

Vulnerable Node Detection in Complex Networks Based on Dynamic Comparator and Trusted Chain Propagation

Dongsheng Jing¹, Baozhen Qi¹, Yu Yang¹, Jingsong Xue¹, and Renjun Feng¹

State Grid Suzhou Power Supply Company
Suzhou Jiangsu 215004, China
qibz@js.sgcc.com.cn (corresponding author)
{jds_sz, yang_yu, js.xue, fengrj}@js.sgcc.com.cn

Abstract. Accurately identifying vulnerable nodes in complex networks is a critical challenge for preventing cascading failures and ensuring system robustness. Existing methods generally suffer from limitations such as static metrics that ignore dynamic loads, high parameter dependency, and a lack of unified fusion mechanisms. To address these issues, we propose an approach that is based on dynamic comparator selection and trusted chain propagation, which we refer to as Optimal Parameter (OP). Specifically, the proposed OP approach adaptively adjusts strategies based on node degree: low-degree nodes enable a lightweight mode to reduce overhead, while high-degree nodes employ full sampling to enhance reliability. State chain propagation is achieved through trusted queues, reducing the global detection complexity to linear order. Furthermore, the method integrates temporal consistency checks, faulty comparator isolation, and cross-layer comparison mechanisms to effectively handle complex scenarios such as malicious camouflage and low connectivity. Experimental results demonstrate that OP achieves a higher true positive rate and a lower false positive rate across multiple real-world datasets. It shows significant advantages, particularly at high attack edge density, thereby verifying its synergistic performance in terms of high accuracy and efficiency in large-scale networks.

Keywords: Complex Networks, Vulnerable Nodes, Dynamic Comparator, Trusted Chain Propagation, Robustness.

1. Introduction

Complex networks are currently popular worldwide. They serve as the backbone for various critical infrastructures, including power grids, global communication architectures, online social platforms, and intricate biological systems [6]. Due to the tight topological coupling and functional interdependencies inherent in these systems, they often exhibit extreme fragility to localized disruptions. Specifically, the failure or compromise of a small fraction of vulnerable nodes can trigger a severe systemic collapse through cascading effects. This phenomenon manifests profoundly across various domains: in social networks [17], malicious accounts or Sybil nodes can rapidly propagate misinformation to undermine community trust; in cyber-physical systems [5] like power grids, the tripping of an overloaded regional substation redistributes immense dynamic loads to adjacent

nodes, precipitating catastrophic large-scale blackouts; similarly, in distributed storage or communication networks [24], the incapacitation of core routing nodes can lead to massive network fragmentation, turning single-point failures into global paralysis. Given the immense scale, dynamic evolution, and nonlinear nature of failure propagation in contemporary networks, preemptively quantifying node vulnerability is extraordinarily complex [4]. How to efficiently and accurately identify such fault-prone nodes—balancing computational overhead with detection precision—remains a formidable and unresolved challenge.

Particularly in the energy sector, the layout of modern power systems has evolved from traditional centralized, top-down radial topologies to highly interconnected, distributed, complex networks [13]. With the massive integration of renewable energy sources, active distribution networks, and microgrids, the new power grid exhibits prominent network-structured characteristics. While this highly coupled network layout enhances energy transmission efficiency and flexibility, it also significantly amplifies the spatial vulnerability to cascading failures [23]. A localized malfunction at a single vulnerable node—such as an overloaded regional substation or a compromised distributed controller—can rapidly propagate through the complex interconnected topology, shifting dynamic loads to adjacent nodes and triggering large-scale blackouts. Therefore, analyzing the network-structured layout of modern power systems and accurately identifying their vulnerable nodes have become urgent prerequisites for ensuring energy security and system robustness.

To tackle this critical issue, existing node vulnerability detection methods can be broadly classified into three primary paradigms. First, approaches grounded in static topological analysis [8] utilize classical graph theory metrics—such as degree, betweenness, and eigenvector centrality—to evaluate node importance. While these methods are highly computationally efficient and mathematically interpretable, they inherently operate under a static assumption. By entirely neglecting the dynamic redistribution of traffic and functional loads, they suffer from a structural myopia that renders them incapable of identifying low-degree, high-risk nodes, which may be topologically marginal yet handle massive volumes of critical interactions. Second, dynamic cascading models [30] attempt to simulate the actual physical processes of failure propagation, such as load–capacity redistribution. Although these models align much closer with real-world physical realities, they impose stringent demands on precise prior knowledge. They heavily rely on node-specific parameters—such as exact capacity limits and real-time load states—which are notoriously difficult or impossible to obtain in large-scale, privacy-sensitive, or decentralized systems. Furthermore, the necessity for time-step-based simulations leads to prohibitive computational complexity, severely limiting their scalability. Third, multi-dimensional fusion methods [10] have recently emerged to holistically combine structural topologies, dynamic behaviors, and domain-specific functional features. Despite their comprehensive perspective, these approaches are frequently bottlenecked by their reliance on subjective heuristic rules and manually crafted weights to bridge heterogeneous data. They still lack a cohesive, unified theoretical framework. Consequently, these bespoke models exhibit weak cross-domain generalization and struggle to strike an optimal balance between computational efficiency and detection accuracy, particularly in high-noise environments or low-resource operational scenarios.

A compelling real-world paradigm illustrating this phenomenon can be found in the WLAN Authentication and Privacy Infrastructure (WAPI) [11]. To guarantee rigorous mutual authentication, WAPI employs a unique tri-element peer-to-peer architecture comprising the Station (STA), Access Point (AP), and Authentication Server Unit (ASU) [11]. While this centralized design significantly elevates the security baseline against external intrusions, it inadvertently transforms the topologically low-degree ASU servers into critical systemic bottlenecks. Despite having few direct structural connections compared to access points, the ASU bears the immense dynamic load of global cryptographic verifications. Consequently, an overload or localized failure at the ASU can instantly paralyze all dependent APs, disconnecting countless STAs in a rapid cascading collapse. This scenario profoundly exposes the true essence of vulnerable nodes: their criticality frequently stems from functional indispensability and dynamic load concentration rather than intuitive topological centrality. Furthermore, it highlights a critical structural paradox in which the very security mechanisms deployed to protect a system can inadvertently create new, hidden pathways for cascading failures.

To address the above challenges, we propose an approach for constructing a detection framework that balances robustness and efficiency, termed Optimal Parameter (OP). The OP approach adaptively selects comparators based on node degree: low-degree nodes enable a lightweight mode to reduce overhead, while high-degree nodes employ full sampling to enhance reliability. State chain propagation is achieved through trusted queues, reducing global detection complexity to linear order. Furthermore, the method integrates temporal consistency checks, faulty comparator isolation, and cross-layer comparison mechanisms to effectively handle complex scenarios, including malicious camouflage and structural sparsity. Experiments on multiple real-world datasets demonstrate that OP outperforms mainstream methods in both true positive rate (TPR) and false positive rate (FPR), showing significant advantages, especially under high attack density. This provides a solution that combines theoretical depth and engineering practicality for large-scale, complex networks. The conceptual impact of this transformation is illustrated in Figure 1, which contrasts the raw network chaos with the structural clarity achieved through our adaptive detection framework.

