Anomalous Event Detection for PingER Data

INTRODUCTION

PingER (Ping End-to-end Reporting) project is the name given to the Internet End – to – end Performance Measurement (IEPM) project to monitor end – to – end performance of Internet links. PingER Malaysia is an extension of the main PingER project led by Stanford Linear Accelerator Center (SLAC) in which University Malaysia Sarawak (UNIMAS) collaborates to monitor and collect data in Malaysia and South East Asia. Apart from the main goal of data collection and monitoring of Internet performance, another equally important goal of the PingER Malaysia initiative is to create as much as research opportunity as possible in order to solve existing problems, and/or improve current performance one of which is anomalous event detections for PingER data.

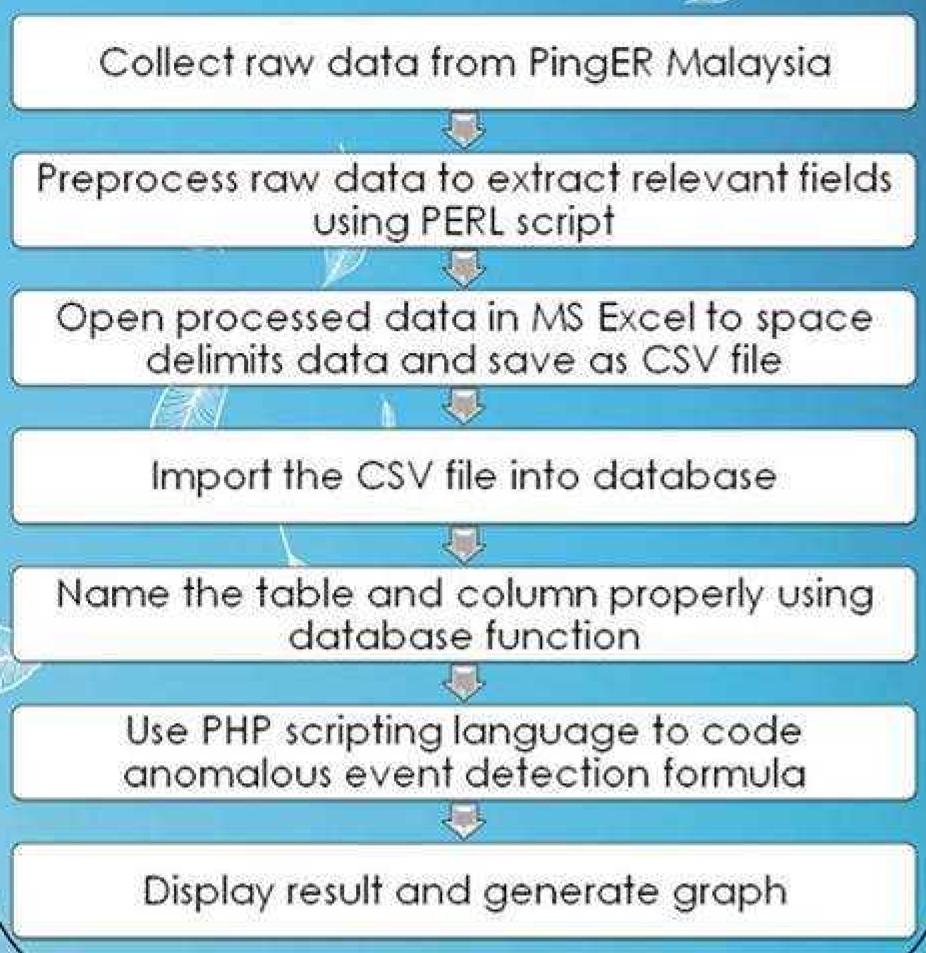
PROBLEM STATEMENT

Several anomalous events also known as spikes/ plateau are identified in round trip time(RTT) graph of PingER data. As a whole, these spikes indicate the performance degradation in the packet transmission between source and destination nodes. Moreover, in current, UNIMAS PingER administrators are manually accessing each RTT graphs of PingER data to identify those spikes for analysis.

OBJECTIVES

- To detect anomalous event(s) found on UNIMAS PingER data using standard average formula for temporal and spatial approaches for three various threshold values.
- To visualize anomalous event detection result in table and graph through a simple web interface.

