Rapid Detection of BGP Anomalies

Bahaa Al-Musawi, Philip Branch and Grenville Armitage

balmusawi, pbranch, garmitage@swin.edu.au

Internet for Things (I4T) Research Group
Swinburne University of Technology

Outline

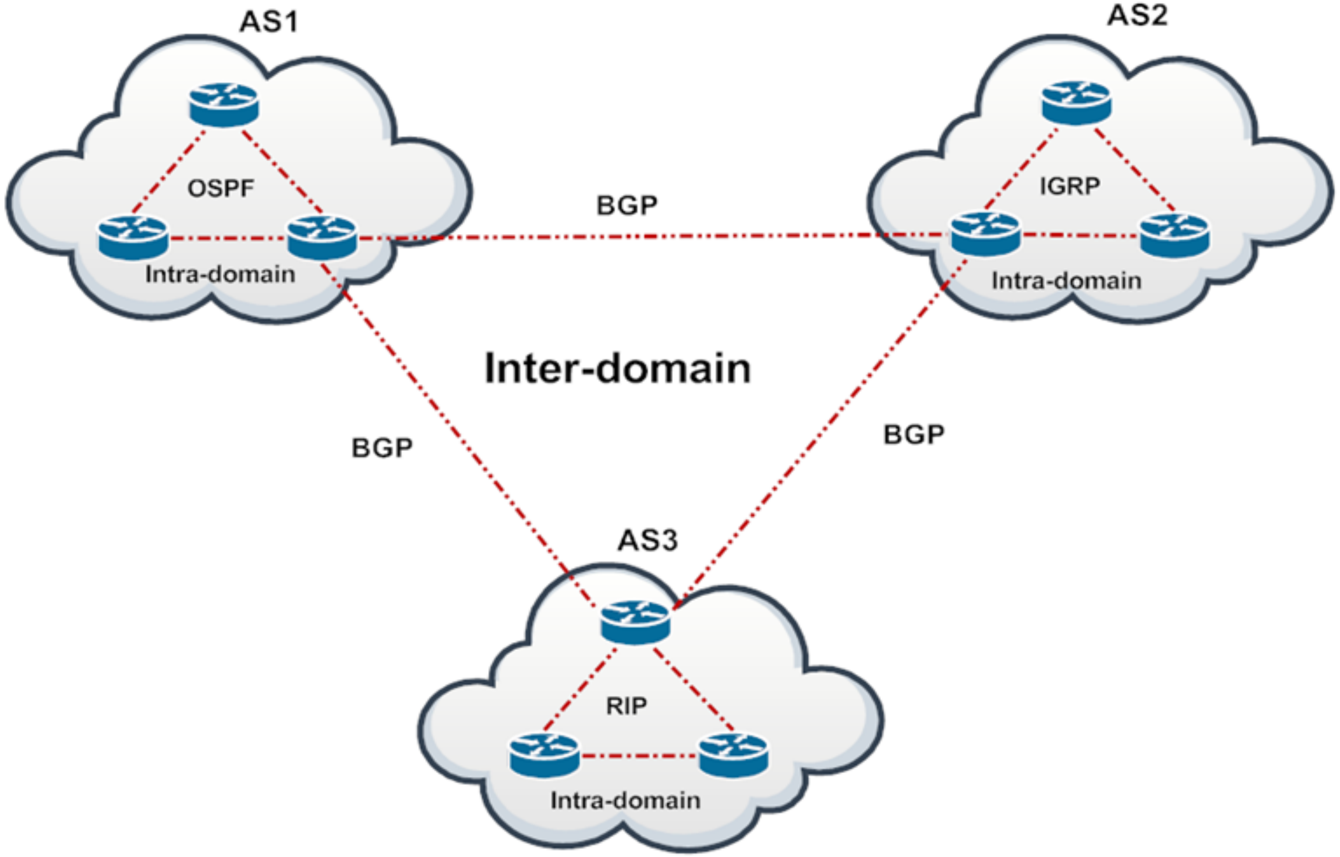
- BGP Anomalies
- Detecting BGP Anomalies using RQA Scheme
- RQA Scheme Evaluation
- Real-time BGP Anomaly Detection Tool (RBADT)
- Conclusion

Outline

- BGP Anomalies
- Detecting BGP Anomalies using RQA Scheme
- RQA Scheme Evaluation
- Real-time BGP Anomaly Detection Tool (RBADT)
- Conclusion

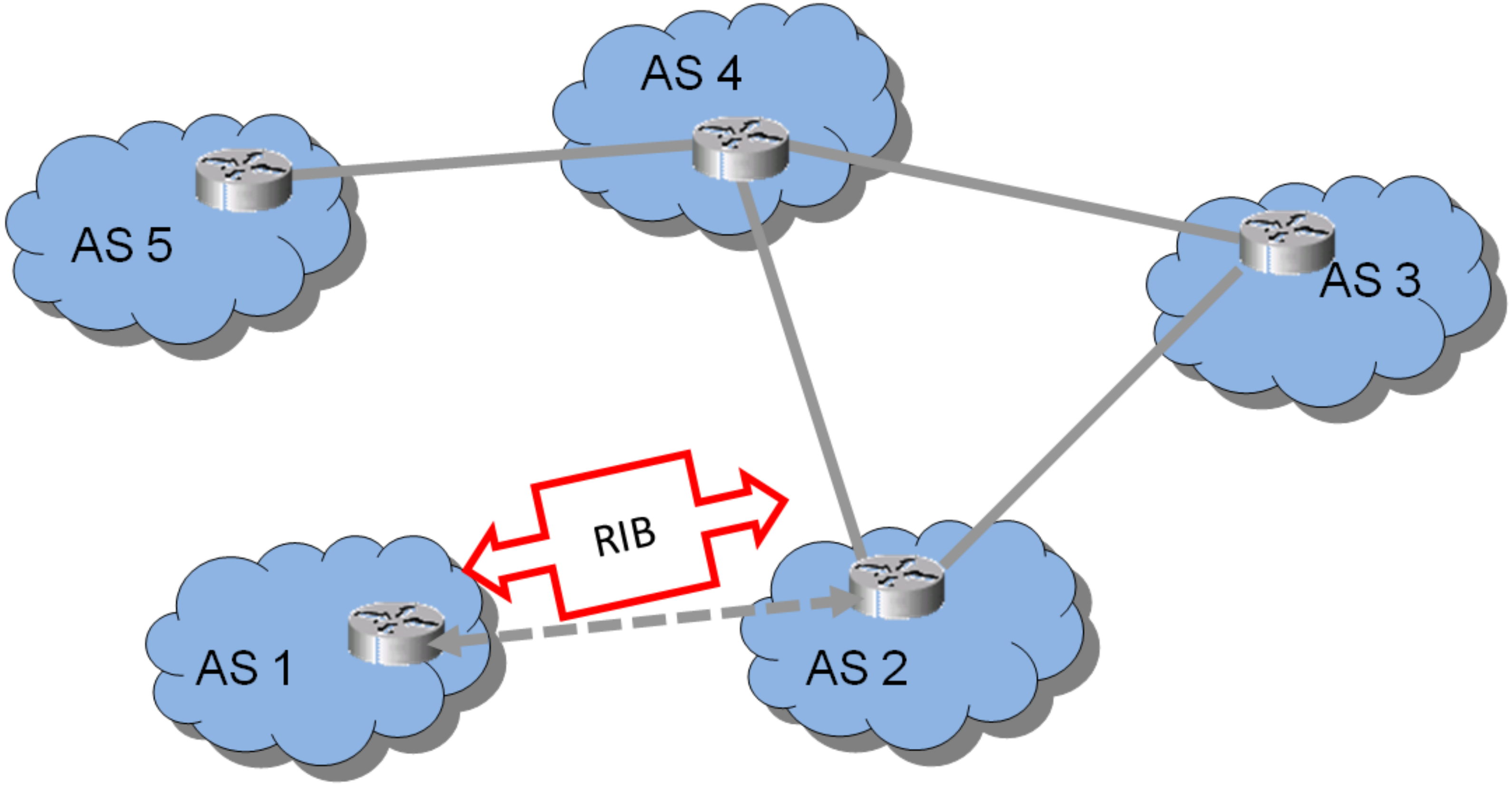
BGP Anomalies

- BGP is the Internet's default inter-domain routing protocol
- Managing NRI between ASes with guarantees of avoiding routing loops



