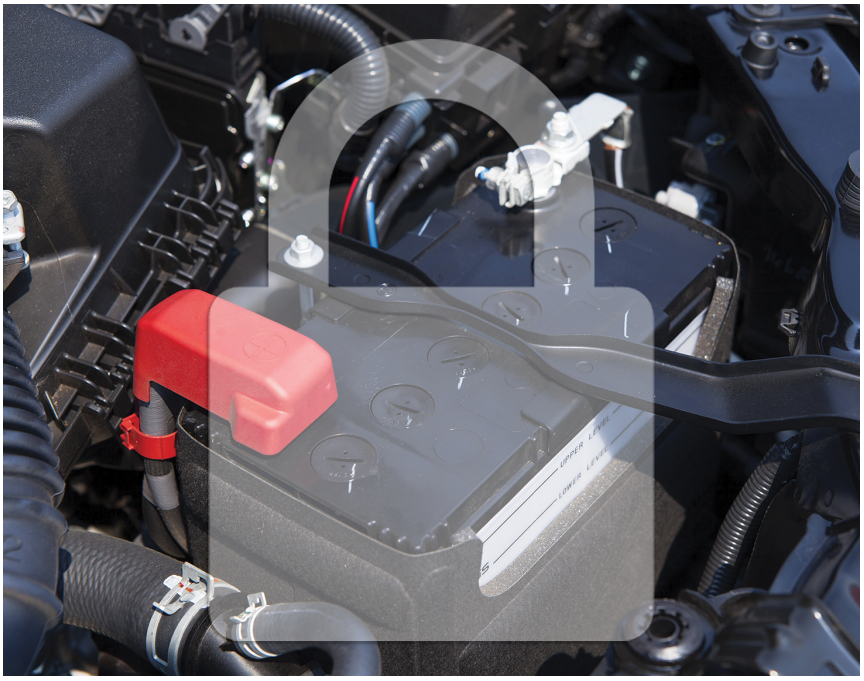
Rethink Physical Security: Protecting Vehicles via Battery-Enabled Sensing and Control

By LIANG HE, *Senior Member IEEE*
Department of Computer Science and Engineering, University of Colorado at Denver, Denver, CO 80204 USA

KANG G. SHIN, *Life Fellow IEEE*
Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI 48109 USA



Cyberization is the foundation of vehicle electrification and automation, requiring ever-increasing deployment of onboard sensing, communication, and computing devices/services. However, vehicle cyberization also exposes new cyber vulnerabilities, as evidenced by a 225% increase in automotive cyber incidents between 2018 and 2021 [1]. The risk of cyberattacks on vehicles is further magnified by two trends. First, for-profit black-hat attackers continue to outpace white-hat hackers, with 63% of automotive cyberattacks launched by black-hat attackers in 2022, up from 49.3% in 2020 [2]. By 2024, the automotive industry is projected to lose $505 billion due to cyberattacks [3]. Second, automotive cyber incidents found on dark webs increased by 253% between 2020 and 2021 [4], indicating that hacking techniques are becoming more accessible to potential hackers, leading to an anticipated surge of automotive cyber incidents in the future. In response to these threats, the United Nations Economic Commission for Europe (UNECE) introduced regulation WP.29 R155 in 2020, mandating the creation of a cybersecurity management system (CSMS) for vehicles.

Fig. 1 shows the two most common vectors used to launch automotive cyberattacks: external wireless accessibility and internal wired networks. Wireless communication interfaces, such as 5G/LTE/Wi-Fi/Bluetooth, allow vehicles to remotely interact with drivers,

Digital Object Identifier 10.1109/JPROC.2023.3285166

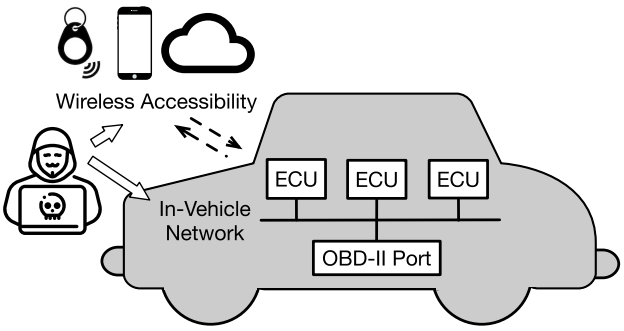


Fig. 1. *Two common cyberattack vectors of vehicles: wireless accessibility and in-vehicle network.*

automakers, and third-party services [5]. However, this wireless accessibility also provides adversaries with an opportunity to hack vehicles remotely through, for example, radio jamming/relaying—leading to widely publicized cases of auto theft exploiting keyless entry systems [6]. The in-vehicle network connects individual cyber components [e.g., electronic control units (ECUs)] and enables their real-time exchange of sensing/control information, which has frequently been exploited by adversaries due to weak security and/or design flaws—such as a lack of network segmentation resulting in unauthorized remote control of the Jeep Cherokee [7]—and its inherent open accessibility through the OBD-II port [8], [9], [10], [11]. According to [4], 89.3% of automotive cyber incidents occurred between 2020 and 2021 through threats to vehicles' communication channels, and 47.1% of automotive cyber incidents occurred through threats to their external connectivity.

