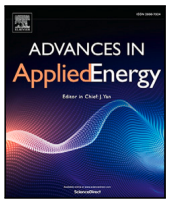
Advances in Applied Energy 17 (2025) 100205

Contents lists available at ScienceDirect

Advances in Applied Energy

journal homepage: www.elsevier.com/locate/adapen



A review of scalable and privacy-preserving multi-agent frameworks for distributed energy resources

Xiang Huo [a,*], Hao Huang [b], Katherine R. Davis [a], H. Vincent Poor [b], Mingxi Liu [c]

[a] Department of Electrical and Computer Engineering, Texas A&M University, College Station, 77843, TX, USA
[b] Department of Electrical and Computer Engineering, Princeton University, Princeton, 08544, NJ, USA
[c] Department of Electrical and Computer Engineering, University of Utah, Salt Lake City, 84112, UT, USA

ARTICLE INFO

Keywords:
Decentralized multi-agent systems
Distributed energy resources
Power systems
Privacy preservation
Cyber–physical system security

ABSTRACT

Distributed energy resources (DERs) are gaining prominence due to their advantages in improving energy efficiency, reducing carbon emissions, and enhancing grid resilience. Despite the increasing deployment, the potential of DERs has yet to be fully explored and exploited. A fundamental question restrains the management of numerous DERs in large-scale power systems, "*How should DER data be securely processed and DER operations be efficiently optimized?*" To address this question, this paper considers two critical issues, namely *privacy* for *processing DER data* and *scalability* in *optimizing DER operations*, then surveys existing and emerging solutions from a multi-agent framework perspective. In the context of scalability, this paper reviews state-of-the-art research that relies on parallel control, optimization, and learning within distributed and/or decentralized information exchange structures, while in the context of privacy, it identifies privacy preservation measures that can be synthesized into the aforementioned scalable structures. Despite research advances in these areas, challenges remain because these highly interdisciplinary studies blend a wide variety of scalable computing architectures and privacy preservation techniques from different fields, making them difficult to adapt in practice. To mitigate this issue, this paper provides a holistic review of trending strategies that orchestrate privacy and scalability for large-scale power system operations from a multi-agent perspective, particularly for DER control problems. Furthermore, this review extrapolates new approaches for future scalable, privacy-aware, and cybersecure pathways to unlock the full potential of DERs through controlling, optimizing, and learning generic multi-agent-based cyber–physical systems.

1. Introduction

1.1. Significance of DERs

Distributed energy resources (DERs), including solar photovoltaics (PVs), wind turbines, fuel cells, energy storage systems (ESSs), and electric vehicles (EVs), refer to a variety of small-scale energy generation and storage devices that are connected to the electric power grid [1]. DERs offer substantial flexibility to power systems at both the grid and customer levels, such as providing ancillary services [2], lowering energy costs [3], decarbonizing power systems [4,5], and enhancing grid resilience [6]. Because of these benefits, the power grid is transitioning toward an increasingly DER-rich electricity system, where the management of DERs is crucial for supporting the integration of renewable energy, enhancing grid resilience, and improving overall energy efficiency [7]. The growing dependence on DERs is reshaping how loads and generation sources are managed for homes and utilities. Additionally, past grid failures from extreme weather events, operational breakdowns, and cyber–physical attacks [8–13] have underscored the need for system operators (SOs), prosumers, and consumers to increasingly rely on DERs, both individually and in aggregate, to bolster grid resilience. Moreover, the importance of DERs is also reflected by their rapid growth and pivotal role in modernizing the grid. The global DER management system market is expected to expand significantly, projected to increase from USD 0.42 billion in 2021 to USD 1.33 billion by 2028, reflecting a compound annual growth rate of 18.0% [14]. In the U.S., the DER market is anticipated to nearly double in capacity from 2022 to 2027, with capital expenditures reaching USD 68 billion per year [15].

1.2. Major DER control challenges

1.2.1. Scalability issues

Traditionally, the power grid is managed in a centralized manner, with a single control problem formulated using data collected from the

* Corresponding author.
E-mail address: xiang.huo@tamu.edu (X. Huo).

https://doi.org/10.1016/j.adapen.2024.100205
Received 18 September 2024; Received in revised form 17 December 2024; Accepted 20 December 2024
Available online 31 December 2024

wide-area power grid network. However, the rapid increase of DERs at various scales makes it challenging to solve such large-scale centralized problems, due to the growing complexity, amount of heterogeneous data, and high computing costs. The high deployment of DERs requires scalable management techniques for greater sustainability and resilience, and accelerated adoption of commercially available grid solutions [4,16]. Broadly, the scalable control of DERs within power systems can be interpreted through a networked multi-agent (we refer to an element of a DER system as an *agent*) problem where agents can operate in parallel. To fully realize the potential of DERs, it is essential to develop scalable multi-agent frameworks incorporating advanced control, optimization, and machine learning theories and tools. These advanced techniques can help solve DER management problems efficiently in a scalable fashion that incorporates grid objectives and constraints, such as multi-agent-based DER management systems [17], data-driven multi-agent power grid control schemes [18], and multi-agent distributed optimal generation control of DERs [19]. All these developments highlight the benefits of developing multi-agent frameworks for DER management to ensure the optimality, scalability, and security of power grid operations.

1.2.2. Privacy threats

Another key consideration is privacy preservation/protection. Privacy breaches can happen during the processing and transmission of DER data, such as the loss of data provenance in the face of dishonest agents and the malicious interception of private information during data transmission [20–23]. For example, by analyzing load data, adversaries can infer consumers' lifestyle patterns, personal preferences, and occupancy profiles [24–26]. The privacy leakages in the power electric sector, especially DER-rich electric power grids, are escalating in both frequency and complexity. In recent years, a series of stringent privacy protection laws have come into effect to increase protections for consumers' personal data. These include the strongest privacy and security law [27], *European Union's General Data Protection Regulation*, effective in 2018, the U.S.'s first privacy law *California Consumer Privacy Act* [28], also effective in 2018, the Virginia's *Consumer Data Protection Act* [29], effective in 2023, and the most recent *Texas Data Privacy and Security Act* [30], effective in 2024. The increased privacy awareness in legislation is driving privacy protection standards in DER-rich power systems. For the cybersecurity of smart grids, the U.S. National Institute of Standards & Technology (NIST) has established the *Guidelines for Smart Grid Cybersecurity* to develop effective cybersecurity strategies for protecting the privacy of smart grid-related data and for securing the supporting communication networks [31]. The European Commission has introduced the *Data Protection Impact Assessment* template for smart grid and smart metering systems, aimed at assessing risks and developing countermeasures to ensure the protection of personal data [32]. Additionally, the International Electrotechnical Commission (IEC) has specified cybersecurity requirements for smart grids through a series of secure data transfer, prevention of eavesdropping, and intrusion detection standards [33]. Therefore, eliminating privacy and security concerns is critical for deploying advanced multi-agent frameworks to optimize DER operations.

1.3. Motivation and contributions

To this end, this paper focuses on two key technical challenges in optimizing DER-rich power systems, i.e., scalability and privacy. The old model of centralized electrical supply is no longer the sole reality, massive DERs with varying attributes require a scalable management plan. Furthermore, privacy-preserving decision-support tools need to be developed, integrated, and tested. The synergy of scalability and privacy protection is becoming a trending research topic among the control, optimization, learning, and power communities. A number of existing reviews have underlined the importance of DER control, along with arising related *privacy* and *cybersecurity* concerns, including DER protocol-level and DER device-level vulnerabilities, attacks, impacts, and mitigations [34,35], cyberattacks and defense mechanisms [36,37] for smart grid energy systems, and privacy-preserving schemes for smart grid applications [38,39]. Despite the aforementioned reviews providing different examinations of DER control, an interdisciplinary review of orchestrated scalable and privacy-preserving solutions is still missing for advanced and practical multi-agent DER control.

Motivated by the proliferation of recent research outcomes on DER control, this paper reviews state-of-the-art techniques for designing scalable and privacy-preserving multi-agent frameworks and their applications on DER control problems. Fig. 1 provides an overview of the review structure. We first survey scalable multi-agent frameworks based on distributed and decentralized information exchange structures, and then review integrated privacy preservation techniques. To the best of our knowledge, this paper, for the first time, surveys the effectiveness of scalability and privacy preservation ability in distributed and decentralized multi-agent frameworks, with an emphasis on large-scale DER control applications. The contributions of this paper include:

1. We conduct and present a systematic review of deploying multi-agent frameworks for DER control in power systems regarding *multi-agent-based problem formulation*, *scalable solutions*, and *privacy preservation techniques*.
2. We survey state-of-art scalable algorithms within multi-agent frameworks based on distributed and decentralized information exchange structures, and we review representative works for DER control problems. Moreover, we identify internal, external, and hierarchical types of adversaries/threats in multi-agent systems that can compromise the system's privacy and security.
3. We categorize representative *privacy preservation techniques* into *differential privacy*, *cyptographic methods*, and other *miscellaneous and emerging methods*, and discuss their features and applications to adapt into the scalable and privacy-preserving DER control.
4. Building on the summarization and discussion of existing works, this review extrapolates new approaches for future scalable, privacy-aware, and cybersecure multi-agent frameworks to unlock the full potential of DERs. These directions include *enhancing accuracy, privacy, and algorithm efficiency*, *establishing trustworthiness across fields*, and *developing zero-trust standards*.

In the rest of this paper, Section 2 provides an overview of deploying multi-agent systems for DER control applications in power systems, detailing the corresponding multi-agent optimization model and the information exchange structures. Within the multi-agent frameworks, Section 3 surveys predominantly scalable solutions and summarizes related privacy threats. To tackle the privacy threats, Section 4 reviews trending privacy preservation techniques that are available for scalable DER control. Section 5 extrapolates new approaches for future scalable, privacy-aware, and cybersecure pathways to unlock the full potential of DERs. Section 6 concludes the paper.

2. Multi-agent systems of DERs

In this section, we present a general multi-agent problem formulation and then delve into the detailed objectives and constraints for multi-agent-based DER control problems.

2.1. Multi-agent-based control of DERs

The management of DERs in power systems can be viewed as the control of agents within a networked multi-agent system. To describe such a multi-agent system, we need to define an *Optimization model* that specifies the problem objectives and constraints and an *Information exchange model* that details the agents' information exchange structure [40]. The optimization model includes cooperative (for the system)

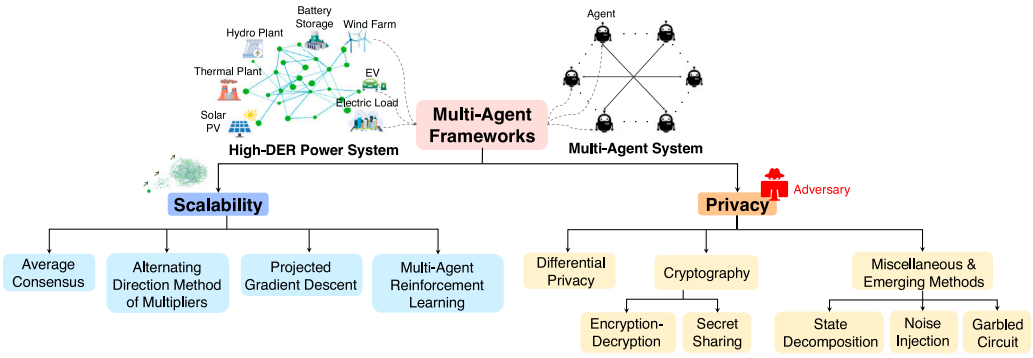


Fig. 1. Review structure of *scalable* and *privacy-preserving* multi-agent frameworks for DERs.

and/or competitive objectives (between agents) and is subject to networked constraints (related to a set of agents) and/or local constraints (related to only an individual agent). For the DER control problems in power systems, we classify the objectives into two categories, including *cooperative grid-level objective* and *competitive DER-level objective*.

The cooperative grid-level objectives support the achievement of system-wide goals, such as achieving overnight valley filling [41,42], minimizing power lines losses [43], reducing the emission of pollutants [44], etc. The competitive DER-level objectives aim at maximizing the benefits of DERs, such as bidding in the electricity market [45], reducing energy costs for consumers [46,47], and minimizing battery degradation costs [48]. The networked constraints can include the nodal voltage deviations and power flow constraints [49,50], which are coupled through the power network topology. The individual DER constraints can include battery charging/discharging rate [51], the capacity of generators [52], solar power availability for PV curtailment [53], etc. Besides, individual DER constraints often need to account for thermal dynamics, which are coupled with the operation of heating, ventilation, and air conditioning (HVAC) systems [54,55].

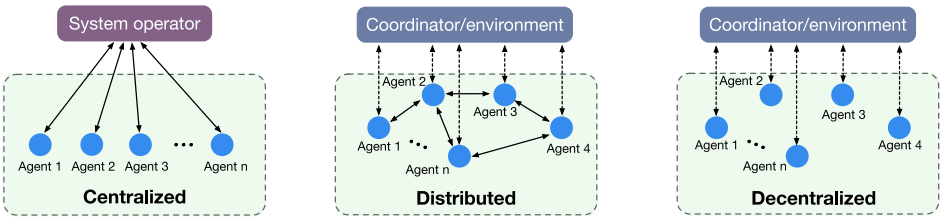
The information exchange model defines the computing and communication structure for solving networked multi-agent problems. Various models have been developed to facilitate control, optimization, and learning in these multi-agent systems [56–62]. To summarize, these models can be classified into *centralized*, *distributed*, and *decentralized* structures, as shown in Fig. 2. Besides, multi-agent frameworks also include *hierarchical* information exchange structures that combine centralized and distributed computing schemes, leveraging the strengths of both approaches to achieve both global oversight and local autonomy. In a hierarchical framework, a centralized layer handles high-level decisions and global optimization, while a distributed layer enables agents to autonomously manage local tasks and adapt to dynamic changes. Following this classification, this paper reviews scalable multi-agent frameworks within distributed and decentralized structures, addressing the interests of different stakeholders when operating DER-rich power systems. The SO (e.g., distribution or transmission SO) functions as a central authority and can provide instructions on coordinating and controlling the power system operations. To clarify, we refer to the coordinator as a central entity that is needed solely for the coordination of signals rather than for directly controlling any agent.

In a centralized setting, the SO manages the entire power system operation by collecting agent and network information, processing it, and sending control commands to all agents [56]. Therefore, the DER control problem is solved centrally where the SO makes strategic decisions on achieving grid-level and/or DER-level objectives, while agents simply follow the SO's commands. Centralized approaches are easy to implement and can often obtain globally optimized solutions. However, they are not scalable and suffer from drawbacks caused by (1) computing and communication overheads imposed on the SO, (2) compromised data privacy and security, and (3) vulnerability during cyber and physical contingencies.

In contrast to centralized methods, distributed and decentralized information exchange structures offer scalability, resilience, and enhanced privacy and cybersecurity, especially when applied to power systems with large DER populations, complex network topologies, and sophisticated control procedures [57–59]. In a distributed setting, the original large-scale problem is decomposed into small-scale subproblems where each agent exchanges information with other agents (e.g., its adjacent neighbors) to update its decision variables. Parallel computing is implemented at local agents to achieve high scalability, such as through the alternating direction method of multipliers (ADMM) [57]. Through efficient information exchange and parallel local computing among agents, distributed structures eliminate the sole reliance on the SO.

Similarly, decentralized approaches also achieve scalability by allocating central computing loads to each local agent, but with an emphasis on eliminating agent-to-agent communications. In decentralized information exchange structures, agents make decisions independently in a possible networked environment without communicating with each other. Compared to distributed structures, decentralized approaches eliminate agent-to-agent communication, thereby reducing privacy risks associated with direct information exchange between agents. However, agents in decentralized structures are often required to interact directly either with the environment or rely on the assistance of a coordinator, both of which can lead to private information leakage, such as in the presence of *honest-but-curious agents*, *external eavesdroppers*, and/or *the coordinator*. In a typical decentralized framework, such as primal–dual-based algorithms [60,61], agents and the coordinator iteratively update the primal variable (decision variable) and the dual variable (Lagrange multiplier), respectively. Owing to the outstanding scalability, distributed and decentralized multi-agent frameworks are well suited for large-scale DER control problems.

As shown in Fig. 2, the frequent and mandated exchange of private information in centralized, distributed, and decentralized multi-agent frameworks renders the system and agents vulnerable to privacy breaches. The acquisition, processing, and transmission of private customer data are typically necessary for delivering grid services and enhancing customer satisfaction [63–65]. However, unauthorized processing and sharing of sensitive information can result in privacy leakages and malicious manipulation of the system, introducing vulnerabilities that hinder the deployment of advanced DER control approaches. To protect the privacy of stakeholders, it is essential to integrate privacy preservation techniques into the design of scalable multi-agent frameworks. To this end, we identify typical adversaries in scalable multi-agent frameworks from internal, external, and hierarchical perspectives. These adversaries present distinct threats with varying attack vectors [20,21,66–71], including *Honest-but-curious agents* who follow the algorithm but may use the accessible information to infer the private data of other participants, *External eavesdroppers* who wiretap the exchanged messages between agents and/or the



(a) Centralized structure. (b) Distributed structure. (c) Decentralized structure.

Fig. 2. Three typical information exchange structures of networked multi-agent systems for managing DERs in power systems: (a) *Centralized* information exchange that relies on a system operator to collect information from all agents, process it, and then send control commands to each agent; (b) *Distributed* structure that allows agents to operate independently, interact with coordinator/environment, and communicate with each other over a network; and (c) *Decentralized* structures that is similar to a *Distributed* structure, but without agent-to-agent communications.

SO/coordinator/aggregator, and *the SO/coordinator/aggregator* who directly communicates with and/or controls the agents and has their private data. Consequently, overcoming privacy challenges in multi-agent systems has become a burgeoning research topic, driving the development of privacy-preserving frameworks that ensure privacy guarantees across diverse operational scenarios for DER control problems.

