IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

IEEE POWER & ENERGY SOCIETY SECTION

Received December 29, 2021, accepted January 12, 2022, date of publication January 20, 2022, date of current version February 4, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3145015

Cyber-Attack Detection and Countermeasure for Distributed Electric Springs for Smart Grid Applications

JIE CHEN[1], ALEXANDER J. GALLO[2], (Member, IEEE), SHUO YAN[3], (Senior Member, IEEE), THOMAS PARISINI[4,5,6], (Fellow, IEEE), AND SHU YUEN RON HUI[4,7], (Fellow, IEEE)

[1]Hivision Technology, Hangzhou 311200, China
[2]Delft Center for Systems and Control, TU Delft, 2628 CD Delft, The Netherlands
[3]Discipline of Electrical and Biomedical Engineering, RMIT University, Melbourne, VIC 3000, Australia
[4]Department of Electrical and Electronic Engineering, Imperial College London, London SW7 2BX, U.K.
[5]Department of Engineering and Architecture, University of Trieste, 34100 Trieste, Italy
[6]KIOS Research and Innovation Centre of Excellence, University of Cyprus, Nicosia 1678, Cyprus
[7]School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798

Corresponding author: Shu Yuen Ron Hui (ron.hui@ntu.edu.sg)

This work was supported in part by the Nanyang Technological University-MediaTek Endowment Fund in Singapore under Grant 03INS001124C140, in part by the European Union's Horizon 2020 Research and Innovation Program under Grant 739551 (KIOS Centre of Excellence), and in part by the Italian Ministry for Research in the Framework of the 2017 Program for Research Projects of National Interest (PRIN) under Grant 2017YKXYXJ.

ABSTRACT With increasing installations of grid-connected power electronic converters in the distribution network, there is a new trend of using distributed control in a cyber layer to coordinate the operations of these power converters for improving power system stability. However, cyber-attacks remain a threat to such distributed control. This paper addresses the cyber-attack detection and a countermeasure of distributed electric springs (ESs) that have emerged as a fast demand-response technology. A fully distributed model-based architecture for cyber-attack detection in the communication network is developed. Based on a dynamic model of ES with consensus control, a local state estimator is proposed and practically implemented to monitor the system. The estimator is fully distributed because only local and neighboring information is necessary. A countermeasure for the distributed ESs to ride through the cyber-attack and maintain regulatory services in a microgrid is demonstrated successfully. Experimental results are provided to verify the effectiveness of the proposed cyber-attack detection method and its ride-through capability.

INDEX TERMS Electric springs, cyber-attack detection, distributed state estimator.

I. INTRODUCTION

Power-electronics-intensive microgrid is an efficient way to achieve high-performance power distribution with increasing penetration of renewable power [1]. In a recent review paper on cyber security in smart grid [2], grid-tied power converters are classified as (i) grid-feeding, (ii) grid-forming and (iii) grid-supporting units. Grid-forming units play a role in regulating the voltage and frequency of the power grid. Grid-feeding units feed energy into the grid. Grid-supporting units offer other auxiliary functions such as power quality enhancement, stability support, ride through and economic dispatch. High-frequency power electronics offers a bottom-up approach to smart grid technology. In a 2020 review article [3], electric spring (ES) is quoted as an example of high-frequency power electronic device for providing electric voltage support, storing electric energy, and damping low-frequency oscillations. Electric spring is a smart grid technology originally introduced as a demand-side management method for achieving instantaneous power balance for microgrid and power grid with substantial penetration of intermittent renewable energy sources. Importantly, recent research shows that ES is a power-electronic unit that could have the triple functions of being grid-forming (for regulating mains voltage and frequency [4]), grid-feeding (for feeding solar energy into the grid [5]) and grid-supporting (for providing auxiliary services such as power quality enhancement [6], power imbalance reduction [7] and power system resilience [8]).

The associate editor coordinating the review of this manuscript and approving it for publication was Nagesh Prabhu.

With the rapid development of the digital control and communication technologies, supervisory information-based control of power electronics converters in microgrids has been widely studied [9]. Compared with communication-free control, communication-based control methods introduce new features such as improved performance of the global average voltage regulation and current sharing [10]. Among different communication-based control methods, distributed control can offer good control performance with very sparse communication links between neighbors [11]. While the extra cyber layer provides a channel for the flow of information and opens the door for distributed control in emerging power electronics-intensive microgrid and power grid, it makes the system vulnerable to potential cyber-attacks. Therefore, the cybersecurity of distributed power electronics systems connected through a cyber layer is an emerging research topic that deserves attention and investigation [12].

According to [2] and [13]–[16], cyber-attacks may take place at the:

(1) hardware devices: the attacker directly attacks the on-board sensors and change the sensed data before it goes into microprocessor;

(2) transmitted data: the attacker can violate the information transmitted over the communication links. Data attacks can be divided as privacy attacks and false-data injection attacks (FDIAs) [16].

In this paper, we consider false-data injection attacks. Indeed, direct attacks on the hardware devices is technically difficult because the attacker must have direct access to the hardware devices. In a privacy attack, the attacker aims to steal the data that smart meters send to the power market and dig out end user's privacy information [9]. This scenario is of great importance, as FDIAs could distort the control information transmitted in the cyber layer and inject wrong data into control loops. Compared with privacy attack, the FDIA is a much bigger threat to the distributed power electronics systems because FDIA could mislead the power electronics devices to make wrong decisions. Related power electronics devices may compete against, instead of cooperating with, one another. In extreme cases, this fault may make the system unstable or damage the electrical equipment. An example is the communication-based cooperative voltage and frequency control of multiple inverters in an islanded ac microgrid. Wrong decisions made by inverters could shift the operating voltage and frequency from their respective nominal values and cause serious consequences. Many research efforts have been devoted to the control design of multiple inverters, but its cybersecurity is not yet well studied.

Because of the fast dynamic of power electronics, traditional cybersecurity methods such as encryption and authorization are too slow to cope with the fast power electronics control loops. Hence, it is necessary to establish an attack detection architecture to provide cybersecurity for power electronics systems. Recent research of power system cybersecurity mainly focused on the generation and transmission level with large-scale centralized supervisory control and data acquisition (SCADA) system [10], [15]. Cyber protection mechanism in distribution network with power electronics converters needs urgent attention.

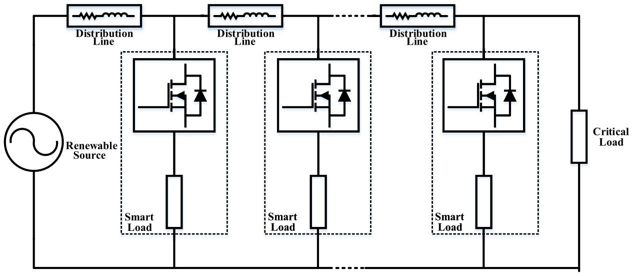


FIGURE 1. Microgrid with a cluster of ESs (physical layer).

Potential FDIA could change the information in the consensus control and alter its final control output to mislead the distributed power electronics system. Due to the limited communication ability in such a distributed control framework, good cyber-attack detection methods should rely only on the local information and data provided by neighbors. Studying a distributed controlled inverter-based microgrid, reference [12] numerically analyses the FDIA effects on the system performance. A stable region is defined where the attack is not serious enough to make the system unstable but only worsens the power-sharing performance. Reference [17] presents a simulation study on the effects of the FDIAs in a distributed controlled DC microgrid. The detection method uses Hunger tool in MATLAB to insert extra detection marks in control signals. Reference [18] uses the consensus algorithm features to find the attacked device and proposes a resilient cooperative control for DC microgrids [18]. This detection method is effective when less than half of the devices are attacked. This control will not eliminate the attacked data but uses an elastic coefficient to suppress the attack effect. References [12], [17] and [18] are based on simulation studies only. Hardware implementation issues for cyber-attack detection and countermeasures need more investigations.

The main contributions of this paper include (i) the design and practical evaluation of a fully distributed model-based detection architecture against cyber-attacks in the communication network between subsystems which are physically interconnected and regulated by a distributed consensus protocol, and (ii) a countermeasure to maintain normal services of a group of distributed ESs under cyber-attack.

