Impact Analysis of Data Integrity Attacks on Power Electronics and Electric Drives

Bowen Yang, Lulu Guo, Fangyu Li, Jin Ye, Wenzhan Song
Center for Cyber-Physical Systems
University of Georgia
Athens, Georgia USA
Email: {bowen.yang, lulu.guo, fangyu.li, jin.ye, wsong}@uga.edu

***Abstract*—In this paper, the impact of various data integrity attacks on electric drive systems of electric vehicles is analyzed. The cyber-physical models of power electronics and electric drives are firstly proposed to investigate the interaction between physical systems and cyber systems. Then, a few predefined performance metrics are introduced, which are needed to evaluate the impact of data integrity attacks on power electronics and electric drives. The simulation is conducted to quantitatively analyze the impact under different attack scenarios. Simulation results show that the metrics are greatly impacted by data integrity attacks and have obvious features different from the ones under healthy conditions. For example, the current distortion could be increased by over 70% by maliciously reducing the current feedback signal to 10% of the original value and the torque ripple could be increased up to 300% of the healthy value by similar attacks.**

***Index Terms*—data integrity attack, electric drive, power electronics, impact analysis**

I. Introduction

The development of internet of things (IoT) enabled intelligent transportation systems and automated vehicles are becoming more vulnerable to cyber and physical threats, especially for automated and connected electric vehicles (EVs) due to the direct connection with battery charging infrastructure, more centralized control architecture and higher electrification. While with the increasing number of EVs and the definite schedules of replacing traditional internal combustion engine vehicles with electric and hybrid electric vehicles, the security challenge have not yet fully explored, which would lead to devastating consequences if not detected in the early stage. Recently, some preliminary works on electric vehicle charging cyber security have been published, such as [1]–[5]. However, none of them investigates the impacts of cyber attacks on power electronics and electric drive systems (EDSs).

Due to the increased cyber threats on physical systems, cyber physical systems (CPS) models have been developed to investigate the interaction between physical systems and cyber systems in smart grids [6]–[8], which can then be used to assess the operational reliability and vulnerability, the transient angle and voltage stability, and the frequency and electricity market operation due to cyber attacks [9]. The impact of cyber attacks on control systems of solar inverter and energy storage are also analyzed in the Monte-Carlo simulation to evaluate microgrid cyber security risks [10]. Although crucial insights on the interaction between control system (cyber system) and physical microgrid are emphasized in these works based on operational cost analysis of microgrids, some other important performance metrics (e.g., power quality, torque ripples, etc.) have not been addressed, particularly of power electronics and electric drives. To our best knowledge, to date, no CPS model has been developed for power electronics and electric drives in EVs, which illustrates the need to explore the impacts of cyber attacks on EDSs, as well as the overall vehicle performance.

Our research is partially sponsored by NSF-ECCS-1725636.

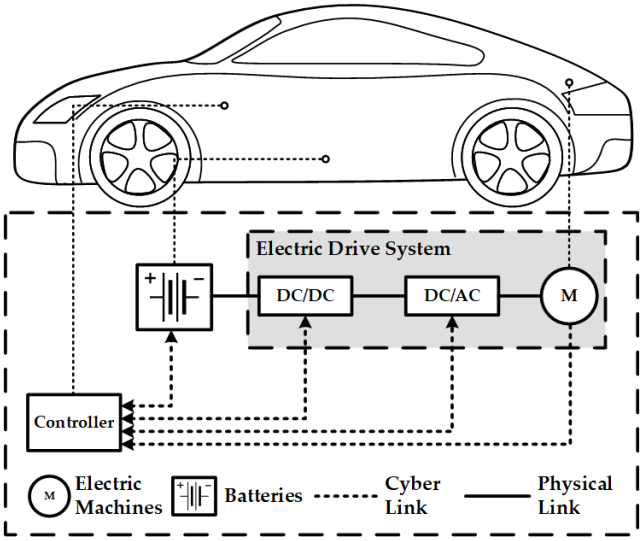

Fig. 1: Electric vehicle system.

In this paper, a CPS model of EDSs in an EV is introduced, and on the basis, the impact of various data integrity attacks is analyzed. The paper is organized as follows. In section II, the CPS model of EDSs in an EV is presented. In section III, several potential cyber attacks are classified and analyzed. The simulation and evaluation results of data integrity attacks are provided to verify the former discussion in section IV, and finally, conclusion and future work are given in section V.

