Contents lists available at ScienceDirect

Engineering

journal homepage: www.elsevier.com/locate/eng

Research
Active Support of Power System to Energy Transition—Article

Programmable Adaptive Security Scanning for Networked Microgrids

Zimin Jiang [a], Zefan Tang [a], Peng Zhang [a,*], Yanyuan Qin [b]

[a] Department of Electrical and Computer Engineering, Stony Brook University, Stony Brook, NY 11794, USA
[b] Department of Computer Science and Engineering, University of Connecticut, Storrs, CT 06269, USA

ARTICLE INFO

Article history:
Received 21 July 2020
Revised 14 November 2020
Accepted 29 March 2021
Available online xxxx

Keywords:
Networked microgrids
Programmable adaptive security scanning
Coordinated detection
Software defined networking

ABSTRACT

Communication-dependent and software-based distributed energy resources (DERs) are extensively integrated into modern microgrids, providing extensive benefits such as increased distributed controllability, scalability, and observability. However, malicious cyber-attackers can exploit various potential vulnerabilities. In this study, a programmable adaptive security scanning (PASS) approach is presented to protect DER inverters against various power-bot attacks. Specifically, three different types of attacks, namely controller manipulation, replay, and injection attacks, are considered. This approach employs both software-defined networking technique and a novel coordinated detection method capable of enabling programmable and scalable networked microgrids (NMs) in an ultra-resilient, time-saving, and autonomous manner. The coordinated detection method efficiently identifies the location and type of power-bot attacks without disrupting normal NM operations. Extensive simulation results validate the efficacy and practicality of the PASS for securing NMs.

1. Introduction

Networked microgrids (NMs) can not only flexibly accommodate distributed energy resources (DERs), but also operate autonomously and cooperatively to overcome possible power deficiencies and prevent power outages [1,2]. As a typical cyber–physical system, NMs increasingly rely on computer networking technologies to manage coordinated operations, handle contingencies, and facilitate the implementation of microgrid applications [3]. However, this introduces potential vulnerabilities [4]. Significant amounts of data, including those measured by sensors monitoring NMs' operational conditions and various control signals applied to accomplish different microgrid applications, need the assurance of confidentiality, integrity, and availability to achieve secure and reliable NM operations [5]. In addition, the distributed and plug-and-play nature of DERs presents challenges because they are owned and operated by separate microgrid owners, while NM operators have insufficient capability to manage high DER security levels. A series of new technical challenges must be addressed by the NMs to manage these emerging risks, specifically the development of new countermeasures to identify and mitigate threats to microgrid operations on DER-targeted attacks [6], that is, the use of power bots, which are DER devices controlled by remote attackers [1]. Therefore, addressing these challenges requires that NM operators implement new approaches to detect cyberattacks on independently owned microgrids.

As fundamental NM components, DERs can not only generate electricity but also serve as sophisticated management tools enabled by multifunctional inverters with wired and/or wireless connections [7]. The prevalence of this DER type and the increased deployment of information and operational technologies significantly extend network connectivity, thus expanding the cyberattack surface. To enable a more flexible, reliable, and resilient system, some inverters often integrate cyber elements, including various communication and computing infrastructures [8]. However, these will inevitably increase the cyberattack risks on portions of the DER inverter functions, even hijacking the entire DER inverter. Therefore, attackers are not constrained to attacking communication-based microgrid functions or applications. These functions or controls of DER inverters depending less on communication, such as droop control, can also be compromised [9]. By compromising the DER inverters, the attacker can severely deteriorate or collapse the microgrids, resulting in a significant loss of power systems. Different attacks have been proposed in recent years, among which the power-bot attack is a critical threat to reliable inverter operations owing to its complexity and drastic destruction [10,11]. A single attack scheme, such as simply

[*] Corresponding author.
E-mail address: p.zhang@stonybrook.edu (P. Zhang).

https://doi.org/10.1016/j.eng.2021.06.007
2095-8099/

Please cite this article as: Z. Jiang, Z. Tang, P. Zhang et al., Programmable Adaptive Security Scanning for Networked Microgrids, Engineering, https://doi.org/10.1016/j.eng.2021.06.007

modifying the parameters of an inverter's controller, is likely to be detected [1,12]. However, these methods fail to work under hybrid cyberattacks.

In practice, attackers are not constrained to follow prescribed schemes. Informed attack schemes combining intrigue, coordinated, and simultaneous attacks can cause more devastating damage [13,14]. Attack detection must make use of certain approaches to identify malicious microgrid attacks and then take effective countermeasures to eliminate their adverse effects on stable and reliable microgrid operations. Recent work on joint attack detection primarily focuses on false data injection, deception, and denial of service attacks on advanced metering infrastructure related functions [15], such as load frequency control. These studies apply residue or state estimation approaches, including the use of Kalman filters [16], state forecasting [17], watermarking [10], and data-driven techniques [18,19]. Reliance on the system model and parameters is the key shortcoming of model-based algorithms for injection and replay attacks. Even slight uncertainties in these parameters may result in a false detection performance [20]. Furthermore, the heavy computational complexity prevents the application and scalability of these algorithms, especially when an iterative process is involved with divergence issues. The selection of a fixed threshold setting may also lead to falsified attack detection performance, especially when the NMs experience dynamic or loading variations. Although the data-driven methods reduce the erroneous detection performance caused by the parameters and modeling uncertainties, the need for extensive training samples along with a time-consuming training process can hardly be suitable for detection of DER-targeted attacks, as these methods may perform well for the selected training cases, but not for all cases, and the inverter controller models and parameters continuously change [21]. Therefore, most of these existing models, parameter-, or data-dependent approaches are hardly appropriate for the detection of more sophisticated power-bot attacks targeting DER controllers with improved privacy and varying control strategies in a dynamic networking environment [22].

Meanwhile, employing advanced communication infrastructure and network management techniques provides significant benefits for NMs [1,8]. Software defined networking (SDN) is an innovative technique that promotes programmable, scalable, and fast-responding operations in NMs [23]. In particular, adopting SDN facilitates the integration of DERs with various communication techniques, direct network programmability, system-wide communication visualization, and enhanced cyber security and system resilience [24]. Moreover, SDN has revolutionized the detection and mitigation of cyberattacks on networks by enabling the implementation of different promising defending algorithms [8,25]. However, there lacks an SDN-integrated scheme for NMs in the literature that is capable of detecting and mitigating multiple power-bot attacks.

To bridge these gaps, this study focuses on the detection and mitigation of power-bot attacks using informed schemes. Specifically, the three most common attack types, namely controller manipulation (topology modification and parameter overwriting), replay, and injection attacks, are considered. A programmable adaptive security scanning (PASS) architecture was devised. This approach employs both the SDN technique and a novel coordinated detection method capable of enabling programmable, scalable, and ultra-resilient NMs in a simplified, time-saving, and autonomous manner. The coordinated detection method equipped with two devised real-time detectors is designed to identify power-bot attacks without restrictions of attack schemes on DER controllers. The key contributions of this study are as follows:

(1) A novel SDN-enabled PASS architecture is designed for the real-time detection of power-bot attacks on DER inverters with significant flexibility, scalability, and ultra-resilience.

(2) A novel coordinated detection method equipped with two detectors was devised to efficiently detect power-bot attacks.

(3) The PASS detection rules in droop-controlled NMs are derived, and the coordination of dynamic probe signals and detectors to distinguish attack schemes is provided.

(4) Extensive simulation studies were performed to validate the effectiveness and practicality of the PASS for securing NMs.

The remainder of this paper is organized as follows: Section 2 describes the overall PASS architecture. Section 3 presents the coordinated detection method and detection principles of the two detectors. In Section 4, tests are performed to validate the effectiveness and practicality of the proposed PASS approach. Finally, Section 5 concludes the paper.

2. SDN-enabled PASS architecture

The generic PASS framework is illustrated in Fig. 1. It consists of three layers: ① DERs in physical NMs; ② an NM control center (NMCC) and SDN-enabled network layer for monitoring operation conditions, sending critical control signals, and generating programmable probe signals; and ③ a power bot-attack detection layer for identifying attacks on the DER inverters via the secured, programmable, and resilient SDN network. The NMCC is responsible for operating and controlling the NMs and coordinating various microgrid applications, including implementing PASS by generating and delivering programmable probe signals. Specifically, the operational status (connected or exited) of all DERs and the inverter controller responses are continuously monitored and transferred back to the NMCC via the SDN network. The NMCC then sends control and probe signals to the DERs for processing NM operations and security scanning.

As shown in Fig. 1, a logically centralized SDN controller is the basis for implementing PASS. It provides advanced communication network visibility and management, and detailed visualization of network conditions, including capacity utilization and communication path selection. Its dynamic programmability and direct network control capability adapt to the characteristics of NMs and facilitate the integration of PASS into NMs [1,8,26]. Specifically, facilitation is due to the following two aspects:

(1) Resilient communication network. The SDN enables intact on-demand communication paths for control and probe signals by reconfiguring switches, thus establishing alternative routes once either a communication attack occurs or the topology changes owing to microgrid application implementation, such as plug-and-play.

(2) Real-time communication network verification. Both the time-critical characteristics of PASS and normal NM operations rely on an entirely continuously accessible communication network. The network visibility and data flow visualization offered by SDN ensure that packets can be sent to the destination DERs even under undesired conditions such as network malfunctions and congestion by developing a self-healing communication network that exploits the SDN offered features of programmable and dynamic configurations.

The overall PASS procedures are summarized as follows:

(1) Detection rules are created within the NMCC based on the output results of the two coordinated detection method detectors under normal conditions, that is, without attack, as discussed in the next section.

(2) Certain probe signals, that is, sinusoidal waves with low amplitude, are sent by the NMCC to the DER controller via the secured SDN network. Once the signal is received by a DER controller, its response is synchronously sent to the NMCC via the SDN network.

