2021-01-1249 Published 21 Sep 2021

Onboard Cybersecurity Diagnostic System for Connected Vehicles

Sumanth Reddy Dadam Wayne State University

Di Zhu North Carolina State University

Vivek Kumar and Vinod Ravi Wayne State University

Venkata Sai Srikar Palukuru

Citation: Dadam, S.R., Zhu, D., Kumar, V., Ravi, V. et al., "Onboard Cybersecurity Diagnostic System for Connected Vehicles," SAE Technical Paper 2021-01-1249, 2021, doi:10.4271/2021-01-1249.

Abstract

Today's advanced vehicles have high degree of interaction due to numerous sensors, actuators and also with complex communication within the control units. In order to hack a vehicle, it has to be within a certain range of communication. Here, we discuss the On-Board Diagnostic (OBD) regulations for next generation BEV/HEV, its vulnerabilities and cybersecurity threats that come with hacking. We propose three cybersecurity attack detection and defense methods: Cyber-Attack detection algorithm, Time-Based CAN Intrusion Detection Method and, Feistel Cipher Block Method. These control methods autonomously diagnose a cybersecurity problem in a vehicle's onboard system using an OBD interface, such as OBD-II when a fault caused by a cyber-attack is detected, All of this is achieved in an internal communication network structure. The results discussed here focus on the first detection method that is Cyber-Attack detection algorithm.

Index Terms

hybrid electric vehicle, onboard diagnostic, autonomous connected vehicle, cybersecurity, control algorithm, battery electric vehicle

Introduction

Most of the vehicles have been isolated from the internet until recently. For vehicle diagnostics OBD-II port is the only special case. These ports currently rely on the physical protection provided by the Network Architecture. But with rapid changes. Current generation vehicles already permit smartphones pairing with the car's infotainment system via Bluetooth. And also adding to that many modern vehicles that are connected to the internet are enabling unlocking, starting, passenger monitoring services in the car. In today's vehicles we observe cars with OTA flash services that have complex network interfaces for software updates.

These days, autonomous vehicles (AV) driving without the intervention of a driver use onboard ECU applications to identify driving conditions. AVs now have the ability to diagnose and check for any hazard causing events using various kinds of sensors installed in the vehicle. These complex diagnostic functions are achieved with Electronic Control Units (ECUs), ECU's play a critical role in today's vehicle and hence its rationality along with complex sensors, actuators and onboard system software ought to be ensured in order to protect for vehicle safety.

A handful of extensively advertised attacks has demonstrated vulnerability, consisting of a 2014 occurrence entailing an OEM. Hackers successfully exposed vulnerabilities by finding a password to a Wi-Fi hot spot as well and then used of vehicle main screen and infotainment system. Adding to that they were able to access the vehicle's interior computer network which led them take control of functions ranging from the door locks, window wipers to other Body control parts. This event recalled 1.4 million vehicles and worked as a cautioning to the market that vehicle networks are no longer islands unto themselves.

From the regulation's perspective, regulatory agencies have started to address cybersecurity threats by establishing regulations that are not specific to one category of vehicles and also conducting cutting edge research right into cybersecurity dangers for next generation vehicles covering all category vehicles, as well as giving standards. In 2012, the National Highway Web Traffic Safety And Security Management (NHTSA) [1] set up a new team to research

drive state. The fault-tolerant capability has been achieved by analyzing the characteristics of the CAN signals. The robustness of the detection can be further improved by adding a second layer of check where in the second-step detection rule includes a rule for detecting a sign of an abnormality assumed to be an attack by performing state transition analysis or time-series (sequence pattern) analysis using a series of received electronic control commands (CAN IDs) as discussed in the time based CAN intrusion detection methods. The performance of the time-based methods and Feistel Cipher block method with improved deep learning models can improve the use case and efficiency of the detection. These methods and its algorithm performance results will be further discussed in future works.

