BIOGRAPHICAL SKETCH

Mr. Moore is a Distinguished Researcher in the Global Security Directorate at Oak Ridge National Laboratory. He has a Masters Degree in Electrical Engineering (Mississippi State Univ BS '85, MS '87) and is working on a PhD in Signal Processing and Machine Learning for Sensors. His current research expertise includes approximately 31 years in Signals and Systems specializing in both EM Fields, Digital Communications, Machine Learning, and Software Defined Radio (SDR). He is a senior member of the IEEE and is a member of AFCEA, the IEEE SCC28 committee on the biological effects of RF and the IEEE 1451 committee on sensor networking.

His more recent areas of research include Electromagnetic Signal Processing, Software Defined Radio, Machine Learning, and Vehicle Security. He has started research programs in each of those areas and worked with many government agencies and commercial collaborators to establish sustained capabilities and funding. He has published approximately 80 peer-reviewed conference papers and technology assessment reports in open venues. He has generated another 40 classified documents that are also technical and reviewed by peers from other National Labs and agency sponsors. He has approximately 15 patents and patent disclosures that span RF hardware, novel hybrid spread spectrum waveforms, and vehicle CAN bus intrusion protection.

EDUCATION

PhD – Tennessee Tech University
Expected graduation December 2018

MS – Mississippi State University
Electrical Engineering, 1987

BS – Mississippi State University
Electrical Engineering, 1985

College of Engineering

TENNESSEE TECH

The Department of

Electrical & Computer Engineering

Announces the Dissertation Defense

of

Michael R. Moore

In Partial Fulfillment of the Requirements

For the degree of

Doctorate of Philosophy

September 24, 2018

Held in

208 Brown Hall at 4:00 p.m.
115 West 10th Street
Tennessee Tech University

FIELD OF STUDY

Signal Processing and Machine Learning for Sensors

DISSERTATION TOPIC

MACHINE LEARNING FOR CYBER PHYSICAL SYSTEM PROTECTION
OF CAN BUS ENABLED VEHICLES
USING DRIVER STATE DISCOVERY

EXAMINING COMMITTEE

Dr. Adam Anderson, Committee Chair
Joint Faculty with the Oak Ridge National Laboratory

Dr. Ghadir Radman
Electrical & Computer Engineering

Dr. Omar Elkeelany
Electrical & Computer Engineering

Dr. Ali T. Alouani
Electrical & Computer Engineering

Dr. Doug Talbert
Computer Science

ABSTRACT

Vehicles are increasingly cyber-physical systems which depend on scores of networked control units. Consequently, modern transportation faces challenges to ensure autonomy, security, and safety. It is imperative to understand the complex decision making, the potential for cyber-attacks, and the vehicle state. Modern vehicles include scores of on-board electronic control units (ECUs) communicating over in-vehicle networks to control safety critical systems. Protecting these networks is especially challenging because there is no publicly available translation of in-vehicle network data to vehicle functions. Thus, intrusion detection systems (IDSs) for controller area networks (CAN) have been previously limited to leveraging statistical properties or protocol standards. An interactive Machine Learning (iML) approach has been developed that produces a model of the physical relationships of CAN signals from only a limited set of CAN packets. These mappings are then used to produce a Hidden Markov Model (HMM) of the driver's actions upon which transaction analysis is performed to optimize the real-time identification of the states. The approach builds an image from the CAN data, then trains a convolution neural network (CNN) to give emission probabilities.

Initial results show that the state of the driver's actions can be predicted with approximately 90% accuracy. Furthermore, it is then shown that within a given driver state, the probability that a cyber-attack is underway can be detected with greater than a 90% accuracy also in near-real time.

The iML approach has been shown to be a rapid modeling capability that supports the production of a digital twin of a system, the mapping of driver states for autonomous decision processes, and optimal utilization of process experts and physical models.