Cyber–physical attacks on power distribution systems

Abdelrahman Ayad1, Hany Farag2, Amr Youssef3, Ehab El-Saadany4

1Electrical and Computer Engineering Department, University of Waterloo, Waterloo, ON, Canada
2Department of Electrical Engineering and Computer Science, York University, ON, Canada
3Concordia Institute for Information Systems Engineering, Concordia University, Montreal, QC, Canada
4Advanced Power and Energy Center, EECS Department, Khalifa University, Abu Dhabi, UAE

Abstract: This study investigates the impacts of stealthy false data injection (FDI) attacks that corrupt the state estimation operation of power distribution systems (PDS). In particular, the authors analyse FDI attacks that target the integrity of distribution systems optimal power flow (DSOPF) in order to maximise the system operator losses. The branch current state estimation method is implemented to accurately model the PDS, and convex relaxations are applied to the DSOPF model. The effects of the FDI attacks are analysed on the IEEE 34-bus unbalanced radial distribution system, with distributed energy resources (DERs) along the feeder. A 24 h DSOPF is performed, and the results depict the changes in the voltage profile and the additional power injection from the DERs, which consequently lead to the increase of the DSOPF cost.

Nomenclature

Constants

- $\delta_i^-$, $\delta_i^+$: lower and upper bounds of attacked power injection at bus $i$, respectively, pu
- $s_{g,i}$: lower and upper bounds of power injection at bus $i$, respectively, pu
- $V_{g,v}$, $V_l$: lower and upper bounds of voltage magnitude at bus $i$, respectively, pu
- $a_{g,1}$, $a_{g,2}$: parameters of DERs cost function, respectively, ($/kWh$), ($$/kWh^2$$)
- $P_{G,max}$, $Q_{G,max}$: power rating of the DER unit, pu
- $S_{G,max}$: MVA rating of the DER unit, pu
- $V_0$: voltage at reference bus, pu
- $y_i$: shunt capacitance bus $i$, pu
- $z_{ij}$: impedance between buses $i, j$, pu

Vectors

- $\hat{x}$: estimated system states vector
- $I_{\phi}^{\text{re}}, I_{\phi}^{\text{im}}$: measured real and imaginary vectors for the branch currents of phase $\phi$, respectively, pu
- $P^{\text{re}}, Q^{\text{im}}$: measured power vector of phase $\phi$
- $V_{\phi}^i$: voltage magnitude vector of phase $\phi$, pu
- $x$: system states vector
- $z$: power flow measurements vector

Indices

- $i$: index for attacked buses
- $\phi$: index for electrical power phases
- $g$: index of DER buses
- $i, j, n$: indices for buses

Sets

- $\mathcal{N}$: set of buses in the test system
- $\mathcal{N}_d$: set of attacked buses in the test system

Variables

- $\theta_j$: voltage phase angle at bus $j$, rad
- $I_{ij}$: branch current between nodes $i$ and $j$, pu
- $I_{ij}^{-}$: slack variable of branch current between buses $i$ and $j$, pu
- $P_j$: power at bus $j$, pu
- $Q_j$: reactive power at bus $j$, pu
- $S_j$: power injection at bus $j$, pu
- $\delta_j$: slack variable of power flow between buses $i$ and $j$, pu
- $V_j$: voltage magnitude at bus $j$, pu
- $V_{\phi j}$: slack variable of voltage magnitude at bus $j$, pu

1 Introduction

Cyber–physical security presents a major challenge for the continuously evolving smart grids. The communication layer is a main component of the modern power networks, as it is essential in monitoring the grid state and coordinating different control signals. Concerning power distribution systems (PDS), the main driving force for the progressive transformation of the network is the large-scale integration of distributed energy resources (DERs), including renewable energy resources, with the aim of a more sustainable and cleaner energy systems [1]. Towards achieving these aspirations, many transformations have been recently occurring, among these the most prominent are: introduction of communication in control and monitoring; implementation of distributed volt/Var control (VVC) strategies [2]; deployment of digital field metres and Phasor Measurement Units (PMUs) [3]; and increasing the number of microgrids and high share of renewable energy sources [1].

Due to the distinctive features of PDS, several dedicated research works have developed specific techniques of state estimation (SE), commonly referred to as distribution systems state estimation (DSSE) tailored to fit the specific needs of distribution networks. The most known and used class of DSSE algorithms is based on the weighted least squares (WLS) method, where system states can be voltage nodes [4] or branch currents [5]. For radial PDS characterised by high imbalance ratio, the branch current state estimation (BCSE) model, based on WLS, is more suitable than node voltages [6], as its computation efficiency allows better...
measurements. The most common technique utilised for this unbalanced radial configuration of the networks. However, the essential component of demand-side management programmes is utilised to send and receive real-time data between digital field nodes [35] and the PDS becomes vulnerable to cyber–physical attacks, which is the attack model considered in this work.

