Transition to Digitalized Paradigms for Security Control and Decentralized Electricity Market

Bellizio, Federica; Xu, Wangkun; Qiu, Dawei; Ye, Yujian; Papadaskalopoulos, Dimitrios; Cremer, Jochen L.; Teng, Fei; Strbac, Goran

DOI
10.1109/JPROC.2022.3161053

Publication date
2022

Document Version
Final published version

Published in
Proceedings of the IEEE

Citation (APA)
Bellizio, F., Xu, W., Qiu, D., Ye, Y., Papadaskalopoulos, D., Cremer, J. L., Teng, F., & Strbac, G. (2022). Transition to Digitalized Paradigms for Security Control and Decentralized Electricity Market. *Proceedings of the IEEE*, *111*(7), 744-761. https://doi.org/10.1109/JPROC.2022.3161053

INVITED PAPER

Transition to Digitalized Paradigms for Security Control and Decentralized Electricity Market

This article analyzes the potential of utilizing digitalization techniques for reliability enhancement and cost reduction in local electricity markets.

By Federica Bellizio, *Student Member IEEE*, Wangkun Xu, *Student Member IEEE*, Dawei Qiu, *Member IEEE*, Yujian Ye, *Senior Member IEEE*, Dimitrios Papadaskalopoulos, *Member IEEE*, Jochen L. Cremer, *Member IEEE*, Fei Teng, *Senior Member IEEE*, and Goran Strbac, *Member IEEE*

ABSTRACT | Digitalization is one of the key drivers for energy system transformation. The advances in communication technologies and measurement devices render available a large amount of operational data and enable the centralization of such data storage and processing. The greater access to data opens up new opportunities for a more efficient and decentralized management of the energy system. At the distribution level of the energy system, local electricity markets (LEMs) provide new degrees of flexibility by trading and balancing the energy locally and offering ancillary services to the wider transmission and distribution system operators. Maximizing the grid impact from this flexibility calls for novel data analytics and artificial intelligence techniques to enhance the system's security and reduce the energy costs of local prosumers. At the same time, however, relying on data-based approaches increases the risk of cyberattacks, and robust countermeasures are, therefore, needed as an integral aspect of digitalization efforts. This article discusses the key role of centralized data analytics to fully benefit from the advantages of LEMs in terms of system's security enhancement and energy costs' reduction. Data-driven paradigms are investigated that allow for flexibility from decentralized markets, mitigate the physical security risks, and devise defensive strategies shielding the system from cyber threats.

KEYWORDS | Artificial intelligence (AI); cybersecurity; digitalization; local electricity markets (LEMs); system security.

I. INTRODUCTION

Power systems are undergoing a fundamental transition from the conventional fossil-fuel-based paradigm to a decentralized and digitalized paradigm based on the massive integration of renewable energy sources (RESs), distributed energy sources (DERs), and advanced communication and information technologies (ICTs). This transition is massively changing the way energy is transmitted, distributed, and managed [1]. In the past, the system inertia from fossil-fuel generators provided imminent flexibility to stabilize operations following disturbances. As DERs and RES are connected through power inverters, they do not provide inertia; instead, they introduce very fast coupling dynamics that are rather challenging for the system's security management [2], [3]. The current strategy to address these emerging challenges follows the centralized

Manuscript received 14 December 2021; revised 16 February 2022; accepted 10 March 2022. Date of publication 12 April 2022; date of current version 13 July 2023. This work was supported in part by the Engineering and Physical Sciences Research Council, U.K., through the Integrated Development of Low-Carbon Energy Systems Programme under Grant EP/R045518/1 and in part by the TU Delft AI Labs Programme, The Netherlands. *(Corresponding authors: Goran Strbac; Yujian Ye; Federica Bellizio.)*

Federica Bellizio, Wangkun Xu, Dawei Qiu, Dimitrios Papadaskalopoulos, Fei Teng, and **Goran Strbac** are with the Department of Electrical and Electronic Engineering, Imperial College London, London SW7 2AZ, U.K. (e-mail: f.bellizio18@imperial.ac.uk; g.strbac@imperial.ac.uk).

Yujian Ye, is with the School of Electrical Engineering, Southeast University, Nanjing 210096, China (e-mail: yujian.ye11@imperial.ac.uk).

Jochen L. Cremer is with the Department of Electrical Sustainable Energy, Delft University of Technology (TU Delft), 2628 CD Delft, The Netherlands.

Digital Object Identifier 10.1109/JPROC.2022.3161053

paradigms from the past. To consider the new dynamics in the timescale of electromagnetic transients, the centralized strategy is to operate with very large static margins and invest in redundant grid infrastructure.

More efficient management of the system can be achieved by the integration of new digital technologies that are more powerful and interconnected and allow for the centralization of the large amount of data coming from phasor measurement units (PMUs). This data centralization enables the use of more advanced processing techniques, such as artificial intelligence (AI) and machine learning (ML), to fully exploit the new flexibility provided by the DERs at the local distribution level. There, novel data-driven paradigms for local electricity markets (LEMs) can benefit: 1) local prosumers by balancing and trading the energy locally and 2) network operators by offering ancillary services (ASs) to alleviate the RES uncertainty and cost-efficiently manage network congestions. The real-time provision of ASs from LEMs would allow operators to include corrective and distributed control approaches in their centralized operating tools and expand the normal physical and cyber-operating limits [4], [5]. However, the risk of relying on such data-driven approaches is cyberattacks by malicious third-party actors. As the extent of digitalization is enhanced, these attacks have increasingly detrimental consequences. Therefore, new defensive measures are needed to protect the cyber–physical system (CPS) [6].

Securely managing congestion when system operations experience physical disturbances and cyberattacks in a decentralized CPS is challenging. Models of the full CPS are only available at centralized operators and face several issues. These models become too complex through the large number of DERs with diverse operating characteristics that change frequently, and these models are easily exposed to targeted, centralized cyberattacks. The high degree of digitalization of the grid and a large amount of data available enable the investigation of decentralized paradigms for secure CPS operation with LEMs that would be infeasible using purely model-driven approaches. Learning decentralized models from locally observed data is promising to address some of the aforementioned issues. These models learn localized actions that support system-important objectives, such as resilience, reliability, security assessment, controlled response to disturbances, cyber robustness, energy balancing, and flexibility trading in LEMs. For instance, ML algorithms can learn effective strategies for real-time dynamic security assessment (DSA) [7], reinforcement learning (RL) models can learn the sequence of trading decisions in LEMs, and defense strategies can mitigate the cyber vulnerabilities from such data-driven models [8]–[10].

This work reviews the key role of digitalization in the shift toward decentralized paradigms for secure and cost-efficient CPS operation with LEMs. The contribution is threefold: 1) a comprehensive data-driven model for dynamically secure system operation and control that considers LEMs; 2) a novel LEM paradigm that enables coordinated local energy trading and provision of ASs to the wider system while adopting a model-free decision-making approach through multiagent RL (MARL); and 3) a layered detection mechanism to identify stealth cyberattacks with high confidence. The rest of this article is structured as follows. In Section II, the data-driven model for security assessment and control is described. Section III introduces the proposed LEM paradigm. In Section IV, the detection algorithm against cyberattacks is presented. Finally, the case study is presented in Section V. Conclusions are drawn in Section VI.

II. SYSTEM'S SECURITY ASSESSMENT AND CONTROL

A decentralized system still requires continuous monitoring and assessment of system's security as the high shares of RES and flexible loads expose the grid to many kinds of new faults and faster dynamics [11], [12]. To maintain secure operations, operators can use new real-time operating tools that consider more flexibility, decentralization, and corrective control or to harden their system infrastructure, which is expensive. New operating approaches that consider these new dynamics allow for decentralization with lowered inertia. Most of the software tools that operators currently use in day-to-day operations only assess the static security of the system for a short list of potential faults, which refers to whether the system subjected to a disturbance fulfills all physical constraints in the postfault steady state [13]. However, the assessment of static security with $N-1$ criteria does not include whether the system survives the transition from prefault to postfault that is considered in DSA. To assess if the system is dynamically secure, a set of typical dynamical phenomena is studied, mainly relating to the stability in rotor angles, i.e., transient stability, frequency, and voltages [14]. Each of these phenomena needs to be analyzed separately, and these conventional analyses require very long computational times as time-domain simulations are computed using numerical integration (e.g., forward Euler or Runge–Kutta methods). Therefore, assessing the dynamic security in real-time operation, which would require computations of few milliseconds (according to the timescale of interest), is infeasible using the conventional, analytical techniques.

Beyond the assessment of security, the low-inertia system requires fast corrective control operating tools that can be applied in real time to control the system's security following potential disrupting faults. When considering dynamic security as reliability criteria, relying only on preventive control is infeasible to consider all eventualities following the $N-1$ criterion in the future, which would be too conservative. Holding manual activation of corrective strategies as a backup strategy as in the past is not sufficient anymore as it is too slow. Promising is combining preventive control tools [e.g., modeled within ac optimal power flow (OPF)] with new corrective control measures in such a way that can optimally balance operating costs and security. However, optimizing this balance may require implementing the system's dynamic response within an ac

OPF. This implementation is very challenging and takes long computational times when conventional approaches are used, e.g., forward Euler or Runge–Kutta methods [4], [5]. Therefore, with conventional approaches, corrective control cannot be used to actively maintain the system stability in real time as only a few milliseconds are available to respond to faults, which is the same conclusion as the previous paragraph on DSA.

ML is promising for real-time DSA and control as predicted security or control actions are instantly available [7], [15]. The idea is that an off-line trained ML model can be used to assess (dynamic) security of many possible fault scenarios and control the operating condition in real time. However, as the ML predictions could be inaccurate, probabilistic security standards are best suitable to use these ML-based real-time DSA approaches. With probabilistic security standards, the risk of inaccuracy can be quantified and considered within probabilistic security assessments in [16].

A. Machine Learning-Based Approaches

The assessment and control of the system's security can be described as statistical classification and regression problems, respectively, from ML. Let $\mathbf{x}(t) = [\mathbf{x}^L(t), \mathbf{x}^G(t), \mathbf{x}^V(t)]$ be the state variables describing the loads (active/reactive loads), generation (active/reactive injected powers), and voltages with $\mathbf{x}^L \in \mathbb{R}^L \subseteq \mathbb{R}^n, \mathbf{x}^G \in \mathbb{R}^G \subseteq \mathbb{R}^n$, and $\mathbf{x}^V \in \mathbb{R}^V \subseteq \mathbb{R}^n$ at time step t and n the number of buses. However, the time dependence is omitted to make the notation clearer. ε_{NET} is the network's physical interconnectivity, and ε_{LEM} is the trading energy network, which are defined as follows:

$$\varepsilon_{\text{NET},ij} = \begin{cases} 1, & \text{if } i,j \text{ adjacent} \\ 0, & \text{otherwise} \end{cases}$$
$$\varepsilon_{\text{LEM},pk} = \begin{cases} 1, & \text{if } p,k \text{ direct trading} \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

where $i, j \in [1, \ldots, n]$ are two different buses and p, k are two different sets of buses that represent the prosumers' DERs described in Section III-A participating in the kth and pth LEMs with $p, k \in [1, \ldots, m]$ [17]. $\mathbf{x}_k = [\mathbf{x}_k^L, \mathbf{x}_k^G, \mathbf{x}_k^V]$ is the subset of state variables for the kth LEM.

The system's security can be expressed as a function $f_a(\mathbf{x}, \varepsilon_{\text{NET}}, \varepsilon_{\text{LEM}})$ where

$$f_a\colon (\mathbf{x}, \varepsilon_{\text{NET}}, \varepsilon_{\text{LEM}}) \longrightarrow y_a = \begin{cases} 1, & \text{insecure} \\ 0, & \text{secure,} \end{cases} \tag{2}$$

Similarly, the optimal controller for system's security is a function $f_c(\mathbf{x}^L, \varepsilon_{\text{NET}}, \varepsilon_{\text{LEM}})$ that

$$f_c\colon \left(\mathbf{x}^L, \varepsilon_{\text{NET}}, \varepsilon_{\text{LEM}}\right) \longrightarrow \left(\mathbf{x}_{\text{opt}}^G, \mathbf{x}_{\text{opt}}^V\right) \tag{3}$$

where $(\mathbf{x}_{\text{opt}}^G, \mathbf{x}_{\text{opt}}^V)$ are the cost-optimal generator settings fulfilling all power system constraints and security criteria. For large systems, the assessment and control functions f_a and f_c are often highly nonlinear and nonconvex, and hence, it is very challenging to find (and evaluate) these functions.

The approach of ML is to learn approximating functions

$$\tilde{f}_a\colon (\mathbf{x}, \varepsilon_{\text{NET}}, \varepsilon_{\text{LEM}}) \longrightarrow \tilde{y}_a$$
$$\tilde{f}_c\colon \left(\mathbf{x}^L, \varepsilon_{\text{NET}}, \varepsilon_{\text{LEM}}\right) \longrightarrow \tilde{\mathbf{y}}_c = \left[\tilde{\mathbf{x}}_{\text{opt}}^G, \tilde{\mathbf{x}}_{\text{opt}}^V\right] \tag{4}$$

such that

$$||y_a - \tilde{y_a}||_p,\ ||\mathbf{y}_c - \tilde{\mathbf{y}}_c||_p \text{ are minimized.} \tag{5}$$

Learning these functions with supervised learning requires creating, as a first step, a database (X, Y) that includes OCs $\mathbf{x}$ (or $\mathbf{x}^L$ for security control) from historical observations and synthetically generated data, including their respective security labels y_a (or optimal generator settings y_c). The synthetic data can be generated by randomly sampling the loads from multivariate Gaussian or C-Vine pair-copula decomposition schemes to generate more representative OCs [18].

