Cybersecurity Analytics using Smart Inverters in Power Distribution System: Proactive Intrusion Detection and Corrective Control Framework

Amin Y. Fard[1], *Student Member*, *IEEE*, Mitchell Easley[1], *Student Member*, *IEEE*, George T. Amariucai[2], *Member, IEEE,* Mohammad B. Shadmand[1], *Member*, *IEEE,* Haitham Abu-Rub[3], *Fellow, IEEE*

[1]Power Electronics and Autonomous Systems Research Laboratory, [1,2]Kansas State University, Manhattan, KS, USA
[3]Texas A&M University at Qatar, Doha, Qatar
mshadmand@ksu.edu

***Abstract*—Power grids with increasing number of distributed energy resources (DERs) equipped with fleet of smart devices are exposed to malicious attacks. These malicious actions can ultimately cause a large-scale blackout if these subversive activities are not prevented, detected, or promptly addressed. Power grids are being threatened by a category of cyber-physical attacks, which target both the physical and cyber layers of the system. This paper proposes an autonomous detection and corrective control framework consisting of two algorithms to identify anomalies and provide a corrective action on the distribution system using smart inverters. The proposed framework detects the inverter abnormal behaviors and identifies them as cyber-physical attack or internal failure of the inverter. A model predictive control (MPC) scheme is proposed to detect the inverter internal failure. In the case of inverter failure, the proposed MPC scheme adopts corrective actions to restore the inverter operation with a pre-defined power injection set-points. Additionally, this paper proposes a cyber-physical attack detection mechanism, based on measurements from a geographic community of smart devices. The proposed framework continuously assists the supervisory control and data acquisition (SCADA) system to differentiate anomalies on the distribution system and decide the appropriate control actions for the entire grid.**

***Keywords*—cyber-physical resiliency, cybersecurity, anomaly detection, smart inverters, model predictive control.**

I. Introduction

The resiliency of the power grid is being threatened by physical, cyber, and cyber-physical attacks. The frequency and complexity of various types of attacks on the power system are mounting [1, 2]. Severe consequences are expected on the grid operation after cyber/cyber-physical attacks like large-scale blackouts, destructive impacts on equipment, market impacts, etc., [3]. To draw a better perspective for the resiliency of the power grid against cyber/cyber-physical sabotages, U.S. Department of Energy (DOE) has published a roadmap to achieve cybersecurity of energy delivery systems in 2011 [4]. Other related studies are Critical Infrastructure Protection Standard by North American Electric Reliability Corporation [5], and Report 7628 prepared by National Institute of Standards and Technology Interagency [6].

The main reason for all the above-mentioned studies and increasing concerns about the cyber/cyber-physical security of the power system is that the traditional power system is experiencing some immense changes like integration of distributed renewable resources (DERs), employing advanced metering infrastructure (AMI) [7], emerging grid of nanogrids [8], etc.

All these changes cause the evolution of the power system from a utility-centered configuration towards a dispersed structure [9]. To enable the integration of increasing DERs, wide-area communication, monitoring, and control are essential [10, 11]. Applications of AMIs and other smart devices such as smart inverters with all their communication capabilities significantly increase the attack surface of the entire power system. Concisely, because the attack surface is being expanded by this transition toward the smarter grid, cyber-physical attack-resilient smart devices seem to be one of the main requirements of the future power systems.

Alongside all these physical, cyber, and cyber-physical threats, which wait in ambush to impose some destructive impacts into the system, ordinary failure of the smart devices (e.g., smart inverters) has high chances of occurrence. To make sure that the supervisory control and data acquisition (SCADA) system of the grid makes accurate decisions based on what is actually happening on the grid, an accurate diagnosis algorithm is needed to differentiate the potential attacks from an ordinary inverter failure. Moreover, the supervisory layer should be able to examine the trustworthiness of the propagated data from the device layer in the field. It is possible that the attacker compromises the transmitted data from the smart devices. These types of attacks are known as false data injection (FDI) [12]. If the data received by the supervisory layer has been subjected to FDI, decisions made by the SCADA would not be proper for the cyber-physical system. These improper decisions caused by FDI could have severe consequences like making the grid phases unbalanced. Ultimately, this can enable a regional blackout.