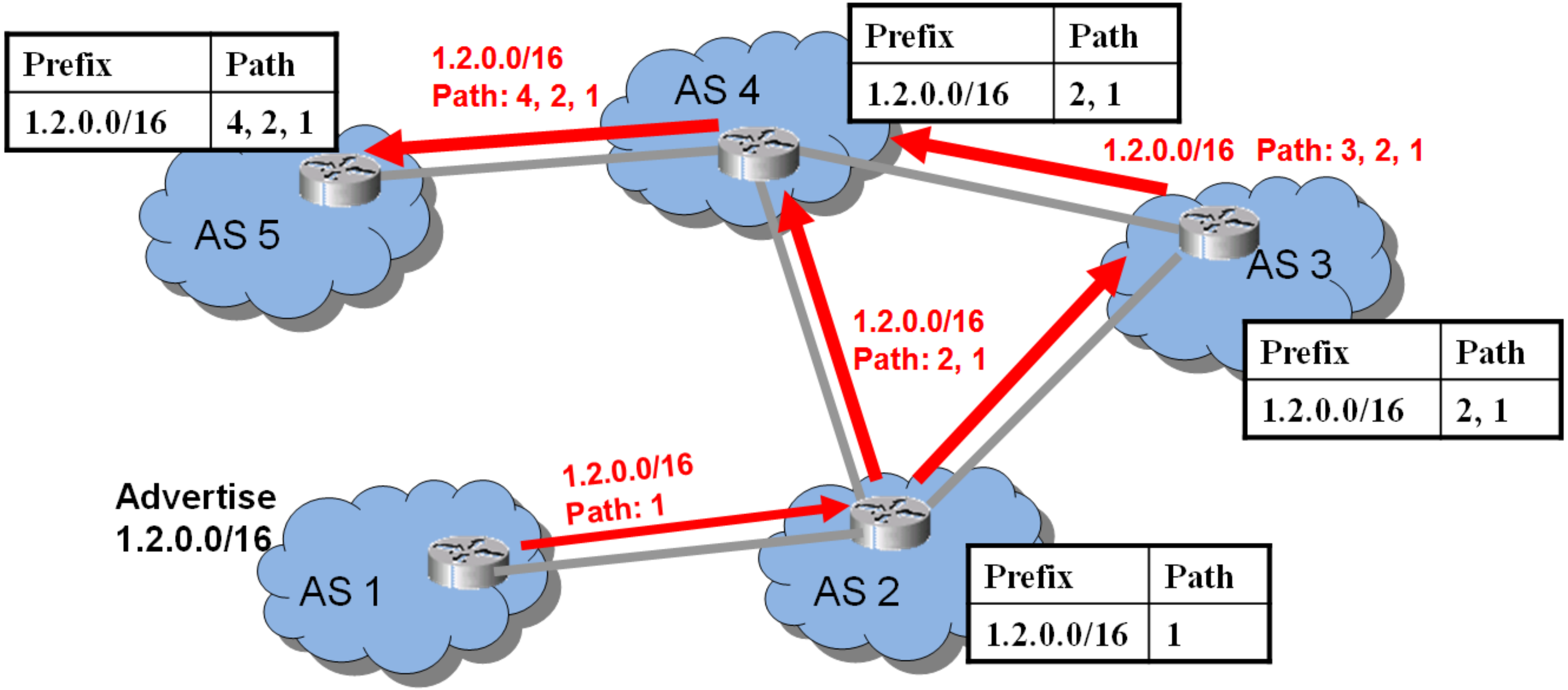
BGP Anomalies

- BGP is an incremental protocol
  - Routing Information Base (RIB)
  - Updates



BGP Anomalies

- BGP is an incremental protocol
  - Routing Information Base (RIB)
  - Updates



Prefix	Path
1.2.0.0/16	4, 2, 1

Prefix	Path
1.2.0.0/16	2, 1

Prefix	Path
1.2.0.0/16	2, 1

Prefix	Path
1.2.0.0/16	1

BGP Anomalies

- Real-world BGP traffic is a substantial volume traffic that do not appear related to events
- It is difficult to define what is meant by an anomaly
- We classify BGP traffic into [1]
  - Unstable BGP traffic
  - Anomalous BGP traffic

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

BGP Anomalies

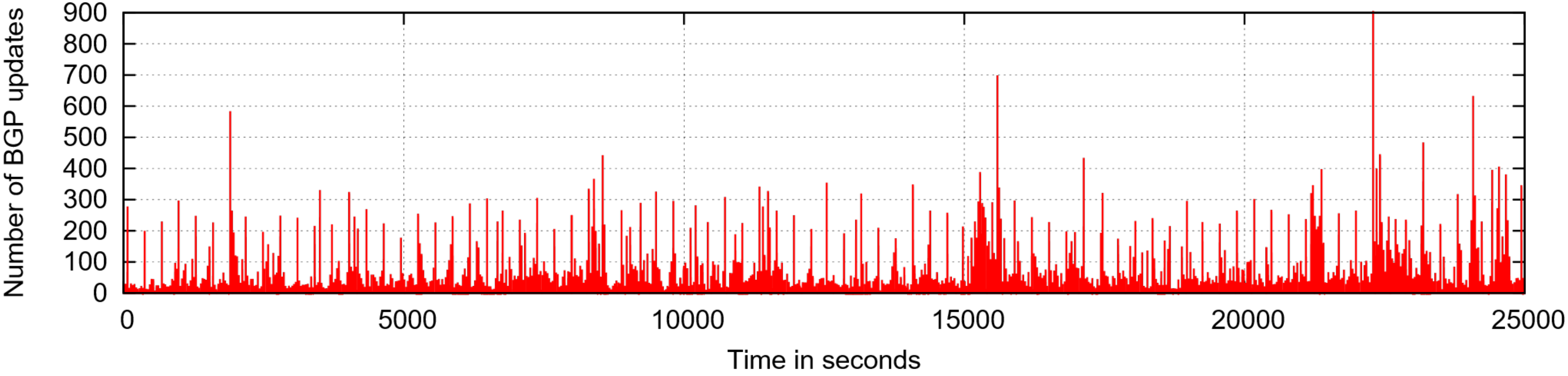
- A single BGP update is categorised as an anomalous update if
  - Contains an invalid AS number
  - Invalid or reserved IP prefixes
  - A prefix announced by an illegitimate AS
- A set of BGP updates are classified as an anomaly if
  - Show a rapid change in the number of BGP updates
  - Containing longest and shortest paths
  - Changes in the behaviour of total BGP traffic over time

BGP Anomalies

- A single BGP update is categorised as an anomalous update if
  - Contains an invalid AS number
  - Invalid or reserved IP prefixes
  - A prefix announced by an illegitimate AS
- A set of BGP updates are classified as an anomaly if
  - Show a rapid change in the number of BGP updates
  - Containing longest and shortest paths
  - Changes in the behaviour of total BGP traffic over time

BGP Anomalies

- BGP traffic has been characterised as
  - Complex
  - Noisy
  - Voluminous, BGP speakers generate up to a GB of BGP traffic/day



Sample of BGP traffic sent by peer AS197264

BGP Anomalies

- BGP anomaly detection
  - Can differentiate between unstable and anomalous traffic
  - Can rapidly detect BGP anomalies
    - 20% of anomalies can affect 90% of the Internet < 2 minutes [1]
  - A lightweight and can work in real-time

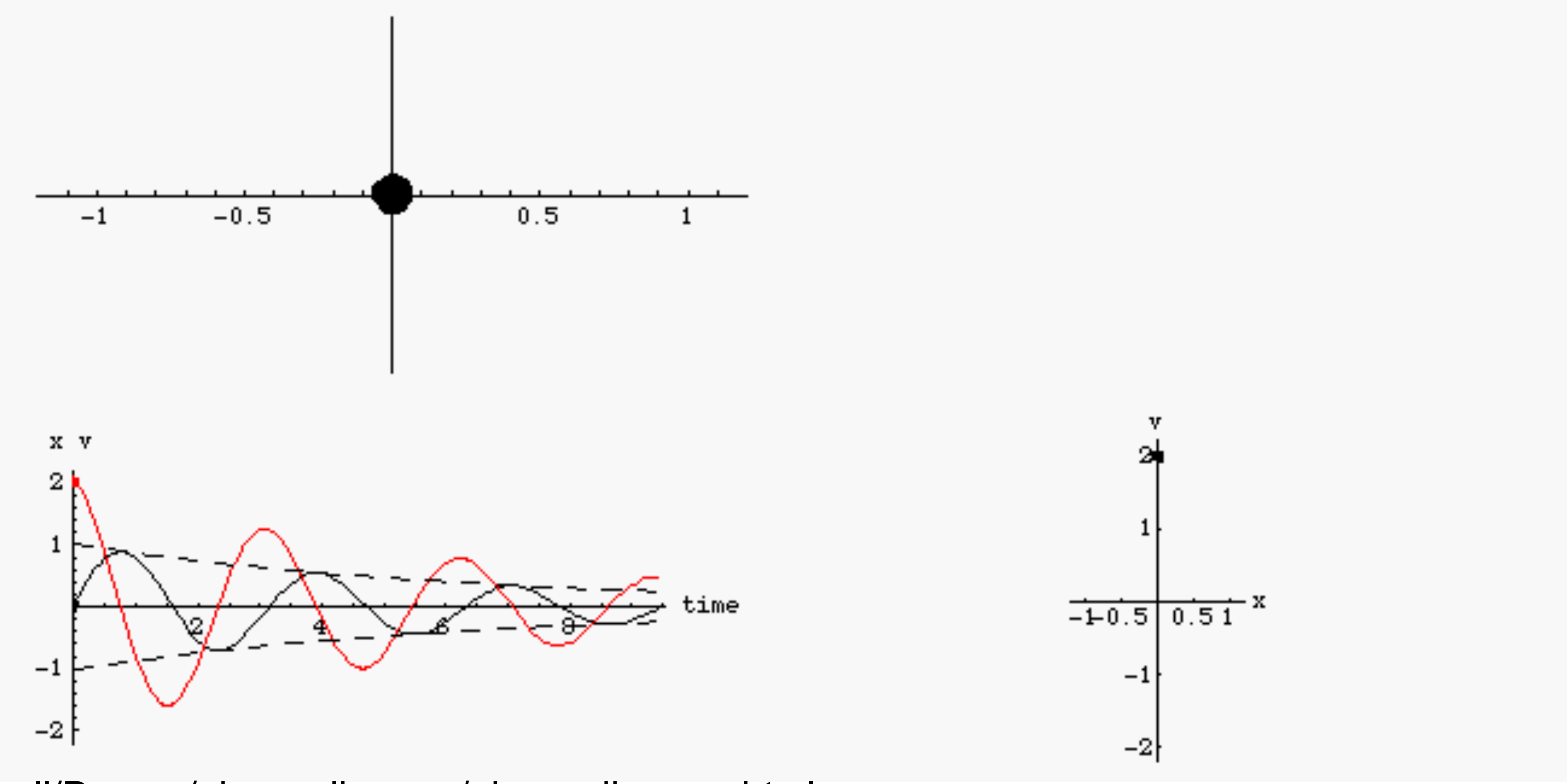
[1] X. Shi, Y. Xian, Z. Wang, X. Yin, and J. Wu, “Detecting prefix Hijacking in the Internet with Argus,” in Proceeding of the 2012 ACM Conference on Internet Measurement Conference, IMC’12, 2012

