SS’06. Berkeley, CA, USA: USENIX Association, 2006.

[76] C. Zheng, L. Ji, D. Pei, J. Wang, and P. Francis, “A Light-weight Distributed Scheme for Detecting IP Prefix Hijacks in Real-time,” in *Proceedings of the 2007 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, ser. SIGCOMM ’07. New York, NY, USA: ACM, 2007, pp. 277–288.

[77] Z. Zhang, Y. Zhang, Y. Hu, Z. Mao, and R. Bush, “iSPY: Detecting IP Prefix Hijacking on My Own,” *IEEE/ACM Transactions on Networking*, vol. 18, no. 6, pp. 1815–1828, Dec 2010.

[78] Internet Routing Registry. [Online]. Available: http://www.irr.net/

[79] L. Blunk, J. Damas, F. Parent, and A. Robachevsky, “Routing Policy Specification Language (RPSL),” RFC 4012(Standards Track), Internet Engineering Task Force, March 2005. [Online]. Available: http://tools.ietf.org/html/rfc4012

[80] APNIC Whois Database. [Online]. Available: http://wq.apnic.net/apnic-bin/whois.pl

[81] G. Siganos and M. Faloutsos, “Analyzing BGP Policies: Methodology and Tool,” in *IEEE INFOCOM 2004*, vol. 3, March 2004, pp. 1640–1651 vol.3.

[82] The Team Cymru Route-server, “IP TO ASN MAPPING.” [Online]. Available: http://www.team-cymru.org/IP-ASN-mapping.html

[83] R. Mahajan, D. Wetherall, and T. Anderson, “Understanding BGP Misconfiguration,” *SIGCOMM Comput. Commun. Rev.*, vol. 32, no. 4, pp. 3–16, Aug. 2002.

[84] M. Cotton, L. Vegoda, R. Bonica, and A. B. Haberman, “Special-Purpose IP Address Registries,” RFC 6890 (Best Current Practice), Internet Engineering Task Force, April 2013. [Online]. Available: http://tools.ietf.org/html/rfc6890

[85] Team Cymru Community Services, “Bogon Route Server Project (Bogons via BGP).” [Online]. Available: http://www.team-cymru.org/Services/Bogons/bgp.html

[86] Bogon Report. [Online]. Available: http://www.cidr-report.org/bogons/

[87] The Team Cymru Route-server, “TEAM CYMRU-Bogon Route Announcements.” [Online]. Available: http://www.cymru.com/BGP/bogons.html

[88] MaxMind GeoLite Country: Open Source IP Address to Country Database. [Online]. Available: http://dev.maxmind.com/geoip/legacy/geolite/

[89] IP2location database. [Online]. Available: http://www.ip2location.com/

[90] A. Dainotti, C. Squarcella, E. Aben, K. C. Claffy, M. Chiesa, M. Russo, and A. Pescapé, “Analysis of Country-wide Internet Outages Caused by Censorship,” *IEEE/ACM Transactions on Networking*, vol. 22, no. 6, pp. 1964–1977, Dec. 2014.

[91] Center for Applied Internet Data Analysis (CAIDA), “Archipelago Measurement Infrastructure.” [Online]. Available: http://www.caida.org/projects/ark/

[92] A. Feldmann, O. Maennel, Z. M. Mao, A. Berger, and B. Maggs, “Locating Internet Routing Instabilities,” *SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 4, pp. 205–218, Aug. 2004.

[93] S. Deshpande, M. Thottan, and B. Sikdar, “An online scheme for the isolation of BGP misconfiguration errors,” *IEEE Transactions on Network and Service Management*, vol. 5, no. 2, pp. 78–90, June 2008.

[94] Q. Gu, Z. Li, and J. Han, “Generalized Fisher Score for Feature Selection,” in *Proceedings of the Twenty-Seventh Conference on Uncertainty in Artificial Intelligence*, ser. UAI’11. Arlington, Virginia, United States: AUAI Press, 2011, pp. 266–273.

[95] H. Peng, F. Long, and C. Ding, “Feature Selection Based on Mutual Information Criteria of Max-Dependency, Max-Relevance, and Min-Redundancy,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 27, no. 8, pp. 1226–1238, Aug 2005.

[96] I. de Urbina Cazenave, E. Kosluk, and M. Ganiz, "An Anomaly Detection Framework for BGP," in *2011 International Symposium on Innovations in Intelligent Systems and Applications*, June 2011, pp. 107–111.

[97] M. Wubbeling, M. Meier, and T. Elsner, "Inter-AS Routing Anomalies: Improved Detection and Classification," in *2014 6th International Conference On Cyber Conflict (CyCon 2014)*. IEEE, 2014, pp. 223–238.

[98] H. Ballani, P. Francis, and X. Zhang, "A Study of Prefix Hijacking and Interception in the Internet," *SIGCOMM Comput. Commun. Rev.*, vol. 37, no. 4, pp. 265–276, Aug. 2007.

[99] T. Wan and P. Van Oorschot, "Analysis of BGP Prefix Origins During Google's May 2005 Outage," in *Proceedings 20th IEEE International Parallel Distributed Processing Symposium*, April 2006, pp. 8–pp.

[100] Micron21 Datacentre, "Micron21 DDoS Soak and Scrub as a Service." [Online]. Available: http://www.micron21.com/ddos-soak-scrub.php

[101] X. Zhao, D. Pei, L. Wang, D. Massey, A. Mankin, S. F. Wu, and L. Zhang, "An Analysis of BGP Multiple Origin AS (MOAS) Conflicts," in *Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement*, ser. IMW '01. New York, NY, USA: ACM, 2001, pp. 31–35.

[102] IETF, "Charter of the IETF Secure Inter-Domain Routing Working Group." [Online]. Available: http://tools.ietf.org/wg/sidr/charters

[103] G. Huston, "Leaking Routes," March 2012. [Online]. Available: http://www.potaroo.net/ispcol/2012-03/leaks.html

[104] I. Shrubbery Networks, "RANCID - Really Awesome New Cisco conflg Differ," 2004. [Online]. Available: http://www.shrubbery.net/rancid/

[105] A. Lutu, M. Bagnulo, and O. Maennel, "The BGP Visibility Scanner," in *2013 Proceedings IEEE INFOCOM*, April 2013, pp. 115–120.