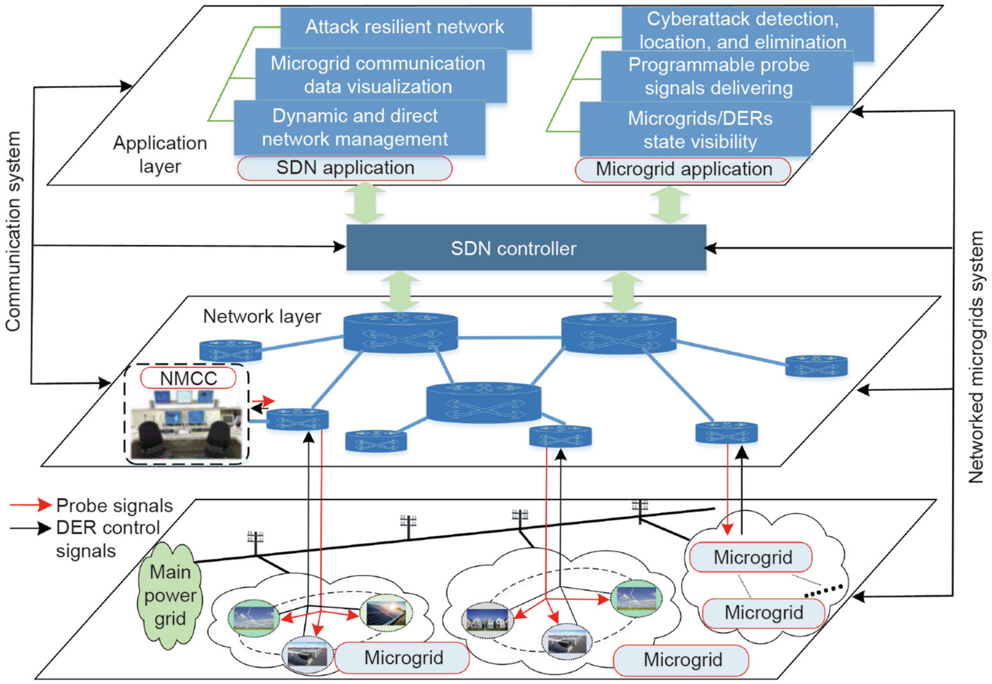
Attack resilient network
Microgrid communication data visualization
Dynamic and direct network management
SDN application
Application layer
Cyberattack detection, location, and elimination
Programmable probe signals delivering
Microgrids/DERs state visibility
Microgrid application
Communication system
SDN controller
Networked microgrids system
Network layer
NMCC
Probe signals
DER control signals
Main power grid
Microgrid
Microgrid
Microgrid
Microgrid

Fig. 1. PASS architecture.

(3) The coordinated detection method is performed within the NMCC to calculate the detection results using the information received from each DER.

(4) The calculated detection results are compared with the detection rules. Once a large deviation occurs, an attack is detected. The type of attack can be identified using the two coordinated detection method detectors.

Specifically, the real-time DER state visualization is conducted in the NMCC to determine whether new probe signals should be generated and delivered. When microgrids experience dynamics, which include connection/disconnection of DERs, control strategy variations and changes in the microgrid topology, the detection procedure should be adjusted accordingly before conducting the attack detection procedure. When the DER connection occurs, two additional steps should be performed: ① programming of suitable probe signals, and ② configuration of the routing path for probe signals and control signals of DER inverters. In contrast, for the DER disconnection, the NMCC terminates the entire procedure. When a control strategy varies, the detection rules should be re-created according to the new control strategy and the probe signals should be re-programmed. When the microgrid topology changes, the communication network should also be reconfigured to ensure that reliable communication exists between DERs and NMCC before conducting the detection procedure.

Owing to the programmability of SDN, it is possible to vary the scanning frequency and target microgrids, and the PASS can easily be extended by incorporating additional detection methods.

3. Coordinated detection method for DER inverter controllers

A malicious attacker can launch different attacks simultaneously to compromise DERs. In this study, the three most common power-bot attacks, namely controller manipulation (i.e., topology modification and parameter overwriting), replay, and injection attacks, are investigated in droop-control-based NMs. Specifically, the attacker can modify the topologies and parameters of inverters' controllers and manipulate the data exchanged among different DERs. An illustration of the three power-bot attack types and the established cyber-secured detection method is shown in Fig. 2.

To effectively identify the three types of attacks, the devised coordinated detection method utilizes two real-time detectors: a synchronous detector (SD) [11] and a Duffing oscillator detector (DOD) [27]. To ensure the real-time power-bot attack detection and normal uninterrupted DER operations, two combined sinusoidal signals with low magnitudes are applied as probe signals with the following two features: ① probe signals pose no impact on the DER inverter performance, and ② probe signals cannot be easily eavesdropped owing to the programmable characteristics. To avoid possible DER disturbances, the probe signals are designed to have three features, which can be mathematically expressed as ① $s(t) = s(t + NT)$, where N is an integer, ② $\| s(f) \| \le \varepsilon$, and $\int_t^{t+T} s(t)\mathrm{d}t = 0$, where t represents any one particular moment on the whole time axis, T is the period of continuous signal $s(t)$, $\| * \|$ is the L_2 norm of the harmonic at the frequency f, and ε is a small threshold. The designed probe signals ensure that their impact on the target DERs within one period is zero; in other words, the probe signals do not change the overall DER controller performance, and thus, the disturbances to the physical systems can also be avoided [1,11]. Specifically, the probe signals $s_d(t)$ and $s_q(t)$ in Fig. 2 can be expressed as follows:

$$s_d(t) = s_{d1}(t) + s_{d2}(t) = \alpha_{d1}\sin(\omega_{d1}t) + \alpha_{d2}\sin(\omega_{d2}t) \tag{1}$$

$$s_q(t) = s_{q1}(t) + s_{q2}(t) = \alpha_{q1}\sin(\omega_{q1}t) + \alpha_{q2}\sin(\omega_{q2}t) \tag{2}$$

where α_{dj} and α_{qj} are the amplitudes (d and q represent direct and quadrature axes, respectively), and ω_{dj} and ω_{qj} (j = 1 or 2) are the frequencies of the sinusoidal signals, respectively. $s_{d1}(t)$ and $s_{q1}(t)$ are utilized to detect modification and overwriting attacks via a synchronous detector. $s_{d2}(t)$ and $s_{q2}(t)$ are used to detect replay and injection attacks via a DOD. To ensure that there is no interference, ω_{d2} and ω_{q2} should be integer multiples (≥ 2) of ω_{d1} and ω_{q1}, respectively.

The coordination of detecting the three types of attacks is based on the following two aspects: ① coordination between pro-

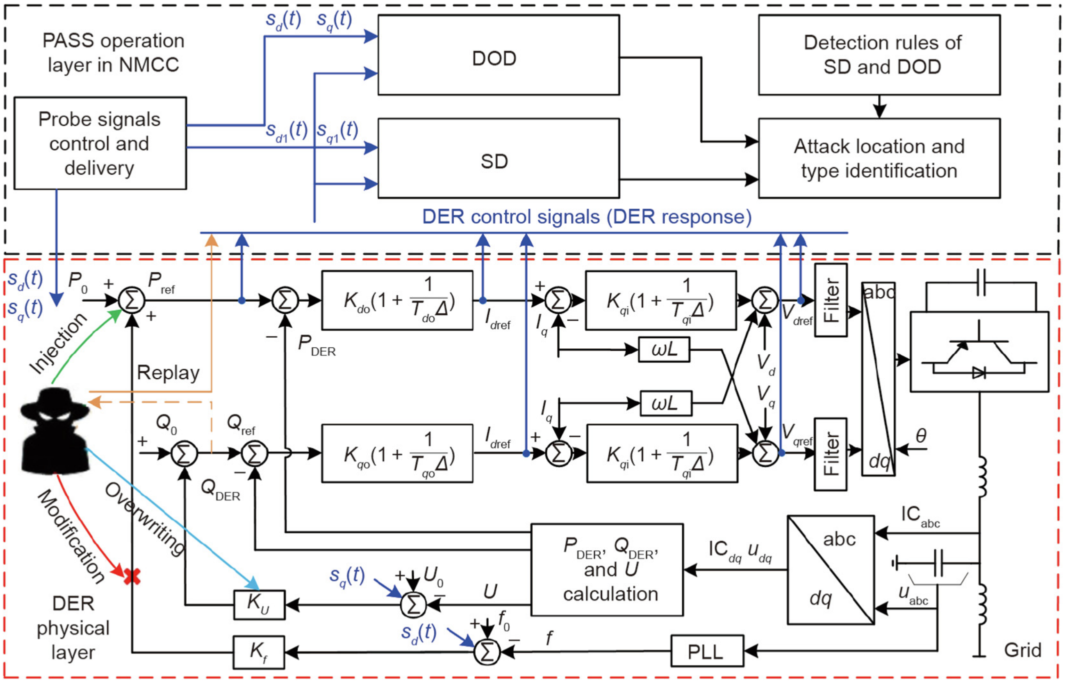
PASS operation layer in NMCC
$s_d(t)$ $s_q(t)$
DOD
Detection rules of SD and DOD
Probe signals control and delivery
$s_{d1}(t)$ $s_{q1}(t)$
SD
Attack location and type identification
DER control signals (DER response)
$s_d(t)$
$s_q(t)$
P_0
P_{ref}
Injection
Replay
$K_{do}(1+\frac{1}{T_{do}\Delta})$
P_{DER}
I_{dref}
I_q
$K_{di}(1+\frac{1}{T_{di}\Delta})$
ωL
V_{dref}
V_d
V_q
Filter
abc
dq
θ
Q_0
Q_{ref}
Q_{DER}
$K_{qo}(1+\frac{1}{T_{qo}\Delta})$
I_{qref}
$K_{qi}(1+\frac{1}{T_{qi}\Delta})$
V_{qref}
Modification
Overwriting
IC_{abc}
P_{DER}, Q_{DER}, and U calculation
IC_{dq} u_{dq}
u_{abc}
$s_q(t)$
U_0
U
K_U
DER physical layer
$s_d(t)$
f_0
f
K_f
PLL
Grid

Fig. 2. Power-bot attacks on droop-control-based DER inverters. DOD: Duffing oscillator detector; SD: synchronous detector; u: instantaneous voltage; IC: instantaneous current; a, b, and c: three phases; d: direct axis; q: quadrature axis; PLL: phase locked loop; θ: voltage phase; ω: angular frequency; L: inductance; f: grid frequency; f_0: initial operating value of frequency; U_0: initial operating value of voltage; U: root mean square (rms) of voltage; I: rms of current; Δ: Laplace operator; PWM: pulse width modulation; P: active power; Q: reactive power; P_0, Q_0: initial active and reactive output power of DER; V: reference voltage; K_{do}, K_{qo}, K_{di}, K_{qi}: parameters of outer and inner loop controllers; K_U, K_f: parameters of droop controllers; T_{do}, T_{qo}, T_{di}, T_{qi}: time constants of outer and inner loop controllers; ref: reference.

grammable probe signals and corresponding detectors, and ② coordination of the two detectors to identify attack types. It should be noted that the two devised detectors can effectively identify the attack without requiring the system model and parameters, computational complexity, and the burden for data processing, which are discussed in subsequent subsections as follows.