Table 1

| Attack type                        | Contribution                     | Algorithm description | Remarks |
|-----------------------------------|----------------------------------|-----------------------|---------|
| falsifying voltage measurements   | mitigation                       | sequential check      | does not consider BDD in SE when constructing the attacks |
| with PV injection nodes           | algorithm                        | of nodal voltage      |         |
| data integrity attack             | stealthy attacks                 | by corruption set     |         |
| attacks [36]                      | algorithm                        | of measurements      |         |
| FDI against approximated DSSE     | attack                            | based on local FDI    |         |
| [34]                              | algorithm                        | states                |         |
| attacks against leverage          | detection                         | identification and    |         |
| measurements [37]                 | algorithm                        | separation of        |         |
| malicious attacks on DERs [38]    | mitigation                       | probabilistic VVC     |         |
|                                   | algorithm                        | optimisation strategy |         |
|                                   |                                  | and forecast aided    |         |
|                                   |                                  | approaches            |         |

In practice, FDI attacks can take place on the communication layer or physical layer by: (i) breaking into substations’ local area networks (LANs): as reported in [25, 26], and as exemplified in practice by the real cyber attacks that sabotaged the Ukrainian power network in 2016 [27], a substation’s LAN is vulnerable to cyber intrusions. This weakness is mainly due to the vulnerability of the communication protocols used in substations, e.g. IEC 61850 [28–30]. (ii) Spoofing substations’ global positioning system (GPS): in this type of attack, the original GPS signal is overwhelmed using the noise of the same frequency, and a counterfeit GPS signal is transmitted instead [31, 32]. This attack can also be carried out by targeting synchronisation protocols [31, 33]. (iii) Breaching the communication link between field devices: currently, a wide range of communication media – e.g. microwaves, radio waves, and wireless communications – is used for sharing remote measurements. If attackers can breach this link, they can manipulate measurements and launch FDI attacks.

Most of the research work in the area of cyber–physical security, however, focused on transmission systems, consequently many of the assumptions made for attacks formulation and detection algorithms do not hold for PDS [3]. In addition, the analysis of the SE and Bad Data Detector (BDD) is usually implemented on the DC power flow, a linear version of the AC power flow. This simplification is acceptable at the transmission level, but it does not suit PDS. For the SE procedure, voltage magnitudes and angles are usually chosen as system states. In particular, regarding the FDI attacks, Liu et al. used the DC power flow to investigate these attacks on the power networks, while Deng et al. [34] were among the first to investigate the FDI attacks on the PDS level. The analysis of attacks was based on the assumption of a single-phase system, with local measurements and single points of attacks and without VVC devices, such as line voltage regulators or shunt capacitors. Table 1 summarises some of the recent work regarding the cyber–physical security on the PDS level.

The literature classifies defense strategies against FDI attacks into protection-based approaches and detection-based approaches [39]. Protection-based approaches depend on protecting measurements of certain sensors from being attacked [40]. The realisation of these approaches depends on the determination of minimal set of measurements needed for protection. However, these approaches cause a drop in measurements redundancy and do not formally guarantee the effectiveness under varying operating conditions [41]. In contrast, the detection-based approaches use the Bayesian framework to detect the attack [42]. The objective of these methods is to detect any anomaly, or abnormal measurements. One general drawback of these methods is the inability of detecting anomalies that fit the historical distribution of the data [41]. Protection strategies may not be directly applicable to PDS since the number of digital field metres is not enough to provide redundancy of measurements [6], and detection strategies are difficult to develop as measurements are not always available [8].

1.2 Motivations and contributions

Motivated by the mentioned research gap, this paper builds on previous works and investigates the effects of FDI attacks that target unbalanced PDS with radial topologies. In particular, the main contributions of this paper are as follows:

i. Formulation of FDI attacks on a radial three-phase unbalanced PDS with DERs using the BCSE. The presented approach differs from the traditional nodal voltage-based approaches in the choice of branch currents as system states, in contrast to converging. Another class of DSSE is dynamic SE, in which recursive estimations are based on consecutive snapshot measurements. The most common technique utilised for this approach is the iterated Kalman filter method [7].

