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

Jie Chen¹, Alexander J. Gallo², Member, IEEE, Shuo Yan³ Senior Member, IEEE, Thomas Parisini⁴, Fellow, IEEE and S.Y.R. Hui⁵, Fellow, IEEE

¹Hivision Technology, Hangzhou, China
²TU Delft, Delft, Netherlands
³Discipline of Electrical and Biomedical Engineering, RMIT University, Australia
⁴Department of Electrical and Electronic Engineering, Imperial College London, UK, with the KIOS Research and Innovation Centre of Excellence, University of Cyprus, Nicosia, Cyprus, and also with the Department of Engineering and Architecture, University of Trieste, Trieste, Italy
⁵School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, and also Department of Electrical and Electronic Engineering, Imperial College London, U.K.

Corresponding author: S.Y.R. Hui (e-mail: ron.hui@ntu.edu.sg).

This work was partially supported by the NTU-MediaTek Endowment fund 03INS001124C140 in Singapore and the European Union’s Horizon 2020 research and innovation program under grant agreement No 739551 (KIOS CoE), and by the Italian Ministry for Research in the framework of the 2017 Program for Research Projects of National Interest (PRIN), Grant no. 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]).

With the rapid development of the digital control and communication technologies, supervisory information-based control of microgrid power electronics converters 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.

Potential FDIA could change the information in the consensus control and alter its final control output to mislead the distributed power electronics systems. 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 microgrid [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 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.

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

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.

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

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

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

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):

\[
\begin{align*}
C_{f} \dot{V}_{es}^{d} &= \frac{1}{X_{C}} V_{es}^{d} + I_{L}^{d} + I_{R}^{d} + I_{I}^{d} \\
C_{f} \dot{V}_{es}^{q} &= -\frac{1}{X_{C}} V_{es}^{q} + I_{L}^{q} + I_{R}^{q} + I_{I}^{q} \\
L_{f} \dot{I}_{L}^{d} &= X_{L} I_{L}^{d} + V_{in}^{d} - V_{es}^{d} (-I_{L}^{d} R_{L}) \\
L_{f} \dot{I}_{L}^{q} &= -X_{L} I_{L}^{q} + V_{in}^{q} - V_{es}^{q} (-I_{L}^{q} R_{L}) \\
L_{n} \dot{I}_{i}^{d} &= X_{L} I_{i}^{d} + V_{in}^{d} - V_{es}^{d} - I_{SL}^{d} R_{nc} - I_{i}^{d} R_{i} \\
L_{n} \dot{I}_{i}^{q} &= -X_{L} I_{i}^{q} + V_{in}^{q} - V_{es}^{q} - I_{SL}^{q} R_{nc} - I_{i}^{q} R_{i} \\
L_{ik} \dot{I}_{i}^{d} &= X_{L} I_{ik}^{d} + V_{in}^{d} - V_{es}^{d} - I_{SL}^{d} R_{nc} - I_{ik}^{d} R_{ik} \\
L_{ik} \dot{I}_{i}^{q} &= -X_{L} I_{ik}^{q} + V_{in}^{q} - V_{es}^{q} - I_{SL}^{q} R_{nc} - I_{ik}^{q} R_{ik}
\end{align*}
\]

where \( V_{es} \) is the output voltage of the ES, \( I_{L} \) is the inductor current, and \( I_{R}, I_{i}, I_{ik} \) are the line currents. \( V_{in} \) is the voltage fed to the \( LC \) filter. \( V_{si}, V_{sk}, \) and \( V_{i} \) 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. \( L_{n}, R_{nc}, L_{i}, \) and \( R_{i} \) 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.: 

\[
X_{L} = \omega L , \quad X_{C} = \frac{1}{\omega C}
\]

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

\[
X_{L} = \omega L , \quad X_{C} = \frac{1}{\omega C}
\]
\[ I_{SL} = \sum_{j \in N_i} I_{ij} \]  

(3)

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

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

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

\[
\begin{align*}
\dot{x}_i &= A_{ij} x_i + B_{ij} u_i + G_{ij} \vec{z}_i \\
y_i &= C_{ij} x_i
\end{align*}
\]

(4)

where \( x_i \) is the state of the ES, \( u_i \) is the control input, \( \vec{z}_i \) 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:

\[
\begin{align*}
x_i &= [V_{es_i}^d, V_{es_i}^q, I_{el_i}^d, I_{el_i}^q, I_{sl_i}^d, I_{sl_i}^q, I_{sk_i}^d, I_{sk_i}^q]^T \\
\vec{z}_i &= [V_{sl_i}^d, V_{sl_i}^q, V_{sk_i}^d, V_{sk_i}^q]^T \\
y_i &= [x_i]
\end{align*}
\]

(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.

