THROUGHPUT ANOMALY DETECTION IN KUBERNETES CLUSER WITH ANTREA

Subramanian Venkataraman, Yongming Ding (Mentor), Salvatore Orlando (Manager)

MOTIVATION

- RCA for complex network issues – pain point for Network and DevOps Engineers – Identification and understanding the problem.
- Not acting on the anomalies on time results in performance degradation of the application.

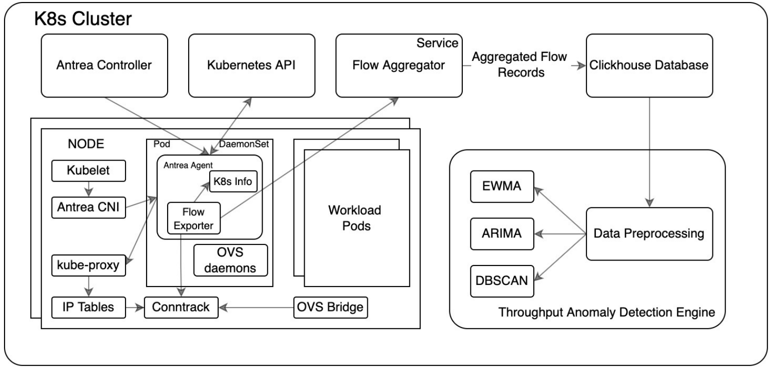
WHAT IS ANTREA?

- Kubernetes-native CNI offering High-performance and is based on the Open vSwitch project (OVS)

HITCH

- Performance analytics tool to provide an automated troubleshooting solution
- Input - Network flow data as Time series from ClickhouseDB

ARCHITECTURE

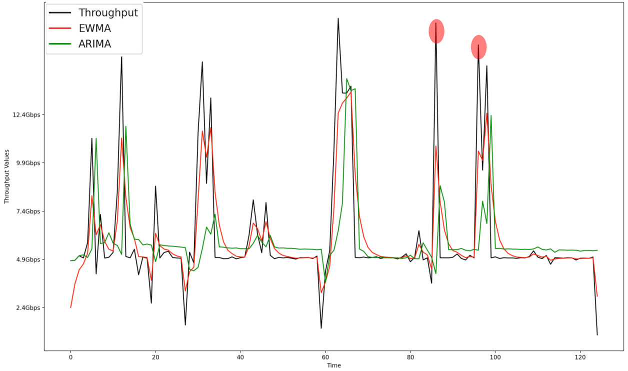


MY CONTRIBUTION (SO FAR…)

- Developed a Spark job to find the anomalies in existing traffic
- Implemented multiple Time Series Algorithms – EWMA and ARIMA to identify anomalies and forecast anomalies

Result	EWMA	ARIMA
Accuracy	93%	95%
Precision	33%	66%
Recall	50%	66%

Calculated on a 30 min iPerf3 Traffic of 5Gbps with multiple spike in throughput values



FUTURE WORK

- Improve Model performances
- Identify anomalies in real time using Spark Streaming APIs
- Develop CLI commands for user interaction