Presented at IEEE CyberPELS 2019

Emerging Cyber-Pyhsical Power Electronics Attacks in Autonomous Electric Vehicles

Mithat C. Kisacikoglu
Dept. of Elect. & Computer Eng.
The University of Alabama
Tuscaloosa, AL
mkisacik@ua.edu

M. Ashiqur Rahman, Kemal Akkaya
Dept. of Elect. & Computer Eng.
Florida International University
Miami, FL
{marahman, kakkaya}@fiu.edu

Bilal Akin
Dept. of Elect. Eng.
University of Texas at Dallas
Dallas, TX
bilal.akin@utdallas.edu

Abstract—Modern automotive cyber-physical systems utilize numerous smart technologies including sensors, wireless communication, electrified and autonomous operation. An average autonomous vehicle (AV), driving an hour per day, is expected to use massive amount of data every day, some of which will need to be communicated to outside of the AV. Meanwhile, electric vehicles (EVs) have been transforming modern transportation and energy systems, introducing fuel savings and environmental benefits which make them an attractive option for autonomous driving as well. Accordingly, to realize truly autonomous electric vehicles (AEVs), it is crucial that 1) the vehicles interact with the physical world seamlessly through sensors such as cameras, radars, and light detection and ranging sensors, and 2) the vehicles have continuous/seamless broadband connectivity with each other and the supporting infrastructure. Nonetheless, this cyberspace provides numerous opportunities for malicious actors threatening the security of the AEVs and their applications, potentially resulting in accidents, injuries, property/infrastructure damages, even taking human lives. In this paper, we analyze emerging power electronics security challenges and propose a novel preliminary countermeasure approach for the secure and dependable operation of the system. The approach considers developing a lightweight, machine learning-based intrusion detection mechanism to be deployed at the power electronics/microcontorller level such that it can deal with malicious data/control commands initiated by attacks at any level, including software, hardware, or firmware-based attacks.

Index Terms—Automotive cyber-physical systems; security; power electronics; intrusion detection; machine learning.

I. Introduction

Modern vehicles are no longer traditional stand-alone mechanical engineering masterpieces. They are now characterized by numerous smart technologies including sensors, wireless communications, more electrification, autonomous operations, and data analytics. For example, such a modern vehicle has over 100 million lines of code which will continue to grow in the near future [1]. As another example, an average autonomous vehicle (AV), driving an hour per day, by itself is expected to use 4,000 gigabytes of data every day [2] (not counting the increased demand from the occupants of the AVs), some of which will need to be communicated to outside of the AV with other vehicles, infrastructure, and people.

In parallel to AVs, electric vehicles (EVs) have been transforming modern transportation and energy systems [3]. The mass adoption of EVs has been steadily increasing for the past two decades across all domains.

