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

Bowen Yang¹, Lulu Guo¹, Fangyu Li¹, Jin Ye¹, Wenzhan Song¹

¹ Center for Cyber-Physical Systems, University of Georgia, Athens, Georgia, USA.

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 first proposed to investigate the interaction between physical systems and cyber systems. Then a few important 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 performance metrics (e.g., total harmonic distortion, torque ripples, etc) are greatly impacted by data integrity attacks. For example, the current Total Harmonic Distortion (THD) could be increased by over 10 times by maliciously adding 10% random noise to current sensors and the torque ripple could be increased up to 159% by maliciously multiplying 1.5 times of current sensor data.

1. INTRODUCTION
The development of IoT (Internet of Things) enabled intelligent transportation systems, vehicles including electric vehicles are becoming more vulnerable to cyber and physical threats. The number of electric vehicle has been growing substantially in recent years and many countries have established their schedules of replacing traditional internal combustion engine vehicles with electric and hybrid electric vehicles. However, the security challenge for electric vehicles have not yet fully explored and will lead to devastating consequences if not detected in the early stage. There are some preliminary works on electric vehicle charging cyber security [1–5], however, none of them investigates the impacts of cyber attacks on power electronics and electric drive systems. Due to 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]. Most CPS models were developed in smart grids in order to assess the operational reliability and vulnerability, the transient angle and voltage stability, frequency and electricity market operation due to cyber attacks. [9] Impact of cyber attacks on the the control systems of solar inverter and energy storage was analyzed in the Monte-Carlo simulation to evaluate microgrid cyber security risks [10]. While the work provides a crucial insight into the interaction between control system (cyber system) and physical microgrid based on
the operational cost analysis of microgrids, it does not evaluate important performance metrics (e.g., power quality, torque ripples, etc) of power electronics and electric drives due to cyber attacks. To the best of our knowledge, to date, no CPS model has been developed for power electronics and electric drives in electric vehicles, which is needed to further explore the impacts of cyber attacks on electric drive systems, and then the overall vehicle performance.

In this paper, a CPS model of electric drive systems is firstly introduced, and the vulnerabilities of the system is discussed. Then, common cyber attacks are classified, and potential impacts are discussed. Simulation results of data integrity attacks will be provided to verify the former discussion. The conclusion and future work are included.

2. CYBER PHYSICAL SYSTEM MODEL OF ELECTRIC DRIVE SYSTEMS

As shown in Figure 1, the electric drive system of the electric vehicle includes batteries, power electronics, electric machines and controllers. Controllers (including sensors and actuators) are the main source of gathering information, computing and generating the control signals. Meanwhile, it also takes charge of communicating with other devices, facilities and higher level control centers. Thus, the controllers are vulnerable to cyber attacks. Once the controllers are compromised, many critical systems including 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 Figure 2, which shows the physical and cyber model of the electric vehicle drive system, often refereed to as the CPS model. In this model, the feedback control system are introduced in details to clarify the interaction between physical systems and cyber systems. The generalized physical model of DC/AC inverter and electric machines is represented by (1):

\[ \dot{i} = A_i + B_1 e + B_2 u, \]  

(1)
where the control signals $u$ is $[s_a \ s_b \ s_c]^T$, and the phase current $i$ is $[i_a \ i_b \ i_c]^T$. It should be noted that control signal $u$ will be sent from the cyber system and it is defined by (2). $e = [e_a \ e_b \ e_c]^T$ is the back Electromotive Force (EMF) vector, and $A = -\frac{R}{L}I$, $B_1 = I$, $B_2 = -\frac{v_{dc}}{3L} \cdot \begin{bmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{bmatrix}$, and $L$ and $R$ is the winding inductance and resistance, $v_{dc}$ is the DC bus voltage.

$$s_a = \begin{cases} 1 & (S_1 = 1, S_4 = 0) \\ 0 & (S_1 = 0, S_4 = 1) \end{cases} ; \quad s_b = \begin{cases} 1 & (S_3 = 1, S_6 = 0) \\ 0 & (S_3 = 0, S_6 = 1) \end{cases} ; \quad s_c = \begin{cases} 1 & (S_5 = 1, S_2 = 0) \\ 0 & (S_5 = 0, S_2 = 1) \end{cases}$$

(2)

3. CLASSIFICATION OF POTENTIAL CYBER ATTACKS AND THEIR IMPACTS

As shown in Figure 2, the virus icons denote the the signals between cyber and physical systems, which is most likely to be attacked. According to the CIA triad (Confidentiality, Integrity and Availability), one of the core principles of information security, cyber attacks could be classified as: [6,11]

(a) **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 more vulnerable to dangers such as crashes and manipulations. Typical interception attacks are eavesdropping, wiretapping, fibber-tapping, packet-sniffing, keystroke logging and traffic monitoring.

