INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 2041-2045

e-ISSN : 2583-1062

Impact Factor: 5.725

CYBER-PHYSICAL SECURITY OF ENERGY MANAGEMENT SYSTEM FOR CONNECTED AND AUTOMATED ELECTRIC VEHICLES

Suchitra Devi A[1], Champana K S[2], D U Kruthika[3], Bhuvan M[4], Gagan R[5]

[1]Asst Professor, Dept. Of Cse, Sambhram Institute of Technology, Bengaluru-560079, Karnataka, India.

[2,3,4,5]Eighth Semester, Dept. Of Cse, Sambhram Institute of Technology, Bengaluru-560079, Karnataka, India.

DOI: https://www.doi.org/10.58257/IJPREMS33506

ABSTRACT

In this project, a systematic assessment of cyberphysical security on the energy management system for connected and automated electric vehicles is proposed, which, to our knowledge, has not been attempted before. The generalized methodology of impact analysis of cyber-attacks is developed, including novel evaluation metrics from the perspectives of steady-state and transient performance of the energy management system and innovative index-based resilience and security criteria. Specifically, we propose a security criterion in terms of dynamic performance, comfortability, and energy, which are the most critical metrics to evaluate the performance of an electronic control unit (ECU). If an attack does not impact these metrics, it perhaps can be negligible. Based on the statistical results and the proposed evaluation metrics, the impact of cyber-attacks on ECU is analyzed comprehensively. The conclusions can serve as guidelines for attack detection, diagnosis, and countermeasures.

Keywords: Analysis, Diagnosis.

1. INTRODUCTION

With the significant increase in the traffic, road, and environmental information enabled by vehicle-to infrastructure/cloud/vehicle communications, the connected and automated vehicle (CAV) technology can significantly enhance the driving safety, comfort, and energy efficiency. However, since a large number of embedded ECUs are integrated into networks, it also brings cyber-security concerns. As demonstrated by recent examples, the vehicles are vulnerable to cyber-attacks, allowing an attacker to circumvent the vehicle control systems, which would lead to severe consequences such as disabling brakes, turning off headlights, and taking over steering. For example, cyber-attacks on anti-lock braking systems in demonstrate that a malicious attacker can modify the feedback measurements through wheel speed sensors and cause life-threatening situations. Spoofing attacks on the global positioning system (GPS) may result in course deviation in an autonomous vehicle. Some cyberattacks through direct (by connecting with onboard diagnostics (OBD-II) port) and remote (through wireless channels like Bluetooth) access have also been reported in the literature.

