Annotated Bibliography

Phineas Giegengack

F. Amato, L. Coppolino, F. Mercaldo, F. Moscato, R. Nardone and A. Santone, "CAN-Bus Attack Detection With Deep Learning," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 8, pp. 5081-5090, Aug. 2021, doi: 10.1109/TITS.2020.3046974.

- High-level description of CAN protocol, CAN packet content, deep learning and statistical methods (Neural Network, Multi-layer perceptron).
- Considers 4 types of CAN bus attacks: Denial of service (DOS), fuzzing, drive gear spoofing, and RPM gauge spoofing.
- Machine learning used to classify CAN messages which are labeled as either 'normal' or one of the four attack types
    - Neural net achieved high precision and recall for all types of attacks
    - MLP was challenged by DOS and fuzzing attacks but adding additional layers allowed it to outperform neural net
- Shows promise for using machine learning to detect CAN bus intrusion, but I suspect their results would not apply to a real-time/real world application.
    - Model does not consider context of each CAN bus message (what message precedes a given message could reveal an attack)
    - Overfitting for spoofing attacks in this dataset (achieved precision and recall of 1.0 for both spoofing attacks which doesn't make sense)

Ma, Haoyu, Cao, Jianqiu, Mi, Bo, Huang, Darong, Liu, Yang, Li, Shaoqian, A GRU-Based Lightweight System for CAN Intrusion Detection in Real Time, Security and Communication Networks, 2022, 5827056, 11 pages, 2022. https://doi.org/10.1155/2022/5827056

- Proposes a system architecture for deploying, training, and updating CAN intrusion detection models over-the-air
- Develops a feature-extraction algorithm for CAN bus messages
- Develops a GRU-based neural network that is lightweight enough to be deployed on embedded hardware
- Feature extraction: uses CAN ID, Data length code, data payload and timestamp
- Trained on a server, ran on Nvidia Jetson
- Hyperparameters are given for each model they tried (could be handy)

- Nvidia Jetson is a fairly low-cost hardware platform (~150$) but I may seek something cheaper/less computational power which will likely yield worse model performance.

J. Guidry, F. Sohrab, R. Gottumukkala, S. Katragadda and M. Gabbouj, "One-Class Classification for Intrusion Detection on Vehicular Networks," 2023 IEEE Symposium Series on Computational Intelligence (SSCI), Mexico City, Mexico, 2023, pp. 1176-1182, doi: 10.1109/SSCI52147.2023.10371899. keywords: {Support vector machine classification;Intrusion detection;Machine learning;Data models;Computer crime;Computational intelligence;Cyber Security;Vehicular Security;One-Class Classification},

- Support Vector Machine (SVM) used to be able to train only on nominal CAN bus data and detect scenarios that fall outside of expected behavior
- Researchers tried numerous state-of-the-art SVM methods to detect CAN bus intrusions
- Collected real CAN bus data from Nissan Leaf and Chevy Volt
- Did not run on embedded hardware
- Researchers acknowledged that the features used were trivial, and better performance may have been achieved with more consideration as to which features of the messages were most descriptive

C. Chupong, N. Junhuathon, K. Kitwattana, T. Muankhaw, N. Ha-Upala and M. Nawong, "Intrusion Detection in CAN Bus using the Entropy of Data and One-class Classification," 2024 International Conference on Power, Energy and Innovations (ICPEI), Nakhon Ratchasima, Thailand, 2024, pp. 157-160, doi: 10.1109/ICPEI61831.2024.10748816. keywords: {Support vector machines;Technological innovation;Accuracy;Intrusion detection;Entropy;Anomaly detection;Testing;CAN bus;intrusion detection;anomaly detection;entropy of data;One-Class SVM},

- Uses a one-class SVM to detect anomalies in CAN bus behavior
- Features include timestamp and entropy, a measure of the randomness of each message
- Feature vector size is reduced by this method, and performance is still generally good, although on a limited data set and not run on real embedded hardware/real time

L. Liang *et al.*, "Intrusion Detection Model for In-vehicle CAN Bus Based on TPE-LightGBM Algorithm," *2025 IEEE 34th Wireless and Optical Communications Conference (WOCC)*, Taipa, Macao, 2025, pp. 419-423, doi: 10.1109/WOCC63563.2025.11082193.

- Most recent (2025) paper on this subject
- Uses Gradient boost model to develop a lightweight detection of CAN bus intrusion
- Includes a nice mathematical description of LightGBM
- Feature extraction focuses on CAN IDs, IDs of previous CAN messages, and time intervals between previous message, and time interval between previous message with same ID