II. PROBLEM FORMULATION

A. THE PHYSICAL AND CYBER LAYERS IN A NETWORK OF ES

Consider an islanded microgrid comprising a weak ac power source and a cluster of loads. The physical layer is shown in Fig.1. The ac power source in this weak grid is fed with intermittent renewable energy sources. Such a weak power

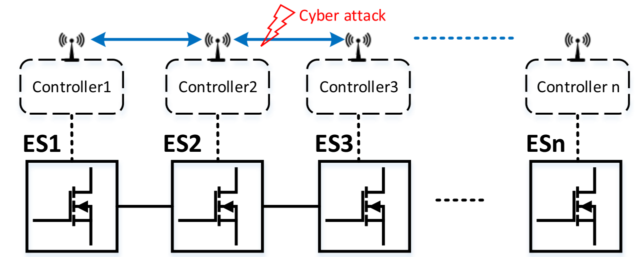


FIGURE 2. Cyber-physical model of a group of distributed ESs.

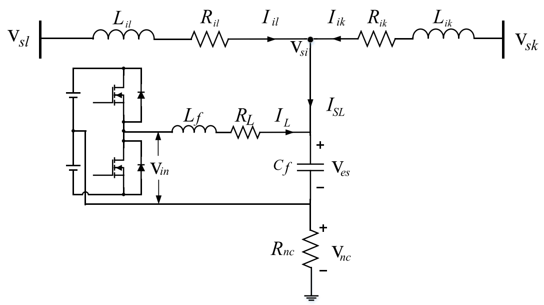


FIGURE 3. Layout of the *i*-th electric spring (ES-*i*).

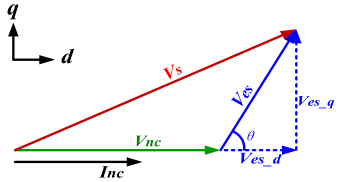


FIGURE 4. Vector diagram of ES in *d-q* frame.

grid can be emulated in hardware setup by programming a pre-recorded mains voltage profile of a renewable energy source in the programmable power source to create a time-varying voltage fluctuation along the distribution line. The cluster of loads consists of a mixture of smart loads and critical loads. Critical loads here refer to sensitive electric loads that require a well-regulated ac mains voltage. Each smart load consists of an ES connected in series with a noncritical load. The noncritical load is one that can tolerate certain voltage variations without causing consumer inconvenience. The ES plays the significant role of regulating the local line voltage and adaptively adjusting the power consumption of each noncritical load to instantaneously balance power supply and demand.

In this study, an additional communication network is added to explore new control features of distributed ESs. As verified in [4], consensus control can coordinate different ESs for the voltage regulation purpose and guarantee the power-sharing ability. Under extreme cases when the communication network collapses, the cyber-physical system can roll back to the simple physical system with only local droop control [4]. Fig. 2 represents the cyber-physical model of multiple ESs. The solid black lines show the physical electric lines between neighboring ESs. The blue arrows represent the two-way communication links between local controllers in the neighborhood. A potential cyber-attack may occur in the communication network.

Assume that there are n ESs in the system and each ES is considered as an agent. Graph $\boldsymbol{G} = (\boldsymbol{V}, \boldsymbol{E})$ is a graph with nodes set $\boldsymbol{V} = [1, 2, \ldots, n]$ and edges $\boldsymbol{E} \subseteq \boldsymbol{V} \times \boldsymbol{V}$. In this study, the nodes are the distributed ESs and the edges represent the communication links among different agents. The adjacency matrix $\mathbf{A} = (a_{\mathrm{ij}})_{nxn}$ has non-negative elements. $a_{\mathrm{ij}} = 1$ if and only if there is a communication link between node i and j. According to [11], the graph $\boldsymbol{G}$ should be a connected undirected graph that guarantees consensus convergence.

B. THE DYNAMIC MODEL OF ES

Without loss of generality, Fig. 3 shows the layout of the i-th ES (ES-i) which is connected to its neighbors: ES-l and ES-k. The dynamics of ES-i should be studied with the considerations of the ES circuit, the noncritical load and the connected lines. The ES is implemented by a half-bridge power inverter connected in series with a resistive noncritical load (R_{nc}).

As shown in Fig.4, a decoupled single-phase d-q framework can be developed by choosing the local smart load current (I_{SL}) as the referenced d vector. The complete dynamics of ES-i can be described by the following set of equations (note: subscript i has been dropped for notational simplicity):

$$\begin{cases} C_f \dot{V}_{es}^d = \dfrac{1}{X_{C_f}} V_{es}^q + I_L^d + I_{ik}^d + I_{il}^d \\ C_f \dot{V}_{es}^q = -\dfrac{1}{X_{C_f}} V_{es}^d + I_L^d + I_{ik}^d + I_{il}^d \\ L_f \dot{I}_L^d = X_{L_f} I_L^q + V_{in}^d - V_{es}^d(-I_L^d R_L) \\ L_f \dot{I}_L^q = -X_{L_f} I_L^d + V_{in}^q - V_{es}^q(-I_L^q R_L) \\ L_{il} \dot{I}_{il}^d = X_{L_{il}} I_{il}^q + V_{s_l}^d - V_{es}^d - I_{SL}^d R_{nc} - I_{il}^d R_{il} \\ L_{il} \dot{I}_{il}^q = -X_{L_{il}} I_{il}^d + V_{s_l}^q - V_{es}^q - I_{SL}^q R_{nc} - I_{il}^q R_{il} \\ L_{ik} \dot{I}_{ik}^d = X_{L_{ik}} I_{ik}^q + V_{s_k}^d - V_{es}^d - I_{SL}^d R_{nc} - I_{ik}^d R_{ik} \\ L_{ik} \dot{I}_{ik}^q = -X_{L_{ik}} I_{ik}^d + V_{s_k}^q - V_{es}^q - I_{SL}^q R_{nc} - I_{ik}^q R_{ik}, \end{cases} \tag{1}$$

where V_{es} is the output voltage of the ES, I_L is the inductor current, and I_{il}, I_{ik} are the line currents. V_{in} is the voltage fed to the LC filter. V_{si}, V_{sl}, and V_{sk} are respectively the line voltage of ES-i, ES-l, and ES-k. V_{nc} is the voltage across the noncritical load. Parameters C_f, L_f, R_L are the values of the filter capacitor, inductor, and inductor's series resistance, respectively. L_{il}, R_{il}, L_{ik}, and R_{ik} are the parameters of the distribution line connecting ES-i to its neighbors k and l, respectively. We define X_L and X_C as the inductive and capacitive reactance, respectively, i.e.:

$$X_L = \omega L, \quad X_C = \frac{1}{\omega C} \tag{2}$$

where $\omega = 2\pi f$. Consider the node of V_{si}, the following smart load current (I_{SL}) equation can be derived by

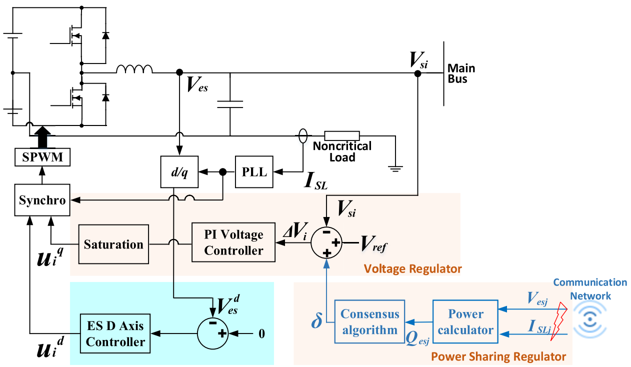


FIGURE 5. Block diagram of consensus control of ES.

Kirchhoff's current law:

$$I_{SL} = \sum_{j \in N_i} I_{ij} \tag{3}$$

where set $N_i = \{l, k\}$. In general, each ES physically connected to ES-i shall be included in group N.

