Title:
Online Anomaly Detection for Optical Networks

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

Abstract:
High-speed optical backbones are constantly hit by network anomalies. These anomalous events span a wide variety of types, from denial-of-service attacks and viruses to large data transfers. Some anomalies are intentionally malicious, while others may be accidental. This necessitates the need for an online and instantaneous anomaly detection mechanism for high-speed optical networks. We propose such a scheme, based on the kernel version of the celebrated Recursive Least-Squares algorithm. Different types of anomalies affect the network in different ways, and it is also not always possible to know a priori, how a potential anomaly would exhibit itself in traffic statistics. Our algorithm learns the characteristics of normal traffic behavior, builds up and maintains a dictionary that approximately spans the subspace of normal behavior, and then raises an alarm immediately upon encountering new data that fall outside the space spanned by the dictionary elements. We test our algorithm on data from the Abilene backbone network.