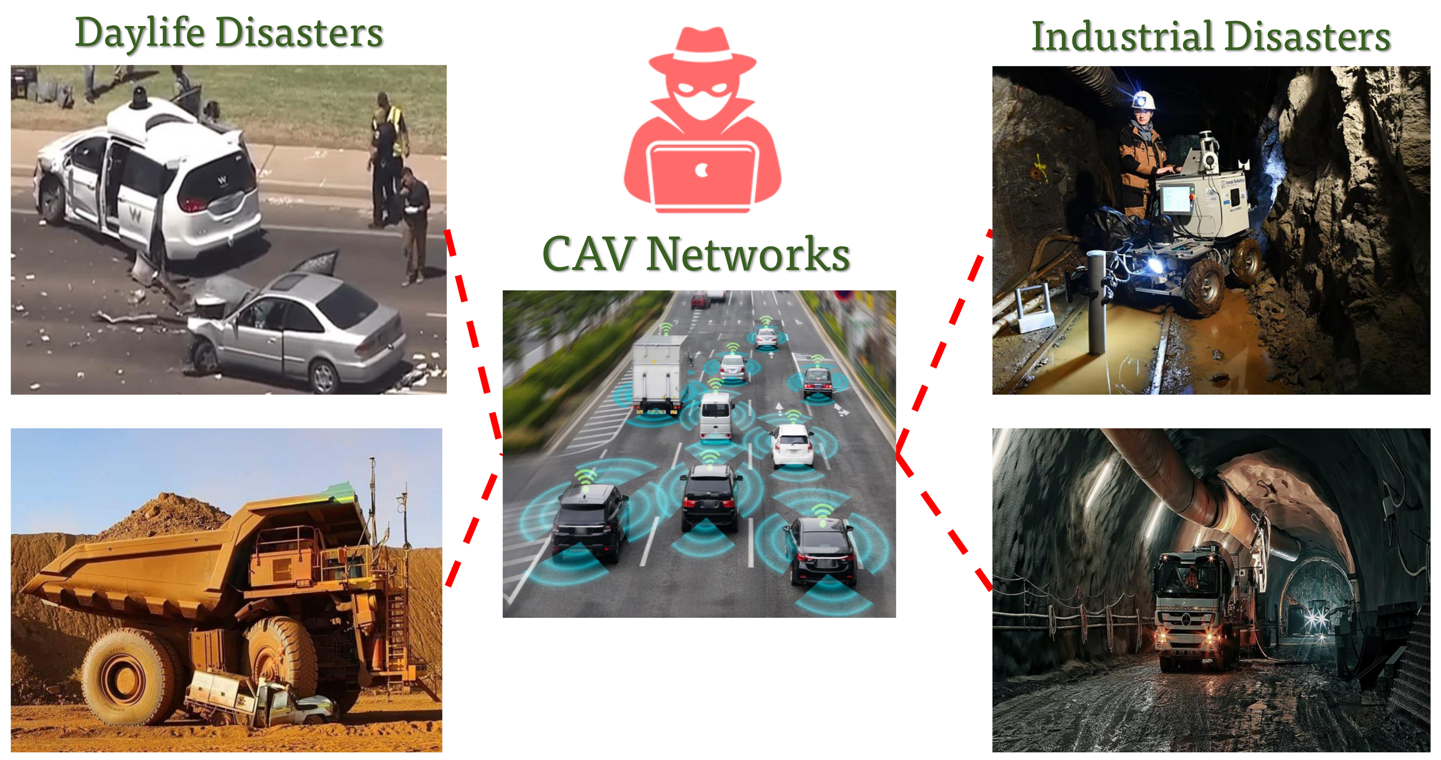
CAV-AD: A Robust Framework For Detection of Anomalous Data and Malicious Sensors in Connected and Autonomous Vehicle Networks

PhD Student: Md Sazedur Rahman
Email:mrvfw@mst.edu

Postdoc: Mohamed Elmahallawy
Email: meqxk@mst.edu

Faculty Advisor: Sanjay Madria
Email: madrias@mst.ed

Motivation



Objectives

1. Avoiding accidents in autonomous vehicle due to sensor failure or cyber attack.
2. Detecting potential anomaly from sensor data in autonomous vehicles.
3. Detection of malicious sensors to help formulating preventive measures.
4. Increasing anomaly detection (AD) accuracy.