Combining (1), (2) and (3), the continuous-time state-space formulation for the ES-i is characterized as:

$$\begin{aligned} \dot{x}_i &= A_{ii}x_i + B_i u_i + G_i \xi_i \\ y_i &= C_i x_i \end{aligned} \tag{4}$$

where x_i is the state of the ES, u_i is the control input, ξ_i is a vector containing the interconnections terms between an ES and its neighbors (the physical connection), and y_i is the output vector. The vectors are explicitly defined as:

$$\begin{aligned} x_i &= [V_{es}^d, V_{es}^q, I_L^d, I_L^q, I_{il}^d, I_{il}^q, I_{ik}^d, I_{ik}^q]^T \\ u_i &= [V_{in}^d, V_{in}^q]^T \\ \xi_i &= [V_{sl}^d, V_{sl}^q, V_{sk}^d, V_{sk}^q]^T \\ y_i &= \mathbf{I}x_i \end{aligned} \tag{5}$$

All matrices are defined in the Appendix.

C. CONSENSUS CONTROL OF ES

The consensus control of distributed ESs has been studied in [2]. The control objectives for ESs can be summarized as voltage/frequency regulation and accurate proportional reactive/active power-sharing. In this paper which focuses on the ES cyber-attack detection problem, the control loop of ES has been simplified to the objectives of voltage regulation and reactive power-sharing. Fig. 5 shows the block diagram of ES consensus control.

Assuming a lossless operation, the ES voltage on the d axis is set to zero by the reference, resulting in an ES voltage perpendicular to the noncritical load current. This indicates that the ES compensates only reactive power for the voltage regulatory service. Hence, the voltage regulation and consensus power-sharing loops are designed to control the variables on the q axis. The reactive power Q_{esi} is defined as:

$$Q_{es_i} = V_{es_i}^d I_{SL_i}^q - V_{es_i}^q I_{SL_i}^d \tag{6}$$

With the objective of sharing reactive power compensation in a distributed scenario, it is necessary for the neighboring ESs to communicate among one another. Each ES will receive the following set of data from its neighboring ES-j:

$$d_{ji}(t) = [V_{es_j}, I_{SL_j}]^T, \quad j \in N_i. \tag{7}$$

The wireless communication links over which information is transferred are marked as the blue arrows (as the inputs to the power calculator) in Fig. 5. Note that the transmitted data shall be in the AC form and can be decoupled in the local d-q frame. Because the real-time value of each ES's reactive power does not change with the reference d-q frame, it is possible to compute ES-j's reactive power by calculating the d/q components of d_{ji} with respect to the local reference of ES-i:

$$d_{ji}^{d/q} = [V_{es_j}^d, V_{es_j}^q, I_{SL_j}^d, I_{SL_j}^q]^T \tag{8}$$

From the received data, ES-i is then able to calculate the reactive power, allowing for the consensus input to be computed. The reactive power values of both neighbor and local ES are then fed into the consensus algorithm. A compensator value δ is generated by the following equation:

$$\dot{\delta} = \mathrm{c}^Q \sum_{j \in N_i} a_{ij}(Q_{esj} - Q_{esi}) \tag{9}$$

where c^Q is the coupling parameter between the voltage and reactive power in the regulator. The error signal is added to the voltage reference V_{ref} to adjust the reference point. The control input in the q-axis is given by:

$$u_i^q = K_P^q(V_{ref} + \delta - V_{si}) + K_I^q \int (V_{ref} + \delta - V_{si}) \tag{10}$$

where V_{si} is the mains bus voltage, K_P^q and K_I^q are the proportional and integrator gains for the q axis, respectively. Similarly, u_i^d can be written as:

$$u_i^d = K_P^d(-V_{es}^d) + K_I^d \int (-V_{es}^d) \tag{11}$$

where K_P^d and K_I^d are the proportional and integrator gains regulating the d-axis voltage, respectively. The input in (5) is the real input voltage V_{in} which can be derived by multiplying u_i^q and u_i^d with a fixed factor. This factor is related to the dc voltage and modulation gain. As proved in [4], the proposed consensus control can guarantee the main bus voltage regulation and reactive power-sharing performance in steady state.

Remark 1: Note that the subscript ji is used rather than j to explicitly emphasize that the communicated data vector is being transmitted from ES-j to ES-i.

To simplify the analysis, the following assumptions about the communication network are clarified:

Assumption 1: The topology of the communication network mirrors that of the physical network.

Reason: In consensus control, neighbor smart loads communicate with one another. This scenario reflects the physical connections in a distribution grid.

Assumption 2: The communication is ideal, i.e., it is instantaneous and exact. No communication delay issue will be studied. The transmitted information is always correct when there is no cyber-attack.

Reason: The communications occur among neighboring devices in the proximity. The latency of the communication system is much smaller than the time scale of a 50Hz/60Hz ac mains.

Specifically, we define the vector ξ_i^r, which is the communicated interconnection term (different from the real interconnection term ξ_i in model (4)), as computed by ES-i:

$$\xi_i^r = \begin{bmatrix} H_l & 0 \\ 0 & H_k \end{bmatrix} \begin{bmatrix} d_{li}^{d/q} \\ d_{ki}^{d/q} \end{bmatrix}, \tag{12}$$

where

$$H_j = \begin{bmatrix} 1 & 0 & R_{nc_j} & 0 \\ 0 & 1 & 0 & R_{nc_j} \end{bmatrix}. \tag{13}$$

This interconnection term will be used for cyber-attack detection.

The usage of a large group of distributed ESs in the power grid could be associated with a wide range of electric loads [6], [7], PV panels [5] and energy storage [21] in the power network. Consequently, the collective stabilizing effects of distributed ESs are less dependent on the power factors of the individual electric loads in practice. The ratings of the ESs are typically less than 15% of those of the noncritical loads [22]. Thus, ES technology is an economical and distributed way to stabilize the power grid.

D. CYBER ATTACK ON ES

The introduction of communication in the control architecture for a network of ESs possibly exposes the ESs to cyber-attacks. As shown in Fig. 5, potential cyber-attacks may tamper with the information package d_{ji}. As a result, the local ES will get the wrong reactive power value of its neighbor and the expected control performance cannot be achieved.

To model the cyber-attack behavior, the action of the attack on the transmitted information can be formalized by defining an additional variable:

$$d_{ji}^r(t) = d_{ji}(t) + \phi_{ji}(t) \tag{14}$$

containing the data as received by ES-i, and where $\phi_{ji}(t)$ is a function defined by the attacker, unknown to the ES controller, with the following characteristics:

$$\phi_{ji} : \begin{cases} = 0, & t < T_a \\ \neq 0, & t > T_a \end{cases} \tag{15}$$

with $T_a > 0$ the time instance at which the attacker starts influencing the communicated data. Furthermore, ξ_i^r in (12) is redefined with the attacked information d_{ji}^r. Given the possible presence of a cyber-attack in the communication infrastructure, it is necessary to design a monitoring strategy to tackle the following "attack detection" problem:

TABLE 1. Experimental setup parameters.

Symbol	Quantity	Value
R_{21}	Line12 resistance	0.2297Ω
L_{21}	Line12 inductance	4.428mH
R_{23}	Line23 resistance	0.2296Ω
L_{23}	Line23 inductance	4.426mH
f_s	Sampling frequency	7.5 kHz
R_{nc1}	Noncritical load1 resistance	39.01Ω
R_{nc2}	Noncritical load2 resistance	41.58Ω
R_{nc3}	Noncritical load3 resistance	40.39Ω
L_{f1}	ES-1 filter inductance	0.5mH
R_{L1}	ES-1 filter inductor resistance	0.0926Ω
C_{f1}	ES-1 filter capacitance	6.6μF
L_{f2}	ES-2 filter inductance	0.5mH
R_{L2}	ES-2 filter inductor resistance	0.0926Ω
C_{f2}	ES-2 filter capacitance	6.6μF
L_{f3}	ES-3 filter inductance	0.6mH
R_{L3}	ES-3 filter inductor resistance	0.1Ω
C_{f3}	ES-3 filter capacitance	6.65μF
	Controller parameter	
K_P^d	d-axis controller proportional gain	3
K_I^d	d-axis controller integral gain	10
K_P^q	q-axis controller proportional gain	0.3
K_I^q	q-axis controller integral gain	4
c^Q	Consensus coupling gain	0.3

Problem 1 (Attack Detection): Given ES-i possibly subject to attacks, design an attack detection module D_i to verify whether:

$$d_{ji}^r(t) = d_{ji}(t), \quad \forall j \in N_i, \tag{16}$$

i.e., whether an attack is active on any communication channel into ES-i or not. The design of the attack detection module will be the subject of the following Section.