**FIGURE 5. Block diagram of consensus control of ES.**

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 \( Q_{es} \) is defined as:

\[ Q_{es} = V_{es}^q I_{SL}^d + V_{sl}^q I_{sl}^d \]  

(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:

\[ d_{ji}(t) = [V_{es_i}, I_{SL_i}]^T, j \in N_i. \]

(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:

\[ d_{ji}^{d/q} = [V_{es_i}, V_{es_j}, I_{SL_i}, I_{SL_j}]^T \]

(8)

From the received data, ES-i 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 \( \delta \) is generated by the following equation:

\[ \delta = c^0 \sum_{j \in N_i} a_{ij} (Q_{es_j} - Q_{es_i}) \]

(9)

where \( c^0 \) 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:

\[ u_i^q = K_p^q (V_{ref} + \delta - V_{sl}) + K_i^q \int (V_{ref} + \delta - V_{sl}) \]

(10)

where \( V_{sl} \) 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:

\[ u_i^d = K_p^d (-V_{sl}) + K_i^d \int (-V_{sl}) \]

(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 \( \xi^r \), which is the communicated interconnection term (different from the real interconnection term \( \xi \) in model (4)), as computed by ES-\( i \):

\[
\xi^r_i = \begin{bmatrix} H_j & 0 \\ 0 & H_j \end{bmatrix} \begin{bmatrix} d^{e/q} \\ d^{s/q} \end{bmatrix},
\]

where

\[
H_j = \begin{bmatrix} 1 & 0 & R_{wi} & 0 \\ 0 & 1 & 0 & R_{wi} \end{bmatrix}.
\]

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 \( d_p \). 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:

\[
d_p^a(t) = d_p(t) + \phi_p(t)
\]

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

\[
\phi_p(t) = \begin{cases} 0, & 0 < t < T_p \\ \neq 0, & t > T_p \end{cases}
\]

with \( T_p > 0 \) the time instance at which the attacker starts influencing the communicated data. Furthermore, \( \xi^r_i \) in (12) is redefined with the attacked information \( d_p^a(t) \). 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:

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

\[
d_p^a(t) = d_p(t), \forall j \in N,
\]

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 next 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:

\[
x_i^+ = \tilde{A}_i x_i + \tilde{B}_i u_i + \tilde{G}_i \xi_i + w_i
\]

\[
y_i = \tilde{C}_i x_i + \rho_i,
\]

where \( w_i \) and \( \rho_i \) 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:

\[
x_i(k) = x_i(t), t = kT_s
\]

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

Assumption 3. For all time instances \( k \in Z_0 \), the process and measurement noises are modeled as independent and identically distributed (i.i.d) Gaussian noise:

\[
w_i(k) \sim N(0, W_i), \rho_i(k) \sim N(0, R_i), \forall k \geq 0,
\]

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

\[
x_i(0) \sim N(x_0^i, \Omega_i^0)
\]

with \( \Omega_i^0 > 0 \), 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 \( \xi_i \) 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:

\[
\tilde{A}_i = A_i e^{A_i T_s}, \quad \tilde{B}_i = A_i^{-1}(1 - e^{-A_i T_s})B_i,
\]

\[
\tilde{G}_i = A_i^{-1}(1 - e^{-A_i T_s})G_i
\]
**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. 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 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 Error! Reference source not found., which states that the following two conditions must be satisfied:

1. Pair $(C, \hat{A})$ is observable;
2. Matrices $C$ and $\hat{B}$ are such that $\text{rank}(C, \hat{B}) = \text{rank}(\hat{B})$.

Through matrix analysis, it can be shown that $\hat{A}$, $\hat{B}$, and $C$ 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 $x_i = [x_i^T \xi_i^T]^T$, where $\xi_i$ is taken to be a constant output bias vector, with the following dynamics:

$$x_i^T = \begin{bmatrix} \hat{A}_i & 0 \\ 0 & 1 \end{bmatrix} x_i + \begin{bmatrix} \hat{B}_i \\ 0 \end{bmatrix} u_i + \begin{bmatrix} \bar{G}_i \\ 0 \end{bmatrix} \xi_i + \begin{bmatrix} I \\ 0 \end{bmatrix} w_i$$

$$y_i = C_i x_i + r_i$$

(22a) (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 $u_i$:

$$\dot{x}_i(k) = \hat{A}_i(k)[A_i \hat{x}_i(k-1) + G_i \xi_i(k-1)] + \hat{L}_i y_i(k)$$

$$\hat{y}_i = C_i \dot{x}_i$$

(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. $\hat{x}_i$ is an estimator of the system state. Note that the interconnection term $\xi_i$ in (22a) is replaced by the communication connection term $\xi_i^*$, 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 $\hat{A}_i$ and $\hat{L}_i$ in (23) are defined as follows:

$$\hat{L}_i(k) = K_i(k) + [I - K_i(k)C_i]BM_i(k)$$

$$\hat{A}_i(k) = [I - K_i(k)C_i][I - BM_i(k)]C_i$$

$$= I - \hat{L}_i(k)C_i$$

(24)