In this paper, a proactive detection framework for cyber-physical intrusions is proposed, which has the capability of adopting corrective control actions in response to anomalies on grid-interactive smart inverters. The proposed framework consists of two algorithms. The first proposed algorithm in this framework detects internal inverter anomalies, i.e. switch faults, and approximates the produced output voltage of a smart inverter based on a model predictive control (MPC) framework [13, 14]. Then, the algorithm monitors if the output voltage of the smart inverter is beyond the pre-defined boundary. In this scenario, the algorithm diagnoses and avoids the control actions to shut down the inverter, which may result in anomalies on the

978-1-7281-5092-5/19/$31.00 ©2019 IEEE

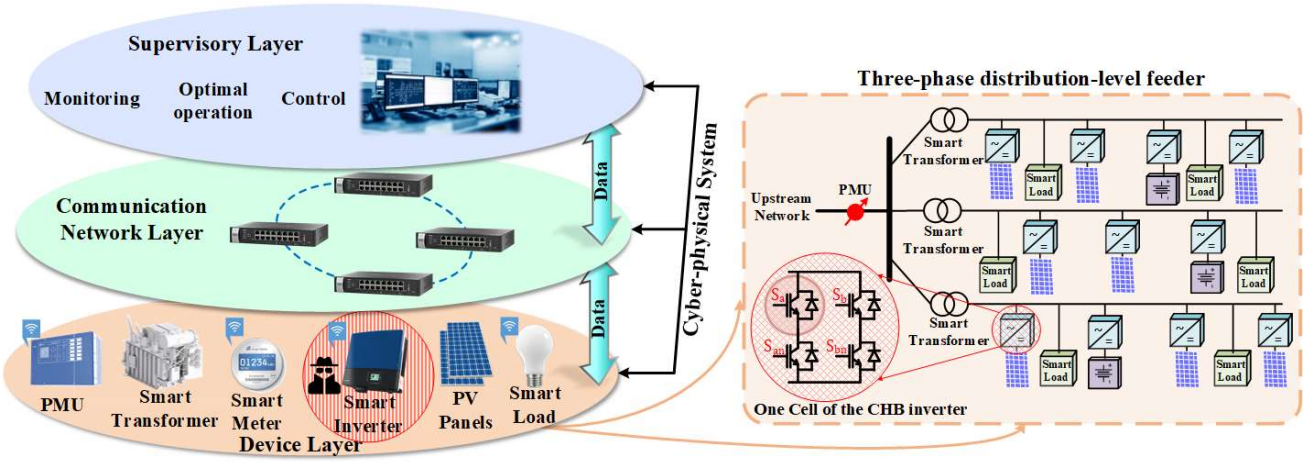

Fig. 1. Communication and control hierarchy of power grid

power distribution network. The superiority of the proposed algorithm is that the inverter internal fault boundary is defined according to the learned performance of the inverter, making it independent of the active/reactive power set-points, sampling frequency, filter size, etc. In the case of inverter failure, the proposed MPC scheme adopts corrective actions to restore the inverter operation with pre-defined power injection set-points.

The proposed framework includes a secondary anomaly detection algorithm at system level, which helps the supervisory layer to detect the cyber-physical attacks. Using this algorithm, the behavior of each smart inverter is interpretable. It means that the supervisory layer will not decide only by trusting the data coming from the inverter itself, which might be controlled by an attacker. This algorithm employs all the voltage measurements coming from smart inverters and smart meters, measurements from the nearby PMU, and switching sequences of all the nearby smart inverters to ensure on integrity of the received data from an inverter.

Considering integrated fleets of smart inverters into the grid, this differentiation feature between cyber-physical intrusion and device-level failure seems inevitable. The supervisory layer will validate the smart inverter's anomaly detection output using the proposed cyber-physical attack detection algorithm. If the output of the two algorithms do not meet on a particular inverter, then the SCADA system will label the data coming from the specific smart inverter as compromised. When the two algorithms align, it is concluded that the inverter has experienced a fault. The smart inverters have the capability to continue injecting power to the grid by eliminating the improper switching sequences. However, the injected power will be limited. The SCADA system will compensate for the reduced amount of power by adjusting the set-points of the nearby inverters, to make sure that the three-phase feeder is not going to be tripped because of an unbalance condition, which might cause problems for adjacent critical infrastructures.

Beyond the introduction, Section II discusses the cyber-physical vulnerabilities of the power grid. Section III explains the localized MPC scheme implemented by the smart inverters. Section IV explains how the smart inverters diagnose and correct anomalous behaviors that result from internal open-circuit switch failures. Section V explains the community-based cyber-physical attack detection mechanism, and Section VI concludes the paper.

II. Cyber-Physical Vulnerabilities of Power Grid

Cyber-physical attacks refer to attacks characterized by sophisticated schemes to exploit the weaknesses in the cyber-physical structure of the power grid [11]. The power grid at the distribution level will house a tremendous number of smart devices at the grid edge, as illustrated in Fig. 1. The visualized smart three-phase feeder of the future in Fig. 1 includes point of PV generation, flexible loads commonly known as smart loads, energy storage units, AMIs such as smart meters, phasor measurement units (PMUs), etc. Such devices are physically located at the grid edge, and form what is called the device layer of the grid. Ultimately, these devices communicate with the supervisory layer through an intermediate communication network layer.

