THE MINISTRY OF HIGHER EDUCATION
AND SCIENTIFIC RESEARCH - IRAQ
UNIVERSITY OF KUFA

Rapid Detection of BGP Anomalies

Dr. Bahaa Al-Musawi

bahaa.almusawi@uokufa.edu.iq

Faculty of Engineering, University of Kufa

Outline

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

BGP Anomalies

Detection Challenges

- BGP traffic is complex, noisy and voluminous
- BGP speakers generate up to a GB of BGP traffic/day
- 20% of BGP anomalies lasted <10 minutes but were able to pollute 90% of the Internet in <2 minutes[1]
- Real-time detection without requiring long history data

1- 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.

BGP Anomalies

BGP Updates

- 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

Detecting BGP anomalies using RQA

- We model BGP speakers as dynamic systems using the concepts of phase plane trajectory[1]
- The outcome of our modelling shows that BGP speaker has the characteristics
  - Determinism
  - Stable
  - Non-linear
  - Recurrent

(1) B. Al-Musawi, P. Branch, and G. Armitage, “Detecting BGP instability using Recurrence Quantification Analysis (RQA),” in *IPCCC*, Dec 2015, pp. 1–8.

Detecting BGP anomalies using RQA

- Recurrence Quantification Analysis (RQA), an advanced non-linear statistical analysis technique based on the concepts of phase plane trajectories
- RQA has multiple measurements such as
  - RR: Probability that a system will recurs after number of time states
  - TT: How long the system remains in a specific state
  - T2: Time taken to move taken to move from one state

