A combined survey on distribution system state estimation and false data injection in cyber-physical power distribution networks

Poornachandratejasvi Laxman Bhattar1 | Naran M. Pindoriya1 | Anurag Sharma2

1Department of Electrical Engineering, Indian Institute of Technology Gandhinagar, Gandhinagar, India
2Electrical Power Engineering, Newcastle University in Singapore, Singapore

Correspondence
Poornachandratejasvi L. Bhattar, Department of Electrical Engineering, Indian Institute of Technology Gandhinagar, Gandhinagar 382355, India.
Email: pooranchandra.tejasi@iitgn.ac.in

Abstract
The penetration of renewable energy sources (RES) in distribution systems has entailed heavy deployment of monitoring and control infrastructure in the distribution system. This deployment of sensors and communication infrastructure has led to the emergence of a modern grid with a complex cyber-physical network. On one hand, the cyber-physical system can play a pivotal role in coordination and control of distribution systems through distribution system state estimation (DSSE). On the other hand, the risk caused by cyber-attack has emerged as a major challenge for grid operation. The modeling aspects, namely DC loads, plug-in-vehicle and distributed generators (DGs) in DSSE and security aspects in cyber-physical distribution systems, are highlighted herein. This paper is divided into different sections emphasizing on the problems and challenges associated with DSSE, cyber-attack focussing primarily on impact of false data injection (FDI) attack and co-simulation platform for investigation of vulnerability of cyber-physical systems. A comparative study among various DSSE and challenges namely, pseudo-measurement, time synchronisation and communication issues are discussed. The potential investigation of FDI and need for a co-simulation platform in distribution systems for risk analysis are also addressed. The opportunities and future research in the field of cyber-physical distribution systems are discussed in depth.

1 | INTRODUCTION

The control and coordination in power systems have necessitated the development of state estimation (SE) in the transmission system. The state estimator monitors the real-time operating states in the power system for effective energy management. SE for a transmission system was well developed. However, there was less focus on the development of SE for conventional distribution systems where power flow was unidirectional. The penetration of distributed energy resources (DERs) and consumers’ ability to participate in the energy market have encouraged utilities to monitor distribution systems via distribution system state estimation (DSSE). At present, the active distribution system should inherit self-healing and restoration capability in the presence of intermittent DERs and uncertain network events namely, faults etc. [1]. The concept of prosumers has emerged, stating consumers and producers to be the same entity where power exchange is done at community level. However, the emerging plug-in electric vehicle (PEV) technology with bidirectional power flow, the distribution system need to be monitored with efficient state estimator for flexible operations [2]. State estimation in distribution system is challenging with large number of nodes and insufficient real-time measurements. The estimation algorithm with branch current as state variable with reduced computational burden and complexity was proposed in ref. [3]. However, it had limitation of including current measurements and forcing the Jacobian matrix to depend on state variables. The revised algorithm was developed to obtain the constant Jacobian matrix independent of the state variables [4]. The node voltage-based state estimator and challenges associated with observability and measurement uncertainty in DSSE were explored in ref. [5–7].

DSSE is the basis of energy management system (EMS) in distribution system which receives the measurement input from physical system. A distribution system operator (DSO)
relies on DSSE for control and monitoring the system. Figure 1 shows the various layer of cyber-physical system (CPS) in distribution network. Physical layer (distribution system) interacts with application and decision layer (state estimation and its functionalities namely, volt-var, fault management etc.) via communication layer through measuring and sensing unit namely, phasor measurement units (PMU’s), synchro-phasor, smart metres and intelligent electronic devices (IED’s). In application and decision layer, measurements from sensing units are processed through state estimators and operating states are estimated. With the knowledge of these states, the operator takes the appropriate decision namely, volt-var control, transformer tap changing, battery scheduling etc. The operator performs the optimal power flow and load flow studies for abovementioned operation with help of estimated states. The information and communication technology (ICT) have leveraged the process of monitoring and control. As shown in Figure 1, possibilities of tampering and damage of sensing and measuring units in CPS cannot be neglected and hardware security in CPS need to be considered. However, with surveillance on sensing and metering unit, physical tampering in CPS is difficult but the risk of tampering cannot be underestimated. The communication layer consisting of LAN, Wi-Fi, WAN etc. are at higher risk and need to be protected from cyber-attack. The application and decision layer utilise the optimization algorithm to derive the control signal to physical system. The cyber-attack namely, false data injection, data spoofing and denial of services on DSSE can disrupts the distribution system operation leading to economic loss and physical damage. Thus, such cyber-attacks need to be explored and investigated.

The common platform to understand distribution system state estimation along with false data injection (FDI) in DSSE is provided herein. It highlights the challenges in DSSE and impact assessment of FDI attack in cyber-physical distribution network. The paper investigates the unexplored bits in DSSE and provides an insight for developments in DSSE algorithms with inclusion of PMU, SCADA, smart metre etc. It also inspects the challenges to incorporate these measurements in DSSE. On another side, owing to cyber-physical nature of distribution system, cyber security aspects focussing on cyber-attack by FDI is reviewed for security and vulnerability assessment of cyber physical distribution system. Various challenges and opportunities are discussed in paper which encourages researchers in this domain to take up these challenges and to provide the best and effective solution to address the problems.

The paper is organised as Section 2 includes the mathematical formulation of DSSE. The DSSE modelling is included in Section 3. Various DSSE algorithms are discussed in Section 4. Insight of cyber-attack is provided SE in discussed in Section 5 followed by challenges and key areas of research and concluding remarks in Section 6.
2 | MATHEMATICAL FORMULATION OF DSSE

State estimations in power system are formulated based on the measurement model as in Equation (1) discussed in Section 2.1. The DSSE incorporate either AC power flow model that is non-linear model or DC power flow model that is linear model. The following sub-section discusses the formulation of non-linear and linear state estimator.

2.1 | Formulation of non-linear state estimator

The traditional state estimator is formulated by weighted least squares (WLS) based on maximum likelihood theory [7, 8]. The measurement model is expressed as Equation (1), where \( z \) consists of \( m \) number of measurements, \( h(x) \) is the vector valued function and \( e \) is the Gaussian noise vector. The residual \( r \) of \( m \)th measurement is as in Equation (2), where, \( \sigma_{zm} \) is the covariance of \( m \)th measurement of \( z \).

\[
z = h(x) + e
\]  

\[
r_m = \frac{z_m - h_m(x)}{\sigma_{zm}}
\]

The covariance \( R_z \) matrix as in Equation (3). The maximum likelihood is obtained by choosing the weights as the inverse of variance.

\[
R_z = \text{diag}(\sigma_{z1}, \sigma_{z2}, \sigma_{z3}, \ldots \sigma_{zm})
\]

The objective function to estimate the state is expressed as in Equation (4) and solved iteratively with Newton method. The general solution for objective function is obtained by the normal equation (NE) where the states can be estimated by Equation (5).

\[
J(r_m) = \min \sum_{m=1}^{m} f(r_m)^2
\]

\[
\Delta x = G^{-1}H^T W (z - b(x))
\]

For \( k \)th iteration, \( x^{k+1} = x^k + \Delta x^{k+1} \). Where, \( G^{-1} = H^TW H; G \) is the gain matrix; \( H = \frac{\partial h(x)}{\partial x} \) = Jacobian matrix; \( W = R_z \) = weight matrix. The solution with NE method may diverge and can cause the convergence issue with higher resistance to reactance ratio [9]. Robust SE algorithm with equality constraint and zero injections was formulated and solved with NE with more efficient [10–13]. The objective function described in Equation (4) subject to zero equality constraint \( c(x) = 0 \). Solution of zero constrained can be obtained iteratively by solving Equation (6). With \( \lambda \) as Lagrange’s Multiplier, Equation (6) is iteratively solved to obtain the estimates. Different state estimators have been formulated based on maximum likelihood criterion. The comparative study among WLS, weighted least absolute square (WLAV) and Schweppe Huber Generalized Estimator (SHGE) was studied in ref. [14].

\[
\begin{bmatrix}
G(x)^k & c(x)^k \\
c(x)^k & 0
\end{bmatrix}
\begin{bmatrix}
\Delta x^k \\
-\lambda^k
\end{bmatrix}
= \begin{bmatrix}
H(x)^k \ T R^{-1} [z - b(x)]^k \\
- c(x)^k
\end{bmatrix}
\]

As in ref. [14], the WLS-based estimator is more consistent and efficient compared to WLAV and SHGE estimator. SE based on non-iterative methods provides the better computational efficiency and improved convergence rate [15–17].

2.2 | Formulation of linear state estimator

Linear state estimators are computationally efficient and state estimation equations are solved for decoupled form [15]. Equation (1) is linearised along the operating point for \( h(x) \) and residual is given by Equation (7). The decoupled form that is separation of real and imaginary part is done to improve the sensitivity of performance matrix, followed by Equation (8).

\[
r = z - bx
\]

where, \( b \) is the Jacobian matrix with suffix \( r \) and \( i \). Index \( r \) and \( i \) indicates the real and imaginary. The estimate \( x_r \) and \( x_i \) are obtained by solving Equation (8) by considering Equation (4).

\[
\begin{bmatrix}
b_r & -b_i \\
b_i & b_r
\end{bmatrix}
\begin{bmatrix}
x_r \\
x_i
\end{bmatrix}
= \begin{bmatrix}
z_r \\
z_i
\end{bmatrix}
\]

2.3 | Handling of high \( r/x \) ratio

The high \( r/x \) ratio results in ill-conditioning of \( H \) matrix. It constitutes the partial derivative of measurement functions with respect to state variables as in Equation (9).

\[
H = \begin{bmatrix}
\frac{\partial P}{\partial \theta} & \frac{\partial P}{\partial \psi} \\
\frac{\partial Q}{\partial \theta} & \frac{\partial Q}{\partial \psi}
\end{bmatrix}
\]

where \( P, Q, \psi, \theta \) indicates the active power flow or injection, reactive power or injection, voltage magnitude and angle measurement. In transmission system, the off-diagonal elements \( \frac{\partial P}{\partial Q} \) and \( \frac{\partial Q}{\partial P} \) are neglected that is \( \frac{\partial P}{\partial Q} \approx \frac{\partial Q}{\partial P} \approx 0 \) because of
weak coupling [5]. With high $r/x$ ratio and strong coupling, the off-diagonal elements cannot be discarded in distribution system. To avoid the ill-conditioning [9] of $H$ matrix, the $P_{abc}$ and $Q_{abc}$ measurements are handled by converting in equivalent current measurement $I_{abc}$ and making the $H$ matrix independent of state variables Equation (10), where $abc$ denotes the phases. The equivalent current measurement can be expressed with voltage or a current variable [3, 18] for every iteration $k$.

$$I^k_{abc} = \left( \frac{P_{abc} + jQ_{abc}}{V^k_{abc}} \right)^*$$  \hspace{1cm} (10)

The structure of $H$ with voltage variable for power injection measurement in rectangular form is expressed as in Equation (11), where the admittance matrix is $[Y_{abc}]_{3 \times 3} = [G_{km} + jB_{km}]_{3 \times 3}$. With branch current as the state variable it consists of $-1$ with power injection and $+1$ in the case power flow measurements. It depends upon the state variables and need to be updated at every iteration with inclusion of voltage measurement and its formulation with current, voltage and PMU measurement is provided in ref. [5, 18, 19].

$$\begin{bmatrix} V^r_{abc} & V^i_{abc} \\ \end{bmatrix} = \begin{bmatrix} \frac{G_{km}}{3} & \frac{B_{km}}{3} \\ \frac{-B_{km}}{3} & \frac{G_{km}}{3} \\ \end{bmatrix}$$  \hspace{1cm} (11)

3 | DSSE MODELLING

The DSSE algorithm requires the network information and mathematical model to represent the distribution system topology. The suitable three phase model should be incorporated for real time monitoring of distribution system and to solve the SE problem. The mathematical model for distribution system elements namely, feeder, underground cable, transformer etc. are briefly discussed in the following section.