The supervisory layer is responsible for acquiring and using the information provided by the smart devices for the purpose of monitoring, optimal operation, and control. Although this envisioned power grid structure is necessary due to increasing penetration of DERs to the distribution network, this structure, along with the increased communication needs, increase the vulnerability of the power grid. Attackers could manipulate one or several inverters entirely, which could mislead the supervisory layer to make improper control and operational decisions for the entire distribution network. For instance, at a three-phase residential feeder, a smart inverter sends an alarm to the upper layers claiming that it experiences difficulties injecting the referenced power into the grid due to an internal fault. This alarm could be false or true. Based on the received data from the device layer, the supervisory controller takes control actions to ensure the three-phase feeder remains balanced, for example by adjusting the power set-points of nearby DERs. If the received message from the device layer is compromised by the attacker, this results in wrong decision by the supervisory system and could cause blackouts in a grid fraction.

In another scenario, a smart meter on one of the feeders claims that the voltage is decreasing on the grid. If the supervisory layer modifies the reactive power set-points of the connected inverters into that feeder, in the case of FDI, the feeder will face unbalance conditions and it might trip entirely.

978-1-7281-5092-5/19/$31.00 ©2019 IEEE

Thus, the supervisory layer must be able to determine if the received data from the field, for instance, from smart inverters or smart meters, is authentic. Furthermore, the supervisory layer must have the capability to differentiate between the internal failures of the smart inverters versus the FDI. This paper proposes a framework that integrates device level and system level analytics to enhance the attack resiliency of power grid by providing two mechanisms for the supervisory layer: a) determination of the inverter internal anomaly, and b) validation of the propagated anomaly signal from the smart devices.

III. Localized Control Scheme

The smart inverters implement a cascaded H-bridge (CHB) topology, as the additional H-bridges allow the inverter to retain operation in the event of open circuit switch faults. Fig. 2 describes the CHB inverter topology and summarizes the localized control. A second order generalized integrator (SOGI) phase locked loop (PLL) detects the grid voltage angle [15]. This PLL is used for its inherent capability to filter grid voltage harmonics, allowing the reference current to be robust to distorted grid conditions. The reference current is assembled in the rotating reference (*dq*) frame, which is then converted to the reference grid current in stationary frame. Converting to the *dq* frame is made possible by the orthogonal signal generation capability of SOGI, where the original and quadrature signals are inputs to the Park transformation. The reference current is determined using equations for single-phase active and reactive power in the *dq* frame,

$$P_k^* = \frac{1}{2}\left(v_{d,k} i_{d,k}^* + v_{q,k} i_{q,k}^*\right) \quad Q_k^* = \frac{1}{2}\left(v_{q,k} i_{d,k}^* - v_{d,k} i_{q,k}^*\right) \tag{1}$$

P^*_k and Q^*_k are the active/reactive power set-points determined by the supervisory system. The subscript k indicates a discrete sampling instant. $v_{d,k}$ and $v_{q,k}$ are the grid's components in the rotating reference frame, and $i^*_{d,k}$ and $i^*_{q,k}$ are decoupled components of the reference current to be solved. This equation is rearranged to calculate the reference current components in the *dq* frame, and then converted to the original time-variant frame using the inverse Park equation.

$$i_{d,k}^* = \frac{2\left(P_k^* v_{d,k} + Q_k^* v_{q,k}\right)}{{v_{d,k}}^2 + {v_{q,k}}^2} \quad i_{q,k}^* = \frac{2\left(P_k^* v_{q,k} - Q_k^* v_{d,k}\right)}{{v_{d,k}}^2 + {v_{q,k}}^2} \tag{2}$$

$$i_k^* = i_{d,k}^* \sin(\theta_k) + i_{q,k}^* \cos(\theta_k) \tag{3}$$

where θ_k is the grid angle detected by the PLL and i^*_k is the time-variant reference current. For current control, the finite-set MPC evaluates each of the switching sequences, or switching states, and compares it to the reference. The output current predictions derive from the AC-side KVL equation,

$$v_{inv} = r(i) + L\frac{di}{dt} + v_g \tag{4}$$

where L and r are the filter inductance and equivalent series resistance, respectively. v_g and v_{inv} are the grid and inverter voltages, respectively. This equation is discretized by approximating the differential using forward Euler, and is rearranged to create an explicit solution for the one-step ahead prediction of the output current,

$$i_{g,k+1}^M = \left(1 - r(L)^{-1} T_S\right) i_{g,k} + T_s (L)^{-1}\left(v_{inv,k+1}^M - v_{g,k}\right) \tag{5}$$
$$M \in \mathbb{Z} : M \in [-3 \;\; 3]$$