[106] E. Zmijewski, "Indonesia Hijacks the World," Renesys Blog, April 2014. [Online]. Available: http://www.renesys.com/2014/04/indonesia-hijacks-world/

[107] A. Toonk, "Turkey Hijacking IP addresses for popular Global DNS providers," March 2014. [Online]. Available: http://www.bgpmon.net/turkey-hijacking-ip-addresses-for-popular-global-dns-providers/

[108] S. Bortzmeyer, “Who has AS 1712?” North American Network Operators Group, November 2009. [Online]. Available: http://seclists.org/nanog/2009/Nov/647

[109] D. Madory, “Bonjour, Y’all! ASN Split Personalities,” Dyn Research, December 2009. [Online]. Available: http://research.dyn.com/2009/12/bonjour-yall-asn-split-persona/

[110] S. Deshpande, M. Thottan, and B. Sikdar, “Early Detection of BGP Instabilities Resulting from Internet Worm Attacks,” in *Global Telecommunications Conference, 2004. GLOBECOM ’04. IEEE*, vol. 4, Nov 2004, pp. 2266–2270 Vol.4.

[111] S. Staniford, V. Paxson, and N. Weaver, “How to Own the Internet in Your Spare Time,” in *Proceedings of the 11th USENIX Security Symposium*. Berkeley, CA, USA: USENIX Association, 2002, pp. 149–167.

[112] A. Roudnev, “Re: More on Moscow power failure( was RE: Moscow: global power outage),” North American Network Operators Group, May 2005. [Online]. Available: https://www.nanog.org/mailinglist/mailarchives/old_archive/2005-05/msg00767.html

[113] Y. Liu, X. Luo, R. K. Chang, and J. Su, “Characterizing Inter-Domain Rerouting by Betweenness Centrality after Disruptive Events,” *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 6, pp. 1147–1157, 2013.

[114] T. Bilski, “Disaster’s Impact on Internet Performance–Case Study,” in *Computer Networks*, ser. Communications in Computer and Information Science. Springer Berlin Heidelberg, 2009, vol. 39, pp. 210–217.

[115] T. Qiu, L. Ji, D. Pei, J. Wang, J. Xu, and H. Ballani, “Locating Prefix Hijackers Using LOCK,” in *Proceedings of the 18th Conference on USENIX Security Symposium*, ser. SSYM’09. Berkeley, CA, USA: USENIX Association, 2009, pp. 135–150.

[116] C. Labovitz, G. R. Malan, and F. Jahanian, “Internet Routing Instability,” *IEEE/ACM Trans. Netw.*, vol. 6, no. 5, pp. 515–528, Oct. 1998.

[117] P. Bloomfield, *Fourier Analysis of Time Series: An Introduction*. John Wiley & Sons, 2004.

[118] P. Abry and D. Veitch, “Wavelet Analysis of Long-Range-Dependent Traffic,” *IEEE Transactions on Information Theory*, vol. 44, no. 1, pp. 2–15, Jan 1998.

[119] J. Zhang, J. Rexford, and J. Feigenbaum, “Learning-based Anomaly Detection in BGP Updates,” in *Proceedings of the 2005 ACM SIGCOMM Workshop on Mining Network Data*, ser. MineNet ’05. New York, NY, USA: ACM, 2005, pp. 219–220.

[120] Y. Xie, H.-A. Kim, D. R. O'Hallaron, M. K. Reiter, and H. Zhang, "Seurat: A Pointillist Approach to Anomaly Detection," in *Recent Advances in Intrusion Detection*, ser. Lecture Notes in Computer Science, E. Jonsson, A. Valdes, and M. Almgren, Eds. Springer Berlin Heidelberg, 2004, vol. 3224, pp. 238–257.

[121] B. A. Prakash, N. Valler, D. Andersen, M. Faloutsos, and C. Faloutsos, "BGP-lens: Patterns and Anomalies in Internet Routing Updates," in *Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, ser. KDD '09. New York, NY, USA: ACM, 2009, pp. 1315–1324.

[122] D. Vernon, *Machine Vision: Automated Visual Inspection and Robot Vision*. Prentice Hall, 1991.

[123] 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.

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

[125] I. H. Witten, E. Frank, and M. A. Hall, *Data Mining: Practical Machine Learning Tools and Techniques*, 3rd ed. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2011.

[126] J. Cowie, A. T. Ogielski, B. Premore, E. Smith, and T. Underwood, "Impact of the 2003 blackouts on internet communications," *Preliminary Report, Renesys Corporation (updated March 1, 2004)*, 2003.

[127] R. J. Elliott, L. Aggoun, and J. B. Moore, *Hidden Markov Models*. Springer, 1994.

[128] A. Lutu, M. Bagnulo, J. Cid-Sueiro, and O. Maennel, "Separating Wheat from Chaff: Winnowing Unintended Prefixes Using Machine Learning," in *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, April 2014, pp. 943–951.

[129] Y. Freund and R. E. Schapire, "A Desicion-Theoretic Generalization of On-line Learning and an Application to Boosting," in *Computational learning theory*. Springer, 1995, pp. 23–37.

[130] 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.

[131] M. Roughan, T. Griffin, M. Mao, A. Greenberg, and B. Freeman, “Combining Routing and Traffic Data for Detection of IP Forwarding Anomalies,” in *Proceedings of the Joint International Conference on Measurement and Modeling of Computer Systems*, ser. SIGMETRICS ’04/Performance ’04. New York, NY, USA: ACM, 2004, pp. 416–417.

[132] M. Ganiz, S. Kanitkar, M.-C. Chuah, and W. Pottenger, “Detection of Interdomain Routing Anomalies Based on Higher-Order Path Analysis,” in *Sixth International Conference on Data Mining (ICDM’06)*, Dec 2006, pp. 874–879.

