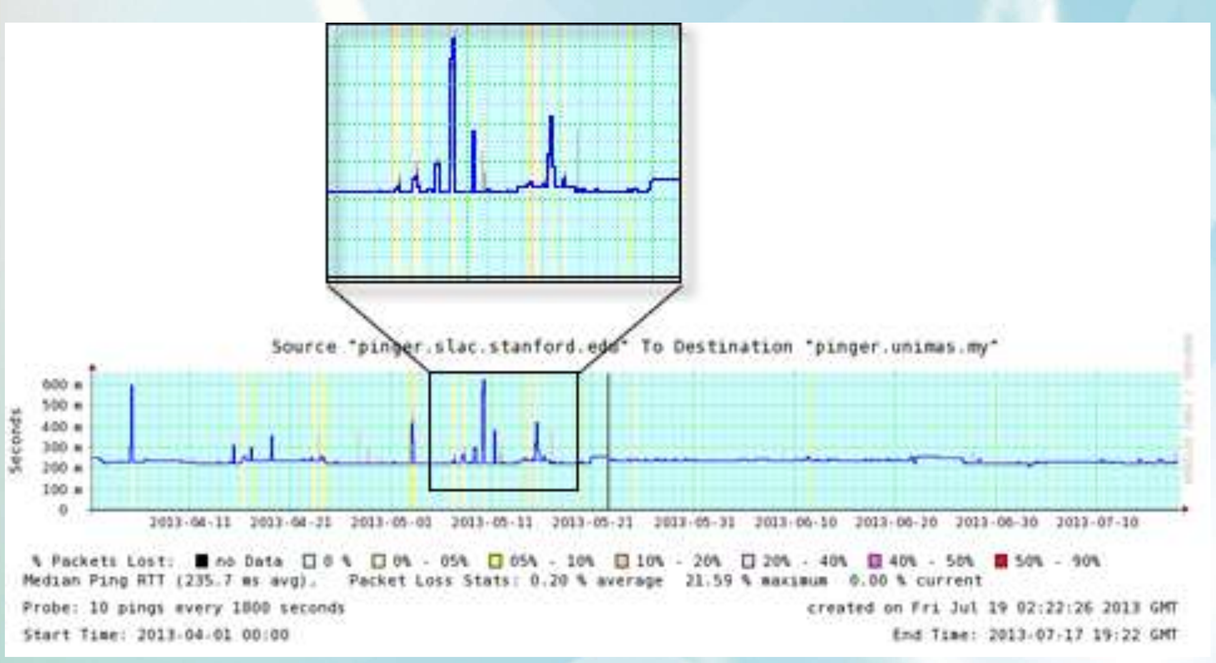
Anomaly Detection Framework for PingER Data

1.0 INTRODUCTION

- The Internet has become a necessity to many organizations and the general public similar to utility such as electricity and water supply.
- Disruption or interruption to Internet availability would means reduced productivity and can be of negative consequence to many organizations.
- Therefore, it is critical that there is a mechanism to monitor Internet performance periodically to detect performance issues.