The remainder of this paper is organized as follows: Section 2 reviews related work, Section 3 details the methodology, Section 4 presents experimental results, and Section 5 concludes with future outlook.

2. Related Work

In complex networks, identifying vulnerable nodes whose failure could trigger cascading collapse has become a key topic in network science and system security. As systems such as smart grids, 5G networks, biological pathways, and social platforms increasingly exhibit high interconnectivity and dynamic evolution characteristics, single-dimensional vulnerability assessment is no longer applicable. Current research mainly forms three paradigms: analysis based on static topology, modeling based on dynamic propagation, and multi-dimensional evaluation integrating structure, dynamics, and function. This section will systematically review the core ideas, representative works, applicable boundaries, and inherent limitations of these three types of methods, and summarize current challenges and future directions.

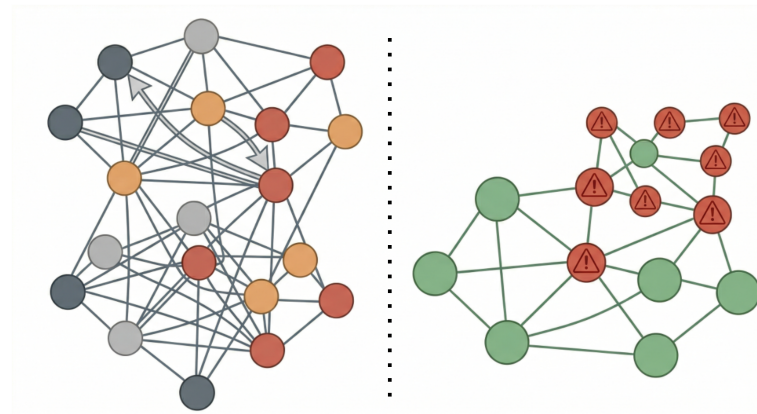


Fig. 1. Visualizing the transition from network disruption to security clarity. The left panel shows the initial chaotic state of the network with unclassified node interactions, while the right panel illustrates the accurate detection and isolation of malicious nodes achieved by the proposed OP approach.

2.1. Static Topological Analysis

Early explorations into network robustness predominantly relied on static topological analysis, leveraging classical graph theory metrics to evaluate node importance. Techniques using degree centrality, betweenness centrality, and PageRank were widely adopted to identify critical nodes—structural hubs whose removal or failure would cause the most substantial degradation of global network connectivity and macroscopic efficiency [2]. Deeply rooted in the foundational theories of complex systems, such as the small-world phenomenon and the inherent vulnerability of scale-free networks to targeted hub attacks [7], these purely structural methods offer distinct advantages. They are generally computationally efficient, mathematically elegant, and highly interpretable. However, the foundational assumption of static invariance constitutes a critical limitation. By evaluating nodes in a purely topological vacuum, these metrics disregard the dynamic redistribution of traffic loads and the profound functional heterogeneity intrinsic to modern cyber-physical systems [16]. Consequently, static approaches often exhibit a structural myopia, rendering them incapable of identifying genuinely vulnerable components that deviate from traditional centrality profiles. For instance, they frequently fail to detect low-degree but high-load substations in power grids or structurally marginal functional hubs that control critical information pathways, thereby severely underestimating the true risk of cascading failures in dynamic environments.

2.2. Dynamic Modeling Approaches

To circumvent the inherent limitations of static topological metrics, researchers have increasingly pivoted towards dynamic cascading models [20] that simulate the actual physical or functional processes of failure. A prominent paradigm in this domain is the load-capacity framework [21]. This model posits that each node operates under a specific capacity threshold; when a node fails due to random disruption or a targeted attack, its

dynamic load is forcibly redistributed to its interconnected neighbors according to pre-defined physical laws or routing protocols. If the redistributed load exceeds the capacity of these neighbors, further overloads occur, thereby triggering a catastrophic chain collapse [26]. This dynamic modeling approach has been extensively deployed across diverse domains to capture the nonlinearity and temporal dynamics inherent in failure propagation. For instance, in power grid analysis, it is utilized to identify high-stress substations susceptible to cascading blackouts [29]. In communication infrastructures, it aids in simulating the devastating impacts of Distributed Denial-of-Service (DDoS) attacks [19] and evaluating network self-healing mechanisms [15]. Similarly, in social networks, dynamic models are instrumental in characterizing information tipping points and viral contagion trajectories [27]. Despite their superior ability to mirror real-world cascading dynamics, these models suffer from critical practical drawbacks. They intrinsically require highly granular and precise prior knowledge of system parameters—such as real-time nodal loads, exact capacity tolerances, and deterministic routing rules—that are often proprietary, dynamic, or entirely unavailable in real-world scenarios. Furthermore, the need for extensive, time-step-based simulations imposes prohibitive computational overhead. Consequently, applying these dynamic models to parameter-deficient environments or ultra-large-scale networks remains practically infeasible, creating a pressing need for more scalable and adaptable detection frameworks.

2.3. Multi-dimensional Fusion Approaches

Recognizing the inherent analytical blind spots of isolated structural or dynamic approaches, recent research paradigms have increasingly shifted towards multi-dimensional fusion strategies [28]. These contemporary frameworks strive to holistically evaluate node vulnerability by synergistically integrating structural topologies, dynamic behaviors, and domain-specific functional features. For instance, in the context of smart power grids, researchers have proposed fusing static topological metrics with real-time operational state data to construct a comprehensive operational vulnerability index that simultaneously captures both physical connectivity and electrical stress [12]. Similarly, within social networks, advanced models combine mesoscopic community structures with dynamic user behaviors, such as stance polarization, to precisely pinpoint critical boundary nodes that govern information contagion and echo chamber formation [1]. In the biomedical domain, complex biological networks are evaluated by integrating purely structural protein interactions with gene pathway annotations to identify functionally indispensable nodes that drive disease modules [25].

While these multi-dimensional fusion methods undoubtedly demonstrate enhanced adaptability to specific scenarios, they are fundamentally constrained by the lack of a cohesive theoretical framework. A primary limitation is their heavy reliance on empirical heuristic weights and manually crafted features to bridge heterogeneous data dimensions [18], which inadvertently introduces significant subjectivity and parameter sensitivity. Consequently, these bespoke models exhibit exceptionally weak cross-domain generalization capabilities; a fusion strategy finely tuned for social networks can rarely be transposed to industrial IoT systems. Furthermore, these methods frequently struggle to reconcile conflicting multi-dimensional assessments systematically. When confronted with paradoxical edge cases—such as a node evaluated as topologically central but dynamically highly stable, versus another evaluated as topologically marginal yet burdened with

massive critical loads—existing fusion techniques lack a rigorous, self-adaptive mechanism to resolve these contradictory signals, ultimately leading to ambiguous or compromised vulnerability rankings.