Outline

- BGP Anomalies
- Detecting BGP Anomalies using RQA Scheme
- RQA Scheme Evaluation
- Real-time BGP Anomaly Detection Tool (RBADT)
- Conclusion

Detecting BGP Anomalies using RQA Scheme

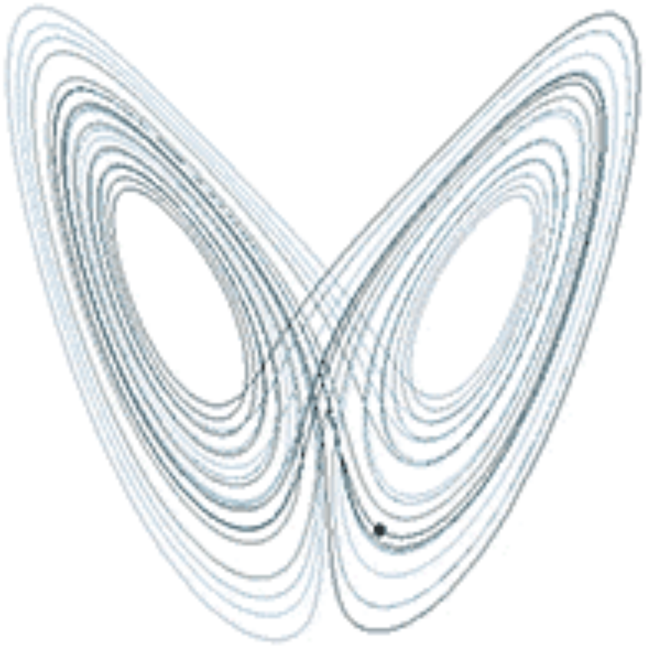
- We model BGP speakers as dynamic systems
- Our modelling uses phase plane concepts



http://www.acs.psu.edu/drussell/Demos/phase-diagram/phase-diagram.html

Detecting BGP Anomalies using RQA Scheme

- We model BGP speakers as dynamic systems
- Our modelling uses phase plane concepts



https://en.wikipedia.org

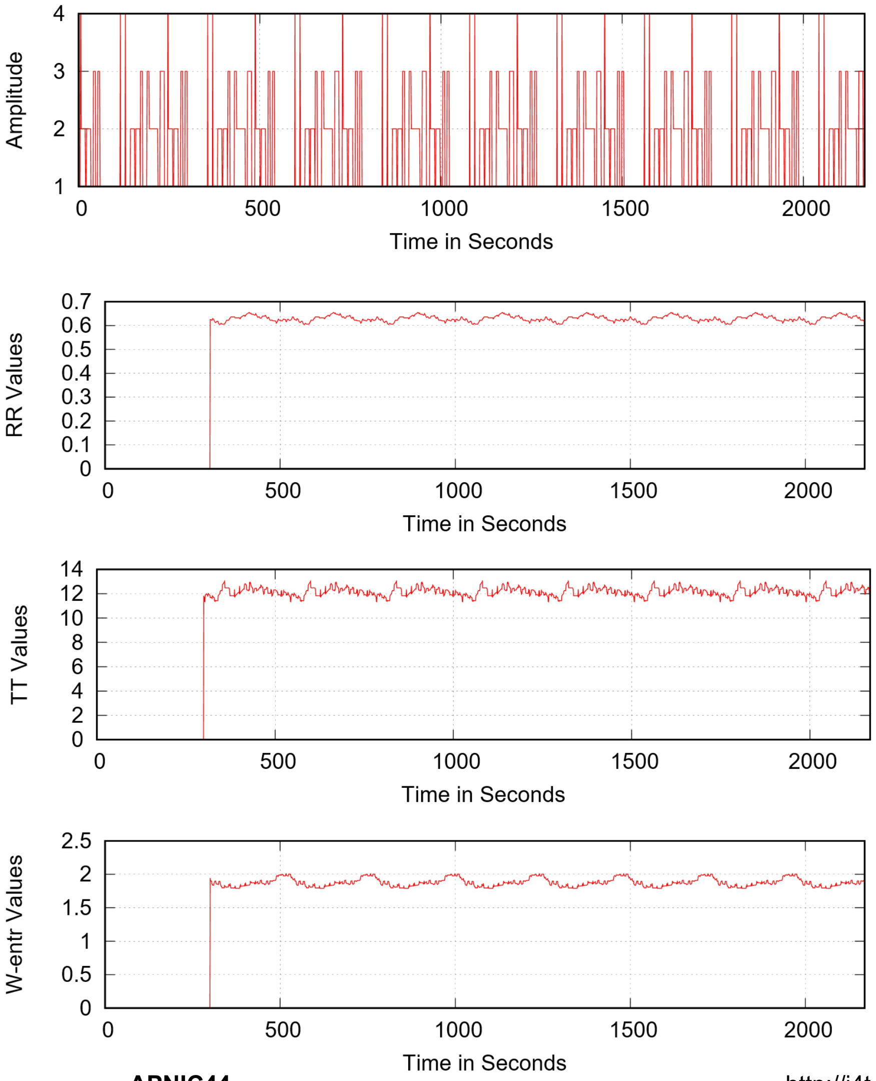
Detecting BGP Anomalies using RQA Scheme

- The outcomes of our modelling
    - Deterministic
    - Stable
    - Non-linear
    - Recurrent

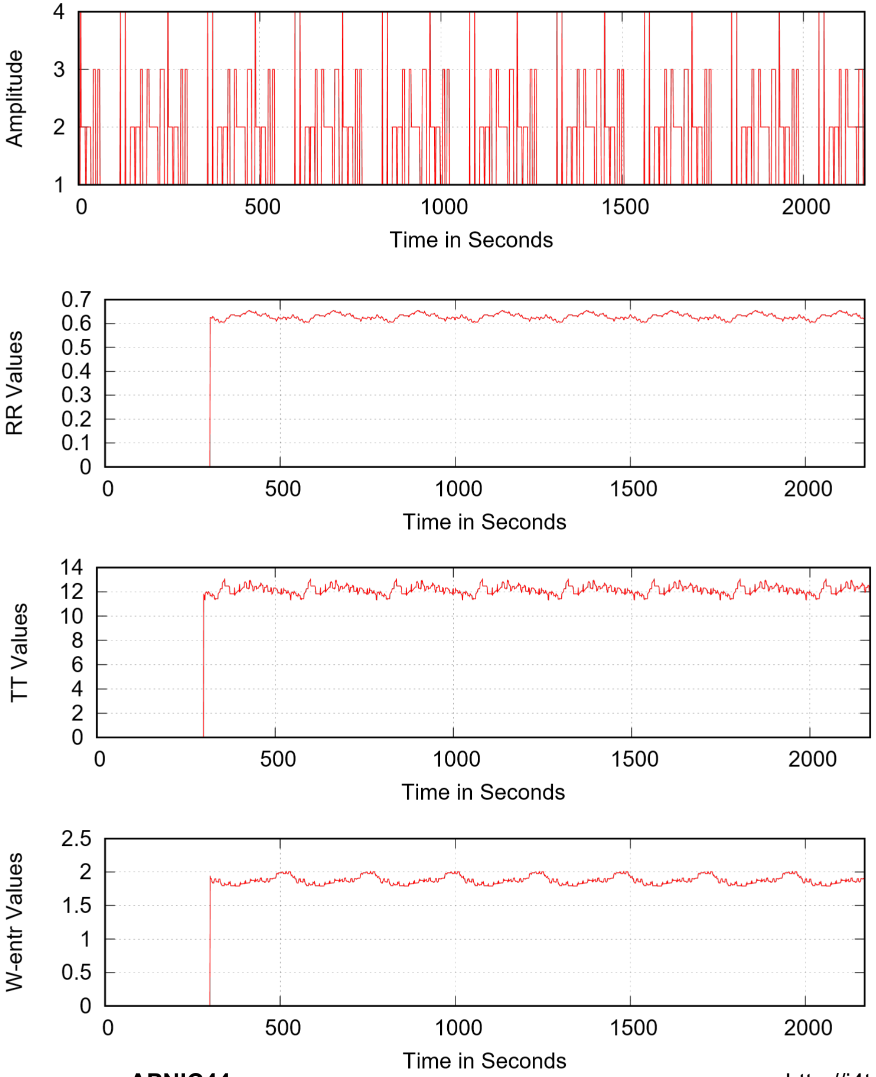
Detecting BGP Anomalies using RQA Scheme

- Recurrence Quantification Analysis (RQA)
- An advanced non-linear analysis technique based on a phase plane concepts
- Has multiple measurements
  - RR, probability that a system will recurs after N time states
  - TT, how long a system remains in a specific state
  - T2, a measure of time taken to move taken to move from one state to another

