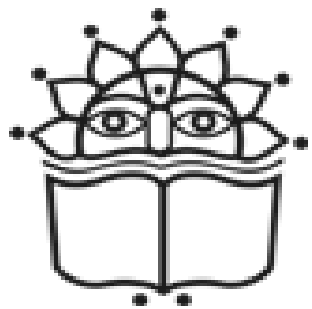
Cyber Attack Detection of Electric Vehicles using Physics Guided Machine Learning

Devrat Yashraj Deepak

yashraj.devrat.aids.2020@vpkbiet.org

Guided by

Prof. Digambar M. Padulkar



Department of Artificial Intelligence & Data Science
Vidya Pratishthan's Kamalnayan Bajaj Institute of Engineering and Technology
Vidyanagari, Baramati-413133

Content

Introduction

New approach for detecting cyberattacks in EVs

- Need for detecting attacks in EVs so designed a new algorithm .
- General algorithm cannot detect attacks on EVs with satisfied output.
- Attackers gain illegle access on electric drive system we can detect signal hampering at early stage and prevent it.

Introduction to Cyberattacks in EVs

- EVs have been the target of a wide range of cyberattacks. Attackers target particular modules and control applications located within the environment of the control system.
- In V2V communication sensor and actuator transfer information to other ECUs, resulting in the development of a very intricate network of hardware and software sub-modules.

Motivation

- Motivation of this project was from the issues electrical engineers were facing during investigating the vehicle problems.
- To protect vehicles from cyberattack use of machine learning technique is required.This technique is efficient which finds fault with high accuracy.
- There are various vehicle network protocols, including Media Oriented Systems Transport, Local Interconnect Network (LIN), FlexRay, and CAN Flexible Data-Rate (CAN FD) (MOST).

Problem Statement

To detect faults in 3 major parts Sensor,Controller, Communication Channels with EMS

Literature Survey

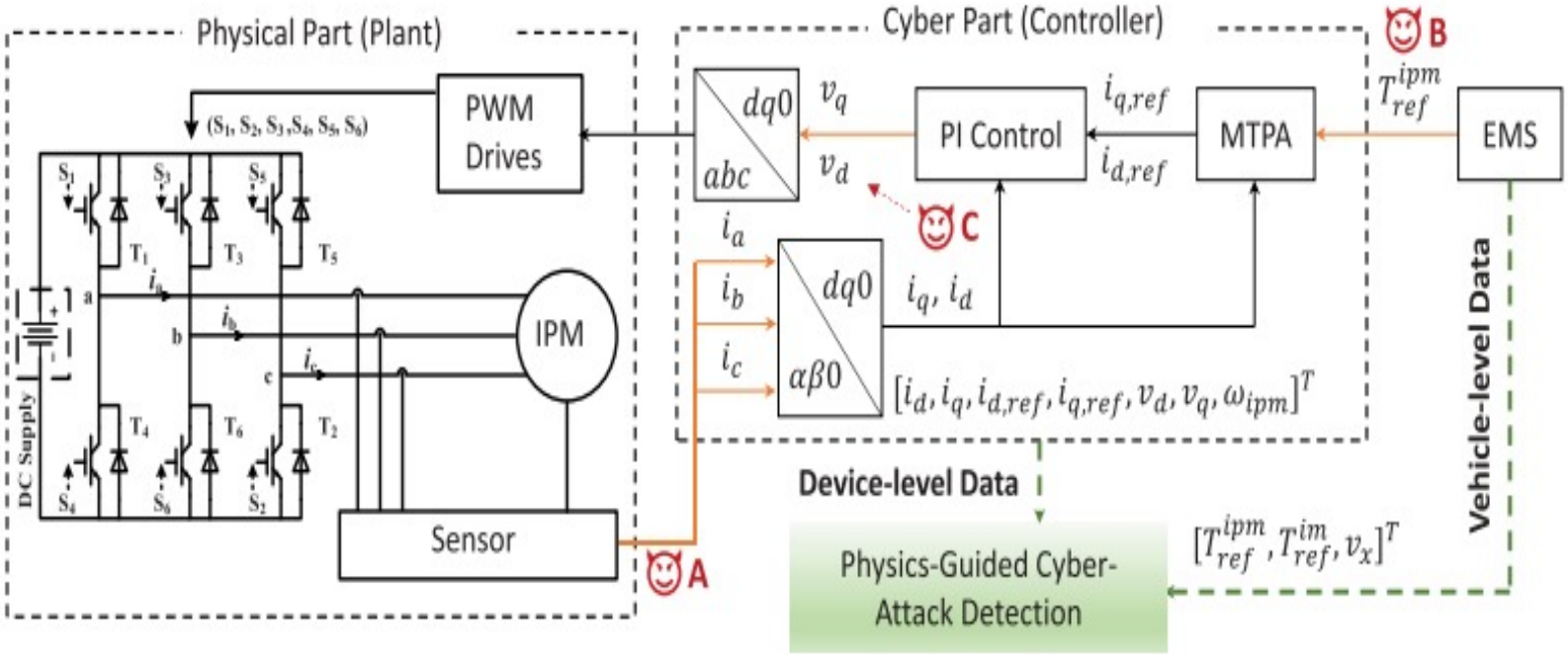
- New type of architecture system presented importance of battery health in EVs and the algorithms for optimizing it.
- Data integrity attacks on ESDs and AGC operation played vital role and caused more impact on power train.
- Analysis of major engine components and elaboration of risk factors associated with it.