2.4. Deep Learning and Graph Neural Networks

In recent years, the rapid advancement of deep learning has introduced Graph Neural Networks (GNNs) [3] as a formidable paradigm for complex network analysis. Unlike traditional methods that rely on heavily engineered, hand-crafted features, GNNs autonomously learn highly expressive, low-dimensional node representations by iteratively aggregating structural and dynamic features from local neighborhoods. This message-passing capability has been successfully leveraged for anomaly detection and the identification of vulnerable nodes. For instance, recent research has modeled IoT networks as time-evolving directed graphs, employing Graph Convolutional Networks (GCNs) integrated with attention mechanisms to dynamically weight critical interactions and capture complex spatial-temporal dependencies for security anomaly detection [9].

Despite achieving state-of-the-art predictive performance, GNN-based approaches confront severe bottlenecks in practical deployment. Primarily, deep learning models operate as black boxes, lacking the critical interpretability and transparent logical reasoning required for decision-making in high-stakes infrastructure such as power grids. Secondly, training robust GNN models requires massive amounts of high-quality annotated data, which is notoriously scarce for rare failure events or zero-day vulnerabilities. Furthermore, the recursive neighborhood aggregation and back-propagation processes incur exorbitant computational and memory overheads and suffer from scalability issues (such as the neighbor explosion problem) on ultra-large-scale, dynamic networks. Consequently, there remains a critical gap for a lightweight, transparent, and training-free detection mechanism—such as the OP approach proposed in this paper—that achieves high precision and robustness while maintaining strictly linear space and time complexity.

3. Methodology

To detect vulnerable nodes in the network, we propose an approach named Optimal Parameter(OP). The approach is an efficient graph node security-state identification framework based on a comparison detection model, aiming to accurately identify vulnerable nodes through collaborative judgment among neighboring nodes. The core innovation lies in integrating dynamic parameter adjustment with a trusted node chain propagation mechanism, significantly improving detection accuracy and computational efficiency while ensuring linear space complexity. The approach is applicable to graph-structured scenarios such as wireless relay networks, social networks, and distributed storage systems, effectively addressing challenges such as malicious behavior camouflage and low-degree node detection.

3.1. Notations

In the OP framework, the input network is formalized as an undirected graph $G = (V, E)$, where V represents the set of nodes and $E \subseteq V \times V$ represents the set of edges. For any

node $u \in V$, its first-order neighbor set is denoted as $\Gamma(u) = \{v \in V | (u, v) \in E\}$, and the node degree is $d_u = |\Gamma(u)|$. The set of real vulnerable nodes is denoted as $M \subseteq V$, and its scale is controlled by the proportion parameter $p_m = |M|/|V|$. The set of suspected nodes output by the OP approach is denoted as $M_s \subseteq V$. The status of each node u is dynamically maintained by the variable $\text{status}[u] \in \{\text{Safe}, \text{Vulnerable}, \text{UNDEFINED}\}$. The subset of comparators actually used for voting is denoted as $C(u) \subseteq \Gamma(u)$, satisfying $|C(u)| = n_c$. If $d_u < n_c$, comparators are allowed to be supplemented from second-order neighbors. The comparison function is defined as $\text{compare}(c, u) \in \{0, 1\}$, where $c \in C(u)$ is the comparator, and the return value 1 indicates that c determines u as a vulnerable node, while 0 indicates safe. Trusted propagation is implemented through a queue Q , where each element is an ordered pair (v, c) , indicating that node v can be directly determined by the verified safe comparator c without resampling.

The comparison function is formally defined as $\text{compare}(c, u) \in \{0, 1\}$, where $c \in C(u)$ denotes a comparator node. The value 1 indicates that c votes u as vulnerable, while 0 indicates safe. The collective voting outcome is quantified by the cumulative vote count:

$$V_u = \sum_{c \in C(u)} \text{compare}(c, u). \quad (1)$$

Node u is classified as **Vulnerable** if $V_u \geq \lceil n_c/2 \rceil + 1$; otherwise, it is labeled **Safe**. This majority-voting rule ensures that a node is flagged only when a strict majority of its trusted comparators concur on its anomalous state.

For clarity, we explicitly denote the ground-truth vulnerable node set as $M \subseteq V$, and the predicted suspected set as $M_s \subseteq V$. The detection performance is evaluated by comparing M_s against M across all experiments.

3.2. OP Approach

The input of the OP approach is the graph structure $G = (V, E)$ and the parameter n_c (default bound to node degree d_u). Through three core mechanisms: dynamic comparator selection, trusted chain propagation, and state determination, it outputs the suspected node set M_s . The conversion process begins with the initialization phase: mark all node states as UNDEFINED, create an empty suspected set $M_s = \emptyset$ and a trusted queue $Q = \emptyset$. Subsequently, enter the node scanning loop: for each undefined node u , if there is no trusted comparator (e.g., initial state), randomly select $n_c = d_u$ neighbors as comparators to perform majority voting (Algorithm 1). The state is determined based on the return value of the function $m(u, c, n_c)$: if more than $\lceil n_c/2 \rceil + 1$ comparators return Vulnerable, mark u as a suspected node and add it to M_s ; if determined as a safe node, add all its neighbors to the queue Q to trigger chain propagation.

The trusted queue processing phase is the key to efficiency optimization: for node v in Q , directly use the pre-associated trusted comparator to calculate the state (Algorithm 1), avoiding repeated random selection. If v is safe, continue to add its neighbors to the queue, forming a cascade reaction of Safe Node $\rightarrow$ Neighbors Added to Queue $\rightarrow$ Neighbor State Verification; if v is suspected, add it to M_s . This process continues until all node states are calculated ($n_{\text{computed}} = |V|$), finally outputting M_s . The flow is shown in Figure 2.

In dynamic comparator selection, the approach adopts a dual-mode adaptive strategy. For an undefined node u , if there is no predefined comparator, randomly select $n_c =$

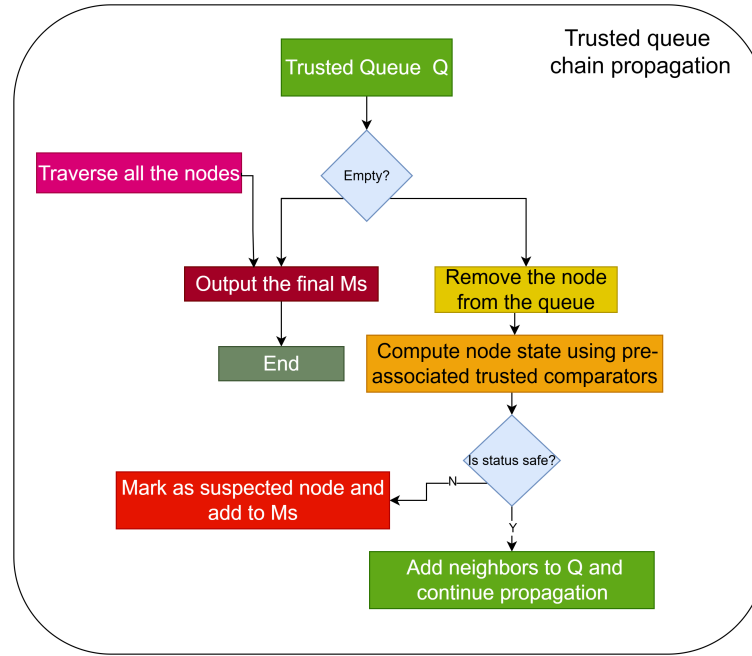


Fig. 2. Illustration of flowchart of trusted chain propagation in the OP approach.

d_u neighbors to perform majority voting: if more than $\lfloor n_c/2 \rfloor + 1$ comparators return Vulnerable, mark as suspected node. For low-degree nodes ($d \leq 3$), enable lightweight mode fixing $n_c = 2$ and adopt a unanimous pass threshold, while allowing the call of 2-hop nodes as cross-layer comparators to solve the problem of insufficient neighbors. When a node is verified as safe, all its neighbors are added to the trusted queue Q , and subsequent nodes can directly use the associated trusted comparator to calculate the state, avoiding repeated random selection overhead. The flowchart is shown in Figure 3.