RQA Scheme Design

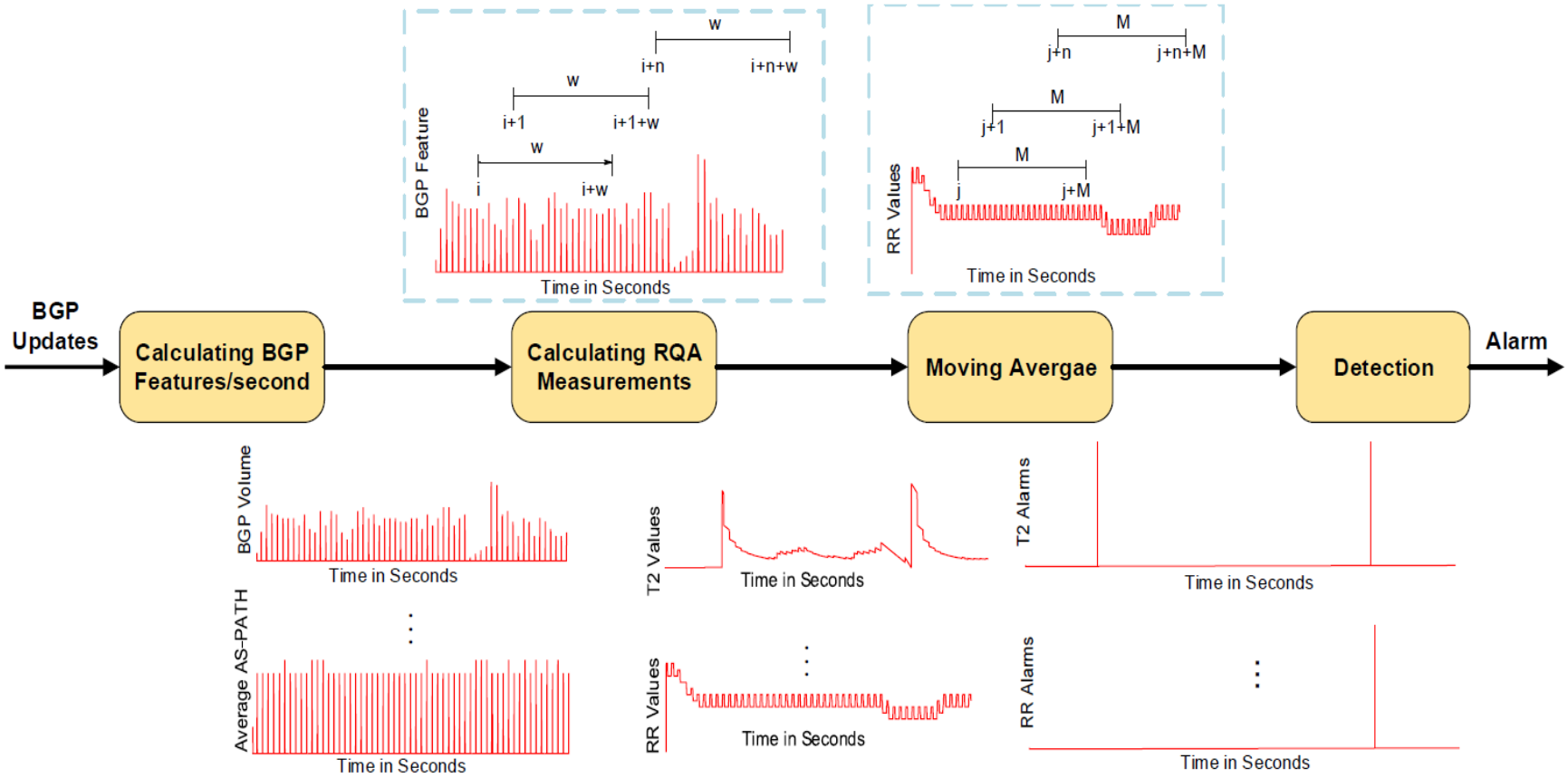


Figure (1): RQA Scheme Design

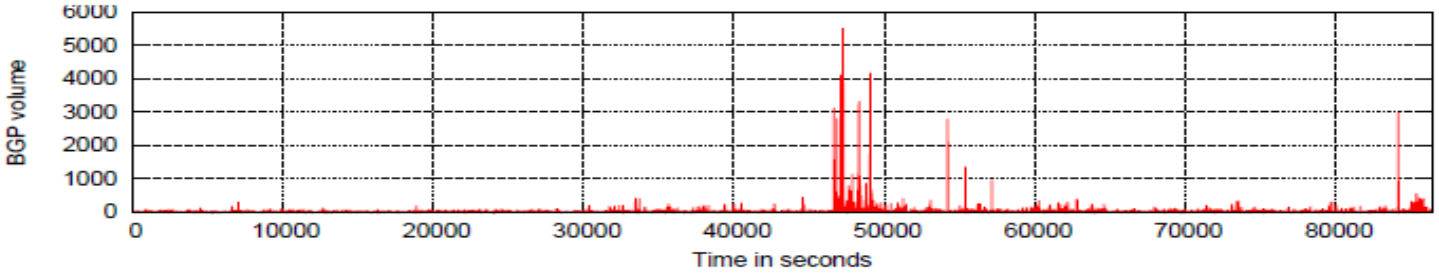
Detecting BGP anomalies using RQA

Evaluation

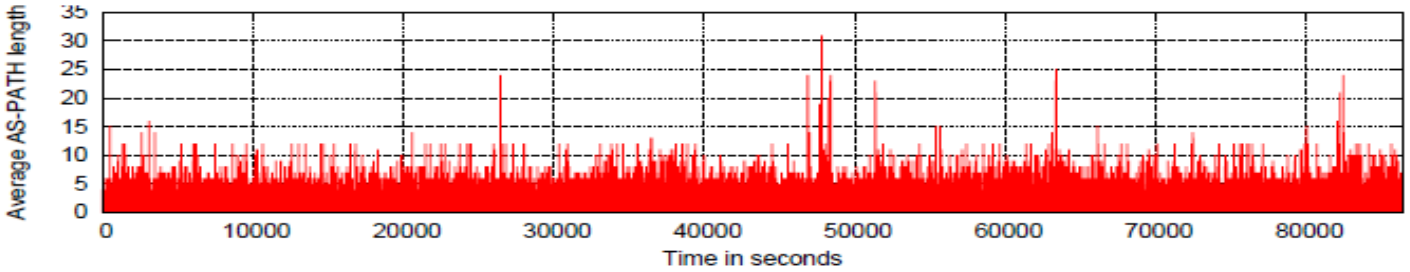
Table(1): List of Notable BGP Events