The non-linear nature of the optimal power flow (OPF) problem makes it difficult to obtain accurate results, especially for distribution systems OPF (DSOPF), as many of the OPF approaches on transmission level are not suitable for optimal operation on the PDS level [8]. A subset of OPF formulations has been tailored to better suit the nature of the PDS, and is known as DSOPF [9, 10]. The DSOPF is an integral part of the PDS, which is used to efficiently optimise the operation of the distribution network. The complexity of DSOPF arises from the three phases, unbalanced radial configuration of the networks. However, the majority of research work assumes a single-phase model, based on the assumption that multi-phase networks can be rendered into equivalent single-phase networks, which does not capture the details of the PDS topologies [11]. A subset of OPF formulations has been tailored to better suit the nature of the PDS, and is known as DSOPF [9, 10]. The DSOPF is an integral part of the PDS, which is used to efficiently optimise the operation of the distribution network. The complexity of DSOPF arises from the three phases, unbalanced radial configuration of the networks. However, the majority of research work assumes a single-phase model, based on the assumption that multi-phase networks can be rendered into equivalent single-phase networks, which does not capture the details of the PDS topologies [11].

Convex relaxation is used to render the DSOPF into a convex problem. Gan and Low [12] proposed semi-definite programming (SDP) convex relaxation and a linear separation of measurements needed for protection. However, these methods is to detect any anomaly, or abnormal measurements. One general drawback of these methods is the inability of detecting anomalies that fit the historical distribution of the data [41]. Protection strategies may not be directly applicable to PDS since the number of digital field metres is not enough to provide redundancy of measurements [6], and detection strategies are difficult to develop as measurements are not always available [8].

1.1 Related works

Malicious cyber–physical attacks can have severe impacts ranging from economical effects to partial malfunctioning of equipment and sub-systems, all the way to cascading failures and shut-down of entire power systems [21, 22]. These attacks can target both the cyber part, which consists of the communication and software layer, and the physical part, which consists of the electrical power devices and equipment [23]. Common attack templates include, but not limited to, man in the middle attacks [24], rogue devices attacks [3], denial of service attacks [18], and false data injection (FDI) attacks [3], which is the attack model considered in this work.

Table 1 Related cyber–physical security work on PDS

| Attack type                        | Contribution                     | Algorithm description | Remarks |
|-----------------------------------|----------------------------------|-----------------------|---------|
| falsifying voltage measurements   | mitigation                       | sequential check      | does not consider BDD in SE when constructing the attacks |
| with PV injection nodes           | algorithm                        | of nodal voltage      |         |
| data integrity attack             | stealthy attacks                 | by corruption set     |         |
| attacks [36]                      | algorithm                        | of measurements      |         |
| FDI against approximated DSSE     | attack                            | based on local FDI    |         |
| [34]                              | algorithm                        | states                |         |
| attacks against leverage          | detection                         | identification and    |         |
| measurements [37]                 | algorithm                        | separation of        |         |
| malicious attacks on DERs [38]    | mitigation                       | probabilistic VVC     |         |
|                                   | algorithm                        | optimisation strategy |         |
|                                   |                                  | and forecast aided    |         |
|                                   |                                  | approaches            |         |

Convergence. Another class of DSSE is dynamic SE, in which recursive estimations are based on consecutive snapshot measurements. The most common technique utilised for this approach is the iterated Kalman filter method [7].

The non-linear nature of the optimal power flow (OPF) problem makes it difficult to obtain accurate results, especially for distribution systems OPF (DSOPF), as many of the OPF approaches on transmission level are not suitable for optimal operation on the PDS level [8]. A subset of OPF formulations has been tailored to better suit the nature of the PDS, and is known as DSOPF [9, 10]. The DSOPF is an integral part of the PDS, which is used to efficiently optimise the operation of the distribution network. The complexity of DSOPF arises from the three phases, unbalanced radial configuration of the networks. However, the majority of research work assumes a single-phase model, based on the assumption that multi-phase networks can be rendered into equivalent single-phase networks, which does not capture the details of the PDS topologies [11].

Formulation of FDI attacks on a radial three-phase unbalanced power flow. This simplification is acceptable at the transmission level, but it does not suit PDS. For the SE procedure, voltage magnitudes and angles are usually chosen as system states. In particular, regarding the FDI attacks, Liu et al. used the DC power flow to investigate these attacks on the power networks, while Deng et al. [34] were among the first to investigate the FDI attacks on the PDS level. The analysis of attacks was based on the assumption of a single-phase system, with local measurements and single points of attacks and without VVC devices, such as line voltage regulators or shunt capacitors. Table 1 summarises some of the recent work regarding the cyber–physical security on the PDS level.

The literature classifies defense strategies against FDI attacks into protection-based approaches and detection-based approaches [39]. Protection-based approaches depend on protecting measurements of certain sensors from being attacked [40]. The realisation of these approaches depends on the determination of minimal set of measurements needed for protection. However, these approaches cause a drop in measurements redundancy and do not formally guarantee the effectiveness under varying operating conditions [41]. In contrast, the detection-based approaches use the Bayesian framework to detect the attack [42]. The objective of these methods is to detect any anomaly, or abnormal measurements. One general drawback of these methods is the inability of detecting anomalies that fit the historical distribution of the data [41]. Protection strategies may not be directly applicable to PDS since the number of digital field metres is not enough to provide redundancy of measurements [6], and detection strategies are difficult to develop as measurements are not always available [8].