3.1 | Line and transformer model

The feeder model for distribution system that is three phase, four wire can be represented as $4 \times 4$ impedance matrix $Z$ with modified Carson method. To simplify the computational burden, the Kron’s reduction is used to reduce $Z$ matrix to $3 \times 3$ [20]. The three phase model of line segment takes mutual impedances in consideration as in Equation (12).

$$Z = \begin{bmatrix} Z_{aa} & Z_{ab} & Z_{ac} \\ Z_{ba} & Z_{bb} & Z_{bc} \\ Z_{ca} & Z_{cb} & Z_{cc} \\ \end{bmatrix}$$  \hspace{1cm} (12)

where $a$, $b$ and $c$ represent the phases; the diagonal elements of $Z$ namely, $Z_{aa}$, $Z_{bb}$ and $Z_{cc}$ represent the self-impedance while off-diagonal elements represent mutual impedances between the phases. The underground cable is modelled similar to overhead line using modified Carson equation with primitive matrix is $6 \times 6$ and simplified to $3 \times 3$ [20].

Modelling of distribution transformer plays a vital role in state estimation, short circuit and load Flow studies. The transformer is represented by nodal admittance matrix $Y_T$ ($6 \times 6$) with current and voltage relation as in Equation (13) [21, 22]. Where, $I_p$, $I_s$ = primary and secondary phase current of transformer; $V_p$, $V_s$ = primary and secondary phase voltage; $Y_T$ consists of submatrices $Y_{pp}$, $Y_{ps}$, $Y_{sp}$ and $Y_{ss}$ of matrix size $3 \times 3$.

$$\begin{bmatrix} I_p \\ I_s \end{bmatrix} = \begin{bmatrix} Y_{pp} & Y_{ps} \\ Y_{sp} & Y_{ss} \end{bmatrix} \begin{bmatrix} V_p \\ V_s \end{bmatrix}$$  \hspace{1cm} (13)

3.2 | Load model

The distribution system includes single and three phase loads with delta and star connected configuration. Loads can be further modelled as constant impedance ($Z$), constant current ($I$) and constant power ($P$) that is ZIP model [23]. The spot and distributed loads were represented by current injection model described in ref. [24].

3.2.1 | Plug-in-electric vehicle

Environmental impact and energy policies have encouraged plug-in-electric vehicle (PEV) in distribution system. Increase in PEV is reshaping the load demand and burdening the distribution transformer. Hence, it is mandatory to understand the PEV load characteristic and its impact on distribution system with appropriate modelling in SE. The PEV is modelled with constant load current to assess the grid stability [25], and as constant power for wide area monitoring application [26]. The power and voltage dependent model with negative exponent ($\alpha = -2$) as in Equation (14) is considered for stability analysis for PEV [27, 28], where $P_0$ is the nominal power with the nominal voltage $V_0$ and $\alpha$ as exponent.

$$P = P_0 \left( \frac{V}{V_0} \right)^\alpha$$  \hspace{1cm} (14)

Constant impedance ($\alpha = 2$), constant current ($\alpha = 1$) and constant power ($\alpha = 0$), the negative alpha draws the system towards the instability. The composite load model that is constant impedance $Z$, constant current $I$ and constant power $P$ was considered with the charging and discharging behaviour of PEV. It is modelled with voltage dependent profile that is $V_i$ measured at $i$th range of state of charge is given by Equations
estimated. For state estimation, the input measurements are system operator to rely on pseudo-measurements (VM) [32] and pseudo-measurements [33]. VM are considered as error free and measured at substation where loads are not connected. These measurements enhance the performance of SE. Pseudo-measurements improve the network observability and are obtained from consumer load curve and demand curve [33]. Another way to obtain pseudo-measurements by using the load flow results and adding the error to mimic the real-time measurements. High penetration of DER and the lack of monitoring units force the state estimators to depend upon the forecasted measurements and making it less accurate because of uncertainty in measurement data. The inclusion of voltage phasor measurement obtained by PMU has elevated the performance of state estimator [34].

3.5 | DG in DSSE

Precise monitoring of DG in distribution system needs suitable mathematical model. The wind and photovoltaics generator are modelled as (1) direct connected, that is, no power electronic converter interfacing. The wind generators are synchronous machines or induction machines are modelled as R-X model. Owing to the stochastic nature of wind, the wind generator cannot be modelled as a constant power model. (2) Indirect connected that is power electronic converter interface with distribution system [35]. The photovoltaics generator is modelled as constant power model with converter interface [36, 37]. The indirect connected DG’s have internal controllable states and actual states that need to be monitored [38]. Precise modelling of DG is required as these states provide the information of asymmetric characteristic in voltage output of DG because of unbalanced load.

- **Modelling aspects of DER**: The wind turbines, gas turbines, micro-turbines and internal combination are directly connected to grid via, synchronous generator and induction generator and indirectly to grid through power electronics converter. The induction and synchronous generator are modelled as the constant power model [38–40].
- **Induction generator**: The active power and reactive power for induction generator is described as $P = f(V, s)$ and $Q = f(V, s)$, where $s$ is slip.
- **Synchronous generator**: The synchronous generator is modelled as voltage controlled node that is PV when the terminal excitation voltage is kept constant while it is modelled as PQ when the excitation voltage is varied. For the rotor wound synchronous machine the active power and reactive is expressed as Equations (20) and (21). $E$ is the no load voltage, $\delta$ power angle. $E$ and $\delta$ are called internal states. The $P$ and $Q$ are active and reactive power of DG.

$$P(E, V, \delta) = \frac{EV}{X_d} \sin \delta$$  \hspace{1cm} (20)
\[ Q(E, V, \delta) = \frac{EV}{X_d} \cos \delta - \frac{V^2}{X_d} \] (21)

- **Sequence modelling unbalanced distribution system:** In unbalanced conditions, DGs are modelled as sequence impedance. The Norton equivalent of DG is represented in Figure 2. The zero sequence, positive sequence and negative sequence admittance are represented as \( y_0, y_1 \) and \( y_2 \). The admittance \( Y_{abc} \) is expressed as in Equation (22) with transformation matrix \( T_s \) [41]. The apparent power in compact is expressed as \( S_g = [V_{abc}^T][I_{abc}]^T \). \( T \) represents the transpose where phase voltages and current are expressed as \( V_{abc} = [V_a, V_b, V_c] \) and \( I_{abc} = [I_a, I_b, I_c]^T \).

\[ Y_{abc} = T_s \begin{bmatrix} y_0 & 0 & 0 \\ 0 & y_1 & 0 \\ 0 & 0 & y_2 \end{bmatrix} T_s^{-1} \] (22)

and

\[ T_s = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 1 & 1 \\ 1 & a^2 & a \\ 1 & a & a^2 \end{bmatrix} \]

The phase current in terms of sequence component is expressed as \( I_{abc} = (1/\sqrt{3})[1 a a^2]^T I_1 \). The grid current \( I_{abc} \) is given in Equation (23).

\[ I_g = I_{abc} - Y_G V_{abc} = \frac{1}{\sqrt{2}} \begin{bmatrix} a^2 & a \\ a & a^2 \end{bmatrix} I_1 - Y_G V_{abc} \] (23)

- **Power electronic-coupled DER:** The power electronic converter coupled with DER are modelled as three wire and four wire in distribution system. With balanced condition, the DG control circuit supply the positive sequence components while the negative and zero sequence with appropriate control in unbalanced condition. However, DG is modelled as PV node when active power exchange is made and PQ when both active and reactive power is exchanged [42].

- **Sequence modelling of transformer:** The admittance matrix \( Y_{abc} \) of transformer can be transformed to sequence components as in Equation (24) with transformation matrix \( T \) [43].

\[ Y_{012} = \begin{bmatrix} T & \end{bmatrix}^{-1} Y_{abc} \begin{bmatrix} T \end{bmatrix} \] (24)

- **Sequence model of line impedance:** The line impedance after Kron’s reduction is transformed to sequence model as in Equation (25), where the off diagonal gives the sequence component of mutual coupling and diagonal elements give the sequence component of phase impedance [43].

\[ Y_{012} = \begin{bmatrix} y_{00} & y_{01} & y_{02} \\ y_{10} & y_{11} & y_{12} \\ y_{20} & y_{21} & y_{22} \end{bmatrix} \] (25)

- **Sequence modelling of load:** The unbalanced load can be represented in positive, negative and zero sequence [43].

- **Technical challenges with DG:** The asymmetric phase output envisage the problem of overvoltage and reverse power flow in unmonitored DG units. Monitoring the actual state becomes mandatory with DG connection. However, distribution system largely depends on pseudo-measurement because of lesser number of measuring devices at DG. The accuracy of pseudo-measurements poses challenge for error-free estimation. The forecasting-based model is adopted for depending on unmonitored DG’s namely, machine-learning-based algorithm with evolutionary algorithms, forecasting model [44]. The stochastic variation of load demand, uncertainty in power generation and presence of various noise levels in telemetered data in DG necessitate the development of appropriate forecasting model for DSSE [45].

## 4 | CLASSIFICATION OF DSSE

DSSE algorithms are the extension of transmission system state estimation algorithms. Owing to complexities in distribution system namely, unbalanced network condition, higher \( r/x \) ratio and insufficient measurements, the DSSE algorithm need to be explored. However, statistical state estimators are popular because of their consistency and accuracy to estimate the states. With penetration of DERs, the data driven and dynamics state estimation were introduced recently in literature are discussed in Section 4.3 and 4.6. In following section,
DSSE algorithms namely, voltage- and current-based state estimator, forecast-aided, multi-area and data driven are summarised.