[133] G. Theodoridis, O. Tsigkas, and D. Tzovaras, “A Novel Unsupervised Method for Securing BGP Against Routing Hijacks,” in *Computer and Information Sciences III*. Springer London, 2013, pp. 21–29.

[134] S. Papadopoulos, G. Theodoridis, and D. Tzovaras, “BGPfuse: Using Visual Feature Fusion for the Detection and Attribution of BGP Anomalies,” in *Proceedings of the Tenth Workshop on Visualization for Cyber Security*, ser. VizSec ’13. New York, NY, USA: ACM, 2013, pp. 57–64.

[135] Y. Xiang, Z. Wang, X. Yin, and J. Wu, “Argus: An Accurate and Agile System to Detecting IP Prefix Hijacking,” in *Network Protocols (ICNP), 2011 19th IEEE International Conference on*, Oct 2011, pp. 43–48.

[136] H. V. Madhyastha, T. Isdal, M. Piatek, C. Dixon, T. Anderson, A. Krishnamurthy, and A. Venkataramani, “iPlane: An Information Plane for Distributed Services,” in *Proceedings of the 7th Symposium on Operating Systems Design and Implementation*, ser. OSDI ’06. Berkeley, CA, USA: USENIX Association, 2006, pp. 367–380.

[137] S. Sanfilippo, “hping,” 2006. [Online]. Available: http://www.hping.org/

[138] G. Fyodor, “Nmap,” 2006. [Online]. Available: http://www.nmap.org/

[139] S. Branigan, H. Burch, B. Cheswick, and F. Wojcik, “What Can You Do with Traceroute?” *IEEE Internet Computing*, vol. 5, no. 5, p. 96, 2001.

[140] Y. C. Hu, “iTraceroute,” Purdue University, West Lafayette, 2009. [Online]. Available: https://engineering.purdue.edu/~ychu/itraceroute/

[141] B. Augustin, X. Cuvellier, B. Orgogozo, F. Viger, T. Friedman, M. Latapy, C. Magnien, and R. Teixeira, “Avoiding Traceroute Anomalies with Paris Traceroute,” in *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*. ACM, 2006, pp. 153–158.

[142] M. Tahara, N. Tateishi, T. Oimatsu, and S. Majima, “A Method to Detect Prefix Hijacking by Using Ping Tests,” in *Proceedings of the 11th Asia-Pacific Symposium on Network Operations and Management: Challenges for Next Generation Network Operations and Service Management*, ser. APNOMS ’08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 390–398.

[143] J.-P. Eckmann, S. O. Kamphorst, and D. Ruelle, “Recurrence Plots of Dynamical Systems,” *Europhys. Lett*, vol. 4, no. 9, pp. 973–977, 1987.

[144] F. Palmieri and U. Fiore, “Network Anomaly Detection Through Nonlinear Analysis,” *Computers & Security*, vol. 29, no. 7, pp. 737–755, 2010.

[145] N. Kanaskar, R. Seker, J. Bian, and V. V. Phoha, “Dynamical System Theory for the Detection of Anomalous Behavior in Computer Programs,” *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 42, no. 6, pp. 1579–1589, Nov 2012.

[146] H. Kantz and T. Schreiber, *Nonlinear Time Series Analysis*. Cambridge university press, 2004, vol. 7.

[147] C. L. Webber Jr and J. P. Zbilut, “Recurrence Quantification Analysis of Nonlinear Dynamical Systems,” *Tutorials in contemporary nonlinear methods for the behavioral sciences*, pp. 26–94, 2005.

[148] M. T. Rosenstein, J. J. Collins, and C. J. De Luca, “A practical method for calculating largest Lyapunov exponents from small data sets,” *Physica D: Nonlinear Phenomena*, vol. 65, no. 1, pp. 117–134, 1993.

[149] H. Kantz, “A robust method to estimate the maximal Lyapunov exponent of a time series,” *Physics letters A*, vol. 185, no. 1, pp. 77–87, 1994.

[150] 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.

[151] D. T. Kaplan, “Exceptional events as evidence for determinism,” *Physica D: Nonlinear Phenomena*, vol. 73, no. 1, pp. 38–48, 1994.

[152] T. Gautama, D. P. Mandic, and M. M. Van Hulle, “The delay vector variance method for detecting determinism and nonlinearity in time series,” *Physica D: Nonlinear Phenomena*, vol. 190, no. 3, pp. 167–176, 2004.

[153] N. Marwan and J. Webber, CharlesL., "Mathematical and Computational Foundations of Recurrence Quantifications," in *Recurrence Quantification Analysis*, ser. Understanding Complex Systems. Springer International Publishing, 2015, pp. 3–43.

[154] J. P. Zbilut and C. L. Webber, "Embeddings and delays as derived from quantification of recurrence plots," *Physics Letters A*, vol. 171, no. 3, pp. 199 – 203, 1992.

[155] A. Elmokashfi, A. Kvalbein, and C. Dovrolis, "BGP Churn Evolution: A Perspective from the Core," *IEEE/ACM Transactions on Networking*, vol. 20, no. 2, pp. 571–584, 2012.

[156] A. Flavel, O. Maennely, B. Chiera, M. Roughan, and N. Bean, "CleanBGP: Verifying the Consistency of BGP Data," in *2008 IEEE Internet Network Management Workshop (INM)*, Oct 2008, pp. 1–6.

[157] M. Vlachos, S. Y. Philip, and V. Castelli, "On Periodicity Detection and Structural Periodic Similarity," in *Proceedings of the 2005 SIAM International Conference on Data Mining*, vol. 5. SIAM, 2005, pp. 449–460.

[158] Asia Pacific Network Information Centre(APNIC), "BGP in 2016." [Online]. Available: https://labs.apnic.net/?p=952

[159] T. G. Griffin and G. Wilfong, "Analysis of the MED Oscillation Problem in BGP," in *10th IEEE International Conference on Network Protocols, 2002. Proceedings*. IEEE, 2002, pp. 90–99.

[160] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly Detection: A Survey," *ACM Comput. Surv.*, vol. 41, no. 3, pp. 15:1–15:58, Jul. 2009.

