Received: 29 November 2023 | Revised: 29 February 2024 | Accepted: 25 March 2024

IET Smart Grid

DOI: 10.1049/stg2.12168

REVIEW

Comprehensive review on dynamic state estimation techniques with cybersecurity applications

Zhuoran Zhou[1] | Xin Zhang[1] | Jinning Zhang[2] | Gareth Taylor[3]

[1]Department of Automatic Control and Systems Engineering, University of Sheffield, Sheffield, UK

[2]School of Engineering, University of Leicester, Leicester, UK

[3]Department of Electronic and Electrical Engineering, Brunel University London, Uxbridge, UK

Correspondence

Xin Zhang, Amy Johnson Building, Portobello Street, Sheffield, S1 4DW, UK.
Email: xin.zhang1@sheffield.ac.uk

Jinning Zhang.
Email: jz388@leicester.ac.uk

Funding information

UK Research and Innovation, Future Leaders Fellowship 'Digitalisation of Electrical Power and Energy Systems Operation', Grant/Award Number: MR/W011360/2

Abstract

The role of cybersecurity in cyber-physical power systems (CPPS) is reviewed, focusing on the applications of dynamic state estimation (DSE) techniques. These DSE techniques are particularly relevant with the integration of phasor measurement units (PMUs) and advanced communication infrastructure. A comprehensive review on DSE techniques and applications to efficiently protect CPPS against cyberattacks is classified into three cyber resilience phases including prevention, detection, and mitigation. The DSE techniques in the prevention phase are surveyed to improve the observability of the CPPS by the robust design of the Kalman filter and optimal protection of PMUs. The DSE techniques in the detection phase are surveyed to improve the adaptability of CPPS in various attack detection scenerios and optimise the detection accuracy. The DSE techniques in the mitigation phase are surveyed to enhance the flexibility of CPPS resource utilisation with compensation-based, isolation-based, and scheduling-based strategies. Finally, the benefits and limitations of each DSE technique are summarised with potential suggestions on research directions for enhancing the cyber resilience of CPPS.

KEYWORDS

power grids, power system control, power system cyber-security and privacy, power system management, power system measurement, power system simulation, security of data

1 | INTRODUCTION

Climate change is driving the energy transition from fossil fuel-based energy sources to renewable and low-carbon alternatives [1]. Wind and solar energy, renowned for their zero carbon emissions, are the most popular renewable energy sources. However, the integration of renewable energy sources into the power grid presents significant technical challenges due to their intermittent nature and inherent uncertainties [2, 3]. Power grids are seeking to maximise renewable energy integration to significantly reduce their carbon footprint. In this context, there are growing power grid requirements to enhance the power quality, meet the increasing energy demand, and adhere to environmental regulations. However, conventional approaches of power system operation cannot manage the significantly increased complexity in renewable energy integrated power systems.

Cyber-physical power system (CPPS) integrates advanced monitoring systems, area networks, bi-directional communication, and intelligent control technologies to facilitate renewable energy integration. CPPS provides a comprehensive framework that enables consumers to engage in bi-directional interaction, promoting active involvement in ancillary power system services. This framework contributes to the advancement of CPPSs, benefiting all stakeholders involved [4]. Broadly, CPPS introduces a new cyber dimension to the traditional power system that intelligently integrates the digitalisation technologies of the entire energy supply chain. Unlike traditional power systems which rely on a one-way centralised supply model [5], CPPS utilises a bi-directional flow model, including both physical and cyber dimensions. The physical dimension includes infrastructure such as power plants and networks, meanwhile the cyber dimension manages information exchange, processing and security across the entire

cyber-physical system. For example, within the CPPS, the new power and information flows from renewable energy to end-users are not only monitored but also controlled more effectively, thereby maximising the reliability, efficiency, and utilisation of renewable energy in the power systems.

However, the integration of information and communications technologies (ICTs) in CPPS also introduces new cybersecurity challenges [6]. The lack of cybersecurity considerations in traditional power systems lead to new cybersecurity vulnerabilities, especially when the CPPS is integrated with cyber infrastructure. The traditionally designed security framework based on physical power systems cannot provide sufficient protection against cyberattacks in the cyber dimension [7].

The energy sector experienced numerous cybersecurity incidents which have been observed in recent years. In the recent year of 2023, there were several reports highlighting those incidents with significant impacts. In April 2023, the Lazarus group exploited a vulnerability known as "Xtrader" to successfully attack two key infrastructures [8]. In May 2023, an organisation named Clop exploited a zero-day vulnerability in the Progress Software's MOVEit platform. Notably, energy organisations such as Schneider Electric and Siemens Energy were both affected by the cyber vulnerability in MOVEit [9]. In May 2023, Mandiant discovered a new malware designed to specifically target industrial control systems. The malware was specifically designed to cause power system outages by targeting certain devices, such as remote terminal units (RTUs). In June 2023, Suncor, a leading Canadian oil corporation, encountered a nationwide cyberattack on their gas stations [10]. As a result, customers had to use cash as the only payment method with significant economic implications. In August 2023, the website of BAZAN Group, largest refinery operator in Israel, experienced widespread inaccessibility across their global regions [11]. The cyber incident was launched by a denial-of-service (DoS) attack targeting the company's network infrastructure, rendering the service inaccessible to users.

Cyber resilience to cope with these cyberattack incidents against CPPS has become a popular research direction. Given the growing threat of cyberattacks [12, 13], cyber resilience has recently been defined as the ability of a system to limit the impact, duration, and degradation caused by cyberattack events [14]. Based on the response to attack events, this review paper proposes a cyber resilience framework into three phases as shown in Figure 1. The three cyber resilience phases are classified as prevention, detection, and mitigation. These three phases are classified in chronological order, and the design of each phase has its significant features. If an overall system is considered, each phase is also designed to contribute to the next phase with the relationships shown in Figure 1. The prevention phase refers to techniques taken to prevent incidents from occurring and to minimise the attack impact. Specifically, for the dynamic state estimation (DSE) techniques in the prevention phase, this paper surveys the observability improvements by DSE techniques, which can ensure physical system observability, metres protection and placement, and enhance the robustness of state estimation to deal with specific

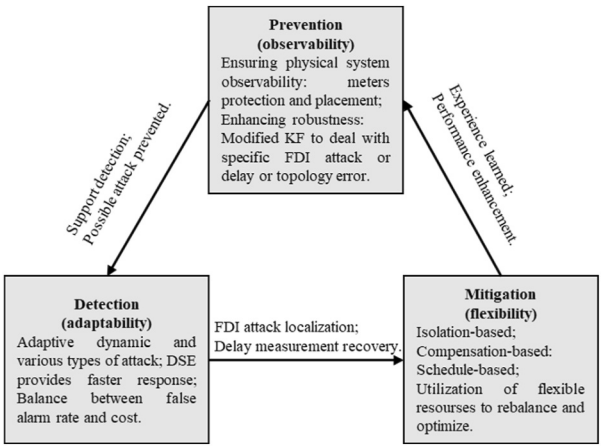

FIGURE 1 The classification of cyber resilience phases.

types of cyberattack. The detection phase refers to the identification techniques of any anomaly attack. To realise this goal, a designed Intrusion Detection System (IDS) continuously monitors the CPPS for any anomalous activity. Detection techniques are mainly classified into two types: model-based and data-driven. Data-driven techniques are mainly based on machine learning, which are independent of the CPPS physical model and utilise the historical data of the observed CPPS for state prediction and classification [15]. Specifically, for the DSE techniques in the detection phase, this paper surveys adaptability improvements by DSE techniques, which can enhance the adaptive dynamics and various types of cyberattacks, provide fast response, and balance between false alarm rate and cost. The mitigation phase reduces the impact of security incidents. Specifically, for the DSE techniques in the mitigation phase, this paper surveys the flexibility improvements on the mitigation strategies including compensation-based, isolation-based, and scheduling-based methods. For example, certain measurements of an attacked system may be isolated or modified to prevent the attack from impacting DSE accuracy. In the cyber dimension, the impact of a DoS attack was compensated by reallocating bandwidth [16] or changing communication channels [17]. In the physical dimension, strategies such as load redistribution may be taken to maintain system stability, and system control inputs may be modified to counter the impact of attack signals [18].

Power system state estimation (PSSE) is an algorithm employed for data processing in order to transform redundant metre readings and other accessible information into an estimation of the power system state variables [19]. The primary aim of PSSE is to provide a precise and continuous representation of the system state using real-time data from various measurement devices, including current transformers, voltage transformers, and power metering devices [20]. Data collection may be inaccurate due to errors in measurement devices, communication errors, or other cyber contingencies. PSSE can provide a consistent description of the system state based on all available measurement data. PSSE can detect inconsistent measurement data, and in some cases, not all components in a

system have accurate measurement devices. PSSE can provide estimates for components that do not have direct measurement devices. However, the accuracy of PSSE is highly dependent on data redundancy [21]. With continuous and accurate knowledge of system state, operators can better assess system performance and ensure safe and reliable operation of the CPPS. Through continuous research and development, PSSE techniques have been significantly improved with enhanced robustness and effectiveness in addressing measurement redundancy and bad data, ensuring reliability and accuracy for decision making and system control.

