Paper Review: Correlating instrumentation data to system states: A building block for automated diagnosis and control

Sohail Ahmed Shaikh

January 28, 2019

1 Summary:

The focus of this paper is the use of statistical models for analysing system metrics. Such models are used for performance diagnosis. The model is built on top of Tree Augmented Bayesian Network (TAN) which helps to correlate the system level metrics and their corresponding threshold values with SLO violations or compliance. The authors evaluate the TAN model on a testbed to determine it's accuracy and efficiency in performance diagnosis in an online or offline environment.

2 Description:

The ever-growing scale of networked systems make it quite complex. The state of the system is depended on the interactions of a lot of metrics such as workload, hardware, traffic, etc. Thus performance diagnosis is not so straightforward and quite tedious.

The authors attempt to address this problem through a statistical learning approach which does not assume a priori knowledge of the system. Models of the system are induced automatically from network services to predict and diagnose failure conditions. Specifically the model leverages TAN for this. The appropriate selection of a TAN classifier is based on heuristically selected subset of metrics. Instead of detecting anomalies in the system the authors resort to classification to predict and diagnose performance problems. The authors introduced balanced accuracy instead of accuracy which accounts for probabilities of correctly identifying compliance and violations of SLO. Hence, this solution can be applied to systems where violations are uncommon.

The performance of the system is also evaluated on varying workloads. The workloads are varied on a number of factor so as to represent real scenarios and cover a wide range of inputs on steady as well as bursty traffic. The SLO requirements defined by threshold values were also varied in the range of 10%-40%. The balanced accuracy in this system was found to be high (in the range of 87%-94%). They also estabilised through the experiments that a single metric does not suffice to capture the state of the system.

Finally, the authors describe the evaluation of accuracy of forecasting SLO violations using their model and show that the accuracy of the system still remains high.

3 Strong points:

1) No previous knowledge is required for a system based on this model.
2) Key measure of accuracy is balanced accuracy which is better than using only accuracy as a measure

in scenarios where failures are uncommon.
3) During evaluation they account for both steady and bursty traffic.
4) Small number of correlated metrics suffice to capture patterns of SLO violations. So overhead is reduced as compared to capturing all the metrics in the system without significant increase in accuracy of identifying SLO conformity.
5) It is possible to incorporate expert knowledge due the modifiability property of Bayesian networks (TAN).

4 Weak points:

1) Number false positives increases as the number of faults increases. This can be a cause of the authors' approach to use classification instead of anomaly detection.
2) On a system running multiple applications, it would be difficult to determine which application caused the performance degradation on the basis of system metrics alone.
3) The appropriate TAN model selection is based on a greedy strategy. However, this may not be the optimal solution.

5 Improvements:

1) The system overhead for implementing the model is not described. This should be explored further.
2) In a constantly failing system, the number of false positives will be quite large. In modern distributed systems with commodity hardware this might be more pervasive. Hence only relying on a classification scheme may not suffice. A probabilistic model that determines anomalies might be better in this case. This requires some research.