Paper Review 5/13

Andres Calderon - SID:861243796

May 18, 2016

Diagnosing Network-Wide Traffic Anomalies (Lakhina et al., 2004)

This paper describes a technique to detect, identify and measure traffic anomalies on a network. It is based on Principal Component Analysis (PCA) of high-dimensional, noisy data. The analysis is able to separate the subspace of the normal traffic and detect the anomalous component corresponding to the anomalies.

Although the evaluation of the method focuses on *volume* anomalies, it is based on correlations of time-series from diverse links and its treatment as a spatial problem. Therefore, the method can be extended to other types of anomalies.

Overall, the paper is interesting and easy to read. Particularly, it is more related to my area of interest (data mining). On that sense, it is well-known that PCA is quite expensive in terms of execution time. I would like to know if other techniques for time-series anomaly detection were considered. Anytime clustering of time-series has shown very efficient results in the analysis of real-time complex problems.