Energy Proceedings
Vol 30, 2023
ISSN 2004-2965

Selective Packet Dropping Attacks to BESS-integrated Smart Grids

Yongdong Wu[1], Xin Li[2*], Zhiquan Liu[1], Jilian Zhang[1], Kaimin Wei[1], Bingwen Feng[1] and Dejia Lin[1]

[1]Jinan University, Guangzhou, China

2 Sinocloud Wisdom Co. Ltd, Beijing, China (Corresponding Author: lixin@yunkouan.com)

ABSTRACT

As an important component for tackling temporal variability of renewable energy sources, a BESS (Battery Energy Storage System) periodically produces control packets to realize conversion between DC battery energy and AC energy. The present paper proposes attacks to a BESS-integrated smart grid by selectively dropping the control packets according to the unique dynamics of DC-AC energy conversion process in a BESS. As the present attacks are able to distort the grid voltage and frequency far beyond the limits specified in IEEE standards 519, hence may have detrimental effects on electrical equipment in single-phase/three-phase smart grids. The analysis and simulation results show that the attacks are viable. Finally, the paper proposes countermeasures on the present attacks by protecting channel's time-stamp and control signals.

Keywords: Smart grid security, Cyber-physical system security, Packet dropping attack, Battery Energy Storage System (BESS)

1. INTRODUCTION

According to the Global Futures Report from REN21 (The Renewable Energy Policy Network for the 21st Century) [1], the greenhouse gas concentration might pass the 400ppm threshold in the global atmosphere and would incur the most catastrophic climate disaster. Luckily, renewable energy sources (*e.g.*, wind and solar power) have a huge potential to reduce the greenhouse gas emissions, hence have been invested by many countries such as China, EU and USA. For example, 70% of net additions to global power generating capacities are renewable power because the cost of wind power and solar photovoltaic devices are continuously decreasing.

However, different from conventional power sources (*e.g.*, coal and crude oil), the renewable power resources (*e.g.*, wind and solar energy) are not always available steadily at any given location [2]. Therefore, a smart grid with high penetration of renewable power is challenged by the stochastic fluctuation of renewable power, and may be more vulnerable than the conventional smart grid in terms of voltage, frequency and phase stability [3].

A Battery Energy Storage System (BESS) provides a practical way to tackle temporal variability of intermittent energy generation by integrating BESS into smart grid. Specifically, BESS converts solar power into chemical energy at day time and releases the power at night with battery array. As a result, the smart grid avoids the adverse effect of peaks and troughs due to renewable power generations. As a BESS has high ramping capability and fast disturbance response property [4], it could obviously improve the stability performance of a smart grid. In addition, it can minimize the operating cost [5] and selectively dispatch the energy units [6]. Thus, BESS is becoming an essential component of a smart grid with renewable resources, and attracts growing interest all over the world [7].

Although BESS has the potential to optimize any smart grid with high penetration of renewable resources, a BESS-integrated smart grid confronts many known attacks [8] as its components, such as sensor, actuator and controller *etc.*, spread over a large public area and link together with a real-time network. Those attacks can be classified into four categories which are able to drive a smart grid out of its state boundaries. (1) *ADS (Adversarial Data Source)* attack which changes the physical variable measured by the sensors. For instance, ADS selectively changes the actual load consumption such that the power meter obtains incorrect readings [9]; (2) *FDI (False Data Injection)* which changes the input data of controller and/or actuator (*e.g.*, [10]). (3) *Delay attack* changes data delivery time [11]. In a closed-loop control system such as smart grid, delay is usually an important factor which reduces the system stability. Hence, if an attacker is able to delay the input of controller or actuator of the grid, the close-loop control system stability will decrease sharply; (4) *Packet dropping attack* takes effect when a component does not receive an expected packet timely and then uses the

previous input or estimate the input [12]. A dropping attack can be realized when an attacker directly drops the packets by sitting in the middle of communication channel, or the recipient drops the packets which are erroneous or timeout due to Denial-of-Service attack [13].

In order to ensure the existing attacks feasible, an attacker has to custom the attacks based on the domain knowledge of the target system. Currently, most of the research works on smart grid attack assume that the electricity energy waveform is sinusoidal (*e.g.*, the output of AC (Alternating Current) synchronization generator). However, in a BESS-integrated smart grid, BESS does not meet this assumption automatically. Instead, BESS needs a sinusoidal reference signal to convert DC (Direct Current) battery energy into AC waveform which must satisfy the compatibility requirement of smart grid [14]. Thus, it is necessary to investigate the security impact due to the DC-AC conversion process. To fill in this gap, the present paper identifies the unique security vulnerability of BESS-integrated smart grids. In brief, this paper presents selective packet dropping attacks which can prevent the controller or actuator from using the original data. The contributions of the present paper are as follows.

- Proposing attacks to BESS-integrated smart grid by dropping control packets for DC-AC conversion, periodically or selectively. The present attacks are
    - unique in BESS-integrated smart grids, simple in principle and easy to realize;
    - very effective in inducing high THD (Total Harmonic Distortion) with regard to the limits of IEEE standards 519 [15], or destabilizing a power grid if a large amount of battery capacities are disconnected from the grid;
    - applicable to single-phase grids, three-phase grids and their parallel forms;
    - different in parameter selecting from the conventional dropping attack.
- Proposing countermeasures on the present attacks by enforcing time synchronization, and replacing time-sensitive control data with time insensitive control data;
- Showing that a packet dropping attack is closely related to delay attack when ZOH (Zero-Order Hold) is considered in the close-loop system of a power grid;
- Performing analysis and simulation to demonstrate that the attacks and countermeasure are viable.

The remainder of this paper is organized as follows. Section 2 introduces BESS. Section 3 presents the packet dropping attack to BESS-integrated smart grid. Section 4 discusses the attack performance and countermeasures, and Section 5 demonstrates the attacks with abundant simulations. Finally, conclusions are drawn in Section 6.

2. BATTERY ENERGY STORAGE SYSTEM

BESS is popularly used to solve the variability and unpredictability problem of smart grid which has a high penetration rate of renewable power sources. To be self-contained, this section introduces the critical BESS structure, conversion mechanism and controllers.

