IET Cyber-Physical Systems: Theory & Applications

Research Article

Mitigating zero dynamic attack in communication link-enabled droop-controlled hybrid AC/DC microgrids

ISSN 2398-3396
Received on 25th June 2019
Revised 13th November 2019
Accepted on 11th February 2020
E-First on 4th March 2020
doi: 10.1049/iet-cps.2019.0043
www.ietdl.org

Arsalan Rasoolzadeh[1] ✉, *Farzad Rajaei Salmasi*[1]

[1]*Electrical and Computer Engineering Department, University of Tehran, Tehran, Iran*

✉ *E-mail: a.rasoolzadeh@ut.ac.ir*

Abstract: This article focuses on mitigation of zero dynamic attack in communication link-enabled droop-controlled hybrid AC/DC microgrids (MGs). To transmit setpoints for droop controllers and to also send measured AC and DC voltages and AC frequency in this sort of MGs, a communication link is required. Such links are exposed to cyber-attacks. First of all, this article tries to indicate that the system would be vulnerable to zero dynamic attack. In the second step, it is shown that zero dynamic attack can be mitigated by closing the secondary control loop. It is also shown that the attack can be distinguished from load/generation disturbances. In order to proceed with the challenge, the control signal in a closed loop system is used as the tricks of the trade. To achieve the goal, parity space as a kind of model-based fault detection approach is applied to a recently proposed dynamic model for droop-controlled hybrid AC/DC MGs. Evaluation of the detecting approach confirms that not only it can detect the attack effectively, but also it distinguishes from disturbance perfectly.

Nomenclature

v_{ac}	AC sub-MG rms phase voltage
f	AC sub-MG frequency
v_{dc}	DC sub-MG voltage
$v_{ref,ac}$	reference of RMS phase voltage for AC sub-MGs
f_{ref}	frequency reference of AC sub-MGs
$v_{ref,dc}$	voltage reference of DC sub-MGs
v_i	state variables of AC MG which are voltages of converters
$\hat{i}_i^*$	state variables of AC MG which are current reference of converters
δ_i	phase angle of voltage of converters with reference of AC link voltage
P_{ex}	exchanging power between the AC and DC networks from DC side to AC side
$i_{o,i,dc}$	state variables of DC MG system which are output currents of converters
P_{ex}^*	reference of exchanging power between the AC and DC networks from DC side to AC side
P_{load}	active power of AC loads
Q_{load}	reactive power of AC loads
I_{load}	current of constant current AC loads
$\theta_{I,load}$	phase angle of constant current AC loads
Z_{load}	impedance of constant impedance AC loads
$\theta_{z,load}$	phase angle of constant impedance AC loads
$\hat{P}_{dc}$	equivalent DC load disturbance
^	small signal sign for variables, inputs, outputs and disturbances
-	steady state sign for variables, inputs, outputs and disturbances

1 Introduction

1.1 Motivation and incitement

Given the growing trend in the usage of both AC and DC distributed resources (DRs) as well as AC/DC consumers, the applications of hybrid microgrids (MGs) have been increased in recent times. DC power consumers are increased in the last decade, because most of the home electrical loads such as LED lights, variable-speed motors, computers, televisions and many other electronic devices consume DC power indeed. Due to this fact, these consumers can use DC power directly instead of converting AC power by using AC/DC converters [1]. Nowadays, thanks to advances in power electronics technology, two independent AC and DC MGs can merge into an integrated hybrid MG. Hybrid MGs eliminate most of the transmission and distribution losses, due to which they avoid the waste of energy concerned with the conversion of AC to DC [2].

Although a hybrid MG possesses the abovementioned advantages, its control complexity leads to some challenges. Utilising hierarchal control in three different levels, such MGs need telecommunication networks to complete control goal [3]. However, insecurity of these telecommunication networks brings about vulnerability of MGs to cyber-attack. Regarding this, cyber-attacks may cause horrible damages to MGs; the concept of cyber-attack detection has been raised as a vitally important issue in recent times. After the happening of Stuxnet attack, the issue has been taken more seriously such that Industrial Cyber Security (ICS) has dramatically attracted control engineers' attention [4]. Consequences of cyber-attacks on SCADA control systems are analysed in [5]. As it is concluded in that article, to have a reliable network, a secure communication is necessary.

There is quite a mixed variety of cyber-attacks intruding into cyber physical systems (CPSs). One of the major categorisations of cyber-attacks is based on the type of cyber security goal which is aimed by the intruder. There are three main goals in cyber security of networks: availability, confidentiality and integrity [6], due to which attacks are classified into three types. Availability is the transmission of data without any interruption, while confidentiality means that private data should not be exposed by strangers. Integrity as the especial goal of this study is transmitting data accurately and without any distortion. According to this classification, cyber-attacks are classified into three main types. The attacks which disturb the availability of data are called denial of service, while the ones which compromise confidentiality are named eavesdropping attacks. The attacks which are more focused on in this article are the ones which disturb the integrity and deviate the values of data. This class of attack is called false data injection attack (FDIA).

FDIAs have some information about the system. Using this information, they can be designed such that remain covert and stealth. Zero dynamic attack can be regarded as a kind of FDIA. Based on zero dynamics of system, there exist some input vectors with specific initial conditions for a system dynamic which have no

influence on observed outputs. This blind spot can be abused by a malicious intruder to manipulate the system.

As it is mentioned in the previous paragraph, zero dynamic attacks need some information about the system. This information includes system model which is derived in our latest studies [7, 8]. In these studies, it is demonstrated that in order to compensate voltage and frequency deviations in communication link-enabled droop-controlled MGs, a supervisory control should be used. In the supervisory control, the revised setpoints of AC and DC voltages and frequency are transmitted from central power management and control unit (PMCU) to each DR. This transmitted data can be distorted by a malicious user in cyber network. Regarding the fact that variables of droop-controlled MGs have always some deviations from their setpoints, detection of deviations' origin is not obvious. The deviation origin may be either droop control characteristics or a cyber-attack. Although thanks to perfect unknown input decoupling (PUID) observers, detection of simple attack – a bias on the setpoint values is possible; detection of zero dynamic attacks is by no means plain sailing. To address this challenge, this paper proposes an approach by which zero dynamic attack is mitigated firstly. Tricks of the trade include but not limited to closing the secondary control loop and observing the control signals. In the second step, by having a mitigated attack a model-based fault detection PUID observer called parity space is utilised for detection purpose.

1.2 Literature review

1.2.1 Cyber-attack in cyber physical systems (CPSs): This subsection contains a brief literature review on cyber-attack detection in CPSs. There is a survey on the security of CPS in [9]. This article consists of three parts: attack detection, attack design and secure estimation and control.

In [10], a very simple detection method is introduced by the author. An intelligent checker sends alarm, once the values get out of their normal interval. As a drawback, it is mentioned in the article that this approach is neither robust to noise nor to sensor failure. Hence it is not complete and prefect.

A review on attack detection and identification in CPSs has been conducted in [11]. In this important article, four kinds of FDIAs are mentioned: static stealth attack, replay attack, covert attack and dynamic false data injection. The effect of these attacks cannot be seen in the outputs of system and zero dynamic attacks can be categorised as dynamic false data injection type.

Authors in [12] enumerate the conditions of feasibility of the replay attack; then it suggests countermeasures that optimise the probability of detection. These countermeasures consist of using unstable dynamic and also applying noisy control via χ^2 detector as well as utilising noisy control via a cross correlator. Authors in [13], instead, have used a spectral estimation approach to detect replay attack in a special type of networked control system involving additive white Gaussian noise channels. Furthermore, there are also some methods which are based on game theory. For instance, a control approach is introduced in [14] which makes an optimal decision between perfect control law and secure control law based on game theory. Secure control law is sensitive to replay attack so that it can detect the attack using χ^2 detector.

A false data injection algorithm is introduced in [15]. This algorithm is based on minimising of the attack influence on Kalman filter state estimation error. The minimisation uses ellipsoidal approximation to compute the inner and outer approximations for the reachable region of the constrained control problem.

Authors in [16] introduce an uncertain descriptor system to detect fault and attack. Then, the authors in [17] introduced a cyber-attack which could influence the electric power market price. There is a signal-based algorithm which can detect integrity attacks using an optimal detector in [18]. Author in [19] has used an ensemble modelling using finite impulse response models and neural network to estimate states in CPSs. Integrity attack can be detected using measurements and estimations.

1.2.2 Cyber-attacks in AC conventional networks: AC electrical power grids as kinds of CPSs are discussed in this subsection. In [20], actuator attacks in AC power systems are detected using a fault detection and isolation approach called generalised observer scheme. It is shown in this article that if the control loop is closed over a communication network, only the compromised node itself can distinguish the nature of the attack. However as a precaution approach, in [21] a method is introduced which can reduce the probability of smart attacks in AC power systems. The AC power system is modelled by algebraic equations of power flow-bus voltage angle. The approach defines a minimum set of nodes that should be protected by a phasor measurement unit (PMU) to block smart attack. PMU can measure the bus voltage angle without any estimation using GPS synchronisation. FDIA in AC power grids are discussed in [22, 23]. It has used principal component analysis to detect the attack. The analysis is based on off-the-shelf convex optimisation algorithms and Lagrangian function. There is an introduction and implementation of security-oriented cyber-physical state estimation for power grid in [24]. This approach consists of three layers of attack detection: inputs layer, offline processing layer and state estimation layer which is online. The state estimation attack detection layer is based on residual generation of power flow-bus voltage angle algebraic equations. There are also other studies on static stealth attack on AC power systems in [25–32]. It is remarkable that none of the mentioned studies has analysed zero dynamic attack in AC power grids [21, 26–32].

1.2.3 Cyber-attack in DC microgrids: DC MG as another kind of CPS is discussed in this subsection. There are some sorts of approaches which address the problem in this system. For instance, a model-based failure detection method in smart grids is discussed based on Petri-net modelling in [33]. The same method can be used in cyber-attack detection. In [34], an approach is introduced to detect FDIA in cyber physical DC MGs. The detection problem is formalised such that an identifier detects changes in the set of inferred candidate invariants. Invariants are properties of MGs that do not change over time. Authors in [35] have presented a signal temporal logic detection approach, which monitors the output voltages and currents against the defined specifications such as operation bounds and over time. There is also a model-based fault detection approach in [36] to detect cyber-attack in the secondary control of DC MGs. The load sharing in the model is based on a master–slave control approach. Authors in [37] have presented a cyber-physical model for a DC MG which is based on average voltage regulation and current sharing. A stealth attack is represented which cannot be observed by regular observers. Then, a cooperative vulnerability factor is defined for each agent by which the attacked nodes can be determined. Similar to AC grids, zero dynamic attack is not analysed in DC MGs too.