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

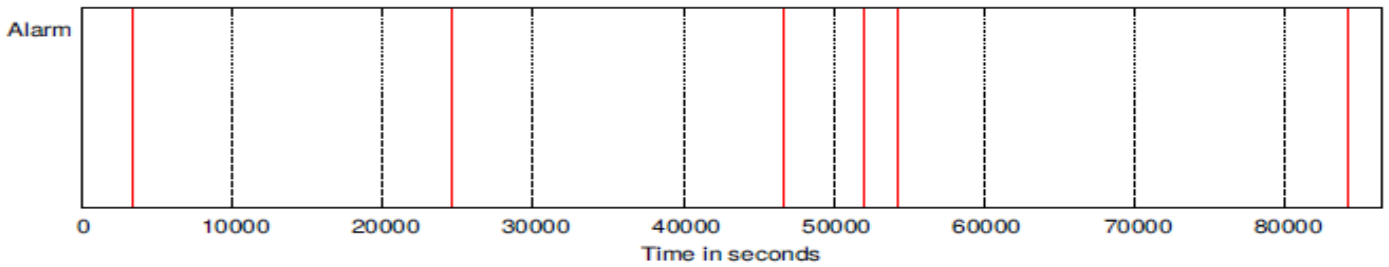
Detecting BGP anomalies using RQA



(a) BGP volume feature over 24 hours



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



(c) Detecting BGP anomalies using RQA scheme