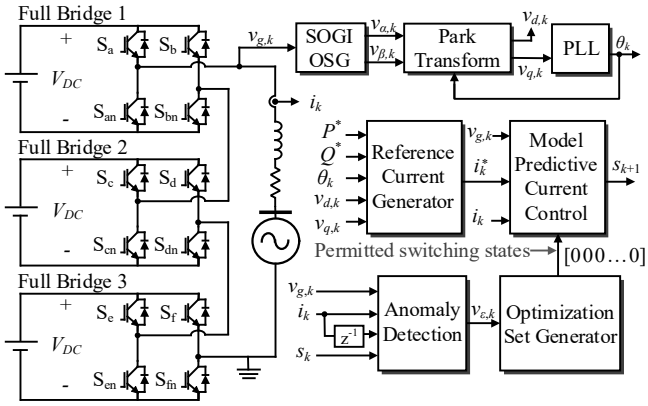

Fig. 2. DER inverter and localized control scheme.

where M is the output voltage level, which is dependent on the gate signals as:

$$M = \sum_{i=a,c,e} S_{i,k} - \sum_{j=b,d,f} S_{j,k} \tag{6}$$

Each switch value is either one (transistor gate logic-high) or zero (transistor gate logic-low). The cost vector J which is subject to minimization is defined as,

$$J = \left| i_k^* - i_{k+1}^M[s] \right| \quad \forall s \text{ s.t. } States[s] = 0 \tag{7}$$

where s is a variable which indexes a specific sequence of gate signals. Note that the next-state predictions are dependent on the voltage level M, while the cost vector is dependent on the switching state s. This is done to exclude switching states according to the diagnosis algorithm, which marks prohibited switching states with a value of one in its respective *States* column. This is described in more detail in the next section. The next-state current prediction vector is indexed according to the voltage level, rather than the switching state, to reduce the size of the vector from 4^C to $2C+1$, where C is the number of H-bridges in the CHB inverter.

IV. Self-Learned Diagnosis Algorithm for Inverter Internal Anomaly

A. Diagnosis Algorithm via Model Predictive Control

Faulty switches are detected by discretizing (4),

$$v_{inv,k} = r(i_k) + v_{g,k} + L(T_s)^{-1}\left(i_k - i_{k-1}\right) + v_{\varepsilon,k} \tag{8}$$

There is a new term, $v_{\varepsilon,k}$, which is the computed error in the Kirchhoff voltage law equation. In healthy inverter operation, $v_{\varepsilon,k}$ is nonzero but small, due to error in the discretized differential term and potential misalignment between the output filter and the model. The $v_{inv,k}$ is the anticipated inverter output voltage, computed using the measured DC link voltages and selected switching state. If a substantial $v_{\varepsilon,k}$ is computed, it is attributed to a substantial difference between the anticipated output voltage and the produced output voltage. This can occur during an open-circuit switch-fault when the faulty switch receives a logic-high signal, as this leaves its output node floating; if the faulty switch receives a logic-low signal, the output voltage is unaffected, since the output node can still clamp to a DC link node from the other switch in the leg. The computed $|v_{\varepsilon,k}|$ is compared to an error threshold, called V_{th}, which is used to test for anomalous behavior in the inverter. V_{th} is adaptive, and its formulation is explained later in the section.

For every switching state, half of the insulated gate bipolar transistors (IGBTs) receive a logic-high signal. To fairly

978-1-7281-5092-5/19/$31.00 ©2019 IEEE

associate anomalous behavior with a particular switch, all possible switching states are tested, and the diagnosis algorithm seeks out a *common denominator switch*. The diagnosis algorithm is explained in Fig. 3, and each of the variables used in the algorithm are defined in Table I. As mentioned in the previous section, output current only depends on the output voltage level, of which there are seven. Meanwhile, there are sixty-four possible switching states. Thus, during the diagnosis algorithm, the predictive controller picks an optimal voltage level, and then will skip over previously tested switching states within the optimal output voltage level. This ensures all switching states are able to be tested, while still adhering to the current control. During testing, if anomalous behavior is noted, it is recorded in the *AnomalyStates* vector, which has a column for each switching sequence. Once all sequences have been tested, *GateSignals* is multiplied by the transpose of *AnomalyStates*. Now, each column of the resultant vector is associated with a switch, and the number contained in the column is equal to the number of times the associated switch received a logic-high and anomalous behavior was detected in the next discrete instant. If a column holds thirty-two (half of the total switching states), it means anomalous behavior was detected each time the respective switch was on, and thus an anomaly was detected independent of the other switches' gate signals. It can be deduced that the switch is faulty.