1.2.4 Zero dynamic attack detection: As it was discussed in previous subsections, detection of zero dynamic attacks is by no means plain sailing. According to [38], to detect zero dynamic attack, not only we need to have a side information matrix $\Omega \in \mathbb{R}^{q\times n}$ but also this matrix should be full rank. The matrix Ω having full column rank corresponds to the case in which y_Ω gives complete information about $x(0)$. The side information y_Ω captures information about the initial state $x(0)$ from the physical description of the system. The side information y_Ω does not rely on sensor measurements. For this reason, the attacker cannot modify the side information y_Ω. Having used Ω and y_Ω, the authors designed an observer which can detect zero dynamic attack if $\Omega \in \mathbb{R}^{q\times n}$ is full column rank. To have a full column rank Ω, the number of outputs should be more than the number of states, which would be a difficult condition.

However as a preventing approach, authors of [39] have used a scaling matrix in the inputs to change the dynamics of system. The attacker is not able to excite the zero dynamics without knowing the scaling matrix. However, if the new information is achieved by attackers, they can implement their malicious intrusion. Due to this fact, the scaling factor should be changed periodically.

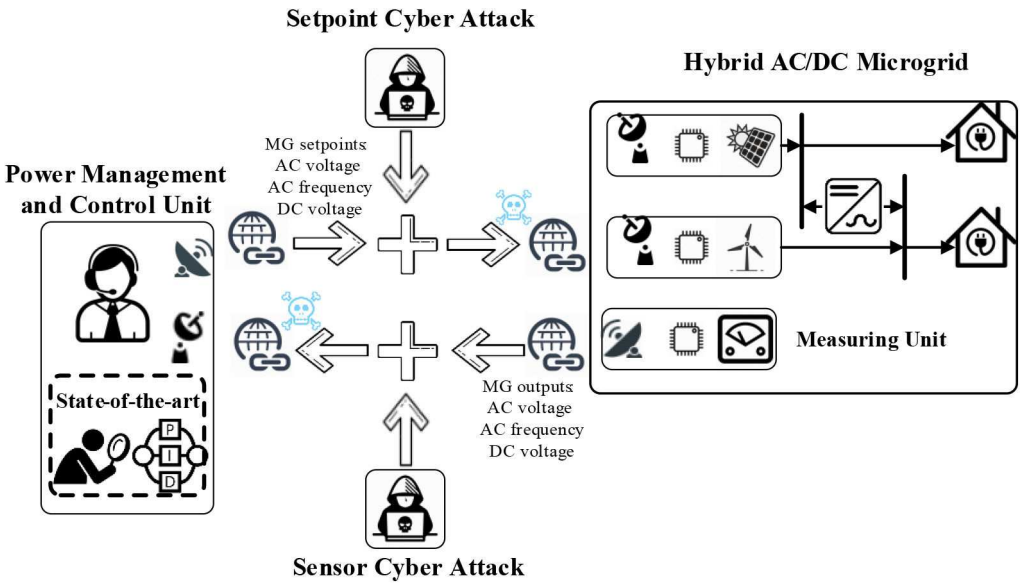

Fig. 1 *Location of possible cyber-attacks in a communication link-enabled droop-controlled hybrid AC/DC MG*

1.3 Motivation

None of these approaches is applicable for our case study because of the following reasons.

Although some approaches have recently been proposed to detect zero dynamic attack in CPSs, none of these studies can be applicable for the case of droop-controlled hybrid AC/DC MGs. Since the side information-based approach in [38] needs the number of outputs to be larger than or equal to states, it cannot be used for this special system. This is due to the fact that our derived model in [7, 8] would have at most one-half of the number of state variables as the outputs (which are all the physical states). Also, since the scaling matrix-based approach in [39] can be discovered by comparing the measured value and transferred data, the attacker can find the scaling factor and the new zero dynamic easily.

1.4 Contribution

Here, it is tried to propose a customised approach for communication link-enabled droop-controlled hybrid AC/DC MGs, which is novel, applicable and with much less complexities to implement. Also, it needs no supplementary infrastructures for implementation i.e. the algorithm can be implemented in the PMCU computer without any need for extra data transfer, thanks to information gained by the control signal of secondary loop.

1.5 Main findings

To the best of our knowledge, this is the first practical approach which can be used for this sort of MG to mitigate zero dynamic attack and detect the mitigated attack.

1.6 Paper organisation

Section 2 states the problem. Section 3 of this article, however, has used our previously derived dynamic model of a hybrid MG to model cyber-attack on setpoints and sensors. Section 4 tries to design zero dynamic attacks which cannot be revealed by regular detectors. In Section 5, it is shown that the zero dynamic attack can be mitigated by closing secondary control loop and utilising control signals. The parity method as a kind of model-based fault detection PUID approach is applied for cyber-attack detection. Section 6 is the simulation section in which the performance of the proposed method is evaluated. Section 7 is the conclusion section. The parity space method as the applied model-based fault detection approach is reviewed in the Appendix.

2 Problem statement

Fig. 1 depicts an overall view of the supervisory control in a communication link-enabled droop-controlled hybrid AC/DC MG.

Droop controller is implemented locally in each DR for proper power sharing. Since in droop-controlled MGs, the voltage and frequency values are varied depending on the power consumption value, a supervisory control is required to compensate the voltage and frequency deviations. Hence, this MG needs a setpoint vector by applying which they can improve their operating condition. To this end, a common setpoint vector is sent from the PMCU via some communication links to every DR. This setpoint vector – which consists of AC voltage, AC frequency and DC voltage – is determined by a human operator as long as the secondary control loop is open. As it was discussed in the Introduction, zero dynamic attack cannot be detected in such MGs because of the abovementioned reasons.

However, by closing the secondary control loop using a proportional integral (PI) controller and observing its integrator signal values, not only will the zero dynamic attack be detected easily, but also we make it relatively impossible for attacker to design a zero dynamic attack. The impossibility of designing a zero dynamic attack for the closed loop system stems from the fact that the PI controller and parity observer are implemented in a common processor, hence they can be coordinated to vary in a regular manner.

3 Modelling cyber-attack on setpoints and sensors

As it was mentioned in the Introduction, a cyber-attack detector will be designed for a converter-based droop-controlled hybrid AC/DC MG. In this kind of MG, DRs are connected to the AC and DC links via converters. In addition to DRs, the studied hybrid MG consists of different types of loads. The loads can be considered as a combination of constant current, constant power and constant impedance loads. The power transfer between the AC and DC links is done using a bidirectional AC/DC converter. In our previous study, we have derived a dynamic model for the MG in [7, 8]. The details of parameters, inputs, outputs, disturbances, dynamic equations and linearisations are also completely explored.

As it is discussed in [3], hierarchical control of MG consists of three control layers, due to which there are different modes of control depending on the conditions of loops. In the case in which secondary control loop is open, the AC/DC exchanging power is calculated by a droop control-based method as it is discussed in [8]. However, in the case in which the secondary control loop is closed, the exchanging power is considered to be constant as it will be discussed in the following. In this section, it is tried to analyse the system dynamics in the case of open secondary control loop.

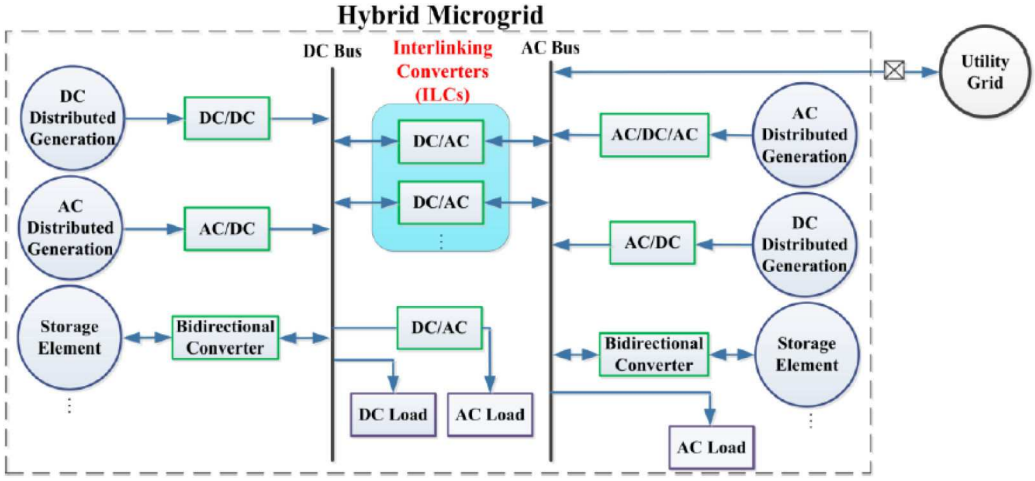

Fig. 2 *Conceptual diagram of a hybrid MG [40]*

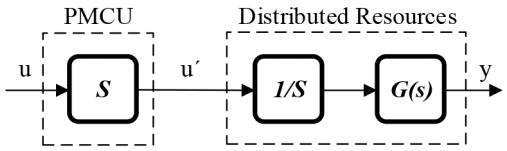

Fig. 3 *Preventing zero dynamic attack by scaling control signal*

The MG is considered to be such that all the DRs and loads are connected to two common links as shown in Fig. 2.

Each individual converter is connected to a PMCU via communication links which can be perverted by cyber-attack.

From the derived dynamic model of our previous study [7, 8], the model is considered to be a linear state space model. In this system, attack can be implemented on both setpoints and sensors. From control engineering perspective, the setpoint attacks can be modelled as actuator faults. Hence, the system can be modelled by

$$\begin{cases} \boldsymbol{M}\dot{x} = \boldsymbol{A}x + \boldsymbol{B}\boldsymbol{u} + \boldsymbol{E}_{\mathrm{d}}w + \boldsymbol{E}_{\mathrm{f}}\boldsymbol{u}_{\mathrm{fa}} + w_{\mathrm{n}} \\ y = \boldsymbol{C}x + \boldsymbol{D}\boldsymbol{u} + \boldsymbol{F}_{\mathrm{d}}w + \boldsymbol{F}_{\mathrm{f}}\boldsymbol{u}_{\mathrm{fa}} + \boldsymbol{u}_{\mathrm{fs}} + v_{\mathrm{n}} \end{cases} \tag{1}$$

In which

$$\boldsymbol{u} = \begin{bmatrix} \hat{v}_{\mathrm{ref,ac}} & \hat{f}_{\mathrm{ref}} & \hat{v}_{\mathrm{ref,dc}} \end{bmatrix}^{\mathrm{T}}$$
$$w = \begin{bmatrix} \hat{P}_{\mathrm{load}} & \hat{\boldsymbol{Q}}_{\mathrm{load}} & \hat{I}_{\mathrm{load}} & \hat{Z}_{\mathrm{load}} & \hat{P}_{\mathrm{dc}} \end{bmatrix}^{\mathrm{T}}$$
$$y = \begin{bmatrix} \hat{v}_{\mathrm{ac}} & \hat{f} & \hat{v}_{\mathrm{dc}} \end{bmatrix}^{\mathrm{T}}$$

in the above model, w_{n} and v_{n} represent the process and observation white Gaussian noises with covariance matrix $\boldsymbol{Q}$ and $\boldsymbol{R}$, respectively, i.e. $w_{\mathrm{n}} \sim N(0, Q_{\mathrm{n}})$ and $v_{\mathrm{n}} \sim N(0, \boldsymbol{R}_{\mathrm{n}})$.