II. Cyber physical system model of EDSs

As shown in Fig. 1, the EDS of an EV consists of batteries, power electronics, electric machines and controllers, wherein, the controllers (including sensors and actuators) are the main source of gathering information, computing and

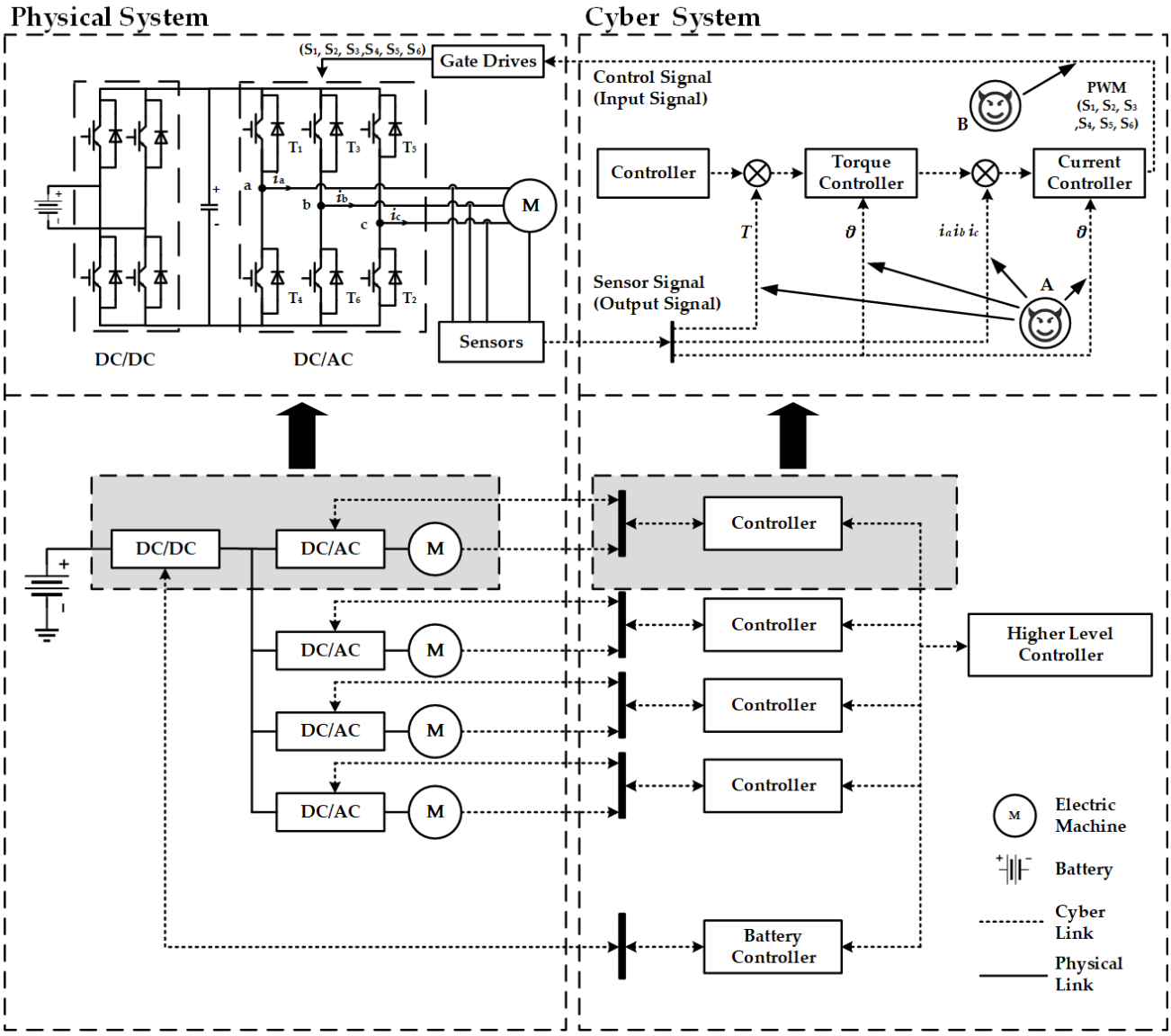

Fig. 2: CPS model of an EDS.

generating the control signals. Meanwhile, it also takes charge of communicating with other devices, facilities and higher level control centers. Therefore, the controllers are considered vulnerable to cyber attacks. Once the controllers in the diagram are compromised, many critical systems like batteries and drives will be impacted and are most likely to be damaged if not detected in the early stage. More details are shown in Fig. 2, which presents the physical and cyber model of the EV drive system. In order to quantitatively analyze the impact on EDS, detailed mathematical model of the electric machine and controller (Cyber System) are discussed as follows.