Traditionally, the static state estimation (SSE) is used to analyse and determine the state of a system at a specific operating condition. This includes the evaluation of variables such as voltage magnitude and phase angle at each node, as well as the assessment of power flow [22, 23]. The assumption is made that the topology of the system remains unchangeable between two continuous observations. This method is mainly used to deal with power systems under steady-state operating conditions. Commonly used SSE algorithms include least squares and weighted least squares (WLS). SSE provides important information for power system optimisation, safety monitoring and fault diagnosis.

In contrast to SSE, DSE emphasises the temporal evolution and dynamic behaviours of the system state. In CPPS, this includes dynamic changes in voltage, frequency, and phase angle, as well as dynamic processes such as generator rotor speed and load fluctuation. The DSE techniques commonly employ dynamic filtering algorithms, such as the Kalman filter (KF). These algorithms are capable of effectively estimating power systems that experience rapid state changes and transient conditions. DSE is crucial in power system dynamic analysis, stability control, and fault protection in the renewable energy integrated CPPS. For example, the integration of distributed energy resources (DERs) in the power generation, the complexity of demand, and the adoption of novel demand response technologies such as electric vehicles and Internet of Things (IoT) devices have increased the unpredictability of fluctuations in both demand and generation. The methods employed by the traditional SSE are inadequate in capturing the inherent uncertainty associated with dynamic characteristics in the CPPS operation. This is limited by the slow scanning speed of supervisory control and data acquisition (SCADA) systems and the lack of time-stamped data, raising concerns about the validity of the steady-state assumption [24]. The utilisation of measurements and communication infrastructures in the CPPS enables DSE techniques as a viable alternative to SSE, effectively capturing the system dynamic behaviours.

Much of the DSE techniques and their applications have been elaborated in the previous literature. Experiments on the single-machine infinite bus power system demonstrated that the observer approach outperformed cubature Kalman filter (CKF) in the estimation of attack vectors and attacked state vectors, with low computational complexity and guaranteed convergence [24]. In [21], the authors described the requirements of DSE in distribution systems. In particular, the potential applications of DSE in the data and feeder models, and different types of DSE methods were described. In [25], the authors focused on the comparison of various performance indicators of DSE and SSE methods such as computational burden and numerical stability. In [26], the authors provided a detailed categorisation of DSE and SSE methods for distribution system applications, and pointed out that DSE required high precision measurements and imposed a large computational burden. In [27], the authors compared different extended Kalman filter (EKF) and unscented Kalman filter (UKF) methods, and focused on the modelling of flexible alternating current (AC) transmission system devices and their impacts on DSE. In [28], the authors described the advantages of the DSE methods in solving the power system control and protection challenges, and pointed out potential directions of DSE applications. In [29], a feedback linearisation method was used to linearise the wide-area control system communication, and an error correction equation for DSE was derived. In general, the main focus of DSE technologies was on the development of error correction methods for protecting the cyber dimension and improving the security with certain computational complexity.

Based on the previous literature, the methods and mathematical principles related to various DSE technologies and their potential applications to the CPPS are surveyed. The main contributions of this review work are as follows:

1. This review investigates the cybersecurity challenges and compares the DSE and SSE technologies in dealing with cyber-attack scenarios. DSE is demonstrated to perform better in handling complex attack events.
2. The existing DSE techniques with special emphasis on KF-based and observer-based methods are investigated. DSE techniques are summarised with methods, characteristics, effectiveness, evaluation metrics and application scenarios.
3. Cyber resilience phases are classified into prevention, detection, and mitigation, providing a comprehensive analysis of the strengths and challenges for each DSE technique in three phases.
4. This review suggests potential directions for further research on DSE techniques with data-based and model-based methods. Proactive prevention and detection techniques are recommended to enable the dynamic change of the system without affecting its stability.

2 | GENERAL SCHEME OF DSE

The KF and the observer are two prominent algorithms utilised for the purpose of DSE. The KF is based on the principle of minimum variance estimation, where it integrates predictions from physical models with sensor measurements. Observers are constructed by utilising sensor measurements obtained from a physical system, typically in accordance with the Luenberger criterion. Both methodologies can be employed for the purpose of estimating the condition of a

dynamic system and yielding feedback signals for the purpose of control.

2.1 | Kalman filter

The state estimation technique known as WLS is widely used in SSE and has been extensively employed in the field of cyber-attack detection. In references [30, 31], the relationship was presented between the measurement vector $z \in R^m$ from the SCADA system and the state vector $x \in R^n$, which includes the magnitudes and phase angles of nodal voltages in an N-bus power system using an AC power flow model, yielding $n = 2N - 1 < m$

$$z = h(x) + e \tag{1}$$

where $h(\cdot): R^n \rightarrow R^m$ is a vector-valued nonlinear mapping function; $e \in R^m$ is denoted as the measurement error vector which is modelled as a normally distributed random variable with a mean of zero and a covariance matrix $R \in R^{m \times m}$. The quasi-static model applies when system operational points evolve gradually and smoothly with instantaneous control actions, thereby making the transient response negligible [32]. The state estimation process is conducted by optimising the WLS criterion, yielding the equation:

$$\hat{x} = \underset{x}{argmin}[z - h(x)]^T R^{-1}[z - h(x)] \tag{2}$$

The state vector can be solved by the Gauss-Newton iterative algorithm:

$$x^{k+1} = x^k + \Delta x^k, k = 1, 2, \ldots \tag{3}$$

$$\Delta x^k = \left(h\left(x^k\right)^T R^{-1} h\left(x^k\right)\right)^{-1} h\left(x^k\right)^T R^{-1}\left(z - h\left(x^k\right)\right) \tag{4}$$

where h is the Jacobian matrix. The algorithm is deemed to have converged when the norm of Δx^k falls below a predetermined threshold. Subsequent to the estimation phase, the presence of anomalous data is determined using a Euclidean norm detector, which assesses the validity of the ensuing inequality as follows:

$$\|r\| = \|z - h(\hat{x})\| \geq \tau, \tag{5}$$

where τ is a detection threshold of the Euclidean norm detector.

The premise is based on a quasi-steady model used for linear SSE. However, actual power systems are dynamically changing due to the stochastic nature of demand and supply variations. Consequently, SSE techniques fall short in reflecting such dynamism. To address this, the static approach necessitates re-assessment and enhancement through the integration of dynamic monitoring instruments [33]. Reference [33] proposed a comprehensive state space model tailored for state estimation, which was the following:

$$x_k = f(x_{k-1}, u_k) + w_k, z_k = h(x_k, u_k) + v_k, \tag{6}$$

where $x_k \in R^n$ is denoted as the vector of system states, which includes internal states such as dynamics of generators and loads; u_k represents the system input vector; z_k is the vector of measurements, which includes a series of data points from pseudo-measurements and measures algebraic variables to real and reactive power injections, flows, and current phasors. The incorporation of pseudo-measurements is essential for the state estimation of networks that are not fully observable [34]. h is the nonlinear measurement function; v_k is the measurement error. The w_k and v_k are usually assumed to be normally distributed with zero mean and covariance matrices of Q_k and R_k, respectively. However, it should be noted that w_k and v_k aggregate various noise and error sources including sensor measurement inaccuracy, communication channel distortion and model limitation, and might not conform to a Gaussian distribution in real-world scenarios [35].

The core of the UKF utilises a deterministic sampling method which is referred to as the unscented transform, where sigma points are carefully selected as a finite collection of representative points. These sigma points are specifically chosen to match the mean and covariance of the prior state distribution such as Gaussian statistics. These sigma points are then propagated through the nonlinear functions $\boldsymbol{f}$ and $\boldsymbol{h}$. Leveraging the structure of the KF, this process derives the estimation for the posterior state statistics, specifically focusing on the mean and covariance of the state estimates. Specifically, given the state estimate at time step $k - 1$ with mean $\hat{x}_{k-1|k-1} \in R$ and covariance matrix $P^{xx}_{k-1|k-1}$, 2n weighted sigma points are generated [36, 37] as follows:

$$\begin{aligned} \chi^j_{k-1|k-1} &= \hat{x}_{k-1|k-1} + \left(\sqrt{nP^{xx}_{k-1|k-1}}\right)_j, \chi^{j+n}_{k-1|k-1} \\ &= \hat{x}_{k-1|k-1} - \left(\sqrt{nP^{xx}_{k-1|k-1}}\right)_j, \end{aligned} \tag{7}$$

where $j = 1, \ldots, n$.