The supervised learning of the functions $\tilde{f}_a$ and $\tilde{f}_c$ involves splitting the database (X, Y) into training $(X_{\text{train}}, Y_{\text{train}})$ and testing dataset $(X_{\text{test}}, Y_{\text{test}})$ with $X_{\text{train}}, X_{\text{test}} \subseteq X$ and $Y_{\text{train}}, Y_{\text{test}} \subseteq Y$ such that $X_{\text{train}} \cap X_{\text{test}} = \emptyset$ and $Y_{\text{train}} \cap Y_{\text{test}} = \emptyset$. An ML-algorithm learns the function $\tilde{f}_{\text{train}}$ from the training set

$$\tilde{f}_{\text{train}}\colon \mathbf{x}_{\text{train}} \longrightarrow \tilde{y}_{\text{train}} \tag{6}$$

with $\mathbf{x}_{\text{train}} \in X_{\text{train}}$ such that

$$|y_{\text{test}} - \tilde{f}_{\text{train}}(\mathbf{x}_{\text{test}})| \text{ is minimized} \tag{7}$$

with $\mathbf{x}_{\text{test}} \in X_{\text{test}}, \mathbf{y}_{\text{test}} \in Y_{\text{test}}$.

Some choices on the candidate function $\tilde{f}_{\text{train}}$ (e.g., parametrisation) need to be made before applying the ML training algorithm. One typical choice is to consider "rules" organized hierarchically and sequentially to predict the label/value [19]. For instance, many researchers have used decision trees (DTs) to learn these rules; a popular algorithm is CART (more example algorithms can be found in [20]) or neural networks (NNs). There, let $\Omega^+ = \{\mathbf{x} \in \mathbb{R}^n\colon f(\mathbf{x}, \varepsilon) = 1\}$ with $\varepsilon = [\varepsilon_{\text{NET}}, \varepsilon_{\text{LEM}}]$ and approximate it as the union of N convex polytopes $\tilde{\Omega}^+ = \cup_{i=1}^N P_i$ with $P_i = \cap_{j=1}^{M_i} H_{ij}$ of M_i half-spaces $H_{ij} = \{\mathbf{x} \in \mathbb{R}^n\colon h_{ij}(\mathbf{x}, \varepsilon) > 0\}$. h_{ij} is the indicator function defined as follows:

$$h_{ij}(\mathbf{x}, \varepsilon) = \begin{cases} 1, & \sum_{k=1}^n \omega_{ij,k} x_k + b_{ij} \geq 0 \\ 0, & \text{otherwise} \end{cases} \tag{8}$$

where $\omega_{ij,k}$ and b_{ij} are the weights and the bias term, respectively. Hence, the approximation function $\tilde{f}_a$ in (4) can be written as a disjunction of conjunctions, also known as disjunctive form

$$\tilde{f}_a(\mathbf{x}, \varepsilon) = \bigvee_{i=1}^{N} \left(\bigwedge_{j=1}^{N} h_{ij}(\mathbf{x}, \varepsilon) \right) \tag{9}$$

such that $\tilde{\Omega}^+ = \{\mathbf{x} \in \mathbb{R}^n : \tilde{f}_a(\mathbf{x}, \varepsilon) = 1\}$ and $\tilde{\Omega}^+$ is an approximation of Ω^+. In a similar way, $\tilde{f}_c$ can be also written as a disjunctive form as follows:

$$\tilde{f}_c\left(\mathbf{x}^L, \varepsilon\right) = \bigvee_{i=1}^{N} \left(\bigwedge_{j=1}^{N} h_{ij}\left(\mathbf{x}^L, \varepsilon\right) \right) \tag{10}$$

with $\tilde{\Omega}^+ = \{\mathbf{x} \in \mathbb{R}^L : \tilde{f}_c(\mathbf{x}, \varepsilon) = 1\}$ and $n_1 = |\tilde{\Omega}^+|$. In this case, the predicted values are calculated as follows:

$$\tilde{\mathbf{y}}_c = \frac{\sum_{k=1}^{n_1} \omega_{ij,k} x_k^L + b_{ij}}{n_1}. \tag{11}$$

Different indicator functions $h_{ij}(\mathbf{x}, \varepsilon)$ correspond to different ML models; for example, an NN can be defined using indicators in (8), but the same indicators, without the bias terms b_{ij}, can be used to represent a DT model as a set of split functions [21]. The two approximation functions $\tilde{f}_a$ and $\tilde{f}_c$ can be also integrated into a single multitask learning (MTL) model, for example, an NN in which the total loss $J(\alpha)$ is the weighted sum of the loss function of the two tasks [22]

$$J(\alpha) = \alpha_1 |y_a - \tilde{y}_a| + \alpha_2 |\mathbf{y}_c - \tilde{\mathbf{y}}_c| \tag{12}$$

with $\alpha = [\alpha_1, \alpha_2]$ being the set of the loss weights for the two tasks.

Not only maximizing predicting accuracy is important but also the interpretability and generalization capability to other network reconfigurations. Although NNs generally provide high accurate predictions, DTs or ensemble of DTs have been mostly adopted for power system applications, above all for DSA, as they are more interpretable than NNs. Interpretability is important to build up the trust of operators in these methods. High model interpretability supports operators to understand how a model predicts and maintains the security with little inspection allowing operators to be still involved in the control loop [23]. However, even the most accurate and interpretable model may not be function anymore when the system configuration is different from the training configuration. As shown in (4), completely different ML models are suitable for different ε_{NET}'s and ε_{LEM}'s, and this, low generalizability, is a key barrier for their applications to power systems. For instance, the ML-based model trained offline for settings ε_{pre} prior to a change may not work anymore for the new system's configurations or trading network $\varepsilon_{\text{post}}$. Therefore, the ML models for system's security and control must have a high level of generalization capability to different system's configurations and trading networks [24]. This becomes important as system's operators use more frequent reconfigurations of the system for maintenance and control purposes in real-time operations, e.g., disconnecting lines, switching ON/OFF generators, shunt components, or merging the substations. To improve the generalization capability of ML models, several approaches were investigated, such as considering different settings in the training databases as in [25] or periodically updating the ML model and the training database as in [26] and [27].

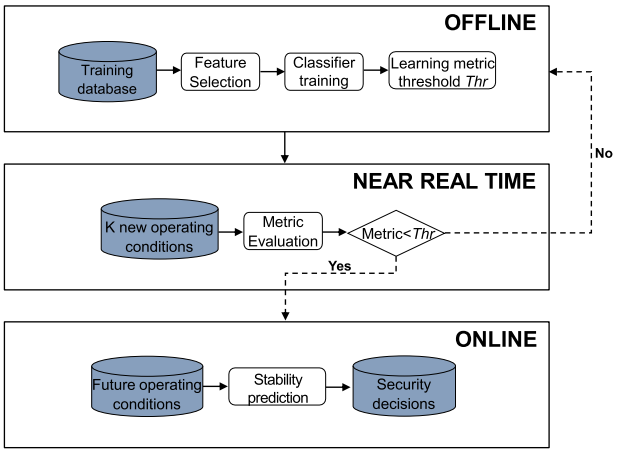

Fig. 1. ***Data-driven workflow for DSA to deal with topology changes [30].***

B. Physics-Informed Machine Learning

Informing ML approaches for system approaches with the known physics of the network is highly promising as it increases their generalization, robustness, and interpretability [28]. Known physics can either be induced or learned when training the model. For models predicting the security, the known physics relate to the swing equations and other dynamics, which can be learned through regularizing the loss functions, as in physics-informed NNs (PINNs) [29]. For models predicting control actions, the known physics relate to the power flow equations (e.g., Kirchhoff's law), which can verify the feasibility of control strategies.

An example for inducing physical knowledge for ML-based DSA is that the network topology ε_{NET} can be used in the correlation structure between the input features and the dynamic security [31]. According to the correlation structure $\rho_{\varepsilon_{\text{NET}}}$, features that are most relevant to security are selected [24]. Then, a metric quantifies the impact of a system's (topology) change and accordingly triggers retraining of the model when the model is expected at low generalizability in [24] (see Fig. 1). By capturing the physical interconnectivity of the network, the ML model is effectively trained and updated very close to real time, which ultimately improves the accuracy.

An example for learning the known physical knowledge in DSA is to consider training losses describing the differences between learned and known physical equations. Misyris *et al.* [29] consider the power system differential and algebraic equations in the loss function when training a PINN that predicts the system dynamics. This approach reduces the data needed for training. In the training approach, the NN predicts the state variables $\tilde{\mathbf{x}}^V$ from inputs $\mathbf{x}^L$, and then, the first-order derivatives of the predicted variables are evaluated using automatic differentiation (AD). These derivatives allow including the physical regularization in the training loss function as follows:

$$J = a_1 \left| \mathbf{x}^V - \tilde{\mathbf{x}}^V \right| + a_2 \left| \tilde{f}\left(\tilde{\mathbf{x}}^V\right) - \dot{\tilde{\mathbf{x}}}^V \right| \tag{13}$$

where the first term is the error between predicted and actual values of the state variable $\mathbf{x}^V$ and the second is the loss from physical regularization. a_1 and a_2 are the loss weights that need to be tuned during the training. PINNs are also used to predict the dynamics of a power system subjected to a fault in [29] and to estimate the nonlinear parameters of power system dynamics in [32]. However, PINNs do not yet scale for larger power systems, and more work is needed to develop them for real-time DSA applicability. A scientific gap is developing ML methods that induce (and learn) system knowledge as bias and adopt such methods for DSA and dynamic controls.

Another example of learning the known physics for the control of dynamics is to consider stability theory. Lyapunov stability with energy functions is mostly used for security assessment [33]. There, Lyapunov functions are very hard to find [34], especially in large systems. However, recent research focused on scalable approaches to identify these functions. The idea is that NNs model the Lyapunov function for large power systems and predict the transient stability of power systems [35]. Moving this approach one step further, the Lyapunov stability allows expressing the system's transient response as linear constraints within the ACOPF that can be solved very quickly in real time to compute preventive and corrective control actions. This idea is similar to the one in Fig. 2 [36] where disjunctive security rules were learned by a DT and considered as linear constraints within an OPF formulation to compute optimal preventive control actions. The ML-based security rules can be also used to derive the optimal corrective control strategy when preventive control fails, as in [37]. Here, the security of the optimized prefault OCs is assessed using a DT. When the OC is insecure, corrective control reduces the difference in generation between this prefault OC and the closest secure one in terms of the Euclidean distance.

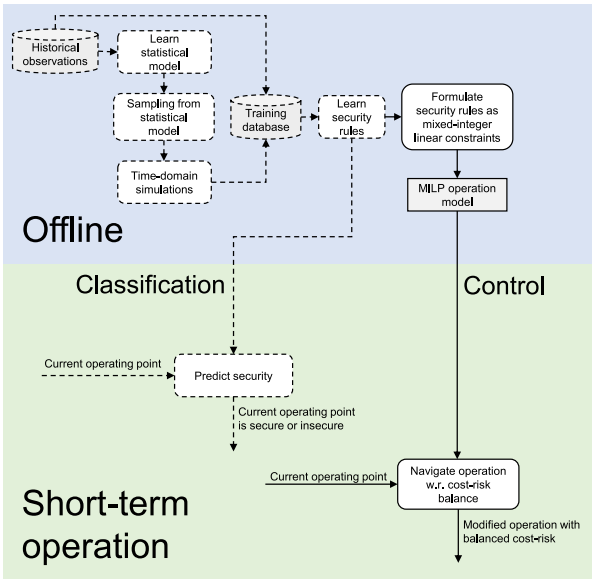

Fig. 2. ***Data-driven workflows for classification (dashed lines) and the control purpose (straight lines) [36].***

III. LOCAL ELECTRICITY MARKETS

A. Context and Motivation

As discussed in Section I, the exploitation of the significant flexibility of DER owned and operated by small-scale prosumers constitutes a critical factor in achieving cost-effective electricity system decarbonization. Nevertheless, beyond setting ambitious decarbonization targets, governments in most parts of the world are committed to follow a deregulated electricity industry framework, where operation and investment decisions are not driven by vertically integrated monopoly utilities but rather by open and competitive electricity markets, encapsulating the economic objectives and technical requirements of multiple independent market participants. This implies that the DER flexibility potential needs to be realized through a suitable integration and active participation of prosumers in the electricity market.

However, the current, largely centralized, structure of electricity markets exhibits fundamental limitations in achieving such integration and active participation [38]. From the market operators' perspective, the retrieval of technoeconomic information from a vast number of small-scale and diverse prosumers and the calculation of the market-clearing solution become intractable due to communication and computational scalability challenges. From the prosumers' perspective, such centralized market mechanisms raise privacy concerns and unmanageable price variability risks. As a result, instead of directly participating in the electricity market, prosumers are implicitly represented by: 1) contracted electricity retailers in the energy segment of the market and 2) by aggregators in ASs markets (although it should be noted that new market entrants, serving the dual role of retailer and aggregators, have been recently witnessed).