The controller responds to this deduction by reducing the optimization set such that the faulty switch is never sent a logic-high signal. This will eliminate either three or negative three as

TABLE I. VARIABLES USED IN DIAGNOSIS ALGORITHM

Variable	Description
$Faults_{1x12}$	A Boolean array where each column indicates the fault-status of an particular switch. Column one relates to S_a, column two with S_{an}, column three with S_b, etc. A value of one in the column indicates that the associated switch is faulty.
$Detection_{1x1}$	A flag indicating that the diagnosis algorithm is running
$TestedStates_{1x64}$	A Boolean array which indicates with a value of one if its respective switching state has been tested during the diagnosis algorithm.
$AnomalyStates_{1x64}$	A Boolean array which indicates with a value of one if an anomaly was detected when its respective switching state was on.
$AnomalyCount_{1x12}$	An array in which each column is respective of an inverter switch (similar to the *Faults* array). The number in each column represents the total number of anomalies that were detected after the associated switch received a logic-high gate signal.
$GateSignals_{12x64}$	A Boolean matrix where each column is associated with a unique switching sequence and each row is associated with a switch. Row one is associated with S_a, row two with S_{an}, etc. A value of one indicates the associated switch receives a logic-high gate signal for the associated switching sequence; similarly, a value of zero indicates the switch is off.
$States_{1x64}$	A Boolean array that determines which switching states are to be considered by the cost optimizer, where each switching state has an associated column. The MPC will ignore a switching state which contains a value of one in its associated states column.

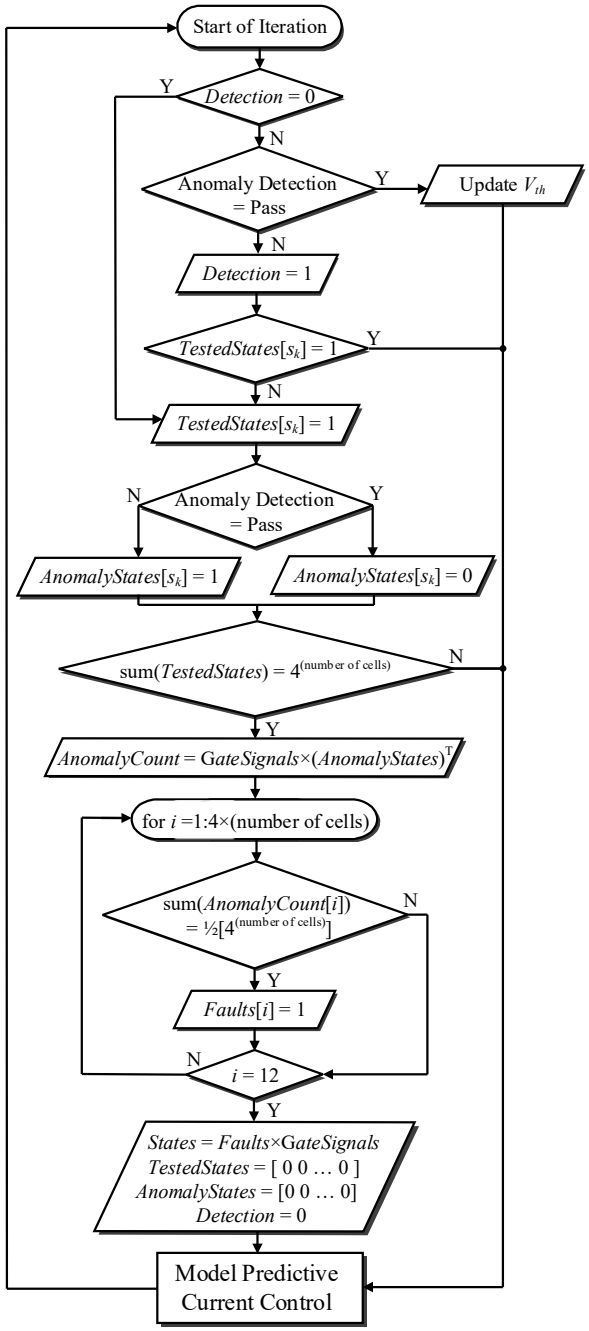

Fig. 3. Fault detection and diagnosis algorithm, variables in this flowchart are defined in Table I.