[161] H. Nguyen, M. Roughan, S. Knight, N. Falkner, O. Maennel, and R. Bush, "How to Build Complex, Large-Scale Emulated Networks," in *Testbeds and Research Infrastructures. Development of Networks and Communities*. Springer, 2010, pp. 3–18.

[162] K. Ishiguro, "Quagga Routing Suite." [Online]. Available: http://www.nongnu.org/quagga/

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

[164] "The Cost of Malware Containment," Ponemon Institute, Tech. Rep., January 2015. [Online]. Available: https://www.ponemon.org/local/upload/file/Damballa%20Malware%20Containment%20FINAL%203

[165] Google Project Hosting, “Simple BGP Peering and Route Injection Script,” February 2016. [Online]. Available: https://code.google.com/archive/p/bgpsimple/

# Appendix A

# BGP replay tool

## A.1 Introduction

This chapter describes the operation of BGP replay tool v0.2 (BRT v0.2) [3], a tool for UNIX and Windows operating systems providing the ability to replay previously BGP updates downloaded from the public route repositories or local log files to test variety of operations. Replying past BGP incidents into a control testbed helps to classify BGP traffic, understand BGP behaviour at BGP speakers level and finally investigating BGP behaviour with different routers Operating Systems (OSs) such as Cisco, Juniper, and Quagga. BRT v0.2 extends the ability BRT v0.1 [2] to peer with different BGP speakers operating systems such as Quagga [162] and real Cisco routers. It is also supporting IPV6 and connecting to multiple peers. The evaluation of the BRT v0.2 has been made using three different types of testbeds. These include real Cisco routers, VIRL [5], an emulation platform by Cisco, and Quagga using generated BGP updates and past BGP anomalies incidents. Comparing with other BGP replay and inject tools, BRT v0.2 does not require kernel modification at host's OS, supports different BGP attributes, supports sending IPv6 BGP updates and peering over IPv6. The evaluation of this tool has been done using real Cisco routers, Quagga and VIRL as controlled testbeds.

BRT v0.2 uses Net::BGP, a module of Perl software, to implement BGP. Net::BGP provides the required functionality to establish BGP peering and exchanging BGP updates. However, Net::BGP does not support BGP updates for IPv6 neither BGP connection over IPv6. Therefore, we develop a patch that supports BGP updates for IPv6 based on using Multiprotocol Reachable Network Layer Reachability Information (NLRI) and Multi-protocol Unreachable NLRI, BGP attributes described in [**?** ]. We also provide a script to calculate nine BGP features for comparing injected and collected BGP updates. These features are total number of IPV4 and IPv6 announcements, IPv4 and IPv6 withdrawals, maximum and average length of AS-PATH, total number of announcements, total number of withdrawals, and

```
BGP4MP|1456214400|A|213.144.128.203|13030|179.125.45.0/24|13030 4230 263629|IGP|213.144.128.203|0|1|13030:1 13030:1013 13030:51904 13030:7184|NAG||
BGP4MP|1456214400|A|213.144.128.203|13030|179.125.46.0/24|13030 4230 263629|IGP|213.144.128.203|0|1|13030:1 13030:1013 13030:51904 13030:7184|NAG||
BGP4MP|1456214444|W|137.164.16.84|2152|95.85.96.0/19
BGP4MP|1456214444|W|137.164.16.84|2152|103.193.104.0/22
BGP4MP|1456214444|W|137.164.16.84|2152|205.71.208.0/20
```

Figure A.1: Example of bgpdump tool with [-m] option

total number of announcements and withdrawals.

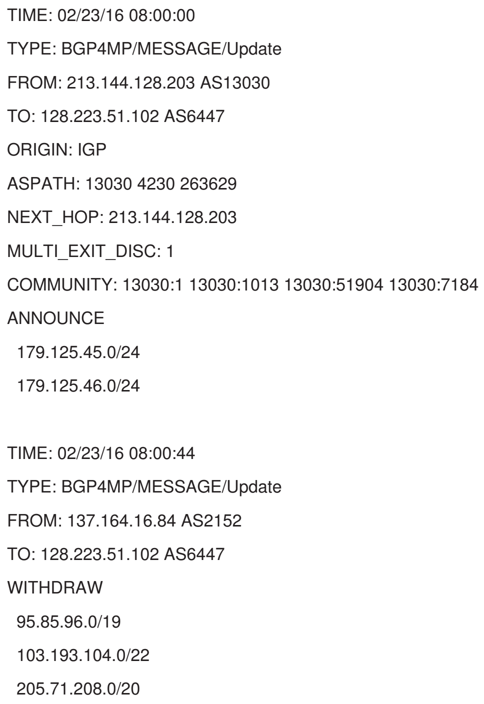
This rest of this chapter is organised as follows: Section A.2 shows the operation of BGP replay tool. Section A.3 contains detailed information about configuration setup for the emulator while in section A.4 represents our evaluation using different controlled testbeds. In section A.5, we conclude our work and outline future directions.

## A.2 BGP replay tool

BRT v0.2 is a Perl script that allows to setup a BGP adjacency with BGP peer. BRT v0.2 enables users to send out BGP updates from a predefined BGP update file. This tool can help researchers and operators to understand BGP behaviour in different circumstances. BGP session and message handling are done by Net::BGP v0.16, a Perl module that implements BGP inter-domain routing protocol. Officially, Net::BGP v0.16 does not support IPv6 BGP updates neither IPv6 BGP peer connection. The Center for Applied Internet Data Analysis (CAIDA) [**?** ] 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 [**?** ]. However, this patch does not support IPv6 prefix withdrawn and required BGP speakers with ADD-PATH capability, an extension to BGP protocol described in [**?** ] 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 at [3].