1.2 Motivations and contributions

Motivated by the mentioned research gap, this paper builds on previous works and investigates the effects of FDI attacks that target unbalanced PDS with radial topologies. In particular, the main contributions of this paper are as follows:

i. Formulation of FDI attacks on a radial three-phase unbalanced PDS with DERs using the BCSE. The presented approach differs from the traditional nodal voltage-based approaches in the choice of branch currents as system states, in contrast to
conventional voltage node methods, as they better fit the PDS topologies, and thus permit a more accurate representation of the system.

ii. Incorporation of the FDI attacks in the DSOPF to select injection values in order to maximise the cost function represented by the power injection of DERs without being detected by the BDD. To generate cases of attack scenarios, attack vectors are generated based on an optimisation model to create maximum losses.

The remainder of this paper is organised as follows: Section 2 reviews the DSSE operation and formulates the BCSE to be incorporated in the attacks model. Also, the DSOPF based on the SDP relaxation formulation is presented. Section 3 presents the FDI attacks based on the BCSE model. Section 4 analyses the optimal FDI attack strategy to corrupt the DSOPF operation. Section 5 presents the case study of the attacks effect on the IEEE-34 bus unbalanced system. Finally, Section 6 presents the conclusion and future work.

2 Power distribution systems

This section provides the overview of the PDS main operation structure related to this work, in addition to the necessary background on the DSSE and DSOPF. A simplified version of a distribution management system (DMS) is represented in Fig. 1, showing a high-level overview of DSSE and DSOPF operations. The DMS processes the measurements, both field and pseudo measurements, to acquire the state of the system and take any necessary control action. The output of the DSSE is passed to the BDD, and if the residue test flags bad or corrupted measurements, the BDD alarm is activated and the PDS operator is alerted. Otherwise, the system states are passed to the DSOPF and finally the optimal solutions are utilised by the system operator. By investigating the internal details of the DMS operations, we are able to consider cyber–physical threats, such as FDI attacks, that can target the DMS.

2.1 Distribution systems state estimation

Distribution system operators rely on the DSSE process to acquire knowledge of the different system states such as node voltages or branch currents. The measurements in PDS can be classified as field measurements received by field metering devices, in addition to pseudo measurements, which are required to overcome measurements data deficiency and ensure system observability [43]. The AC power flow measurement model is described by

$$ z = h(x) + e $$

where \( z \) is the power flow measurements vector, \( x \) is the state variables vector, and \( e \) is the measurements error vector. The BCSE model is used for SE in PDS, as it is more accurate and is more efficient for the SE iterative procedure in radial systems [44]. In contrast with other works, which used voltage node-based DSSE, the usage of BCSE allows the decoupling of the phases in unbalanced systems. Therefore, the attack vectors will be constructed for each phase separately. Branch currents are determined from the real and reactive power flow measurements as follows:

$$ I_{re}^\phi + jI_{im}^\phi = \left( \frac{P^{\phi,i} + jQ^{\phi,i}}{V_\phi^i} \right)^* $$

where \( P^{\phi,i} \) and \( Q^{\phi,i} \) are the real and imaginary components of the branch currents, respectively, with the superscript \( m \) indicating a measured quantity from field devices. Real and reactive power measurements are represented by \( P^{\phi,i} \) and \( Q^{\phi,i} \), respectively, and \( V_\phi^i \) is the node voltage, for each phase \( \phi \), and the * is the conjugate operator. The measurement function \( h(x) \) maps the measurement effects on the system states vector \( x \), and thus it reveals which measurements to be altered in order to change a given state. The mapping function of the current measurement is represented by

$$ h_{re}^\phi(I_{re}^\phi) + jh_{im}^\phi(I_{im}^\phi) = I_{re}^\phi + jI_{im}^\phi $$

where \( h_{re}^\phi(I_{re}^\phi) + jh_{im}^\phi(I_{im}^\phi) \) is the branch current magnitude measurement function. The BCSE minimisation problem can be formatted for each phase \( \phi \) by optimising the function \( J(\cdot) \) as follows:

$$ \text{minimise } J(I) $$

$$ = \sum_i^{ms} \left( (I_{re,i}^\phi - h_{re,i}^\phi(I_{re,i}^\phi))^2 + (I_{im,i}^\phi - h_{im,i}^\phi(I_{im,i}^\phi))^2 \right) $$