$\left(\sqrt{nP^{xx}_{k-1|k-1}}\right)_j$ represents the jth column vector of the associated matrix. These sigma points are propagated through f to generate the transformed sigma points:

$$\chi^j_{k|k-1} = f\left(\chi^j_{k-1|k-1}\right). \tag{8}$$

Then, the predicted state vector $\hat{x}_{k|k-1}$ and its covariance matrix are approximated by the weighted sample mean and sample covariance matrix of the transformed sigma points, respectively as follows:

$$\hat{x}_{k|k-1} = \sum_{j=1}^{2n} w_j \chi^j_{k|k-1}, \tag{9}$$

$$P^{xx}_{k|k-1} = \sum_{j=1}^{2n} w_j \left(\chi^j_{k|k-1} - \hat{x}_{k|k-1}\right)\left(\chi^j_{k|k-1} - \hat{x}_{k|k-1}\right)^T + Q_k \tag{10}$$

where the weight is 1/2n. Subsequently, the sigma points are updated to capture the information of the system process noise:

$$\chi^j_{k|k-1} = \hat{x}_{k|k-1} + \left(\sqrt{nP^{xx}_{k|k-1}}\right)_j, \tag{11}$$

$$\chi^j_{k|k-1} = \hat{x}_{k|k-1} - \left(\sqrt{nP^{xx}_{k|k-1}}\right)_j, \tag{12}$$

The predicted measurement vector is given by the following:

$$\hat{z}_{k|k-1} = \sum_{j=1}^{2n} w_j h\left(\chi^j_{k|k=1}\right), \tag{13}$$

with its associated error covariance matrix as follows:

$$P^{zz}_{k|k-1} = \sum_{j=1}^{2n} w_j \left(z^j_{k|k-1} - \hat{z}_{k|k-1}\right)\left(z^j_{k|k-1} - \hat{z}_{k|k-1}\right)^T + R_k \tag{14}$$

2.2 | Observer

An Observer is a system-theoretic construct for the state estimation of a system that is not directly measurable from its outputs. The main purpose is to reconstruct the internal state of a system from known system models and input and output data. The observer uses a mathematical model of the system to process the input and output signals and generate an estimate of the system's internal state. This process attempts to minimise estimation errors introduced by model errors and measurement noise [38-40].

For a general state space equation as the following:

$$\dot{x}(t) = Ax(t) + Bu(t) + Dd(t)\ y(t) = Cx(t) \tag{15}$$

where **A** is the state matrix, **B** in the input matrix, **C** is the output matrix, and **D** is the disturbance or unknown input (UI) matrix, x is the state vector, u is the input vector, and d is disturbance or UI vector, an observer can be built as follows:

$$\dot{z}(t) = Nz(t) + Gu(t) + Qy(t)\ \hat{x}(t) = z(t) - Hy(t), \tag{16}$$

where z is the state vector of designed unknown input observer (UIO) and $\hat{x}$ is the estimated state of the original system. The matrix **F**, **T**, **G**, **N** need to be designed for the UIO to track the state of the system and eliminate the state estimation error. In this way, the state estimation error tends to be 0 in the presence of UI as follows:

$$x(t) - \hat{x}(t) = e_x(t) \to 0 \tag{17}$$

The derivation of the state estimation error is

$$\begin{aligned}\dot{e}_x(t) = {} & (A - HCA - Q_1C)e_x(t) + (G - (I - HC)B)u(t) \\ & + (Q_2 - (A - HCA - Q_1C))y(t) \\ & + (N - (A - HCA - Q_1C))z(t) + (HC - I)Dd(t)\end{aligned} \tag{18}$$

For the realisation and accuracy of the proposed UIO, that is, if $e_x(t)$ must converge to zero,

$$\dot{e}_x(t) = (A - HCA - Q_1C)e_x(t) \tag{19}$$

The following conditions must be satisfied

$$\begin{aligned}H = (CD)^{-1}D\ \ G = B - HCB\ \ N \\ = A - HCA - Q_1C\ \ Q_2 = NH\end{aligned} \tag{20}$$

$$Q = Q_1 + Q_2.$$

If a system is not observable, it's impossible to construct an asymptotic observer. So, the sufficient condition for the existence of a UIO are given as

- $rank(CD) = rank(D)$,
- (C, C^*) is detectable, where $C^* = A - D\left((CD)^T CD\right)^{-1} (CD)^T CA$.

Most observers make no assumptions about the statistical distribution of the process and measurement model, and assume with the certain presence of UIs and sensor noise. This is due to the fact that deterministic observers perform well for all types of noise distributions. However, most observers are based on a time-invariant system setup and are sensitive to model errors when the model parameters are uncertain.

3 | DSE TECHNIQUES IN PREVENTION

3.1 | Generalised maximum likelihood iterative extended Kalman filter

In ref. [41], a fusion of the generalised maximum likelihood (GM) approach with an iterative extended Kalman filter (IEKF) was demonstrated. The IEKF further improved upon EKF by iteratively linearising the non-linear dynamics around the current estimate, which could provide better estimation accuracy. The goal of the GM approach is to find the parameter values that maximise the likelihood of the observed

data, according to the given model. The method exhibits greater robustness to system process noise compared to UKF when dealing with state estimation of nonlinear systems. Generalised maximum likelihood iterative extended Kalman filter (GM-IEKF) can be used for centralised DSE as well as decentralised DSE, but decentralised DSE imposes an unknown communication bandwidth burden and adds a greater computational burden compared to UKF and EKF. The main drawback is that the GM-IEKF produces unreliable system state estimates with strong nonlinearity and is susceptible to system parameter errors and structural noise, therefore, GM-IEKF requires significant measurement redundancy. The computational burden resulted in nearly doubling the computation time when comparing with the experiment in [41]. For instance, EKF took 3.94 ms, while GM-IEKF took 5.96 ms.

3.2 | Constrained robust unscented Kalman filter

The existing centralised DSE techniques did not normally consider the important inequality constraints related to reactive power, voltage regulators, and governors, while implicit constraints existed but were not enforced in decentralised DSE. In ref. [37], a framework of constrained robust UKF considered equality and inequality constraints was proposed. Algebraic equality constraints were treated as pseudo-measurements, while inequality constraints were managed through a projection operator. This approach mapped unconstrained estimates to the boundaries of an admissible region, defined by the established lower and upper limits of the state variables and inputs. The method improved the state estimation accuracy and robustness to measurement errors. Since this constrained robust UKF approach did not consider multiscale system dynamics, it could only guarantee the validity of short-term transient states and was not suitable for long-term stability analysis. Moreover, this approach could not distinguish between measurement errors resulting from malicious attacks and those arising from incorrect constraints. When considering the computational burden, UKF took 0.28 ms and the constrained robust UKF took 0.81 ms for the same scenario.

3.3 | S-robust extended Kalman filter

The S-based EKF exhibited better resilience in terms of breakdown points when comparing with both the Huber M-estimator and GM-estimator [42]. The breakdown point represented the threshold proportion of outlier data that an estimator could handle before yielding unreliable results. The advantage of the S-estimator was its consistent high breakdown point, regardless of an increase in system size, making it particularly beneficial for large scale power systems with a growing number of phasor measurement units (PMUs). In contrast, the GM-estimator demonstrated a reduction in breakdown points, as the number of state dimensions and the estimated parameters were increased. When handling errors, the S-estimator employed a strategy of downweighting values with substantial errors and then utilised the remaining clean values for WLS. The method was robust to randomly occurring topological errors and Gaussian noise.

3.4 | Robust cubature Kalman filter

Reference [43] introduced a robust cubature Kalman filter (RCKF) method for the DSE of generators under cyberattacks. Given the memoryless nature of DoS attacks, which were captured by the Bernoulli process, the corresponding distribution was employed to model the packet loss resulting from these attacks. The RCKF adjusted erroneous data by integrating robust M-estimation theory with the conventional CKF framework, and adopted a refined measurement error covariance matrix during the measurement update, which diverged from the standard practice of utilising the constant variance matrix. This approach enabled the RCKF to dynamically adapt the measurement noise statistics online, and the RCKF could maintain accurate state estimation results even in the presence of measurement error. Numerical experiments showed that the impact of the error on the false data injection (FDI) was relatively modest compared to the CKF, but the error on the DoS was significantly reduced and the computational time only increased slightly, which was suitable for real-time state estimation within the acceptable practical limits.

3.5 | Graph-theory based sensor recovery

The single time scale distributed estimation method addressed system dynamics and distributed estimation simultaneously within the same time framework [44]. This technique integrated the processes of achieving consensus and exchanging measurements into a single event, eliminating the numerous iterations of consensus at each stage of dynamic evaluation, as opposed to the dual-time-scale strategy. By streamlining these processes, the single time-scale model enhanced the speed of tracking system changes and reduced the load on communication networks. Overall, numerical-based approaches could become very complex and time-consuming when sensors in large-scale systems fail and lose observability. This observability could be restored by adding new sensors to the network and utilising a graph-theoretic approach, which could quickly and efficiently provide solutions for large-scale systems.

3.6 | Phasor measurement unit placement for outage prevention

In ref. [45], the focus of defensive strategies shifted from exclusively countering attacks to enhancing system resilience, specifically through minimising disruptions and optimising the

placement of PMUs, thereby safeguarding existing sensor networks. The PMU placement for outage prevention (PPOP) issue was formulated as a tri-level nonlinear optimisation challenge within the framework of the direct current (DC) flow model. This was subsequently transformed into a bi-level mixed integer linear programming problem. To address this, an innovative alternating optimisation approach was employed, which incorporated constraints, and two novel algorithms were developed to facilitate constraint generation. The optimisation structure was divided into three hierarchical levels, wherein the intermediate level was strategically designed to prevent the attacker from causing line overloads through load redistribution, while ensuring such activities remain undetected. Such overloads, if successful, led to line voltage drop. The lower level dealt with security-constrained economic dispatch to ensure efficient and secured energy delivery. The upper level was concerned with the challenge of PMU placement. A PMU placement solution designed to prevent overload-induced trips in the most critical scenarios could also prevent such trips under normal operational conditions, provided that the load remained within the anticipated boundaries.