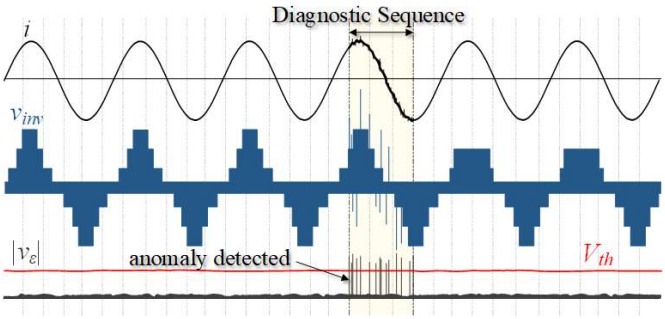

Fig. 4. Concept of localized fault detection and diagnosis.

a possible value for M, depending on which leg the switch-fault occurred. Here, it should be noted that the value of V_{th} is critical, and a hard-programmed value could result in the algorithm failing. An example of the algorithm is demonstrated in Fig. 4.

B. Self-Learning Approach for Adaptive Anomaly Detection

The behavior of $|v_{\varepsilon,k}|$ is likely to vary for each inverter, according to its sampling frequency, active/reactive power set points, filter size, etc. Thus, the V_{th} should be unique for each inverter, and decided based on the learned performance of its respective inverter. This is achieved by storing sufficient $|v_\varepsilon|$ computations (e.g. one second). Each measurement is stored in a vector, and the vector is updated as a ring buffer to retain computational efficiency. The average $|v_{\varepsilon,k}|$ at instant k is based on the $|v_\varepsilon|$ data stored in the vector. To avoid re-summation of all components, the average is updated by subtracting the outgoing datum and adding the incoming datum as follows:

$$\mu_{\varepsilon,k} = \mu_{\varepsilon,k-1} + \frac{|v_{\varepsilon,k}|}{N} - \frac{|v_{\varepsilon,k-N+1}|}{N} \tag{9}$$

where $\mu_{\varepsilon,k}$ is the updated mean and N is the vector length. The standard deviation of the data can also be updated efficiently, by first updating the sum-squared difference between the data and computed mean, as follows:

$$\begin{aligned}\psi_k &= \sum_{i=0}^{N-1}\left[\left|v_{\varepsilon,k-i}\right| - \mu_{\varepsilon,k}\right]^2 \\ &= \psi_{k-1} + \left(\left|v_{\varepsilon,k}\right| - \mu_{\varepsilon,k-1}\right)\left(\left|v_{\varepsilon,k}\right| - \mu_{\varepsilon,k}\right) \\ &\quad - \left(\left|v_{\varepsilon,k-N+1}\right| - \mu_{\varepsilon,k-1}\right)\left(\left|v_{\varepsilon,k-N+1}\right| - \mu_{\varepsilon,k}\right)\end{aligned} \tag{10}$$

where ψ_k is the sum-squared difference from the computed mean. This computationally efficient equation, similar to the moving average, only requires the incoming and outgoing $|v_\varepsilon|$ measurements. The subtracted product in (9) is a modification of the Welford's algorithm for rolling variance [16], allowing the sum-squared difference to apply only to the $|v_\varepsilon|$ measurements in the vector. Thus, we are able to update the standard deviation of the vector:

$$\sigma_k = \sqrt{\frac{\psi_k}{N-1}} \tag{11}$$

The updated mean and standard deviation are used to define anomalous behavior by updating V_{th} for each iteration:

$$V_{th} = \mu_{\varepsilon,k} + 5\sigma_{\varepsilon,k} \tag{12}$$

Five standard deviations from the computed average is considered anomalous. Thus, the anomaly detection is performance-based and unique to each inverter. Upon detection of an anomaly and initiation of the diagnosis sequence, the collection of $|v_\varepsilon|$ computations and updates to V_{th} is halted, so the abnormal measurements anticipated during the diagnosis algorithm do not substantially perturb or desensitize the anomaly detection.

V. Cyber-Physical Attack Detection Algorithm

So far, we have discussed the identification and management of flaws inside a smart inverter, with no consideration for cyber-physical attacks. Under our attack model, the attacker might have whole access to one or multiple smart inverters. This means that the smart inverters receive their respective P^*_k and Q^*_k commands from the supervisory layer, but rather than choosing their switching sequences to satisfy these commands, they may misbehave by choosing some random, or optimally derived (to maximize impact) switching sequences, but without reporting any failures. An attacker may also misbehave by following the prescribed sequences, but informing the supervisory layer that they used a different, incorrect switching sequence (perhaps motivated by a false internal failure), or they can simply report the wrong voltage measurements.