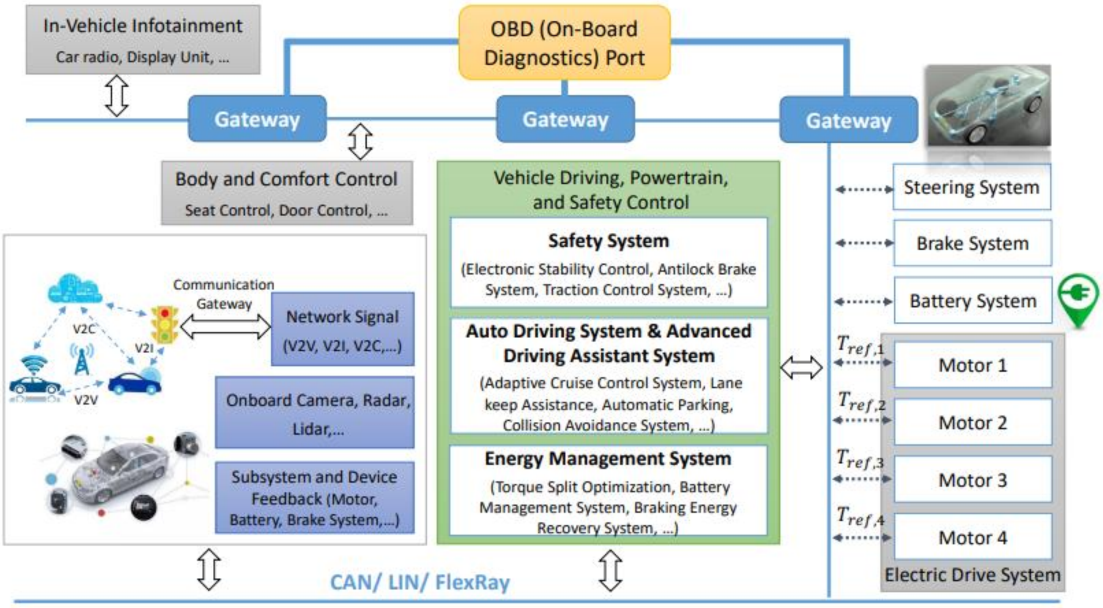

In-Vehicle Infotainment
Car radio, Display Unit, ...
OBD (On-Board Diagnostics) Port
Gateway
Gateway
Gateway
Body and Comfort Control
Seat Control, Door Control, ...
Vehicle Driving, Powertrain, and Safety Control
Safety System
(Electronic Stability Control, Antilock Brake System, Traction Control System, ...)
Auto Driving System & Advanced Driving Assistant System
(Adaptive Cruise Control System, Lane keep Assistance, Automatic Parking, Collision Avoidance System, ...)
Energy Management System
(Torque Split Optimization, Battery Management System, Braking Energy Recovery System, ...)
Steering System
Brake System
Battery System
$T_{ref,1}$
$T_{ref,2}$
$T_{ref,3}$
$T_{ref,4}$
Motor 1
Motor 2
Motor 3
Motor 4
Electric Drive System
Communication Gateway
V2C
V2I
V2V
Network Signal (V2V, V2I, V2C,...)
Onboard Camera, Radar, Lidar,...
Subsystem and Device Feedback (Motor, Battery, Brake System,...)
CAN/ LIN/ FlexRay

Fig. 1. System design

Furthermore, cyber-attacks in connected and automated vehicles (CAVs) through vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) are discussed and have received increased attention in real-life scenarios in the last two years.

In particular, due to the connection with battery charging infrastructure, more centralized control architecture, and higher electrification, the cyber-physical security in connected and automated electric vehicles (CAEVs) is receiving much more attention compared to an internal combustion engine (ICE) vehicle. For example, the connectivity between CAEVs, charging stations and smart grid may expose the CAEVs to the cyberattacks. Compared to conventional cyber approaches for ICE vehicles, for instance, that focus on a vehicle's entry points cyber-physical security monitoring can serve as a second line of protection because an abnormal system measurement is a clear indicator for potential cyber-attacks. However, cyberphysical security on CAEVs is still in its infancy. Due to the lack of security monitoring, they are prone to a wide range of cyber-attacks ranging from conventional eaves-dropping and denial of service (DOS) attacks to man-in-the-middle (MiTM) attacks that degrade the vehicle's performance. The consequences can be catastrophic as they have the ability to cause physical damage to vehicles, people, and the infrastructure (the grid). There have been some preliminary works on cyber-security of battery management systems.

2. METHODOLOGY

Generalized methodology for cyber attack impact analysis: This involves creating new evaluation metrics to assess the impact of cyberattacks on the EMS.

These metrics consider:

- Steady-state performance: How the attack affects the system's stable operation.
- Transient performance: How the attack impacts the system's behavior during sudden changes.

3. LITERATURE SURVEY

The growing range of cyber-security risks shown above has been promoting the development of vehicle cyber-security techniques for both theoretical and application aspects. The efforts can be categorized into two schemes. The first scheme focuses on the ability to prevent malicious attacks. For instance, throughout the vehicle development cycle, automakers can define core performance requirements of subsystems to automotive parts suppliers, and then the subsystems are designed by considering its security within the software. To prevent malicious attacks through direct contact with the OBD-II port, the communication protocol of the OBD-II is kept secret to the public. Several critical practices, like secure hardware, secure software updates, penetration testing, and code reviews, are also widely used by the automotive industry. Besides, approaches concerning information security during driving, such as message authentication and encryption, the firewall between external networks and vehicle devices are also taken into consideration.

Although these conventional vehicle cybersecurity and information-security approaches can be used to prevent attacks, they alone cannot guarantee the security of the whole system. Therefore, cyber-physical security from the control perspective that concentrates on improving the resilience of the automotive control system to attack should be addressed, including impact analysis, attack detection and diagnosis, and resilient control While these efforts provide some technical foundations, cyber-physical security challenges in CAEVs remains significant:

(1) Most of the existing works are developed for connected and automated ICE vehicles rather than CAEVs.