In addition to measurement noise represented by v_{n}, model uncertainties are represented by w_{n} as discussed in [41].

It is also noteworthy that the setpoints, as the inputs of the system and outputs of the supervisory control, are normally updated in about 5- to 10-s intervals [3]; while the communication delays are in the order of milliseconds according to IEC 61850 standards; hence the delays can be ignored in the model.

It is also remarkable that the meaningful physical variables of MG are obtained by decomposing the state vector of x to two equal size sub-vector states x_1 and x_2 such that $x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$. Calculation of $x_1 + \dot{x}_2$ yields the physical variables as follows: (see equation below). As the setpoint cyber-attack can be regarded as a deviation in inputs, it can be modelled as actuator faults. Hence, the matrices $\boldsymbol{E}_{\mathrm{f}}$ and $\boldsymbol{F}_{\mathrm{f}}$ which model dynamic of cyber-attack are equal to $\boldsymbol{B}$ and $\boldsymbol{D}$, respectively, as it is described in [41, (3.33) and (3.34)]. $\boldsymbol{u}_{\mathrm{fa}}$ is a vector of setpoint deviation and $\boldsymbol{u}_{\mathrm{fs}}$ is a vector of sensor deviation. The matrices $\boldsymbol{M}$, $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$, $\boldsymbol{D}$, $\boldsymbol{E}_{\mathrm{d}}$ and $\boldsymbol{F}_{\mathrm{d}}$ are all defined in [7, 8]. $\boldsymbol{u}_{\mathrm{fa}}$ and $\boldsymbol{u}_{\mathrm{fs}}$ are three-dimensional vectors, in which the first elements are deviation attacks on $\hat{v}_{\mathrm{ref,ac}}$ and $\hat{v}_{\mathrm{ac}}$, the second elements are deviation attacks on $\hat{f}_{\mathrm{ref}}$ and $\hat{f}$ and the third elements are deviation attacks on $\hat{v}_{\mathrm{ref,ac}}$ and $\hat{v}_{\mathrm{ref}}$, respectively:

$$\boldsymbol{E}_{\mathrm{f}} = \boldsymbol{B}, \quad \boldsymbol{F}_{\mathrm{f}} = \boldsymbol{D}, \quad \boldsymbol{u}_{\mathrm{fa}} = \begin{bmatrix} u_{\mathrm{fa1}} \\ u_{\mathrm{fa2}} \\ u_{\mathrm{fa3}} \end{bmatrix}, \quad \boldsymbol{u}_{\mathrm{fs}} = \begin{bmatrix} u_{\mathrm{fs1}} \\ u_{\mathrm{fs2}} \\ u_{\mathrm{fs3}} \end{bmatrix}$$

The theorem of detecting fault from disturbance in Rosen Brock system says that to decouple fault and disturbance, the following condition should be held [41]

$$\mathrm{rank}\left(\begin{bmatrix} \boldsymbol{A} - s\boldsymbol{M} & \boldsymbol{E}_{\mathrm{d}} \\ \boldsymbol{C} & \boldsymbol{F}_{\mathrm{d}} \end{bmatrix}\right) < \mathrm{rank}\left(\begin{bmatrix} \boldsymbol{A} - s\boldsymbol{M} & \boldsymbol{E}_{\mathrm{d}} & \boldsymbol{E}_{\mathrm{f}} \\ \boldsymbol{C} & \boldsymbol{F}_{\mathrm{d}} & \boldsymbol{F}_{\mathrm{f}} \end{bmatrix}\right) \tag{2}$$

In other words, if the number of outputs of system is less than the number of disturbances, to recognise disturbance from faults, the number of outputs of system should be increased.

Hence to decouple the disturbance and fault, since the number of outputs is three while the number of disturbances is five, three other outputs should be added to equations. To this end, state variables corresponding to the PI controller in the secondary control loop can be used as other outputs.

4 Designing zero dynamic attack on setpoints

In this section, it is tried to design zero dynamic attack which has as little as possible influence on the outputs of system while the secondary control loop is open. Zero dynamic attacks cannot be detected by regular detectors. Change in unobserved states of system while the outputs are unchanged can be harmful for the system.

Based on zero dynamics of system, there exist some input vectors with specific initial conditions for a system dynamic which have no influence on outputs. Although the effect of these inputs cannot be seen in output, they cause some deviation in unobserved states (Fig. 3).

These initial conditions and input vectors can be determined by calculating transmission zeros and zero input direction. Transmission zeros are the values for υ which decreases the rank of the following matrix:

$$x_1 + \dot{x}_2 = \begin{bmatrix} \hat{i}_1^* & \dots & \hat{i}_m^* & \hat{v}_1 & \dots & \hat{v}_m & \hat{\delta}_1 & \dots & \hat{\delta}_m & \hat{P}_{\mathrm{ex}} & \dot{\hat{P}}_{\mathrm{ex}} & \hat{i}_{\mathrm{o},1} & \dots & \hat{i}_{\mathrm{o,n}} & \hat{P}_{\mathrm{ex}}^* \end{bmatrix}^{\mathrm{T}}$$

$$P(\upsilon)=\begin{bmatrix}\upsilon \boldsymbol{M}-\boldsymbol{A} & -\boldsymbol{E}_{\mathrm{f}}\\ \boldsymbol{C} & \boldsymbol{F}_{\mathrm{f}}\end{bmatrix} \tag{3}$$

Zero input direction g and its initial value x_0 can be obtained by the following equation:

$$\begin{bmatrix}\upsilon \boldsymbol{M}-\boldsymbol{A} & -\boldsymbol{E}_{\mathrm{f}}\\ \boldsymbol{C} & \boldsymbol{F}_{\mathrm{f}}\end{bmatrix}\begin{bmatrix}x_0\\ g\end{bmatrix}=\begin{bmatrix}0\\ 0\end{bmatrix} \tag{4}$$

By having g and υ the attack can be designed such that it has not any influence on outputs

$$\begin{cases}a_k=\upsilon^k g \text{ for discretised system}\\ a_k=e^{\upsilon t} g \text{ for continuous system}\end{cases} \tag{5}$$

Authors of [42] have provided a clear definition of the zero dynamic attack as well as other attacks

If the initial condition of system at the moment of attack is equal to x_0, it has not any transient effect on the outputs; otherwise if it differs from x_0, some transients may be seen in the outputs. To prevent attack, as it is declared in [39] and depicted in Fig. 3, a scaling matrix in the inputs can be used to change the dynamics of system. Zero dynamic will be changed by changing the dynamic of system. This prevention approach can be discovered by the attacker easily. The scaling matrix can be calculated using steady state values of measured signal y_{ss} and transfer data $\boldsymbol{u}'_{\mathrm{ss}}$ vectors as follows:

$$1/S=(I\times \boldsymbol{u}'_{\mathrm{ss}})^{-1}\times\left(I\times G^{-1}(0)y_{\mathrm{ss}}\right)$$

5 Zero dynamic attack mitigation with closing the secondary control loop

As it was mentioned and discussed in [3], hierarchical control of MG consists of three control layers. The tertiary control is used when the MG is connected to a grid. It calculates the setpoints of AC voltage and bus angle such that a defined value of Q and P is transmitted between the MG and grid. In this case, the transmitted power between the grid and MG can be modelled by a constant power AC load which can be negative or positive. The outputs of tertiary controller are the reference values for the secondary controller. The secondary control loop is used to compensate the setpoint deviation caused by the primary droop control loop. The deviation can be compensated using a PI controller for each setpoint command. Knowing that closing the secondary control loop makes the dynamic different, here it is tried to derive the closed loop dynamic. The control signals of the secondary control loop can be used in an attack detection approach.

Remark: One important issue which should be regarded in the case in which secondary control loop is closed is that the setpoints of AC bus voltage and DC bus voltage are independent. This is while in the open loop system, the global droop control logic sets the AC/DC exchanging power reference such that AC and DC side voltages are regulated. The regulating logic is such that load dispatches in DC and AC sides are proportional. This logic makes the voltages of two sides to be dependent. However, if the secondary control loop is closed, the voltages of AC and DC sides will be independent. This conflict makes us to disable the global droop control and make the droop control local at each side. The global droop control logic has been discussed in detail, in our previous study [8]. To localise the global droop control, it is adequate to substitute the coefficients of the controller of exchanged power reference P^*_{ex} equal to zero.

Regarding that the open loop system dynamic is given by

$$\begin{cases}\boldsymbol{M}\dot{x}=\boldsymbol{A}x+\boldsymbol{B}u+\boldsymbol{E}_{\mathrm{d}}w+w_{\mathrm{n}}\\ y=\boldsymbol{C}x+\boldsymbol{D}u+\boldsymbol{F}_{\mathrm{d}}w+v_{\mathrm{n}}\end{cases} \tag{6}$$

The dynamic of closed loop system can be obtained by substituting $\boldsymbol{u}$ from the secondary controller output. With the assumption that the setpoint command is the secondary loop controller output and also assuming that the controller input consist of setpoint error, it can be written

$$\begin{cases}\boldsymbol{u}=v+\boldsymbol{u}_{\mathrm{fa}}\\ e=y-\boldsymbol{u}_{\mathrm{s}}+\boldsymbol{u}_{\mathrm{fs}}\end{cases} \tag{7}$$

in which v is the secondary controller output, $\boldsymbol{u}_{\mathrm{fa}}$ and $\boldsymbol{u}_{\mathrm{fs}}$ are setpoint and sensor cyber-attacks of open loop system. Also $\boldsymbol{u}_{\mathrm{s}}$ is the setpoints of secondary control loop. A setpoint attack on the voltages and frequency setpoints may happen in the case in which DRs' locations are far from the PMCU location and this data is required to be transmitted by communication links. A sensor attack on the voltages and frequency values can be happened in the case in which the AC or DC buses locations are far from the PMCU location and this data is required to be transmitted by communication links.