External wireless communications and in-vehicle networks are intrinsically vulnerable due to their open accessibility. Adversaries can eavesdrop on and potentially extract encrypted authentication information and proprietary control messages. These accessibility-induced vulnerabilities were highlighted in the cat-and-mouse incident with Tesla. In 2017, hackers reported a vulnerability in Tesla's keyfob, which Tesla addressed with improved cryptography in 2018. However, the same hackers were able to hack the keyfob again in 2019, demonstrating that the security solutions built on easily accessible information are not entirely secure—especially as adversaries gain more knowledge about them.

I. PHYSICALLY SECURING VEHICLES USING AUTOMOTIVE BATTERIES

To mitigate these vulnerabilities that arise from their open accessibility, it is crucial to provide vehicles with security protections that do not rely on the common cyberattack vectors mentioned above. The following research tenet presents a promising solution for implementing such "physical" protections in vehicles.

> ***Batteries as Sensors and Actuators:*** The universally deployed 12-/24-V automotive battery offers a secure channel to monitor and control vehicle operation in physical isolation from common cyberattack vectors.

Specifically, a battery-enabled CSMS (B-CSMS) can provide vehicles with threefold physical security protection, including driver authentication, vehicle access control, and vehicle intrusion detection, as shown in Fig. 2. By introducing the innovative concept of batteries-as-sensors/actuators, the physical security provided by B-CSMS serves as an excellent last-line defense when traditional cybersecurity solutions, such as encryption, distance-bounding wireless communication, proprietary protocols, and others, become vulnerable. B-CSMS is particularly important because the automotive industry is undergoing a disruptive transformation fueled by four technological trends: autonomous driving, connected vehicles, vehicle electrification, and shared mobility. These trends are expected to increase automotive revenue by 30% and add up to $1.5 trillion [12]. All these trends further drive the need for B-CSMS: 1) autonomous/connected/electric vehicles increase vehicle cyberization and, therefore, magnify their cyber vulnerabilities, making physical security solutions such as B-CSMS increasingly vital and 2) shared mobility requires the removal of car keys/keyfobs and the ability to identify drivers, for which B-CSMS provides an efficient solution.

II. BATTERY-ENABLED DRIVER AUTHENTICATION

Car keys (or keyfobs) are the most commonly deployed driver authentication solutions. However, automakers are improving, or even replacing, car keys to gain competitiveness in the $18.89B market of automotive antitheft systems [13], driven by the following two limitations of car keys. First, car keys have been shown to be vulnerable to a variety of attacks [6], [14], [15]. In 2019, the German General Automobile Club tested 237 vehicle models from 33 automakers and found that 99% of them suffered from wireless vulnerabilities [16]. Second, car keys cannot differentiate between drivers, which is necessary for customized services, such as fleet management and personalized speed control. Fig. 3 summarizes the results collected from our survey of 786 car owners regarding their perceptions of the limitations of car keys (or keyfobs). The results show that the top concerns among car owners are the cyber vulnerabilities and the single point of failure of keys. The remaining eight limitations can be generally classified as the inconvenience of using and maintaining a car key.

Automotive batteries can be exploited to enable a new driver authentication that mitigates the

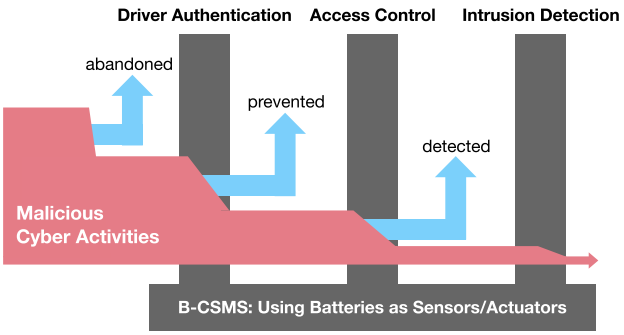


Fig. 2. *Use automotive batteries as sensors/actuators to provide vehicles with three-pronged physical security.*

