ISSN 2616-5775 Vol. 8, Issue 7: 105-114, DOI: 10.25236/AJCIS.2025.080713

A Security Assessment Method for Low Earth Orbit Satellite Internet of Things Based on Multi-Dimensional Resilience Indicators

Shihua Pan[1,2,a], Yunlong Xiang[1,2,b], Fei Xie[1,2,c], Yong Wang, [1,2,d], Yihua Hu[1,2,e], Qingsong Zhao[1,2,f,*]

[1]The College of Electronic Engineering, National University of Defense Technology, Hefei, 230037, China
[2]The Anhui Province Key Laboratory of Electronic Restriction, Hefei, Anhui, 230037, China
[a]psh2001@nudt.edu.cn, [b]xylhf_2010@126.com, [c]xiemw@nudt.edu.cn, [d]wyeei@126.com, [e]skl_hyh@163.com, [f]zqs_pine@nudt.edu.cn
[*]Corresponding author

Abstract: *As Low Earth Orbit (LEO) satellite Internet of Things emerges as a critical global infrastructure, traditional static or single-dimensional security assessment methods fail to effectively characterize system resilience performance when facing complex security threats. To address this problem, this paper proposes a security assessment method for LEO satellite IoT communication systems based on multi-dimensional resilience indicators. The method innovatively decomposes system resilience into three mutually orthogonal dimensions: anti-degradation capability, system adaptability, and system stability, and employs weighted geometric mean to fuse the three-dimensional indicators for calculating comprehensive resilience. Simulation experimental results demonstrate that the proposed multi-dimensional resilience assessment method can accurately reflect the resilience variation characteristics of systems facing threats such as jamming attacks, DDoS attacks, and replay attacks, providing analytical tools for security assessment and design optimization of LEO satellite IoT systems. It also provides powerful quantitative analysis tools for robustness design, risk management, and operational optimization of LEO satellite IoT, laying a foundation for building next-generation satellite communication systems with greater survivability.*

Keywords: *Satellite Communication, Internet of Things Security, System Resilience, Security Assessment*

1. Introduction

With the rapid development and commercial deployment of Low Earth Orbit (LEO) satellite constellation technology, LEO satellite communication networks have become an important component of global Internet of Things infrastructure[1]. Compared to traditional Geostationary Earth Orbit (GEO) satellites, LEO satellites possess significant advantages such as low orbital altitude, small transmission delay, and relatively low launch costs, providing important communication support for IoT applications in remote areas, marine environments, and emergency communications[2]. The successive advancement of major LEO constellation projects such as SpaceX's Starlink, Amazon's Kuiper, and OneWeb marks the arrival of the satellite IoT era. However, the openness, dynamics, and resource constraints of LEO satellite IoT systems subject them to unprecedented security challenges (as shown in Figure 1). The highly dynamic characteristics of satellite links result in frequent network topology changes, making traditional security protection mechanisms based on static topology difficult to apply effectively[3]. The harsh and open nature of the space environment provides convenient conditions for various physical layer attacks, where attackers can interfere with, eavesdrop on, or spoof satellite signals through ground equipment. The limited computational and storage resources of satellites restrict the deployment of complex security algorithms, making systems susceptible to performance degradation or even service interruption when facing high-intensity or persistent attacks[4]. Therefore, the system's ability to maintain core functions, ensure service stability, and adapt during attacks (i.e., System Resilience) becomes more important than mere defense.