Regarding that the controller is PI type, v (controller output) can be decomposed to proportional part (y_{p}) and integral part (y_{i}), which are defined as follows:

$$\begin{aligned}&y_{\mathrm{p}}=e=\boldsymbol{C}x+\boldsymbol{D}(v+\boldsymbol{u}_{\mathrm{fa}})+\boldsymbol{F}_{\mathrm{d}}w+v_{\mathrm{n}}+\boldsymbol{u}_{\mathrm{fs}}-\boldsymbol{u}_{\mathrm{s}}\\ &y_{\mathrm{i}}=\int e\,\mathrm{d}t=z\\ &v=-K_{\mathrm{p}}y_{\mathrm{p}}-K_{\mathrm{i}}y_{\mathrm{i}}\end{aligned} \tag{8}$$

Considering that the output of system y which is seen by the secondary loop controller is sum of the real output and cyber-attack, the system dynamic can be rewritten as follows:

$$\begin{cases}\boldsymbol{M}\dot{x}=\boldsymbol{A}x+\boldsymbol{B}(v+\boldsymbol{u}_{\mathrm{fa}})+\boldsymbol{E}_{\mathrm{d}}w+w_{\mathrm{n}}\\ y=\boldsymbol{C}x+\boldsymbol{D}(v+\boldsymbol{u}_{\mathrm{fa}})+\boldsymbol{F}_{\mathrm{d}}w+\boldsymbol{u}_{\mathrm{fs}}+v_{\mathrm{n}}\end{cases} \tag{9}$$

The closed loop dynamic can be written by

$$\begin{aligned}&\begin{bmatrix}\boldsymbol{M} & 0\\ 0 & I\end{bmatrix}\begin{bmatrix}\dot{x}\\ \dot{z}\end{bmatrix}=\begin{bmatrix}\boldsymbol{A} & 0\\ \boldsymbol{C} & 0\end{bmatrix}\begin{bmatrix}x\\ z\end{bmatrix}+\begin{bmatrix}\boldsymbol{B}\\ \boldsymbol{D}\end{bmatrix}(v+\boldsymbol{u}_{\mathrm{fa}})+\begin{bmatrix}0\\ I\end{bmatrix}\boldsymbol{u}_{\mathrm{fs}}\\ &\qquad+\begin{bmatrix}\boldsymbol{E}_{\mathrm{d}}\\ \boldsymbol{F}_{\mathrm{d}}\end{bmatrix}w-\begin{bmatrix}0\\ I\end{bmatrix}\boldsymbol{u}_{\mathrm{s}}+\begin{bmatrix}w_{\mathrm{n}}\\ v_{\mathrm{n}}\end{bmatrix}\\ &\begin{bmatrix}y\\ y_{\mathrm{p}}\\ y_{\mathrm{i}}\end{bmatrix}=\begin{bmatrix}\boldsymbol{C} & 0\\ \boldsymbol{C} & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}x\\ z\end{bmatrix}+\begin{bmatrix}\boldsymbol{D}\\ \boldsymbol{D}\\ 0\end{bmatrix}(v+\boldsymbol{u}_{\mathrm{fa}})+\begin{bmatrix}I\\ I\\ 0\end{bmatrix}\boldsymbol{u}_{\mathrm{fs}}\\ &\qquad+\begin{bmatrix}\boldsymbol{F}_{\mathrm{d}}\\ \boldsymbol{F}_{\mathrm{d}}\\ 0\end{bmatrix}w-\begin{bmatrix}0\\ 1\\ 0\end{bmatrix}\boldsymbol{u}_{\mathrm{s}}+\begin{bmatrix}v_{\mathrm{n}}\\ v_{\mathrm{n}}\\ 0\end{bmatrix}\end{aligned} \tag{10}$$

Using the equation $v=-K_{\mathrm{p}}y_{\mathrm{p}}-K_{\mathrm{i}}y_{\mathrm{i}}$ and substituting y_{p} and y_{i} in it, we have

$$v=-K_{\mathrm{p}}(\boldsymbol{C}x+\boldsymbol{D}(v+\boldsymbol{u}_{\mathrm{fa}})+\boldsymbol{F}_{\mathrm{d}}w+v_{\mathrm{n}}+\boldsymbol{u}_{\mathrm{fs}}-\boldsymbol{u}_{\mathrm{s}})-K_{\mathrm{i}}z \tag{11}$$

hence

$$\begin{aligned}v=\left(I+K_{\mathrm{p}}D\right)^{-1}\big(&-K_{\mathrm{p}}\boldsymbol{C}x-K_{\mathrm{p}}\boldsymbol{F}_{\mathrm{d}}w-K_{\mathrm{p}}v_{\mathrm{n}}-K_{\mathrm{p}}\boldsymbol{D}\boldsymbol{u}_{\mathrm{fa}}\\ &-K_{\mathrm{p}}\boldsymbol{u}_{\mathrm{fs}}+K_{\mathrm{p}}s-K_{\mathrm{i}}z\big)\end{aligned} \tag{12}$$

Substituting the above equation in state space equation yields

$$\begin{aligned}\begin{bmatrix}\boldsymbol{M} & 0\\ 0 & I\end{bmatrix}\begin{bmatrix}\dot{x}\\ \dot{z}\end{bmatrix}=&\begin{bmatrix}\boldsymbol{A} & 0\\ \boldsymbol{C} & 0\end{bmatrix}\begin{bmatrix}x\\ z\end{bmatrix}+\begin{bmatrix}\boldsymbol{B}\\ \boldsymbol{D}\end{bmatrix}\left(I+K_{\mathrm{p}}\boldsymbol{D}\right)^{-1}\big(-K_{\mathrm{p}}\boldsymbol{C}x\\ &-K_{\mathrm{p}}\boldsymbol{F}_{\mathrm{d}}w-K_{\mathrm{p}}v_{\mathrm{n}}-K_{\mathrm{p}}\boldsymbol{D}\boldsymbol{u}_{\mathrm{fa}}-K_{\mathrm{p}}\boldsymbol{u}_{\mathrm{fs}}+K_{\mathrm{p}}\boldsymbol{u}_{\mathrm{s}}-K_{\mathrm{i}}z\\ &+\begin{bmatrix}\boldsymbol{B}\\ \boldsymbol{D}\end{bmatrix}\boldsymbol{u}_{\mathrm{fa}}+\begin{bmatrix}0\\ I\end{bmatrix}\boldsymbol{u}_{\mathrm{fs}}+\begin{bmatrix}\boldsymbol{E}_{\mathrm{d}}\\ \boldsymbol{F}_{\mathrm{d}}\end{bmatrix}w-\begin{bmatrix}0\\ I\end{bmatrix}\boldsymbol{u}_{\mathrm{s}}+\begin{bmatrix}w_{\mathrm{n}}\\ v_{\mathrm{n}}\end{bmatrix}\end{aligned}$$

thus (see (13)) . Substituting the v equation in output equation leads to

$$y = \boldsymbol{C}x + \boldsymbol{D}(v + \boldsymbol{u}_{\mathrm{fa}}) + \boldsymbol{F}_{\mathrm{d}}w + \boldsymbol{u}_{\mathrm{f}s} + v_{\mathrm{n}} \tag{14}$$

hence

$$\begin{aligned} y = {} & \boldsymbol{C}x + \boldsymbol{D}\big(I + K_{\mathrm{p}}\boldsymbol{D}\big)^{-1}\big(-K_{\mathrm{p}}\boldsymbol{C}x - K_{\mathrm{p}}\boldsymbol{F}_{\mathrm{d}}w - K_{\mathrm{p}}v_{\mathrm{n}} \\ & -K_{\mathrm{p}}\boldsymbol{D}\boldsymbol{u}_{\mathrm{fa}} - K_{\mathrm{p}}\boldsymbol{u}_{\mathrm{fs}} + K_{\mathrm{p}}\boldsymbol{u}_{\mathrm{s}} - K_{\mathrm{i}}z\big) + \boldsymbol{D}\boldsymbol{u}_{\mathrm{fa}} + \boldsymbol{F}_{\mathrm{d}}w + \boldsymbol{u}_{\mathrm{fs}} + v_{\mathrm{n}} \end{aligned} \tag{15}$$

and finally,

$$\begin{aligned} y = {} & \Big[\boldsymbol{C} - \boldsymbol{D}\big(I + K_{\mathrm{p}}\boldsymbol{D}\big)^{-1}K_{\mathrm{p}}\boldsymbol{C} - \boldsymbol{D}\big(I + K_{\mathrm{p}}\boldsymbol{D}\big)^{-1}K_{\mathrm{i}}\Big]\begin{bmatrix} x \\ z \end{bmatrix} \\ & + \Big[I - \boldsymbol{D}\big(I + K_{\mathrm{p}}\boldsymbol{D}\big)^{-1}K_{\mathrm{p}}\Big]\boldsymbol{F}_{\mathrm{d}}w \\ & + \Big[-\boldsymbol{D}\big(I + K_{\mathrm{p}}\boldsymbol{D}\big)^{-1}K_{\mathrm{p}}\boldsymbol{D} + \boldsymbol{D}\Big]\boldsymbol{u}_{\mathrm{fa}} \\ & + \Big[I - \boldsymbol{D}\big(I + K_{\mathrm{p}}\boldsymbol{D}\big)^{-1}K_{\mathrm{p}}\Big]\boldsymbol{u}_{\mathrm{f}s} + \Big[\boldsymbol{D}\big(I + K_{\mathrm{p}}\boldsymbol{D}\big)^{-1}K_{\mathrm{p}}\Big]\boldsymbol{u}_{\mathrm{s}} \\ & + \Big[I - \boldsymbol{D}\big(I + K_{\mathrm{p}}\boldsymbol{D}\big)^{-1}K_{\mathrm{p}}\Big]v_{\mathrm{n}} \end{aligned} \tag{16}$$

Thus, the closed loop dynamic of the system is obtained in this section. As it can be seen, the dynamic is affected by the PI coefficients of the secondary control loop. To prevent the system from identification by the attacker, the PI coefficient can be changed periodically. Since the observer can be implemented in the same processor as the one in which the secondary controller is implemented, the observer can be updated immediately after the PI coefficients are changed. The observer updating needs no communication link. This type of dynamic change is the easiest, cheapest and the most secure type of dynamic change. This is while, scaling the inputs and outputs – the approach in [39] can be identified by the attacker easily; and also changing dynamic by changing the converters' PI coefficients has implementation and coordination difficulties.