Concerning the former, retailers absorb the wholesale price risks on behalf of the prosumers and sell energy to them based on less variable and more predictable retail

tariffs. However, most retailers still offer completely "flat" retail tariffs that do not reflect the time-specific value of energy in the system or fixed time-of-use (ToU) tariffs with limited time variability [38]. As a result, prosumers are prevented from mobilizing their DER flexibility toward consuming energy during periods of abundant renewable generation and low demand, and avoiding consumption during periods of low renewable generation and high demand. This challenge is gradually resolved with the introduction of highly dynamic retail tariffs, linked to the wholesale energy prices by new competitive retailers. Furthermore, the offered import tariffs (for buying energy from the grid) are significantly higher than the offered export tariffs (for selling energy to the grid), which, beyond factoring in the required network costs, is driven by the retailers' strategic, profit maximization objectives [39].

In AS markets, and especially balancing markets that become crucial as the penetration of renewable generation in electricity systems is increased, the majority of markets impose excessively strict limits on the minimum size and minimum temporal availability of the participants [38]. Therefore, in a similar fashion with energy markets discussed above, small prosumers are represented by aggregators that operate DER portfolios with critical volumes and diversity to access such markets and distribute the obtained revenues to their contracted prosumers accordingly. However, this aggregation requirement entails significant economic (in terms of sacrificing part of the value of DER in AS to compensate the aggregators' activities) and regulatory (in terms of aggregating DER of prosumers settled by different retailers in the energy market) challenges. Furthermore, the largest proportion of balancing services (BSs) is currently procured by system operators over long horizons (even months-ahead) with "flat" prices that do not reflect the time-specific value of BSs (depending, for example, on the demand levels, renewable output levels, and system inertia). This prevents the mobilization of DER flexibility in balancing markets (considering the prosumers' uncertainties over such long horizons) and results in risks of overprocurement (with cost implications) or underprocurement (with security implications) of BSs.

In this context, the attention of the research community has recently shifted to decentralized, LEMs [40], as a new framework toward enabling the market-based realization of the DER flexibility potential while addressing the above scalability, privacy, and economic efficiency challenges. Instead of merely relying on a centralized electricity market with limited access and complex intermediary (i.e., retailers and aggregators) arrangements, the LEM concept introduces localized electricity marketplaces, enabling more direct access for local prosumers and breaking down the system-wide market coordination to the coordination of smaller, more manageable DER clusters. Furthermore, LEMs enable direct energy trading among the participating prosumers, which promises a reduction of their net energy costs. This is because the import–export tariff differential creates an economic motivation for self-consumption of any excess energy through the suitable management of flexible DERs. Local energy trading enhances the overall extent of self-consumption by harnessing the excess generation and flexibility of all participating prosumers' DER compared to a case where each prosumer relies solely on its own excess generation and flexible DERs, considering the natural diversity of different prosumers [39]. Finally, LEMs can implicitly serve the role of aggregating DER portfolios for accessing balancing markets, without the above-discussed economic and regulatory challenges associated with external aggregators.

B. Previous Work and Relevant Contributions

The rich and fast-developing literature on the coordination of LEMs can be concretely reviewed against three distinct criteria. The first one lies in the coordination architecture of the LEMs, based on which the existing literature can be broadly classified in: 1) system-centric coordination architectures [41]–[44], resembling the architecture of national markets and involving a central coordinator responsible for DERs' information collection and dispatch (based on a central optimization function); despite their solution optimality in theoretical terms, such architectures are characterized by scalability, privacy, and reliability challenges and 2) prosumer-centric coordination architectures [45]–[51] where the prosumers do not share information with the central coordinator and are responsible for their DERs' dispatch; although such architectures cannot generally guarantee solution optimality, they address the above practical challenges.

The second criterion lies in the decision-making approach, based on which the existing literature can be broadly classified in: 1) model-based optimization approaches [41]–[46], [50], [51] that require knowledge of the complex DER operating models and accurate forecasts of uncertain parameters; such requirements involve massive monitoring, computational, and forecasting costs and 2) model-free, data-driven approaches [47]–[49], with deep RL (DRL) receiving particular attention recently; the decision-making entities are modeled as agents gradually learning effective dispatch policies based on data and experiences from the repeating interactions with their environment, without explicit knowledge of the latter or external forecasts.

The last criterion lies in the market functionalities of the LEMs, based on which the existing literature can be classified in: 1) LEMs focusing on local energy trading [41], [42], [45]–[49]; 2) LEMs focusing on the provision of AS to the national transmission system and/or to the local distribution network [43], [44]; and 3) LEMs combining local energy trading and provision of AS [50], [51], which constitutes a major challenge toward maximizing the economic value of LEMs.

Based on the above review, no previous work has adopted a prosumer-centric architecture and a model-free decision-making approach, while, at the same time,

exploring LEMs enabling both local energy trading and AS provision; addressing this gap constitutes the relevant contribution of this work.

C. Problem Setting

The focus lies in the coordination of an LEM consisting of a group of residential prosumers, each of which owns and operates a diverse DER portfolio, generally including a PV generator, inflexible demand, an electric vehicle (EV) with smart charging and discharging flexibility, and an energy storage (ES) system, as illustrated in Fig. 3. A standard set of EV and ES operating constraints is considered in this work, including energy balance constraints, minimum/maximum energy limits, maximum charging/discharging power limits, and avoidance of simultaneous charging and discharging (for both EV and ES), as well as traveling times and energy requirements for traveling (for EV alone). An LEM platform constitutes the interface between the participating prosumers and external market entities.

This LEM allows local energy trading among the participating prosumers, enabling the latter to maximize their collective self-consumption and reduce their net energy costs (see Section IV-A). Any residual demand or excess generation is traded with the retailer according to the latter's import or export tariffs, respectively. The LEM platform sets the local energy prices and coordinates the residual trading with the retailer. Concerning the former task, the mid-market rate (MMR) mechanism is employed due to its comparative advantages against alternative mechanisms [48], [49].

Beyond local energy trading, this LEM allows provision of AS to external system operators (which may generally include the national ESO, the local DSO, or both) by the flexible subset of the considered DER (namely EV and ES). In order to capture the general principles of AS, two generic types of AS are considered: 1) upward AS (increasing generation/reducing demand of DER with respect to their baseline energy generation/demand) and 2) downward AS (reducing generation/increasing demand of DER with respect to their baseline energy generation/demand). The LEM platform aggregates and sells the upward and downward ASs to the external system operators. The upward and downward AS prices constitute exogenous input parameters, determined by the system operators.

The overall objective of the LEM lies in minimizing the net cost of the group of participating prosumers, involving the difference between the import energy cost (cost of buying residual demand from the retailer), the export energy revenue (revenues of selling excess generation to the retailer), and the AS revenue.

D. Markov Game Formulation of LEM Coordination Problem

Since the focus lies in a combination of a prosumer-centric coordination architecture along with a model-free decision-making approach, the examined LEM coordination problem is formulated as a finite Markov game (MG) with discrete time periods. The MG is defined by N agents (which correspond to the participating prosumers) with a set of states $\mathcal{S}$ describing the global state, a collection of private observations $\{\mathcal{O}_{1:N}\}$, a collection of action sets $\{\mathcal{A}_{1:N}\}$, a collection of reward functions $\{\mathcal{R}_{1:N}\}$, and a state transition function $\mathcal{T}$. The time interval between two consecutive periods is Δt.

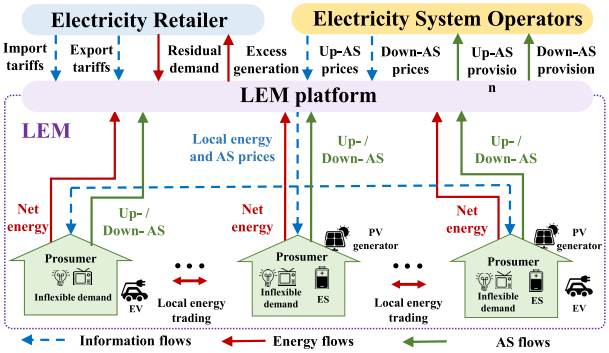

Fig. 3. *Illustration of examined problem setting.*

Instead of possessing explicit knowledge of their DER operating models (as in model-based optimization approaches), the agents determine their actions in an agnostic environment and the operating constraints of their DER are imposed ex post. Specifically, at each period t, each agent n selects an action $a_{n,t}$, and the environment moves to the next state according to the state transition function and all agents' actions. The agent receives a reward $r_{n,t}$ and a private observation for the next period $o_{n,t+1}$ and aims at maximizing a cumulative discounted reward $R_n = \sum_{t=0}^{T} \gamma^t r_{n,t}$, where $\gamma \in [0, 1)$ is the discount factor. A more detailed discussion of the MG components is provided in the following.

1) Observation: The observation $o_{n,t}$ of each agent n at period t is defined as $o_{n,t} = [t, P^{\text{id}}_{n,t}, P^{\text{pv}}_{n,t}, E^{\text{ev}}_{n,t-1}, E^{\text{es}}_{n,t-1}, A^{\text{ev}}_{n,t}, \lambda^{b}_{t}, \lambda^{s}_{t}, \lambda^{A,u}_{t}, \lambda^{A,d}_{t}]$, where $P^{\text{id}}_{n,t}$ and $P^{\text{pv}}_{n,t}$ denote the inflexible demand and PV generation of prosumer n at period t; $E^{\text{ev}}_{n,t-1}$ and $E^{\text{es}}_{n,t-1}$ denote energy in EV and ES of prosumer n at the end of period $t-1$; $A^{\text{ev}}_{n,t}$ is a binary parameter indicating whether the EV of prosumer n is connected to the grid at period t ($A^{\text{ev}}_{n,t} = 1$) or not ($A^{\text{ev}}_{n,t} = 0$); $\lambda^{b}_{t}, \lambda^{s}_{t}, \lambda^{A,u}_{t}$, and $\lambda^{A,d}_{t}$ denote the retail import and export energy tariffs and upward and downward AS prices at period t. The global state of the LEM environment s_t is derived as the concatenation of all agents' observations at period t, i.e., $s_t = (o_{1,t}, o_{2,t}, \ldots, o_{N,t})$.

2) Action: The action $a_{n,t}$ of each agent n at period t is defined by its energy and AS provision decisions with respect to its flexible DER (EV and ES). Actions $a^{\text{ev}}_{n,t} \in [-1, 1]$ represent the size of the charging (positive) and discharging (negative) power of the EV as a ratio

of its maximum power limit $\overline{P}_n^{\mathrm{ev}}$. The actual charging ($P_{n,t}^{\mathrm{evc}}$)/discharging ($P_{n,t}^{\mathrm{evd}}$) power of the EV is imposed ex post by the environment according to (14)/(15), where the first terms in the min operator impose its power limits and the second terms impose its energy limits

$$P_{n,t}^{\mathrm{evc}} = \min\left(a_{n,t}^{\mathrm{ev}} A_{n,t}^{\mathrm{ev}} \overline{P}_n^{\mathrm{ev}}, \frac{\overline{E}_n^{\mathrm{ev}} - E_{n,t-1}^{\mathrm{ev}}}{\Delta t \eta_n^{\mathrm{evc}}}\right) \tag{14}$$

$$P_{n,t}^{\mathrm{evd}} = \min\left(-a_{n,t}^{\mathrm{ev}} A_{n,t}^{\mathrm{ev}} \overline{P}_n^{\mathrm{ev}}, \frac{\left(E_{n,t-1}^{\mathrm{ev}} - \underline{E}_n^{\mathrm{ev}}\right)\eta_n^{\mathrm{evd}}}{\Delta t}\right) \tag{15}$$

where $\underline{E}_n^{\mathrm{ev}}, \overline{E}_n^{\mathrm{ev}}$ denote the minimum and maximum energy limits of the EV battery of prosumer n, respectively; η_n^{evc} and η_n^{evd} denote the charging and discharging efficiencies of the EV of prosumer n, respectively.

Based on $P_{n,t}^{\mathrm{evc}}$ and $P_{n,t}^{\mathrm{evd}}$, and according to the energy balance constraint of EV, the transition of $E_{n,t}^{\mathrm{ev}}$ is imposed ex post by the environment as

$$E_{n,t}^{\mathrm{ev}} = E_{n,t-1}^{\mathrm{ev}} + P_{n,t}^{\mathrm{evc}} \eta_n^{\mathrm{evc}} \Delta t - P_{n,t}^{\mathrm{evd}} \Delta t / \eta_n^{\mathrm{evd}} - E_{n,t}^{\mathrm{tr}} \tag{16}$$

where $E_{n,t}^{\mathrm{tr}}$ denotes the energy requirement of the EV of prosumer n for traveling purposes at period t.

The net power of the EV is subsequently defined as $P_{n,t}^{\mathrm{ev}} = P_{n,t}^{\mathrm{evc}} - P_{n,t}^{\mathrm{evd}}$ and actions $a_{n,t}^{\mathrm{ev,au}}$ and $a_{n,t}^{\mathrm{ev,ad}} \in [0,1]$, which represent the size of the upward and downward AS provisions of the EV as a ratio of its maximum power limits. The actual upward AS ($\mathrm{AU}_{n,t}^{\mathrm{ev}}$)/downward AS ($\mathrm{AD}_{n,t}^{\mathrm{ev}}$) provision is imposed ex post according to (17)/(18), where the first terms in the min operator impose its power limits and the second terms impose its energy limits

$$\mathrm{AU}_{n,t}^{\mathrm{ev}} = \min\left(a_{n,t}^{\mathrm{ev,au}} A_{n,t}^{\mathrm{ev}} \left(\overline{P}_n^{\mathrm{ev}} + P_{n,t}^{\mathrm{ev}}\right), \frac{\left(E_{n,t}^{\mathrm{ev}} - \underline{E}_n^{\mathrm{ev}}\right)\eta_n^{\mathrm{evd}}}{\Delta t}\right) \tag{17}$$

$$\mathrm{AD}_{n,t}^{\mathrm{ev}} = \min\left(a_{n,t}^{\mathrm{ev,ad}} A_{n,t}^{\mathrm{ev}} \left(\overline{P}_n^{\mathrm{ev}} - P_{n,t}^{\mathrm{ev}}\right), \frac{\overline{E}_n^{\mathrm{ev}} - E_{n,t}^{\mathrm{ev}}}{\Delta t \eta_n^{\mathrm{evc}}}\right). \tag{18}$$

The respective quantities of the ES of each agent n, i.e., $P_{n,t}^{\mathrm{esc}}$, $P_{n,t}^{\mathrm{esd}}$, $E_{n,t}^{\mathrm{es}}$, $\mathrm{AU}_{n,t}^{\mathrm{es}}$, and $\mathrm{AD}_{n,t}^{\mathrm{es}}$, are derived in a similar fashion with (14)–(18) but neglecting the grid connection parameter $A_{n,t}^{\mathrm{ev}}$ and the traveling energy requirement $E_{n,t}^{\mathrm{tr}}$.

