EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Distributed Graph Publication and Dual-Granularity Privacy Protection Mechanism for Regenerative Braking Control

XueFei Xie[1,*], Lin Chen[1]

[1]School of Automotive and Traffic Engineering, NanTong Vocational University, Nantong, 226007, Jiangsu, China

Abstract

To address the risk of equipment privacy and operational information leakage caused by centralized publication of vehicle states, energy-storage SOC, and energy-interaction relationships in regenerative braking control, this paper proposes a lightweight distributed graph publication mechanism with dual-granularity privacy protection based on node-attribute LDP (NA-LDP) and Edge-LDP. First, vehicles, energy storage units, substations, and loads are abstracted as nodes in a dynamic directed graph, while energy interactions, braking associations, and communication links are modeled as directed edges. Second, adjacency pruning, index-weight encoding, and control-sensitive feature projection are used to reduce the publication dimension and communication overhead. Furthermore, dynamic privacy budget allocation is combined with SAC/DDPG to realize privacy-aware regenerative braking force allocation and energy-storage power scheduling. Experimental results show that when εtot = 2.0, the proposed method achieves a graph-feature MSE of 0.032, an MAE of 0.109, an energy recovery efficiency of 91.05%, an SOC out-of-bounds penalty of 0.019, and reduces the communication overhead to 24.7%. Under a 10% random edge-disconnection condition, it still maintains an energy recovery efficiency of 88.43%, demonstrating that the proposed method can balance graph data utility, control performance, and robustness.

Keywords: regenerative braking control, distributed graph publication, local differential privacy, node-attribute LDP, Edge-LDP, privacy protection, deep reinforcement learning

Received on 01 June 2026, accepted on 11 August 2026, published on 24 September 2026

doi: 10.4108/eetsis.13271

*Corresponding author. Email: 3211014@ntvu.edu.cn

1. Introduction

With the continuous advancement of green mining, energy conservation in urban rail transit, and intelligent new-energy transportation equipment, regenerative braking energy recovery has become an important technical approach for improving the energy efficiency, driving range, and operating economy of electric transportation systems. A regenerative braking system converts part of the kinetic energy of a vehicle or train during deceleration into electrical energy and stores or reuses it through traction batteries, supercapacitors, flywheel energy storage, or wayside energy storage devices.

Existing studies show that regenerative braking systems have evolved from basic energy recovery devices to integrated control systems oriented toward energy efficiency, braking stability, driving comfort, and coordinated optimization of storage life [1]. In typical scenarios such as electric mining vehicles, heavy-duty transport vehicles, and urban rail trains, long slopes, frequent starts and stops, heavy-load braking, and multi-vehicle interactions generate a large amount of recoverable braking energy. Therefore, efficient absorption, storage, and reuse of regenerative braking energy have become key issues for energy-saving operation of new-energy transportation equipment.

In urban rail transit, the effective utilization of regenerative braking energy usually depends on timetable optimization, wayside energy storage systems, onboard energy storage systems, reversible substations, and coordinated traction power-supply control. Khodaparastan et al. [2] systematically analyzed the major technical routes for regenerative braking energy recovery in electrified rail transit, including train timetable optimization, onboard/wayside energy storage systems, and reversible substations. Domínguez et al. [3] further pointed out that railway energy storage systems can utilize the regenerative energy produced by train braking, and that different storage technologies vary significantly in cycle life, power density, efficiency, cost, and engineering applicability. Thus, regenerative braking control is no longer limited to single-vehicle braking force allocation, but is gradually evolving into a distributed energy management problem involving vehicles, trains, traction substations, energy storage systems, and edge controllers.

In recent years, data-driven control has become an important development direction for regenerative braking control and energy storage management. For the coupled operation of photovoltaic generation, regenerative braking, and hybrid energy storage systems in urban rail traction networks, Li and Or [4] proposed a multi-timescale energy management method based on multi-agent deep reinforcement learning to coordinate distributed energy storage systems. Zhong et al. [5] proposed a rule-mining-based coordinated control framework for onboard and wayside energy storage systems in urban rail transit to enhance regenerative braking energy absorption and reduce regenerative failure. Yang et al. [6] reviewed energy-efficient train operation methods for urban rail transit and indicated that train operation control, timetable optimization, and traction energy management are important ways to improve system efficiency. Zhu et al. [7] introduced multi-agent deep reinforcement learning into distributed cooperative control of multiple energy storage systems in urban railways, indicating that regenerative braking energy management is moving from single-controller optimization to multi-agent cooperative decision-making. Yang et al. [8] studied a deep-reinforcement-learning-based energy management strategy for supercapacitor storage systems, providing an intelligent control idea for strongly nonlinear and time-varying urban rail traction power-supply systems.

However, while data-driven regenerative braking control improves energy recovery efficiency, it also introduces significant data leakage and privacy security risks. Data such as vehicle speed, acceleration, road slope, load, battery SOC, charge-discharge rate, storage SOC, traction-network voltage, braking energy flow, train operating state, and control communication relationships not only reflect real-time equipment states, but may also reveal line topology, vehicle dispatching patterns, storage configuration strategies, battery health conditions, and enterprise operational secrets. If centralized data collection and unified modeling are adopted, raw data may be vulnerable to eavesdropping, reconstruction, association inference, and membership inference during upload, aggregation, computation, and publication, thereby causing leakage of equipment privacy and operational secrets.

Differential privacy provides a provable mathematical framework for publishing sensitive data. Dwork et al. [9] proposed injecting random noise calibrated to sensitivity into query results so that the influence of a single record on the published result is strictly bounded. Kasiviswanathan et al. [10] further studied private learning in the local model, showing that random perturbation can be completed before data leave the data owner, thereby reducing reliance on a trusted third party. Erlingsson et al. [11] proposed RAPPOR, demonstrating the feasibility of local differential privacy in large-scale client-side statistical collection. Wang et al. [12] systematically reviewed local differential privacy models, basic mechanisms, and typical tasks, providing a theoretical basis for distributed device data collection. For distributed scenarios such as electric mining vehicles, urban rail trains, wayside storage devices, and edge controllers, local differential privacy has strong applicability.

The devices, energy flows, and control relationships in regenerative braking control systems naturally exhibit graph-structured characteristics. Vehicles, trains, energy storage systems, traction substations, and edge controllers can be abstracted as graph nodes, while energy transfer relationships, communication connections, control dependencies, and state-coupling relationships can be abstracted as graph edges. Graph-based modeling helps characterize the cooperative effects among multiple nodes, multiple edges, and multiple state variables in distributed regenerative braking systems. However, graph-structured data are highly correlated, and node attributes and edge relationships may jointly expose system topology, device identity, and operating strategy. Mueller et al. [13] noted that nonlinear, sparse, and interdependent relationships among individuals in graph data make the definition, sensitivity computation, and utility preservation of differential privacy in graph scenarios more challenging. Li et al. [14] also pointed out that private graph publication algorithms need to balance privacy protection and graph structural utility.

Therefore, distributed graph publication for regenerative braking control needs to solve two core problems: first, how to publish graph statistical information for control optimization without centrally exposing raw operating data; second, how to preserve regenerative braking control accuracy while protecting node-state privacy and edge-relationship privacy. Existing studies show that local differential privacy has been applied to social network publication [15], decentralized social graph generation [16], decentralized attributed graph collection and generation [17], and graph metric estimation [18]. Imola et al. [19] studied locally differentially private graph statistics and provided local privacy estimation methods for triangle counts and k-star counts. Liu et al. [20] further investigated graph degree distribution publication under graph Node-LDP, where privacy is defined over node-level changes in adjacency data. This structural notion should be distinguished from local protection of continuous node attributes. Hou et al. [21] proposed an Edge-LDP-based decentralized social graph clustering method, offering a reference for edge-relationship

privacy protection and graph utility preservation. Chen et al. [22] studied graph algebraic connectivity publication under edge differential privacy from the perspective of multi-agent systems, indicating an intrinsic relationship between graph topology privacy protection and distributed control performance.

In summary, this paper studies distributed graph publication and node-edge dual-granularity privacy protection for regenerative braking control in electric mining vehicles and urban rail energy storage systems. This research has both theoretical significance and engineering value. On the one hand, it incorporates vehicle operating states, storage states, traction power-supply states, and energy-interaction relationships into a unified graph-structured modeling framework, providing a more expressive data organization method for distributed regenerative braking control. On the other hand, by introducing node-level and edge-level privacy protection mechanisms, it balances device-state protection, control-relationship protection, and control utility preservation, thereby supporting a safe, trustworthy, and efficient regenerative braking control system. The overall framework of this paper is shown in Fig. 1. The framework consists of five parts: physical system, graph modeling, graph publication, graph reconstruction, and privacy-aware control, and is used to realize regenerative braking optimization under privacy protection constraints.

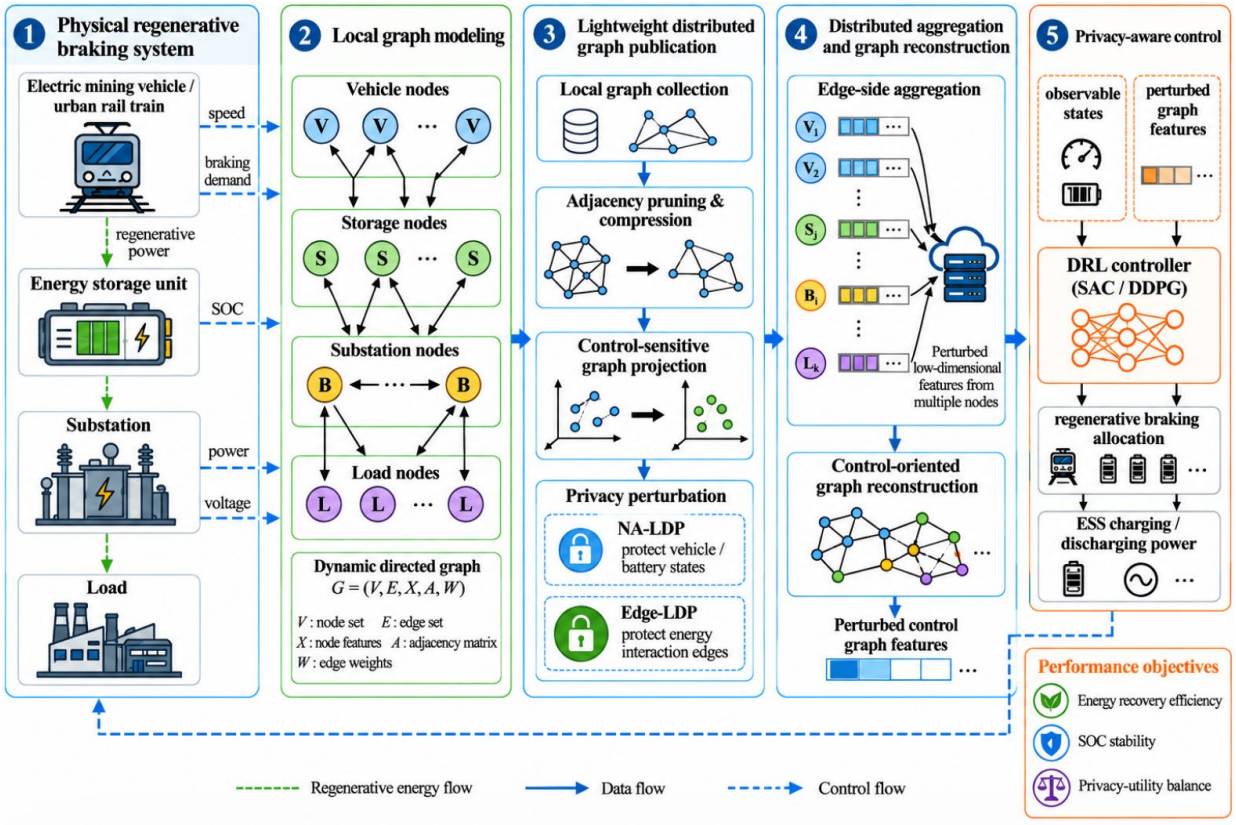

Figure 1. Privacy-aware regenerative braking workflow

For readability, the annotations in Figs. 1-6 use a consistent abbreviation set: ESS denotes energy storage system, SOC denotes state of charge, RR denotes randomized response, LDP denotes local differential privacy, and DRL denotes deep reinforcement learning.

2. Related Work

Existing studies on regenerative braking control mainly focus on improving energy recovery efficiency, ensuring braking safety, coordinating energy storage systems, and intelligent energy management. Early studies mostly adopted rule-based braking force allocation strategies, in which the mechanical and electric braking proportions were determined according to vehicle speed, braking intensity, motor torque, battery SOC, and braking safety constraints. Such methods are clear in structure and easy to deploy, but they are often unable to achieve global optimality under complex slopes, load variations, and strongly time-varying operating conditions. In recent years, model predictive control, dynamic programming, reinforcement learning, and multi-agent reinforcement learning have been gradually introduced into regenerative braking control to enhance the adaptability of control strategies to complex operating conditions.