3.7 | Semi-definite programming convexification

The aim of FDI is to strategically design a vector that manipulates sensor measurement, leading to the inaccuracies in state estimation. The complexity of these attacks results from the integration of continuous and discrete non-linear components, which can be attributed to the non-linear measurement model of AC and the fundamental constraints. The nonlinearity of equality power-flow constraints also makes the coexistence of multiple states and spurious solutions possible. The presence of nonlinearity allows multiple coexisting states and solutions, facilitating sparse FDI in AC settings. In order to tackle AC-constrained FDI challenges, a novel convexification approach utilising semi-definite programming (SDP) was proposed, aiming to achieve the approximation of global optimal state [46]. With the SDP approach it was possible to assign an attackable region to arbitrary measurements and topologies, which made this method extendable to different grid and convex optimisation problems. The study represented the preliminary investigation of AC power grids vulnerability to FDI. It emphasised the complex and computationally intensive nature of these nonconvex problems, while also recognised the challenge of executing such attacks without significantly modifying measurement data. The study made an example for SDP convexification, modified the penalty function to reduce the error introduced by convexification, and obtained an approximated global optimal solution. The results revealed the state estimation mechanism of AC grids and informed the design of new bad data detection (BDD) systems for FDI. In addition, a defence method was proposed to prevent the FDI attack by placing secure measurement in the attackable region.

3.8 | Summary of prevention techniques

The prevention techniques primarily focus on the observability of DSE performance in processing the measurement data. As summarised in Table 1, extensive research has been conducted for the robust design of KFs, and there are many statistical methods to optimise the filtering performance in the presence of potential cyber-attack data. Since the accuracy of the DSE is mainly affected by measurements and system models, the prevention approach focuses on how to improve observability and provide reliable data under cyber-attacks. The observability of the CPPS provides the necessary conditions for the subsequent cyber resilience phases of detection and mitigation. The FDI attack can modify the measurements to compromise the DSE. However, most research work assumed that the cyber-attackers had access to the complete system topology information, that is, the Jacobi matrix [36]. In this way, FDI attacks can be designed to hide from BDD with normal detection residuals. In reality, the attackers do not possess the real-time knowledge of the various system components. Moreover, the injected false data may appear to be suspicious to the system operator if the attack vector reaches certain threshold values. Therefore, the attacker's capabilities (i.e., the attack intensity) are often bounded when considering the performance and robustness of the existing DSE techniques.

The DSE techniques in the prevention phase are divided into two parts. The first part is to improve the observability of the CPPS with strategic PMU placement and protection of measurement metres. Metre protection and placement can improve the observability of the system with significant costs saving. Therefore, convex optimisation methods are used to solve the trade-off between system observability and measurement costs. In Table 1, the pros and cons of DSE techniques are surveyed with application scenarios for each reference. 3.5 provided a graph-theory method to add new sensors to ensure the observability of large-scale systems. This method reduced the computational burden when comparing traditional methods in tracking dynamics. 3.6 presented an optimisation framework for the PMU placement problem for large-scale nonlinear systems, taking into account power distribution constraints. 3.7 investigated the design of attack vectors from the attacker's point of view and derived the attackable region for arbitrary measurements and topology systems, which inspired the design of BDDs and improved the observability. In the second part of DSE techniques in processing the attacked measurements, there are certain statistical methods applied to the KF to improve the performance. The GM-IEKF, provided in 3.1, was used for processing measurements in nonlinear system and applicable to centralised DSE. 3.2 similarly improved the state estimation in the presence of measurement errors by adding physical constraints, but this method was not applicable to large-scale systems or having limitation in distinguishing between attacks and measurement errors. 3.3 and 3.4, on the other hand, were applicable to large-scale systems of DSE and focused on the robustness to topology errors and errors introduced by DoS, respectively.

TABLE 1 Summary of DSE prevention techniques.

Technique	Ref.	Pros	Cons	Application scenario
GM-IEKF	[41]	1. Resilience against observation noise and Gaussian and non-Gaussian system process noise 2. Performable after minor topological changes	1. Limited state estimation performance under strong nonlinearity 2. Diffuse with increasing error between actual measurement and predicted state. 3. Dependent on redundancy measurements.	Centralised and decentralised DSE
Constrained robust UKF	[37]	1. Estimate without linearising 2. High performance under strong nonlinear systems 3. High accuracy under observation noise 4. Detect bad data and erroneous constraints	1. The selection of sigma points is deterministic, which may lead to unstable values. 2. Short-term validity	1. Adaptive relay protection 2. Motor prediction control 3. Decentralised DSE in small scale CPPS
S-robust EKF	[42]	1. High breakdown point in the high dimension system 2. Robust to system topology errors 3. High accuracy of estimation when noise is Gaussian distributed	1. High computational burden and inaccuracy. 2. Need large numbers of PMUs to provide data in real time. 3. Effective only for Gaussian noise	Track generators' phase angle and rotor speed in large-scale CPPS
Robust Cubature Kalman Filter	[43]	1. Advanced performance compared to CKF 2. Adjust measurement noise online to eliminate data errors caused by DoS and FDI	The estimation performance severely degraded under certain attacks that RCKF cannot handle.	DSE of generators in large-scale CPPS
Sensor Recovery	[44]	Quickly track system dynamics while reducing the communication burden	Increase the cost and complexity of the system	Single time scale distributed estimation in large-scale CPPS
PMU placement	[45]	1. Prevent outage by allowing the presence of undetectable attacks 2. Robustness to load redistribution attacks in AC models	1. Lack of robustness to faults in the PMU and measurement errors caused by FDIs 2. Long convergence time in a large-scale CPPS	Extended DC power flow model in large-scale CPPS
SDP convexification	[46]	1. Results used to redesign the BDD programme 2. Derive performance bounds of stealthy and sparse FDI	1. Simplified conditions to real CPPS 2. Not cover all types of nonconvexity	Arbitrary measurement and topology

Abbreviations: CKF, cubature Kalman filter; DSE, dynamic state estimation; RCKF, robust cubature Kalman filter.

From Table 1, the KF-based DSE technique still has certain shortcomings: 1. It has limited performance in systems with strong nonlinearities; 2. It does not rely on linearisation methods, which imposes an excessive computational burden and complexity; 3. It is accurate in assumed Gaussian noises, and further research is needed to deal with the uncertainties of real noises; and 4. It lacks of robustness to the errors caused by the changes in the system parameters, whereas the actual power systems also encounter topology changes.

For the DSE techniques in the prevention phase of cyber resilience, the following research directions are suggested: firstly, the DSE techniques are needed for more accurate state tracking using less measurement redundancy in CPPS models, which is the development of more sophisticated modelling methods to estimate the real system dynamics. Secondly, the process of measurement noise should also be improved, and new statistical methods and filter designs should be explored to improve the reliability of the data. In addition, in response to the evolving feature of cyber-attack, it is also crucial to investigate more robust defence mechanisms, which should not only enhance the system's ability to prevent known attack patterns, but also enhance its ability to resist unknown or mutated cyber-attacks. Meanwhile, the design and application of distributed and centralised DSE techniques are also one of the focuses of future research. The trade-off between complexity and accuracy will be a major challenge, and future research work needs to find the balance in real-time operation with accuracy. Finally, the robustness of the DSE techniques requires to be improved, which may require the development of new adaptive algorithms that allow the state estimator to maintain stable operation in a system changing environment.

4 | DSE TECHNIQUES IN DETECTION

4.1 | Prioritised-experience-replay based deep reinforcement learning detection

The research challenges in SSE mainly focused on how to predict the system state and used current state data to figure out the probability that a cyberattack would happen. Therefore, the effectiveness of SSE was limited in the analysis of system dynamics under attacks [47]. Compared to SSE, DSE can utilise advanced deep reinforcement learning (DRL) methods to deal with continuous and variable attack patterns. Furthermore, it should be noted that the impact of an attack was limited to a small portion of the overall operational state of the grid. The probability of encountering compromised states was relatively low. This factor posed a challenge to the effectiveness of previous detection methods based on reinforcement learning [48]. The utilisation of prioritised experience replay improved the probability of learning in the context of attack scenarios. In order to enhance the accuracy of detection, a DSE methodology was developed to identify FDI attacks by adopting a viewpoint of attackers. This approach involved employing a model that was based on a partially observable Markov decision process (POMDP). The detection method presented in reference [49] introduced the utilisation of DRL to detect system compromises. This DSE approach involved the use of a long short-term memory (LSTM) network to analyse state from previous time steps in order to identify current compromises in the system. The detection scheme defended against FDI attacks without obtaining the adversary's strategy in advance, which had a false alarm rate of 0% under either continuous or non-continuous attacks. However, the difficulty of detecting discontinuous attacks was higher for DRL, and the delay error rate was close to 5%.

