Article
Detection of Stealthy False Data Injection Attacks in Modular Multilevel Converters
Xingxing Chen 1 and Shuguang Song 2,*

1 Department of Electrical and Electronic Engineering, The Hong Kong Polytechnic University, Hong Kong 999077, China; xingstarxjtu@163.com
2 College of New Energy, China University of Petroleum (East China), Qingdao 266580, China
* Correspondence: shuguang.song.chine@gmail.com

Abstract: A modular multilevel converter (MMC) in a high-voltage direct-current (HVDC) transmission system consists of an electric-coupled physical system and a communication-coupled cyber system, leading to a cyber-physical system (CPS). Such a CPS is vulnerable to false data injection attacks (FDIA), which are the main category of cyberattacks. FDIA can be launched by injecting false data into the control or communication system of the MMC to change the submodule (SM) capacitor voltage seen by the central controller. Consequently, the capacitor voltage of the attacked SM will deviate from its normal value and thus threaten the safe operation of the converter. Stealthy FDIA characterized by elaborated attack sequences are more dangerous because they can deceive and bypass the attack detector presented in the existing literature for the MMC. To address this issue, this paper proposes a stealthy FDIA detection method to obtain the real SM capacitor voltages. Thus, the attacked SM can be located by comparing its real capacitor voltage with prespecified thresholds. Simulation results validate the effectiveness of the proposed detection and protection strategies.

Keywords: modular multilevel converter; cyberattack; stealthy false data injection attack

1. Introduction

Compared to alternating current transmission systems, high-voltage direct-current (HVDC) electric power transmission technology offers various advantages. It is capable of high-power transfer over long distances with lower cost and higher efficiency. In the past two decades, many HVDC projects have been developed, such as the Transbay Cable project in the United States [1], the Ultranet project in Germany [2], and the Zhoushan project in China [3].

The modular multilevel converter (MMC) is the predominant topology implemented in recent voltage source converter-based HVDC (VSC-HVDC) transmission projects. It features many advantages, such as modularity, scalability, reduced voltage stress on power switches, and high-quality output waveforms [4,5]. Since Prof. R. Marquardt proposed this topology in 2001 [6], plenty of studies have been carried out to optimize the design and operation performance of the converter. Research topics on MMC include submodule (SM) capacitor voltage balancing [7,8], circulating current suppression [9], modulation methods [10,11], IGBT open-circuit fault diagnosis [12,13], model predictive control [14], and so on. However, little attention has been paid to cyberattacks in the MMC.

The modern power system, including the MMC-based HVDC transmission, is a cyber-physical system (CPS), which means that the system is composed of an electric-coupled physical system and a communication-coupled cyber system. The CPS architecture is illustrated in Figure 1a [15]. Cybersystems link with physical systems through communication networks, sensors, and actuators. The CPS integrates real-world hardware, digital software, and networking elements to monitor and manage physical processes. This integration enhances interaction with physical processes; however, such a system is vulnerable to cyberattacks [16–18].
This integration enhances interaction with physical processes; however, such a system is vulnerable to cyberattacks [16–18].

A cyberattack is any offensive maneuver that targets communication networks, control centers, and infrastructure, which can threaten the safe operation of a CPS. Examples of cyber-physical attacks include slammer worm penetration in the control system of a nuclear plant [19], attacks on circuit breakers [20], power blackouts in Ukraine [21], and nuclear fuel enrichment facilities attacked by the Stuxnet worm [22]. To deal with cyberattacks and ensure system security, an effective diagnosis strategy must be designed for CPSs. There are several types of cyberattacks, such as random attacks, denial of service (DoS), false data injection attacks (FDIAs), jamming, and malware. Among these cyberattacks, FDIA represents an important type with widely varied types and impacts. The FDIA is realized by injecting false data into any of the compromised components in a CPS to alter the system state [23,24]. This paper mainly focuses on the impact analysis and detection of FDIA for the MMC.

