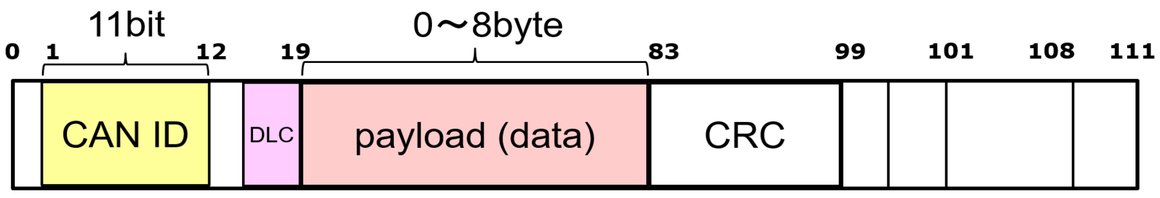
Long Short-Term Memory-based Intrusion Detection System for In-Vehicle Controller Area Network Bus

Md Delwar Hossain
Nara Institute of Science and Technology
E-Mail: hossain.md_delwar.hi5@is.naist.jp

Background & Motivation

The Controller Area Network (CAN) bus system works inside connected cars as a central system for communication between electronic control units (ECUs)



CAN message format (11bit mode, DLC=8)

Fig. 1: CAN Message Format

Security Issues of the CAN message System:

- ❑ CAN does not support an authentication mechanism.
- ❑ CAN messages are broadcast without basic security features.
- ❑ CAN Bus system does not support any encryption-decryption algorithms.

Contributions

- ❑ We develop CAN system attacks (DoS, fuzzing, spoofing) datasets by using the CAN messages of a real car.
- ❑ To the best of our knowledge, we are the first to propose an efficient LSTM-based IDS for in-vehicle CAN bus systems for well-known network attacks: DoS, Fuzzing and Spoofing.
- ❑ We introduce how to select the best hyper-parameter values to develop effective CAN bus IDS based on LSTM.

LSTM-based NIDS

We used the **categorical_crossentropy** as the loss function. The **Nadam** optimizer was applied with a learning rate of 0.0001, and the rest of the parameters kept their default values and **softmax** was used as an activation function output

Fig. 4 shows the flowchart of our proposed IDS. Fig. 5 schematizes the deep neural network model wherein we can input the CAN bus data into the input layer and, after processing the classifier, it will provide the output as a benign or attack class.