(b) **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 leads to the system crash. Some typical integrity attacks are sensor feedback signal modification and controller output control signal modification.

(c) **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. Some typical DoS attacks include communication link jamming, software modification to prevent accurate execution and data erasure.

4. SIMULATION VALIDATION

In this section, integrity attack targeting the sensor feedback signal is discussed and then impact on power electronics and electric drives will be evaluated in the simulation.

Two typical data integrity attack models are constructed as:

$$\hat{y} = y + rand(a, b), \quad (3)$$

$$\hat{y} = \alpha \cdot y, \quad (4)$$
where \( y \) is the real sensor signal, \( \hat{y} \) is the modified sensor signal, and \( \alpha \) and the \( \text{rand}(a, b) \) is the modification parameter. By changing the parameters, the sensor signal could be changed to different values.

To quantify the impact of data integrity attacks on power electronics and electric drive systems, a number of quality indexes are defined by (5) - (8)

\[
THD = \sqrt{\sum_{n=2}^{\infty} \frac{i_n^2}{i_1^2}} \quad \text{(current THD)} \tag{5}
\]

\[
\omega_{\text{ripple}} = \frac{\omega_{\text{max}} - \omega_{\text{min}}}{\omega_{\text{ave}}} \quad \text{(speed ripple)} \tag{6}
\]

\[
T_{\text{ripple}} = \frac{T_{\text{max}} - T_{\text{min}}}{T_{\text{ave}}} \quad \text{(torque ripple)} \tag{7}
\]
\[ T_{RMSE} = \sqrt{\frac{1}{T} \int_0^T (T_{ref} - T)^2 d\tau} \] (8)

An interior permanent magnet synchronous machines (IPM) is built and four different integrity attacks targeting the current feedback signals are simulated in MATLAB Simulink. Table 1 shows the simulation results when one of the phase current sensor feedback signals is modified by different attack parameters. Figure 3 shows comparison of torque waveform under normal and attack scenarios.

Table 1: Simulation results

<table>
<thead>
<tr>
<th>( rand(a,b) )</th>
<th>normal</th>
<th>(-15,+15)</th>
<th>(-50,+50)</th>
<th>( \alpha )</th>
<th>0.5</th>
<th>1.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>THD%</td>
<td>37.99</td>
<td>108.10</td>
<td>523.11</td>
<td>THD%</td>
<td>22.73</td>
<td>36.87</td>
</tr>
<tr>
<td>( \omega_{\text{ripple}}% )</td>
<td>0.0603</td>
<td>0.0425</td>
<td>0.0412</td>
<td>( \omega_{\text{ripple}}% )</td>
<td>0.0435</td>
<td>0.27</td>
</tr>
<tr>
<td>( T_{\text{ripple}}% )</td>
<td>64.4</td>
<td>78.8</td>
<td>108</td>
<td>( T_{\text{ripple}}% )</td>
<td>104</td>
<td>159</td>
</tr>
<tr>
<td>( T_{RMSE} )</td>
<td>7.11</td>
<td>7.21</td>
<td>7.741</td>
<td>( T_{RMSE} )</td>
<td>22.6</td>
<td>27.5</td>
</tr>
</tbody>
</table>

From the result, it is obvious that integrity attack to the feedback signals can lead to abnormal current THD, torque and speed ripples. For example, the current THD, torque ripples, and \( T_{RMSE} \) could be increased by up to 523.12\%, 159\%, and the 27.5 NM, respectively. As the current controller is the inner loop of the system, the data attacks targeting the current sensing signals seems not to impact the rotating speed significantly. This could be caused by large inertia of the system. These negative impacts could lead to damages such as efficiency dropping, overheat, or bearing aging.

Figure 3: Simulation Result - Torque Waveform

5. CONCLUSION AND FUTURE WORK

In this paper, the impact of various data integrity attacks on electric drive systems of electric vehicle has been analyzed and compared in various cases based on a few important performance metrics (e.g., THD, torque ripples, torque tracking errors, etc.). The simulation results shows that cyber attacks could have malicious impact on the overall performance of electric drive systems and could be a big threat to next generation of electric vehicles. To assure the safety and security, in our future work, we will focus on more advanced models to reflect closer interaction between cyber systems and physical systems in electric vehicles.
References