The architecture of the power system, including MMC-based HVDC converter stations, is shown in Figure 1b. In the HVDC converter station, the control center, or supervisory control and data acquisition (SCADA) system, monitors and manages the MMC hardware circuit through the communication infrastructure. Moreover, one converter station also communicates with the power grid dispatching center and other converter stations through outer communication networks. The communication infrastructure based on local area networks (LAN), field area networks (FAN), and wide area networks (WAN) is vulnerable.
to cyberattacks. The attackers can access the communication networks and control center to inject false data to alter the system state. Ref. [25] is the first paper to discuss the cyberattack in the MMC. This paper assesses the impact of cyberattacks on the control system of the MMC-based HVDC system and shows that cyberattacks can affect system stability. Unlike the centralized control architecture analyzed in [25], ref. [26] shows the effect of the FDIA on the capacitor voltage balancing of the MMC under a distributed control structure. The real capacitor voltage of the attacked SM will deviate from the normal value after injecting the false data; however, the SM capacitor voltages seen by the controller are still well-balanced. In follow-up studies, ref. [27] presents a reinforcement learning-based method to exploit the vulnerabilities of FDIA detectors in the MMC. The proposed method reveals the weakness of the fault detector given in [26] and provides a solution for researchers to motivate future research in this area. To the best of our knowledge, refs. [25–27] are all the related publications regarding the topic of cyber-attack in the MMC.

Compared to the FDIA step analyzed in [26], stealthy false data injection with a more elaborate attack sequence can deceive the protection system and bypass the fault detector [27]. This type of FDIA is more dangerous to the safe operation of CPS. However, the detection of stealthy FDIAs in MMC has not been studied in the existing literature. To fill this research gap, this paper proposes a detection method that can obtain the real capacitor voltage of the attacked SM during the modulation process. Since the real capacitor voltage of the attacked SM will be increased or decreased to deviate from the normal value, the FDIA can be detected by comparing the real SM capacitor voltage with prespecified thresholds. The attacked SM is isolated from the arm circuit after detecting FDIA. Simulation results verify the effectiveness of the proposed detection method.

The rest of the paper is organized as follows: Section 2 describes the basic structure, modulation, and capacitor voltage balancing of the MMC; Section 3 analyzes the performance of the MMC under cyberattacks; Section 4 presents the proposed detection method; Section 5 shows the simulation results; and Section 6 concludes the paper.

2. System Description of the MMC

2.1. Structure of the MMC

The circuit configuration of a single-phase MMC is shown in Figure 2, where the upper and lower arms both include N ordinary half-bridge SMs and M redundant half-bridge SMs. \( U_{dc} \) represents the dc bus voltage. \( i_u \) and \( i_l \) denote the upper and lower arm currents, respectively. \( u_u \) and \( u_l \) denote the upper and lower arm voltages, respectively. \( L \) is the arm inductance, \( R_o \) is the load resistance, and \( L_o \) is the load inductance. \( i_o \) and \( u_o \) represent the load current and load voltage, respectively. \( C \) and \( U_C \) stand for the SM capacitance and the capacitor voltage, respectively. \( B_s \) is the bypass switch that is used to isolate the SM from the arm circuit.

The half-bridge SM of the MMC has two operating modes: inserted and bypassed. When the upper switch \( T_1 \) and lower switch \( T_2 \) are turned on and off, respectively, the SM output voltage is equal to the capacitor voltage \( U_C \), and the SM is inserted. In contrast, the SM is bypassed when the upper switch \( T_1 \) and lower switch \( T_2 \) are turned off and on, respectively; thus, the SM output voltage is zero. The ordinary and redundant SMs are treated identically by the control system in this paper, which means that the SMs are set to the active redundant mode [28]. The average dc value of the SM capacitor voltage is equal to \( U_{dc}/N \) under normal operating conditions.

According to Kirchhoff’s circuit laws, the upper and lower arm voltages can be expressed as follows:

\[
\begin{align*}
u_u &= \frac{U_{dc}}{2} - L \frac{di_u}{dt} - L_o \frac{di_o}{dt} - R_o i_o, \\
u_l &= \frac{U_{dc}}{2} + L \frac{di_l}{dt} + L_o \frac{di_o}{dt} + R_o i_o.
\end{align*}
\]
where \( N_u \) is the reference of the corresponding arm voltage (the upper arm and lower arm are represented by subscripts \( u \) and subscript \( l \), respectively, i.e., \( x = u, l \)).