III. CYBER ATTACK DETECTION

To detect cyber-attacks in the communication between neighboring ESs, it is necessary to equip each ES with a local monitoring tool (called a *diagnoser*). The diagnoser consists of a distributed state estimator (from which a residual is generated) and a detection algorithm. In this section, a discretization method for the system model is described first. Then, the distributed estimator and the detection method are explained.

A. MODEL DISCRETIZATION

The design of the attack detection module is implemented on a digital controller. Based on the state-space model of the ES, the discretized dynamic model with the additional unstructured and unknown disturbance terms is expressed as:

$$\begin{aligned} x_i^+ &= \bar{A}_{ii} x_i + \bar{B} u_i + \bar{G}_i \xi_i + w_i \\ y_i &= C_i x_i + \rho_i \end{aligned} \tag{17}$$

where w_i and ρ_i are the process and measurement noise terms. The notation x_i^+ is used as a shorthand for $x(k+1)$, where $k \in Z_0$ is the index indicating the time instance. Rewrite x_i in the discrete form:

$$x_i(k) = x_i(t), \quad t = kT_s \tag{18}$$

where T_s is the sampling time. The following two assumptions are considered for (18):

Assumption 3: For all time instances $k \in \mathrm{Z}_0$, the process and measurement noises are modeled as independent and identically distributed (i.i.d) Gaussian noise:

$$w_i(k) \sim N(0, W_i), \quad \rho_i(k) \sim N(0, R_i), \quad \forall k \geq 0, \tag{19}$$

where $W_i > 0, R_i \geq 0$ are known covariance matrices, and we assume that the initial state is i.i.d. Gaussian:

$$x_i(0) \sim N\left(\bar{x}_i^0, \Pi_i^0\right) \tag{20}$$

with $\Pi_i^0 > 0$, and is independent of the noise terms, for all $k \geq 0$.

Assumption 4:For all time in between sampling intervals, $t \in [k, k+1)$ input terms u_i and ξ_i are approximated as being constant.

The discrete-time dynamics matrices in (17) are computed using exact discretization from the equations in (4) and Assumption 4, as follows:

$$\begin{aligned} \bar{A}_{ii} &= e^{A_{ii}T_s}, \quad \bar{B}_i = A_{ii}^{-1}(I - e^{A_{ii}T_s})B_i, \\ \bar{G}_i &= A_{ii}^{-1}(I - e^{A_{ii}T_s})G_i \end{aligned} \tag{21}$$

Remark 2 (PWM Input Voltage): The input to the ES is defined as a PWM input voltage. Thus, V_{in} is a highly nonlinear, switching input. Thus, to improve the performance of the state estimator (to be defined in the following section), we suppose that V_{in} is an *unknown input*. This, on the one hand, binds us to the use of those state estimators that are decoupled to the input u_i, on the other hand it allows us to remove the error caused by approximating V_{in} as a sine wave.

B. DISTRIBUTED STATE ESTIMATOR

As anticipated in Remark 2, a state estimator for which V_{in} is an unknown input can be used to decouple the estimation error from the nonlinearities introduced by the PWM input voltage. Here we exploit the use of the *unbiased* Kalman Filter (KF) proposed in [12], which states that the following two conditions must be satisfied:

i. *Pair $(C_i, \bar{A}_{ii})$ is observable;*

ii. *Matrices C_i and $\bar{B}_i$ are such that $rank(C_i\bar{B}_i) = rank(\bar{B}_i)$.*

Through matrix analysis, it can be shown that $\bar{A}_{ii}$, $\bar{B}_i$, and C_i as defined in (4) and (21) meet these conditions.

To remove any possible bias from the estimation error (i.e., the difference between the estimated parameters and the real values of the electrical components), we augment the ES's state by defining $\mathrm{x}_i = [\,x_i^T \;\; \zeta_i^T\,]^T$, where ζ_i is taken to be a constant output bias vector, with the following dynamics:

$$\begin{aligned} \mathrm{x}_i^+ &= \begin{bmatrix} \bar{A}_{ii} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} \end{bmatrix} \mathrm{x}_i + \begin{bmatrix} \bar{B}_i \\ \mathbf{0} \end{bmatrix} u_i + \begin{bmatrix} \bar{G}_i \\ \mathbf{0} \end{bmatrix} \xi_i + \begin{bmatrix} \mathbf{I} \\ \mathbf{0} \end{bmatrix} w_i \\ &= \mathbf{A}_{ii}\mathrm{x}_i + \mathbf{B}_i u_i + \mathbf{G}_i \xi + \mathbf{w}_i \end{aligned} \tag{22a}$$

$$\begin{aligned} y_i &= [\,C_i \quad I\,]\mathrm{x}_i + \rho_i \\ &= \mathbf{C}_i \mathrm{x}_i + \rho_i \end{aligned} \tag{22b}$$

Note that the conditions *i.* and *ii.* remain satisfied by the matrices defined in (22a) and (22b). The following equations define the dynamics of the state estimator unbiased by u_i:

$$\begin{aligned} \hat{\mathrm{x}}_i(k) &= \bar{\mathbf{A}}_i(\mathrm{k})[\mathbf{A}_{ii}\hat{\mathrm{x}}_i(\mathrm{k}-1) + \mathbf{G}_i\xi_{ij}^r(k-1)] + \bar{\mathbf{L}}_i y_i(k) \\ \hat{y}_i &= \mathbf{C}_i\hat{\mathrm{x}}_i \end{aligned} \tag{23}$$

Note that the input value u_i does not appear in (23), as the estimator is designed to be independent of the unknown switching input. $\hat{\mathrm{x}}_i$ is an estimator of the system state. Note that the interconnection term ξ_i in (22a) is replaced by the communication connection term ξ_{ij}^r, which may be corrupted by a cyber-attack. This allows for cyber-attack detection because when an attack is active, it will introduce an error between the ES's state x_i and the state estimate $\hat{x}_i$. The matrices $\bar{\mathbf{A}}_i$ and $\bar{\mathbf{L}}_i$ in (23) are defined as follows:

$$\begin{aligned} \bar{\boldsymbol{L}}_i(k) &= \boldsymbol{K}_i(k) + [\boldsymbol{I} - \boldsymbol{K}_i(k)\boldsymbol{C}_i]\boldsymbol{B}_i\boldsymbol{M}_i(k) \\ \bar{\boldsymbol{A}}_i(k) &= [\boldsymbol{I} - \boldsymbol{K}_i(k)\boldsymbol{C}_i][\boldsymbol{I} - \boldsymbol{B}_i\boldsymbol{M}_i(k)\boldsymbol{C}_i] \\ &= \boldsymbol{I} - \bar{\boldsymbol{L}}_i(k)\boldsymbol{C}_i \end{aligned} \tag{24}$$

The estimation error is defined as $\varepsilon_i = x_i - \widehat{x}_i$ and the residual is given by $r_i = y_i - \widehat{y}_i$. Fig. 6 shows the block diagram of the state estimator, as defined in (23). Therefore, the proposed Kalman filter can estimate ES-i's state with input u_i unknown to the estimator.

