Machine Learning Approaches for Intrusion Detection and Amelioration in Connected Vehicle Systems

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

Machine Learning Approaches for Intrusion Detection and Amelioration in Connected Vehicle Systems

Committee: Mohamed Zohdy, Ph.D. (Chair), Debatosh Debnath, Ph.D. (Co-Chair), Rakan Chabaan, Ph.D., George Corser, Ph.D.

Time: **1:00 - 3:00 p.m.**
Date: **Thursday, January 31, 2019**
Location: **347 EC**

Connected vehicles (CVs) otherwise known as Vehicular Ad-hoc Network (VANETs) are created on the notion and principle of Mobile Ad-hoc Network (MANET). In CVs, vehicles communicate with one another directly without the presence of an infrastructure or any central entity. Vehicles communicate through dedicated short range wireless communication technology which is combined with GPS technology. Controller Area Network (CAN) Bus is a central networking system responsible for in-vehicle communication between nodes (electronic control units) without a host computer or any dedicated wiring. This simplification comes with a price. An attacker can introduce bogus messages into the CAN Bus network as messages are broadcast to nodes connected to a Bus, which may lead to attacks such as Denial of Service (DoS). In this research, we implement both Supervised and Unsupervised efficient machine learning techniques to detect intrusion in the CAN Bus network. An adversary can also compromise a large number of nodes (vehicles) through spoofing of the nodes identification numbers (ids), and then broadcast bogus messages (supposedly from legitimate nodes) to the network to overwhelm the network and render services such as warning or advice of a potential accident, traffic congestion, severe weather condition, among other things, unavailable. In line with this, this dissertation proposes a framework based on Software Defined Network to detect Distributed Denial of Service Attack (DDoS) in Connected Vehicles using Supervised Machine Learning techniques. Our approach shows that DDoS attack on the centralized SDN controller can be efficiently detected using Supervised Machine Learning henceforth boosting the overall security of CVs.