Obtaining a closed loop dynamic of system, we can design a model-based fault detection PUID observer to detect cyber-attack and diagnose it from disturbances. The approach we have used in this article is called parity approach. To detect attack using the parity approach, the model should be discretised first. Parity space will be calculated by having the discretised model. The inputs of observer for detecting attack are $[\boldsymbol{u}_{\mathrm{s}},\ \boldsymbol{y}_{\mathrm{s}}]$ vectors. These vectors can be constructed as discussed in the Appendix by making a train of sampled inputs and outputs. By using the train of sampled $\boldsymbol{u}_{\mathrm{s}}$ to construct U_{s}, and also using the train of sampled $\begin{bmatrix} y^{\mathrm{T}} & z^{\mathrm{T}} \end{bmatrix}^{\mathrm{T}}$ to construct Y_{s}, as follows

$$\begin{aligned} Y_{\mathrm{s}}(k) &= \begin{bmatrix} \begin{bmatrix} y^{\mathrm{T}}(k-s) & z^{\mathrm{T}}(k-s) \end{bmatrix}^{\mathrm{T}} \\ \begin{bmatrix} y^{\mathrm{T}}(k-s+1) & z^{\mathrm{T}}(k-s+1) \end{bmatrix}^{\mathrm{T}} \\ \vdots \\ \begin{bmatrix} y^{\mathrm{T}}(k) & z^{\mathrm{T}}(k) \end{bmatrix}^{\mathrm{T}} \end{bmatrix}, \\ U_{\mathrm{s}}(k) &= \begin{bmatrix} u_{\mathrm{s}}(k-s) \\ u_{\mathrm{s}}(k-s+1) \\ \vdots \\ u_{\mathrm{s}}(k) \end{bmatrix} \end{aligned} \tag{17}$$

the residue can be obtained by the following matrix:

$$r(k) = v_{\mathrm{s}}\big(Y_{\mathrm{s}}(k) - H_{u,\mathrm{s}}U_{\mathrm{s}}(k)\big) \tag{18}$$

$r(k)$ is calculated in each step time as explained in Section 9.1. Once the magnitude of $r(k)$ exceeds a threshold, it illustrates that the system is under cyber-attack. The threshold is necessary for the residue, because of the uncertainties and noises in the model.

6 Simulation and verification

As it is mentioned in previous section, to detect any deviation in the transmitted data between the PMCU and the DRs, the PUID method has been used. PUID is a class of model-based fault detection approach in which an observer generates a residue which is independent of disturbance and the initial conditions [41]. The residue increases when some defined faults occur in the system. The setpoint and feedback cyber-attack in this article has been regarded as a kind of actuator and sensor faults, respectively. This article has used a class of PUID method called parity space method to detect cyber-attack in the system. The approach is general and can be used for any converter-based MGs with any quantity of nodes. Parity approach is discussed in Section 9.

As an approving instance, a four source hybrid MG is used. The MG consist of the following nodes:

- *Power exchanging converter:* bidirectional CPF-OCC AC–DC converter which connects AC MG to DC MG
- *DC Resource 1:* DC–DC full bridge converter which is connected to a DC voltage resource
- *DC Resource 2:* DC–DC full bridge converter which is connected to a DC voltage resource
- *AC Resource 1:* An inverter in which switching is based on comparing a sinusoidal wave with a saw-tooth one
- *AC Resource 2:* An inverter in which switching is based on comparing a sinusoidal wave with a saw-tooth one
- *DC loads:* Constant resistance, current and power
- *AC consumer:* An RL load and a constant power load which has both active and reactive power

The simulated MG is depicted in Fig. 4. The outputs and states values of dynamical model for four different scenarios are depicted in Figs. 5–10. The simulations are run, respectively, for zero dynamic setpoint attack and sensor attack in open loop system, and also zero dynamic setpoint attack and feedback attack in the closed loop system. A randomly constructed simple attack is also happened at 7.5 s in all the simulations. The residues for the mentioned simulations are also depicted in Fig. 10. For the simulations of open loop system, all of the system's parameters are the same as those in [7] and also, in the case in which secondary control loop is closed, all of the system's parameters are the same as those in [7] and except for the PI coefficients of P^{*}_{ex} controller. Since the droop cannot be global for the secondary control closed loop system, the coefficients of this controller are regarded to be zero. The parameters of secondary loop PI controller are shown in Table 1.

Simulations are performed with the following conditions:

(i) Setpoint attack in the open loop system:

- *Disturbance:* 16.7% decrease in R_{load} magnitude and 1000 W load increase at 3 s,
- *Setpoint zero dynamic attack:* [4.24 vAC, −0.01 Hz, −2.65 vDC] with discrete $\upsilon = 0.9883$ at 6 s,
- *Simple attack:* +4 vAC at 7.5 s.

(ii) Sensor attack in open loop system:

- *Disturbance:* 16.7% decrease in R_{load} magnitude and 1000 W load increase at 3 s,
- *Sensor zero dynamic attack:* [−4.26 vAC, 0.005 Hz, 2.62 vDC] with discrete $e\upsilon = 0.987$ at 6 s
- *Simple attack:* +4 vAC at 7.5 s.

(iii) Setpoint attack in closed loop system:

- *Disturbance:* 16.7% decrease in R_{load} magnitude, 1500 W load increase and 33% AC load increase at 3 s,
- *Setpoint zero dynamic attack:* [−0.22 vAC, −0.0133 Hz, −5 vDC] with discrete $\upsilon = 1$ at 6 s,
- *Simple attack:* −5 vAC at 7.5 s.

(iv) Feedback attack in closed loop system:

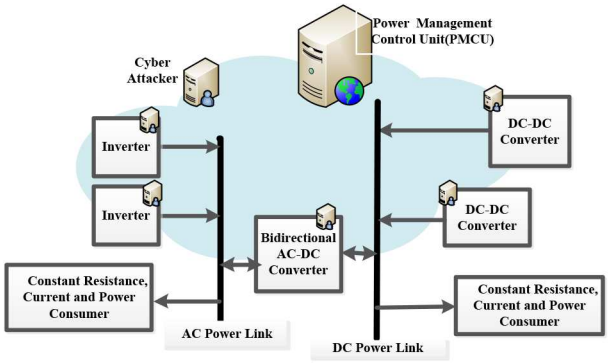

Fig. 4 *Conceptual diagram of simulated hybrid MG*

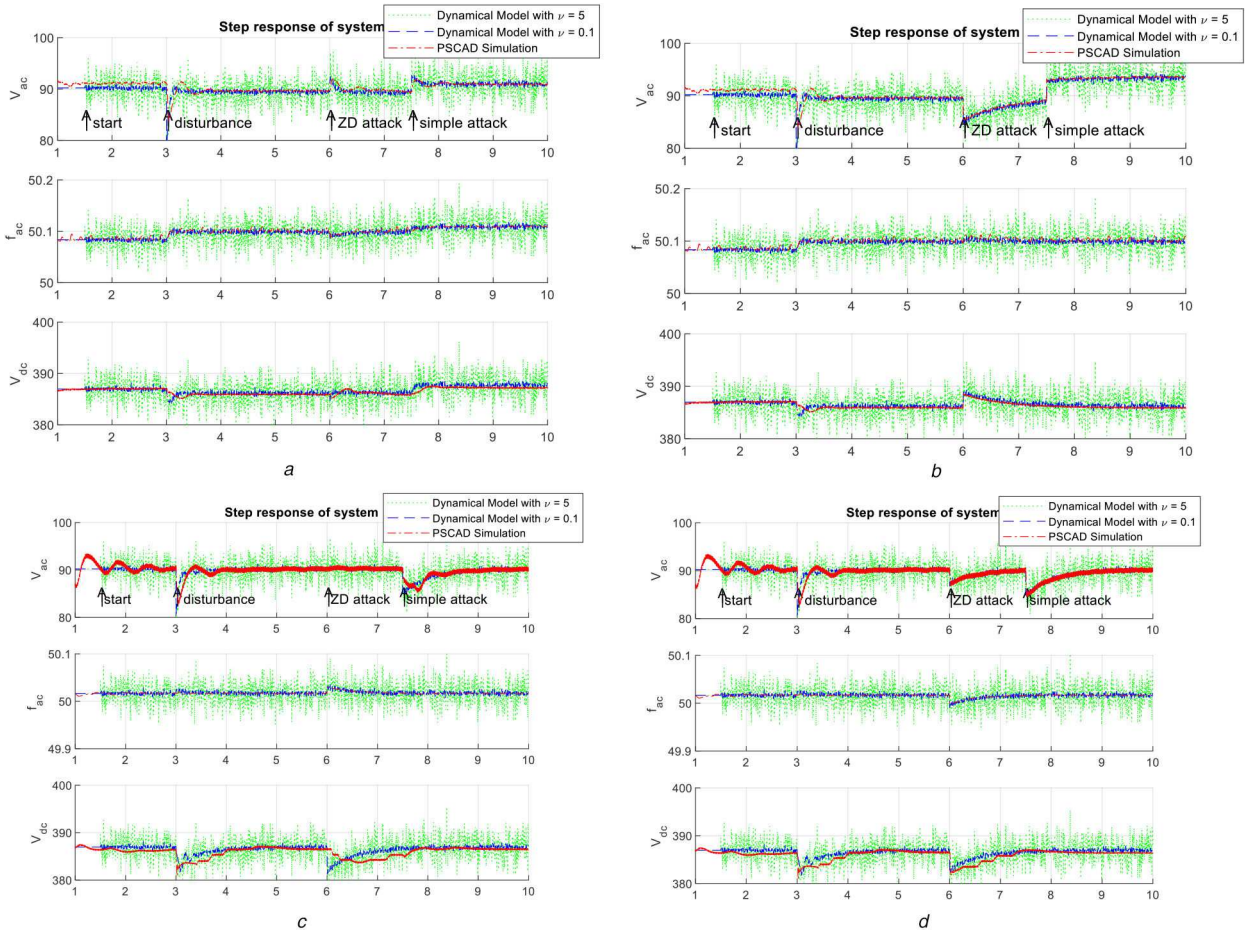

Fig. 5 *Outputs of system*

(a) Setpoint zero dynamic attack in open loop system, ***(b)*** Sensor zero dynamic attack in open loop system, ***(c)*** Setpoint zero dynamic attack in closed loop system, ***(d)*** Feedback zero dynamic attack in closed loop system

- *Disturbance:* 16.7% decrease in R_{load} magnitude, 1500 W load increase and 33% AC load increase at 3 s,
- *Feedback zero dynamic attack:* [−2.7335 vAC, −0.0190 Hz, −4.1866 vDC] with discrete $\upsilon = 1$ at 6 s,
- *Simple attack*: −5 vAC at 7.5 s.