Naturally, other well-behaved smart inverters will do their best to achieve their specified P^*_k and Q^*_k values, despite the possible discrepancies in the expected (here, "expected" refers to the point of view of the supervisory layer– the smart inverters do not know any better) grid voltage values at these inverters. Some may succeed, some not. If some inverters are unsuccessful in injecting their specified powers into the grid, they inject the maximum possible power, and report to the supervisory layer that they altered their settings from the prescribed ones.

In any case, at time k, the supervisory layer has the following information: (a) the vector v_g of measured voltages at all smart inverters and smart meters in the neighborhood, (b) complete measurements from the PMU installed on the bus serving the neighborhood – we denote the voltage from the PMU by v_0 and include it in the voltage vector: $\boldsymbol{v}=[\boldsymbol{v_g}^T v_0]^{\mathbf{T}}$ and (c) the switching sequences used by all smart inverters, as well as the current measurements from all smart meters at time *k-1*. From the switching sequences, the supervisory layer can calculate the injected currents, form the load/generator current vector $\boldsymbol{i}$ (including the current $\boldsymbol{i_0}$ determined by the PMU at the feeder) and further calculate the currents $\boldsymbol{i_l}$ on the lines between the loads/generators as $\boldsymbol{i_l = A\, i}$.

Now, since the scale of a neighborhood is well below the wavelength, we can write a set of node voltage equations as $\boldsymbol{Bv = Ci_l}$, or for simplicity:

$$\begin{bmatrix}\boldsymbol{B} & \boldsymbol{CA}\end{bmatrix}\begin{bmatrix}\boldsymbol{v} \\ \boldsymbol{i}\end{bmatrix} = 0 \tag{13}$$

where the matrix on the left has full row rank, but not full rank. When one or multiple smart inverters are misbehaving, the injected currents do not follow the prescribed sequences (or the sequences reported back to the central controller, if the reporting occurs). This is reflected in the voltage values at the next step. Indeed, the misbehaving inverters either may communicate the correct values of the measured voltages, or may report incorrect values. This translates into having one or multiple errors in the vector $[\boldsymbol{v}\ \boldsymbol{i}]^T$, and a non-zero value on the right-hand side of (13) which we can write as:

$$\begin{bmatrix}\boldsymbol{B} & \boldsymbol{CA}\end{bmatrix}\begin{bmatrix}\boldsymbol{v'} \\ \boldsymbol{i'}\end{bmatrix} = \boldsymbol{d} \tag{14}$$

or equivalently, denoting $\boldsymbol{d_v} = \boldsymbol{v'-v}$ and $\boldsymbol{d_i} = \boldsymbol{i'- i}$,

$$\begin{bmatrix} \boldsymbol{B} & \boldsymbol{CA} \end{bmatrix} \begin{bmatrix} \boldsymbol{d}_v \\ \boldsymbol{d}_i \end{bmatrix} = \boldsymbol{d} \tag{15}$$

Two assumptions are required at this point. First, we assume that the deviation vector $[\boldsymbol{d}_v^T \boldsymbol{d}_i^T]^T$ is sparse, i.e. that among the many smart inverters in the neighborhood, relatively few are misbehaving. Second, we assume that secure channels (authenticated encryption) protect the communications between all smart inverters and smart meters, so the misbehaving inverters cannot guess the current and voltage values observed at the other inverters, or at the PMU, and neither can they modify the data transmitted from the other, well-behaved inverters and meters. Along with the first assumption, this implies that in general, the misbehaving inverters cannot produce deviation vectors that are located in the kernel of the matrix $[\boldsymbol{B} \quad \boldsymbol{CA}]$, thus they cannot avoid detection.

Based on the sparsity assumption, once the supervisory controller notices a discrepancy between the expected and reported grid status (i.e. $\boldsymbol{d} \neq \boldsymbol{0}$), the deviation vector $[\boldsymbol{d}_v^T \boldsymbol{d}_i^T]^T$ is computed as the most sparse solution of the under-determined system in (15). Similar to [17], we choose to address the problem by using a version of the orthogonal matching pursuit (OMP) algorithm of [18]. An interesting consequence of this approach is that it can handle scenarios in which some of the generator/load voltages and currents are unknown – these are simply replaced with randomly chosen or estimated values, and the sparse solution provided by the OMP algorithm is constrained to contain the indices of these voltages and currents in its support – in essence, the OMP algorithm is artificially started with the columns of $[\boldsymbol{B} \quad \boldsymbol{CA}]$ that correspond to the unknown quantities.

Once a feasible solution has been identified, a diagnosis command is sent to the identified misbehaving inverters. The purpose of this procedure is to enable the inverters to auto-correct their set-point power operation, in the event that their misbehavior is due to faulty functionality, rather than malicious attack.