A. Electric machine

As interior permanent magnet synchronous machine (IPM) is widely used in applications of Electric Vehicles for its smooth torque production, high efficiency and high power density, it is adopted in the work as a demonstration. Under the traditional three-phase stationary reference frame, the electrical relationships of IPM could be described as

$$\begin{bmatrix} \Lambda_a \\ \Lambda_b \\ \Lambda_c \\ \Lambda_f \end{bmatrix} = \begin{bmatrix} L_{aa} & L_{ab} & L_{ac} & L_{af} \\ L_{ba} & L_{bb} & L_{bc} & L_{bf} \\ L_{ca} & L_{cb} & L_{cc} & L_{cf} \\ L_{fa} & L_{fb} & L_{fc} & L_{ff} \end{bmatrix} \begin{bmatrix} i_a \\ i_b \\ i_c \\ i_f \end{bmatrix}, \quad (1)$$

$$\begin{bmatrix} v_a \\ v_b \\ v_c \\ v_f \end{bmatrix} = \begin{bmatrix} R_a & 0 & 0 & 0 \\ 0 & R_b & 0 & 0 \\ 0 & 0 & R_c & 0 \\ 0 & 0 & 0 & R_f \end{bmatrix} \begin{bmatrix} i_a \\ i_b \\ i_c \\ i_f \end{bmatrix} + \frac{d}{dt} \begin{bmatrix} \Lambda_a \\ \Lambda_b \\ \Lambda_c \\ \Lambda_f \end{bmatrix}, \quad (2)$$

where Λ_x, i_x, v_x, and R_x $(x = a, b, c)$ are the flux linkage, phase current, phase voltage and winding resistance of each phase; L_{xy} $(x, y = a, b, c)$ is the inductance of and between

each phase. As the rotor of IPM is mounted with permanent magnet instead of windings, $\Lambda_f = \Lambda_{pm}$ is the flux linkage produced by the magnet, and v_f, i_f, R_f are the equivalent excitation voltage, current and resistance, respectively; L_{fx} and L_{xf} $(x = a, b, c)$ reflect the flux linkage in each phase provided by the rotor magnet.

To simplify the analyzing process, Direct-Quadrant-Zero (DQZ) Transformation is adopted to transfer the AC variables in the stator stationary reference frame to the DC variables in the rotating d-q axis reference frame. The transformation is achieved by multiplying the original vectors with the Park Matrix, expressed as

$$\mathbf{S_{dq0}} = \mathbf{P} \cdot \mathbf{S_{abc}}, \tag{3}$$

where $\mathbf{S_{dq0}} = [S_d, S_q, S_0]^T$ is the transformed variables in the d-q axis reference frame, $\mathbf{S_{abc}} = [S_a, S_b, S_c]^T$ is the original variables in the stator reference frame, and the Park transformation matrix is defined as

$$\mathbf{P} = \frac{2}{3}\begin{bmatrix} \cos(\theta_r) & \cos(\theta_r - \nu) & \cos(\theta_r + \nu) \\ -\sin(\theta_r) & -\sin(\theta_r - \nu) & -\sin(\theta_r + \nu) \\ 1/2 & 1/2 & 1/2 \end{bmatrix},$$

where $\nu = 120°$. Then, the electric machine model can be described as follows:

1) Flux Linkage:

$$\begin{cases} \Lambda_d = L_d i_d + \Lambda_{pm} \\ \Lambda_q = L_q i_q \end{cases} \tag{4}$$

2) Voltage:

$$\begin{cases} v_d = R_s i_d + L_d \frac{di_d}{dt} - \omega_e L_q i_q \\ v_q = R_s i_q + L_q \frac{di_q}{dt} + \omega_e L_d i_d + \omega_e \Lambda_{pm} \end{cases} \tag{5}$$

3) Torque:

$$T_e = \frac{3}{2} p[\Lambda_{pm} i_q + (L_d - L_q) i_d i_q], \tag{6}$$

where L_d and L_q are the inductance of d-axis and q-axis, respectively; ω_e is the electrical angular speed; p is number of pole pairs; and R_s is the equivalent winding resistance in the d-q axis reference frame. It should be pointed out that when the stator winding is connected in 'Y' model, the zero component will always be 0, as suggested by Kirchhoffs Law. That is why the zero component is not included in the DQZ model.

