

Anti-Interference And Secure Communication For Distributed Power Line Inspection Networks Based On The BeiDou Short Message Service

Lianfei Zhao¹, Fulong Ji^{2*}, and Yongmao Zhao³

¹ State Grid Jilin Electric Power Co., Ltd., Changchun 130022, Jilin, China

² State Grid Location Based Service Co., Ltd., Beijing 102211, Beijing, China

³ Beijing Sinan Beidou Technology Development Co., Ltd., Beijing 100029, Beijing, China

* Corresponding author. E-mail: power_bds@163.com

Received: Jul. 22, 2026; Accepted: Aug. 19, 2026

Distributed power line inspection networks in mountainous areas and post-disaster sites often suffer from link outages, high-power interference, queue congestion, and false alarms due to weak public-network coverage, making critical alarm delivery unreliable. We propose BD-SASC, jointly modeling cellular, dedicated power, edge multi-hop, and BeiDou short-message links, evaluating latency, interference, reliability, security risk, and trustworthiness for adaptive link selection, with priority-based scheduling, field compression, lightweight authentication, and trusted edge forwarding ensuring prioritized P1 alarm delivery. With 500 nodes and 10% malicious nodes, BD-SASC maintains 91.6% secure delivery under strong interference (vs. 61.8% Cellular-only, 78.4% Fixed-BDS, 71.4% Encryption-only), reduces average P1 latency to 4.31s under burst alarms (vs. 12.46s/8.92s baselines), and maintains 92.4% delivery at 1000 nodes.

Keywords: BeiDou short-message service; distributed power line inspection; anti-interference communication; security authentication; power IoT; scalable information system

© The Author(s). This is an open-access article distributed under the terms of the [Creative Commons Attribution License \(CC BY 4.0\)](https://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are cited.

http://dx.doi.org/10.6180/jase.202701_36.001

1. Introduction

As transmission-line assets expand, power line inspection is shifting to collaborative drone, sensor, and edge-intelligence inspection across wide, heterogeneous, event-vulnerable networks. In mountainous, forested, and post-disaster sites, terminals may lack reliable cellular access, so alarms can be delayed by outages or interference - making secure delivery under weak-connectivity conditions key for these information systems.

BeiDou-3 short-message service supports location reporting, emergency rescue, and lowcapacity exchange [1]; vehicle-mounted systems work with ad hoc networks for forest-fire reporting without public coverage [2]; and BDS-3 links support satellite command exchange under constraints [3]. For power inspection, BeiDou suits fault alarms, coordinates, equipment numbers, risk levels, and authenti-

cation tags rather than images/video - serving as an emergency channel alongside cellular, dedicated power, LoRa, UAV relay, and edge caching.

Direct BeiDou use faces three challenges: limited payload/frequency may let routine summaries crowd out emergency alarms; random noise, sweeping interference, and outages make fixed link-selection strategies hard to adapt; and without lightweight authentication and trusted forwarding, attackers can disrupt scheduling by forging alarms or replaying messages.

Satellite IoT surveys show value for wide-area coverage in maritime and remote regions [4] but remain constrained by latency, scheduling, and power [5]. Satellite-terrestrial/space-airground integrated network research for 6G emphasizes balancing coverage, scalable access, offloading, and security [6] - providing an architectural foun-

dation for this study.

Space-air-ground-sea network security studies show open wireless links and cross-domain collaboration enable identity forgery, denial of service, and tampering [7]; blockchain-enabled integrated networks improve cross-domain trust and auditing but add overhead [8]; and satellite communication security reviews identify interference, spoofing, replay, and hijacking as typical threats [9] — so a BeiDou-based network cannot rely on encryption alone; reliability, authentication, scheduling, and trusted forwarding must be designed together.

Anti-jamming research uses reinforcement learning to deceive reactive jammers [10], and lightweight secure transmission to balance security and robustness [11] - informing this paper's interference-aware link assessment, though not tailored to low-load BeiDou links or power inspection priority and trusted forwarding.

IoT/smart grid security research shows sensing, communication, and application layers need unified architecture [12]; smart grid reviews summarize layered requirements [13]; smart grid key-exchange schemes inform this paper's authentication design.

We propose BD-SASC, a BeiDou-assisted scalable anti-interference secure communication framework. Contributions: a BeiDou-assisted secure architecture carrying critical status, alarms, and security tags; an interference-aware link reliability model for adaptive selection; priority-compressed scheduling for emergency alarms; a lightweight authentication and antireplay mechanism with reputation decay; and validation across reliability, attacks, scale, burst alarms, and interpretable responses.

Compared with existing satellite IoT and anti-jamming studies, BD-SASC couples BeiDou payload constraints with message priority, trust decay, and heterogeneous link selection - treating emergency alarm delivery as a joint communication-security-scheduling problem rather than a single-link fallback.

2. Methods

2.1. Distributed Power Inspection Network Model

This study considers a distributed power inspection network with four node types: inspection sensing nodes (drones, tower sensors, terminals) collecting status and alarms; edge collaboration nodes handling caching and link selection; BeiDou communication nodes transmitting key alarms via satellite; and cloud dispatch nodes performing authentication and auditing.

Let the inspection network contain N inspection nodes, and denote the node set as follows:

$$\mathcal{V} = \{v_1, v_2, \dots, v_N\}, \quad \mathcal{G} = \{g_1, g_2, \dots, g_M\}. \quad (1)$$

where $\mathcal{V}$ is the set of inspection nodes and $\mathcal{G}$ is the set of edge gateways. This can be represented by the set of communication links as follows:

$$\mathcal{L} = \{l_c, l_p, l_e, l_b\}, \quad (2)$$

Different links have different bandwidth, latency, reliability, energy consumption, and security overhead: cellular or edge caching is prioritized for general summaries, while BeiDou short messages transmit minimum necessary information for critical alarms during publicnetwork interruption or sudden failures (Fig. 1). l_c, l_p, l_e, l_b