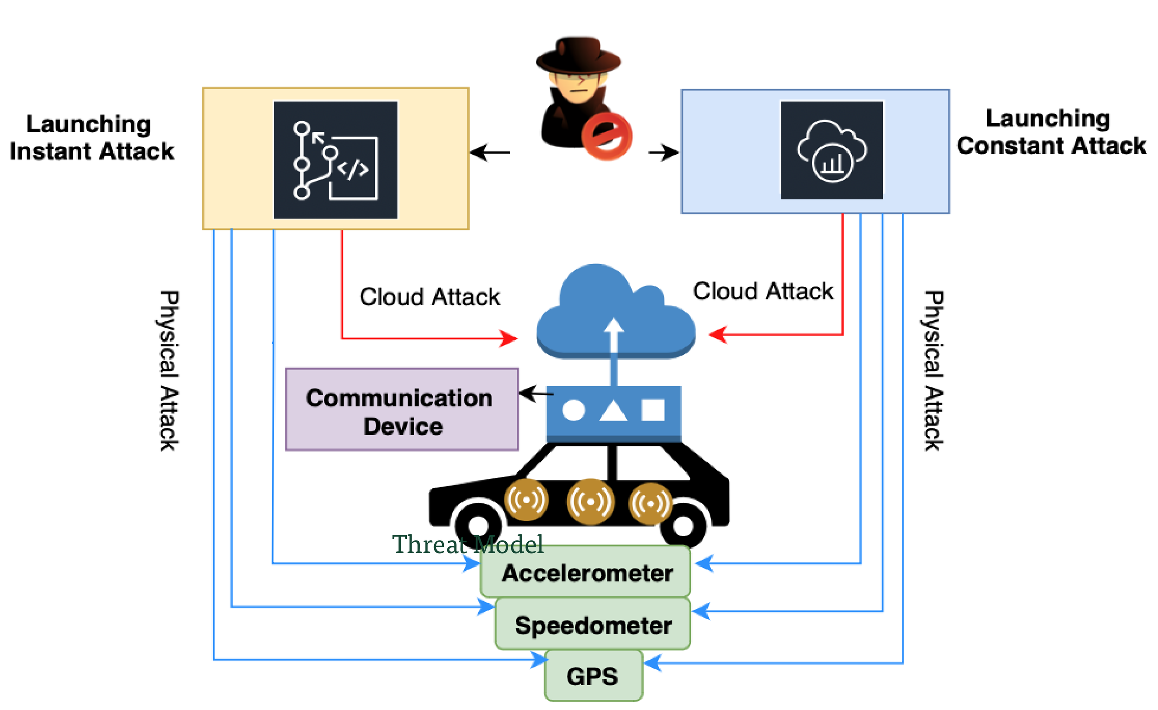
Challenges:

1. Identify the specific sensor being attacked.
2. Detect multiple anomalies in specific sensors with high accuracy or F1 score.