(2) Only safety-critical systems are addressed while long-term specification like efficiency performance (e.g., energy management system (EMS)) receives little attention. It is essential particularly for CAEVs because of the limited battery capacity and the 'range anxiety.'

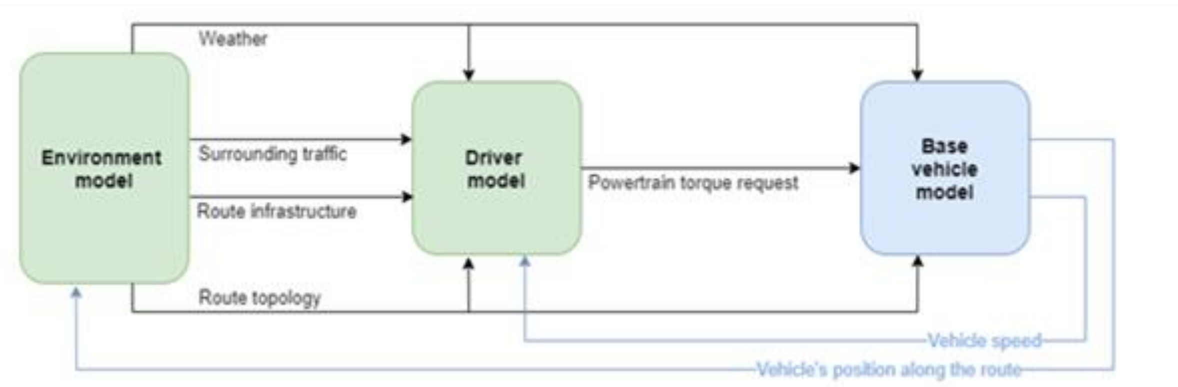
For instance, the authors provide a physics-driven approach to assess the vulnerability of EV batteries, and the results have shown that cyber-attacks can lead to faster deterioration in power capability and battery life. Furthermore, most of the existing literature is cyber-based methods and rely heavily on communication technology. There is little work on impact analysis on cyber-attacks. Although there have been some researches focusing on impact analysis of cyber threats on cyber-physical systems, e.g., electric systems and smart grids, they mainly focus on few metrics such as active (or reactive) power, system frequency, node voltage, and power angle. For example, the authors analyzed the data integrity attacks on automatic generation control loop for smart grids; the cybersecurity policies for flexible alternating current transmission devices are discussed; presented the impact of integrity attacks on electric market operations; used reachability methods in graph theory to assess the risks and vulnerabilities of two-area power systems. For a complicated control system in a CAEV, such as safety system (electronic stability control, antilock brake, etc.), auto driving system (adaptive cruise control system, lane keep assistance, etc.), and EMS (torque split optimization, battery management system, etc.), more detailed models and metrics should be considered to evaluate the system comprehensively. For example, the upper autonomous controller or human driver requires a fast and accurate dynamic response, reasonable power output, low torque ripple, as well as minimizing energy consumption in various drive cycles. These performances should be particularly addressed for control systems in CAEVs while these approaches for electric systems and smart grids are unfeasible. In summary, it is essential to emphasize the cyber-security challenge of the ECUs in CAEVs, and novel methodologies of vulnerability assessment should be developed.

4. PROBLEM STATEMENT

Cyber-physical security challenges in CAEVs remains significant: (1) Most of the existing works are developed for connected and automated ICE vehicles rather than CAEVs. (2) Only safety-critical systems are addressed while long-term specification like efficiency performance (e.g., energy management system (EMS)) receives little attention. It is essential particularly for CAEVs because of the limited battery capacity and the ’range anxiety.’

5. SYSTEM DESIGN

This project provides a general guidance for vulnerability assessment of core control systems for CAEVs, with which the impact of cyber-attacks on different critical systems and signals, as well as the interaction between these subsystems can be analyzed comprehensively. We are simulating the results of the data in CAEV networks.



We have designed this application as a simulation where vehicles will move on a road by receiving commands from ECU and then we will monitor vehicle velocity to detect normal and attack scenarios and then record energy consumption in both scenarios.