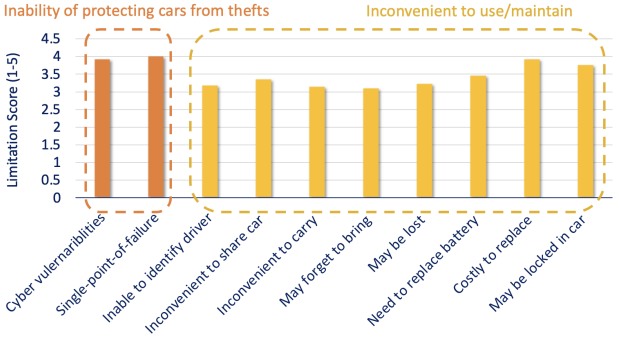


Fig. 3. *Car owners' concerns on car keys.*

limitations of traditional car keys. Specifically, the 12-/24-V power network in a vehicle, which is isolated from the wireless communication and in-vehicle networks, connects a variety of electric (e-) systems to the battery. This widely deployed power-line network can be used as a physical channel to authenticate drivers to the battery, by using battery voltage and/or current as the signal carrier. For example, this power-line network can be leveraged to develop a behavior-based driver authentication system that allows drivers to define their passcode in the form of customized e-system operations. The system can then validate the passcode by examining the resulting battery voltage and current. Fig. 4(a)–(d) plots the voltages and currents of a 2018 Subaru XV's battery while performing four different e-system operations. The results show that the voltages and currents vary with the operation being performed (i.e., they are unique) but are consistent for the same operation (i.e., highly repeatable). This suggests the feasibility of using battery voltages and currents to fingerprint e-system operations and, hence, the driver's identity. In our preliminary study [17], we captured this dependency between e-operations and battery voltage/current using the Thevenin circuit model, developed a set of data cleaning schemes, and used dynamic time warping to quantify the similarity of the voltages for 20 different e-operations, as shown in Fig. 4(e). The fact that the shortest warp distance is always achieved between the same operation corroborates the feasibility of this behavior-based authentication. Designing such a fingerprinting method, however, is nontrivial because the voltage of a given operation may vary depending on the contexts defined by the vehicle, people, and battery. For example, the background operations of the vehicle's e-systems increase the battery current and lower the voltage. In addition, both the relative levels of voltage and their durations may vary even for the same operation, due to the difficulty in repeating certain e-system operations precisely every time. Furthermore, the voltage dynamic is magnified due to its dependency on factors such as temperature, state of charge, and aging.

Another possibility is to design a customized vehicular power-line communication (PLC) system to enable driver-to-battery communication (and hence driver authentication). However, it is important to note that existing PLC solutions cannot be applied to achieve this driver-to-battery communication. First, the results on PLC systems for power distribution grids or power transmission inside buildings cannot be applied to vehicles because the geometric characteristics and tree-shaped topologies of the cable bundles in these environments are very different. According to [18], vehicular PLC is not yet mature, and the standards for use in vehicles are still in their infancy. Second, the driver-to-battery PLC system is different from the limited vehicular PLC designs in the literature (e.g., [19] and [18]): existing vehicular PLC systems usually consider the communication between peer loads in the power-line network, while we must realize the PLC connecting the power source, that is, the battery. The power-line channel connecting the battery suffers from high attenuation, large noise, and low impedance, all of which degrade communication reliability. We have reported an early design of this driver-to-battery PLC system, together with its security analysis, in [20], which authenticates drivers with >99.9% accuracy. We have also demonstrated its utility and effectiveness via a survey of 612 car owners.

III. BATTERY-ENABLED VEHICLE ACCESS CONTROL

Two types of access control are commonly provided on commodity vehicles: entry control by (un)locking the doors and drivability control by (dis)allowing the cranking of engine. Both of these existing access controls are implemented over the

