Cyber-Physical Security of Energy-Efficient Powertrain System in Hybrid Electric Vehicles against Sophisticated Cyber-Attacks

Lulu Guo, Jin Ye, *Senior Member, IEEE,* and Liang Du, *Senior Member, IEEE*

***Abstract*—In this paper, an innovative approach to improving the cyber-physical security of energy-efficient powertrain system in a hybrid electric vehicle (HEV) against sophisticated cyber-attacks is presented. To the best of our knowledge, cyber-attacks, especially sophisticated and subtle cyber-attacks, have not yet been studied in energy management systems (EMSs) for HEVs. First of all, we present a systemic assessment of long-term sophisticated cyber-attacks that aim to deteriorate the battery lifetime and energy efficiency of HEVs. Specifically, three levels of attack taxonomy according to the skill level of the attackers are considered, which are sophisticated and can hardly be detected by the human driver. In addition to levels 1 and 2 cyber-attacks that do not or partially require prior knowledge of the vehicle, we explore two other types of level 3 damage-oriented controller attacks made by highly-skilled attackers who have sufficient knowledge of the system. Such sophisticated attacks will potentially cause severe damages, such as decreasing battery capacity and energy by up to 50%. For a comprehensive vulnerability assessment, we propose innovative evaluation metrics to analyze the impact and stealthiness of sophisticated attacks. Finally, a preliminary probability-based detection method for sophisticated damage-oriented controller attacks is developed to improve the cyber-physical security of energy-efficient powertrain system in HEVs.**

***Index Terms*—Hybrid electric vehicles, Vehicle powertrain systems, Vehicle cyber-physical security, Vulnerability assessment, Sophisticated attacks.**

I. Introduction

CONNECTED electric vehicles have recently received increasing attention with the rapid growth of automobile communication technologies, including vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). In recent years, both the industry and academia have focused on developing advanced functionality and improving the overall driving performance, such as higher energy efficiency, added safety features, and enhanced comfortability [1], [2]. As the number and complexity of embedded electronic control units (ECUs) increase rapidly, a large number of ECUs need to communicate with each other via communication buses or with external cars or infrastructure via networks [3].

This communication will inevitably expand the attack surfaces and their ultimate impacts, such as disabling brakes, turning off headlights, taking over steering [4]–[6], and some real incidents, e.g., attacks on Cherokee Jeep [7] and Tesla [8]. In the public service announcement on 17 March 2016, the Federal Bureau of Investigation along with the Department of Transportation and the National Highway Traffic Safety Administration released the increasing vulnerability due to remote exploits of modern automobiles [9], wherein, the ways of accessing the vehicle networks and driver data were also discussed. Aware of the cybersecurity problem, the automotive industry has attempted to develop security standards, such as the Society of Automotive Engineers (SAE) J3061 [10], International Organization for Standardization (ISO) 26262 [11], and committee draft of the "ISO-SAE Road Vehicles - Cybersecurity Engineering" standard [12]. In academia, several surveys are available in the literature summarizing the updated works on vehicle cybersecurity. Specifically, the various threats that potentially compromise the vehicle networks are discussed in [9], [13]–[19]. To address the issue of vehicle cybersecurity, approaches from information technology and control perspectives are proposed to defend against the network attacks on vehicles. In general, the vehicle has two lines of defense against invaders. The first line of defense is information security that aims to prevent malicious attacks, e.g., secure hardware, secure communication techniques, firewall, secure software update, etc. In general, designing safer network architecture, powerful in-vehicle network firewall, and reliable hardware are the main consideration [13], [16], [17]. In [9], the authors illuminated a series of cybersecurity issues in CAVs (malware threats, on-board diagnostic (OBD) vulnerabilities, and automobile apps attacks) and demonstrated the defending mechanisms to them. Three main approaches were presented to protect or defend connected vehicles against cybersecurity threats, including over-the-air updates, cloud-based solutions to secure connected vehicles, and a layer-based solution [20]. In [21], the author discussed the typical methods that have been used to secure in-vehicle networks and their limitations. Several challenges in defending vehicles against malware were pointed out, and a cloud-assisted defense framework was proposed to protect the vehicle against malware. In [22], mitigation techniques for cyber-attacks on telematics and electric vehicle supply equipment, considering both physical and remote threats. Besides, approaches concerning message authentication and encryption, the firewall between external networks and vehicle devices, are also taken into consideration in [18].

Although these information-security approaches provide technical foundations and protections against malicious attacks,

Manuscript received XXX, 2020; revised XXX, 2020; accepted XXX, 2020; online XXX, 2020. This work was supported in part by the National Science Foundation under Grant ECCS-1946057. (*Corresponding author: Jin Ye.*)

L. Guo and J. Ye are with the Intelligent Power Electronics and Electric Machine Laboratory, University of Georgia, Athens, GA 30602, USA (e-mail: lulu.guo@uga.edu, jin.ye@uga.edu).

L. Du is with the Department of Electrical and Computer Engineering, Temple University, Philadelphia, PA 19122, USA (e-mail:ldu@temple.edu).

they alone cannot guarantee the security of the whole system. One critical issue needs to be addressed: once the car has been compromised, what should we do to assess, detect, and mitigate such attacks and ensure the normal operation of the ECUs? Therefore, cyber-physical security from the control perspective, including impact analysis [23], [24], attack detection and diagnosis [25], and resilient control [26], must be addressed by carmakers and researchers, which is considered as the second line of defense. However, from the control perspective, enhancing the cyber-physical security and resilience of ECUs is still a significant challenge, especially considering that ECUs in a vehicle usually come from different vendors, making it not feasible to design one security solution for the whole system. Another challenge is that real-world driving conditions of vehicles change massively, even in normal circumstances. In contrast, in other applications, e.g., power grids, the sensor data in regular situations vary within a certain range. The specific feature of varying working conditions in vehicles may lead to failures in cyber-attack identification. Therefore, cyber-physical security under various driving conditions needs to be concerned. Notice that from the perspective of hardware implementation of automotive control systems, all of the control systems are realized by using embedded ECUs, and sensor measurements, data processing, and control algorithms are integrated into a specific controller chip. Hence in the paper, "attack ECUs" is equivalent to attack the control system directly.

While there is an urgent need for studying cyber-physical security in HEVs, there is little work in this area. Due to increasing complexity in ECUs, most recent works focus only on one specific function or control system. For instance, literature [27] analyzed the impact of security attack (rear-end collision) on the connected adaptive cruise control and cooperative driving. In [28], [29], mitigation strategies were proposed to reduce accidents for vehicle platooning systems. Although the literature mainly focuses on cyber-attacks causing serious consequences/damages to vehicles, such as catastrophic multi-vehicle crashes, causing a life-threaten accident is not the only purpose of a malicious attacker. As one of the CIA (confidentiality, integrity, and availability) triad for carrying out risk assessments on cyber-physical security [30], [31], in confidentiality attacks, besides life-threaten objective, the possible reasons for cyber-attacks on modern vehicles include financial gain, collecting private information, and gaining priority access to infrastructure [5], [22]. Further, in recent work [32], the authors systematically analyzed cyber-attacks against electric vehicles. For clear expression, they divided the impacts into three categories: physical, strategic, and financial losses. The physical threat addresses safety-critical events such as loss of control, accident, and other physical attacks, which generally occur over short timescales. The strategic attacks aim at large-scale systems like local traffic congestion and multiple vehicle accidents. The cyber-attacks that address financial impacts assume to cause reduction of vehicle's monetary value.

While cyber-attacks on EMSs may not immediately cause physical damages, it will potentially result in severe degradation of battery capacity and energy efficiency [32], [33], reducing the vehicle's monetary value. For example, in [17], the author addressed that there is not much incentive to hack into a car to harm the passengers. The motivation of hackers is more likely to follow financial motivation. In [32], the impact of long-term cyberattacks on battery in EVs that aim to cause economic and strategic losses were analyzed. It demonstrated that attacks on EV subsystems, such as auxiliary components, can undoubtedly lead to the trivial effect of draining the battery, which could be up to 20% per hour and could deteriorate the performance over more extended periods. In [33], an efficiency-motivated attack against autonomous vehicular transportation was proposed, the results of which illustrated that this effect could be used to increase the energy expenditure of surrounding vehicles by 20% to 300%. In [34], for the cybersecurity issues of battery systems in EVs, a framework for analysis, comparison, and test of standards is presented by identifying the critical player in-vehicle cybersecurity. Similarly, considering cybersecurity vulnerabilities of the inter-vehicle network of EVs, cyber-attacks on electric drives can severely impact motor current signature and cause performance degradation [35], [36].

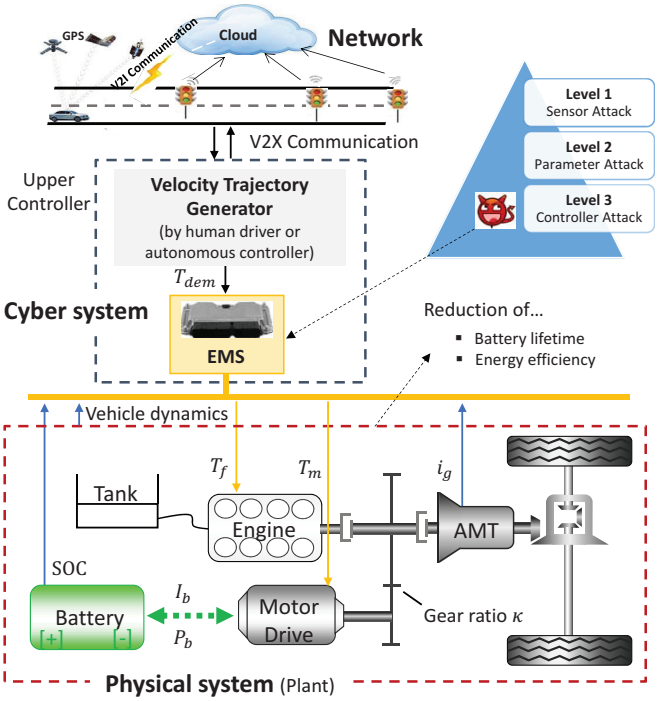


Fig. 1: System diagram of the HEVs, where AMT means automated mechanical transmission.

