CAN Bus Intrusion Detection System For Connected Vehicles

Team Members: Amanuel Kidanu, Lia Chiflemariam, Luke Francis, Walid Jami

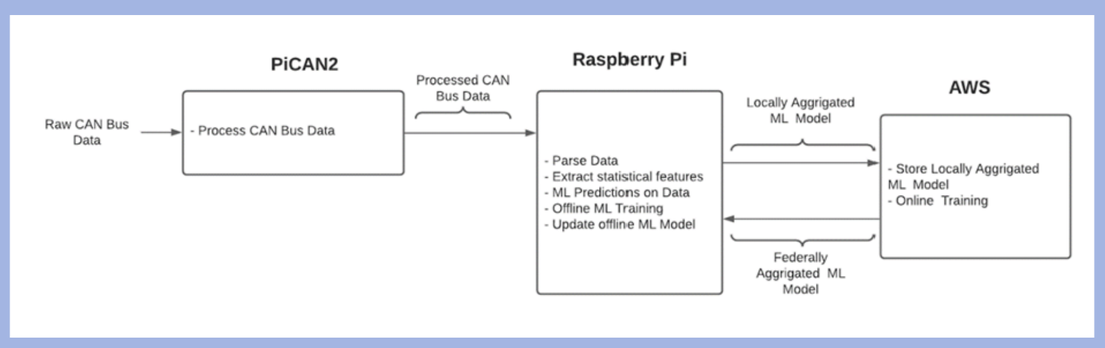
Faculty Supervisor: Dr. Kai Zeng

I. Abstract

The Controller Area Network (CAN) bus is the standard that connects all of the electronic control units of an automobile. This centralized network is efficient, simple, and low-cost; however, it was not created with security in mind. CAN bus messages require neither authentication nor encryption, which can lead to the detection of sensitive user information and the manipulation of vehicle operation. We have designed and built a CAN Bus intrusion detection system using a small-scale PiCAN 2, Raspberry Pi, and cloud-based service to identify malicious attacks on the CAN bus in real-time.

II. Design

System Architecture



III. Testing

Algorithm

After the retraining of our model was completed, we updated the following attributes of the models: the intercept values, the multiplication of the SVM dual coefficients with their target values, and the support vectors.

$$\boldsymbol{w} = \sum_{\mathrm{SV}} \alpha_n y_n \boldsymbol{z}_n$$

$$b : y_m(\langle \boldsymbol{w}, \boldsymbol{z}_m \rangle + b) = 1$$

(Equation 1 shows the equation of the margin boundary vector represented as the summation of the product of the dual coefficients, target values, and mapped inputs of each support vector)

(Equation 2 shows the intercept equation in relation to the inner product of the boundary vector and each input)

Sample of retraining cycles

```
Number of batches: 2
Buffer full...

Loss: 0.32 Accuracy: 0.84
Loss: 0.24 Accuracy: 0.88
Loss: 0.24 Accuracy: 0.88
Loss: 0.16 Accuracy: 0.92
Loss: 0.16 Accuracy: 0.92
Loss: 0.16 Accuracy: 0.92
Loss: 0.16 Accuracy: 0.92
Loss: 0.16 Accuracy: 0.92
Loss: 0.08 Accuracy: 0.96
Loss: 0.08 Accuracy: 0.96
Maximum accuracy: 0.96
Minimum loss: 0.08

Number of batches: 3
Buffer full...

Loss: 0.48 Accuracy: 0.76
Loss: 0.24 Accuracy: 0.88
Loss: 0.24 Accuracy: 0.88
Loss: 0.24 Accuracy: 0.88
Loss: 0.16 Accuracy: 0.92
Loss: 0.16 Accuracy: 0.92
Loss: 0.16 Accuracy: 0.92
Loss: 0.16 Accuracy: 0.92
Loss: 0.08 Accuracy: 0.96
Loss: 0.08 Accuracy: 0.96
Maximum accuracy: 0.96
Minimum loss: 0.08

Number of batches: 4
Buffer full...
```

IV. Results

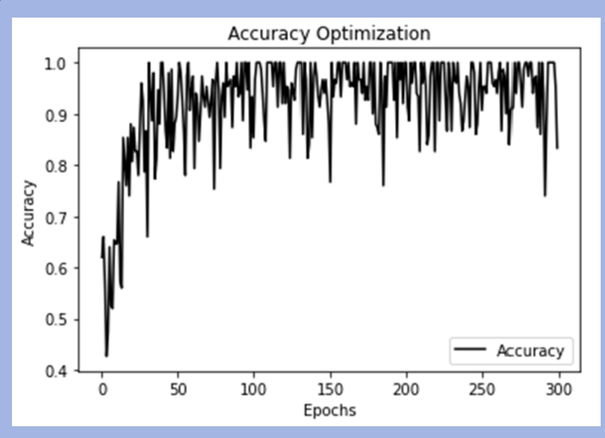


Figure 1. shows the maximum accuracy after a certain number of epochs of training.