4.2 | Information filter

The paper [50] investigated the online detection of FDI attacks and DoS attacks in CPPS. The system was modelled as a discrete-time linear dynamic system and a KF was used for DSE. Generalised accumulation algorithms were used to achieve the fast detection of cyberattacks. Detectors in both centralised and distributed setups were proposed. The advantage of the cumulative sum algorithm (CUSUM) was demonstrated in its robustness to time varying states, multiple types of attacks, and dynamic system parameters. The CUSUM's ability in the online estimation of unknown attack variables was crucial for fast system detection. The CUSUM detected the known-topology-FDI more efficiently than traditional least squares and BDD methods based on measurement residuals, providing a faster and more accurate response. It also provided maximum likelihood estimation (MLE) for unknown attack variables, which could be used for system state tracking by replacing the attack value with the estimated optimal value. In a distributed setup, the local centre could only transmit quantised messages to the global centre due to bandwidth constraints, so a novel event-based sampling scheme called transgressive sampling with delay was proposed, which had significant advantages over the traditional isochronous sampling scheme. In addition, a distributed DSE method based on information filters was proposed. MLE provided online estimation capability for unknown attack variables, which was crucial for fast detection in the CPPS with adaptability in bandwidth-constrained situations.

4.3 | Finite-time secure state estimator

In ref. [51], a type of DSE in finite time was presented to localise and reconstruct the FDI vector. The proposed DSE method was based on a set of local finite-time state estimators running on a subset of sensors that were designed to estimate the dynamic state of CPPS affected by UIs. When a cyberattack launched on certain sensors, the local finite-time estimators using measurements from the attacked sensors might be corrupted. Therefore, a DSE detection algorithm was proposed for identifying effective local estimators. The data obtained from the effective local estimator was subsequently utilised to facilitate the secure estimation of the system state and localisation of an injected attack vector. The efficiency of the proposed approach was validated through the execution of online software-in-the-loop (SiL) testing on a model of a DC motor. The simulation and real-time test results showed that the algorithm was able to accurately estimate the motor state in a finite amount of time. The DSE detection algorithm not only successfully converged to the real state variables within 0.25 s, but also maintained the estimation error within 0.01 under 20 dB of measurement noise.

4.4 | State forecast

The authors in ref. [52] pointed out that the current offline defence methods, such as increasing the redundancy of measurements and enhancing the cybersecurity of sensors and communication channels, were inadequate for dynamically changing cyber threats and system configuration. Therefore, an online anomaly detection algorithm was proposed, that identified FDI in measurements by utilising load forecasts, generation schedules, and synchronised phase data. An empirical method was proposed for determining the minimum magnitude of an attack as well as a detection threshold that satisfied a specific false-positive and true-positive rate. Through testing of an IEEE 14-node power system model, the study observed that the accuracy of load forecasting had the greatest impact on the false positive rate (FPR), and the average minimum magnitude of attacks and detection thresholds were calculated for each state variable. The constraints of an FPR of 0.01 and a true positive rate of 0.95 could be satisfied when the minimum attack magnitude of the state variable affected the line flow variations from 0.095 to 0.098 p.u.

4.5 | UIO-based intrusion detection system

The frequency control system in the standalone microgrid, in ref. [53], was meant to keep an efficient operation of diesel plant, solar power plant, and battery bank. From the attacker's point of view, the study focused on the effects of two FDI attacks: inserting and multiplying frequency control error signals. The study proposed a new DSE method that used the UIO approach from a defensive point of view. In addition, a strategy was developed for identifying attacks. Within the UIO system, the attack detection scheme was put into action by creating an output residual function. Along with this, the attack was reconfigured by putting together the UIs using the UIO system's input-output inversion process. The method utilised DSE to improve the performance of frequency control, and the identification of unknown frequency attacks was enhanced.

4.6 | Kalman filter with delayed measurements

Under the limitation of PMUs' high installation costs, full replacement of all existing RTUs with PMUs is impractical. The mixed measurement of PMU and RTU data to conduct the state estimation of CPPS is a feasible method to enhance the performance of DSE. However, the delay due to the data transmission burden over the communication channel is a problem that cannot be ignored. In the presence of measurement delay, the traditional chi-square estimator is less effective in detecting the stealthy FDI attack, and the existing techniques cannot distinguish whether the error is caused by the delay or the attack. The study in ref. [54] designed a DSE method for a mixture of PMU and RTU data that was robust to delay. This KF-based method could detect FDI attacks in the presence of delayed measurements. The equations for discrete time systems described the linear dynamic relationship between voltage and active and reactive power measurements. The stochastic delay of the measurements was described as a Bernoulli process, and the measurements for delay occurrence were computed using the values from the last sampling time. The KF gain was derived by minimising the covariance of the state variable errors. Finally, a new cardinality detector was designed that utilised the residuals of the measurements under delay as a detection quantity, which allowed the identification of the FDI attack with delayed measurements. The advantage of DSE was demonstrated to effectively detect FDI attacks by minimising the covariance of the state variable errors with robustness to delay using mixed PMU and RTU data.

4.7 | Summary of detection techniques

DSE Detection techniques have evolved to identify more effectively and counter complex attacks that can occur in the CPPS as summarised in Table 2. Prioritised-experience-replay method in 4.1 was designed for continuous and various attacks, while CUSUM enhanced the detection for stealthy FDI. Certain DSE techniques focused specifically on improving robustness to delay, such as mixing PMU and RTU data in 4.6, and the design of information filter in 4.2, which were capable of effectively detecting FDI attacks even in the presence of delayed measurements. Techniques in 4.2 and 4.3 demonstrated the efficiency of decentralised DSE by saving communication burden with less data processing requirements. Also, decentralised DSE had more adaptability to topology change and large-scale systems, which provided a higher level of adaptability and responsiveness. Other centralised DSE techniques, due to the simplicity of the model and the high consistency of the data, were more feasible for cyber-attacks detection. With the assumption that the attacker had access to all or part of the system parameters, detection methods have shifted from a single static analysis to a diversified strategy that included state prediction, as the cyber-attacks were designed to be stealthier and more sophisticated. The evolution of these detection approaches also reflected the response to ongoing cybersecurity threats, from traditional offline defence (e.g., increased redundancy) to more proactive and intelligent online detection mechanisms (e.g., machine learning and online anomaly detection algorithms).

For the future development of DSE detection techniques, the advanced functionality of detection techniques is required to include reconstruction for FDI attack vectors. By distinguishing between attack vectors and UIs, it is possible to obtain the knowledge of the system and provide guidance for mitigating the impact of the cyber-attacks. A comprehensive detection strategy needs to be proposed, which should be able to effectively deal with unknown, asynchronous, synchronous and collaborative cyber-attacks. The goal of the detection strategy is to rapidly track, localise, and reconstruct the attack vectors to achieve an optimal balance between accuracy and speed of DSE detection techniques, taking into account cost-effectiveness. In addition, the detection strategy should support adaptability in centralised and decentralised architectural designs, possess a high degree of robustness to measurement noise and topology parameter variations, and distinguish system noise and UIs from actual cyber-attacks. Meanwhile, a comprehensive evaluation system needs to be constructed in order to fully assess the effectiveness of the DSE detection methods. Finally, passive detection methods need to combine with proactive detection measures such as moving target defence (MTD) [55, 56] to enhance the overall CPPS security.

5 | DSE TECHNIQUES IN MITIGATION

5.1 | Optimal filter and Bayesian learning

To mitigate FDI attacks that altered sensor measurements, the ref. [57] proposed a distributed DSE algorithm based on

TABLE 2 Summary of DSE detection techniques.

Technique	Ref.	Scenario	Methods	Evaluation metrics
DRL	[47]	Centralised DSE	Prioritised-experience-replay	Detection index: Normalised innovation vector
	[48]			Attack: Continuous and discontinuous FDI
	[49]			Effectiveness: Delay error rate 2%–5% and false alarm rate 0%
Information filter	[50]	Centralised and decentralised DSE	CUSUM	Detection index: Measurement residual
				Attack: Known and unknown FDI
				Random DoS
				Effectiveness: Trade-off between detection delay and false alarm rate
Finite-time secure state estimator	[51]	Decentralised DC-motor model	Luenberger observer	Detection index: Residual signal
				Attack: FDI on state vector
				Effectiveness: Detection time 0.25s; attack reconfiguration
Load forecast	[52]	IEEE 14 bus power system with SCADA networks	Online phasor detection	Detection index: State estimation deviation
				Attack: FDI
				Effectiveness: FPR 1%
UIO-based attack vector reconfiguration	[53]	LFC of standalone Microgrid	Centralise UIO	Detection index: Frequency deviation, state estimation error
				Attack: FDI on frequency measurement
				Effectiveness: FPR 0.02%
				Attack reconfiguration
KF with delayed measurement	[54]	Modified chi-square detection	Centralised KF	Detection index: MSE, voltage
				Attack: Designed FDI
				Effectiveness: MSE under threshold

Abbreviations: DRL, deep reinforcement learning; DSE, dynamic state estimation.

optimal filtering and graph theory. Specifically, the local gain of the distributed scheme was obtained using optimal filtering theory, while the neighbourhood gain was determined through a convex optimisation process and graph theory. Optimal filters enabled the gains to be obtained from both local and neighbourhood information, which in turn improved the accuracy and robustness of the overall grid state estimation. This approach was particularly suitable for distributed CPPS because it could efficiently process information from various parts of the CPPS without relying on a centralised control centre. The key role of the Bayesian approach was to obtain the attack parameters when calculating the local gains. Through the Bayesian learning process, parameters and probability estimated about the cyber-attacks were obtained so that any potential errors could be considered and corrected during the estimation process. This allowed the PSSE process to continuously provide accurate state for the operator under cyber-attacks. By using the mean square error (MSE) principle, a distributed DSE algorithm was designed. In addition, the convergence condition of the method was derived with convergence time which was almost half of the time than the method proposed in [58].