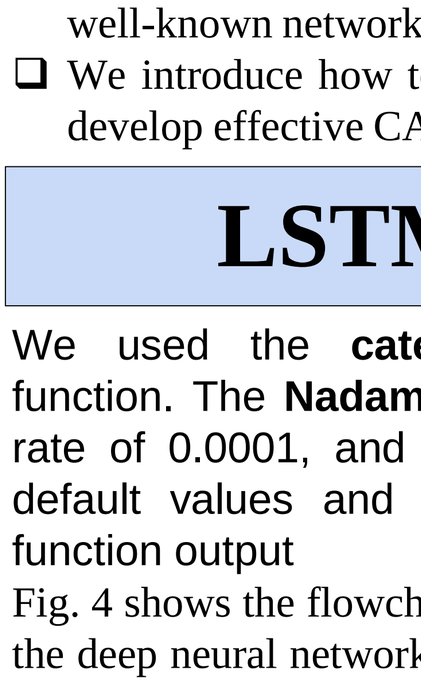


Fig. 4: IDS FlowChart

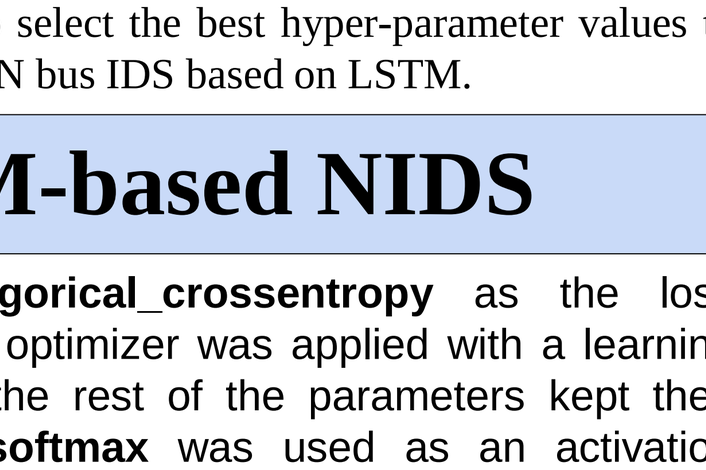


Fig. 5: DNN IDS Architecture

Attack Scenarios

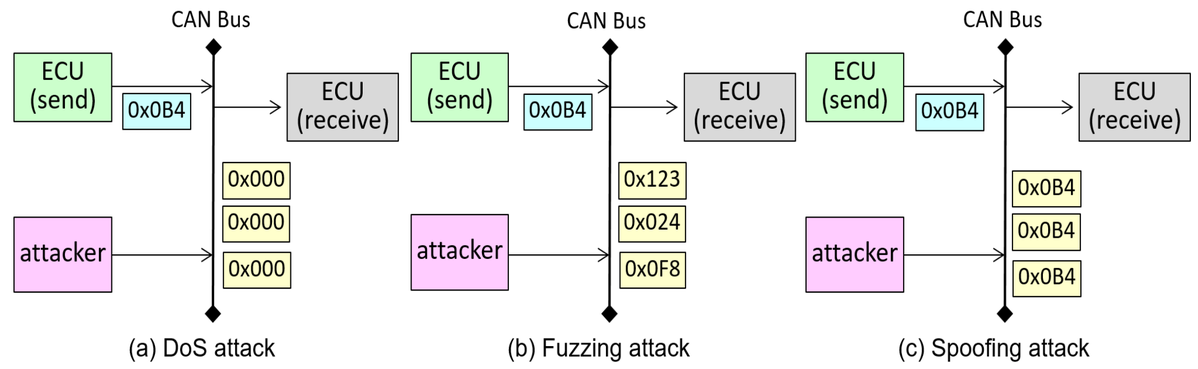


Fig. 2: Attack Scenarios

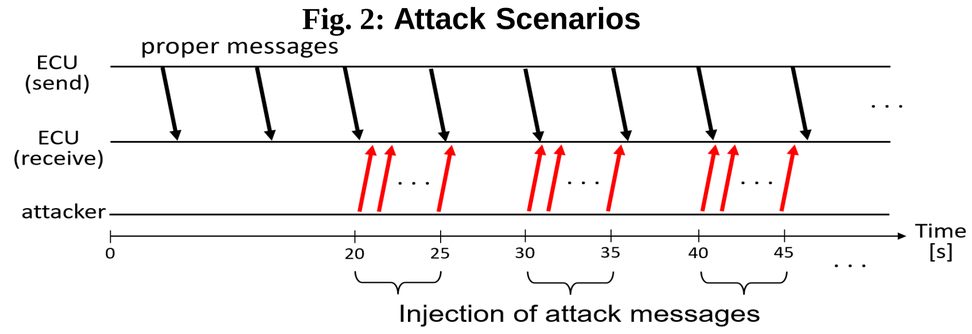


Fig. 3: Injection of Messages

We experiment mainly with three types of attacks in this paper: **Denial of Service (DoS), Fuzzing, and Spoofing**.

DoS Attack: During a DoS attack, the CAN bus system is flooded with messages; thus, the ECU's regular communication triggers an interruption and the CAN network become unavailable to legitimate users.

Fuzzing Attack: During this attack, an attacker randomly injects a vast amount of CAN packets with arbitrary data.

Spoofing Attack: In a Spoofing attack, an intruder targets specific CAN IDs to inject modified messages, thus, the ECU gets biased. Consequently, it becomes challenging to identify the legitimate messages, and the system may start to malfunction.

Experiment Results

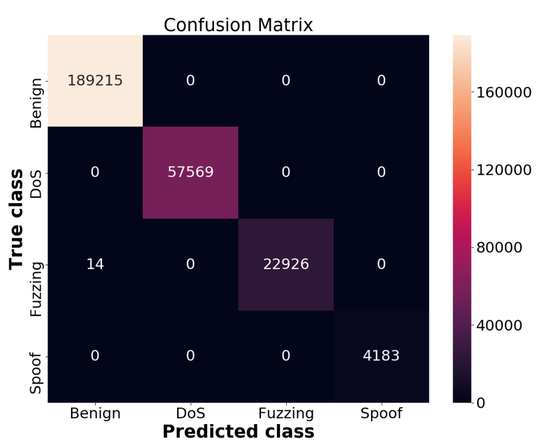


Fig. 6: Confusion Matrix

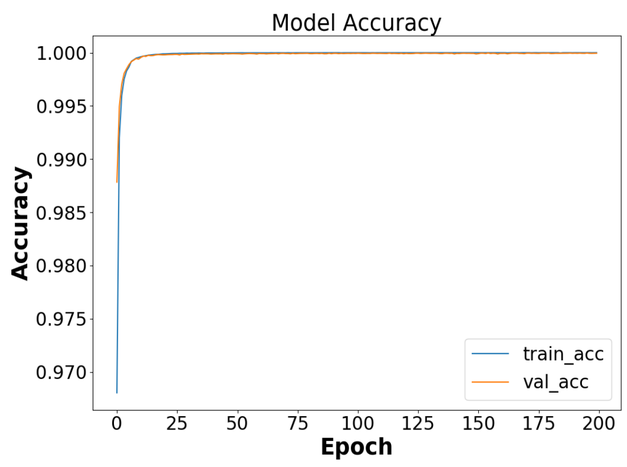


Fig. 7: Model Accuracy

Attack	Accuracy	TPR	TNR	FPR	FNR	AUC
DoS	100%	1.00	1.00	0.00	0.00	1.00
Fuzzing	99.9802%	0.9993	1.00	0.00002	0.0007	1.00
Spoofing	100%	1.00	1.00	0.00	0.00	1.00

Fig. 8: Binary Classification Result

LAYER-WISE MULTICLASS CLASSIFICATION RESULTS (WGT AVG)

Layer	Accuracy	TPR	TNR	FPR	FNR
L1	**99.9949%**	0.9998	1.0000	0.00004	0.00015
L2	99.9883%	0.9997	0.9999	0.0001	0.0003
L3	99.9781%	0.9993	0.9998	0.0002	0.0007
L4	99.9872%	0.9996	0.9999	0.0001	0.0004
L5	99.9887%	0.9997	0.9999	0.0001	0.0003

Fig. 9: LSTM Layer-wise Classification Result

https://iplab.naist.jp/

iplab Laboratory for Cyber Resilience