Cyber Attack Detection for Electric Vehicles using Physics Guided Machine Learning

A SEMINAR REPORT

submitted to the Savitribai Phule Pune University, Pune
In the partial fulfilment of the requirements
for the award of the degree

BACHELOR OF ENGINEERING
(AI&DS)

BY

Devrat Yashraj Deepak
Roll No: 2237031

Under the guidance of

Prof. Digambar Padulkar
Assistant Professor

DEPARTMENT OF AI&DS
Vidya Pratishthan's Kamalnayan Bajaj Institute of Engineering and Technology,
Vidyanagari Bhigwan Road
Baramati- 413133

2022-23

CERTIFICATE

This is to certify that **Mr Devrat Yashraj Deepak** has successfully submitted his seminar report to the Department of Artificial Intelligence and Data Science, VPKBIET, Baramati,on

"Cyber attack detection for electric vehicles using physics guided machine learning"

during the academic year 2022-2023 in the partial fulfilment towards completion of Third Year of Bachelor of Engineering in Artificial Intelligence & Data Science .

Digambar Padulkar Guide, Dept of AI&DS .	Dr. A. M. Jagtap HOD, Dept of AI&DS .

Dr. R.S.Bichkar
Principal
VPKBIET, Baramati.

Place:Vidya Pratishthan's Kamalnayan Bajaj Institute of Engineering and Technology, Baramati.
Date :29-Sept-2022 ____________________

Acknowledgments

I am feel happy in forwarding this seminar report as an image of sincere efforts. The Successful seminar reflects my work, effort of my guide in giving me good information.

I would like to express my heartiest thanks to my seminar guide **Mr Digambar Padulkar** for his undying support which makes me possible to make this seminar knowledgeable. He not only provided me the literature and guidance to study but also the platform which required for me to prepare best for this seminar.

I am also equally indebted to our seminar coordinator I am also equally indebted to our seminar coordinator **Mrs R.S.Naik** who has been a constant source of inspiration and guiding star in achieving my goal.

I thank **Dr A.M.Jagtap**, Head of Department of AI&DS Engineering and respected Principal **Dr R.S.Bichkar** for supporting and providing all facilities to complete the work. I am thankful to and fortunate enough to get constant encouragement, support and guidance from entire teaching staff of Department of AI&DS engineering which helped me in successfully completing my seminar work.

Devrat Yashraj Deepak

Abstract

Cybersecurity issues are affecting every element of an EV, including battery management, motor drives, braking, and steering, as a result of IoT and connectivity in the in-vehicle network. Potential cyberattacks that could shorten battery life are also assessed. Similar to this, given the intervehicle network of EVs' cybersecurity flaws, cyberattacks on electric drives can significantly affect motor current signature and result in performance degradation. The physical layer-based detection techniques based on hardware and software were deemed preferable for the cybersecurity solution. As networks and intellectualization continue to advance, power electronics systems' cyber-physical security is becoming more and more important.

Modern electric vehicle (EV) powertrain systems, which typically consist of one or more electric drives, are becoming more susceptible to cyberthreats as a result of their connection to external networks in the intelligent traffic environment. Numerous data-driven techniques exist today for addressing security challenges, including support vector machines (SVM), machine learning, deep learning, leverage scores, geometrically built residual filters, and generalised likelihood ratios. First, to build the cyberattack detection, we use vehicle-level signals indicating transitory vehicular states in addition to the device-level signals, current, and voltage in the motor drive. Second, novel data features are proposed for important system performance and vehicle physical properties, using data-driven approach and highly accurate physical power electronics and vehicle models.

Keywords : data integrity attack, electric drives , power electronics, impact analysis, power train system, physics guided Machine Learning.

Contents

List of Figures

Chapter 1

Introduction

1.1 Introduction

Industrial Control Systems (ICS) have been the target of a wide range of cyber attacks, which have shown just how sophisticated the attackers are. The attacks target particular vital control applications located within the environment of the control system. This demonstrates that skilled attackers are well-versed in not just the control and automation computer systems, as well as their weaknesses, but they also have a working knowledge of the physical system's dynamics to ensure maximum impact.The power system Supervisory Control and Data Acquisition (SCADA) systems, are examples ofmodern ICS networks.

In-vehicle network protocol is used to transfer sensor and actuator information to other ECUs, resulting in the development of a very intricate network of hardware and software sub-modules. CAN, CAN Flexible Data-Rate, and other in-vehicle network protocols are among them.

In-vehicle network protocol is used to transfer sensor and actuator information to other ECUs, resulting in the development of a very intricate network of hardware and software sub-modules. There are various in-vehicle network protocols, including Media Oriented Systems Transport, Local Interconnect Network (LIN), FlexRay, and CAN Flexible Data-Rate (CAN FD) (MOST). Among the various procedures described above, Due to their direct connection to infrastructure for battery charging, more centralised control architecture, and increased electrification, automated and connected electric vehicles (EVs) are particularly vulnerable to cyber and physical threats. This is especially true of intelligent transportation systems and automated vehicles that are internet of things (IoT) enabled. While with the rise of EVs and the planned replacement of conventional internal combustion engine cars In order to assess the cyber security concerns associated with microgrids, a Monte-Carlo simulation was used to study assaults on the control systems of solar inverter and energy storage.