Methodology

Techniques used for getting output

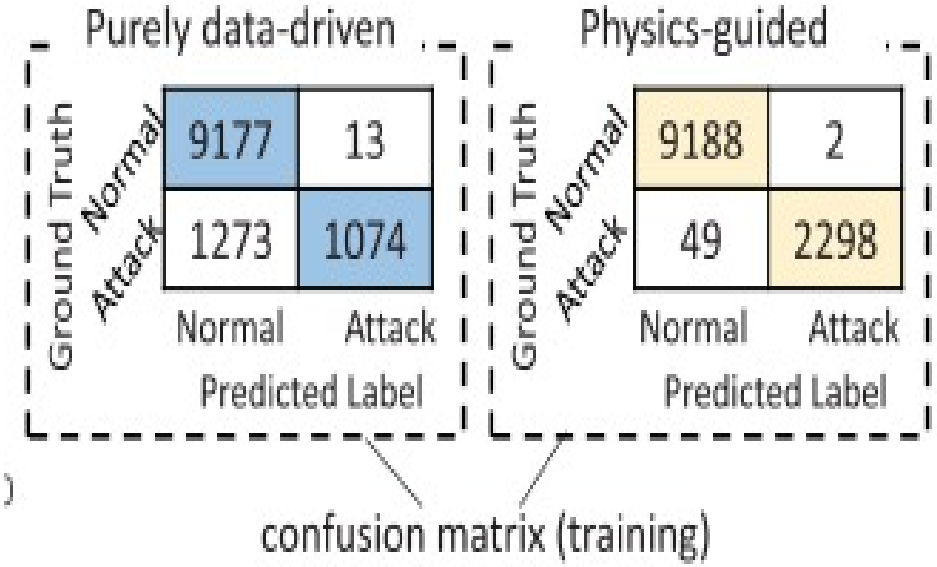
1. SVM is a supervised machine learning algorithm which can be used for classification or regression problems
2. It uses a technique called the kernel trick to transform your data and then based on these transformations it finds an optimal boundary between the possible outputs.
3. Decision Tree The goal of using a Decision Tree is to create a training model that can use to predict the class or value of the target variable by learning simple decision rules inferred from prior data(training data)

System Architecture



Schematic of the IPMSM drive and the signals that are potentially affected by a malicious attacker

Observations/Results



Matrix of Physic guided vs Purely Data Driven Technique

- We have used decision tree (DT), SVM, K-nearest neighbor (KNN), and naive Bayes classifier (NB).
- The results shows that the proposed physics-guided LSTM had achieved the best performance.

Conclusion

With the use of currently available tools and techniques, future study on the security of data and communication in the EV infrastructure can be conducted. The machine algorithm technique proposed can predict attacks at early stage from getting it to severe.

References

[base paper]Lulu Guo , Jin Ye , Senior Member, IEEE, and Bowen Yang , Graduate Student Member, IEEE .
[1] C. Hodge, K. Hauck, S. Gupta, and J. C. Bennett, "Vehicle cybersecurity threats and mitigation approaches," Nat. Renew. Energy Lab.(NREL), Golden, CO, USA, Tech. Rep. NREL/TP-5400-74247, 2019. [Online]. Available: https://www.nrel.gov/docs/fy19osti/74247.pdf .
[2]S. Chakraborty, M. A. Al Faruque, W. Chang, D. Goswami, M. Wolf, and Q. Zhu, "Automotive cyber–physical systems: A tutorial introduction," IEEE Des. Test, vol. 33, no. 4, pp. 92–108, Aug. 2016

References

[3]M. Levi, Y. Allouche, and A. Kontorovich, "Advanced analytics for connected car cybersecurity," in Proc. IEEE 87th Veh. Technol. Conf. (VTC Spring), Jun. 2018, pp. 1–7.
[4]Shao, C. Dong, and L. Dong, "Research on detection and evaluation technology of cybersecurity in intelligent and connected vehicle," in Proc. Int. Conf. Artif. Intell. Adv. Manuf. (AIAM), Oct. 2019,pp. 413–416

[5]Y. Xun, J. Liu, N. Kato, Y. Fang, and Y. Zhang, "Automobile driver fingerprinting: A new machine learning based authentication scheme," IEEE Trans. Ind. Informat., vol. 16, no. 2, pp. 1417–1426, Feb. 2020.

Thank You