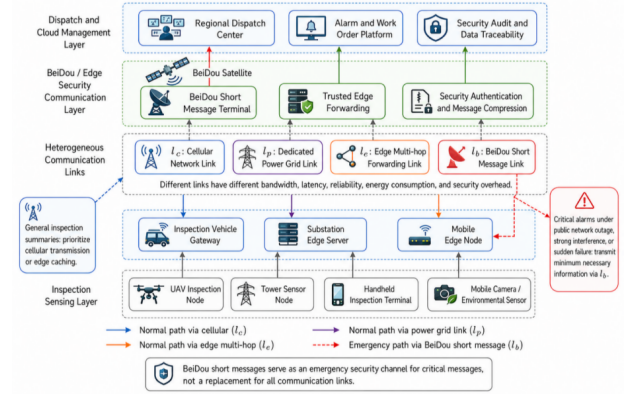


Fig. 1. BeiDou-short-message-assisted secure communication architecture for distributed power inspection networks

Fig. 1 shows BeiDou short messages serve as an emergency secure channel for critical messages in weak-coverage, high-risk scenarios rather than replacing all links - avoiding using short-message links for high-capacity multimedia and reducing queue congestion.

2.2. BeiDou Short Message Constrained Communication Model

The BeiDou short-message link provides wide coverage, strong independence, and support for low-capacity critical data transmission, but it is constrained by payload size, transmission frequency, and queue resources. To adapt to these constraints, the inspection message is represented as follows:

$$m_i(t) = \{ID_i, Loc_i, Type_i, Pri_i, Risk_i, H_i, T_i, Nonce_i, Auth_i\}. \quad (3)$$

where ID_i represents the node number, Loc_i represents the location i coordinates, $Type_i$ represents the message type, Pri_i represents the message priority, $Risk_i$ represents the event risk level, H_i represents the original data digest hash, T_i represents the timestamp, $Nonce_i$ represents the random number, and $Auth_i$ represents the authentication tag.

Short-message transmission resource constraints are defined as follows:

$$\sum_{i=1}^N \text{size}(m_i) x_i(t) + \sum_{i=1}^N \chi_i(t) \text{AuthLen}_i \leq C_b(t), \quad (4)$$

Here, $x_i(t)$ indicates whether the message is scheduled, $\chi_i(t)$ whether the message requires secure encapsulation, AuthLen_i the length of the authentication field, $c_b(t)$ and the current available payload capacity for BeiDou short messages. This constraint illustrates that short message transmission is affected not only by the size of the service field but also by the authentication overhead. Therefore, security design cannot be discussed in isolation from payload constraints.

In implementation, the scheduler checks the encapsulation flag and authentication-field length before dispatching a message, ensuring that security protection remains compatible with the limited BeiDou payload instead of being added as an independent post-processing step.

To reduce short-message payload, the system sends only fault category, device number, risk level, image digest hash, edge recognition result, and retransmission index rather than complete images or videos; complete files are retransmitted through high-bandwidth links after public-network restoration-making BeiDou messages a critical alarm channel rather than a highcapacity data link.

2.3. Interference Model

Inspection networks may encounter random noise, frequency-sweeping interference, localized suppression disabling local links, burst alarms causing queue backlogs, and malicious nodes consuming forwarding resources via low-value messages, causing application-layer congestion.

This paper defines v_i the comprehensive interference intensity of a node at time t as:

$$J_i(t) = \alpha_1 \frac{N_i(t)}{S_i(t) + \epsilon} + \alpha_2 L_i(t) + \alpha_3 D_i(t) + \alpha_4 Q_i(t) + \alpha_5 B_i(t) \quad (5)$$

where the interference terms are noise power, signal strength, packet loss rate, abnormal delay, queue congestion level, and abnormal burst intensity, weighted

to avoid a zero denominator. Unlike a single signal-to-noise ratio model, this jointly considers physical, network, queue, and application layer effects, matching the multi-layer coupling of distributed inspection networks. $N_i(t)S_i(t)L_i(t)D_i(t)Q_i(t)B_i(t)\alpha_1\alpha_5\epsilon$

2.4. Security Threat Model

This paper considers attackers with limited active capabilities who may eavesdrop, replay alarms, forge node identity, tamper with messages, inject false alarms, or cause congestion via low-priority messages, but cannot crack the long-term master key. Security objectives include identity authenticity, message integrity, replay protection, critical alarm reachability, abnormal-node traceability, and low authentication overhead. v_i

$$\begin{aligned} \text{SecRisk}_i(t) = & \rho_1 \text{Rep}_i(t) + \rho_2 \text{Forge}_i(t) + \rho_3 \text{Tamper}_i(t) \\ & + \rho_4 \text{Flood}_i(t) - \rho_5 \text{Trust}_i(t). \end{aligned} \quad (6)$$

Here, $\text{Rep}_i(t)$, $\text{Forge}_i(t)$, $\text{Tamper}_i(t)$ and $\text{Flood}_i(t)$ represent the intensity of replay, forgery, tampering, and congestion behaviors, respectively; $\text{Trust}_i(t)$ represents the node's trustworthiness; ρ_1 and ρ_5 is the risk weight. This risk score will play a role in both link selection and message scheduling.

The threat model assumes that attackers can manipulate communication behavior but cannot obtain long-term master keys. This assumption reflects field inspection scenarios in which ordinary terminals may be exposed, disconnected, or impersonated, while master-key management remains under dispatch-center and gateway control.

2.5. Overall Architecture

BD-SASC has five modules: message-priority determination, interference-aware link assessment, priority-compressed scheduling, lightweight secure encapsulation, and trusted distributed forwarding. Nodes generate summaries and risk levels; edge nodes select transmission strategy by event, location, link status, and trustworthiness; stable links carry complete data while unstable/emergency conditions trigger minimum BeiDou messages; the dispatch center authenticates and verifies on receipt.

BD-SASC follows four principles: BeiDou short messages carry only critical messages and summaries; link selection jointly considers latency, interference intensity, security risk, and reliability; short-message scheduling prioritizes emergency alarms; and security authentication remains lightweight to avoid excessive consumption of payload by authentication fields. Fig. 3 illustrates the secure communication process of BD-SASC.