3) Reward: The reward $r_{n,t}$ of agent n at period t is defined as its net cost, which includes the cost/revenue associated with buying/selling energy at the local energy prices and the revenue associated with providing upward and downward ASs

$$r_{n,t} = \lambda_t^{L,b}\left[l_{n,t}\right]^+ + \lambda_t^{L,s}\left[l_{n,t}\right]^- - \left(\lambda_t^{A,u}\mathrm{AU}_{n,t}^{\mathrm{pro}} + \lambda_t^{A,d}\mathrm{AD}_{n,t}^{\mathrm{pro}}\right) \tag{19}$$

$$l_{n,t} = P_{n,t}^{\mathrm{id}} - P_{n,t}^{\mathrm{pv}} + P_{n,t}^{\mathrm{evc}} - P_{n,t}^{\mathrm{evd}} + P_{n,t}^{\mathrm{esc}} - P_{n,t}^{\mathrm{esd}} \tag{20}$$

Table 1 Summary of State-of-the-Art MADRL Approaches

Feature \ Approach	Centralised	Concurrent	CTDE	MAAC
Training	Centralised	Decentralised	Centralised	Centralised
Execution	Centralised	Decentralised	Decentralised	Decentralised
Privacy preserving	No	Yes	No	Yes
Non-stationarity	No	Yes	No	No
Computational complexity	High	High	High	Low

where $l_{n,t}$, $\mathrm{AU}_{n,t}^{\mathrm{pro}} = \mathrm{AU}_{n,t}^{\mathrm{ev}} + \mathrm{AU}_{n,t}^{\mathrm{es}}$, and $\mathrm{AD}_{n,t}^{\mathrm{pro}} = \mathrm{AD}_{n,t}^{\mathrm{ev}} + \mathrm{AD}_{n,t}^{\mathrm{es}}$ represent the net demand, total upward AS provision, and total downward AS provision of prosumer n at period t, respectively; $\lambda_t^{L,b}$ and $\lambda_t^{L,s}$ denote the local energy buy and sell prices of the LEM, which are derived based on the MMR mechanism (see Section IV-C).

E. Multiagent Deep Reinforcement Learning

The existing literature has proposed four different MADRL approaches for driving coordinated learning of multiple prosumer agents, the main features of which are summarized in Table 1.

Centralized learning seeks for a joint model for the actions and observations of all agents and constructs a centralized policy, connecting the joint observation of all agents to joint action. A major limitation of this approach lies in the fact that both training and execution phases are performed in a centralized fashion, leading to an exponential expansion in the observation and action spaces with the number of agents, which quickly becomes intractable in real-world applications. Furthermore, the implementation of this approach may raise prosumers' opposition since they are generally unwilling to disclose their private information and exchange such information with others.

In concurrent learning, each agent learns independently its individual policy, mapping its private observation to its own action. An advantage of this approach is that it enables exploring agents with distinct policies, which may promise benefits in applications where agents take on different roles and feature different reward structures. However, as many agents are learning and adapting their policies independently, the frequent change in these policies yields environmental nonstationarity, which may lead to instability. Furthermore, learning unique policies does not scale to large numbers of agents. Since each agent needs to train its own policy, significant computational and memory burdens arise when the policies are represented by complex models, such as deep NNs. Finally, this approach suffers from low sampling and learning efficiency since no experience is shared between the agents.

Finally, the centralized training and decentralized training (CTDE) framework provides an effective remedy to eliminate environmental nonstationarity. Specifically, a centralized critic network guides the optimization of individual agents' policies during training. The critic takes as input the actions and states from all agents to estimate

the joint *action-value* function (or *Q* value function). Since the critic is learned separately, agents can have arbitrary reward structures, similar to concurrent learning. During test time, the critic is not needed, and policy execution is fully decentralized through each agent's actor network, which only takes as input its own observation. Nevertheless, as in centralized learning, CTDE is not privacy-preserving and suffers from a similar curse of dimensionality in training the central critic, which is problematic in practical large-scale multiagent applications.

In order to overcome the above privacy, nonstationarity, and computational complexity limitations of previous MADRL approaches, this work adopts the multiactor-attention-critic (MAAC) approach, which has been recently proposed by Ye *et al.* [49]. This approach still falls within the CTDE paradigm, effectively eliminating environmental nonstationarity. However, in contrast to centralized learning that incorporates the observations and actions of all agents in training their critics (including physical private information), MAAC enables joint learning of all agents' critics by sharing a set of learnable nonphysical parameters (i.e., critics' weights) among the agents. Furthermore, it employs an attention mechanism that allows selectively "paying attention" to the relevant information of other agents during training; therefore, the input dimension of the critic can be compressed significantly, improving the scalability in large-scale applications.

IV. ADVERSARIAL ATTACK AND DETECTION IN POWER SYSTEM

A. Vulnerabilities in Cyber–Physical Power System

The broad application of ICTs has transformed the traditional power system into a CPS that integrates computing and physical processes to deliver flexible operations and reliable services. At the transmission level, the supervisory control and data acquisition (SCADA) has been broadly used to collect the measurements from substations, and the energy management system (EMS) can analyze the grid operation state, which is crucial to the decision making of the system operators [52]. At the distribution level, the advanced metering infrastructure (AMI) already shows its power on demand response and outage management system (OMS) [53]. Furthermore, the research on data-driven decision-making, such as ML methods, provides more flexibility on grid operation and control. However, this new trend also raises new CPS vulnerabilities that are not seen before [8]–[10].

In the conventional power system, electricity generation, transmission, and distribution are settled by the same company. Therefore, encrypted communication can be easily established and verified. Traditionally, communications between field devices (e.g., RTUs, relays, and transformers) are established via individual copper cable [53]. In contrast, a digital communication channel allows several signals to be simultaneously transmitted. Moreover, the occurrence of DERs hastens the local energy market (LEM) where the prosumers can participate in the electricity auctions [39]. DERs can also participate in power system auxiliary activities, such as voltage regulation by digital controls on the smart inverters [54]. The decentralized and digitalized activities of new stakeholders challenge the existing intranet communication. In the meantime, most of the power system facilities were established before the flourishing digitization age, leaving them vulnerable to cyberattacks. For instance, the intruder can break through the MODBUS and DNP3 that are commonly used in SCADA [55].

B. Data Integrity Attacks

With the development of advanced data-driven techniques, the intruder has become more intelligent and purposive. For example, intelligent intruders are shown to conduct persistent reconnaissance and learn useful grid information, such as the cyberattack on the Ukrainian power grid in December 2015 where the intruders installed the malware several months prior to the attack while hijacking telephone and communication networks to hinder the restoration operation [56].

Referring to different impacts, the attacks can be classified into integrity attacks by injecting or modifying the system data, confidentiality attacks by violating the privacy of various stakeholders, and availability attacks by crashing the grid devices [57]. Due to its high practicability and severe consequences, this article narrows the discussion on integrity attacks from a technical perspective. Specifically, we classify the integrity attacks as attacks targeting the ML algorithms (e.g., adversarial attack), attacks targeting on the state estimation (e.g., false data injection (FDI) attack), and attacks not targeting the state estimation (e.g., market attack).

1) Adversarial Attacks: Despite the great performance of the data-driven algorithms on optimal grid operation and control, their robustness and vulnerability on adversarial perturbation are not fully aware by the community. One prerequisite for any data-driven algorithm is the legit training and testing datasets. Using the voltage assessment problem as an example, it should be assumed that the data that are used to train the model are legit and accurate. In the meantime, the testing data should follow the same (or similar) distribution as the training dataset. However, as the cyber–physical power system is prone to malicious activities, those prerequisites on legit datasets may be violated. For instance, the data source of grid operation algorithms can be corrupted (data poisoning attack), while the trained model can be exposed to or learned by the attackers (exploratory or evasion attack). In the literature, the corruption of ML algorithms is referred to as an adversarial attack [58]. Unlike the adversarial attack targeted to computer science applications, power system activities follow unique physical rules and, therefore, need different treatments.

Specifically, we use the security assessment problem mentioned in Section II as an example. The effectiveness of voltage stability assessment relies on the accurate state estimation, e.g., the voltage magnitude $\mathbf{x}^V$, which is prone to attack. Indeed, the attacker's goal is to change the classification result. To achieve the attack purpose, a perturbation signal on the test set can be constructed

$$\mathbf{c}\text{: } f_a\left(\mathbf{x}+\mathbf{c}, \varepsilon_{\mathrm{NET}}, \varepsilon_{\mathrm{LEM}}\right) \longrightarrow y_a^{adv} = \begin{cases} 1, & y_a = 0 \\ 0, & y_a = 1 \end{cases} \tag{21}$$

where $\mathbf{c}$ is a perturbation signal on the state variable and y_a is the decision made by the contaminated state data. To avoid being easily detected, $\mathbf{c}$ should be designed small enough to bypass the filtering method. In voltage stability assessment, a wrongly classified operation sample can lead to catastrophic failure. On the one hand, a false negative, which represents classifying insecure sample into a secure sample, can lead to erroneous fault detection and isolation. On the other, a false positive, which represents classifying a secure sample as an insecure sample, can cause unnecessary reactions, such as load-shedding [59].

2) False Data Injection Attacks: In this section, we discuss an organized integrity attack on the power system state estimation, which is referred as FDI attack in the literature. For the convenience, the power system is modeled as a graph $\mathcal{G}(\mathcal{N}, \mathcal{E})$ with $|\mathcal{N}| = n+1$ buses and $|\mathcal{E}| = m$ branches in this section. The notation in Section II is changed into the standard state estimation settings and denotes the measurement equation as $\mathbf{z} = \mathbf{h}(\mathbf{x}) + \mathbf{e}$, where $\mathbf{h} \in \mathbb{R}^p$ is the vector of measurement equations consisting of balanced power injections and flows; $\mathbf{x} \in \mathbb{R}^{2n}$ is the system state consisting of voltage magnitude and phase angle at all nonreference buses; and $\mathbf{e} \sim \mathcal{N}(\mathbf{0}, \mathbf{R})$ is the sensor noise vector with covariance matrix $\mathbf{R}$.

Power system state estimation finds the voltage magnitude and phase angle at each bus by solving the following weighted least-squares problem [60]:

$$\hat{\mathbf{x}} = \arg\min_{\mathbf{x}} \left\| \mathbf{R}^{-\frac{1}{2}} \left(\mathbf{z} - \mathbf{h}\left(\mathbf{x}\right)\right) \right\|_2^2 \tag{22}$$

and the residual γ of $\mathbf{z}$ is written as

$$\gamma = \left\| \mathbf{R}^{-\frac{1}{2}} \left(\mathbf{z} - \mathbf{h}\left(\hat{\mathbf{x}}\right)\right) \right\|_2^2 \tag{23}$$

which approximately follows χ^2 distribution with degree of freedom $p-2n$, e.g., $\gamma \sim \chi^2_{p-2n}$. A detection threshold τ_α can then be determined by the system operator according to the confidence level α, which implies that the FPR of χ^2 detector is $\Pr(\gamma \geq \tau_\alpha) = \alpha$.

To avoid being detected, the attacker designs the perturbation signal $\mathbf{c}$ following the physical constraint of the power system. In particular, an FDI attack can be construed as [61]

$$\mathbf{a} = \mathbf{h}\left(\hat{\mathbf{x}} + \mathbf{c}\right) - \mathbf{h}\left(\hat{\mathbf{x}}\right) \tag{24}$$

where $\mathbf{c} \in \mathbb{R}^{2n}$ is the injection vector to the estimated state. Denoting the state and the measurement after attack as $\mathbf{z}_a = \mathbf{z} + \mathbf{a}$ and $\hat{\mathbf{x}}_a = \hat{\mathbf{x}} + \mathbf{c}$, respectively, the residual on attack vector $\mathbf{z}_a$ is unchanged as (23)

$$\begin{aligned} \gamma_a &= \| \mathbf{R}^{-\frac{1}{2}} \left(\mathbf{z}_a - \mathbf{h}\left(\hat{\mathbf{x}}_a\right)\right) \|_2^2 \\ &= \| \mathbf{R}^{-\frac{1}{2}} \left(\mathbf{z} + \mathbf{h}\left(\hat{\mathbf{x}} + \mathbf{c}\right) - \mathbf{h}\left(\hat{\mathbf{x}}\right) - \mathbf{h}\left(\hat{\mathbf{x}} + \mathbf{c}\right)\right) \|_2^2 \\ &= \gamma. \end{aligned} \tag{25}$$

Consequently, the χ^2 BDD cannot raise an alarm on the FDI attack formulated by (24). To successfully hide the attack, the attack shall know the exact system topology and parameters. The assumptions on the attackers' ability are summarized according to various studies.