Given their definition in [12], matrices $\mathbf{M}_i(k)$ and $\mathbf{K}_i(k)$ guarantee that the estimation error does not depend on the switching input u_i. $\mathbf{M}_i(k)$ is designed at each time step k such that the following proposition holds:

Lemma 1: Consider the joint input and state estimator in (23), where $\mathbf{M}_\mathrm{i}(\mathrm{k})$ satisfies:

$$M_i(k)C_iG_i = \mathbf{I}_{gi}, \quad \forall k \geq 0. \tag{25}$$

Thus, if $\mathbf{M}_\mathrm{i}(\mathrm{k})$ and $\mathbf{K}_\mathrm{i}(\mathrm{k})$ are designed as in [12], the model estimator (23) is an unbiased estimate of $\mathbf{x}_\mathrm{i}(\mathrm{k})$, minimizing the mean square error over the class of all linear unbiased estimates based on $\bar{x}_i^0$ and $y_i(\kappa), 0 \leq \kappa \leq k$.

The dynamics of estimation error $\boldsymbol{\varepsilon}_i$ and residual can be derived from (22) and (23):

$$\begin{aligned} \boldsymbol{\varepsilon}_i(k) &= \bar{\mathbf{A}}_i(\mathrm{k})[\mathbf{A}_{ii}\boldsymbol{\varepsilon}_i(\mathrm{k}-1) + \mathbf{G}_i(\lambda_i(k-1)) + w_i(k-1)] \\ &\quad - \bar{\mathbf{L}}_i(k)\rho_i(k) \\ r_i(k) &= C_i\boldsymbol{\varepsilon}_i(k) + \rho_i(k) \end{aligned} \tag{26}$$

where $\lambda_i = \xi_i - \xi_{ij}^r$ models the difference between the interconnection with neighboring states and the measurements which are transmitted to ES-i. Note that, under normal conditions, this difference is the measurement noise. Hence, it follows an independent and identically distributed (i.i.d.) Gaussian distribution $\lambda_i \sim (0, \Lambda_i)$, where Λ_i is a linear combination of $R_j, j \in N_i$. Hence, the estimation error and residual covariance matrices can be expressed as:

$$\begin{aligned} \Pi_i(k) &= \bar{A}_i(k)\left(A_{ii}\Pi_i(k-1)A_{ii}^\top + G_i\Lambda_iG_i^\top + W_i\right)\bar{A}_i^\top(k) \\ &\quad + \bar{L}_i(k)R_i\bar{L}_i^\top(k). \end{aligned} \tag{27}$$

$$P_i(k) = C_i\Pi_i(k)C_i^\top + R_i - C_i\bar{L}_i(k)R_i - R_i\bar{L}_i^\top(k)C_i^\top. \tag{28}$$

C. ATTACK DETECTION STRATEGY

From the definition of the residual and its covariance [13], the cyber-attack detection strategy is presented here. Under normal conditions, both the estimation error and the residual of the unbiased Kalman Filter approach asymptotically zero-mean Gaussian processes. However, after the onset of a cyber-attack, which is a non-zero deterministic signal, the residual will not be zero mean, but rather:

$$r_i(k) = \mathrm{r}_i^h(k) + r_i^a(k), \quad \forall k \geq T_a \tag{29}$$

where r_i^h and r_i^a are respectively the *healthy* and *attacked* components of the residual. While the healthy portion of the residual, r_i^h, has the same definition of the residual in nominal conditions (26), r_i^a is defined as follows:

$$r_i^a(k) = \mathbf{C}_i \boldsymbol{\varepsilon}_i^a(k) = \mathbf{C}_i \overline{\mathbf{A}}_i(k) G_i \tilde{H}_i \phi_{ji}(k-1) \tag{30}$$

where $\tilde{H}_i$ is a block matrix which is nonzero in correspondence to the attacked information from the neighbor j. Hence, for $\phi_{ji} \neq 0$, $r_i^a \neq 0$.

Given the change in the mean of the residual after an attack, it is possible to exploit well-established change detection algorithms available in the literature [18]. These algorithms exploit the stochastic properties of the residual to discriminate between the following hypotheses:

$$\begin{aligned} \mathcal{H}_i^0 &: r_i = r_i^h \\ \mathcal{H}_i^1 &: r_i = r_i^h + r_i^a, \end{aligned} \tag{31}$$

where $\mathcal{H}_i^0$ is the null-hypothesis, i.e., the diagnostic supposes the system is not under attack. If $\mathcal{H}_i^1$ is chosen, then an attack is thought to be present on the communication link between ES-i and its neighbors, i.e., detection occurs.

In this work, we exploit a detection scheme similar to that described in [12]. We start by introducing an auxiliary variable $T_i(r_i, k)$ and an appropriately defined threshold $\theta_i(k)$, such that when

$$T_i(r_i, k) = \sum_{\kappa=k-W_i+1}^{k} r_i(\kappa)^{\mathrm{T}} P_i(\kappa)^{-1} r_1(\kappa) > \theta_i(k) \tag{32}$$

holds, $\mathcal{H}_i^1$ is thought to be active. Otherwise $\mathcal{H}_i^0$ is chosen. W_i is the length of a window over which T_i is computed.

Remark 3: The choice of the detection threshold $\theta_i(k)$ is fundamental to the performance of the detection scheme. If the threshold is selected to be too high, (32) will not hold except in the most extreme cases. If it is selected too low, it may lead to a high probability of false alarms, i.e., saying $\theta_i(k)$ is active while there is no attack. While this aspect is out of the scope of this paper, readers interested in it should refer to [18] and [19] and their citations therein for methods of threshold selection. Note, specifically, that there exist methods to define $\theta_i(k)$ such that certain properties are guaranteed by the detection scheme, e.g., user-defined false-alarm rates.

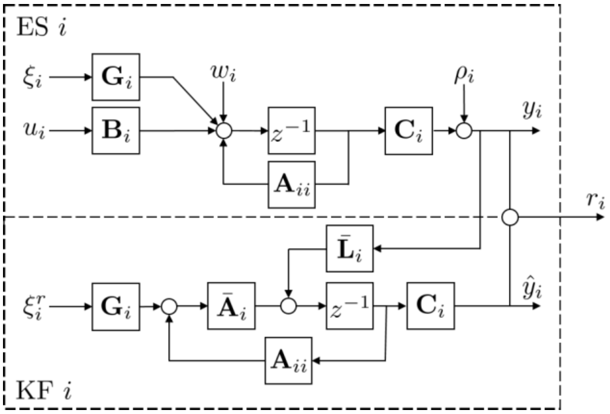


FIGURE 6. Block diagram of the state estimator (Kalman filter).

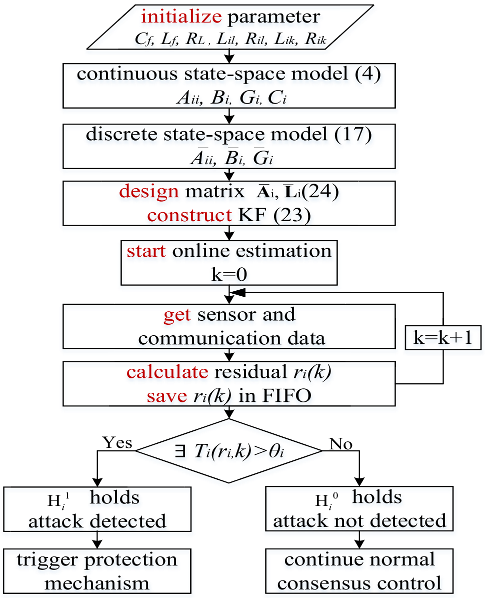

initialize parameter
$C_f, L_f, R_L, L_{il}, R_{il}, L_{ik}, R_{ik}$
continuous state-space model (4)
A_{ii}, B_i, G_i, C_i
discrete state-space model (17)
$\bar{A}_{ii}, \bar{B}_i, \bar{G}_i$
design matrix $\bar{\mathbf{A}}_i, \bar{\mathbf{L}}_i$(24)
construct KF (23)
start online estimation
k=0
get sensor and communication data
k=k+1
calculate residual $r_i(k)$
save $r_i(k)$ in FIFO
Yes
$\exists\ T_i(r_i,k)>\theta_i$
No
H_i^1 holds
attack detected
H_i^0 holds
attack not detected
trigger protection mechanism
continue normal consensus control

FIGURE 7. Flowchart of the estimator design and attack detection method.