The waveforms of the arm-inserted SM numbers and the load voltage of the MMC using NLM with eight SMs per arm are shown in Figure 3. \( u_x^* \) denotes the reference of the load voltage. The arm-inserted SM number changes in a staircase manner, and the value of each step is equal to 1. It should be noted that although there are \( N + M \) SMs in each arm, the maximum value of the arm-inserted SM number using NLM in one control cycle is \( N \) [28], because the active redundant mode [28] is applied in this paper.

After calculating the arm-inserted SM numbers according to the NLM principle, the reduced-switching-frequency (RSF) voltage balancing algorithm [8] is applied to balance the SM capacitor voltages. The implementation diagram is shown in Figure 4. \( i_x \) represents the arm current. \( \Delta N_{\text{out}} \) denotes the extra inserted or bypassed SM number during the following control cycle. \( \Delta N_{\text{out}} \) is expressed as follows:

\[
\Delta N_{\text{out}} = N_{\text{out}}(k) - N_{\text{out}}(k - 1),
\]

where \( N_{\text{out}}(k) \) and \( N_{\text{out}}(k - 1) \) are inserted SM numbers in the arm at control steps \( k \) and \( k - 1 \), respectively. For instance, if \( N_{\text{out}}(k) = 4 \) and \( N_{\text{out}}(k - 1) = 3 \), then \( \Delta N_{\text{out}} = 1 \), which means that one extra SM needs to be inserted. In contrast, if \( N_{\text{out}}(k) = 3 \) and \( N_{\text{out}}(k - 1) = 4 \), then \( \Delta N_{\text{out}} = -1 \) and one extra SM needs to be bypassed.

Figure 2. Circuit configuration of a single-phase MMC.

2.2. Modulation and SM Capacitor Voltage Balancing for the MMC

There are two widely applied modulation methods for the MMC, i.e., pulse-width modulation (PWM) and nearest-level modulation (NLM) [11]. The total harmonic distortion (THD) using the PWM method is lower for the MMC with fewer SMs. However, as the SM number per arm increases to hundreds for HVDC applications, the NLM method is preferred because of its low switching frequency characteristic and simple implementation. The arm-inserted SM number using the NLM method is obtained as follows:

\[
N_{\text{on,x}} = \text{round}\left(\frac{N u_x^*}{U_{dc}}\right),
\]

where \( u_x^* \) is the reference of the corresponding arm voltage (the upper arm and lower arm are represented by subscripts \( u \) and subscript \( l \), respectively, i.e., \( x = u, l \)).
where Nonx(k) and Nonx(k − 1) are inserted SM numbers in the arm at (i.e., ΔNonx = 0), then the SMs will keep their gating signals.

Figure 3. Inserted SM numbers in the arms and load voltage of the MMC using NLM.

\[
\Delta N_{\text{ins}} = N_{\text{ins}}(k) - N_{\text{ins}}(k-1)
\]

If \(\Delta N_{\text{ins}} > 0\)
1. Insert |\(\Delta N_{\text{ins}}|\) SMs with the lowest voltages among \([N+M-N_{\text{ins}}(k-1)]\) bypassed state SMs.

2. Insert |\(\Delta N_{\text{ins}}|\) SMs with the highest voltages among \([N+M-N_{\text{ins}}(k-1)]\) bypassed state SMs.

Bypass |\(\Delta N_{\text{ins}}|\) SMs with the highest voltages among \(N_{\text{ins}}(k-1)\) inserted state SMs.

Bypass |\(\Delta N_{\text{ins}}|\) SMs with the lowest voltages among \(N_{\text{ins}}(k-1)\) inserted state SMs.

Figure 4. RSF voltage balancing algorithm.

The basic principles of the RSF balancing algorithm are further explained as follows:

- If extra |\(\Delta N_{\text{ins}}|\) SMs need to be inserted during control cycle \(k\), then |\(\Delta N_{\text{ins}}|\) SMs that are currently in the bypassed state with the lowest (highest) voltages will be inserted when the arm current is positive (negative). Those SMs currently in the inserted state just keep their operating mode;
- If extra |\(\Delta N_{\text{ins}}|\) SMs need to be bypassed during control cycle \(k\), then |\(\Delta N_{\text{ins}}|\) SMs that are currently in the inserted state with the highest (lowest) voltages will be bypassed when the arm current is positive (negative). Those SMs currently in the bypassed state just keep their operating mode;
- If no extra SMs need to be bypassed or inserted during the following control cycle (i.e., \(\Delta N_{\text{ins}} = 0\)), then the SMs will keep their gating signals.
3. FDIAs in the MMC

In this section, different types of MMC control architectures will be introduced. On this basis, the performance of the MMC under FDIAs will be analyzed.