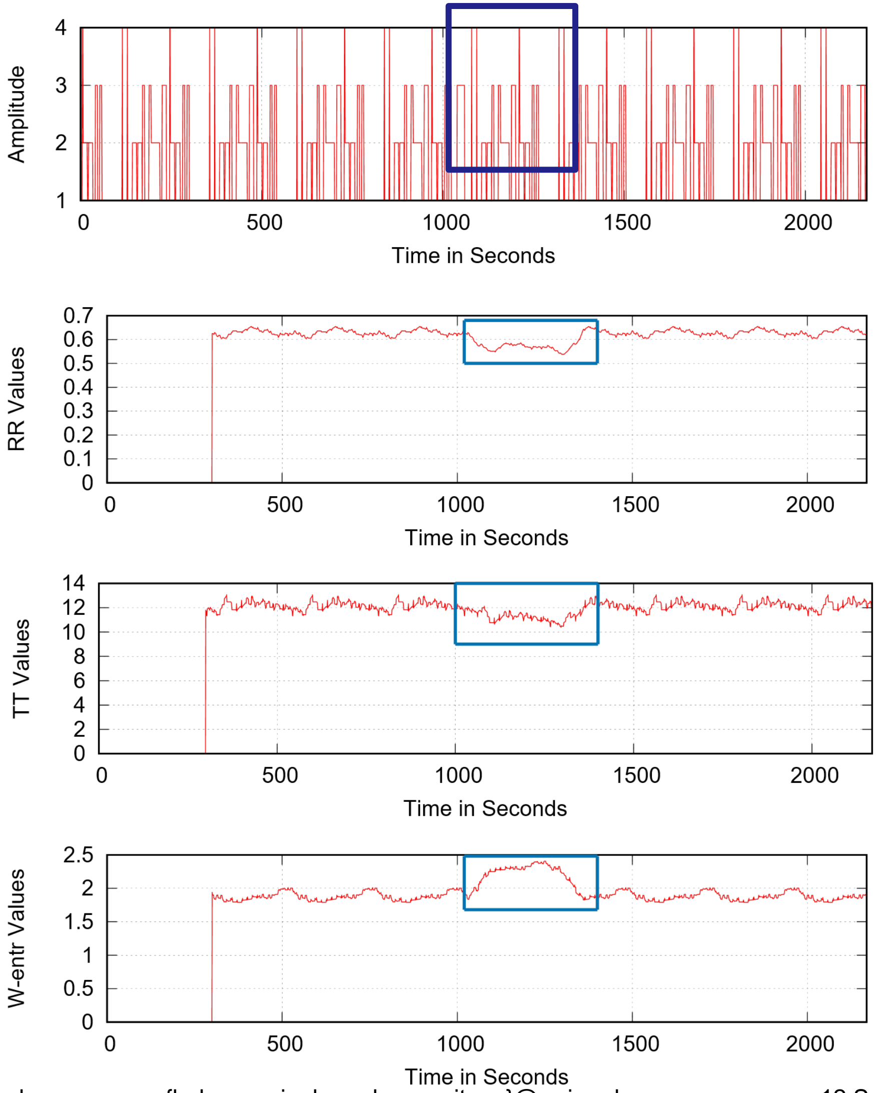
Detecting BGP Anomalies using RQA Scheme



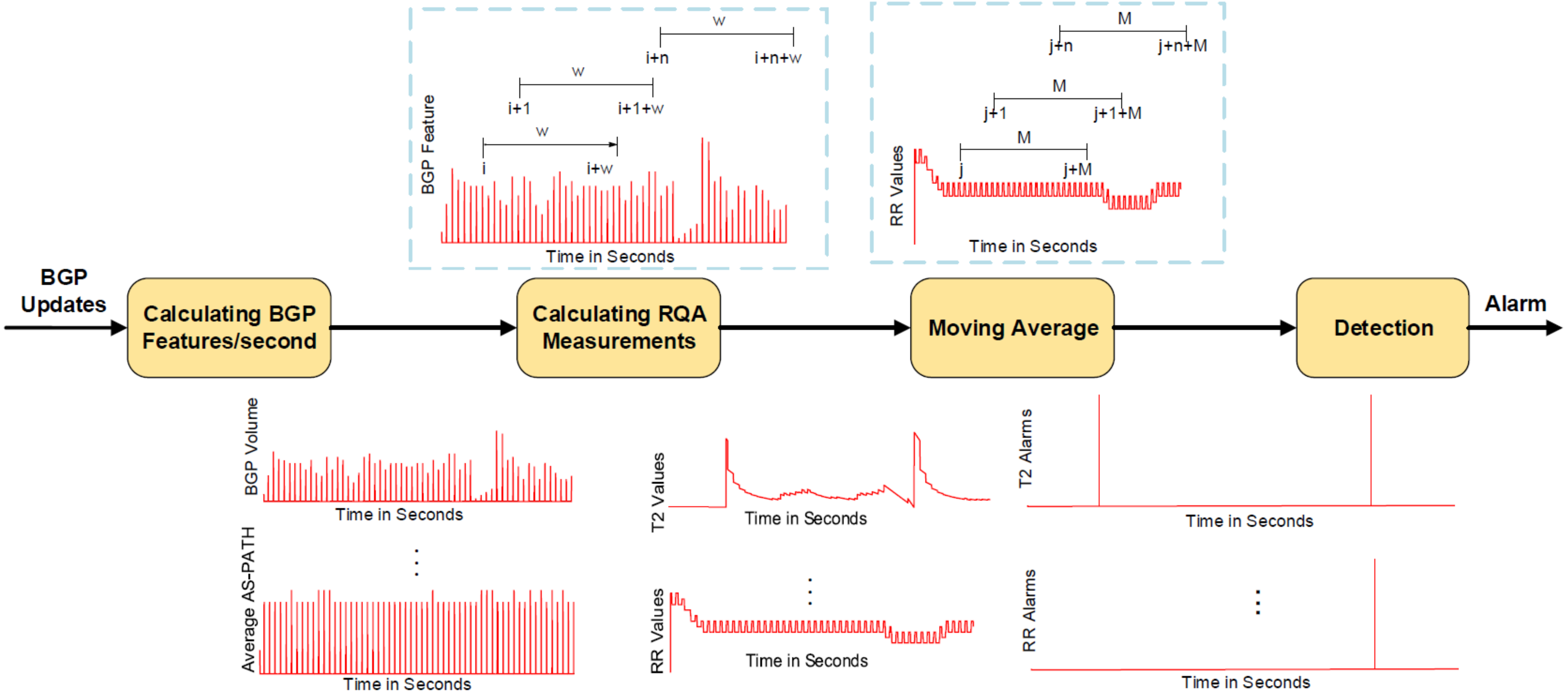
Detecting BGP Anomalies using RQA



1040-1060 seconds from 1 to 3



Detecting BGP Anomalies using RQA Scheme



RQA Scheme Design

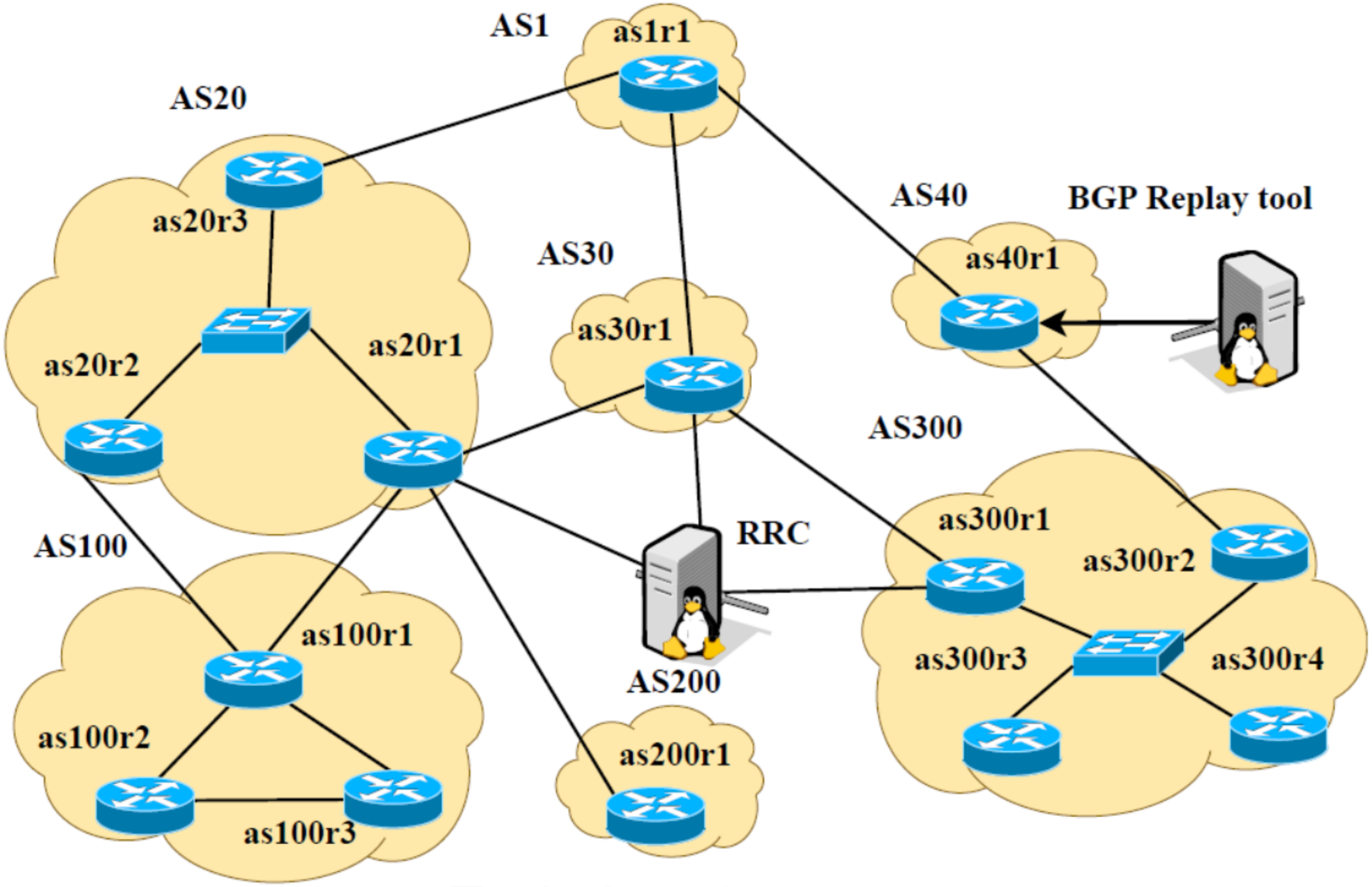
Detecting BGP Anomalies using RQA Scheme