4.1 Voltage-based and branch current-based state estimator

Over the time, different state estimators were developed and measurement data were processed to determine the operating state through WLS-based optimization technique. Based on selection of state variable either as voltage or branch current, voltage-based state estimator (VBSE) [5, 18], and branch current-based (BCBSE) [3] were developed. The BCBSE was found to be computationally efficient because of a constant Jacobian matrix. The authors in ref. [46] suggest that BCBSE have better performance and accuracy with ease to implement in real time operation compared to VBSE. They showed the similar performance under same error propagation in measurement data. However, the gross error in measurement data deteriorated the performance of VBSE and BCBSE. With increased number of smart metre, the nodal power injection measurements are significant for state estimation observability. These measurements are modelled as the injection power measurement and handled converting with equivalent current injection in BCBSE and with sequence component transformation in VBSE.

4.2 Robust state estimator

Conventional estimator is well developed for over-determined systems (number of equations are more than number of unknown). In the case of under-determined systems (lesser number of equations than the number of unknown), solving estimation problem is challenging and obtained results might diverge from the true estimation. The robust estimators are capable to produce results in the presence of measurement data error for under-determined system. The framework for robust state estimation was provided in ref. [47] by using the closed loop information flow; machine learning algorithm for load estimation and robust algorithm for the pseudo-measurement generation. The adaptive non-linear auto-regressive model was developed for SE and load estimation [48]. The machine learning techniques were used for load estimation and to generate the pseudo-measurements to make the SE functionally more robust by handling the bad data detection [49–51]. SE was formulated as mixed integer optimization problem has improved accuracy and was capable to handle bad data [47]. The robust estimator discussed in ref. [51, 52] namely, quadratic constant estimator, M-estimator, maximum exponential absolute value (MLAV), Schweppes Huber Generalized (SHG) etc., performs better in the presence of noisy measurement other than Gaussian noise. In overview, these class of estimators are capable to deal with under-determined system and cope with different noise level in measurements obtained from SCADA and PMU.

4.3 Forecast aided state estimator

The distribution system with considerable level of uncertainty in load demand, intermittent nature of DERs and availability of large data in distribution system have encouraged the forecast aided state estimators (FASE) to deal with uncertainties [53–55]. In FASE, Kalman-based filtering is adopted to capture the distribution system dynamics. The pseudo-measurements are forecasted using the consumer load profile. The method proposed in ref. [56] utilises the load flow and unsealted Kalman filtering approach (UKF). The point-based Gaussian filter was developed for state estimation and results were found to be better than the conventional UKF [57]. Multi-layered hierarchical SE using FASE with non-iterative method using augmented Kalman filtering with complex variables have been proposed [55]. The past aware state estimator (PASE) utilising the historical database is discussed in ref. [58]. As discussed in above-mentioned literatures, various FASE are developed. However, it would be important to understand comparative performance of FASE. The comparative study between Ensemble Kalman Filter (EnKF)-based FASE and WLS was studied in ref. [58]. It uses the load forecasted measurements and the data from PMU merged with different time horizon. It has proved to have the benefits over the WLS, where the requirement of PMU in EnKF (number of PMU = 4) were less compared to WLS (number of PMU = 3) because of load evolution model used in EnKF (for 33 bus system). The EnKF performs better than the WLS with forecasted load consisting large error. However, the lower time step increases the computational burden in Kalman filtering compared to WLS-based state estimation. The performance parameter Equations (26–28) of state estimator is expressed in terms of percentage error (PE), average percentage error (APE), mean absolute error (MAE) and root mean square error (RMSE). \( \frac{\text{est}_t}{\text{act}_t} = \frac{y_t^\text{est} - y_t^\text{act}}{y_t^\text{act}} \times 100 \) (26)

\[
\text{MAE} = \frac{1}{N} \sum_{t=1}^{N} \frac{1}{\text{L}_t} \sum_{i=1}^{\text{L}_t} |y_i^\text{est} - y_i^\text{act}| 
\]

\[
\text{RMSE} = \frac{1}{N} \sum_{t=1}^{N} \left( \frac{1}{\text{L}_t} \sum_{i=1}^{\text{L}_t} (y_i^\text{est} - y_i^\text{act})^2 \right)^{1/2} 
\]

4.4 Multi-area state estimator

Owing to large distribution network and control centre located at different geographical location, single SE was insufficient to monitor the real time operation. The monitoring area was divided into different zones acquainted with
measurement correlation and reduced communication units is discussed in ref. [64]. In ref. [65], the framework for the MASE with self-weight updating method is discussed. The MASE may utilise one or combination of the mentioned state estimator: statistical state estimator, robust state estimator and forecast-aided state estimation. The choice for multi-area state estimation can be made on computational speed and convergence ratio. The various type of DSSE, their pros and cons are summarised in Table 1.

### 4.5 Data-driven state estimator

The data driven approaches are becoming popular to address the large data from smart metres and fewer real-time measurement. The hybrid state estimator with a combination of data driven and statistical estimation was proposed with inclusion of smart metre data [70]. The large data coming from network which includes the customer information and metred data need to be handled with systematic manner [60]. Handling large volume of data pose a challenge for data-driven estimator. To address this issue, the neural network-based NARX model was developed for state estimation and monitoring [48], ANN-based scalable state estimator incorporating local state estimation was developed [71]. The data based on forecasting of load and generation was utilised to train neural network with supervised learning to handle uncertainties [72]. The deep neural network-based DSSE utilising the historical and load data for generation of measurement along with SCADA and AMI was proposed [73]. Based on data correlation and redundancy, the input variable selection is proposed in ref. [74] to reduce the computational burden. The relevance vector machine (RVM) was used to generate the pseudo-measurements by considering the weather conditions [68, 75]. The data-driven estimator can play vital role in LV/MV monitoring with large available with smart devices.

### 4.6 Comparative study for various DSSE

The comparative study among DSSE’s based on accuracy, computational burden, complexity, mean absolute percentage error (MAPE), absolute value error etc. are summarised in Table 2 from available literatures [62, 67, 76–80] for proper selection and modification of DSSE algorithm.

### 5 CHALLENGES AND FUTURE RESEARCH IN DSSE

In previous section, different classes of DSSE are elaborated. Following section is dedicated to highlight the challenges and future work in state estimation. In over-view, the section includes the issues associated with PMU, SCADA and smart metre. With emergence of cyber layer, the issues associated with cyber security in distribution system namely FDI attack model and detection method, and co-simulation platform is discussed.
The distribution system relies on the SCADA to capture the dynamic scenarios and to monitor the status of distribution system accurately. The large number of PMU’s need to deployed to monitor the voltage phasors and current phasor on incident bus with synchronised GPS [81]. The existing challenge in SE is to synchronise the measurement information obtained on different time scales as PMUs provide measurements within a millisecond whereas SCADA measurements are obtained within an interval of 2 to 10 s. The incoming information of PMU and SCADA need to be processed to avoid the information loss that is packet loss [19]. The measurement data obtained from SCADA and PMU are processed independently with multistage-SE and leading to computational burden [82]. However, these measurements are contaminated with noise other than Gaussian error and need to explored [52]. The large number of nodes in distribution network makes economically infeasible to implement PMUs, the criteria to choose minimum number of PMUs need to be well established for DSSE along with development of low cost PMU. The selection of optimal number and optimal location of PMU poses a challenge for DSSE in distribution system [83]. The DSSE is leveraged with inclusion of PMUs, SCADA and smart metres. Inclusion of smart metre with PMUs and SCADA lead to problem of non-synchronised when measurements are fetched at different time horizon, respectively [84, 85]. The absence of metring in medium voltage (MV) distribution system makes the utility to depend on pseudo-measurements. However, with installation of smart metres in low voltage (LV) and MV estimation have become possible [66]. The DSO relies on the aggregated load data from smart metre and incorrect aggregated load data impacts the voltage and angle estimation in DSSE severely. The insecure smart metre raises the challenges associated with privacy and security of consumer. The utility company enforce the revised policies and regulation for collaborative working with government to preserve the consumer privacy.

5.2 | Miscellaneous challenges in algorithms

With discussion of various DSSE method in Section 4, this section emphasises on miscellaneous challenges in DSSE discussed in selective papers. The real-time monitoring in distribution system is complicated because of network type namely, radial distribution system, meshed and weakly meshed system with varieties of phasing, balanced and unbalanced system. The research is focussed on utilising the data namely, load data (historical data or forecasted data) and to deal with uncertainty in measurement to obtain the correct estimation in DSSE. Table 3 includes miscellaneous collection of paper addressing the problem and research gap in DSSE algorithm.

5.3 | Microgrid state estimation

In the previous section, the brief literature on DSSE algorithms were discussed. The application of static and dynamic state estimator for microgrid state is challenging. DSSE in microgrid need to be explored to capture the real-time events like fault identification, detection and status of circuit breaker [89]. DSSE algorithms are sensitive with measurement data. The microgrid

| Type of DSSE | Algorithm | Pros | Cons |
|-------------|-----------|------|------|
| Voltage based state estimator (VBSE) [5, 18] | Weighted least squares (WLS) | Fast computation | Convergence problem with higher r/x ratio |
| Branch current-based estimator (BCBSE) [3, 46] | WLS | Computationally efficient and can handle unbalanced network | Issue to handle uncertainty in the presence of noise |
| Optimization model-based state estimator [67] | Extended OPF with WLS | Uses the aggregated smart metre data instead of pseudo-measurement | Level of error increases with aggregated metre data than the individual metre data |
| Robust state estimator [48–51] | WLS with machine learning algorithm | Robust for topological variation and can handle under-determined system | Pseudo-measurements depend upon the historical data, needs appropriate co-relation for measurements since accuracy largely depends on historical data |
| Forecast aided state estimator [55–58] | Kalman-based filtering | Predicted states have good accuracy for DERs | Computational burden |
| Multi-area state estimation [63–65, 68, 69] | WLS, and Kalman filtering | Accurate estimation for large area | Results depends on overlapping areas and need to deal with communication errors |