3.1. Synchronous detector and its detection rules

(1) **Detector for droop-control-based DERs:** Droop control can enable flexible switching between grid-connected and island type operations. The droop coefficients are important in maintaining the rated frequency and voltage. Consequently, attacks on droop controllers are threatening because they can result in immediate deterioration or even collapse of NMs. In this section, the detection of the f–P and U–Q type of droop controller is presented as an example for creating the detection rules of the synchronous detector. It should be noted that this method works for widely applied dq double-loop controllers with different control strategies, and the corresponding detection rules can be derived in a similar manner. This is described as follows.

The synchronous detector works in real time to obtain the detection signals as

$$D=\frac{1}{T}\int_t^{t+T} s(t)\cdot r(t)\mathrm{d}t \tag{3}$$

where $s(t)$ refers to $s_{d1}(t)$ or $s_{q1}(t)$; $r(t)$ represents the DER response, that is, $P_{\rm dref}$, $Q_{\rm dref}$, $I_{\rm dref}$, $I_{\rm qref}$, $V_{\rm dref}$, or $V_{\rm qref}$. D is the detection signal, that is, D_f, D_U, $D_{\rm do}$, $D_{\rm qo}$, $D_{\rm di}$, or $D_{\rm qi}$. The meaning of the subscripts has been defined in the caption of Fig. 2.

(2) **Detection rules:** Given the topologies and parameters of the DER controllers, the detection signals can be obtained. Taking $D_{\rm di}$ as an example, we can express it as follows:

$$\begin{aligned}
D_{\rm di} &= \tfrac{1}{T}\int_t^{t+T} s_{d1}(t)\cdot V_{\rm dref}\mathrm{d}t\\
&= \tfrac{1}{T}\int_t^{t+T} s_{d1}(t)\cdot\left\{(I_{\rm dref}-I_d)K_{\rm di}(1+\tfrac{1}{T_{\rm di}\Delta})-I_q\omega L+V_d\right\}\mathrm{d}t\\
&= \tfrac{1}{T}\int_t^{t+T} s_{d1}(t)\cdot\left\{(I_{\rm dref}-I_d)K_{\rm di}(1+\tfrac{1}{T_{\rm di}\Delta})\right\}\mathrm{d}t+\tfrac{1}{T}\int_t^{t+T} s_{d1}(t)\cdot(-I_q\omega L+V_d)\mathrm{d}t\\
&= \tfrac{1}{T}\int_t^{t+T} s_{d1}(t)\cdot\left\{(I_{\rm dref}-I_d)K_{\rm di}(1+\tfrac{1}{T_{\rm di}\Delta})\right\}\mathrm{d}t+0\\
&= \tfrac{K_fK_{\rm do}K_{\rm di}}{T}\int_t^{t+T} s_{d1}^2(t)(1+\tfrac{1}{T_{\rm do}\Delta})(1+\tfrac{1}{T_{\rm di}\Delta})\mathrm{d}t+\tfrac{K_fK_{\rm do}K_{\rm di}}{T}(1+\tfrac{1}{T_{\rm do}\Delta})(1+\tfrac{1}{T_{\rm di}\Delta})\\
\int_t^{t+T} & s_{d1}(t)s_{d2}\mathrm{d}t=\frac{\alpha_{d1}^2\cdot K_f\cdot K_{\rm do}\cdot K_{\rm di}}{2}(1-\frac{1}{T_{\rm do}T_{\rm di}\omega_{d1}^2})
\end{aligned} \tag{4}$$

where T is the period of $s_{d1}(t)$ and other parameters have been defined in Fig. 2. Note that ω_{d2} = $N\omega_{d1}$, where N is an integer, and $N\geq 2$. Thus, $\frac{1}{T}\int_t^{t+T} s_{d1}(t)\cdot s_{d2}(t)\mathrm{d}t=0$. Similarly, D_f, D_U, $D_{\rm do}$, $D_{\rm qo}$, and $D_{\rm qi}$ under normal operations can be derived as follows:

$$D_f=\frac{1}{T}\int_t^{t+T} s_{d1}(t)P_{\rm ref}\mathrm{d}t=\frac{\alpha_{d1}^2K_f}{2} \tag{5}$$

$$D_U=\frac{1}{T}\int_t^{t+T} s_{q1}(t)Q_{\rm ref}\mathrm{d}t=\frac{\alpha_{q1}^2K_U}{2} \tag{6}$$

$$D_{\rm do}=\frac{1}{T}\int_t^{t+T} s_{d1}(t)I_{\rm dref}\mathrm{d}t=\frac{\alpha_{d1}^2K_fK_{\rm do}}{2} \tag{7}$$

$$D_{\rm qo}=\frac{1}{T}\int_t^{t+T} s_{q1}(t)I_{\rm qref}\mathrm{d}t=\frac{\alpha_{q1}^2K_UK_{\rm qo}}{2} \tag{8}$$

$$D_{\rm qi}=\frac{1}{T}\int_t^{t+T} s_{q1}(t)\cdot V_{\rm qref}\mathrm{d}t=\frac{\alpha_{q1}^2\cdot K_f\cdot K_{\rm qo}\cdot K_{\rm qi}}{2}(1-\frac{1}{T_{\rm qo}T_{\rm qi}\omega_{q1}^2}) \tag{9}$$

From Eqs. (4)–(9), it can be seen that each D is determined only by the controller coefficients and the amplitude or frequency of the probe signal. Any attack on the controller that alters the coefficients can result in abnormal detection results. The designed detector in Eq. (3) only requires the controllers' responses and, hence, will not impact the privacy of DERs.

When all the DER controllers are intact, the detection signal steady-state values D_f, D_U, D_{do}, D_{qo}, D_{di}, and D_{qi} are equal to the values calculated in Eqs. (4)–(9), respectively. Once an attack is launched, the calculated values deviate from the established norm. Specifically, the abnormal values under two types of controller manipulation attacks, namely, ① topology modification and ② controller parameter overwriting/changing, are summarized in Table 1. It should be noted that the values shown in Table 1 are derived under the assumed steady state of specific attacks similar to Eqs. (4)–(9), and these values may not be equal to the detection values in reality owing to caused disturbances. Table 1 clearly shows the corresponding variation in the detection values of the two types of controller manipulation attacks for all possible locations. By detecting abnormal values in comparison to Eqs. (4)–(9) and comparing them with those in Table 1, the two controller manipulation attack types and their locations can be identified.

3.2. DOD and its detection rules

Both data sent from the DERs to the NMCC and control signals sent in the reverse direction are likely to be exposed to attackers. In this subsection, we present the second detector, namely the DOD, for detecting the replay and injection attacks coordinated with the SD. Specifically, the attacker can launch replay attacks by first replicating the recorded responses and then sending them to the NMCC repeatedly or with a delay to disable the SD, because the NMCC cannot receive the actual inverter controller responses. The injection attack can be conducted by injecting additive malicious signals either into the DER controllers or directly into the detection layer to disrupt the stable microgrid operation or disable the SD.

The idea of the DOD is to superimpose weak dynamic authentication signals on the DER control signals. The DOD is able to detect weak sinusoidal signals with a very low magnitude and is immune to noise [27–29]. In this study, the frequencies and magnitudes of *$s_{d2}(t)$ and $s_{q2}(t)$ can easily be dynamically adjusted to construct the authentication signals, which are then detected by the Duffing oscillator. Any replay of recorded inverters' responses will alter the predetermined dynamic authentication signals as well as the corresponding DOD operation patterns, and thus will be detected. Conversely, the injection attack has no impact on the DOD operation pattern owing to its selectivity, but can be detected by the SD [27]. Therefore, the two types of attacks can be identified by the coordination of the two detectors.*

(1) **DOD:** The normal Duffing equation can be written as follows [29]:

$$\frac{\mathrm{d}^2x}{\mathrm{d}t^2}+\delta\frac{\mathrm{d}x}{\mathrm{d}t}-x+x^3=\gamma\cos(t), \tag{10}$$

where δ is the damping ratio, the polynomial "$-x + x^3$" is the nonlinear restoring force, and $\gamma\cos(t)$ is either the periodic driving force or the reference signal. If δ is fixed and γ increases, the system state changes from chaotic motion to large periodic motion. When γ reaches the signal magnitude threshold (i.e., 0.82 in this study when δ is 0.5), the system enters the critical state, where the Duffing oscillator becomes very sensitive [28]. To obtain γ_{critical}, one can simply increase the driving force amplitude and observe the Duffing oscillator system phase trajectory. Specifically, only when the signal to be detected has the same frequency as the driving force, the Duffing oscillator phase trajectory rapidly enters the periodic state; otherwise, the system is still chaotic. This is the Duffing oscillator selectivity and can be utilized to detect replay attacks as follows.

To detect the authentication probe signal, the Duffing oscillator must inject an input signal (reference signal). The probe signal to be detected can be regarded as a reference signal perturbation. The frequencies and magnitudes of these two signals are dynamically coordinated within the NMCC. According to the DOD phase trajectory change DOD, the detected signal, whether or not it contains the probe signals sent from the NMCC, can be determined. Note that the Duffing oscillator is immune to noise because it only affects the local trajectory with no state transition.

Table 1
Values of synchronous detector under attacks.