where \( I = [I_{re,1}, \ldots, I_{re,ms}, I_{im,1}, \ldots, I_{im,ms}] \) is the branch currents vector, \( ms \) denotes the number of power measurements, and \( \sigma_i \) denotes the error variance of the \( i \)th bus. The choice of branch currents for SE in distribution systems results in a linear function of the measurements, which is very efficient in converging the state estimator in radial topologies [44]. This improved convergence will be essential in the attacker optimisation problem formulation. In order to validate the BCSE model, the node voltages, obtained from the branch current phasors and power flow measurements, are compared with the voltage profile of the IEEE-34 bus system reported in [45]. Fig. 2 shows the comparison between the voltage magnitudes (in pu). The results confirm the accuracy of the BCSE for estimating the node voltages for all the nodes.

2.2 Distribution systems optimal power flow

The DSOPF processes in power systems encompass optimisation problems that aim to optimise certain operation objectives using the numerical analysis. System operators rely on the DSOPF to minimise operation costs, limit voltage deviations, define system supply security, and ensure optimal planning and allocation of DER units across the smart grid. The standard representation of an optimisation problem is as follows:

$$ \text{minimise } f(x) $$

subject to

$$ g(x) = 0, $$

$$ h(x) \leq 0 $$

where \( f(x) \) is the objective function, \( g(x) \) is the set of equality constraints, and \( h(x) \) is the set of inequality constraints. The objective function expresses the quantity to be optimised, the equality constraints represent the physical laws such as nodal power balance and Kirchoff's laws, and the inequality constraints define bounds of operations and contingency constraints on
voltages and power flows. The two sets of constraints have to be obeyed while solving the DSOPF problem. To tackle the non-convex nature of the DSOPF problem, one approach used is the convex relaxation of the constraints. The three main concerns in regard to the OPF convex relaxations in general are [12]: (i) feasibility of global optimal solution through convex relaxations, (ii) efficient convex relaxation computations, and (iii) numerical stability. To this regard, the convex relaxation based on SDP is chosen for its numerical stability and its suitability for the PDS [46]. The optimisation problem can be cast as an SDP problem as follows:

\[
\begin{align*}
\text{minimise} & \quad \sum_{i \in G} C_i(s) \\
\text{subject to} & \quad \sum_{j} (S_{ij} - z_i j_i) + s_j + y_j v_j = \sum_{j} \text{diag}(S_{jk}) y_j, \\
& \quad v_j = v_j^0 - (S_j v_j^0 + S_{ij}^H \omega_j + z_j j_i v_j^0), \\
& \quad y_j \leq \text{diag}(v_j) \leq \bar{y}_j, \\
& \quad \gamma_i = V_{i}^0 |V_{i}^0|^H, \\
& \quad \begin{bmatrix} v_j^0 \\ S_{ij}^H \end{bmatrix} \geq 0 
\end{align*}
\]

where \(G\) is the set of injection buses, \(C_i(s)\) denotes the real power injections at bus \(i\), and \(s_j\) is the branch power injection, \(V_i\) denotes the voltage at node \(i\), while \(j_i\) denotes the branch current between nodes \(i\) and \(j\). Control variables are defined by \(v_{ij} = V_i V_j^H\), \(l_{ij} = I_j R_{ij}^H\), and \(S_{ij} = V_i^H R_{ij}^H\), with the superscript \(H\) indicating the Hermitian transpose, and superscript \(\phi\) as phase index. Constraint (6b) describes the power flow balance equation, Kirchhoff’s voltage law is described by (6c), lower and upper voltage bounds are enforced by (6d), while the source voltage node is enforced by (6e), and (6f) is the positive semi-definite constraint.

### 3 FDI attacks

The problem of FDI attacks is concerned with the manipulation of a specific set of measurements in the system. A specific target of FDI attacks is the alteration of SE process to deceive the system operators through intelligent manipulation of the power flow measurements that alter the operator’s perceived system states [47]. Assuming that the attacker has access to the system information (e.g. topology), it is possible to alter the system states by intelligently manipulating specific measurements while keeping the residue norm unchanged in order not to raise the BDD alarm as follows:

\[
\| z_i - h(\hat{x}_{\text{bad}}) \| = \| z - h(\hat{x}) \| \leq \tau
\]

where \(z_i\) is the resulting manipulated measurements vector, \(\hat{x}\) is the states estimate vector, \(h(\hat{x}_{\text{bad}})\) is the altered states estimate vector, and \(\tau\) is the BDD detection threshold. Without loss of generality, in this work, only manipulation of field measurements is considered. The criterion of an AC-based FDI hidden attack is given by

\[
\lambda = h(x + c) - h(\hat{x})
\]