2.2. General problem formulation

Generically, the DER control problem (e.g., DER management system elicited by Fig. 3) can be framed into a multi-agent setting, with decision variables (e.g., charging/discharging of batteries and flexible loads), cooperative (grid-level) and competitive (DER-level) objectives, network models (e.g., power distribution and transmission networks), network constraints (e.g., current and voltage constraints), and individual constraints (e.g., DER's operational constraints). Fundamentally, we provide a generic optimization model that can describe the DER control problem as:

$$\begin{aligned} &\underset{\text{Decision Variables}}{\text{Optimize}} && \text{Cooperative} + \text{Competitive} && \text{(1a)}\\ &\text{s.t.} && \text{Network Models} && \text{(1b)}\\ &&& \text{Network Constraints} && \text{(1c)}\\ &&& \text{Individual Constraints} && \text{(1d)} \end{aligned}$$

Problem (1) can be broadly applied to a variety of power system applications, with goals such as grid modernization, decarbonization, and resilience.

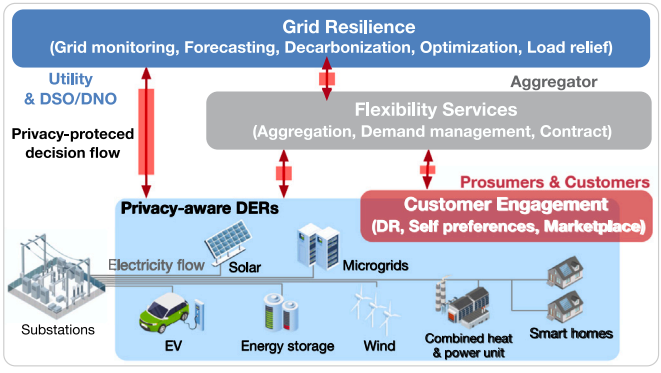


Fig. 3. Conceptualization of a privacy-preserving DER management system.

Fig. 3 shows the conceptualization of a privacy-preserving DER management system, where the prosumers, customers, aggregators, utilities, and distribution network/system operators (DNO/DSO) collaborate to achieve grid-level objectives and customer-side goals. In the subsequent section, the multi-agent-based DER control problem will be detailed using the formulation of Problem (1).

2.3. Network models, objectives, and constraints

2.3.1. Network models

Power flow model. The power flow model is built upon power network topology, loads, and generation sources. DERs can function as flexible loads or generation units in power distribution and transmission networks. We next present the control of DERs in distribution systems using the nonlinear DistFlow branch model [72]. Consider a radial distribution network described by a connected graph $G = \{\mathcal{N}, \mathcal{E}\}$, where $\mathcal{N} = \{0, 1, \ldots, n\}$ denotes a set of nodes/buses, $\mathcal{E} \subset \mathcal{N} \times \mathcal{N}$ denotes a set of directed edges/lines. The network is tree-structured where Node 0 serves as the slack bus and V_0 denotes the constant voltage magnitude of Node 0.

Let V_j denote the voltage magnitude of Node j, C_j denote the set of children of Node j, and let the line $l_{jk} \in \mathcal{E}$ connect two neighboring nodes, Node j and Node k. The active and reactive power flows from Node i and Node j are represented by $\mathcal{P}_{ij}$ and $\mathcal{Q}_{ij}$, respectively, the resistance and reactance of the line l_{ij} are given by r_{ij} and x_{ij}, respectively. Let P_i, Q_i, p_i, and q_i denote the active power consumption, reactive power consumption, active power injection, and reactive power injection to Node i, respectively.

The DistFlow branch equations can be written in the real form as [72,73]:

$$\sum_{k \in C_j} \mathcal{P}_{jk} = \mathcal{P}_{ij} - P_j + p_j - r_{ij}\mathcal{I}_{ij}^2, \qquad \forall j \in \mathcal{N} \qquad \text{(2a)}$$

$$\sum_{k \in C_j} \mathcal{Q}_{jk} = \mathcal{Q}_{ij} - Q_j + q_j - x_{ij}\mathcal{I}_{ij}^2, \qquad \forall j \in \mathcal{N} \qquad \text{(2b)}$$

$$V_i^2 - V_j^2 = 2(r_{ij}\mathcal{P}_{ij} + x_{ij}\mathcal{Q}_{ij}) - (r_{ij}^2 + x_{ij}^2)\mathcal{I}_{ij}^2, \qquad \forall ij \in \mathcal{E} \qquad \text{(2c)}$$

$$\mathcal{I}_{ij}^2 = (\mathcal{P}_{ij}^2 + \mathcal{Q}_{ij}^2)/V_i^2, \qquad \forall ij \in \mathcal{E} \qquad \text{(2d)}$$

where $\mathcal{I}_{ij}$ denotes the current flow from Node i to Node j. A typical power flow problem aims to solve (2) for voltages and power flows, given the active and reactive power injections and line resistances and reactances. The nonlinear DistFlow branch model can be further linearized using LinDistFlow by the approximation of $\mathcal{I}_{ij}^2 \approx 0$, given the fact that line losses are small compared to the line flows [74].

Other coupled network models. Another recently developed network model in power systems is the carbon flow model [75]. Chen et al. in [75] introduce a flow-based emission model that is analogous to the power flows. The carbon flow model tracks carbon emissions from generators as they are transmitted through power grids, creating a virtual carbon flow within the power network. Other geo-related network models, such as gas [76], water [77], and electrified transportation network models [78], are also commonly coupled with the power system networks. Optimizing the usage of controllable grid-tied assets across different networked systems shows great promise in enhancing power grid operation, contributing to more flexible and resilient integrated power and energy systems.

2.3.2. Constraints

Network constraints. Power system network constraints ensure standard power system operations when providing electricity. The management of DERs must align with grid-level constraints, such as current, voltage, and thermal constraints. For example, the voltage constraint can be expressed as:

$$\underline{v}V_0 \le V_i \le \bar{v}V_0, \qquad \forall i \in \mathcal{N} \tag{3}$$

which requires that the voltage magnitudes of all nodes must be constrained within the range $[\underline{v}V_0, \bar{v}V_0]$, $\underline{v}$ and $\overline{v}$ represent the lower and upper bounds, respectively.

Similarly, the current constraint can be written into [79]:

$$\underline{I}_{ij} \le I_{ij} \le \overline{I}_{ij}, \qquad \forall ij \in \mathcal{E} \tag{4}$$

where $\underline{I}_{ij}$ and $\overline{I}_{ij}$ represent the lower and upper current bounds, respectively.

The carbon flow model also introduces networked constraints on carbon emission capacity, which can be imposed at the nodal level by:

$$w_i P_i \le \bar{R}_i, \qquad \forall i \in \mathcal{N} \tag{5}$$

where $\bar{R}_i$ denotes the nodal emission capacity of Node i.

Local constraints of DERs. In addition to network constraints that can reflect the joint impacts of DERs, local constraints reflect individual DER's operational requirements. For example, the operation of ESSs is subject to a set of local constraints, including state of charge (SoC) bounds, charging/discharging power limits, and energy efficiency constraints. Solar and wind power supplies are often constrained by the maximum available energy.

DERs, such as solar PVs or ESSs, often provide energy or manage energy distribution to maintain comfort levels in buildings, particularly through HVACs. The operation of an HVAC system can also be interpreted as a type of thermostatically controlled load (TCL) that couples thermal dynamics (e.g., insulation, ambient temperature) and electricity consumption (e.g., On and Off cycles). For example, an HVAC can affect the indoor temperature according to the following linear dynamics [54]:

$$\theta_t^{\text{in}} = \theta_{t-1}^{\text{in}} + \alpha_h(\theta_t^{\text{out}} - \theta_{t-1}^{\text{in}}) + \beta_h x_t^{\text{H}} \tag{6}$$

where x_t^{H} denotes the active power consumption of the HVAC at time t, θ_t^{in} and θ_t^{out} denote the indoor and outdoor temperatures at time t, respectively. The parameters α_h and β_h define the heat transfer properties of the environment and the thermal efficiency of the TCL appliance, respectively. The comfort zone constraint defines that the average temperature of the building should remain within the range of:

$$\underline{\theta} \le \boldsymbol{\theta}^{\text{in}} \le \overline{\theta} \tag{7}$$

where $\boldsymbol{\theta}^{\text{in}} \in \mathbb{R}^T$ denotes the indoor room temperature across T time intervals, $\underline{\theta}$ and $\overline{\theta}$ denote the lower and upper bounds of the comfort zone, respectively.

Without loss of generality, we describe individual constraints of the $\hat{\imath}$th DER via a feasible set $\mathcal{X}_{\hat{\imath}}$, defined as:

$$\mathcal{X}_{\hat{\imath}} := \{\hat{\imath} \in \hat{\mathcal{N}} \mid \underline{x}_{\hat{\imath}} \le x_{\hat{\imath}} \le \bar{x}_{\hat{\imath}}\} \tag{8}$$

where $x_{\hat{\imath}}$ denotes decision variable of the $\hat{\imath}$th DER, $\hat{\mathcal{N}}$ denotes the set of DERs, and $\underline{x}_{\hat{\imath}}$ and $\bar{x}_{\hat{\imath}}$ denote the lower and upper operational bounds, respectively.

2.3.3. Objective functions

The integration of DERs enables both *cooperative grid-level objectives* and *competitive DER-level objectives*, highlighting their multi-faceted roles in power system operations. The cooperative and competitive objectives can be summarized into a general quadratic formulation as:

$$f_{\text{quad}}(\boldsymbol{x}) = a_1 \left\| \boldsymbol{A}\boldsymbol{x} + \boldsymbol{P}_t \right\|_2^2 + \boldsymbol{C}^T \boldsymbol{x} + a_2 \tag{9}$$

where $\boldsymbol{x}_{\hat{\imath}} \in \mathbb{R}^T$ denotes the decision variable of the $\hat{\imath}$th agent expanded across T time slots, $\boldsymbol{x} = [\boldsymbol{x}_1^\top, \dots, \boldsymbol{x}_{\hat{n}}^\top]^\top \in \mathbb{R}^{\hat{n}T}$, $\hat{n}$ denotes the total number of agents, a_1 and a_2 denote cost parameters for adjusting objective weights, and $\boldsymbol{A} \in \mathbb{R}^{T \times \hat{n}T}$, $\boldsymbol{P}_t \in \mathbb{R}^T$, $\boldsymbol{C} \in \mathbb{R}^{\hat{n}T}$ denote parameter matrices. The quadratic objective in (9) is applicable for various power system applications, such as load shifting [80], voltage regulation [81], and EV charging control problems [41,82].

Cooperative grid-level objective functions. It refers to controlling DERs cooperatively to provide grid services such as for peak shaving, valley filling, voltage regulation, frequency control, and demand response. For example, the load-shaping objective takes the form of:

$$f_{\text{shape}}(\boldsymbol{x}) = \frac{1}{2} \left\| \boldsymbol{A}\boldsymbol{x} + \boldsymbol{P}_t \right\|_2^2 \tag{10}$$

where the physical interpretation of the vector $\boldsymbol{P}_t \in \mathbb{R}^T$ can represent the baseline load in valley-filling problems.

Some other cooperative grid-level objectives like frequency control and voltage regulation aim to keep the power system's frequency or voltage close to its nominal values. For example, the voltage regulation objective minimizes the squared deviation of the bus voltage magnitude by [83]:

$$f_{\text{voltage}}(\boldsymbol{x}) = \sum_{i \in \mathcal{N}} \|V_i(\boldsymbol{x}) - \hat{V}_i(\boldsymbol{x})\|_2^2 \tag{11}$$

where $\hat{V}_i(\boldsymbol{x})$ denotes the nominal voltage magnitude output of bus i.

Power loss minimization is another cooperative grid-level objective that closely relates to the grid's power flow model. The supplies and demands from DERs are flexible and can be adjusted to reduce power losses. For instance, the active power loss can be represented by [84]:

$$f_{\text{active}}(\boldsymbol{x}) = \sum_{l_{ij} \in \mathcal{L}} r_{ij} \left(\frac{\mathcal{P}_{ij}^2(\boldsymbol{x}) + \mathcal{Q}_{ij}^2(\boldsymbol{x})}{V_i^2(\boldsymbol{x})} \right). \tag{12}$$

where $\mathcal{P}_{ij}(\boldsymbol{x})$ and $\mathcal{Q}_{ij}(\boldsymbol{x})$ denote the active and reactive power flow outputs of the line l_{ij}, respectively.

Besides, the environmental objective functions, such as minimization of CO_2 emissions, can be expressed as [85]:

$$f_{\text{env}}(\boldsymbol{x}) = c_s p^{\text{grid}}(\boldsymbol{x}) + \sum_{i \in \mathcal{N}} \sum_{u \in \hat{\mathcal{N}}_i} g_{i,u} p_{i,u}^{\text{fuel}}(\boldsymbol{x}_u) \tag{13}$$

where $p^{\text{grid}}(\boldsymbol{x})$ denotes the total consumer power of grid electricity, multiplied by c_s that denotes the carbon intensity of the grid electricity, $\hat{\mathcal{N}}_i$ denotes the set of agents connected to bus i, $p_{i,u}^{\text{fuel}}(\boldsymbol{x}_u)$ is the consumed fuels from other DER and non-DER sources, $\boldsymbol{x}_u$ denotes the decision variables of the uth fuel source, and $g_{i,u}$ denotes the carbon intensity of the specific fuel u at bus i.

Competitive DER-level objective functions. DERs have their own objective functions based on their operational requirements and end-user needs. These types of objective functions, i.e., $f_{\hat{\imath}}(\boldsymbol{x}_{\hat{\imath}})$, are referred to as competitive because they reflect the interest of an individual agent associated with a specific DER and involve only one decision variable (or a group of DERs acting as a single agent).

The quadratic objective in (9) also applies to a wide range of competitive DER-level objectives. For example, ESSs often suffer from battery degradation caused by frequent charging and discharging of batteries over time. The minimization of battery degradation cost is frequently required in plug-in EVs [86] and off-grid power systems [87]. To this end, the following battery degradation cost objective can reduce the charging and discharging cycles by [82,86]:

$$f_{\text{battery}}(\boldsymbol{x}_{\hat{\imath}}^{\text{b}}) = \|\boldsymbol{x}_{\hat{\imath}}^{\text{b}}\|_2^2 \tag{14}$$

where $\boldsymbol{x}_{\hat{\imath}}^{\text{b}} \in \mathbb{R}^T$ denotes the charging/discharging profiles of the $\hat{\imath}$th ESS over T time slots. Similarly, capacitors and regulators are also often penalized by frequent switching control costs to slow the devices from wearing out [88].

The comfort to users based on electrical usage of common appliances, such as washing machines and HVAC systems, is also commonly

considered a DER-level objective. The On-Off status of an HVAC can be controlled by end users to maintain room temperature within a specific comfort zone, i.e., $[\underline{\theta}, \overline{\theta}]$. To this end, the indoor room temperature comfort objective can be enforced by:

$$f_{\text{HVAC}}(\boldsymbol{x}_{\hat{i}}^{\text{H}}) = \|\boldsymbol{\theta}^{\text{in}} - \hat{\boldsymbol{\theta}}^{\text{in}}\|_2^2 \tag{15}$$

where $\hat{\boldsymbol{\theta}}^{\text{in}} \in \mathbb{R}^T$ denotes the desired room temperature across T time intervals, e.g., the averaged temperature of $(\underline{\theta} + \overline{\theta})/2$.

Washing appliances, like dishwashers and clothes washers, provide comfort to users when tasks are completed by a specific time [54], defined by:

$$f_{\text{machine}}(\boldsymbol{x}_{\hat{i}}^{\text{M}}) = |\sum_{t=1}^{T}(\boldsymbol{x}_{\hat{i},t}^{\text{M}} \cdot \Delta t) - \hat{e}_T^{\text{M}}|^2 \tag{16}$$

where $\boldsymbol{x}_{\hat{i}}^{\text{M}} \in \mathbb{R}^T$ denotes the active power consumption of the $\hat{i}$th washing machine across T time intervals, Δt denotes the time interval length, and $\hat{e}_T^{\text{M}}$ denotes the desired energy level at the end of the period.

Another exemplary DER-level objective is the minimization of operational curtailment costs. The curtailment cost of a solar PV can be calculated based on the inverter's active and reactive power generations by [53,89]:

$$f_{\text{curtail}}(\boldsymbol{x}_{\hat{i}}^{\text{pv}}) = \|\boldsymbol{x}_{\hat{i}}^{\text{pv}} - \bar{\boldsymbol{x}}_{\hat{i}}^{\text{pv}}\|_2^2 + f^{\text{pvg}}(\boldsymbol{s}^{\text{pv}}) \tag{17}$$

where $\boldsymbol{x}_{\hat{i}}^{\text{pv}} \in \mathbb{R}^T$ and $\bar{\boldsymbol{x}}_{\hat{i}}^{\text{pv}} \in \mathbb{R}^T$ denote the curtailed and original active power generation from the solar PV, respectively, and $f^{\text{PVG}}(\boldsymbol{s}^{\text{pv}})$ denotes the solar PV generation cost that can be described via a polynomial of the apparent power $\boldsymbol{s}^{\text{pv}} \in \mathbb{R}^T$, e.g., $f^{\text{pvg}}(s_t^{\text{pv}}) = c_1^{\text{pv}}(s_t^{\text{pv}})^2 + c_2^{\text{pv}} s_t^{\text{pv}} + c_3^{\text{pv}}$, whose coefficients c_1^{pv}, c_2^{pv}, and c_3^{pv} can determined by curve fitting from the manufacturer. Additionally, the competitive DER-level objectives also include the aggregated decision-making for a group of DERs, such as the bidding plans from distribution companies and DER aggregators [45] and the negotiation on locational marginal price from multiple prosumers [90].