5.2 | Joint state and unknown-input estimation

The aim of ref. [59] was to design a distributed DSE technique for simultaneously estimating the state and UIs of nonlinear systems affected by DoS attacks and random disturbances. A new dynamic event-triggered (ET) mechanism aimed at improving resource utilisation was proposed. This ET mechanism was applied in the proposed DSE to ensure measurement protection. Compared with existing studies, the new ET mechanism effectively reduced unnecessary data transmissions during DoS attacks. This was verified in simulation experiments, which achieved a 75% reduction in data transmission compared to traditional methods.

5.3 | Long short-term memory and convolutional neural network

The paper [60] discussed the problem of how to accurately distinguish real data and false data in power systems integrated with wind power plants. Wind power plants

generated real data fluctuations, but false data could also be injected stealthily as fluctuating data. Therefore, an improved DSE method based on three-level false data identification was proposed. The specific implementation was as follows: the first level determined whether there was a mutation in the real and false data by innovation vector; the second level set a threshold to determine the temporal correlation between real-time data and historical data by LSTM; the third level extracted the spatial correlation features of the data by training the convolutional neural network (CNN) model, which was constructed from the historical data to identify the authenticity. This technique could accurately identify fluctuation data and false data, recognise and correct false data, overcome the problem of over-estimation of the robust state estimation algorithm on the measured data, and adapt to the fluctuation characteristics of the renewable energy integrated power system.

5.4 | UIO attack reconfiguration and optimal economic dispatch

To distinguish the error caused by cyber-attacks and system noise, an effective hybrid DSE method was proposed. Initially, a UIO was deployed to estimate the system state, followed by the acquisition of attack vector dynamics from this preliminary estimation. Subsequently, the KF algorithm co-estimated both the system state and attack vector. The results in ref. [38] validated the defence strategy's effectiveness by demonstrating the variation in generator output before and after an attack. The approach integrated a robust intermediate observer for security DSE and attack reconstruction, with the attack vector serving as the observer's estimation parameter. The mitigation approach introduced an optimal-economic-dispatch based defence strategy, optimised generator outputs through convex optimisation to recalibrate current distribution, and stabilised the CPPS to prevent overloading of critical lines.

5.5 | UIO-based estimator and attack compensation controller

There is no systematic framework in the previous literature that can directly estimate FDI attack signals and automatically compensate for FDI attacks in real-time, as well as proactively mitigate the impact of FDI attacks by reconfiguring the closed-loop feedback controller based on the attack compensation. In ref. [40], an observer-based output feedback control model was introduced and mitigated the adverse effects of both FDI and DOS automatically. A new model was introduced to simulate intermittent DoS attacks using only uniform upper and lower bounds on the cyber-attack's active times. The output feedback control could automatically estimate and compensate for unknown FDI attacks while mitigating the effects of coordinated FDI and DoS attacks. A switching pulse observer was proposed for estimating the unknown FDI attack signal and the system state, respectively. Specifically, the state observer was constructed through the following model: when the system was in normal operation, the state observer predicted the next state based on the system model, and at the same time corrected the prediction error using the system output feedback; when a FDI attack signal was detected, the state observer switched to the corresponding attack model, which was used to correct the DSE error caused by the attack. The estimation of the FDI attack signal, on the other hand, was based on an external dynamic system, and the attack signal was reconstructed by observing the difference between the system output and the expected output. This approach enabled real-time estimation and compensation of FDI and DoS attacks without the need to know the frequency and duration of the attacks, which effectively improved the flexibility of the system in response to unknown and non-periodic attacks. In addition, an exponential stability criterion for output-feedback multi-area LFC systems under DoS and FDI attacks was derived by using a time-varying Lyapunov function approach with attack parameter dependence. Then, a robust attack-compensated feedback controller was developed to realise the frequency control in multi-area LFC systems.

5.6 | Sliding mode observer for risk mitigation

Despite extensive research on power system dynamics modelling, a discrepancy remains between mathematical comprehension and the real system dynamic process. Relying solely on these models might lead to suboptimal control or estimation. Modelling of UI and cyber-attacks is important in order to reduce discrepancies between estimated and real system dynamics. When modelling the UIs, the model in ref. [61] considered unknown plant disturbances, unknown control inputs and potential actuator failures. The gain of UIs were formulated as a random matrix to enhance the robustness of observer. A sliding mode observer was designed, which differed from the KF-based estimator with no assumptions on the distribution of measurement noise and process noise. After the UIs and cyber-attack signals were reconstructed, a filter for residual detection of impaired measurements was designed. In the risk mitigation module, the weighted deterministic threat level was used to decide whether the PMU data needed to be isolated. The proposed sliding mode observer still satisfied the observability after isolating the erroneous data for cyber-attack risk mitigation.

5.7 | Summary of mitigation techniques

DSE mitigation techniques are classified into isolation-based, compensation-based, and scheduling-based according to their mechanisms. Compensation-based methods can be used for both FDI and DoS attacks, and require the integration of DSE or neural network methods to estimate and compensate for the compromised cyber-attack data. Isolation-based intrusion mitigation system (IMS) can be seen as a feasible strategy, but IMS is only applicable to FDI attacks and is limited by the number of attacks. Scheduling-based IMS can mitigate the

effects of FDI and DoS attacks by utilising additional flexible resources such as extra generators to re-achieve power balance and optimal power flow. Mitigation methods often have limitations in capabilities, depending on the flexibility of risk mitigation resources and system reconfiguration in response to the strength of cyber-attacks. As summarised in Table 3, both DSE mitigation techniques in 5.1 and 5.2 used decentralised structures to maximise the use of neighbourhood and local information networks, which improved the cyber resource utilisation and increased the accuracy of DSE. For the UIs and fluctuating data existing in CPPS, both LSTM in 5.3 and sliding mode observer in 5.4 performed effectively to detect the stealthy cyber-attacks and improved the flexibility to complex and multiple attack situations. 5.5 investigated DSE under the coordinate FDI and DoS, which significantly improved the robustness of multi-region LFC and overcome the detection limitations of existing models. By integrating the optimal economic dispatch methods and feedback controllers, the defence against cyber-attacks was enhanced while the grid operation was optimised. Isolation-based IMS in 5.6 optimised the flexibility which was provided by measurement redundancy to ensure system observability.

Current research on DSE mitigation methods requires improvement in enhancing CPPS security. In particular, data-based IMS mostly rely on specific datasets for validation, lack general applicability, and may not achieve the same expected results in different data environments. Meanwhile, advanced mitigation methods such as deep learning have high computational requirements, which may limit their applications and real-time response in resource-constrained systems. Another challenge is that existing mitigation strategies may not be sufficient to cope with attack patterns changing, which require the development of DSE mitigation techniques to have flexibility in adapting to complex and multiple attacks. For future development of DSE mitigation techniques, cost-effective methods should be developed to reconstruct system states and attacks, consider the co-occurrence of multiple attacks in complex environments, and enhance the mitigation

TABLE 3 Summary of DSE mitigation techniques.

Technique	Ref.	Methods	Scenario	Attack	Effectiveness
Distributed state estimation	[57] [58]	1. Optimal filter 2. Bayesian learning approach 3. Compensation-based	Power distribution system with multiple synchronous generators	1. FDI 2. Replay attack	The convergence time was reduced by half than existing method in ref. [58].
Joint state and unknown-input estimation	[59]	1. Dynamic event triggered communication 2. Isolation-based	Wireless sensor network	DoS	75% reduction in unnecessary data transmission compared to traditional methods.
Multi-level FDI identification	[60]	1. LSTM-CNN 2. Compensation-based	Wind power generation systems with high data volatility	FDI	The CNN model identified the flase data form fluctuation and overcome the over-estimation problem.
UIO attack reconfiguration and optimal economic dispatch	[38]	1. UIO 2. Convex optimisation 3. Scheduling-based	Optimal economic scheduling under attack in nonlinear continuous-time systems	FDI on generators' state	The mitigation mehod avoided overloading of critical lines by optimising the active power of unattacked generators in optimal-economic-dispatch-based criterions.
UIO-based estimator and attack compensation controller	[40]	1. UIO 2. Time-varying Lyapunov function 3. Compensation-based	Multi-area load frequency control system	1. FDI: Load disturbance 2. DoS 3. Coordinated DoS and FDI	The proposed scheme had no limitations on the bound of FDI attacks and on the frequency of DoS attack. The proposed scheme could mitigate the adverse effect of DoS and FDI.
Risk mitigation for DSE	[61]	1. Sliding mode observer 2. Dynamic risk mitigation optimisation 3. Isolation-based	SCADA	1. FDI 2. DoS 3. Replay attack	The risk mitigation scheme isolated the most impactable PMU and ensured CPPS's observability through avaliable, safe measurement.

Abbreviation: DSE, dynamic state estimation.

impacts on the physical and cyber dimensions. In addition, future research will be critical to build flexible and self-learning IMS, which are able to enhance the flexibility and learning capacity, so that the DSE mitigation techniques can adapt to the emerging cyber-attack patterns and guarantee the continuous safe operation of CPPS.