where \(\lambda\) is the structured attack vector to be added to the measurements. Based on (8), the attacker must consider the output value of the measurement function \(h(x)\) to successfully launch a stealthy attack. The vector \(c\) corresponds to the alteration in the state variables from the attack vector \(\lambda\) on the measurements. To launch constrained FDI attacks on power flow measurements that only target buses belonging to the subset \(\mathcal{N}_i\), an indispensible condition for the success of such attacks is the ability to target specific state variables, as outlined in the attack formulation. As shown in [47], it is possible to target specific system states to be manipulated during the FDI attack. The choice of target states to be manipulated is explained in Section 4.1, while the remaining states are left unchanged from the SE process. The index \(i\) determines the value of the attack element \(c_i\) to be added to the system state estimate \(\hat{x}_i\), as per (9), as follows:

\[
\hat{x}_{\text{bad},i} = \begin{cases} \hat{x}_i + c_i & \text{if } i \in \mathcal{N}_i \\ \hat{x}_i & \text{otherwise} \end{cases}
\]

The attacker is constrained by the following in order to successfully launch a hidden FDI attack: (i) the attack vector \(c\) has non-zero entries only for load buses, (ii) the attacks are launched on buses that are not constant current loads, as it can be easily verified if the current values are altered, and (iii) injection of non-load buses cannot be altered [48]. To achieve a load distribution attack (i.e. where the net change in the system remains zero), the attacker considers the nodal balance for each non-load bus \(j\):

\[
P_j = V_j \sum_{\mu \in \mathcal{N}} V_{\mu} (G_{\mu,\cos(\theta_{\mu})} + B_{\mu,\sin(\theta_{\mu})})
\]

\[
Q_j = V_j \sum_{\nu \in \mathcal{N}} V_{\nu} (G_{\nu,\sin(\theta_{\nu})} - B_{\nu,\cos(\theta_{\nu})})
\]

where \(P_j\) and \(Q_j\) are the active and reactive power, respectively, at bus \(j\). \(G_{\mu,\cos(\theta_{\mu})}\) and \(B_{\mu,\sin(\theta_{\mu})}\) are the \((j, \nu)\) entry of the complex bus admittance matrix and \(\theta_{\mu} = \theta_j - \theta_{\mu}\) is the angle difference between buses \(j\) and \(\nu\), and \(\mathcal{N}\) is the set of buses. The attacker must constrain the attack vectors to these conditions in order to keep the attack undetected by the BDD without violation of the electrical physical laws of the system. To validate the FDI effectiveness, attack vectors are constructed and added to healthy measurements to compare the residuals norm before and after the attacks. Fig. 3 shows a comparison of the norm of the residual differences for attacked and healthy measurements, for 100 vectors of measurements. It is noted that the residuals are almost identical and cannot be distinguished using the BDD detector.

### 4 Attacks on DSOPF

#### 4.1 Optimal attacks strategy

Equipped with the FDI stealthy formulation, the adversary is able to incorporate the attack vectors formulated in the previous section in order to maximise the losses on the system. The optimal attack
The formulation is derived through an optimisation problem that mimics the features of the original DSOPF that the system operator utilises. The attack strategy flowchart is shown in Fig. 4, detailing the work done by the attacker to construct the attack vectors, to be injected in the measurements received by the DSSE process. The first (left) part of the flowchart shows the steps done by the attacker, while the second (right) part is the normal DSOPF operations run by the PDS operator. For the adversary, the attack strategy is as follows:

i. The first step is getting access to the measurements sent from RTUs and PMUs [49, 50].

ii. The second step is deploying the DSSE to get an estimate of the system states based on the available measurements.

iii. The third step consists of running a modified DSOPF problem, which has similar constraints to the operator’s DSOPF, but with a modified objective function, which maximises the losses of the PDS operator. The derivation of this problem is explained in the next section.

iv. After running the optimisation problem, the solution point represents the maximum losses of the system given the system parameters and constraints. The arguments of the optimal solution represent the values of the variables that lead to this solution. The gap between the resulting arguments and the arguments from the uncompromised DSOPF represents the values of injection to be added to the measurements, according to the FDI attacks process. These vectors can be injected into the measurements data received from the metres without triggering the BDD alarm. Since the vectors are synthesised from the modified DSOPF, they represent the optimal attack vectors to be added to the measurements.

v. The corrupted measurements are passed to the PDS system operator. Consequently, the system operator runs, unwittingly, the DSSE and DSOPF with bad measurements.