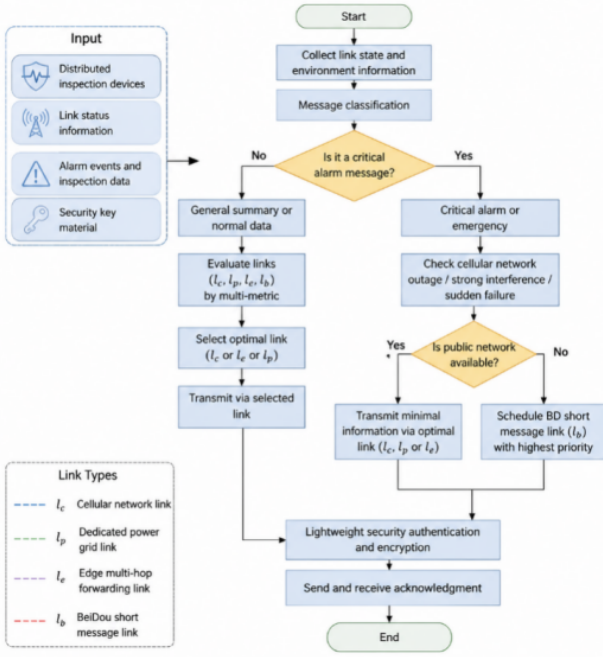


Fig. 2. Flowchart of the BD-SASC anti-interference secure communication algorithm

subsectionReliability Assessment of Interference-Aware Links Define link reliability scores for nodes v_i and links: l_k

$$R_{i,k}(t) = \omega_1 PDR_{i,k}(t) + \omega_2 SNR_{i,k}(t) + \omega_3 Trust_i(t) - \omega_4 J_{i,k}(t) - \omega_5 Delay_{i,k}(t) - \omega_6 Cost_{i,k}(t). \quad (7)$$

where $PDR_{i,k}(t)$ represents message delivery rate, $SNR_{i,k}(t)$ represents signal-to-noise ratio, $Trust_i(t)$ represents node trustworthiness, $J_{i,k}(t)$ represents interference intensity, $Delay_{i,k}(t)$ represents end-to-end latency, and $Cost_{i,k}(t)$ represents communication and authentication overhead. The system selects the link that maximizes overall utility.

$$l_i^*(t) = \underset{l_k \in \mathcal{L}}{\operatorname{argmax}} \left[R_{i,k}(t) + \lambda_1 Pri_i + \lambda_2 Risk_i - \mu SecRisk_i(t) - \nu Q_b(t) \right]. \quad (8)$$

where $Q_b(t)$ represents the BeiDou short-message queue pressure, λ_1 and λ_2, μ and ν represent the priority, service risk, security risk, and queue pressure weight, respectively. For Level 1 emergency alarms, if the reliability of the cellular network and the dedicated power grid is below the threshold, the system directly activates the BeiDou short-message link; if the short-message queue is severely congested, dual-path redundant transmission us-

ing BeiDou short messages and edge trusted forwarding is adopted.

2.6. Priority-Based Short Message Scheduling

Inspection messages are classified into four types (Table 1): P1 (emergency alarms - line breaks, fires, tower collapses, personnel hazards); P2 (important anomalies - insulator damage, icing risk, temperature rise); P3 (periodic summaries, node status, routine data); and P4 (images, videos, logs retransmittable later). The queue prioritizes P1/P2, batch-compresses P3, and sends only summary indexes for P4.

The scheduling objective is:

$$\max \sum_{i=1}^N x_i(t) \cdot Pri_i \cdot Risk_i \cdot R_{i,k}(t) \cdot U_i(t) - \xi \sum_{i=1}^N x_i(t) \text{size}(m_i), \quad (9)$$

The constraints are:

$$\sum_{i=1}^N \text{size}(m_i) x_i(t) \leq C_b(t) \\ Delay_i(t) \leq D_{\max}^{Pri}, \quad x_i(t) \in \{0, 1\}. \quad (10)$$

For messages exceeding payload limits, BD-SASC compresses fields by priority: Level 1 alarms retain node number, location, fault type, risk level, timestamp, digest hash, and authentication tag; Level 2 retains device number, event type, risk level, digest hash, and tag; Level 3 undergoes batch digest processing; Level 4 sends only index and hash, bypassing the high-priority queue. $U_i(t)C_b(t)D_{\max}^{Pri}$

The compression policy is priority-preserving: it removes redundant descriptive fields from low-priority messages first, while retaining identity, location, risk level, timestamp, digest, and authentication information for P1 alarms. This design keeps emergency messages verifiable even when the payload budget is tight.

2.7. Lightweight Secure Encapsulation and Replay Protection Mechanism

To accommodate short-message payload constraints, this paper employs a lightweight message authentication mechanism. Nodes v_i share session keys with the scheduling center or regional edge gateway k_i . For messages $m_i(t)$, the authentication tag is defined as:

$$Auth_i = MAC_{k_i}(ID_i || T_i || Nonce_i || H_i || Pri_i || Risk_i). \quad (11)$$

This H_i includes a summary of the original inspection data:

Table 1. Inspection Message Priority Classification and Short-Message Transmission Strategy

Priority	Typical Message	Reserved Short-Message Fields	Transmission Strategy
P1	Line break, fire, tower collapse, personnel hazard	Node, location, fault type, risk level, timestamp, hash, authentication tag	Send immediately, with dual-path redundancy if necessary
P2	Insulator damage, icing risk, abnormal temperature rise	Device number, event type, risk level, hash, authentication tag	BeiDou-priority transmission or trusted edge forwarding
P3	Routine inspection summary, node status	Batch summary, time range, node set, authentication tag	Batch transmission during low congestion
P4	Images, videos, complete logs	Index, hash, and retransmission address	Local caching until a high-bandwidth link is available

$$H_i = \text{Hash}(\text{Data}_i \parallel \text{Loc}_i \parallel \text{Type}_i \parallel \text{Risk}_i \parallel T_i). \quad (12)$$

The receiving end checks whether the timestamp window and random number are duplicated (indicating replay) and whether the authentication tag matches (indicating forgery/tampering); after successful authentication, the scheduling center generates an alarm ticket by priority and risk level. $\text{Auth}_i \text{ Nonce}_i$

To prevent malicious nodes from continuously sending abnormal messages, this paper introduces node trustworthiness updates:

$$\begin{aligned} \text{Trust}_i(t+1) = & \eta \text{Trust}_i(t) \\ & + (1-\eta) [\beta_1 S_i(t) + \beta_2 F_i(t) \\ & - \beta_3 A_i(t) - \beta_4 \text{Drop}_i(t)]. \end{aligned} \quad (13)$$

Here, $S_i(t)$ represents the authentication success rate, $F_i(t)$ represents the effective forwarding contribution, $A_i(t)$ represents the intensity of abnormal behavior, $\text{Drop}_i(t)$ represents the abnormal discarded records, η and is the historical memory coefficient. When a node's trustworthiness falls below the threshold, the system reduces its forwarding priority and requires the edge gateway to perform secondary verification.