6 | CONCLUSION

This paper comprehensively reviews the recent research advances of DSE techniques and their applications in the cybersecurity of CPPS. Two main methods of KF and UIO are analysed by investigating their modelling algorithms and evaluating their benefits and limitations. Subsequently, the existing DSE techniques for the CPPS resilience framework are categorised into three phases: prevention, detection, and mitigation. Within each phase, a comprehensive review is provided with application scenarios. DSE prevention techniques balance the observability and economic costs as an optimisation problem by efficiently placing PMUs. Multiple KF-based and UIO-based techniques are introduced to deal with the noise. DSE detection techniques for real-time have been able to identify complex noise and attack vectors. DSE mitigation techniques have proven solutions for both latency due to DoS and system state deviation due to the FDI, and take full advantage of the flexible resources provided by CPPS.

The research gaps are identified in DSE techniques with future research directions. Future research needs to consider the trade-offs between model complexity and processing time for handling highly nonlinear systems. Future DSE techniques can combine certain active defence techniques such as MTD, and design a changing system mechanism to improve the detection rate of stealth cyber-attacks. Data-based and model-based DSE methods can be combined to create a fusion detection system. Research on mitigation techniques can combine the advantages of various mitigation methods and establish more flexible mitigation strategies to deal with complex cyber-attacks.

AUTHOR CONTRIBUTIONS

Zhuoran Zhou: Formal analysis; Methodology; Software; Writing – original draft; Writing – review & editing. **Xin Zhang:** Conceptualization; Funding acquisition; Investigation; Supervision; Writing – original draft; Writing – review & editing. **Jinning Zhang:** Investigation; Resources; Validation; Visualization; Writing – review & editing. **Gareth Taylor:** Funding acquisition; Resources; Validation.

ACKNOWLEDGEMENTS

This work has been funded by UK Research and Innovation Future Leaders Fellowship (grant number: MR/W011360/2): 'Digitalisation of Electrical Power and Energy Systems Operation'.

NOMENCLATURE

AC	Alternating Current
ADT	Average Dwell Time
AGC	Automatic Generation Control
BDD	Bad Data Detection
CKF	Cubature Kalman Filter
CNN	Convolutional Neural Network
CUSUM	Cumulative Sum Algorithm
CPPS	Cyber-Physical Power System
DC	Direct Current
DER	Distributed Energy Resource
DoS	Denial of Service
DRL	Deep Reinforcement Learning
DSE	Dynamic State Estimation
ET	Event Trigger
EKF	Extended Kalman Filter
FACTS	Flexible AC Transmission System
FDI	False Data Injection
FPR	False Positive Rate
GM	Generalised Maximum Likelihood
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IEKF	Iterative Extended Kalman Filter
IMS	Intrusion Mitigation System
IoT	Internet of Things
KF	Kalman Filter
LFC	Load Frequency Control
LSTM	Long Short-Term Memory
MILP	Mixed Integer Linear Programming
MSE	Mean Square Error
MLE	Maximum Likelihood Estimation
MTD	Moving Target Defence
PMU	Phasor Measurement Unit
POMDP	Partially Observable Markov Decision Process
PPOP	PMU Placement for Outage Prevention
PSSE	Power System State Estimation
RCKF	Robust Cubature Kalman Filter
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SCED	Security-Constrained Economic Dispatch
SDP	Semi-Definite Programming
SSE	Static State Estimation
SiL	Software-in-the-Loop
TPR	True Positive Rate
UI	Unknown Input
UIO	Unknown Input Observer
UKF	Unscented Kalman Filter
WACS	Wide-Area Control System
WLS	Weighted Least Square.

CONFLICT OF INTEREST STATEMENT

The authors declare that they have no known conflicts of interest, competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

DATA AVAILABILITY STATEMENT

Data will be made available for research and non-commercial purpose, and can be requested from the corresponding author.

ORCID

Xin Zhang https://orcid.org/0000-0002-6063-959X

REFERENCES

1. Santos da Silva, S.R., et al.: Power sector investment implications of climate impacts on renewable resources in Latin America and the Caribbean. Nat. Commun. 12(1), 1276 (2021). https://doi.org/10.1038/s41467-021-21502-y
2. Geleta, D.K., Manshahia, M.S.: Gravitational search algorithm-based optimization of hybrid wind and solar renewable energy system. Comput. Intell. 38(3), 1106–1132 (2022). https://doi.org/10.1111/coin.12336
3. Du, D., et al.: A review on cybersecurity analysis, attack detection, and attack defense methods in cyber-physical power systems. J. Mod. Power Syst. Clean Ener. 11(3), 727–743 (2023). https://doi.org/10.35833/MPCE.2021.000604
4. Kong, P.Y.: Optimal configuration of interdependence between communication network and power grid. IEEE Trans. Ind. Inf. 15(7), 4054–4065 (2019). https://doi.org/10.1109/TII.2019.2893132
5. Fang, X., et al.: Smart grid - the new and improved power grid: a survey. IEEE Commun. Surv. Tutor. 14(4), 944–980 (2012). https://doi.org/10.1109/SURV.2011.101911.00087
6. Wang, Y., et al.: A tri-level programming-based frequency regulation market equilibrium under cyber attacks. Prot. Control Mod. Power Syst. 8(1), (2023). https://doi.org/10.1186/s41601-023-00332-8
7. Hussain, S., et al.: A novel hybrid cybersecurity scheme against false data injection attacks in automated power systems. Prot. Control Mod. Power Syst. 8(1), (2023). https://doi.org/10.1186/s41601-023-00312-y
8. How the Lazarus Group is Stepping up Crypto Hacks and Changing its Tactics." https://www.elliptic.co/blog/how-the-lazarus-group-is-stepping-up-crypto-hacks-and-changing-its-tactics
9. Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft." https://www.mandiant.com/resources/blog/zero-day-moveit-data-theft
10. Suncor Energy Hit by Cyberattack; Petro-Canada Gas Stations Impacted." [Online]. https://calgaryherald.com/business/energy/suncor-energy-petro-canada-cybersecurity-incident
11. Israel's Largest Oil Refinery Website Offline After DDoS Attack by Ax Sharma July 30, 2023 05:40 AM 1." Accessed: Nov. 09, 2023. [Online]. https://www.bleepingcomputer.com/news/security/israels-largest-oil-refinery-website-offline-after-ddos-attack/#google_vignette
12. Arghandeh, R., et al.: On the definition of cyber-physical resilience in power systems. Renew. Sustain. Energy Rev. 58, 1060–1069 (2016). https://doi.org/10.1016/j.rser.2015.12.193
13. Paul, S., et al.: On vulnerability and resilience of cyber-physical power systems: a review. IEEE Syst. J. 16(2), 2367–2378 (2022). https://doi.org/10.1109/JSYST.2021.3123904
14. Liu, M., et al.: Enhancing Cyber-Resiliency of Der-Based Smartgrid: A Survey. [Online]. http://arxiv.org/abs/2305.05338 (2023)
15. Chen, B., et al.: Detection of false data injection attacks on power systems using graph edge-conditioned convolutional networks. Prot. Control Mod. Power Syst. 8(1), (2023). https://doi.org/10.1186/s41601-023-00287-w
16. Hossain, M.M., et al.: Bandwidth allocation-based distributed event-triggered LFC for smart grids under hybrid attacks. IEEE Trans. Smart Grid 13(1), 820–830 (2022). https://doi.org/10.1109/TSG.2021.3118801
17. Cameron, C., et al.: Using self-organizing architectures to mitigate the impacts of denial-of-service attacks on voltage control schemes. IEEE Trans. Smart Grid 10(3), 3010–3019 (2019). https://doi.org/10.1109/TSG.2018.2817046
18. Wang, C., et al.: State prediction using LSTM with optimized PMU deployment against DoS attacks. J. Intell. Fuzzy Syst. 42(6), 5957–5971 (2022). https://doi.org/10.3233/JIFS-212593
19. Schweppe, F.C., Rom, D.B.: Power system static-state estimation, Part II: approximate model. IEEE Trans. Power Apparatus Syst. PAS-89(1), 125–130 (1970). https://doi.org/10.1109/TPAS.1970.292679
20. Chen, J., Dong, Y., Zhang, H.: Distribution system state estimation: a survey of some relevant work. In: Chinese Control Conference, CCC (2016). https://doi.org/10.1109/ChiCC.2016.7554934
21. Primadianto, A., Lu, C.N.: A review on distribution system state estimation. IEEE Trans. Power Syst. 32(5), 3875–3883 (2017). https://doi.org/10.1109/TPWRS.2016.2632156
22. Valverde, G., Terzija, V.: Unscented Kalman filter for power system dynamic state estimation. IET Gener., Transm. Distrib. 5(1), 29 (2011). https://doi.org/10.1049/iet-gtd.2010.0210
23. Do Coutto Filho, M.B., Stacchini de Souza, J.C.: Forecasting-aided state estimation - Part I: panorama. IEEE Trans. Power Syst. 24(4), 1667–1677 (2009). https://doi.org/10.1109/TPWRS.2009.2030295
24. Taha, A.F., et al.: Dynamic State Estimation Under Cyber Attacks: A Comparative Study of Kalman Filters and Observers. [Online]. http://arxiv.org/abs/1508.07252 (2015)
25. Sharma, A., Jain, S.K.: A review and performance comparison of power system state estimation techniques. In: International Conference on Innovative Smart Grid Technologies, ISGT Asia 2018 (2018). https://doi.org/10.1109/ISGT-Asia.2018.8467861
26. Ahmad, F., et al.: Distribution system state estimation-A step towards smart grid. Renew. Sustain. Energy Rev. 81, 2659–2671 (2018). https://doi.org/10.1016/j.rser.2017.06.071
27. Karamta, M.R., Jamnani, J.G.: A review of power system state estimation: techniques, state-of-the-art and inclusion of FACTS controllers. In: International Conference on Electrical Power and Energy Systems, ICEPES 2016 (2017). https://doi.org/10.1109/ICEPES.2016.7915986
28. Liu, Y., et al.: Dynamic state estimation for power system control and protection. IEEE Trans. Power Syst. 36(6), 5909–5921 (2021). https://doi.org/10.1109/tpwrs.2021.3079395
29. Hu, Q., et al.: Secure state estimation and control for cyber security of the nonlinear power systems. IEEE Trans. Control Netw. Syst. 5(3), 1310–1321 (2018). https://doi.org/10.1109/TCNS.2017.2704434
30. Abur, A., Exposito, A.G.: Power System State Estimation: Theory and Implementation (2004)
31. Conejo, A.J.: Power system state estimation-theory and implementations [book review. IEEE Power Energy Mag. 3(2), 64–65 (2005). https://doi.org/10.1109/mpae.2005.1405872
32. Musleh, A.S., Chen, G., Dong, Z.Y.: A survey on the detection algorithms for false data injection attacks in smart grids. IEEE Trans. Smart Grid 11(3), 2218–2234 (2020). https://doi.org/10.1109/TSG.2019.2949998
33. Zhao, J., et al.: Power system dynamic state estimation: motivations, definitions, methodologies, and future work. IEEE Trans. Power Syst. 34(4), 3188–3198 (2019). https://doi.org/10.1109/TPWRS.2019.2894769
34. Clements, K.A.: The impact of pseudo-measurements on state estimator accuracy. In: IEEE Power and Energy Society General Meeting (2011). https://doi.org/10.1109/PES.2011.6039370
35. Wang, S., et al.: Assessing Gaussian assumption of PMU measurement error using field data. IEEE Trans. Power Deliv. 33(6), 3233–3236 (2018). https://doi.org/10.1109/TPWRD.2017.2762927
36. Zhao, J., Mili, L.: A robust generalized-maximum likelihood unscented kalman filter for power system dynamic state estimation. IEEE J.Select. Top. Signal Process. 12(4), 578–592 (2018). https://doi.org/10.1109/JSTSP.2018.2827261
37. Zhao, J., Mili, L., Gómez-Expósito, A.: Constrained robust unscented kalman filter for generalized dynamic state estimation. IEEE Trans. Power Syst. 34(5), 3637–3646 (2019). https://doi.org/10.1109/TPWRS.2019.2909000
38. Su, Q., et al.: Cyber-attacks against cyber-physical power systems security: state estimation, attacks reconstruction and defense strategy. Appl. Math. Comput. 413, 126639 (2022). https://doi.org/10.1016/j.amc.2021.126639
39. Aluko, A.O., Dorrell, D.G., Ojo, E.E.: Observer-based detection and mitigation scheme for isolated microgrid under false data injection attack. In: 2021 IEEE Southern Power Electronics Conference, SPEC 2021 (2021). https://doi.org/10.1109/SPEC52827.2021.9709472
40. Chen, X., et al.: Co-estimation of state and FDI attacks and attack compensation control for multi-area load frequency control systems under FDI and DoS attacks. IEEE Trans. Smart Grid 13(3), 2357–2368 (2022). https://doi.org/10.1109/TSG.2022.3147693