In rail transit, efficient utilization of regenerative braking energy generally depends on traction power-supply system modeling, operation timetable optimization, and energy storage management. Existing studies have formed a relatively complete research basis in regenerative braking energy recovery technologies [2], applicability analysis of railway energy storage systems [3], multi-timescale energy management [4], coordinated control of onboard and wayside energy storage [5], energy-efficient train operation [6], distributed reinforcement learning control of multiple storage systems [7], and deep reinforcement learning control of supercapacitor storage systems [8]. These studies show that regenerative braking control is developing from single-device control toward multi-node, multi-energy, and multi-timescale cooperative optimization. However, most existing studies focus on energy saving, economy, carbon emissions, and voltage stability, while paying insufficient attention to the privacy leakage risks of the control data themselves.

In terms of privacy protection, differential privacy and its local extensions have become important theoretical foundations for data publication. Differential privacy reduces the influence of a single record on the published result through randomized mechanisms [9], while local differential privacy further moves the perturbation process to the data owner side [10]. Mechanisms such as RAPPOR verify its application value in large-scale client-side statistical collection [11]. With the development of the Internet of Things, mobile terminals, and edge computing, privacy protection requirements in distributed data collection are becoming increasingly prominent. Local differential privacy is highly applicable because it does not require a trusted third party [12]. For regenerative braking control, vehicles, trains, and energy storage devices are usually distributed across different physical locations and communication domains; therefore, centralized privacy protection methods cannot fully adapt to the deployment environment, and local perturbation and privacy protection need to be completed at the terminal side.

In graph data privacy protection, researchers have proposed various differential privacy methods for graph publication, graph statistics, and graph learning tasks. Unlike relational data, graph-structured data contain complex dependencies among nodes, edges, and attributes, making privacy definitions, noise injection, and utility evaluation more challenging [13]. Surveys on private graph data release show that existing methods mainly focus on anonymization, differentially private synthetic graph generation, graph statistics publication, and graph machine learning. The key challenge is how to preserve graph structural information such as degree distribution, clustering coefficient, community structure, and path features simultaneously [14]. In localized graph publication, Liu et al. [15] proposed a local differential privacy method for social network publication, Qin et al. [16] proposed LDPGen for generating locally differentially private decentralized social graphs, and Wei et al. [17] further studied the collection and generation of decentralized attributed graphs. These works provide methodological references for graph-structured data publication in distributed regenerative braking systems involving vehicles, storage, and substations.

In graph statistics collection, Ye et al. [18] proposed the LF-GDPR framework for estimating graph metrics under local differential privacy and improved estimation accuracy through privacy budget allocation and calibration. Imola et al. [19] studied locally differentially private graph statistics and could estimate important structural metrics such as triangle counts and k-star counts. Liu et al. [20] studied graph degree distribution publication under graph Node-LDP, in which the privacy unit is a node together with its incident structural relationships. This definition provides stronger graph-structural protection than Edge-LDP but does not directly represent continuous node attributes such as SOC, power, or voltage. Attributed-graph LDP research such as AsgLDP [17] shows that attribute data can instead be locally randomized before publication. Accordingly, this paper reserves the term Node-LDP for the graph-structural definition in [20] and uses node-attribute LDP for continuous operating states.

In edge-level privacy protection, Edge-LDP is more suitable for protecting edge existence, direction, and relationship strength, and usually provides better graph structural utility. Hou et al. [21] proposed Wdt-SCAN, a decentralized graph clustering method that uses degree-vector encoding and a two-stage clustering mechanism under Edge-LDP. Chen et al. [22] studied graph algebraic connectivity publication under edge differential privacy for multi-agent systems, indicating that topology metrics related to consensus convergence can still be estimated while protecting edge privacy. Yuan et al. [23] proposed PrivGraph, which exploits community information to generate differentially private synthetic graphs and improves structural preservation. Li et al. [24] studied graph embedding based on local differential privacy, demonstrating that local perturbation can be combined with graph representation learning. Mendonça et al. [25] proposed PEG for edge-labeled graphs, emphasizing the importance of edge attributes or relationship types in private graph publication. Xu et al. [26] studied continuous publication of weighted graphs under local differential privacy, providing inspiration for publishing dynamic energy flows and continuous operating states. Mundra et al. [27] further studied graph analytics under local edge differential privacy, offering more practical edge-level privacy protection for structural analysis tasks such as triangle counting and k-core decomposition.

Overall, existing studies have achieved considerable progress in regenerative braking energy recovery, urban rail energy storage control, differential privacy, local differential privacy, graph data publication, and private graph analytics. However, several limitations remain. First, existing regenerative braking control studies mainly focus on control strategies and energy recovery performance, while rarely modeling the interactions among vehicles, energy storage systems, substations, and controllers as a unified distributed graph. Second, existing graph publication and graph-statistics privacy protection methods mainly target social networks, communication networks, and general graph analysis tasks, and have not been fully integrated with the real-time requirements, control accuracy, energy-flow direction, and

storage constraints of regenerative braking control. Third, a single node-attribute LDP or Edge-LDP mechanism cannot simultaneously satisfy the privacy protection requirements of device states and control relationships, and a dual-granularity privacy adaptation mechanism for node attributes and edge relationships is lacking. Fourth, existing private graph publication studies mostly use graph statistical error, clustering quality, and structural preservation as evaluation metrics, while less attention is paid to the impact of privacy perturbation on regenerative braking energy recovery efficiency, storage SOC stability, and control decision accuracy. Therefore, it is necessary to study distributed graph publication and dual-granularity privacy protection mechanisms for regenerative braking control.

A direct comparison with recent privacy-preserving MPC and federated energy-management frameworks is provided in Section 7.5.

3. Distributed Topology Graph Modeling of Regenerative Braking Systems

To describe the energy interactions and control coupling among vehicles, energy storage units, substations, and loads in a regenerative braking system, this paper abstracts the regenerative braking process as a distributed directed graph. The model can describe the transmission paths of regenerative braking energy among multiple nodes and also provides a unified data representation basis for subsequent distributed graph publication and dual-granularity privacy protection. The regenerative braking energy flow and its distributed directed graph abstraction are shown in Fig. 2.

As shown in Fig. 2, vehicles, energy storage units, substations, and loads are abstracted as different types of nodes, while energy interactions, braking associations, and communication links are modeled as directed edges. This graph model provides a unified topological representation for subsequent graph feature extraction, lightweight graph publication, and privacy-preserving control.

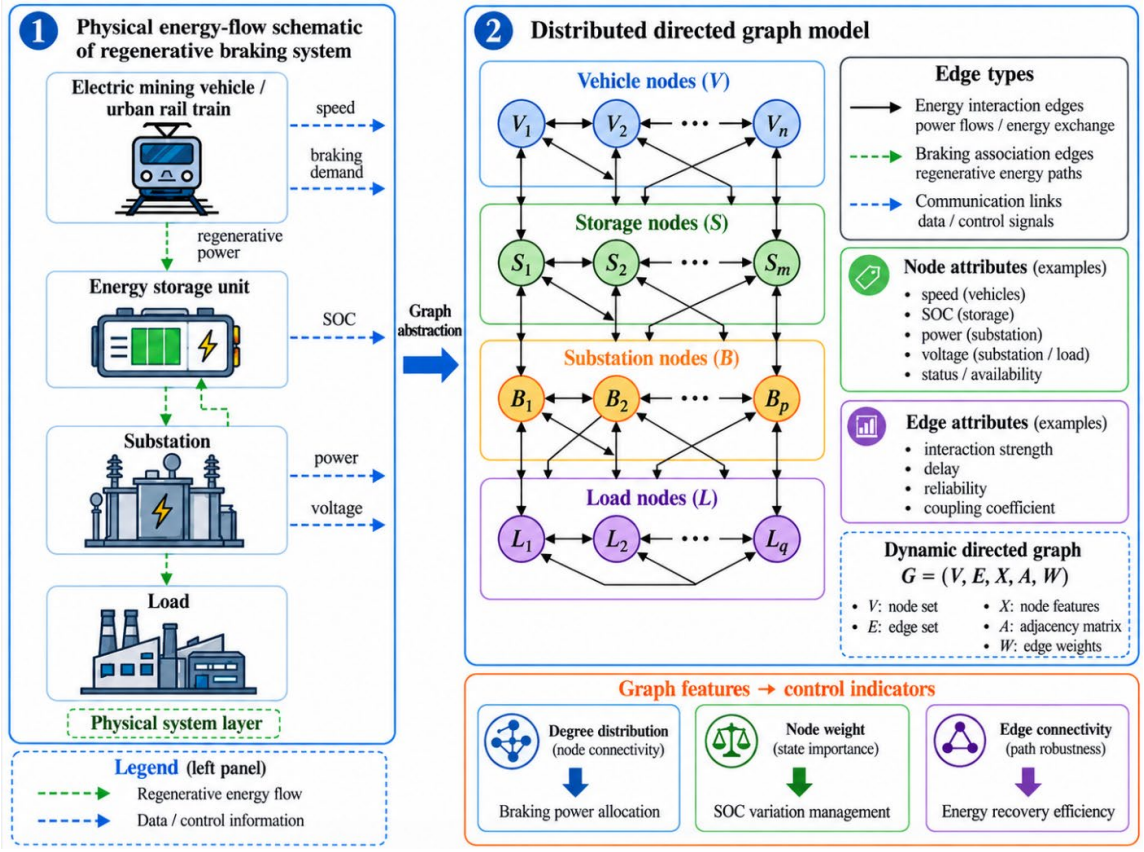

Figure 2. Physical energy flow and directed-graph abstraction

3.1. Regenerative Braking Energy Flow and Topology Structure

During the operation of electric mining vehicles and urban rail trains, when a vehicle decelerates, travels downhill, or brakes before entering a station, the traction motor switches from the motoring state to the generating state and converts

part of the kinetic or potential energy into electrical energy. This energy can be absorbed and reused by onboard batteries, wayside energy storage systems, adjacent traction loads, or traction power-supply networks [1-4]. Therefore, the energy flow of a regenerative braking system is no longer a local process within a single vehicle, but a distributed energy interaction process among vehicles, storage units, substations, and loads.

Let the braking force demand of vehicle unit i at time t be denoted as follows. It is jointly provided by mechanical braking force and regenerative braking force:

$$F_{b,i}^{\mathrm{dem}}(t) = F_{m,i}(t) + F_{e,i}(t) \tag{1}$$

where the two terms denote the mechanical braking force and the regenerative braking force, respectively.

Constrained by the motor output limit, battery charging power, and state of charge (SOC), the regenerative braking force satisfies:

$$0 \le F_{e,i}(t) \le \min\left\{F_{b,i}^{\mathrm{dem}}(t), F_{e,i}^{\max}\left(v_i\right), \frac{P_{b,i}^{\mathrm{ch,max}}(t)}{\eta_i v_i(t) + \varepsilon}\right\} \tag{2}$$

where the variables denote vehicle speed, the maximum regenerative braking force allowed by the motor, the maximum charging power of the battery/energy storage unit, the energy conversion efficiency, and a small positive constant to avoid a zero denominator, respectively.

The regenerative braking power output by the vehicle is expressed as:

$$P_{r,i}(t) = \eta_i F_{e,i}(t) v_i(t) \tag{3}$$

At the system level, let the total regenerative braking power, the absorbable traction load power, and the absorbable storage power be given. The recoverable system power is then:

$$P_{\mathrm{rec}}(t) = \min\left\{P_r^{\mathrm{sum}}(t), P_l^{\mathrm{abs}}(t) + P_s^{\mathrm{abs}}(t)\right\} \tag{4}$$

The regenerative braking energy recovery efficiency is defined as:

$$\eta_{\mathrm{rec}} = \frac{\sum_{t=1}^{T} P_{\mathrm{rec}}(t)\Delta t}{\sum_{t=1}^{T} P_r^{\mathrm{sum}}(t)\Delta t + \varepsilon} \tag{5}$$

Equations (1)-(5) show that regenerative braking performance depends not only on the vehicle operating state, but also on the absorption capability of the storage system, the power demand of traction loads, and the energy transmission paths. Therefore, a distributed graph model should be constructed from a topological perspective to describe the energy flow and control coupling among multiple nodes.