The trust threshold can be configured according to the security level of an inspection area. In high-risk corridors, the threshold may be raised to accelerate secondary verification; in low-risk routine inspection, it may be relaxed to reduce false isolation of temporarily unstable nodes.

2.8. Trusted Distributed Forwarding

When public-network coverage is weak or the queue is congested, nodes perform multi-hop forwarding through

trusted edge nodes, selected by link quality, trustworthiness, remaining energy, historical success rate, and security risk.

$$\begin{aligned} G_j(t) = & \gamma_1 R_j(t) + \gamma_2 \text{Trust}_j(t) + \gamma_3 E_j(t) \\ & - \gamma_4 \text{Delay}_j(t) - \gamma_5 \text{SecRisk}_j(t) \\ & - \gamma_6 \text{Load}_j(t). \end{aligned} \quad (14)$$

Here, $E_j(t)$ represents the remaining energy, and $\text{Load}_j(t)$ represents the current forwarding load. The system selects the node with the highest score and a credibility level above the threshold as the forwarding node. For P1 type messages, the system can simultaneously select BeiDou short messages and trusted edge links for redundant transmission to improve alarm reachability in extreme scenarios.

2.10 Interference-Aware Secure Link-Selection Algorithm

The link-selection algorithm takes node status, message priority, candidate links, interference intensity, queue length, and trustworthiness as input, computing each candidate link's reliability score adjusted by priority (higher-priority messages weight reliability/security more, routine messages weight energy/queue resources more); when all ground-link scores fall below threshold, BeiDou activates, and congestion triggers trusted edge forwarding.

The algorithm's complexity is $O(NK)$, where n is the number of nodes and K is the number of candidate links. Since the types of links in real-world systems are limited and K typically small, this process can meet the real-time decision-making requirements of edge nodes.

2.9. Priority-Based Short Message Scheduling Algorithm

The algorithm first calculates the message scheduling score based on message priority, risk level, link reliability, and waiting time:

Algorithm 1. Interference-Aware Secure Link Selection

Require: Nodes v_i , messages $m_i(t)$, candidate link set $\mathcal{L}$, interference intensity $J_{i,k}(t)$, node trustworthiness $\text{Trust}_i(t)$
Ensure: Optimal communication link $l_i^*(t)$

- 1: **for** each candidate link $k \in \mathcal{L}$ **do**
- 2: Calculate $PDR_{i,k}(t)$, $SNR_{i,k}(t)$, $\text{Delay}_{i,k}(t)$, and $\text{Cost}_{i,k}(t)$
- 3: Calculate $J_{i,k}(t)$ according to the interference model
- 4: Calculate $\text{SecRisk}_i(t)$ based on the historical behavior of node v_i
- 5: **for** each candidate link $k \in \mathcal{L}$ **do**
- 6: Compute the comprehensive link score using the link utility function
- 7: **if** $\text{Pri}_i = P1$ **and** the ground-link score is below the threshold **then**
- 8: Enable the BeiDou short-message service
- 9: **if** the short-message queue is overloaded **then**
- 10: Select trusted edge forwarding as the backup path
- 11: Select the link with the highest score satisfying the security constraints
- 12: **return** $l_i^*(t)$

$$\begin{aligned} \text{Score}_i(t) = & \delta_1 \text{Pri}_i + \delta_2 \text{Risk}_i + \delta_3 \text{Wait}_i(t) \\ & + \delta_4 R_i(t) - \delta_5 \text{Size}_i - \delta_6 \text{SecRisk}_i(t). \end{aligned} \quad (15)$$

The messages are then sorted according to their scheduling scores, and eligible messages are selected sequentially under the short-message capacity constraint. If the message length exceeds the payload limit, field compression is performed; if it still exceeds the limit, only the fault type, location, risk level, and data digest are sent. This algorithm can be implemented using a priority queue with a complexity of $O(N \log N)$.

2.10. Lightweight Authentication and Replay Detection Algorithm

The authentication algorithm maintains time-window, random-number cache, and trustworthiness tables: messages passing timestamp, duplication, and tag checks enter the risk queue; failures enter the anomaly audit queue with reduced trustworthiness. Since caches use hash tables, average detection complexity is low. $O(1)$

2.11. Scalability Analysis

BD-SASC's scalability has three aspects: link-selection complexity scales linearly with nodes; short-message scheduling uses priority queues for rapid filtering during burst alarms; and authentication relies on lightweight hashing rather than complex certificate exchange. Edge gateways process node status by inspection area while the scheduling center receives only key alarm summaries, reducing centralized cloud pressure.