| TABLE 1 Summary of DSSE |
## TABLE 2 Comparison of various DSSE

| Properties                  | Static state estimator                                                                 | Dynamic State estimation                                                                 |
|-----------------------------|----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| DSSE                        | WLS based [14, 76–80]                                                                   | Kalman Filtering Based [88, 6267]                                                         |
|                            | IEEE 13, IEEE 37, IEEE 123                                                             | MV 46 node, smart HG                                                                      |
|                            | MV-46 node, smart HG                                                                    | 12- bus, UK-GDS, IEEE 123                                                                |
|                            | BMVS-46 node                                                                           | MV-46 node                                                                               |
|                            | BC-DSSE rectangular                                                                    | EKF                                                                                        |
|                            | NV-DSSE rectangular                                                                    | EKF-R                                                                                     |
|                            | NV-DSSE polar                                                                          | ACF                                                                                        |
|                            | WLS-reiterative                                                                        |                                             |
|                            | WLV                                                                                        |                                             |
|                            | SHG                                                                                        |                                             |
|                            |                                               |                                             |
| Computation property       | The missing data are considered as equally as bad data. The performance deteriorates above 30% error. | The performance is better upto 35% error. However, in large networks, these estimators are inconsistent |
|                            | The performance is better within 30% error.                                             | These estimators perform better above 30%–40% error. Owing to predictor steps, these estimators perform better. |
|                            | Computation burden                                                                     |                                             |
|                            | Less execution time (app. 21 ms) and iteration (app. 5) to achieve solution             |                                             |
|                            | Slightly more time (app. 45 ms) and iteration (app. 5) to achieve solution              |                                             |
|                            | More time (app. 96.38 ms) and iteration (app. 10)                                       |                                             |
|                            | Higher computational burden (app. 62 ms) and iteration (app. 10)                          |                                             |
|                            | Less execution time (app. 68 ms) and iteration (app. 15)                                |                                             |
| Execution time and iteration | WLS based, that is, static state estimator depends on the size and sparsity of gain matrix. The rectangular based state estimator has superior performance compared to polar co-ordinate based state estimation. | Dynamic state estimators require higher execution time compared to WLS because of predictor steps. |
| Impact of physical property | Less sensitive to network size and convergence as discussed earlier in Section 2)       |                                             |
|                            | Moderate sensitive to network size and convergence is more robust                       |                                             |
|                            | More sensitive to network size and less robust, the estimator takes longer time         |                                             |
|                            | Highly sensitive to network size and less robust                                       |                                             |
|                            | More sensitive to network size and robust                                               |                                             |
| Network parameter error    | Cause the cumulative error in estimation because of forward sweep                       |                                             |
|                            | Cause the uniform deviation in estimation results                                       |                                             |
|                            | Cause the cumulative error resulting into large error in estimation                     |                                             |
|                            | The estimation results are affected severely                                           |                                             |
|                            | Larger deviation in estimated results                                                   |                                             |
| Loading (as in Figures 3–6, Comparison with MPE and APE) | MPE is lesser                        |                                             |
|                            | MPE is less                                                                           |                                             |
|                            | MPE is more and results are affected by loading                                       |                                             |
|                            | MPE is relative less under light loading condition and affects severely under heavy loading and unbalanced condition |                                             |
|                            | MPE is relative less than NV-DSSE polar                                                 |                                             |
|                            | MPE is better compared to WLV                                                           |                                             |
|                            | MPE is better than WLS based estimator                                                  |                                             |
|                            | Overall MPE is less                                                                   |                                             |
| Network topology error     | Convergence rate is not affected                                                       |                                             |
|                            | Convergence rate is affected                                                            |                                             |
|                            | Convergence rate is affected                                                            |                                             |
|                            | Convergence rate is affected severely                                                  |                                             |
|                            | Convergence rate is affected severely                                                  |                                             |
|                            | Convergence rate is affected severely                                                  |                                             |
|                            | Convergence rate is affected severely                                                  |                                             |
|                            | Convergence rate is not affected                                                       |                                             |
|                            | Overall MPE is less                                                                   |                                             |
| AMI and PMU                | Inclusion of AMI and PMU further reduces the execution time and iteration. The PMU inclusion improves the performance of DSSE. |                                             |
| Properties | DSSE Properties | Dynamic State Estimation | Kalman Filtering Based [38, 6267] |
|------------|----------------|---------------------------|----------------------------------|
| 8. Pseudo-measurement | Lesser iteration (app. 6) and execution time (app. 21.45 ms) | Higher number of iterations compared to WLA V (app. 210 ms) and (app. 33) | Estimated results are not consistent in the presence of pseudo-measurement |
| 9. Real-time measurement | The real-time measurement improves the accuracy. However, in the presence of lesser number of real-time measurements, dynamic estimator performs better | The number of iterations are higher and execution time are higher compared to WLS (app. 80 ms) | Estimated results are consistent in the presence of pseudo-measurement |
| 10. Branch power flow and load measurement | Branch power flow improves the performance of estimators. Presence of load measurement increases the computational burden | Higher number of iterations compared to WLS (app. 8) and execution time (app. 98.38 ms) | Estimated results are consistent in the presence of pseudo-measurement |
| 11. Voltage measurement (with reference to 2) | Requires higher computation times | Improved performance and computation time | Improved performance and computation burden |
| 12. Current measurement (with reference to 2) | Improves performance and lesser computation times | Higher computation time and improves the performance | Improved performance and computation burden |
| Performance Indices | MPE | MPE | MPE |
| 13. $|v|_{\text{mean}}$ | $WLS - R > WLS > EKF > WLA V > EKF - R > ACKF$ | $|v|_{\text{mean}}$ |
| 14. $|v|_{\text{max}}$ | $WLS - R > EKF - R > EKF > ACKF > WLS > WLA V$ | $|v|_{\text{max}}$ |
with communication suffers ‘packet data loss’ leading to information loss. To address this issue, filtering techniques namely, Kalman filtering, unscented Kalman filtering and fading channel were proposed in Ref. [90, 91]. The challenges associated with reconfiguration of topological structure in DSSE need to be addressed. The centralised estimator is popular to estimate the observable and controllable states in microgrid. However, corrupt information in centralised state estimation abruptly provide the incorrect estimation. The distributed dynamic DSSE can overcome the central information processing. However, it requires large number of communication channel and parallel processor. DSSE provide the steady state estimation while the electrical transients handling is less investigated. Capturing the transient data is challenging as data has to be sampled at higher rate for providing as input to the state estimators. The communication challenges like bandwidth, resolution and packet data loss need to addressed in microgrid for DSSE algorithm. With proliferation of IoTs, handling and processing of large data is complex and challenging which need to investigated thoroughly [92].

5.4 Harmonic estimation with DSSE

Power electronic converters interfaced with DGs for efficient power flow control contribute to harmonics with other nonlinear loads affecting the power quality. The harmonic estimation and harmonics source estimation play a vital role in DSSE for control decision to incorporate appropriate harmonic compensators for power quality improvement. In DSSE, the states are calculated with fundamental frequency while the harmonics states are estimated with integral multiple of fundamental frequencies. The DSSE is severely affected by impact of harmonics on CT and PT which are used as measuring equipment [93]. The Bayesian approach-based harmonics source estimation with uncertainties is modelled with Gaussian noise in ref. [94]. Owing to the nature of distribution system, obtaining the analytic solution for harmonic estimation is challenging and numerical solver need to be explored without compromising the accuracy. Identification of harmonics sources and their modelling namely, current source and voltage source harmonics need to be investigated [95]. The dynamic filtering algorithms are capable to estimate the harmonics and their sources. However, inter-harmonics problem need to be addressed [96]. Estimation of harmonics sources is complex in absence of measuring devices. With inclusion of PMUs at the harmonic sources can solve the problem. The solution of harmonics estimation in unobservable system is challenging [97]. Harmonic estimation with optimization technique using daily load profile is investigated in ref. [98]. However, the estimation algorithms depending on load curves are time consuming for estimating each harmonic component and harmonics sources. Techniques like singular valued decomposition and Fast Fourier Transform are applied for harmonics state estimation. However, these conventional techniques pose the computational burden and packet fence problem in FFT [99].

| TABLE 2 (Continued) | DSSE | WLS-based [14, 74–76] | Kalman Filtering Based [9, 60–67] | WLS-rectangular | $\text{IEEE 13, IEEE 37, IEEE 123 MV 46 node, smart HG}$ | IEEE-R | $\text{IEEE-R, IEEE 37, IEEE 123 MV 46 node, smart HG}$ | NV-DSSE polar | $\text{IEEE 13, IEEE 37, IEEE 123 MV 46 node, smart HG}$ | WLSV | $\text{IEEE 13, IEEE 37, IEEE 123 MV 46 node, smart HG}$ | WLSAV | $\text{IEEE 13, IEEE 37, IEEE 123 MV 46 node, smart HG}$ | |
|----------------------|-------|-----------------------|---------------------------------|-----------------|---------------------------------|--------|---------------------------------|--------|---------------------------------|--------|---------------------------------|--------|---------------------------------|--------|---------------------------------|
| Properties | $\delta | \text{mean}$ | EKF $>$ WLSAV $> WLS > R > \text{ACKF}< \text{WLS}$ | $\delta | \text{max}$ | WLS $> R > \text{ACKF} > \text{WLSAV} > \text{WLS}$ | $\delta | \text{mean}$ | WLS $> \text{WLSAV} > \text{ACKF} > \text{WLS}$ | $\delta | \text{max}$ | WLS $> \text{WLSAV} > \text{ACKF} > \text{WLS}$ | $\delta | \text{mean}$ | WLS $> \text{WLSAV} > \text{ACKF} > \text{WLS}$ | $\delta | \text{max}$ | WLS $> \text{WLSAV} > \text{ACKF} > \text{WLS}$ | |
| 15. Path value deviation | Approximately identical among statistical estimator | Approximately identical among statistical estimator | Moderately robust | Moderately robust | Moderately robust | Moderately robust | Moderately robust | Moderately robust | Moderately robust | Moderately robust | Moderately robust | Moderately robust | Moderately robust | |
| 16. Power data deviation | Robust, breakdown: Gross error greater than 40 | Robust, breakdown: Gross error greater than 40 | Robust, breakdown: Gross error greater than 40 | Robust, breakdown: Gross error greater than 40 | Robust, breakdown: Gross error greater than 40 | Robust, breakdown: Gross error greater than 40 | Robust, breakdown: Gross error greater than 40 | Robust, breakdown: Gross error greater than 40 | Robust, breakdown: Gross error greater than 40 | Robust, breakdown: Gross error greater than 40 | Robust, breakdown: Gross error greater than 40 | Robust, breakdown: Gross error greater than 40 | Robust, breakdown: Gross error greater than 40 | |
| 17. Gross error | Breakdown reaches in number of gross error greater than 9. Less robust | Breakdown reaches in number of gross error greater than 9. Less robust | Breakdown reaches in number of gross error greater than 9. Less robust | Breakdown reaches in number of gross error greater than 9. Less robust | Breakdown reaches in number of gross error greater than 9. Less robust | Breakdown reaches in number of gross error greater than 9. Less robust | Breakdown reaches in number of gross error greater than 9. Less robust | Breakdown reaches in number of gross error greater than 9. Less robust | Breakdown reaches in number of gross error greater than 9. Less robust | Breakdown reaches in number of gross error greater than 9. Less robust | Breakdown reaches in number of gross error greater than 9. Less robust | Breakdown reaches in number of gross error greater than 9. Less robust | |
| 18. Bad data detection | Approximately identical among statistical estimator | Approximately identical among statistical estimator | Approximately identical among statistical estimator | Approximately identical among statistical estimator | Approximately identical among statistical estimator | Approximately identical among statistical estimator | Approximately identical among statistical estimator | Approximately identical among statistical estimator | Approximately identical among statistical estimator | Approximately identical among statistical estimator | Approximately identical among statistical estimator | Approximately identical among statistical estimator | Approximately identical among statistical estimator | |
5.5 | Interaction between TSO and DSO

DSSE plays a key role in energy management of active distribution systems. Integration of DER with transmission system has encouraged the ancillary service. Similar idea of ancillary service support needs to be extended in active distribution system. The interaction between transmission system operator (TSO) and DSO is important for energy trading and flexible grid operation. The DSO can support the TSO with active power support in case of congestion. The interaction between TSO and DSO need to be encouraged with ancillary services and energy transaction policies. Hence, it is necessary to develop the effective co-ordination and control tools to monitor transmission and distribution system. However, combined state estimation between the transmission and distribution system need to be established for effective monitoring. Issues and challenges in TSO and DSO interaction are addressed in Ref. [100–103].

