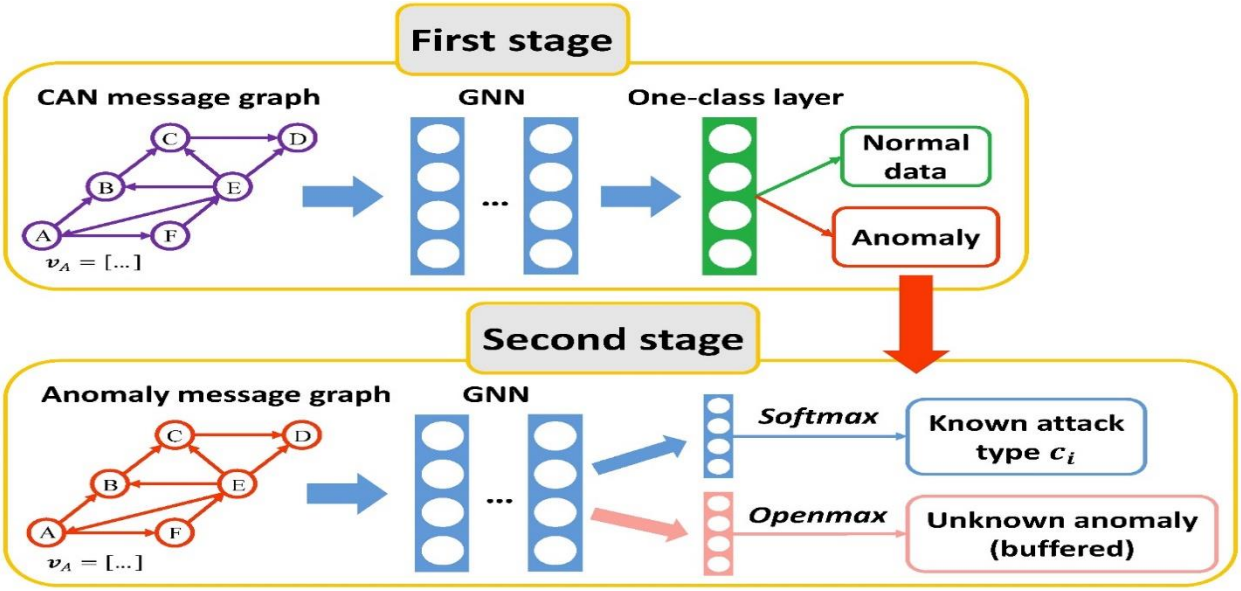
Vehicle Controller Area Network (CAN) Bus With Improved Real-Time Anomaly Detection

22-014

Graph Neural Network (GNN) Machine Learning Detects CAN Bus Message Attacks in Real Time

This technology protects an automobile's main communication system, the CAN bus, from being hacked. The CAN bus controller supervises component electronic control units (ECUs) including the engine, air bags, brake actuator, GPS, and more recently, the Vehicle to Everything (V2X) Connectivity Control Unit (CCU). The V2X CCU permits data exchange between vehicles and is a key element to future driving assist systems and autonomous driving. However, the CAN bus protocol has no mechanism to prevent an operations compromise via message attacks. Some examples of message attacks include Denial of Service (DoS), suspension of normal messages, falsified data content, and forged messages. Intrusion Detection Systems (IDS) have been implemented to try and stop the forged messages, but that is not enough. The computational complexity of message processing and resulting intrusion detection delay makes the CAN bus still vulnerable to compromise. Operational safety is put at extreme risk.

Researchers at George Mason have invented a real-time CAN bus anomaly detection system. This detection system employs a two-stage Graph Neural Network (GNN) based classifier cascade. The cascade from a first stage to a second stage allows the classifier to train and build an improved IDS using machine learning. The first stage has a functionality similar to existing IDS's. The CAN message graph is sorted by the GNN into an Anomaly Message Graph (AMG) of "Normal" and "Anomaly" data. In the second stage, the AMG is sorted by the GNN into a Softmax layer and an Openmax layer. The Softmax layer processes known attack type messages. It has the same number of nodes as an output layer of the AMG. The Openmax layer is a Softmax layer substitute for "unknown unknowns." This is how the GNN uses machine learning to enable real-time anomaly detection of all vehicle CAN bus message attacks.



For More Information contact:
George Mason University, Office of Technology Transfer
703-993-8933 ott@gmu.edu https://ott.gmu.edu/