ISSN 2616-5775 Vol. 8, Issue 7: 105-114, DOI: 10.25236/AJCIS.2025.080713

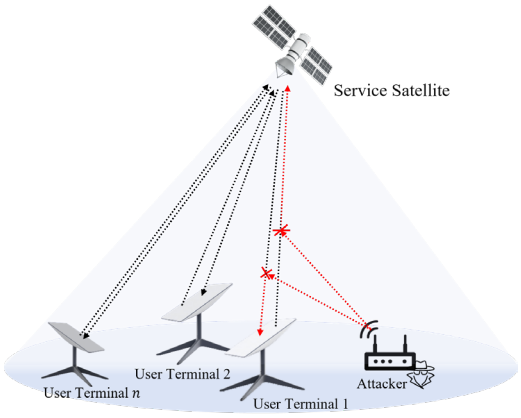

Figure 1 Security Threat Scenarios for LEO Satellite IoT Systems

Traditional network security assessment methods primarily focus on threat identification, vulnerability analysis, and risk level classification. While these methods can help understand the security threats faced by systems, they have obvious deficiencies in quantitatively assessing overall system resilience[5]. Existing quantitative methods often employ single performance indicators (such as throughput or delay), but these cannot comprehensively characterize the complex behavior of systems under attack. For example, a system might maintain throughput through high-intensity retransmissions (high anti-degradation capability), but at the cost of enormous delay jitter and service instability (low system stability). Single indicators cannot distinguish this "fragile balance." Additionally, existing resilience models are mostly designed for terrestrial networks and fail to fully consider the characteristics of LEO satellite networks such as high dynamics and resource constraints. To address the above problems, this paper proposes a security assessment method for LEO satellite IoT communication systems based on multi-dimensional resilience indicators. The main contributions of this paper include the following aspects:

- Innovative three-dimensional resilience model: We decompose system resilience into three mutually orthogonal dimensions: Anti-degradation Capability (ADC), Adaptability (ADP), and System Stability (STS).

- Accurate quantitative calculation method: We design a mathematical method based on system performance time series analysis, achieving accurate quantification of the three resilience dimensions through indicators such as performance retention rate, performance coefficient of variation, and performance degradation frequency, and employ weighted geometric mean for multi-dimensional fusion.

- Comprehensive experimental verification and analysis: We systematically evaluate various attack scenarios in simulation environments, revealing the differential impacts of different attack patterns on various dimensions of system resilience, and verify the effectiveness, accuracy, and practicality of the proposed method.

2. Related Work

In the area of LEO satellite IoT system security assessment, early research primarily employed qualitative assessment methods for security analysis. Samuel et al. proposed a risk assessment framework for satellite communication systems based on expert experience, identifying major security risks through threat matrices and impact assessment models[6]. With the development of simulation technology, researchers began adopting quantitative assessment methods based on performance indicators. Zhang et al. evaluated the security status of LEO satellite networks by analyzing changes in key performance indicators such as system throughput, transmission delay, and packet loss rate[7]. However, these methods often focus only on single or few performance indicators, making it difficult to comprehensively reflect system security performance, particularly prone to assessment bias when dealing with complex attack scenarios. System resilience originally emerged from ecology and was later introduced to engineering and network security fields. Tran et al. divided resilience into three dimensions: absorption capacity, adaptation capacity, and recovery capacity, emphasizing the response characteristics of systems at different stages[8]. Ayyoob et al. proposed a multiple-dimensional resilience model based on prevention, protection, mitigation, and recovery[9]. In terms of quantitative methods, existing research mainly adopts different technical approaches based on graph theory, Markov chains, and performance curve analysis.

ISSN 2616-5775 Vol. 8, Issue 7: 105-114, DOI: 10.25236/AJCIS.2025.080713

Pereira et al. assessed resilience by analyzing network topology connectivity and robustness, finding that network resilience is closely related to its topological structure. Haimes et al. established a system resilience assessment model based on Markov processes, capable of describing the transition patterns of systems between different states[10]. Bruneau et al. proposed a resilience calculation method based on performance loss integration, defining resilience as the reciprocal of the performance loss area during attacks[11].

Although these theories laid the foundation for resilience assessment, they still have limitations when applied to LEO satellite IoT: existing resilience assessment methods struggle to adapt to the special characteristics of LEO satellite IoT systems such as high dynamics, resource constraints, and openness; most research adopts single-dimensional resilience definitions, unable to comprehensively reflect the multi-dimensional response behavior of LEO satellite IoT systems when facing complex threats. This paper addresses the above limitations by proposing a security assessment method for LEO satellite IoT communication systems based on multi-dimensional resilience indicators.

3. Multi-dimensional Resilience Assessment Model

The multi-dimensional resilience indicator-based assessment method proposed in this paper not only considers the system's ability to resist attacks but also fully considers its capability to adapt to dynamic threats and maintain service stability.