The total system overhead can be expressed as:

$$\begin{aligned} C_{\text{total}} &= C_{\text{link}} + C_{\text{queue}} + C_{\text{auth}} + C_{\text{audit}} \\ &= O(NK) + O(N \log N) + O(N) + O(M). \end{aligned} \quad (16)$$

Algorithm 2. Priority-Based Short Message Compressed Scheduling

Require: Message queue Q , short-message capacity $C_b(t)$, maximum allowable delay $D_{\text{max}}^{\text{Pri}_i}$
Ensure: Short-message transmission set S

- 1: Initialize $S \leftarrow \emptyset$
- 2: **for** each message $m_i(t) \in Q$ **do**
- 3: Calculate the priority score $\text{Score}_i(t)$
- 4: Sort messages in descending order of $\text{Score}_i(t)$
- 5: **for** each message $m_i(t)$ in the sorted queue **do**
- 6: **if** $\text{Pri}_i \in \{P1, P2\}$ **then**
- 7: Give the message priority for inclusion in S
- 8: **if** message length $> C_b(t)$ **then**
- 9: Perform field compression
- 10: **if** compressed message length $> C_b(t)$ **then**
- 11: Generate and transmit a minimum-risk digest
- 12: **else**
- 13: Add the compressed message to S
- 14: **else**
- 15: Add the original message to S
- 16: **else if** $\text{Pri}_i = P3$ **then**
- 17: **if** the short-message queue is idle **then**
- 18: Add the message to a batch-transmission set
- 19: **else if** $\text{Pri}_i = P4$ **then**
- 20: Retain only the message index and hash
- 21: Wait for retransmission over a high-bandwidth link
- 22: **return** S

where M represents the number of edge gateways. When K and M are relatively stable, the system overhead is mainly $O(N \log N)$ determined by the queue scheduling of, which can meet the real-time requirements of a 1000-node-level inspection network.

This overhead analysis clarifies why BD-SASC scales mainly with queue scheduling and gateway partitioning rather than with a centralized exhaustive search. As the node scale increases, regional edge gateways absorb local status updates and forward only alarm summaries and audit records to the dispatch center.

2.12. Simulation Scenario

This paper simulates a 30km×30km mountainous transmission corridor with substations, mountain towers, forest lines, weak-coverage areas, and interference zones. Nodes (drones, tower sensors, handheld terminals, vehicle gateways) range from 50 to 1000 for scalability testing, across cellular, dedicated power, edge multi-hop, and BeiDou links.

Message load has three levels: low (0.2/node/min), medium (0.5/node/min), and burst (many simultaneous localized alarms within 5 min); malicious-node ratios are 0-20%; interference intensities are 0.1-0.9; each experiment is repeated 30 times and averaged.

The selected parameter ranges are intended to cover weak coverage, moderate interference, severe interference,

Algorithm 3. Lightweight Authentication and Anti-Replay Detection

Require: Short message $m_i(t)$, node key k_i , nonce cache table $\mathcal{N}$, time window ΔT

Ensure: Authentication result and node trust update value

- 1: Extract timestamp T_i , nonce Nonce_i , and authentication tag Auth_i
- 2: **if** $|T_{\text{recv}} - T_i| > \Delta T$ **then**
- 3: Mark the message as invalid due to timestamp expiration
- 4: Write the abnormal event to the security audit table
- 5: Reduce node trustworthiness
- 6: **return** authentication failure
- 7: **if** $\text{Nonce}_i \in \mathcal{N}$ **then**
- 8: Mark the message as a potential replay attack
- 9: Write the abnormal event to the security audit table
- 10: Reduce node trustworthiness
- 11: **return** authentication failure
- 12: Recalculate the authentication tag Auth'_i using $m_i(t)$ and k_i
- 13: **if** $\text{Auth}'_i \neq \text{Auth}_i$ **then**
- 14: Mark the message as forged or tampered with
- 15: Write the abnormal event to the security audit table
- 16: Reduce node trustworthiness
- 17: **return** authentication failure
- 18: **else**
- 19: Accept the message
- 20: Add Nonce_i to the cache table $\mathcal{N}$
- 21: Increase or maintain node trustworthiness
- 22: **return** authentication success

routine operation, and localized emergency bursts. Repeating each experiment 30 times reduces the influence of random topology and attack-position variation on the reported average results.

2.13. Simulation Parameter Settings

Table 2 shows the main simulation parameters.

2.14. Comparison Algorithms and Evaluation Metrics

Five comparison methods are used: Cellular-only (public network, waits for recovery when unavailable); Fixed-BDS (BeiDou without interference-aware selection or priority scheduling); Random-Relay (random edge forwarding without trust); Delay-Minimum (lowest-delay link regardless of security/priority); and Encryption-only (encryption without interference-aware scheduling or trusted forwarding) - isolating each design element's contribution. Delay

The comparison baselines are selected to isolate the contribution of each design element. Cellular-only tests dependence on terrestrial links, Fixed-BDS tests nonadaptive satellite fallback, Random-Relay tests forwarding without trust, Delay-Minimum tests latency-only routing, and Encryption-only tests security without scheduling awareness.

The following metrics are used to evaluate system performance. Message delivery rate:

$$PDR = \frac{N_{\text{recv}}}{N_{\text{sent}}}, \quad (17)$$

The secure delivery rate is:

$$SDR = \frac{N_{\text{valid}}}{N_{\text{sent}}}, \quad (18)$$

The emergency alarm success rate is:

$$ESR = \frac{N_{P1}^{\text{valid}}}{N_{P1}^{\text{sent}}}, \quad (19)$$

The average end-to-end latency is:

$$\text{Delay} = \frac{1}{N_{\text{recv}}} \sum_{i=1}^{N_{\text{recv}}} (t_i^{\text{recv}} - t_i^{\text{send}}). \quad (20)$$

Scalability degradation rate:

$$SD = \frac{\text{Metric}_{c50} - \text{Metric}_{c1000}}{\text{Metric}_{50}}. \quad (21)$$

3. Results and discussion

3.1. Communication Reliability Under Different Interference Intensities

Fig. 4 shows secure delivery rate under different interference intensities (500 nodes, 10% malicious): Cellular-only falls to 61.8%; Fixed-BDS falls to 78.4% from burst-load queue backup; Encryption-only intercepts some forgeries but doesn't improve link selection; BD-

SASC maintains 91.6% via combined interference-aware selection, priority scheduling, and trusted forwarding.