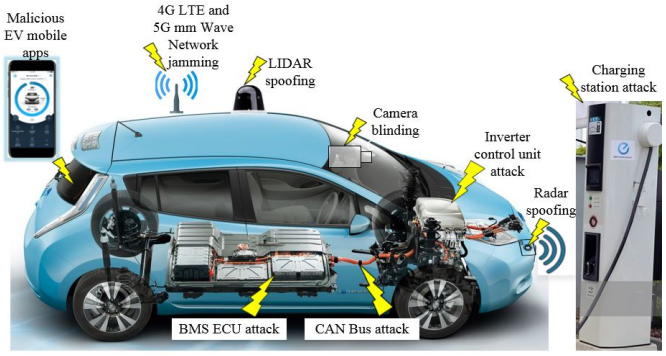


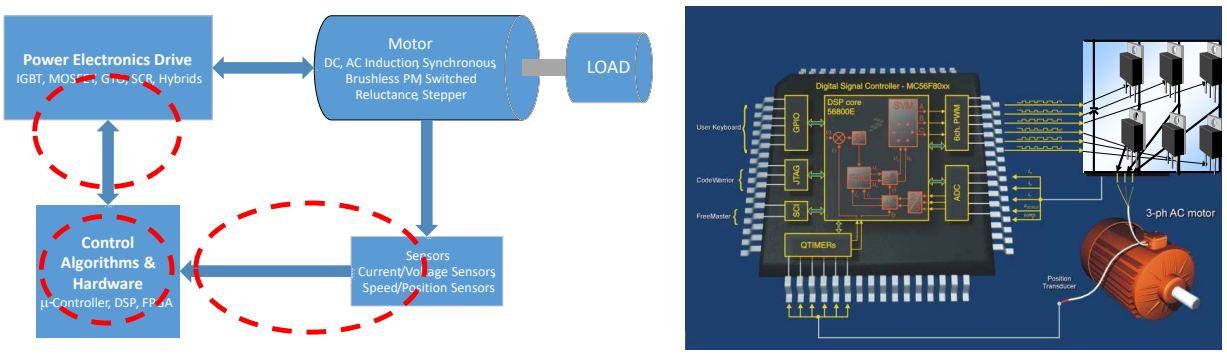
Fig. 1. Automotive cyber physical system in a AEV with its various elements.

Considering fuel savings and environmental impacts, EVs and AVs are perfectly aligned [4], [5]. Hence, automotive systems are going through massive transformation to increase vehicle safety, efficiency, and reliability to realize autonomous EVs (AEVs).

Nonetheless, the cyberspace of these AEVs provides numerous opportunities for malicious actors threatening their security [6]–[9] as illustrated in Fig. 1. Unprotected or improperly protected systems can be easily exploited for malicious use. Indeed, AEVs are under constant threat of increasing number of cyber-attacks through their sensory or wireless channels, hardware, software, controllers or actuators. Given the growing number of security threats to the AEVs, securing them against malicious activities is of utmost importance. Otherwise, malfunctioning of mission-critical applications can cause injury and damage at personal/public and business levels.

While a large body of research exists on vehicular communication security (spanning communications both within and outside of a vehicle) [10]–[18], the proliferation of AEVs raises new security challenges that need to be tackled. These challenges relate to the control aspects when there are attacks to various elements of the AEVs, such as electronic control units (ECUs) of the vehicle to control the battery charging and traction drives and higher levels of automated driving, including multiple bus systems in use.

In this paper, we briefly discuss the emerging power electronics security challenges in AEVs. Our discussion



(a) (b)

Fig. 2. (a) Schematic diagram of a traction drive control loop and (b) an example traction system [20].

considers on the traction drive of a AEV as a case study. We then discuss the potential countermeasure approaches and their shortcomings. Finally, we propose a machine learning-based defense mechanism to be developed at the power electronic level. The study is limited into a preliminary discussion about the approach and corresponding implementation challenges.

This paper is ogranized as follows. Section II presents a brief discussion of the power electronics in AEVs and the emerging power electronics security challenges. In the following section, an IDS-based countermeasure approach is proposed with a preliminary discussion about the technique. The paper is concluded in Section IV.

II. Vehicle Power Electronics Security

There are many ECUs in AEVs including engine control unit, battery management system (BMS) control unit, electronic brake control module, autopilot and transmission control module. Unfortunately, these ECUs are subject to attacks and being compromised [19]. In this section, we briefly discuss ECUs, the power electronics in AEVs, as well as potential security issues.

A. Power Electronics in AEVs

Today, there are various high-performance microcontrollers that are designed to control power electronics systems and provide advanced communication and digital signal processing options in industrial and automotive applications. Most of these microcontrollers have developed to provide very high precision sensing, powerful processing through accelerators or dual cores to enable design engineers to create highly efficient power systems.