3.1 Resilience Definition and Dimension Division

In the context of LEO satellite IoT system security assessment, this paper redefines system resilience as: the comprehensive ability of a system to maintain its core communication functions and quickly recover to normal operating state after attack termination when facing various security threats. Based on the temporal characteristics and behavioral patterns of system responses to security threats, resilience is divided into three mutually orthogonal dimensions:

Anti-degradation Capability (ADC): Reflects the system's ability to maintain performance levels during attacks. When a system is under attack, good anti-degradation capability ensures that the system's core functions do not completely fail, creating conditions for subsequent recovery.

System Adaptability (ADP): Embodies the system's ability to adjust operational strategies according to changes in the threat environment. A system with good adaptability can proactively adjust its working mode after detecting attacks, mitigating attack impacts through resource allocation reconfiguration, protocol parameter modification, or working frequency switching.

System Stability (STS): Represents the system's ability to maintain performance stability and reduce fluctuations during attacks. Good system stability ensures that the system does not experience severe performance fluctuations when facing threats, maintaining relatively stable service quality.

3.2 Mathematical Modeling of Resilience Indicators

Let $P(t)$ represent the core performance indicator of system operational status (such as system throughput, transmission success rate, average delay, etc.). For the attack time interval $[t_1, t_2]$, define the following basic parameters: baseline performance P_{baseline} represents the normal performance level of the system before attack, obtained through statistical analysis of performance data over a period before the attack; attack period performance P_{attack} represents the average performance level of the system during the attack duration; recovery period performance $P_{\text{recovery}}(t)$ represents the variation of system performance over time after attack termination.

$$\begin{cases} P_{baseline} = \dfrac{1}{t_0}\displaystyle\int_0^{t_1} P(t)dt \\ P_{attack} = \dfrac{1}{t_2 - t_1}\displaystyle\int_{t_1}^{t_2} P(t)dt \\ P_{recovery}(t) = P(t),\ t > t_2 \end{cases} \tag{1}$$

3.2.1 Anti-degradation Capability

Anti-degradation capability reflects the degree to which the system maintains performance during

ISSN 2616-5775 Vol. 8, Issue 7: 105-114, DOI: 10.25236/AJCIS.2025.080713

attacks. The model focuses on comparing attack period performance with baseline performance. Considering that different types of attacks may lead to different degrees of performance degradation, this paper uses normalized performance retention rate to define anti-degradation capability, as shown in equation (2):

$$ADC = max\left(0, \frac{P_{attack}}{P_{baseline}}\right) \tag{2}$$

The value range of this indicator is [0,1], where ADC=1 indicates that system performance is completely undiminished during attacks, and ADC=0 indicates that the system completely fails during attacks. When multiple discontinuous attack periods exist, the comprehensive calculation of anti-degradation capability is:

$$ADC_{total} = \frac{1}{n}\sum_{i=1}^{n} ADC_i \tag{3}$$

Where n is the number of attack periods. To more precisely reflect the degree of performance degradation, the concept of performance degradation rate is introduced, represented by equation (4).

$$\delta_{degradation} = 1 - ADC = \frac{P_{baseline} - P_{attack}}{P_{baseline}} \tag{4}$$

3.2.2 Adaptability

Adaptability reflects the flexibility of the system in adjusting operational states when facing threats. Its quantification needs to consider the variation patterns of system performance during attack periods. The standard deviation of performance during attack periods can be defined by equation (5):

$$\sigma_{attack} = \sqrt{\frac{1}{t_2 - t_1}\int_{t_1}^{t_2}\left[P(t) - P_{attack}\right]^2 dt} \tag{5}$$

A system with good adaptability should be able to quickly adjust its operational strategy after detecting attacks, thereby maintaining relatively stable performance levels during attack periods. This paper uses the negative exponential function of the coefficient of variation of performance during attack periods as shown in equation (6) to define adaptability:

$$\begin{cases} CV_{attack} = \dfrac{\sigma_{attack}}{P_{attack}} \\ ADP = exp\left(-\alpha \cdot CV_{attack}\right) \end{cases} \tag{6}$$

Where CV_{attack} is the coefficient of variation of performance during attack periods, and α is the adjustment parameter. A smaller coefficient of variation indicates that the system can maintain relatively stable performance levels during attack periods, demonstrating good adaptability. The use of exponential functions ensures that the adaptability indicator is within the [0,1] interval while effectively distinguishing different degrees of adaptive capability. To consider the dynamic adaptive capability of the system, a performance adjustment speed factor is introduced:

$$v_{adapt} = \frac{1}{t_2 - t_1}\int_{t_1}^{t_2}\left|\frac{dP(t)}{dt}\right| dt \tag{7}$$

