DeepTraLog: Trace-Log Combined Microservice Anomaly Detection through Graph-based Deep Learning

A microservice system in industry is usually a large-scale distributed system consisting of dozens to thousands of services running in different machines. An anomaly of the system often can be reflected in traces and logs, which record inter-service interactions and intra-service behaviors respectively. Existing trace anomaly detection approaches treat a trace as a sequence of service invocations. They ignore the complex structure of a trace brought by its invocation hierarchy and parallel/asynchronous invocations. On the other hand, existing log anomaly detection approaches treat a log as a sequence of events and cannot handle microservice logs that are distributed in a large number of services with complex interactions. In this paper, we propose DeepTraLog, a deep learning based microservice anomaly detection approach. DeepTraLog uses a unified graph representation to describe the complex structure of a trace together with log events embedded in the structure. Based on the graph representation, DeepTraLog trains a GGNNs based deep SVDD model by combing traces and logs and detects anomalies in new traces and the corresponding logs. Evaluation on a microservice benchmark shows that DeepTraLog achieves a high precision (0.93) and recall (0.97), outperforming state-of-the-art trace/log anomaly detection approaches with an average increase of 0.37 in F1-score. It also validates the efficiency of DeepTraLog, the contribution of the unified graph representation, and the impact of the configurations of some key parameters.

Camera ready version to come soon.