References

1. NHTSA, *Nhtsa and Vehicle Cybersecurity* (Washington, DC, USA: National Highway Traffic Safety Administration, 2018)
2. CARB. *California Air Resource Board OBD regulations*, www.arb.ca.gov.
3. Baek, S. and Jang, J., "Implementation of Integrated OBD-II Connector with External Network," *Science Direct Journal* (2014).
4. Khorsravinia, K. et al., "Integrated OBD-II and Mobile Application for Electric Vehicle (EV) Monitoring System," in *IEEE end International Conference on Automatic Control and Intelligent Systems*, 2017.
5. Heineman, L. and Zettel, A., ZERO EMISSIONS VEHICLES (ZEV'S) AND OBD, in *SAE On-board Diagnostics Symposium Americas*, Garden Grove, CA, USA, 2019
6. Zettel, A., *EV Roundtable Discussions*, SAE On-board Diagnostics Symposium Digital Summit, Online Virtual Event, 2020.
7. Nilsson, D.K. and Larson, U.E., "Simulated Attacks on Can Buses: Vehicle Virus," in in *Proc. Int. Conf. on Communication Systems and Networks*, Langkawi, Malaysia, 2008, pp. 66-72.
8. Checkoway, S., McCoy, D., Kantor, B., Anderson, D. et al., "Comprehensive Experimental Analyses of Automotive Attack Surfaces," in *Proc. 20th USENIX Security*, San Francisco, CA, 2011.
9. Yan, W., "A Two-year Survey on Security Challenges in Automotive Threat Landscape," in in *Proc. IEEE ICCVE*, Shenzhen, Oct. 2015, 185-189.
10. Zhang, T., Antunes, H., and Aggarwal, S., "Defending Connected Vehicles Against Malware: Challenges and a Solution Framework," *IEEE Internet of Things* 1, no. 1 (Feb 2014): 10-21.
11. Shoukry, Y., Martin, P., Yona, Y., Diggavi, S., and Srivastava, M., "PyCRA: Physical Challenge-Response Authentication for Active Sensors Under Spoofing Attacks," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur. CCS*, 2015, pp. 1004-1015, doi:10.1145/2810103.2813679.
12. Ljung, L., "System Identification: Theory for the User," *Pearson Education* (1998).
13. Zhou, Yong Bin, Feng, Deng Guo, "Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing," in *International Association for Cryptologic Research*, 2005, https://eprint.iacr.org/2005/388.
14. van Roermund, T. and Bening, A., NXP Automotive Business Unit, "Cybersecurity for ECUs: Attacks and Countermeasures,"[online]. Available: https://www.nxp.com/docs/en/white-paper/Cybersecurity-ECUs-WP.pdf.
15. Farhadi, M. and Abapour, M., "Three-Switch Three-Phase Inverter with Improved DC Voltage Utilization," *IEEE Transactions on Industrial Electronics* 66, no. 1 (2018): 14-24.
16. Elektrotechnik-und, Z.-Z., "Handbook for Robustness Validation of Auto- Motive Electrical/Electronic Modules."
17. Nathan, S., "Hackers After Your Car? Tackling Automotive Cyber Security," The Engineer, Sept. 24, 2015, [Online]. Available: https://www.theengineer.co.uk/hackers-after-your-car-tackling-automotive-cyber-security/ [Accessed 2016 03 21].
18. Khandelwal, S., "Car Hackers Could Face Life In Prison. That's Insane!," The Hacker News, May 01, 2016, [Online]. Available: http://thehackernews.com/2016/05/car-hacker-prison.html [Accessed 2016 05 23].
19. Greenberg, A., "Hackers Remotely Kill a Jeep on the Highway - with Me in It," WIRED, July 21, 2015, [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ [Accessed 2015 09 30].
20. Lodge, D., "Hacking the Mitsubishi Outlander PHEV hybrid," PenTestPartners, June 05, 2016, [Online]. Available: https://www.pentestpartners.com/blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv/ [Accessed 2016 08 14].
21. Garcia, F.D., Oswald, D., Kasper, T., and Pavlidès, P., "Lock It and Still Lose It —on the (In)Security of Automotive Remote Keyless Entry Systems," in *Proc. 25th USENIX Security*, Austin, TX, 2016.
22. Hull, R., "Nissan Disables Leaf Electric Car App After Revelation that Hackers Can Switch on the Heater to Drain the Battery," Thisismoney, Feb. 26, 2016.[Online]. Available: http://www.thisismoney.co.uk/money/cars/article-3465459/Nissan-disables-Leaf-electric-car-app-hacker-revelation.html [Accessed 2016 06 27].
23. Link, R., "Is Your Car Broadcasting Too Much Information?," Trend Micro Inc., July 28, 2015, [Online]. Available: http://blog.trendmicro.com/trendlabs-security-intelligence/is-your-car-broadcasting-too-much-information/?_ga=1.215918871.1268134788.1466680640 [Accessed 2016 06 27].
24. Curtis, S., "Self-Driving Cars Can Be Hacked Using a Laser Pointer," The Telegraph, Sept. 08, 2015, [Online]. Available: http://www.telegraph.co.uk/technology/news/11850373/Self-driving-cars-can-be-hacked-using-a-laser-pointer.html [Accessed 2016 06 25].
25. TU-Automotive Ltd, TU-Automotive Cyber Security Europe, 2-3 November 2016, ICM - Internationales Congress Center München, Germany. [Online]. Available: http://www.tu-auto.com/cyber-security-europe/ [Accessed 2016 06 25].
26. Studnia, I., Nicomette, V., Alata, E., Deswarte, Y., Kaâniche, M. and Laarouchi, Y., "Survey on Security Threats and

Protection Mechanisms in Embedded Automotive Networks," in in *Proc. IEEE DSN-W*, Budapest, June 2013, pp. 1-12.