- BGP Controlled Testbed
  - Lack of time-stamp information for past BGP events
  - Provide ground truth validation
  - Helps to understand BGP behaviour at BGP speaker level
  - It also helps to classify BGP updates

BGP Controlled Testbed

- Virtual Internet Routing Lab (VIRL)
  - Linux KVM hypervisor
  - OpenStack
  - A set of virtual machines running real Cisco operating systems
- BRT, a tool to replay past BGP updates with time stamps
  - Uses Net::BGP and Multiprotocol Extensions for BGP, RFC4760
  - Supports different BGP attributes, IPv6 BGP updates and peering
  - Evaluated using real Cisco router, VIRL, and Quagga

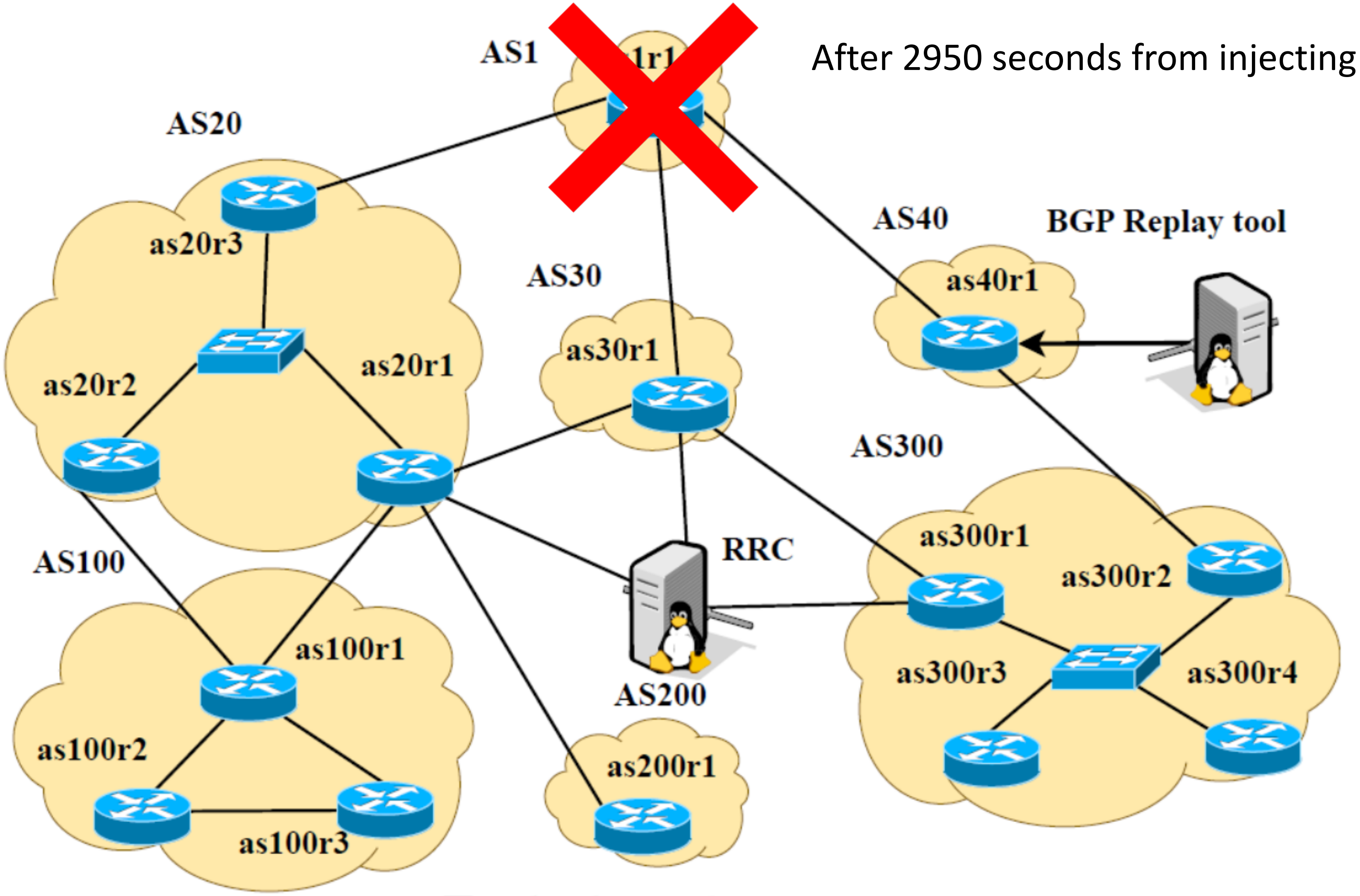
BGP Controlled Testbed



Testbed topology

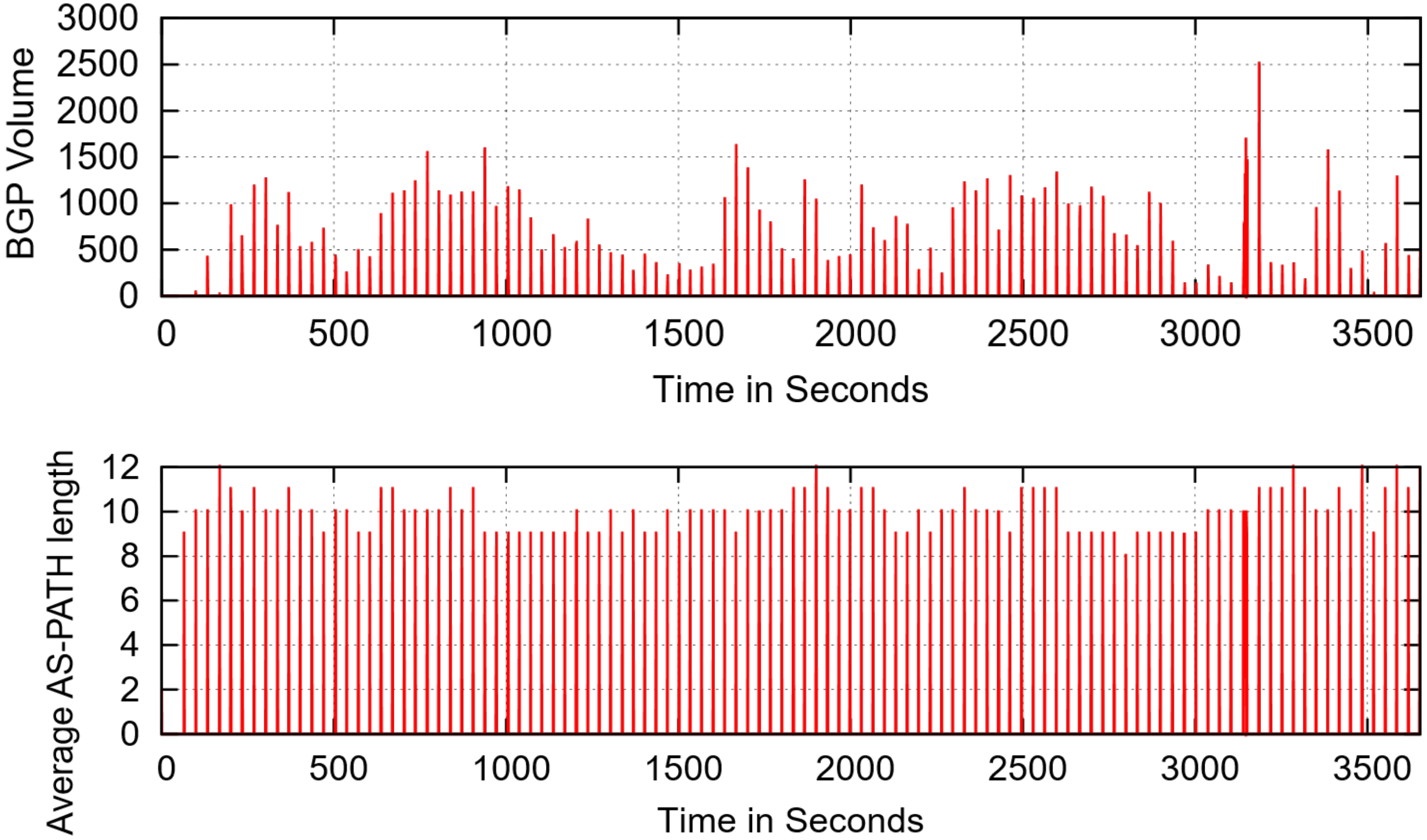
BGP Controlled Testbed

After 2950 seconds from injecting BGP traffic



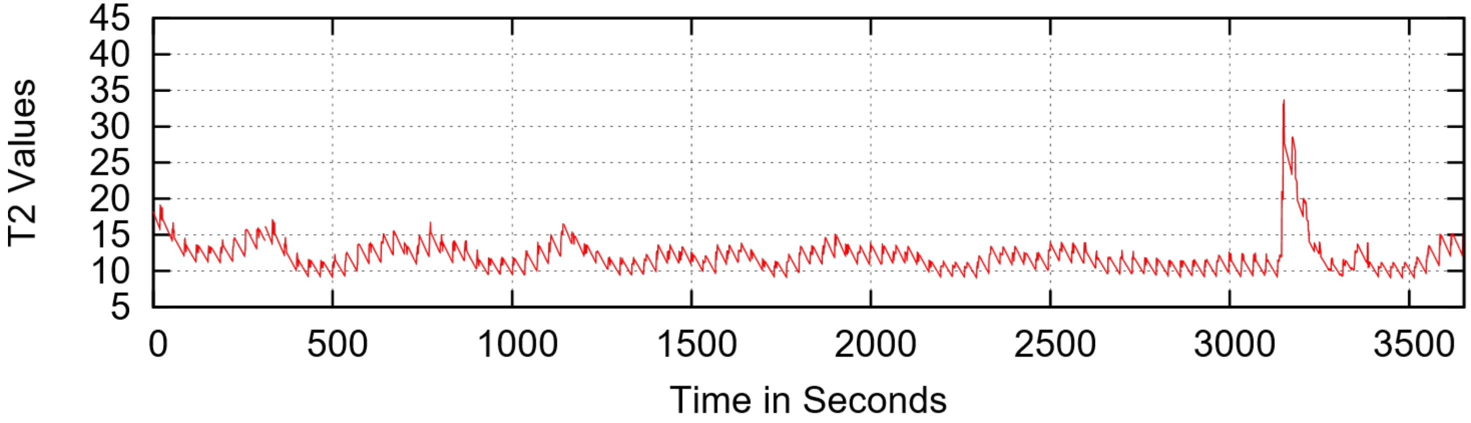
Testbed topology

BGP Controlled Testbed

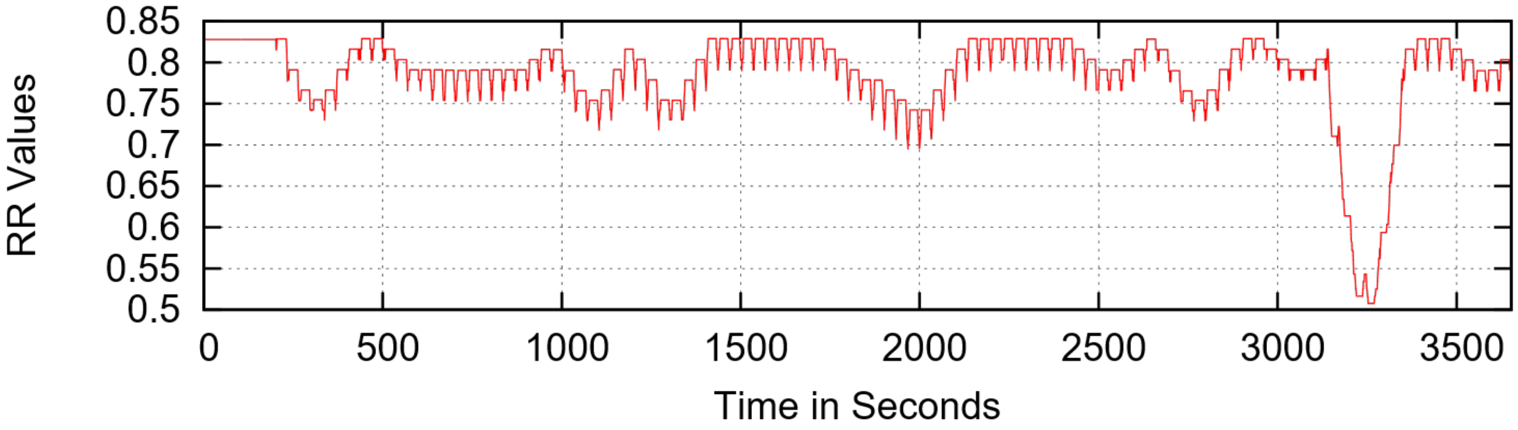


BGP volume and average AS-PATH length features of as20r1