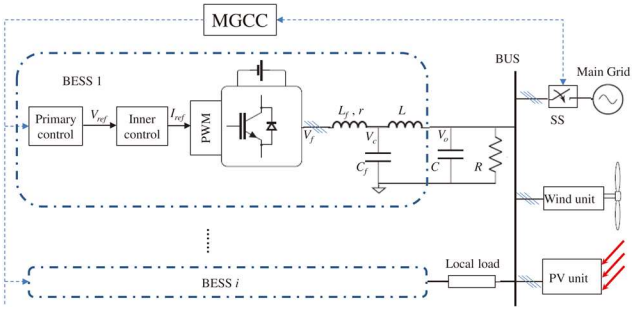

Fig. 1. Schema of a BESS-integrated smart grid. MGCC is used to integrate all the BESS, renewable power sources and the power bus. The primary and inner control enables to generate PWM to meet the power demand. The BESS output voltage $\mathrm{V_o}$ *is linked with local load* C, R *and power bus.*

2.1 BESS structure

As shown in Fig.1, a BESS consists of battery arrays used to store/release energy, inverters used for power conversion between DC and AC, LCL (including inductors L_f and L, capacitor C_f) resonance circuit to regulate the AC power into sine/cosine waveform. Optionally, a resistor r may be added to damp the LCL resonance and improve the system stability. In addition, the BESS is interfaced with local load (capacitor C, resistor R, and inductive load which is merged with inductor L) and MGCC (Micro-Grid Control Center) used to manage a multiple of BESS [16]. Due to the variety of renewable energy sources and requirements, a smart grid consists of multiple control layers: inner control, primary control, secondary control and tertiary control. The lowest layer is the inner control which is used to directly tune the generator or inverter [17]; primary control which responses with local BESS measurements [18]; secondary control is used to compensate the voltage and frequency deviations and performs the grid synchronization [19];

and the highest layer is tertiary control which performs the power regulation. Usually a lower layer controller has smaller step response time. In addition, a switch SS is used to connect with (and/or disconnect from) the main grid.

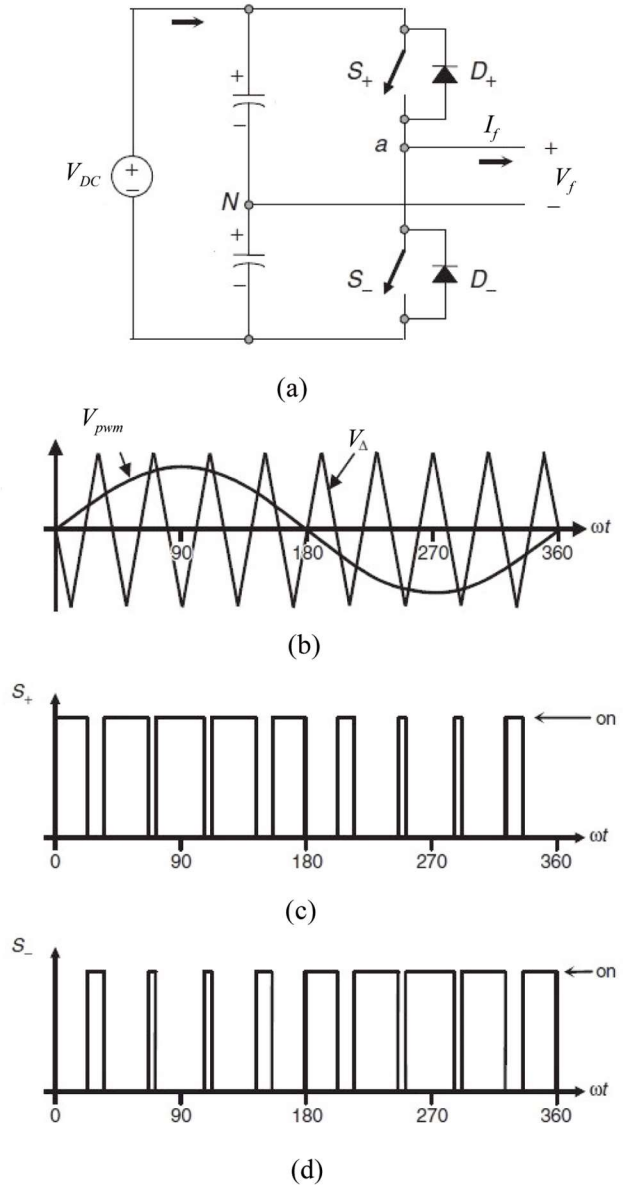

Fig. 2 Electricity energy DC/AC conversion. (a) Single-phase half-bridge VSI (Voltage Source Inverter); (b) Carrier V_Δ *and modulation signal* $\mathrm{V}_{\mathrm{pwm}}$*; (c) PWM for switch* S_+*; (d) PWM for switch* S_-*. Adapted from [20].*

2.2 DC-AC inversion in BESS

Fig.2 shows the process of DC-AC conversion with a half-bridge circuit [20]. In Fig.2a, the battery V_{DC} is the energy source, and switches S_+ and S_- (*e.g.*, Insulated Gate Bipolar Transistor, or IGBT for short) are used to control the direction of the output current I_f. Fig.2b exemplifies the generation of switch control according to a sinusoidal modulating signal V_{pwm} and triangular carrier signal V_Δ. Concretely, if $V_{pwm} > V_\Delta$, the control signals for S_+ is positive. Otherwise, the control signal for S_+ is negative. That is to say, the control signal for S_+ is a PWM (Pulse Width Modulation) signal as shown in Fig.2c. Meanwhile, the control signal for S_- is a complement of the control signal for S_+, as shown in Fig.2d. As a result, the output voltage V_f is AC when the PWM signals are used in controlling the switches in Fig.2a. For the full-bridge inversion and 3-phase DC-AC inversion, please refer to [20].

2.3 Inner controller of BESS

The ENTSO-E (European Network of Transmission System Operators for Electricity) specifies a non-critical frequency window for charging and discharging the battery. This window avoids running BESS primary control at near nominal frequency. However, the specification only regulates the power frequency at a coarse granularity. Moreover, it has less stability range and selective performance than a BESS inner control system [21].