To the best of our knowledge, cyber-attacks, especially sophisticated and subtle cyber-attacks, have not yet been studied in EMSs for HEVs. In this paper, we present a systematic assessment of long-term sophisticated cyber-attacks that aim to deteriorate the battery lifetime and energy efficiency and propose a preliminary probability-based detection method for sophisticated damage-oriented controller attacks. The system structure of the HEVs is shown in Fig. 1. In the "cyber" part, the velocity trajectory is generated either by the human driver or the autonomous controller and provides the required acceleration to EMS. The physical plant, including engine, motor, converter, battery, and gearbox, is the "physical" part. The main focus of this paper is cyber-security of the energy-

efficient powertrain system, which is based on the background of a connected vehicle. Specifically, from the perspective of the second line of defense against invaders, we address the impact of cyber-attacks aiming to deteriorate the energy efficiency of the connected electric vehicle. Thus, the considered varied parameters are for the powertrain in the context of connected vehicles, not specific about information communicated with "other" vehicles. The main contributions of the paper are as follows:

- Three levels of attack taxonomy specific to EMSs in an HEV are proposed according to the skill level of the attackers, which are sophisticated and can hardly be detected by the human driver. Besides levels 1 and 2 that do not or partially require prior knowledge of the vehicle, we explore two other types of level 3 damage-oriented controller attacks made by highly-skilled attackers who have sufficient knowledge of the system.
- Innovative evaluation metrics are developed to analyze the impact and stealthiness of sophisticated attacks. With these metrics, we analyze the cyber-physical security of HEVs with transient and statistic results; assessment results can serve as guidelines for attack detection and countermeasures.
- The stealthiness of sophisticated attacks is evaluated, and a probability-based detection method is proposed for damage-oriented controller attacks to improve the cyber-physical security of energy-efficient powertrain system in HEVs.

The paper is organized as follows. In Section II, the vehicle modeling and EMS are described. Section III provides the attack modeling and statements, and section IV presents the innovative evaluation metrics and vulnerability assessment of the vehicle. In Section V, the sophisticated attacks are discussed, and a preliminary probability-based detection method for damage-oriented controller attacks is proposed. Finally, conclusions are given in Section VI.

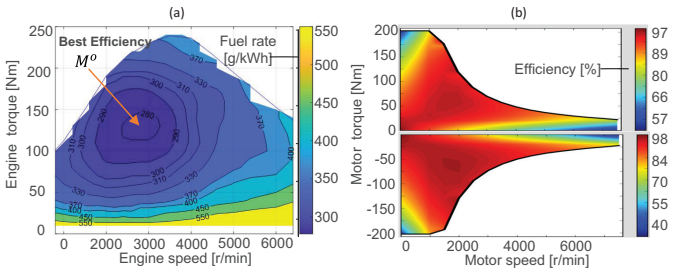


Fig. 2: Efficiency maps of the power sources, where (a) represents the fuel rate of the engine $\mathcal{M}(T_f, \omega_f)$ (g/kWh) and (b) represents the power efficiency of the motor $\eta(T_m, \omega_m)$.

II. Energy Management System

Given the acceleration of the vehicle, it is easy to derive the total torque required by the velocity trajectory generator using the longitudinal vehicle dynamics, as described in [37]. In response to the positive torque demand, we consider the constraint $T_f + \kappa T_m = T_{dem}$, where T_f and T_m represent the torques output from the engine and motor, respectively; T_{dem} denotes the total torque demand; and κ is the vehicle parameter determined by the construction. Then, the torque split ratio $\mathcal{R} = T_f/T_{dem}$ can be obtained by solving the optimization

$$\mathcal{R} = \arg \min_{0 \le \mathcal{R} \le \mathcal{R}_{max}} \mathcal{F}(T_f, \omega_f) + \lambda \mathcal{G}(T_m, \omega_m), \quad (1)$$

where λ represents the fuel-electricity coefficient; $\mathcal{R}_{max}$ is determined by the physical limits of the power sources as

$$\mathcal{R}_{max} = \min\{T_{f,max}/T_{dem}, 1 - \kappa T_{m,min}/T_{dem}\} \quad (2)$$

in which, $T_{f,max}$ is the maximum engine torque and $T_{m,min} < 0$ is the minimum motor torque; ω_f and ω_m (r/min) represent the engine and motor speed, respectively, which can be derived by the vehicle velocity v (m/s), gear ratio i_g of the transmission (corresponding to the gear position $i_{g,u}$), and tire radius r_w, as [38]

$$\omega_f = 60 i_g v/(2\pi r_w), \ \omega_f = \omega_m/\kappa, \quad (3)$$

where $60/2\pi$ is used to fulfill the relationship between the units r/min and m/s. In the above equations, $\mathcal{F}(T_f, \omega_f)$ (g/s) is the fuel rate of the engine, and $\mathcal{F}(T_f, \omega_f) = p_{eng}\mathcal{M}(T_f, \omega_f)T_f\omega_f$ on condition that the engine is well warmed up; $\mathcal{M}(T_f, \omega_f)$ (g/kWh) represents the fuel efficiency of the engine (see Fig. 2(a)) and p_{eng} is a constant to match the units; $\mathcal{G}(T_m, \omega_m)$ (kW) is the power consumption of the motor, expressed as

$$\mathcal{G}(T_m, \omega_m) = \begin{cases} p_{mot} T_m \omega_m \eta^{-1}(T_m, \omega_m), & T_m \ge 0 \\ p_{mot} T_m \omega_m \eta(T_m, \omega_m), & T_m < 0, \end{cases} \quad (4)$$

wherein $\eta(T_m, \omega_m)$ is the motor efficiency (see Fig. 2(b)), and p_{mot} is a constant for unit conversion.

III. Attack Taxonomy

A. Assumptions and statements

In the paper, we assume that the attacker can illegally access in-vehicle communication buses, arbitrarily modify the sensor measurements, and hijack the EMS. The ultimate objective is to reduce the battery lifetime and energy efficiency while satisfying the desired torque reference of the velocity trajectory generator. Several statements are as follows: (i) three kinds of threats are considered here: sensor, parameter, and controller attacks. In each case, the EMS satisfies the power demand of the upper controller to ensure the driving requirement. (ii) During being attacked, the operating points of the power sources meet the physical constraints, and the battery SOC is always in a reasonable range such that the EMS can keep working. (iii) The transmission control unit (TCU) may not be attacked because the damaged TCU would cause jerk and discomfort, which means that the control law in the TCU and its control command to the actuator would not be attacked. However, the gear information from the TCU, as a feedback signal of the EMS can be attacked, and the modified gear information will not influence the safety and functionality of the vehicle since it is feedback signal used in EMS rather than vehicle control unit. If the gear information is compromised by an attacker, the performance of EMS will degrade, causing higher energy consumption.

Besides, we denote the signal being attacked as $\{\cdot\}^{atk}$. All of the intensity of attacks are approximate for a fair comparison, and specifically, deviation of actual SOC and v is limited to $\pm 20\%$, and the variation of gear position is ± 1. Then, three levels of attack taxonomy specific to EMSs in HEVs are proposed according to the skill level of the attackers, which can hardly be detected by the human driver. Level 1 (sensor attacks) does not require the attacker to have prior knowledge of the EMS; level 2 (parameter attacks) requires attackers to have the partial knowledge; level 3 (controller attacks) requires attackers to have the sufficient knowledge.

B. Level 1: sensor attacks (Cases 1-4)

In the case of level 1, a malicious attacker can either physically or remotely gain access to the powertrain sensors and generate false signals to perform the attack. According to the EMS described above, the most dominating signals that might be attacked include vehicle speed v, gear position $i_{g,u}$ and revolution speeds of the engine and motor ($\tilde{\omega}_f$ and $\tilde{\omega}_m$, respectively). Due to the physical limits in the powertrain topology, two possible cooperate cyber-attacks are considered, as $\{\tilde{\omega}_f^{atk}, i_{g,u}, v^{atk}\}$ and $\{\tilde{\omega}_f^{atk}, i_{g,u}^{atk}, v\}$ ($\tilde{\omega}_m$ is always synchronized with $\tilde{\omega}_f$) while satisfying the relationship in (3).

C. Level 2: parameter attacks on battery SOC (Cases 5-11)

In the second level, the attackers can gain communication access on the internal controller area network and a certain estimator to modify the crucial parameters in EMS, e.g., SOC estimator in EMS or battery management system. In this paper, we present the cyber-attacks on SOC. The specific expressions of levels 1 and 2 are given in the Appendix A.

D. Level 3: damage-oriented controller attacks

Unlike sensor and parameter attacks, in level 3, the attacker can reprogram the EMS and inject harmful control inputs into the closed-loop system. The aim is to deteriorate the battery lifetime and energy efficiency without affecting the vehicle's dynamic performance. In this subsection, we provide a potential attack model causing maximum damage to the system. In real-world attack scenarios, the malicious attacker may hijack the microcontroller and rewrite the control law of EMS with more advanced algorithms, not by simply changing the parameter and sensor measurements in the EMS. The results of the designed controller attacks can help observe and evaluate the maximum impact of cyber-attacks in terms of energy efficiency and battery lifetime, which is necessary for further research on detection, diagnosis, and mitigation of cyber-attacks.

1) Energy efficiency-motivated attack (Case 12): The energy efficiency-motivated attack is performed by

$$\mathcal{R}^{atk} = \arg \max_{0 \le \mathcal{R} \le \mathcal{R}_{max}} \mathcal{F}(T_f, \omega_f) + \lambda_s (\mathrm{SOC}_{k+1} - \mathrm{SOC}_{init})^2 \tag{5}$$

subject to the dynamics $\mathscr{S}$: $\mathrm{SOC}_{k+1} = \mathrm{SOC}_k - (I_b/C_b)\Delta t$ to maximize the fuel consumption while satisfying the constraints $\mathrm{SOC} \in [\mathrm{SOC}_{min}, \mathrm{SOC}_{max}]$, where λ_s is the weighting factor; SOC_k and SOC_{k+1} denote the current and the next values of battery state of charge, respectively; SOC_{init} is the initial SOC; SOC_{min} and SOC_{max} represent the minimum and maximum safe values; Δt is the fixed time interval; C_b is the nominal battery capacity; $I_b = -\sqrt{V_{oc}^2 - 4R_bP_b}/(2R_bC_b)$ represents the current; V_{oc} is the battery open circuit voltage; R_b is the battery internal resistance; P_b is the battery power, which is determined by $P_b = \mathcal{G}(T_m, \omega_m)$.