6 | CYBERSECURITY ASPECTS IN DSSE

In a CPS, the application and decision layer receives the telemetryed data from a measuring and sensing units via communication layer as shown in Figure 1. In order to understand the DSSE in CPS, consider Figure 7, where the control centre receives data from RTUs via the ICT network and estimate the state of a distribution system with DSSE in EMS platform. Figure 7 illustrates the interaction among the physical system with a help of bidirectional communication network. These communication network namely, wide area network (WAN), neighbourhood area network (NAN), home area network (HAN) along with information network plays the crucial role for system operation [104, 105]. However, they are also vulnerable to cyber-attacks as shown with RED dots in Figure 7 and provide an opportunity to compromise the system. It is noted that cyber-attack can be in the form of denial of service (DoS), data spoofing or FDI [106]. As the focus of this review paper is on FDI, following section investigates only FDI attack on DSSE in distribution system. In order to understand the impact of an FDI attack (in cyber layer) on a physical system, consider a targeted and random FDI attack at RTU to manipulate the measurement data. This manipulated data processed with DSSE in control centre generates an inappropriate reference and actuating signal to mislead the operator for undesired system operation and further disrupting the physical infrastructure.

This can be understood in detail from Figure 8 where an FDI attack on power system affecting state estimation in EMS. The deceptive FDI bypass the bad data detection (BDD) misleading the DSO to take incorrect decision in distribution system functionalities namely, forced volt-var operation affecting physical infrastructure. However, an early detection of FDI attack aids the DSO in implementing corrective actions. It is noted that the cyber-attacks on state estimations are financially motivated to cause economical and physical loss [107–109]. The FDI attack in transmission system are well known and such attack in distribution system are least explored. Table 4 provides the summary of FDI attacks and their impact. In order to protect the distribution system from cyber threat, it is mandatory to understand the attack strategy. This section highlights the construction of attack vector, detection methods and the impact of FDI attack on the system.

6.1 | FDI attack on power system communication

With the IoT’s, the devices talk and communicate each other through the exchange of packet data. The intentional and careful injection of these packet data leads to modification of packet causing the false information. The FDI attack on PMU data includes the replay type attack where the data are repeated
after time interval, and GPS spoofing [136]. However, these FDI attack challenges are growing concern for power grid operator where the IoT devices operates on interoperability principle and the information of operating devices becomes easily to available for third party [137].

6.2 Mathematical model of FDI

The DSSE determines the operating states namely, voltage magnitude and angle, status of circuit breakers (CB), status of capacitor bank and taps of transformer. The intentional manipulated measurements bypass the BDD in DSSE and mislead the operator to take unintentional action namely, opening of CB, load shedding etc. The FDI attack model in distribution system is derived from the concept of FDI attack on dc power flow model. The linearised measurement model is $z = Hx + e$ where $z = z + a; x = x + a$. The attack vector $a$ is expressed as the linear combination of error vector $e$ as $a = Hc$ [107]. In the case of AC power flow-based DSSE, for the measurement function (Equation 1) the attack vector is derived as Equation (29) [107]. Where $a = b(x_a) - b(x)$, the attack vector $a$ has to be designed such that $z - b(x) \leq \tau$ where $\tau$ is the threshold.

$$r_a = z_a - b(x_a) = z_a - b(x_a) + b(x) - b(x) = z + a$$

$$- b(x_a) + b(x) - b(x) = z + a - b(x_a) + b(x)$$

(29)

In three phase distribution system, the power flow equation is expressed as Equations (30) and (31) [139]. $P$ and $Q$ are power injection; $i$ and $j$ are the node; $N$ is the total number of nodes; $\alpha$ and $\beta$ are the phase; $\alpha, \beta \in \{a, b, c\}$. For the distribution system, the increment or decrement in power equation needs to be computed to bring the estimated change in state variable.

$$P_i^e = V_i^a \sum_{\beta=a,b,c}^N \sum_{j=1}^{N_{\beta}} V_j^a \left( G_{ij}^\alpha \cos\theta_{ij}^\beta + B_{ij}^\beta \sin\theta_{ij}^\beta \right)$$

(30)

$$Q_i^e = V_i^a \sum_{\beta=a,b,c}^N \sum_{j=1}^{N_{\beta}} V_j^a \left( G_{ij}^\alpha \sin\theta_{ij}^\beta - B_{ij}^\beta \cos\theta_{ij}^\beta \right)$$

(31)

As discussed in ref. [119], the condition like energy balance, KCL and KVL need to be satisfied for successful attack. The FDI attack on optimal power in distribution system is investigated in ref. [141] to maximise the generation cost $C_i$ for
The generation of complex power $s_i$ with decision variable $s$ and voltage $V$ as in Equation (32).

$$\text{Minimize } \sum_{i \in N} C_i(s_i, \Theta)$$  \hspace{1cm} (32)

Subject to:

a. Ohm’s law: $I_{ij} = y_{ij}(V^{\Theta}_{ij} - V^{\Theta}_{ji})$

b. Current balance: $I_i = \sum_{j \neq i} I_{ij}$

TABLE 4  Summary of impact/analysis and scope in cyber attack

| Impact/analysis                                      | Method                                                                 | Scope                                                                 |
|------------------------------------------------------|------------------------------------------------------------------------|----------------------------------------------------------------------|
| FDI on contingency analysis to change the locational marginal price with security constrained economic dispatch by using DC state estimation [110, 111] | Estimation attack using MILPMislead the operator by manipulating contingency | No defence mechanism is provided along. AC state estimation need to be investigated along with FDI impact on dynamic contingency analysis |

The false data injection attacks are much popular as they impact the economy with malicious intention to again the profit or make loss of rival. Some attacks like ramp-based attack on multi-settlement market with false virtual bid may sabotage the market operation [112–121].

Risk assessment by FDI construction

FDI construction using the linear property

Assumption: Attacker have network information

The blind attack with no network information was investigated [117]

Construction by the principal component analysis

Assumption: Attacker has no network information (blind attack).

Topology attack [118]

FDI by heuristic algorithm

The scope of topology attack can be extended to study cyber vulnerability in physical system

Risk and vulnerability assessment are the prime concern for FDI, the scope should be extended to develop of co-simulation platform for assessing the FDI attacks. However, understanding cyber-physical infrastructure plays the vital role for vulnerability assessment [69, 119–122].

FDI detection

Short term forecasting temporal correlation [123]

Infinite and L2 norm

Topology attack and load distribution attack

Investigated the false positive and false negative rate and effect on economic dispatch was studied to compare the predicted state and to compute the threshold [124]

Online anomaly detection

Attack vector is constructed according linear combination to pass the bad data detection as guidance provided in ref. [125]

Real time detection of FDI [126]

Based on Bayesian properties and user defined rules Adaptive CUSUM method. Performance analysis Markov chain based to perform analytical model

Load/generation disruption and joint consideration with PMU

Detection of FDI is the challenging, where it requires to understand the attacker’s/adversary’s policies. Further, literature on real time detection based on statistics and expert system can be found in Ref. [123, 124, 125–128].

Denial of service (DoS) [129, 130]

Kalman filter with disturbance observer emulates the sensor. Chi-square method and statistical method is used to cluster SCADA is serves as the fundamental layer for communication protocol, the DNP3 communication protocol need to investigated for protection from DoS

SCADA is serves as the fundamental layer for communication protocol

Impact on distributed energy resources

FDI impact on load sharing of inverter in microgrid [131]

FDI on discrete consensus algorithm (attack model)

Detection system and defending method need to be developed

Impact on voltage control by accessing the converter to increase or decrease the voltage [132]

Based on the knowledge on voltage limits Assumption: The knowledge of control is known by attacker

High proliferation of DERs with cyber physical component is prone to the cyber-attacks. The attacker with knowledge of DER control scheme is capable to change the references for reactive power and thus can affect the voltage stability further levitating to voltage collapse. Understanding the DER for the risk assessment is prime concern [133–135].
The FDI attacks are initiated to minimise the social welfare [141] with objective function is expressed as Equation (33), \[ |\text{Bid}_N| \] bid price for node N with change in power \( \Delta S_N \) with constraints as (a)-(e).

\[
\text{Minimize } \sum_{n=1}^{N} -|\text{Bid}_n| \Delta s_n \tag{33}
\]

The distribution system control by SCADA plays the vital information exchange from substation equipment to DSO through communication protocol namely, DNP3, Modbus etc. The FDI attack at substation on load tap changer transformer (LTC) was investigated [142] with an objective to decrease the efficiency and to increasing the operating cost of transformer. The attack model is described in Equation (34).

\[
V_{\text{FDI}} = V_{\text{reg}} - \Delta V_{\text{tap}} \ast (k + \Delta k) \tag{34}
\]

where \( V_{\text{FDI}} \) is the voltage reference with additional tap \( \Delta k \) and \( \Delta V_{\text{tap}} \) change voltage. The \( \Delta k \) is manipulated so that limit is not violated and the attack remains deceptive (Equation 35).

\[
k_{\text{min}} \leq (k + \Delta k) \leq k_{\text{max}} \tag{35}
\]

The game theoretic approach plays the significant role to build the attacker’s model. Based on this approach, the volt-var control was misguided to increase the cost of operation. The objective function is defined with operating constraints is to maximise \( f(x, c) \) where \( f \) is the cost function \( x \) is the operating constraints, \( c \) denotes the capacitor bank [143].