1) *Assumption One:* To formulate the structured attack (24), the attackers should know grid topology and parameters to form measurement equation $\mathbf{h}(\cdot)$.
2) *Assumption Two:* The attacker can have access to any measurement in $\mathbf{z}$ but can only modify the measurement with a nonzero value. Meanwhile, the strength of the state injection $\mathbf{c}$ should be limited.

As the attack strength $\|\mathbf{c}\|_2^2$ is small, the injection vector can be approximated by the first-order Taylor expansion on (24) [62]

$$\begin{aligned} \mathbf{a} &= \mathbf{h}\left(\hat{\mathbf{x}}\right) + \mathbf{J}\mathbf{c} - \mathbf{h}\left(\hat{\mathbf{x}}\right) \\ &= \mathbf{J}\mathbf{c} \end{aligned} \tag{26}$$

where $\mathbf{J} = [\frac{\partial \mathbf{h}_i}{\partial \mathbf{x}_j}]_{\mathbf{x}=\hat{\mathbf{x}}}$ is the Jacobian matrix of $\mathbf{h}(\mathbf{x})$ with respect to the estimated state vector.

Let $\mathcal{I}_0 = \{i | \mathbf{z}_i = 0, i = 1, 2, \ldots, p\}$ and $\mathcal{I}_a = \{i | \mathbf{c}_i = 0, i = 1, 2, \ldots, 2n\}$ represent the index set of the bus with constant zero power injection and the index set of the target bus under attack. As attacking on the power injections in set $\mathcal{I}_0$ leads an immediate detection, the attack vector can be formulated as the following optimization problem:

$$\begin{aligned} &\min_{\mathbf{c}} \ \frac{1}{2}\|\mathbf{J}\mathbf{c}\|_2^2 \\ &\text{s.t.} \ \underbrace{\left[\mathbf{D}_a^T, \mathbf{J}^T\mathbf{D}_0^T\right]^T}_{\mathbf{A}} \mathbf{c} = \underbrace{\left[\mathbf{c}_a^T, \mathbf{0}^T\right]^T}_{\mathbf{b}} \end{aligned} \tag{27}$$

where $\mathbf{c}_a \in \mathbb{R}^{|\mathcal{I}_a|}$ is the nonzero attack vector; $\mathbf{D}_a \in \mathbb{R}^{|\mathcal{I}_a| \times 2n}$ is the attack incidence matrix with $\mathbf{D}_a(i,j) = 1$ if the ith attack is on state j and 0 otherwise; $\mathbf{0}_a \in \mathbb{R}^{|\mathcal{I}_0|}$ is a zero vector representing the zero-entries of $\mathbf{a}$; and $\mathbf{D}_0 \in \mathbb{R}^{|\mathcal{I}_0| \times p}$ is the zero-measurement incidence matrix with $\mathbf{D}_0(i,j) = 1$ if the ith zero measurement is on measurement j and 0 otherwise. The cost of (27) is to

minimize the attack strength. In the simulation, it is shown that τ can be specifically designed to bypass the BDD while significantly changing the classification result of voltage stability assessment.

The optimization problem (27) is an equality constrained convex quadratic minimization whose optimum $(\mathbf{c}^*, \mathbf{v}^*)$ can be found as the solution of the KKT system [63]

$$\underbrace{\begin{bmatrix} \mathbf{J}^T\mathbf{J} & \mathbf{A}^T \\ \mathbf{A} & \mathbf{0} \end{bmatrix}}_{\mathbf{K}} \begin{bmatrix} \mathbf{c}^* \\ \mathbf{v}^* \end{bmatrix} = \begin{bmatrix} \mathbf{0} \\ \mathbf{b} \end{bmatrix} \tag{28}$$

where $\mathbf{K}$ is called as KKT matrix. If $\mathbf{K}$ is nonsingular, then (28) has unique solution, and (27) has unique primal-dual optimum $(\mathbf{c}^*, \mathbf{v}^*)$.

In the case study, we simulate FDI attacks (27) on voltage magnitude to explicitly show the impact on voltage stability assessment algorithms.

3) Local Market Attacks: Apart from the FDI attacks on the state estimation, attackers tend to intrude the economic system for chasing profit. The promising LEM is vulnerable to cyberattackers due to two reasons. First, the power grids span a wide area, and the growing amount of DERs is geometrically sensitive, which exposes the risk of attacking both the public and private communication links [53]. For instance, the smart PV inverters allow the operators to set different active power limits. To gain the maximum profit, the maximum power point tracking technique is usually adopted. However, as demonstrated by Dafalla *et al.* [64], the set point of PV inverter under IEC-61850 protocol can be compromised by the man-in-the-middle attacks, causing PV curtailment and economic loss. Second, the participant of prosumers in the LEM requires two-way communications [65]. Attack through communication channels can cause individual financial loss, privacy leakage, risk of robbery, and disturbance of normal market operation [66]. As we will show in the case study, by randomly contaminating the price information sent by the unprotected downstream channels, the prosumers' actions are misled, and the market efficiency is reduced.

C. Detection Algorithms of Integrity Attacks

In the literature, the detection algorithms of integrity attacks can be broadly classified into model-based and data-driven methods.

1) Model-Based Detection: Traditional BDD involves solving the static state estimation problem and calculating the deviation between the real time and reconstructed measurements [60]. However, as the static model cannot capture the dynamics of the power system, it is not effective in detecting structured attacks, such as FDI attacks [67]. As a result, dynamic state estimation is applied to capture the temporal correlations in load and generation patterns, and alerts the system operator when this "trend" is violated. Dynamic state estimation based on the Kalman filter (KF) is one of this kind [68].

The model-based detectors fully use the knowledge of the system model and dynamics, which can be easily interpreted and adopted by the system operator. Although the static model is reliable for decision-making, it can be easily targeted by reconnaissance attacks. As already discussed in Section IV-B, grid topology and parameters can be retrieved by deliberate attackers using topology identification algorithms. Once the grid knowledge is learned, the attacker can formulate the attack vector to bypass the model-based detector.

To break the static nature of the model-based approaches, moving target defense (MTD) is proposed to actively detect FDI attacks. With the help of the distributed flexible ac transmission system (D-FACTS) devices, the power system operator can change the branch reactances, which is unknown to the attacker. Therefore, the defender can take advantage of the new system topology to detect the attack. Examples of using the MTD approach to detect FDI attacks include random D-FACTS device placement and perturbation [69], specific D-FACTS device placement by minimizing the attack space [70], and the robust D-FACTS device perturbation by explicitly considering the measurement noise [71]. Recently, hidden MTD is also researched to avoid the grid parameters changes being noticed by the attacker [72].

As the cyberattack is rare in real-time power grid operation, the cost of frequently changes on grid parameters can be hardly accepted by the system operator. Therefore, Lakshminarayana and Yau [73] propose to combine the detection performance of MTD with the OPF problem to simultaneously minimize the generator cost. However, the MTD is still triggered periodically to be synchronized with state estimation; the inevitable cost is still significant when considering the small chance of the grid being attacked by the FDI attacks. How to balance the detection performance and extra operational cost remains an open question.

2) Data-Driven Detection: As the improvement of the number and resolution of the grid measurements, the data-driven method is armed to model the complex grid dynamics and uncertainties. Broadly speaking, learning algorithms for detecting attacks can be classified into supervised learning and unsupervised learning. In the supervised setting, the detection is directly achieved by learning a mapping from the input (feature) space $x_i \in \mathcal{X}$ to the binary classification $y_i \in \mathcal{Y} = \{0, 1\}$, e.g., f_θ: $\mathcal{X} \longrightarrow \mathcal{Y}$. The model fit on the training dataset can be directly used to classify the legitimacy of the test set. The support vector machine (SVM) [74], the naive Bayesian classifier (NBC) [75], and DTs [76] generally belong to this category.

To enrich a balanced dataset for supervised learning, attack samples are synthetically generated in the literature [77]. However, the synthetic attack data may not be representative of the actual attack attempts,

leveraging the detection performance of the supervised classifier. To overcome the problem, unsupervised and semisupervised methods are considered to detect FDI attacks by learning the latent representation of the legit measurements. Let $\mathcal{X}$ be the input (feature) space and $\mathcal{Z}$ be the latent space. The unsupervised learning can be represented by f_θ: $\mathcal{X} \longrightarrow \mathcal{Z}$ where the latent representation can be used for clustering or dimension reduction. Unlike the supervised detector, an implicit classifier should be built on the latent space $\mathcal{Z}$ to detect the attack. The unsupervised/semisupervised learning approach includes isolation forest [78], semisupervised SVM [79], autoencoder [80], and the prediction-based algorithm, where a predictor is built on normal data, and the attack is detected by violating the distribution of the prediction errors [81]. Despite the high detection rate of unsupervised detectors, they suffer from high FPR on a legit measurement under the test set and roundabout training target during the training. For example, in [82], up to 20% FPR is committed to achieve 90% TPR.

D. Data-Triggered Moving Target Defense

Due to the rarity of attacks, the system operator may be not willing to adopt costly detection mechanisms to overcome the attacks. To overcome the high FPR of unsupervised learning detectors, a novel attack verification algorithm using MTD is proposed. As FPR under each D-FACTS set point is unchanged and controllable, the decision made by the MTD can be willingly accepted by the system operator.

To show the advances of the proposed two-stage method, an autoencoder FDI attack detector is applied as the trigger to the MTD. Let $\mathcal{Z} = \{\mathbf{z}_1, \mathbf{z}_2, \ldots, \mathbf{z}_N\}$ be the training dataset composed of legit measurements from the power grid. The autoencoder learns a map f_θ: $\mathcal{Z} \longrightarrow \mathcal{X} \longrightarrow \mathcal{Z}$, where $\mathcal{X}$ represents the implicitly learned latent feature. Note that the meanings of $\mathcal{Z}$ and $\mathcal{X}$ are exchanged to conform to the power system convention. Due to the nonlinear activation functions and bottleneck model structure, the hidden representation of legit measurements is embedded by the encoder $\mathcal{Z} \longrightarrow \mathcal{X}$ and decoder $\mathcal{X} \longrightarrow \mathcal{Z}$ pairs using the following mean squared empirical loss:

$$\mathcal{L}_\theta\left(\mathcal{Z}_i\right) = \frac{1}{|\mathcal{Z}_i|}\sum_{j=1}^{|\mathcal{Z}_i|}\left\|\mathbf{z}_j - f_\theta\left(\mathbf{z}_j\right)\right\|_2^2 \tag{29}$$

where $\mathcal{Z}_i$ represents the ith training batch. Once the autoencoder is trained as f_θ^*, a threshold can be determined by ranking the reconstruction errors of the validation set. Let α_{AE} be the confidence level (FPR) on the validation data; the threshold $\tau_{\mathrm{AE}}(\alpha_{\mathrm{AE}})$ can be found as the reconstruction error at the upper α-quantile. Therefore, the autoencoder-based detector can be summarized as

$$D\left(\mathcal{Z}_i\right) = \begin{cases} 1, & \text{if } \mathcal{L}\left(\mathcal{Z}_i\right) \geq \tau_{\mathrm{AE}} \\ 0, & \text{otherwise.} \end{cases} \tag{30}$$

After the AE-detector raises an alarm, an MTD can be implemented by randomly changing the set points of D-FACTS devices or other more advanced implementation of MTD [71]. As the branch reactances are changed, a new measurement equation is set up

$$\mathbf{h}_B\left(\cdot\right) \xrightarrow{\text{MTD}} \mathbf{h}_{B'}\left(\cdot\right) \tag{31}$$

where subscript B represents the dependence of measurement equations on the susceptance matrix and B' represents the susceptance matrix after the MTD.

Let $\hat{\mathbf{x}}_a'$ be the estimated state based on the post-MTD measurement equation under attack

$$\hat{\mathbf{x}}_a' = \arg\min_{\mathbf{x}}\left\|\mathbf{R}^{-\frac{1}{2}}\left(\mathbf{z}_a' - \mathbf{h}_{B'}\left(\mathbf{x}\right)\right)\right\|_2^2 \tag{32}$$

by Gauss–Newton iterations. $\mathbf{z}_a'$, which represents the attacked measurement after MTD, can be written as

$$\mathbf{z}_a' = \mathbf{h}_{B'}\left(\mathbf{x}'\right) + \mathbf{e} + \mathbf{h}_B\left(\hat{\mathbf{x}}' + \mathbf{c}\right) - \mathbf{h}_B\left(\hat{\mathbf{x}}'\right) \tag{33}$$

with $\hat{\mathbf{x}}'$ solved by the attacker based on the pre-MTD model.

First, as the system parameter changes, the weighted least square (32) cannot converge to the desired contaminated state $\hat{\mathbf{x}}' + \mathbf{c}$ by the attacker. Second, the residual on the measurement under attack after MTD becomes

$$\begin{aligned}\gamma_a' &= \left\|\mathbf{R}^{-\frac{1}{2}}\left(\mathbf{z}_a' - \mathbf{h}_{B'}\left(\hat{\mathbf{x}}_a'\right)\right)\right\|_2^2 \\ &= \left\|\mathbf{R}^{-\frac{1}{2}}\left(\mathbf{z}' + \mathbf{h}_B\left(\hat{\mathbf{x}}' + \mathbf{c}\right) - \mathbf{h}_B\left(\hat{\mathbf{x}}'\right) - \mathbf{h}_{B'}\left(\hat{\mathbf{x}}_a'\right)\right)\right\|_2^2\end{aligned} \tag{34}$$

which no longer equals to γ any more. Consequently, the MTD can be used to reject the false alarm made by the data-driven detector without significantly influencing the detection rate.