The input of the BRT v0.2 tool is a human readable BGP updates with Unix time stamps. Tools such as bgpdump [64] and pybgpdump [65] are used to convert BGP updates format (MRT), non readable format, to readable format. For example, the bgpdump tool provides three options of conversion, this include [-H], [-m], and [-M] options. The [-H] option is the default option and used to convert MRT file to multi-line human readable. The [-m] option is used to produce one-line per entry with Unix time stamps while [-M] produce one-line per entry with human readable time stamps. 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.



```
TIME: 02/23/16 08:00:00
TYPE: BGP4MP/MESSAGE/Update
FROM: 213.144.128.203 AS13030
TO: 128.223.51.102 AS6447
ORIGIN: IGP
ASPATH: 13030 4230 263629
NEXT_HOP: 213.144.128.203
MULTI_EXIT_DISC: 1
COMMUNITY: 13030:1 13030:1013 13030:51904 13030:7184
ANNOUNCE
  179.125.45.0/24
  179.125.46.0/24

TIME: 02/23/16 08:00:44
TYPE: BGP4MP/MESSAGE/Update
FROM: 137.164.16.84 AS2152
TO: 128.223.51.102 AS6447
WITHDRAW
  95.85.96.0/19
  103.193.104.0/22
  205.71.208.0/20
```

Figure A.2: Example of bgpdump tool with [-H] option

BRT v0.2 tool has optional and mandatory command line arguments as shown in Table A.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.

A simple example for using the BRT for a simple BGP topology shown in Figure A.3 is:

```
$ perl brt-0.2.pl -brtas 65001 -brtip 172.16.2.2 -peeras 65002 -peerip
   172.16.2.1 -f BGP_updates
```

BRT v0.2 also supports replay BGP updates to multiple BGP peers at once by storing BRT v0.2 tool arguments (command line arguments) for each peer as a line in a text file and specify that file to the tool after '-m' argument. In this case, we only need two arguments. That is, <-f> to specify BGP updates file and <-m> to specify all other mandatory and optional attributes. For example, the content of <-m> file for the topology shown in Figure A.4 is:

Table A.1: BRT v0.2 tool command line arguments

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

```
-brtas 65001 -brtip 172.16.1.100 -brtipv6 fc00:3::1 -peeras 65002 -
   peerip 172.16.1.200 -peeripv6 fc00:3::2
-brtas 65001 -brtip 172.16.1.100 -brtipv6 fc00:3::1 -peeras 65003 -
   peerip 172.16.1.201 -peeripv6 fc00:3::3
```

BRT v0.2 is highly experimental, and could be improved and extended in many ways. BRT v0.2 has been used and tested on IPV4 and IPv6 peers with Quagga, real Cisco routers and VIRL as peer BGP speakers but it may also work with other BGP speakers such as Juniper routers.

Table A.2: Comparison among BGP tools

| Feature | MDFMT | bgpsimple | BRT v0.2 |
|---|---|---|---|
| Replay BGP update with time stamp | Yes | No | Yes |
| Require modification in the Kernel | Yes | No | No |
| Supporting multiple attributes | No | No | Yes |
| Supporting IPV6 | No | No | Yes |
| Supporting connection to multiple peers | No | No | Yes |
| Checking AS number with the implemented topology | No | No | Yes |

Table A.2 shows a comparison of techniques described in [69, 165] as well as our tool.

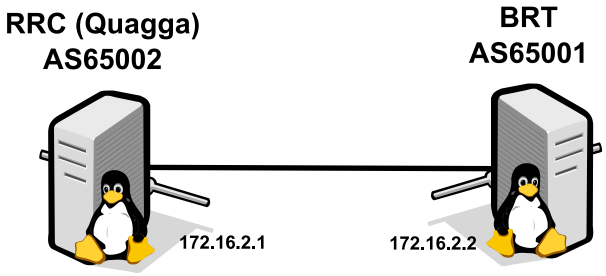


Figure A.3: Simple topology with only RRC

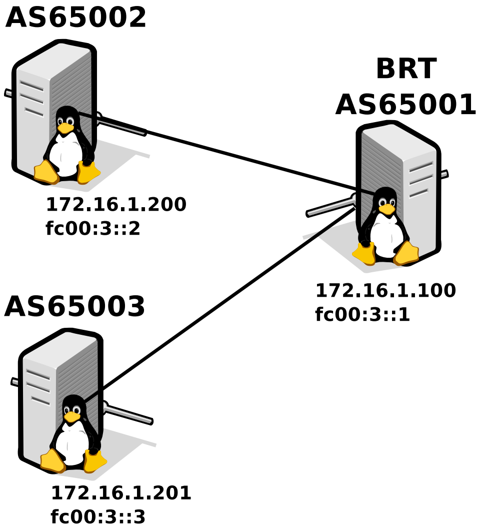


Figure A.4: An example of peering BRT with two peers

MRT Dump File Manipulation Toolkit (MDFMT) [69] is a pseudo BGP speaker. It requires kernel modification at host's OS to replay past BGP updates. MDFMT does not support IPv6 peer connection neither IPv6 BGP updates. It also does not support many BGP attributes such as the community attribute. bgpsimple is a tool to inject BGP updates from a selected file. This tool does not send BGP updates based on time stamp. bgpsimple does not also support IPv6 for BGP updates and peering. In contrast, the BRT v0.2 tool does not require modification in the kernel of host's OS and support many attributes. Furthermore, BRT v0.2 supports sending IPv6 BGP updates and supports BGP peering over IPv6. It also supports many BGP attributes such as the community, aggregation, and MED.

## A.3 Emulator setup

To emulate past BGP updates with a controlled testbed network, we use BRT v0.2 to inject past BGP updates and RRC to collect BGP updates. Figure A.3 shows a simple topology to replay BGP updates and check the received data. RRC needs Quagga to be installed. Quagga

Table A.3: Quagga BGP configuration at RRC

| | |
|---|---|
| dump bgp updates updates.dump | Dump BGP updates to file updates.dump in the current directory. It is necessary that the output directory exists and is writable by Quagga. |
| debug bgp | Enable logging |
| debug bgp events | Enable logging of BGP events |
| debug bgp updates | Enable logging of BGP advertisements |
| router bgp 65002 | Set AS number 65002 for the RRC |
| bgp router-id 172.16.2.1 | Set router ID 172.16.2.1 to the RRC |
| bgp log-neighbor-changes | Enable logging of BGP neighbor status changes (up or down) |
| neighbor 172.16.2.2 remote-as 65001 | Set 172.16.2.2 as a peer AS65002 |
| neighbor 172.16.2.2 filter-list 20 out | Do not send back BGP updates to BRT. |
| address-family ipv6 | Configure IPv6 BGP |
| neighbor 172.16.2.2 activate | Activate172.16.2.2 peer to use IPv6 updates |
| exit-address-family | Finish IPv6 BGP configurations |
| ip as-path access-list 20 deny .* | Applies the filter-list 20 to all addresses |

is a routing software package that provides TCP/IP based routing services for different protocols such as OSPF, IS-IS, and BGP [162]. Quagga is made from several daemons that work together to build the routing table. These daemons include ospfd, ripd, bgpd, and zebra where zebra represents the kernel routing manager. Figure A.5 shows Quagga system architecture.