The simulation framework has been used in a first phase to aid project partners in the sizing of components for their demonstrators by supporting the engineering decisions. The framework is later used to develop the advanced energy and thermal management strategies in a virtual environment prior to being implemented and tested in the demonstrator vehicles.

6. IMPLEMENTATION

6.1 Dataset Collection

- We use the EMS-EVs dataset to evaluate the performance of the proposed intelligent attack detection method. The dataset is a benchmark dataset for network intrusion, which is an improved version of the EMS-EVs dataset.
- The Dataset contains 125,973 training traffic samples and 22,554 test traffic samples. For training seven weeks of network traffics were collected in the form of raw tcpdump format, and the following two weeks of network traffics were also collected for testing.
- To make the attack detection task realistic, there are many attacks that did not appear during the collection phase of training data. Attacks fall into four main categories according to their characteristic: DOS, U2R, R2L, Probe.

6.2 Data Preprocessing

A preprocessing step is to transform the input data into a matrix format that can be vectorized. The common operations include data sampling, data cleansing and data dimensionality reduction. The processing step is the same during the training and testing phase.

6.3 Classification of attacks

In this module we will use the models which gives more accuracy to classify the types of attacks in Energy Management Systems in Electric Vehicles.

7. TRAINING

7.1 AdaBoost

- AB is a tree-based ensemble classifier that incorporates many weak classifiers to reduce misclassification errors. It selects the training set and iteratively assigns the weights depending on the previous training precision for retraining the algorithm. In order to train any weak classifier, an arbitrary subset of the full training set is used and AB assigns weights to each instance and classifier. The following equation defines the combination of several weak classifiers:
- where H(x) defines the output of the final model through combining the weak classifiers and ht(x) represents the output of classifier t for input x and αt specifies the weight assigned to the classifier.

$$H(x) = Sign(\sum_{t=1}^{T} \alpha_t h_t(x))$$

7.2 KNN

KNN classifies the test data by utilizing the training data directly by calculating the K value, indicating the number of KNN. For each instance, it computes the distance between all the training instances and sorts the distance. Furthermore, a majority voting technique is employed to assign the final class label to the test data. This research applies Euclidean distance to calculate the distances among instances. The following equation represents the Euclidean distance calculation:

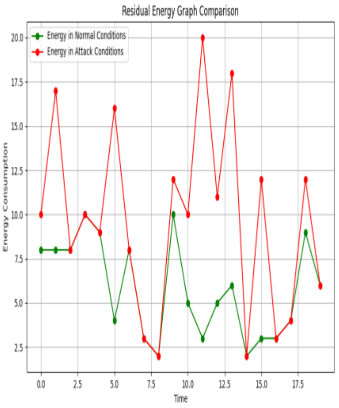
$$D_e = \sqrt{\sum_{i=1}^{n} (X_i - Y_i)^2}$$

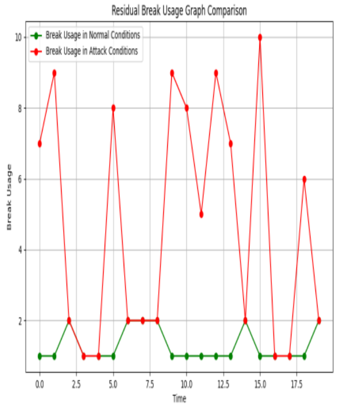
7.3 Logistic Regression

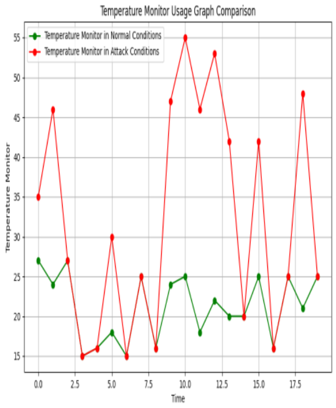
Based on a given dataset of independent variables, logistic regression calculates the likelihood that an event will occur, such as voting or not voting. Given that the result is a probability, the dependent variable’s range is 0 to 1. In logistic regression, the odds—that is, the likelihood of success divided by the probability of failure-are transformed using the logit formula. The following formulae are used to express this logistic function, which is sometimes referred to as the log odds or the natural logarithm of odds.