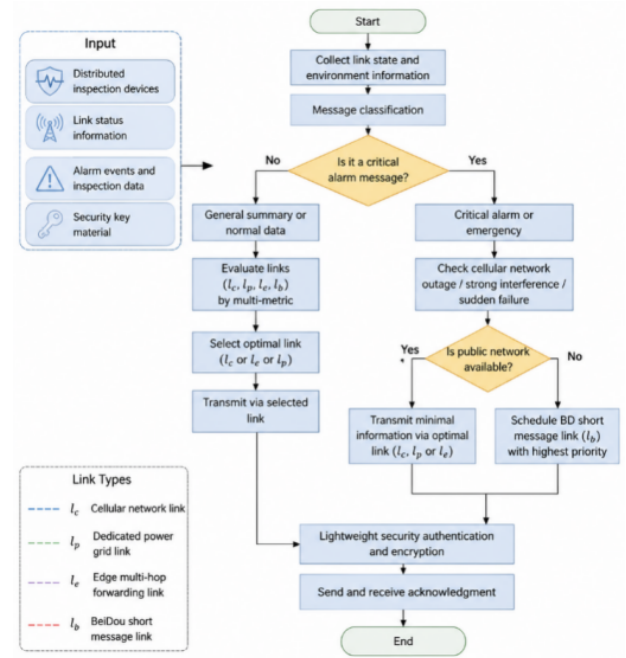
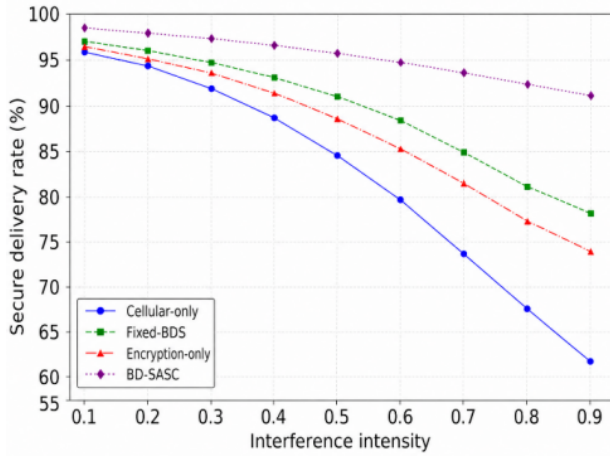


Fig. 3. Flowchart of the BD-SASC anti-interference secure communication algorithm

Table 2. Simulation Parameter Settings

Parameter	Value	Description
Simulation area	30 km × 30 km	Mountain power transmission corridor
Number of inspection nodes	50, 100, 200, 500, 1000	Scalability testing
Number of edge gateways	5, 10, 20	Partition forwarding and caching
Interference intensity	0.1, 0.3, 0.5, 0.7, 0.9	From low interference to strong interference
Malicious-node ratio	0%, 5%, 10%, 15%, 20%	Forgery, replay, and congestion attacks
Message load	Low, medium, and burst	Routine inspections and post-disaster repairs
P1 maximum latency	8 s	Emergency alarm constraint
P2 maximum latency	20 s	Important anomaly constraint
Number of repetitions	30	Results are averaged over all repetitions.

**Fig. 4.** Comparison of secure delivery rates of different algorithms under different interference intensities

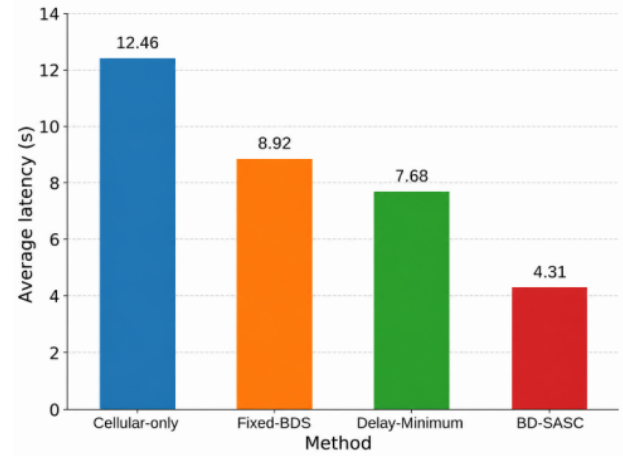
BD-SASC's advantage comes from coordinating multiple mechanisms: prioritizing lowlatency links when ground quality is good, increasing BeiDou/trusted-forwarding weight under interference, and increasing authentication-risk weight under attack - achieving balanced reliability and security improvement rather than acting as a simple satellite backup.

This result indicates that BD-SASC is not simply a satellite backup channel. Its gain comes from coordinating link assessment, queue control, and trust-aware forwarding, which is particularly important when physical interference and malicious traffic occur at the same time.

3.2. Emergency Message Latency in Burst-Alarm Scenarios

Fig. 5 shows average P1 message latency when 80 nodes generate burst alarms within 5 minutes: Cellular-only reaches 12.46s in weak-coverage areas; Fixed-BDS reaches 8.92s from routing everything into the short-message queue; Delay-Minimum reaches 7.68s from choosing low-stability fast links under burst load; BD-SASC's priority scheduling and field compression reduce average latency

to 4.31s.

**Fig. 5.** Comparison of average P1-message latency in burst-alarm scenarios

Short-message links don't automatically guarantee low latency - only combined prioritization, compression, and scheduling prevent low-value messages from consuming critical alarm resources. BD-SASC retains minimum necessary fields for P1 messages and delays P3/P4 retransmission, enabling faster critical alarm reporting.

The latency result further explains why compression and scheduling must be considered together. Without priority-aware compression, even a reliable satellite channel can be delayed by low-value traffic and cannot guarantee rapid transmission of emergency alarms.

3.3. Security Performance Under Different Attack Ratios

Table 3 shows attack detection and false-positive rates as malicious-node ratio rises from 5% to 20%: Cellular-only, Random-Relay, and Delay-Minimum lack complete authentication and provide weak protection; Encryption-only verifies integrity but wastes queue resources without reputation decay or trusted forwarding; BD-SASC combines authentication tags, timestamps, random-number caching,

and trustworthiness, maintaining 95.4% detection even at 20% malicious nodes. Delay

The security advantage of BD-SASC mainly comes from replay detection based on timestamps and random-number caches, together with abnormal-behavior-driven trust decay. Even if malicious nodes obtain short-term access, they are unlikely to occupy high-priority forwarding resources for long periods. This makes BD-SASC suitable for inspection scenarios with many nodes, where some nodes may become disconnected or be impersonated.

3.4. Node-Scale Expansion Experiment

To verify scalability, nodes increase from 50 to 1000 (Fig. 6, moderate interference, 10% malicious): queue pressure and authentication overhead increase for all methods, but BD-SASC degrades least, maintaining 92.4% secure delivery at 1000 nodes, while Fixed-BDS's queue pressure grows rapidly without priority scheduling and Cellular-only drops to 68.9% in weak-coverage areas.