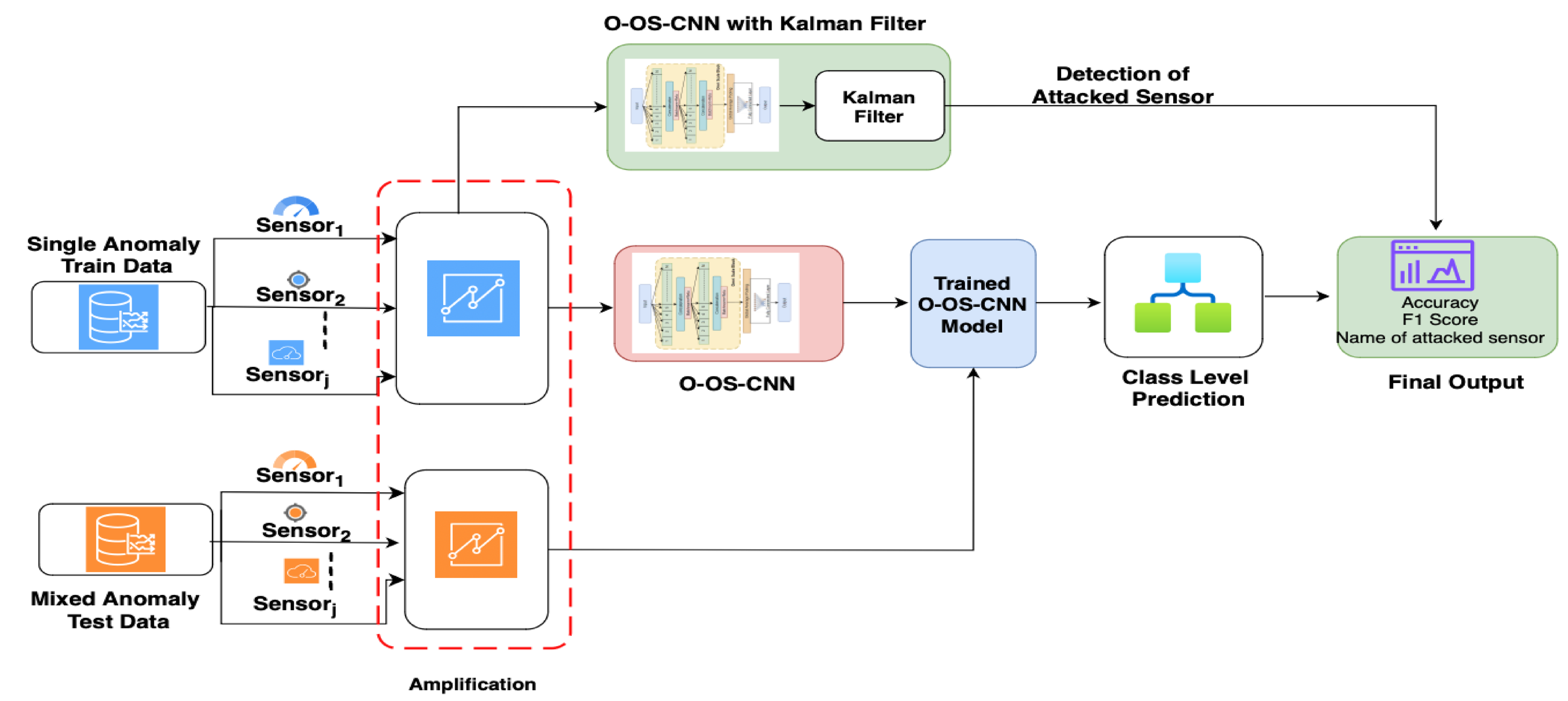
Anomaly Detection

1. AD is the identification of patterns or data points that deviate from normal behavior within a dataset.
2. AD in Connected and Autonomous Vehicles (CAVs) involves identifying abnormal behavior or events within the vehicle's data streams, such as sensor readings, communication signals, or system diagnostics, to ensure safety, security, and efficient operation.

Threat Model



CAV -AD Framework



Phase I : Amplification

- It enhances the amplitude of potential data from train and test set.
- Makes the model enable to extract anomaly features.