BGP Controlled Testbed



T2 measurement for BGP volume feature



RR measurement for average AS-PATH length feature

Outline

- BGP Anomalies
- Detecting BGP Anomalies using RQA Scheme
- RQA Scheme Evaluation
- Real-time BGP Anomaly Detection Tool (RBADT)
- Conclusion

RQA Scheme Evaluation

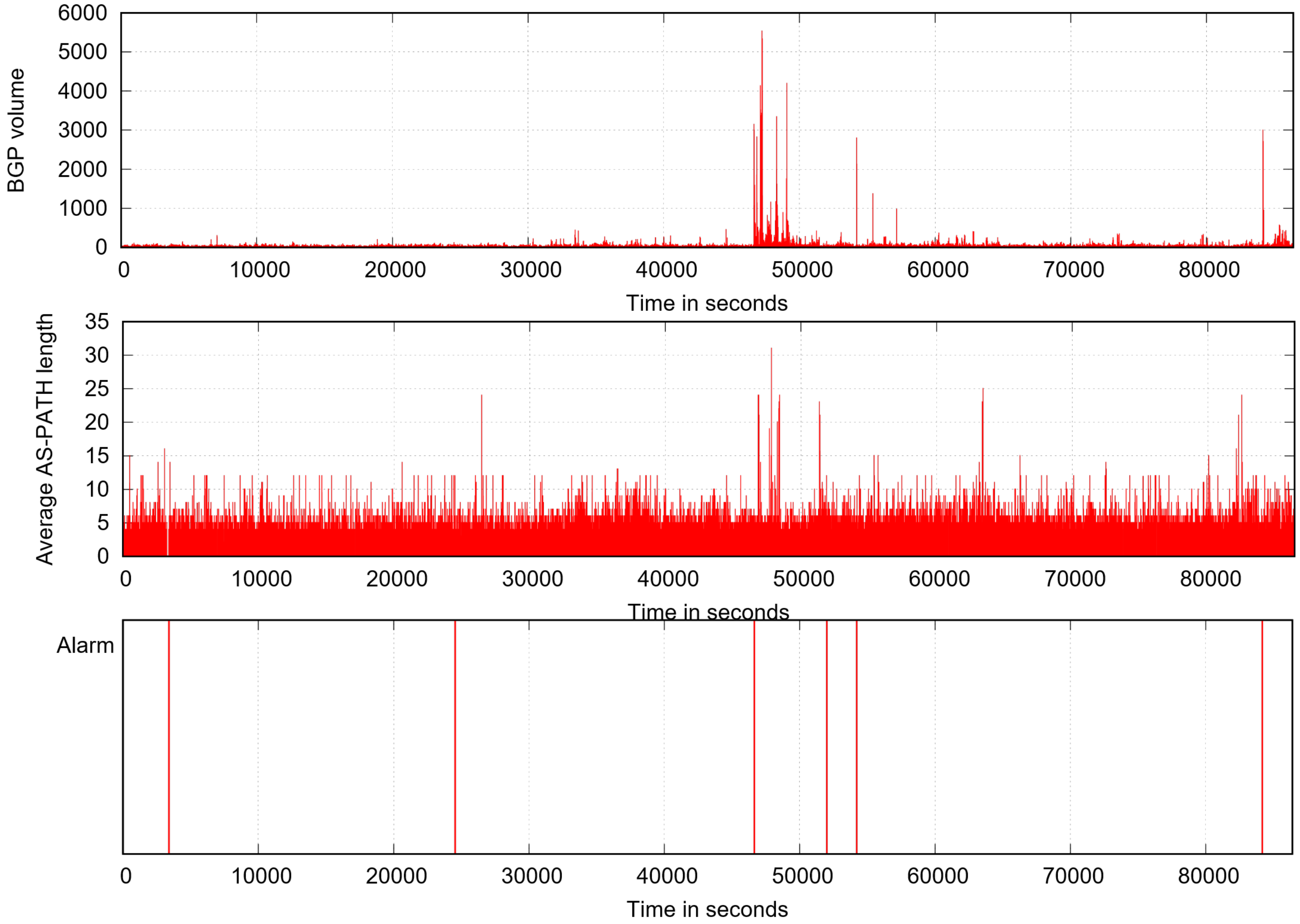
- TP: Number of anomalies classified as anomalies
- TN: Number of normal events classified as normal
- FP: Number of normal events classified as anomalous
- FN: Number of anomalous events classified as normal

RQA Scheme Evaluation

- TP: Number of anomalies classified as anomalies
- TN: Number of normal events classified as normal
- FP: Number of normal events classified as anomalous
- FN: Number of anomalous events classified as normal

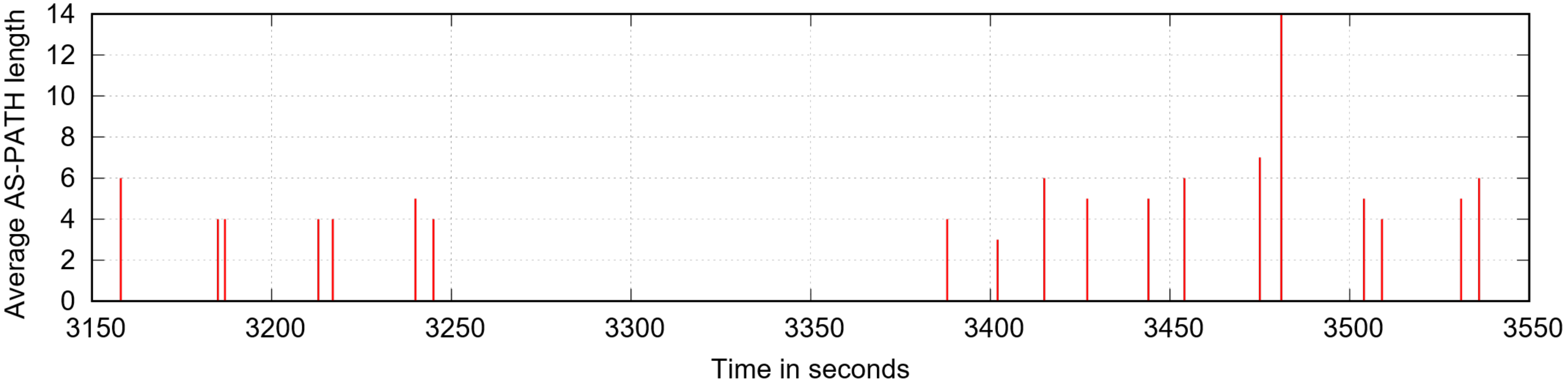
Event	Type of Anomaly	Date
Nimda	DoS attack	September 2001
TTNet	BGP misconfiguration	December 2004
Mosco blackout	Hardware failure	May 2005
TMnet	BGP misconfiguration	June 2015