2) Battery lifetime-motivated attack (Case 13): The battery life-motivated attack is orchestrated to cause reduction of battery capacity by solving the following optimization

$$\mathcal{R}^{atk} = \arg \max_{0 \le \mathcal{R} \le \mathcal{R}_{max}} \mathcal{H}(\cdot) + \lambda_{bat} (\mathrm{SOC}_{k+1} - \mathrm{SOC}_{init})^2 \tag{6}$$

subject to $\mathscr{S}$, where $\mathcal{H}(\cdot)$ means $\mathcal{H}(T_m, \omega_m, \mathrm{SOC})$, which reflects the transient battery health; λ_{bat} represents the weighting factor. Note that λ_s and λ_{bat} in the cost functions are different because they establish different equivalent relationships: (i) fuel consumption and SOC; (ii) battery health and SOC. Meanwhile, they should also be tuned according to the different variation range of $\mathcal{F}$ and $\mathcal{H}$.

Generally speaking, the rate of battery capacity loss is dictated by many factors, such as extreme temperature, high C-rate, high or low SOC, and excessive depth of discharge [39], [40]. For reliable lifetime predictions of lithium-ion batteries, models for cell degradation are developed in the literature. Among these battery models, calendar aging or cycle aging models are widely considered effective in evaluating battery health and lifetime degradation [41]–[43]. In [43], based on a reduced set of internal cell parameters and physically supported degradation functions, a comprehensive semi-empirical model approach for the capacity loss of lithium-ion batteries was presented. In this work, the temperature dependence of the cycle aging mechanisms was fully discussed, and the long-term tests validated the high prediction accuracy. However, despite the high accuracy, calendar aging models are often too complicated to design a real-time EMS algorithm. Therefore, in many research works focusing on EMS of HEVs, the complicated battery lifetime model is often replaced by an Ah-throughput model and other simplified formulations, see [40], [44]–[46]. Besides the complexity, since the EMS algorithm can only determine the output power or current of the battery, other factors like temperature are challenging to be considered in the optimization problem. Then, for a favorable compromise between simplicity and accuracy, Ah-throughput based model is often used to describe the main degradation mechanisms when designing a real-time EMS. Because the main focus of this paper is to develop a damage-oriented controller attack and evaluate its effect on the vehicle, we use the Ah-throughput battery model proposed in [40], [47], the parameters in which were fitted by using experimental data obtained from aging tests. Although the battery life model is not as realistic as the cycling aging model, we can observe the impact of cyber-attacks on the controller by comparing the results under normal and abnormal conditions; in both scenarios, the battery model is the same. The battery life under different conditions can be defined as Ah-throughput model: $\gamma = \int_0^{EOL} |I_b(t)| dt$, where EOL represents the battery lifetime under nominal conditions,

and $I_b(t)$ is the real-time battery current. By using the battery aging data calibrated from real-life tests, γ can be quantified by the fitting form

$$\gamma = \left[\frac{20}{(\alpha \cdot \text{SOC} + \beta) \exp(\frac{-31700+163.3I_c}{RT})} \right]^{\frac{1}{0.57}} \quad (7)$$

with α and β defined as follows: $\alpha = 1287.6$ for SOC ≤ 0.45 and else, $\alpha = 1385.5$; $\beta = 6356.3$ for SOC ≤ 0.45 and else, $\beta = 4193.2$. In the above equations, R is the gas constant; T represents the battery temperature expressed in Kelvin; and $I_c = I_b/C_b$ is determined by the battery current. Then, the index affecting the battery life depletion due to charge exchange is defined as

$$\mathcal{L}_{bat}(t) = \int_0^t \frac{\Gamma}{\gamma} |I_b(\tau)| d\tau, \quad (8)$$

where $\Gamma = \int_0^{EOL} |I_{nom}(t)| dt$ denotes the nominal battery life, and I_{nom} is the nominal current profile. In consequence, $\mathcal{L}_{bat}(0) = 0$ implies no capacity loss, and $\mathcal{L}_{bat}(t) = \Gamma$ means the end of battery life. Finally, we define

$$\mathcal{H}(T_m, \omega_m, \text{SOC}) = \frac{\Gamma}{\gamma} |I_b(t)| \quad (9)$$

to represent the relative aging effects, which can be considered a transient evaluation coefficient of battery health.

In fact, the damage-oriented optimization problem presented above is one-step-ahead predictive control, which has been widely used in literature [48]–[50]. The basic principle is that the control input is determined at each point in time so as to bring the system output at a one-step ahead future time instant (e.g., SOC_{k+1}) to a desired value. Because in the presented damage-oriented controllers, the dimension of the control input is only one (torque split ratio $\mathcal{R}$), we use a basic optimization method - enumeration method. As an example, the specific derivation of the solution of the optimization problem presented in (6) is given as follows: (i) Initialize the vehicle parameters and obtain the necessary system states and requirements, such as SOC, ω_m, ω_f, T_{dem}, etc. (ii) Calculate the boundary of the control input - $\mathcal{R}_{max}$ by (2), where $T_{f,max}$ and $T_{m,min}$ are determined by the current speeds and the maximum torque profiles of the engine and motors, respectively. (iii) Discretize the feasible region of $\mathcal{R}$ into N_{cal} segments. Then, given a fixed control input, denoted as $\mathcal{R}_i$, $i = 1, 2, ..., N_{cal}$, calculate the index $\mathcal{H}(T_m, \omega_m, \text{SOC})$ and SOC_{k+1} by using (7)-(9). The corresponding costs defined in (6) is J_i. (iv) Finally, the optimal solution of is obtained by $\mathcal{R}^{atk} = \arg\max J_i$. Similarly, the solution of the optimization problem (5) can be obtained.

To observe the extra computational burden required for this controller attack when applied in a real-time situation, we record the developed detector's computational time under the Urban Dynamometer Driving Schedule (UDDS) driving cycle. The simulation is run on an Intel(R) Core (TM) i7-9750 CPU (2.60GHz), and the computational time is obtained by using the CPU command in MATLAB. The computational time of the optimization problems in (5) and (6) are given in Fig. 3, wherein we set $N_{cal} = 25$. From the results, we can see that despite the basic enumeration method, the average computational burden is less than 10-15ms, which to some extent indicate the practicability in real-time driving condition. Notice that for the purpose of higher computational efficiency, one can also use advanced integration algorithms to solve the problem, for instance, Newton iteration [51], Sequential quadratic programming (SQP) [52], inner-point method [53], etc. Because the main focus of the paper is impact analysis of cyber-attacks, fast algorithms for real-time tests will not be further discussed.

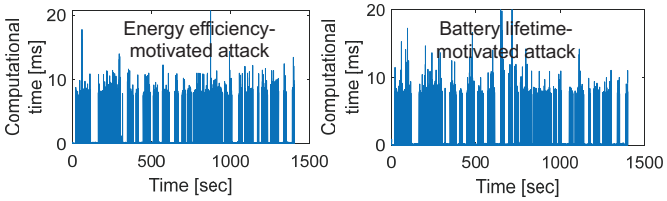


Fig. 3: Computational time of the optimization problems (5) and (6) under the UDDS driving cycle.

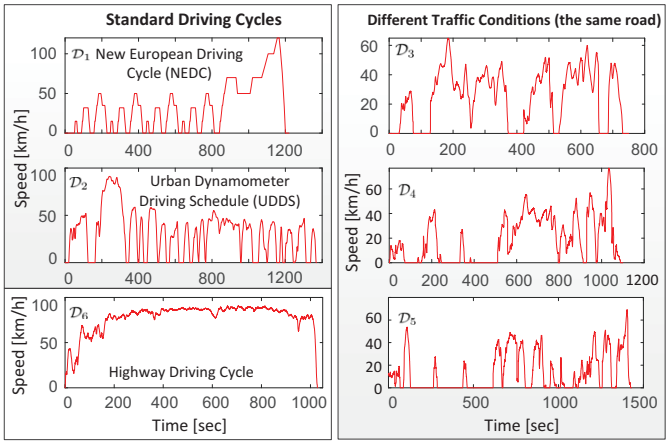


Fig. 4: Driving cycles under different roads conditions.

IV. Vulnerability Assessment

A. Innovative evaluation metrics

As stated above, these stealthy cyber-attacks are orchestrated to cause reduction of energy efficiency and battery lifetime while satisfying the basic dynamic performance. For objective comparison between different cyber-attacks under various driving conditions, we consider the influence of different initial and final SOCs. For example, when the final SOC is lower than others, the fuel consumption would decrease since more battery power electricity is used to drive the car. To reduce this impact, we introduce an artificial velocity profile after the terminal time of attacks, repeating the previous driving cycles until the SOC reaches its equilibrium. Suppose the driving cycle is $\mathcal{D}_i (i = 1, 2, ..., 6)$ as shown in Fig. 4. Then the time horizon of the attacked and artificial phases are $[t_i^{atk}, t_i^{atk} + T_{i,j}^{atk}]$ and $[t_i^{atk} + T_{i,j}^{atk}, t_i^{atk} + T_{i,j}^{atk} + T_{i,j}^{art}]$, respectively, where t_i^{atk} represents the starting time of attacks, and

$$T_{i,j}^{atk} = n_{i,j}^{atk} T_{di}, \; T_{i,j}^{art} = n_{i,j}^{art} T_{di} \quad (10)$$

with $n_{i,j}^{atk}, n_{i,j}^{art} \in \mathbb{N}$; $\{i,j\}$ representing the jth attack case under the ith driving cycle $\mathcal{D}_i$; and T_{di} represents the time of the driving cycle $\mathcal{D}_i$. Without loss of generality, it is assumed that $t_i^{atk} \equiv 0$. To mitigate the effect of the artificial velocity profile on the long-term attack results, there should be $n_{i,j}^{atk} \gg n_{i,j}^{art}$. This relationship is only suitable for scenarios that cyber-attacks have a long-term influence on the SOC, and in a short-period attack time, there is no obvious change in SOC. The mentioned equilibrium of SOC is defined as follows:

Proposition 1. *Assume that the SOC at $t = 0$ is $SOC(t) = SOC_0$, and after $m \in \mathbb{N}$ driving cycles, the initial and terminal SOCs of the mth driving cycle are $SOC_{m,init}$ and $SOC_{m,final}$. If $SOC_{m,init} \approx SOC_{m,final}$, then $SOC_{m,final}$ is defined as the equilibrium, which varies with the driving conditions.*

Based on the statement, the equilibrium under different driving conditions with attacks is defined as $\text{SOC}_{eqm,i,j}^{atk}$, the first m to reach the equilibrium as $m_{i,j}^{atk}$, and the equilibrium under normal conditions as $\text{SOC}_{eqm,i,j}^{nom}$.

