IoT Attack Detection and Classification Using Tiered Hidden Markov Models

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

IoT Attack Detection and Classification Using Tiered Hidden Markov Models

Committee: Mohamed Zohdy, Ph.D. (Chair), Debatosh Debnath, Ph.D. (Co-Chair), Richard Olawoyin, Ph.D., Erica Ruegg, Ed.D.

Time: **9:30 – 11:30 a.m.**
Date: **Monday, February 11, 2019**
Location: **347 EC**

Internet of Things (IoT) attacks have rapidly risen in frequency in recent years as IoT devices become more commonplace in industry, businesses, and homes. Since these devices have very basic functionality and are not designed with security in mind, they are easy targets for attacks that can steal data or gain access to the network the devices are connected to.

Here I propose a tiered system of Hidden Markov Models (HMMs) for identifying these attacks and classifying them by type of attack. This system has a tree-based structure, with the main Hidden Markov Model being applied to the raw network data to identify attacks. This main Hidden Markov Model branches off into separate HMMs for each type of attack to classify the attacks according to how important the consequences of the attack are and how likely each attack is to happen.