3.1. Architecture of the MMC Control System

There are three main control architectures for the MMC [29,30], i.e., centralized, decentralized, and distributed, as shown in Figure 5. $S_{xi}$ stands for the switching function of the $i$th SM in arm $x$ ($i = 1, 2, \ldots, N + M, x = u, l$). $S_{xi}$ is equal to 1 and 0 when the SM is inserted and bypassed, respectively. The $MP$ signal represents the measurement and protection signals, if needed.

![Figure 5. Control architectures of the MMC.](image)

The centralized control architecture uses one central controller, which is responsible for control, modulation, and system-level protection tasks. The local controller in the SM sends the measured capacitor voltage to the central controller and receives the switching function from the central controller. A detailed illustration of the centralized control architecture is shown in Figure 6. To reduce the computation burden of the central controller, a decentralized control architecture can be used with a central controller and multiple arm- or group-level controllers. The load current and voltage controls can be executed by the central controller. Modulation and capacitor voltage balancing control are undertaken in the arm/group controllers. In the distributed control architecture, the transmission of SM capacitor voltages can be avoided to reduce the bandwidth requirement of the communication networks. System-level controls (current and voltage controls) and modulation can be allocated in various ways to the central and local controllers.

The distributed control architecture with the PWM method for the MMC has not been widely used in practical HVDC projects [29]. Therefore, this paper mainly focuses on centralized and decentralized control architectures. The analysis and detection of the FDIAs in the following sections of this paper are based on the centralized control architecture; however, they are also applicable to the decentralized control architecture. For both architectures, FDIAs can alter the SM capacitor voltages seen by the central or arm controller and cause unbalanced capacitor voltages. The stealthy FDIA detection method for distributed control architectures needs to be studied in future research.
### Parameters of the simulation system.

Table 1.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Symbol</th>
<th>Simulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC-link voltage</td>
<td>$U_{dc}$</td>
<td>60 kV</td>
</tr>
<tr>
<td>Ordinary SM number</td>
<td>$N$</td>
<td>40</td>
</tr>
<tr>
<td>Redundant SM number</td>
<td>$M$</td>
<td>2</td>
</tr>
<tr>
<td>Submodule capacitance</td>
<td>$C$</td>
<td>6 mF</td>
</tr>
<tr>
<td>Arm inductance</td>
<td>$L$</td>
<td>30 mH</td>
</tr>
<tr>
<td>Load inductance</td>
<td>$L_o$</td>
<td>30 mH</td>
</tr>
<tr>
<td>Load resistance</td>
<td>$R_o$</td>
<td>25 Ω</td>
</tr>
<tr>
<td>Output voltage frequency</td>
<td>$f_o$</td>
<td>50 Hz</td>
</tr>
<tr>
<td>Control period</td>
<td>$T_s$</td>
<td>50 µs</td>
</tr>
</tbody>
</table>
False data can be injected into the cybersystem of the MMC to alter the SM capacitor voltage seen by the central controller. The SM capacitor voltage seen by the central controller can be written as follows:

\[ U_{Cxi} = U_{Cxi_{\text{real}}} + w U_{Cxi_{\text{inj}}} \]  

where \( U_{Cxi_{\text{inj}}} \) denotes the injected false data. \( w \) equals 1 and 0 for the SM with and without FDIA, respectively. For the SM without FDIA, its capacitor voltage seen by the central controller equals its real capacitor voltage. However, \( U_{Cxi} \) is not equal to \( U_{Cxi_{\text{real}}} \) for the SM with FDIA.