2.3.4. Illustrative problem formulation

After identifying the objective functions and constraints, we present the mathematical formulation of the DER control problem as:

$$\begin{aligned} \min_{\boldsymbol{x}} \quad & \sum_{\hat{i}\in\mathcal{I}} f_{\hat{i}}(\boldsymbol{x}_{\hat{i}}) + g(\boldsymbol{x}) \\ \text{s.t.} \quad & \boldsymbol{x}_{\hat{i}} \in \mathcal{X}_{\hat{i}}, \ \forall \hat{i} \in \mathcal{I} \\ & \boldsymbol{x} \in \mathcal{G}. \end{aligned} \tag{P1}$$

Problem (P1) aligns with (1) where the $\hat{i}$th agent is associated the decision variable $\boldsymbol{x}_{\hat{i}} \in \mathbb{R}^T$ and the objective function $f_{\hat{i}}(\cdot) : \mathbb{R}^T \mapsto \mathbb{R}^1$, $\mathcal{I}$ denotes the set of agents, T denotes the dimension, $\mathcal{X}_{\hat{i}}$ denotes the feasible region of the decision variable $\boldsymbol{x}_{\hat{i}}$, $\boldsymbol{x} = [\boldsymbol{x}_1^\top, \dots, \boldsymbol{x}_{\hat{n}}^\top]^\top$, $g(\cdot) : \mathbb{R}^{\hat{n}T} \mapsto \mathbb{R}^1$ denotes a coupled objective function whose inputs are collected decision variables from all agents, and $\mathcal{G}$ denotes a feasible set that describes the coupled constraints including the network model and network constraints.

Problem (P1) represents a generalized DER control problem formulation, containing global objective functions and constraints (e.g., (10)–(13), and (3)–(5)), and local objective functions and constraints (e.g., (14)–(17), and (6), (7)). Problem (P1) has been broadly adopted to optimize the operation of power electric systems, such as demand response [91], optimal power flow [92], management of grid-interactive efficient buildings [93], and EV charging control problems [94].

3. Scalable methods

Previously, Section 2 establishes fundamentals on the deployment of multi-agent systems in DER control. This section aims to provide reviews on state-of-the-art scalable approaches within different multi-agent frameworks. We select representative works under each category of scalable multi-agent approaches and show their applications in DER control with highlighted key features (see Table 1). At the end, we discuss related privacy leakage issues in these typical multi-agent frameworks for DER control.

3.1. Distributed and decentralized algorithms

3.1.1. Average consensus

Average consensus (AvgC) includes *dynamic AvgC*, where agents seek to compute the average of individual time-varying signals, and *static AvgC*, where agents reach the average of their initial values. The convergence of AvgC is first proved by DeGroot [108], then further studied by many researchers (see, e.g., [58,95,109]). To provide a straightforward explanation, we refer to AvgC as the static one and introduce its theoretical foundations. AvgC-based algorithms are commonly used in multi-agent systems to collaboratively compute the average of agents' local values. Suppose each agent has an initial scalar state $x_{\hat{i}}^0$. The average consensus asymptotically converges to an "agreement", e.g., a constant c, under suitable assumptions on the coefficients and graph connectivity. At the ℓth iteration, agent $\hat{i}$ updates its decision variable $x_{\hat{i}}^{\ell} \to x_{\hat{i}}^{\ell+1}$ by [95,108]:

$$x_{\hat{i}}^{\ell+1} = \sum_{\hat{j}=1}^{\hat{n}} a_{\hat{i}\hat{j}}^{\ell} x_{\hat{j}}^{\ell} \tag{18}$$

where $x_{\hat{i}}^{\ell+1}$ is the weighted average held by the agent $\hat{i}$, $a_{\hat{i}\hat{j}}^{\ell}$ denotes the averaging coefficient. Follow (18), the averaged consensus is achieved at $\lim_{\ell\to\infty} x_{\hat{i}}^{\ell} = c, \forall \hat{i} \in \mathcal{I}$.

Based on the distributed multi-agent information exchange structure, the $\hat{i}$th agent can achieve AvgC by interacting only with its neighbors as [58]:

$$x_{\hat{i}}^{\ell+1} = x_{\hat{i}}^{\ell} + \epsilon \sum_{\hat{j}\in\mathcal{B}_{\hat{i}}} \phi_{\hat{i}\hat{j}} \left(x_{\hat{j}}^{\ell} - x_{\hat{i}}^{\ell} \right) \tag{19}$$

where $\mathcal{B}_{\hat{i}}$ denotes the set of neighbors of agent $\hat{i}$, ϵ denotes the step size, and $\phi_{\hat{i}\hat{j}}$ denotes the adjacency coefficient of the network, i.e., $\phi_{\hat{i}\hat{j}} = 0$ if $\hat{j} \notin \mathcal{B}_{\hat{i}}$. Follow the distributed information exchange structure, the decision variables $x_{\hat{i}}^{\ell}$, $\forall \hat{i} \in \mathcal{B}$ converge to the averaged value $c = \sum_{\hat{i}=1}^{\hat{n}} x_{\hat{i}}^0/\hat{n}$, under balanced digraph and other numerical assumptions (see more details in [58,109]). Therefore, AvgC is efficient for distributed coordination and primarily used for tasks like distributed averaging, decentralized estimation, and synchronization in networked multi-agent systems. The distributed architecture of AvgC enables scalable multi-agent decision-making for DER control problems, such as achieving optimal DER management for supply–demand balance [110–112]. However, AvgC-based methods are often limited to scenarios where all agents must reach the same consensus value. Additionally, future research is needed to accelerate convergence in large networks or those with weak connectivity and to reduce sensitivity to time delays and changes in network topology. Variations of AvgC-based algorithms have been developed to handle asynchronous and time-varying environments [113], accelerate convergence through linear predictors [114], and incorporate quantization techniques that refine intervals as the algorithm progresses [115]. These techniques contribute to the research and development in the power and energy field, as power systems are intrinsically networked and operate in dynamic environments.

3.1.2. Alternating direction method of multipliers

Alternating direction method of multipliers (ADMM) is initially developed in [116] based on the augmented Lagrangian and later independently rediscovered and popularized by Boyd et al. [57]. ADMM has been popular in optimizing large-scale multi-agent systems owing to its decomposition ability. Specifically, it focuses on solving a type of optimization problem:

$$\begin{aligned} \min_{\tilde{\boldsymbol{x}},\tilde{\boldsymbol{y}}} \quad & f(\tilde{\boldsymbol{x}}) + g(\tilde{\boldsymbol{y}}) \\ \text{s.t.} \quad & \boldsymbol{D}\tilde{\boldsymbol{x}} + \boldsymbol{G}\tilde{\boldsymbol{y}} = \boldsymbol{h} \end{aligned} \tag{P2}$$

where $\tilde{\boldsymbol{x}} \in \mathbb{R}^{T_1}$ and $\tilde{\boldsymbol{y}} \in \mathbb{R}^{T_2}$ are variables, $\boldsymbol{D} \in \mathbb{R}^{m\times T_1}$ and $\boldsymbol{G} \in \mathbb{R}^{m\times T_2}$ are two matrices, and $\boldsymbol{h} \in \mathbb{R}^m$ is a m-dimensional vector. The objective functions, $f(\cdot)$ and $g(\cdot)$, are assumed to be convex.

ADMM forms an augmented Lagrangian of (P2) as:

Table 1
Representative works on scalable multi-agent frameworks and their applications in DER control.

Method	Reference	Structure	Applications	Key features
AvgC	[95]	Distributed	Networked multi-agent systems	1-Consider both fixed and time-varying topologies; 2-study convergence rates.
AvgC	[96]	Distributed	Networked multi-agent systems	1-Consensus of networked agents under noisy measurements; 2-stochastic approximation-type algorithms with a decreasing step size.
AvgC	[97]	Distributed	Load balancing	1-Approximate consensus problem for stochastic networks with nonlinear agents; 2-consider switching topology, noisy, and delayed information about agent states.
AvgC	[98]	Distributed	DC microgrids	1-Nonlinear consensus-like system of differential–algebraic equations; 2-controllers to converge to weighted power measurement at the sources.
ADMM	[99]	Distributed	Microgrids with DERs	1-Online energy management based on ADMM; 2-explore the use of regret minimization; 3-utility microgrid buys/sells power from/to other microgrids.
ADMM	[90]	Distributed	Coordination of prosumer-owned DERs	1-An affinely adjustable robust extension of ADMM that is resilient to forecast deviations; 2-enable prosumers to take local "wait-and-see" recourse decisions that compensate real-time forecast deviations.
ADMM	[100]	Distributed	AC optimal power flow	1-Distributed three-block algorithm; 2-introduce carefully tuned delays in the Volt-Var control block update to circumvent unstable numerical behavior.
ADMM	[101]	Decentralized	AC optimal power flow	1-Use machine learning to speed up the convergence of ADMM; 2-develop novel data-filtering techniques to identify high-quality training data.
PGD	[60]	Distributed	Multi-agent problems	1-Adopt Tikhonov regularization to deal with coupling objectives and constraints; 2-allow for differing step lengths across users as well as across the primal and dual space.
PGD	[82]	Decentralized	EV charging control	1-Decentralized EV charging control for valley-filling; 2-nonseparable objective function and coupled inequality constraints; 3-develop a shrunken-primal–dual subgradient algorithm.
PGD	[102]	Decentralized	Networked multi-agent systems	1-Two-facet scalability *w.r.t.* both the agent population size and the network dimension; 2-computing load reduction compared to full-dimension cases.
PGD	[103]	[a]	Smooth convex optimization	1-Prove convergence of gradient descent using nonconstant, long stepsize patterns, for smooth convex optimization; 2-computer-assisted analysis.
MARL	[104]	Hierarchical (partially observable)	Mobile power sources and repair crews	1-Formulate a resilience-driven dispatch problem; 2-a hierarchical MARL with embedded function encapsulating system dynamics.
MARL	[105]	Centralized training with decentralized execution	Residential hybrid energy system	1-A multi-stage proximal policy optimization on-policy framework with imitation learning; 2-improve indoor thermal comfort and energy efficiency.
MARL	[106]	Distributed training without global observability	Multi-agent problems	1-Safe MARL formulation that extends beyond cumulative forms in both the objective and constraints; 2-a scalable primal–dual actor-critic method.
MARL	[107]	Distributed	Networked multi-agent problems	1-Maximize the average of their entropy-regularized long-term rewards; 2-localized policy iteration algorithm that provably learns a near-globally-optimal policy using only local information.

[a] Not defined in the literature AvgC: Average consensus ADMM: Alternating direction method of multipliers PGD: Projected gradient descent MARL: Multi-agent reinforcement learning.

$$\mathcal{L}_\rho(\tilde{\boldsymbol{x}}, \tilde{\boldsymbol{y}}; \lambda) = f(\tilde{\boldsymbol{x}}) + g(\tilde{\boldsymbol{y}}) + \lambda^\top(\boldsymbol{D}\tilde{\boldsymbol{x}} + \boldsymbol{G}\tilde{\boldsymbol{y}} - \boldsymbol{h}) + \frac{\rho}{2}\|\boldsymbol{D}\tilde{\boldsymbol{x}} + \boldsymbol{G}\tilde{\boldsymbol{y}} - \boldsymbol{h}\|_2^2 \tag{20}$$

where $\lambda \in \mathbb{R}^m$ denotes the Lagrange multiplier associated with the equality constraint, and $\rho > 0$ denotes the penalty parameter associated with the penalty term $\|\boldsymbol{D}\tilde{\boldsymbol{x}} + \boldsymbol{G}\tilde{\boldsymbol{y}} - \boldsymbol{h}\|_2^2$. The penalty term, or regularization, adds an extra cost to the optimization function, penalizing the model when it deviates from the constraint.

Based on the augmented Lagrangian, the ADMM updates the primal (decision variable) and the dual variable (Lagrange multiplier) by:

$$\tilde{\boldsymbol{x}}^{\ell+1} = \underset{\tilde{\boldsymbol{x}}}{\operatorname{argmin}}\ \mathcal{L}_\rho\left(\tilde{\boldsymbol{x}}, \tilde{\boldsymbol{y}}^{\ell}; \lambda^{\ell}\right) \tag{21a}$$

$$\tilde{\boldsymbol{y}}^{\ell+1} = \underset{\tilde{\boldsymbol{y}}}{\operatorname{argmin}}\ \mathcal{L}_\rho\left(\tilde{\boldsymbol{x}}^{\ell+1}, \tilde{\boldsymbol{y}}; \lambda^{\ell}\right) \tag{21b}$$

$$\lambda^{\ell+1} = \lambda^{\ell} + \rho\left(\boldsymbol{D}\tilde{\boldsymbol{x}}^{\ell+1} + \boldsymbol{G}\tilde{\boldsymbol{y}}^{\ell+1} - \boldsymbol{h}\right). \tag{21c}$$

Since $f(\tilde{\boldsymbol{x}})$ and $g(\tilde{\boldsymbol{y}})$ have uncorrelated decision variables, the decomposability of ADMM allows $\tilde{\boldsymbol{x}}$ and $\tilde{\boldsymbol{y}}$ to be updated separately in a sequential (alternating) fashion. The distributed nature of ADMM enables scalability in solving large-scale multi-agent optimization problems. By decomposing large problems into smaller sub-problems, ADMM-based approaches allow individual agents to solve these sub-problems locally. Therefore, ADMM-based methods are well-suited for solving large-scale DER optimization problems, such as the management of DERs with high

uncertainty of power generation and load forecasts [90,99], the decomposition of OPF [100,117], and asynchronous distributed optimization algorithms for oscillation monitoring [118]. Despite the merits, ADMM-based methods can suffer from high communication overhead between agents due to the need for iterative message exchanges. Recently, ADMM has been extensively studied and improved with a number of generalizations, including approaches for tackling nonseparable optimization problem formulations [119], nonconvex problems [120], as well as other heuristic ADMM-based approaches [121,122].

3.1.3. Projected gradient descent

Gradient descent is a fundamental method to solve unconstrained optimization problems. Gradient descent iteratively moves toward the minimum of a function by taking steps proportional to the negative of the gradient of the function. Compared to gradient descent, projected gradient descent (PGD) uses additional projection operations to enforce constraints by projecting the solution back into the feasible region after updating primal and/or dual variables. PGD-based methods are well suited to solving constrained optimization problems, particularly large-scale optimization tasks with numerous local constraints.

For example, the relaxed Lagrangian function of problem **(P1)** is:

$$\mathcal{L}_r(\boldsymbol{x};\lambda) = \sum_{i\in I} f_i(\boldsymbol{x}_i) + g(\boldsymbol{x}) + \lambda^{\top}(\boldsymbol{A}\boldsymbol{x} - \boldsymbol{h}) \tag{22}$$

where $\mathcal{G}$ in **(P1)** is defined as $\mathcal{G} := \boldsymbol{A}\boldsymbol{x} - \boldsymbol{h} \le \boldsymbol{0}$.

Subsequently, PGD updates the primal (23a) and dual (23b) variables by [59]:

$$\boldsymbol{x}_{\hat{i}}^{\ell+1} = \Pi_{\mathbb{X}_{\hat{i}}}[\boldsymbol{x}_{\hat{i}}^{\ell} - \alpha_{\hat{i}}\nabla_{\boldsymbol{x}_{\hat{i}}}\mathcal{L}_r\left(\boldsymbol{x}_1^{\ell},\ldots,\boldsymbol{x}_{\hat{n}}^{\ell};\lambda^{\ell}\right)] \tag{23a}$$

$$\lambda^{\ell+1} = \Pi_{\mathbb{R}^+}[\lambda^{\ell} + \beta\nabla_{\lambda}\mathcal{L}_r\left(\boldsymbol{x}_1^{\ell},\ldots,\boldsymbol{x}_{\hat{n}}^{\ell};\lambda^{\ell}\right)] \tag{23b}$$

where $\alpha_{\hat{i}}$ and β denote the primal and dual step sizes, respectively, $\mathcal{L}_r(\boldsymbol{x}_1^{\ell},\ldots,\boldsymbol{x}_{\hat{n}}^{\ell};\lambda^{\ell})$ denotes the relaxed Lagrangian function at the ℓth iteration, $\Pi_{\mathcal{X}_{\hat{i}}}[\cdot]$ denotes the Euclidean projection operator, and $\mathbb{R}^+$ denotes the positive real set.

PGD-based methods are straightforward to implement and computationally efficient for large-scale multi-agent problems. The PGD allows agents to handle local constraints individually, making it a good fit for decentralized settings. Demonstration initiatives of PGD-based (and gradient-based) approaches for managing DER-rich power grids include solving online load flow optimization problems [123], decentralized management of renewable generation and demand response [124], and voltage regulation using DERs [125]. However, PGD can suffer from slow convergence when addressing non-convex problems or poorly conditioned constraints, as it is sensitive to step size choices and requires careful tuning for optimal performance. Additionally, agents must perform a projection step, which can be computationally expensive for certain constraint sets. To enhance scalability, generality, and convergence in optimizing multi-agent systems, PGD-based algorithms have been continuously improved, such as the regularized primal–dual subgradient method that can deal with non-separable objectives and constraints [60], shrunken primal–dual subgradient that eliminates the regularization errors [82], and shrunken primal-multi-dual subgradient that achieves two-facet scalable *w.r.t.* both the network dimension and the agent population size [55].

3.1.4. Multi-agent reinforcement learning

Learning-aided approaches, especially multi-agent reinforcement learning (MARL), are efficient for data-driven decision-making for power systems with proliferating DERs [126]. Mathematically, the decision-making is formulated into a *Markov Decision Process* (MDP), defined by the state space $\mathcal{S}$, action space $\mathcal{A}$, the transition probability function $\mathbb{P}(\cdot|s,a)$ that maps a state–action pair $(s,a) \in \mathcal{S}\times\mathcal{A}$ to a distribution on the state space, and the reward function $r(s,a)$. The agents aim to find an optimal policy π^* that maximizes the expected infinite horizon discounted reward $J(\pi)$, defined by [127]:

$$\pi^* \in \arg\max_{\pi} J(\pi) = \mathbb{E}_{s_0\sim\mu_0}\mathbb{E}_{\pi}\sum_{t=0}^{\infty}\gamma^t r\left(s_t,a_t\right) \tag{24}$$

where $\mathbb{E}$ denotes the expectation, s_0 is drawn from an initial state distribution μ_0, a_t is taken according to the policy π, $\gamma^t \in (0,1)$ denotes the discounting factor for the future rewards at time t. By interacting with the environment, RL agents learn the optimal policy without the knowledge of the model, i.e., via the transition probability and the reward function.