The flowchart in Fig. 7 presents the proposed cyber-attack detection method. The method starts by initializing the offline ES state-space model with circuit parameters. The model is then discretized by (17). A Kalman filter can be constructed as a local estimator based on (23) and (24). Then, the distributed state estimator can be implemented as a module in the ES controller which requires only local and neighboring data. At each sampling step, the residual signal $r_i(k)$ is calculated and saved in a FIFO (first-in, first-out) buffer. The cyber-attack module then compares $T_i(r_i, k)$ with the threshold $\theta_i(k)$ to detect the presence of an attack. If a cyber-attack is detected, a protection mechanism will be triggered. The consensus control will ignore the attacked neighboring data and will use the previous consensus data during the attack. After the attack disappears, consensus control output can be updated with normal data. This mechanism can ride through the cyber-attack smoothly and preserve power-sharing ability during the attack.

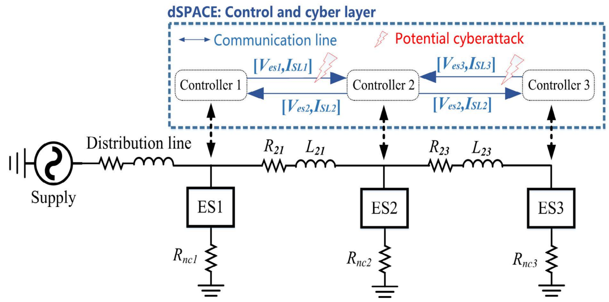


FIGURE 8. Experiment setup of three distributed ESs in a microgrid.

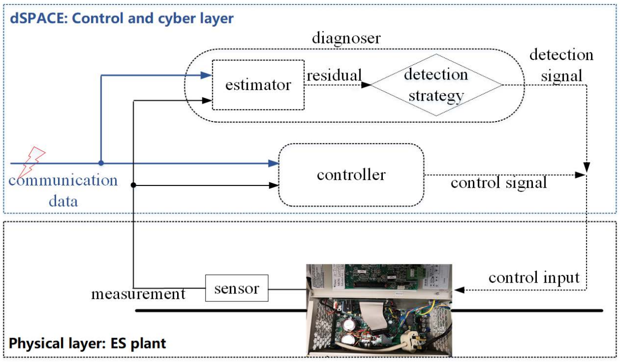


FIGURE 9. Implementation of a cyber-attack diagnoser in the ES.

IV. EXPERIMENTAL TESTS

A. EXPERIMENT SETUP

The proposed cyber-attack detection method is validated in an experimental test. The hardware setup involves a 110V AC microgrid with three distributed ESs as shown in Fig. 8. A programmable power source (California Instruments CSW550) is used to emulate a power system with changing renewable power. Three ESs are located along the distribution line, and each is connected in series with a resistance load. Lead-acid battery cells with Model No. LC-R127R2NA (and ratings of 12V, 7.2 Ah/20 hr) are used in the experiment. The three controllers and communication networks are implemented in the dSPACE system. For the control layer, three virtual control blocks are established in the dSPACE. Each controller collects local ES sensors' data and sends the real-time PWM signal to the ES hardware. According to Assumption 2, the communication links are ideal and simulated in dSPACE. The cyber layer has a chain topology which is the same as the physical layer.

Each ES is equipped with a specially designed cyber-attack detection module, as shown in Fig. 9. The diagnoser consists of a state estimator and a cyber-attack detection strategy as presented in Section III. The designing process of the detection module follows the steps shown in flowchart Fig. 7. Implemented in dSPACE, the diagnoser collects real-time local sensor measurements and communication data. Working parallelly with the local controller, the detection module generates a detection signal and triggers the alarm in case of any cyber-attack. Here we choose ES-*2* as the test subject and ignore the duplicated results on different ESs. Potential cyber-attacks may change the data sent from ES-*1* to ES-*2* and ES-*3* to ES-*2* as marked in red in Fig. 8. The parameters of the experimental setup are listed in TABLE 1.

B. EXPERIMENTAL RESULTS: DETECTION OF CYBER-ATTACK

The proposed cyber-attack detection method is verified by experimental results, as shown in Fig. 10. A cyber-attack occurs in the communication link between ES-*1* and ES-*2* at $t = 13.13$s. The attack changes the ES-*2*'s received data V$_{es1}$ (ES-*1* voltage) to a sinusoidal signal with a constant 30V amplitude (RMS value 21.21V). The attacked signal has the same phase with the real V$_{es1}$ signal in the test. Before the attack, the line voltages V$_{s1}$, V$_{s2}$, V$_{s3}$ are well regulated at 110V (RMS value) and V$_{es2}$ = 30V(RMS). The constant attack is then injected into the consensus control loop to change the consensus equilibrium of the system. As protection operation is not considered yet, the attack will keep influencing the system dynamic until the end. As shown in Fig. 10(b), ES-*2* voltage drops immediately after the attack and moves slowly to a new equilibrium around 21.21V RMS. Consequently, all ESs reduce the output power and cannot support the system voltage adequately. This leads to a drop in the line voltage as shown in Fig. 10(a). Fig. 10(c)-(h) show the auxiliary variables $T_i(r_i, k)$ compared to an appropriate threshold $\theta_i(k)$ which is designed such that the overall probability of false alarm is 5% [12]. Note that instead of the original residual signals, the auxiliary variables $T_i(r_i, k)$ are used. In the test, we replace line current I_{21} and I_{23} by local net current I$_{SL}$ assuming only the net current is measurable, as $I_{SL} = I_{21} + I_{23}$. The dotted lines are the threshold value. As shown in the figure, the residual signals are near zero in normal state and increase in response to the attack. Three residual signals generated by V_{es}^d, V_{es}^q and I_L^d exceed the threshold and trigger the detection alarm as shown in Fig. 10(c), (d) and (e). At around $t = 13.14$s, the cyber-attack is detected rapidly (i.e., a detection time of 0.01s.)

C. EXPERIMENTAL RESULTS: COUNTERMEASURE TO TACKLE CYBER-ATTACK

Strategies to tackle cyber-attacks on distributed ESs depend on the persistence of the attack. For non-persistent attacks (e.g., within a few seconds), the original control data can be retained for the distributed ESs to ride through the attacks via consensus control. Tests based on the setup in Fig. 8 have been conducted. Fig. 11 shows the practical measurements of the nodal voltages (V_{s1}, V_{s2} and V_{s3}) of the distributed ESs. The consensus control successfully maintains voltage regulations for the local voltages during the attack and also resumes normal services after the attack.

Fig. 12 shows the experimental results when the attack is persistent. If the persistent attack lasts longer than the ride-through period based on the previous control data, resuming consensus control with false data cannot lead to normal services as shown in Fig. 12. In this case, individual inbuilt

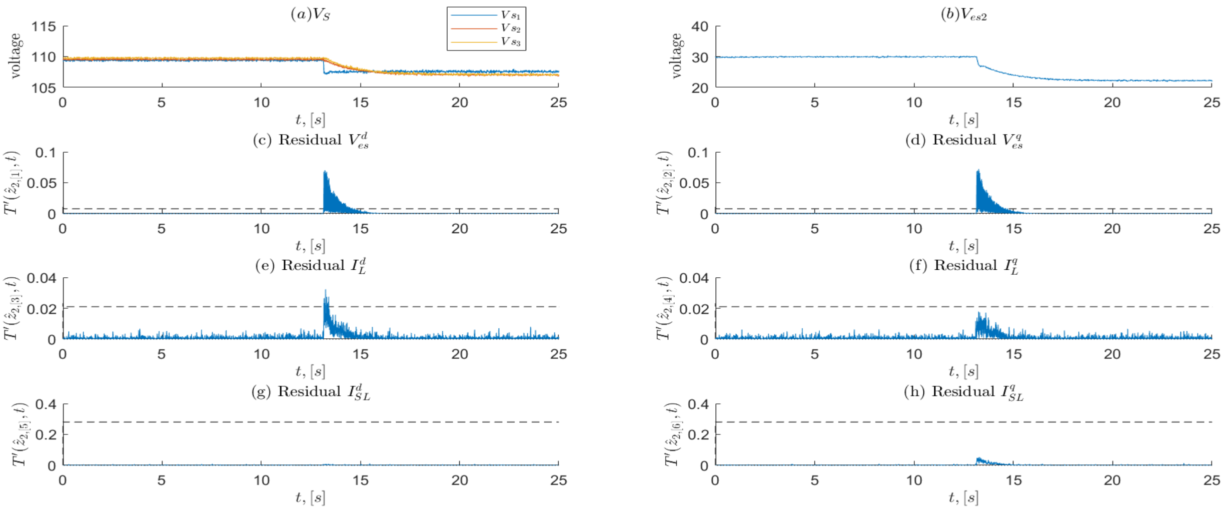


FIGURE 10. Experiment results of a cyber-attack with a constant amplitude 30V in the communication link.

