



Thesis Defense

Computer Science Master's Program

“Trim-Transfer: A Transfer Learning Approach for Cross-Trim Level CAN Intrusion Detection”

By **Baylor Whitehead**

Abstract:

Modern vehicles contain many Electronic Control Units (ECUs) that communicate through CAN. While CAN enables efficient data communication, it lacks built in authentication and encryption, allowing adversarial actors to inject malicious CAN messages. This limitation has motivated the development of CAN intrusion detection systems (IDS). However, deploying IDS across a vehicle lineup requires collecting large labeled datasets and retraining models, increasing development cost and limiting scalability.

This thesis investigates the use of transfer learning with LSTM-based deep neural networks to reduce retraining cost while maintaining model detection performance. A baseline LSTM model is trained using CAN data from a base vehicle configuration and then adapted via transfer learning on an expanded CAN dataset while requiring less vehicle specific data. Performance is evaluated under combined binary classifications and compared against the base model. Experimental results demonstrate that transfer learning reduces required training data by 75% while improving detection performance. The transfer model achieves an F1-score of 0.99997, maintains the baseline model F1-score of 0.99903 despite requiring substantially less vehicle specific data. These results indicate that transfer learning enables a cost-effective, scalable deployment of CAN IDS across vehicle variants without full retraining.

Date: Wednesday, April 22nd, 2026

Time: 10:00 AM – 12:00 PM

Location: 14-238b

Committee: Dr. DeBruhl, Dr. Beard, Dr. Pantoja