In MARL-based DER control, various grid components, such as generators, controllers, or local operators, can act as independent agents that operate within the grid environment. In MARL, the $\hat{i}$th agent takes an action $a_t^{\hat{i}} \in \mathcal{A}_{\hat{i}}$, given the state s_t, and receives a reward $r_t^{\hat{i}}(s_t,\{a_t^{\hat{i}}\}_{\hat{i}\in I})$, then the system state s_t transits into s_{t+1}. In power system applications, the states can include currents or voltages at different buses, real and reactive power demands, line flows, the status of DERs (e.g., battery energy level), transformer tap positions, etc. The actions can be taken on adjusting active/reactive power outputs, changing transformer tap settings, and reconfiguring network topology, etc.

Based on the information exchange pattern between agents and the SO or coordinator, MARL algorithms can also be categorized into three representative types as presented in Fig. 2, including *centralized* (also referred to as centralized training with decentralized execution), *decentralized*, and *distributed* structures (also referred to as decentralized setting with networked agents), see [128] for more details. Scalable MARL methods are powerful and promising tools for controlling DERs in large-scale power system networks with high-dimensional data streams [129–131]. However, MARL-based methods commonly face high computational complexity and slow convergence in large-scale systems due to the curse of dimensionality and exploration–exploitation trade-offs. Besides, coordination between agents is challenging in dynamic power systems, especially in partially observable environments. Another future direction involves addressing the requirement for extensive training data, as learned policies may not generalize well to new scenarios, such as cyber and physical attacks in power systems [132].

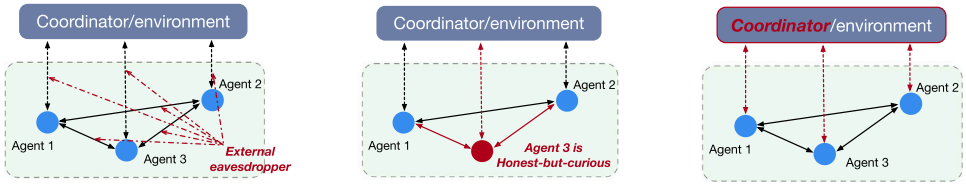
3.2. Privacy leakages

The acquisition, processing, and transmission of private customer data (e.g., energy consumption patterns, demographic data, locations, and regional statistics) are generally required to achieve grid services and improve customer satisfaction (e.g., billing, load monitoring, and demand response [63–65]). However, unauthorized usage of private data can lead to privacy leakages and malicious manipulation of the system [133,134]. For example, smart metering data can provide highly precise real-time information about household appliance energy usage, which could potentially be used to infer human activities within the home [135].

To ensure the warranted use of private information from all stakeholders, it is crucial to synthesize privacy preservation techniques into the design of scalable DER control strategies. Toward this goal, we summarize the typical adversaries/threats in multi-agent computing frameworks, including external eavesdroppers, honest-but-curious agents, and the SO and/or coordinators/aggregators, each representing a distinct type of threat with different attack vectors. By examining these three adversaries, we cover a broad spectrum of external, internal, and hierarchical privacy threats in multi-agent systems, helping guide the design of privacy-preserving frameworks in different multi-agent operational scenarios.

3.2.1. External eavesdroppers

External eavesdroppers are external adversaries who wiretap and intercept the communication channels of the power systems, e.g., data transmitted between smart meters and energy retailers. Through the acquisition of private customer and/or system information, external eavesdroppers can ‘observe’ the system status and exploit system vulnerabilities without tempering the system, causing adverse effects such as financial losses, reputational damage, and operational disruptions.



(a) An external eavesdropper. (b) An honest-but-curious agent. (c) The coordinator.

Fig. 4. Illustration of privacy breaches from *external eavesdroppers, honest-but-curious agents*, and *the coordinator* in a distributed three-agent information exchange structure: The *External eavesdroppers* wiretap all communication channels in the network; Agent 3 is an *Honest-but-curious agent* who attempts to infer other agents' private information based on its accessible information; *The Coordinator* might have access to agents' private data and/or critical system information.

3.2.2. Honest-but-curious agents

Honest-but-curious agents, also referred to as 'semi-honest agents,' are internal adversaries who follow the problem-solving procedures but are curious and try to infer the privacy of other participants. Being 'honest' is the primary characteristic of this type of adversary, indicating that it must follow the prescribed procedures and cannot send any falsified message. Despite their honest intentions, their curiosity may motivate them to steal others' private information based on their legitimately received messages and internal knowledge about the system. In contrast to external eavesdroppers, honest-but-curious agents cannot intercept communication channels. However, given their role as internal participants, they present a more significant challenge due to their privileged internal access.

3.2.3. The system operator and/or coordinators/aggregators

The system operator (SO)/coordinators/aggregators are usually responsible for ensuring the reliable operation of power grids. Therefore, these roles often have access to critical system information, such as network topology, protection settings, and historical demand data. Even though the SO and/or coordinators/aggregators are typically perceived as trustworthy, a dishonest or corrupted SO/coordinator/aggregator can ultimately result in the privacy compromise of the entire system. On the one hand, the SO/coordinators/aggregators may attempt to learn the DERs' decision variables by conveniently collecting and analyzing the acquired and belonged data. On the other hand, consumers and prosumers are often reluctant to disclose personal private information to any third party.

Fig. 4 shows the potential privacy breaches caused by the aforementioned three types of adversaries, exemplified in a distributed information exchange structure with three agents. To summarize, privacy protection emphasizes adversarial scenarios where all participants adhere to the algorithm/protocol steps but try to get insights into the system or agent information. These adversaries are often referred to as *passive* adversaries, meaning that each participant must not alter input variables or parameters and must accurately compute the outputs based on the algorithm design because they wish to learn the correct results. Therefore, this paper focuses on reviewing scalable and privacy-preserving multi-agent frameworks in the presence of only passive adversaries. More details on *passive* and *active* adversaries can be referred to Remark 1.

Remark 1. In privacy-aware and cybersecure computing, two primary types of adversaries can be categorized based on their divergence from the protocol, i.e., *passive* and *active* adversaries. The passive adversaries adhere to the protocol to obtain the correct results of its execution, but they also attempt to gather additional information about other participants' private information beyond what they are authorized to know. In contrast, active adversaries deviate from the protocol and tend to disrupt the computing process by modifying inputs, injecting malicious content, and tampering with intermediate results to compromise privacy or security. Therefore, passive adversaries are more stealthy and even harder to detect due to their stealthy actions. □

4. Privacy preservation techniques

Based on the representative privacy threats identified in Section 3.2, this section explores the details of both mainstream and emerging privacy preservation techniques for scalable multi-agent frameworks and demonstrates their applications in DER control problems (see Tables 2, 3, 4, and 5). Furthermore, we discuss potential research directions on applying different privacy preservation techniques for multi-agent-based control of DERs.

4.1. Differential privacy

The concept of *differential privacy (DP)*, first introduced by Dwork [166,167], captures the increased risk to one's privacy incurred by participating in a database. By adding random noise to the database, a curator (or SO) can release statistical information output of a data analysis result without compromising any individuals' privacy. Owing to its rigorous mathematical definition, DP has been a *de facto* standard in developing privacy preservation/protection techniques (Note that 'preservation' can imply a stronger standard than 'protection'. For example, privacy is not completely preserved by DP since it only limits privacy leakage and does not eliminate it. In this paper, we refer to the broad concept of 'protection' when using both terms). DP-based methods can quantify the privacy loss at a differential change in a database (i.e., adding or removing one entry), described by a privacy parameter ϵ that captures the privacy loss.

DP is a powerful privacy preservation architecture to make confidential data widely available for data analysis in the broad areas of artificial intelligence [168,169] and power and energy systems [135, 170,171]. To aid in understanding, the definition of ϵ-DP is given here [167]:

Definition 1. A randomized algorithm $\mathcal{K}$ with domain C is ϵ-differentially private if, for all data sets $c_1 \in C$ and $c_2 \in C$ differing on at most one element, and for any possible output S of the algorithm, the following inequality holds:

$$\mathbb{P}\left[\mathcal{K}\left(c_1\right) = S\right] \leq e^{\epsilon} \cdot \mathbb{P}\left[\mathcal{K}\left(c_2\right) = S\right] \tag{25}$$

where $\mathbb{P}$ denotes the probability and ϵ denotes a non-negative parameter. ■

The parameter ϵ in (25) controls the level of privacy, i.e., a smaller ϵ implies stronger privacy guarantees, as it limits the difference in the output probabilities between adjacent datasets. Definition 1 provides information-theoretic protection against the maximum amount of information an adversary can acquire about any specific agent in the database. Therefore, a curator can utilize a randomized function $\mathcal{K}(\cdot)$

Table 2
Differential-Privacy (DP)-based scalable and privacy-preserving methods.

Method	Reference	Problem	Structure	Adversaries	Key features
DP	[136]	Multi-agent convex programs	Decentralized	Honest-but-curious agents, the cloud, (ϵ, δ)-DP	1-Require a trusted cloud computer; 2-the cloud adds noise to data.
DP	[137]	EV charging control with solar PVs and ESSs	Centralized training with decentralized execution	(ϵ, δ)-DP	1-Multi-level deep RL structure for DERs; 2-agents cooperate to maximize the revenue of smart charging station.
DP	[138]	Consensus for multi-agent system	Distributed	Byzantine and malicious agents, ϵ-DP	1-A subset of agents is adversarial; 2-achieve resilient asymptotic consensus with correctness, accuracy and DP properties.
DP	[139]	Consensus for multi-agent system	Distributed	Honest-but-curious agents	1-Server-based randomized mechanism; 2-adversaries can observe the messages and states of the server and a subset of the clients.
DP	[66]	Convex constrained optimization	Distributed	Honest-but-curious agents	1-Individual objective function is kept private; 2-both input and output-perturbation methods.
DP	[64]	Optimal power flow	Distributed	An adversarial inference model	1-Develop an adversarial inference model for OPF; 2-introduce static and dynamic random perturbations of OPF sub-problem; 3- ϵ-DP.
DP	[140]	Optimal power flow	Distributed	A hypothetically strong adversary	1-DP projected subgradient; 2-non-differentiable concave objective function.
DP	[141]	EV charging control	Distributed	Adversaries and their collaboration with some users	1-Adopt adaptive composition theorem; 2-view the DP algorithm as stochastic gradient descent.
DP	[142]	Optimization with gradient tracking	Distributed	ϵ-DP	1-Add noise to the decision variables and the estimate of the aggregated gradient; 2-prove the impossibility of simultaneous exact convergence and DP preserving.
DP	[143]	Multi-agent systems	Distributed	ϵ-DP	1-Tailor gradient methods for differentially private distributed optimization; 2-based on static and dynamic consensus gradient methods.
DP	[144]	Distributed energy management	Distributed	(ϵ, δ)-DP, out-neighbors, eavesdroppers	1-A secret-function-based privacy-preserving algorithm; 2-nodes add zero-sum and exponentially decaying noise to the original data for communications.

DP: Differential privacy.

to mask agents' private data when releasing information. If (25) is satisfied, the released statistical information will not compromise the privacy of any individual agents.

The rigorous theoretical foundation of DP has led to extensive privacy protection applications in multi-agent systems. A series of pilot projects also demonstrate the potential of employing DP for DER control in power systems [63,64,135,140]. These DP-based methods add calibrated noise into smart meter data and/or into the computing process, therefore protecting the attributes of any single individual's smart meter readings. For example, DP-based methods have been integrated into scalable methods to achieve privacy protection while achieving grid-level and/or DER-level objectives, such as protecting consumers' smart meter data [63], power flow problems [64,140], and EV charging control [137]. Based on DP, Hale and Egerstedt [136] develop a privacy-preserving primal–dual optimization framework for multi-agent convex programs and solve it using the PGD. It keeps each agent's state trajectory private from all other agents and any external eavesdroppers. Han et al. [141] develop a distributed privacy-preserving optimization algorithm based on DP to preserve the privacy of the participating agents in constrained optimizations. To broaden the range of adversaries, Fiore and Russo [138] design a DP-based consensus algorithm for multi-agent systems where a subset of agents could be honest-but-curious. In [63], a DP-based privacy preservation algorithm is developed to protect consumers' smart meter data. Dvorkin et al. [64] develop an adversarial inference model based on DP that first questions the privacy properties of distributed OPF. Subsequently, the authors develop a differentially private variant of the ADMM to ensure information privacy during information exchanges between neighbors. This model is later extended in [140] for the distributed optimization of AC power flow problems. In [170], a DP-based obfuscation mechanism is proposed with guarantees of AC feasibility to protect the private parameters of transmission lines and transformers. Lee and Choi [137] develop a DP-based multilevel deep RL algorithm for privacy-preserving EV charging operations, ensuring optimized data privacy, revenue, and energy costs.

To summarize, DP has become a foundational principle in the privacy protection field, with wide-ranging power system applications evolving alongside recent advancements in scalable multi-agent frameworks. The potential of DP can be further explored from the following directions: (1) *Reduce the privacy-accuracy gap*. DP-based methods commonly suffer from loss of accuracy caused by the added noise. A balance between privacy and accuracy can be achieved via the design of carefully calibrated noise. (2) *Extension of DP for both privacy (passive adversaries) and security (active adversaries) scenarios*. When faulty agents maliciously deviate from the computing policy or network communication protocol, the effectiveness of DP in maintaining both privacy and security can be compromised [172,173]. The co-design of a privacy-preserving and cybersecure multi-agent framework is worth further investigation. (3) *Enhanced compatibility for the next generation of learning-aided methods*. DP has shown strong cohesion in preserving privacy for learning-aided methods, including training train neural networks for deep learning models [174], employing stochastic gradient descent for machine learning [175], reducing sample complexity with new expansion on DP [176]. The rapid evolution of DP also shows strong compatibility in addressing emerging privacy concerns in learning-aided approaches, such as the deployment of large language models in the electric power sector [177].

Table 3
Encryption–Decryption (ED)-based scalable and privacy-preserving methods.

Method	Reference	Problem	Structure	Adversaries	Key features
ED	[145]	Multi-agent cooperative optimization	Decentralized	Honest-but-curious agents, eavesdroppers, the system operator	1-Applicable on general primal–dual-based algorithms; 2-real-world experimental demonstration.
ED	[146]	Constrained decentralized optimization	Decentralized	Honest-but-curious agents, eavesdroppers	1-Integrate partially homomorphic cryptography; 2-applicable to average consensus problem.
ED	[147]	Smart meter data aggregation	Decentralized	External and internal adversaries	1-Boneh-Goh-Nissim public key cryptography; 2-consider both privacy, authentication, and integrity; 3-involve a trusted third party and an aggregator.
ED	[148]	Optimal dispatch of wind farms and shared ESSs	Decentralized	Other wind farms (Honest-but-curious)	1-Wind power uncertainty is handled through chance constraints; 2-include physical and virtual ESS components.
ED	[68]	Optimal power flow	Distributed	Honest-but-curious agents, external eavesdropper, the system operator	1-ADMM-based structure; 2-encrypt the dual update by the Paillier cryptosystem; 3-relax the augmented term of the primal update.
ED	[20]	Projected gradient-based algorithm	Distributed	Honest-but-curious agents, eavesdroppers, the system operator	1-Based on secure multiparty computation; 2-develop private and public key secure computation algorithms.
ED	[67]	Average consensus	Distributed	Honest-but-curious agents	1-Assume the presence of a trusted node; 2-privacy preservation via multiple encrypted ratio consensus iterations.
ED	[149]	Distributed economic dispatch of microgrids	Distributed	Honest-but-curious nodes, eavesdroppers	1-Coordinate the power outputs of distributed generators; 2-based on Paillier cryptosystem; 3-converge to the optimal solution under finite quantization levels.
ED	[150]	IoT-based active distribution network	Distributed	Eavesdroppers	1-Homomorphically encrypted energy management system for economic coordination and power sharing; 2-preserve privacy of distributed generators and customers' loads.
ED	[151]	Distributed learning	Distributed	Up to $N-1$ colluding parties	1-Enable the privacy-preserving execution of the cooperative gradient descent; 2-build on a multi-party fully homomorphic encryption scheme.
ED	[152]	Quadratic optimization problem	Distributed	Semi-honest colluding parties (agents coalitions, cloud coalitions, target node coalitions)	1-Protect privacy-sensitive objective function and constraints; 2-privacy guarantees are analyzed using zero-knowledge proof.

ED: Encryption–decryption.

Table 4
Secret Sharing (SS)-based scalable and privacy-preserving methods.

Method	Reference	Problem	Structure	Adversaries	Key features
SS	[153]	Partitioned DER control	Decentralized	Server (the resource operator), other agents	1-Ensure client privacy and system integrity; 2-applicable on resource constrained embedded systems.
SS	[21]	Average consensus	Distributed	Honest-but-curious agents	1-Achieve security in clique-based networks; 2-allow weaker model of active attacks.
SS	[69]	Multi-agent cooperative optimization	Distributed	Honest-but-curious agents, eavesdroppers	1-Coordinate EVs to achieve overnight valley filling; 2-applicable to projected gradient-based algorithms.
SS	[154]	Average consensus	Distributed	Honest-but-curious agents, eavesdroppers	1-Agents reach an agreement while keeping their states private until finalized; 2-resistant to the collusion of any neighbors.
SS	[70]	Multi-party collaborative optimization	Distributed	Honest-but-curious agents	1-Exchange shares between agents; 2-decomposition and coordination among agents for convergence.
SS	[155]	Vehicle-to-grid communication infrastructure	Distributed	Honest-but-curious (aggregator, collusion of aggregators, anonymizer)	1-Schedule EV charge/discharge times; 2-protect users' traveling habits, battery level, and the amount of refilled energy.
SS	[156]	DER aggregation and control	Hierarchical	Honest-but-curious agents, external eavesdroppers	1-Develop a hierarchical DER aggregation and control framework; 2-privacy-preserving optimization based on SS with privacy protection guarantees.