Chapter 2

Literature Survey

2.1 New type of architecture system battery health[1]

This paper provides a high level overview of architecture applications such as semiconductor reliability and system level control.Innovating new CPS designed mthodology.

2.2 Data Integrity attack on EDSs

From this paper I get information about various attack on overall performance of EDSs . We will more focus on advance tools and methodology for reflecting accurate relationship between cyber attack and physical response.

2.3 Data Integrity attack on AGC operation

This paper gives information of anomaly detection algorithm was measured in terms of false positive rates.

Table 2.1: Literature Survey

Sr.no	Paper	Technique Used	Advantages	Gaps
1	[1] Lulu Guo,2021	SVM(Support Vector Machine)	understandable margin of dissociation between classes	Algorithm is not suitable for large dataset.
2	[2] Cabell Hodge.,2019	Mitigation for CAV's	Secured communication infrastructure.	This research lays down the framework
3	[3] Samarjit Chakraborty, 2016	Nondominated sorting genetic algorithms	1. It has excellent parallel capabilities	1. Difficult to understand
4	[4] Fei Miao.,2018	Fault detection isolation and reconfiguration (FDIR)	1. Expensive Technique	Algorithm is not suitable for large data sets.
5	[5]Siddharth Sridhar,2014	Statistical Learning Algorithm	Collects data from previous experience	Low accuracy

Chapter 3

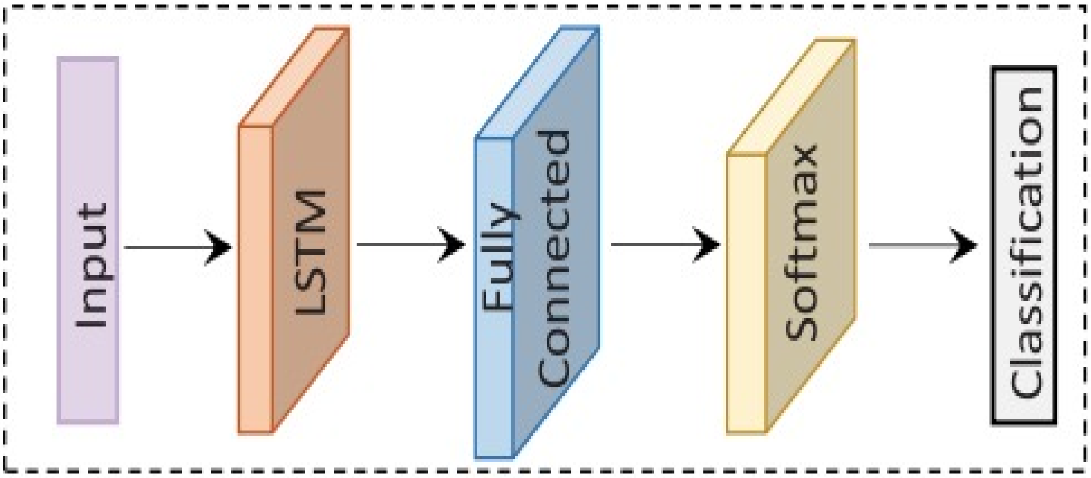
Motivation

1. Motivation of this project was from the issues mechanical engineers were facing during investigating the vehicle problems.
2. To protect vehicles from cyberattack on EVs use of machine learning technique.

   is required
3. This technique is efficient which finds fault with high accuracy.
4. Industrial Communication System are continuously getting captured by the Malacious hackers .So there came a need of providing security to them.

Chapter 4

System Architecture



LSTM Network

Architecture of an LSTM memory cell is illustrated in the figure, It consist of forget, input, and output gates are used to solve the issue of vanishing gradients in a recurrent neural network. Specially, given an input x1 and the previous timestamp output h1 , at each time step, an LSTM first generates a candidate
cell state ct with ht and xt , as ct = tanh(Wch ht1 + Wcx xt), and calculates the forget gate, input gate, and output gate

Accuracy = TP + TN/ TP + TN + FP + FN
where true positive (TP), true negative (TN), false positive (FP), and false negative (FN) denote the number of examples that the actual attack is correctly identified as attack, the actual normal is correctly identified as normal, the actual attack is wrongly identified as normal, and the actual normal is wrongly identified as attack, respectively