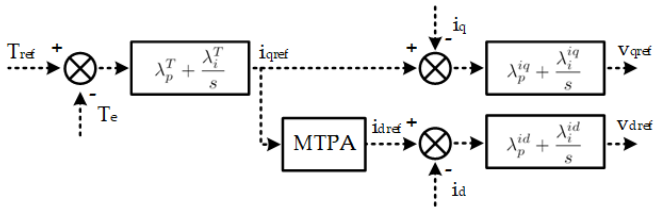

Fig. 3: Control diagram of the three PI controllers.

B. Controllers Design

PI (Proportional-Integral) controller is one of the most widely used controllers in the industrial environment, thus the EDS under investigated in the paper adopts three PI controllers to regulate the error between the reference and the actual torque, d-axis and q-axis current. The model is shown in Fig. 3, wherein, the transfer functions of each PI controllers are

$$i_{qref} = (T_{ref} - T_e)(\lambda_p^T + \frac{\lambda_i^T}{s}), \tag{7}$$

$$v_{dref} = (i_{dref} - i_d)(\lambda_p^{id} + \frac{\lambda_i^{id}}{s}), \tag{8}$$

$$v_{qref} = (i_{qref} - i_q)(\lambda_p^{iq} + \frac{\lambda_i^{iq}}{s}). \tag{9}$$

where λ_p^T, λ_i^T, λ_p^{id}, λ_i^{id}, λ_p^{iq}, and λ_i^{iq} are the PI parameters.

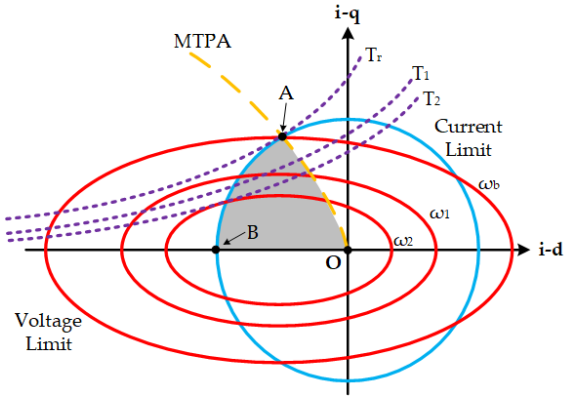

Fig. 4: Diagram of the reference current vector optimization.

C. Maximum Torque Per Ampere (MTPA) Control

MTPA control is widely adopted in the industrial application for copper loss minimization purpose. To minimize the copper loss, the minimum current should be achieved to generate maximum torque. The optimal current reference is chosen by

$$i_{dref} = \frac{\Lambda_{pm}}{2(L_q - L_d)} - \sqrt{\frac{\Lambda_{pm}^2}{4(L_q - L_d)^2} + i_{qref}^2}. \tag{10}$$

Meanwhile, it should be noted that the IPM has current and voltage limitation, derived by

$$I_s = \sqrt{i_d^2 + i_q^2} \leqslant I_{smax}, \; V_s = \sqrt{v_d^2 + v_q^2} \leqslant V_{smax}. \tag{11}$$

When the optimal current vector is out of the boundary, flux weakening control should be adopted, as

$$i_{dref} = -\frac{\Lambda_{pm}}{L_d} + \frac{1}{L_d}\sqrt{(\frac{V_{smax}}{\omega_e})^2 - (L_q i_{qref})^2}. \tag{12}$$

The optimal current vector should be chosen in the area OAB depicted in Fig. 4 to achieve the copper loss minimization.