In this paper, FDIAs are classified into two categories: step FDIAs and stealthy FDIAs. The step FDIA means that \( |U_{Cxi_{\text{inj}}}| \) in (5) suddenly changes to a large value, as shown in Figure 8a. The value of the step FDIA at control cycle \( k \) can be expressed as follows:

\[ U_{Cxi_{\text{inj}}}(k) = \begin{cases} 0 & k < k_0 \\ a_0 & k \geq k_0 \end{cases} \]  

where \( a_0 \) is the value of the injected false data and \( k_0 \) is the number of the injection control cycle. The capacitor voltage waveforms of the MMC under a step FDIA are shown in Figure 8b,c. It can be observed that the SM capacitor voltages seen by the central controller are quickly balanced after step FDIA occurs, attributable to the RSF voltage balancing; however, the real capacitor voltage of the attacked SM is increased to a large value. In Figure 8, the value of the injected false data is \( a_0 < 0 \), which leads to an increase in \( U_{Cxi_{\text{real}}} \). If \( a_0 > 0 \), \( U_{Cxi_{\text{real}}} \) will be reduced.

![Figure 8](image_url)

Figure 8. Waveforms of the MMC under step FDIA. SM1 in the upper arm is attacked as an example: (a) step FDIA; (b) SM capacitor voltages seen by the central controller; and (c) real SM capacitor voltages.

The difference value of the injected false data between adjacent control cycles \( k_0 - 1 \) and \( k_0 \) equals \( a_0 \) for step FDIA, according to (6). The value of \( |a_0| \) is larger than a threshold value of \( \Delta U_{Cth1} \). Specifically, \( \Delta U_{Cth1} \) is set to 0.1 kV in this paper. In contrast, the difference value of the injected false data between any two adjacent control cycles for stealthy FDIA is much smaller than \( \Delta U_{Cth1} \). A ramp-decreased stealthy FDIA and the capacitor voltage
waveforms of the MMC are shown in Figure 9. $U_{Cu1, inj}$ gradually decreases in Figure 9a, and $\Delta U_{\text{Cth1}}$ is always much smaller than $\Delta U_{\text{Cth1}}$. Similarly, the SM capacitor voltages seen by the central controller are well balanced after stealthy FDIA; however, the real capacitor voltage of the attacked SM deviates from its normal value. It should be noted that there are many other types of stealthy FDIAs besides the ramp-change type shown in Figure 9. However, they are all in accordance with the characteristic that $|U_{Cu1, inj}(k) - U_{Cu1, inj}(k-1)|$ is always much smaller than $\Delta U_{\text{Cth1}}$.

![Figure 9. Waveforms of the MMC under stealthy FDIA. SM1 in the upper arm is attacked as an example: (a) stealthy FDIA; (b) SM capacitor voltages seen by the central controller; and (c) real SM capacitor voltages.

4. FDIA Detection Methods

Since the detection method given in [26] is the only FDIA detection method proposed in the existing literature for the MMC, this section will first explain the mechanism of this method and disclose the issue of this method. It is found that the detection method given in [26] can fail to detect stealthy FDIA. In order to address this issue, Section 4.2 presents the implementation details of the proposed detection method.

4.1. FDIA Detection Method Given in [26]

Ref. [26] proposes an FDIA detection method for the MMC based on the dynamic equation of the SM capacitor voltage [14], which is expressed as follows:

$$C \frac{dU_{Ci}}{dt} = S_{Ci}i_{Cxi}. \quad (7)$$

The SM capacitor voltage under NLM can be predicted according to the discretization of (7) (the Euler discretization method is used to discretize (7)), which is obtained as follows:

$$U_{Ci, pre}(k) = U_{Ci, pre}(k-1) + \frac{T_s}{C}S_{Ci}(k-1)i_{Cxi}(k-1) \quad (8)$$
where $U_{Cxi, pre}(k)$ and $U_{Cxi, pre}(k - 1)$ are the predicted capacitor voltages of the $i$th SM in arm $x$ at control steps $k$ and $k - 1$, respectively. $T_s$ denotes the control period. $i_x(k - 1)$ and $S_{xi}(k - 1)$ are the arm current and SM switching functions, respectively, at the control step $k - 1$.