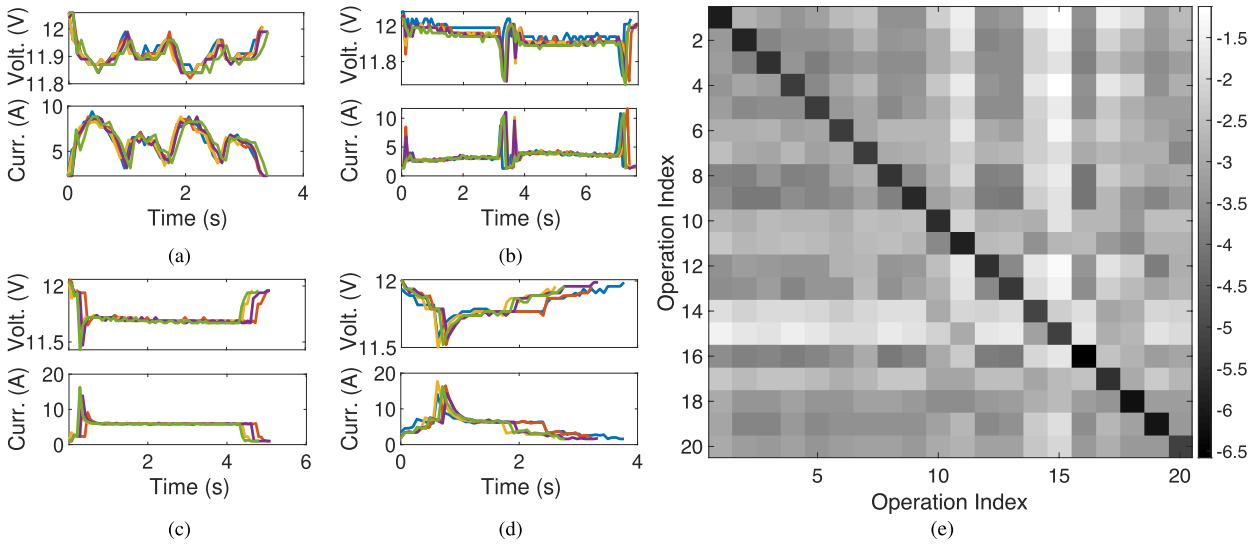


Fig. 4. *Operating a vehicle's e-system triggers unique battery voltages/currents (see details in [17]). (a) Swipe front wiper twice. (b) Roll window down&up. (c) Turn headlight on&off. (d) Turn fan to max and off. (e) Log-scale warp distance of 20 e-operations.*

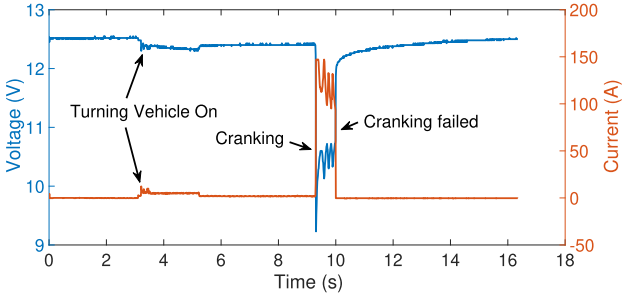


Fig. 5. *Reducing battery's power capacity to disable the cranking of engine.*

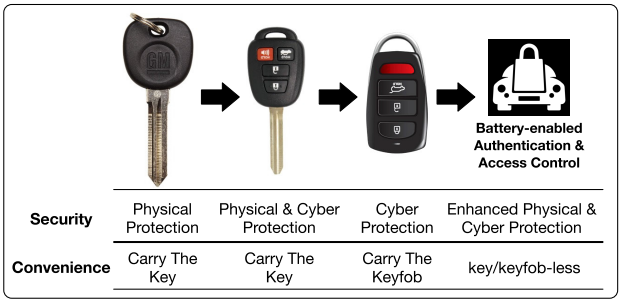


Fig. 6. *New era of vehicle usage.*

in-vehicle network and are thus vulnerable to cyberattacks due to the open accessibility of OBD-II ports. Automotive batteries can be exploited to control vehicle entry and drivability in physical isolation from the in-vehicle network, by using the batteries' power capacity as the control mechanism. Specifically, the battery-enabled drivability control system exploits the fact that cranking the engine requires significantly more power than the vehicle's other e-systems, typically between 2 and 9 kW for 0.3–3 s depending on the type of vehicle [21]. This fact encompasses a current level that supports the above battery-enabled driver authentication but does not crank the engine, allowing the use of the battery's power capacity as the control mechanism to disable/enable the cranking of the engine based on the authentication result. This battery power control system must meet several requirements. First, it must be able to absorb excessive battery power swiftly and safely, as this may cause significant heating. Second, it must adaptively adjust the power thresholds for each specific vehicle, as power consumption varies with the vehicle type. Third, it must keep the battery and the vehicle connected at all times to avoid reserve voltage/current surges that could shorten the lifetime of the vehicle's hardware modules and the power control module itself. Finally, it must be able to withstand the harsh thermal environment of the vehicle's engine compartment, where temperatures can easily rise to over 200°F while driving. Fig. 5 plots a failure of engine cranking when a preliminary design of this power controller is used to limit the battery's maximum current output to 50 A [17]. A similar idea can be extended to provide entry control to vehicles, e.g., by controlling the battery power to disable/enable the unlocking of vehicle doors: unlocking the vehicle doors requires an electric current of several amperes, while monitoring a parked vehicle requires only the order of milliamperes. The

