Paper Review: Capturing, Indexing, Clustering and Retrieving System History

Sohail Ahmed Shaikh

January 28, 2019

1 Summary:

The authors describe a method of formulating indexable signatures that represent essential characteristics of the system state and clustering them to aid systematic problem diagnosis in a complex system. Such a method would help in determining if the current state is similar to a previously observed state. This would help operators to identify recurrent problems and leverage previous diagnostic eﬀorsts, if some problem in a system is the same as before. The authors further enumerate that collecting only raw values is ineﬀective and instead adopt a statistical modelling approach. The authors demonstrate this on a synthetic system as well as in a production environment with real data.

2 Description:

Modern software systems are complex and determining the cause of problems arising in such a system is diﬃcult because they arise from a number of low level metrics. Moreover, focusing on a single metric is not accurate as a number of low level metrics might be interdependent. Due to inadequate methods of representing such problems, it is diﬃcult to leverage past eﬀorts spent on a recurrent problem or even to identify that a particular problem has occurred before.

To solve this problem the paper describes a formal representation of the metrics of a system or signatures to capture essential state of a system. This method is more eﬀective as compared to just storing raw data because clustering is poor in this naive approach. Tree-Augmented Naive Bayes(TAN) model is used for statistic modelling of low level system metrics such as CPU utilization, average response time, throughput, etc. The TAN model describes the relationship between Service Level Objective (SLO) state and the metric which is likely to contribute to this state probabilistically. Such a model is calculated by continuously monitoring the low level metrics and many such models are constructed at every 5 minute interval epoch. A subset of these models are chosen which had a higher accuracy in estimating the SLO state. From these models a set of abnormal metrics are extracted and these contribute to signatures of the system at each epoch.

The authors show that these signatures can be clustered. Clustering helps to group together similar states of a system and can help determining clustering of signatures having similar performance problems. Such clusters are generated using iterative algorithms such as k-medians to ﬁnd k cluster centers. Each cluster has an entropy associated with it to determine how much the signatures within a cluster diﬀer. In ideal conditions there should be no entropy for a cluster. The authors have evaluated the system for k=5 clusters with good results.

Finally, the authors describe a procedure by which N closest signature are retrieved, given a signature based on precision and recall values. So, an operator who has to determine if a problem has occurred in the past could just feed the current signature to the system and get N closest signatures.

The authors also describe the evaluation of their system in a simulated environment as well as data from a real production environment.

3 Strong points:

1) The workload generator and testing done on the representative data are quite exhaustive and have a wide range of operations.
2) It works on annotated as well as non annotated data. In real systems most of the metrics may not be annotated or would be partially annotated.
3) They showed a provable advantage over using raw data to represent the state of a system.
4) This system helps in identifying recurrent problems which is very vital in saving the time spent on debugging a problem. It can also help identify possible regressions.
5) The authors showed that the signatures can be used across different sites to identify similar problems.
6) They have formulated a systematic way in which operators can diagnose and troubleshoot a problem and try to determine it's root cause.

4 Weak points:

1) In testing of this system in a real application the authors have verified the information retrieval only in the small subset of data for which they had annotations. This picture may not represent the true accuracy of the system.
2) They don't describe why they chose k=5 as a value for clusters.
3) Some of the metrics discarded as irrelevant could be actually useful in the future performance.
4) The authors correlate performance of precision/recall with attribution. However the direct causality between the two is not substantiated.
5) The accuracy demonstrated by the authors of the test data is 92% which they claim is sufficient. However, in real data this may not be so as considerable time might be spent on false positives.
6) The system has some overhead for continuous monitoring of metrics and signature generation. However, that is to be expected if want to aid debugging and leverage past data.

5 Improvements:

1) Some details regarding the values chosen for clusters, must be provided and the accuracy of the system with varying cluster size should be studied.
2) Some heuristics might be incorporated to identify periodic patterns in occurrence of problems by incorporating time information.
3) The system must be evaluated with non annotated or partially annotated data to get a true representation of the accuracy.
4) Instead of monitoring the system metrics continuously the overhead of the system can possibly be reduced by incorporating a reactive approach, i.e. start capturing the system metrics when the degradation starts.