III. Classification of Potential Cyber Attacks

As shown in Fig. 2, the virus icons denote the signals between cyber and physical systems, which is most likely to be attacked. According to the confidentiality, integrity and availability (CIA) triad, one of the core principles of

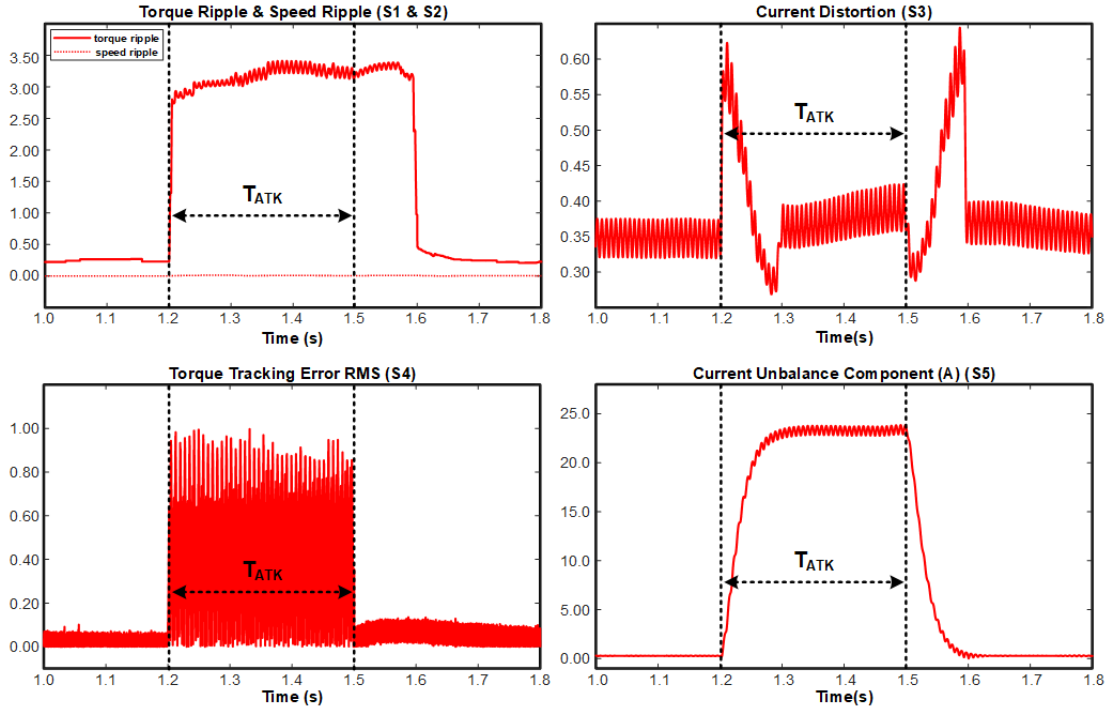

Fig. 5: $\hat{y} = 0.1y$, $t \in \mathbf{T_{ATK}}$, targeting phase A.

information security, cyber attacks could be classified as follows [6], [11]:

1) **Interception** refers to attacks targeting the information confidentiality, which means an unauthorized party gains access to a cyber asset. Losing such information may make the vehicle systems even more vulnerable to dangers such as crashes and lane deviations. Typical interception attacks are eavesdropping, wiretapping, fibber-tapping, packet-sniffing, keystroke logging and traffic monitoring.
2) **Modification** refers to attacks targeting the information integrity, which means an unauthorized party gains access to and tampers with a cyber asset. It could also be called as data integrity attack. For example, the attacker may try to change the parameter of the controllers and sensors, which cause the system performance damaged and even unstable. Some typical integrity attacks are sensor feedback signal modification and controller output control signal modification.
3) **Interruption** refers to attacks targeting the information availability, which means an unauthorized party destroys a cyber asset or makes it unavailable, for example, the attacker blocks the control signals of a controller to damage the stability of the system. It is mainly caused by denial-of-service (DoS) attacks, which includes communication link jamming, software modification to prevent accurate execution and data erasure.

In this paper, only integrity attacks targeting on phase current sensor is considered, but notice that the mythology proposed can be used to analyze other types of attacks.