Controllers under attack	Attack types	D_f	D_U	D_{do}	D_{qo}	D_{di}	D_{qi}
Droop loop	①	0	0	0	0	0	0
	②	$\frac{\alpha_{d1}^2K_f'}{2}$	$\frac{\alpha_{q1}^2K_U'}{2}$	$\frac{\alpha_{d1}^2K_f'K_{do}}{2}$	$\frac{\alpha_{q1}^2K_U'K_{qo}}{2}$	$\frac{\alpha_{d1}^2K_f'K_{do}K_{di}}{2}\left(1-\frac{1}{T_{do}T_{di}\omega_{d1}^2}\right)$	$\frac{\alpha_{q1}^2K_U'K_{qo}K_{qi}}{2}\left(1-\frac{1}{T_{qo}T_{qi}\omega_{q1}^2}\right)$
Outer loop	①	$\frac{\alpha_{d1}^2K_f}{2}$	$\frac{\alpha_{q1}^2K_U}{2}$	0	0	0	0
	②	$\frac{\alpha_{d1}^2K_f}{2}$	$\frac{\alpha_{q1}^2K_U}{2}$	$\frac{\alpha_{d1}^2K_fK_{do}'}{2}$	$\frac{\alpha_{q1}^2K_UK_{qo}'}{2}$	$\frac{\alpha_{d1}^2K_fK_{do}'K_{di}}{2}\left(1-\frac{1}{T_{do}'T_{di}\omega_{d1}^2}\right)$	$\frac{\alpha_{q1}^2K_UK_{qo}'K_{qi}}{2}\left(1-\frac{1}{T_{qo}'T_{qi}\omega_{q1}^2}\right)$
Inner loop	①	$\frac{\alpha_{d1}^2K_f}{2}$	$\frac{\alpha_{q1}^2K_U}{2}$	$\frac{\alpha_{d1}^2K_fK_{do}}{2}$	$\frac{\alpha_{q1}^2K_UK_{qo}}{2}$	0	0
	②	$\frac{\alpha_{d1}^2K_f}{2}$	$\frac{\alpha_{q1}^2K_U}{2}$	$\frac{\alpha_{d1}^2K_fK_{do}}{2}$	$\frac{\alpha_{q1}^2K_UK_{qo}}{2}$	$\frac{\alpha_{d1}^2K_fK_{do}K_{di}'}{2}\left(1-\frac{1}{T_{do}T_{di}'\omega_{d1}^2}\right)$	$\frac{\alpha_{q1}^2K_UK_{qo}K_{qi}'}{2}\left(1-\frac{1}{T_{qo}T_{qi}'\omega_{q1}^2}\right)$
Droop and outer loop	①	0	0	0	0	0	0
	②	$\frac{\alpha_{d1}^2K_f'}{2}$	$\frac{\alpha_{q1}^2K_U'}{2}$	$\frac{\alpha_{d1}^2K_f'K_{do}'}{2}$	$\frac{\alpha_{q1}^2K_U'K_{qo}'}{2}$	$\frac{\alpha_{d1}^2K_f'K_{do}'K_{di}}{2}\left(1-\frac{1}{T_{do}'T_{di}\omega_{d1}^2}\right)$	$\frac{\alpha_{q1}^2K_U'K_{qo}'K_{qi}}{2}\left(1-\frac{1}{T_{qo}'T_{qi}\omega_{q1}^2}\right)$
Droop and inner loop	①	0	0	0	0	0	0
	②	$\frac{\alpha_{d1}^2K_f'}{2}$	$\frac{\alpha_{q1}^2K_U'}{2}$	$\frac{\alpha_{d1}^2K_f'K_{do}}{2}$	$\frac{\alpha_{q1}^2K_U'K_{do}}{2}$	$\frac{\alpha_{d1}^2K_f'K_{do}K_{di}'}{2}\left(1-\frac{1}{T_{do}T_{di}'\omega_{d1}^2}\right)$	$\frac{\alpha_{q1}^2K_U'K_{qo}K_{qi}'}{2}\left(1-\frac{1}{T_{qo}T_{qi}'\omega_{q1}^2}\right)$
Outer and inner loop	①	$\frac{\alpha_{d1}^2K_f}{2}$	$\frac{\alpha_{q1}^2K_U}{2}$	0	0	0	0
	②	$\frac{\alpha_{d1}^2K_f}{2}$	$\frac{\alpha_{q1}^2K_U}{2}$	$\frac{\alpha_{d1}^2K_fK_{do}'}{2}$	$\frac{\alpha_{q1}^2K_UK_{qo}'}{2}$	$\frac{\alpha_{d1}^2K_fK_{do}'K_{di}'}{2}\left(1-\frac{1}{T_{do}'T_{di}'\omega_{d1}^2}\right)$	$\frac{\alpha_{q1}^2K_UK_{qo}'K_{qi}'}{2}\left(1-\frac{1}{T_{qo}'T_{qi}'\omega_{q1}^2}\right)$
Droop, outer, and inner loop	①	0	0	0	0	0	0
	②	$\frac{\alpha_{d1}^2K_f'}{2}$	$\frac{\alpha_{q1}^2K_U'}{2}$	$\frac{\alpha_{d1}^2K_f'K_{do}'}{2}$	$\frac{\alpha_{q1}^2K_U'K_{qo}'}{2}$	$\frac{\alpha_{d1}^2K_f'K_{do}'K_{di}'}{2}\left(1-\frac{1}{T_{do}'T_{di}'\omega_{d1}^2}\right)$	$\frac{\alpha_{q1}^2K_U'K_{qo}'K_{qi}'}{2}\left(1-\frac{1}{T_{qo}'T_{qi}'\omega_{q1}^2}\right)$

K' represents the modified parameters of DER controllers by attackers (K). Attack types: ① topology modification; ② controller parameter overwrighting/changing.

To use Eq. (10) to detect signals with different frequencies, a frequency transformation should be performed. Defining $y = \mathrm{d}x/\mathrm{d}t = \dot{x}$, Eq. (10) can be rewritten as

$$\dot{x} = y, \tag{11}$$

$$\dot{y} = -\delta y + x - x^3 + \gamma\cos(t). \tag{12}$$

Let $t = \omega\tau$ (τ is an intermediate variable for transformation). The following equations hold:

$$x(t) = x(\omega\tau) = x_*(\tau), \tag{13}$$

$$\frac{\mathrm{d}x(t)}{\mathrm{d}t} = \frac{\mathrm{d}x(\omega\tau)}{\mathrm{d}(\omega\tau)} = \frac{1}{\omega}\frac{\mathrm{d}x(\omega\tau)}{\mathrm{d}\tau} = \frac{1}{\omega}\frac{\mathrm{d}x_*(\tau)}{\mathrm{d}\tau}, \tag{14}$$

$$\frac{\mathrm{d}^2x(t)}{\mathrm{d}t^2} = \frac{\mathrm{d}^2x(\omega\tau)}{\mathrm{d}(\omega\tau)^2} = \frac{1}{\omega^2}\frac{\mathrm{d}^2x(\omega\tau)}{\mathrm{d}\tau^2} = \frac{1}{\omega^2}\frac{\mathrm{d}^2x_*(\tau)}{\mathrm{d}\tau^2}. \tag{15}$$

Substituting Eqs. (13)–(15) into Eqs. (11) and (12), and omitting the intermediate variable x_* subscript, the equations suitable for different frequencies are as follows:

$$\dot{x} = \omega y, \tag{16}$$

$$\dot{y} = \omega(-\delta y + x - x^3 + \gamma\cos(\omega t) + \Delta\gamma_t), \tag{17}$$

where $\Delta\gamma_t$ is the input signal, including the probe signal and noise. Because Eqs. (16) and (17) are derived from Eq. (10), the system properties and critical values are not altered. Thus, after filtering the direct current (DC) component, the DER control signals can be injected into Eqs. (16) and (17) to detect replay attacks.

To demonstrate the working principle, the two states of the Duffing oscillator are illustrated in Fig. 3, where the sum of the distances l from the moving point in the locus to $(-1, 0)$ and $(1, 0)$ is used to facilitate fast automatic state identification. Comparing l under the two states, it can be noted that l is always greater than three under the large periodic state, while l is between two and four under the chaotic state. Therefore, a threshold, l = 2.5, was used in this study to identify the states, as indicated by the red dashed line in Fig. 3. Once l is less than 2.5, it can be confirmed that the Duffing oscillator is in a chaotic state; otherwise, the Duffing oscillator is in a large periodic state.

(2) **Detection rules:** The Duffing oscillator reference signal is set such that it operates in chaotic motion. Specifically, the amplitudes of probe signals $s_{d2}(t)$ and $s_{q2}(t)$ coordinated with the reference signals are programmed to change every 0.05 or 0.1 s to make the oscillator operate alternatively between the two motion states, as shown in Fig. 4. Because the frequencies are no larger than 0.1 s, the signals injected into the Duffing detector by replay and injection attackers are different from those generated in the NMCC. Thus, the operational state pre-defined by the NMCC will be broken owing to its sensitivity and selectivity, and replay and injection attacks will be detected.

3.3. Detection rules for attack types and locations

The NMCC delivers programmable probe signals to DERs. Coordinated with the above two detectors, the attack types can be determined based on the detection rules of the coordinated detection method given in Algorithm 1. The attack locations can be identified based on the detection results with abnormal values. In particular, the detection rules for simultaneous injection and overwriting attacks are slightly different based on different injection signal types. If the injected signals are DC components, the simultaneous attacks cannot be identified with Algorithm 1, because the detection results are the same as those under only the overwriting attack. Considering that the injected signals can be seen as corresponding references to each loop and the NMCC continuously monitors each loop's control signals, which are also each loop's responses, the NMCC can easily identify the simultaneous attacks by comparing the responses of each loop with those under normal controls. If the controller response is normal, while the synchronous detector detection result deviates from the normal values, it means that only an overwriting attack is occurring. If the controller response is abnormal, while the detection values are normal, then only an injection attack is occurring. If both the controller response and detection values are abnormal, then injection and overwriting attacks are occurring. If the injected signals are not DC components, the attack type can be identified using either the method for DC component injection attack or Algorithm 1 because the detection results are different from those only under an overwriting attack.

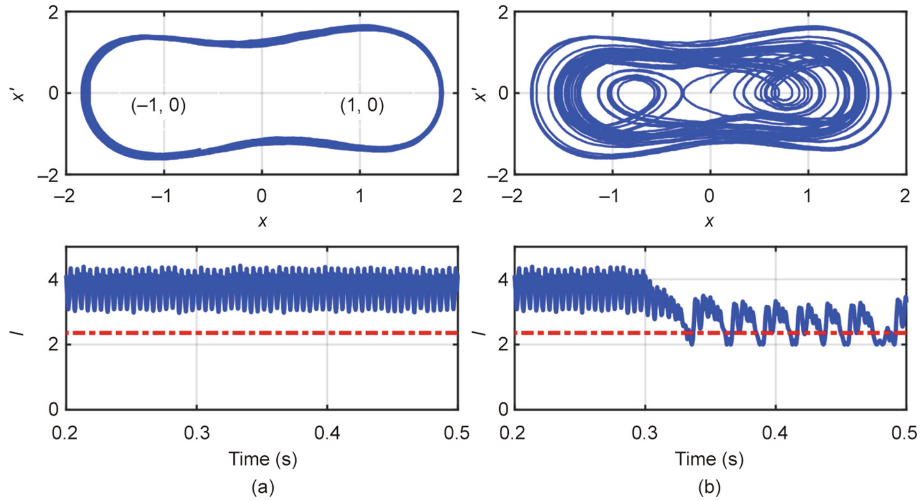

Fig. 3. Two Duffing oscillator states: (a) periodic motion and (b) chaotic motion. x: variable of the Duffing oscillator equation; x': derivative of x.