If there is no FDIA and the injected false data $U_{Cxi, inj}$ is zero, as shown in Figure 10a, the SM capacitor voltage seen by the central controller at control step $k$ should approximate $U_{Cxi, pre}(k)$, i.e., $U_{Cxi}(k) \approx U_{Cxi, pre}(k)$. Otherwise, there will be a significant difference between $U_{Cxi}(k)$ and $U_{Cxi, pre}(k)$, as shown in Figure 10b. Based on this phenomenon, a detection principle is proposed in [26]: if the difference between $U_{Cxi}(k)$ and $U_{Cxi, pre}(k)$ exceeds a prespecified threshold, i.e., $|U_{Cxi}(k) - U_{Cxi, pre}(k)| > \Delta U_{Cth2}$, FDIA on $i$th SM in arm $x$ is detected. $\Delta U_{Cth2}$ is set to 0.1 kV in this paper.

![Figure 10. Capacitor voltages of the MMC: (a) no FIDA in the MMC; and (b) FIDA occurs in the MMC.](image)

As explained in Section 3.2, the difference value of the injected false data between adjacent control cycles $k_0 - 1$ and $k_0$ equals $\delta_0$ for step FDIA. $|\delta_0|$ is large enough to trigger the detection principle $|U_{Cxi}(k) - U_{Cxi, pre}(k)| > \Delta U_{Cth2}$ given in [26]. In this case, the detection method proposed in [26] can detect the step FDIA for the MMC. However, for stealthy FDIA, the difference of the injected false data between any two adjacent control cycles is much smaller than $\Delta U_{Cth1}$, i.e., $|U_{Cxi, inj}(k) - U_{Cxi, inj}(k - 1)| << \Delta U_{Cth1}$. So the detection principle given in [26] cannot be satisfied, i.e., $|U_{Cxi}(k) - U_{Cxi, pre}(k)|$ is always smaller than $\Delta U_{Cth2}$. That means this detection method can fail to detect the stealthy FDIA for the MMC.

4.2. Proposed FDIA Detection Method

It can be seen in Figures 8 and 10 that no matter which type of FDIA occurs, the real capacitor voltage of the attacked SM will deviate from its normal value. If the real SM capacitor voltage can be obtained for the central controller, both step and stealthy FDIs can be detected by comparing the real capacitor voltage $U_{Cxi, real}$ with prespecified thresholds. In order to obtain the real capacitor voltage of an SM, the difference value of the arm voltages between adjacent control steps should be calculated for the proposed detection method. A detailed explanation is given below.

By applying the RSF voltage balancing algorithm and NLM principle, the SMs in each arm of the MMC will be inserted or bypassed one by one. As shown in Figure 11a, if SM$_1$ is inserted at control step $k - 1$, the arm voltage $u_x(k - 1)$ can be expressed as follows:

$$u_x(k - 1) = U_{Cxi, real} + u_{SMs},$$ (9)
where $u_{SMs}$ is the voltage of the cascaded SMs ($SM_2$-$SM_{N+M}$), as shown in Figure 11a. When SM$_1$ is bypassed at the next control step $k$, the arm voltage $u_x(k) = u_{SMs}$. The change of the SM state leads to the change of the arm voltage, and the real capacitor voltage of SM$_1$ can be obtained as follows:

$$U_{C_{x, real}} = |u_x(k) - u_x(k-1)|.$$  (10)

Similarly, when SM$_1$ is bypassed and inserted at control steps $k-1$ and $k$, respectively, as shown in Figure 11b, the real capacitor voltage can also be calculated according to (10).

As the SMs in the arm are bypassed or inserted one by one, the real capacitor voltages of the other SMs can be obtained in a similar method.

One technique to derive the arm voltage of the MMC in (10) is to install an arm voltage sensor, as shown in Figure 12. However, this method will increase the cost of the whole MMC system. To avoid using extra voltage sensors or hardware circuits, the arm voltages can be estimated according to the discretization results of Equations (1) and (2) (the Euler discretization method is used to discretize (1) and (2)), which are expressed as follows:

$$u_x(k-1) = \frac{U_{dc}}{2} - L_A u_x - L_o A_o - R_o i_o(k-1),$$  (11)
MMC system. To avoid using extra voltage sensors or hardware circuits, the arm voltages can be estimated according to the discretization results of Equations (1) and (2) (the Euler discretization method is used to discretize (1) and (2)), which are expressed as follows:

\[
\begin{align*}
    u_u(k-1) &= \frac{U_{dc}}{2} - L A_u - L_o A_o - R_o i_o(k-1), \\
    u_i(k-1) &= \frac{U_{dc}}{2} - L A_i + L_o A_o + R_o i_o(k-1), \\
    A_u &= \frac{i_u(k) - i_u(k-1)}{T_s}, \\
    A_i &= \frac{i_i(k) - i_i(k-1)}{T_s}, \\
    A_o &= \frac{i_o(k) - i_o(k-1)}{T_s}
\end{align*}
\]

where \( U_{dc}, i_u(k-1), i_u(k), i_i(k), i_o(k), i_o(k-1) \) and \( i_o(k) \) are the measured voltages and currents. After obtaining the arm voltages of the MMC according to (11) and (12), the real SM capacitor voltage can be calculated according to (10).