VI. Conclusion

The supervisory layer in power grid needs to differentiate between cyber-physical attacks and device internal failures. Device internal failure is a common incident, which depends on operating situation, lifespan, etc. Moreover, by growing the number of smart devices on the grid, the frequency of these failures will increase as well. On the other hand, malicious attacks on the grid are mounting steadily, becoming more complicated.

The proposed framework includes two layers of anomaly detection algorithms to assist the supervisory layer of the grid in this regard. The first layer of the algorithm is considered as a local controller for the smart inverters. The localized control scheme investigates if all the switching sequences are achievable or not. In the case of switch failure, the algorithm will detect the failed switch and will eliminate all the switching sequences which activate the failed switch. Then, specific control actions will be adopted to continue power injection, although the power injection capability will be limited. All this data is transmitted to the supervisory layer. The supervisory layer must be able to determine that the received data from a specific inverter is trustworthy or an attacker is controlling the inverter. The second layer of the proposed framework assists the SCADA system located at supervisory layer to evaluate the integrity of the data received. If the cyber-physical attack detection algorithm approves the integrity of the received data, the SCADA system will decide on a healing action for distribution system based on it, otherwise, the data coming from that specific device will be labeled as malicious and this data will not play a role in the supervisory layer's decision-making process. The proposed framework helps the supervisory layer of the grid to make accurate decisions based on what is really happening on the cyber-physical system.

References

[1] T. A. Johnson, *Cybersecurity: Protecting critical infrastructures from cyber attack and cyber warfare*. CRC Press, 2015.

[2] "*Cyber Attack Task Force*," North American Electric Reliability Corporation, Report. May 9, 2012.

[3] J. Qi, S. Mei, and F. Liu, "Blackout Model Considering Slow Process," *IEEE Trans. Power Systems,* vol. 28, no. 3, pp. 3274-3282, 2013.

[4] D. Batz and e. al., "Roadmap to Achieve Energy Delivery Systems Cybersecurity," U.S. Department of Energy, September 2011.

[5] "Critical Infrastructure Protection (CIP) Standards," North American Electric Reliability Corporation (NERC), 2015, [Online]. Available: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

[6] "Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements," National Institute of Standards and Technology, vol. 1.

[7] F. M. Cleveland, "Cyber security issues for Advanced Metering Infrasttructure (AMI)," in *IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, 2008, pp. 1-5.

[8] M. S. Pilehvar, M. B. Shadmand, and B. Mirafzal, "Analysis of Smart Loads in Nanogrids," *IEEE Access,* vol. 7, pp. 548-562, 2019.

[9] J. Taft and A. Becker-dippmann, "Grid Artitecture," Pacific Northwest National Laboratory, January 2015.

[10] J. Qi, A. Hahn, X. Lu, J. Wang, and C. Liu, "Cybersecurity for distributed energy resources and smart inverters," *IET Cyber-Phys. Syst., Theory Appl.,* vol. 1, no. 1, pp. 28-39, 2016.

[11] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid," *Proceedings of the IEEE,* vol. 105, no. 7, pp. 1389-1407, 2017.

[12] 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, 2017.

[13] M. Easley, S. Jain, M. B. Shadmand, F. Fateh, and B. Mirafzal, "Hierarchical Model Predictive Control for Cascaded Multilevel Inverters," in *IEEE Applied Power Electronics Conference and Exposition (APEC)*, 2019, pp. 614-619.

[14] M. Easley, A. Y. Fard, F. Fateh, M. B. Shadmand, and H. Abu-Rub, "Auto-tuned Model Parameters in Predictive Control of Power Electronics Converters," in *IEEE Energy Conversion Congress and Exposition (ECCE)*, 2019.

[15] M. Ciobotaru, R. Teodorescu, and F. Blaabjerg, "A new single-phase PLL structure based on second order generalized integrator," in *37th IEEE Power Electronics Specialists Conference*, 2006, pp. 1-6.

[16] B. Welford, "Note on a method for calculating corrected sums of squares and products," *Technometrics,* vol. 4, no. 3, pp. 419-420, 1962.

[17] H. Zhu and G. B. Giannakis, "Sparse Overcomplete Representations for Efficient Identification of Power Line Outages," *IEEE Trans. Power Systems,* vol. 27, no. 4, pp. 2215-2224, 2012.

[18] T. T. Cai and L. Wang, "Orthogonal Matching Pursuit for Sparse Signal Recovery With Noise," *IEEE Trans. Inform. Theory,* vol. 57, no. 7, pp. 4680-4688, 2011.

978-1-7281-5092-5/19/$31.00 ©2019 IEEE