Figure (2): BGP Features sent by the peer AS12793 during TTNet event and RQA scheme output

Detecting BGP anomalies using RQA

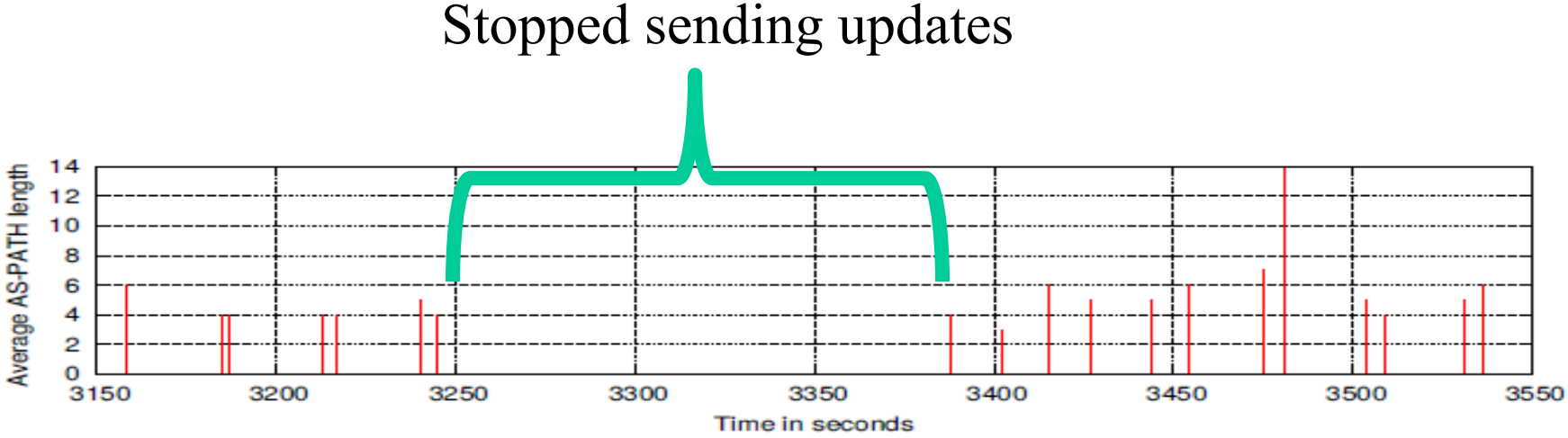
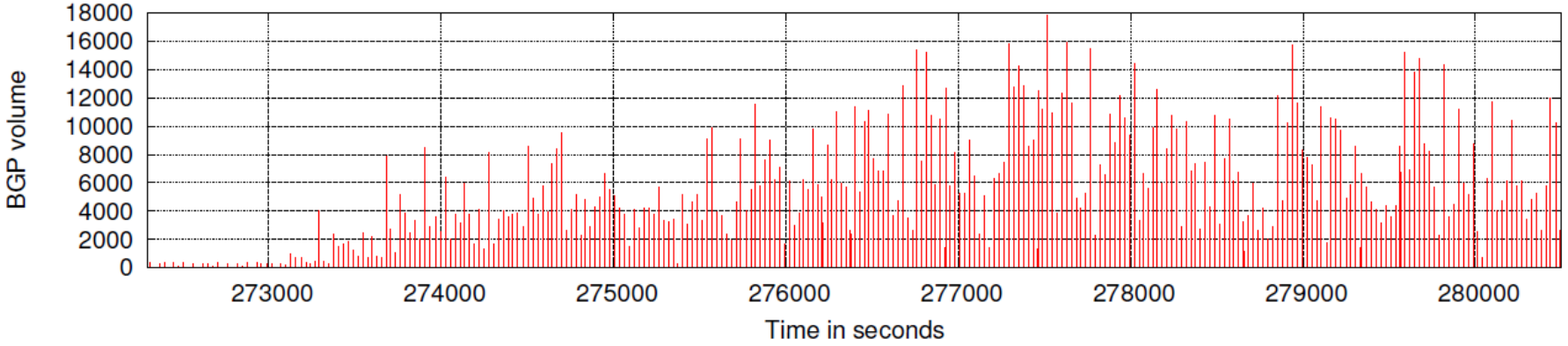
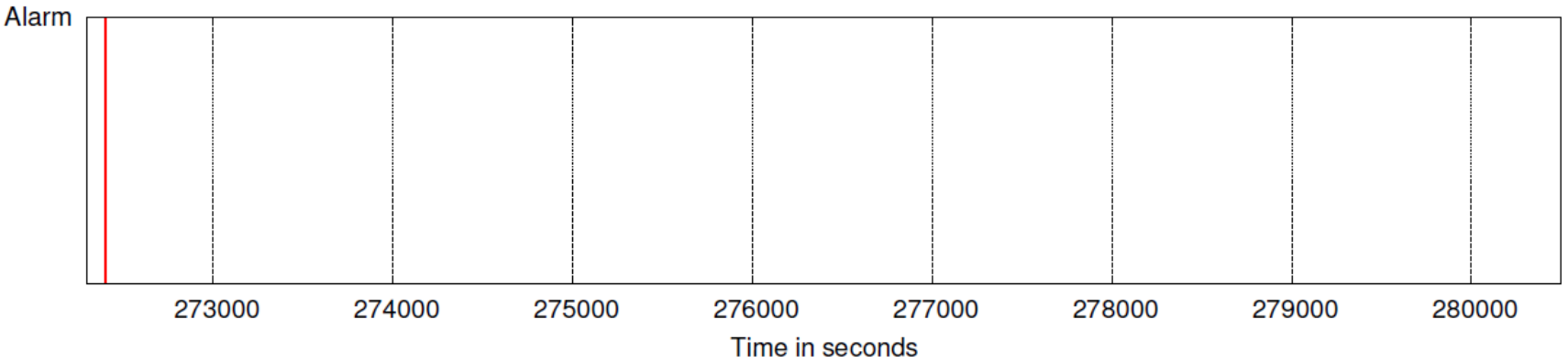