It should be noted that the above discussion is actually on the basis that the SOC can reach a balanced position after several driving cycles despite the cyber-attacks, as discussed above. However, for those threats that have a significant influence on SOC in a short period, the system may not satisfy the relationship $\text{SOC}_{m,init} \approx \text{SOC}_{m,final}$ and no equilibrium is available. For instance, consider Cases 5 and 6 in Appendix A. If the SOC is mistakenly given as a high-level constant, then the EMS always tends to use the purely electric driving mode, giving rise to the much lower battery state without the possibility of recovery during attacks as shown in Fig. 5. Conversely, SOC would constantly increase until reaching its upper boundary. To address this issue, we use an intermittent strategy for these cyber-attacks, which means that, once SOC reaches the upper boundary, the attacker would withdraw the threats until it recovers to its normal value $\text{SOC}_{eqm,i,j}^{nom}$. Then, the time under attacks is set as $n_{i,j}^{atk} = 1$ and the recovery time with normal EMS is $n_{i,j}^{art} \geq n_{i,j}^{atk}$. In consequence, the attack period is

$$[(\xi - 1)T_{di} + (\xi - 1)T_{i,j}^{art}, \xi T_{di} + (\xi - 1)T_{i,j}^{art}], \tag{11}$$

where $\xi \in \mathbb{N}$ and $t_i^{atk} \equiv 0$ is used. For these intermittent cyber-attacks (Cases 5 and 6), we record results in several periods to establish the evaluation metrics.

In the following subsections, innovative evaluation metrics are proposed to emphasize the damage caused by the malicious behaviors in terms of system performance and requirements.

1) Energy consumption: To evaluate the average energy efficiency of the vehicle compared to normal EMS, the fuel consumption at timing t is expressed as

$$\boldsymbol{E}(t) = \int_0^t \mathcal{F}(T_f, \omega_f, \tau) d\tau, \tag{12}$$

which denotes the total energy cost during the driving cycles if SOC remains unchanged. Then, the evaluated metric that focuses on fuel consumption can be described as

$$\mathcal{I}_{eng,i,j} = \boldsymbol{E}_{i,j}^{atk} / \boldsymbol{E}_{i,j}^{nom}, \tag{13}$$

where $\boldsymbol{E}_{i,j}^{atk}$ represents the fuel consumption in the jth attack scenario under the ith driving cycle. For sustained attack cases, there is $\boldsymbol{E}_{i,j}^{atk} = \boldsymbol{E}(T_{i,j}^{atk} + T_{i,j}^{art})$, and for the intermittent attacks (Cases 5 and 6), we set $\boldsymbol{E}_{i,j}^{atk} = \boldsymbol{E}(\xi T_{di} + \xi T_{i,j}^{art})$. In both attack types, $\boldsymbol{E}_{i,j}^{nom}$ is determined by the total fuel consumption over the same time horizon with no cyber-attacks.

2) Energy efficiency: Subsequently, two indexes to reflect the efficiency are given by

$$\mathcal{I}_{eff,i,j}^{e}(t) = \frac{\mathcal{M}^o}{\mathcal{M}(T_f(t), \omega_f(t))} \leq 1, \tag{14}$$

$$\mathcal{I}_{eff,i,j}^{m}(t) = \eta(T_m(t), \omega_m(t)) \leq 1, \tag{15}$$

where $\mathcal{I}_{eff,i,j}^{e}$ represents the relative efficiency of the engine, and $\mathcal{I}_{eff,i,j}^{m}$ represents the efficiency of the motor. Here $\mathcal{M}^o$ is the best fuel efficiency of the engine (see Fig. 2(a)), which is used to normalize the engine efficiency. Then, the maximum value of $\mathcal{I}_{eff,i,j}^{e}$ is limited to 1, just as the same as $\mathcal{I}_{eff,i,j}^{m}$.

3) Battery lifetime: To evaluate the impact of the cyber-attacks on battery lifetime. In the long-term horizon formulation, we examine the relative capacity loss by

$$\mathcal{I}_{bat,i,j} = \mathcal{L}_{bat}^{atk} / \mathcal{L}_{bat}^{nom} \tag{16}$$

with $\mathcal{L}_{bat}^{atk}$ and $\mathcal{L}_{bat}^{nom}$ defined by (8). Similarly to the energy consumption metrics, for intermittent attacks, $\mathcal{L}_{bat}^{atk} = \mathcal{L}_{bat}(\xi T_{i,j}^{atk} + \xi T_{i,j}^{art})$, and in other cases, $\mathcal{L}_{bat}^{atk} = \mathcal{L}_{bat}(T_{i,j}^{atk} + T_{i,j}^{art})$. Also, the nominal results $\mathcal{I}_{bat,i,j}^{nom}$ are obtained under the same driving cycles with no cyber-attacks.

B. Simulation results and impact analysis

In this subsection, we present the evaluation results of the specified attack cases under multiple driving cycles, as shown in Fig. 4. Firstly, as many research works do, we choose two standard driving cycles in the automotive industry - New European Driving Cycle (NEDC) and UDDS, which are supposed to represent the typical usage of a car in Europe and the United States, respectively. Then, to cover more real-world driving conditions, we choose one highway driving cycle from a road test car, and three city driving cycles on the same road segment. The comparison between the results under different driving conditions can help obtain more robustness and convincing conclusions of vulnerability assessment for vehicles.

1) Observation of specific cases: For the sake of the detailed analysis of these cyber-attacks, we show the results of Cases 5, 6, 12 and 13 in Fig. 5, wherein $\mathcal{I}_{eng,2,5} = 1.0402$, $\mathcal{I}_{eng,2,6} = 1.0804$, $\mathcal{I}_{bat,2,5} = 1.1617$, $\mathcal{I}_{bat,2,6} = 0.8772$, $\mathcal{I}_{eng,2,12} = 1.4694$, $\mathcal{I}_{eng,2,13} = 1.0911$, $\mathcal{I}_{bat,2,12} = 1.0429$ and $\mathcal{I}_{bat,2,13} = 1.4897$. All of the cases are conducted under the same driving conditions, as UDDS. Among these figures, the upper curves show the results of two intermittent attacks (level 2: parameter attacks) with $\xi = 1|_{\text{Case5}}$ and $\xi = 3|_{\text{Case6}}$, which suggest that the attacks on SOC have a significant impact on battery and may even lead to radical changes in SOC and fuel consumption. These results can be expected because the EMS is highly sensitive to the mean values of SOC. For instance, once it is overwritten with a constant and low value, the system tends to use the engine-driven mode

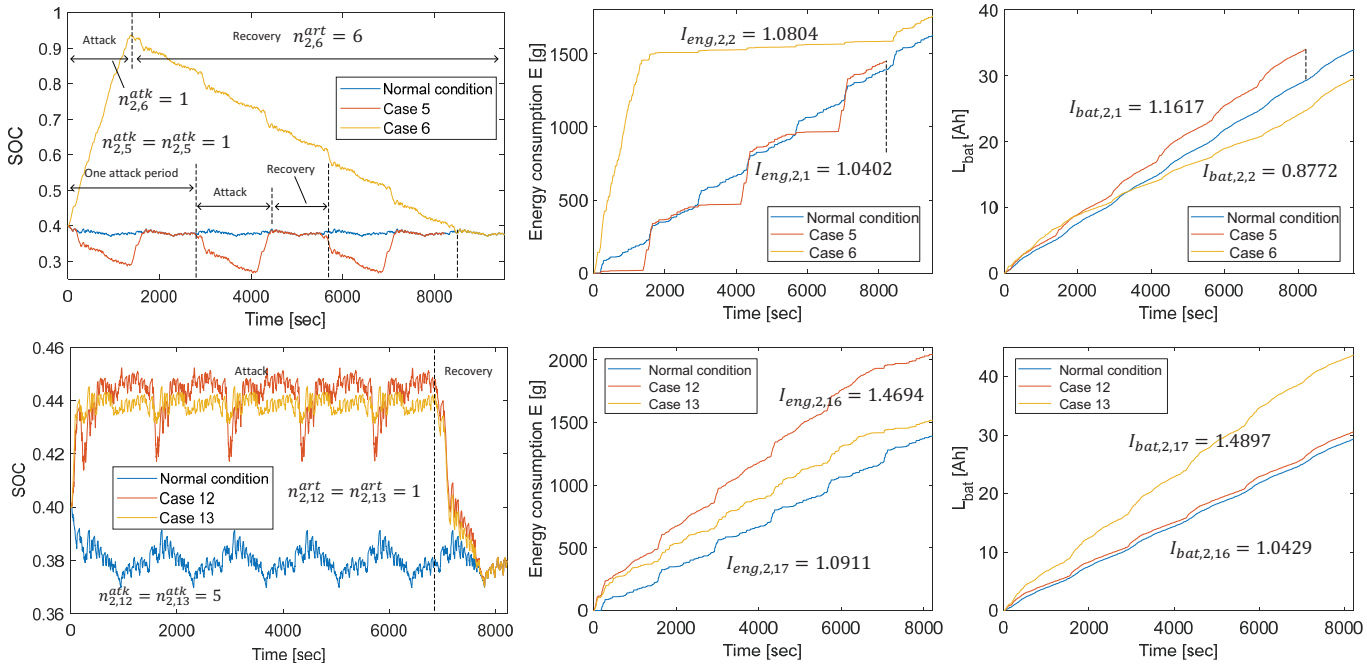


Fig. 5: Results of Cases 5, 6, 12 and 13 under UDDS.