3.2. Distributed Directed Graph Model Definition

This paper abstracts the regenerative braking system as a dynamic directed graph, expressed as follows:

$$G(t) = (V(t), E(t), \mathbf{X}(t), \mathbf{A}(t), \mathbf{W}(t)) \tag{6}$$

where V(t) is the node set, E(t) is the edge set, X(t) is the node attribute matrix, A(t) is the adjacency matrix, and W(t) is the edge-weight matrix or edge-attribute tensor. The node set consists of four types of functional nodes:

$$V = V_{\mathrm{veh}} \cup V_{\mathrm{ess}} \cup V_{\mathrm{sub}} \cup V_{\mathrm{load}} \tag{7}$$

where Vveh denotes vehicle nodes, including electric mining vehicles and urban rail trains; Vess denotes energy storage nodes, including onboard batteries, supercapacitors, and wayside energy storage systems; Vsub denotes substation nodes; and Vload denotes traction load nodes. For any node, its node attribute vector is defined as:

$$\mathbf{x}_i(t) = \left[c_i, p_i(t), v_i(t), S_i(t), P_i(t), U_i(t), q_i(t)\right] \tag{8}$$

where ci denotes the node type, pi(t) denotes the position or section index, vi(t) denotes the operating speed, Si(t) denotes the SOC, Pi(t) denotes the node power, Ui(t) denotes the node voltage, and qi(t) denotes the operating state. Vehicle nodes can be in traction, braking, or coasting states, while energy storage nodes can be in charging, discharging, or standby states.

The system edge set is divided into three categories according to function:

$$E = E_{\mathrm{en}} \cup E_{\mathrm{brk}} \cup E_{\mathrm{com}} \tag{9}$$

where Een denotes energy interaction edges, representing electrical energy transfer among nodes; Ebrk denotes braking association edges, representing the coupling between braking power allocation and storage absorption; and Ecom denotes communication link edges, representing state information exchange and control command transmission among nodes.

For a directed edge, its edge attribute vector is defined as:

$$\mathbf{w}_{ij}(t) = \left[r_{ij}, P_{ij}(t), \tau_{ij}(t), \rho_{ij}(t), \gamma_{ij}(t)\right] \tag{10}$$

where rij denotes the edge type, Pij(t) denotes the energy transmission power or interaction strength, τij(t) denotes the communication delay, ρij(t) denotes link reliability, and γij(t) denotes the braking-control coupling coefficient.

The adjacency relationship is determined as follows: if node vi and node vj have an energy interaction, braking association, or communication connection, the corresponding adjacency matrix element is 1; otherwise, it is 0:

$$A_{ij}(t) = 1; \quad \text{otherwise, } A_{ij}(t) = 0 \tag{11}$$

According to the functional types of edges, the overall adjacency matrix is decomposed into three topological submatrices:

$$\mathbf{A}(t) = \left\{\mathbf{A}^{\mathrm{en}}(t), \mathbf{A}^{\mathrm{brk}}(t), \mathbf{A}^{\mathrm{com}}(t)\right\} \tag{12}$$

where the three submatrices correspond to energy interaction topology, braking association topology, and

communication topology, respectively. The energy transmission power should satisfy the link capacity constraint:

$$0 \le P_{ij}(t) \le \bar{P}_{ij} A_{ij}^{\text{en}}(t) \tag{13}$$

where the parameter denotes the maximum transmission power of edge eij. The operation of an energy storage node should satisfy the SOC constraint:

$$S_j^{\min} \le S_j(t) \le S_j^{\max}, \quad v_j \in V_{\text{ess}} \tag{14}$$

Communication links should satisfy the real-time delay constraint for control:

$$\tau_{ij}(t) \le \tau^{\max}, \quad e_{ij} \in E_{\text{com}} \tag{15}$$

Finally, the dynamic topology over the whole operating horizon can be represented as a graph sequence:

$$\mathsf{G} = \{G(1), G(2), \ldots, G(T)\} \tag{16}$$

The objective of the subsequent privacy-preserving graph publication is to generate a perturbed graph sequence without revealing raw node attributes and edge connections, while retaining the core topological features required for regenerative braking control.

3.3. Mapping Between Graph Features and Braking Control Performance

The structural features of a distributed topology graph can characterize the energy absorption capability, control coupling strength, and communication reliability of the regenerative braking system. This paper selects three core graph features: node degree distribution, node weight, and edge connectivity, and establishes their mapping relationships with braking power, energy recovery efficiency, and SOC variation.

First, node degree is defined to describe the connection relationship among nodes. For any node vi, its in-degree and out-degree are expressed as:

$$d_i^{\text{in}}(t) = \sum_j A_{ji}(t), \quad d_i^{\text{out}}(t) = \sum_j A_{ij}(t) \tag{17}$$

In the energy interaction topology, the out-degree of a vehicle node represents the number of available transmission paths for regenerative braking energy, while the in-degree of a storage node represents the number of accessible braking energy sources. A larger vehicle out-degree and storage in-degree indicate a stronger overall energy interaction capability of the system. Next, node weight is defined to quantify the energy state and regulation potential of a node:

$$\omega_i(t) = \alpha_1 P_i(t) + \alpha_2 S_i(t) + \alpha_3 U_i(t) \tag{18}$$

where α1, α2, and α3 are weighting coefficients. The weight of a vehicle node reflects its braking energy output potential, while the weight of a storage node reflects its energy absorption capability and SOC margin. The effective edge connectivity indicator is defined to describe the actual reachability of energy flows and communication links:

$$\chi_{ij}(t) = A_{ij}(t)\rho_{ij}(t)\left(1 - \frac{\tau_{ij}(t)}{\tau^{\max}}\right) \tag{19}$$

where ρij(t) is link reliability and τij(t) is communication delay. A larger value indicates stronger energy interaction and control communication capability between nodes. Based on the above features, the node topological coordination indicator is constructed as follows:

$$\Psi_i(t) = \beta_1 d_i^{\text{out}}(t) + \beta_2 d_i^{\text{in}}(t) + \beta_3 \omega_i(t) + \beta_4 \sum_j \chi_{ij}(t) \tag{20}$$

where β1, β2, β3, and β4 are tunable parameters. This indicator is used to evaluate the energy interaction and control coordination level of a node in the topological network. The regenerative braking allocation coefficient is further constructed as:

$$\mu_i^{\text{reg}}(t) = \sigma\left(\theta_0 + \theta_1 \Psi_i(t) + \theta_2 \Delta S_i(t) + \theta_3 \Delta U_i(t)\right) \tag{21}$$

where σ(·) is the Sigmoid function, and the two terms denote the SOC charging margin and voltage margin, respectively.

Combining the braking force demand, the optimal regenerative braking force is obtained as:

$$F_{e,i}^{*}(t) = \mu_i^{\text{reg}}(t) F_{b,i}^{\text{dem}}(t) \tag{22}$$

The system energy recovery efficiency can be expressed as a function of topology attributes, node features, and control variables:

$$\hat{\eta}_{\text{rec}}(t) = f_\eta(\mathbf{X}(t), \mathbf{A}(t), \mathbf{W}(t), \mathbf{u}(t)) \tag{23}$$

where u(t) is the control action vector, including braking force allocation, energy storage charging/discharging power, and load coordination strategy. After introducing the privacy protection mechanism, the controller can only obtain perturbed topology and node data, and the energy recovery efficiency is expressed as:

$$\hat{\eta}_{\text{rec}}^{\text{priv}}(t) = f_\eta(\mathbf{X}(t), \ \mathbf{A}(t), \ \mathbf{W}(t), \mathbf{u}(t)) \tag{24}$$

Equations (17)-(24) indicate that distributed graph features are core inputs for regenerative braking control. Node degree determines the scale of energy transmission paths, node weight reflects energy throughput capability, and edge connectivity determines the transmission reliability of energy flows and control commands. Meanwhile, data privacy perturbation changes the graph feature calculation results, thereby affecting braking force allocation, energy recovery efficiency, and storage SOC state. Therefore, graph data publication should consider node-attribute privacy, link privacy, and system control performance simultaneously.

4. Lightweight Distributed Graph Publication Method for Regenerative Braking

To address the high communication overhead and privacy leakage risks caused by direct transmission of the original topology graph in regenerative braking systems, this paper proposes a lightweight distributed graph publication method. Instead of transmitting the complete adjacency matrix and raw node data over the network, each node locally performs adjacency vector pruning, dimensionality compression, and control-sensitive feature projection, and only publishes low-dimensional perturbed graph data that meet control requirements, thereby optimizing graph structural utility, communication load, and privacy protection simultaneously.

4.1. Overall Graph Publication Process

The distributed graph publication process for regenerative braking control consists of four stages: local graph collection, privacy perturbation, distributed aggregation, and control-end graph reconstruction. The lightweight distributed graph publication process is shown in Fig. 3.

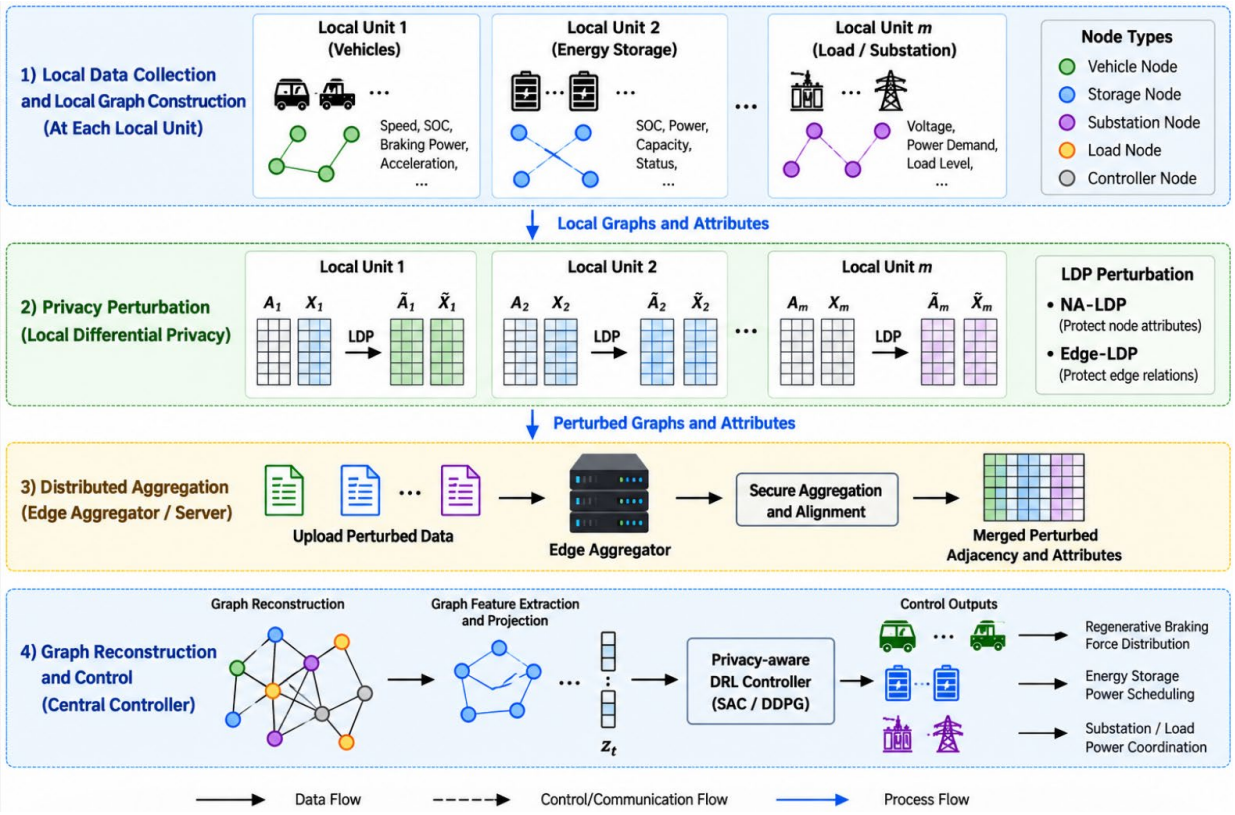

Figure 3. Lightweight distributed graph publication pipeline

As shown in Fig. 3, each local node first constructs a local graph and performs privacy perturbation. Then the edge aggregation unit summarizes the perturbed features, and finally the control end reconstructs an approximate topology for braking control. This process avoids uploading the complete adjacency matrix and raw node attributes, thereby reducing communication overhead and privacy leakage risks.

1) Local Graph Collection

Node vi collects only its own attributes and one-hop neighborhood information to construct a local graph:

$$G_i(t) = \left(V_i(t), E_i(t), \mathbf{x}_i(t), \mathbf{a}_i(t), \mathbf{w}_i(t)\right) \tag{25}$$

where the terms denote the local neighborhood node set of node vi, the node attribute vector, the adjacency vector, and the edge-weight vector, respectively. Unlike centralized collection, this method retains only local information related to regenerative braking control and does not require uploading the global topology.

2) Privacy Perturbation

Node vi applies privacy perturbation locally to adjacency relationships, node states, and edge-weight features to generate a lightweight vector to be published:

$$\mathbf{y}_i(t) = \mathrm{M}_i\left(\mathbf{x}_i(t), \mathbf{a}_i(t), \mathbf{w}_i(t)\right) \tag{26}$$

where the term denotes the local publication mechanism. The perturbation intensity can be differentially set according to the sensitivity of nodes and links, thereby avoiding direct leakage of raw sensitive information such as vehicle operating states, storage SOC, and energy interaction relationships.