Figure 12. Arm voltage measurement.

Figure 13 shows an example of deriving the real SM capacitor voltage. The switching function of SM1 in the upper arm changes from 1 to 0 in Figure 13a, indicating that the SM is bypassed during the modulation process. After one control cycle delay, the real capacitor voltage \( U_{Cu1,real} \) is obtained according to (10), as shown in Figure 13b. The flowchart shown in Figure 13c illustrates the process of determining the capacitor voltage.

Generally, the principle of the proposed detection method can be summarized as follows: when the SM of the MMC is bypassed or inserted, its real capacitor voltage can be obtained according to the changing arm voltage. If \( U_{Cxi,real} > U_{Cth1} \) or \( U_{Cxi,real} < U_{Cth2} \), this SM is detected as an attacked SM and can be isolated from the arm circuit. \( U_{Cth1} \) and \( U_{Cth2} \) in this paper are set to 1.2\( U_{dc}/N \) and 0.8\( U_{dc}/N \), respectively. The proposed detection method can detect both step and stealthy FDIAs for the MMC, and the effectiveness of the method will be validated in the next section.
The detection flag is set to 0. When the step FDIA occurs, the false data is injected, the SM capacitor voltages seen by the central controller are identical with the real SM capacitor voltages. The corresponding parameters are listed in Table 1. There are 40 ordinary SMs and two redundant SMs in each arm of the MMC. The control period is set to 50 μs.

Figure 14 shows the waveforms of the MMC under a step FDIA. The detection method proposed in [26] is used in Figure 14. Before the false data is injected, the SM capacitor voltages seen by the central controller are identical with the real SM capacitor voltages. The detection flag is set to 0. When the step FDIA occurs, the false data $U_{C1_{j}}$ jumps to $-0.5$ as shown in Figure 14a, and the capacitor voltage $U_{C1}$ seen by the central controller is suddenly reduced as shown in Figure 14b. The step FDIA is detected according to the principle given in Section 4.1, and the detection flag is set to 1 to indicate there is an attacked SM in the arm. SM$_1$ is then isolated from the arm circuit by enabling the bypass switch, and the capacitor in SM$_1$ will be gradually discharged through a parallel-connected resistor.

Figure 15 shows the waveforms of the MMC using the proposed detection method under a step FDIA. The injected false data $U_{C1_{j}}$ is smaller than 0, which will reduce the capacitor voltage of SM$_1$ seen by the central controller. In this case, the capacitor voltage balancing algorithm will tend to increase the charging priority of SM$_1$ according to the principles presented in Section 2.2. Although the capacitor voltages seen by the central controller are gradually balanced, the real capacitor voltage of SM$_1$ is increased. After $U_{C1_{real}}$ exceeds the threshold, SM$_1$ can be detected when its operating mode is changed according to the detection principle proposed in Section 4.2.

Figure 13. Real capacitor voltage obtained according to (10): (a) switching function of SM$_1$ in the upper arm; (b) real capacitor voltage calculation; and (c) flowchart illustrates the process of deriving the real SM capacitor voltage.

5. Validation and Comparisons

The circuit of the MMC shown in Figure 2 was developed based on PSCAD/EMTDC. The corresponding parameters are listed in Table 1. There are 40 ordinary SMs and two redundant SMs in each arm of the MMC. The control period is set to 50 μs.
UCu1_real exceeds the threshold, SM 1 can be detected when its operating mode is changed to bypass switch, and the capacitor in SM 1 will be gradually discharged through a parallel-resistive path. The detection flag is set to 1. The stealthy FDIA can be bypassed by the cyberattack detector proposed in [26]. SM 1 in the upper arm is attacked as an example: (a) SM capacitor voltages seen by the central controller; (b) real SM capacitor voltages; and (c) detection flag. (d) SM in the upper arm is isolated.

