COLLOQUIUM - NETWORK MONITORING: SEQUENTIAL ONLINE ANOMALY DETECTION BY MARK J. COATES

AARON BEACH

1. Overview

This talk dealt with an online, sequential anomaly detection algorithm designed by the Author. It is online and learneing (building up a dictionary over time) that tries to define a space of "normal behavior". This space is then checked against monitored statistics - which set off alarms when out of "normal" bounds.

2. Background

Mark J. Coates received his BE from Univ. of Adelaide in Australia and a PhD from Cambridge (UK) in 1999. He is a professor at McGill U. in Montreal now. His work is mostly concerned with network security (monitoring), sensor networks, signal processing (and related algorithms), &c. His algorithm is based on the recursive least squares algorithm, and assumed no specific model for network traffic.

3. Evaluation & Novelty

He compared the algorithm with existing off-line methods and demonstrated that his ONLINE algorithm was equally effective while being less complex to calculate (quicker!). His algorithm comes out of study on many subjects ranging from classical network security approaches fused with signal processing style anomaly detection, causal analysis and interference systems.

Date: 10 - 09 - 2006.