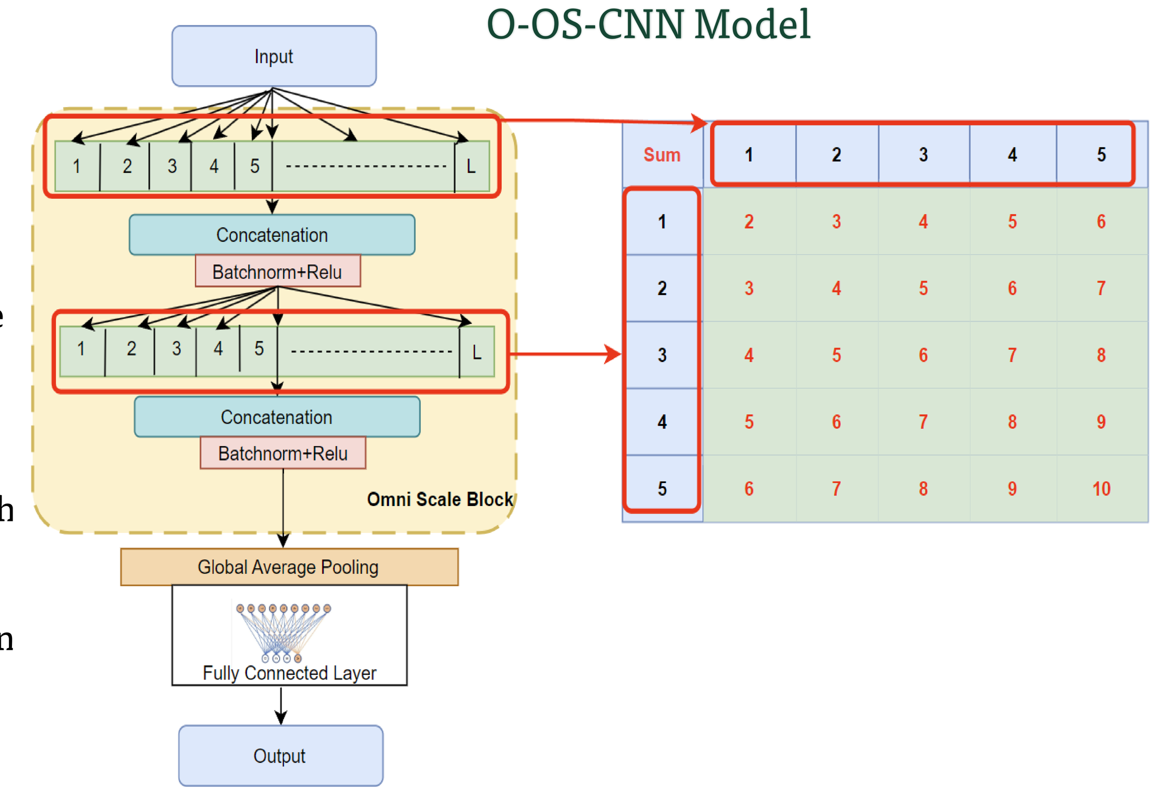
Phase II: O-OS-CNN Model

- Explore every potential kernel size across the entire Input length.
- Enhances the range of feature extraction.

Phase III :Detection of Malicious Sensors

- Dynamically applies Kalman filter (KF) to each sensor.
- Predicts the next normal reading.
- Absolute Difference between incoming readin and predicted reading is measured.

O-OS-CNN Model



Experiments

Experimental Setup:

- We consider a train set having two real life anomaly –instant, constant
- We consider test set having four anomalies- instant, constant, gradual drift, bias.
- We evaluate the CAV-AD framework on SPMD dataset [1].
- CAV-AD predicts the instant and constant anomaly.
- We evaluate the performance using Accuracy, F1 score.
- We compare with two state-of-the-art methods [2][3].

Experimental Results:

(1) Anomaly Detection

- Instant Anomaly

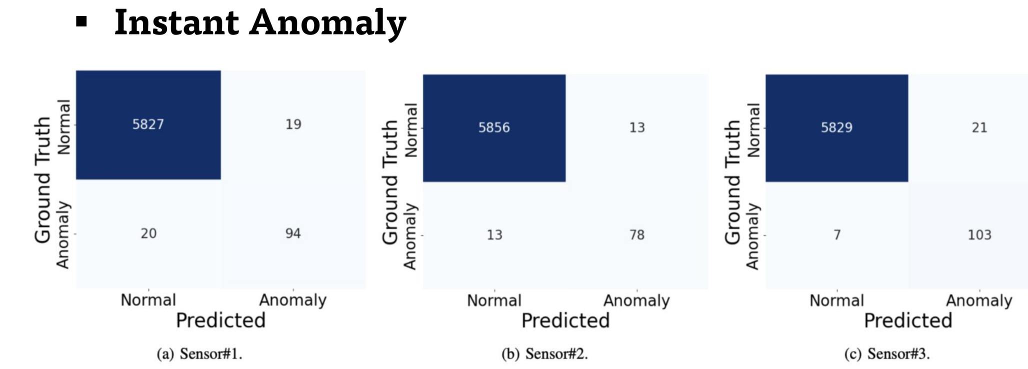
Anomaly	Sensors	Acc.	Prec.	F1
Instant	1	99.3	81.3	83.4
	2	99.5	85.7	88.7
	3	99.5	83.0	88.0

- Constant Anomaly

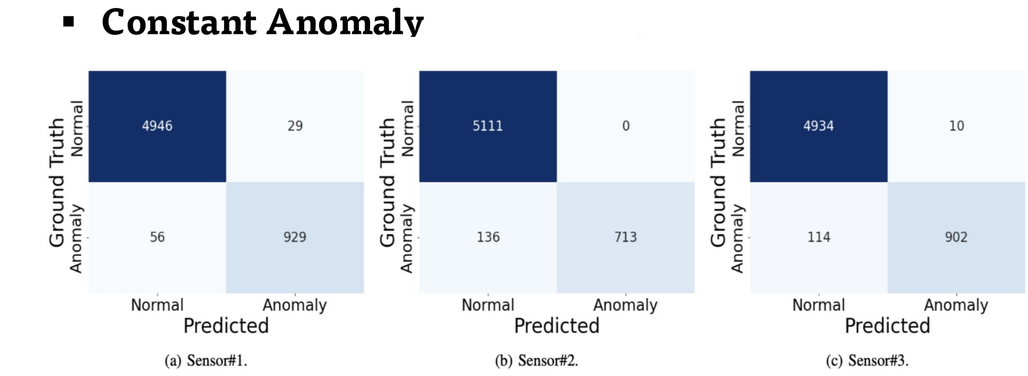
Anomaly	Sensors	Acc.	Prec.	F1
Constant	1	98.5	96.9	95.6
	2	97.7	99.9	91.2
	3	97.9	98.9	93.5