RQA Scheme Evaluation-TTNet event



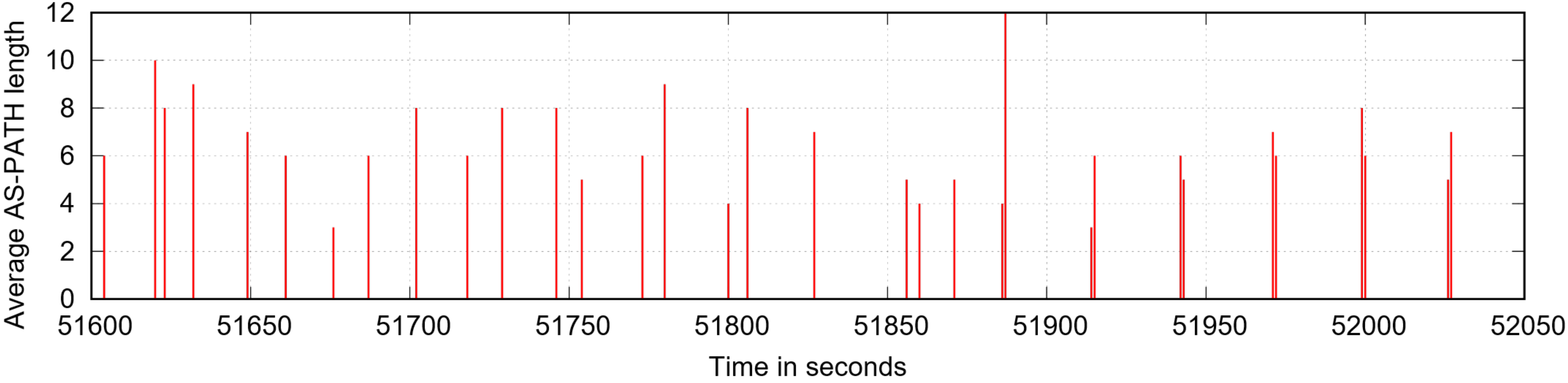
BGP Traffic sent by the peer AS12793 at rrc05

RQA Scheme Evaluation-TTNet event



Hidden anomalous behaviour-stop sending BGP updates for two minutes

RQA Scheme Evaluation-TTNet event



Hidden anomalous period in the underlying system behaviour

RQA Scheme Evaluation

- Applying RQA scheme over 1233794 seconds (14.28 days or 342.72 hours)
- **An average of one FP alarm every 42.84 hours**

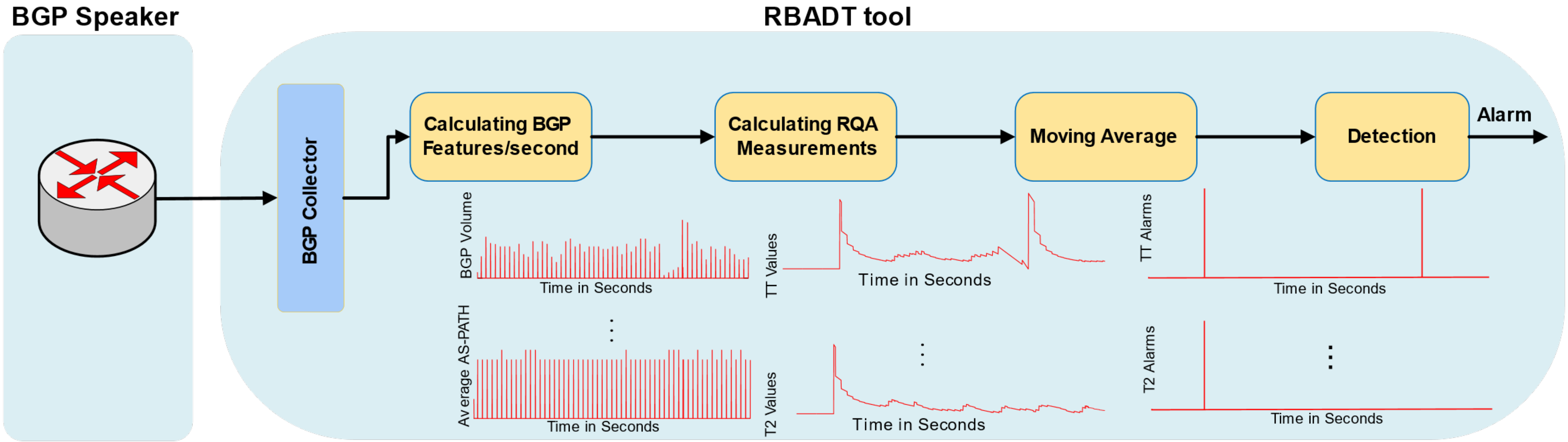
Event	TP	TN	FP	FN
Nimda	7	421405	5	0
TTNet	6	85201	0	0
Mosco blackout	9	597376	3	0
TMnet	8	85205	0	0
Summary	30	1233739	8	0

Outline

- BGP Anomalies
- Detecting BGP Anomalies using RQA
- RQA Scheme Evaluation
- Real-time BGP Anomaly Detection Tool (RBADT)
- Conclusion

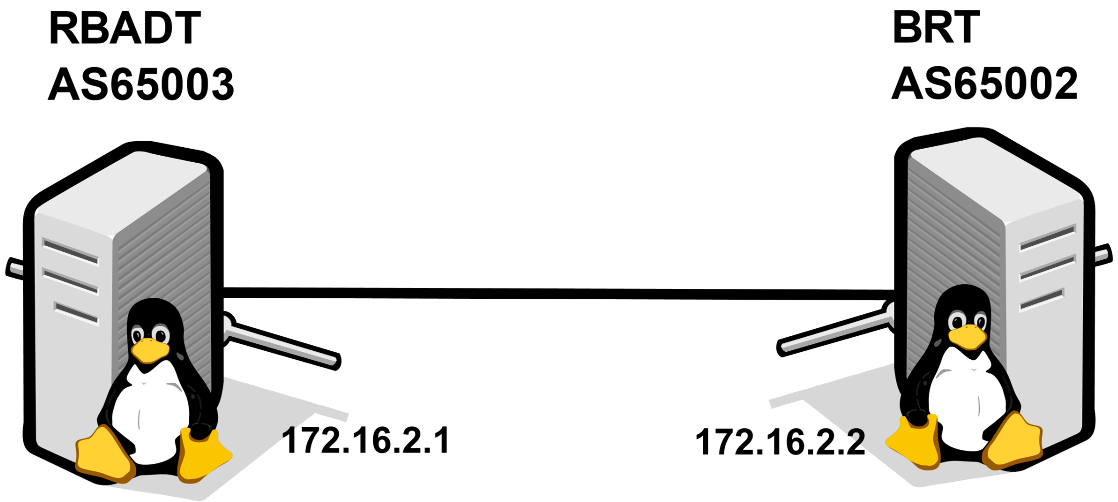
Real-time BGP Anomaly Detection Tool (RBADT)

- BGP collector
  - Net::BGP does not support IPV6 prefixes/connection
  - Develop a patch based on Multiprotocol Extensions for BGP, RFC4760

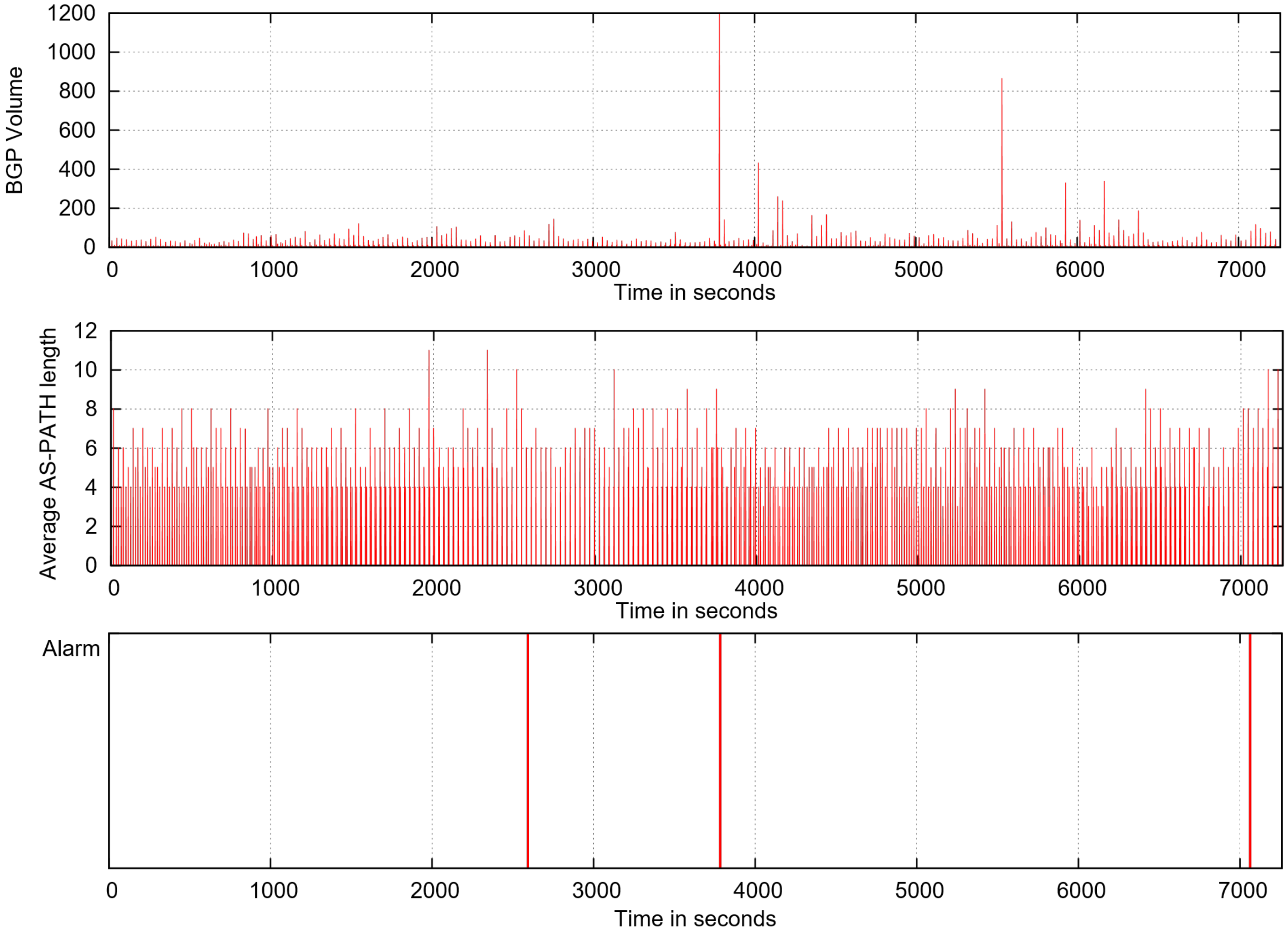


Real-time BGP Anomaly Detection Tool (RBADT)