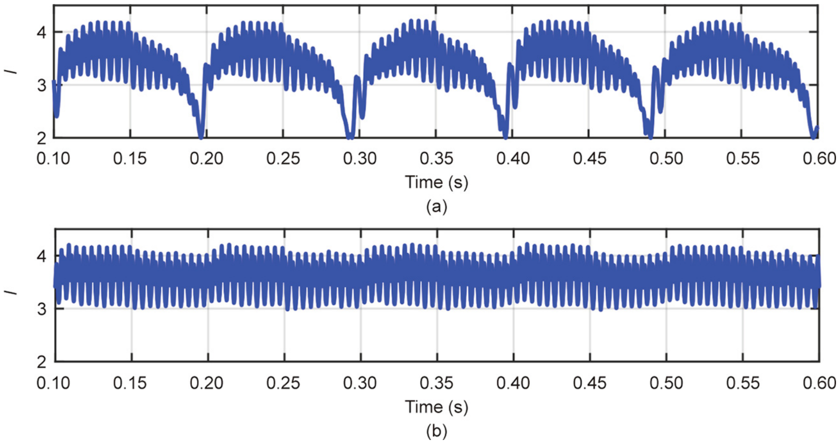

Fig. 4. Duffing oscillator for attack detection. (a) Alternating motion state of DOD; (b) large periodic motion state of DOD.

Algorithm 1: Detection rules for attack types

```
for all values of $D_f$, $D_U$, $D_{do}$, $D_{qo}$, $D_{di}$, $D_{qi}$ do
    if there exists 0 then
        Topologies modification attack detected;
    else
        if $D_f$, $D_U$, $D_{do}$, $D_{qo}$, $D_{di}$, $D_{qi}$ are normal then
            if Duffing detectors results are normal then
                There are no attacks.
            else
                Replay attacks detected.
            end
        else
            if $D_f$, $D_U$, $D_{do}$, $D_{qo}$, $D_{di}$, $D_{qi}$ are normal then
                Injection attacks detected.
            else
                Parameters overwriting attacks detected.
            end
        end
    end
end
```

4. Test and validation

The effectiveness and practicality of PASS in detecting powerbot attacks were tested and validated with a typical NM system, as shown in Fig. 5. The test system consisted of six microgrids and operated in the island mode. The NMs were modeled in MATLAB/Simulink, and the simulation time step was 50 μs. The probe signals are programmed within the NMCC and delivered to the destination DERs through SDN simulated in Mininet [30]. Specifically, the effectiveness of the two detectors under each single attack is validated in Sections 4.1 and 4.2. Then, the performance of the two detectors under complex attacks are evaluated in Section 4.3. Finally, the effectiveness of the proposed coordinated detection method is verified in Section 4.4.

To illustrate the proposed SDN-enabled implementation method, we provide the details of the testing environment setup, network connection, and system operation process. The PASS testing environment consists of a microgrid simulator, an SDN simulator, and an NMCC. The network connection of the three components and a flow chart for the implementation of the coordinated detection method running in the NMCC are shown in Fig. 6.

This NM test system includes six microgrids, operates in the island mode, and is developed and compiled in MATLAB/Simulink. More test system details are presented in Fig. 6. The built-in Simulink sender and receiver modules were used for communication. The internet protocol (IP) addresses of the six microgrids are set from 10.0.0.1 to 10.0.0.6. The DER inverter control signal measurements are transmitted through the SDN and sent to the NMCC, whose IP address is 10.0.0.7. The NMCC runs on a remote server, which can receive the DER operational status (connected or disconnected) and the inverter control signals and sends the programmable probe signals back to MATLAB/Simulink, to perform PASS with the implementation of the coordinated detection method, programming, and delivering probe signals. After being connected to the simulator, the server enters the listening mode and receives packets whose destination IP and port match those of the server, and then performs the PASS. The middle of Fig. 6 shows the SDN topology used for the networked microgrid system, which includes five switches and one SDN OpenFlow controller Ryu [30]. The SDN network runs in a Mininet environment. In Mininet, the bandwidth for each link is set to one gillion bits per second (Gbps), which is a common practice applied in the Ethernet network. The user datagram protocol (UDP) [31] is used to transmit data packets between NMs and the NMCC through Mininet [32].

4.1. Verification of synchronous detector for modification and overwriting attacks

(1) **Modification attack:** In this test case, a modification attack occurs on the inverter's outer loop power controller of Battery 31 in Microgrid 4 at 1.10 s (Fig. 5). Two subcases are performed to demonstrate the testing system performance with and without the synchronous detector. When the detector is activated, $\alpha_{d1} = \alpha_{q1} = 0.06$, and $\omega_d = \omega_q = 1256$ rad·s^{-1} (1 rad = 180°/π). Fig. 7 illustrates the current responses (three phases: a, b, and c) at Buses 20 and 31 and the output power of the droop-controlled DERs when the synchronous detector is disabled. Fig. 8 shows the three-phase current and power responses under protection. The changes in D_{do} in Battery 31 are shown in Fig. 9.

From Figs. 6–8, the modification attack is identified by the synchronous detector at $t = 1.11$ s when D_{do} reaches zero, and Circuit breaker (CB) 7 is immediately opened to disconnect Microgrid 4 and isolate the attack.

(2) **Overwriting attack:** In this test case, an overwriting attack is launched on the droop controller of Fuel cell 13 in Microgrid 1 at $t = 1.10$ s (Fig. 5). The testing system operation was also provided to validate the SD efficacy. The current responses at Buses 13 and 27 and the output power of the droop-controlled DERs are presented in Fig. 10 without SD. When SD is put into use, the current response at Bus 27 and the output power of the droop-controlled

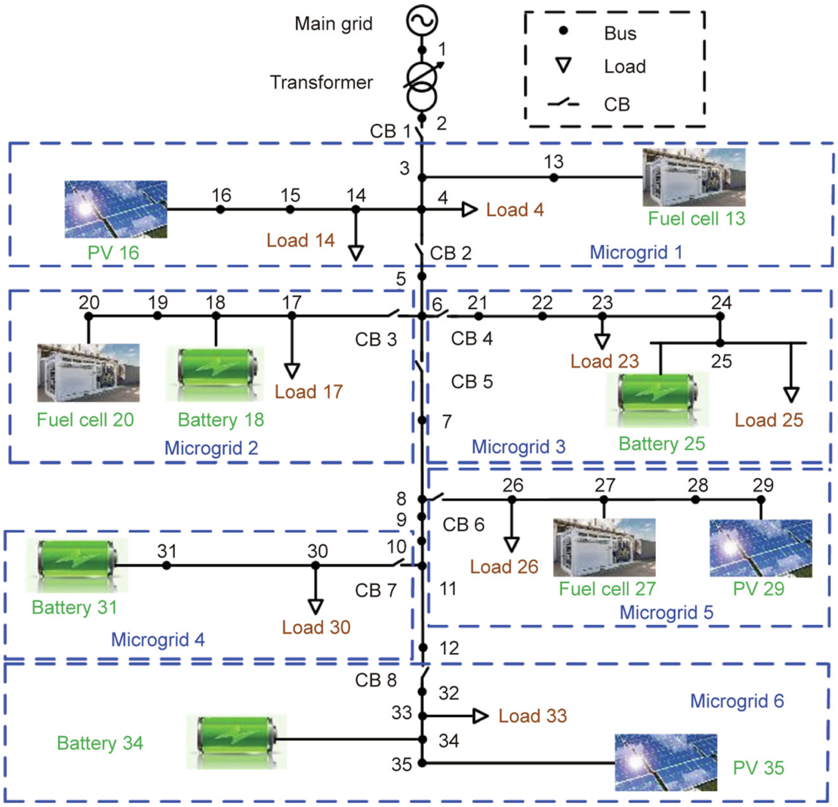

Fig. 5. Networked microgrids for validation of coordinated detection. CB: circuit breaker; PV: photo voltaic; 1–35 are bus numbers.

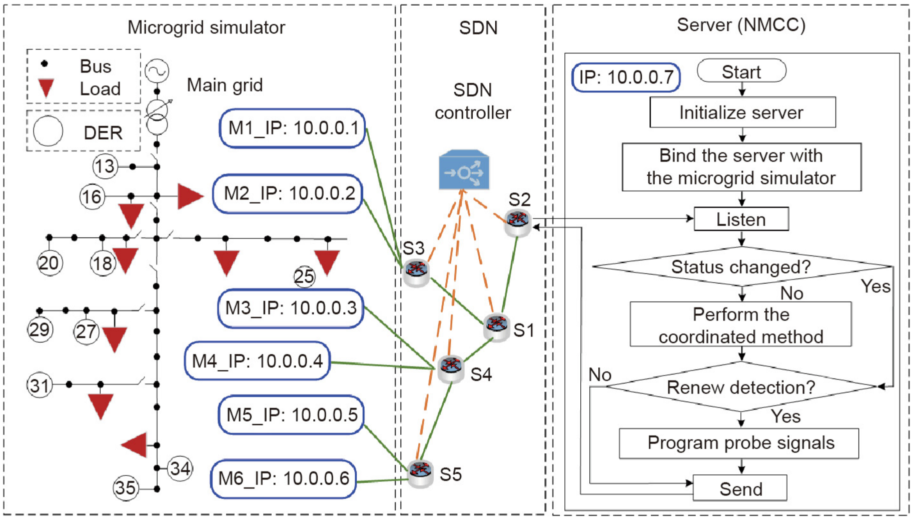

Fig. 6. Network connection of the PASS simulation system. M1–M6 are six microgrids; S1–S5 are five switches; IP: internet protocol.

DERs are shown in Fig. 11. The attack is identified at $t = 1.12$ s and D_{do} deviates from the normal value significantly, as shown in Fig. 12.

From Figs. 7–12, it can be observed that the impacts of modification and overwriting attacks rapidly spread across the NMs without SD, and NM performance is severely deteriorated (Figs. 7 and 10). With SD, the attacks can be identified and their NM impacts can also be mitigated, as illustrated in Figs. 8 and 11, which verifies the SD effectiveness in defending against power-bot attacks.