$$\begin{bmatrix} \boldsymbol{M} & 0 \\ 0 & I \end{bmatrix} \begin{bmatrix} \dot{x} \\ \dot{z} \end{bmatrix} = \begin{bmatrix} \boldsymbol{A} - \boldsymbol{B}(I + K_{\text{p}}\boldsymbol{D})^{-1}K_{\text{p}}\boldsymbol{C} & -\boldsymbol{B}(I + K_{\text{p}}\boldsymbol{D})^{-1}K_{\text{i}} \\ \boldsymbol{C} - \boldsymbol{D}(I + K_{\text{p}}\boldsymbol{D})^{-1}K_{\text{p}}\boldsymbol{C} & -\boldsymbol{D}(I + K_{\text{p}}\boldsymbol{D})^{-1}K_{\text{i}} \end{bmatrix} \begin{bmatrix} x \\ z \end{bmatrix} + \begin{bmatrix} -\boldsymbol{B}(I + K_{\text{p}}\boldsymbol{D})^{-1}K_{\text{p}}\boldsymbol{D} + \boldsymbol{B} \\ -\boldsymbol{D}(I + K_{\text{p}}\boldsymbol{D})^{-1}K_{\text{p}}\boldsymbol{D} + \boldsymbol{D} \end{bmatrix} \boldsymbol{u}_{\text{fa}} + \begin{bmatrix} -\boldsymbol{B}(I + K_{\text{p}}\boldsymbol{D})^{-1}K_{\text{p}} \\ I - \boldsymbol{D}(I + K_{\text{p}}\boldsymbol{D})^{-1}K_{\text{p}} \end{bmatrix} \boldsymbol{u}_{\text{fs}} + \begin{bmatrix} \boldsymbol{E}_{\text{d}} - \boldsymbol{B}(I + K_{\text{p}}\boldsymbol{D})^{-1}K_{\text{p}}\boldsymbol{F}_{\text{d}} \\ \boldsymbol{F}_{\text{d}} - \boldsymbol{D}(I + K_{\text{p}}\boldsymbol{D})^{-1}K_{\text{p}}\boldsymbol{F}_{\text{d}} \end{bmatrix} w - \begin{bmatrix} -\boldsymbol{B}(I + K_{\text{p}}\boldsymbol{D})^{-1}K_{\text{p}} \\ I - \boldsymbol{D}(I + K_{\text{p}}\boldsymbol{D})^{-1}K_{\text{p}} \end{bmatrix} \boldsymbol{u}_{\text{s}} + \begin{bmatrix} -\boldsymbol{B}(I + K_{\text{p}}\boldsymbol{D})^{-1}K_{\text{p}} \\ I - \boldsymbol{D}(I + K_{\text{p}}\boldsymbol{D})^{-1}K_{\text{p}} \end{bmatrix} v_{\text{n}} + \begin{bmatrix} I \\ 0 \end{bmatrix} w_{\text{n}} \tag{13}$$

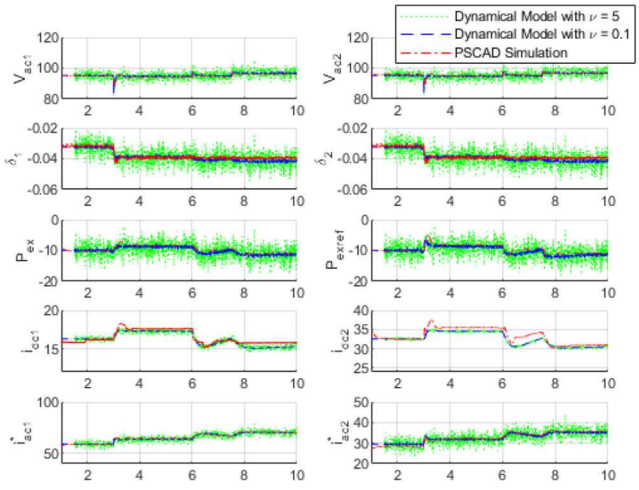

Fig. 6 *State variables of system (a) Setpoint attack in open loop system*

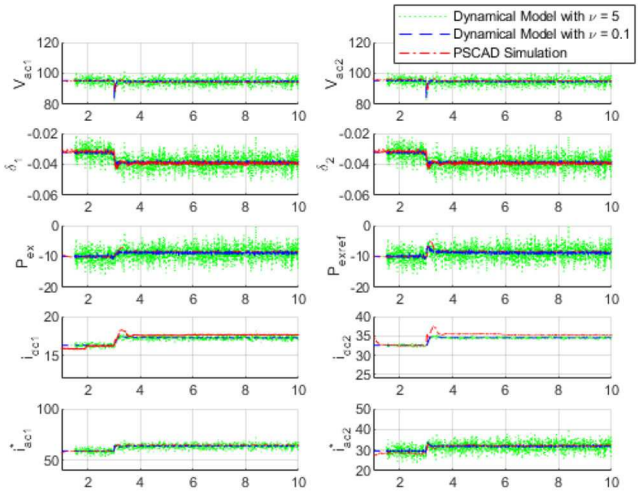

Fig. 7 *State variables of system (b) Sensor zero dynamic attack in open loop system*

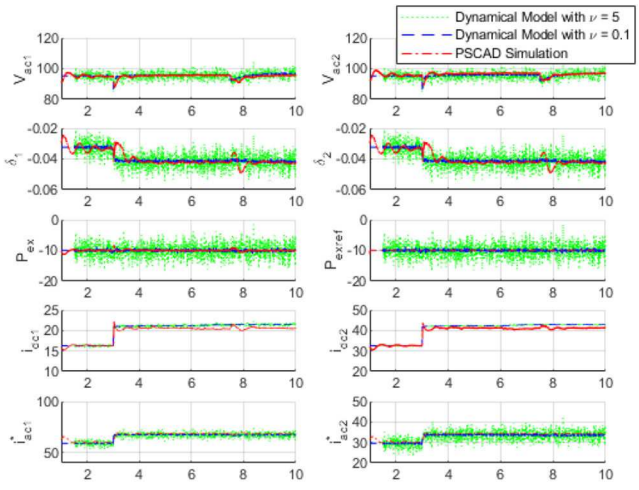

Fig. 8 *State variables of system (c) Setpoint zero dynamic attack in closed loop system*

As it can be seen in Figs. 10*a* and *b* the zero dynamic setpoint attack and sensor attack for open loop system cannot be detected by the observer. However, the zero dynamic attack in the closed loop system is detected by the observer as shown in Figs. 10*c* and *d*. To have appropriate criteria for the residue magnitude, there are some methods for 'residual evaluation and threshold computation'. As it is discussed in [41], the methods can be either 'norm-based' or 'statistical methods'.

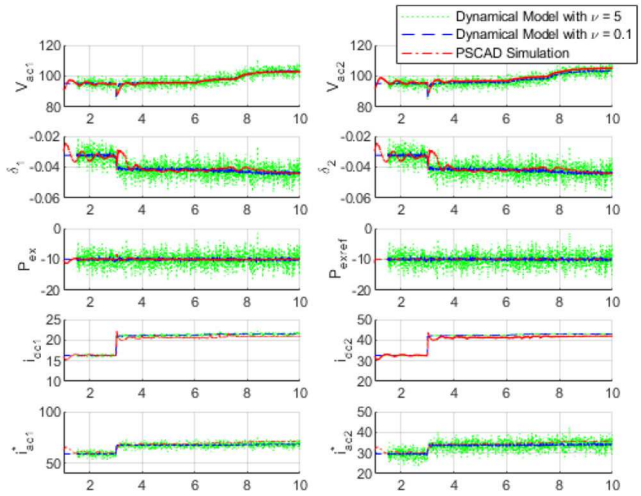

Fig. 9 *State variables of system (d) Feedback zero dynamic attack in closed loop system*

The comparison of the achieved results with two other methods of detecting zero dynamic attack is not feasible. For the first method – side information matrix–, a great number of outputs is needed for observer which is not available in this case and cannot be applied. Also for the second method – scaling matrix–, if the scaling matrix is identified by attacker, the zero dynamic attack will be successful.

Simulation of zero dynamic attack for the open loop system shows that although the frequency of AC sub-MG is deviated by the attack, the residue returns to zero after some short transients and the observer is not successful in detection. It is also remarkable that the residue transient is caused by the difference between initial state of system at the moment of attack and zero dynamic initial condition. Regarding the fact that the frequency change can be occurred by droop control characteristics, the deviation may seem to be normal; hence, the origin of frequency deviation cannot be distinguished easily.

However, as it can be seen the zero dynamic attack in the open loop system can be mitigated by closing the secondary control loop of system. By adding the control signals of secondary control loop to the parity observer inputs, the zero dynamic attack is detected perfectly.

In order to know how to implement the model and the observer, the block diagram of the simulation is depicted in Fig. 11. As it can be seen in the diagram, to implement the observer inputs, outputs and control signal of secondary control loop in needed. Since all the mentioned signals are available in the PMCU computer, to implement the algorithm no supplementary infrastructure is required.

The proposed method can be applied to large scale systems by obtaining its equivalent in the form of Fig. 4 i.e. the one-bus topology. This transformation can be performed by applying superposition theorem and using Thevenin equivalent simultaneously.

Furthermore, the robustness of observer to model uncertainty can be guaranteed by transforming the uncertainty to disturbance. The approach of this transformation is given in [41]. Regarding this disturbance in the design of PUID detector, we can claim that the algorithm is stable and robust to model uncertainty.

To evaluate the approach, a real MG is implemented in Power System Computer Aided Designer (PSCAD) which is a professional and practical simulator for power systems. The results of PSCAD simulation are depicted in dashed red lines, while those of mathematical model are shown in blue lines in Figs. 5–10. Comparing the results, it can be seen that the approach has perfectly performed in a real system. In addition, noise effect on residue with different variances mentioned in Table 2 is considered in the dynamic model simulations. As it can be seen the effect of noise on the residue is only some fluctuations in the residue signal, thanks to using a Butterworth filter on the observer inputs with cut-off frequency of 30 rad/s.