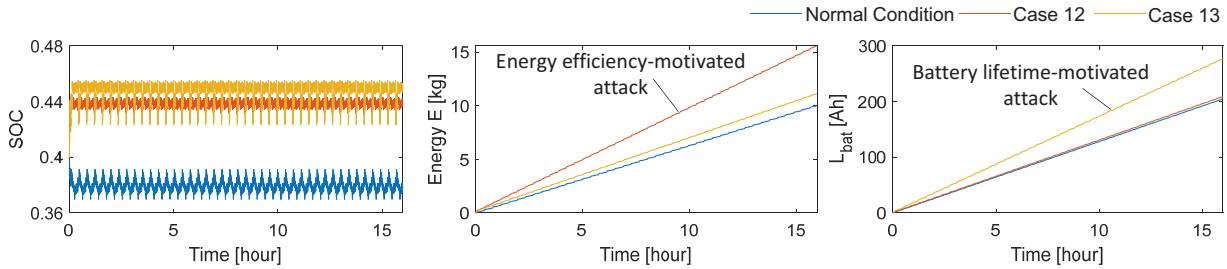


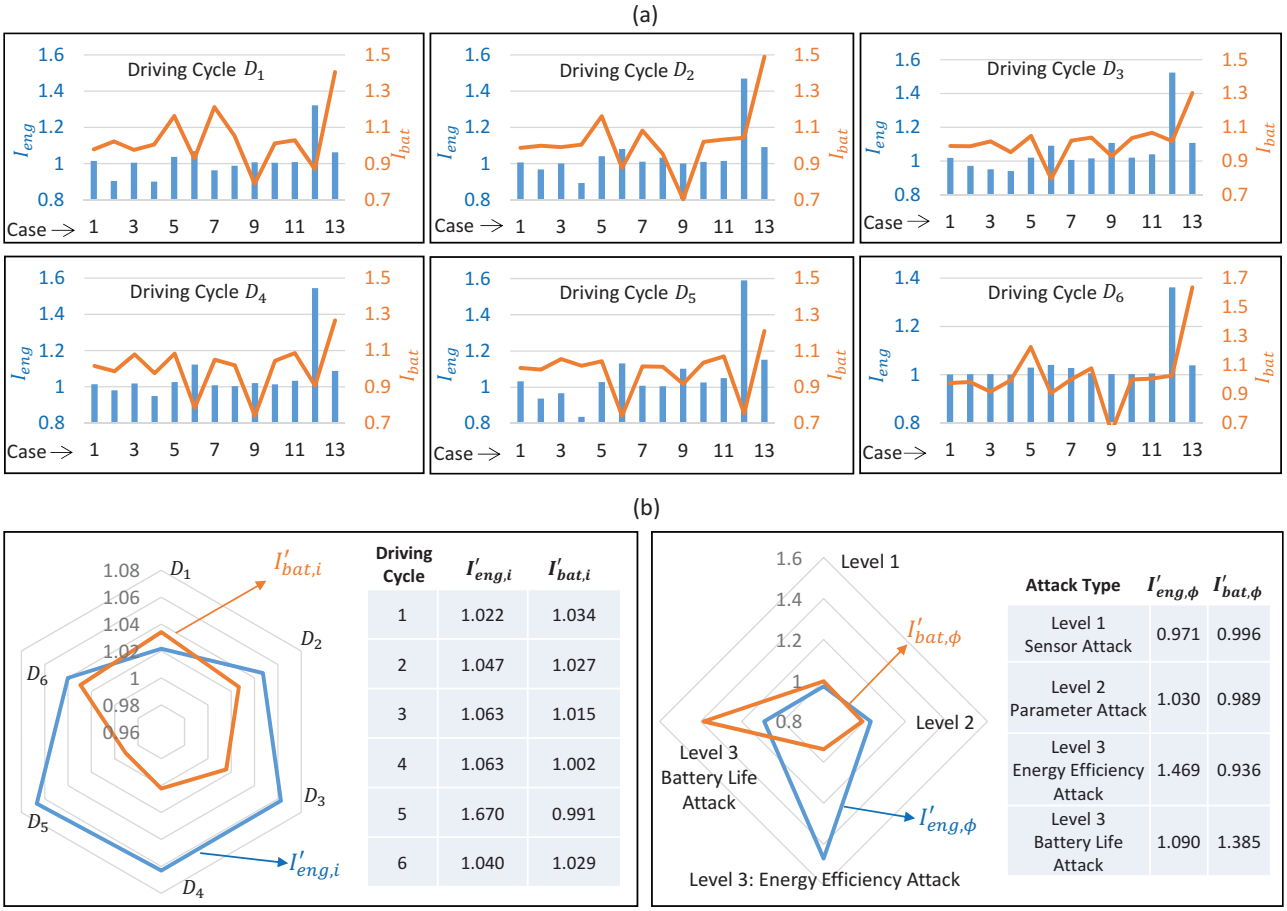
Fig. 6: Results of Cases 12 and 13 under long-term UDDS.

or even recharging mode (the engine supplies extra power to the generator) to control the vehicle. Then, accompanied by the increasing battery level, the fuels of the engine would be quickly consumed. We note that although the overall energy consumption increases in Case 6, the loss of battery capacity is reduced. This indicates that if the cyber-attacks are not orchestrated with the known system characteristics, performance degradation cannot always be realized. Another primary reason is that the battery capacity is not considered in the original (or normal) EMS. Therefore, from the viewpoint of optimization, some other torque split sequences, even though caused by cyber-attacks, may produce better results. Such a scenario is entirely possible in real engineering systems because most of the energy management strategies only focus on energy improvement without considering battery health.

From the results of controller attacks (level 3: Cases 12 and 13), it can be observed that the well-designed attacks may cause a significant drop in long-term performance (up to 50%) from both energy and battery capacity. Based on the comparison between the two SOC profiles, although the trends are similar, they exhibit different effects on energy efficiency and battery life. This implies that goal-oriented controller attacks are generally utilized to cause performance degradation of specific objectives while almost having no effect on other features, making it more challenging to detect the threats due to less effective observations.

In should be noted that the word "long-term cyber-attack" is defined relative to those safety-critical attacks. Typically, in a safety-critical attack, the attack period is second level or even millisecond level. In efficiency-motivated attacks, because the main aim is to degrade energy efficiency and battery health, the attack period will be much more extended, up to days or even months. For visible observation on the effect, we extended the UDDS driving cycle to 500km. The results are shown in Fig. 6, from which we can see that the effect of attacks will increase with time. Then, even though the attack may be detected during car maintenance, a significant drop in battery and energy efficiency may occur within the interval time.

2) Statistical results and impact analysis: Based on the massive results, the statistical graphs are given in Fig. 7(a). For comprehensive analysis of these impacts with different driving



Driving Cycle	$I'_{eng,i}$	$I'_{bat,i}$
1	1.022	1.034
2	1.047	1.027
3	1.063	1.015
4	1.063	1.002
5	1.670	0.991
6	1.040	1.029

Attack Type	$I'_{eng,\phi}$	$I'_{bat,\phi}$
Level 1 Sensor Attack	0.971	0.996
Level 2 Parameter Attack	1.030	0.989
Level 3 Energy Efficiency Attack	1.469	0.936
Level 3 Battery Life Attack	1.090	1.385

Fig. 7: Statistical graph of different attack cases.

cycles, these metrics are reformulated by

$$\mathcal{I}'_{eng,i} = \frac{1}{N_c}\sum_{j=1}^{N_c}\mathcal{I}_{eng,i},\ \mathcal{I}'_{bat,i} = \frac{1}{N_c}\sum_{j=1}^{N_c}\mathcal{I}_{bat,i}, \tag{17}$$

where $N_c = 13$ is the total cases in one driving cycles; $\mathcal{I}'_{eng,i}$ and $\mathcal{I}'_{bat,i}$ represent the average indexes values of the ith driving cycle. Similarly, we calculate the average values of metrics with respect to four attack types: level 1 sensor attack, level 2 parameter attack, level 3 energy efficiency-motivated attack, and level 3 battery life-motivated attack, marked as $\phi = \{1, 2, 3, 4\}$, respectively. Then, the corresponding indexes are

$$\mathcal{I}'_{eng,\phi} = \frac{1}{6(N_\phi - n_\phi + 1)}\sum_{i=1}^{6}\sum_{j=n_\phi}^{N_\phi}\mathcal{I}_{eng,i,j}, \tag{18}$$

$$\mathcal{I}'_{bat,\phi} = \frac{1}{6(N_\phi - n_\phi + 1)}\sum_{i=1}^{6}\sum_{j=n_\phi}^{N_\phi}\mathcal{I}_{bat,i,j}, \tag{19}$$

where $n_\phi = \{1, 5, 12, 13\}$ and $N_\phi = \{4, 11, 12, 13\}$; $\mathcal{I}'_{eng,\phi}$ and $\mathcal{I}'_{bat,\phi}$ represent the average metrics of the ϕth attack types. The results are shown in Fig. 7(b).