Existing/Potential Solutions	Technical Design					Security		Usability		Potential	
	Collector (or Form of Identify)	Betw. Collector& Authenticator	Authenticator	Betw. Authenticator & Controller	Controller (or Control Knob)	Resist. To Wireless Attacks	Resist. To OBD Hacking	Pervasive	Carry-less	Replace Keys	Identify Drivers
RF Keys/Keyfobs	Digital Code via RF Keys	Wireless signal	Transponder ECU	In-Vehicle Network	Power Control ECU	✗	✗	✓	✗	N.A.	✓
Phone-As-Key	Digital Code via Phone	Wireless signal	Transponder ECU	In-Vehicle Network	Power Control ECU	✗	✗	✗	✗	✗	✓
Tesla's Pin-2-Drive	Digital Code via Control Panel	In-Vehicle Network	Transponder ECU	In-Vehicle Network	Power Control ECU	✗	✗	✗	✓	✗	✓
After-Market Alarms, e.g., Pandora/Viper	Digital Code via Token/Phone	Wireless signal	OBD Dongle	In-Vehicle Network	Power Control ECU	✗	✗	✗	✗	✗	✓
Tire/Steering Locks	Metal Keys	N.A.	Metal Locks	N.A.	Metal Locks	✓	✓	✓	✗	✗	✗
Kill-Switch	Digital Code via Token	Wireless signal	On-board Controller	N.A.	Switch	✗	✓	✓	✗	✗	✗
	Hidden Button	Additional Wiring	On-board Controller	N.A.	Switch	✓	✓	✓	✓	✗	✗
	Button Switch in Engine Cabin	N.A.	Switch	N.A	Switch	✓	✓	✓	✓	✗	✗
Proposed Solution: B-CSMS	E-system Operation	Battery Voltage or Current	Back-End Authenticator	N.A.	Battery Power	✓	✓	✓	✓	✓	✓

Fig. 7. ***Comparison of B–CSMS with existing vehicle immobilizers.***

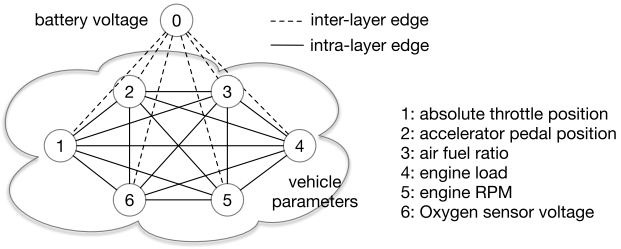


Fig. 8. ***Abstract vehicles using a two-layer correlation graph (with six vehicle parameters as an example).***

extended access control, together with the battery-enabled driver authentication, has the potential to replace existing car keys (or keyfobs), as shown in Fig. 6. Fig. 7 compares B–CSMS, or its driver authentication and vehicle access control, with existing vehicle immobilizers.

IV. BATTERY-ENABLED VEHICLE INTRUSION DETECTION

Numerous cyberattacks involving the injection and modification of data packets in the in-vehicle network have been reported in the literature [22]. Previously, we have also demonstrated the feasibility of modifying the data transmitted in the in-vehicle network [23]. Existing intrusion detection systems (IDSs) are commonly implemented at vehicles' ECUs as part of the in-vehicle network and thus suffer from the security risks thereof, making the IDS itself susceptible to compromises [24]. In contrast to these existing solutions, the use of automotive batteries can enable vehicle intrusion detection without relying on the in-vehicle network [25]. The fundamental idea is to cross-validate a vehicle's operational parameters—the cyber information is continuously collected, processed, and exchanged in the in-vehicle network—using the automotive battery as a physical root of trust. This concept is inspired by two observations. First, since a vehicle is a system of subsystems, the operations of many physically interconnected modules (including, but not limited to, the battery) are closely coupled, getting manifested as correlations among the vehicle's operational parameters in the digital space. Second, battery voltage and current can be measured in physical isolation from the in-vehicle network, thus allowing the battery to serve as a physical root of trust for building the cross-validation mechanism that remains secure even when the in-vehicle network is compromised.

The physical couplings among a vehicle's subsystems are the foundation of battery-enabled intrusion detection and must thus be identified first. This can be done by modeling the pairwise couplings between vehicle parameters (including battery information) and determining whether there is a correlation between two vehicle parameters via model-based cross prediction. This process can identify a large number of correlations among vehicle parameters, which must be effectively and thoroughly described. A large number of correlations among vehicle parameters could be identified, which we need to describe effectively and thoroughly. A two-layer correlation graph $\mathbb{G}$ can be used to capture these correlations and define the coverage of the battery-enabled intrusion detection, that is, what kinds of anomalies can be detected (see Fig. 8 for an example). In this graph, the vertex set represents the vehicle/battery parameters with the battery (other nonbattery) parameters at the upper (lower) layer, and the edge set captures the correlations among vehicle parameters. In this way, $\mathbb{G}$ consists of two types of edges: the interlayer edges representing the correlations between battery information and other vehicle parameters and the intralayer edges capturing the correlations among (nonbattery) vehicle parameters. Using $\mathbb{G}$, we can detect vehicle intrusions by checking real-time vehicle information using norm models describing $\mathbb{G}$'s interlayer edges. To reduce false detections, we can further verify the detected intrusions by checking $\mathbb{G}$'s intralayer edges (and thus being independent