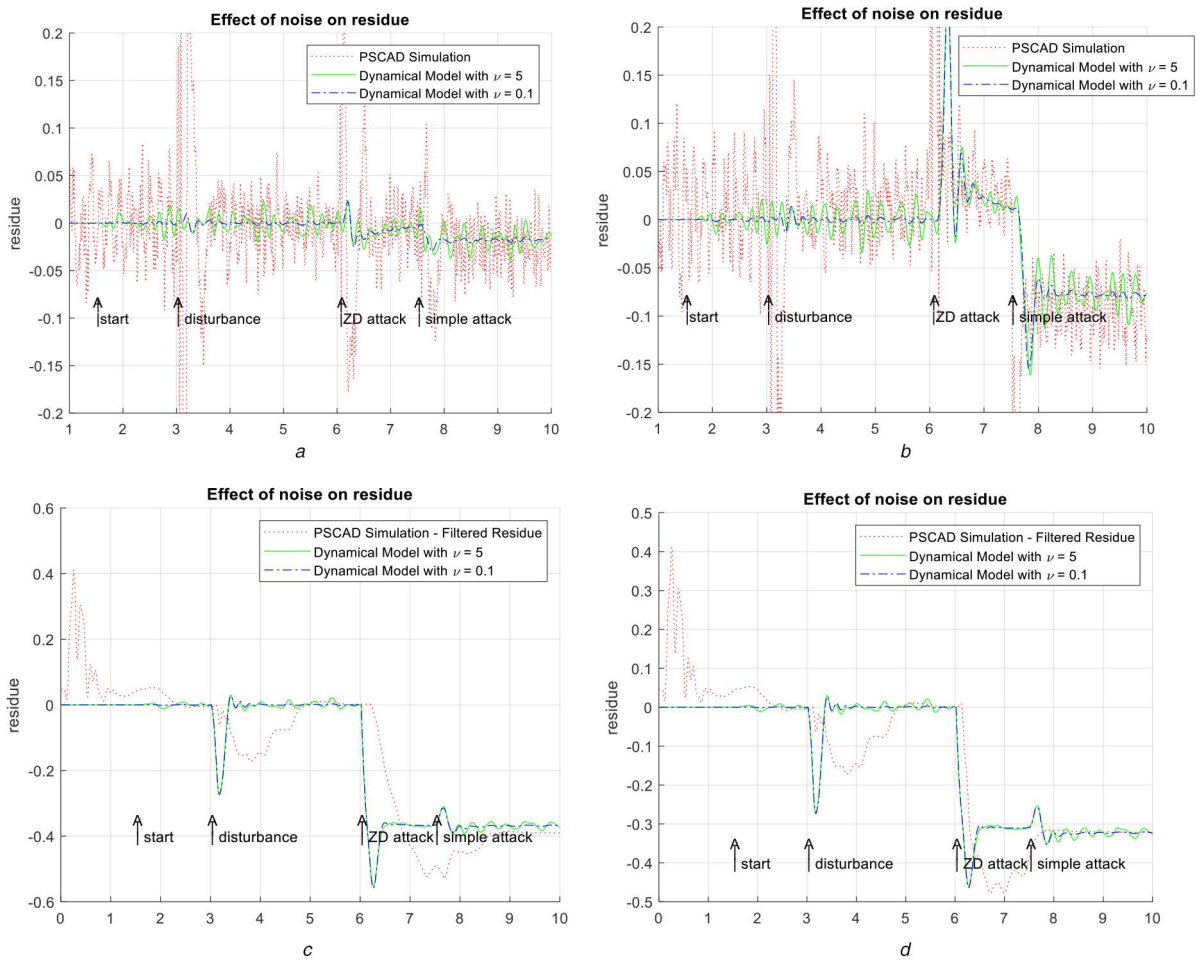

Fig. 10 *Derived observer's residue of system*

(a) Setpoint zero dynamic attack in open loop system, ***(b)*** Sensor zero dynamic attack in open loop system, ***(c)*** Setpoint zero dynamic attack in closed loop system-filtered, ***(d)*** Feedback zero dynamic attack in closed loop system-filtered

Table 1 Parameter values of secondary loop controller

Parameter	Value	Unit
$K_{\mathrm{P},i}\ i=1,2,3$	1.04×10^{-4}	—
$K_{\mathrm{I},i}\ i=1,2,3$	1.9681	$1/s$

$i=1$: AC voltage secondary loop controller.

$i=2$: AC frequency secondary loop controller.

$i=3$: DC voltage secondary loop controller.

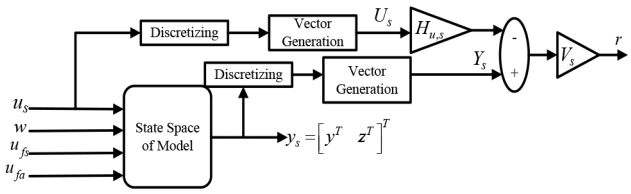

Fig. 11 *Implementation of simulation in MATLAB*

7 Conclusion

This article has used a closed loop dynamic of droop-controlled hybrid MG to mitigate and detect zero dynamic FDIA. FDIAs are modelled by a mismatch between the sent and received data between DRs and PMCU. Four types of zero dynamic attacks are discussed in this article: setpoint and sensor attack in an open loop system and setpoint and feedback attack in a closed loop system. Setpoint commands of system are AC and DC voltage setpoints and also frequency of AC side which are sent from PMCU to DRs.

To mitigate zero dynamic attack, control signal of closed loop system is used in addition to inputs and outputs of the system. These signals are applied to the parity space detector for decoupling of cyber-attack from disturbances. It can be seen that although the parity space fault detection approach is unable to detect zero dynamic attack in the open loop system, it has worked perfectly for the closed loop system using control signals. To prevent closed loop system identification by the attacker, it is suggested to change the PI coefficients of secondary control loop periodically.

7.1 Comparison with other methods

Although there are two other methods of detecting zero dynamic attack in the literature, none of them is applicable for this case. One of them needs a large number of outputs for the model to achieve the goal, and another which uses a scaling matrix can be identified

Table 2 Noise variance of state variables

Variable	Variance	Unit
v_{ac}	1ν	V
f	0.01ν	Hz
v_{dc}	1ν	V
$\hat{i}_i^*,\ i=1,2$	1ν	A
$v_i,\ i=1,2$	1ν	V
$\delta_i,\ i=1,2$	0.002ν	rad
$i_{o,i,\mathrm{dc}},\ i=1,2$	0.1ν	A
$P_{ex}\ P_{ex}^*$	1ν	W

Here $\nu = [0.1, 5]$.

by the attacker easily. The proposed method in this article does not only have any implementation difficulties, but also it would not be identified by the attacker. The algorithm can be implemented in the PMCU computer. Since the inputs, outputs and control signals of the system are all available in the computer, no transfer of supplementary data via communication link is needed.

In comparison with other model-based observers, since the parity approach calculates the algebraic equation (18), its speed of calculation and process is relatively high. This is while other observers need to solve differential equations; hence their solving methods are more complex than parity.

8 References

[1] Zhong, X., Yu, L., Brooks, R., *et al.*: 'Cyber security in smart dc microgrid operations'. Int. Conf. DC Microgrids (ICDCM), Atlanta, GA, 2015, pp. 86–91

[2] Singh, R., Shenai, K.: 'DC microgrids and the virtues of local electricity', Available at http://spectrum.ieee.org/green-tech/buildings/dc-microgrids-and-the-virtues-of-local-electrcity

[3] Guerrero, J.M., Vasquez, J.C., Matas, J., *et al.*: 'Hierarchical control of droop-controlled AC and DC microgrids – a general approach toward standardization', *IEEE Trans. Ind. Electron.*, 2011, **58**, (1), pp. 158–172

[4] Afshar, A., Termehchy, A., Golshan, A., *et al.*: 'Survey on cyber security of industrial control systems', *Iran. Soc. Instrum. Control Eng.*, 2014, **8**, (1), pp. 31–45

[5] Sridhar, S., Manimaran, G.: 'Data integrity attacks and their impacts on SCADA control system'. IEEE PES General Meeting, Minneapolis, MN, 2010

[6] Andress, J.: '*The basics of information security: understanding the fundamentals of infosec in theory and practice*' (Elsevier Science, Steven Winterfeld, Ed. Waltham, USA, 2014, 2nd edn.) p. 5

[7] Rasoolzadeh, A., Rajaei Salmasi, F.: 'Reduced-order dynamic model for droop-controlled inverter/converter-based low-voltage hybrid AC/DC microgrids – part 1: AC sub-microgrid', *IET Smart Grid*, 2018, **1**, (4), pp. 123–133

[8] Rasoolzadeh, A., Rajaei Salmasi, F.: 'Reduced-order dynamic model for droop-controlled inverter/converter-based low-voltage hybrid AC/DC microgrids – part 2: DC sub-microgrid and power exchange', *IET Smart Grid*, 2018, **1**, (4), pp. 134–142

[9] Wu, G., Sun, J., Chen, J.: 'A survey on the security of cyber-physical systems', *Control Theory Technol.*, 2016, **14**, (1), pp. 2–10

[10] Sabaliauskaite, G., Mathur, A.P.: 'Intelligent checkers to improve attack detection in cyber physical systems'. Int. Conf. on Cyber-Enabled Distributed Computing and Knowledge Discovery, Beijing, People's Republic of China, 2013, pp. 27–30

[11] Pasqualetti, F., Dörfler, F., Bullo, F.: 'Attack detection and identification in cyber-physical systems', *IEEE Trans. Autom. Control*, 2013, **58**, (11), pp. 2715–2729

[12] Mo, Y., Chabukswar, R., Sinopoli, B.: 'Detecting integrity attacks on SCADA systems', *IEEE Trans. Control Syst. Technol.*, 2013, **22**, (4), pp. 1396–1407

[13] Tang, B., Alvergue, L.D., Gu, G.: 'Secure networked control systems against replay attacks without injecting authentication noise'. Am. Control Conf., Chicago, IL, USA, 2015, pp. 6028–6033

[14] Miao, F., Pajic, M., Pappas, G.J.: 'Stochastic game approach for replay attack detection'. IEEE Conf. Decision Control, Florence, Italy, 2013, pp. 1854–1859

[15] Mo, Y., Garone, E., Casavola, A., *et al.*: 'False data injection attacks against state estimation in wireless'. IEEE Conf. Decision Control, Atlanta, GA, USA, 2010, pp. 5967–5972

[16] Bishop, A.N., Savkin, A.V.: 'Set-valued state estimation and attack detection for uncertain descriptor systems', *IEEE Signal Process. Lett.*, 2013, **20**, (11), pp. 1102–1105

[17] Esmalifalak, M., Shi, G., Han, Z., *et al.*: 'Bad data injection attack and defense in electricity market using game theory study', *IEEE Trans Smart Grid*, 2013, **4**, (1), pp. 160–169

[18] Mo, Y., Hespanha, J.P., Sinopoli, B.: 'Resilient detection in the presence of integrity attacks', *IEEE Trans. Signal Process.*, 2014, **62**, (1), pp. 31–43

[19] Ntalampiras, S.: 'Detection of integrity attacks in cyber-physical critical infrastructures using ensemble modeling', *IEEE Trans. Ind. Inf.*, 2015, **11**, (1), pp. 104–111

[20] Teixeira, A., Sandberg, H., Johansson, K.H.: 'Networked control systems under cyber attacks with applications to power networks'. Am. Control Conf., Marriott Waterfront, Baltimore, MD, USA, 2010, pp. 3690–3696

[21] Kim, T.T., Poor, H.V.: 'Strategic protection against data injection attacks on power grids', *IEEE Trans Smart Grid*, 2011, **2**, (2), pp. 326–333

[22] Liu, L., Esmalifalak, M., Han, Z.: 'Detection of false data injection in power grid exploiting low rank and sparsity'. Int. Conf. Commun., Budapest, Hungary, 2013, pp. 4461–4465

[23] Liu, L., Esmalifalak, M., Ding, Q., *et al.*: 'Detecting false data injection attacks on power grid by sparse optimization', *IEEE Trans Smart Grid*, 2014, **5**, (2), pp. 612–621

[24] Zonouz, S., *et al.*: 'SCPSE: security-oriented cyber-physical state estimation for power grid critical infrastructures', *IEEE Trans Smart Grid*, 2012, **3**, (4), pp. 1790–1799

[25] Nudell, T.R., Chakrabortty, A.: 'A graph-theoretic algorithm for disturbance localization in large'. Am. Control Conf., Washington, DC, 2013

[26] Bobba, R.B., *et al.*: 'Detecting false data injection attacks on dc state estimation'. Workshop on Secure Control Sys. (SCS), Stockholm, Sweden, 2010