SS: Secret sharing.

Table 5
Miscellaneous and emerging scalable and privacy-preserving methods.

Method	Reference	Problem	Structure	Adversaries	Key features
SD	[71]	Average consensus	Distributed	Honest-but-curious agents, eavesdroppers	1-Each agent decomposes its state into two substates and only one substate is visible to others; 2-achieve exact consensus.
SD	[157]	Dynamic average consensus	Distributed	Honest-but-curious agents, eavesdroppers	1-Agents cooperatively track the average of local time-varying reference signals; 2-convergence guaranteed.
SD	[158]	Distributed economic dispatch	Distributed	Honest-but-curious agents, eavesdroppers, ϵ-DP	1-SD is carried out at each iterative step; 2-hybrid of SD and addition of Laplacian noise.
SD	[159]	Average consensus	Distributed	Honest-but-curious agents, eavesdroppers	1-A push-sum algorithm with communication over directed graphs.
NI	[160]	Average consensus	Distributed	Maximum likelihood estimate	1-Provide exact mean square convergence rate; 2-characterize the covariance matrix of the maximum likelihood estimate.
NI	[161]	Average consensus	Distributed	Honest-but-curious nodes	1-Ratio consensus under time-varying delays; 2-exact average; 3-use constant positive weights and adding an offset.
NI	[162]	Economic dispatch	Distributed	Eavesdropper	1-A privacy-preserving distributed optimization algorithm over time-varying directed communication networks; 2-add conditional noise to the exchanged states.
NI	[163]	Distributed signal processing	Distributed	Honest-but-curious agents, eavesdropper	1-Use subspace perturbation for privacy-preserving distributed optimization; 2-insert noise in the non-convergent subspace through the dual variable; 3-preserve accuracy.
GC	[164]	Secure multi-party computation	(N/A)	Semi-honest adversary (coalition of at most $\lfloor n/2 \rfloor$ corrupt players)	1-Compile the function into a description as a Boolean circuit; 2-perform a distributed evaluation of the circuit while revealing nothing else but the result of the function.
GC	[165]	Secure multi-party computation	(N/A)	Semi-honest adversary	1-Generate and optimize compressed Boolean circuits; 2-provide scalable emulations via sequential circuit description.

(N/A): Not applicable SD: State decomposition NI: Noise injection GC: Garbled circuit.

Remark 2. The DP technique can be categorized into global DP and local DP depending on whether the server (e.g., SO/coordinator/aggregator) can be trusted during the computing process. In global DP, privacy is maintained by adding noise at the central server level (e.g., database query), while in local DP, privacy is preserved by individuals before sending any raw data to the central server (e.g., adding noise to smart meter data). In practice, choosing between global and local DP depends on the use case and the level of trust in the central server, i.e., global DP is common when a central server is trusted [136], while local DP is preferred when trust is an issue and individual-level privacy must be ensured [138]. Note that, the definition of centralized, distributed, and decentralized information exchange structures are categorized based on their communication patterns, i.e., how private information flows between different parties, while the categorization of DP reflects the trustworthiness of the central server. □

4.2. Cryptographic methods

The protection of privacy in multi-agent frameworks can also be achieved through the integration of cryptographic techniques. This section surveys *encryption–decryption-based* and *secret sharing-based* methods.

4.2.1. Encryption–decryption-based methods

Encryption–decryption (ED)-based methods utilize a cryptosystem that typically consists of three components: An encryption algorithm, a decryption algorithm, and key management. Specifically, a plaintext m is encrypted into a ciphertext $\mathcal{E}(m)$ using an encryption function $\mathcal{E}(\cdot)$. By applying a decryption function $D(\cdot)$ to the ciphertext, the original plaintext can be correctly retrieved as $m = D(\mathcal{E}(m))$. Fig. 5 shows the realization of secure communications using a cryptosystem. A sender (e.g., DER owner) sends certain sensitive plaintexts to a receiver (e.g., a coordinator) in the form of ciphertexts using a cryptosystem such that any party intercepting/eavesdropping on the communication channel only has access to the ciphertexts, instead of knowing the plaintexts.

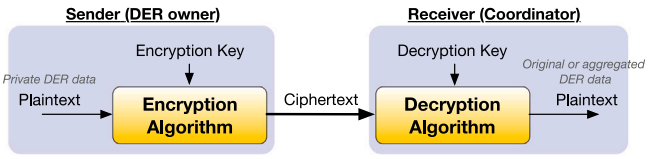


Fig. 5. Secure communications between a sender (DER owner) and a receiver (Coordinator) using a cryptosystem.

Among various cryptosystems, homomorphic cryptosystems are well-suited for multi-agent computing and communications. Essentially, a homomorphic cryptosystem enables users to perform computations on encrypted data without having to decrypt it first. The homomorphic properties are typically necessary for performing secure arithmetic operations in multi-agent systems [20,67,68,145,146,178], offering significant potential for power system applications, such as optimal power flows [68] and economic dispatch [148]. Homomorphic schemes can be classified according to the types of mathematical operations that can be performed on ciphertexts: (1) *Partially homomorphic* that supports either addition or multiplication operation, but not both simultaneously, and (2) *fully homomorphic* that concurrently support addition and multiplication operations. For a cryptosystem to be fully homomorphic, it needs to satisfy $D(\sum_{e=1}^{\bar{e}} \mathcal{E}(m_e)) = \sum_{e=1}^{\bar{e}} m_e$ and D

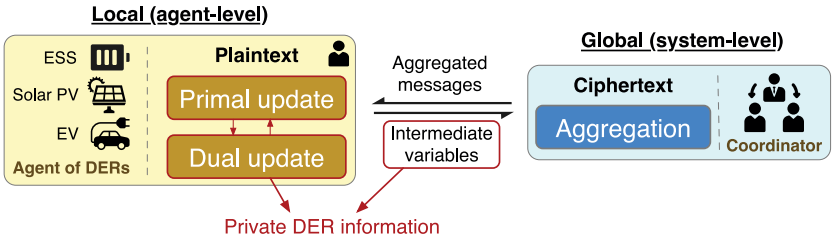


Fig. 6. Private information is calculated in plaintexts and transmitted in ciphertexts in a decentralized primal–dual computing framework [145].

$(\prod_{e=1}^{\bar{e}} \mathcal{E}(m_e)) = \prod_{e=1}^{\bar{e}} m_e$, where m_e denotes the eth plaintext and $\bar{e}$ denotes the total number of plaintexts.

The Paillier cryptosystem [179], for example, is partially homomorphic, allowing the addition of two ciphertexts and only the multiplication of a ciphertext by a plaintext. The Paillier cryptosystem is constructed by generating a set of public and private keys, where plaintexts are encrypted using the public key, and ciphertexts can be decrypted using the private key. The security of the Paillier cryptosystem relies on the decisional composite residuosity assumption (DCRA) [179], which is computationally hard due to the difficulty of distinguishing residues for large composite numbers, similar to the challenge of factoring them. The spectrum of adversaries in ED-based strategies can be proven from the secure multi-party computing perspective against different adversaries, such as honest-but-curious agents, external adversaries, and the SO/coordinator/aggregator [67,68,146,180,181].

Example 1 (*Integration of ED into PGD*)**.** Consider the PGD in Section 3.1.3, we give an example of integrating ED into PGD-based scalable multi-agent frameworks. As shown in Fig. 6, plaintexts (e.g., private charging/discharging profiles of ESSs) need to be calculated and transmitted iteratively between agents and the coordinator in a primal–dual-based computing scheme. By using ED, agents can encrypt private information (e.g., decision variables, private coefficients, subgradients, objective functions [20,145]) and then send encrypted intermediate variables to the coordinator only in the form of ciphertexts. The coordinator can access, aggregate, and compute ciphertexts based on the cryptosystem's homomorphic properties. The primal and dual updates can be executed in the space of ciphertexts. □

ED-based methods have been widely integrated within the design of scalable and privacy-preserving multi-agent frameworks. Lu and Zhu [20] first raise the question of how to securely compute certain given functions between the SO and a group of agents. Then, they develop homomorphic-encryption-based schemes to achieve secure multi-party computing in distributed projected gradient-based algorithms. Along with this research direction, a privacy-preserving decentralized multi-agent cooperative optimization paradigm is proposed in [145] by integrating additively homomorphic cryptosystem into decentralized optimization. In [146], a decentralized privacy-preserving algorithm based on the Paillier cryptosystem is developed to protect agents' intermediate variables in distributed systems. Hadjicostis et al. [67] develop a privacy-preserving AvgC method using the Paillier cryptosystem. It allows agents to reach a consensus on the average of their initial integer values while maintaining the confidentiality of these values in the presence of honest-but-curious agents.

In the power systems field, ED-based methods are well-suited for real-world implementation due to their compatibility with complex computing and communication structures. Moreover, the scalability and privacy protection capabilities of ED-based methods enhance the industry relevance of multi-agent frameworks for DER management, aligning them with electrical engineering standards such as IEC 62351, IEEE 1815-2012 (DNP3), and NERC reliability standards [33,182,183]. The theoretical findings of ED-based multi-agent frameworks have been translated into practical power system applications, such as the protection of sensitive customer load profiles, power system operational status, and operator control commands [68,147,184]. To preserve the private voltage and current measurements, Wu et al. [68] develop a privacy-preserving distributed OPF algorithm based on partially homomorphic cryptosystems. To eliminate the privacy concerns of economic dispatch problems in microgrids, a homomorphically encrypted algorithm is developed to achieve consensus without disclosing agents' private or sensitive state information [184]. The computing cost of ED-based methods is generally high due to their data size, making the design of computationally efficient cryptographic algorithms essential for scalable DER operations. He et al. [147] develop a computationally efficient data aggregation scheme based on public key cryptography to prevent the extraction of consumers' electricity consumption information against internal and external attackers.

ED-based methods continue to evolve as one of the mainstream privacy preservation measures, attracting significant attention for secure computing in multi-agent systems. Here are some future directions for ED-based methods: (1) *Decrease the computing overhead.* The complexity of a cryptosystem, the key length, and the size of encrypted or decrypted data all largely impact the computing cost. Designing computationally efficient cryptographic algorithms is critical for enabling scalable and privacy-preserving DER operations [147]. (2) *Trustworthy key management.* In establishing and executing cryptographic protocols, participants must manage keys (initialize, update, rotate, or revoke) in a secure way. The leakage of keys can lead to direct corruption of a cryptographic scheme. Therefore, establishing trustworthy key management is essential for controlling DERs with tremendous end-users. (3) *Interoperability within industrial standards.* Cryptographic algorithms should be deployed in an interoperable way with modern electric engineering standards. There is also the need for standardized cryptographic practices that can be uniformly applied across various customers and vendors in the electric power sector.

4.2.2. Secret sharing-based methods

Secret sharing (SS) is a lightweight cryptographic protocol that can split a secret into multiple shares and distribute the shares among a group of participants. The essential idea behind SS is to ensure that the secret can only be reconstructed by combining an adequate number of shares. Meanwhile, any subset of shares smaller than a threshold yields no useful information about the secret. Shamir's SS [185] is a widely recognized method for SS, where the secret shares are generated using a polynomial. Specifically, Shamir's SS is developed based on the concept of polynomial interpolation, defined as [186]:

Theorem 1 (*Polynomial Interpolation*)**.** *Let* $\{(z_1, f_1), \ldots, (z_{\bar{d}}, f_{\bar{d}})\} \subseteq \mathbb{R}^2$ *be a set of points whose values of* z_d *are all distinct. Then, there exists a unique polynomial* $f^{(\bar{d}-1)}$ *of degree* $\bar{d}-1$ *that satisfies* $f_d = f^{(\bar{d}-1)}(z_d), \forall d = 1, \ldots, \bar{d}$. ■

Theorem 1 states that a minimum number of $d+1$ points equal to the degree of the polynomial are required to reconstruct the secret. This ensures information-theoretic security, meaning that even if an adversary obtains some shares, it is impossible to reconstruct the secret unless they have acquired the *quorum* number of shares.

Example 2 (*Division of Shares and Secret Reconstruction in SS*)**.** The procedures of Shamir's SS [185], including the division of shares and the reconstruction of secrets, are given in Fig. 7.

Representatively, Shamir's SS can be executed in three steps: *(1) Polynomial generation:* A manager (secret holder) constructs a random polynomial $f(z) = s + c_1 z + \cdots + c_{\bar{d}-1} z^{\bar{d}-1}$, where s denotes the secret, the coefficients $c_1, \ldots, c_{k-1}$ are randomly chosen from a uniform distribution in an integer field $\mathbb{E} \triangleq [0, e)$, where e denotes a large prime number; *(2) Division of shares:* The manager computes the shares with a non-zero integer input and obtains the output, e.g., set $i = 1, \ldots, n$ to retrieve $\mathrm{S}_i = (i, f(i) \pmod e)$. Then, it distributes the share S_i to the ith agent; *(3) Secret reconstruction:* Therefore, based on Theorem 1, at least $\bar{d}$ points are needed to reconstruct the polynomial and calculate the secret s.

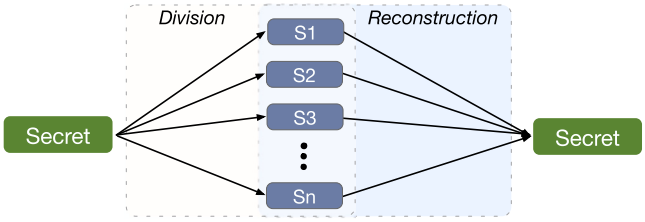


Fig. 7. An illustration of Shamir's secret sharing, showing the division of shares and the secret reconstruction process.

The efficient division of shares and reconstruction of secrets make SS highly suitable for privacy-preserving applications in multi-agent systems, particularly protecting privacy for controlling grid-edge energy resources in power systems, including electricity theft detection [187] and vehicle-to-grid integration [69,155]. Adopting SS, Nabil et al. [187] design a privacy-preserving detection scheme to identify electricity theft from malicious consumers. Only masked meter readings from consumers are collected and sent to the SO, therefore preventing data leakage. In [69], an SS-based cooperative EV charging control protocol is developed to achieve overnight valley filling without compromising the privacy of EV owners' charging profiles. The distributed protocol enjoys high computation efficiency and accuracy. In [155], a privacy-preserving communication protocol based on SS is proposed for vehicle-to-grid integration. The proposed protocol ensures that the existing battery charge level, the quantity of replenished energy, and the duration of EVs being plugged in remain undisclosed to aggregators.

To summarize, as a threshold scheme based on polynomials and finite geometries, Shamir's SS is well-suited for secure computation and key sharing in cryptographic applications among multiple stakeholders. Some potential future directions include: (1) *Homomorphic SS*. Combining SS with homomorphic properties allows computations to be performed on the shared data without revealing the secret. It is worth investigating efficient homomorphic operations within the SS framework for privacy-preserving computing in scalable multi-agent systems. (2) *Threshold cryptography in dynamic environments*. Traditional SS requires a predefined number of participants. However, real-world power system applications often involve dynamic groups and changing environments. Research could focus on adapting SS to handle dynamic groups, where agents can join or leave without compromising the shared secret. (3) *Power system applications*. Future research could focus on how SS can be adapted in different power system communication topologies, such as federated, distributed, and decentralized mechanisms.

4.3. Other miscellaneous and emerging methods

4.3.1. State decomposition

Wang [71] initiates the concept of state decomposition (SD) that can achieve AvgC while protecting the privacy of all participating agents. In SD, an agent decomposes its state into two distinct sub-states, with only one substrate visible to others, thus protecting the true original state. In contrast to DP-based methods that rely on adding additional noise, SD ensures convergence of the AvgC to the desired value without any accuracy error. Subsequently, the authors also extend SD on a dynamic consensus algorithm of multi-agent systems [157].

The establishment of SD has led to critical research outcomes that can guarantee the convergence of AvgC to the exact desired value. Inspired by SD, Wang et al. [188] develop a privacy-preserving consensus algorithm where each agent is decomposed into homologous subagents based on the number of its neighbors. The homologous subagents exchange information directly, while the information interaction between non-homologous subagents is encrypted by homomorphic cryptography. In [22], an SD mean-subsequence-reduce algorithm is designed to address privacy preservation in the resilient consensus of discrete-time multi-agent systems. The designed method considers the worst-case malicious behaviors against active adversarial agents who may update their state values in a completely arbitrary way. To summarize, SD-based approaches can effectively eliminate numerical errors caused by the accuracy-privacy trade-off. Future research could focus on extending SD-based approaches from AvgC to other scalable multi-agent frameworks and inspect their applications on DER control problems.

4.3.2. Noise injection

Analogous to DP, noise injection (NI) or perturbation-based methods add random noise/offsets to the private data to ensure privacy-preserving computing and communications. Typical injected noise processes include independent and exponentially decaying Laplacian noise [163], Gaussian noise [161,189,190], and certain conditional noise [162].

Apart from privacy, accuracy and algorithm efficiency are two important attributes that are often considered in designing NI-based methods. In [163], a subspace perturbation method is developed to achieve privacy-preserving distributed optimization with a focus on circumventing the privacy and accuracy trade-off. Charalambous et al. [161] design a privacy-preserving ratio consensus algorithm that can converge to the exact average of the nodes' initial values, even in the presence of bounded time-varying delays. In [189], a privacy-preserving transmission scheduling strategy is proposed to defend against eavesdropping, which demonstrates the correlation between the optimal transmission decision and the intensity of the injected noise. To summarize, NI-based methods aim at overcoming the algorithm efficiency limitations and lifting the privacy-accuracy trade-offs. Notably, emerging NI-based methods have demonstrated the potential to reduce computing and communication overhead. Future research could investigate how varied NI methods can further improve algorithm performance to a new level.