3) Distributed Aggregation

The edge aggregation unit receives the perturbed vectors from all nodes and calculates global graph statistical features:

$$\tilde{\mathbf{z}}(t) = \mathrm{A}\left(\tilde{\mathbf{y}}_1(t), \tilde{\mathbf{y}}_2(t), \ldots, \tilde{\mathbf{y}}_n(t)\right) \tag{27}$$

where the term denotes the distributed aggregation function, and the result contains control-required features such as the perturbed node degree distribution, node weights, edge connectivity, and energy interaction strength.

4) Control-End Graph Reconstruction

The control end does not need to recover the complete original topology, but generates an approximate topology adapted to regenerative braking control based on the perturbed features:

$$G(t) = (V(t),\ E(t),\ \mathbf{X}(t),\ \mathbf{A}(t),\ \mathbf{W}(t)) \tag{28}$$

The approximate topology can be directly used for braking force allocation, energy storage power scheduling, and energy recovery efficiency calculation. Because the control end only obtains low-dimensional perturbed data, it effectively avoids the risk of original topology privacy leakage and greatly reduces system communication and computation overhead.

4.2. Adjacency Vector Pruning and Dimensionality Compression

In a distributed regenerative braking system, directly transmitting a node adjacency vector with a dimension proportional to the number of nodes causes communication overhead to increase linearly with network scale. In addition, many non-critical edges introduce redundant interference and reduce graph data utility. Therefore, this paper proposes adjacency vector pruning and dimensionality compression to retain only the adjacency relationships that play a core role in regenerative braking control.

Graph sparsification and graph-sketching studies show that a carefully selected sparse edge set or compact sketch can preserve key structural information while reducing storage and communication costs [28-30]. Research on distributed consensus with limited communication further indicates that data compression and encoding should be designed jointly with networked-control requirements [31]. Motivated by these results, this paper retains edges with high control relevance, transmits neighbor indices together with edge weights, and imposes a minimum-connectivity constraint to preserve control-relevant topology under a limited communication budget.

First, a control relevance score is defined for each edge:

$$R_{ij}(t) = \lambda_1 \bar{P}_{ij}(t) + \lambda_2 \rho_{ij}(t) + \lambda_3 \gamma_{ij}(t) - \lambda_4 \tau_{ij}(t) \tag{29}$$

where the terms denote normalized energy interaction power, link reliability, braking-control coupling strength, communication delay, and weighting coefficients, respectively. A larger score indicates a greater influence of the edge on braking control.

According to the score, node vi selects the top-k key adjacent edges:

$$\mathrm{N}_i^{\,k}(t) = \mathrm{TopK}_{j \in \mathrm{N}_i(t)}\left(R_{ij}(t)\right) \tag{30}$$

The pruned adjacency vector is then constructed as:

$$a_{ij}^k(t) = \begin{cases} 1, & j \in \mathrm{N}_i^{\,k}(t), \\ 0, & \text{otherwise}. \end{cases} \tag{31}$$

The original adjacency vector is compressed into a sparse adjacency vector. When the number of retained neighbors satisfies k << n, the node communication complexity is reduced from O(n) to O(k). To remove invalid zero elements in the sparse vector, an index-weight joint encoding is further used for dimensionality reduction:

$$\mathbf{c}_i(t) = \left[\left(j_1, w_{ij_1}\right), \left(j_2, w_{ij_2}\right), \ldots, \left(j_k, w_{ij_k}\right)\right] \tag{32}$$

where the terms denote the retained neighbor indices and the corresponding edge weights. This method only transmits key neighbor indices and edge weights, greatly reducing data dimensionality.

To ensure that the pruned topology can still support control tasks normally, a minimum connectivity constraint is imposed:

$$\sum_j a_{ij}^k(t) \geq k_{\min} \tag{33}$$

where kmin is the minimum number of adjacent nodes required for normal system control. If the number of valid neighbors of a node is less than kmin, all adjacent relationships are retained; otherwise, only the edges with the highest control relevance are retained. The adjacency vector pruning and control-sensitive feature projection process is shown in Fig. 4. As shown in Fig. 4, a node first collects one-hop adjacency vectors and edge-weight information, then selects top-k key edges according to control relevance, compresses the adjacency representation using index-weight encoding, and finally projects it into low-dimensional control features. This process reduces the graph publication dimension while preserving key control information.

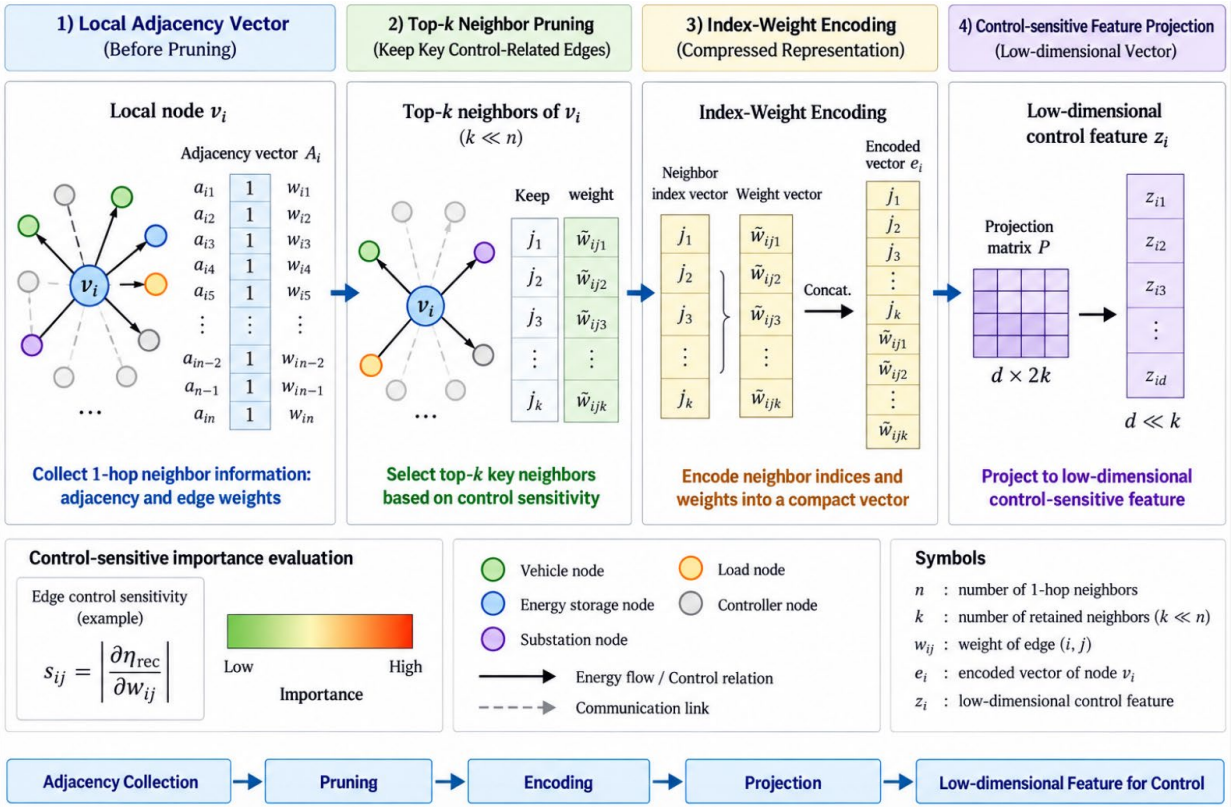

Figure 4. Top-k adjacency pruning and control-sensitive feature projection

4.3. Graph Projection Based on Control-Sensitive Features

Although adjacency vector pruning reduces the graph structure dimension, it is still necessary to extract core features related to regenerative braking control. Therefore, this paper proposes a graph projection method based on control-sensitive features, which maps the high-dimensional topology graph into a low-dimensional feature space. The pruned local graph feature vector is defined as:

$$\mathbf{h}_i(t) = \left[d_i^{\text{in}}(t), d_i^{\text{out}}(t), \omega_i(t), \sum_j \chi_{ij}(t), S_i(t), P_i(t) \right] \quad (34)$$

where the terms denote node in-degree, node out-degree, node weight, edge connectivity indicator, state of charge (SOC), and node power, respectively. This vector includes the core variables required for braking force allocation, storage energy absorption, and energy recovery efficiency calculation. To realize lightweight data publication, the graph projection mapping is constructed as:

$$\mathbf{g}_i(t) = \mathbf{Q}\mathbf{h}_i(t) \quad (35)$$

where the projection matrix, the original feature dimension, and the projected dimension are given. The matrix can be constructed by random projection, principal component mapping, or control-sensitivity-weighted projection. During the process, features that have significant influence on control performance, such as SOC margin, node power, edge connectivity, and energy interaction strength, are prioritized. Control sensitivity is used to quantify the importance of each feature:

$$\zeta_l = \left| \frac{\partial \eta_{\text{rec}}}{\partial h_l} \right| + \left| \frac{\partial F_e^*}{\partial h_l} \right| \quad (36)$$

where hl is the l-th graph feature, ηrec is the energy recovery efficiency, and the other term denotes the optimal regenerative braking force. A larger value indicates a stronger influence of the feature on the control effect, and therefore a higher weight is assigned during projection.

Privacy perturbation is applied to the projection result to obtain the final lightweight vector to be published:

$$\tilde{\mathbf{g}}_i(t) = \mathrm{P}\left(\mathbf{Q}\mathbf{h}_i(t)\right) \quad (37)$$

where the term denotes the privacy perturbation operator. The edge aggregation end summarizes data from all nodes to generate global control features:

$$\tilde{\mathbf{G}}_c(t) = \mathrm{Agg}\left(\tilde{\mathbf{g}}_1(t), \tilde{\mathbf{g}}_2(t), \ldots, \tilde{\mathbf{g}}_n(t)\right) \quad (38)$$

The control end uses the global features to perform regenerative braking force allocation and energy storage power scheduling:

$$\mathbf{u}^*(t) = \pi\left(\tilde{\mathbf{G}}_c(t), \mathbf{s}(t)\right) \tag{39}$$

where $\pi(\cdot)$ is the control policy function and s(t) is the observable system state. Compared with transmitting the complete topology graph, this scheme publishes only compressed core control features, removes redundant information, effectively reduces communication overhead, and narrows the privacy leakage surface.

In summary, the proposed method realizes a low-dimensional representation of the topology graph through adjacency pruning, dimensionality compression, and control-sensitive feature projection. It retains effective control information such as node degree, node weight, and edge connectivity while avoiding the external transmission of the original adjacency matrix and node plaintext data, and it also provides a lightweight input basis for the subsequent node-edge dual-granularity privacy protection mechanism.

5. Dual-Granularity Privacy Protection Mechanism Based on Node-Attribute LDP/Edge-LDP

To address the risks of node-state leakage and edge-relationship inference during regenerative braking topology graph publication, this paper proposes a dual-granularity privacy protection mechanism integrating node-attribute local differential privacy (NA-LDP) and Edge-LDP. Here, NA-LDP denotes standard local differential privacy applied to a node's continuous attribute vector (e.g., vehicle operating parameters, battery SOC, and storage SOC), rather than graph Node-LDP, which protects node existence together with incident edges [20]. This attribute-level use is consistent with local perturbation of attributed graph data [17] and general LDP principles [10,12]. Edge-LDP is used to protect edge-relationship data such as energy interactions, braking associations, and communication links [21,22,27]. The mechanism performs data perturbation locally at each node, does not rely on a trusted central server, and is suitable for distributed regenerative braking control scenarios. The dual-granularity privacy protection mechanism is shown in Fig. 5.