4.2 DSOPF attacks formulation

The alteration of the system state variables is achieved by manipulating the measurements vector $z$ to change the $i$th entry in attack vector $c$ by using (8), with $c_i = 0$ if the $i$th state is not to be changed. The attacker runs the DSOPF with the objective of maximising the losses, instead of minimising it, as follows:

$$\text{maximise} \quad \sum C_i(s_i)$$ (12a)

subject to: (6b), (6c), (6d), (6e), (6f),

$$\| \text{diag}(z - h(\tilde{x}_{bad})) \| \leq \tau$$ (12c)

$$\bar{s}_{ij} \leq s_{ij} \leq \tilde{s}_{ij}$$ (12d)

where $s_{ij}$ and $\tilde{s}_{ij}$ are the lower and upper bounds of power injections after alterations of measurements using (8) of pre-specified limits by the attacker, inspired by the AC attacks formulation [48]. Constraint (12c) is added to ensure that the altered measurements bypass the BDD according to (7). Note that this DSOPF, run by the attacker, is similar to the original problem with a different objective function, and is used to determine the deviation in current state variables $I_{ij}$ to be injected for maximum losses in the DSOPF. The affected currents represent the subgraph of measurements needed to be changed to hide the attack. The choice of the BCSE allows one to add the linear measurement function as a convex constraint implicit in constraint (7) as part of the solved DSOPF problem.

5 Case study

5.1 Test system

In order to investigate the effects of FDI attacks on the DSOPF, the attack model is tested on the IEEE-34 bus unbalanced radial distribution system. The study has been carried over the testing period of 24 h, where the DSOPF was run on hourly basis. Fig. 5 shows the load profile over the testing period. DERs were modelled as PV, wind sources, and dispatchable DER units. DERs operate in PQ mode, with a $\text{pf} = 0.9$ and the output power is constrained by
injection per phase, and by the system operator. In this case study, the losses are determined here.

Loads are represented using the exponential load model, and represented in Fig. 6. Fig. 7 depicts the modified three-phased generation output of the PV and wind DERs in a typical day is here.

Table 2 DERs data

| Node | Type               | Rating, kW | Phases |
|------|--------------------|------------|--------|
| 838  | dispatchable unit  | 600        | ABC    |
| 848  | dispatchable unit  | 450        | B      |
| 860  | dispatchable unit  | 450        | C      |
| 828  | PV                 | 150        | A      |
| 842  | PV                 | 200        | ABC    |
| 820  | wind               | 200        | A      |
| 832  | wind               | 250        | ABC    |

Fig. 6 PV and wind output power profile

Fig. 7 Modified IEEE-34 distribution system with DER units

Table 3 Dispatchable DERs cost function data

| Node | $a_1$, $$/kWh$ | $a_2$, $$/kWh^2$ |
|------|---------------|-----------------|
| 838  | 0.02          | 0.0004          |
| 848  | 0.03          | 0.0002          |
| 860  | 0.03          | 0.0003          |

\[
P_{G,\text{max}} = S_{G,\text{max}}
\]

\[
Q_{G,\text{max}} = \sqrt{(S_{G,\text{max}})^2 - (P_{G,\text{max}})^2}
\]

where $S_{G,\text{max}}$, $P_{G,\text{max}}$, and $Q_{G,\text{max}}$ are the MVA rating, maximum active power, and reactive power of the DER unit, respectively. Table 2 provides the DERs data and nodes placement. The hourly generation output of the PV and wind DERs in a typical day is represented in Fig. 6. Fig. 7 depicts the modified three-phased unbalanced system [45], with the installation locations of DERs.

5.2 DSOPF power losses

The attacker objective is to maximise the losses of the DSOPF run by the system operator. In this case study, the losses are determined from the cost function of dispatchable DER units (hosted on nodes 838, 848, and 860). The DSOPF objective function is formulated as

\[
C = \sum_{g \in \Omega} \alpha_1 (P_{g1} + P_{g2} + P_{g3}) + \alpha_2 (P_{g1} + P_{g2} + P_{g3})^2
\]

where $G$ is the set of dispatchable DERs, $P_g$ is the active power injection per phase, and $\alpha_1$ and $\alpha_2$ are the parameters of the cost function per DER unit. Table 3 lists the parameters for each DER unit. Loads are represented using the exponential load model, and the substation voltage is set at 1.05 pu. It is assumed that measurements taken in the system are active and reactive power flows on all branches. The system modelling was implemented in MATLAB and the CVX optimisation toolbox [51] was used to solve the SDP convex optimisation problem. The total hourly real power injection $P_g$ for the three dispatchable DERs is displayed for each phase ($A$, $B$, $C$) in Fig. 8. For each hour, the power injection in the attacked case is greater than or equal to the original power injection. As a result of the increase in power injection for the dispatchable DERs, the objective function solution increases by 30% from $4993 to $6632 due to the FDI attack vectors. The original and attacked voltage profiles of the three phases for node DG (node 838) is depicted in Fig. 9, while the one-phase voltage profile of DG (node 848) and DG (node 860) is depicted in Fig. 10. The voltage profiles of original and attacked DSOPF are both within the permissible voltage upper and lower boundaries, and therefore do not signal any attack indication or voltage violation. However, the slightly lower voltage profile of the attacked version of the DSOPF is in accordance with the increase of power injections due to the FDI attacks.