4.3.3. Garbled circuit

Hardware-based methods such as Boolean/arithmetic circuits can both be utilized to achieve secure computing between multiple parties [164]. The classic garbled circuit (GC) is initially proposed by Yao in [191] to address the secure two-party computing using Boolean circuits. As a cryptographic technique, GC protocol enables secure evaluation of a function expressed as a Boolean circuit composed of binary gates. In this process, the inputs and outputs of each gate are masked, ensuring that the party evaluating the GC cannot access any information about the inputs or intermediate results during the function's evaluation, thereby securing against honest-but-curious adversaries.

As shown in [192], Boolean formulas can be garbled in a privacy-free setting, where no ciphertexts are produced. To improve computing efficiency, a GC accelerator and compiler are developed in [193] to reduce computing overheads in practical privacy-preserving computations. Songhori et al. [165] design a sequential circuit description tool for generating and optimizing compressed Boolean circuits used in secure computation, such as Yao's GC [191]. GC-based methods demonstrate effectiveness in supporting confidential computing, controlling data usage, and processing arbitrary functions. However, GC-based approaches with affordable bitwise computations for binary operation-oriented applications in power systems are still in early development. Hardware-based methods are less susceptible to certain types of software vulnerabilities (e.g., malware or hacking attacks), making them a valuable complement or alternative to software-based power system applications. Therefore, the integrated design of hardware-software methods for enhanced privacy protection and cybersecurity is a viable future research direction.

4.4. Pilot projects and impacts

The *DataGuard Energy Data Privacy Program (DataGuard)* released by the U.S. Department of Energy's Office of Electricity [194] addresses the associated privacy concerns between utilities, consumers, and vendors. It requires a comprehensive approach to enhancing consumers' security, tackling identity theft, and improving privacy. The reviewed comprehensive privacy preservation techniques hold huge potential for addressing privacy challenges in pilot DER projects at scale. In what follows, we give some real-world DER projects that encounter privacy concerns. The U.S.'s *Xcel Energy Wind and Solar Program* [195] integrates renewables for consumers to offset carbon footprints. It involves collecting detailed operational data from consumers that can raise risks of unauthorized access to sensitive generation and consumption patterns. The flagship *Horizon Europe Program* funded by the *European Union* [196], which emphasizes smart grid integration of DERs and citizen-led initiatives (e.g., community energy projects). Privacy breaches in data management and sharing among different stakeholders can increase the risks of customer data misuse. Another example is the U.K.'s *Open Networks Project* [197], which aims to harmonize DER visibility information through consistent data flow from DERs to distribution network operators. The project addresses the potential privacy breaches associated with the exposure of DER data during information exchange between stakeholders, necessitating the adoption of privacy-preserving and scalable information exchange structures reviewed in the paper.

To summarize, pilot DER projects have demonstrated the importance of addressing privacy and scalability challenges and the potential of applying surveyed approaches, such as scalable DP-, ED-, and SS-based methods. These reviewed methods expect to mitigate privacy risks with broad impacts associated with internal, external, and hierarchical adversaries, therefore highlighting their applications for pilot large-scale DER projects.

5. Future directions on scalable and privacy-preserving DER control

With the increasing penetration of DERs, advanced scalable multi-agent control, optimization, and learning frameworks have been developed to adapt to DER-rich power systems. These advancements largely enhance system scalability but also exacerbate the power system's vulnerability to new privacy breaches and security threats. In this section, we extrapolate new approaches for future scalable, privacy-aware, and cybersecure pathways to unlock the full potential of DERs, as well as control, optimize, and learn generic multi-agent-based cyber–physical systems.

5.1. Improving accuracy, privacy, and algorithm efficiency

Enhancing accuracy, privacy, security, and the efficiency of computing and communication is a key research priority in the design of scalable and privacy-preserving multi-agent frameworks. Admittedly, scalability can be achieved via distributed and decentralized structures that enable parallel computing and communications across agents. However, the local computing costs and agent-to-agent or agent-to-coordinator communications can still be high to pose algorithm efficiency challenges. For example, in distributed settings, it is crucial to explore accelerated algorithm convergence with reduced communications, such as when each agent interacts with only a limited number of its neighbors, while in decentralized structures, agents should minimize dependence on the coordinator to efficiently manage resource constraints, especially in situations involving node failures, network partitions, or malicious attacks.

For example, DP-based methods quantify privacy risks using a rigorous mathematical framework, but they inevitably suffer from the loss of accuracy due to the added noise. Research efforts have been made to limit or eliminate the privacy-accuracy trade-offs in DP-based approaches. Nozari et al. [66] develop a DP-based distributed functional perturbation framework that bounds the error between the perturbed and true optimizers. This methodology permits the utilization of any distributed algorithm to solve optimization problems on noisy functions while protecting agents' private objective functions. In [23], a DP-based distributed stochastic approximation-type algorithm is designed to preserve privacy in solving stochastic aggregative games. Mini-batch methods are used to decrease the influence of added privacy noise on the algorithm's performance.

In contrast to DP, ED-based methods can attain higher precision at the cost of extra computing loads and increased communication. This is because ED-based strategies often need to transform real numbers into integers and then compute on large integers with large key sizes, e.g., 1024-bit key size in Paillier's key generation. The intensive mathematical calculations on the large ciphertexts (i.e., encrypting and decrypting data) can also result in communication latency. Compared to ED-based techniques, SS-based methods simplify key management by allowing participants to only manage shares rather than a complex set of keys. SS-based schemes primarily rely on polynomial interpolation and simple arithmetic operations over finite fields, which is less computationally expensive. However, SS-based methods can demand more frequent communications when exchanging shares, especially within multi-agent frameworks. Apart from software-based methods, hardware-based strategies such as GC are also viable in achieving privacy-preserving data analysis, private information retrieval, and secure multi-party computation. Despite efforts made to mitigate computing overhead, GC's outlook still needs further exploration considering other factors, e.g., low usability and scalability in regenerating circuits. Other emerging obfuscation tools such as NI, are up-and-coming to lift the privacy-accuracy trade-off. To summarize, while there has been great enthusiasm toward balancing or eliminating the trade-offs between accuracy, privacy, security, computing and communication efficiency, developing scalable and privacy-preserving algorithms with comprehensively enhanced performance still requires future efforts.

5.2. Establishing trustworthiness across fields

The integration of DERs is creating profound impacts on the electric power sector, fostering a highly interconnected community with *everything as a grid* [198]. The highly connected nature of modern power grids requires the establishment of strengthened 'trustworthiness' across different fields. The definition of *trustworthiness across fields* is summarized into three key aspects: (1) trustworthy data and features for the artificial intelligence (AI) model; (2) trustworthy analytical results for the DER control; and (3) trustworthy human-machine interaction for the system management.

Trustworthy data and features for the AI model. As power grids transition alongside the rapid progress of AI, the broad capabilities of AI offer new possibilities for consolidating DERs. However, the need to collect, process, and transfer sensitive system and customer data for fine-tuning learning models can raise new technical, economic, and ethical risks. To address this, the *U.S. National Institute of Standards and Technology* has developed a comprehensive AI risk management framework [199] related to individuals, organizations, and society. Therefore, it is essential to securely collect accurate, unbiased, and representative real-world data for AI models to make fair decisions without violating the privacy and security of the system. *Trustworthy analytical results for the DER control*. The privacy and cybersecurity challenges in the AI field are propagating into the power energy field, e.g., privacy challenges in natural language processing based on machine learning in the electric energy sector [177] and power system fault diagnosis within quantum computing field [200]. Majumder et al. [177] point out that privacy and cybersecurity emerge as a paramount concern when integrating large language models (LLMs) into electric energy systems. Besides, emerging PGD-based adversarial attacks can cause devastating attack results for LLMs [201], resulting in catastrophic failures if deployed in power systems. Moreover, by leveraging the principles of quantum mechanics, quantum computing can break widely-used cryptographic systems by making it possible to factor large numbers efficiently. Zhou and Zhang in [202] show the potential of quantum machine learning in providing resilient and secure decision-making of large-scale power systems. The quantum-inspired methods can enhance security via quantum key distribution [203], resist quantum computing attacks, and open new possibilities for data transfer and information processing, e.g., quantum cryptography [204] and quantum communication [205]. Therefore, there is a need to incorporate trustworthy analytical results from various fields to benefit the power and energy community. *Trustworthy human-machine interaction for the system management*. Enhancing the safety and security of human-machine interaction is also critical for making decisions to manage the DER-rich power systems. It requires consideration of coupled cyber–physical power system architecture [206], the interconnected industrial networks [207], and the stochastic human factors on DER control, such as from the behavioral science perspective.

5.3. Developing zero-trust standards

The reviewed methods address system scalability and privacy challenges in DER-rich power systems. However, there remains a significant need to tackle the escalating vulnerabilities associated with privacy breaches and security threats. With the growing demands for data confidentiality and system integrity, holistic privacy-aware and cybersecure frameworks capable of addressing both passive and active adversaries are needed. Consequently, the development of privacy-aware and cybersecure multi-agent frameworks must integrate various access control, communication, computation, detection, and mitigation techniques. Toward this goal, we explore the concept of *zero-trust (ZT)* to highlight efforts aimed at achieving comprehensive privacy and security standards. ZT is initially proposed to protect resources under the assumption that trust is never implicitly granted [208]. Within ZT, the range of cybersecurity paradigms shifts from static network-based perimeters to a focus on users, assets, and resources. Moreover, ZT can consolidate a set of guiding principles for workflow, system design, and operations to improve the security posture to any sensitivity level. As a generic network security model, ZT architecture secures a system's overall information security, including applications such as cyber supply chain security [209], secure cloud computing [210], and the industry internet of things [211].

The increasing adoption of DERs and the ever-complicating adversarial landscape in power systems highlight the need for a holistic privacy-aware and cybersecure framework. Ultimately, it should provide multi-layer internal, external, and hierarchical protection against existing and unforeseen passive and active adversaries, even in the failure of multiple agents or leaders (e.g., the SO, coordinators, and aggregators). Research efforts have identified the possibility of deploying *zero-trust architectures (ZTAs)* to manage grid-tied resources in various locations, such as commercial, residential, or governmental areas [212–215]. In [213], ZTA is applied to virtual power plants to achieve enhanced protection of virtual power devices. Zanasi et al. in [214] explore the application of ZTA in industrial systems to minimize cyber risks. In [215], ZT is applied to enforce identity and access management, securing data communication between EV chargers and cloud platforms while avoiding user-level privacy leakage.

Despite the established fundamentals of *ZT*, the deployment of ZTAs in large-scale DER control problems is still in its early stages. The challenges include the costs associated with upgrading legacy power system infrastructure, interoperability issues due to varying protocols and standards, potential communication latency, and the significant investment required. In the future, leveraging high-standard privacy and security concepts to develop privacy-aware and cybersecure frameworks that are deployable for power systems will be a challenging research focus.

6. Conclusion

With the increasing integration of distributed energy resources (DERs) in large-scale power grids, many power system control, optimization, and learning problems require scalable solutions within a multi-agent framework. Besides, the frequent and mandated exchange of sensitive information among agents makes the entire multi-agent system vulnerable to privacy breaches. These privacy breaches can cause privacy and cybersecurity risks to threaten the function of the entire power grid. Therefore, it is crucial to protect privacy and achieve scalability when deploying multi-agent frameworks for DER control, targeting for greater sustainability, security, and resilience.

This paper has provided a comprehensive review of recent advancements in scalable and privacy-preserving multi-agent frameworks from multi-disciplinary research areas, highlighting their applications for controlling DER in power systems. It has offered a systematic summary of multi-agent frameworks based on their scalable computing and information exchange structures, illustrating their applications in DER control problems across different disciplines. This review has identified internal, external, and hierarchical types of adversaries in multi-agent-based DER control problems, including *external eavesdroppers*, *honest-but-curious agents*, and *system operators and/or coordinators/aggregators*. Regarding privacy protection, this paper has further explored mainstream privacy preservation techniques, such as *differential privacy*, *encryption–decryption-based cryptosystem*, and *Shamir's secret sharing*, along with other and emerging methods such as *state decomposition*, *noise injection*, and *garbled circuits*. Recent advancements have underscored the significant scalability and privacy preservation capabilities of these approaches for the electric power sector. Finally, this paper has discussed three potential research directions on *improving accuracy, privacy, and algorithm efficiency*, *establishing trustworthiness across fields*, and *developing zero-trust standards*.

CRediT authorship contribution statement

Xiang Huo: Writing – original draft, Methodology, Investigation, Conceptualization. **Hao Huang:** Writing – review & editing, Methodology, Investigation, Conceptualization. **Katherine R. Davis:** Writing – review & editing, Supervision, Resources, Funding acquisition. **H. Vincent Poor:** Writing – review & editing, Supervision, Resources, Funding acquisition. **Mingxi Liu:** Writing – review & editing, Supervision, Resources, Funding acquisition.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: The author Dr. Mingxi Liu is on the Young Editorial Board of *Advances in Applied Energy*.

Acknowledgments

The authors would like to acknowledge the National Science Foundation, USA under Grant 2220347 and Grant 2145408, the US Department of Energy under award DE-CR0000018 and award DE-EE0009658, and grants from Princeton University's School of Engineering and Applied Science, USA and Andlinger Center for Energy and the Environment, USA, for their support of this work.

Data availability

Data will be made available on request.