Figure (3): Detecting hidden anomalous behaviour by RQA, AS12793 stopped sending BGP updates for two minutes

Detecting BGP anomalies using RQA



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



(b) Early detection of BGP anomalies during Moscow blackout

Figure (4): Detecting BGP anomaly before 730 seconds of sending high volume of BGP traffic

Detecting BGP anomalies using RQA

Evaluation Summary

- RQA Scheme requires only **20 minutes** of history to detect anomalies in a range **1-200 seconds**

Table(2): Evaluation Summary

Event	TP	TN	FP	FN	Precision	Sensitivity	Accuracy	F-score
Nimda	7	421405	5	0	0.5833	1	0.9999	0.7368
TTNet	6	85201	0	0	1	1	1	1
Moscow	9	597376	3	0	0.75	1	0.9999	0.8571
TMnet	8	85205	0	0	1	1	1	1
Summary	41	1233739	8	0	**0.8367**	**1**	**0.9999**	**0.91111**

Real-time BGP Anomaly Detection Tool (RBADT)

- real-time plot
- logs all detected BGP anomalies with their time stamps
- logs last 20 minutes of BGP features
- offers the facility of sending an e-mail notification

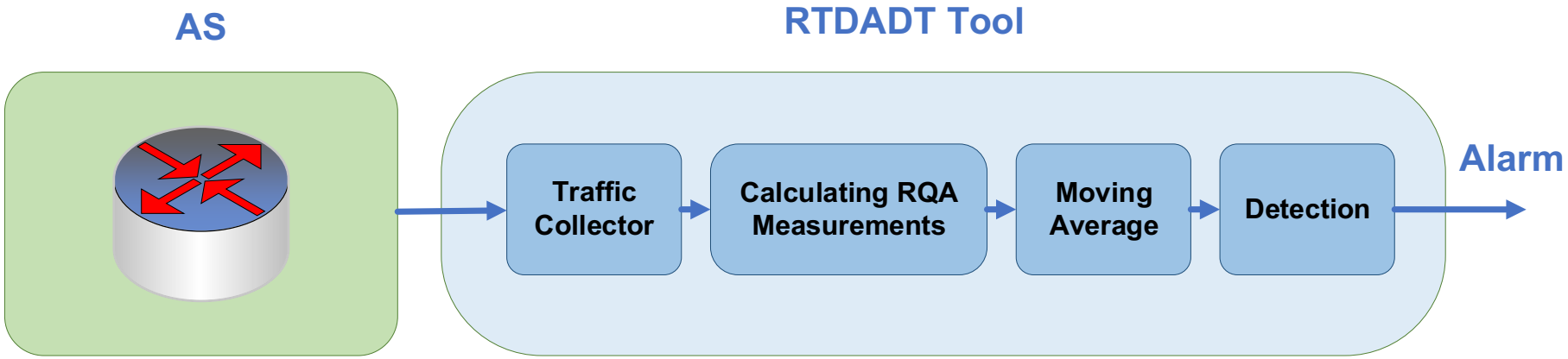


Figure (5): RBADT System Design

RTBADT available on:http://caia.swin.edu.au/tools/bgp/brt/rtbadt-0.1.tgz

Real-time BGP Anomaly Detection Tool (RBADT)