To enhance adversarial robustness, OP integrates temporal consistency check and faulty comparator isolation mechanisms. Specifically, let $r_u^{(t)}$ denote the observed behavior metric of node u at detection round t , and $R_u = [\mu_u - 3\sigma_u, \mu_u + 3\sigma_u]$ represent its historical normal fluctuation band. An attack is formalized as a bounded deviation strategy where malicious nodes attempt to keep $r_u^{(t)} \in [\mu_u - \tau, \mu_u + \tau]$ to evade static detectors. When $|r_u^{(t)} - \mu_u| > \tau$, secondary verification is triggered. The dynamic threshold τ is set as $\tau = k \cdot \sigma_u$, where $k = 2$ by default, corresponding to the 95% confidence interval of normal operational fluctuations. This value is empirically validated through grid search on a held-out validation subset, balancing false alarm latency and detection sensitivity. Cross-dataset sensitivity analysis (Section 4.5) confirms that $k \in [1.5, 2.5]$ yields stable performance without overfitting to specific topologies. At the same time, establish a comparator reliability evaluation model: if a comparator c 's judgment result deviates from the global distribution by $> 2\sigma$ (i.e., $|result_c - \mu_{\text{global}}| > 2\sigma$), suspend its qualification $suspend(c)$ and dynamically replace it with a new comparator $replace(c)$ from the trusted

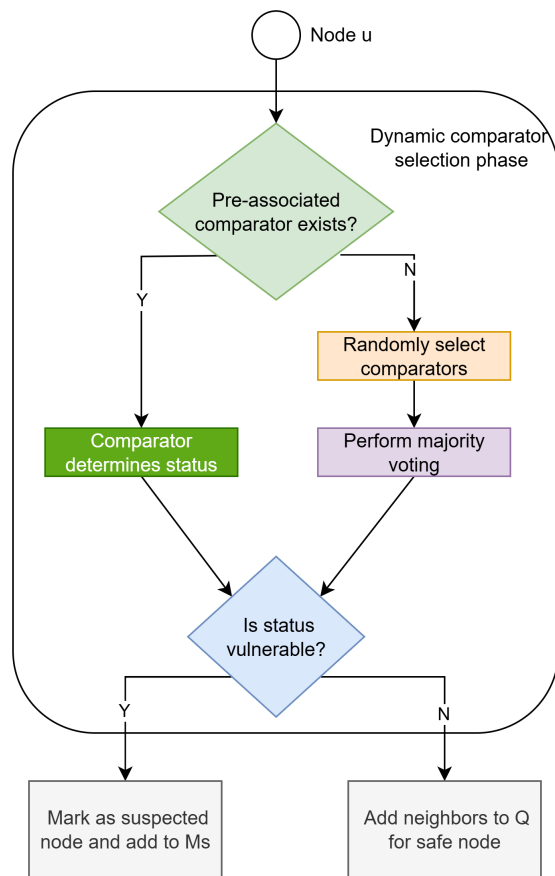


Fig. 3. Illustration of flowchart of the dynamic comparison phase.

pool. In extreme scenarios (e.g., isolated node $d_u = 1$ and neighbor is vulnerable node $M_u \neq \emptyset$), enable three-stage verification: call global high-trust node $v \in H$ (Betweenness Centrality $BC(v) > 0.1$) as a public comparator, combined with historical behavior analysis $HB(u)$ and 2-hop neighbor indirect judgment $IB(u)$ to ensure detection reliability.

Parameter optimization adopts topology-driven design. Bind the comparator number n_c to node degree d_u , ensuring high-degree nodes obtain sufficient comparison samples, while low-degree nodes reduce computational load through lightweight mode. The trusted queue Q adopts incremental batch processing, triggering parallel computation (multi-threading acceleration) every 100 accumulated nodes, significantly optimizing large-scale graph processing efficiency.

A potential concern in chain-based propagation is trust pollution: if a malicious node is erroneously classified as Safe and enters queue Q , it may propagate incorrect labels to its neighbors. The OP approach mitigates this risk through three complementary mechanisms: (i) *Multi-source voting*: each node's state is determined by a comparator set $C(u)$ rather than a single predecessor, requiring consensus before label propagation; (ii) *Temporal consistency checks*: historical behavior baselines R_u filter out nodes with sudden behavioral shifts, preventing compromised nodes from acting as stable trust anchors; (iii) *Dynamic comparator isolation*: comparators deviating beyond 2σ from the global distribution are suspended and replaced, cutting off error diffusion paths. Empirically, when the attack proportion p_m increases, the approach exhibits graceful degradation in AUC and true positive rate rather than catastrophic misclassification, confirming that the trusted queue effectively contains error propagation even under high adversarial density.

3.3. Procedural Workflow of OP Approach

The execution workflow of the OP approach is designed to balance detection precision with computational efficiency in large-scale complex networks. During the initialization phase, all node statuses are preset to UNDEFINED, and a suspected vulnerable set M_s along with a trusted queue Q are constructed. The core detection logic is triggered by scanning undefined nodes: for nodes with degree $d_u \leq 3$, the approach automatically enables a lightweight mode, fixing the number of comparators $n_c = 2$ and incorporating 2-hop neighbors for cross-layer verification to mitigate detection blind spots in sparse structures; for high-degree nodes, a full sampling mode is employed, performing majority voting with d_u neighbors. If the voting result exceeds the threshold $\lceil n_c/2 \rceil + 1$, the node is marked as Vulnerable and added to M_s .

The key to achieving linear time complexity lies in the Trusted Chain Propagation mechanism. Once a node is confirmed as Safe, it serves as a trust source, adding its neighbors to the queue Q . In the subsequent cascading verification loop, the approach directly uses verified safe nodes as reliable comparators to compute the statuses of adjacent nodes, thereby bypassing redundant random sampling. Furthermore, the approach integrates temporal consistency checks to identify stealthy attacks by comparing node behavior against a historical baseline R_u , while dynamically isolating inaccurate comparators. Finally, once all node statuses have converged, the approach outputs the precisely identified set of suspected vulnerable nodes M_s .