The actual D_{do} values before the attacks were close to the values calculated according to the detection function. As shown in Figs. 9 and 12, the D_{do} values are 3.63 and 1.44, respectively, under the two cases, which are in close proximity to the calculated values, that is 3.60 and 1.44, respectively. The D_{do} values change continuously after Microgrid 4 is disconnected. The values violate the detection values shown in Table 1. This is because the disconnected microgrid operates abnormally, whereas Table 1 provides the steady-state of the detection rules. In practice, attack alarms should be raised once the detection results deviate from normal values to a certain extent, that is, greater than 1.5 or less than 0.5 times the normal operational state values. To protect more critical DERs, narrower thresholds can be set for raising alarms.

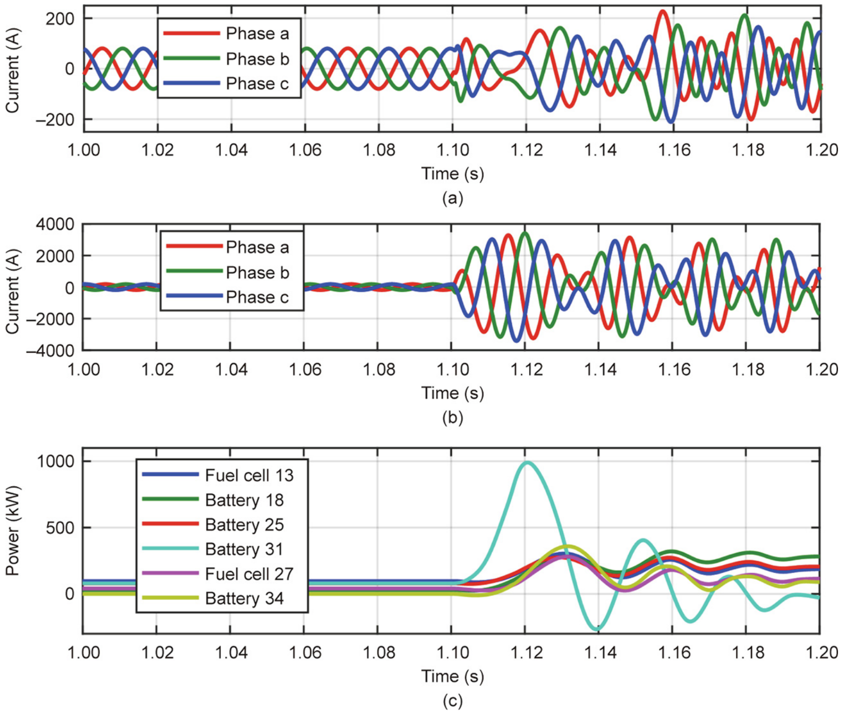

Fig. 7. (a, b) Current response of Buses 20 and 31 and (c) DER power response under modification without SD.

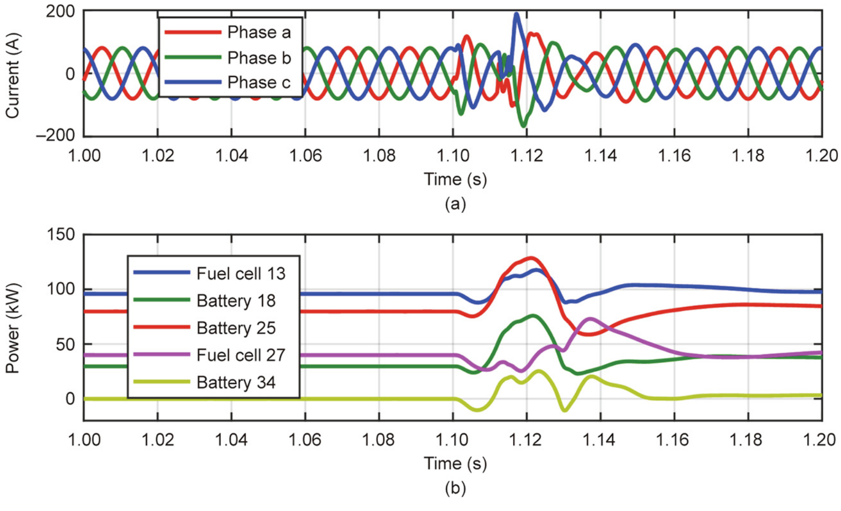

Fig. 8. (a) Current response of Bus 20 and (b) DER output power response with SD.

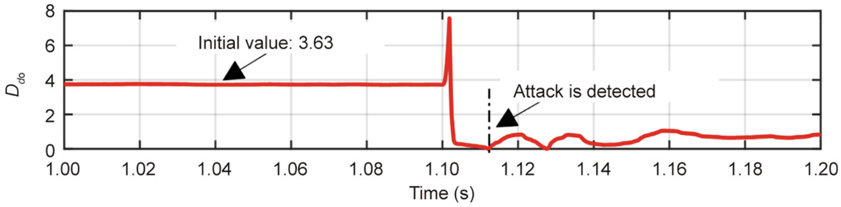

Fig. 9. Detection function value of D_{do} in Battery 31.

4.2. Validation of DOD for replay attack

(1) **Replay attack:** In this test case, a replay attack is launched on the inner loop controller of Battery 34 in Microgrid 6 by injecting the recorded normal operation data. When the DOD is activated, α_{d2} = α_{q2} = 0.01 and the DOD state is programmed to alter the frequency every 0.1 s in the NMCC. The frequency of the recorded signal does not match the dynamically changed signal

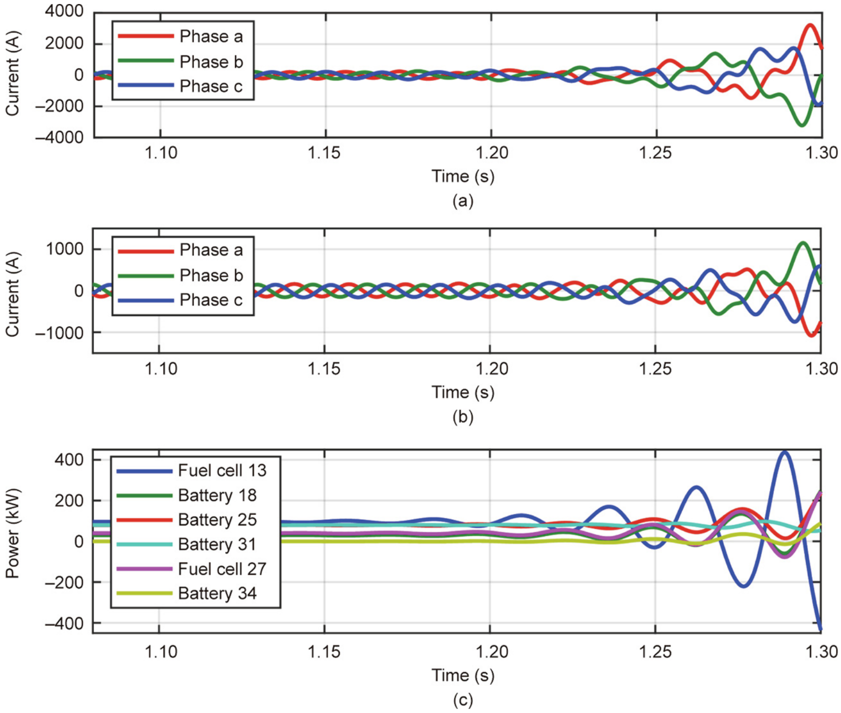

Fig. 10. (a, b) Current responses of Buses 13 and 27 and (c) DER power response without SD.

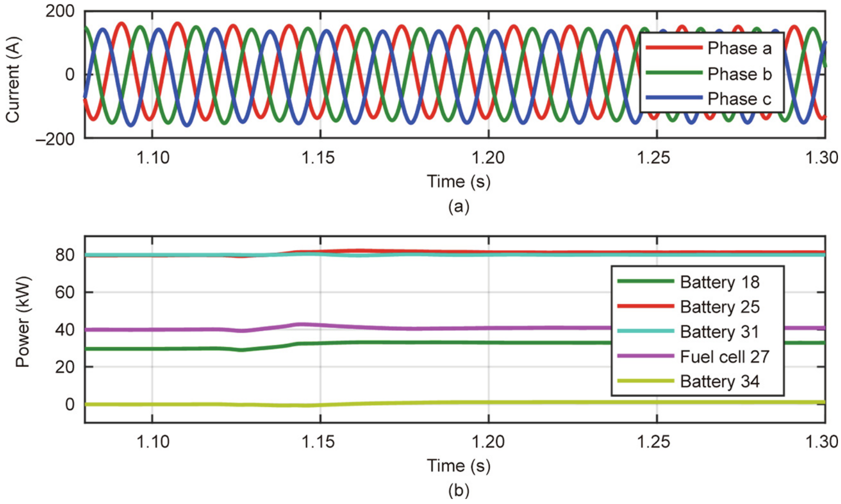

Fig. 11. (a) Current response of Bus 27 and (b) DER output power response with SD.

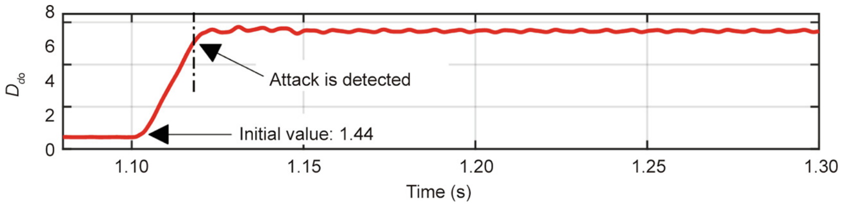

Fig. 12. Detection function value of D_{do} in Fuel cell 13.

generated in the NMCC. Thus, the DOD motion state variation takes place upon the occurrence of a replay attack. As shown in Fig. 13, the replay attack is launched at t = 0.9 s and detected at t = 0.94 s.