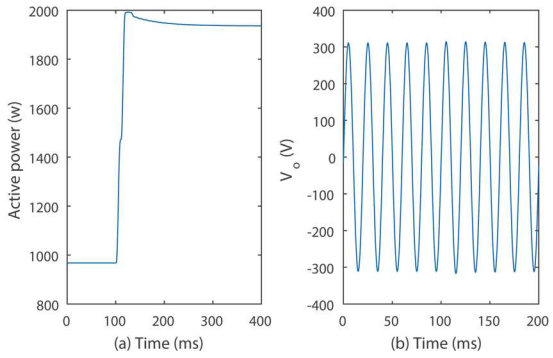

Fig. 3 Step response in BESS-integrated power system when the load demand is doubled from 968W ($= 220^2/50$*) to 1936W (*$= 220^2/25$*) at the time 100ms, by changing resistor* R *in Fig.1 from* 50Ω *to* 25Ω*. The RMS (Root Mean Square) of voltage is 220V.*

With regard to Fig.1, a BESS inner control system includes one current controller and one voltage controller. The reference input V_{ref} to the voltage controller is generated from the primary controller, and the reference input to the current controller is generated from the voltage controller. Current (and voltage) controller samples the LCL resonance circuit current (voltage respectively) as a feedback signal. The output V_{pwm} of current controller is compared with a predefined triangular signal V_Δ to generate a PWM

signal, as described in Subsection 2.2. The PWM signal is used to drive the inverters to empower local loads or global loads of smart grid. The popular controllers comprise PID (Proportional-Integral-Derivative) controller and PR (Proportional-Resonant) controller [22]. Because PID ensures a BESS-integrated power system to have a good step response in terms of output power and voltage stability (Fig.3), it is adopted to describe our attacks in the following.

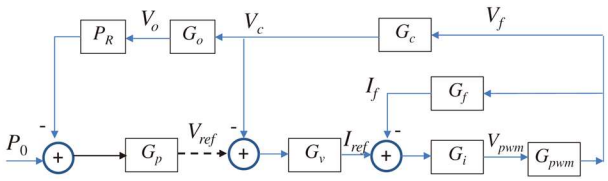

Fig. 4 System block diagram corresponding to Fig.1. The dashed line indicates the potential attack point. P_0 *is the power setpoint, and* $\mathrm{V}_{\mathrm{pwm}}$ *is used for generating PWM signal in Fig.2.*

2.4 Transfer functions of BESS

Fig.4 shows the diagram of a BESS system in Fig.1, where the inner controller, including a PID voltage controller $G_v(s)$ and PID current controller $G_i(s)$, is used to tune the electricity waveform, and PID primary controller $G_p(s)$ is used to adjust the active power. Their transfer functions are

$$G_i(s) = K_{ip} + \frac{K_{ii}}{\mathrm{s}} \quad (1)$$

$$G_v(s) = K_{vp} + \frac{K_{vi}}{\mathrm{s}} \quad (2)$$

$$G_p(s) = K_{pp} + \frac{K_{pi}}{\mathrm{s}} \quad (3)$$

for some control parameters such as K_{ip}, K_{ii} etc. Moreover, denote the L-R-C impedance in Fig.1 as

$$Z_o(s) = sL + \frac{R}{1+sRC} \quad (4)$$

and the total impedance

$$Z_f(s) = sL_f + \frac{Z_o}{1+sZ_oC_f} \quad (5)$$

Then, other transfer functions in Fig.4 are as follows.

$$G_f(s) = \frac{I_f(s)}{V_f(s)} = \frac{1}{Z_f} \quad (6)$$

$$G_c(s) = \frac{V_c(s)}{V_f(s)} = \frac{Z_o}{Z_f} \quad (7)$$

$$G_o(s) = \frac{V_o(s)}{V_c(s)} = \frac{\frac{R}{1+sRC}}{Z_o} = \frac{R}{s^2RLC+sL+R} \quad (8)$$

According to [16], the output of a primary controller $G_p(t)$ is $E(t)$, and the primary controller delivers the reference signal $V_{ref}(t) = E(t)cos(\omega t)$ to the voltage controller G_v. In addition, as the DC-AC conversion process $G_{pwm}()$ and power $P_R()$ are non-linear, it is hard to represent them with transfer functions.

3. ATTACKS TO BESS-INTEGRATED POWER GRIDS

In a BESS-integrated power system, the control schemes such as [23] are beneficial for the performance enhancement in either distributed or central smart grids. However, as the control signal will be communicated over a network, smart grid may suffer from the following attacks.

3.1 Security model

As a BESS-integrated power system will be one of most important infrastructures in the near future, its failure may result in significant loss in asset and even human life. Hence, an adversary aims to incur high disturbance to the BESS-integrated power system given that he is capable of

- *Knowing the detail of the target BESS-integrated power system to some extent*. Usually, the BESS system structure is publicly accessible for the sake of system compatibility;
- *Intercepting the network packet*. In a distributed smart grid, the control signal and system status may be delivered over a network such as 5G/TSN (Time Sensitive Network) which is accessible to the attacker;
- *Dropping the network packet*. An adversary is able to induce packet errors or make packet timeout, such that the receiver has to drop the packet.

In order to maximize his benefits, an attacker attempts to compromise a small number of BESS units or communication channels, but incur large damage to the main grid. Therefore, he will properly select attack points and attack methods. The attack point can be the control signal V_{pwm}, or reference signal V_{ref} in Fig.4. However, the former is usually very close to the battery array and may be tightly protected by the power operator. Hence, in this paper, the attacker is assumed to choose to manipulate the latter because V_{ref} varies over a large range and may be delivered over a wide-area (wireless/wired) network. The attack methods will be elaborated in Subsections 3.2 $\sim$ 3.3.

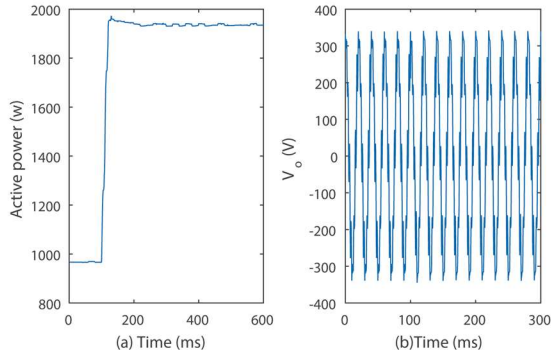

Fig. 5 Step response performed as Fig.3, but under periodic packet dropping attack. (a) the active power fluctuates, (b) the voltage is not sinusoidal clearly.

3.2 Time-selective packet dropping attack

In a BESS-integrated smart grid, the voltage controller will sample the input channel and output a control signal periodically. If it does not receive the control signal $V_{ref}(t)$ correctly and timely, it will ignore the control signal $V_{ref}(t)$, and may reuse the latest valid control signal $V_{ref}(t')$, $t' < t$, in the control algorithm. Hence, if the adversary continuously blocks the control channel, he may attack the BESS unit successfully. For instance, the attacker drops all the packets for $V_{ref}(t)$ if $t \in (2k, 2k+1)$ in millisecond, k is integer, the output active power fluctuates as shown in Fig.5a, and the output voltage waveform is not sinusoidal. That is to say, a packet dropping attack may decrease the quality of electricity power.