The high-end controllers offer single-cycle operations and up to 300 MIPS coupled with a highly-optimized peripherals and interrupt management bus for a variety of control applications. Typically, there are a number of accelerators supporting the high performance CPU core for fast and ultra efficient processing power required for highly complicated non-linear system control in real-time such as, floating-point accelerator, complex math accelerator, trigonometric math accelerator, and control law accelerators. Thanks to these accelerators, CPU bandwidth can be used much more efficiently [21]. Moreover, these controllers provide specific peripherals to enable system-on-chip solutions for various closed-loop control applications. Sensing peripherals can be fully synchronized to timing peripherals to yield accurate control update, and industry standard communication peripherals enables connected and intelligent applications. High-end controllers include communication peripherals such as ethernet, UART, CAN, SPI, SCI etc. which are essential for connected systems but at the same time constitute one of the weakest point in terms of security.

Enabled by all these features, these microcontrollers are deployed in transportation electrification, such as on-board and off-board chargers, traction or propulsion motor control, power steering to name a few. In addition, they are widely deployed in renewable energy systems, power grid automation, robotics and various industrial applications. Fig. 2(a) shows a schematic diagram of a traction drive system, presenting the control loop, i.e., data and control command flow. Fig. 2 shows an example traction drive.

B. Security Threats

There are many different mechanisms of compromising a power electronics system. This can be done through vehicular communication network, or exploiting the control module directly through different levels of connectivity (physical, remote, etc.) [12].

There are mission-critical components of an AEV such as the battery pack and the traction drive system. A power electronics circuit operates in a way to ensure an efficient, stable, and high-quality power conversion and control of the power flow from energy storage unit to electric motor during traction or from utility grid to energy storage unit during external battery charging. Thus, the safety of power electronics that control the power flow when the vehicle is moving and being charged are of utmost importance. The engine ECU communicates with the individual power converter controllers to drive the vehicle in a stable way and to control the vehicle based on physical/autonomous driver's requests. The conventional precautions taken for the protection of the traction drive inverter or on-board/off-board charger include over-voltage/current and

over-temperature protection of the circuitry. The fidelity of the sensed values such as current, voltage, or motor position are very important elements for the safe operation of the vehicle. The motor controller parameters that result in stable operation of the motor are also crucial. Further, the controller parameters for on-board/off-board charger is also important to protect the battery and grid operation.

This paper presents in particular the vulnerabilities on AEV power components and its controllers. These components include power electronics circuits and BMS, which are supervised by ECUs. Vulnerabilities related to control of battery charging and traction drive are possible at different levels as shown by the red circles in Fig. 2(a). Below are some possible attack models:

1) An attacker can compromise the BMS to do critical damage to battery system thermal stability. This can be through physical access.
2) An attacker can compromise the traction drive in various ways. Here are some examples:
   - Changing the controller parameters of the traction inverter.
   - Clearing the dead-time of the phase-leg switches.
   - Changing the sensor signals that are retrieved from the inverter and electric motor.
3) An attacker can compromise a charging station to do damage to power grid operations.

In addition to these specific attacks, there are always possibilities to compromise AEVs through other means like firmware updates.

It is crucial to keep the AEV power electronics secure from possible potential attacks. In particular it is important to ensure that control decisions are taken (by the microcontrollers) on the true data, the control functions are executed properly, and the true commands are sent to the actuating devices (e.g., motors).

III. Vehicle Power Electronics Defense

Possible ways of attack mitigation on power electronic systems on AEVs include ensuring message authentication and data integrity, However, applying proper cryptography-based solutions incurs high overhead as it requires dealing with large keys and expensive crypto computations. This overhead is not suitable for power electronic devices/controllers as they are resource constrained in terms of both memory and computing capacity, as we discussed in Section II-A.