The estimation error is defined as $e_i = x_i - \hat{x}_i$, and the residual is given by $r_i = y_i - \hat{y}_i$. 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 Error! Reference source not found., matrices $M_i(k)$ and $K_i(k)$ guarantee that the estimation error does not depend on the switching input $u_i$. $M_i(k)$ 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 $M_i(k)$ satisfies:

$$M_i(k)C_i = I_{s_i}, \forall k \geq 0.$$  

(25)

Thus, if $M_i(k)$ and $K_i(k)$ are designed as in Error! Reference source not found., the model estimator (23) is an unbiased estimate of $x_i(k)$, minimizing the mean square error over the class of all linear unbiased estimates based on $x_i^0$ and $y_i(k), 0 \leq k \leq k$.

The dynamics of estimation error $e_i$ and residual can be derived from (22) and (23):

$$e_i(k) = \hat{A}_i(k)[A_i e_i(k-1) + G_i (\lambda_i(k-1)) + w_i(k-1)]$$

$$- \hat{L}_i(k) \rho_i(k) + r_i(k)$$

$$r_i(k) = C_i e_i(k) + \rho_i(k)$$

(26)

where $\lambda_i = \xi_i - \xi_i^*$ 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 $\Lambda_i$ is a linear combination of $R_{ij}, j \in N_i$. Hence, the estimation error and residual covariance matrices can be expressed as:

$$\Pi_i(k) = \hat{A}_i(k)\left[\Pi_i(k-1)A_i^* + G_i \Lambda_i G_i^* + W_i\right]A_i^* + L_i k R_i L_i^*$$

$$P_i(k) = C_i \Pi_i(k) C_i^* + R_i - C_i L_i(k) R_i - R_i L_i(k) C_i^*$$

(27) (28)

**C. ATTACK DETECTION STRATEGY**

From the definition of the residual and its covariance [12], 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:

$$r_i(k) = r_i^0(k) + r_i^a(k), \forall k \geq T_a$$

(29)
where $r^h$ and $r^a$ are respectively the healthy and attacked components of the residual. While the healthy portion of the residual, $r^h$, has the same definition of the residual in nominal conditions (26), $r^a$ is defined as follows:

$$ r^a(k) = C_i e^a(k) = C_i \hat{X}_i(k) G \hat{H}_i \phi_i(k-1) $$

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

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. **Reference source not found.** These algorithms exploit the stochastic properties of the residual to discriminate between the following hypotheses:

$$ H_0^0 : r = r^h $$

$$ H_1^0 : r = r^h + r^a $$

where $H_0^0$ is the null-hypothesis, i.e. the diagnostic supposes the system is not under attack. If $H_1^0$ 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

$$ T_i(r_i, k) = \sum_{k=k-W}^{k} r_i(k) P_i(k) r_i(k) > \theta_i(k) $$

holds, $H_1^1$ is thought to be active. Otherwise $H_0^0$ 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 [18] 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.

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 $r(k)$ 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.

**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 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 I.

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

![Image of three distributed ESs in a microgrid](image.png)

TABLE I

| Symbol | Quantity | Value |
|--------|----------|-------|
| $R_{L1}$ | Line12 resistance | 0.229Ω |
| $L_{L1}$ | Line12 inductance | 4.428mH |
| $R_{L2}$ | Line23 resistance | 0.229Ω |
| $L_{L2}$ | Line23 inductance | 4.426mH |
| $f_s$ | Sampling frequency | 7.5 kHz |
| $R_{mc1}$ | Noncritical load1 resistance | 39.01Ω |
| $R_{mc2}$ | Noncritical load2 resistance | 41.58Ω |
| $R_{mc3}$ | Noncritical load3 resistance | 40.39Ω |
| $L_{L1}$ | ES-1 filter inductance | 0.5mH |
| $R_{L1}$ | ES-1 filter inductor resistance | 0.926Ω |
| $C_{L1}$ | ES-1 filter capacitance | 6.6µF |
| $L_{L2}$ | ES-2 filter inductance | 0.5mH |
| $R_{L2}$ | ES-2 filter inductor resistance | 0.0926Ω |
| $C_{L2}$ | ES-2 filter capacitance | 6.6µF |
| $L_{L3}$ | ES-3 filter inductance | 0.6mH |
| $R_{L3}$ | ES-3 filter inductor resistance | 0.1Ω |
| $C_{L3}$ | 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
- $c^c$: Consensus coupling gain 0.3