From the results, we can conclude that both the two sophisticated damage-oriented controller attacks (level 3) can heavily damage the system, leading to significant performance degradation up to 50%. Following the controller attacks, the impact of parameter attacks on SOC (level 2) is much lower, and generally speaking, the performance reduction is within 10-20% (see Fig 7(a)). Although these threats can lead to a sharp change in SOC, as shown in Fig. 5, the impacts are often attenuated by the later normal conditions, especially for the intermittent cases. On the one hand, it is because in the strategy of the EMS, the battery capacity is not considered, and thus the baseline is not satisfactory. On the other hand, despite the lower value of impact, cyber-attacks on system states and parameters also need to be considered because the cost of attacks on sensors is much lower than that of controller attacks. In controller attacks, malicious attackers must reprogram the EMS and inject harmful control inputs into the closed-loop system. Also, they require prior knowledge of the vehicle. In contrast, for cyber-attacks on sensors and parameters, they only need to conduct some typical attack types, such as denial of service (DoS) attack, replay attack, etc., without any vehicle knowledge, which will significantly reduce the cost of attacks. Based upon the comparison between different $\mathcal{I}'_{eng,i}$ in Fig. 7(b), it is apparent that the driving cycles can affect the results despite the same attack scenarios. Specifically, the overall impacts of driving cycles 3-5 are more significant than others, illustrating that lousy driving conditions may enhance the vulnerability to attacks. It should be noted that, although to some extent, we can deduce some conclusions

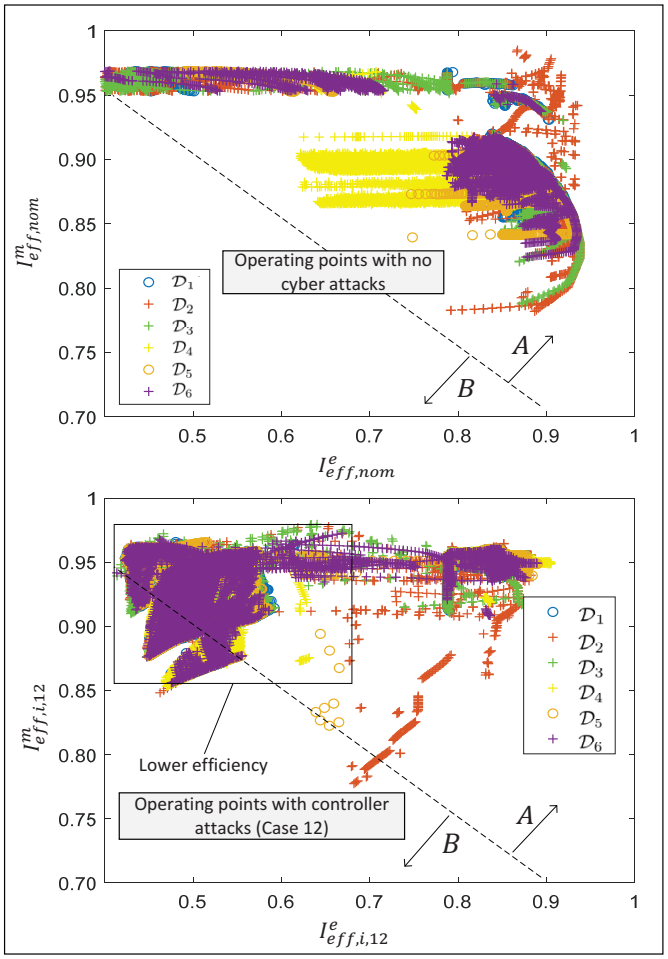


Fig. 8: Operating points under different conditions.

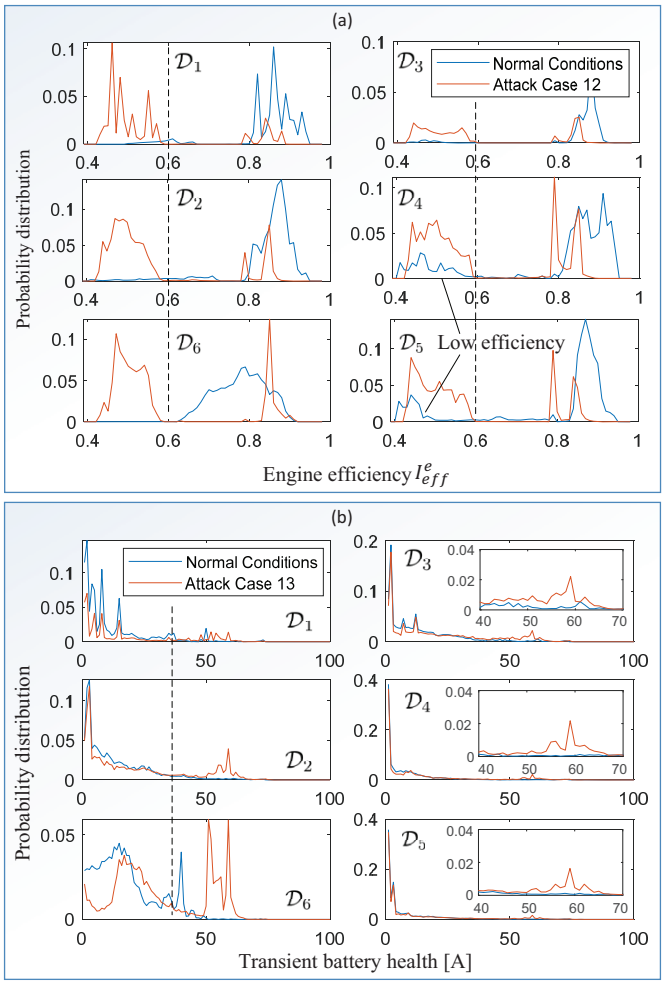


Fig. 9: Probability distribution of the engine efficiency and battery transient health under different driving cycles.

based on prior knowledge of vehicles, for example, attacks on efficiency and battery life have a significant impact on fuel consumption and battery health, we need to use the simulation results for quantitative analysis on the effect of attacks. From the above analysis, we believe that the simulation results in Fig. 7, including the radars in Fig. 7(b), are useful and necessary for research on a more comprehensive vulnerability analysis of cyber-attacks.

In the sensor attacks (level 1) on powertrain signals, it suggests that the designed EMS is not sensitive to the varying powertrain signals. In many scenarios, these sensor attacks may even result in better fuel efficiency. As discussed in the above subsection, it is because the EMS is not an optimal global result over the whole driving cycle, so a changed equilibrium point of SOC may be closer to the optimal profiles. It should be noted that the results reported in the graphs do not imply that the powertrain signal attacks have no influence on the energy and battery life of the vehicle when considering the limitation of attacks. Once this intensity is enlarged, the impact would be noticeable.

Concerning the cost of attacks, although long-term attacks are named continuous attacks, it does not mean that the attacker needs to perform the attacks consistently. For example, the malicious attacker may hijack the microcontroller and rewrite the control law by the elaborate algorithm. Then, after the invading action of the attacker, the compromised EMS would control the vehicle continuously over time without additional intervention. In such a case, only if the driver notices the compromised controller, it would continually influence vehicle performance. Besides real-time malware attacks during driving, a likelihood for malware to enter a vehicle is the case that the software update package is infected with malware before it is loaded onto a car. This way is possible because any repair shop and personnel can update ECU firmware through the Onboard Diagnostic (OBD) port. Several other scenarios where malware could exploit vulnerabilities to infect a vehicle were thoroughly discussed in [21]. If the controller efficiency- and battery lifetime-motivated attacks are performed through these ways, the cost of long-term attacks would not be so high compared to the negative and persistent effect.

V. Anomaly Detection

A. Stealthiness of attacks: attacks or bad driving conditions?

Due to the variable driving conditions in real-life applications, the operating points may be distributed throughout the various regions, leading to a wide range of energy efficiency. Therefore,

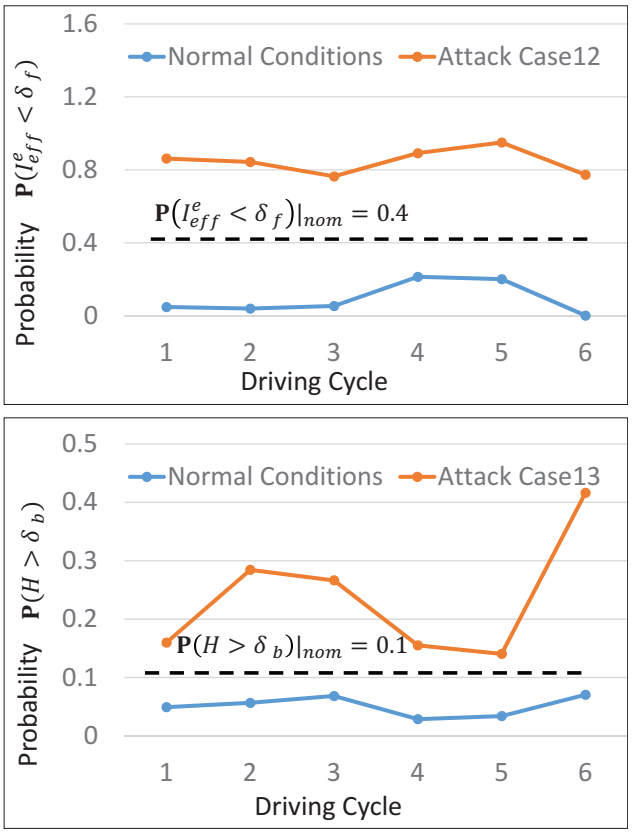


Fig. 10: Probability of the judgement conditions.

unlike the physical attacks described above, the threats targeted by an attacker who aims to cause energy efficiency reduction cannot be detected without considering the critical factor: the difference between malicious system modifications and regular operation in bad driving conditions (e.g., traffic jams, uphill, rough road, etc.) or unskilled driving behavior. To provide visible observation, we run the HEV with the designed EMS under different driving cycles from $\mathcal{D}_1$ to $\mathcal{D}_6$, and obtain the efficiency map of these operating points as shown in Fig. 8. As can be seen from the results, while different traveling conditions have a significant influence on energy efficiency, most of the operating points are located in area A. It illustrates that if the attacked points appear in B due to erroneous sensor measurements or controller algorithms, e.g., controller attack in Case 12, it is reasonable to conclude that the EMS probably has been attacked although the efficiency of the motor is higher, as shown in Fig. 8.

Unfortunately, this turns out not always the case. For example, the attacker may also utilize this conclusion to evade attack investigation by considering the constrains $\{\mathcal{I}^e_{eff,i,j}(t), \mathcal{I}^m_{eff,i,j}(t)\} \in \Omega_A,\ \forall t \in [t_i^{atk}, t_i^{atk} + T_{i,j}^{atk}]$ in the optimization (5), where Ω_A represents the set of operating points in area A. Moreover, an attacker is also motivated to exploit the illegitimate control in the EMS to realize lower efficiency, especially for the engine, as shown in the marked area in Fig. 8. Besides Case 12, those cyber-attacks launched to slightly falsify the signals may also lead to lower energy efficiency while ensuring most operating points in A.