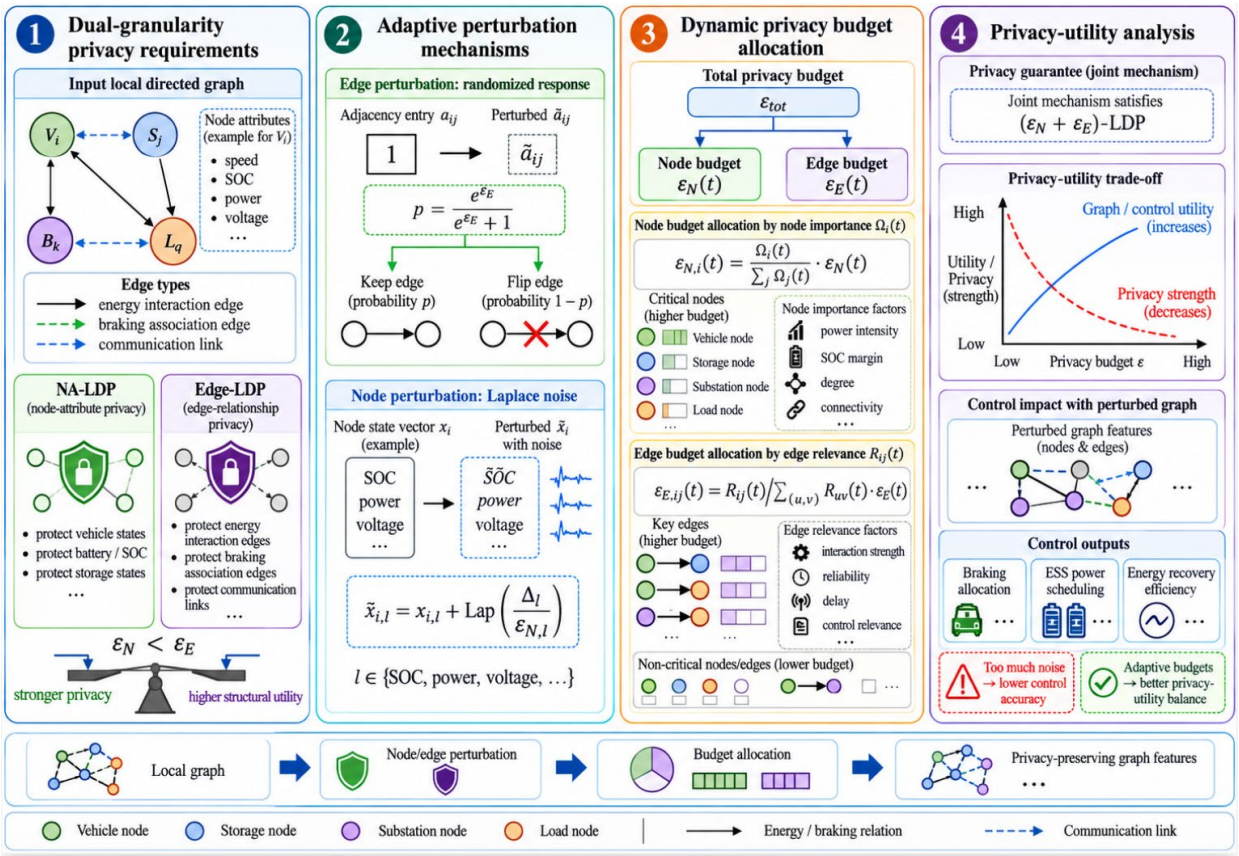

Figure 5. Dual-granularity NA-LDP/Edge-LDP protection

As shown in Fig. 5, NA-LDP protects continuous node attributes such as vehicle states, battery SOC, storage SOC, power, and voltage, while Edge-LDP protects energy-interaction edges, braking-association edges, and

communication links. Through adaptive perturbation and dynamic privacy budget allocation, a balance between attribute privacy, relationship privacy, and graph data utility can be achieved.

5.1. Dual-Granularity Privacy Requirements

Let x_i denote the normalized and sensitivity-bounded continuous attribute vector of node v_i, including vehicle speed, braking state, storage SOC, node power, voltage, and other operating data. Following the standard local differential privacy definition [10,12], this paper uses the term node-attribute LDP (NA-LDP) for local protection of these attributes; this definition is distinct from graph Node-LDP in [20].

If a randomized perturbation mechanism satisfies the following condition for any two admissible node-attribute vectors x_i and x_i':

$$\Pr\left[\mathrm{M}_N(\mathbf{x}_i)=y\right]\le e^{\varepsilon_N}\Pr\left[\mathrm{M}_N(\mathbf{x}_i')=y\right] \tag{40}$$

then the mechanism is said to satisfy εN-NA-LDP with respect to node attributes [10,12,17].

The edge set E represents energy transmission, braking coupling, and communication connections among nodes, reflecting the system topology and control dependencies. Edge-LDP is adopted for fine-grained relationship protection [21,22,27]. If a randomized mechanism satisfies the following condition for any two adjacency vectors that differ in only one edge:

$$\Pr\left[\mathrm{M}_E(\mathbf{a}_i)=z\right]\le e^{\varepsilon_E}\Pr\left[\mathrm{M}_E(\mathbf{a}_i')=z\right] \tag{41}$$

then it is said to satisfy εE-Edge-LDP [21,27]. This paper sets:

$$\varepsilon_N<\varepsilon_E \tag{42}$$

The above operation realizes a dual-granularity privacy protection strategy that separately protects continuous node attributes and edge relationships.

5.2. Adaptive Randomized Response and Laplace Noise Injection

For the pruned adjacency vector, the randomized response mechanism [11] is used to perturb edge relationships:

$$\tilde{a}_{ij}(t)=\begin{cases}a_{ij}(t), & p\\ 1-a_{ij}(t), & 1-p\end{cases},\quad p=\frac{e^{\varepsilon_E}}{e^{\varepsilon_E}+1} \tag{43}$$

This mechanism satisfies εE-Edge-LDP [21,27] and can effectively hide the connection states of energy interaction edges and communication links. Different privacy budgets are configured for different edge types:

$$\varepsilon_E^r\in\left\{\varepsilon_{\text{en}},\varepsilon_{\text{brk}},\varepsilon_{\text{com}}\right\} \tag{44}$$

corresponding to energy interaction edges, braking association edges, and communication link edges, respectively. For continuous node attributes such as SOC, node power, voltage, and node weight, the Laplace mechanism [9,12,17] is used for local perturbation:

$$\tilde{x}_{i,l}(t)=x_{i,l}(t)+\mathrm{Lap}\left(\frac{\Delta_l}{\varepsilon_{N,l}}\right) \tag{45}$$

where Δl is the sensitivity of the l-th attribute and εN,l is the corresponding privacy budget. The perturbed graph data finally published by the node are:

$$\tilde{y}_i(t)=[\tilde{x}_i(t),\tilde{a}_i^k(t),\tilde{w}_i(t)] \tag{46}$$

5.3. Dynamic Privacy Budget Allocation

A fixed privacy budget cannot adapt to the dynamic operating characteristics of the regenerative braking system. To balance control accuracy and privacy protection capability, this paper dynamically allocates the privacy budget according to the importance of nodes and edges to the control task. The node control importance is defined as:

$$\Omega_i(t)=\eta_1|P_i(t)|+\eta_2(1-S_i(t))+\eta_3 d_i(t)+\eta_4\sum_j\chi_{ij}(t) \tag{47}$$

where the terms denote node power magnitude, storage charging margin, node degree, and edge connectivity indicator, respectively. A higher node importance indicates a greater influence on braking force allocation and energy recovery efficiency. Under the total privacy budget constraint, budget allocation is completed according to node importance and edge relevance:

$$\varepsilon_{N,i}(t)=\varepsilon_N(t)\cdot\frac{\Omega_i(t)}{\sum_{j=1}^{n}\Omega_j(t)+\varepsilon} \tag{48}$$

$$\varepsilon_{E,ij}(t)=\varepsilon_E(t)\cdot\frac{R_{ij}(t)}{\sum_{(p,q)\in E}R_{pq}(t)+\varepsilon} \tag{49}$$

Upper and lower bounds of the budget are also set to avoid extreme perturbation intensity:

$$\varepsilon_{\min}\le\varepsilon_{N,i}(t),\varepsilon_{E,ij}(t)\le\varepsilon_{\max} \tag{50}$$

This strategy allocates a higher privacy budget to core braking nodes and key energy interaction edges, thereby reducing control error, while increasing perturbation for non-critical nodes and edges to enhance privacy security.

5.4. Privacy-Utility Theoretical Analysis

Under the standard composition property of differential privacy [9,12], if the node-attribute mechanism satisfies εN-NA-LDP and the edge mechanism satisfies εE-Edge-LDP, then releasing both outputs yields the following joint

mechanism for the combined node-attribute/edge neighboring relation:

$$\mathrm{M}(G) = \left(\mathrm{M}_N(\mathbf{X}), \mathrm{M}_E(\mathbf{A}, \mathbf{W})\right) \tag{51}$$

satisfies an εN+εE-LDP bound for the combined release:

$$\varepsilon_{\text{total}} = \varepsilon_N + \varepsilon_E \tag{52}$$

Under the randomized response mechanism [11,27], the unbiased estimator of the edge state is:

$$\hat{a}_{ij} = \frac{\tilde{a}_{ij}(t) - (1-p)}{2p-1} \tag{53}$$

A larger εE leads to a smaller edge-state estimation error, but the strength of edge-relationship privacy protection decreases accordingly. The perturbation error introduced by the Laplace mechanism [9,12] satisfies:

$$\mathrm{E}\left[\left(\tilde{x}_{i,l} - x_{i,l}\right)^2\right] = 2\left(\frac{\Delta_l}{\varepsilon_{N,l}}\right)^2 \tag{54}$$

A smaller εN provides stronger node-attribute privacy protection, but the errors of control inputs such as SOC, power, and voltage increase accordingly. The system control utility loss function is defined as:

$$L = \left|\eta_{\text{rec}} - \tilde{\eta}_{\text{rec}}\right| + \lambda \left\|\mathbf{u}^* - \tilde{\mathbf{u}}^*\right\|_2^2 \tag{55}$$

where ηrec and the corresponding perturbed value denote the energy recovery efficiencies under raw and perturbed data, respectively, and u* and its perturbed counterpart denote the corresponding control commands. The essence of privacy budget allocation is to achieve an optimal trade-off between privacy security and system control utility.

In summary, the proposed dual-granularity privacy protection mechanism relies on NA-LDP and Edge-LDP to protect continuous node attributes and topological edge relationships, respectively. Combined with dynamic budget allocation, it reduces perturbation bias in key features and provides a secure, lightweight, and highly usable graph publication scheme for regenerative braking control systems with privacy protection requirements.

6. Privacy-Preserving Regenerative Braking Control Strategy

Based on the preceding distributed graph publication and dual-granularity privacy perturbation, the control end obtains perturbed graph features rather than the original topology graph. Therefore, the regenerative braking control strategy must ensure the decision robustness of braking power allocation, storage SOC variation, and energy recovery efficiency under privacy perturbation. This paper builds a deep reinforcement learning control framework that integrates privacy-protected graph features to realize regenerative braking force allocation and energy storage power scheduling under privacy constraints. The privacy-preserving deep reinforcement learning control framework is shown in Fig. 6.

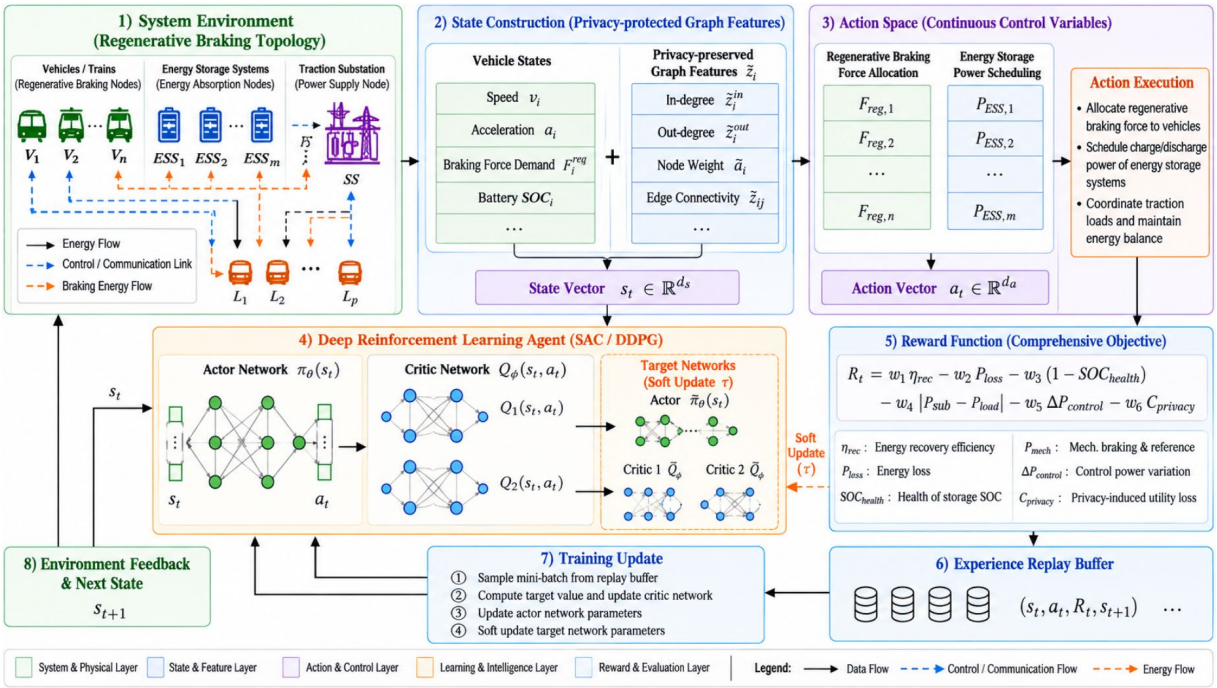

Figure 6. Privacy-aware SAC/DDPG regenerative braking control

As shown in Fig. 6, the controller uses vehicle operating states and privacy-protected graph features as inputs, outputs the regenerative braking force allocation coefficient and storage power scheduling variable through SAC/DDPG, and constructs reward feedback by considering energy recovery, SOC constraints, and privacy loss. The framework can realize regenerative braking optimization control while protecting node and edge information.