Corresponding to Fig.5b, Fig.6 shows that there are many harmonic frequency components, which significantly decreases voltage quality measured with total harmonic distortion

$$THD = \frac{\sqrt{a_2^2 + \cdots + a_i^2 + \cdots + a_N^2}}{a_1} \qquad (9)$$

where N is the number of frequencies in total, a_i is the voltage RMS (Root Mean Square) of the i-th harmonic frequency component, particularly, a_1 is the voltage RMS of the nominal frequency (*e.g.*, 50Hz in EU) component.

THD in Fig.6 is 25% which is much higher than the low-voltage harmonics limit 8% recommended in the IEEE-std 519 [15], and the highest individual harmonic frequency magnitude is 19% which is also much higher than the standard limit 5%. As harmonic distortion may cause high temperatures in conductors and transformers, as well as strong electronic-magnetic interference, the dropping attack can have detrimental effects on electrical equipment in the smart grid.

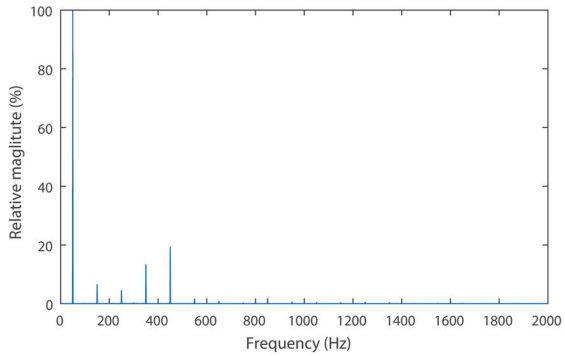

Fig. 6 The y-axis represents the RMS ratio $\frac{a_i}{a_1} \times 100\%$, a_i *is the RMS of the* ith *harmonic frequency component for the voltage waveform in Fig.5b.*

Although a periodic packet dropping attack is able to compromise a BESS-integrated smart grid and easy to be launched, it can be easily detected by the operator.

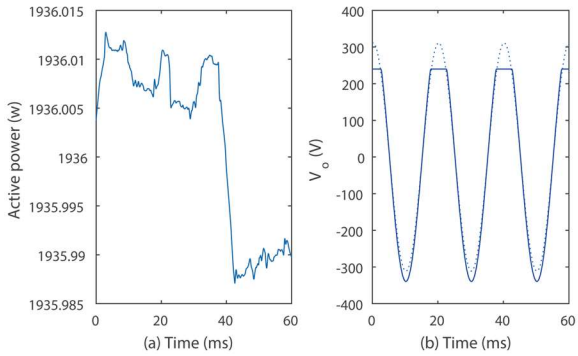

Fig. 7 Selectively drop packets for $V_{ref}(t)$ *whose phase angle is in the interval* $(-45^\circ, 45^\circ)$. *(a) Active power output; (b) The output voltage without attack (dash line) and with attack (solid line). The difference between these two lines is the difference* $V_b(t)$.

3.3 Value-selective packet dropping attack

If the adversary is able to sniff the reference signal V_{ref} from the transmission channel, or estimate V_{ref} with voltage and/or current measurement, he can selectively block the packets whose voltage $V_{ref}(t)$ are higher than a predefine value v_0. Therefore, the voltage controller receives $\tilde{V}_{ref}(t) = V_{ref}(t) - V_b(t)$, where $V_b(t)$ is the error due to attack. If $V_b(t)$ is periodic, there are noisy harmonic frequency components.

Fig.7 illustrates the effect of selective packet dropping attack, where an adversary blocks the packets for reference voltage $V_{ref} > v_0 = 220\sqrt{2}cos(45^\circ)$,

whose phase angle is in the interval $(-45^{\circ}, 45^{\circ})$. $V_b(t)$ is the difference between two lines in Fig.7b. Clearly, $V_b(t)$ has non-zero mean and harmonic frequency components, thus the output voltage (solid line in Fig.7b) also has non-zero mean and high harmonic distortion ($THD = 10.7\%$), although the output power in Fig.7a is normal.

4. DISCUSSIONS

This section will address attack feasibility, relationship of the attacks, performance analysis, extensions to more complex BESS, as well as countermeasures.

4.1 Attack feasibility

1) Attack process: In order to launch the present attacks, the adversary is required to access the channel used for delivering control signal. There are two options to satisfy the requirement: injecting malicious code (*e.g.*, the well-known Stuxnet attack) or interfering wireless communication.

Malicious code injection means that the adversary need insert some codes into the primary controller, voltage controller or current controller. Nonetheless, it is not required to change the controller code, but controller output time only. One example of such an injection code is a dummy function which consumes a lot of controller computation time or network communication bandwidth, such that the voltage controller can not receive or process the signal V_{ref} timely. For instance, if packet P will be sent at time t_0, the injection code will make the communication channel busy by continuously sending dummy packets between $(t_0, t_0 + t_1)$. Then P will be delivered at time $t_0 + t_1$ with a very high probability, i.e., its delay time is t_1. Similarly, given that packet P is delivered with period τ, if the injection code makes the communication channel busy for 3τ, two of three packets P will be dropped due to timeout. There are many real cases of code injection (*e.g.*, Stuxnet, PLC virus etc).

Presently, wireless communication (*e.g.*, 5G) is fast enough for real-time control system [24]. For a distributed BESS-integrated power grid, a wireless control channel has several advantages, including less connecting lines, strong anti-interference ability, low system redundancy, high reliability and easy expansion [25]. Thus, wireless control system will be promising in real-time industrial applications. However, wireless communication channel is vulnerable to jamming attack [26] which enables the adversary to choose packet delay time or produce erroneous packets. Once a packet is erroneous, the packet will be retransmitted. Thus, the jamming time determines the successful re-transmission time, i.e., packet delay. If the jamming time is longer than the control period, the delayed packet will be dropped due to timeout.

2) Parameter selection: In order to realize the present packet dropping attacks, the attacker shall choose suitable attack parameters, *i.e.*, threshold value v_0. To this end, the attacker will randomly start the attack with random value v_0, or phase angle ϕ_0. As the output voltage of the smart grid is public, the attacker is able to measure the THD easily. If the THD is smaller (*e.g.*, too small to activate the switch SS in Fig.1) after attacking the grid for 1 second, the attacker will start a new phase angle the $\phi_0 \longleftarrow \phi_0 - \Delta_0$ for some step Δ_0, and repeat the attack process. Subsection 5.4 shows that the trial-and-error searching process can converge quickly.