Another potential defense strategy can be developing intrusion detection systems for the ECUs. However, providing a comprehensive solution, which often needs extensive data analysis, may not be possible to run at the real-time on the resource constrained controller. These network-based detection systems may not be effective for attacks that are launched within the system (e.g., firmware, hardware trojans, etc.). In this respect, a suitable option is developing a power electronics/microcontroller-level detection mechanism, which will allow detecting incorrect inputs and outputs at the digital signal processor (DSP)/gate drive. Fig. 3 shows the potential placement of

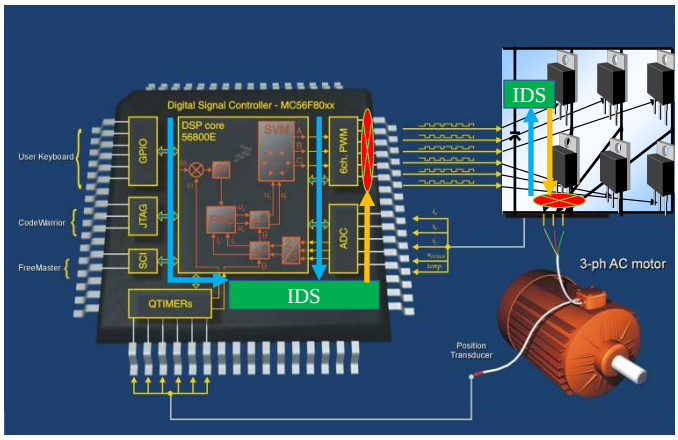


Fig. 3. IDS-based defense strategy for AEV power electronics security.

such an on-chip-based IDS, which will detect the malicious control parameters by checking the input and/or output patterns, and can protect the system by stopping the transmission of (potentially) malicious commands to the actuating devices.

This lower-level detection system can apply machine learning (ML) for detecting malicious control parameters. As the resource is limited in the power electronic devices, the effectiveness of the ML-based model will greatly depend on choosing the right model to be executed on the controller.

A. Proposed Learning Approach

The controller sets certain register bits each time there is an action to be taken. Depending on the application, the actions are standard and can be learnt. We propose to train our machine learning model by collecting all possible bit configurations (i) sent to the controller (i.e., inputs to the DSP), (ii) sent from the controller (i.e., outputs from the DSP), and the patterns between these input and output bit configurations (in Fig. 3, the blue arrows to the IDS). This training will be done in advance (offline) as there is not resource to do online training.

The model will be developed based on the application, e.g., EV traction drive, EV charger, PV inverter, etc., as the bit configurations differ based on the control system/process. Various lightweight models such as decision tree, Naïve Bayes, etc. can be applied as the power electronic devices are resource constrained. Another option would be to use a Markov-chain, where an update to the register bits will be considered as a change in the state.

B. Potential Placement of IDS

Once the IDS is built, i.e., the model is successfully trained, validated, and tested, the model can be installed as a firmware, as a part of the controller firmware, or a separate component on the integrated hardware. Another option can be a separately added hardware component between input (sender)/output (receiver) devices and the power electronic/microcontroller. As part of the defense strategy, if an anomaly is detected, the IDS will be capable

to stop the actuation process (in Fig. 3, the yellow arrows to the crossed red circles).

In a scenario with multiple microcontrollers, functionally interdependent or running control loops with correlated sensor data, the detection mechanism can follow a complex pattern according to the inputs and outputs of the microcontrollers. Here, multiple detection models may be required while a model will consider the inputs/outputs of the other interdependent controlling devices. These detection models will need to be placed appropriately between the devices. In the future, we would like to implement the proposed ML-based IDS and evaluate the efficacy of the system in defending the power electronics, particularly, in AEVs.

IV. Conclusion

This study focuses on investigating security on power electronics controllers/actuators to address the attacks stemming from sensors and communication channels on AEVs. The possible attack trajectories are explained, and the crucial operational vulnerabilities are described.

We presented a preliminary description of a potential countermeasure approach that will apply an ML-based detection and prevention system to be built at the power electronic/controller level. Our future work will include collecting the input and output data for AEV power electronics, designing/training/building the ML-based classifier/IDS, and deploying the model on the integrated microcontroller/power electronics hardware, and evaluating the efficacy of the defense solution.

Acknowledgement

The authors would like to thank Dr. Ismail Guvenc from North Carolina State University and Dr. Ali Gurbuz from Mississippi State University for their comments on possible attack models on AEVs.