Considering the dynamic adjustment parameter γ, the system adaptability indicator expression can be modified to equation (8).

$$ADP_{dynamic} = ADP \cdot exp\left(-\gamma \cdot \frac{v_{adapt}}{P_{attack}}\right) \tag{8}$$

3.2.3 System Stability

System stability focuses on the degree of performance stability and fluctuation characteristics when the system faces threats. In actual satellite communications, good system stability can provide predictable service quality for upper-layer applications, avoiding application interruptions caused by performance fluctuations. Performance volatility reflects the severity of system performance changes during attack periods, while performance degradation frequency embodies the frequency of the system suffering continuous impacts. These two factors interact and jointly determine the system's stability level. This

ISSN 2616-5775 Vol. 8, Issue 7: 105-114, DOI: 10.25236/AJCIS.2025.080713

paper comprehensively considers two key factors: performance volatility and performance degradation frequency, using equation (9) to represent system stability.

$$\begin{cases} STS = STS_{base} \cdot \left(1 - \delta_{degradation}\right) \\ STS_{base} = 0.6 \cdot S_{volatility} + 0.4 \cdot S_{frequency} \end{cases} \tag{9}$$

Where $\delta_{\text{degradation}}$ has been defined by equation (4), and STS_{base} combines volatility and frequency dimensions through weighted combination to obtain the basic stability score. The weight setting reflects the higher importance of volatility relative to frequency, as continuous high volatility has a more severe impact on system stability than occasional performance degradation. $S_{\text{volatility}}$ and $S_{\text{frequency}}$ can be represented by equation (10).

$$\begin{cases} S_{volatility} = max\left(0,1 - 3 \cdot CV_{attack}\right) \\ S_{frequency} = max\left(0,1 - 2 \cdot f_{drop}\right) \end{cases} \tag{10}$$

Where CV_{attack} has been defined by equation (6). When the coefficient of variation exceeds 0.33, the volatility score drops to 0. A smaller coefficient of variation indicates that the system can maintain relatively stable performance levels during attack periods, while a larger coefficient of variation indicates that the system is susceptible to attack impacts and produces severe fluctuations. f_{drop} can be represented by equation (11). When the degradation frequency exceeds 50%, the frequency score drops to 0. This indicator reflects the time proportion of significant performance degradation during attack periods; the higher the frequency, the worse the system stability.

$$f_{drop} = \frac{\left|\left\{j \in I_{attack} : P\left(t_j\right) < 0.8 \cdot P_{baseline}\right\}\right|}{\left|I_{attack}\right|} \tag{11}$$

3.3 Comprehensive Resilience Assessment

Compared to linear weighting, geometric mean has several important advantages: it is more sensitive to extreme values, effectively preventing extremely poor performance in one dimension from being masked by other dimensions; it reflects the interdependent relationships among dimensions, better conforming to the essential characteristics of resilience; it has good mathematical properties, ensuring the stability and comparability of assessment results. Therefore, this paper uses equation (12) to calculate the comprehensive resilience indicator.

$$Resilience = \left(ADC^{w_1} \cdot ADP^{w_2} \cdot STS^{w_3}\right)^{\frac{1}{w_1 + w_2 + w_3}} \tag{12}$$

Where w_1, w_2, w_3 are the weight coefficients of each dimension, reflecting the importance of each dimension in different application scenarios. In specific application scenarios, the importance of each dimension may differ. For example, for critical mission communication systems, anti-degradation capability might be more important because any performance degradation could lead to serious consequences; for general IoT applications, system stability might be the main concern because users care more about service continuity and predictability. To adapt to such differential requirements, this paper introduces a dynamic weight adjustment mechanism:

$$w_i(threat_{level}) = w_{i,base} \cdot \left(1 + \lambda_i \cdot f_i(threat_{level})\right) \tag{13}$$

Where $w_{i,\text{base}}$ is the base weight, λ_i is the adjustment coefficient, and f_i is the threat level response function. Dynamic weight adjustment enables resilience assessment to better adapt to different threat environments and application requirements, improving the flexibility and applicability of the assessment method.

