Anomaly Detection in Massive Network Traffic using Hidden Markov Models

The Oakland University and School of Engineering and Computer Science communities are invited to attend Sulaiman Alhaidari's defense of his Ph.D. dissertation. Seating is limited. RSVP with Katie Loodeen at loodeen@oakland.edu.

Anomaly Detection in Massive Network Traffic using Hidden Markov Model

Committee: Mohamed A. Zohdy, Ph.D. (Chair), Debatosh Debnath, Ph.D. (Co-Chair), Hua Ming, Ph.D., Xiaodong Deng, Ph.D.

Time: **9:00 - 11:00 a.m.**
Date: **Wednesday, January 30, 2019**
Location: **347 EC**

With the growing number of attacks and malicious threats on the internet services and network infrastructures, the need for techniques to identify and detect attacks is increasing. Therefore, using machine learning techniques along traditional security mechanisms such as firewall and authentication mechanisms, can improve the performance of intrusion detection systems (IDSs).

Network anomaly detection has become very important area for both industrial application and academic research in the recent years. Detecting anomalies (Attacks are detected as anomalies) in data is a crucial problem to diverse real-world applications. Hidden Markov Models (HMM) have been applied to anomaly detection in a variety of applications. The previous researches applying HMM were limited to small data sets. In our work, we have used the term anomaly detection to describe the process of differentiating abnormal behavior from normal behavior on datasets available in this study. In this dissertation, we describe our research contributions for detecting anomalous patterns in massive network traffic using HMM. We built HMM correlates the observation sequences and state transitions to predict the most probable intrusion state sequences that is capable of reducing false positives rate.