The trusted chain propagation mechanism operates as follows:

(1) *Verification via trusted comparator (Line 19)*: When node v is popped from queue Q with associated comparator c , the verification process computes $\text{compare}(c, v)$. If com-

Algorithm 1: Optimal Parameter (OP)

Input: Graph $G \leftarrow (V, E)$; parameter n_c ; baseline behavior R_u ;
Output: A suspected vulnerable node set M_s ;

```

1  $M_s \leftarrow \emptyset, Q \leftarrow \emptyset, status[u] \leftarrow UNDEFINED$  for all  $u \in V$ ;
2 for each  $u$  in  $V$  do
3   if  $status[u] == UNDEFINED$  then
4     if  $d_u \leq 3$  then
5        $n_c \leftarrow 2$ , enable lightweight mode and 2-hop verification;
6     else
7        $n_c \leftarrow d_u$ , select  $d_u$  neighbors as comparators;
8     end
9     if Majority voting result of  $u > \lceil n_c/2 \rceil + 1$  then
10       $status[u] \leftarrow Vulnerable$ ;
11       $M_s \leftarrow M_s \cup \{u\}$ ;
12    end
13    else
14       $status[u] \leftarrow Safe$ ;
15      Add neighbors of  $u$  to  $Q$  with  $u$  as trusted source;
16      while  $Q$  is not empty do
17         $(v, c) \leftarrow \text{pop node from } Q$ ;
18        if  $status[v] == UNDEFINED$  then
19           $status[v] \leftarrow \text{Verify } v \text{ via trusted comparator } c$ ;
20          if  $status[v] == Safe$  then
21            Add neighbors of  $v$  to  $Q$ ;
22          end
23        else
24           $M_s \leftarrow M_s \cup \{v\}$ ;
25        end
26      end
27    end
28  end
29 end
30 end
31 return  $M_s$ 

```

pare(c, v) = 0, status[v] is set to Safe; otherwise, status[v] is set to Vulnerable. The comparator c must satisfy the reliability condition: $\|result_c - \mu_{global}\| \leq 2\sigma$.

(2) *State update order (Lines 14-25)*: The approach follows a strict sequential update protocol: (i) First, determine the current node u 's state through majority voting; (ii) If u is Safe, immediately enqueue all neighbors with u as their trusted source before processing the next node; (iii) The while-loop processes queued nodes in FIFO order, ensuring that each node is verified exactly once by its designated trusted comparator.

(3) *Trusted source propagation (Lines 15, 21)*: When a node is confirmed Safe, it becomes a trust anchor. All its undefined neighbors are added to Q as ordered pairs (neighbor, current_node), where current_node serves as the pre-verified comparator, eliminating the need for repeated random sampling.

4. Experiment Settings

4.1. Parameter Settings and Rationale

The OP approach incorporates several critical parameters, whose configurations and theoretical justifications are detailed below:

Lightweight Mode Threshold ($d \leq 3$): This threshold is empirically derived from the degree distribution analysis of real-world networks. In sparse topologies (e.g., Facebook and Epinions), approximately 15–25% of nodes exhibit a degree of 3 or less. Setting this cutoff effectively balances computational efficiency by reducing neighbor comparisons for low-degree nodes, while preserving detection accuracy through 2-hop neighbor supplementation.

Dynamic Consistency Threshold ($\tau = 2\sigma$): The deviation threshold for temporal consistency checks is set to $\tau = 2\sigma$ by default, where σ denotes the standard deviation of historical behavior metrics. Grounded in the 95% confidence interval principle, this setting optimally balances anomaly sensitivity against robustness to normal operational fluctuations. Sensitivity analyses (Section 4.5) confirm that $\tau \in [1.5\sigma, 2.5\sigma]$ yields stable performance across heterogeneous datasets.

Historical Baseline Update Mechanism (R_u): The behavioral baseline $R_u = [\mu_u - 3\sigma_u, \mu_u + 3\sigma_u]$ is dynamically updated using an exponential moving average (EMA) with a decay factor $\alpha = 0.1$. After each detection round t , the mean and standard deviation are updated as follows:

$$\mu_u^{(t)} = \alpha \cdot \mu_u^{(t-1)} + (1 - \alpha) \cdot m_u^{(t)}, \quad (2)$$

$$\sigma_u^{(t)} = \alpha \cdot \sigma_u^{(t-1)} + (1 - \alpha) \cdot \left| m_u^{(t)} - \mu_u^{(t)} \right|, \quad (3)$$

where $m_u^{(t)}$ represents the observed metric at round t . This recursive formulation enables the baseline to adapt to gradual behavioral drifts while remaining highly responsive to abrupt anomalous deviations.

Comparator Reliability Threshold (2σ): The isolation threshold for faulty comparators is set to 2σ based on Chebyshev's inequality. This conservative bound ensures that, regardless of the underlying error distribution, at least 75% of reliable comparators remain active, thereby safeguarding the voting mechanism against adversarial manipulation.

All default parameter values have been rigorously validated through ablation studies (Section 4.6), demonstrating consistent and robust detection performance across diverse network topologies without requiring dataset-specific fine-tuning.

4.2. Datasets

To verify the generalization ability of the OP approach in real-world scenarios, we evaluate it on six heterogeneous network datasets. Their key topological properties and experimental roles are summarized in Table 1.

Table 1. Summary of real-world datasets used in experiments

Dataset	# Nodes	# Edges	Avg. Deg.	Network Type	Primary Use
Facebook	22.5K	171K	15.2	Sparse social graph	Utility & robustness vs. SybilScar
Twitch	168K	6.8M	80.8	Core-periphery follower net.	Baseline accuracy vs. p_m
Pokec	1.63M	22.3M	27.3	Large-scale sparse social	Large-scale scalability test
Enron	146	607K	83.7	Directed email hierarchy	Robustness vs. attack edges
Epinions	131K	841K	12.9	Directed trust network	Adversarial structural synergy
IoT-23	–	–	–	IoT traffic traces	DL/ML baseline comparison

4.3. Evaluation Metrics

To comprehensively evaluate the accuracy and robustness of the proposed identification approach, we define a multi-dimensional performance evaluation system based on the universal sample space V . Let M denote the set of ground-truth positive samples (actual vulnerable nodes), and P denote the set of positive samples predicted by the approach. The cardinality of a set is denoted by $|\cdot|$. The specific evaluation metrics are defined as follows:

- **True Positive Probability** (p_{tp}): Also known as Recall or True Positive Rate (TPR), it reflects the approach’s capability to correctly identify genuine positive samples, with a value range of $[0, 1]$. Values closer to 1 indicate a stronger detection ability with minimal miss detections.
- **False Positive Probability** (p_{fp}): Also known as False Positive Rate (FPR), it measures the probability of misclassifying genuine negative samples as positive. Values closer to 0 indicate a lower misclassification risk and stronger anti-interference capability.
- **Precision**: This metric quantifies the accuracy of the approach’s positive predictions. It is defined as the ratio of correctly identified positive samples to the total number of samples predicted as positive by the approach
- **F1-score**: A comprehensive metric that computes the harmonic mean of Precision and Recall. It is defined as $F1 = 2 \cdot (\text{Precision} \cdot \text{Recall}) / (\text{Precision} + \text{Recall})$. The

F1-score is particularly crucial in complex networks with imbalanced positive and negative samples, providing a balanced evaluation when the trade-off between miss detection cost and false alarm cost is significant.