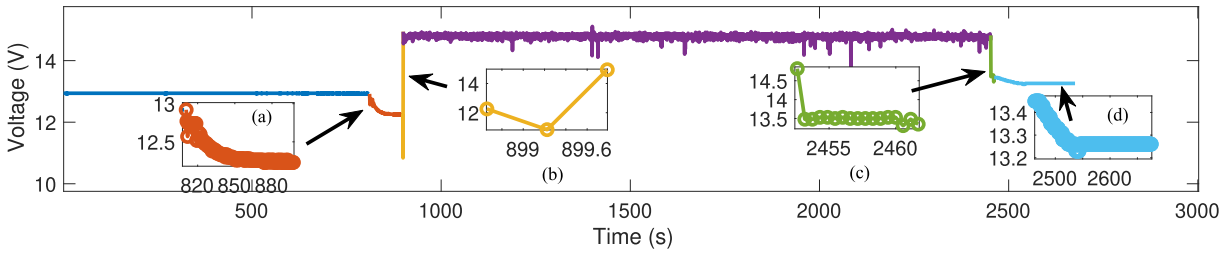


Fig. 9. *Voltage patterns of the four events defining a vehicle's real-time status.*

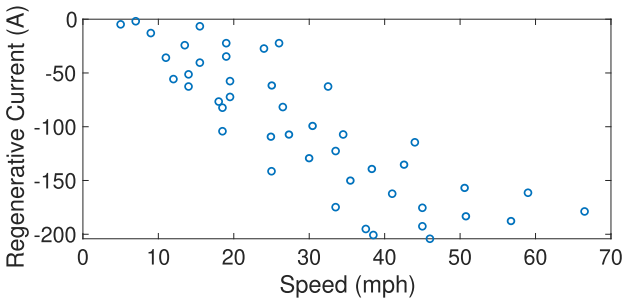


Fig. 10. *Dependency between EV speed and battery current.*

of the intrusion detection), based on the fact that a hacked vertex of $\mathbb{G}$ will also fail the checking of its intralayer edges. We have validated this battery-enabled intrusion detection with the detection of anomalies in engine RPMs as a case study, achieving >86% (up to 99%) average detection rate [25].

V. INTEGRATION BASED ON BATTERY-ENABLED VEHICLE STATUS MONITORING

The above three physical protections can be integrated into a comprehensive vehicle CSMS. We also need to monitor a vehicle's real-time status to determine which physical protection should be activated in real time. The vehicle status can be determined based on four vehicle events: turning on/off the ignition key (or the keyfob's entrance/exit of the proximity of the vehicle) and cranking/stopping the engine. These events can be identified based on their respective voltage patterns, as plotted in Fig. 9. We can further improve the event detection by exploiting their ordering dependencies, e.g., it is impossible to turn off the ignition after cranking the engine without stopping the engine first. We evaluated this voltage-based event detection on a 2008 Honda Fit by repeating the operations of turning on/off the ignition key and cranking/stopping the engine 20 times. The results show 100% true-positive rates and 0% false-positive rates in detecting these events [17].

VI. FURTHER DISCUSSION

A. Detection of Weak Batteries

The accurate and timely detection of weak batteries is crucial to B-CSMS's reliability since it uses the battery to protect vehicles. B-CSMS can estimate the battery's power capacity by taking the battery voltage/current during vehicle operation as input and use this estimation to determine whether the battery is strong enough to provide sufficient power to crank the vehicle engine. It should be noted that B-CSMS draws only negligible power from automotive batteries. For instance, the PLC system discussed in [20] requires only 12 W for 1–2 s to complete the authentication, which is over two orders of magnitude smaller than cranking the engine (which typically requires 2–9 kW [21]).

B. Extension and Application to Electric Vehicles

B-CSMS is built on the 12-/24-V automotive battery and hence is also applicable to EVs where the low-voltage battery is universally deployed as well. Actually, EVs offer additional opportunities for B-CSMS's vehicle protection because of their high-voltage battery packs and the much more strengthened physical coupling between battery and vehicle operation. For example, a new opportunity offered by EVs is to monitor/control the vehicle acceleration/speed using their high-voltage battery packs based on the physical dependency between EV operation and battery power, as shown in Fig. 10.