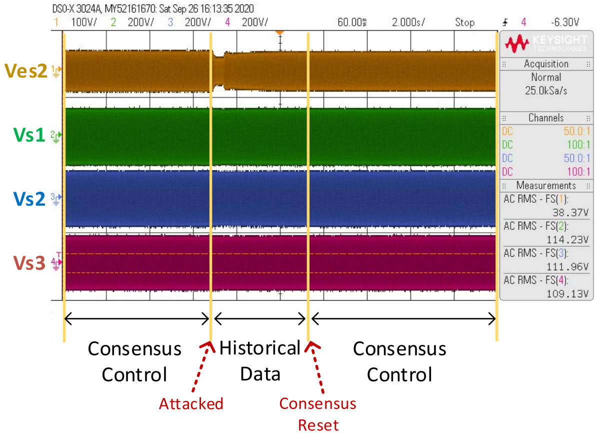


FIGURE 11. Practical results of the countermeasure to ride through non-persistant cyber-attack.

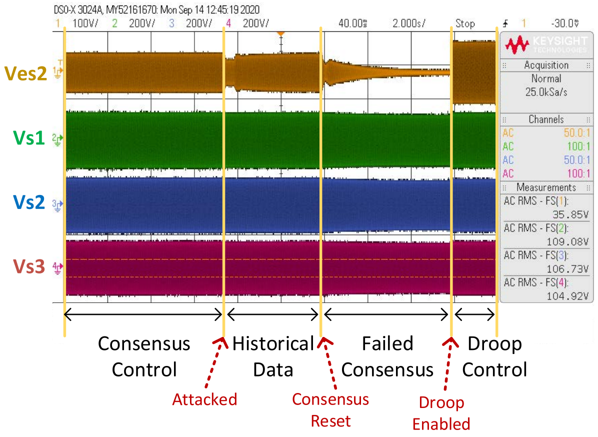


FIGURE 12. Practical results of the countermeasure for persistent cyber-attack based on consensus and droop control.

droop control in each ES can take over so that normal voltage regulation can be achieved, despite that responsibility sharing among the distributed ESs will be abandoned temporarily. As mentioned previously in [4] and [20], the advantage of distributed ESs is that ESs can operate individually and collectively with droop control even if there is no cyber-layer for consensus control. But the availability of the consensus control in the cyber layer provides the extra advantage of allowing the distributed ESs to share responsibility in providing their voltage and/or frequency regulatory functions in the power grid.

V. CONCLUSION

In this paper, a distributed cyber-attack detection architecture for ESs in a microgrid and a countermeasure are proposed and practically evaluated. A local attack diagnoser composed of a state estimator and detection algorithm is designed for each ES. The residual signal and threshold are designed to perform the detection strategy. The protection mechanism will be triggered to smooth the dynamics during cyber-attacks. A practical evaluation of this distributed detection architecture is presented with experimental results. The proposed method can be applied in principle to detect cyber-attack in distributed control of grid-connected power electronic equipment. A strategy of countermeasure based on the persistence of the attack has been developed and implemented. It is confirmed that retention of the control data before the attack can allow the distributed ESs to ride through non-persistent cyber-attack with consensus control. However, if the cyber-attack persists, the ESs can revert to their individual droop control to continue voltage and/or frequency regulatory services. This important feature of distributed ESs provides extra robustness to power system stability. With the urgent need to increase renewable energy generation of intermittent nature to combat climate change, the consensus control of distributed ESs could offer a drastic solution to increase wind and solar power generation without causing power system instability.

APPENDIX

$$A_{ii} = \begin{bmatrix} 0 & \omega & \frac{1}{C_f} & 0 & \frac{1}{C_f} & 0 & \frac{1}{C_f} & 0 \\ -\omega & 0 & 0 & \frac{1}{C_f} & 0 & \frac{1}{C_f} & 0 & \frac{1}{C_f} \\ -\frac{1}{L_f} & 0 & -\frac{R_L}{L_f} & \omega & 0 & 0 & 0 & 0 \\ 0 & -\frac{1}{L_f} & -\omega & -\frac{R_L}{L_f} & 0 & 0 & 0 & 0 \\ -\frac{1}{L_{il}} & 0 & 0 & 0 & -\frac{R_{nc}+R_{il}}{L_{il}} & \omega & -\frac{R_{nc}}{L_{il}} & 0 \\ 0 & -\frac{1}{L_{il}} & 0 & 0 & -\omega & -\frac{R_{nc}+R_{il}}{L_{il}} & 0 & -\frac{R_{nc}}{L_{il}} \\ -\frac{1}{L_{ik}} & 0 & 0 & 0 & -\frac{R_{nc}}{L_{ik}} & 0 & -\frac{R_{nc}+R_{ik}}{L_{ik}} & \omega \\ 0 & -\frac{1}{L_{ik}} & 0 & 0 & 0 & -\frac{R_{nc}}{L_{ik}} & -\omega & -\frac{R_{nc}+R_{ik}}{L_{ik}} \end{bmatrix}$$

$$B_i = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ \frac{1}{L_f} & 0 \\ 0 & \frac{1}{L_f} \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \quad G_i = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{L_{il}} & 0 & 0 & 0 \\ 0 & \frac{1}{L_{il}} & 0 & 0 \\ 0 & 0 & \frac{1}{L_{ik}} & 0 \\ 0 & 0 & 0 & \frac{1}{L_{ik}} \end{bmatrix}$$

REFERENCES

[1] F. Blaabjerg, Z. Chen, and S. B. Kjaer, "Power electronics as efficient interface in dispersed power generation systems," *IEEE Trans. Power Electron.*, vol. 19, no. 5, pp. 1184–1194, Sep. 2004.

[2] S. Sahoo, T. Dragicevic, and F. Blaabjerg, "Cyber security in control of grid-tied power electronic converters—Challenges and vulnerabilities," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 5, pp. 5326–5340, Oct. 2021.

[3] M. Chen and H. V. Poor, "High-frequency power electronics at the grid edge: A bottom-up approach toward the smart grid," *IEEE Electrific. Mag.*, vol. 8, no. 3, pp. 6–17, Sep. 2020.

[4] J. Chen, S. Yan, T. Yang, S.-C. Tan, and S. Y. Hui, "Practical evaluation of droop and consensus control of distributed electric springs for both voltage and frequency regulation in microgrid," *IEEE Trans. Power Electron.*, vol. 34, no. 7, pp. 6947–6959, Jul. 2019.

[5] T. Yang, K.-T. Mok, S.-S. Ho, S.-C. Tan, C.-K. Lee, and R. S. Y. Hui, "Use of integrated photovoltaic-electric spring system as a power balancer in power distribution networks," *IEEE Trans. Power Electron.*, vol. 34, no. 6, pp. 5312–5324, Jun. 2019.

[6] S. Yan, S.-C. Tan, C.-K. Lee, B. Chaudhuri, and S. Y. R. Hui, "Use of smart loads for power quality improvement," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 5, no. 1, pp. 504–512, Mar. 2017.