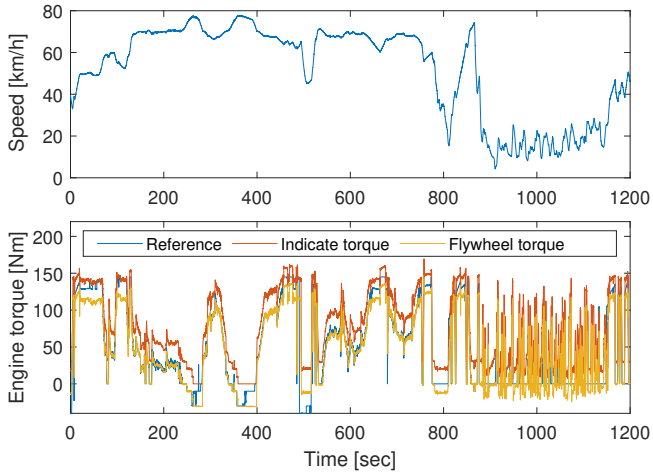


Fig. 11: Engine operations in road test.

Apparently, only exploiting the distribution area of the operating points is insufficient. To solve such a problem, we present a probability-based detection method to distinguish between subtle cyber-attacks and bad conditions, as an illustrative example, aiming at Cases 12 and 13.

B. Preliminary detection method using probability distribution

Fig. 9 shows the probability distribution of the efficiency metrics under different driving cycles. From the results, we can see that in normal conditions most engine efficiency is higher than a certain value (0.6 in the results), but it is not always the case, as illustrated in the probability distribution of $\mathcal{D}_3$ and $\mathcal{D}_4$, which represent jam urban traffics. We can also note that the probability of the engine efficiency within $[0.4, 0.6]$ shows significant distinction among these normal and attack profiles. Therefore, a probability-based method is introduced to detect this controller attacks, as follows:

Proposition 2. *Suppose the probability distribution of the engine efficiency index over the past time horizon can be known to the monitor, then we set the probability of the engine efficiency that less than* $\delta_f = 0.6$ *as* $\mathbf{P}(I^e_{eff} < \delta_f)$ *and the corresponding normal value as* $\mathbf{P}(I^e_{eff} < \delta_f)|_{nom}$. *If* $\mathbf{P}(I^e_{eff} < \delta_f) > \mathbf{P}(I^e_{eff} < \delta_f)|_{nom}$, *the system would be warned being attacked by energy efficiency-motivated attacks.*

Fig. 10(a) shows the $\mathbf{P}(I^e_{eff} < \delta_f)$ of Case 12 and normal conditions under different driving cycles. From the conspicuous distinction between the normal and attacked conditions, we can easily conclude that the proposed method is effective for identifying the cyber-attacks aiming at reducing energy efficiency. Similarly, one can alert the alarm of battery life-motivated attacks by using the criterion $\mathbf{P}(\mathcal{H} > \delta_b) > \mathbf{P}(\mathcal{H} > \delta_b)|_{nom}$, as shown in Fig. 9(b) and Fig. 10, where $\mathcal{H}$ represents the transient performance of battery health defined in (9) and $\delta_b = 40$A. To address the other factors that may also affect engine efficiency, such as engine cooling conditions, battery temperature, transmission temperature, etc., a few points should be noted as follows:

Firstly, the proposed probability-based detection method is a preliminary concept that is suitable for those subtle cyber-attacks causing significant degradation of energy and battery performance. The given threshold (0.6) serves as an example to show the results of detection. In real applications, the threshold parameters in the presented probability-based detection method, e.g., $\mathbf{P}(I^e_{eff} < \delta_f)|_{nom}$ and δ_f need to be extracted from a large number of real test data under normal cases. Although there have many other factors that may influence engine efficiency, their impact is within a reasonable bound in normal daily conditions. Besides, despite those uncertain factors, the primary engine efficiency is generally determined by the operation points of the engine, which are calculated by the EMS. Therefore, by using the road test data, we can obtain relatively reasonable bounds of results in normal conditions, based on which, the threshold can be defined.

Secondly, compared to those residual-based detection approaches with mean-value of residual, for instance, only using the value of engine efficiency to identify the presence of cyber-attacks, such as $I^e_{eff} < \delta_r$ (δ_r is the threshold), the concept of using the probability of low engine efficiencies have better robustness because it allows low efficiency caused by uncertain situations. This detection approach is based on the assumption that for a well-designed vehicle, the average performance in terms of the energy efficiency is stable.

Thirdly, in real applications, the torque used to derive the engine efficiency should be the indicate torque of the engine, instead of the flywheel torque. Actually, in the engine management system, besides the required torque reference from the EMS, the extra torque needed by other factors, such as air conditioning (for some vehicle models), are also considered. For example, as shown in Fig. 11, we present an engine torque profile in a road test collected from the engine management system in a passenger car. From the results, we can see that the actual indicate torque is always higher than flywheel torque and the torque reference from the EMS. The extra torque from the engine is used to drive the other equipment. Therefore, if we use the indicate torque of the engine to calculate the efficiency, to some extent, we have already considered several uncertain factors that may lead to "inefficient" engine operation.

Finally, based on the framework of probability-based detection methodology, further works need to be considered: adaptive threshold, cyber-attack detection with multiple identification indexes, physical-based and learning-based methods, etc. For example, besides the statistical method, one can use a physical-based method to determine an approximate range of δ_f. Based on the known nominal control logic and the necessary information in the past time horizon, e.g., speed, battery states, operations of engine and motor, and road information, the nominal range of efficiency can be obtained, which can help to determine an adaptive δ_f in real-time driving. In particular, for those cyber-attacks that slightly affect the vehicle, more signal data, such as speed profile, SOC, gear ratio of the transmission, battery current, battery voltage, etc., need to be used to distinguish between them cyber-attacks, faults, and various normal driving conditions.

VI. Conclusion

This paper has presented a systemic assessment of long-term sophisticated cyber-attacks that aim to deteriorate the battery lifetime and energy efficiency of an HEV, which can provide a general guide for cyber-threat impact analysis, detection and threat-resilient control for other crucial systems in connected vehicles, for instance, battery management system, eco-driving systems in automated vehicles (e.g., energy-efficient cruise control system), and other automotive controls that concentrate on energy savings. Three levels of attack taxonomy specific to EMSs according to the skill level of the attackers were proposed, which will potentially cause severe damages, such as decreasing battery capacity and energy by up to 50%, while being sophisticated and can hardly be detected by the human driver. To analyze the impact and stealthiness of the sophisticated attacks, we introduced innovative evaluation metrics, and finally, to improve the cyber-physical security of energy-efficient powertrain system in HEVs, we proposed and validated a preliminary probability-based detection method for damage-oriented controller attacks. It should be noted that besides the work of the second line of defense against cyber-attacks, the first line of defense - information security needs to be also considered to reduce the probability of cyber-attacks reaching the in-vehicle network. Collaborative efforts from both information and control security perspectives should be made in real-time applications, which may help develop cyber-security monitoring systems in vehicles.

Appendix A

The attacks in levels 1 and 2 are summarized in Table I. In Cases 5 and 6, intermittent attack strategy is used. In Cases 7 and 8, $\text{SOC}^{atk} = \mathbf{Y}$, where $\mathbf{Y}$ is the past SOC within a time horizon $[t - t^{atk}_{rpl}, t]$ (t represents the current time), In Cases 9-11, there is $\{\varepsilon, \nu\} = \{0.8, 0\}, \{1.2, 0\}, \{1, 0.1\}$, which represent Cases 9, 10 and 11, respectively.

TABLE I: Attack Modeling and Case Definition

Case definition		No.
Level 1	$v^{atk} = \mu v, \mu = \{0.8, 1.2\}$	1, 2
	$i^{atk}_g = i^{atk}_g + 1$ and $i^{atk}_g = i^{atk}_g - 1$	3, 4
Level 2	SOC$\equiv$ 0.5 and 0.3	5, 6
	$t^{atk}_{rpl} = \{5, 10\}$min	7, 8
	$\text{SOC}^{atk} = \varepsilon\text{SOC} + \nu$	9, 10, 11

References

[1] S. Haghbin, S. Lundmark, M. Alakula, and O. Carlson, "Grid-connected integrated battery chargers in vehicle applications: Review and new solution," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 2, pp. 459–473, 2012.

[2] R. Xiong, R. Yang, Z. Chen, W. Shen, and F. Sun, "Online fault diagnosis of external short circuit for lithium-ion battery pack," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 2, pp. 1081–1091, 2019.

[3] S. Chakraborty, M. A. Al Faruque, W. Chang, D. Goswami, M. Wolf, and Q. Zhu, "Automotive cyber–physical systems: A tutorial introduction," *IEEE Design & Test*, vol. 33, no. 4, pp. 92–108, 2016.

[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 *IEEE Symposium on Security and Privacy*, 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 *USENIX Security Symposium*, vol. 4, 2011, pp. 447–462.

[6] L. Guo, B. Yang, J. Ye, H. Chen, F. Li, W.-Z. Song, L. Du, and L. Guan, "Systematic assessment of cyber-physical security of energy management system for connected and automated electric vehicles," *IEEE Transactions on Industrial Informatics*, 2020.

[7] A. Greenburg, "Hackers remotely kill a Jeep on the highway - with me in it," [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/, Tech. Rep., Jul. 2015.

[8] "Cyber attacks in connected cars: what Tesla did differently to win," [Online]. Available: https://www.appknox.com/blog/cyber-attacks-in-connected-cars, Tech. Rep., Sep. 2017.

[9] 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.

[10] "Vehicle electrical system security committee: SAE J3061 cybersecurity guidebook for cyber-physical automotive systems," SAE, Tech. Rep., 2016.

[11] "International organization for standardization: ISO 26262 road vehicles functional safety part 1–10. technical report, international organization for standardization," ISO, Tech. Rep., 2011.

[12] C. Schmittner and G. Macher, "Automotive cybersecurity standards-relation and overview," in *International Conference on Computer Safety, Reliability, and Security*. Springer, 2019, pp. 153–165.