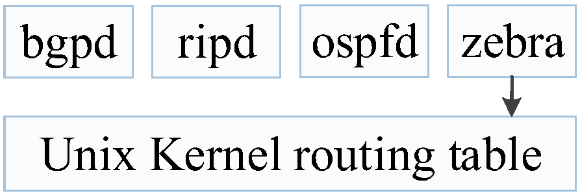


Figure A.5: Quagga system architecture

RRC runs Ubuntu 14.04 LTS and Quagga version 0.99.23.1. The configuration files for Quagga installed in Ubuntu OS is under /etc/quagga where /etc/quagga/Quagga.conf is the configuration file of configuring routing. Table A.3 shows an example of /etc/quagga/Quagga.conf to establish a peer connection between RRC and AS65001 for the topology shown in Figure A.3.

BRT v0.2 requires using Net::BGP, a module of Perl software. Additionally, IO::Socket::INET6 module should be installed to add support for IPv6 BGP connection for the patched Net::BGP module. These modules can be installed as follows:

```
#perl -MCPAN -e shell
cpan[1]> install Net::BGP
cpan[1]> install IO::Socket::INET6
```

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:

```
# tar xzfv ipv6_bgpnet-0.1.tgz
# cd ipv6_bgpnet-0.1
# ./patch.sh
```

## A.4 Evaluation

We evaluate the functionality of BRT v0.2 with three different types of testbeds. These include Quagga, VIRL, and real Cisco routers. VIRL is a powerful network emulation system uses Linux KVM hypervisor, OpenStack, and a set of virtual machines running real Cisco network operating systems to emulate complex network [5]. We conduct two experiments in the evaluation. In the first experiment we inject a simple series of generated BGP updates into the three types of testbed while in the second experiment we use one of the past well-know BGP incident.

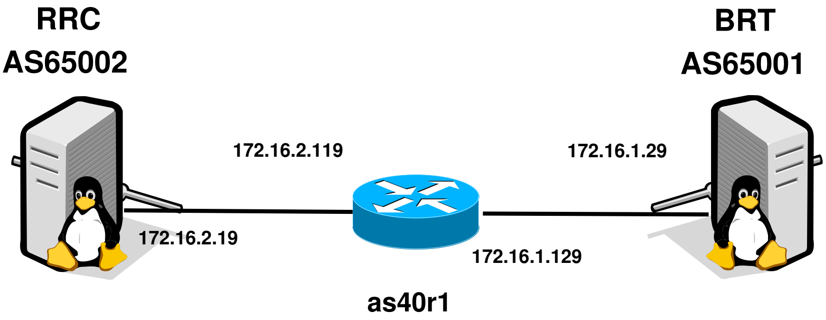


Figure A.6: Simple topology with a Cisco router

### A.4.1 Replay a generated series of BGP updates

In this experiment, we inject a simple set of generated BGP updates that represents a series of announcements and withdrawals of IPv4 and IPv6 prefixes for a period of 100 seconds. In this experiment, we use three different types of testbed. That is, Quagga testbed for the topology shown in Figure A.3, VIRL and real Cisco routers for the topology shown in Figure A.6. Both BRT v0.2 and RRC are running Ubuntu 14.04.2 LTS operating system.