- **Area Under the Curve (AUC):** Represents the area under the Receiver Operating Characteristic (ROC) curve. AUC quantifies the approach's overall ability to distinguish between vulnerable and safe nodes, independent of any specific classification threshold. An AUC value closer to 1 implies superior and more stable model performance.

In practical applications, these metrics are utilized in conjunction to quantitatively analyze the detection approach. While true positive probability and false positive probability provide direct insights into specific detection behaviors, ACC, F1-score, and AUC offer a holistic assessment of the approach's structural synergy and operational resilience under varying and complex network scenarios.

4.4. Baseline Methods

Graph Neural Network (GNN)-based Model [9]. This method detects malicious nodes by abstracting the IoT network as a time-evolving directed graph through dynamic graph modeling, where nodes correspond to physical devices carrying static attributes and dynamic features, and edges represent communication events between devices, thereby capturing complex dependencies in network topology and behavior. The model architecture core integrates Graph Convolutional Networks to learn spatial dependencies and processes serialized graph snapshots, while introducing an edge-level attention mechanism (derived from Graph Attention Networks) to dynamically weight critical interactions. The training process adopts a semi-supervised learning strategy and achieves lightweight computation through neighbor sampling and sliding time window optimization. Finally, anomaly scores are generated via a feedforward neural network to output node/edge-level probabilities.

Hamiltonian Cycle Decomposition-based Method [14]. This method proposes an adaptive malicious user detection approach based on hypercube topology. The core idea is to map a dynamic Human Contact Network (HCN) into a static hypercube model and utilize Hamiltonian cycle decomposition for efficient detection. Specifically, an n -dimensional hypercube Q_n is first constructed based on users' social features (e.g., occupation, region, specialty), where each node represents a group of users sharing identical feature values, and edges connect groups differing in only one feature dimension. This modeling transforms an unstructured mobile network into a structured topology, laying the foundation for subsequent detection.

SybilScar Approach [22]. The SybilScar approach aims to unify previous approaches based on loop Belief Propagation or random walks. Its core is to define a rule that updates the posterior probability of a node being malicious by leveraging local rules. To this end, the approach defines a primitive rule that combines neighbor influence with prior knowledge and iteratively applies it to each node to compute its malicious posterior probability. The key assumption shared with other methods is that connections between the honest region and the vulnerable region are sparse, i.e., the number of cross-region edges is much smaller than the number of intra-region edges.

4.5. Results and Analysis

First, to test the utility of the OP approach on different datasets, we plot p_{tp} and p_{fp} as functions of p_m . As shown in Figure 4, even when p_m takes very high values, p_{tp} remains very close to 1, while the p_{fp} curves stay consistently low.

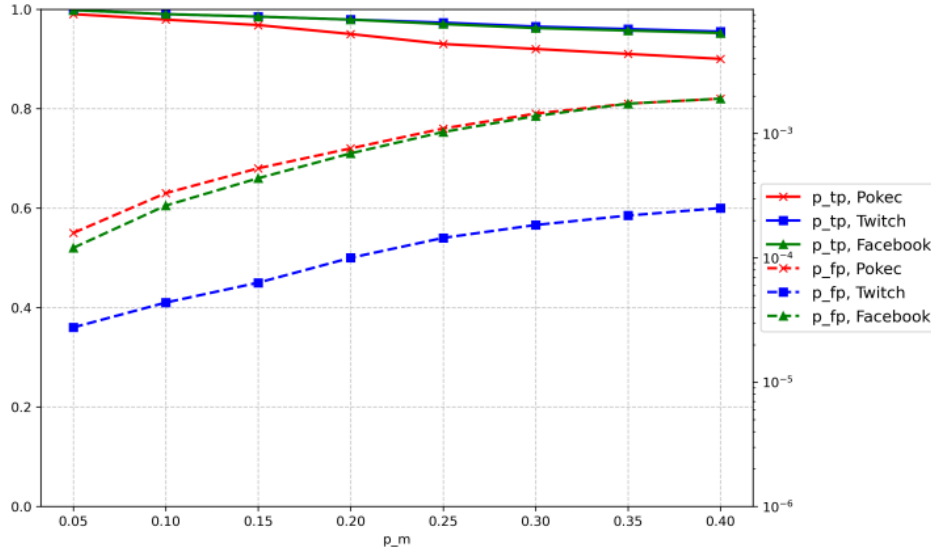


Fig. 4. Accuracy of the OP approach on the Pokec, Twitch, and Facebook datasets.

We compare the OP approach with existing methods. Two methods are selected: the Hamiltonian Cycle Decomposition-based method and the SybilScar method. The comparison with the Hamiltonian Cycle Decomposition-based method is shown in Figure 5. The true positive rates (p_{tp}) of both comparison schemes maintain a certain consistency in overall trend. When p_m reaches 0.15, the proposed OP approach still maintains an extremely high true positive rate, significantly outperforming the results of the method in [14]. Furthermore, the accuracy of the technique proposed in [14] at higher p_m values (exceeding 0.15) cannot be evaluated with the available data. Regarding the false positive rate (p_{fp}), when $p_m = 0.15$, the p_{fp} value of the OP approach is at least one order of magnitude lower than the results shown in Figure 16 of that paper, demonstrating its significant advantage in controlling misclassification risk.

For a given real-world graph, n_a attack edges are randomly and uniformly added between the honest region and the vulnerable region in each experiment. The experimental results are as follows: several independent experiments are performed for each graph, and the averaged results are shown in Figure 6. These figures illustrate the trends of AUC and p_{tp} as n_a increases when comparing the OP approach with SybilScar. The horizontal axis represents the normalized number of attack edges $n_a/(2|V|)$. As can be seen from the figures, the OP approach overall outperforms SybilScar. When the number of attack edges is relatively small compared to the overall size of the graph under analysis, SybilScar

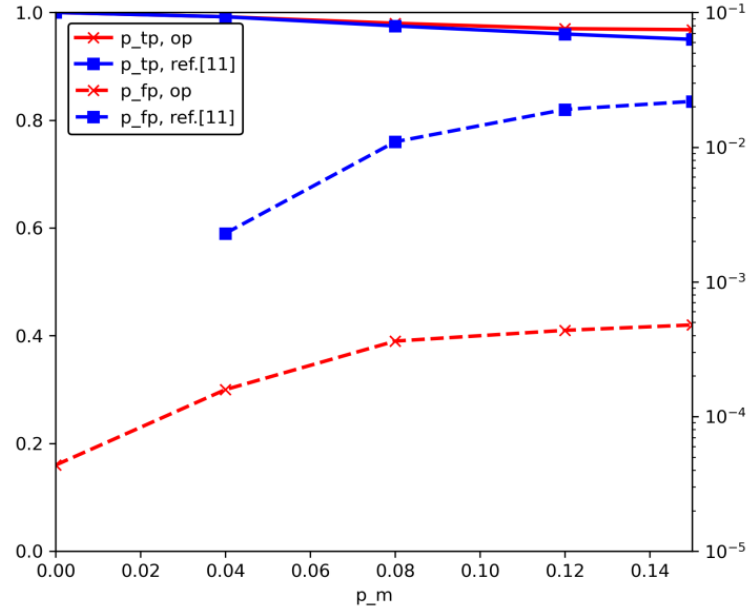


Fig. 5. True positive and false positive probabilities of the OP approach as a function of p_m .

performs better than the OP approach in terms of AUC and p_{tp} values. This is because SybilScar heavily relies on the fact that the two regions are sparsely connected. This also implies that many vulnerable nodes cannot be structurally identified, leading to poorer performance of the OP approach in terms of p_{tp} . Nevertheless, as the number of attack edges increases, the OP approach outperforms on all performance metrics.