- Emulate TMNet event by injecting BGP traffic using BRT
- TMNet an example of BGP misconfiguration
  - AS4788 announced 179,0000 prefixes to level3
  - Significant packet loss
  - Slow Internet service around the world

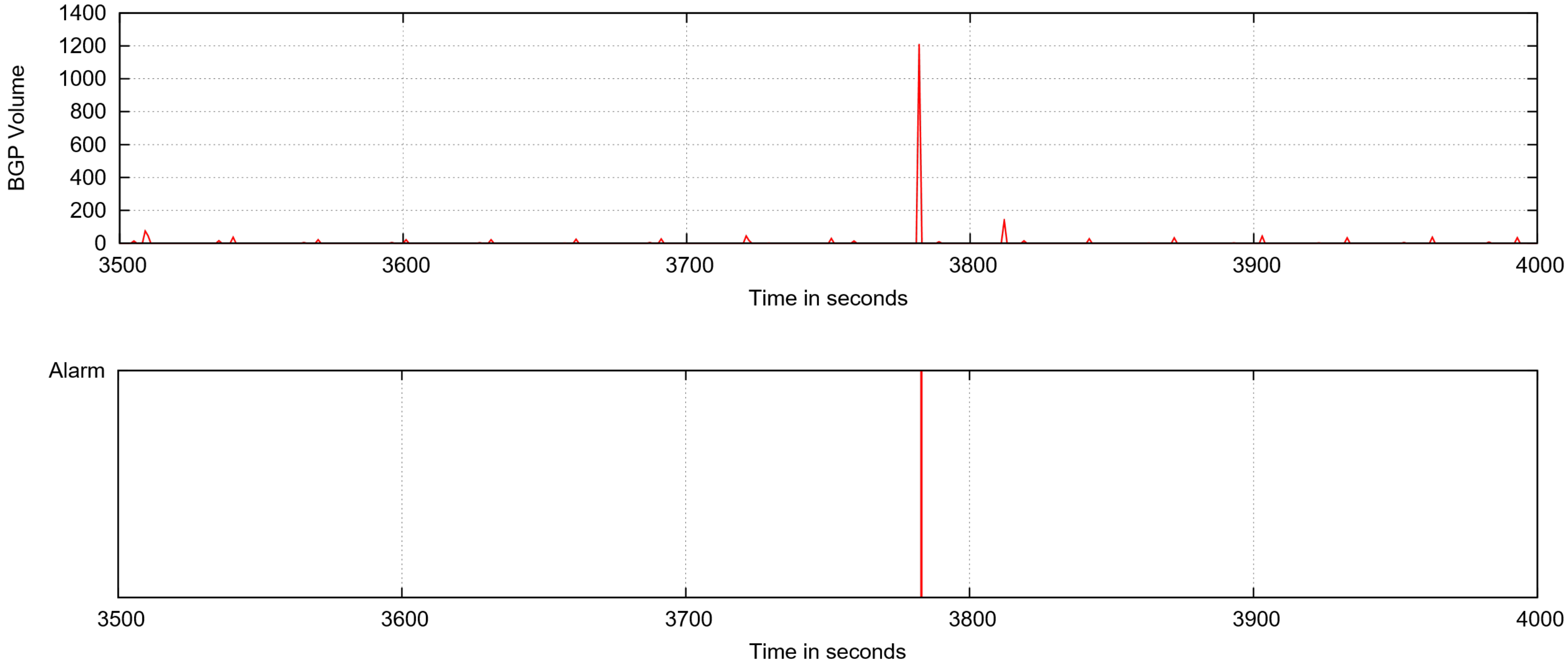


Real-time BGP Anomaly Detection Tool (RBADT)



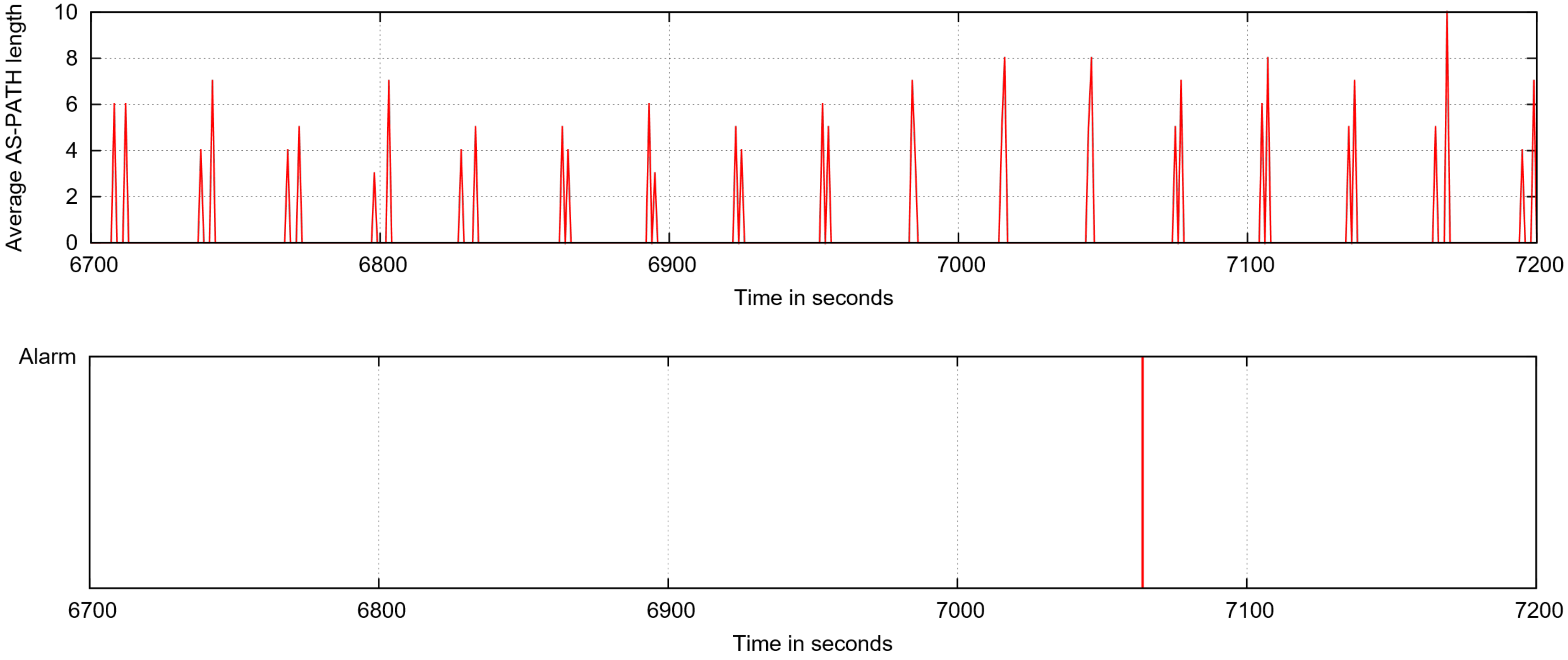
Real-time BGP Anomaly Detection Tool (RBADT)

- Detecting high volume of BGP traffic
  - High volume time 3782 seconds, detection time 3784 seconds



BGP Controlled Testbed

- Detecting hidden anomalous period in the underlying system behaviour
  - 6984-7046 seconds Detection at 7065 seconds



Outline

- BGP Anomalies
- Detecting BGP Anomalies using RQA
- RQA Scheme Evaluation
- Real-time BGP Anomaly Detection Tool (RBADT)
- Conclusions

Conclusions

- BGP is vulnerable to different types of attacks
- Detecting BGP anomalies is a challenge
- A technique is needed to rapidly differentiate between unstable and anomalous BGP traffic
- BGP speakers are stable, non-linear, and deterministic
- RQA can rapidly detect BGP anomalies
- RQA can detect hidden abnormal behaviours that may pass without observation
- RQA can detect BGP anomalies with an average of one FP alarm every 42.84 hours

Acknowledgements

- BGP Replay Tool (BRT) v0.2 and RBADT v0.1 (under development) was supported under part by "APNIC Internet Operations Research Grant" under the ISIF Asia 2016 grant scheme ISIF Asia 2016 grant recipients
- VIRL team at Cisco for providing free license and support

Useful links and sources

- Rapid detection of BGP anomalies- project http://caia.swin.edu.au/tools/bgp/brt/

- B. Al-Musawi, P. Branch, and G. Armitage, " *Detecting BGP Instability Using Recurrence Quantification Analysis*", in 34th International Performance Computing and Communications Conference (IPCCC), 14 - 16 December 2015
- 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, “*Recurrence Behaviour of BGP Traffic*,” in International Telecommunication Networks and Applications Conference (ITNAC) 2017, Melbourne, Australia, 22 November 2017
- 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. I4TRL-TR-170606A, 06 June 2017. [Online]. Available: http://i4t.swin.edu.au/reports/I4TRL-TR-170606A.pdf