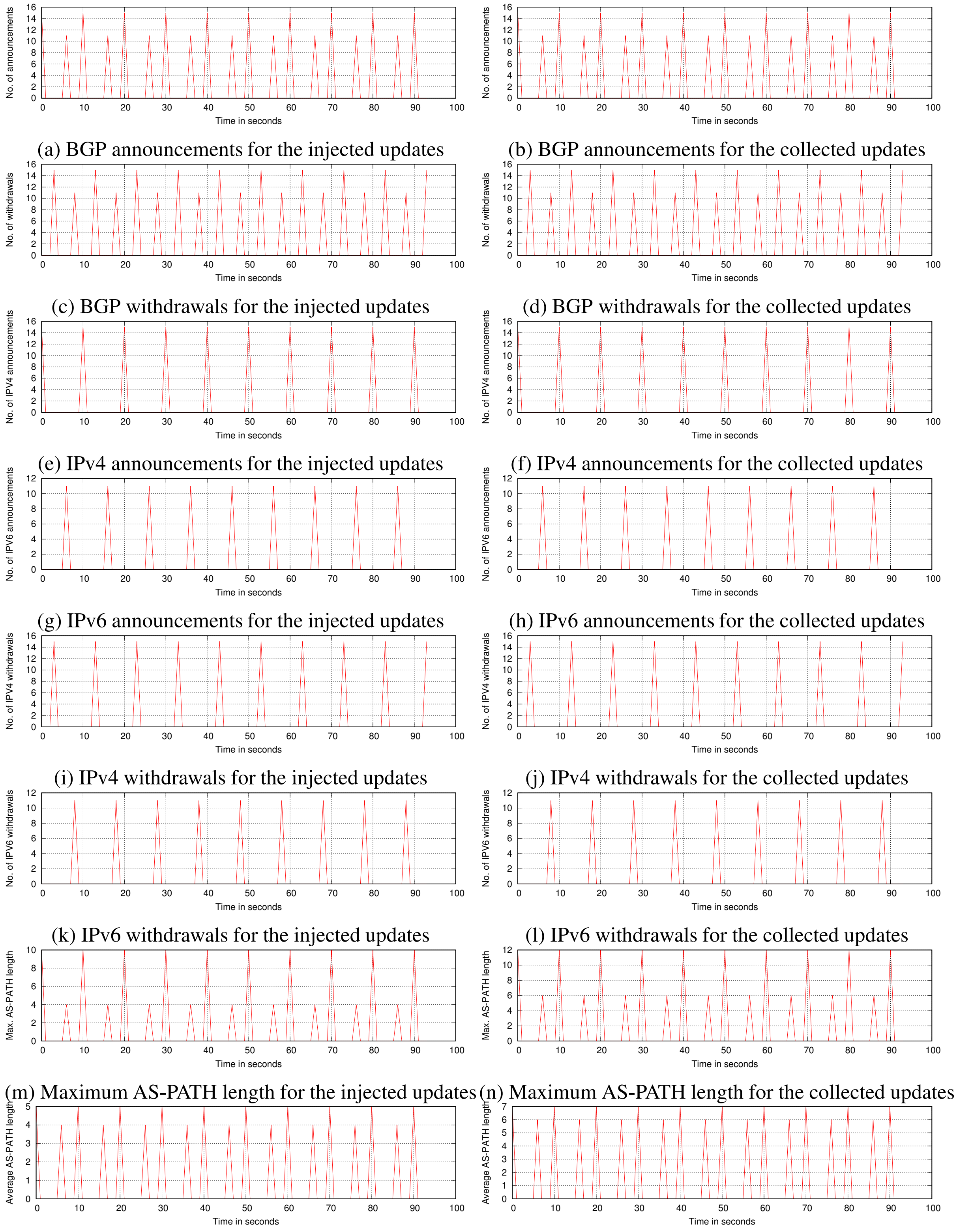
In all our experiments, we use Quagga version 0.99.23.1, VIRL BGP routers run Cisco IOSv 15.2(2)T and real Cisco BGP routers run Cisco IOSv 15.1(4)M10. For a simple investigation and monitoring, we set the value of MRAI to zero for VIRL and real Cisco routers for both IPv4 and IPv6. The MRAI refers to the minimum amount of time between two subsequent advertisements to a particular destination, the default value in Cisco routers is 30 seconds while it is zero in Quagga. For example, setting the value of MRAI to zero in Cisco routers can be done as following:

```
en
conf t
router bgp 40
neighbor 172.16.2.19 advertisement-interval 0
neighbor 172.16.1.29 advertisement-interval 0
address-family ipv6
neighbor 172.16.2.19 advertisement-interval 0
neighbor 172.16.1.29 advertisement-interval 0
exit-address-family
```

Figure A.7 shows BGP features for the injected and collected BGP updates using real Cisco routers. These include BGP volume (total number of announcements and withdrawals), total number of announcements, total number of withdrawals, IPv4 announcements and withdrawals, IPv4 announcements and withdrawals, maximum and average length of AS-PATH. These BGP features are extracted using bgp-features-0.2.pl, a Perl script available within BRT v0.2 package. All the calculated features for the injected and collected BGP updates are identical except those related to AS-PATH as a result of increasing the number of hops (AS65001 and AS40).

### A.4.2 Replay past BGP event

In this experiment we emulate TMnet event, an example of BGP instability incident observed on the 12th of June 2015 by Telekom Malaysia (TMnet) which caused significant network problems for the global routing system [8]. We use BGP updates downloaded from route-views4 in the RouteViews during TMnet event. During the events, there were 31 peers connected to route-views4 in the RouteViews. We recall our simple topology shown in Figure A.3 to replay 9001 seconds (around 2.5 hours) of BGP updates collected from the peer AS2914, one of the most peers that sent BGP updates during the event. Figure A.8 shows BGP features for injected and collected BGP updates related to TMnet event. As shown in the figure, we can find a difference in the value of amplitudes for many BGP features. We do investigation to find if this difference as a result of unsynchronised clock, or time skew, between the two nodes [**?** ] or a bug in the BRT. For that purpose, we enable a debugging message which notify users if BRT spends more than one second for a series of BGP updates with same time stamp. During the period of injected TMnet data (9001 seconds), BRT shows its ability to send all BGP updates with same time stamp within less than one second. Furthermore, RRC collected the same number of BGP updates which are by the BRT.