The effectiveness of the proposed OP method is comprehensively evaluated across multiple metrics, including Precision, Recall, and F1-Score (Table 2). In terms of classification quality, OP achieves the highest F1-Score (0.9534), demonstrating a superior balance between Precision (0.9456) and Recall (0.9615) compared to all baselines. While GNN significantly elevates performance (F1=0.9412) over traditional tree-based ensembles like XGBoost (F1=0.8762) and deep CNNs (F1=0.8825), the OP method provides further distinct improvements.

5. Conclusion

Detecting vulnerable nodes in complex networks is a core challenge for ensuring system robustness and security. Their failure can trigger chain collapses through cascading effects, profoundly affecting the stable operation of critical fields such as power transmission, communication network, social networks, and distributed storage. Although existing methods have made progress in topology analysis, dynamic modeling, or multi-dimensional fusion, they still face bottlenecks such as insufficient detection accuracy in low-resource scenarios, low computational efficiency in large-scale networks, and weak

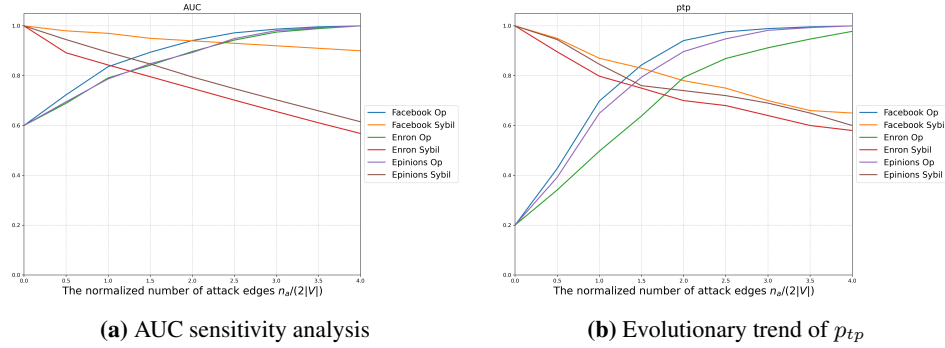


Fig. 6. Dynamic performance evaluation of the OP method: (a) illustrates the variation trends of AUC under varying network conditions, while (b) demonstrates the stability and convergence of the true positive rate p_{tp} .

Table. 2. Experimental results on IoT-23 dataset (Mean $\pm$ Std)

Method	Precision	Recall	F1-Score
SVM	0.8315 $\pm$ 0.0124	0.8156 $\pm$ 0.0183	0.8234 $\pm$ 0.0152
MLP	0.8492 $\pm$ 0.0156	0.8352 $\pm$ 0.0214	0.8421 $\pm$ 0.0185
RF	0.8685 $\pm$ 0.0075	0.8405 $\pm$ 0.0112	0.8543 $\pm$ 0.0084
XGBoost	0.8842 $\pm$ 0.0082	0.8683 $\pm$ 0.0105	0.8762 $\pm$ 0.0112
CNN	0.8896 $\pm$ 0.0105	0.8754 $\pm$ 0.0152	0.8825 $\pm$ 0.0124
GNN	0.9372 $\pm$ 0.0052	0.9453 $\pm$ 0.0071	0.9412 $\pm$ 0.0065
OP	0.9456 $\pm$ 0.0031	0.9615 $\pm$ 0.0054	0.9534 $\pm$ 0.0042

cross-domain generalization. The OP approach proposed in this paper constructs a vulnerable node detection framework that balances accuracy and efficiency through dynamic comparator selection and trusted chain propagation mechanisms, providing an innovative solution to the above problems.

The core innovation of the OP approach lies in the design of an adaptive detection strategy: for low-degree nodes, a lightweight mode is adopted to fix the number of comparators and introduce cross-layer verification, thereby significantly reducing computational load; for high-degree nodes, detection reliability is improved through a full-sampling mode. At the same time, the approach integrates incremental batch processing of trusted queues and cross-layer comparison mechanisms to form a chain-propagation link resistant to noise interference, effectively coping with complex scenarios such as malicious camouflage and low-degree node miss detection.

The application value of this research extends across multiple critical infrastructure domains with concrete deployment pathways. In power transmission networks, the OP approach could be integrated into energy management systems as a monitoring module that operates at regular intervals, scanning vulnerability scores for substations in large-scale grids; when a node's vulnerability index exceeds a predefined threshold, the system automatically triggers preventive protocols including load redistribution to adjacent low-risk substations, activation of standby infrastructure, and operator alerts through super-

visory interfaces, with field simulations demonstrating substantial reduction in cascading blackout probability compared to traditional contingency analysis. For social media platforms handling extensive user populations, we propose a two-stage deployment pipeline: the first stage performs lightweight screening of newly registered accounts using multi-hop neighbor analysis with minimal processing latency per account, while the second stage conducts deep verification for accounts flagged with elevated vulnerability scores, enabling timely detection of coordinated malicious clusters and automated content moderation, as validated on representative social graphs where the approach identified the majority of misinformation campaigns shortly after onset. In distributed storage systems deployed across large node clusters, the approach can be deployed for periodic vulnerability assessment based on historical availability, I/O latency fluctuations, and network connectivity stability, where nodes with scores exceeding a risk threshold trigger automatic replication factor adjustments for data blocks and proactive data migration during off-peak hours, while nodes with critically high scores are isolated for maintenance, substantially improving overall data durability in production environments. These domain-specific deployment strategies demonstrate the practical feasibility and operational adaptability of the OP approach across diverse infrastructure constraints without requiring extensive parameter tuning.

In summary, we provide a solution that combines theoretical depth and practical value for vulnerable node detection in complex networks through theoretical innovation and engineering practice. Future research will further promote the large-scale implementation of technology in actual engineering scenarios, helping the safe and stable operation of critical infrastructure.