References

[1] R. Charette, "This car runs on code," vol. 43, no. 3, p. 3, 2009.

[2] P. Nelson. (2016, Dec.) Just one autonomous car will use 4,000 GB of data/day. Network World. [Online]. Available: https://www.networkworld.com/article/3147892/internet/one-autonomous-car-will-use-4000-gb-of-dataday.html

[3] M. Ehsani, Y. Gao, S. Longo, and K. Ebrahimi, Modern electric, hybrid electric, and fuel cell vehicles. CRC press, 2018.

[4] T. Litman, Autonomous vehicle implementation predictions. Victoria Transport Policy Institute, 2017.

[5] D. J. Fagnant and K. M. Kockelman, "The travel and environmental implications of shared autonomous vehicles, using agent-based model scenarios," Transportation Research Part C: Emerging Technologies, vol. 40, pp. 1–13, 2014.

[6] S. Karnouskos and F. Kerschbaum, "Privacy and integrity considerations in hyperconnected autonomous vehicles," Proceedings of the IEEE, vol. 106, no. 1, pp. 160–170, 2018.

[7] H. S. M. Lim and A. Taeihagh, "Autonomous vehicles for smart and sustainable cities: An in-depth exploration of privacy and cybersecurity implications," arXiv preprint arXiv:1804.10367, 2018.

[8] M. H. Eiza and Q. Ni, "Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity," IEEE Vehicular Technology Magazine, vol. 12, no. 2, pp. 45–51, 2017.

[9] A. C.-F. Chan and J. Zhou, "A secure, intelligent electric vehicle ecosystem for safe integration with the smart grid," IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 6, pp. 3367–3376, 2015.

[10] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: design and architecture," IEEE Communications Magazine, vol. 46, no. 11, 2008.

[11] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on vanet security challenges and possible cryptographic solutions," Vehicular Communications, vol. 1, no. 2, pp. 53–66, 2014.

[12] 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 Security and Privacy (SP), 2010 IEEE Symposium on. IEEE, 2010, pp. 447–462.

[13] S. Parkinson, P. Ward, K. Wilson, and J. Miller, "Cyber threats facing autonomous and connected vehicles: future challenges," IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 11, pp. 2898–2915, 2017.

[14] D. Wampler, H. Fu, and Y. Zhu, "Security threats and countermeasures for intra-vehicle networks," in 2009 Fifth International Conference on Information Assurance and Security, vol. 2, Aug 2009, pp. 153–157.

[15] Q. Wang and S. Sawhney, "Vecure: A practical security framework to protect the can bus of vehicles," in Internet of Things (IOT), 2014 International Conference on the. IEEE, 2014, pp. 13–18.

[16] X. Zheng, L. Pan, H. Chen, and P. Wang, "Investigating security vulnerabilities in modern vehicle systems," in International Conference on Applications and Techniques in Information Security. Springer, 2016, pp. 29–40.

[17] L. Bariah, D. Shehada, E. Salahat, and C. Y. Yeun, "Recent advances in vanet security: a survey," in Vehicular Technology Conference (VTC Fall), 2015 IEEE 82nd. IEEE, 2015, pp. 1–7.

[18] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "Vanet security surveys," Computer Communications, vol. 44, pp. 1–13, 2014.

[19] A. Knight. (2016) Understanding electronic control units in connected automobiles and how they can be hacked. [Online]. Available: https://www.alienvault.com/blogs/security-essentials/understanding-electronic-control-units-ecus-in-connected-automobiles-and-how-they-can-be-hacked

[20] C. Wu. (2010) Introduction of ACIM and PMSM motor control. [Online]. Available: https://www.nxp.com/files-static/ftf_2010/Americas/WBNR_FTF10_IND_F0487.pdf

[21] K. W. Schachter. (2016) Accelerators: Enhancing the capabilities of the C2000 MCU family. [Online]. Available: http://www.ti.com/lit/an/spry288a/spry288a.pdf