6.1. Braking Control Framework Based on Deep Reinforcement Learning

The regenerative braking control problem is modeled as a Markov decision process:

$$\mathrm{M} = (\mathrm{S}, \mathrm{A}, \mathrm{P}, \mathrm{R}, \gamma) \tag{56}$$

where S is the state space, A is the action space, P is the state transition function, R is the reward function, and γ is the discount factor.

Because regenerative braking force allocation and energy storage power scheduling are both continuous control problems, SAC [32] or DDPG [33] is selected as the basic policy optimization method. The control state is jointly composed of vehicle operating states and privacy-protected graph features:

$$\mathbf{s}(t) = \left[\mathbf{o}(t),\ \tilde{\mathbf{G}}_c(t) \right] \tag{57}$$

where o(t) includes vehicle speed, braking demand, storage SOC, voltage margin, and load demand, and the graph feature term denotes the privacy-perturbed graph control features. The control action is defined as:

$$\mathbf{a}(t) = \left[\mu^{\mathrm{reg}}(t), P_{\mathrm{ess}}(t) \right] \tag{58}$$

where the first term denotes the regenerative braking force allocation coefficient and the second term denotes the charging/discharging power of the energy storage system. The corresponding regenerative braking force is expressed as:

$$F_e^*(t) = \mu^{\mathrm{reg}}(t) F_b^{\mathrm{dem}}(t) \tag{59}$$

The control action must simultaneously satisfy braking safety, energy storage power, and SOC operating boundary constraints:

$$0 \le \mu^{\mathrm{reg}}(t) \le 1, \quad S^{\min} \le S(t) \le S^{\max}, \quad \left| P_{\mathrm{ess}}(t) \right| \le P_{\mathrm{ess}}^{\max} \tag{60}$$

6.2. Robust Graph-Feature Input Under Privacy Perturbation

Node-attribute local differential privacy (NA-LDP) and edge local differential privacy (Edge-LDP) introduce random deviations into graph features. To weaken the influence of perturbation on control decisions, this paper smooths the perturbed graph features over time:

$$\alpha \tilde{\mathbf{G}}_c(t) + (1-\alpha) \overline{\mathbf{G}}_c(t-1) \tag{61}$$

where the parameter denotes the smoothing coefficient. A perturbation uncertainty vector is further introduced:

$$\boldsymbol{\sigma}_G(t) = \left[\sigma_X(t), \sigma_A(t), \sigma_W(t) \right] \tag{62}$$

The three terms represent the uncertainties of node attributes, adjacency relationships, and edge-weight features, respectively. The final control input is constructed as:

$$\mathbf{s}^p(t) = \left[\mathbf{o}(t), \overline{\mathbf{G}}_c(t), \boldsymbol{\sigma}_G(t) \right] \tag{63}$$

This input structure allows the control policy to perceive the credibility of graph features. When perturbation is strong, the dependence on topology information is reduced; when perturbation is weak, graph structure information is fully utilized to improve the control effect.

6.3. Reward Function Design Considering Privacy Loss

To simultaneously optimize energy recovery, braking safety, SOC constraints, and privacy budget consumption, the reward function is constructed as follows:

$$r(t) = \lambda_1 r_{\mathrm{rec}}(t) + \lambda_2 r_{\mathrm{soc}}(t) + \lambda_3 r_{\mathrm{safe}}(t) + \lambda_4 r_{\mathrm{priv}}(t) \tag{64}$$

where rrec(t) is the energy recovery reward, rsoc(t) is the SOC out-of-bounds penalty, rsafe(t) is the braking safety penalty, and rpriv(t) is the privacy loss term. The terms are defined as follows:

$$r_{\mathrm{rec}}(t) = \frac{P_{\mathrm{rec}}(t)}{P_r^{\mathrm{sum}}(t) + \varepsilon} \tag{65}$$

$$r_{\mathrm{priv}}(t) = \frac{\varepsilon_N(t) + \varepsilon_E(t)}{\varepsilon_{\mathrm{tot}}} \tag{66}$$

The privacy loss term is used to limit excessive consumption of the privacy budget, ensuring that the policy maintains the privacy protection level while improving energy recovery efficiency.

6.4. Control Policy Optimization Under Dual-Granularity Constraints

Under dual-granularity privacy constraints, the control policy optimization objective is:

$$\arg\max_{\pi} \mathrm{E}_{\pi} \left[\sum_{t=1}^{T} \gamma^{t-1} r(t) \right] \tag{67}$$

It must satisfy the privacy budget constraints:

$$\varepsilon_N(t) + \varepsilon_E(t) \le \varepsilon_{\mathrm{tot}}, \quad \varepsilon_N(t) < \varepsilon_E(t) \tag{68}$$

The control action must also satisfy the feasible action domain:

$$\mathbf{a}(t) \in \mathrm{A}_c \tag{69}$$

where the feasible action set is determined by braking safety, motor performance, energy storage power, and SOC boundaries.

For different algorithms, differentiated optimization is adopted. SAC improves policy exploration by maximizing entropy-regularized cumulative rewards, while DDPG relies on deterministic policy gradients to optimize in continuous action spaces. Both algorithms use the privacy-processed robust state as input and output the regenerative braking force allocation coefficient and the energy storage charging/discharging power.

In summary, this paper incorporates perturbed graph features into a deep reinforcement learning control framework. By combining robust input design, a privacy-loss reward function, and dual-granularity privacy budget constraints, the regenerative braking control strategy can maintain high energy recovery efficiency and operational stability even when node and edge information is protected.

7. Simulation and Result Analysis

7.1. Experimental Platform and Parameters

The simulation platform contains four coupled modules: the regenerative-braking plant, dynamic topology generation, privacy-preserving graph publication, and the SAC-based control module. All comparison methods share the same plant, topology sequence, normalized inputs, and controller architecture so that performance differences are attributable to the privacy mechanism.

The default network contains vehicle, energy-storage, substation, and load nodes connected by energy-interaction, braking-association, and communication edges. Continuous node and edge attributes are normalized to [0,1] before sensitivity calibration and privacy perturbation.

The reported results use a discrete control step, a fixed operating horizon, top-k adjacency pruning, and low-dimensional control-sensitive projection. The privacy-budget sensitivity experiment varies the total budget while retaining the same operating trajectories and random-seed protocol.

The comparison set includes No Privacy, NA-LDP only, Edge-LDP only, Fixed Dual-LDP, and the proposed adaptive dual-granularity mechanism. SAC [32] is used as the default continuous-action optimizer, whereas DDPG [33] is retained as an alternative implementation of the same state, action, and reward definitions. All methods use the same topology sequence and evaluation protocol. Because only aggregate outputs from the original simulations are available, this version does not claim run-level standard deviations; the resulting reproducibility limitation is stated in Section 7.5.

The complete network, privacy, attack-evaluation, and controller settings are summarized in Table 1.

Table 1. Main simulation, privacy, attack, and controller settings

Category	Parameter	Symbol	Setting
Network	Node composition	n	72 nodes: 36 vehicles, 12 ESS units, 8 substations, and 16 loads
Network	Raw node-feature dimension	d	9 normalized features
Compression	Retained neighbors / projected dimension	k / r	6 / 8; (r+2k)/(n+d)=24.7%
Simulation	Control step / operating horizon	Δt / T	0.1 s / 600 s
Operating range	Vehicle speed / storage SOC	v / S	0-80 km h^-1 / 0.20-0.90
Communication	Delay / reliability	τ / ρ	5-50 ms / 0.90-1.00
Privacy	Total budget values / default	εtot	{0.5, 1.0, 2.0, 4.0, 8.0} / 2.0
Privacy	Initial attribute-edge split	εN / εE	0.8 / 1.2 before importance-based reallocation
Privacy	Budget bounds / normalized sensitivity	εmin, εmax / Δl	0.05, 4.0 / 1.0
SAC	Actor and critic networks	-	Two hidden layers, 256 units per layer

SAC	Learning rate / discount / target update	α / γ / τSAC	3×10^-4 / 0.99 / 0.005
Training	Batch / replay buffer / episodes	-	256 / 10^6 / 1000
Statistics	Reporting protocol	-	Aggregate outputs under a common evaluation protocol; run-level standard deviations are not available
Attack test	Attempts / node-state tolerance	Natt / δx	10,000 / 0.05 in normalized units

7.2. Evaluation Metrics

This paper adopts multiple types of indicators for comprehensive performance evaluation, as defined below.

1) Privacy Protection Strength

Privacy strength is characterized by the node-attribute privacy budget εN, edge-level privacy budget εE, and total privacy budget εtot. A smaller privacy budget indicates stronger privacy protection, whereas a larger budget indicates higher data publication utility.

2) Graph Publication Utility

Mean squared error and mean absolute error are used to quantify the feature deviation between the perturbed graph and the original graph:

$$\mathrm{MSE}_G = \frac{1}{N}\sum_{i=1}^{N}\left(z_i - \tilde{z}_i\right)^2 \tag{70}$$

$$\mathrm{MAE}_G = \frac{1}{N}\sum_{i=1}^{N}\left|z_i - \tilde{z}_i\right| \tag{71}$$

where the terms denote the original graph features and the perturbed graph features, respectively.

3) Braking Control Performance

The energy recovery efficiency is defined as:

$$\eta_{\mathrm{rec}} = \frac{\sum_{t=1}^{T} P_{\mathrm{rec}}(t)\Delta t}{\sum_{t=1}^{T} P_r^{\mathrm{sum}}(t)\Delta t + \varepsilon} \tag{72}$$

SOC stability is measured by the SOC out-of-bounds penalty:

$$J_{\mathrm{SOC}} = \sum_{t=1}^{T}\left[\max(0, S(t) - S^{\max}) + \max(0, S^{\min} - S(t))\right] \tag{73}$$

The impact on battery life is approximated by the charge-discharge power fluctuation penalty:

$$J_{\mathrm{bat}} = \sum_{t=1}^{T}\left|P_{\mathrm{bat}}(t) - P_{\mathrm{bat}}(t-1)\right| \tag{74}$$

Smaller values of these indicators indicate smoother operation of the energy storage system and less influence on battery life.

4) Simulated Privacy Disclosure Evaluation

The honest-but-curious edge-aggregator model is retained to characterize potential disclosure, but the current study does not include an independently trained adversarial model or externally validated attack benchmark. Equation (75) therefore defines a simulation-derived joint disclosure indicator: an instance is counted when the reconstructed edge agrees with the original edge and the inferred normalized node state lies within δx of the original value.

$$\mathrm{ASR} = \frac{1}{N_{\mathrm{att}}}\sum_{q=1}^{N_{\mathrm{att}}}\mathbf{1}\left(\hat{A}_q = A_q \wedge \left|\hat{x}_q - x_q\right| \le \delta_x\right) \tag{75}$$

The sensitivity experiment uses Natt=10,000 sampled node-edge instances and δx=0.05. Accordingly, Table 3 reports a simulated joint disclosure rate generated by the original experimental procedure, rather than attack accuracy obtained from a separately trained adversary. Releasing the per-attempt records and evaluation code is necessary before these percentages can be treated as an independently reproducible attack benchmark.

5) Theoretical Privacy-Utility Bound and Budget Optimization

Proposition 1. Assume that the feature projection is Lg-Lipschitz and the control policy is Lπ-Lipschitz. For normalized node attributes perturbed by Laplace noise and retained edges estimated through randomized response, define the aggregate perturbation factor as follows:

$$B(\varepsilon) = \sum_{I} 2\left(\frac{\Delta_I}{\varepsilon_{N,I}}\right)^2 + \sum_{e\in E'}\omega_e^2\frac{e^{\varepsilon_{E,e}}}{\left(e^{\varepsilon_{E,e}}-1\right)^2} \tag{76}$$

The first term follows from the variance of the Laplace mechanism, and the second term follows from the variance of the unbiased randomized-response estimator in Eq. (53). Consequently, the graph-feature error and the control-utility loss are bounded by:

Proof sketch. Conditional on the allocated privacy budgets, let z_N denote mutually independent zero-mean Laplace perturbations, where $\mathrm{Var}\left(z_{N,I}\right) = 2\left(\Delta_I / \varepsilon_{N,I}\right)^2$. Let zE denote the mutually independent centered errors of the unbiased binary randomized-response estimators. For $p_e = e^{\varepsilon_{E,e}} / \left(e^{\varepsilon_{E,e}} + 1\right)$, the corresponding estimation-error

variance is $p_e(1-p_e)/(2p_e-1)^2 = e^{\varepsilon_{E,e}}/\left(e^{\varepsilon_{E,e}}-1\right)^2$. Because both noise components are zero-mean and mutually independent, the expected squared norm of the weighted aggregate perturbation is B(Ɛ) in Eq. (76). Let Φ denote the graph-feature mapping and assume that it is Lg-Lipschitz. It follows that

$$\mathsf{E}\left[\|\tilde{\mathbf{g}}-\mathbf{g}\|_2^2\right] \le L_g^2 B(\boldsymbol{\varepsilon}) \tag{77}$$

Furthermore, assume that the energy-recovery function is Lη-Lipschitz with respect to the graph features and that the control policy π is Lπ-Lipschitz. For the utility loss defined in Eq. (55), the Cauchy–Schwarz inequality yields:

$$\mathsf{E}[L] \le \left(L_\eta + \lambda_u L_\pi\right) L_g \sqrt{B(\boldsymbol{\varepsilon})} \tag{78}$$

This result is an upper bound under the normalization, conditional-independence, and Lipschitz assumptions and is not claimed to be tight.

