Omar

Intro

A modern vehicle can have more than 80 electric control units (ECU) continuously

communicating via the CAN bus.

CAN is a serial communication protocol designed to regulate networks of old basic

automotive.

So, with the rise of autonomous technologies, it has become vulnerable to security breaches via

any access points.

Aya

Problem Statement

Developing compact reactive deep learning-based Intrusion Detection System (IDS) has been a

crucial goal in the industry.

They require high computational resources, preventing them from operating on embedded

electronics, in real time.

Scope

So how have we approached this?

We have developed a compressed and accelerated deep learning based IDS, deployed it on a

microcontroller.

We integrate the microcontroller into the CAN bus to monitor it and detect any deviant activity in

real time while keeping its performance intact.

Mostafa

During Pre-processing we merged both attack free and attack datasets while labeling the unlabeled data to identify it, reduce dimensionality by extracting most features and applied encoding methods to suit the input format.

During Processing Data is fed to the model to distinguish the Packets sent to CAN, generalization tested with validation dataset, model is optimized by adjusting the hyper-parameters and evaluated by feeding unseen data.

Pretrained model is optimized to compress and accelerate the model to achieve optimal computational and memory requirements of the Microcontroller

“Show graph” =>as the graph depicts, the model stream packet through CAN, preprocessing receives the packet before classifying its benign or malicious packet, if it’s an attack its discarded, saved in log file.

Impact

Socially: After deployment of model on MCU it will not only increase security level of cars but also increase safety rate of drivers and passengers.

Industrially: Safety of goods will increase which will spare the shipping company compensation fees

Omar

Our IDS has similar counterparts in the field which made us aim to be different and achieve more, as we were able after several tests to create a compressed, accelerated and small-sized model with high accuracy, real-time detection, and low false positive and false negative rates which made our model the 1st of its type in the industry. Our problem that we focused on was getting our IDS to a state ready for the ECU that exist in CAN bus.

We used LSTM a very prominent deep learning network that got a great reputation in the machine learning field. We used Raspberry Pi 4 to act as our microcontroller **maintaining** the IDS **whilst** utilizing TensorFlow Lite API to compress and Accelerate the model

Marc

As the image shows, this is our hardware representation composed of two main elements Bread board and Microcontroller , with the Bread Board representing the CAN BUS inside the car. Here u can see the MCP chips and the wiring connected to our Microcontroller we used Raspberry pi 4. The 4 Leds are connected from the CAN to the Raspberry pi to light up on upon each packet received either a benign packet or one of the 3 attacks we are detecting. As with accuracy over 90% upon detection of each packet received .

We are seeking to complete the simulation of the entire script on the Raspberry Pi as it is one of our main targets.