### 6.3 FDI in distribution system

The FDI attacks in distribution system are crucial and less investigated owing to absence of large monitoring system. At present, the increased number of ICT in distribution system with inclusion of PMU, SCADA and AMI have increased the risk of cyber-attack namely, FDI on DSSE. Undetected FDI attack impacts the distribution system operation namely, volt-var, voltage level etc. [144]. The attack vectors were constructed to modify the power flow and injection measurement with strong relaxation that is information of neighbouring states at attack points are known [144]. Due to high \( r/x \) ratio, the FDI constructed with ac model have lesser probability of getting detected compared to attack vector constructed with dc model [144]. Very few literatures are available on FDI attack for unbalanced distribution system [145, 146]. The attacker needs the information of system topology and access to measurement to compromise large number of state variables in unbalanced and multi-phase system for successful attack. With available information, the attacker develops the linear state estimator for attack construction [146]. The large amount of data is fetched through smart metres and synchrophasors. Any corruption in these data made intentionally affects the reference generated by state estimator. For example, the feeder voltage profile controlled by volt-var optimization by utilising data from smart metres. Such data need to be secured which are utilised to derive a control signal in distribution system. In ref. [147], attack vector was constructed with mixed integer linear programing to mislead DSO. The cyber risks associated with distribution system automation were discussed and security protocols were proposed [148, 149].

### 6.4 FDI attack in microgrid

The community-based microgrid is serving as backbone to satisfy the peak energy demand and are monitored with state estimator. Recently, the vulnerabilities of microgrids with FDI and DoS attacks have been studied. The cyber-attacks can impact on functionalities such as voltage regulation, load curtailment, load sharing and battery dispatchment. The power electronics converter interfaced with renewable energy sources are operated with centralised or decentralised controllers with communication and control variables are estimated with distributed state observer. In FDI attack, the attacker gain access to few control variables limiting attack zone and other possibility that attacker can access all control variable to have maximum impact of damage. Hence, it becomes necessary for system operator to protect the set measurements optimally so as to avoid the FDI attack. The attack vectors in microgrid are constructed without violating the energy balance [150]. FDI attacks in the microgrid operation were investigated with connected graph constrained Knapsack (CGKP) and security matrix was proposed [151]. The agent-based control in microgrid for central energy has been implemented in literature [151]. The attacker formulated unit commitment problem to construct FDI successfully for load curtailment [152]. In community-based microgrid optimal attack vectors are constructed to make profit by intervening in market operation [153]. In multi-agent, the agents are assumed to be communicating with synchronous time step whereas synchronous update makes difficult to identify the corrupt agent. The secure DSSE with diffusion algorithm to identify the corrupt agent was proposed [153]. However, the challenges in smart communication have been discussed in literature [154]. The temporal logic-based detection techniques have been proposed in dc microgrid [155]. FDI attack detection with deceptive attack strategy is challenging. Hence, the framework for attack detection and mitigation should be addressed for detection and mitigation.

### 6.5 FDI attack detection

Securing the power system offers the challenge to system operator because of stealth and deceptive attack. The FDI...
attack detection techniques developed for transmission system are applicable to distribution system. The detection techniques are categorised as follow:

- **Traditional detection method (TDM)** [7, 156]: The normalised residual method and chi-square based method are used to detect the false data and these methods fail to detect the stealth attack.

- **Tempo-spatial detection (TSD)** [157, 158]: Spatial correlation region for the estimates is defined and those sets belonging to regions are considered to be consistent. The sets $s_{ij}$ and $s_{ji}$ are the correlation estimates for time $t$ and smart component $i$ and $j$, respectively. For the consistency the datasets are processed through principal component analysis (PCA). The Figure 9 depicts the consistency region. The other method is trust-based voting where $G$ is the correlation space. Let $N_i$ be the set of all estimation and $N_i^c$ denotes the consistent estimation. $N_i$ and $N_i^c$ $\in G$. The estimation sets are reliable when $\frac{|N_i|}{|N_i^c|} \geq 50\%$ rest are classified as anomaly.

- **Data science-based method**: The binary classification problem for detection of FDI is given as Equation (36) [159].

$$ y = \begin{cases} 1, & \text{if } a \neq 0 \text{ i.e. attackable} \\ -1, & \text{if } a = 0 \text{ i.e. non-attackable} \end{cases} \quad (36) $$

The comparison among the FDI detectors with the support vector machine (SVM), K-nearest neighbour (KNN) and extended nearest neighbour (ENN) were comparatively studied with detection accuracy (37) as performance matrix [159]. Let $tp$, $tn$, $fp$ and $fn$ be true positive, true negative, false positive and false negative. $P$ denotes the fractional of measurement compromised where $P = \frac{tp}{tp + tn + fp + fn}$. $m$: total measurement, $k$: Number of measurement compromised. $A$ denotes the variance. The detection accuracy (acc) as given in Equation (37). The detection method with $0.5 \leq P \leq 0.8$ and $0.1 \leq A \leq 0.2$ detection accuracy for SVM is $90\% - 95\%$ while $80\% - 85\%$ in KNN and ENN as shown in Figure 10.

$$ acc. = \frac{|tp| + |tn|}{|tp| + |tn| + |fp| + |fn|} \quad (37) $$

- **Miscellaneous detection**: The attack detection method namely, binary-based, singular value decomposition and Kalman filtering is explored in briefly with centralised and distributed controller [160, 161].

- **Issues with detection**: The window selection in tempo-spatial plays the critical role in identification of bad data. The false positive in tempo-spatial detection can be overcome by machine learning algorithm. The real-time FDI detection needs to be robust and address the missing data in detection method [157, 158, 161]. The practical detection method performance varies with type of attack and the attack may pass undetected. The detection method should be robust and updated over the span of time. The much of control strategy is focussed on centralised state estimation. However, owing to emergence of distributed state estimation where the local states and physical system are known and easy access to local variable is possible. This opens the challenge for attack detection in distributed state estimation.

### 6.6 Vulnerability of DSSE algorithm to FDI attack

As discussed briefly in Section 4, the performance and estimation capability of DSSE algorithm depends on factors such as measurement model, measurement type namely, metered and pseudo-measurement. There exists a strong correlation between system measurements and state variables in DSSE, and a cyber-attacker can exploit the measurements variance to construct the FDI attack vectors. The methods of FDI attack vector construction discussed in Ref. [139–155, 163] are based on assumption of prior knowledge of network information, state variables and state estimator. A comparative study of FDI attack on different DSSE algorithms is not available in literature and it would be interesting to understand the impact of FDI attack on different DSSE algorithms in terms of estimation result. The authors are currently working on it and believe that among static, dynamic and data-driven DSSE, the data-driven estimator could be a powerful tool to predict the residues prior to estimation [164]. However, it’s necessary to develop attack resilient DSSE in the presence of deceptive attacks. The FDI attack strategy on
different DSSE algorithms needs to be investigated as part of vulnerability and security analysis of distribution system.

6.7 | Co-simulation platform

Figure 1 describes the more generic layout for the CPS, enforcing the need of interacting platform between the physical power network and the information and communication network. The different layers as shown in Figure 1, need to be simulated and modelled with different computing software platform which is collectively termed as the co-simulation platform. The co-simulation platform for CPS is built with extreme knowledge of modelling of physical network with application of optimization to mimic the real-world scenario. Different co-simulation platform are discussed in literature [163–165]. The open source platforms are playing major role for the development of co-simulation platform. The benchmarking of co-simulation was provided with open source software on the cloud-based interface [150]. Developments of co-simulation platform helps to analyse the power network failure and communication mal-function caused by faults or caused with intentionally like cyber-attack. The major challenge for co-simulation is to model the events that are time based like power network event or the discrete events like the communication and to synchronise the time-based and discrete events. The interoperability among different software namely, open source (licenced in public domain) and the paid software (licenced to individuals) need to be addressed [69, 168, 169].

7 | CONCLUSION

The interaction of physical and cyber layer plays a vital role for the controlling the power system operations where DSSE has the significant role in energy management system. Owing to present scenario with distributed energy resources, monitoring the grid status is mandatory. As part of DSSE, the problem related to time synchronisation among smart metre, PMU and SCADA need to be investigated for better performance in DSSE. Along the line, the algorithm having low computational burden need to be investigated and process to handle the pseudo-measurements need to be developed extensively in multi-area state estimation. The security concern of state estimation cannot be discarded, as efforts have to make for protection and detection of cyber-attacks like false data injection (FDI) attack, denial of service and data spoofing. The FDI attack is critical issue that can disrupt the system operation. However, through the literature survey along the security aspects and the impacts of FDI have been discussed. The risk assessment has to be carried so as to protect the cyber-physical system (CPS) against cyber-attacks. The denial of service attack is more critical in security aspects of power network, the focus should be made to know and to understand such attacks in CPS. Owing to interaction of information and communication layer in power network, the software platform that is co-simulation should be developed more accurately to mimic the real time scenario to understand the power network operation in case of cyber-attacks or the ICT failures.

ORCID
Poornachandratejavi Laxman Bhattar © https://orcid.org/0000-0002-8918-0305
Naran M. Pindoriya © https://orcid.org/0000-0002-0551-2828