4. Simulation Experiments and Analysis

To verify the effectiveness and practicality of the proposed multi-dimensional resilience assessment method, this chapter designs a series of simulation experiments. The experiments adopt software simulation methods by programming to construct a LEO satellite IoT communication system simulation environment.

ISSN 2616-5775 Vol. 8, Issue 7: 105-114, DOI: 10.25236/AJCIS.2025.080713

4.1 Experimental Setup

The construction of the simulation environment follows the actual architecture and technical characteristics of LEO satellite IoT systems. The system contains 10 IoT terminal nodes communicating with ground control centers through a single LEO satellite. Each node adopts the slotted ALOHA protocol for medium access control, which has advantages of simple implementation and relatively low synchronization requirements in satellite communication environments, suitable for resource-constrained IoT devices. The key parameter settings of the system fully consider the technical constraints and performance characteristics of actual LEO satellite IoT systems.

In terms of communication parameters, the system adopts 1 MHz channel bandwidth with a carrier-to-noise ratio set at 10 dB, reflecting the signal quality of typical LEO satellite links. Data packet length is set to 200 bits with a payload of 100 bits and coding rate of 0.5, balancing transmission efficiency and error correction capability. Propagation delay is set to 10 milliseconds with acknowledgment timeout of 200 milliseconds, reflecting LEO satellite orbital characteristics and communication protocol requirements.

In terms of protocol parameters, each node's data packet generation rate is set to 0.1 packets/second, maximum retransmission count to 10 times, and backoff parameter to 20 time slots. These parameter settings ensure that the system can maintain stable communication performance under normal conditions while having certain fault tolerance capability. Simulation duration is set to 1000 seconds with time step of 0.002 seconds and data recording interval of 1 second, balancing the capture of system dynamic behavior and simulation computational efficiency.

4.2 Threat Scenarios

To comprehensively evaluate the performance of the resilience assessment method under different threat environments, this paper designs multiple typical attack scenarios. Jamming attacks are one of the main threats faced by LEO satellite IoT systems[12]. In simulations, jamming attacks are modeled by reducing the signal-to-interference-plus-noise ratio of channels, where attackers interfere with normal satellite communications by transmitting high-power noise signals. DDoS attacks consume system resources through multiple malicious nodes simultaneously sending false data packets to the system. In simulations, DDoS attacks are modeled by adding additional malicious traffic sources[13]. Replay attacks deceive systems by repeatedly sending previously intercepted legitimate data packets[14]. In simulations, replay attacks are modeled by repeatedly sending historical data packets with certain probabilities. Besides single attack scenarios, experiments also design multiple combined attack scenarios to verify the performance of resilience assessment methods in complex threat environments, simulating coordinated attacks that may occur in actual environments and testing system performance when threatened.

4.3 Resilience Assessment Results Analysis

Based on the experimental setup in section 4.1 and threat scenarios in section 4.2, this paper conducted extensive simulation experiments. The experimental results in Table 1 show that different types of attacks exhibit distinct differential characteristics in their impact on system resilience. Under light attack intensity, all attack types have relatively small impacts on system resilience, indicating that the system has good basic protection capabilities.

Table 1 Comparison of resilience indicators for different attack types and intensities

Attack Type	Attack Intensity	ADC	ADP	STS	Comprehensive Resilience	Maximum Performance Degradation (%)	Average Performance Degradation (%)	Attack Period Availability
No Attack	None	1.0000	1.0000	1.0000	1.0000	0.00%	0.00%	100.00%
Jamming Attack	Light	1.0000	1.0000	1.0000	1.0000	2.44%	0.00%	100.00%
Jamming Attack	Medium	0.7399	0.8753	0.8264	0.8139	16.14%	12.47%	87.53%
Jamming Attack	Heavy	0.5652	0.6559	0.3456	0.5222	28.53%	23.50%	65.59%
DDoS Attack	Light	1.0000	1.0000	1.0000	1.0000	11.78%	0.00%	100.00%
DDoS Attack	Medium	0.8321	0.9530	0.8535	0.8795	10.19%	4.70%	95.30%
DDoS Attack	Heavy	0.4803	0.5510	0.3382	0.4565	36.66%	32.54%	55.10%
Replay Attack	Light	1.0000	1.0000	1.0000	1.0000	21.88%	0.00%	100.00%
Replay Attack	Medium	0.7000	0.8381	0.7988	0.7790	24.23%	16.19%	83.81%
Replay Attack	Heavy	0.6000	0.6906	0.4450	0.5785	26.51%	20.83%	69.06%