(2) **Robustness verification:** In practice, DOD should be reliable and robust to be applicable, which means: ① The sinusoidal signals α_{d2} and α_{q2} should not impact NM normal operations, because the signal amplitude is lower than that of the SD probe signal, the

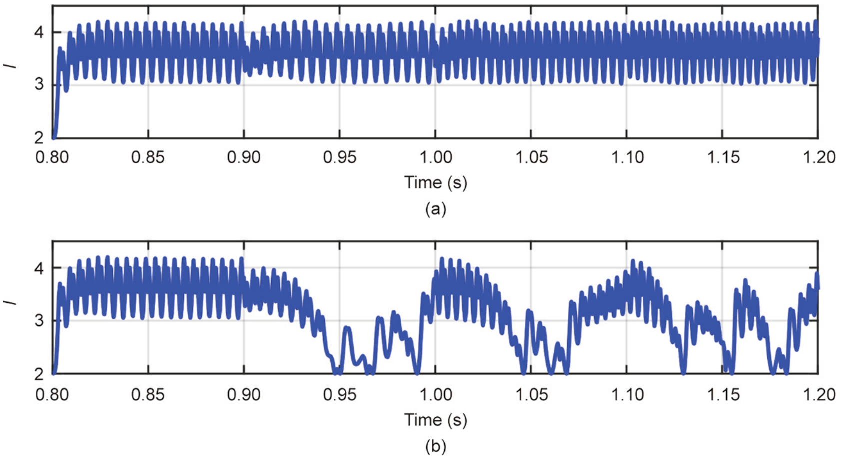

Fig. 13. Detection of replay attack. (a) Motion state of DOD without replay attack; (b) motion state of DOD under replay attack.

impact can be ignored; and ② the DOD should guarantee the correct detection of weak signals with intense noise. The lowest sinusoidal signal amplitude that can be identified by the Duffing oscillator is 0.0001, and the lowest reachable signal-to-noise ratio (SNR) is −51 dB, as reported in Ref. [27]. To demonstrate the competence of the DOD in detecting weak signals with low SNRs, the simulation results are illustrated in Fig. 14.

4.3. Incompetence of single detector for attack detection

(1) **Malfunction of SD:** An additional signal with the same and different $s_{d1}(t)$ frequencies is injected into the controllers of Batteries 31 and 18 at t = 1.10 s, respectively (Fig. 5). The changes in D_{do} during the process are illustrated in Fig. 15, respectively. As shown in Fig. 15, Microgrids 2 and 4 are disconnected because of the significant D_{do} deviation. In fact, the inverter controller parameters are not attacked. Thus, SD cannot accurately identify the attack type under an injection attack, although it can isolate the attack.

However, under replay and overwriting attacks, the SD is unable to detect them. Before the overwriting attack is launched at t = 1.10 s, the actual control signals are replaced with the prerecorded signals and reported to the NMCC. Fig. 16 shows the output power of the droop-controlled DERs and the change in D_{do} in Battery 31. The NM performance deteriorates severely and eventually crashes. However, the SD cannot identify and mitigate attacks in a timely manner.

(2) **Malfunction of DOD:** As introduced in Section 3.2, the DOD itself cannot determine the injection attack because of its selectivity. The motion state does not change, as shown in Fig. 17(a), when Fuel cell 13 is compromised. Thus, this attack could not be identified.

4.4. Verification of coordinated detection method

(1) **Detection of overwriting and injection:** When only the injection attack occurs in Fuel cell 13, the change of D_{do} and the state of DOD are shown in Fig. 17(b). It can be seen that, D_{do} changes when the injection attack is launched, while the motion state of DOD and the NMs remain normal operations. Although the SD is misled by the injection attack, the attack's type can also be identified accurately.

When overwriting and injection attacks occur simultaneously in Battery 18 not only will the D_{do} deviate from the normal value, but the motion state will also be altered, as illustrated in Fig. 18. In comparison with Fig. 15(b), the overwriting and injection attacks can be accurately distinguished with the cooperation of the two detectors.

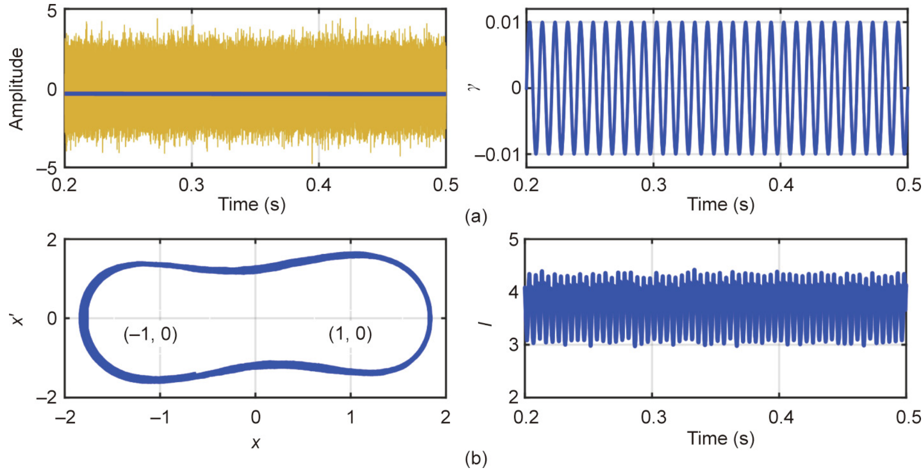

Fig. 14. Detection of weak signal with low SNR. (a) Weak signal with intense noise; (b) motion state of DOD with noise.

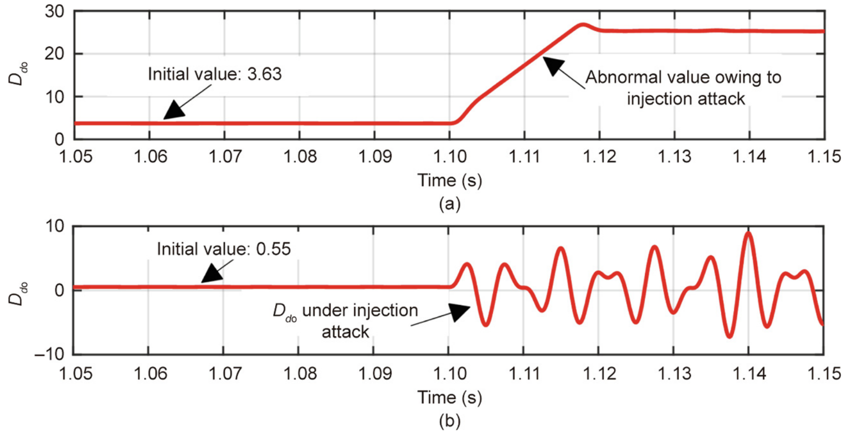

Fig. 15. (a) Change of D_{do} in Battery 31 and (b) change of D_{do} in Battery 18 under injection attack.

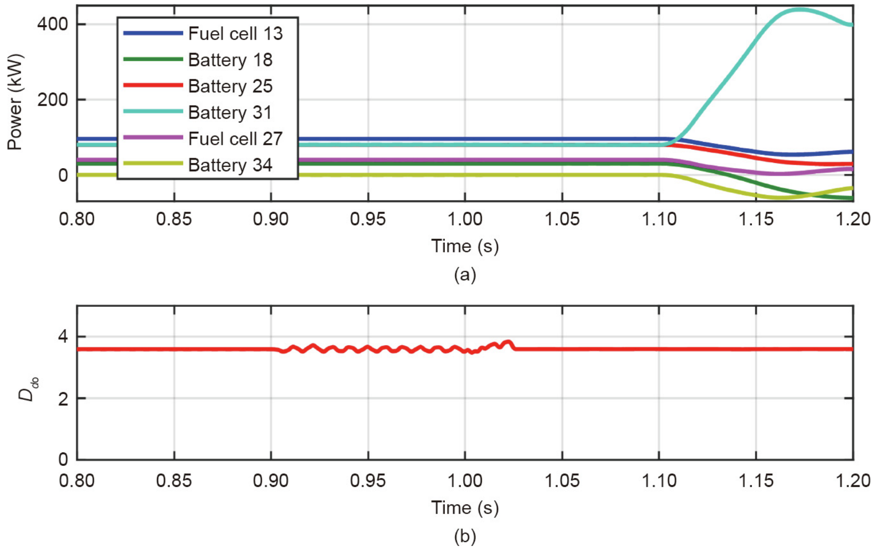

Fig. 16. (a) DER power response and (b) D_{do} of Battery 31 under two attacks with only SD.

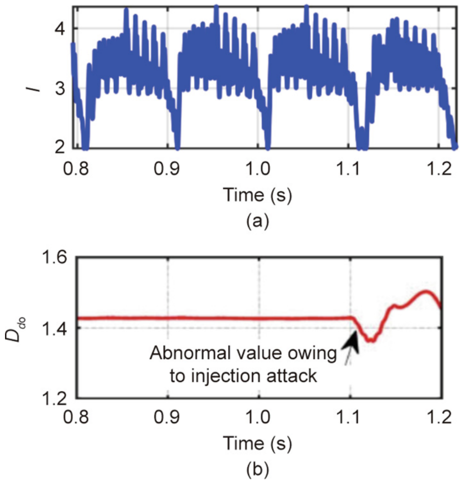

Fig. 17. Detection results of (a) DOD and (b) SD in Fuel cell 13.

(2) **Detection of modification and replay attacks:** A replay attack is launched in Battery 31 by recording the normal operation data and injecting them at t = 1.00 s to the NMCC. Meanwhile, a modification attack is launched at t = 1.10 s. The D_{do} of Battery 31 and the DER output power without the coordinated detection method are shown in Fig. 16. When the coordinated detection is activated, the DOD motion states before and after the attack, and the DER output power are shown in Fig. 19.

As shown in Figs. 16 and 19, the modification attack was undetectable because D_{do} scarcely changed during the joint attack. Consequently, the microgrid cannot be segregated in a timely manner to isolate the attack. When the coordinated detection method is applied, the motion state of the Duffing oscillator changes once the replay attack is launched, as shown in Figs. 19(a) and (b). The attack can be detected using the coordinated detection method, and the types are identified. Its impact can also be mitigated to ensure stable NM operation, which validates the effectiveness of the established method.

From the simulations above, when a single detector is activated, the complex malicious attacks can not only mistakenly report attack types but also become undetectable. The devised coordinated detection method is capable of identifying attacks regardless of the attack strategies employed by malicious attackers. The coordinated probe signals are programmed in the NMCC with the SDN-based PASS strategy, which is practically implementable and reliable for NM protection.