[27] Pasqualetti, F., Carli, R., Bullo, F.: 'A distributed method for state estimation and false data detection in power networks'. Int. Conf. Smart Grid Commun., Brussels, 2011

[28] Liu, Y., Ning, P., Reiter, M.K.: 'False data injection attacks against state estimation in electric power grids'. Association for Computing Machinery, Chicago, Illinois, 2009

[29] Kosut, O., Jia, L., Thomas, R.J., *et al.*: 'Malicious data attacks on smart grid state estimation: attack strategies and countermeasures'. Int. Conf. Smart Grid Commun., Gaithersburg, MD, 2010

[30] Vukovic, O., Sou, K.C., Dan, G., *et al.*: 'Network-layer protection schemes against stealth attacks on state estimators in power systems'. IEEE Smart Grid Commun., Brussels, Belgium, 2011

[31] Sou, K.C., Sandberg, H., Johansson, K.H.: 'Detection and identification of data attacks in power system'. Am. Control Conf., Montréal, Canada, 2012

[32] Sandberg, H., Teixeira, A., Johansson, K.H.: 'On security indices for state estimators in power networks'. First Workshop on Secure Control Syst. (SCS), Stockholm, 2010

[33] Calderaro, V., Hadjicostis, C.N., Piccolo, A., *et al.*: 'Failure identification in smart grids based on Petri net modeling', *IEEE Trans. Ind. Electron.*, 2011, **58**, (10), pp. 4613–4623

[34] Beg, O.A., Johnson, T.T., Davoudi, A.: 'Detection of false-data injection attacks in cyber-physical dc microgrids', *IEEE Trans. Ind. Inf.*, 2017, **13**, (5), pp. 2693–2703

[35] Beg, O.A., Nguyen, L.V., Johnson, T.T., *et al.*: 'Signal temporal logic-based attack detection in DC microgrids', *IEEE Trans Smart Grid*, 2019, **10**, (4), pp. 3585–3595

[36] Gallo, A.J., *et al.*: 'Distributed cyber-attack detection in the secondary control of DC microgrids'. Eur. Control Conf., Limassol, Cyprus, 2018

[37] Sahoo, S., Mishra, S., Peng, J.C.H., *et al.*: 'A stealth cyber attack detection strategy for DC microgrids', *IEEE Trans. Power Electron.*, 2019, **34**, (8), pp. 8162–8174

[38] Chen, Y., Kar, S., Moura, J. M. F.: 'Dynamic attack detection in cyber-physical systems with side initial state information', *IEEE Trans. Autom. Control*, 2017, **62**, (9), pp. 4618–4624

[39] Hoehn, A., Zhang, P.: 'Detection of covert attacks and zero dynamics attacks in cyber-physical systems'. Am. Control Conf. (ACC), Boston, MA, USA, 2016

[40] Nejabatkhah, F., Li, Y.W.: 'Overview of power management strategies of hybrid AC/DC microgrids', *IEEE Trans. Power Electron.*, 2015, **30**, (12), pp. 7072–7089

[41] Ding, S.X.: '*Model-based fault diagnosis techniques*' (Springer Verlag, Berlin Heidelberg, 2008)

[42] Teixeira, A., Pérez, D., Sandberg, P., *et al.*: 'Attack models and scenarios for networked control systems'. Int. Conf. on High Confidence Networked Syst., Beijing, China, 2012, pp. 55–64

9 Appendix: Parity space [41]

9.1 Introduction to parity space

Parity space is one of the model-based approaches of generating residual for fault detection. In this approach, the residual should be designed such that it is not dependent on disturbance and initial condition of the system, but it is sensitive to a specified fault in the system. In parity method, the system should be transformed to a discrete system. By determining the vector of inputs and outputs, fault detection can be done. In this method, to have a perfect decupling between disturbance and fault, the pair (A, C) should be observable. Also the number of discretised input and output series should not be less than the degree of system.

The parity approach is based on the logic of finding a matrix form filter such that the disturbance vector is in the null space of it but fault vector is not in its null space.

If the discretised system has the form

$$\begin{cases} x(k+1) = \boldsymbol{A}x(k) + \boldsymbol{B}\boldsymbol{u}_{\mathrm{s}}(k) + \boldsymbol{E}_{\mathrm{d}}w(k) + \boldsymbol{E}_{\mathrm{f}}\boldsymbol{u}_{\mathrm{f}}(k) \\ y_{\mathrm{s}}(k) = \boldsymbol{C}x(k) + \boldsymbol{D}\boldsymbol{u}_{\mathrm{s}}(k) + \boldsymbol{F}_{\mathrm{d}}w(k) + \boldsymbol{F}_{\mathrm{f}}\boldsymbol{u}_{\mathrm{f}}(k) \end{cases}$$

by supposing no fault and disturbance the following series in time can be formed for the outputs:

$$\begin{aligned} y_{\mathrm{s}}(k-s) &= \boldsymbol{C}x(k-s) + \boldsymbol{D}\boldsymbol{u}_{\mathrm{s}}(k-s) \\ y_{\mathrm{s}}(k-s+1) &= \boldsymbol{C}x(k-s+1) + \boldsymbol{D}\boldsymbol{u}_{\mathrm{s}}(k-s+1) \\ &= \boldsymbol{CA}x(k-s) + \boldsymbol{CB}\boldsymbol{u}_{\mathrm{s}}(k-s) + \boldsymbol{D}\boldsymbol{u}_{\mathrm{s}}(k-s+1) \\ y_{\mathrm{s}}(k-s+2) &= \boldsymbol{CA}^2x(k-s) + \boldsymbol{CAB}\boldsymbol{u}_{\mathrm{s}}(k-s) \\ &\quad + \boldsymbol{CB}\boldsymbol{u}_{\mathrm{s}}(k-s+1) + \boldsymbol{D}\boldsymbol{u}_{\mathrm{s}}(k-s+2) \\ &\vdots \\ y_{\mathrm{s}}(k) &= \boldsymbol{CA}^s x(k-s) + \boldsymbol{CA}^{s-1}\boldsymbol{B}\boldsymbol{u}_{\mathrm{s}}(k-s) \\ &\quad + \cdots + \boldsymbol{CB}\boldsymbol{u}_{\mathrm{s}}(k-1) + \boldsymbol{D}\boldsymbol{u}_{\mathrm{s}}(k) \end{aligned}$$

This series can be shown in matrix form by

$$Y_{\mathrm{s}}(k) = H_{\mathrm{o,s}}x(k-s) + H_{\mathrm{u,s}}U_{\mathrm{s}}(k)$$

in which

$$Y_{\mathrm{s}}(k) = \begin{bmatrix} y_{\mathrm{s}}(k-s) \\ y_{\mathrm{s}}(k-s+1) \\ \vdots \\ y_{\mathrm{s}}(k) \end{bmatrix}, \quad U_{\mathrm{s}}(k) = \begin{bmatrix} u_{\mathrm{s}}(k-s) \\ u_{\mathrm{s}}(k-s+1) \\ \vdots \\ u_{\mathrm{s}}(k) \end{bmatrix}$$

$$H_{\mathrm{o,s}} = \begin{bmatrix} \boldsymbol{C} \\ \boldsymbol{CA} \\ \vdots \\ \boldsymbol{CA}^s \end{bmatrix}, \quad H_{\mathrm{u,s}} = \begin{bmatrix} \boldsymbol{D} & 0 & \cdots & 0 \\ \boldsymbol{CB} & \boldsymbol{D} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ \boldsymbol{CA}^{s-1}\boldsymbol{B} & \cdots & \boldsymbol{CB} & \boldsymbol{D} \end{bmatrix}$$

By choosing $v_{\mathrm{s}} \in R^{(n+1)m}$ in the left null space of $H_{\mathrm{o,s}}$, we have $v_{\mathrm{s}}H_{\mathrm{o,s}} = 0$, thus

$$r(k) = v_{\mathrm{s}}(Y_{\mathrm{s}}(k) - H_{\mathrm{u,s}}U_{\mathrm{s}}(k)) = v_{\mathrm{s}}H_{\mathrm{o,s}}x(k-s) = 0$$

All the vectors that have the mentioned characteristics form a parity space, and each of them is named by a parity vector $P_{\mathrm{s}} = \{v_{\mathrm{s}} | v_{\mathrm{s}}H_{\mathrm{o,s}} = 0\}$.

9.2 Parity space observer

If disturbance and fault vectors are regarded in equations, the output vector has the form

$$Y_{\mathrm{s}}(k) = H_{\mathrm{o,s}}x(k-s) + H_{\mathrm{u,s}}U_{\mathrm{s}}(k) + H_{\mathrm{f,s}}U_{\mathrm{f,s}}(k) + H_{\mathrm{d,s}}W_{\mathrm{s}}(k)$$

in which

$$U_{\mathrm{f,s}}(k) = \begin{bmatrix} u_{\mathrm{f}}(k-s) \\ u_{\mathrm{f}}(k-s+1) \\ \vdots \\ u_{\mathrm{f}}(k) \end{bmatrix}, \quad W_{\mathrm{s}}(k) = \begin{bmatrix} w(k-s) \\ w(k-s+1) \\ \vdots \\ w(k) \end{bmatrix}$$

$$H_{\mathrm{f,s}} = \begin{bmatrix} \boldsymbol{F}_{\mathrm{f}} & 0 & \cdots & 0 \\ \boldsymbol{CE}_{\mathrm{f}} & \boldsymbol{F}_{\mathrm{f}} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ \boldsymbol{CA}^{s-1}\boldsymbol{E}_{\mathrm{f}} & \cdots & \boldsymbol{CE}_{\mathrm{f}} & \boldsymbol{F}_{\mathrm{f}} \end{bmatrix},$$

$$H_{\mathrm{d,s}} = \begin{bmatrix} \boldsymbol{F}_{\mathrm{d}} & 0 & \cdots & 0 \\ \boldsymbol{CE}_{\mathrm{d}} & \boldsymbol{F}_{\mathrm{d}} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ \boldsymbol{CA}^{s-1}\boldsymbol{E}_{\mathrm{d}} & \cdots & \boldsymbol{CE}_{\mathrm{d}} & \boldsymbol{F}_{\mathrm{d}} \end{bmatrix}$$

If $v_{\mathrm{s}} \in P_{\mathrm{s}}$ is selected such that $v_{\mathrm{s}}H_{\mathrm{f,s}} \neq 0$ and $v_{\mathrm{s}}H_{\mathrm{d,s}} = 0$ then

$$r(k) = v_{\mathrm{s}}(Y_{\mathrm{s}}(k) - H_{\mathrm{u,s}}U_{\mathrm{s}}(k)) = v_{\mathrm{s}}H_{\mathrm{f,s}}U_{\mathrm{f,s}}(k)$$

in which residual depends only on fault, and neither disturbances nor zero state of system affects the residue.