This bound yields the following dual-granularity privacy allocation problem:

$$\varepsilon^* = \arg\min_{\varepsilon} B(\varepsilon)$$
$$\text{s. t.} \sum_i \varepsilon_{N,i} + \sum_e \varepsilon_{E,e} \le \varepsilon_{\text{tot}}, \quad \varepsilon_{\min} \le \varepsilon \le \varepsilon_{\max}, \quad \varepsilon_{N,i} \le \varepsilon_{E,e} \tag{79}$$

The importance-weighted rules in Eqs. (48)-(50) are used as a low-complexity online surrogate for Eq. (79): larger budgets are assigned to terms that contribute more strongly to B(ε) and to the control objective. The bound also explains the monotonic trends in Table 3 and Fig. 8.

7.3. Comparative Experiments and Analysis

All five privacy mechanisms are evaluated with identical topology, operating profiles, normalized inputs, and SAC hyperparameters. Figure 7 visualizes the main trade-offs, and Table 2 reports the corresponding numerical results.

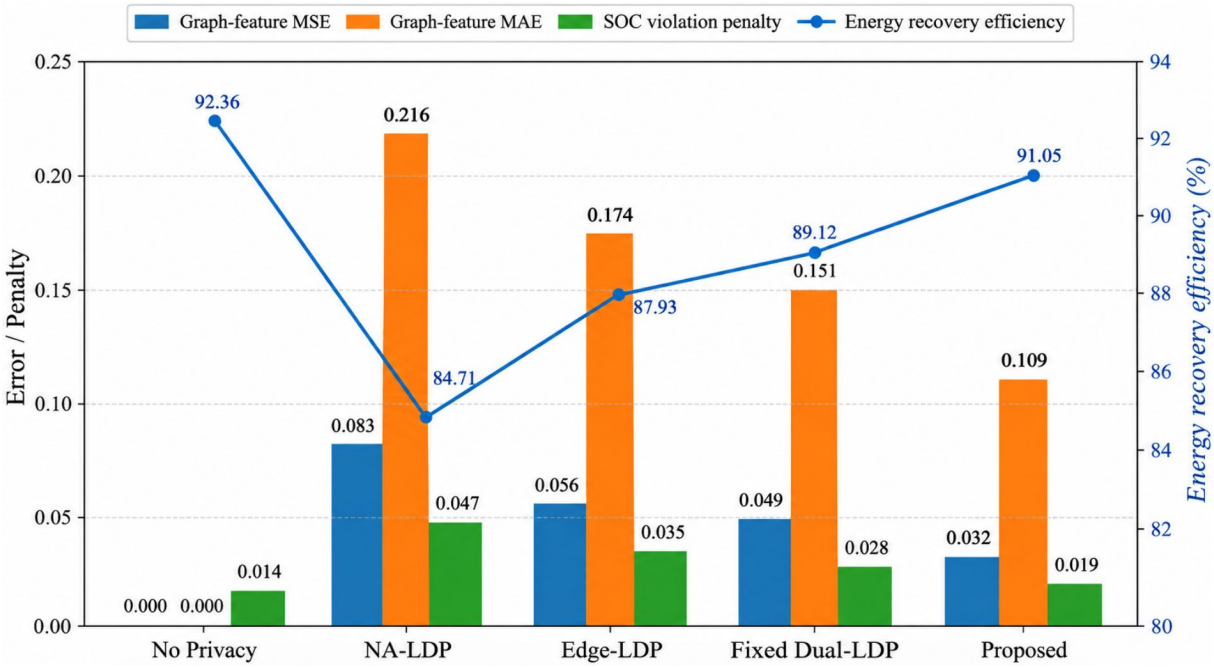

Figure 7. Publication utility and control performance across privacy mechanisms

As shown in Fig. 7, the Proposed method retains control performance close to No Privacy while substantially reducing graph-feature error and SOC violations relative to the single-granularity mechanisms.

Table 2. Graph publication utility and control performance of different methods

Method	Graph Feature MSE	Graph Feature MAE	Energy Recovery Efficiency / %	SOC Out-of-Bounds Penalty	Battery Power Fluctuation
No Privacy	0	0	92.36	0.014	1.000
NA-LDP	0.083	0.216	84.71	0.047	1.286
Edge-LDP	0.056	0.174	87.93	0.035	1.192
Fixed Dual-LDP	0.049	0.151	89.12	0.028	1.108
Proposed	0.032	0.109	91.05	0.019	1.041

Table 2 confirms that the NA-LDP-only baseline incurs the largest utility loss, whereas Edge-LDP better preserves topology but does not fully protect continuous node states. Relative to Fixed Dual-LDP, dynamic budget allocation reduces MSE from 0.049 to 0.032 and increases energy recovery efficiency from 89.12% to 91.05%. The influence of ε_{tot} is reported in Table 3.

Table 3. Sensitivity analysis under different privacy budgets

ε_{tot}	Graph Feature MSE	Graph Feature MAE	Energy Recovery Efficiency / %	Simulated Joint Disclosure Rate / %
0.5	0.071	0.226	87.42	52.8
1.0	0.048	0.169	89.63	59.4
2.0	0.032	0.109	91.05	67.1
4.0	0.021	0.081	91.68	75.6
8.0	0.014	0.057	92.03	83.9

Table 3 and Fig. 8 exhibit the expected privacy-utility trade-off: increasing ε_{tot} reduces perturbation and improves graph/control utility, but simultaneously raises the simulated joint disclosure rate. The default $\varepsilon_{tot}=2.0$ yields 91.05% recovery efficiency and a 67.1% simulated disclosure rate, providing a middle operating point between stronger privacy and higher control utility.

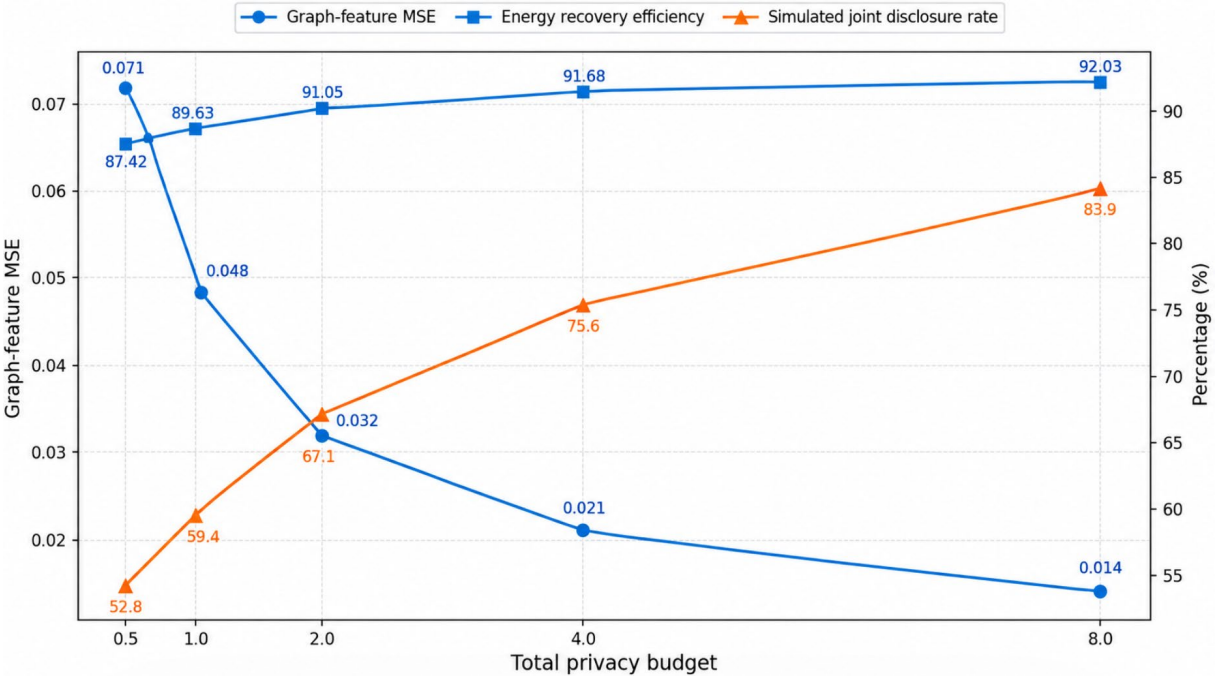

Figure 8. Effects of the total privacy budget on utility, control, and simulated joint disclosure

To isolate the contribution of each component, the full model is compared with four ablated variants in Table 4.

Table 4. Ablation study results

Method	Adjacency Pruning	Graph Projection	Dynamic Budget	Robust Input	Energy Recovery Efficiency / %	Graph Feature MSE
Full model	✓	✓	✓	✓	91.05	0.032
w/o pruning	×	✓	✓	✓	90.42	0.039
w/o projection	✓	×	✓	✓	90.11	0.043
w/o dynamic budget	✓	✓	×	✓	89.12	0.049
w/o robust input	✓	✓	✓	×	89.76	0.036

Table 4 identifies dynamic budgeting as the most influential component: removing it increases MSE to 0.049 and reduces energy recovery efficiency to 89.12%. Robust input smoothing is the next most important control-side module, whereas pruning and projection primarily reduce redundancy and communication load. The communication comparison is reported in Table 5.

Table 5. Communication overhead of different graph publication methods

Method	Per-node Upload Dimension	Communication Complexity	Relative Communication Overhead / %
Full adjacency upload	(n+d)	O(n)	100
Edge-LDP full vector	(n+d)	O(n)	100
Top-k pruning	(2k+d)	O(k+d)	25.9
Proposed	(r+2k)	O(k+r)	24.7

Table 5 shows that full adjacency upload and full-vector Edge-LDP retain O(n) communication. A top-k sparse baseline must transmit both neighbor indices and edge weights in addition to the d raw node features, so its per-node dimension is 2k+d, corresponding to 25.9% under Table 1 rather than the previously reported 36.4%. The proposed method replaces the d raw features with the r-dimensional control-sensitive projection and therefore requires r+2k values per node, corresponding to 24.7% of full transmission.

Taken together, Tables 2-5 show that the proposed mechanism improves graph utility and control stability without sacrificing the communication advantage of local lightweight publication.

7.4. Robustness Verification Under Operating Conditions

Robustness is evaluated under load, slope, communication-delay, and random edge-disconnection disturbances. The corresponding results are listed in Table 6.

Table 6. Robustness under different operating conditions

Working Condition	Graph Feature MSE	Energy Recovery Efficiency / %	SOC Out-of-Bounds Penalty	Control Action Fluctuation
Baseline Condition	0.032	91.05	0.019	1.000
20% Load Increase	0.035	90.12	0.023	1.067
30% Slope Increase	0.038	89.64	0.026	1.094
50% Communication Delay Increase	0.041	88.97	0.031	1.138
10% Random Edge Disconnection	0.045	88.43	0.034	1.176

Table 6 shows a gradual, bounded degradation as the disturbance severity increases. Under 10% random edge disconnection, the graph-feature MSE rises to 0.045 and energy recovery efficiency decreases by 2.62 percentage points, while the SOC penalty remains 0.034. This behavior is attributable to key-edge retention, dynamic budget prioritization, and temporal smoothing of perturbed features.

Networked-control studies show that communication delay, packet loss, and other network imperfections can degrade closed-loop estimation and control performance [34].

This general result supports the use of key-edge retention and temporally smoothed graph features in the present robustness tests, although [34] does not directly validate the numerical values reported in Table 6.

Across all disturbances, control-action fluctuation remains below 1.176, and no unstable oscillation is observed in the simulated horizon.

These results support the numerical robustness of the lightweight publication, dual-granularity privacy, and privacy-aware control modules under the tested conditions.

7.5. Comparison with Privacy-Preserving Control and Deployment Limitations

Recent privacy-preserving control studies include affine masking for nonlinear cloud MPC [35], finite-budget differentially private distributed MPC with stability guarantees [36], adaptive differential-privacy protection for federated edge communication [37], decentralised multi-agent coordination for distributed solar-storage systems [38], and hardware-in-the-loop validated federated energy management for connected hybrid electric vehicles [39].