- Evaluation of RTBADT-TMnet event

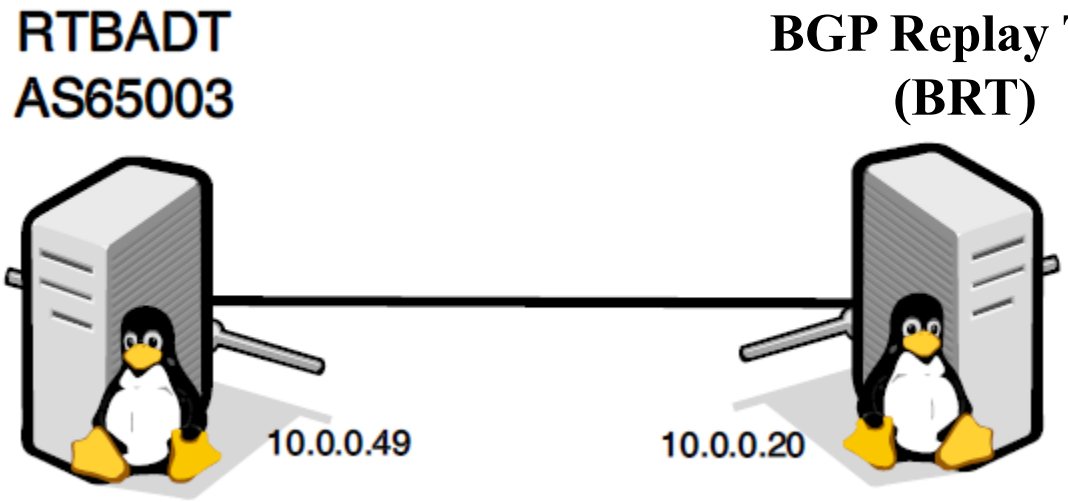


Figure (6): A Simple example to monitor an AS using RDTD tool

BRT available on: http://caia.swin.edu.au/tools/bgp/brt/brt-0.2.tgz

Evaluation of RTBADT-TMnet event

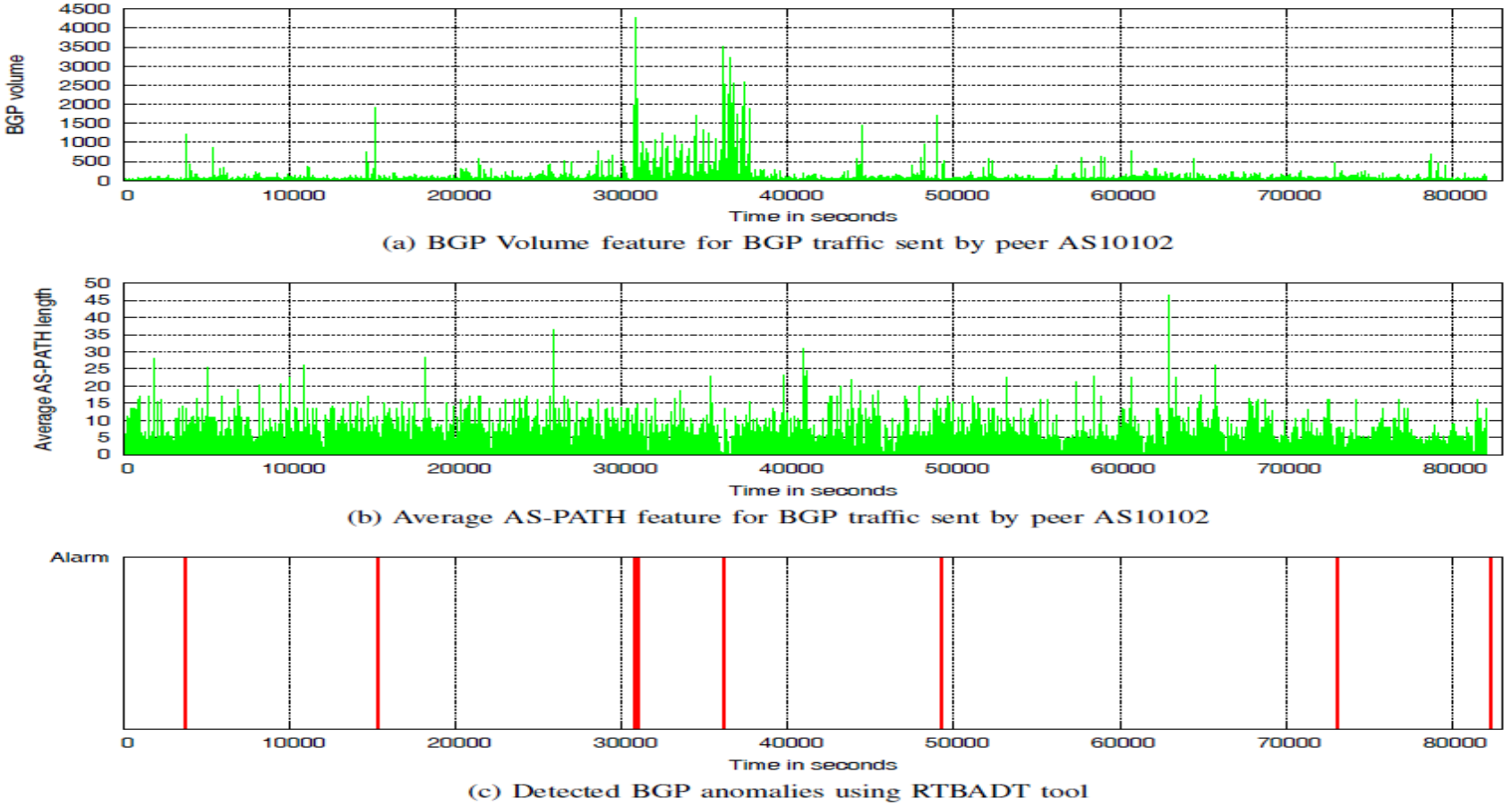
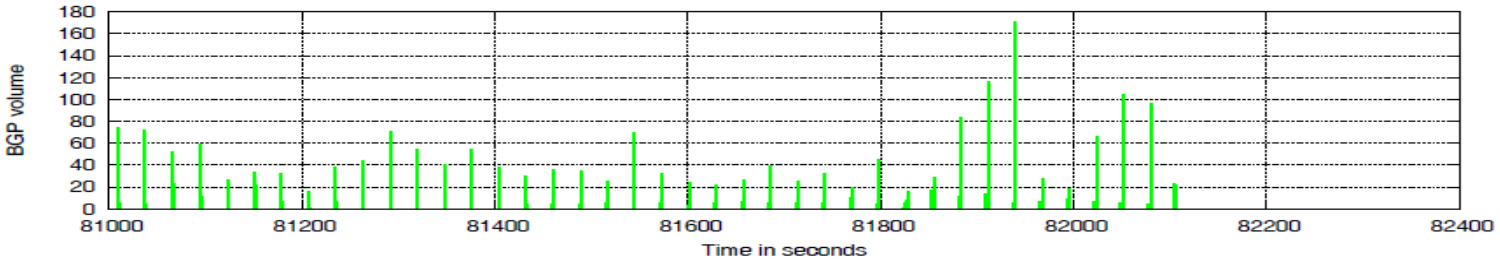
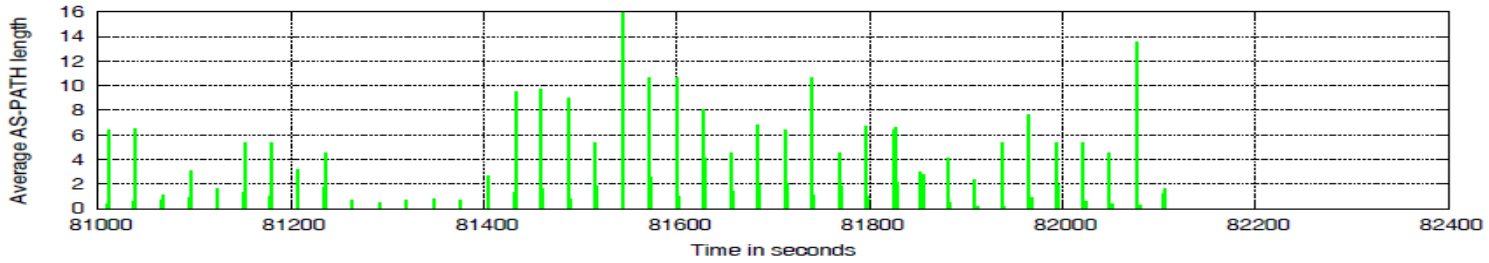