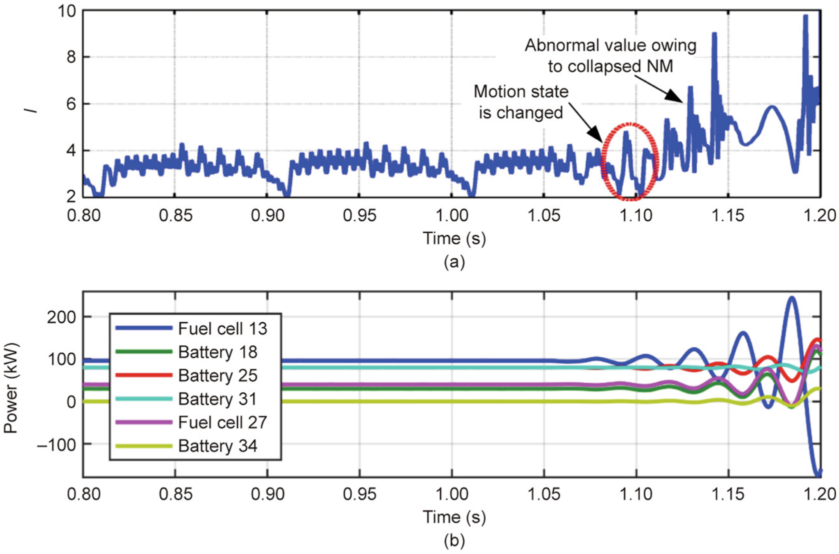

Fig. 18. Validation of coordinated detection under overwriting and injection attacks. (a) The motion state of Duffing oscillator under attack; (b) power response of DERs.

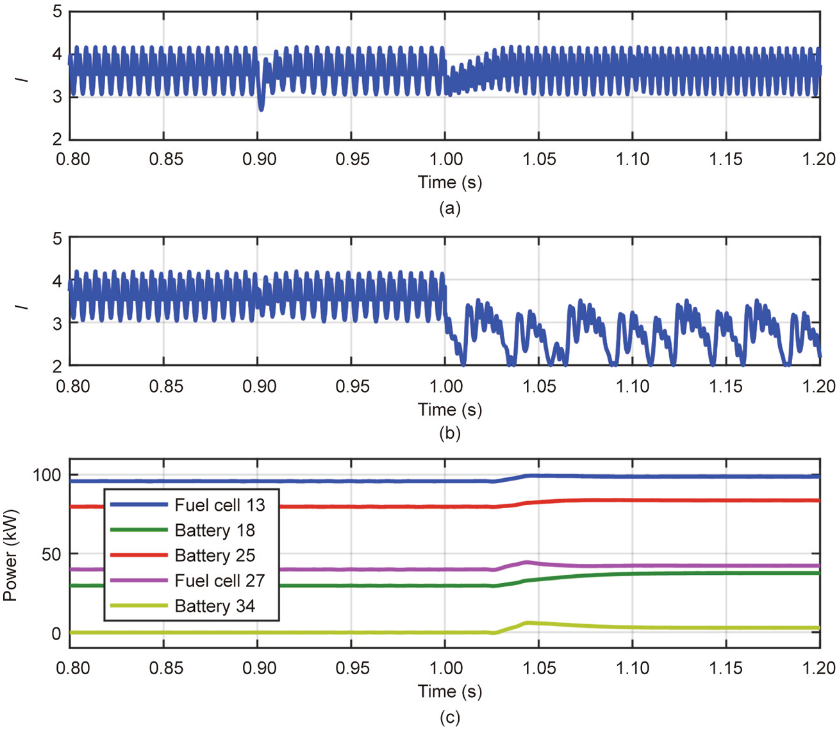

Fig. 19. Validation of coordinated detection under modification and replay attacks. (a, b) The motion state of Duffing oscillator under normal condition and under attack, respectively; (c) the power response of DERs.

5. Conclusions

In this study, an SDN-enabled PASS approach is presented to identify and mitigate complex cyberattacks in NMs. Probe signals are programmed in the NMCC and forwarded to the DER controllers to detect sophisticated attacks, including modification, overwriting, injection, and replay attacks, regardless of the attack templates employed by malicious attackers. By devising a coordinated detection method, the types and attack locations can be detected. The designed programmable strategy can be efficiently implemented to enable microgrid plug-and-play functions. The efficacy and reliability of the proposed method were validated through extensive tests.

Acknowledgements

This work was supported in part by the National Science Foundation, USA (ECCS-2018492, CNS-2006828, ECCS-2002897, and OIA-2040599).

Compliance with ethics guidelines

Zimin Jiang, Zefan Tang, Peng Zhang, and Yanyuan Qin declare that they have no conflict of interest or financial conflicts to disclose.

References

[1] Zhang P, editor. Networked microgrids. Cambridge: Cambridge University Press; 2021.
[2] Tang Z, Zhang P, Krawec WO, Jiang Z. Programmable quantum networked microgrids. IEEE Trans Quantum Engineer 2020;1:1–13.
[3] Tang Z, Qin Y, Jiang Z, Krawec WO, Zhang P. Quantum-secure microgrid. IEEE Trans Power Syst 2021;36(2):1250–63.
[4] Lu LY, Liu HJ, Zhu H, Chu CC. Intrusion detection in distributed frequency control of isolated microgrids. IEEE Trans Smart Grid 2019;10(6):6502–15.
[5] Farhady H, Lee H, Nakao A. Software-defined networking: a survey. Comput Netw 2015;81:79–95.
[6] Tang Z, Zhang P, Krawec WO. A quantum leap in microgrids security: the prospects of quantum-secure microgrid. IEEE Electrific Mag 2021;9(1):66–73.
[7] Hatziargyriou ND, Kleftakis V, Papadimitriou CN, Messinis G. Microgrids in distribution. In: Liu CC, MaArthur S, Lee SJ, editors. Smart grid handbook. Hoboken: John Wiley & Sons, Ltd.: 2016.
[8] Zhang P, Wang B, Luh PB, Ren L, Qin Y, inventors; University of Connecticut, assignee. Enabling resilient microgrid through ultra-fast programmable network. United States patent US 20170324671. 2017 Apr 28.
[9] Wang L, Qin Y, Tang Z, Zhang P. Software-defined microgrid control: the genesis of decoupled cyber–physical microgrids. IEEE Open Access J Power Energy 2020;7:173–82.
[10] Huang T, Satchidanandan B, Kumar PR, Xie Le. An online detection framework for cyber attacks on automatic generation control. IEEE Trans Power Syst 2018;33(6):6816–27.
[11] Ravichandran MT. Resilient monitoring and control systems: design, analysis, and performance evaluation [dissertation]. Michigan: University of Michigan; 2015.
[12] Li Y, Zhang P, Zhang L, Wang B. Active synchronous detection of deception attacks in microgrid control systems. IEEE Trans Smart Grid 2017;8(1):373–5.
[13] Pan K, Teixeira A, Cvetkovic M, Palensky P. Cyber risk analysis of combined data attacks against power system state estimation. IEEE Trans Smart Grid 2019;10(3):3044–56.
[14] Skopik F, Smith PD, editors. Smart grid security: innovative solutions for a modernized grid. Burlington: Syngress; 2015.
[15] Kurt MN, Yilmaz Y, Wang X. Real-time detection of hybrid and stealthy cyber-attacks in smart grid. IEEE Trans Inform Forensics Security 2019;14(2):498–513.
[16] Manandhar K, Cao X, Hu F, Liu Y. Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. IEEE Trans Cont Network Syst 2014;1(4):370–9.
[17] Tang Z, Jiao J, Zhang P, Yue M, Chen C, Yan J. Enabling cyberattack-resilient load forecasting through adversarial machine learning. 2020. arXiv:2001.02289.
[18] Tan S, De D, Song WZ, Yang J, Das SK. Survey of security advances in smart grid: a data driven approach. IEEE Comm Surv Tutor 2017;19(1):397–422.
[19] Musleh AS, Chen G, Dong ZY. A survey on the detection algorithms for false data injection attacks in smart grids. IEEE Trans Smart Grid 2020;11(3):2218–34.
[20] Wang J, Qin Y, Tang Z, Zhang P. Software-defined cyber–energy secure underwater wireless power transfer. IEEE J Emerg Sel Topics Ind Electron 2021;2(1):21–31.
[21] He Y, Mendis GJ, Wei J. Real-time detection of false data injection attacks in smart grid: a deep learning-based intelligent mechanism. IEEE Trans Smart Grid 2017;8(5):2505–16.
[22] Babahajiani P, Wang L, Liu J, Zhang P. Push-sum-enabled resilient microgrid control. IEEE Trans Smart Grid. In press.
[23] Ren L, Qin Y, Wang B, Zhang P, Luh PB, Jin R. Enabling resilient microgrid through programmable network. IEEE Trans Smart Grid 2017;8(6):2826–36.
[24] Moslemi R, Mesbahi A, Velni JM. A fast, decentralized covariance selection-based approach to detect cyber attacks in smart grids. IEEE Trans Smart Grid 2018;9(5):4930–41.
[25] Wan W, Bragin MA, Yan B, Qin Y, Philhower J, Zhang P, et al. Distributed and asynchronous active fault management for networked microgrids. IEEE Trans Power Syst 2020;35(5):3857–68.
[26] Kreutz D, Ramos FMV, Esteves Verissimo P, Esteve Rothenberg C, Azodolmolky S, Uhlig S. Software-defined networking: a comprehensive survey. Proc IEEE 2015;103(1):14–76.
[27] Akilli M, Yilmaz N. Study of weak periodic signals in the EEG signals and their relationship with postsynaptic potentials. IEEE Trans Neural Syst Rehabil Eng 2018;26(10):1918–25.
[28] Vahedi H, Gharehpetian GB, Karrari M. Application of duffing oscillators for passive islanding detection of inverter-based distributed generation units. IEEE Trans Power Deliv 2012;27(4):1973–83.
[29] Jalilvand A, Fotoohabadi H. The application of Duffing oscillator in weak signal detection. ECTI Trans Electr Engineer Electron Commun 2011;9(1):1–6.
[30] Fujita T. Introduction to Ryu SDN framework [Internet]. Tokyo: Ryu SDN Framework Community; 2013 Apr 15 [cited 2020 Jul 20]; Available from: https://ryu-sdn.org/slides/ONS2013-april-ryu-intro.pdf.
[31] Wang MH, Chi PW, Guo JW, Lei CL. SDN storage: a stream-based storage system over software-defined networks, In: proceedings of 2016 IEEE Conference on Computer Communications Workshops; 2016 Apr 10–14; San Francisco, CA, USA; New York: IEEE; 2016. p. 598–9.
[32] Chithaluru P, Prakash R. Simulation on SDN and NFV models through mininet. In: Damka A, editor. Innovations in software-defined networking and network functions virtualization. Hershey: IGI Global; 2018. p. 149–74.