(a) BGP announcements for the injected updates

(b) BGP announcements for the collected updates

(c) BGP withdrawals for the injected updates

(d) BGP withdrawals for the collected updates

(e) IPv4 announcements for the injected updates

(f) IPv4 announcements for the collected updates

(g) IPv6 announcements for the injected updates

(h) IPv6 announcements for the collected updates

(i) IPv4 withdrawals for the injected updates

(j) IPv4 withdrawals for the collected updates

(k) IPv6 withdrawals for the injected updates

(l) IPv6 withdrawals for the collected updates

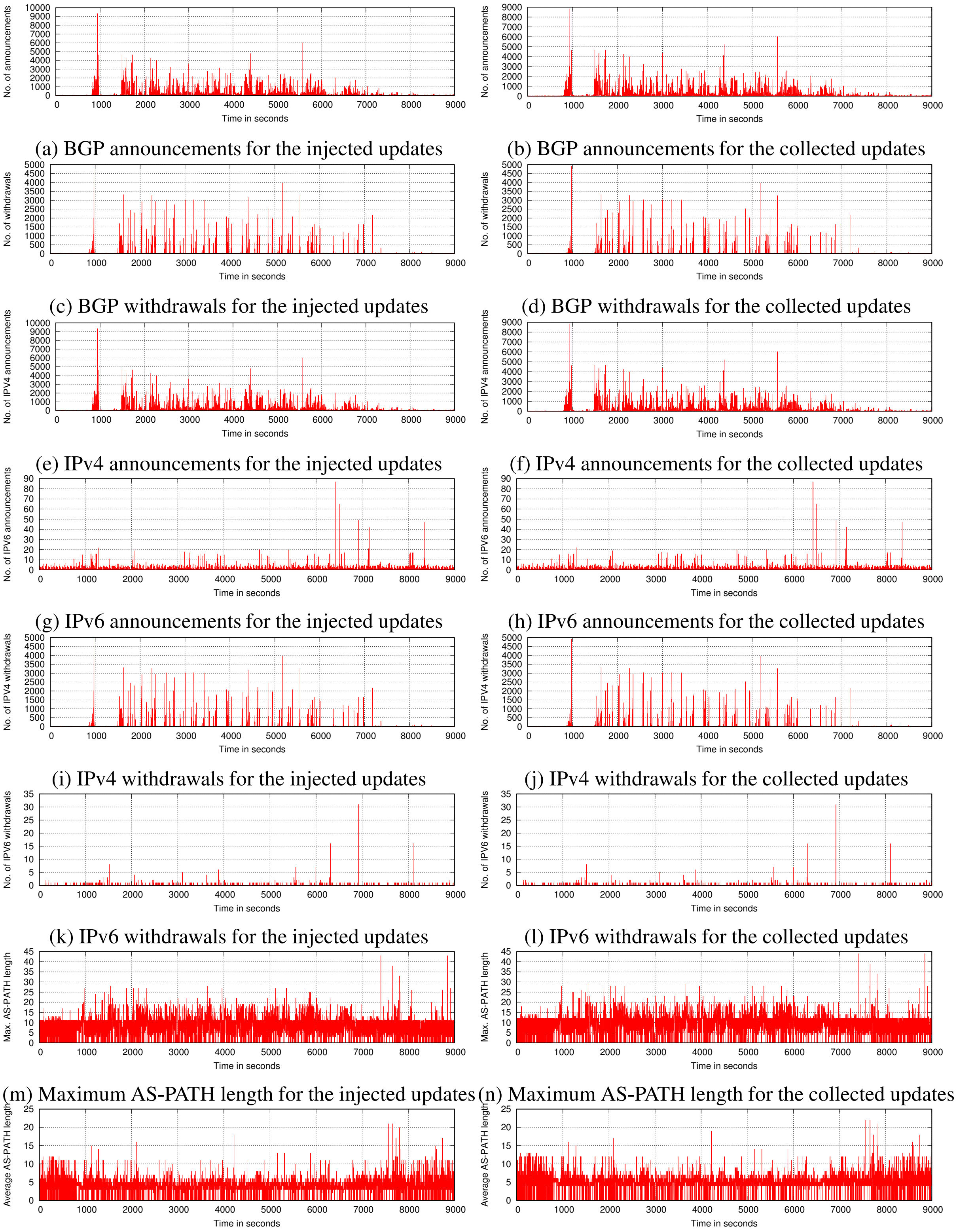
(m) Maximum AS-PATH length for the injected updates

(n) Maximum AS-PATH length for the collected updates

(o) Average AS-PATH length for the injected updates

(p) Average AS-PATH length for the collected updates

Figure A.7: BGP features for the injected and collected data of experiment-1 using real Cisco routers



(a) BGP announcements for the injected updates (b) BGP announcements for the collected updates

(c) BGP withdrawals for the injected updates (d) BGP withdrawals for the collected updates

(e) IPv4 announcements for the injected updates (f) IPv4 announcements for the collected updates

(g) IPv6 announcements for the injected updates (h) IPv6 announcements for the collected updates

(i) IPv4 withdrawals for the injected updates (j) IPv4 withdrawals for the collected updates

(k) IPv6 withdrawals for the injected updates (l) IPv6 withdrawals for the collected updates

(m) Maximum AS-PATH length for the injected updates (n) Maximum AS-PATH length for the collected updates

(o) Average AS-PATH length for the injected updates (p) Average AS-PATH length for the collected updates

Figure A.8: BGP features for the injected and collected for the TMnet incident

### A.4.3 Known issues

Although BRT v0.2 tool has been tested with Windows OS, we have occasionally experienced unknown error during the implementation. However, BRT v0.2 shows very reliable and stable performance with Unix OS such as Debian, Ubuntu and FreeBSD.

BRT v0.2 has been tested to send different types and numbers of BGP updates using a desktop computer with 3 GHz Intel Core2 Duo CPU processor, 4GB memory, and 1Gpbs of network interface card. BRT v0.2 can send >15000 updates per second. However, this number may vary based on computer specification that uses BRT v0.2 and types of information in the BGP updates.

## A.5 Conclusions

BRT is a tool to replay BGP updates with time stamps. This tool can be used to inject a list of BGP updates and replay BGP updates based on time stamps. It helps operators and researchers to understand BGP behaviour at BGP speaker level, classify BGP updates, and investigate BGP behaviour at different routers OS such as Quagga, Cisco and Juniper IOS.

BRT v0.2 supports many BGP attributes such as community, AGGREGATOR, LOCAL-PREF, and MED. It also supports sending BGP updates of IPv6 and peering over IPv6. Furthermore, it supports connection to multiple peers. The evaluation of the BRT v0.2 has been implemented using Quagga, real Cisco routers, and VIRL as a testbed. Our future work will involve developing Net::BGP patch that supports IPv6 for listener mode. This help to avoid using RRC and enable real-time monitoring.

# List of Publications

A number of peer-reviewed papers have been published or accepted for publication based on material and discussion in this thesis, as listed below:

- 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, First quarter 2017.
- 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.
- 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.

I also have co-authored the following technical reports:

- B. Al-Musawi, P. Branch, and G. Armitage, "BGP Replay Tool (BRT) v0.1," Centre for Advanced Internet Architectures, Swinburne University of Technology, Melbourne, Australia, Tech. Rep. 160304A, 04 March 2016. [Online]. Available: http://caia.swin.edu.au/reports/160304A/CAIA-TR-160304A.pdf
- B. Al-Musawi, R. Al-Saadi, P. Branch, and G. Armitage, "BGP Replay Tool (BRT) v0.2," I4T Research Lab, Swinburne University of Technology, Tech. Rep. 170606A, 06 June 2017. [Online]. Available: http://i4t.swin.edu.au/reports/I4TRL-TR-170606A.pdf