27. Nilsson, D.K. and Larson, U.E., "Simulated Attacks on Can Buses: Vehicle Virus," in in *Proc. Int. Conf. on Communication Systems and Networks*, Langkawi, Malaysia, 2008, pp. 66-72.
28. Checkoway, S., McCoy, D., Kantor, B., Anderson, D. et al., "Comprehensive Experimental Analyses of Automotive Attack Surfaces," in *Proc. 20th USENIX Security*, San Francisco, CA, 2011.
29. Yan, W., "A Two-year Survey on Security Challenges in Automotive Threat Landscape," in in *Proc. IEEE ICCVE*, Shenzhen Oct. 2015, pp. 185-189.
30. Lyamin, N., Vinel, A., Jonsson, M., and Loo, J., "Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks," *IEEE Commu. Letters* 18, no. 1 (Jan. 2014): 110-113.
31. Ericsson, "Connected Vehicle Cloud Under the Hood," Ericsson, 2015, [Online]. Available: http://archive.ericsson.net/service/internet/picov/get?DocNo=287 01-FGD101192 [Accessed 2016 04 18]
32. National Highway Traffic Safety Administration, "Cybersecurity Best Practices for Modern Vehicles," Report No. DOT HS 812 333, Washington, DC, Oct 2016.[Online]. Available: https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityF orModernVehicles.pdf [Accessed 2017 01 10]
33. Dadam, S., Sharma, S., and Jentz, R., Method for variable position exhaust tuning valve diagnostic, US Patent 10844762.
34. Dadam, S., Jentz, R., lenzen, T., and Meissner, H., "Diagnostic Evaluation of Exhaust Gas Recirculation (EGR) System on Gasoline Electric Hybrid Vehicle," SAE Technical Paper 2020-01-0902 (2020), https://doi.org/10.4271/2020-01-0902.
35. ZHU, D., PRITCHARD, E., DADAM, S.R. et al., "Optimization of Rule-Based Energy Management Strategies for Hybrid Vehicles Using Dynamic Programming," in:, *Combustion Engines*, (2021), https://doi.org/10.19206/CE-131967.
36. Van Nieuwstadt, M.J., Lehmen, A., Martin, D.R., Rollinger, J.E. et al., Gasoline particulate filter diagnostics. US Patent 10323562.
37. Jentz, R., Lenzen, T., Dadam, S., Meissner, H. et al., Method and system for exhaust gas recirculation system diagnostics. US Patent 10632988.
38. Jentz, R.R., Sharma, S., Dadam, S., Heat exchanger for exhaust tuning systems. US Patent 10436087.
39. Exhaust gas heat recovery system with integrated Phase Change Material Heat Exchanger. US Patent 10961884.
40. Dadam, S., GPF Downstream Hose EGHR Diagnostic on Hybrids. US Patent 10928275.
41. Snyder, K. and Ku, J., "Plug-in Hybrid Electric Vehicle Reengineering of a Conventional Sedan for EcoCAR2," SAE Technical Paper 2015-01-1235 (2015), https://doi.org/10.4271/2015-01-1235.
42. Snyder, K. and Ku, J., "Advancement and Validation of a Plug-In Hybrid Electric Vehicle Plant Model," SAE Technical Paper 2016-01-1247 (2016), https://doi.org/10.4271/2016-01-1247.
43. Rehman, A., Ur Rehman, S., Khan, M., Alazab, M. et al., "CANintelliIDS: Detecting In-Vehicle Intrusion Attacks on a Controller Area Network using CNN and Attention-based GRU," *IEEE Transactions on Network Science and Engineering*, doi:10.1109/TNSE.2021.3059881.
44. Blevins, D., Moriano, P., Bridges, R., Verma, M. et al., (2021), Time-Based CAN Intrusion Detection Benchmark. 10.14722/autosec.2021.23013.
45. Plug-N-pwned: Comprehensive vulnerability analysis of OBD-II dongles as a new over-the-air attack surface in automotive IoT(2020). 29th {USENIX} Security Symposium ({USENIX} Security 20)

ISSN 0148-7191