The proposed two-stage algorithm on FDI attacks targeting the voltage stability assessment will be applied in the simulation.

E. Prediction-Based Attack Detection

In this section, a prediction-based detection algorithm to detect the attack on the retail electricity prices in LEM is proposed.

At each time step t, a sequence of past $T \geq 2$ prices $\mathcal{X}_t = \{\mathbf{x}_{t-T}, \mathbf{x}_{t-T+1}, \ldots, \mathbf{x}_{t-1}\}$ can be constructed to predict the current price $\mathbf{x}_t$. Specifically, two market prices, the energy import and export, are considered. In practice, these two prices are determined by the retailer and sent to each household through communications, such as smart meters, which are vulnerable to attack. In the meantime, we also feed in the time stamp represented periodically by

the coordinate on the unit cycle for each element in the sequence. It gives that $\mathbf{x}_i \in \mathbb{R}^4$, and $\mathbf{y}_i \in \mathbb{R}^2$ represents the target price vector. To learn the temporal correlations in $\mathcal{X}_t$s, a fold of long short-term memory (LSTM) [83] cells is applied to construct the NN followed by a feedforward layer. Indeed, we train the LSTM network by minimizing the following empirical loss:

$$\mathcal{L}_\theta = \frac{1}{N-T}\sum_{t=T}^{N-1}\left\|\mathbf{y}_{t+1} - f_\theta\left(\mathcal{X}_t\right)\right\|_2^2 \tag{35}$$

where N is the number of data in the training set. After the model is trained, a confidence interval can be determined by ranking the prediction errors, and any prediction that is outside this interval is marked as attack.

V. CASE STUDY

This case study focuses on the application of centralized data analytics to the security of decentralized systems with LEMs considering both physical disturbances and cyberattacks. After stating the test system and the key assumptions, the first study is on the physical, dynamic security; the second study is on the detection of cyberattacks; and the third study is on the economic value of decentralized systems with LEMs. Within each case study, cyberattacks were simulated according to settings in Section IV.

A. Test System and Assumptions

A modified version of the IEEE nine-bus system from [84] was considered in this case study. The modification included integrated DERs, EV fleets acted as ES capacity of 20 MWh at each generator bus, and 25% of fossil fuel generation replaced by wind power. 1000 load scenarios were sampled from a Latin hypercube with uniform distribution around $\pm 50\%$ of the nominal value for the active power and $\pm 20\%$ for the reactive power. The relaxed SDP ACOPF was then solved to get the cost-optimal OCs corresponding to the sampled loads [85]. A short circuit at bus 8 at time 0.1 s was considered as a fault to assess the system's security. The fault was then cleared at 0.25 s by opening the line between buses 8 and 9. The total simulation time was $T = 10$ s. The OCs were assessed as dynamic secure if the integral square generator angle (ISGA) index was ≤ 0.47, otherwise insecure [86]. The resulting training database considered the cost-optimal OCs and their corresponding security labels.

To simulate the integrity attacks on voltage assessment, FDI attacks were generated from (27) by solving (28). First, the system state (bus voltage magnitude and phase angle) was calculated through the Gauss–Newton method [60]. Then, randomly one to five buses were picked out of the eight available buses, and their voltage magnitude was changed by -1.5%. After determining the voltage perturbation, the corresponding attack vector $\mathbf{a}$ was calculated by (26) and injected into the legit measurement. Finally, the "contaminated" measurement (load and generation) was fed into the trained security classifier.

To simulate the ML-based security assessment, the classifier evaluated security on a false (attacked, contaminated) prefault OC, which was different to the real OC. As neither the operator nor the classifier identifies the attack, inaccurate security labels and control actions may be the result, which is what this case study further investigates. For all the generated attacks, 1000 attack vectors were sampled with the largest element smaller than 0.05. To study the dynamic system's security, four different control approaches were compared: i) no control approach; ii) centralized corrective control approach; iii) centralized corrective control approach under a cyberattack; and iv) decentralized corrective control approach under a cyberattack. In ii)–iv), the corrective control approach described in [37] was applied only once the fault was cleared. For this, a DT classifier was trained "offline" using the generated training database. The classifier predicted security and accordingly selected the corrective control action.

Finally, an open-source, large-scale dataset produced by the Australian distribution company Ausgrid [87] was used to simulate a realistic setting of the LEM, including demand and PV generation data for 300 real residential prosumers, over a yearly horizon with a half-hourly resolution. To factor the prosumers' natural heterogeneity in terms of their flexible DERs, 300 prosumers were divided into four different classes: 1) 75 prosumers without flexible DERs (EV or ES); 2) 75 prosumers with an EV with smart charging and discharging flexibility; 3) 75 prosumers with an ES unit; and 4) 75 prosumers with both a flexible EV and an ES unit. Furthermore, the values of the operating parameters of these flexible DERs were diversified among the different prosumers of each class, within realistic value ranges derived from [88]; for EV, in particular, two trips per day and a home-charging scenario (implying that the EV were connected to the grid before the first and after the second trip) were assumed. As discussed in Section IV-E, the recently proposed MAAC approach was adopted for training the prosumer agents, which has been implemented in Python with PyTorch [89]. One day from each of the 53 weeks of the original dataset was randomly selected for the testing dataset, which was used for performance evaluations, while the remaining days were included in the training dataset.

B. Security of Decentralized CPS Operation

This study investigated the system's security in a decentralized CPS operation with LEMs. The benefits of LEMs in terms of system's security were first investigated in ii) where the provision of AS from LEMs made centralized corrective control tools available. However, in the simulated real-time operation, such corrective control approaches can be attacked: attacks in iii) may attack centrally with a large and high-magnitude attack. Conversely, in the decentralized approach iv), a low-magnitude

Table 2 Security of Four Control Approaches With 25% Renewable Integration

	Approaches			
	No control	Centralised corrective	Attacked centralised corrective	Attacked decentralised corrective
Insecure OCs	928/1000	95/1000	204/1000	148/1000

attack across all decentralized buses was assumed as the additional information from LEMs allows to better contain and restrict the attack. In all i)–iv), then the classifier assessed the system's security of the (attacked) prefault OCs in "real time." When the (attacked) OC was predicted as insecure, in response, the corrective control was triggered. This corrective control action was then applied to (and tested on) the real OC. The results in Table 2 for all studied OCs showed that: 1) centralized corrective control ii) reduced the number of insecure OCs by 90% compared to i); 2) attacks in iii) and iv) resulted in increases of insecure OCs compared to ii); and 3) attacked centralized control resulted in an increase of insecure OCs by 38% compared to the attacked decentralized control. This led to the conclusion that cyberattacks generally have impacts on system's security. In particular, in a centralized operating approach, such attacks had a much higher impact than in a decentralized approach as no additional information from LEMs was available. Therefore, decentralized CPS operating approaches can enhance the system's security, while a more robust attack detection is needed in centralized operating paradigms with high-impact attacks. All the corrective control approaches ii)–iv) significantly improved the system's security compared with approach i) where no control was applied. This highlighted the need for corrective control in future power systems with a high share of renewables and DERs and the key role of LEMs in providing such services.

C. Performance of Layered Detection Framework

This study investigated the detection of the FDI attacks (see Section IV-B) by applying the data-driven MTD algorithm proposed in Section IV-D. 4000 new load scenarios were augmented on the original 1000 load scenarios using the Dirichlet distribution [90]. Second, the ACOPF was solved, and the measurements of each scenario were recorded. The standard deviation of the Gaussian measurement noise was set as 0.01 p.u., and the FPR of BDD was set at 0.01. It was assumed that the attack is on the voltage magnitude, and the legit measurement $\mathbf{z} = [\mathbf{Q}_I^T, \mathbf{Q}_F^T, \mathbf{V}^T]^T \in \mathbb{R}^{27}$ is fed into the autoencoder NN, where $\mathbf{Q}_I$, $\mathbf{Q}_F$, and $\mathbf{V}$ are the vector of reactive power injection, reactive power flow, and voltage magnitude, respectively. Min–max normalization was used on $\mathbf{z}$, and 250 out of 5000 samples were used as validation. Upon the trained autoencoder network, the detection threshold was determined by finding the 5% upper quantile of the reconstruction error on the validation set.

Once the autoencoder detector raised an alarm, the MTD was triggered where the branch susceptance was randomly altered by ±(10%–40%) of the nominal value to verify the positive decision made by the autoencoder. A new residual based on the new system parameters was calculated by (34). The simulation results were summarized in Table 3 where AE represented the detection result of an autoencoder and the AE-MTD represented the detection result of χ^2 detector after the event-triggered MTD. First, recall that the detection threshold of AE was set at upper 5.0% quantile, and the higher FPR 7.1% implied that the trained model was overfitted. Once the MTD was triggered by the positive alarms, a new hypothesis test can be made by the χ^2 detector with around 1% FPR by sacrificing 1% TPR.

To sum up, the data verification on the voltage security assessment can be fulfilled by the event-triggered MTD where the physics information is added to reduce the false positive rate.

D. Economic Value of Proposed LEM

This study investigated the economic value of LEM. Four different scenarios regarding the involved prosumers' coordination were implemented and compared. In all these scenarios, following the discussion in Section IV-A, it was assumed that the import energy tariff followed the wholesale energy prices (in particular, the U.K. wholesale prices, which were derived from [91]), while the export energy tariff was assumed to be 50% of the import tariff at each half-hourly period.

1) *STATUS-QUO:* Following the conventional paradigm, no LEM was established, and each of the 300 prosumers traded energy independently with the contracted retailer.
2) *LEM-EN:* An LEM was established, and it only enabled local energy trading among the 300 prosumers (but not AS provision to external system operators).
3) *LEM-BSF:* An LEM was established, enabling both local energy trading and AS provision. Specifically, the focus was on BSs (due to their significance for emerging electricity systems; see Section IV-A) and particularly on the upward direction (as downward balancing is generally less critical due to the ability to curtail renewable generation). In this scenario, the ESO was assumed to procure such BS with a "flat" price throughout the examined horizon, equal to 5.67 £/MW/h, reflecting the current pricing regime in most balancing markets (see Section IV-A).
4) *LEM-BSV:* This scenario was similar to the previous one, with the difference that the pricing regime for

Table 3 Detection Performance of the Proposed Algorithm

	AE	AE-MTD
TPR	0.989	0.975
FPR	0.071	0.012

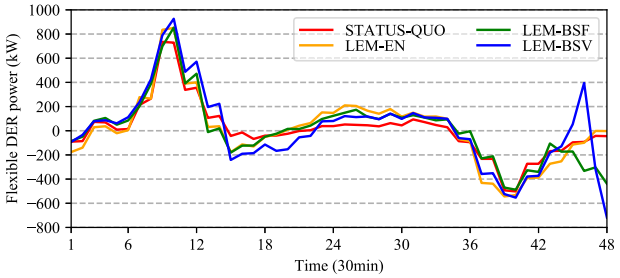

Fig. 4. *Aggregate energy dispatch of flexible DER (EV and ES) of 300 prosumers under the examined scenarios (averaged over the 53 test days).*

BS was variable, better reflecting their time-specific value (see Section IV-A). Specifically, this price was assumed to equal to 17 £/MW/h for the off-peak hours 23:00–7:00 (considering that the combination of lower demand and higher wind generation during these hours reduced system inertia and increased the balancing requirements of the system) and equal to 0 for the remaining hours of the day (for comparison consistency reasons, the average BS price throughout the day is the same in scenarios LEM-BSF and LEM-BSV).

For each of these four scenarios, Fig. 4 presented the aggregate energy dispatch of the flexible DER (EV and ES) of the 300 prosumers (with positive values indicating charging and negative values indicating discharging), while Fig. 5 presented the net energy demand (positive for importing energy from the retailer and negative for exporting energy to the retailer) of the 300 prosumers (including for comparison purposes the inflexible net demand, given by the difference between inflexible demand and PV generation). Fig. 6 presented the aggregate amount of upward BS provided by the flexible DER of the prosumers in scenarios LEM-BSF and LEM-BSV (which is zero by definition for the first two scenarios). Finally, Table 4 summarized the daily net cost of the 300 prosumers under each of the examined scenarios, including its components (import energy cost, export energy revenue, and BS revenue).

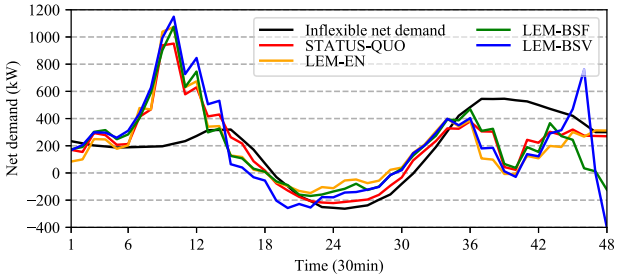

Fig. 5. *Net demand of 300 prosumers under the examined scenarios (averaged over the 53 test days).*

Table 4 Daily Net Cost of 300 Prosumers and Its Components Under the Examined Scenarios (Averaged Over the 53 Test Days)

Scenario	Import energy cost (£)	Export energy revenue (£)	BS revenue (£)	Net cost (£)
STATUS-QUO	216.26	41.85	-	174.41
LEM-EN	155.96	12.96	-	143.00
LEM-BSF	168.89	16.80	150.46	1.63
LEM-BSV	182.58	27.62	228.02	-73.06

Figs. 4 and 5 demonstrated that the four examined scenarios involved some similarities in terms of the energy dispatch of the flexible DER. First, these flexible DER were charging during midday periods (see Fig. 4) in order to locally consume as much of the excess PV generation as possible (i.e., the self-consumption effect discussed in Section IV-A) and, thus, reduce the excess generation sold to the retailer (see Fig. 5). Furthermore, flexible DERs were charging during the off-peak morning periods that are characterized by a lower import energy tariff (see Fig. 4). Finally, flexible DERs were discharging during the peak evening periods that are characterized by a high import energy tariff (see Fig. 4).