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

![Image of implementation of a cyber-attack diagnoser in the ES](image.png)

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 $t=13.13s$. The attack changes the ES-2’s received data $V_{e31}$ (ES-1 voltage) to a sinusoidal signal with a constant 30V amplitude (RMS value 21.21V). The attack signal has the same phase with the real $V_{e31}$ signal in the test. Before the attack, the line voltages $V_a$, $V_b$, $V_c$ are well regulated at 110V (RMS value) and $V_{e31}=30V$(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 \( V_{e1}^d \), \( V_{e2}^d \) and \( I_T^d \) exceed the threshold and trigger the detection alarm as shown in Fig. 10(c), (d) and (e). At around \( t = 13.14s \), 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 structure 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 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. CONCLUSIONS

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.
Unbalanced Three-Phase Power Systems Using the Instantaneous Power Theory," in *IEEE Trans. on Power Electronics*, vol. 33, no. 7, pp. 5784-5795, July 2018.

[8] L. Liang, Y. Hou, D. J. Hill and S. Y. R. Hui, "Enhancing Resilience of Microgrids With Electric Springs," in *IEEE Trans. on Smart Grid*, vol. 9, no. 3, pp. 2235-2247, May 2018.

[9] E. Hassain, 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. Dörrler, J. C. Vasquez, J. M. Guerrero and F. Bullo, "Secondary Frequency and Voltage Control of Islanded Microgrids via Distributed Averaging," in *IEEE Trans. on Ind. Elec.*, vol. 62, no. 11, pp. 7025-7038, Nov. 2015.

[11] R. Olfati-Saber, J. A. Fax and R. M. Murray, "Consensus and Cooperation in Networked Multi-Agent Systems," in *Proceedings of the 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. 33, no. 4, pp. 111–116, May 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," 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSI), 2016, pp. 60-63.

[14] S. Sahoo, S. Mishra, J. C. -H. Peng and T. Dragičević, "A Stealth Cyber-Attack Detection Strategy for DC Microgrids," in *IEEE Trans. on Power Electron.*, vol. 34, no. 8, pp. 8162-8174, Aug. 2019.

[15] Y. Yang, K. McLaughlin, T. Little, S. Sezer, B. Pranggono and H. F. Wang, "Intrusion Detection System for IEC 60870-5-104 based SCADA networks," 2013 IEEE Power & Energy Society General Meeting, 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," in *IEEE Trans. on Industrial Informatics*, vol. 13, no. 2, pp. 411-423, April 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," 2019 IEEE 58th Conference on Decision and Control (CDC), 2019, pp. 5623-5628.

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

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

[20] S. Y. Hui, C. K. Lee and F. F. Wu, "Electric Springs—A New Smart Grid Technology," in *IEEE Trans. on Smart Grid*, vol. 3, no. 3, pp. 1552-1561, Sept. 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. on Smart Grid*, Vol.9, Issue 3, Pages: 1943-1951, 2018.

[22] D. Chakravorty, Z. Akhar, B. Chaudhuri; S.Y.R. Hui, “Comparison of primary frequency control using two smart load types”, IEEE Power and Energy Society General Meeting (PESGM) 2016.

## APPENDIX

\[
A_t = \begin{bmatrix}
0 & 1/C_f & 0 & 1/C_f & 0 & 1/C_f & 0 \\
\omega & -1/L_t & 0 & 0 & 0 & 0 & 0 \\
-\omega & 0 & 1/C_f & 0 & 1/C_f & 0 & 1/C_f \\
0 & 0 & -1/L_t & \alpha & 0 & 0 & 0 \\
-1/L_t & 0 & 0 & 0 & -\omega & 0 & 0 \\
0 & 0 & 0 & \omega & -1/L_t & 0 & 0 \\
0 & 0 & 0 & 0 & -1/L_t & \alpha & 0 \\
0 & 0 & 0 & 0 & 0 & -\omega & 1/L_{\alpha} \\
\end{bmatrix}
\]

\[
B_t = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1/L_t & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 \\
\end{bmatrix}
\]

\[
G_t = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 \\
\end{bmatrix}
\]