Table 7 highlights the methodological differences between these approaches and the proposed graph-publication mechanism.

Table 7. Comparison with representative privacy-preserving control frameworks

Framework	Privacy/control principle	Formal guarantee	Applicability and principal limitation
Affine-masked cloud MPC [35]	Transforms states and inputs before cloud optimization	Algebraic indistinguishability; no control degradation	Lightweight for nonlinear MPC, but assumes a cloud formulation and does not protect graph topology
DP-DMPC [36]	Adds calibrated noise to distributed dual variables	Finite ε-DP, convergence, recursive feasibility, and stability	Strong theory for linear constrained systems; not designed for dynamic node/edge publication
Adaptive-DP federated edge privacy [37]	Local model training, adaptive DP perturbation, and edge aggregation without transmitting raw sensing data	Adaptive differential privacy with a performance-loss constraint; no node-attribute/edge-LDP distinction	Relevant to local perturbation and edge aggregation, but not graph-topology privacy or regenerative braking control
Decentralised solar-storage coordination [38]	Hierarchical PPO/MADDPG, a DAG-based execution ledger, and Paillier encryption for distributed-energy scheduling	Cryptographic protection and verifiable execution; no explicit node-attribute/edge-LDP guarantee	Relevant to distributed storage coordination and secure graph-supported energy management, but not regenerative braking energy flows
Federated connected-HEV ITEM [39]	Federated multi-agent energy and thermal control	Data locality with HIL feasibility evidence	Strong vehicle deployment relevance, but no explicit graph release or dual-granularity LDP
Proposed method	Local NA-LDP + Edge-LDP, pruning, projection, and SAC control	$\varepsilon N+\varepsilon E$ composition and the bound in Eqs. (76)-(78)	Protects states and relationships with low communication; current validation remains simulation-based

The present study is simulation-based. The trajectories and operating ranges in Table 1 are representative parameterized profiles rather than field-measured records from a specific rail line or mining fleet; therefore, the reported gains should not be interpreted as field certification. In addition, only aggregate outputs from the original simulation runs are available, so run-level variance, confidence intervals, and independent attack logs cannot be reconstructed from the current records. Real deployment requires hardware-in-the-loop testing, fail-safe mechanical-braking supervision, sensor-drift calibration, long-horizon privacy accounting,

latency measurements on embedded controllers, and preservation of complete experimental logs.

Scalability is also bounded by the growth of privacy composition over time and by aggregation/reconstruction costs at very large node counts, even though the local upload complexity remains O(k+r). Future work will validate the method using authorized rail/mining operational data, asynchronous communication, larger dynamic graphs, and a hardware-in-the-loop or digital-twin platform.

8. Conclusion

This paper proposes a lightweight distributed graph publication and dual-granularity privacy protection method for regenerative braking control. Through dynamic graph modeling, adjacency pruning, and control feature projection, the per-node upload dimension is compressed to r + 2k, and the relative communication overhead is reduced to 24.7%. Through NA-LDP/Edge-LDP and dynamic budget allocation, the proposed method achieves a graph-feature MSE of 0.032 and an energy recovery efficiency of 91.05% when εtot = 2.0. Compared with NA-LDP, the MSE is reduced by 61.45% and the energy recovery efficiency is increased by 6.34 percentage points. Compared with the fixed dual-granularity mechanism, the energy recovery efficiency is improved by 1.93 percentage points and the SOC out-of-bounds penalty is reduced to 0.019. Robustness tests show that under a 20% load increase, 30% slope increase, 50% communication delay increase, and 10% random edge disconnection, the system still maintains an energy recovery efficiency of 88.43%-90.12%, demonstrating that the proposed method can maintain good control performance under privacy protection constraints.

Acknowledgements.

Jiangsu Provincial Funding for Basic Science Research in Higher Education Institutions (Natural Science) Project - Study on Thermal Rise Characteristics of Vehicle Brake System for Long Downhill Driving of Pure Electric Commercial Vehicles（24KJB580012）

References

[1] Szumska E M. Regenerative Braking Systems in Electric Vehicles: A Comprehensive Review of Design, Control Strategies, and Efficiency Challenges[J]. Energies, 2025, 18(10): 2422.

[2] Khodaparastan M, Mohamed A A, Brandauer W. Recuperation of Regenerative Braking Energy in Electric Rail Transit Systems[J]. IEEE Transactions on Intelligent Transportation Systems, 2019, 20(8): 2831-2847.

[3] Domínguez M, Fernández-Cardador A, Fernández-Rodríguez A, Cucala A P, Pecharromán R R, Urosa Sánchez P, Vadillo Cortázar I. Review on the Use of Energy Storage Systems in Railway Applications[J]. Renewable and Sustainable Energy Reviews, 2025, 207: 114904.

[4] Li G, Or S W. Multi-Agent Deep Reinforcement Learning-Based Multi-Time Scale Energy Management of Urban Rail Traction Networks with Distributed Photovoltaic–Regenerative Braking Hybrid Energy Storage Systems[J]. Journal of Cleaner Production, 2024, 466: 142842.

[5] Zhong Z, Mi J, Zhao Y, Yang Z, Lin F. Coordinated Control of the Onboard and Wayside Energy Storage System of an Urban Rail Train Based on Rule Mining[J]. Urban Rail Transit, 2024, 10: 232-247.

[6] Yang X, Li X, Ning B, Tang T. A Survey on Energy-Efficient Train Operation for Urban Rail Transit[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(1): 2-13.

[7] Zhu F, Yang Z, Lin F, Xin Y. Decentralized Cooperative Control of Multiple Energy Storage Systems in Urban Railway Based on Multiagent Deep Reinforcement Learning[J]. IEEE Transactions on Power Electronics, 2020, 35(9): 9368-9379.

[8] Yang Z, Zhu F, Lin F. Deep-Reinforcement-Learning-Based Energy Management Strategy for Supercapacitor Energy Storage Systems in Urban Rail Transit[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(2): 1150-1160.

[9] Dwork C, McSherry F, Nissim K, Smith A. Calibrating Noise to Sensitivity in Private Data Analysis[C]//Theory of Cryptography Conference. Berlin: Springer, 2006: 265-284.

[10] Kasiviswanathan S P, Lee H K, Nissim K, Raskhodnikova S, Smith A. What Can We Learn Privately?[J]. SIAM Journal on Computing, 2011, 40(3): 793-826.

[11] Erlingsson Ú, Pihur V, Korolova A. RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response[C]//Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2014: 1054-1067.

[12] Wang T, Zhang X, Feng J, Yang X. A Comprehensive Survey on Local Differential Privacy toward Data Statistics and Analysis[J]. Sensors, 2020, 20(24): 7030.

[13] Mueller T T, Usynin D, Paetzold J C, Braren R, Rueckert D, Kaissis G. Differentially Private Guarantees for Analytics and Machine Learning on Graphs: A Survey of Results[J]. Journal of Privacy and Confidentiality, 2024, 14(1).

[14] Li Y, Purcell M, Rakotoarivelo T, Smith D, Ranbaduge T, Ng K S. Private Graph Data Release: A Survey[J]. ACM Computing Surveys, 2023, 55(11): 1-39.

[15] Liu P, Xu Y, Jiang Q, Tang Y, Guo Y, Wang L, Li X. Local Differential Privacy for Social Network Publishing[J]. Neurocomputing, 2020, 391: 273-279.

[16] Qin Z, Yu T, Yang Y, Khalil I, Xiao X, Ren K. Generating Synthetic Decentralized Social Graphs with Local Differential Privacy[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2017: 425-438.

[17] Wei C, Ji S, Liu C, Chen W, Wang T. AsgLDP: Collecting and Generating Decentralized Attributed Graphs with Local Differential Privacy[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 3239-3254.

[18] Ye Q, Hu H, Au M H, Meng X, Xiao X. LF-GDPR: A Framework for Estimating Graph Metrics with Local Differential Privacy[J]. IEEE Transactions on Knowledge and Data Engineering, 2022, 34(10): 4905-4920.

[19] Imola J, Murakami T, Chaudhuri K. Locally Differentially Private Analysis of Graph Statistics[C]//30th USENIX Security Symposium. Berkeley: USENIX Association, 2021: 983-1000.

[20] Liu S, Cao Y, Murakami T, Yoshikawa M. A Crypto-Assisted Approach for Publishing Graph Statistics with Node Local Differential Privacy[C]//2022 IEEE International Conference on Big Data. Piscataway: IEEE, 2022: 5765-5774.

[21] Hou L, Ni W, Zhang S, Fu N, Zhang D. Wdt-SCAN: Clustering Decentralized Social Graphs with Local Differential Privacy[J]. Computers & Security, 2023, 125: 103036.

[22] Chen B, Hawkins C, Yazdani K, Hale M. Edge Differential Privacy for Algebraic Connectivity of Graphs[C]//Proceedings

of the 60th IEEE Conference on Decision and Control. Piscataway: IEEE, 2021: 276-281.
[23] Yuan Q, Zhang Z, Du L, Chen M, Cheng P, Sun M. PrivGraph: Differentially Private Graph Data Publication by Exploiting Community Information[C]//32nd USENIX Security Symposium. Berkeley: USENIX Association, 2023: 3241-3258.
[24] Li Z, Li R H, Liao M, Jin F, Wang G. Privacy-Preserving Graph Embedding Based on Local Differential Privacy[C]//Proceedings of the 33rd ACM International Conference on Information and Knowledge Management. New York: ACM, 2024: 1316-1325.
[25] Mendonça A L C, Brito F T, Machado J C. PEG: Local Differential Privacy for Edge-Labeled Graphs[C]//Proceedings of the 28th International Conference on Extending Database Technology. OpenProceedings.org, 2025: 490-502.
[26] Xu W, Qiao P, Liu S, Zheng Z, Cao Y, Li Z. Continuous Publication of Weighted Graphs with Local Differential Privacy[J]. Proceedings of the VLDB Endowment, 2025, 18(11): 4214-4226.
[27] Mundra P, Papamanthou C, Shun J, Liu Q C. Practical and Accurate Local Edge Differentially Private Graph Algorithms[J]. Proceedings of the VLDB Endowment, 2025, 18(11): 4199-4213.
[28] Spielman D A, Srivastava N. Graph Sparsification by Effective Resistances[J]. SIAM Journal on Computing, 2011, 40(6): 1913-1926.
[29] Batson J, Spielman D A, Srivastava N. Twice-Ramanujan Sparsifiers[J]. SIAM Journal on Computing, 2012, 41(6): 1704-1721.
[30] Ahn K J, Guha S, McGregor A. Graph Sketches: Sparsification, Spanners, and Subgraphs[C]//Proceedings of the 31st ACM SIGMOD-SIGACT-SIGAI Symposium on Principles of Database Systems. New York: ACM, 2012: 5-14.
[31] Li T, Fu M, Xie L, Zhang J F. Distributed Consensus with Limited Communication Data Rate[J]. IEEE Transactions on Automatic Control, 2011, 56(2): 279-292.
[32] Haarnoja T, Zhou A, Abbeel P, Levine S. Soft Actor-Critic: Off-Policy Maximum Entropy Deep Reinforcement Learning with a Stochastic Actor[C]//Proceedings of the 35th International Conference on Machine Learning. PMLR, 2018, 80: 1861-1870.
[33] Lillicrap T P, Hunt J J, Pritzel A, Heess N, Erez T, Tassa Y, Silver D, Wierstra D. Continuous Control with Deep Reinforcement Learning[C]//International Conference on Learning Representations. 2016.
[34] Hespanha J P, Naghshtabrizi P, Xu Y. A Survey of Recent Results in Networked Control Systems[J]. Proceedings of the IEEE, 2007, 95(1): 138-162.
[35] Zhang K, Li Z, Wang Y, Li N. Privacy-Preserving Nonlinear Cloud-Based Model Predictive Control via Affine Masking[J]. Automatica, 2025, 171: 111939.
[36] Zhang K, Wang Y, Song Z, Li Z. Differentially Private Distributed Model Predictive Control of Linear Discrete-Time Systems With Global Constraints[J]. IEEE Transactions on Automatic Control, 2026, 71(4): 2676-2683.
[37] Xue J, Yan W. Edge Computing Communication Privacy Protection Method Based on Federated Learning Algorithm[J]. EAI Endorsed Transactions on Scalable Information Systems, 2026, 12(9).
[38] Li B, Ge Y F, Miao Y, Cui R, Li X, Wang K, Wang H. A Decentralised Coordination Framework for Demand-Side Solar-Storage and Its Electricity Market Participation[J]. EAI Endorsed Transactions on Scalable Information Systems, 2026, 12(8).
[39] Khalatbarisoltani A, Han J, Saeed M, Liu C Z, Hu X. Privacy-Preserving Integrated Thermal and Energy Management of Multi-Connected Hybrid Electric Vehicles With Federated Reinforcement Learning[J]. Applied Energy, 2025, 385: 125386.