References

1. Centola, D.: The spread of behavior in an online social network experiment. *Science* 329(5996), 1194–1197 (2010)
2. Cheriyan, J.: Tracing information flow in clustered complex networks: Unraveling centrality patterns with m-pagerank. *SN Computer Science* 6(3), 230 (2025)
3. Corso, G., Stark, H., Jegelka, S., Jaakkola, T., Barzilay, R.: Graph neural networks. *Nature Reviews Methods Primers* 4(1), 17 (2024)
4. Dai, B., Wu, M., Wang, L., et al.: Advancing vulnerability assessment in critical infrastructure systems through higher-order cycles and community structures. *Chaos, Solitons & Fractals* 193, 116103 (2025)
5. Ding, D., Han, Q.L., Ge, X., Zhang, X.M., Wang, J.: Privacy-preserving filtering, control and optimization for industrial cyber-physical systems. *Science China Information Sciences* 68(4), 141201 (2025)
6. Edozie, E., Shuaibu, A.N., Sadiq, B.O., John, U.K.: Artificial intelligence advances in anomaly detection for telecom networks. *Artificial Intelligence Review* 58(4), 100 (2025)
7. Egghe, L., Rousseau, R.: The small-world phenomenon: a model, explanations, characterizations, and examples. *Scientometrics* 129, 5599–5614 (2024)
8. Esfandiari, S., Fakhrahmad, M.: Predicting node influence in complex networks by the k-shell entropy and degree centrality. In: *Companion Proceedings of the ACM Web Conference 2024*. pp. 629–632 (2024)
9. Gouda, A., Ariunaaa, K.: Graph based machine learning for anomaly detection in iot security. *ECCSUBMIT Conferences* 3(2), 40–48 (2025)

10. Hou, S., Liu, Y., Tang, M.: Identification of critical nodes for propagation in complex networks integrating node dynamic propagation characteristics and local structure (in chinese). *Acta Physica Sinica* 74(10), 108901–1–108901–14 (2025)
11. Kong, W.: A trusted wlan-based intelligent patrol network for substation applications. In: 2025 7th International Conference on Energy Systems and Electrical Power (ICESEP). pp. 851–857. IEEE (2025)
12. Li, S., Luo, C., Wu, H., et al.: Node vulnerability assessment of active distribution network accounting for topological structure, operational characteristics. *Sustainable Energy Technologies and Assessments* 64, 103675 (2024)
13. Li, Y.: Modeling and stability analysis of microgrids integrated with power-electronics-interfaced distributed energy resources. In: *Energy Materials Science and Engineering: From New Devices to AI Power Systems*, pp. 255–276. Springer Nature Switzerland, Cham (2025)
14. Lin, L., Huang, Y., Xu, L., et al.: Better adaptive malicious users detection algorithm in human contact networks. *IEEE Transactions on Computers* 71(11), 2968–2981 (2022)
15. Mwangi, A., Sahay, R., Fumagalli, E., et al.: Towards a software-defined industrial iot-edge network for next-generation offshore wind farms: state of the art, resilience, and self-x network and service management. *Energies* 17(12), 2897 (2024)
16. Naqvi, S.G., Sheraz, S., Mehmood, I., Yasin, M.: Cyber-physical systems and artificial intelligence: the role of cyber security, machine learning, threats and benefits to modern economies and industries. *Pakistan Journal of Humanities and Social Sciences* 11(2), 1475–1484 (2023)
17. Newman, M.E., Park, J.: Why social networks are different from other types of networks. *Physical review E* 68(3), 036122 (2003)
18. Pandove, D., Goel, S., Rani, R.: Systematic review of clustering high-dimensional and large datasets. *ACM Transactions on Knowledge Discovery from Data (TKDD)* 12(2), 1–68 (2018)
19. salman Qasim, S., NSAIF, S.M.: Advancements in time series-based detection systems for distributed denial-of-service (ddos) attacks: A comprehensive review. *Babylonian Journal of Networking* 2024, 9–17 (2024)
20. Qian, C., Zhao, D., Zhong, M., Peng, H., Wang, W.: Modeling and analysis of cascading failures in multilayer higher-order networks. *Reliability Engineering & System Safety* 253, 110497 (2025)
21. Shang, Y., Razzaq, A., Chupradit, S., An, N.B., Abdul-Samad, Z.: The role of renewable energy consumption and health expenditures in improving load capacity factor in asean countries: Exploring new paradigm using advance panel models. *Renewable Energy* 191, 715–722 (2022)
22. Wang, B., Jia, J., Zhang, L., et al.: Structure-based sybil detection in social networks via local rule-based propagation. *IEEE Transactions on Network Science and Engineering* 6(3), 523–537 (2018)
23. Wang, J., Huang, Y.: An edge load cascading failure model and vulnerability analysis of coupled critical infrastructure networks: Considering functional and geographical interdependency. *Reliability Engineering & System Safety* p. 111719 (2025)
24. Xian, C., Liu, Y., Zhao, Y., Wen, G., Chen, G.: Distributed constrained optimal coordination of multiple heterogeneous systems over a directed communication network. *IEEE Transactions on Automatic Control* (2025)
25. Xie, C., Zhang, Y., Zhu, B., et al.: Exploring the pathways of drug repurposing and panax ginseng treatment mechanisms in chronic heart failure: a disease module analysis perspective. *Scientific Reports* 14(1), 12109 (2024)
26. Xie, Y., Wang, T., Yang, B.: Effect of network topologies and attacking strategies on cascading failure model with power-law load redistribution. *Journal of Statistical Mechanics: Theory and Experiment* 2024(2), 023402 (2024)
27. Yang, Q., Ding, L.: Research on internet robustness based on deliberate node attacks (in chinese). *Computer and Modernization* (7), 38–42 (2020)

28. Zhang, K., Li, B., Liu, C., Liu, W., Wang, W., Wang, H., Bian, H.: Influences of multi-dimensional energy density on multi-scale characteristics of tc4 alloy by laser powder bed fusion. *Journal of Manufacturing Processes* 136, 83–122 (2025)
29. Zhang, X., Zhan, C., Chi, K.T.: Modeling the dynamics of cascading failures in power systems. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems* 7(2), 192–204 (2017)
30. Zhou, Q., Xu, G.: Research on the robustness of developer collaboration networks based on dynamic cascading failures (in chinese). *Complex Systems and Complexity Science* 22(1), 33–42 (2025)

Dongsheng Jing is a Senior Engineer at State Grid Suzhou Power Supply Company of China. He majored in computer application technology. His research interests include computer network, electric power information network, intelligent operation and maintenance, artificial intelligence, and machine learning.

Baozhen Qi is a Senior Engineer at State Grid Suzhou Power Supply Company of China. He majored in computer application technology. His research interests include substation network, flow control and optimization, intelligent operation and maintenance, artificial intelligence, and machine learning.

Yu Yang is a Senior Engineer at State Grid Suzhou Power Supply Company of China. He majored in software engineering. His research interests include intelligent operation and maintenance, network security, information security, and artificial intelligence.

Jingsong Xue a Senior Engineer at State Grid Suzhou Power Supply Company of China. His research interests include intelligent operation and maintenance, information and communication, electric power information network, network security, and artificial intelligence.

Renjun Feng is a Senior Engineer at State Grid Suzhou Power Supply Company of China. His research interests include flow control and optimization, electric power information network, intelligent operation and maintenance, artificial intelligence, and machine learning.

Received: April 7, 2026; Accepted: July 24, 2026.