METHODOLOGY



Collect raw data from PingER Malaysia

Preprocess raw data to extract relevant fields using PERL script

Open processed data in MS Excel to space delimits data and save as CSV file

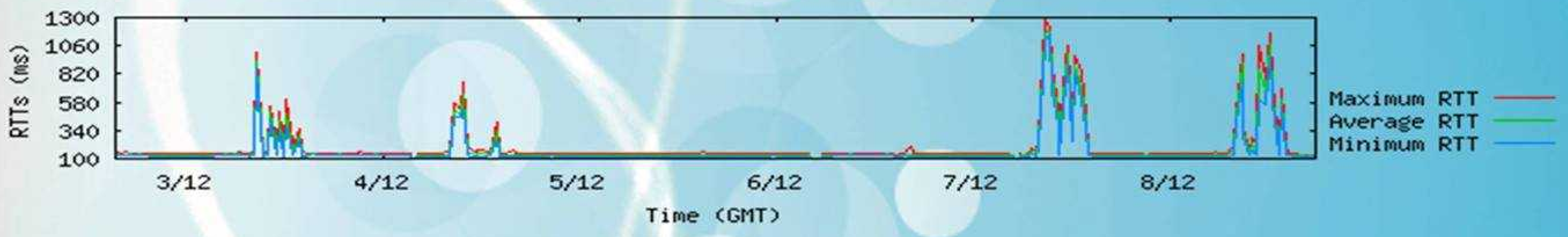
Import the CSV file into database

Name the table and column properly using database function

Use PHP scripting language to code anomalous event detection formula

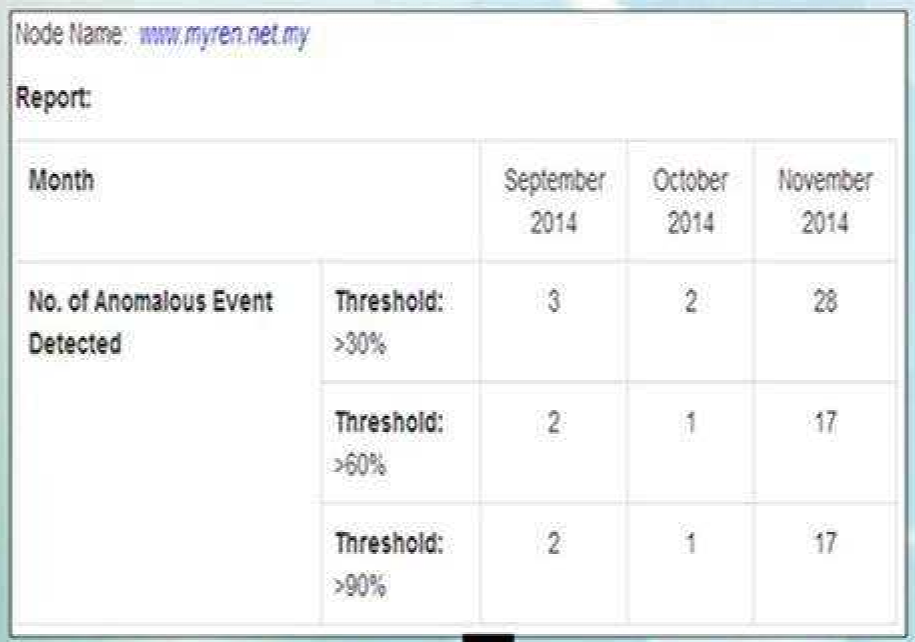
Display result and generate graph

SCENARIO



OUTCOME

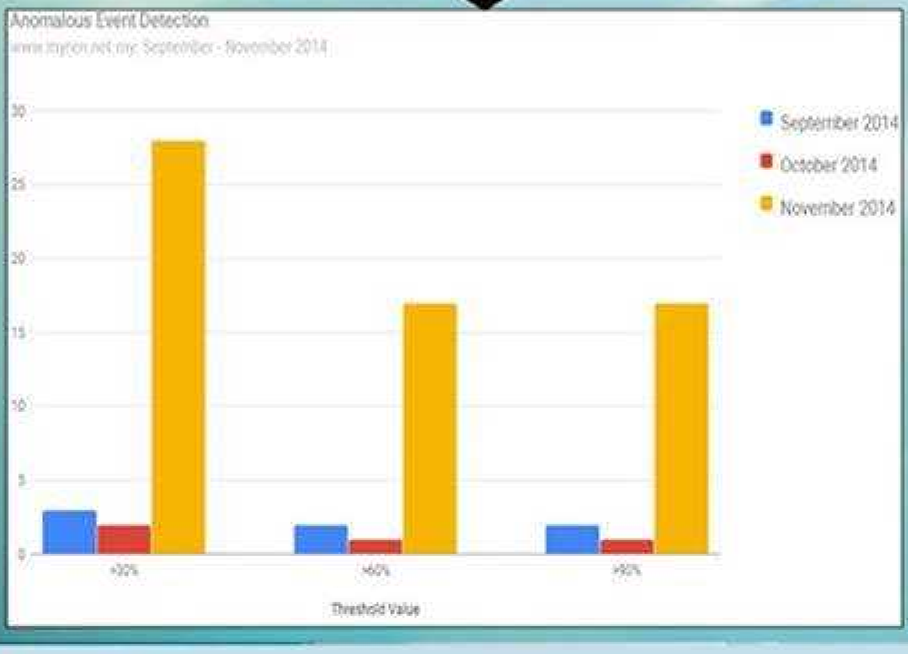
a) Temporal



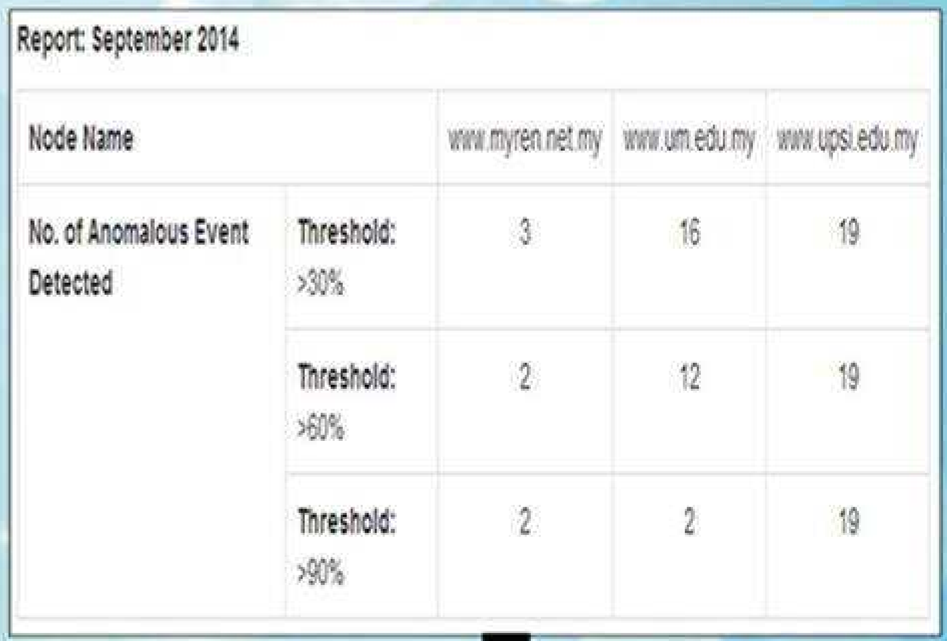
Node Name: www.myren.net.my

Report:

Month		September 2014	October 2014	November 2014
No. of Anomalous Event Detected	Threshold: >30%	3	2	28
	Threshold: >60%	2	1	17
	Threshold: >90%	2	1	17

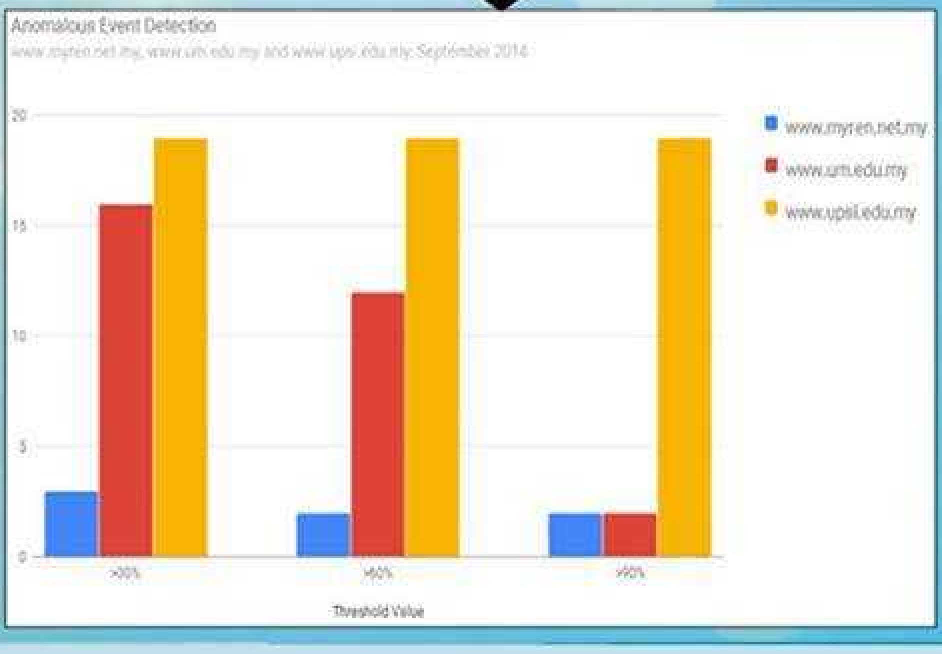


b) Spatial



Report: September 2014

Node Name		www.myren.net.my	www.um.edu.my	www.upsi.edu.my
No. of Anomalous Event Detected	Threshold: >30%	3	16	19
	Threshold: >60%	2	12	19
	Threshold: >90%	2	2	19



METHOD

Using Standard Average Calculation

$$\% = \frac{t_2 - ((t_1 + t_2) / 2)}{(t_1 + t_2) / 2} \times 100\%$$

Benchmark:
Threshold >30%, >60% and >90%

CONCLUSION & FUTURE WORKS

The main objective of this research - to detect anomalous event found on the time series graph of PingER data is able to achieve with appropriate steps to create superior result. It is truly hoped that the developed system is able to reduce the workload of system administrator in detecting and reporting anomalous event. As for future enhancement of the system, the scope of the system need to expand to allow user to select *from* and *end* date to view the number of anomalous event detected during that period. Alarm in the form of email or short message service (sms) can be included into the system as well.

Reseacher:

Kayathiri a/p Batumalai

Network Computing, Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak

kayathiribatumalai@gmail.com

Acknowledgement:

Acknowledgement of gratitude is dedicated towards Dr.Johari bin Abdullah (supervisor), Universiti Malaysia Sarawak (Institution), family and friends for invaluable guidance that provide ability to tackle challenges head on.