IV. Simulation and Impact Analysis

To quantitatively evaluate the impact on the electric system, a model based on a 50kW IPM is constructed in MATLAB Simulink. Five metrics are defined for the evaluation, as

$$\begin{aligned} S_1 &= \frac{T_{max}(t) - T_{min}(t)}{T_{ave}(t)}, \; S_2 = \frac{n_{max}(t) - n_{min}(t)}{n_{ave}(t)}, \\ S_3 &= \sqrt{\frac{\int_{-\infty}^{f_l} I(f)^2 df + \int_{f_u}^{+\infty} I(f)^2 df}{\int_{f_l}^{f_u} I(f)^2 df}}, \\ S_4 &= \frac{\sqrt{\int_{t_0}^{t_0+T_w} (T_{ref}(t) - T_e(t))^2 dt / T_w}}{T_{ave}}, \end{aligned} \tag{13}$$

where S_1 and S_2 are the torque and speed ripple, respectively; S_3 denotes the current distortion, which is calculated by Fourier Transformation; S_4 reflects the torque tracking error. Another metrics S_5 is calculated from the asymmetry component method to show the current unbalance component [12].

Meanwhile, we introduce four kinds of attacks to the system as four cases. For clear description, the attacked signal is marked as $\hat{y}$; the original signal is y; the attack duration is defined as a time period $\mathbf{T_{ATK}}$; and all the values are calculated within a sliding window with a window size of T_w.

A. Case A: decreasing attack

When the sensor signal is modified, decreasing the original value by some coefficients is a common manipulating method. In case A, an attack modeled is introduced to phase A current sensor, expressed by Eq.(14) Here the current feedback signal of phase A is decreased to 10% of the original value. The results

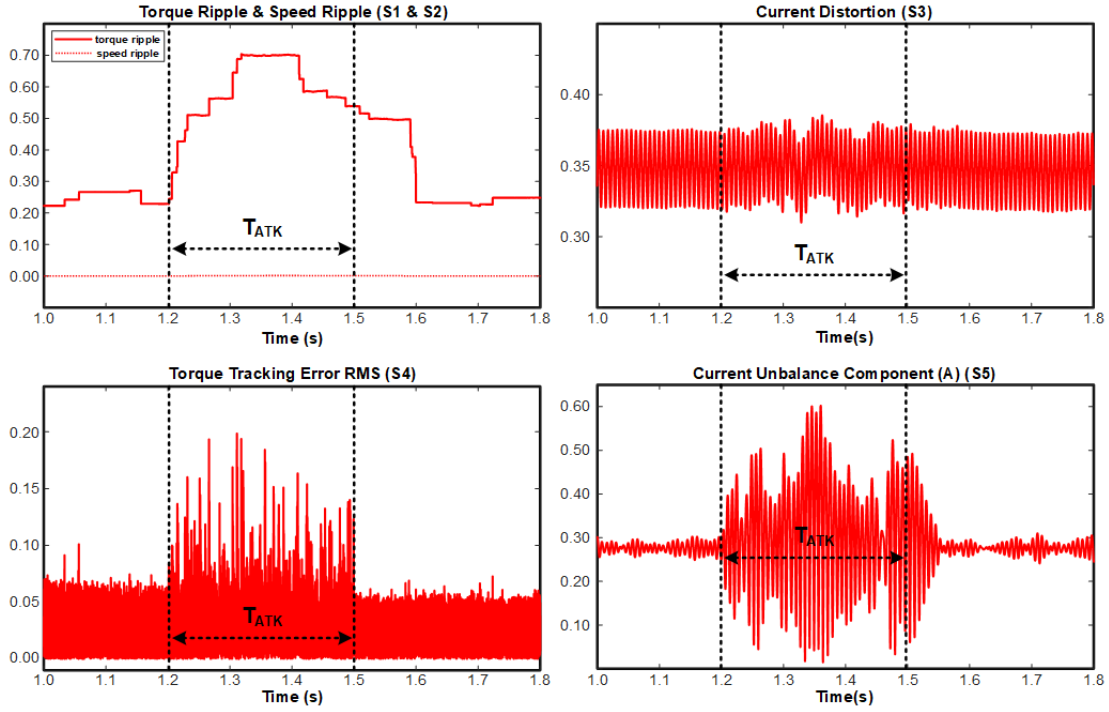

Fig. 6: $\hat{y} = y +$ white noise, $t \in \mathbf{T_{ATK}}$, targeting phase A.