References

[1] National Renewable Energy Laboratory. Using Distributed Energy Resources. URL https://www.nrel.gov/docs/fy02osti/31570.pdf.
[2] Wang Q, Zhang C, Ding Y, Xydis G, Wang J, Østergaard J. Review of real-time electricity markets for integrating distributed energy resources and demand response. Appl Energy 2015;138:695–706.
[3] Lee S, Shenoy P, Ramamritham K, Irwin D. AutoShare: Virtual community solar and storage for energy sharing. Energy Inform 2021;4:1–24.
[4] Denholm P, Brown P, Cole W, Mai T, Sergi B, Brown M, Jadun P, Ho J, Mayernik J, McMillan C, et al. Examining supply-side options to achieve 100% clean electricity by 2035. Tech. rep., National Renewable Energy Laboratory; 2022.
[5] Akorede MF, Hizam H, Pouresmaeil E. Distributed energy resources and benefits to the environment. Renew Sustain Energy Rev 2010;14(2):724–34.
[6] Basak P, Chowdhury S, nee Dey SH, Chowdhury S. A literature review on integration of distributed energy resources in the perspective of control, protection and stability of microgrid. Renew Sustain Energy Rev 2012;16(8):5545–56.
[7] Energy Systems Integration Group. The transition to a high-DER electricity system. URL https://www.esig.energy/wp-content/uploads/2022/08/ESIG-DER-integration-US-initiative-report-2022.pdf.
[8] Panteli M, Mancarella P. Influence of extreme weather and climate change on the resilience of power systems: Impacts and possible mitigation strategies. Electr Power Syst Res 2015;127:259–70.
[9] Shi Q, Liu W, Zeng B, Hui H, Li F. Enhancing distribution system resilience against extreme weather events: Concept review, algorithm summary, and future vision. Int J Electr Power Energy Syst 2022;138:107860.
[10] Abdelmalak M, Benidris M. Enhancing power system operational resilience against wildfires. IEEE Trans Ind Appl 2022;58(2):1611–21.
[11] Habib HF, Lashway CR, Mohammed OA. A review of communication failure impacts on adaptive microgrid protection schemes and the use of energy storage as a contingency. IEEE Trans Ind Appl 2017;54(2):1194–207.
[12] Deng R, Xiao G, Lu R, Liang H, Vasilakos AV. False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey. IEEE Trans Ind Inf 2016;13(2):411–23.
[13] Lai C, Jacobs N, Hossain-McKenzie S, Carter C, Cordeiro P, Onunkwo I, Johnson J. Cyber security primer for DER vendors, aggregators, and grid operators. Tech. Rep., Vol. 12, Sandia National Laboratories; 2017.
[14] Fortune Business Insights. Distributed Energy Resource Management System Market, 2021–2028. URL https://www.fortunebusinessinsights.com/enquiry/request-sample-pdf/distributed-energy-resource-management-system-market-100825.
[15] Wood Mackenzie. US distributed energy resource (DER) outlook 2023. URL https://www.woodmac.com/reports/power-markets-us-distributed-energy-resource-der-outlook-2023-150135819/.
[16] US Department of Energy. Innovative Grid Deployment Liftoff. URL https://liftoff.energy.gov/innovative-grid-deployment/.
[17] Radhakrishnan BM, Srinivasan D. A multi-agent based distributed energy management scheme for smart grid applications. Energy 2016;103:192–204.
[18] Wang S, Duan J, Shi D, Xu C, Li H, Diao R, Wang Z. A data-driven multi-agent autonomous voltage control framework using deep reinforcement learning. IEEE Trans Power Syst 2020;35(6):4644–54.
[19] Fan Z, Zhang W, Liu W. Multi-agent deep reinforcement learning-based distributed optimal generation control of DC microgrids. IEEE Trans Smart Grid 2023;14(5):3337–51.
[20] Lu Y, Zhu M. Privacy preserving distributed optimization using homomorphic encryption. Automatica 2018;96:314–25.
[21] Li Q, Christensen MG. A privacy-preserving asynchronous averaging algorithm based on Shamir's secret sharing. In: Proceedings of the European signal processing conference. A Coruña, Spain; 2019, p. 1–5.
[22] Zhang Y, Peng Z, Wen G, Wang J, Huang T. Privacy preserving-based resilient consensus for multi-agent systems via state decomposition. IEEE Trans Control Netw Syst 2022;10(3):1172–83.
[23] Wang J, Zhang J-F, He X. Differentially private distributed algorithms for stochastic aggregative games. Automatica 2022;142:110440.
[24] Lisovich MA, Mulligan DK, Wicker SB. Inferring personal information from demand-response systems. IEEE Secur Priv 2010;8(1):11–20.
[25] Greveler U, Glösekötterz P, Justusy B, Loehr D. Multimedia content identification through smart meter power usage profiles. In: Proceedings of the international conference on information and knowledge engineering. 2012, p. 1–8.
[26] Chin J-X, De Rubira TT, Hug G. Privacy-protecting energy management unit through model-distribution predictive control. IEEE Trans Smart Grid 2017;8(6):3084–93.
[27] General Data Protection Regulation. URL https://gdpr-info.eu.
[28] California Consumer Privacy Act. URL https://oag.ca.gov/privacy/ccpa.
[29] Consumer Data Protection Act. URL https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/.
[30] Texas Data Privacy and Security Act. URL https://capitol.texas.gov/tlodocs/88R/billtext/pdf/HB00004F.pdf#navpanes=0.
[31] National Institute of Standards and Technology. NIST IR 7628 Rev.1 Guidelines for Smart Grid Cybersecurity. URL https://csrc.nist.gov/pubs/ir/7628/r1/final.
[32] Europe Commission. Data protection impact assessment for smart grid and smart metering environment. URL https://energy.ec.europa.eu/topics/markets-and-consumers/smart-grids-and-meters/data-protection-impact-assessment-smart-grid-and-smart-metering-environment_en.
[33] International Electrotechnical Commission. Cyber security: Understanding IEC 62351. URL https://www.iec.ch/blog/cyber-security-understanding-iec-62351.
[34] Zografopoulos I, Hatziargyriou ND, Konstantinou C. Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations. IEEE Syst J 2023.
[35] Tuyen ND, Quan NS, Linh VB, Van Tuyen V, Fujita G. A comprehensive review of cybersecurity in inverter-based smart power system amid the boom of renewable energy. IEEE Access 2022;10:35846–75.
[36] Ghiasi M, Niknam T, Wang Z, Mehrandezh M, Dehghani M, Ghadimi N. A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. Electr Power Syst Res 2023;215:108975.
[37] Hasan MK, Habib AA, Shukur Z, Ibrahim F, Islam S, Razzaque MA. Review on cyber–physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. J Netw Comput Appl 2023;209:103540.
[38] Ferrag MA, Maglaras LA, Janicke H, Jiang J, Shu L. A systematic review of data protection and privacy preservation schemes for smart grid communications. Sustainable Cities Soc 2018;38:806–35.
[39] Sebastian Cardenas DJ, Mukherjee M, Ramirez JE. A review of privacy in energy application. Tech. rep., Pacific Northwest National Laboratory; 2023.
[40] Nedic A, Ozdaglar A. Distributed subgradient methods for multi-agent optimization. IEEE Trans Autom Control 2009;54(1):48–61.
[41] Gan L, Topcu U, Low SH. Optimal decentralized protocol for electric vehicle charging. IEEE Trans Power Syst 2012;28(2):940–51.
[42] Zhang L, Jabbari F, Brown T, Samuelsen S. Coordinating plug-in electric vehicle charging with electric grid: Valley filling and target load following. J Power Sources 2014;267:584–97.
[43] Sultana U, Khairuddin AB, Aman M, Mokhtar A, Zareen N. A review of optimum DG placement based on minimization of power losses and voltage stability enhancement of distribution system. Renew Sustain Energy Rev 2016;63:363–78.
[44] Khan I. Importance of GHG emissions assessment in the electricity grid expansion towards a low-carbon future: A time-varying carbon intensity approach. J Clean Prod 2018;196:1587–99.
[45] Xiao X, Wang F, Shahidehpour M, Li Z, Yan M. Coordination of distribution network reinforcement and DER planning in competitive market. IEEE Trans Smart Grid 2020;12(3):2261–71.
[46] Akhter Q, Siddique A, Alqahtani SA, Mahmood A, Alam M, Mushtaq Z, Qureshi MF, Aslam W, Pathak PK. Efficient energy management for household: Optimization-based integration of distributed energy resources in smart grid. IEEE Access 2023;11:85716–27.
[47] Hu J, Shan Y, Yang Y, Parisio A, Li Y, Amjady N, Islam S, Cheng KW, Guerrero JM, Rodríguez J. Economic model predictive control for microgrid optimization: A review. IEEE Trans Smart Grid 2023;15(1):472–84.
[48] Chen Z, Li Z, Chen G. Optimal configuration and operation for user-side energy storage considering lithium-ion battery degradation. Int J Electr Power Energy Syst 2023;145:108621.
[49] Dommel HW, Tinney WF. Optimal power flow solutions. IEEE Trans Power Appar Syst 1968;(10):1866–76.

[50] Sun S, Haque KA, Huo X, Homoud Al L, Hossain-McKenzie S, Goulart A, Davis K. A reinforcement learning engine with reduced action and state space for scalable cyber–physical optimal response. 2024, arXiv preprint arXiv:2410.04518.

[51] Awad AS, El-Fouly TH, Salama MM. Optimal ESS allocation for load management application. IEEE Trans Power Syst 2014;30(1):327–36.

[52] Wu D, Yang T, Stoorvogel AA, Stoustrup J. Distributed optimal coordination for distributed energy resources in power systems. IEEE Trans Autom Sci Eng 2016;14(2):414–24.

[53] Wang T, O'Neill D, Kamath H. Dynamic control and optimization of distributed energy resources in a microgrid. IEEE Trans Smart Grid 2015;6(6):2884–94.

[54] Li N, Chen L, Low SH. Optimal demand response based on utility maximization in power networks. In: Proceedings of the 2011 IEEE power and energy society general meeting. Detroit, MI, USA; 2011, p. 1–8.

[55] Huo X, Dong J, Cui B, Liu B, Lian J, Liu M. Two-level decentralized-centralized control of distributed energy resources in grid-interactive efficient buildings. IEEE Control Syst Lett 2022;7:997–1002.

[56] Jian L, Zheng Y, Shao Z. High efficient valley-filling strategy for centralized coordinated charging of large-scale electric vehicles. Appl Energy 2017;186:46–55.

[57] Boyd S, Parikh N, Chu E. Distributed optimization and statistical learning via the alternating direction method of multipliers. Now Publishers Inc; 2011.

[58] Olfati-Saber R, Fax JA, Murray RM. Consensus and cooperation in networked multi-agent systems. Proc IEEE 2007;95(1):215–33.

[59] Bertsekas D, Tsitsiklis J. Parallel and distributed computation: Numerical methods. Athena Scientific; 2015.

[60] Koshal J, Nedić A, Shanbhag UV. Multiuser optimization: Distributed algorithms and error analysis. SIAM J Optim 2011;21(3):1046–81.

[61] Liu H, Hu Z, Song Y, Lin J. Decentralized vehicle-to-grid control for primary frequency regulation considering charging demands. IEEE Trans Power Syst 2013;28(3):3480–9.

[62] Zhang Q, Guo Y, Wang Z, Bu F. Distributed optimal conservation voltage reduction in integrated primary-secondary distribution systems. IEEE Trans Smart Grid 2021;12(5):3889–900.

[63] Gough MB, Santos SF, AlSkaif T, Javadi MS, Castro R, Catalão JPS. Preserving privacy of smart meter data in a smart grid environment. IEEE Trans Ind Inf 2022;18(1):707–18.

[64] Dvorkin V, Van Hentenryck P, Kazempour J, Pinson P. Differentially private distributed optimal power flow. In: Proceedings of the IEEE conference on decision and control. Jeju, Korea (South); 2020, p. 2092–7.

[65] Atmaca UI, Biswas S, Maple C, Palamidessi C. A privacy-preserving querying mechanism with high utility for electric vehicles. IEEE Open J Veh Technol 2024.

[66] Nozari E, Tallapragada P, Cortés J. Differentially private distributed convex optimization via functional perturbation. IEEE Trans Control Netw Syst 2016;5(1):395–408.

[67] Hadjicostis CN, Domínguez-García AD. Privacy-preserving distributed averaging via homomorphically encrypted ratio consensus. IEEE Trans Autom Control 2020;65(9):3887–94.

[68] Wu T, Zhao C, Zhang Y-JA. Privacy-preserving distributed optimal power flow with partially homomorphic encryption. IEEE Trans Smart Grid 2021;12(5):4506–21.

[69] Huo X, Liu M. Distributed privacy-preserving electric vehicle charging control based on secret sharing. Electr Power Syst Res 2022;211:108357.

[70] Tian N, Guo Q, Sun H, Zhou X. Fully privacy-preserving distributed optimization in power systems based on secret sharing. iEnergy 2022;1(3):351–62.

[71] Wang Y. Privacy-preserving average consensus via state decomposition. IEEE Trans Autom Control 2019;64(11):4711–6.

[72] Baran ME, Wu FF. Network reconfiguration in distribution systems for loss reduction and load balancing. IEEE Power Eng Rev 1989;9(4):101–2.

[73] Farivar M, Chen L, Low S. Equilibrium and dynamics of local voltage control in distribution systems. In: Proceedings of the 52nd IEEE conference on decision and control. 2013, p. 4329–34.

[74] Baran M, Wu FF. Optimal sizing of capacitors placed on a radial distribution system. IEEE Trans Power Deliv 1989;4(1):735–43.

[75] Chen X, Chao H, Shi W, Li N. Towards carbon-free electricity: A flow-based framework for power grid carbon accounting and decarbonization. 2023, arXiv:2308.03268.

[76] Wang S, Zhai J, Hui H. Optimal energy flow in integrated electricity and gas systems with injection of alternative gas. IEEE Trans Sustain Energy 2023;14(3):1540–57.

[77] Zamzam AS, Dall'Anese E, Zhao C, Taylor JA, Sidiropoulos ND. Optimal water–power flow-problem: Formulation and distributed optimal solution. IEEE Trans Control Netw Syst 2018;6(1):37–47.

[78] Unterluggauer T, Rich J, Andersen PB, Hashemi S. Electric vehicle charging infrastructure planning for integrated transportation and power distribution networks: A review. ETransportation 2022;12:100163.

[79] Shchetinin D, De Rubira TT, Hug G. On the construction of linear approximations of line flow constraints for AC optimal power flow. IEEE Trans Power Syst 2018;34(2):1182–92.

[80] Li X, Ma R, Gan W, Yan S. Optimal dispatch for battery energy storage station in distribution network considering voltage distribution improvement and peak load shifting. J Mod Power Syst Clean Energy 2020;10(1):131–9.

[81] Robbins BA, Domínguez-García AD. Optimal reactive power dispatch for voltage regulation in unbalanced distribution systems. IEEE Trans Power Syst 2015;31(4):2903–13.

[82] Liu M, Phanivong PK, Shi Y, Callaway DS. Decentralized charging control of electric vehicles in residential distribution networks. IEEE Trans Control Syst Technol 2019;27(1):266–81.

[83] Salgado R, Rangel Jr E. Optimal power flow solutions through multi-objective programming. Energy 2012;42(1):35–45.

[84] Mahmoud K, Yorino N, Ahmed A. Optimal distributed generation allocation in distribution systems for loss minimization. IEEE Trans Power Syst 2015;31(2):960–9.

[85] Ren H, Zhou W, Nakagami K, Gao W, Wu Q. Multi-objective optimization for the operation of distributed energy systems considering economic and environmental aspects. Appl Energy 2010;87(12):3642–51.

[86] Ma Z, Zou S, Liu X. A distributed charging coordination for large-scale plug-in electric vehicles considering battery degradation cost. IEEE Trans Control Syst Technol 2015;23(5):2044–52.

[87] Bordin C, Anuta HO, Crossland A, Gutierrez IL, Dent CJ, Vigo D. A linear programming approach for battery degradation analysis and optimization in offgrid power systems with solar energy integration. Renew Energy 2017;101:417–30.

[88] Fan T-H, Lee XY, Wang Y. Powergym: A reinforcement learning environment for volt-var control in power distribution systems. In: Proceedings of the 4th annual learning for dynamics and control conference. 2022, p. 21–33.

[89] Su X, Masoum MA, Wolfs PJ. Optimal PV inverter reactive power control and real power curtailment to improve performance of unbalanced four-wire LV distribution networks. IEEE Trans Sustain Energy 2014;5(3):967–77.

[90] Attarha A, Scott P, Thiébaux S. Affinely adjustable robust ADMM for residential DER coordination in distribution networks. IEEE Trans Smart Grid 2019;11(2):1620–9.

[91] Diekerhof M, Peterssen F, Monti A. Hierarchical distributed robust optimization for demand response services. IEEE Trans Smart Grid 2017;9(6):6018–29.

[92] Peng Q, Low SH. Distributed algorithm for optimal power flow on a radial network. In: Proceedings of the IEEE conference on decision and control. Los Angeles, CA, USA; 2014, p. 167–72.

[93] Yu L, Yue D, Tan Y, Zhang S, Yang Y, Dou C, Kuzin V. Online distributed coordination operation for grid-interactive efficient residential buildings. IEEE Trans Smart Grid 2023.

[94] Rivera J, Goebel C, Jacobsen H-A. Distributed convex optimization for electric vehicle aggregators. IEEE Trans Smart Grid 2016;8(4):1852–63.

[95] Olshevsky A, Tsitsiklis JN. Convergence speed in distributed consensus and averaging. SIAM J Control Optim 2009;48(1):33–55.

[96] Huang M, Manton JH. Coordination and consensus of networked agents with noisy measurements: Stochastic algorithms and asymptotic behavior. SIAM J Control Optim 2009;48(1):134–61.

[97] Amelina N, Fradkov A, Jiang Y, Vergados DJ. Approximate consensus in stochastic networks with application to load balancing. IEEE Trans Inform Theory 2015;61(4):1739–52.

[98] De Persis C, Weitenberg ER, Dörfler F. A power consensus algorithm for DC microgrids. Automatica 2018;89:364–75.

[99] Ma W-J, Wang J, Gupta V, Chen C. Distributed energy management for networked microgrids using online ADMM with regret. IEEE Trans Smart Grid 2016;9(2):847–56.

[100] Gebbran D, Mhanna S, Chapman AC, Verbič G. Multiperiod DER coordination using ADMM-based three-block distributed AC optimal power flow considering inverter volt-var control. IEEE Trans Smart Grid 2022;14(4):2874–89.

[101] Mak TW, Chatzos M, Tanneau M, Van Hentenryck P. Learning regionally decentralized AC optimal power flows with ADMM. IEEE Trans Smart Grid 2023;14(6):4863–76.

[102] Huo X, Liu M. Two-facet scalable cooperative optimization of multi-agent systems in the networked environment. IEEE Trans Control Syst Technol 2022;30(6):2317–32.

[103] Grimmer B. Provably faster gradient descent via long steps. SIAM J Optim 2024;34(3):2588–608.

[104] Wang Y, Qiu D, Teng F, Strbac G. Towards microgrid resilience enhancement via mobile power sources and repair crews: A multi-agent reinforcement learning approach. IEEE Trans Power Syst 2023;39(1):1329–45.

[105] Wang Z, Xiao F, Ran Y, Li Y, Xu Y. Scalable energy management approach of residential hybrid energy system using multi-agent deep reinforcement learning. Appl Energy 2024;367:123414.

[106] Ying D, Zhang Y, Ding Y, Koppel A, Lavaei J. Scalable primal-dual actor-critic method for safe multi-agent RL with general utilities. Adv Neural Inf Process Syst 2024;36:36524–39.

[107] Zhang Y, Qu G, Xu P, Lin Y, Chen Z, Wierman A. Global convergence of localized policy iteration in networked multi-agent reinforcement learning. Proc ACM Meas Anal Comput Syst 2023;7(1):1–51.

[108] DeGroot MH. Reaching a consensus. J Amer Statist Assoc 1974;69(345):118–21.

[109] Horn RA, Johnson CR. Matrix analysis. Cambridge University Press; 2012.

[110] Khazaei J, Miao Z. Consensus control for energy storage systems. IEEE Trans Smart Grid 2016;9(4):3009–17.

[111] Huang C, Weng S, Yue D, Deng S, Xie J, Ge H. Distributed cooperative control of energy storage units in microgrid based on multi-agent consensus method. Electr Power Syst Res 2017;147:213–23.

[112] Li Q, Gao DW, Zhang H, Wu Z, Wang F-y. Consensus-based distributed economic dispatch control method in power systems. IEEE Trans Smart Grid 2017;10(1):941–54.

[113] Ren W, Beard RW. Consensus seeking in multiagent systems under dynamically changing interaction topologies. IEEE Trans Autom Control 2005;50(5):655–61.

[114] Aysal TC, Oreshkin BN, Coates MJ. Accelerated distributed average consensus via localized node state prediction. IEEE Trans Signal Process 2008;57(4):1563–76.

[115] Thanou D, Kokiopoulou E, Pu Y, Frossard P. Distributed average consensus with quantization refinement. IEEE Trans Signal Process 2012;61(1):194–205.

[116] Gabay D, Mercier B. A dual algorithm for the solution of nonlinear variational problems via finite element approximation. Comput Math Appl 1976;2(1):17–40.

[117] Magnússon S, Weeraddana PC, Fischione C. A distributed approach for the optimal power-flow problem based on ADMM and sequential convex approximations. IEEE Trans Control Netw Syst 2015;2(3):238–53.

[118] Zhang J, Nabavi S, Chakrabortty A, Xin Y. ADMM optimization strategies for wide-area oscillation monitoring in power systems under asynchronous communication delays. IEEE Trans Smart Grid 2016;7(4):2123–33.

[119] Mihić K, Zhu M, Ye Y. Managing randomization in the multi-block alternating direction method of multipliers for quadratic optimization. Math Program Comput 2021;13(2):339–413.

[120] Themelis A, Patrinos P. Douglas–Rachford splitting and ADMM for nonconvex optimization: Tight convergence results. SIAM J Optim 2020;30(1):149–81.