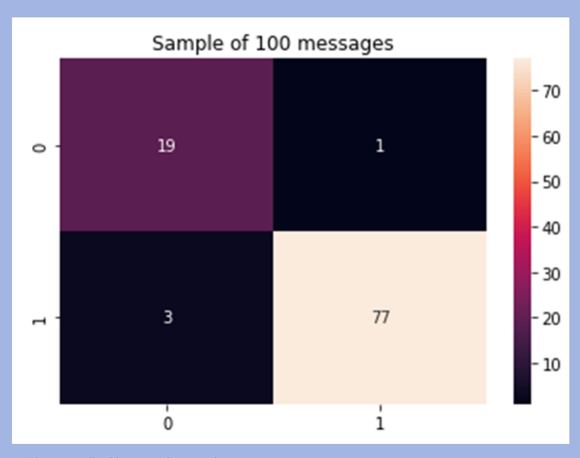


Figure 2. illustrates the confusion matrix of our classifier with 100 sample messages. The top left and bottom right boxes indicate the number of correctly predicted attack and normal messages, and the top right and bottom left boxes indicate the messages incorrectly labeled as attack and normal data. Our classifier had an average accuracy of 96%, which is consistent with the confusion matrix distribution.

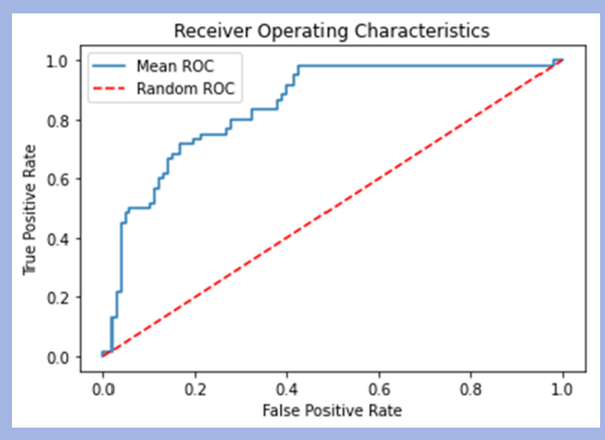
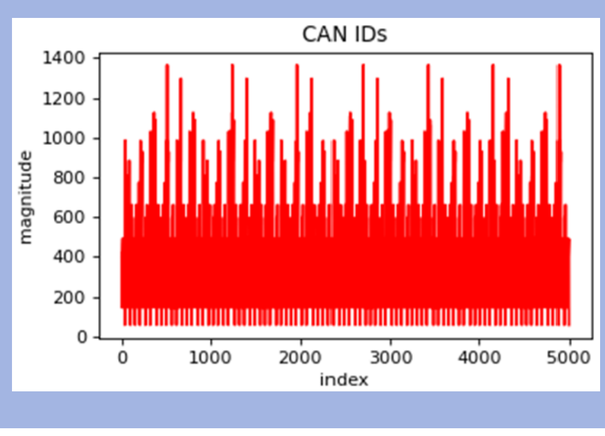


Figure 3. shows the Receiver Operation Characteristics (ROC) curve. This graph compares the false positive rate with the true positive rate (the number of messages incorrectly classified as normal/malicious vs. those that are correctly classified as normally/malicious). Ideally, the graph should have a straight line at the true positive rate of 1.0 regardless of the false positive rate value.



V. Conclusion

Our federated learning system successfully achieved a minimum offline accuracy of 96% and performs equally against all variations of attack injections. Federated learning provides a robust solution to the vulnerabilities of the interactions within a large and public network of users and increases the potential for a more secure vehicle system in the future.

VI. The Team

Team members (L to R):
Lia Chiflemariam,
Luke Francis,
Amanuel Kidanu,
& Walid Jami