are shown in Fig. 5. As the feedback signal reduced, the actual current flowing in phase A will get larger to trace the current reference. Once the current of phase A increases, the current of phase B and phase C will drop to fulfill the Kirchhoff current theorem. The consequence is that the three phases become unbalance, which is reflected by S_5 profile. Meanwhile, as the inaccuracy of the current value, torque ripple will be increased and the current distortion will be worsened. Besides, when the attack is eliminated, the system could be restored, but transient period is required.

$$\hat{y} = \begin{cases} y & (t \notin \mathbf{T_{ATK}}) \\ 0.1y & (t \in \mathbf{T_{ATK}}). \end{cases} \tag{14}$$

B. Case B: white noise attack

Noise attacks are also one of the most common attacks on the sensor signals. In such attacks, a white noise with certain amount of energy is injected into phase A current feedback signal, as

$$\hat{y} = \begin{cases} y & (t \notin \mathbf{T_{ATK}}) \\ y + \text{white noise} & (t \in \mathbf{T_{ATK}}), \end{cases} \tag{15}$$

where the white noise has a frequency of 1000Hz. As shown in Fig. 6, because the low-power attack noise is mixed with the original noise, it is hard to observe the attack from the current distortion. However, as the noise introduced random variation of the signals, the current unbalance component has an obvious change, so does the torque ripple and tracking error. In addition, the power of the noise in this simulation is considered relatively low, once raising the noise power, this kind of attack could easily damage the system's stability.

C. Case C: mixed attack

Eq.(16) models an attack combining the attacks described in case A and case B. And the results are shown in Fig.8. And Fig.7 shows the raw waveform of three phase current to provide a more direct observation.

$$\hat{y} = \begin{cases} y & (t \notin \mathbf{T_{ATK}}) \\ 0.1y + \text{white noise} & (t \in \mathbf{T_{ATK}}), \end{cases} \tag{16}$$

As shown in these figures, when the attacks are added together, it is more likely to generate more ripples and distortion. And as the attack targets on single phase, the unbalance component S_5 is quite huge.

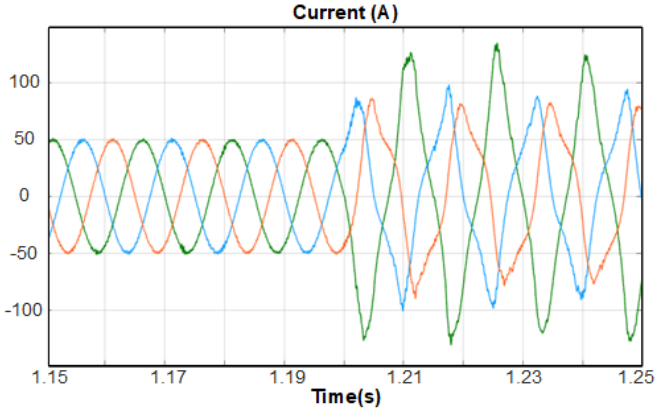

Fig. 7: Original Current Waveform of Case C.

Meanwhile, it could be observed that the feature of the reducing attack demonstrated in case A is dominant in Fig.8.