REFERENCES
1. Liu, S., et al.: The healing touch: tools and challenges for smart grid restoration/IEEE Power Energy Mag. 12(1), 54–63 (2014)
2. Fernandez, L.P., et al.: Assessment of the impact of plug-in electric vehicles on distribution networks/IEEE Trans. Power Syst. 26(1), 206–213 (2010)
3. Baran, M.E., Kelley, A.W.: A branch-current-based state estimation method for distribution systems/IEEE Trans. Power Syst. 10(1), 483–491 (1995)
4. Wang, H., Schulz, N.N.: A revised branch current-based distribution system state estimation algorithm and meter placement impact/IEEE Trans. Power Syst. 19(1), 207–213 (2004)
5. Baran, M.E., Kelley, A.W.: State estimation for real-time monitoring of distribution systems/IEEE Trans. Power Syst. 9(3), 1601–1609 (1994)
6. London, J.B.A., et al.: Redundancy and observability analysis of conventional and PMU measurements. IEEE Trans. Power Syst. 24(3), 1629–1630 (2009)
7. Alber, A., Espósito, A.G.: Power system state estimation: theory and implementation. CRC Press (2004)
8. Monticelli, A.: Electric power system state estimation. Proc. IEEE. 88(2), 262–282 (2000)
9. Gu, J.W., et al.: The solution of ill-conditioned power system state estimation problems via the method of Peters and Wilkinson. IEEE Trans. Power Appar. Syst. 10, 3473–3480 (1983)
10. Hansen, C.W., Debs, A.S.: Power system state estimation using three-phase models/IEEE. Trans. Power Syst. 10(2), 818–824 (1995)
11. Whi-Min, L., Jen-Hao, T.: State estimation for distribution systems with zero-injection constraints/IEEE. Trans. Power Syst. 11(1), 518–524 (1996)
12. Lin, W.M., Teng, J.H.: State estimation for distribution systems with zero-injection constraints. In: Proceedings of Power Industry Computer Applications Conference, pp. 523–529. IEEE (1995)
13. Korres, G.N.: A robust algorithm for power system state estimation with equality constraints/IEEE. Trans. Power Syst. 25(3), 1531–1541 (2010)
14. Singh, R., Pal, B.C., Jabar, R.A.: Choice of estimator for distribution system state estimation/ IET Gener. Transm Distrib. 3(7), 666–678 (2009)
15. Haughton, D.A., Heydt, G.T.: A linear state estimation formulation for smart distribution systems/IEEE. Trans. Power Syst. 28(2), 1187–1195 (2012)
16. Jiang, X.T., et al.: Power system state estimation using a direct non-iterative method/Int. J. Electr. Power Energy Syst. 73, 361–368 (2015)
17. Jiang, X.T., et al.: Pre-commercial demonstration of a direct non-iterative state estimator. In: 2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), pp. 1–9. IEEE (2018)
18. Lu, C.N., Teng, J.H., Liu, W.-H.: Distribution system state estimation. IEEE Trans. Power Syst. 10(1), 229–240 (1995)
19. Das, K., et al.: Real-time hybrid state estimation incorporating SCADA and PMU measurements. In: 2012 3rd IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe), pp. 1–8. IEEE (2012)
20. Kersting, W.H.: Distribution system modelling and analysis. CRC Press (2012)
21. Xiao, P., Yu, D.C., Yan, W.: A unified three-phase transformer model for distribution load flow calculations. IEEE. Trans. Power Syst. 21(1), 153–159 (2006)
64. Muscas, C., et al.: Multiarea distribution system state estimation. IEEE Trans. Instrum. Meas. 64(5), 1140–1148 (2015)

65. Kang, J.-W., Choi, D.-H.: Distributed multi-area WLS state estimation integrating measurements weight update. IET Gener. Transm. Distrib. 11(10), 2552–2561 (2017)

66. Ni, F., et al.: Three-phase state estimation in the medium-voltage network with aggregated smart meter data. Int. J. Electr. Power Energy Syst. 98, 463–473 (2018)

67. Hayes, B., Prodanovic, M.: A comparison of MV distribution system state estimation methods using field data. In: 2015 IEEE Power & Energy Society General Meeting, pp. 1–5. IEEE (2015)

68. Muscas, C., et al.: Fast multi-area approach for distribution system state estimation. In: 2016 IEEE International Instrumentation and Measurement Technology Conference Proceedings, pp. 1–6. IEEE (2016)

69. Pan, K., et al.: Cyber risk analysis of combined data attacks against power system state estimation. IEEE Trans. Smart Grid. 10(3), 3044–3056 (2018)

70. Huang, M., et al.: Hybrid state estimation for distribution systems with AMI and SCADA measurements. IEEE Access. 7, 120350–120359 (2019)

71. Ferdowsi, M., et al.: A scalable data-driven monitoring approach for distribution systems. IEEE Trans. Instrum. Meas. 64(5), 1292–1305 (2015)

72. Weng, Y., et al.: Robust data-driven state estimation for smart grid. IEEE Trans. Smart Grid. 8(4), 1956–1967 (2016)

73. Zamzam, A.S., Fu, X., Sidirooulos, N.D.: Data-driven learning-based optimization for distribution system state estimation. IEEE Trans. Power Syst. 34(6), 4796–4805 (2019)

74. Ferdowski, M., et al.: Measurement selection for data-driven monitoring of distribution systems. IEEE Trans. Syst. J. 13(4), 4260–4268 (2019)

75. Dehghanpour, K., et al.: A game-theoretic data-driven approach for pseudo-measurement generation in distribution system state estimation. IEEE Trans. Smart Grid. 10(6), 5942–5951 (2019)

76. Alzate, E.B., et al.: Distribution system state estimation to support coordinated voltage-control strategies by using smart meters. IEEE Trans. Power Syst. 34(6), 5198–5207 (2019)

77. Primadianto, A., Lin, W.T., Lu, C.N.: Performance comparison of distribution system state estimation methods. In: 2016 IEEE Innovative Smart Grid Technologies-Asia (ISGT-Asia), pp. 1121–1126. IEEE 2016

78. Pau, M., Pegoraro, P.A., Sulis, S.: Performance of three-phase WLS distribution system state estimation approaches. In: 2015 IEEE International Workshop on Applied Measurements for Power Systems (AMPS), pp. 138–143. IEEE (2015)

79. Primadianto, A., et al.: Requirements of state estimation in smart distribution grid. In: Proc. 23rd Int. Conf. Electr. Distrib. 2015, 2015 (2015)

80. Pohlner, B.R., Bak-Jensen, B., R Pillai, J.: Integrated approach for network observability and state estimation in active distribution grid. Energies. 12(12), 2230 (2019)

81. Huang, Y.-F., et al.: State estimation in electric power grids: meeting new challenges presented by the requirements of the future grid. IEEE Signal Process. Mag. 29(5), 33–43 (2012)

82. Albuquerque, A., Bez, D., Simões, A.: Multistage strategies to incorporate phasor measurements into power system state estimation’ 2015 IREP Symposium Bulk Power System Dynamics and Control-IX Optimization, Security and Control of the Emerging Power Grid’ pp. 1–11. IEEE. (2013)

83. Maci, D., Barchi, G., Schenato, L.: On the role of phasor measurement units for distribution system state estimation. In: 2014 IEEE Workshop on Environmental, Energy, and Structural Monitoring Systems Proceedings, pp. 1–6. IEEE (2014)

84. Alimardani, A., et al.: Distribution system state estimation based on nonsynchronized smart meters. IEEE Trans. Smart Grid. 6(6), 2919–2928 (2015)

85. Chen, Q., et al.: Impact of smart metering data aggregation on distribution system state estimationIEEE Trans. Ind. Inform. 12(4), 1426–1437 (2016)

86. Majidi, M., Etezadi-Amoli, M., Livani, H.: ‘Distribution system state estimation using compressive sensing’ Int. J. Electr. Power Energy Syst., 88, pp. 175–186 (2017)

87. Al-Wakeel, A., Wu, J., Jenkins, N.: State estimation of medium voltage distribution networks using smart meter measurements. Appl. Energy. 184, 207–218 (2016)

88. Majidi, M., et al.: Distribution systems state estimation using sparsified voltage profile. Electr. Power Syst. Res. 136, 69–78 (2016)

89. Choi, S., Meliopoulos, A.P.S.: Effective real-time operation and protection scheme of microgrids using distributed dynamic state estimation. IEEE Trans. Power Deliv. 32(1), 504–514 (2017)

90. Huang, J., Gupta, V., Huang, Y.-F.: Electric grid state estimators for distribution systems with microgrids. In: 2012 46th Annual Conference on Information Sciences and Systems (CISS), pp. 1–6 (2012)

91. Rana, M.M.: Modelling the microgrid and its parameter estimations considering fading channels. IEEE Access. 5, 10953–10958 (2017)

92. Rana, M.M., Xiang, W., Wang, E.: IoT-based state estimation for microgrids. IEEE Internet Things J. 5(2), 1345–1346 (2018)

93. Muscas, C.: Power quality monitoring in modern electric distribution systems. IEEE Instrum. Meas. Mag. 13(5), 19–27 (2010)

94. D’Antona, G., Muscas, C., Sulis, S.: State estimation for the localization of harmonic sources in electric distribution systems. IEEE Trans. Instrum. Meas. 58(5), 1462–1470 (2009)

95. Kawasaki, S., Ogasawara, G.: Influence analyses of harmonics on distribution system in consideration of non-linear loads and estimation of harmonic source. J. Int. Counc. Electr. Eng. 7(1), 76–82 (2017)

96. Singh, S.K., et al.: Several variants of Kalman Filter algorithm for power system harmonic estimation. Int. J. Electr. Power Energy Syst. 78, 793–800 (2016)

97. Melo, I.D., et al.: Harmonic state estimation for distribution networks using phasor measurement units. Electr. Power Syst. Res. 147, 133–144 (2017)

98. Melo, I.D., et al.: ‘Harmonic state estimation for distribution systems based on optimization models considering daily load profiles. Electr. Power Syst. Res. 170, 303–316 (2019)

99. D’Antona, G., et al.: Harmonic source estimation in distribution systems. In: 2010 IEEE International Workshop on Applied Measurements for Power Systems, pp. 59–63 (2010)

100. Silva, J., et al.: The challenges of estimating the impact of distributed energy resources flexibility on the TSO/DSO boundary node operating points. Comput. Oper. Res. 96, 294–304 (2018)

101. Gerard, H., Rivero Puente, E.I., Six, D.: Coordination between transmission and distribution system operators in the electricity sector: a conceptual framework. Util. Policy. 50, 40–48 (2018)

102. Hadush, S.Y., Meeus, L.: DSO–TSO interaction: active distribution network for TSO ancillary services provision. Electr. Power Syst. Res. 163, 226–230 (2018)

103. Capitanescu, F.: TSO–DSO interaction: active distribution network power chart for TSO ancillary services provision. Electr. Power Syst. Res. 163, 226–230 (2018)

104. Yu, R., et al.: Cognitive radio based hierarchical communications infrastructure for smart grid. IEEE Netw. 25(5), 6–14 (2011)

105. Sun, C.-C., Liu, C.-C., Xie, J.: Cyber-physical system security of a power grid: state-of-the-art. Electronics. 5(3), 40 (2016)

106. Liang, G., et al.: The 2015 Ukraine Blackout: implications for false data injection attacks. IEEE Trans. Power Syst. 32(4), 3317–3318 (2017)

107. Liu, Y., Ning, P., Reiter, M.K.: False data injection attacks against state estimation in electric power grids. ACM Trans. Int. Syst. Secur. TISSEC. 14(1), 1–33 (2011)

108. Liang, G., et al.: A review of false data injection attacks against modern power systems. IEEE Trans. Smart Grid. 8(4), 1630–1638 (2016)

109. Deng, R., et al.: False data injection on state estimation in power systems---attacks, impacts, and defense: a survey. IEEE Trans. Ind. Inform. 13(2), 411–423 (2016)

110. Kang, J.-W., Joo, I.-Y., Choi, D.-H.: False data injection attacks on contingency analysis: attack strategies and impact assessment. IEEE Access. 6, 8841–8851 (2018)
111. Che, L., et al.: False data injection attacks induced sequential outages in power systems. IEEE Trans. Power Syst. 34(2), 1513–1523 (2018)

