Paper Review 5

Bharath Venkatesh
bharat

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

Summary

The core idea of this paper is to build a *domain agnostic* automated model for analysis of instrumentation data from network services in order to forecast,diagnose and repair failure conditions. It uses *Tree Augmented Naive Bayesian Networks* [TAN] as the basis of performance diagnosis and forecast. The induced TAN model selects a combination of metrics that correlate with high level performance states with a goal of building a *classifier* that predicts whether the system will be in compliance over a given interval of time. It involves two stages: In the first stage, it induces a classifier function F that maps the universe of possible values[M] to the range of System states{compliance, violation}. The measure of accuracy at this stage is evaluated based on *"Balanced Accuracy"* that accounts equally for correct classification of both SLO states in the system. In the second stage, a TAN based Bayesian Network model is built that represents the relationship between the M and S in a way that is compact, accurate and efficient to process. Since a subset of metrics and threshold values is sufficient to approximate the distribution efficiently in a TAN,the model restricts the form of Bayesian Network to a TAN and further selects an optimal TAN classifier over a heuristically selected subset of the metrics. The user also has an option to *"seed"* the model by preselecting a set of metrics that must appear in the model and the range of values that it can occupy. The model ensures robustness by following *ten-fold cross validation*. The model was tested on a three tier web application under three different workloads. Results showed that, given N samples of the n metrics, the algorithm runs in $O(n^2.N)$ time and has a Balanced Accuracy of 87-94%.

Pros: Why the Paper Should be accepted

- The key take away from this model is the fact that it built performance models that are *application agnostic* in nature. It does not require any prior knowledge of the system and builds performance models based on passive measurements alone.
- Secondly, the model correlates system level metrics with application performance and thus can *adapt to changes in system* more rapidly and at lower expense. It also *minimizes false alarms* that are raised due to such changes.
- Appreciably, the use of TAN model presents two practical advantages: *Interpretability and Modifiability.* The Interpretability property allows one to interrogate the model to identify specific metrics that affect the classifier choice. The Modifiability property allows the model to incorporate expert knowledge and constraints into the model efficiently.
- The model is cheap to induce and thus the system can *refresh periodically* to account for change in workload characteristics. It also allows multiple such models to be in *run in parallel* to account for more dynamic and real-time cases.
- Since the model efficiently identifies metrics and threshold values that correlate with SLO violations,the classifier indirectly *identifies system elements* that are most likely to be *involved in failures and violations in future*.

Cons: Why the paper may be rejected

- A key constraint to this approach is that, it is supervised and requires a considerable amount of *previous traces to be available and labeled* into complaint and anomalous. This raises a concern on its applicability in systems where such trace labellings are not available.
- Though the approach predicts violations and compliance with good accuracy, it does not provide any information on what caused the problem and *how to adapt to such SLO violations*.
- Another key drawback of the algorithm is that, it is sensitive to workload and SLO definitions. The results of the tests conclude an alarmingly *high rate of false alarms as the SLO threshold increases*.
- Since the classifier function gives an entire set of values consisting of both compliance and violations, it contains a lot of i*rrelevant metrics* that yield no information on the SLO state.

Ideas for Future Research

- A more complete model for adaptive self managing systems can be obtained by *combining apriori models with the proposed automatically induced systems*.
- An interesting improvement over the existing approach would be to extend it to *adapt automatically for changing conditions and workloads* in the system.
- Although the model accurately determines the cause for problems that have occurred, efficient forecasting techniques that *predict the duration and severity of future impending violations* would increase the usability of the system.
- Another area of research would be to build a model that utilizes the information provided by this model to *deduce what needs to be done to bring the system to SLO compliant state*.

Capturing, Indexing, Clustering, and Retrieving System History

Summary

The paper presents a method for automatically extracting an indexable signature that represents the essential state of an enterprise system. This signature is subjected to automated clustering mechanisms and similarity based retrieval to identify if the observed state has ever occurred before during its run. The mechanism effectively helps operators in distinguishing recurrent conditions from a transient, first time condition and applying the repair procedure that was previously annotated for the problem. It involves three stages: In the first stage, time is divided into regular epochs and a for every epoch, a subset of models with high accuracy score in estimating the SLO state of the window is selected. Further a signature vector S is extracted representing the characterization of the system both in compliance and violation periods during the epoch. Second stage involves clustering these signatures to represent a collective characterization of different performance problems and normal operational regimes. The proposed approach uses a distance metric to measure the sum of distance of each signature to the cluster center and further introduces a "purity" measure to evaluate how good the cluster represents the state of the system. An average entropy nearing zero indicates a pure cluster containing only compliance or violation. During the third stage, we retrieve all previous instances that are similar to a specific signature. This helps the model to leverage past diagnoses and repairs in resolving the current issue. A measure of the accuracy in retrieving these signatures is performed by two qualities: Precision- A measure of the fraction of the returned items having a matching annotation

and Recall – A measure of the percentage of signatures in the database actually retrieved. The paper includes a detailed case study validating its claims in building signatures, identifying a recurrent problem and leveraging signatures in solving problems across sites.

Pros: Why the Paper Should be accepted

- One of the key take away from this approach is the fact that is was the first concrete approach to construct an appropriate representation of the state of the system and evaluate its efficacy.
- This approach helps in distinguishing recurrent problems from transient ones and thus helps in re-usability of previous solutions. It also helps in annotating first time occurring problems with a repair procedure for future reference.
- Since the approach accounts for solving problems spread across sites, it helps in reducing redundant diagnostic efforts across time, geography and organizational boundaries.
- Since the overhead involved in computations take minimal time, the approach is well suitable for real-time applications.

Cons: Why the paper may be rejected

- Since the approach is solely based on the accuracy of the signature extracted, it might suffer serious problems if an SLO state over a specific period of time *maps to two or more different set of metrics.*
- Another key drawback discussed in the paper is its *inability to find the actual root cause of the problem.* The paper solely bases its diagnosis on the state of the system and thus does not point out the actual cause that led to the state.
- The algorithm is very stringent in terms of the signature matches and thus will be able to map recurrent solutions that only exactly matched the current state. However in several situations it be useful to consider partial matches and extract the information inherent in them.

Ideas for Future Research

- An avenue for future research would be to consider making the algorithm *more scalable and robust* to handle huge amount of data in a data center like environment.
- Since the model constructs signatures only based on running traces, it might be interesting to consider an extension that takes into account *both the system state and the source code for the application.*
- A more flexible *Pattern recognition* framework can be built above the model to account for partial signature matches and extracting key information from them.
- An approach to solve synonyms in states could be to predetermine such matching synonyms and pick a combination of metrics from all matching sets.