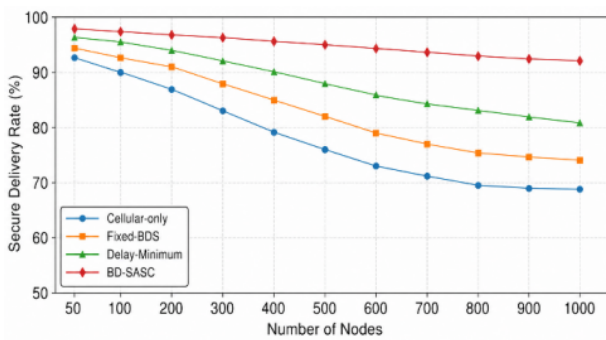


Fig. 6. Comparison of secure delivery rates of different algorithms under different network sizes

In terms of scalability, the advantage of BD-SASC comes from layered processing: inspection nodes generate summaries and authentication tags, edge gateways evaluate links and schedule queues, and the scheduling center receives key alarms and audit results. This design reduces centralized cloud pressure and prevents all messages from entering the short-message link directly and causing congestion.

3.5. Ablation Study

Table 4 analyzes module contributions via BD-SASC-I (no interference-aware assessment), BD-SASC-P (no priority scheduling), BD-SASC-T (no trusted forwarding), and BD-SASC-R (no replay detection) at 500 nodes, 0.7 interference, 15% malicious nodes.

Ablation shows interference-awareness mainly improves secure delivery under strong interference; priority scheduling mainly reduces emergency latency;

trusted forwarding mainly improves reachability in weak-coverage/partial-failure scenarios; and replay detection has the greatest effect on attack detection - the complete framework achieving the best performance through module cooperation.

The ablation study also provides module-level evidence for deployment. Operators can prioritize interference awareness in high-jamming regions, trusted forwarding in weakcoverage corridors, and replay detection in areas where node impersonation or repeated alarm injection is more likely.

3.6. Multi-Algorithm Real-Scenario Response Visualization Analysis

Fig. 7 visualizes the real-scenario responses of multiple algorithms. The figure uses a mountainous power transmission corridor as the background, with 40 tower nodes, three areas of strong localized interference, and five burst-alarm points. Each algorithm runs in the same scenario, and the figure shows successfully delivered nodes, failed nodes, and P1 alarm nodes.

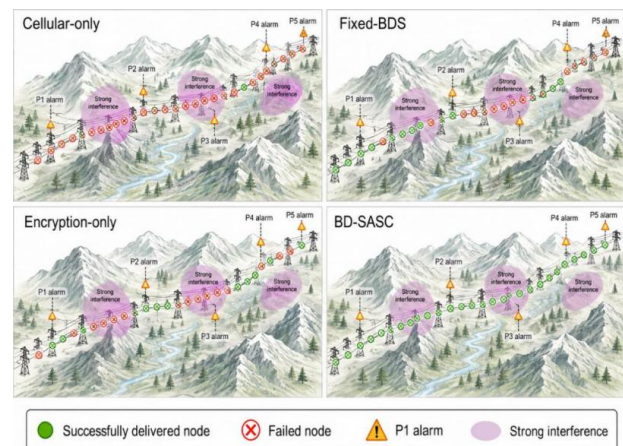


Fig. 7. Visual comparison of real-scenario responses across algorithms

Fig. 7 shows failure causes differ by algorithm: Cellular-only fails mainly in weakcoverage areas; Fixed-BDS suffers queue congestion during simultaneous burst alarms; Encryption-only improves forgery interception but not link selection or scheduling, so nodes still fail in interference areas; BD-SASC prioritizes BeiDou in strong-interference areas, trusted forwarding in weak-coverage areas, and compressed P1 priority in burst-alarm areas, yielding the fewest failed nodes.

The visualization complements the numerical metrics by showing where failures occur spatially. This is useful for engineering deployment because weak public-network

Table 3. Security Performance Under Different Attack Ratios

Attack ratio	Cellular-only ADR	Encryption-only ADR	BD-SASC ADR	BD-SASC False Alarm Rate
5%	41.3%	89.5%	96.8%	2.7%
10%	38.6%	87.2%	96.5%	3.1%
15%	35.4%	84.6%	96.2%	3.6%
20%	32.8%	81.7%	95.4%	4.2%

Table 4. Ablation Study Results

Method	Secure delivery rate	P1 alarm success rate	Average latency (s)	Attack detection rate
BD-SASC-I	85.7%	89.4%	7.26	94.1%
BD-SASC-P	88.2%	86.9%	8.11	95.7%
BD-SASC-T	89.6%	91.8%	6.73	95.9%
BD-SASC-R	91.4%	94.2%	5.38	73.6%
Full BDSASC	93.2%	96.4%	4.47	96.2%

areas, interference zones, and burst-alarm locations often overlap only partially in real transmission corridors.

3.7. Deployment Discussion

BD-SASC suits mountainous transmission lines, forest inspection, post-disaster repair, remote substations, and unstable-coverage areas. BeiDou terminals can be installed on inspection vehicles, drone base stations, or edge gateways; routine data uses public or dedicated networks, while unavailable networks or emergencies trigger BeiDou key-field transmission, with images/video retransmitted at full resolution after high-bandwidth link restoration.

Implementation must also consider key management, node registration, terminal energy consumption, short-message tariffs, edge-device stability, and power security zoning. For nodes that remain unattended for long periods, authentication overhead and communication frequency should be reduced. Mobile inspection terminals should support key updates and identity revocation. The dispatch center must maintain traceability between alarm summaries and original inspection data.

From a business-process perspective, BD-SASC can be integrated with inspection work orders, equipment ledgers, and dispatch alarm platforms. The equipment number, location, risk level, summary, and hash contained in a short message can be used to locate faults quickly, trigger emergency work orders, and verify subsequent retransmission data.