41. Zhao, J., Netto, M., Mili, L.: A robust iterated extended kalman filter for power system dynamic state estimation. IEEE Trans. Power Syst. 32(4), 3205–3216 (2017). https://doi.org/10.1109/TPWRS.2016.2628344
42. Chakhchoukh, Y., Lei, H., Johnson, B.K.: Diagnosis of outliers and cyber attacks in dynamic PMU-based power state estimation. IEEE Trans. Power Syst. 35(2), 1188–1197 (2020). https://doi.org/10.1109/TPWRS.2019.2939192
43. Li, Y., Li, Z., Chen, L.: Dynamic state estimation of generators under cyber attacks. IEEE Access 7, 125253–125267 (2019). https://doi.org/10.1109/ACCESS.2019.2939055
44. Doostmohammadian, M., et al.: Distributed estimation recovery under sensor failure. IEEE Signal Process. Lett. 24(10), 1532–1536 (2017). https://doi.org/10.1109/LSP.2017.2749265
45. Huang, Y., et al.: Preventing outages under coordinated cyber-physical attack with secured PMUs. IEEE Trans. Smart Grid 13(4), 3160–3173 (2022). https://doi.org/10.1109/TSG.2022.3165768
46. Jin, M., Lavaei, J., Johansson, K.H.: Power Grid AC-based state estimation: vulnerability analysis against cyber attacks. IEEE Trans. Automat. Control 64(5), 1784–1799 (2019). https://doi.org/10.1109/TAC.2018.2852774
47. Chen, Y., et al.: Evaluation of reinforcement learning-based false data injection attack to automatic voltage control. IEEE Trans. Smart Grid 10(2), 2158–2169 (2019). https://doi.org/10.1109/TSG.2018.2790704
48. Gers, F.A., Schmidhuber, J., Cummins, F.: Learning to forget: continual prediction with LSTM. Neural Comput. 12(10), 2451–2471 (2000). https://doi.org/10.1162/089976600300015015
49. An, D., et al.: Data integrity attack in dynamic state estimation of smart grid: attack model and countermeasures. IEEE Trans. Autom. Sci. Eng. 19(3), 1631–1644 (2022). https://doi.org/10.1109/TASE.2022.3149764
50. Kurt, M.N., Yilmaz, Y., Wang, X.: Distributed quickest detection of cyber-attacks in smart grid. IEEE Trans. Inf. Forensics Secur. 13(8), 2015–2030 (2018). https://doi.org/10.1109/TIFS.2018.2800908
51. Kazemi, Z., et al.: Finite-time secure dynamic state estimation for cyber-physical systems under unknown inputs and sensor attacks. IEEE Trans. Syst .Man Cybern. Syst. 52(8), 4950–4959 (2022). https://doi.org/10.1109/TSMC.2021.3106228
52. Ashok, A., Govindarasu, M., Ajjarapu, V.: Online detection of stealthy false data injection attacks in power system state estimation. IEEE Trans. Smart Grid 9(3), 1 (2018). https://doi.org/10.1109/TSG.2016.2596298
53. Aluko, A.O., et al.: Real-time cyber attack detection scheme for standalone microgrids. IEEE Internet Things J. 9(21), 21481–21492 (2022). https://doi.org/10.1109/JIOT.2022.3180939
54. Cheng, Z., et al.: Security analysis for dynamic state estimation of power systems with measurement delays. IEEE Trans. Cybern. 53(4), 2087–2096 (2023). https://doi.org/10.1109/TCYB.2021.3108884
55. Liu, M., et al.: Converter-based moving target defense against deception attacks in DC microgrids. IEEE Trans. Smart Grid 13(5), 3984–3996 (2021). https://doi.org/10.1109/TSG.2021.3129195
56. Liu, M., et al.: PDDL: proactive distributed detection and localization against stealthy deception attacks in DC microgrids. IEEE Trans. Smart Grid 14(1), 714–731 (2023). https://doi.org/10.1109/TSG.2022.3188489
57. Rana, M.M., Bo, R., Abdelhadi, A.: Distributed grid state estimation under cyber attacks using optimal filter and Bayesian approach. IEEE Syst. J. 15(2), 1970–1978 (2021). https://doi.org/10.1109/JSYST.2020.3010848
58. Rana, M.M.: Least mean square fourth based microgrid state estimation algorithm using the internet of things technology. PLoS One 12(5), e0176099 (2017). https://doi.org/10.1371/journal.pone.0176099
59. Basit, A., et al.: Distributed state and unknown input estimation under denial-of-service attacks: a dynamic event-triggered approach. IEEE Trans. Circ. Syst. II: Exp. Brief. 70(6), 2266–2270 (2023). https://doi.org/10.1109/TCSII.2022.3229412
60. Gao, Z., et al.: Dynamic state estimation of new energy power systems considering multi-level false data identification based on LSTM-CNN. IEEE Access 9, 142411–142424 (2021). https://doi.org/10.1109/ACCESS.2021.3121420
61. Taha, A.F., et al.: Risk mitigation for dynamic state estimation against cyberattacks and unknown inputs. IEEE Trans. Smart Grid 9(2), 886–899 (2018). https://doi.org/10.1109/TSG.2016.2570546

How to cite this article: Zhou, Z., et al.: Comprehensive review on dynamic state estimation techniques with cybersecurity applications. IET Smart Grid. 1–16 (2024). https://doi.org/10.1049/stg2.12168