4.2 The delay factor of dropping attacks

It is well-known that delay factor will decrease the system stability in control community. Indeed, packet dropping attack has similar effect as delay attack. Specifically, in the system diagram Fig.1, the controllers sample the LCL circuit and load, then produce the control output in a control period τ. Hence a ZOH (Zero Order Hold) is necessary to keep the input and output constant in the period τ. ZOH's transfer function.

$$G_{ZOH}(s) = \frac{1 - e^{-s}}{s\tau}, \qquad (10)$$

and frequency response function

$$G_{ZOH}(j\omega) = \frac{1 - e^{-j\omega\tau}}{j\omega\tau} \approx \frac{\sin\left(\frac{\omega\tau}{2}\right)}{\frac{\omega\tau}{2}} e^{-\frac{j\omega\tau}{2}} \qquad (11)$$

That is to say, ZOH has a delay factor $e^{-s\tau/2}$ approximately. Thus, if an adversary launches packet dropping attack such that only one control packet is received for every period $k\tau$, where k is a predefined positive integer, the control period is implicitly increased to $k\tau$. *i.e.*, by changing the number of dropping packets, the attacker can realize the delay attack effect too.

4.3 THD analysis

In order to investigate its stability, smart grid is usually approximated as a linear time-invariant system. According to the smart grid model in Fig.4, if the control signal V_{ref} is constrained, output voltage V_o will be restrained similarly.

Suppose V_{ref} is a sinusoidal function, the attacker selects the positive constraining point $v_0 = |V_{max}cos(\phi_0)|$ for some constrained voltage angle ϕ_0, and drops all the packets whose control value $V_{ref}(t) =$

$V_{max}cos(\omega t) > v_0$. Let's represent the signal $\tilde{V}_{ref}(t)$ received by the voltage controller as Fourier series

$$\tilde{V}_{ref}(t) = a_0 + \sum_{n=1}^{+\infty} a_n \cos(n\omega t) + b_n sin\ (n\omega t)$$
$$= a_0 + \sum_{n=1}^{+\infty} a_n \cos(n\omega t) \quad (12)$$

where Eq.(12) holds because $\tilde{V}_{ref}(t)$ is an even function. If the adversary launches the single-side attack, *i.e.*, any packet for control data $V_{ref} > v_0$ will be dropped, the total harmonic distortion is

$$THD = \sqrt{\frac{|a_2|^2 + |a_3|^2 + \cdots + |a_n|^2 + \cdots}{|a_1|^2}}$$
$$\approx \sqrt{\frac{|a_2|^2 + \cdots + |a_n|^2 + \cdots + |a_N|^2}{|a_1|^2}} \quad (13)$$

where Eq.(13) is derived because $|a_N|$ $(n > N)$ is sufficiently small for large N.

Similarly, if the adversary launches the double-side attack, *i.e.*, all the packets for control value $|V_{ref}(t)| > v_0$ are blocked. Then $\tilde{V}'_{ref}(t) = \sum_{n=1}^{+\infty} a'_n cos(n\omega t)$. Therefore, the total harmonic distortion due to the double-side attack is

$$bTHD \approx \sqrt{\frac{|a'_2|^2 + \cdots + |a'_n|^2 + \cdots + |a'_N|^2}{|a'_1|^2}} \quad (14)$$

Fig.8 illustrates Eq.(13) and Eq.(14). THD is usually higher than the limit 8% recommended in the IEEE-std 519 [15], in either single-side attack or double-side attack when the constrained angle $\phi_0 > 5^\circ$. Therefore, the output voltage $V_o(t)$ will have high THD in the BESS model, *i.e.*, the selective dropping attack is effective. Similar analysis shows that other present attacks are viable too.

4.4 Extension to one-phase BESS-integrated Micro-grids

When a multiple of BESS are linked to the power bus in parallel as shown in Fig.1, the present attacks will still be applicable to each BESS. In addition, if an adversary attacks the control signals of all but one BESS unit, the non-attacked BESS unit may have a large direct current input from other units, hence may be damaged. This case is similar to charging battery with large current. For instance, assume that all the BESS units are identical, and the MGCC issues the same command to them. If the BESS unit U is not attacked, but others are attacked by selectively dropping attacks introduced in Subsection 3.3, unit U will have the DC power flow and stay in charging or discharging status all the time, and hence become malfunction.

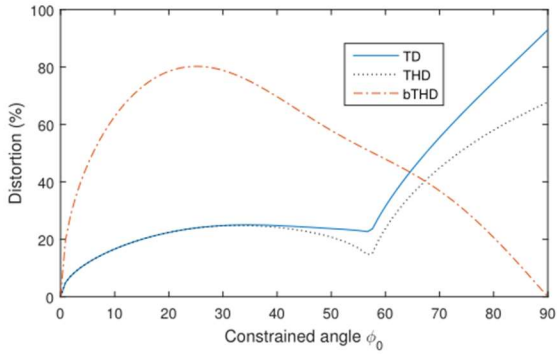

Fig. 8 THD varies with restraining point. TD is the distortion which includes the DC component.

4.5 Extension to three-phase BESS-integrated Micro-grids

Nowadays, there are three major controllers for three-phase BESS: ABC controller, $\alpha\beta$ controller, and dq controller. In the ABC controller, each phase is operated independently. Thus, the attacks addressed in Section 3 can be directly launched on each phase. In another two controllers, Clarke-Park transformation [27] are employed to decouple the correlation among the ABC phases, and then the controller signal is produced and executed on each transformed signal independently. Thus, the attacks addressed in Section 3 can be directly started on the transformed domain too.

4.6 Extension to BESS-integrated main grids

Based on the status of power bus, a switch SS is used to connect/disconnect with the main grid so as to provide a stable and economical power supply. However, if a large number of BESS are connected with the same main grid, the attacker can attack the main grid indirectly because a compromised BESS will become a very high disturbance source. Specifically, the attacker compromises a sufficient number of BESS simultaneously such that their output powers are of low quality in terms of voltage value, frequency or phase. In this case, the main grid will immediately be disconnected with the compromised BESS in order to guarantee its quality of power. As a large amount of power supply lost suddenly, the main grid may be blackout. For example, if the grid-scale 300 MW lithium-ion battery energy storage in California USA is disconnected, the main grid in California may suffer seriously.

4.7 Countermeasures

Abnormality detection is an effective way to thwart attacks. If a BESS is being attacked with the present schemes, a BESS controller is able to detect the abnormal THD, and autonomously disconnected from the BUS or main grid in Fig.1. Although the above abnormal detection method is able to prevent hazardous effect propagation to the smart grid, it is a passive and after-fact protection mechanism. Even worse, this countermeasure may propagate the damage to main grid (Refer to Subsection 4.6).