[13] G. K. Rajbahadur, A. J. Malton, A. Walenstein, and A. E. Hassan, "A survey of anomaly detection for connected vehicle cybersecurity and safety," in *IEEE Intelligent Vehicles Symposium (IV)*, 2018, pp. 421–426.

[14] J. Liu, S. Zhang, W. Sun, and Y. Shi, "In-vehicle network attacks and countermeasures: Challenges and future directions," *IEEE Network*, vol. 31, no. 5, pp. 50–58, 2017.

[15] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546–556, 2015.

[16] C. Miller and C. Valasek, "A survey of remote automotive attack surfaces," *black hat USA*, vol. 2014, p. 94, 2014.

[17] A. Weimerskirch and R. Gaynier, "An overview of automotive cybersecurity: Challenges and solution approaches." in *TrustED@ CCS*, 2015, p. 53.

[18] 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.

[19] S. Abbott-McCune and L. A. Shay, "Intrusion prevention system of automotive network can bus," in *IEEE International Carnahan Conference on Security Technology (ICCST)*, 2016, pp. 1–8.

[20] "Cybersecurity best practices for modern vehicles," National Highway Traffic Safety Administration. Report No. DOT HS 812 333., Tech. Rep., 2016.

[21] 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.

[22] C. Hodge, K. Hauck, S. Gupta, and J. C. Bennett, "Vehicle cybersecurity threats and mitigation approaches," National Renewable Energy Lab.(NREL), Golden, CO (United States), Tech. Rep., 2019.

[23] R. van der Heijden, T. Lukaseder, and F. Kargl, "Analyzing attacks on cooperative adaptive cruise control (CACC)," in *IEEE Vehicular Networking Conference (VNC)*, 2017, pp. 45–52.

[24] P. Johannessen, F. Törner, and J. Torin, "Actuator based hazard analysis for safety critical systems," in *International Conference on Computer Safety, Reliability, and Security*. Springer, 2004, pp. 130–141.

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

[26] 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.

[27] M. Amoozadeh, A. Raghuramu, C.-N. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 126–132, 2015.

[28] I. Sajjad, D. D. Dunn, R. Sharma, and R. Gerdes, "Attack mitigation in adversarial platooning using detection-based sliding mode control," in *ACM Cyber-Physical Systems-Security and/or PrivaCy*, 2015, pp. 43–53.

[29] A. Ferdowsi, S. Ali, W. Saad, and N. B. Mandayam, "Cyber-physical security and safety of autonomous connected vehicles: optimal control meets multi-armed bandit learning," *IEEE Transactions on Communications*, vol. 67, no. 10, pp. 7228–7244, 2019.

[30] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, 2015.

[31] M. Aminzade, "Confidentiality, integrity and availability–finding a balanced it framework," *Network Security*, vol. 2018, no. 5, pp. 9–11, 2018.

[32] S. Sripad, S. Kulandaivel, V. Pande, V. Sekar, and V. Viswanathan, "Vulnerabilities of electric vehicle battery packs to cyberattacks," *arXiv preprint arXiv:1711.04822*, 2017.

[33] R. M. Gerdes, C. Winstead, and K. Heaslip, "CPS: an efficiency-motivated attack against autonomous vehicular transportation," in *ACM Computer Security Applications Conference*, 2013, pp. 99–108.

[34] A. Khalid, A. Sundararajan, A. Hernandez, and A. I. Sarwat, "Facts approach to address cybersecurity issues in electric vehicle battery systems," in *Technology & Engineering Management Conference (TEMSCON)*. IEEE, 2019, pp. 1–6.

[35] B. Yang, L. Guo, F. Li, J. Ye, and W. Song, "Vulnerability assessments of electric drive systems due to sensor data integrity attacks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 5, pp. 3301–3310, 2019.

[36] ——, "Impact analysis of data integrity attacks on power electronics and electric drives," in *IEEE Transportation Electrification Conference and Expo (ITEC)*, 2019, pp. 1–6.

[37] H. Chen, L. Guo, H. Ding, Y. Li, and B. Gao, "Real-time predictive cruise control for eco-driving taking into account traffic constraints," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 8, pp. 2858–2868, 2018.

[38] D. Crolla and B. Mashadi, *Vehicle powertrain systems*. John Wiley & Sons, 2011.

[39] J. Wang, P. Liu, J. Hicks-Garner, E. Sherman, S. Soukiazian, M. Verbrugge, H. Tataria, J. Musser, and P. Finamore, "Cycle-life model for graphite-LiFePO4 cells," *Journal of power sources*, vol. 196, no. 8, pp. 3942–3948, 2011.

[40] L. Tang, G. Rizzoni, and S. Onori, "Energy management strategy for HEVs including battery life optimization," *IEEE Transactions on Transportation Electrification*, vol. 1, no. 3, pp. 211–222, 2015.

[41] J. Schmalstieg, S. Käbitz, M. Ecker, and D. U. Sauer, "A holistic aging model for Li (NiMnCo) O2 based 18650 lithium-ion batteries," *Journal of Power Sources*, vol. 257, pp. 325–334, 2014.

[42] E. Sarasketa-Zabala, E. Martinez-Laserna, M. Berecibar, I. Gandiaga, L. Rodriguez-Martinez, and I. Villarreal, "Realistic lifetime prediction approach for Li-ion batteries," *Applied energy*, vol. 162, pp. 839–852, 2016.

[43] M. Schimpe, M. E. von Kuepach, M. Naumann, H. C. Hesse, K. Smith, and A. Jossen, "Comprehensive modeling of temperature-dependent degradation mechanisms in lithium iron phosphate batteries," *Journal of The Electrochemical Society*, vol. 165, no. 2, p. A181, 2018.

[44] F. Martel, Y. Dubé, S. Kelouwani, J. Jaguemont, and K. Agbossou, "Long-term assessment of economic plug-in hybrid electric vehicle battery lifetime degradation management through near optimal fuel cell load sharing," *Journal of Power Sources*, vol. 318, pp. 270–282, 2016.

[45] L. Serrao, S. Onori, A. Sciarretta, Y. Guezennec, and G. Rizzoni, "Optimal energy management of hybrid electric vehicles including battery aging," in *IEEE American control conference*, 2011, pp. 2125–2130.

[46] T. M. Padovani, M. Debert, G. Colin, and Y. Chamaillard, "Optimal energy management strategy including battery health through thermal management for hybrid vehicles," *IFAC Proceedings Volumes*, vol. 46, no. 21, pp. 384–389, 2013.

[47] S. Onori, P. Spagnol, V. Marano, Y. Guezennec, and G. Rizzoni, "A new life estimation method for lithium-ion batteries in plug-in hybrid electric vehicles applications," *International Journal of Power Electronics*, vol. 4, no. 3, pp. 302–319, 2012.

[48] C. Kambhampati, J. Mason, and K. Warwick, "A stable one-step-ahead predictive control of non-linear systems," *Automatica*, vol. 36, no. 4, pp. 485–495, 2000.

[49] G. K. Venayagamoorthy, K. Rohrig, and I. Erlich, "One step ahead: short-term wind power forecasting and intelligent predictive control based on data analytics," *IEEE Power and Energy Magazine*, vol. 10, no. 5, pp. 70–78, 2012.

[50] G. C. Goodwin and K. S. Sin, *Adaptive filtering prediction and control*. Courier Corporation, 2014.
[51] J. F. Traub and H. Woźniakowski, "Convergence and complexity of newton iteration for operator equations," *Journal of the ACM (JACM)*, vol. 26, no. 2, pp. 250–258, 1979.
[52] P. T. Boggs and J. W. Tolle, "Sequential quadratic programming," *Acta numerica*, vol. 4, no. 1, pp. 1–51, 1995.
[53] D. Yang, J. Wen, K. Chan, and G. Cai, "Dispatching of wind/battery energy storage hybrid systems using inner point method-based model predictive control," *Energies*, vol. 9, no. 8, p. 629, 2016.

Lulu Guo received the B.S. degree in vehicle engineering and the Ph.D. degree in control engineering from Jilin University, Changchun, China, in 2014 and 2019, respectively.

He is currently a Postdoctoral Research Associate with the University of Georgia, Athens, GA, USA. His current research interests include advanced vehicle control, energy management, and vehicle cybersecurity.

Jin Ye (S'13-M'14-SM'16) received the B.S. and M.S. degrees in electrical engineering from Xi'an Jiaotong University, Xi'an, China, in 2008 and 2011, respectively, and the Ph.D. degree in electrical engineering from McMaster University, Hamilton, ON, Canada, in 2014.

She is currently an Assistant Professor of electrical engineering and the Director of the Intelligent Power Electronics and Electric Machines Laboratory, University of Georgia, Athens, GA, USA. Her current research interests include power electronics, electric machines, energy management systems, smart grids, electrified transportation, and cyber-physical systems.

Dr. Jin Ye is the General Chair of 2019 IEEE Transportation Electrification Conference and Expo (ITEC), and the Publication Chair and Women in Engineering Chair of 2019 IEEE Energy Conversion Congress and Expo (ECCE). She is an Associate Editor for IEEE TRANSACTIONS ON POWER ELECTRONICS, IEEE OPEN JOURNAL OF POWER ELECTRONICS, IEEE TRANSACTIONS ON TRANSPORTATION ELECTRIFICATION, and IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY.

Liang Du (S'09–M'13–SM'18) received the Ph.D. degree in electrical engineering from Georgia Institute of Technology, Atlanta, GA in 2013.

He was a Research Intern at Eaton Corp. Innovation Center (Milwaukee, WI), Mitsubishi Electric Research Labs (Cambridge, MA), and Philips Research N.A. (Briarcliff Manor, NY) in 2011, 2012, and 2013, respectively. He was also an Electrical Engineer with Schlumberger, Sugar Land, TX, from 2013 to 2017. He is currently an Assistant Professor with Temple University, Philadelphia.

Dr. Du received the Ralph E. Powe Junior Faculty Enhancement Award from ORAU in 2018 and currently serve as an associate editor for IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS and IEEE TRANSACTIONS ON TRANSPORTATION ELECTRIFICATION.