5.3 Discussion

As seen from the results, the FDI attack successfully manipulates the measurements over the three phases to increase the cost function of the system operator. In comparison with other attack schemes, the proposed method has several distinctions including:

i. The FDI vectors are constructed based on the AC SE model, in contrast to other approaches that consider DC models [52, 53]. The comparison of residual norm errors of adopting the DC versus the AC non-linear detailed model is shown in Fig. 11. The proposed method gives almost identical residual errors, where the DC model results in significantly higher residual error values. The gap in residual error norm magnitude between both the no-attack and AC FDI vectors versus the DC FDI vectors confirms that the threshold BDD cannot identify the FDI DC attacks, in contrast to the FDI AC attacks.

ii. The FDI attack model considers the three-phase unbalanced phases, unlike other AC attack models that are based on single-phase assumptions [48]. This is evident in the results of voltage violation.
and power injections that vary across the three phases, as depicted in Figs. 8 and 9, respectively. In addition, the attacks are launched on multiple nodes simultaneously to maximise the attack damages, and the power losses were quantified by the increase in the objective function. Related works on the PDS level have not considered a stealthy attack model that maximises losses [35], or have only considered a single node of attack [34] which yields less power losses as the power losses is defined as the increase in power injection of all power injection nodes.

iii. Different from the FDI attack models on the transmission level, it is not suitable to treat PDS loads as constant power. Therefore, the proposed model considered the ZIP model [54] for determining the states variables. As shown in Fig. 12, for phase A at hour 12 of the load profile, the absolute voltages change due to the attack vectors vary on all node voltages for three different load models. Configuration $O$ is the standard IEEE-34 load configuration [45], which is a mixture of constant impedance, constant current, and constant power loads; configuration $P$ assumes that all loads are constant power; and configuration $Z$ assumes that all loads are constant impedance. The analysis demonstrates that the attack effects are highly dependent on the system configuration and load types. The constant impedance loads present the lowest sensitivity of voltage variations due to the power measurement alterations. Hence, the adversary can target the constant impedance loads to maximise the variations in power measurements with minimal deviations in voltage magnitudes.

6 Conclusion

The effects of FDI attacks on DSOPF for radial unbalanced PDS are investigated, where it is shown that how attackers can formulate undetectable attacks based on the BCSE model to ensure convergence of the SE after measurements manipulation. This, in turn, allows crafting the FDI attacks as constraints in the DSOPF, which enables undetectable manipulation of measurements to maximise the system losses while keeping the attacks undetectable. The study was conducted on three-phase radial distribution systems, with multiple DERs along the feeder. The attack vectors caused the increase of the power injection from the dispatchable units. Compromising the DSOPF to maximise the losses highlights the importance of securing PDS against FDI attacks and their potential impacts on the system security and efficiency. For future work, a detection and mitigation mechanism to limit the effects of the FDI attacks is to be developed, in addition to considering different attack models.

7 References

[1] Lopes, J.P., Hatziargyriou, N., Mutale, J., et al.: ‘Integrating distributed generation into electric power systems: a review of drivers, challenges and opportunities’, Electr. Power Syst. Res., 2007, 77, (9), pp. 1189–1203
[2] Farag, H.E., El-Saadany, E.F., Seethapathy, R.: ‘A two ways communication-based distributed control for voltage regulation in smart distribution feeders’, IEEE Trans. Smart Grid, 2012, 3, (1), pp. 271–281
[3] Tesfay, T.T.: ‘Cybersecurity solutions for active power distribution networks’. Technical Report, EPFL, 2017
[4] Baran, M.E., Kelley, A.W.: ‘State estimation for real-time monitoring of distribution systems’, IEEE Trans. Power Syst., 1994, 9, (3), pp. 1601–1609
[5] Baran, M.E., Jung, J., McDermott, T.E.: ‘Including voltage measurement in branch current state estimation for distribution systems’. 2009 IEEE Power Energy Society General Meeting, Calgary AB, Canada, July 2009, pp. 1–5
[6] Primadianto, A., Lu, C.N.: ‘A review on distribution system state estimation’, IEEE Trans. Power Syst., 2017, 32, (5), pp. 3875–3883
[7] Do Coutto Filho, M.B., de Souza, J.C.S.: ‘Forecasting-aided state estimation – part I: panorama’, IEEE Trans. Power Syst., 2009, 24, (4), pp. 1667–1677