8. RESULTS

The outcomes that we found after testing and putting the suggested algorithms into practice will be covered in this part.







9. CONCLUSION AND FUTURE ENHANCEMENT

This project provided a general guidance for vulnerability assessment of core control systems for CAEVs, with which the impact of cyber-attacks on different critical systems and signals, as well as the interaction between these subsystems can be analyzed comprehensively. As a case study, we have developed an MPC-based EMS for CAEVs with four in-wheel motors and presented a systematic vulnerability assessment on cyber-threats. Then, innovative index-based evaluation metrics in terms of dynamic performance, comfortability, energy, and system security and resilience are established to evaluate the critical performance. Following, we give a few remarks on practical applications and future works. In the project, we have demonstrated that an attacker can degenerate the overall performance of the vehicle through data integrity attacks, e.g., higher velocity tracking error and torque ripples, lower energy efficiency, and even instability. For the developed MPC-based EMS, the results have shown that all of the evaluation metrics, including the proposed indices of recovery time and resilience, can reflect the impact of various cyber-attacks. Then, by using these metrics, one can develop data-based or model-based detection and diagnosis approaches in practical applications. Also, the statistical results can help to identify the critical signals, so that they pay more attention to it when designing a system.

It should be noted that besides the detailed impact analysis of cyber-threats on EMS, this paper provides a general framework of vulnerability assessment of a control system in the ECU (from the control perspective). For other systems, e.g., safety system and advanced driver assistance systems in Fig. 1, one needs to conduct a detailed impact analysis by using the potential signal inputs and objectives stated in Section II (under a variety of cyber-physical attacks according to specific demands). Particularly, for those learning-based systems, e.g., a pedestrian detection system in deep learning approaches in rough weather, although vulnerability assessment can be addressed by designing various cyber-physical attacks and evaluation metrics as described in the paper, because of the unique algorithm structure compared to traditional control methodologies, further research is needed.

10. REFERENCES

[1] J. K. Naufal, J. B. Camargo, L. F. Vismari, J. R. de Almeida, C. Molina, R. I. R. Gonzalez, R. Inam, and E. Fersman, "A ´ 2 CPS: A vehicle-centric safety conceptual framework for autonomous transport systems," IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 6, pp. 1925–1939, 2017.

[2] M. Pajic, J. Weimer, N. Bezzo, O. Sokolsky, G. J. Pappas, and I. Lee, "Design and implementation of attack-resilient cyberphysical systems: With a focus on attack-resilient state estimators," IEEE Control Systems Magazine, vol. 37, no. 2, pp. 66–81, 2017.

[3] P. Guo, H. Kim, L. Guan, M. Zhu, and P. Liu, "Vcids: Collaborative intrusion detection of sensor and actuator attacks on connected vehicles," in 2017 International Conference on Security and Privacy in Communication Systems. Springer, 2017, pp. 377–396.

[4] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham et al., "Experimental security analysis of a modern automobile," in 2010 IEEE Symposium on Security and Privacy. IEEE, 2010, pp. 447–462.

[5] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno et al., "Comprehensive experimental analyses of automotive attack surfaces." in 2011 USENIX Security Symposium. San Francisco, 2011, pp. 447–462.

[6] C. Valasek and C. Miller, "Adventures in automotive networks and control units," Technical White Paper, IOActive, 2014.

[7] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava, "Non-invasive spoofing attacks for anti-lock braking systems," in 2013 International Workshop on Cryptographic Hardware and Embedded Systems. Springer, 2013, pp. 55–72.

[8] N. O. Tippenhauer, C. Popper, K. B. Rasmussen, and S. Capkun, "On ¨ the requirements for successful GPS spoofing attacks," in 2011 ACM Symposium on Computer and communications security. ACM, 2011, pp. 75–86.

[9] T. Zhang, H. Antunes, and S. Aggarwal, "Defending connected vehicles against malware: Challenges and a solution framework," IEEE Internet of Things journal, vol. 1, no. 1, pp. 10–21, 2014.

[10] D. Wise, "Vehicle cybersecurity dot and industry have efforts under way, but dot needs to define its role in responding to a real-world attack," Gao Reports. US Government Accountability Office, 2016..