112. Choi, D.-H., No, L.: Ramp-induced data attacks on load-ahead dispatch in real-time power markets. IEEE Trans. Smart Grid. 4(3), 1235–1243 (2013)

113. Jiongcong, C., et al.: Impact analysis of false data injection attacks on power system static security assessment. J. Mod. Power Syst. Clean Energy. 4(3), 496–505 (2016)

114. Moslemi, R., Mesbahi, A., Velni, J.M.: Design of robust profitable false data injection attacks in multi-settlement electricity markets. IET Gener. Transm. Distrib. 12(6), 1263–1270 (2017)

115. Choi, D.-H., No, L.: Economic impact assessment of topology data attacks with virtual bids. IEEE Trans. Smart Grid. 9(2), 512–520 (2016)

116. Bobba, R.B., et al.: Detecting false data injection attacks on state estimation. In: Preprints of the First Workshop on Secure Control Systems. CPSWEEK’ (2010)

117. Yu, Z.H., Chen, W.-L.: Blind false data injection attack using PCA approximation method in smart grid. IEEE Trans. Smart Grid. 6(3), 1219–1226 (2015)

118. Liu, X., Li, Z.: Local topology attacks in smart grids. IEEE Trans. Smart Grid. 8(6), 2617–2626 (2016)

119. Hug, G., Giampapa, J.A.: Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. IEEE Trans. Smart Grid. 3(3), 1362–1370 (2012)

120. Ozay, M., et al.: Sparse attack construction and state estimation in the smart grid: centralized and distributed models. IEEE J. Sel. Areas Commun. 31(7), 1306–1318 (2013)

121. Liang, J., Sankar, L., Kout, O.: Vulnerability analysis and consequences of false data injection attack on power system state estimation. IEEE Trans. Power Syst. 31(5), 3864–3872 (2015)

122. Ding, Z., Xiang, Y., Wang, L.: Incorporating unidentifiable cyberattacks into power system Reliability assessment. In: 2018 IEEE Power & Energy Society general meeting, pages 1–5. IEEE (2018)

123. Zhao, J., et al.: Short-term state forecasting-aided method for detection of smart grid general false data injection attacks. IEEE Trans. Smart Grid. 8(4), 1580–1590 (2015)

124. Ashok, A., Govindarasu, M., Aijarapu, P.: Online detection of stealth false data injection attacks in power system state estimation. IEEE Trans. Smart Grid. 9(3), 1636–1646 (2016)

125. Xu, C., Abur, A.: Robust linear state estimation for large multi-area power grids. In: 2016 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT), pp. 1–5. ISGT (2016)

126. Singh, S.K., et al.: Joint-transformation-based detection of false data injection attacks in smart grid. IEEE Trans. Ind. Inform. 14(1), 89–97 (2017)

127. He, Y., Mendis, G.J., Wei, J.: Real-time detection of false data injection attacks in smart grid: a deep learning-based intelligent mechanism. IEEE Trans. Smart Grid. 8(5), 2505–2516 (2017)

128. Kurt, M.N., Yilmaz, Y., Wang, X.: Real-time detection of hybrid and stealthy cyber-attacks in smart grid. IEEE Trans. Inf. Forensics Secur. 14(2), 498–513 (2018)

129. Rigatos, G., Serpanos, D., Zervos, N.: Detection of attacks against power grid sensors using Kalman filter and statistical decision making. IEEE Sensors J. 17(2), 7641–7648 (2017)

130. Manandhar, K., et al.: Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. IEEE Trans. Control Netw. Syst. 1(4), 370–379 (2014)

131. Zhang, H., et al.: Distributed load sharing under false data injection attack in an inverter-based microgrid. IEEE Trans. Ind. Electron. 66(2), 1543–1551 (2018)

132. Isosaki, Y., et al.: Detection of cyber attacks against voltage control in distribution power grids with PVs. IEEE Trans. Smart Grid. 7(4), 1824–1835 (2016)

133. Sharma, D.D., et al.: Agent-based distributed control schemes for distributed energy storage systems under cyber attacks. IEEE J. Emerg. Sel. Top. Circuits Syst. 7(2), 307–318 (2017)

134. Teymouri, A., Mehtiz-Sani, A., Liu, C.-C.: Cyber security risk assessment of solar PV units with reactive power capability. In: IEEE 2018-44th Annual Conference of the IEEE Industrial Electronics Society, pp. 2872–2877. IEEE (2018)

135. Majumdar, A., et al.: Centralised volt–var optimization strategy considering malicious attack on distributed energy resources control. IEEE Trans. Sustain. Energy. 9(1), 148–156 (2018)

136. Shepard, D.P., Humphreys, T.E., Finsler, A.A.: Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. Int. J. Crit. Infrastr. Prot. 5(3), 146–153 (2012)

137. Sundararajan, A., et al.: Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies. J. Mod. Power Syst. Clean Energy. 7(3), 449–467 (2019)

138. Rahman, M.A., Mohsenian-Rad, H., pp. 1–5: False data injection attacks against nonlinear state estimation in smart power grids. 2015 IEEE Power & Energy Society General Meeting (2013)

139. Wang, Y., et al.: Linear three-phase power flow for unbalanced active distribution networks with PV nodes. CSEE J. Power Energy Syst. 3(3), 321–324 (2017)

140. Ayad, A., et al.: Cyber-physical attacks on power distribution systems. IET Cyber-Phys. Syst. Theory Appl. (2020)

141. Yanikson, S., Ghamkhari, M.: Transactive energy to thwart load altering attacks on power distribution systems. Future Internet. 12(1), 4 (2020)

142. Anwar, A., Mahmood, A.N., Ahmed, M.: False data injection attack targeting the LTC transformers to disrupt smart grid operation. In: International Conference on Security and Privacy in Communication Networks, pp. 252–266. Springer International Publishing (2015)

143. Teixeira, A., et al.: Security of smart distribution grids: data integrity attacks on integrated volt/VAR control and countermeasures. In: 2014 American Control Conference, pp. 4372–4378. IEEE (2014)

144. Deng, R., Zhuang, P., Liang, H.: False data injection attacks against state estimation in power distribution systems. IEEE Trans. Smart Grid. 10(3), 2871–2881 (2018)

145. Yufei, S., et al.: Intelligent data attacks against power systems using incomplete network information: a review. J. Mod. Power Syst. Clean Energy. 6(4), 630–641 (2018)

146. Zhuang, P., Deng, R., Liang, H.: False data injection attacks against state estimation in multiphase and unbalanced smart distribution systems. IEEE Trans. Smart Grid. 10(6), 6000–6013 (2019)

147. Choeum, D., Choi, D.-H.: OLTC-induced false data injection attack on volt/VAR optimization in distribution systems. IEEE Access. 7, 34508–34520 (2019)

148. Ye, X., et al.: Quantitative vulnerability assessment of cyber security for distribution automation systems. Energies. 8(6), 5266–5286 (2015)

149. Lim, I.H., Hong, S., Choi, M.S., et al.: Security protocols against cyber attacks in the distribution automation system. IEEE Trans. Power Deliv. 25(1), 448–455 (2009)

150. Sahoo, S., et al.: A stealth cyber-attack detection strategy for DC microgrids. IEEE Trans. Power Electron. 34(8), 8162–8174 (2019)

151. Dou, C.-X., Liu, B.: Multi-agent based hierarchical hybrid control for smart microgrid. IEEE Trans. Smart Grid. 4(2), 771–778 (2013)

152. Kushal, T.R.B., Lai, K., Illindala, M.S.: Risk-based mitigation of load curtailment cyber attack using intelligent agents in a shipboard power system. IEEE Trans. Smart Grid. 10(5), 4741–4750 (2018)

153. Gintuglu, M.H., Ishchenko, D.: Secure distributed state estimation for networked microgrids. IEEE Internet Things J. 6(5), 8046–8055 (2019)

154. Ma, R., et al.: Smart grid communication: its challenges and opportunities. IEEE Trans. Smart Grid. 4(1), 36–46 (2013)

155. Beg, O.A., et al.: Signal temporal logic-based attack detection in DC microgrids. IEEE Trans. Smart Grid. 10(4), 3585–3595 (2018)

156. Koglin, H.-J., et al.: Bad data detection and identification. Int. J. Electr. Power Energy Syst. 12(2), 94–103 (1990)

157. Chen, P.-Y., et al.: Detection of false data injection attacks in smart-grid systems. IEEE Commun Mag. 53(2), 206–213 (2015)

158. Chandola, V., Banerjee, A., Kumar, V.: Anomaly detection: a survey. ACM Comput. Surv. CSUR. 41(3), 1–58 (2009)
159. Yan, J., Tang, B., He, H.: Detection of false data attacks in smart grid with supervised learning. In: 2016 International Joint Conference on Neural Networks (IJCNN), pp. 1395–1402. IEEE. 2016

160. Yang, Q., Chang, L., Yu, W.: On false data injection attacks against Kalman filtering in power system dynamic state estimation. Wiley Online Libr. 9(9), 833–849 (2013)

161. Tan, S., et al.: Brief survey on attack detection method for cyber-physical systems. IEEE Syst. J., 1–11 (2020)

162. Li, B., et al.: Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system. J. Parallel Distrib. Comput. 103, 32–41 (2017)

163. Zhang, X., et al.: On false data injection attacks against the dynamic microgrid partition in the smart grid. In: 2015 IEEE International Conference on Communications (ICC), pp. 7222–7227. IEEE (2015)

164. Ganjkhani, M., et al.: A novel detection algorithm to identify false data injection attacks on power system state estimation. Energies. 12(11), 2209 (2019)

165. Li, W., et al.: Cosimulation for smart grid communications. IEEE Trans. Ind. Inform. 10(4), 2374–2384 (2014)

166. Strasser, T., et al.: Co-simulation training platform for smart grids. IEEE Trans. Power Syst. 29(4), 1989–1997 (2014)

167. Adewole, A.C., Tsoneva, R.: Co-simulation platform for integrated real-time power system emulation and wide area communication. IET Gener. Transm Distrib. 11(12), 3019–3029 (2017)

168. Pallonetto, F., et al.: SimApi, a smartgrid co-simulation software platform for benchmarking building control algorithms. SoftwareX. 9, 271–281 (2019)

169. Müller, S.C., et al.: Interfacing power system and ict simulators: challenges, state-of-the-art, and case studies. IEEE Trans. Smart Grid. 9(1), 14–24 (2016)

How to cite this article: Bhattar PL, Pindoriya NM, Sharma A. A combined survey on distribution system state estimation and false data injection in cyber-physical power distribution networks. IET Cyber-Phys. Syst., Theory Appl. 2021;6:41–62. https://doi.org/10.1049/cps2.12000