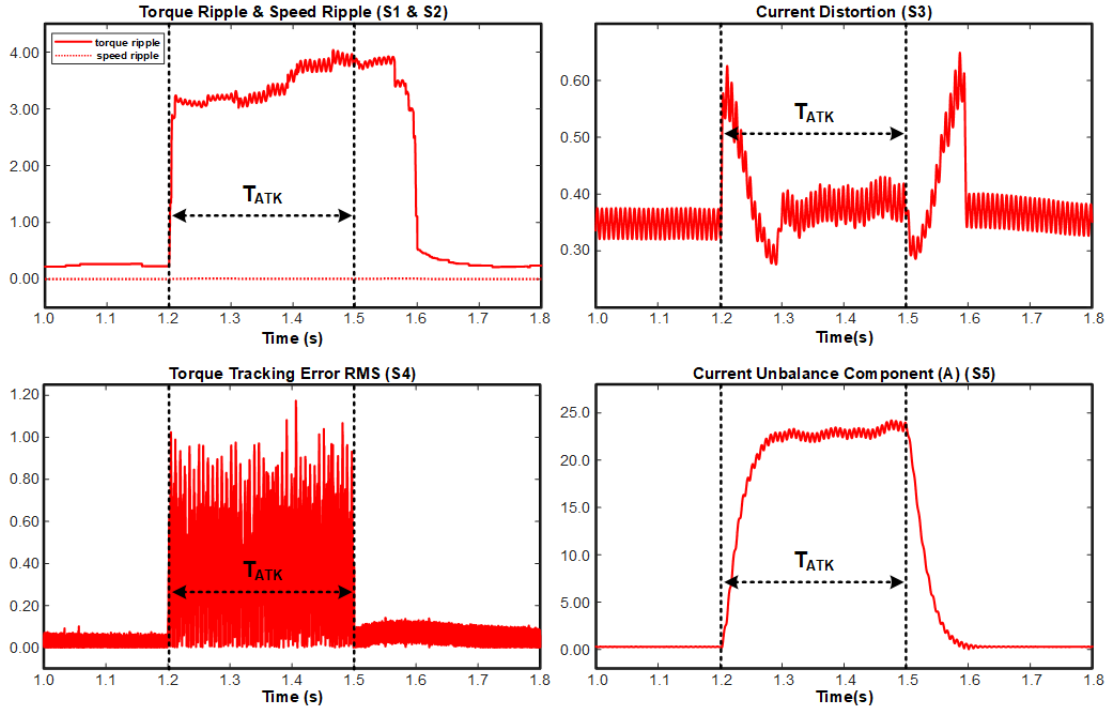

Fig. 8: $\hat{y} = 0.1y +$ white noise, $t \in \mathbf{T_{ATK}}$, targeting phase A.

This is because the white noise power is relatively small. However, as it is discussed in case B, once the white noise power is large enough, its feature will become more obviously.

V. Conclusion and Future Work

In this paper, the impact of various data integrity attacks on EDSs has been analyzed and compared in various cases based on redefined performance metrics. The simulation results show that cyber attacks could have malicious impact on the overall performance of EDSs and could be a big threat to next generation EVs. Meanwhile, the evaluation results also indicate that the predefined metrics are useful tools for detecting and diagnosing the cyber attacks, as good designed metrics could reflect the features of the attacks such as fixed frequency of an periodic attack signal. In our future work, in order to assure the security of the EDSs, we will focus on more advanced models and more sophisticated metrics to reflect accurate relationship between cyber attacks and physical response, and provide general guidelines for further detection and diagnosis of EDSs.

References

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

[2] R. M. Gerdes, C. Winstead, and K. Heaslip, "Cps: an efficiency-motivated attack against autonomous vehicular transportation," in *Proceedings of the 29th Annual Computer Security Applications Conference*. ACM, 2013, pp. 99–108.

[3] Y. Fraiji, L. B. Azzouz, W. Trojet, and L. A. Saidane, "Cyber security issues of internet of electric vehicles," in *Wireless Communications and Networking Conference (WCNC), 2018 IEEE*. IEEE, 2018, pp. 1–6.

[4] K. Harnett, B. Harris, D. Chin, G. Watson *et al.*, "Doe/dhs/dot volpe technical meeting on electric vehicle and charging station cybersecurity report," John A. Volpe National Transportation Systems Center (US), Tech. Rep., 2018.

[5] 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.

[6] B. Chen, S. Mashayekh, K. L. Butler-Purry, and D. Kundur, "Impact of cyber attacks on transient stability of smart grids with voltage support devices," in *Power and Energy Society General Meeting (PES), 2013 IEEE*. IEEE, 2013, pp. 1–5.

[7] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards a framework for cyber attack impact analysis of the electric smart grid," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. IEEE, 2010, pp. 244–249.

[8] S. Xin, Q. Guo, H. Sun, B. Zhang, J. Wang, and C. Chen, "Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2375–2385, 2015.

[9] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A framework for modeling cyber-physical switching attacks in smart grid," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 2, pp. 273–285, 2013.

[10] P. Zhang, W. Li, S. Li, Y. Wang, and W. Xiao, "Reliability assessment of photovoltaic power systems: Review of current status and future perspectives," *Applied energy*, vol. 104, pp. 822–833, 2013.

[11] T. Flick and J. Morehouse, *Securing the smart grid: next generation power grid security*. Elsevier, 2010.

[12] A. Von Jouanne and B. Banerjee, "Assessment of voltage unbalance," *IEEE transactions on power delivery*, vol. 16, no. 4, pp. 782–790, 2001.