1) This dependency offers an opportunity to equip B-CSMS with a new ability of continuous driver authentication because the battery power consumption is determined by the driving behavior, and thus, driving information could be extracted from battery voltage/current. Note that this is different from [26], which authenticates EV drivers using their charging behavior, but their authentication is not "continuous."
2) This dependency allows the control of vehicle acceleration/speed by regulating battery power, which can also be extended in the time dimension to control the vehicle's driving distance by regulating battery energy. This allows the physical realization of personalized vehicle usage control without using vulnerable wireless communication or in-vehicle networks, which is particularly important for autonomous vehicles. EVs' existing hardware support for controlling their battery packs' power capacity facilitates the deployment of this control [27].
3) This dependency enlarges B-CSMS's coverage of vehicle intrusion detection by increasing both the upper layer vertices

and the interlayer edges of the vehicle's graph model in Fig. 8. On the other hand, these new edges may share overlapped physical dependencies with the original graph, thus requiring the combination/selection/scheduling of the edge checking to facilitate real-time intrusion detection.

VII. CONCLUSION

This article presents the disruptive concept of using 12-/24-V automotive batteries as a means of physically securing vehicles and introduces B-CSMS, a battery-enabled CSMS that aligns with the UN WP.29 R155 regulation, offering a three-pronged security solution consisting of driver authentication, vehicle access control, and vehicle intrusion detection. It also discusses the challenges and open problems associated with this approach and highlights the potential for further exploration of physical security in a world that is becoming increasingly cyberized and connected. ■

Acknowledgment

This work was supported in part by the National Science Foundation (NSF) under Grant 2245224, Grant 2245223, and Grant 2231759; and in part by the Colorado Office of Economic Development and International Trade (OEDIT) under Grant 2022-2453.

REFERENCES

[1] *Cyber Attacks on Cars up 225 Percent: How Hackers Could Be Targeting Your Vehicle*. Accessed: Jun. 20, 2023. [Online]. Available: https://www.express.co.uk/life-style/cars/1632500/hackers-target-drivers-cyber-attacks-cars

[2] *2023 Global Automotive Cybersecurity Report*, Upstream Secur. Ltd., Ann Arbor, MI, USA, 2023, pp. 1–110.

[3] *Automotive Cybersecurity: A New Frontier*. Accessed: Jun. 20, 2023. [Online]. Available: https://thecyberexpress.com/automotive-cybersecurity-a-new-frontier/

[4] *2022 Global Automotive Cybersecurity Report*, Upstream Secur. Ltd., Ann Arbor, MI, USA, 2022, pp. 1–90.

[5] C. Miller and C. Valasek, "A survey of remote automotive attack surfaces," in *Proc. BlackHat USA*, 2015, pp. 1–90.

[6] L. Csikor, H. W. Lim, J. W. Wong, S. Ramesh, R. P. Parameswarath, and C. M. Choon, "RollBack—A new time-agnostic replay attack against the automotive remote keyless entry systems," in *Proc. BlackHat USA*, 2022, pp. 1–24.

[7] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," in *Proc. BlackHat USA*, 2015, pp. 1–91.

[8] S. Checkoway et al., "Comprehensive experimental analyses of automotive attack surfaces," in *Proc. 20th USENIX Secur. Symp. (USENIX Security)*. San Francisco, CA, USA: USENIX Association, Aug. 2011, p. 2021. [Online]. Available: https://www.usenix.org/conference/usenix-security-11/comprehensive-experimental-analyses-automotive-attack-surfaces

[9] K. Koscher et al., "Experimental security analysis of a modern automobile," in *Proc. IEEE Symp. Secur. Privacy*, Jun. 2010, pp. 447–462.

[10] S. Kulandaivel, S. Jain, J. Guajardo, and V. Sekar, "CANNON: Reliable and stealthy remote shutdown attacks via unaltered automotive microcontrollers," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2021, pp. 195–210.

[11] D. Frassinelli, S. Park, and S. Nürnberger, "I know where you parked last summer: Automated reverse engineering and privacy analysis of modern cars," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2020, pp. 1401–1415.