In order to protect the BESS proactively, the controller hardware and software shall be trusted, *e.g.*, by code attestation, so as to prevent code injection attack. Afterwards, it shall prevent the adversary from taking advantage of the communication channel. Although it is hard to prevent an adversary from sniffing the communication network, especially the wireless network, the following steps significantly enhance data and time resilience of the communication channel.

Firstly, the devices within the grid must be ensured to be synchronized such that their time differences are within a predefined interval in normal cases, by adopting NTP (Network Time Protocol), GTP (Grid Time Protocol), or other protocols. Afterwards, for each message transferred between two devices, the sender adds a timestamp t_0 and the receiver will check the timestamp t_0 against its local time t_1. Once the number of timeout packets or erroneous packets is beyond the predefined threshold interval, the BESS-integrated power system shall raise an alarm, or take other predefined actions.

Secondly, the primary controller delivers $E(t)$, instead of $V_{ref}(t)$, to the voltage controller control. After receiving $E(t)$, the voltage controller re-calculates $V_{ref}(t) = E(t)cos(\omega t)$ with a new pre-processing module. Empirically, $E(t)$ is only slightly changed in a short period, *i.e.*, $E(t) \approx E(t')$, where $t = t' + \delta$ for some small positive δ and $E(t')$ is the latest data accepted by the receiver. After receiving $E(t)$ as input, the pre-processing module derives the reference value

$$V_{ref}(t) = E(t)cos(\omega t) = E(t)cos(\omega(t' + \delta)) \approx E(t')cos(\omega t') = V_{ref}(t') \quad (15)$$

where Eq.(15) holds as $cos(\omega\delta) \approx 1$ and $sin(\omega\delta) \approx 1$ for small δ. Hence, packet delay and/or dropping only have minor impact on the input of G_v, thus the countermeasure will defeat the present attacks.

Fig.9 is used to demonstrate the countermeasure effect. As shown in Fig.9a, if at least one control packet is received within 20ms, power consumption will become stable due to the above countermeasure. Similarly, Fig.9b also demonstrates that the voltage waveform in Fig.7b will become normal due to the second step of the above countermeasure.

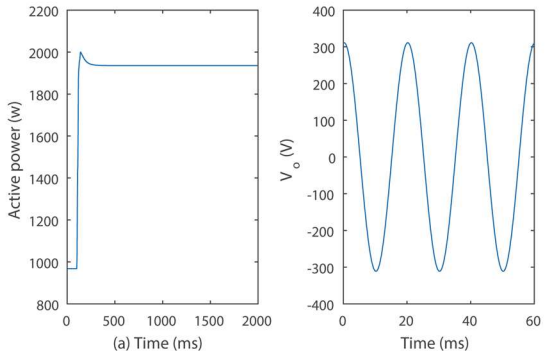

Fig. 9 Countermeasure against packet dropping attack (with reference to Fig.7b) by replacing $\mathrm{V_{ref}(t)}$ *with* $\mathrm{E(t)}$ *in the communication channel.*

Note that the channel between primary controller and voltage controller shall be protected with the well-known methods. That is to say, before being sent over the communication channel, any message m (including timestamp and $E(t)$) shall be authenticated and encrypted as $\mathcal{E}(key, m|\mathcal{H}(m))$, where $\mathcal{E}(\cdot)$ is a standard cipher (*e.g.*, AES), $\mathcal{H}(\cdot)$ is the standard hash function (*e.g.*, SHA-1), $x|y$ is the concatenation of strings x and y, and key is a key shared between the sender and the receiver. Thus the attacker is unable to know the control message m, and unable to change m without being detected either.

5. EXPERIMENTS

In the following experiments, the parameters in Fig.1 are as follows: system parameters $\boldsymbol{L_f}$ = 2.66 mH, $\boldsymbol{C_f}$ = 470 $\boldsymbol{\mu}$F, $\boldsymbol{C} = \boldsymbol{2.66\,\mu}$F, $\boldsymbol{L}$ = 3.55 mH, $\boldsymbol{R}$ = 50 $\boldsymbol{\Omega}$. The primary controller $\boldsymbol{G_p(s) = K_p + K_i/s = 0.15 + 1.5/s}$, the voltage controller $\boldsymbol{G_v(s) = 3 + 5/s}$, and the current controller $\boldsymbol{G_i(s) = 3 + 10/s}$. The triangular frequency $\boldsymbol{f_s}$ = **10**kHz, the nominal frequency $\boldsymbol{f_0}$ = **50**Hz, AC voltage RMS is 220V, and the battery voltage $\boldsymbol{V_{DC}}$ = 600 Vdc.

5.1 Sensitivity of estimate error in packet dropping attack

If the communication channel for $V_{ref}(t)$ is authentically encrypted with the above countermeasure, an attacker is unable to know $V_{ref}(t)$ correctly. Thus, to start packet dropping attack, the attacker has to derive the estimate $\hat{V}_{ref}(t)$ of $V_{ref}(t)$ based on the BESS model and measurement on the power line, and then selectively drops the packets for voltage $V_{ref}(t)$ whose estimate $\hat{V}_{ref}(t) > v_0$.

As shown in Fig.10, the selective dropping attack always incurs a high THD when the ratio of estimate error ($\hat{V}_{ref}/V_{ref} - 1$) varies over interval (-50%, +50%). It means that the packet dropping attack is insensitive to estimate error.

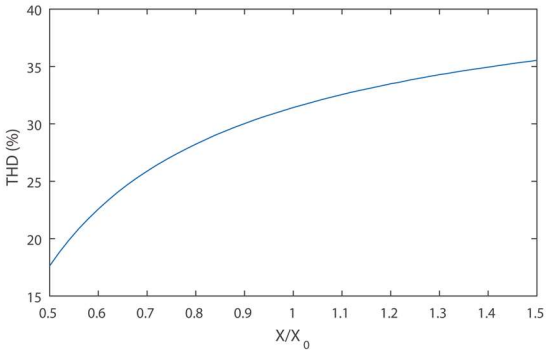

Fig. 10 The effect of selective dropping attack when the attacker has to estimate the reference voltage $\mathrm{V_{ref}(t)}$*, where* $\mathrm{v_0 = 100}$*V, x-axis* $\mathrm{X/X_0}$ *is the ratio between attacker's estimate* $\hat{V}_{ref}$ *and original* $\mathrm{V_{ref}}$.

5.2 Impact of system parameters on packet dropping attack

In this experiment, we evaluate the attack performance by changing the BESS parameters and primary controller parameters. To this end, we change parameters (K_i, K_p, C_f, L_f) one by one when $v_0 = 100$V. As shown in Fig.11, when the ratio of parameter value varies over the interval (-50%, +50%), the THD due to the dropping attack is always high. Thus, the dropping attack is robust against system parameter deviation.