Figure (7): Detecting BGP Anomalies using RBADT through replaying TMNet event

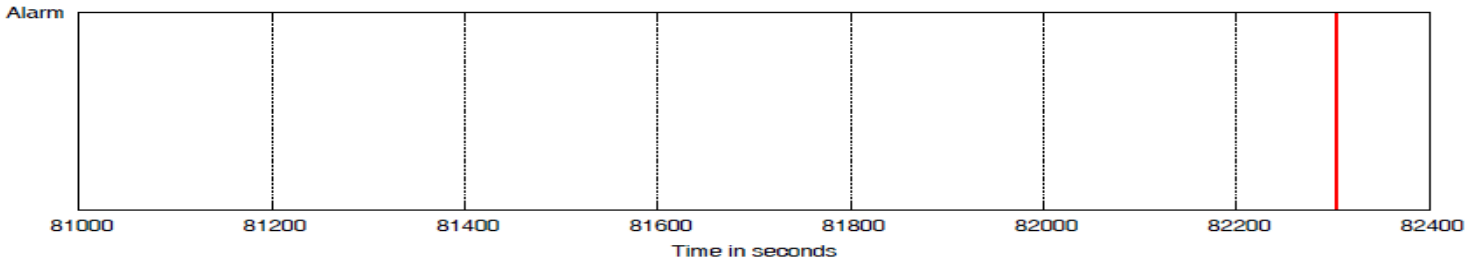
Evaluation of RTBADT-TMnet event



(a) BGP Volume feature



(b) Average AS-PATH feature



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

Figure (8): RTBADT raised an alarm when the monitored BGP stopped sending BGP updates

Conclusion

- Detecting BGP anomalies is a challenge
- RQA requires 20 minutes of past BGP traffic to detect anomalies in a range of 1-200 seconds
- RQA can detect hidden abnormal behaviours that may pass without observation
- RQA scheme can detect BGP anomalies with 99% accuracy and 91% of F-score

Our Next step

- Deploy RTBADT to a realistic scenario (call ISPs to deploy RTBADT)

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 2017 27th International Telecommunication Networks and Applications Conference (ITNAC). Melbourne, Australia: IEEE, Nov. 2017, pp. 1–7

Questions


THE MINISTRY OF HIGHER EDUCATION
AND SCIENTIFIC RESEARCH - IRAQ
UNIVERSITY OF KUFA