Chapter 5

Approaches for Solving the Problem

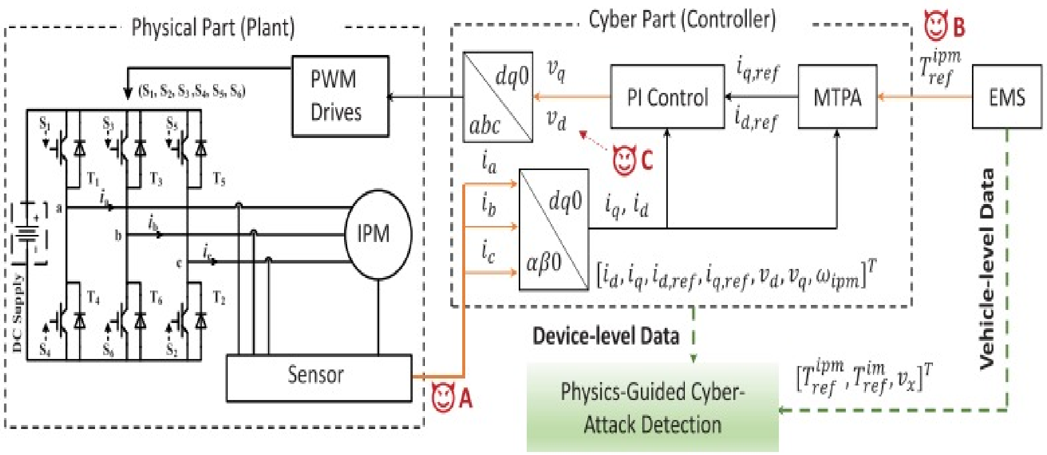


Figure 5.1: Schematic of the IPMSM drive and the signals that are potentially affected by a malicious attacker

The control variable of the PID is the total required torque.As the focus of this article is to identify cyberattacks on the electric drives, the EMS is designed by a simple methodology such that torque makes an equal basis to all machine .It contains of two parts physical and cyber part in which data is sensed from sensory device then the controller goes to hacker to malaciously attack on the vehicles.

Chapter 6

Algorithm

LSTM (Long Short Term Memory) is type of RNN .It is capable of long term dependencies , especially sequence prediction problems. It has gates for regulating the output data . The proposed physics-guided LSTM can deal with varying working conditions. The reason is that physics modeling can effectively extract the vehicle features and, thus, can reflect abnormal circumstances.

Chapter 7

Advantages and Disadvantages

7.1 Advantages

1. It gives ease to detect cyberattacks on electric vehicles in less time.
2. Without damaging any component we know about the malacious attack.

7.2 Disadvantages

1. Frequent attack on vehicles system can cause damage to components.
2. It is not easy task for the attacker if the vehicle system is complex.

Chapter 8

Future Scope

This project has vast scope in future we can add additional features to the program and make it more efficient. In the devolping era of automation industry .The machine algorithm technique proposed can predict attacks at early stage from getting it to severe. Vehicles will be more secured with high security as frequently we check the performance of vehicles it will be safe and protected from external virus attacks. We will concentrate on more modern models to ensure the safety of EVs. With more sophisticated metrics, as well as general guidelines for further EV identification and diagnosis, to represent an actual relationship between cyber attacks and physical response.

Our upcoming effort includes creating defences against coordinated cyberattacks on power system control and attacks that affect how the electricity market operates through AGC. With the use of currently available tools and techniques, future study on the security of data and communication in the EV charging infrastructure can be conducted. It should come as no surprise that such technologies are now utilised to analyse or assess the security of the wider smart grid or a part of it, such as cyber-physical systems. To learn more about related tools, we advise reading the material below. Other than the methods listed in Section V-A that are appropriate for technical study of particular protocols, simulation of the power network or the communication network, or a co-simulation of both, is a frequently used methodology.

Chapter 9

Summary

We have demonstrated, assessed , and explained how effectively a machine learning algorithm guided by physics may identify a cyberattack on electric vehicles. Advanced physic to reflect the fleeting physical qualities of the vehicle,guided features are also employed. In actual implementations, the system is trained offline before being used to detect cyberattacks in real time. Despite the training process's satisfactory detection accuracy, there are still a number of problems that need to be resolved before practical applications can be made.The detection of performance during no network connectivity is one of the issues, particularly during taking into account the changing external driving environment, Data-driven techniques can be conceptualised generally as using trained models to identify unusual system behaviour based on observational data gathered from the system. This strategy is frequently based on the idea that, in ideal conditions, the observation data would be constant with few variations caused by measurement flaws and system noise. Our main motive will be cyber attack detection that can be modified using system and more on detailed physical engine properties of electric vehicles.

Bibliography

[1] Lulu Guo , Jin Ye , Senior Member, IEEE, and Bowen Yang , Graduate Student Member, IEEE

[2] 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

[3] 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

[4] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas, “Coding sensor outputs for injection attacks detection,” in Proc. 53rd IEEE Conf. Decis. Control, Dec. 2014, pp. 5776–5781.

[5]] S. Sridhar and M. Govindarasu, “Model-based attack detection and mitigation for automatic generation control,” IEEE Trans. Smart Grid, vol. 5, no. 2, pp. 580–591, Mar. 2014.