5.3 Selection of dropping attack time

Let the ratio $\rho = \frac{\sigma}{\mu}$ as an indicator of the active power stability, where the active power is the load consumption in Fig.1, its standard variance is σ, and mean is μ.

Denote the phase of $V_{ref}(t)$ as $\phi(t) \in [-180^{\circ}, 180^{\circ})$. In this experiment, the attacker drops packets for $V_{ref}(t)$ whose phase $\phi \in (-\phi_0, \phi_0)$ for some $\phi_0 \in (0, 90^{\circ})$. Hence the dropping attack time is $T\phi_0/180$ for the nominal electricity period T.

With reference to Fig.12, when the dropping attack time increases, the disturbance of output power tends to be higher. However, there are some peaks (x_i, y_i) in Fig.12. That is to say, longer dropping attack time does not mean better attack effect. To find the optimal dropping attack time x_i, the attacker shall measure the output voltage/current of smart grid, and then adjust his attack time to maximize the power fluctuation. In addition, as packet dropping attack is closely related to delay attack (Subsection 4.2), and a long dropping attack means large delay which will result in high instability. However, this experiment shows that the present dropping attack to DC-AC mechanism is different from general dropping attack.

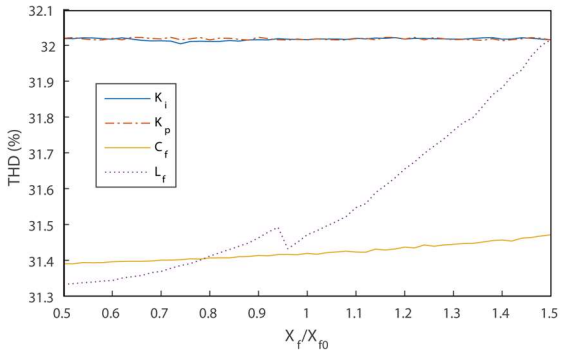

Fig. 11 Robustness of packet dropping attack, where $\mathrm{v_0 = 100}$ *V. The x-axis is the change ratio of parameters* $(\mathrm{K_i, K_p, C_f, L_f})$.

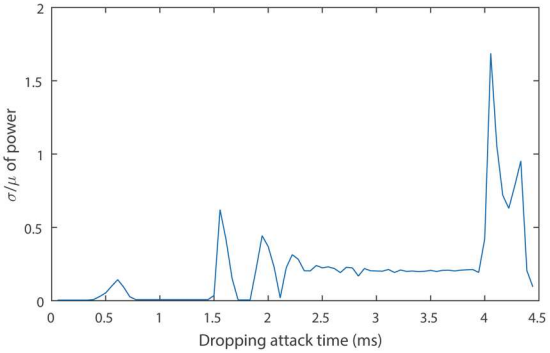

Fig. 12 Power stability due to dropping attack time, $\mathrm{T = 20}$ *ms. All the packets in the dropping period are discarded assuming that the attacker knows the time of phase angle 0.*

5.4 Sensitivity of selective dropping parameters

As a generalization of the attack described in Subsection 5.3, the attacker will drop packets for reference voltage angle $\phi \in (-\phi_0, len - \phi_0)$for some $\phi_0 \in (0, 90^{\circ})$, whether $T \times len/360$ is the dropping attack time. In Subsection 5.3, $len = 2\phi_0$. Let's study the impact of (ϕ_0, len) on attack performance.

In the first experiment, let $\phi_0 = -45^{\circ}$, and the packet dropping time len is changed. With regard to Fig.13, a dropping attack with a random len will result in a higher THD than the limits of IEEE-std 519 with a high probability.

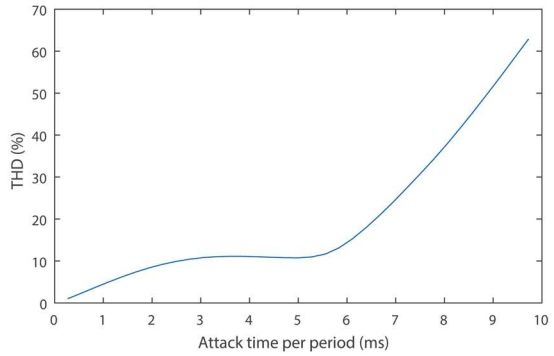

Fig. 13 THD varies with the dropping attack time len*, where* $\phi_0 = -45^{\circ}$.

In the second experiment, let $\phi_0 = 54^{\circ}$ and the start attack angle ϕ_0 is changed. With reference to Fig.14, a dropping attack with a random ϕ_0 will also result in the similar effect as the first experiment.

According to the above two experiments, we know that there are many pairs of (ϕ_0, len) which can distort the smart grid. As it is easy and quick for an attacker to verify whether the attack is successful or not, the attacker can find a suitable (ϕ_0, len) pair to launch the packet dropping attack.

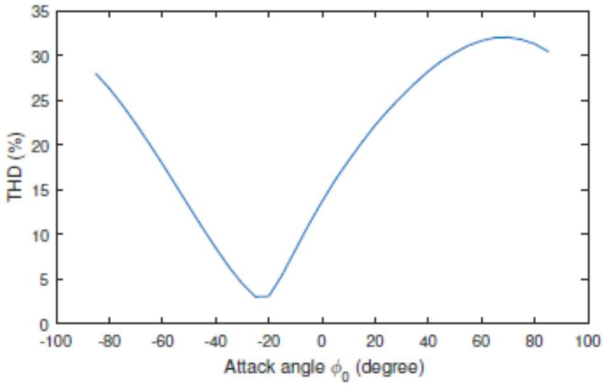

Fig. 14 THD varies with angle ϕ_0*, where* $\mathrm{len} = 54^{\circ}$.

6. CONCLUSION

The large-scale integration of renewable generation directly affects the reliability of smart grid. Although BESS has clear benefits in improving the reliability of the grid, it can also bring new security challenges in malicious situations.

As BESS-integrated smart grid usually adopts PWM control on DC-AC inverters, the control signal must be produced from external reference sources to meet the external power demand. By exploiting this control mechanism, the present paper enables to degrade the BESS-integrated smart grid by selectively dropping the control packets. According to the analysis and simulation results, the attacks are viable even if the BESS parameters vary over a wide range. In addition, the dropping attacks are closely related to the delay attack because an adversary can make ZOH in the close-loop BESS as a controllable delay factor.

As the present attacks do not modify the hardware/software in the BESS-integrated smart grid, they are immune to the defense technologies based on cryptographic primitives. In order to defeat the present attacks, the control components shall be synchronized to diagnose the communication channels, and the reference signal is generated in the inner controller.