Limitations: experiments use simulation and typical-scenario modeling requiring further field testing; the study focuses on key short-message transmission rather than cross-link multimedia retransmission; lightweight authentication could be strengthened with zero-trust architecture or blockchain auditing; and interference modeling could incorporate real spectrum-sampling data and time-varying

link prediction.

To avoid overstating the contribution, the revised discussion positions the results as simulation-based evidence rather than field proof. The next stage should test real BeiDou terminals, gateway placement, tariff constraints, and electromagnetic measurements in representative mountain-line corridors.

4. Conclusions

This paper addresses critical-message transmission in distributed power grid inspection networks under weak coverage, interference, and attacks via BD-SASC, using BeiDou short messages as an emergency channel for critical alarms. Through interference-aware link assessment, priority-compressed scheduling, lightweight encapsulation, and trusted forwarding, it jointly optimizes reliability, security, and scalability. Results show 91.6% secure delivery under strong interference and 15% malicious nodes, 92.4% delivery and 3.7% queue overflow at 1000 nodes, with visualization confirming stable responses in complex scenarios.

Future research will focus on three aspects. First, field verification will be conducted with real BeiDou short-message terminals and mountainous power transmission lines. Second, multi-link collaborative transmission among BeiDou short messages, UAV relays, 5G private networks, and edge intelligence will be studied. Third, zero-trust identity management and cross-regional security audit mechanisms will be introduced to strengthen the long-term secure operation of large-scale power inspection networks.

Future work will also evaluate parameter sensitivity, including trust thresholds, queue capacity limits, payload-compression ratios, and gateway density, so that the method can be configured for different regional inspection

policies and communication budgets.

References

- [1] G. Li, S. Guo, J. Lv, K. Zhao, and Z. He, (2021) "Introduction to Global Short-Message Communication Service of BeiDou-3 Navigation Satellite System" **Advances in Space Research** 67(5): 1701–1708. DOI: [10.1016/j.asr.2020.12.011](https://doi.org/10.1016/j.asr.2020.12.011).
- [2] C. Xu, S. Sun, Y. Zhou, and Z. Ding, (2024) "Research on a Vehicle-Mounted Emergency Communication System Using BeiDou Regional Short Message Communication (RSMC) for Firefighting Operations in Forest Areas Without a Public Network" **Forests** 15(7): 1185. DOI: [10.3390/f15071185](https://doi.org/10.3390/f15071185).
- [3] C. Li, P. Liu, S. Fu, Y. Jiao, and W. Zhang, (2023) "Requirement-Oriented TT&C Method for Satellite Based on BDS-3 Short-Message Communication System" **Space: Science & Technology** 3: 0038. DOI: [10.34133/space.0038](https://doi.org/10.34133/space.0038).
- [4] M. Centenaro, C. E. Costa, F. Granelli, C. Sacchi, and L. Vangelista, (2021) "A Survey on Technologies, Standards and Open Challenges in Satellite IoT" **IEEE Communications Surveys & Tutorials** 23(3): 1693–1720. DOI: [10.1109/COMST.2021.3078433](https://doi.org/10.1109/COMST.2021.3078433).
- [5] X. Chen, Z. Xu, and L. Shang, (2023) "Satellite Internet of Things: Challenges, Solutions, and Development Trends" **Frontiers of Information Technology & Electronic Engineering** 24(7): 935–944. DOI: [10.1631/FITEE.2200648](https://doi.org/10.1631/FITEE.2200648).
- [6] X. Zhu and C. Jiang, (2022) "Integrated Satellite-Terrestrial Networks Toward 6G: Architectures, Applications, and Challenges" **IEEE Internet of Things Journal** 9(1): 437–461. DOI: [10.1109/JIOT.2021.3126825](https://doi.org/10.1109/JIOT.2021.3126825).
- [7] H. Guo, J. Li, J. Liu, N. Tian, and N. Kato, (2022) "A Survey on Space-Air-Ground-Sea Integrated Network Security in 6G" **IEEE Communications Surveys & Tutorials** 24(1): 53–87. DOI: [10.1109/COMST.2021.3131332](https://doi.org/10.1109/COMST.2021.3131332).
- [8] Y. Wang, Z. Su, J. Ni, N. Zhang, and X. Shen, (2022) "Blockchain-Empowered Space-Air-Ground Integrated Networks: Opportunities, Challenges, and Solutions" **IEEE Communications Surveys & Tutorials** 24(1): 160–209. DOI: [10.1109/COMST.2021.3131711](https://doi.org/10.1109/COMST.2021.3131711).
- [9] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, (2022) "Satellite-Based Communications Security: A Survey of Threats, Solutions, and Research Challenges" **Computer Networks** 216: 109246. DOI: [10.1016/j.comnet.2022.109246](https://doi.org/10.1016/j.comnet.2022.109246).
- [10] A. Pourranjbar, G. Kaddoum, F. Ferdowsi, and W. Saad, (2021) "Reinforcement Learning for Deceiving Reactive Jammers in Wireless Networks" **IEEE Transactions on Communications** 69(6): 3682–3697. DOI: [10.1109/TCOMM.2021.3062854](https://doi.org/10.1109/TCOMM.2021.3062854).
- [11] M. Letafati, A. Kuhestani, K.-K. Wong, and M. J. Piran, (2021) "A Lightweight Secure and Resilient Transmission Scheme for the Internet of Things in the Presence of a Hostile Jammer" **IEEE Internet of Things Journal** 8(6): 4373–4388. DOI: [10.1109/JIOT.2020.3026475](https://doi.org/10.1109/JIOT.2020.3026475).
- [12] J. Zhang, Y. Ye, C. Hu, and B. Li, (2021) "Architecture Design and Demand Analysis on Application Layer of Standard System for Ubiquitous Power Internet of Things" **Global Energy Interconnection** 4(3): 304–314. DOI: [10.1016/j.gloi.2021.07.001](https://doi.org/10.1016/j.gloi.2021.07.001).
- [13] Z. Alavikia and M. Shabro, (2022) "A Comprehensive Layered Approach for Implementing Internet of Things-Enabled Smart Grid: A Survey" **Digital Communications and Networks** 8(3): 388–410. DOI: [10.1016/j.dcan.2022.01.002](https://doi.org/10.1016/j.dcan.2022.01.002).