[7] S. Yan, M.-H. Wang, T.-B. Yang, S.-C. Tan, B. Chaudhuri, and S. Y. R. Hui, "Achieving multiple functions of three-phase electric springs in unbalanced three-phase power systems using the instantaneous power theory," *IEEE Trans. Power Electron.*, vol. 33, no. 7, pp. 5784–5795, Jul. 2018.

[8] L. Liang, Y. Hou, D. J. Hill, and S. Y. R. Hui, "Enhancing resilience of microgrids with electric springs," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 2235–2247, May 2018.

[9] E. Hossain, Z. Han, and H. V. Poor, *Smart Grid Communications and Networking*. Cambridge, U.K.: Cambridge Univ. Press, 2012.

[10] J. W. Simpson-Porco, Q. Shafiee, F. Dörfler, J. C. Vasquez, J. M. Guerrero, and F. Bullo, "Secondary frequency and voltage control of islanded microgrids via distributed averaging," *IEEE Trans. Ind. Electron.*, vol. 62, no. 11, pp. 7025–7038, May 2015.

[11] R. Olfati-Saber, J. A. Fax, and R. M. Murray, "Consensus and cooperation in networked multi-agent systems," *Proc. IEEE*, vol. 95, no. 1, pp. 215–233, Jan. 2007.

[12] S. Gillijns and B. De Moor, "Unbiased minimum-variance input and state estimation for linear discrete-time systems," *Automatica*, vol. 43, no. 1, pp. 111–116, Jan. 2007.

[13] S. A. Yadav, S. R. Kumar, S. Sharma, and A. Singh, "A review of possibilities and solutions of cyber attacks in smart grids," in *Proc. Int. Conf. Innov. Challenges Cyber Secur. (ICICCS-INBUSH)*, Feb. 2016, pp. 60–63.

[14] S. Sahoo, S. Mishra, J. C.-H. Peng, and T. Dragicevic, "A stealth cyber-attack detection strategy for DC microgrids," *IEEE Trans. Power Electron.*, vol. 34, no. 8, pp. 8162–8174, Aug. 2019.

[15] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, B. Pranggono, and H. F. Wang, "Intrusion detection system for IEC 60870-5-104 based SCADA networks," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2013, pp. 1–5.

[16] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 411–423, Apr. 2017.

[17] A. Barboni, A. J. Gallo, F. Boem, and T. Parisini, "A distributed approach for the detection of covert attacks in interconnected systems with stochastic uncertainties," in *Proc. IEEE 58th Conf. Decis. Control (CDC)*, Dec. 2019, pp. 5623–5628.

[18] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki, *Diagnosis and Fault-Tolerant Control*, 3rd ed. New York, NY, USA: Springer, 2003.

[19] S. M. Kay, *Fundamentals of Statistical Signal Processing: Detection Theory*. Upper Saddle River, NJ, USA: Prentice-Hall, 1993.

[20] S. Y. Hui, C. K. Lee, and F. F. Wu, "Electric springs—A new smart grid technology," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1552–1561, Sep. 2012.

[21] T. Yang, K. T. Mok, S.-C. Tan, C.-K. Lee, and S.-Y.-R. Hui, "Electric springs with coordinated battery management for reducing voltage and frequency fluctuations in microgrids," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1943–1952, May 2018.

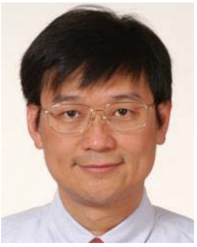
[22] D. Chakravorty, Z. Akhtar, B. Chaudhuri, and S. Y. Ron Hui, "Comparison of primary frequency control using two smart load types," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2016, pp. 1–5.

JIE CHEN received the B.Eng. degree in electronic information and electrical engineering from Shanghai Jiao Tong University, Shanghai, China, in 2015, and the Ph.D. degree in power electronics from the Department of Electrical and Electronic Engineering, The University of Hong Kong, Hong Kong, in 2019. He is currently with Hivision Technology, Hangzhou, China. His research interests include smart grid technologies, electric springs, and consensus control.

ALEXANDER J. GALLO (Member, IEEE) received the Ph.D. degree from Imperial College London. He is currently a Postdoctoral Researcher at the Technical University of Delft, Delft, The Netherlands, as part of the AIM Wind Project. His main research interests include distributed cyber-security and fault tolerant control for large-scale interconnected systems, with a particular focus on energy distribution networks, as well as health-aware and fault tolerant control of wind turbines.

SHUO YAN (Senior Member, IEEE) received the B.Eng. degree in electrical engineering from the University of South China, Hengyang, China, in 2007, the M.Eng. degree in electrical engineering from Southeast University, Nanjing, China, in 2010, and the Ph.D. degree in electrical engineering from The University of Hong Kong, Hong Kong, SAR, in 2016. From 2016 to 2019, he worked as a Postdoctoral Fellow in power electronics and control at The University of Hong Kong. He is currently a Senior Lecturer and a Program Manager at RMIT University, Australia. His current research interests include power electronics, smart grids, renewable energy, and advanced control theory. He is an Associate Editor of *e-Prime, Advances in Electrical Engineering, Electronics and Energy*.

THOMAS PARISINI (Fellow, IEEE) received the Ph.D. degree in electronic engineering and computer science from the University of Genoa, in 1993, and the Ph.D. degree (Hons.) from the University of Aalborg, Denmark, in 2018. He was with the Politecnico di Milano. Since 2010, he has been holding the Chair of Industrial Control. Since 2001, he has been also a Danieli Endowed Chair of Automation Engineering with the University of Trieste. From 2009 to 2012, he was the Deputy Rector with the University of Trieste. In 2021, he worked as the Deputy Chair of the Employment & Education Task Force of the B20–Italy. He is currently the Director of Research at Imperial College London. He is the Deputy Director of the KIOS Research and Innovation Centre of Excellence, University of Cyprus. He authored or coauthored more than 350 research papers in archival journals, book chapters, and international conference proceedings. He was a recipient of the 2007 IEEE Distinguished Member Award. He was a co-recipient of the IFAC Best Application Paper Prize of the *Journal of Process Control* (Elsevier), for the three year period 2011–2013 and of the 2004 Outstanding Paper Award of the IEEE Transactions on Neural Networks. In 2016, he was awarded as Principal Investigator at Imperial of the H2020 European Union Flagship Teaming Project KIOS Research and Innovation Centre of Excellence led by the University of Cyprus. He serves as the 2021–2022 President for the IEEE Control Systems Society and has served as the Vice-President for Publications Activities. During 2009-2016, he was the Editor-in-Chief of the IEEE Transactions on Control Systems Technology. Since 2017, he has been the Editor of *Control Applications of Automatica*. Since 2018, he has been the Editor-in-Chief of the *European Journal of Control*.



SHU YUEN RON HUI (Fellow, IEEE) received the B.Sc. (Eng.) (Hons.) in electrical and electronic engineering from the University of Birmingham, in 1984, and the D.I.C. and Ph.D. degrees in electrical engineering from Imperial College London, in 1987.

He was previously a Philip Wong Wilson Wong Professor at The University of Hong Kong. He currently holds the MediaTek Endowed Professorship at Nanyang Technological University and a Chair Professorship of power electronics at Imperial College London. He has published over 500 research articles, including 300 refereed journal publications. Over 120 of his patents have been adopted by industry worldwide. His research interests include power electronics, wireless power, sustainable lighting, and smart grid. His inventions on wireless charging platform technology underpin key dimensions of Qi, the world's first wireless power standard, with freedom of positioning and localized charging features for wireless charging of consumer electronics. He also developed the Photo-Electro-Thermal Theory for LED Systems. He is a fellow of the Australian Academy of Technological Sciences & Engineering, the U.S. National Academy of Inventors, and the Royal Academy of Engineering, U.K. He received the IEEE Rudolf Chope Research and Development Award and the IET Achievement Medal (The Crompton Medal) in 2010 and the IEEE William E. Newell Power Electronics Award in 2015. During 2021–2022, he is the Chair of the IEEE Medal in Power Engineering Committee.