Nevertheless, the four scenarios involved important differences that were driven by the effects of local energy trading and BS provision. When comparing the STATUS-QUO against the LEM-EN scenario, both the extent of PV self-consumption during midday periods and the extent of net demand reduction during evening periods were enhanced in the LEM-EN scenario, rendering a flatter net demand profile compared to the STATUS-QUO scenario. As discussed in Section IV-A, this trend was driven by the fact that local energy trading allowed more comprehensive self-balancing for the 300 prosumers as a whole, considering the natural diversity of these prosumers. As a consequence, both the import energy cost and the export energy revenue were lower in the LEM-EN scenario compared to the STATUS-QUO scenario, implying that the extent of trading with the contracted retailer was reduced. Going further, the reduction of the import energy cost was more significant than the reduction of the export energy revenue (as the import tariffs were higher than the export tariffs), overall resulting in a reduced net cost (see Table 4).

Moving to the LEM-BSF scenario, the extent of PV self-consumption during midday periods and the extent of net demand reduction during evening periods were still higher compared to the STATUS-QUO scenario but lower compared to the LEM-EN scenario. This trend emerged as part of the available flexibility of EV and ES was preserved for the provision of BS to the external ESO, limiting the flexibility dedicated to local self-balancing. In other words, in this more advanced LEM design, the LEM aimed at optimizing the tradeoff between local energy balancing and provision of flexibility to the wider electricity system. As a consequence, both the import energy cost and the export energy revenue were higher in the LEM-BSF scenario compared to the LEM-EN scenario with the former's

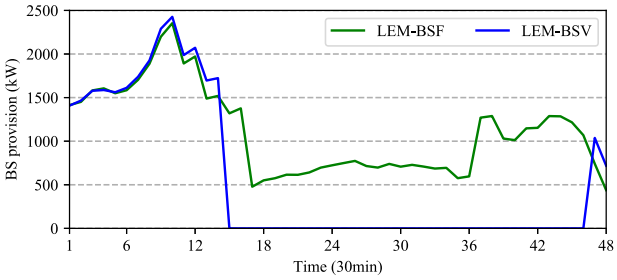

Fig. 6. *Aggregate upward BS provision of flexible DER (EV and ES) of 300 prosumers under the examined scenarios (averaged over the 53 test days).*

increase dominating (as the import tariffs are higher than the export tariffs). However, the additional BS provision revenue generated in the LEM-BSF was much higher than this import energy cost increase, overall resulting in a very low net cost (see Table 4).

Finally, when comparing the LEM-BSF against the LEM-BSV scenario, the former exhibited a higher extent of EV and ES charging during midday periods and a lower extent of EV and ES discharging during evening periods, in order to increase their upward BS provisions, driven by the fact that these periods exhibited a higher BS price in the LEM-BSF scenario (5.67 £/MW/h) compared to the LEM-BSV scenario (0). On the other hand, the LEM-BSV scenario exhibited a higher extent of EV and ES charging during morning periods, in order to increase their upward BS provisions, driven by the fact that these periods exhibited a higher BS price in the LEM-BSV scenario (17 £/MW/h) compared to the LEM-BSF scenario (5.67 £/MW/h). Interestingly enough, although the total amount of provided BS was significantly higher in the LEM-BSF scenario (since the respective amount in the LEM-BSV scenario was zero during midday and evening periods due to the 0 BS price; see Fig. 6) and the average BS price was the same in the two scenarios, the overall BS revenue was significantly higher in the LEM-BSV scenario, overall resulting in a lower net cost (which is actually negative; see Table 4). This effect was driven by the fact that the amount of provided BS in the LEM-BSF scenario during midday and evening periods was not as high as the one during morning periods since: 1) the majority of EV was not connected to the grid (and, thus, cannot provide BS) during midday periods (due to the home-charging assumption) and 2) EV and ES were discharging during evening periods (in order to avoid a high import energy tariff), implying that the amount of upward BS that they can provide was lower. Overall, this result implied that variable pricing of BS does not only reflect the balancing requirements of the system more accurately (see Section IV-A), but it is also more profitable for flexible prosumers.

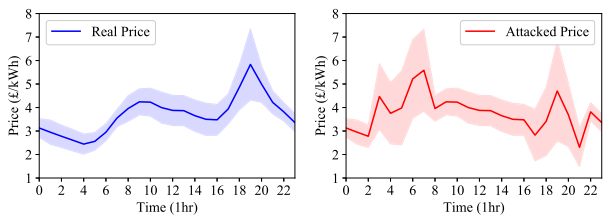

Fig. 7. *Mean and standard deviation of daily retail import prices for real market and under attack (over the 53 test days).*

Table 5 Daily Net Cost of 300 Prosumers for Real Market Prices and Attacked Prices Under LEM-BSV Scenario (Aggregated Over the 53 Test Days)

Retail import price signals	Net cost (£)
Real market	-73.06
Under attack	-54.21

To further investigate the impact of cyberattacks on LEMs, we performed the following steps based on the previous setting.

1) Random noises to the original retail import price signals for two typical periods (morning from 4:00 to 8:00 and night from 18:00 to 22:00) were added. These noises can be assumed as the attacked retail import price signals observed by prosumers in the LEM.
2) Prosumers observing these attacked retail import price made energy and AS provision decisions based on their learned control policies from the MARL method.
3) In the real market, the prosumers' net costs were calculated by the product of their made energy and AS provision decisions (under the attacked prices) and the real market retail import prices. The net costs calculated above were assumed as the attacked costs.
4) The difference between the real costs (making decisions and calculating costs are both based on real prices) and the attacked costs (making decisions based on attacked prices and calculating costs based on real prices) was finally compared.

Fig. 7 illustrates the daily retail import prices (mean $\pm$ std) over the 53 test days before (blue) and after (red) cyberattacks. Table 5 compares the aggregated daily net cost over the 53 test days of 300 prosumers for these two scenarios. It can be observed from Table 5 that the net cost of 300 prosumers under attacked prices was much lower than the cost under real market prices, showing the impacts of cyberattacks on LEMs. The prediction-based detector described in Section IV-E was adopted with sequence length $T = 6$ to detect such attacks at each household. By setting a 5.0% FPR, the detection rate on the above attacks was reported as 95.16%. Subsequently, mitigation actions can be made to correct the agent actions in the following step.

VI. CONCLUSION

Digitalization can enhance the reliability and cost-efficiency of power systems operation. This work discusses

how centralized data analytics allow to fully benefit from the advantages of LEMs in terms of system's security and energy costs' reduction. The digitalized, decentralized paradigm for secure CPS operation with LEMs not only benefits local prosumers but also enhances the security of supply. The key contribution of this work is to holistically analyze the impact of ML on security corrective-control, cyberattack detection, and the economic value of LEMs. Case studies have demonstrated that considering novel ML-based LEM paradigms in the system operation can reduce the impact of physical and cyberattacks by 38% and improve the detection of varying attack strengths. At the same time, such data-driven LEM models not only can substantially enhance self-consumption effects and reduce the energy costs of flexible prosumers but also generate significant revenues from the provision of ASs to wider system operators. This article recommends considering novel LEM paradigms in the system operation, which can still be secure through advanced ML approaches for the detection of cyberattacks and security assessments. Then, as this article demonstrated, a significant step forward could be made toward reducing energy costs of prosumers and simultaneously enhancing the system's security.

Acknowledgment

This work is supported by the Engineering and Physical Sciences Research Council (UK) under the Integrated Development of Low-Carbon Energy Systems programme (EP/R045518/1), and by the TU Delft AI Labs Programme, NL, The Netherlands. ■

REFERENCES

[1] M. L. Di Silvestre, S. Favuzza, E. Riva Sanseverino, and G. Zizzo, "How decarbonization, digitalization and decentralization are changing key power infrastructures," *Renew. Sustain. Energy Rev.*, vol. 93, pp. 483–498, Oct. 2018.

[2] J. Fang, H. Li, Y. Tang, and F. Blaabjerg, "On the inertia of future more-electronics power systems," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 7, no. 4, pp. 2130–2146, Dec. 2019.

[3] F. Milano, F. Dorfler, G. Hug, D. J. Hill, and G. Verbic, "Foundations and challenges of low-inertia systems (invited paper)," in *Proc. Power Syst. Comput. Conf. (PSCC)*, Jun. 2018, pp. 1–25.

[4] Y. Pipelzadeh, R. Moreno, B. Chaudhuri, G. Strbac, and T. C. Green, "Corrective control with transient assistive measures: Value assessment for Great Britain transmission system," *IEEE Trans. Power Syst.*, vol. 32, no. 2, pp. 1638–1650, Mar. 2017.

[5] R. Moreno, D. Pudjianto, and G. Strbac, "Transmission network investment with probabilistic security and corrective control," *IEEE Trans. Power Syst.*, vol. 28, no. 4, pp. 3935–3944, Nov. 2013.

[6] A. Rhodes, "Digitalisation of energy: An energy futures lab briefing paper," Imperial College London, London, U.K., Tech. Rep., 2020.

[7] I. Konstantelos *et al.*, "Implementation of a massively parallel dynamic security assessment platform for large-scale grids," *IEEE Trans. Smart Grid*, vol. 8, no. 3, pp. 1417–1426, May 2017.

[8] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[9] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836–1846, Nov. 2008.

[10] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 998–1010, 4th Quart., 2012.

[11] P. Panciatici, G. Bareux, and L. Wehenkel, "Operating in the fog: Security management under uncertainty," *IEEE Power Energy Mag.*, vol. 10, no. 5, pp. 40–49, Sep. 2012.

[12] B. Kroposki *et al.*, "Achieving a 100% renewable grid: Operating electric power systems with extremely high levels of variable renewable energy," *IEEE Power Energy Mag.*, vol. 15, no. 2, pp. 61–73, Mar. 2017.

[13] F. R. Segundo Seville *et al.*, "State-of-the-art of data collection, analytics, and future needs of transmission utilities worldwide to account for the continuous growth of sensing data," *Int. J. Electr. Power Energy Syst.*, vol. 137, May 2022, Art. no. 107772. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0142061521009947

[14] P. Kundur, "Definition and classification of power system stability IEEE/CIGRE joint task force on stability terms and definitions," *IEEE Trans. Power Syst.*, vol. 19, no. 3, pp. 1387–1401, May 2004.

[15] N. Guha, Z. Wang, M. Wytock, and A. Majumdar, "Machine learning for AC optimal power flow," 2019, *arXiv:1910.08842*.

[16] J. L. Cremer and G. Strbac, "A machine-learning based probabilistic perspective on dynamic security assessment," *Int. J. Electr. Power Energy Syst.*, vol. 128, Jun. 2021, Art. no. 106571.

[17] J. Stańczak and W. Radziszewska, "Modeling of dynamic market of energy with local energy clusters," *Control Cybern.*, vol. 47, no. 2, pp. 157–172, 2018.

[18] I. Konstantelos, M. Sun, S. H. Tindemans, S. Issad, P. Panciatici, and G. Strbac, "Using vine copulas to generate representative system states for machine learning," *IEEE Trans. Power Syst.*, vol. 34, no. 1, pp. 225–235, Jan. 2019.

[19] M. Sajjadi, M. Seyedhosseini, and T. Tasdizen, "Disjunctive normal networks," *Neurocomputing*, vol. 218, pp. 276–285, Dec. 2016.

[20] L. Duchesne, E. Karangelos, and L. Wehenkel, "Recent developments in machine learning for energy systems reliability management," *Proc. IEEE*, vol. 108, no. 9, pp. 1656–1676, Sep. 2020.

[21] M. Seyedhosseini and T. Tasdizen, "Disjunctive normal random forests," *Pattern Recognit.*, vol. 48, no. 3, pp. 976–983, Mar. 2015.

[22] Z. Wan, Z. Yu, L. Shu, Y. Zhao, H. Zhang, and K. Xu, "Intelligent optical performance monitor using multi-task learning based artificial neural network," *Opt. Exp.*, vol. 27, no. 8, pp. 11281–11291, 2019.

[23] J. L. Cremer, I. Konstantelos, and G. Strbac, "From optimization-based machine learning to interpretable security rules for operation," *IEEE Trans. Power Syst.*, vol. 34, no. 5, pp. 3826–3836, Sep. 2019.

[24] F. Bellizio, J. L. Cremer, M. Sun, and G. Strbac, "A causality based feature selection approach for data-driven dynamic security assessment," *Electr. Power Syst. Res.*, vol. 201, Dec. 2021, Art. no. 107537.

[25] Y. Xu, Z. Y. Dong, J. H. Zhao, P. Zhang, and K. P. Wong, "A reliable intelligent system for real-time dynamic security assessment of power systems," *IEEE Trans. Power Syst.*, vol. 27, no. 3, pp. 1253–1263, Aug. 2012.