[12] *Automotive Revolution*. Accessed: Jun. 20, 2023. [Online]. Available: https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/disruptive-trends-that-will-transform-the-auto-industry/de-de

[13] *Vehicle Anti-Theft Market Worth USD 18.89 Billion by 2027*. [Online]. Available: https://www.globenewswire.com/news-release/2021/08/04/2274880/0/en/Vehicle-Anti-Theft-Market-worth-USD-18-89-billion-by-2027-registering-a-CAGR-of-7-12-Report-by-Market-Research-Future-MRFR.html

[14] *Hackers Can Steal a Tesla Model S in Seconds by Cloning its Key FOB*. Accessed: Jun. 20, 2023. [Online]. Available: https://www.wired.com/story/hackers-steal-tesla-model-s-seconds-key-fob/

[15] *Criminals Cloning Your Key FOB, Easily Taking Your Car*. Accessed: Jun. 20, 2023. [Online]. Available: https://www.news5cleveland.com/news/criminals-cloning-your-key-fob-easily-taking-your-car

[16] *Only One Carmaker Is Impossible to Hack*. Accessed: Jun. 20, 2023. [Online]. Available: https://carbuzz.com/news/only-one-carmaker-is-impossible-to-hack

[17] L. He, Y. Shu, Y. Lee, D. Chen, and K. G. Shin, "Authenticating drivers using automotive batteries," in *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, Dec. 2020, vol. 4, no. 4, pp. 1–27, doi: 10.1145/3432198.

[18] T. A. Vincent, B. Gulsoy, J. E. H. Sansom, and J. Marco, "A smart cell monitoring system based on power line communication—Optimization of instrumentation and acquisition for smart battery management," *IEEE Access*, vol. 9, pp. 161773–161793, 2021.

[19] J. Jousse, N. Ginot, C. Batard, and E. Lemaire, "Power line communication management of battery energy storage in a small-scale autonomous photovoltaic system," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2129–2137, Sep. 2017.

[20] L. He and K. G. Shin, "Battery-enabled anti-theft vehicle immobilizer," in *Proc. 20th Annu. Int. Conf. Mobile Syst., Appl. Services*. New York, NY, USA: Association for Computing Machinery, Jun. 2022, pp. 142–154, doi: 10.1145/3498361.3539772.

[21] R. Bosch, *Bosch Automotive Electrics and Automotive Electronics*. Cham, Switzerland: Springer, 2014.

[22] C. Miller and C. Valasek, *CAN Message Injection*. Accessed: Jun. 20, 2023. [Online]. Available: http://illmatics.com/can%20message%20injection.pdf

[23] K.-T. Cho and K. G. Shin, "Error handling of in-vehicle networks makes them vulnerable," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.* New York, NY, USA: Association for Computing Machinery, Oct. 2016, pp. 1044–1055, doi: 10.1145/2976749.2978302.

[24] P. E. Lanigan, S. Kavulya, P. Narasimhan, T. E. Fuhrman, and M. A. Salman, "Diagnosis in automotive systems: A survey," 2011.

[25] L. He, L. Kong, Z. Liu, Y. Shu, and C. Liu, "Diagnosing vehicles with automotive batteries," in *Proc. 25th Annu. Int. Conf. Mobile Comput. Netw.* New York, NY, USA: Association for Computing Machinery, Aug. 2019, doi: 10.1145/3300061.3300126.

[26] L. Kang and H. Shen, "Preventing battery attacks on electrical vehicles based on data-driven behavior modeling," in *Proc. 10th ACM/IEEE Int. Conf. Cyber-Phys. Syst.*, Apr. 2019, pp. 35–46.

[27] P. Kiley, "Reverse engineering the Tesla battery management system to increase power available," in *Proc. BLACK HAT*, 2020, pp. 1–27.

ABOUT THE AUTHORS

Liang He (Senior Member, IEEE) worked as a Research Fellow at the University of Michigan, Ann Arbor, MI, USA, from 2015 to 2017. He is currently an Assistant Professor with the University of Colorado at Denver, Denver, CO, USA. His research interests include cyber-physical systems (CPS), the Internet of Things (IoT), and mobile computing.

Kang G. Shin (Life Fellow, IEEE) is currently the Founding Director of the Real-Time Computing Laboratory, University of Michigan, Ann Arbor, MI, USA, where he is also the Kevin and Nancy O'Connor Professor of Computer Science. He has been working on the characterization of the cyber–physical coupling and its application to the design and analysis of cyber and physical subsystems over more than four decades and has also championed for the establishment of the National Science Foundation Cyber-Physical Systems (NSF CPS) Program. He has led large systems research projects under the auspices of NSF, Defense Advanced Research Projects Agency (DARPA), Office of Naval Research (ONR), Army Research Office (ARO), and Air Force Office of Scientific Research (AFOSR). He has served as a technical consultant for major IT and automotive companies. He has supervised 91 Ph.D. students, a large number of postdoctoral students, and M.S. students. He has published more than 1000 technical articles and more than 40 U.S. and international patents with four patents licensed to the industry.

Dr. Shin received the 2006 Ho-Am Prize in Engineering (the highest honor bestowed to Korean-origin engineers), the 2002 Stephen Attwood Award (the highest honor given to Michigan Engineering faculty), and many other institutional and professional society awards.