(2) Confusion Matrix:

- Instant Anomaly

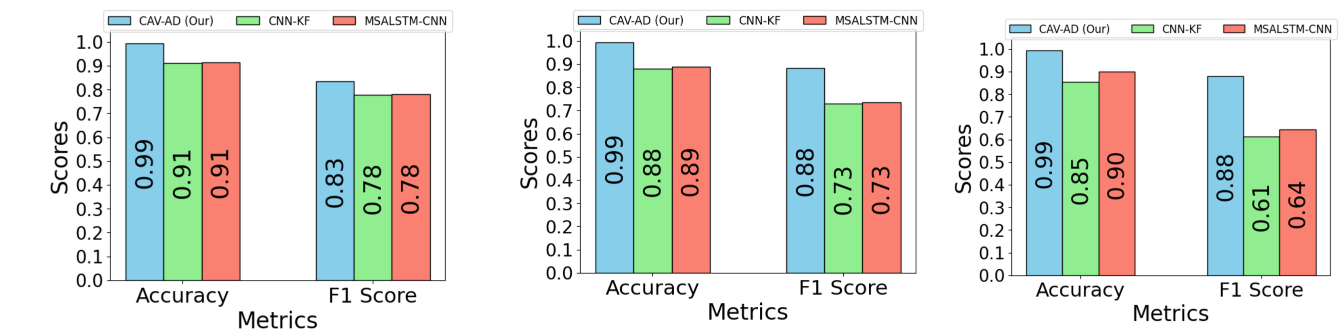


- Constant Anomaly

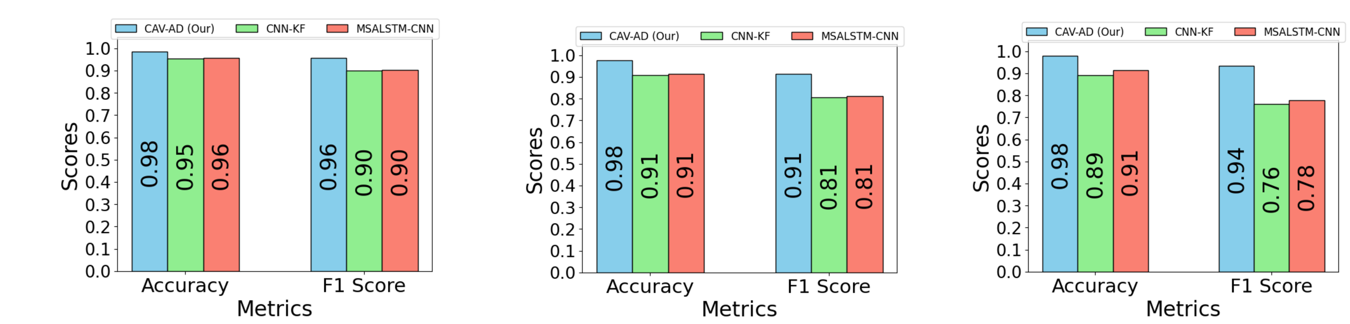


(3) Comparison with state-of-the-art (SPMD dataset)

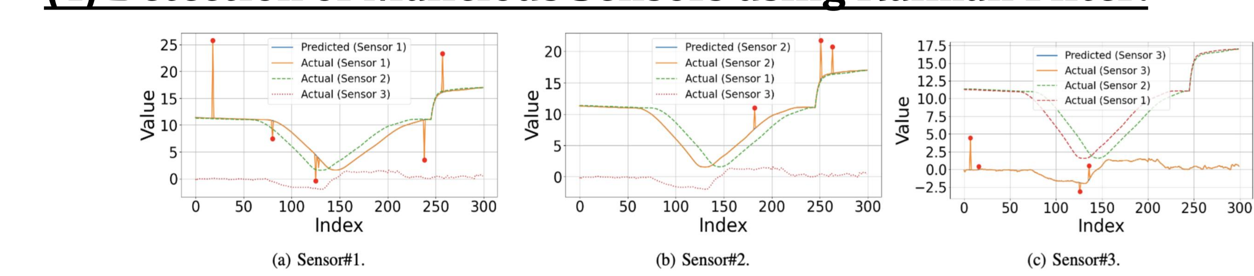
- Instant Anomaly : CAV-AD vs CNN-KF vs MSALSTM-CNN