Figure 14. Waveforms of the MMC under step FDIA after enabling the detection method proposed in [26]. SM1 in the upper arm is attacked as an example: (a) step FDIA; (b) SM capacitor voltages seen by the central controller; (c) real SM capacitor voltages; and (d) detection flag.

SM1 in the upper arm is attacked as an example: (a) SM capacitor voltages seen by the central controller; (b) real SM capacitor voltages; and (c) detection flag. (d) SM in the upper arm is isolated.

Figure 15. Waveforms of the MMC under step FDIA after enabling the proposed detection method. SM1 in the upper arm is attacked as an example: (a) step FDIA; (b) SM capacitor voltages seen by the central controller; (c) real SM capacitor voltages; and (d) detection flag.
The simulation results shown in Figures 14 and 15 verify that the detection methods proposed in [26] and this paper can both detect the step FDIA for the MMC.

The waveforms of the MMC using the detection method proposed in [26] under a stealthy FDIA are shown in Figure 16. It can be observed that the real SM capacitor voltage, \( U_{Cu1_{real}} \), increases to a large value, which can threaten the safe operation of the MMC. The cyberattack detector given in [26] fails to detect the stealthy FDIA, and the detection flag is always 0. It should be noted that various stealthy FDIAs other than the type shown in Figure 16 can be injected. Although the forms of stealthy FDIAs are different, they all can bypass the cyberattack detector proposed in [26].

Figure 16. Waveforms of the MMC under stealthy FDIA after enabling the detection method proposed in [26] SM\(_1\) in the upper arm is attacked as an example: (a) stealthy FDIA; (b) SM capacitor voltages seen by the central controller; (c) real SM capacitor voltages; and (d) detection flag.

Figure 17 shows the waveforms of the MMC using the proposed detection method. The performance is similar to the results shown in Figure 15. The stealthy FDIA can be successfully detected when the real capacitor voltage and operating mode transition of SM\(_1\) satisfy the detection principles. SM\(_1\) in the upper arm is isolated after the detection flag is set to 1.
Figure 17. Waveforms of the MMC under stealthy FDIA after enabling the proposed detection method. SM1 in the upper arm is attacked as an example: (a) stealthy FDIA; (b) SM capacitor voltages seen by the central controller; (c) real SM capacitor voltages; and (d) detection flag.

6. Conclusions

The MMC is the state-of-the-art topology used in recent VSC-HVDC systems. A cyberattack occurring in MMC can affect the normal operation of the converter system and even lead to damage to the components. FDIA represents a typical cyberattack with widely varied types and impacts. The stealthy FDIA with a more elaborate attack sequence can deceive and bypass the fault detector of the MMC proposed in the existing literature. In this case, although the capacitor voltages seen by the central controller of the MMC are well-balanced, the real capacitor voltage of the attacked SM will deviate from the normal value. To address this issue, this paper proposes a detection method to obtain the real SM capacitor voltages during the modulation process. The real capacitor voltage can be calculated according to the difference value of the arm voltage between two adjacent control steps. The FDIA on an SM is detected if the real SM capacitor voltage exceeds the prespecified thresholds. The proposed detection method is applicable to both centralized and decentralized control architectures for the MMC. The calculations given in (10–15) are realized in the central controller for the centralized control architecture. Instead, the calculations can be realized in the arm controller for the decentralized control architecture. Moreover, the proposed method can detect different FDIA forms (such as step data attack, ramp-changed data attack, and impulse data attack) once the real capacitor voltage of the attacked SM exceeds the threshold values. Simulation results verified the effectiveness of the proposed detection method.
Author Contributions: Methodology implementation and manuscript—writing, X.C.; document preparation and manuscript—writing, S.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

12. Cheng, G.; Song, S. Fault detection and identification in MMCs based on DSCNNs. Energies 2023, 16, 3427. [CrossRef]
15. Bae, W.; Zhou, M.; Abusorrah, A. A survey of cyber attacks on cyber physical systems: Recent advances and challenges. IEEE/CAA J. Autom. Sin. 2022, 9, 784–800. [CrossRef]


**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.