2.0 WHAT IS PingER

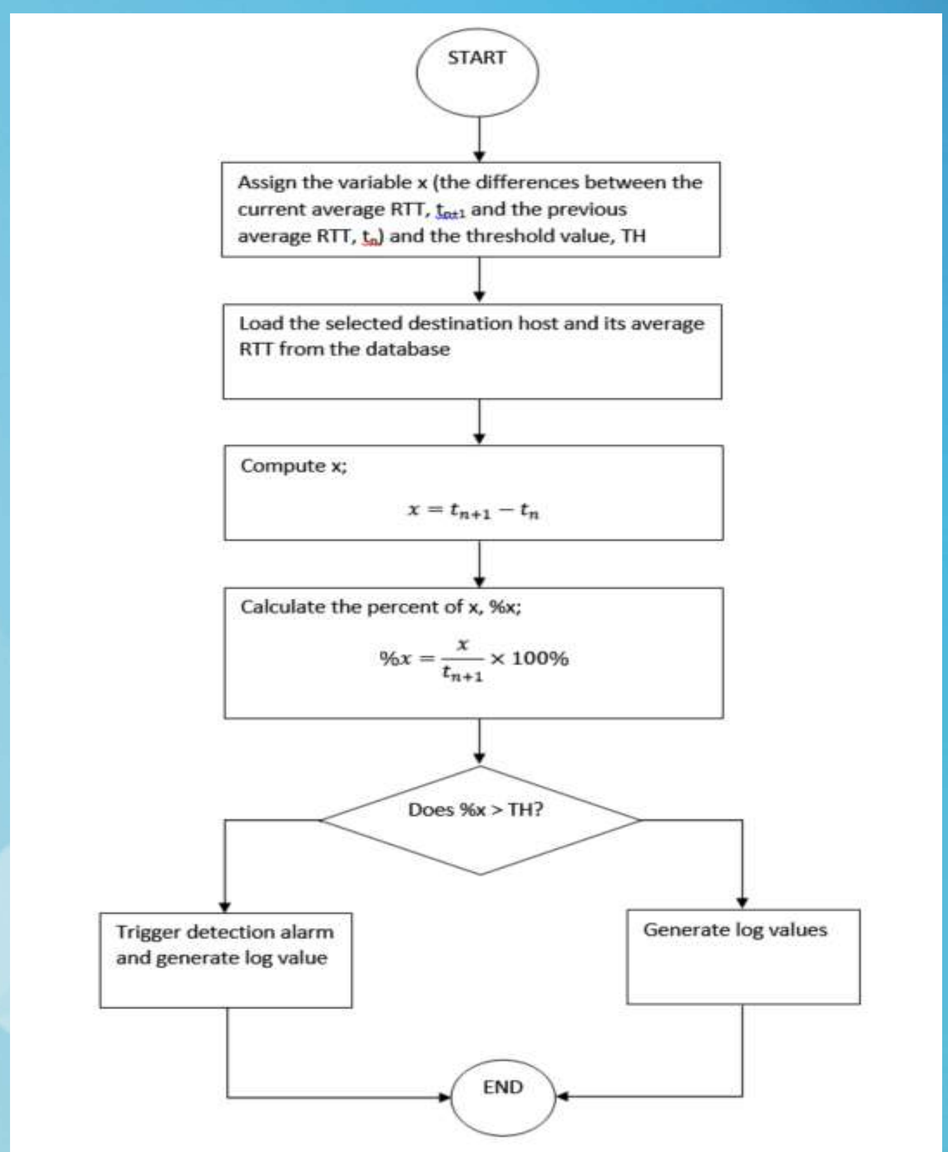
- PingER – Ping End-to-End Reporting
- A monitoring platform whereby UNIMAS has two monitoring nodes that collect network performance data.
- Currently no mechanism to detect when there is an anomaly in the network performance.
- ANOMALY = sudden increase or decrease in data collected (time) which indicates potential abnormal condition.



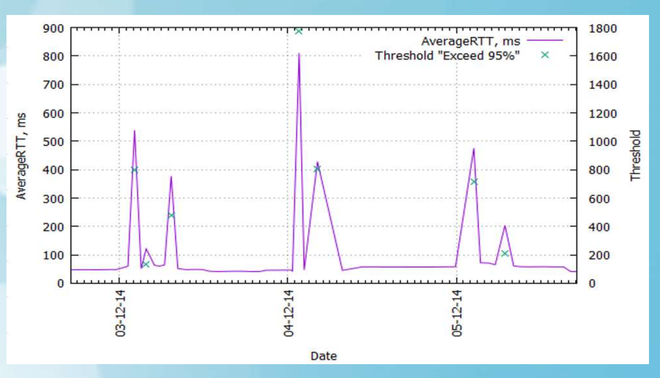
3.0 OBJECTIVES

1. To design and develop an Anomaly Detection Framework for PingER data.
2. To investigate potential algorithm to detect anomaly.
3. To conduct empirical study to verify the effectiveness of selected algorithm.

4.0 FRAMEWORK

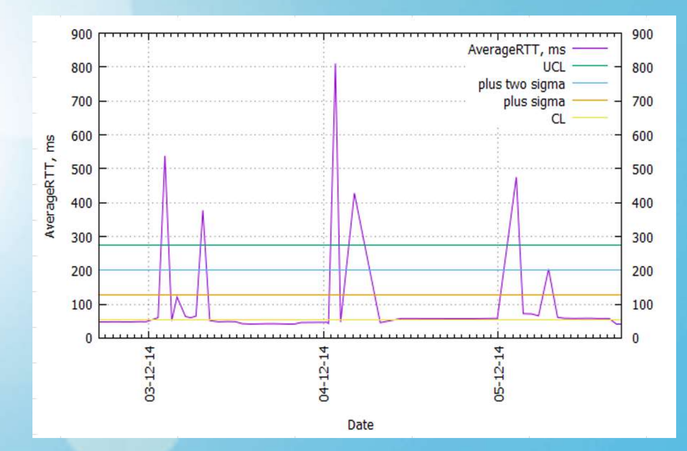


5.0 RESULT



ALGORITHM 1:

Average approach: 100% anomaly detection at 95% threshold level.



ALGORITHM 2:

Statistical approach: 100% Detection of anomaly at plus one sigma.

6.0 CONCLUSION

- Both algorithms manage to detect network anomaly in PingER data.
- The statstical approach perform better since its able to detect all anomaly at plus one sigma as compared to average approach that requires up to 90% threshold level.

Researchers:

Danny Wilson, Johari Abdullah.

Faculty of Computer Science & Information Technology, Universiti Malaysia Sarawak, 94300 Sarawak, Malaysia

Acknowledgement:

This project is under the FRGS grant FRGS/1/2013/ICT03/UNIMAS/02/2.