- Constant Anomaly : CAV-AD vs CNN-KF vs MSALSTM-CNN

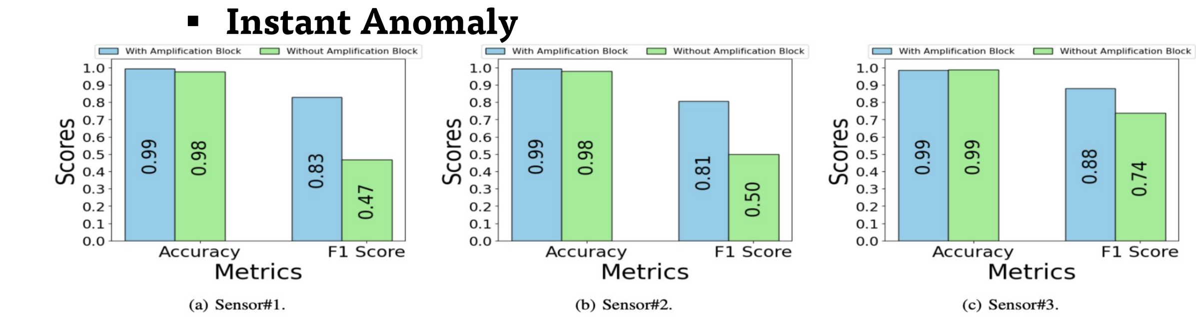


(4) Detection of Malicious Sensors using Kalman Filter:

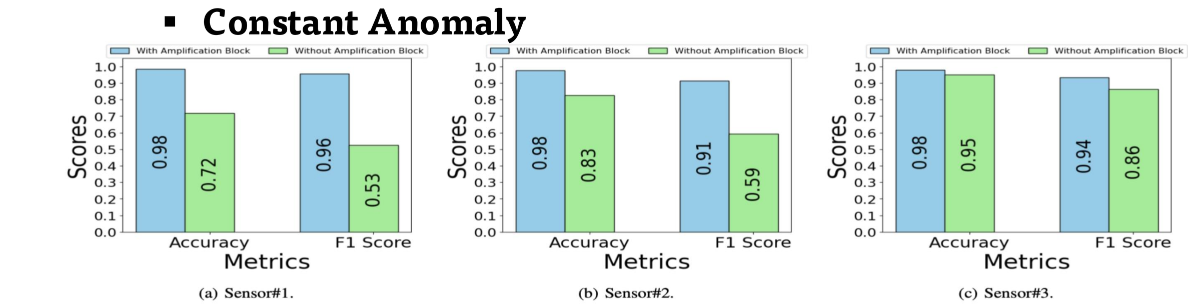


(5) Ablation Study: Effect of Amplification block

- Instant Anomaly



- Constant Anomaly



Conclusion and Future Work

- Robust Framework CAV-AD
- O-OS-CNN Model to capture features using every possible kernel sizes.
- Detection of malicious sensors using KF.
- Accuracy of 90% and F1 score of 96%

- Considering more types of anomaly
- Detecting anomaly type.
- More complex vehicle environments

References

[1] D. Bezzina and J. Sayer, "Safety pilot model deployment: Test conductor team report," Report No. DOT HS, vol. 812, no. 171, p. 18, 2014.

[2] Van Wyk, Franco, et al. "Real-time sensor anomaly detection and identification in automated vehicles." *IEEE Transactions on Intelligent Transportation Systems* 21.3 (2019): 1264-1276.

[3] Javed, Abdul Rehman, et al. "Anomaly detection in automated vehicles using multistage attention-based convolutional neural network." *IEEE Transactions on Intelligent Transportation Systems* 22.7 (2020): 4291-4300. [4] Rahamn, Md Sazedur, et al. "CAV-AD: A Robust Framework For Detection of Anomalous Data and Malicious Sensors in Connected and Autonomous Vehicle Networks ." IEEE International Conference on Mobile Ad-Hoc and Smart Systems (Submitted).

Computer Science