[26] K. Sun, S. Likhate, V. Vittal, V. S. Kolluri, and S. Mandal, "An online dynamic security assessment scheme using phasor measurements and decision trees," *IEEE Trans. Power Syst.*, vol. 22, no. 4, pp. 1935–1943, Nov. 2007.

[27] M. He, J. Zhang, and V. Vittal, "A data mining framework for online dynamic security assessment: Decision trees, boosting, and complexity analysis," in *Proc. IEEE PES Innov. Smart Grid Technol. (ISGT)*, Jan. 2012, pp. 1–8.

[28] G. E. Karniadakis, I. G. Kevrekidis, L. Lu, P. Perdikaris, S. Wang, and L. Yang, "Physics-informed machine learning," *Nature Rev. Phys.*, vol. 3, no. 6, pp. 422–440, 2021.

[29] G. S. Misyris, A. Venzke, and S. Chatzivasileiadis, "Physics-informed neural networks for power systems," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Aug. 2020, pp. 1–5.

[30] F. Bellizio, J. L. Cremer, and G. Strbac, "Machine-learned security assessment for changing system topologies," *Int. J. Electr. Power Energy Syst.*, vol. 134, Jan. 2022, Art. no. 107380.

[31] K. A. Loparo and F. Abdel-Malek, "A probabilistic approach to dynamic power system security," *IEEE Trans. Circuits Syst.*, vol. 37, no. 6, pp. 787–798, Jun. 1990.

[32] J. Stiasny, G. S. Misyris, and S. Chatzivasileiadis, "Physics-informed neural networks for non-linear system identification for power system dynamics," in *Proc. IEEE Madrid PowerTech*, Jun. 2021, pp. 1–6.

[33] A. Michel, A. Fouad, and V. Vittal, "Power system transient stability using individual machine energy functions," *IEEE Trans. Circuits Syst.*, vol. CAS-30, no. 5, pp. 266–276, May 1983.

[34] S. Hafstein and P. Giesl, "Review on computational methods for Lyapunov functions," *Discrete Continuous Dyn. Syst. Ser. B*, vol. 20, no. 8, pp. 2291–2331, Aug. 2015.

[35] T. Zhao, J. Wang, X. Lu, and Y. Du, "Neural Lyapunov control for power system transient stability: A deep learning-based approach," *IEEE Trans. Power Syst.*, vol. 37, no. 2, pp. 955–966, Mar. 2022.

[36] J. L. Cremer, I. Konstantelos, S. H. Tindemans, and G. Strbac, "Data-driven power system operation: Exploring the balance between cost and risk," *IEEE Trans. Power Syst.*, vol. 34, no. 1, pp. 791–801, Jan. 2019.

[37] I. Genc, R. Diao, V. Vittal, S. Kolluri, and S. Mandal, "Decision tree-based preventive and corrective control applications for dynamic security enhancement in power systems," *IEEE Trans. Power Syst.*, vol. 25, no. 3, pp. 1611–1619, Aug. 2010.

[38] G. Strbac *et al.*, "Decarbonization of electricity systems in Europe: Market design challenges," *IEEE Power Energy Mag.*, vol. 19, no. 1, pp. 53–63, Jan. 2021.

[39] D. Qiu, Y. Ye, and D. Papadaskalopoulos, "Exploring the effects of local energy markets on electricity retailers and customers," *Electr. Power Syst. Res.*, vol. 189, Dec. 2020, Art. no. 106761.

[40] T. Pinto, Z. Vale, and S. Widergren, *Local Electricity Markets*. Amsterdam, The Netherlands: Elsevier, 2021.

[41] M. S. H. Nizami, M. J. Hossain, and E. Fernandez, "Multiagent-based transactive energy management systems for residential buildings with distributed energy resources," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 1836–1847, Mar. 2020.

[42] J. Li, Y. Ye, D. Papadaskalopoulos, and G. Strbac, "Computationally efficient pricing and benefit distribution mechanisms for incentivizing stable

peer-to-peer energy trading," *IEEE Internet Things J.*, vol. 8, no. 2, pp. 734–749, Jan. 2021.
[43] A. Vicente-Pastor, J. Nieto-Martin, D. W. Bunn, and A. Laur, "Evaluation of flexibility markets for retailer–DSO–TSO coordination," *IEEE Trans. Power Syst.*, vol. 34, no. 3, pp. 2003–2012, May 2019.
[44] H. Khajeh, H. Firoozi, M. R. Hesamzadeh, H. Laaksonen, and M. Shafie-Khah, "A local capacity market providing local and system-wide flexibility services," *IEEE Access*, vol. 9, pp. 52336–52351, 2021.
[45] S. Cui, Y.-W. Wang, Y. Shi, and J.-W. Xiao, "A new and fair peer-to-peer energy sharing framework for energy buildings," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 3817–3826, Sep. 2020.
[46] D. H. Nguyen, "Optimal solution analysis and decentralized mechanisms for peer-to-peer energy markets," *IEEE Trans. Power Syst.*, vol. 36, no. 2, pp. 1470–1481, Mar. 2021.
[47] H.-M. Chung, S. Maharjan, Y. Zhang, and F. Eliassen, "Distributed deep reinforcement learning for intelligent load scheduling in residential smart grids," *IEEE Trans. Ind. Informat.*, vol. 17, no. 4, pp. 2752–2763, Apr. 2021.
[48] D. Qiu, Y. Ye, D. Papadaskalopoulos, and G. Strbac, "Scalable coordinated management of peer-to-peer energy trading: A multi-cluster deep reinforcement learning approach," *Appl. Energy*, vol. 292, Jun. 2021, Art. no. 116940.
[49] Y. Ye, Y. Tang, H. Wang, X.-P. Zhang, and G. Strbac, "A scalable privacy-preserving multi-agent deep reinforcement learning approach for large-scale peer-to-peer transactive energy trading," *IEEE Trans. Smart Grid*, vol. 12, no. 6, pp. 5185–5200, Nov. 2021.
[50] K. Zhang, S. Troitzsch, S. Hanif, and T. Hamacher, "Coordinated market design for peer-to-peer energy trade and ancillary services in distribution grids," *IEEE Trans. Smart Grid*, vol. 11, no. 4, pp. 2929–2941, Jul. 2020.
[51] Y. Zhou, J. Wu, G. Song, and C. Long, "Framework design and optimal bidding strategy for ancillary service provision from a peer-to-peer energy trading community," *Appl. Energy*, vol. 278, Nov. 2020, Art. no. 115671.
[52] A. Gómez-Expósito, A. J. Conejo, and C. Cañizares, *Electric Energy Systems: Analysis and Operation*. Boca Raton, FL, USA: CRC Press, 2018.
[53] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *Int. J. Elect. Power Energy Syst.*, vol. 99, pp. 45–56, Jul. 2018.
[54] J. Wang, W. Xu, Y. Gu, W. Song, and T. Green, "Multi-agent reinforcement learning for active voltage control on power distribution networks," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 34, 2021. [Online]. Available: https://proceedings.neurips.cc/paper/2021/file/1a6727711b84fd1efbb87fc565199d13-Paper.pdf
[55] A. Shahzad, S. Musa, A. Aborujilah, and M. Irfan, "Industrial control systems (ICSs) vulnerabilities analysis and SCADA security enhancement using testbed encryption," in *Proc. 8th Int. Conf. Ubiquitous Inf. Manage. Commun. (CUIMC)*, 2014, pp. 1–6.
[56] R. Lee, M. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid," E-ISAC, Washington, DC, USA, 2016. [Online]. Available: https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf
[57] X. Huang, Z. Qin, and H. Liu, "A survey on power grid cyber security: From component-wise vulnerability assessment to system-wide impact analysis," *IEEE Access*, vol. 6, pp. 69023–69035, 2018.
[58] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, "Rethinking the inception architecture for computer vision," in *Proc. IEEE Conf. Comput. Vis. pattern Recognit.*, 2016, pp. 2818–2826.
[59] Q. Song, R. Tan, C. Ren, and Y. Xu, "Understanding credibility of adversarial examples against smart grid: A case study for voltage stability assessment," in *Proc. 12th ACM Int. Conf. Future Energy Syst.*, Jun. 2021, pp. 95–106.
[60] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Implementation*. Boca Raton, FL, USA: CRC Press, 2004.
[61] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.
[62] C. Liu, H. Liang, T. Chen, J. Wu, and C. Long, "Joint admittance perturbation and meter protection for mitigating stealthy FDI attacks against power system state estimation," *IEEE Trans. Power Syst.*, vol. 35, no. 2, pp. 1468–1478, Mar. 2020.
[63] S. Boyd, S. P. Boyd, and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[64] Y. Dafalla, B. Liu, D. A. Hahn, H. Wu, R. Ahmadi, and A. G. Bardas, "Prosumer nanogrids: A cybersecurity assessment," *IEEE Access*, vol. 8, pp. 131150–131164, 2020.
[65] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security Privacy*, vol. 8, no. 1, pp. 81–85, Jan./Feb. 2010.
[66] R. Dasgupta, A. Sakzad, and C. Rudolph, "Cyber attacks in transactive energy market-based microgrid systems," *Energies*, vol. 14, no. 4, p. 1137, Feb. 2021.
[67] M. N. Kurt, Y. Yılmaz, and X. Wang, "Real-time detection of hybrid and stealthy cyber-attacks in smart grid," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 498–513, Feb. 2019.
[68] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 4, pp. 370–379, Dec. 2014.
[69] K. L. Morrow, E. Heine, K. M. Rogers, R. B. Bobba, and T. J. Overbye, "Topology perturbation for detecting malicious data injection," in *Proc. 45th Hawaii Int. Conf. Syst. Sci.*, Jan. 2012, pp. 2104–2113.
[70] C. Liu, J. Wu, C. Long, and D. Kundur, "Reactance perturbation for detecting and identifying FDI attacks in power system state estimation," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 4, pp. 763–776, Aug. 2018.
[71] W. Xu, I. M. Jaimoukha, and F. Teng, "Robust moving target defence against false data injection attacks in power grids," 2021, *arXiv:2111.06346*.
[72] M. Higgins, F. Teng, and T. Parisini, "Stealthy MTD against unsupervised learning-based blind FDI attacks in power systems," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1275–1287, 2021.
[73] S. Lakshminarayana and D. K. Y. Yau, "Cost-benefit analysis of moving-target defense in power grids," *IEEE Trans. Power Syst.*, vol. 36, no. 2, pp. 1152–1163, Mar. 2021.
[74] Z. Chu, O. Kosut, and L. Sankar, "Detecting load redistribution attacks via support vector models," 2020, *arXiv:2003.06543*.
[75] M. Cui, J. Wang, and B. Chen, "Flexible machine learning-based cyberattack detection using spatiotemporal patterns for distribution systems," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 1805–1808, Mar. 2020.
[76] A. Jindal, A. Dua, K. Kaur, M. Singh, N. Kumar, and S. Mishra, "Decision tree and SVM-based data analytics for theft detection in smart grid," *IEEE Trans. Ind. Informat.*, vol. 12, no. 3, pp. 1005–1016, Jun. 2016.
[77] T. Wu *et al.*, "Extreme learning machine-based state reconstruction for automatic attack filtering in cyber physical power system," *IEEE Trans. Ind. Informat.*, vol. 17, no. 3, pp. 1892–1904, Mar. 2021.
[78] S. Ahmed, Y. Lee, H. Seung-Ho, and I. Koo, "Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 10, pp. 2765–2777, Mar. 2019.
[79] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 8, pp. 1773–1786, Aug. 2016.
[80] C. Wang, S. Tindemans, K. Pan, and P. Palensky, "Detection of false data injection attacks using the autoencoder approach," 2020, *arXiv:2003.02229*.
[81] J. Zhao, G. Zhang, M. La Scala, Z. Y. Dong, C. Chen, and J. Wang, "Short-term state forecasting-aided method for detection of smart grid general false data injection attacks," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1580–1590, Jul. 2017.
[82] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of stealthy false data injection attacks in power system state estimation," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1636–1646, May 2018.
[83] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, 1997.
[84] J. H. Chow, *Time-Scale Modeling of Dynamic Networks With Applications to Power Systems*, vol. 46. Cham, Switzerland: Springer, 1982.
[85] D. K. Molzahn, J. T. Holzer, B. C. Lesieutre, and C. L. DeMarco, "Implementation of a large-scale optimal power flow solver based on semidefinite programming," *IEEE Trans. Power Syst.*, vol. 28, no. 4, pp. 3987–3998, Nov. 2013.
[86] G. Li and S. M. Rovnyak, "Integral square generator angle index for stability ranking and control," *IEEE Trans. Power Syst.*, vol. 20, no. 2, pp. 926–934, May 2005.
[87] E. L. Ratnam, S. R. Weller, C. M. Kellett, and A. T. Murray, "Residential load and rooftop PV generation: An Australian distribution network dataset," *Int. J. Sustain. Energy*, vol. 36, no. 8, pp. 787–806, Sep. 2017.
[88] D. Papadaskalopoulos and G. Strbac, "Nonlinear and randomized pricing for distributed management of flexible loads," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 1137–1146, Mar. 2016.
[89] A. Paszke *et. al*, "PyTorch: An imperative style, high-performance deep learning library," in *Proc. 33rd Conf. Neural Inf. Process. Syst. (NIPS)*, Vancouver, BC, Canada, Dec. 2019, pp. 8026–8037.
[90] W. Xu and F. Teng, "A deep learning based detection method for combined integrity-availability cyber attacks in power system," 2020, *arXiv:2011.01816*.
[91] N. Pool. (2021). *Historical Market Data*. [Online]. Available: https://www.nordpoolgroup.com/historical-market-data/