ACKNOWLEDGEMENT

This work was in part supported by Key-Area Research and Development Program of Guangdong Province (Grant No. 2020B0101090004), National Natural Science Foundation of China (Grant No. 61932011), Guangdong Key R&D Plan2020 (Grant No. 2020B0101090002), Guangdong Basic and Applied Basic Research Foundation (Grant No. 2019B1515120010, No. 2019B03030200), National Key Research and Development Plan of China (Grant No. 2020YFB1005600) and National Joint Engineering Research Center for Network Security Detection and Protection Technology, Guangdong Key Laboratory for Data Security and Privacy Preserving.

REFERENCE

[1] REN21, "Renewables Global Futures Report: Great debates towards 100 % renewable energy," 2017. http://www.ren21.net/future-of-renewables/global-futures-report/

[2] A. Berrada and K. Loudiyi, "Operation, Sizing, and Economic Evaluation of Storage for Solar and Wind Power Plants," Renewable and Sustainable Energy Reviews 59, pp.1117-1129, 2016.

[3] P. Kundur, et al. "Definition and Classification of Power System Stability: IEEE/CIGRE Joint Task Force on Stability Terms and Definitions," IEEE Trans. on Power Systems, 19(3):1387-1401, 2004.

[4] H.-I Su and A. E. Gamal, "Modeling and Analysis of the Role of Energy Storage for Renewable Integration: Power Balancing," IEEE Trans. On Power Systems, 28(4):4109-4117, Nov. 2013.

[5] Y. J. Zhang, C. Zhao, W. Tang, and S. H. Low, "Profit-Maximizing Planning and Control of Battery Energy Storage Systems for Primary Frequency Control," IEEE T. on Smart Grid (TSG), 9(2):712-723, 2018.

[6] O. Megel, et al., "Distributed Secondary Frequency Control Algorithm Considering Storage Efficiency," TSG, 9(6):6214-6228, 2018.

[7] Z. G. Yang, “It’s Big and Long-Lived, and It Won’t Catch Fire: The Vanadium Redox-Flow Battery,” IEEE Spectrum, 26 Oct. 2017.
[8] M. Stone, “Are energy storage systems open to cyberattacks?,” http://energystoragereport.info/. 23 Jul. 2018.
[9] Y. Wu, et al., “False Load Attack to Smart Meters by Synchronously Switching Power Circuits,” TSG, 10(3):2641-2649,2019.
[10] H. Baskaran, et al., “Data falsification attacks in advanced metering infrastructure,” Bul. of Elec. Eng. and Inf., 10(1):412-418, Feb. 2021
[11] X. Lou, C. Tran, R. Tan, D. K.Y. Yau, and Z. T. Kalbarczyk, “Assessing and Mitigating Impact of Time Delay Attack: A Case Study for Power Grid Frequency Control,” ACM/IEEE Conf. on CPS, 2019.
[12] P. Mahish, A. K. Pradhan, and A. K. Sinha,, “Wide Area Predictive Control of Power System Considering Communication Delay and Data Drops,” IEEE Trans. on Industrial Informatics, 15(6):3243-3253, 2019.
[13] A. Huseinovic, et al., “A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid,” IEEE Access, pp. 177447-177470, 2020.
[14] S. Liu, et al., “Stability Analysis of Grid-Interfacing Inverter Control in Distribution Systems With Multiple Photovoltaic-Based Distributed Generators,” IEEE Trans. on Ind. Electronics, 63(12):7339-7348, 2016.
[15] IEEE Std 519, IEEE Recommended Practice and Requirements for Harmonic Control in Electric Power Systems, New York, IEEE. 2014.
[16] I. Ziouani, et al.,“Hierarchical Control for Flexible Microgrid Based on Three-Phase Voltage Source Inverters Operated in Parallel,” Electrical Power and Energy Systems 95, pp.188-201, 2018.
[17] P. Rodriguez, et al.,“Flexible Grid Connection and Islanding of SPC-Based PV Power Converters,” IEEE Trans. on Industry Applications, 54(3):2690-2702, 2018.
[18] Z. Akhtar, B. Chaudhuri, Shu Yuen Ron Hui, “Primary Frequency Control Contribution from Smart Loads Using Reactive Compensation,” IEEE Trans. on Smart Grid, 6(5):2356-2365, 2015.
[19] Q. Shafiee, J. M. Guerrero, and J. C. Vasquez, “Distributed Secondary Control for Islanded Microgrids - A Novel Approach,” IEEE Trans. On Power Electronics, 29(2):1018-1031, Feb. 2014.
[20] J. R. Espinoza, “Inverters,” Chapter 15, Power Electronics Handbook: Devices, Circuits and Applications (3rd Edition), Elsevier, 2011.
[21] P. Yang, Y. Xia, M. Yu, W. Wei, and Y. Peng, “A Decentralized Coordination Control Method for Parallel Bidirectional Power Converters in a Hybrid AC-DC Microgrid,” IEEE Trans. on Industrial Electronics, 65(8):6217-6228, 2018.
[22] J. C. Vasquez, J. M. Guerrero, M. Savaghebi, J. Eloy-Garcia, and R. Teodorescu, “Modeling, Analysis, and Design of Stationary-Reference-Frame Droop-Controlled Parallel Three-Phase Voltage Source Inverters,” IEEE Trans. on Industrial Electronics, 60(4):1271-1280, 2013.
[23] T. Zhao and Z. Ding, “Cooperative Optimal Control of Battery Energy Storage System Under Wind Uncertainties in a Microgrid,” IEEE Trans. on Power Systems, 33(2):2292-2300, 2018.
[24] J. M. Guerrero, J. Matas, L. Vicuna, M. Castilla, J. Miret, “Wireless-Control Strategy for Parallel Operation of Distributed-Generation Inverters,” IEEE Trans. on Industrial Electronics, 53(5):1461-1470, 2006.
[25] X. Guo and W. Chen, “Control of Multiple Power Inverters for More Electronics Power Systems: A Review,” CES Trans. on Electrical Machines and Systems, 2(3):255-263, 2018.
[26] P. Danzi, C. Stefanovic, L. Meng, J. M. Guerrero, and P. Popovski, “On the Impact of Wireless Jamming on the Distributed Secondary Microgrid Control,” in Proc. IEEE Globecom Workshops, pp.1-6, 2016.
[27] S. Golestan, J. M. Guerrero, and J. C. Vasquez, “Three-Phase PLLs: A Review of Recent Advances,” IEEE Trans. on Power Electronics, 32(3):1894-1907, Mar. 2017.