[121] Takapoui R, Moehle N, Boyd S, Bemporad A. A simple effective heuristic for embedded mixed-integer quadratic programming. Internat J Control 2020;93(1):2–12.

[122] Diamond S, Takapoui R, Boyd S. A general system for heuristic minimization of convex functions over non-convex sets. Optim Methods Softw 2018;33(1):165–93.

[123] Hauswirth A, Bolognani S, Hug G, Dörfler F. Projected gradient descent on Riemannian manifolds with applications to online power system optimization. In: Proceedings of the 2016 54th annual allerton conference on communication, control, and computing. 2016, p. 225–32.

[124] Bahrami S, Amini MH, Shafie-Khah M, Catalao JP. A decentralized renewable generation management and demand response in power distribution networks. IEEE Trans Sustain Energy 2018;9(4):1783–97.

[125] Zhou X, Liu Z, Zhao C, Chen L. Accelerated voltage regulation in multi-phase distribution networks based on hierarchical distributed algorithm. IEEE Trans Power Syst 2019;35(3):2047–58.

[126] Chen X, Qu G, Tang Y, Low S, Li N. Reinforcement learning for selective key applications in power systems: Recent advances and future challenges. IEEE Trans Smart Grid 2022;13(4):2935–58.

[127] Sutton RS, Barto AG. Reinforcement learning: An introduction. MIT Press; 2018.

[128] Zhang K, Yang Z, Başar T. Multi-agent reinforcement learning: A selective overview of theories and algorithms. In: Handbook of reinforcement learning and control. Springer; 2021, p. 321–84.

[129] Charbonnier F, Morstyn T, McCulloch MD. Scalable multi-agent reinforcement learning for distributed control of residential energy flexibility. Appl Energy 2022;314:118825.

[130] Cui K, Tahir A, Ekinci G, Elshamanhory A, Eich Y, Li M, Koeppl H. A survey on large-population systems and scalable multi-agent reinforcement learning. 2022, arXiv:2209.03859.

[131] Zhang Q, Dehghanpour K, Wang Z, Qiu F, Zhao D. Multi-agent safe policy learning for power management of networked microgrids. IEEE Trans Smart Grid 2020;12(2):1048–62.

[132] North American Electric Reliability Corporation. Cyber-Informed Transmission Planning Framework (CITPF). URL https://www.nerc.com/comm/RSTC_Reliability_Guidelines/ERO_Enterprise_Whitepaper_Cyber_Planning_2023.pdf.

[133] Tan O, Gündüz D, Poor HV. Increasing smart meter privacy through energy harvesting and storage devices. IEEE J Sel Areas Commun 2013;31(7):1331–41.

[134] Hong Y, Liu WM, Wang L. Privacy preserving smart meter streaming against information leakage of appliance status. IEEE Trans Inf Forensics Secur 2017;12(9):2227–41.

[135] Zhao J, Jung T, Wang Y, Li X. Achieving differential privacy of data disclosure in the smart grid. In: Proceedings of IEEE INFOCOM -IEEE conference on computer communications. 2014, p. 504–12.

[136] Hale MT, Egerstedt M. Cloud-enabled differentially private multiagent optimization with constraints. IEEE Trans Control Netw Syst 2017;5(4):1693–706.

[137] Lee S, Choi D-H. Multilevel deep reinforcement learning for secure reservation-based electric vehicle charging via differential privacy and energy storage system. IEEE Trans Veh Technol 2024.

[138] Fiore D, Russo G. Resilient consensus for multi-agent systems subject to differential privacy requirements. Automatica 2019;106:18–26.

[139] Huang Z, Mitra S, Dullerud G. Differentially private iterative synchronous consensus. In: Proceedings of the 2012 ACM workshop on privacy in the electronic society. 2012, p. 81–90.

[140] Ryu M, Kim K. A privacy-preserving distributed control of optimal power flow. IEEE Trans Power Syst 2021;37(3):2042–51.

[141] Han S, Topcu U, Pappas GJ. Differentially private distributed constrained optimization. IEEE Trans Autom Control 2016;62(1):50–64.

[142] Huang L, Wu J, Shi D, Dey S, Shi L. Differential privacy in distributed optimization with gradient tracking. IEEE Trans Autom Control 2024.

[143] Wang Y, Nedić A. Tailoring gradient methods for differentially private distributed optimization. IEEE Trans Autom Control 2023;69(2):872–87.

[144] Zhao C, Chen J, He J, Cheng P. Privacy-preserving consensus-based energy management in smart grids. IEEE Trans Signal Process 2018;66(23):6162–76.

[145] Huo X, Liu M. Encrypted decentralized multi-agent optimization for privacy preservation in cyber–physical systems. IEEE Trans Ind Inf 2021;19(1):750–61.

[146] Zhang C, Wang Y. Enabling privacy-preservation in decentralized optimization. IEEE Trans Control Netw Syst 2018;6(2):679–89.

[147] He D, Kumar N, Zeadally S, Vinel A, Yang LT. Efficient and privacy-preserving data aggregation scheme for smart grid against internal adversaries. IEEE Trans Smart Grid 2017;8(5):2411–9.

[148] Mu C, Ding T, Yuan Y, Zhang B, Han Z, Shahidehpour M. Decentralized and private solution for the optimal dispatch of integrated wind farms with shared energy storage systems. IEEE Trans Power Syst 2024;1–12.

[149] Chen W, Wang Z, Ge Q, Dong H, Liu G-P. Quantized distributed economic dispatch for microgrids: Paillier encryption–decryption scheme. IEEE Trans Ind Inf 2024;20(4):6552–62.

[150] Hu Q, Bu S, Su W, Terzija V. A privacy-preserving energy management system based on homomorphic cryptosystem for IoT-enabled active distribution network. J Mod Power Syst Clean Energy 2023;12(1):167–78.

[151] Froelicher D, Troncoso-Pastoriza JR, Pyrgelis A, Sav S, Sousa JS, Bossuat J-P, Hubaux J-P. Scalable privacy-preserving distributed learning. Proc Priv Enhanc Technol 2021;2021(2):323–47.

[152] Shoukry Y, Gatsis K, Alanwar A, Pappas GJ, Seshia SA, Srivastava M, Tabuada P. Privacy-aware quadratic optimization using partially homomorphic encryption. In: Proceedings of the 55th IEEE conference on decision and control. 2016, p. 5053–8.

[153] Laufer E, Levis P, Rajagopal R. Privacy-preserving control of partitioned energy resources. In: Proceedings of the 15th ACM international conference on future and sustainable energy systems. 2024, p. 610–24.

[154] Zhang S, Ohlson Timoudas T, Dahleh MA. Consensus with preserved privacy against neighbor collusion. Control Theory Technol 2020;18:409–18.

[155] Rottondi C, Fontana S, Verticale G. Enabling privacy in vehicle-to-grid interactions for battery recharging. Energies 2014;7(5):2780–98.

[156] Huo X, Liu M. On privacy preservation of distributed energy resource optimization in power distribution networks. IEEE Trans Control Netw Syst 2024;1–12.

[157] Zhang K, Li Z, Wang Y, Louati A, Chen J. Privacy-preserving dynamic average consensus via state decomposition: Case study on multi-robot formation control. Automatica 2022;139:110182.

[158] Sun L, Ding D, Dong H, Bai X. Privacy-preserving distributed economic dispatch for microgrids based on state decomposition with added noises. IEEE Trans Smart Grid 2023.

[159] Chen X, Huang L, Ding K, Dey S, Shi L. Privacy-preserving push-sum average consensus via state decomposition. IEEE Trans Autom Control 2023;68(12):7974–81.

[160] Mo Y, Murray RM. Privacy preserving average consensus. IEEE Trans Autom Control 2016;62(2):753–65.

[161] Charalambous T, Manitara NE, Hadjicostis CN. Privacy-preserving average consensus over digraphs in the presence of time delays. In: Proceedings of the 57th annual allerton conference on communication, control, and computing. 2019, p. 238–45.

[162] Mao S, Tang Y, Dong Z, Meng K, Dong ZY, Qian F. A privacy preserving distributed optimization algorithm for economic dispatch over time-varying directed networks. IEEE Trans Ind Inf 2021;17(3):1689–701.

[163] Li Q, Heusdens R, Christensen MG. Privacy-preserving distributed optimization via subspace perturbation: A general framework. IEEE Trans Signal Process 2020;68:5983–96.

[164] Ben-David A, Nisan N, Pinkas B. FairplayMP: A system for secure multi-party computation. In: Proceedings of the 15th ACM conference on computer and communications security. 2008, p. 257–66.

[165] Songhori EM, Hussain SU, Sadeghi A-R, Schneider T, Koushanfar F. Tinygarble: Highly compressed and scalable sequential garbled circuits. In: Proceedings of the IEEE symposium on security and privacy. 2015, p. 411–28.

[166] Dwork C, McSherry F, Nissim K, Smith A. Calibrating noise to sensitivity in private data analysis. In: Proceedings of the theory of cryptography conference. New York, NY, USA; 2006, p. 265–84.

[167] Dwork C. Differential privacy. In: Proceedings of the international colloquium on automata, languages, and programming. Venice, Italy; 2006, p. 1–12.

[168] Abadi M, Chu A, Goodfellow I, McMahan HB, Mironov I, Talwar K, Zhang L. Deep learning with differential privacy. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016, p. 308–18.

[169] Wei K, Li J, Ding M, Ma C, Yang HH, Farokhi F, Jin S, Quek TQ, Poor HV. Federated learning with differential privacy: Algorithms and performance analysis. IEEE Trans Inf Forensics Secur 2020;15:3454–69.
[170] Fioretto F, Mak TW, Van Hentenryck P. Differential privacy for power grid obfuscation. IEEE Trans Smart Grid 2019;11(2):1356–66.
[171] Eibl G, Engel D. Differential privacy for real smart metering data. Comput Sci Res Dev 2017;32:173–82.
[172] Miao G, Ding AA, Wu SS. Linear model against malicious adversaries with local differential privacy. 2022, arXiv:2202.02448.
[173] Zhang T, Ye D, Zhu T, Liao T, Zhou W. Evolution of cooperation in malicious social networks with differential privacy mechanisms. Neural Comput Appl 2023;35(18):12979–94.
[174] Bu Z, Dong J, Long Q, Su WJ. Deep learning with gaussian differential privacy. Harv Data Sci Rev 2020;2020(23):10–162.
[175] Wu N, Farokhi F, Smith D, Kaafar MA. The value of collaboration in convex machine learning with differential privacy. In: Proceedings of the IEEE symposium on security and privacy. 2020, p. 304–17.
[176] Pillutla K, Andrew G, Kairouz P, McMahan HB, Oprea A, Oh S. Unleashing the power of randomization in auditing differentially private ML. Adv Neural Inf Process Syst 2024;36:66201–38.
[177] Majumder S, Dong L, Doudi F, Cai Y, Tian C, Kalathil D, Ding K, Thatte AA, Li N, Xie L. Exploring the capabilities and limitations of large language models in the electric energy sector. Joule 2024;8(6):1544–9.
[178] Yuan Z-P, Li P, Li Z-L, Xia J. A fully distributed privacy-preserving energy management system for networked microgrid cluster based on homomorphic encryption. IEEE Trans Smart Grid 2023.
[179] Paillier P. Public-key cryptosystems based on composite degree residuosity classes. In: Proceedings of the international conference on the theory and applications of cryptographic techniques. Prague, Czech Republic; 1999, p. 223–38.
[180] Zhang C, Ahmad M, Wang Y. ADMM based privacy-preserving decentralized optimization. IEEE Trans Inf Forensics Secur 2018;14(3):565–80.
[181] Huo X, Liu M. Privacy-preserving distributed multi-agent cooperative optimization — paradigm design and privacy analysis. IEEE Control Syst Lett 2022;6:824–9.
[182] Harris GE. Distributed Network Protocol 3. URL https://www.dnp.org/About/Overview-of-DNP3-Protocol1.
[183] North American Electric Reliability Corporation. NERC Reliability Standards. URL https://www.iec.ch/blog/cyber-security-understanding-iec-62351.
[184] Chen W, Liu L, Liu G-P. Privacy-preserving distributed economic dispatch of microgrids: A dynamic quantization-based consensus scheme with homomorphic encryption. IEEE Trans Smart Grid 2022;14(1):701–13.
[185] Shamir A. How to share a secret. Commun ACM 1979;22(11):612–3.
[186] Humpherys J, Jarvis TJ. Foundations of applied mathematics, Volume I: Mathematical analysis. Society for Industrial and Applied Mathematics; 2020.
[187] Nabil M, Ismail M, Mahmoud MM, Alasmary W, Serpedin E. PPETD: Privacy-preserving electricity theft detection scheme with load monitoring and billing for AMI networks. IEEE Access 2019;7:96334–48.
[188] Wang Y, Lu J, Zheng WX, Shi K. Privacy-preserving consensus for multi-agent systems via node decomposition strategy. IEEE Trans Circuits Syst I Regul Pap 2021;68(8):3474–84.
[189] Zou J, Liu H, Liu C, Ren X, Wang X. Optimal privacy-preserving transmission schedule against eavesdropping attacks on remote state estimation. IEEE Control Syst Lett 2024.
[190] Huo X, Liu M. On privacy preservation of electric vehicle charging control via state obfuscation. In: Proceedings of the 62nd IEEE conference on decision and control. 2023, p. 6564–9.
[191] Yao AC. Protocols for secure computations. In: Proceedings of the 23rd annual symposium on foundations of computer science. Chicago, IL, USA; 1982, p. 160–4.
[192] Kondi Y, Patra A. Privacy-free garbled circuits for formulas: Size zero and information-theoretic. In: Proceedings of advances in cryptology. 2017, p. 188–222.
[193] Mo J, Gopinath J, Reagen B. HAAC: A hardware-software co-design to accelerate garbled circuits. In: Proceedings of the 50th annual international symposium on computer architecture. 2023, p. 1–13.
[194] US Department of Energy. DataGuard Energy Data Privacy Program (DataGuard). URL https://www.energy.gov/oe/dataguard-energy-data-privacy-program.
[195] Xcel Energy. Introducing Our New Wind- and Solar-Powered Renewable Energy Programs. URL https://stories.xcelenergy.com/ArticlePage/?id=Introducing-our-new-wind--and-solar-powered-renewable-energy-programs.
[196] European Union. Horizon Europe (2021–2027). URL https://horizoneurope.ie.
[197] Energy Networks Association. Open Networks. URL https://www.energynetworks.org/work/open-networks/.
[198] National Renewable Energy Laboratory. Electrification Futures Study. URL https://www.nrel.gov/analysis/electrification-futures.html.
[199] National Institute of Standards and Technology. NIST AI Risk Management Framework. URL https://www.nist.gov/itl/ai-risk-management-framework.
[200] Fei X, Zhao H, Zhou X, Zhao J, Shu T, Wen F. Power system fault diagnosis with quantum computing and efficient gate decomposition. Sci Rep 2024;14(1):16991.
[201] Geisler S, Wollschläger T, Abdalla M, Gasteiger J, Günnemann S. Attacking large language models with projected gradient descent. 2024, arXiv:2402.09154.
[202] Zhou Y, Zhang P. Noise-resilient quantum machine learning for stability assessment of power systems. IEEE Trans Power Syst 2022;38(1):475–87.
[203] Yan R, Wang Y, Dai J, Xu Y, Liu AQ. Quantum-key-distribution-based microgrid control for cybersecurity enhancement. IEEE Trans Ind Appl 2022;58(3):3076–86.
[204] Pirandola S, Andersen UL, Banchi L, Berta M, Bunandar D, Colbeck R, Englund D, Gehring T, Lupo C, Ottaviani C, et al. Advances in quantum cryptography. Adv Opt Photonics 2020;12(4):1012–236.
[205] Gisin N, Thew R. Quantum communication. Nat Photonics 2007;1(3):165–71.
[206] Alvarez-Alvarado MS, Apolo-Tinoco C, Ramirez-Prado MJ, Alban-Chacón FE, Pico N, Aviles-Cedeno J, Recalde AA, Moncayo-Rea F, Velasquez W, Rengifo J. Cyber–physical power systems: A comprehensive review about technologies drivers, standards, and future perspectives. Comput Electr Eng 2024;116:109149.
[207] Huang H, Poor HV, Davis KR, Overbye TJ, Layton A, Goulart AE, Zonouz S. Toward resilient modern power systems: From single-domain to cross-domain resilience enhancement. Proc IEEE 2024;112(4):365–98.
[208] Rose S, Borchert O, Mitchell S, Connelly S. Zero trust architecture. NIST Spec Publ 2020;800:207.
[209] do Amaral TMS, Gondim JJC. Integrating Zero Trust in the cyber supply chain security. In: Proceedings of the 2021 workshop on communication networks and power systems. Brasilia, Brazil; 2021, p. 1–6.
[210] Sarkar S, Choudhary G, Shandilya SK, Hussain A, Kim H. Security of zero trust networks in cloud computing: A comparative review. Sustainability 2022;14(18):11213.
[211] Li S, Iqbal M, Saxena N. Future industry internet of things with zero-trust security. Inf Syst Front 2022;1–14.
[212] He Y, Huang D, Chen L, Ni Y, Ma X. A survey on zero trust architecture: Challenges and future trends. Wirel Commun Mob Comput 2022;2022(1):6476274.
[213] Alagappan A, Venkatachary SK, Andrews LJB. Augmenting Zero Trust Network Architecture to enhance security in virtual power plants. Energy Rep 2022;8:1309–20.
[214] Zanasi C, Magnanini F, Russo S, Colajanni M. A zero trust approach for the cybersecurity of industrial control systems. In: Proceedings of the IEEE international symposium on network computing and applications. Vol. 21, Boston, MA, USA; 2022, p. 1–7.
[215] Li P, Ou W, Liang H, Han W, Zhang Q, Zeng G. A zero trust and blockchain-based defense model for smart electric vehicle chargers. J Netw Comput Appl 2023;213:103599.