Title:
Machine Learning Algorithms for Anomaly Detection in Agile All-Photonic Networks

Authors:
Tarem Ahmed and Mark Coates
tarem.ahmed@mail.mcgill.ca, coates@ece.mcgill.ca

Abstract:

High-speed, backbone networks are known to experience a wide range of anomalous behaviour. Our objective is to develop anomaly detection algorithms suitable for use in an agile all-photonic network. Machine learning techniques enable the development of algorithms that are non-parametric and adaptive to changes in the characteristics of normal behaviour, making the algorithms robust over time and portable across applications. In this research, we develop the recursive Kernel-based Online Anomaly Detection (KOAD) algorithm and apply it to anomaly detection in a large, high-speed network. The KOAD algorithm has been extended from our earlier online anomaly detection algorithm based on Kernel Recursive Least Squares, and shown to produce quick detection with high accuracy and low false alarm rates. We also investigate relationships between the *region of normality* identified by our KOAD algorithm and the concept of minimum volume sets, and apply the block-based One-Class Neighbour Machine algorithm developed by Muñoz and Moguerza. We test our algorithms on a timeseries of *entropies* of the main IP packet headers traversing the Abilene backbone network. The entropy statistic captures the distribution of the traffic, and spotting sudden changes in the entropy enables the detection of a wide range of anomalies.