However, as attack intensity increases, the impact patterns of various attacks begin to show significant

ISSN 2616-5775 Vol. 8, Issue 7: 105-114, DOI: 10.25236/AJCIS.2025.080713

differences. Among them, jamming attacks are most prominent. Under medium attack intensity, ADC drops to 0.7399, ADP is 0.8753, STS drops to 0.8264, and comprehensive resilience is 0.8139. When attack intensity increases to heavy, ADC further drops to 0.5652, STS suffers severe impact dropping to 0.3456, and comprehensive resilience score falls to 0.5222. This result indicates that jamming attacks mainly affect system performance by reducing channel quality, with particularly obvious impact on system stability, causing severe performance fluctuations during attack periods. The impact pattern of DDoS attacks differs significantly from jamming attacks. Under medium DDoS attacks, the system's ADP reaches as high as 0.9530, with comprehensive resilience of 0.8795. This indicates that compared to jamming attacks, the system has better adjustment capability when facing resource consumption attacks. However, under heavy DDoS attacks, all resilience indicators show significant decline, particularly ADC dropping to 0.4803, reflecting the severe impact of high-intensity resource consumption attacks on core system functions. The impact of replay attacks is relatively mild but persistent. Under medium replay attacks, the system's comprehensive resilience is 0.7790, with relatively balanced indicators across dimensions. Although heavy replay attacks reduce comprehensive resilience to 0.5785, compared to other attack types of equal intensity, their impact is relatively light. This is mainly because replay attacks primarily target communication integrity and validity, with relatively limited impact on system availability.

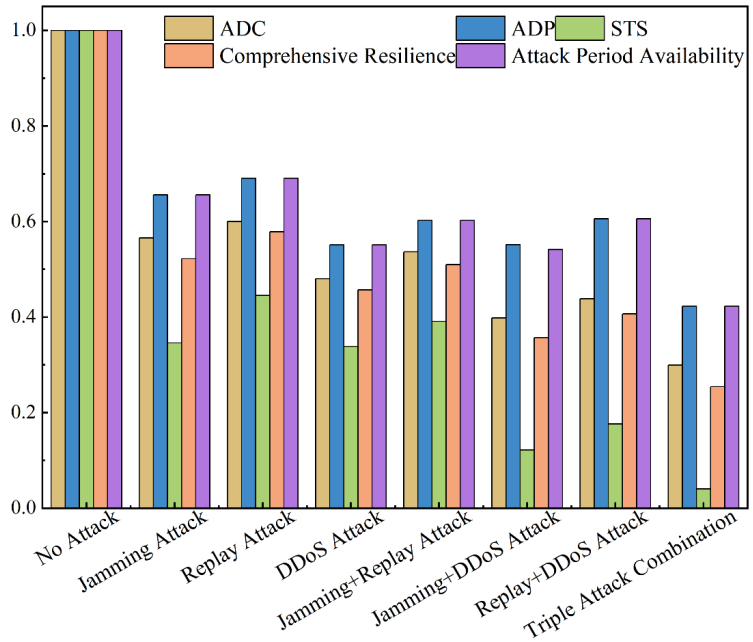

Figure 2 Resilience Comparison between Combined Attacks and Single Attacks

Figure 2 shows the comparison results between combined attacks and single attacks. Experimental results indicate that combined attacks indeed have greater impact on system resilience, but their comprehensive impact is not a simple linear superposition. Among dual attack combinations, the jamming + DDoS attack combination has the most severe effect, with comprehensive resilience dropping to 0.3568, significantly lower than single jamming attack's 0.5222 and single DDoS attack's 0.4565. This combined attack simultaneously impacts the system's physical layer and data link layer, causing system stability to plummet to 0.1213, indicating that multi-layer coordinated attacks can effectively destroy the system's overall protection framework. In contrast, the jamming + replay attack combination has relatively lighter impact with comprehensive resilience of 0.5097, mainly because replay attacks and jamming attacks have certain complementarity in attack mechanisms, allowing the system to partially mitigate attack impacts through retransmission mechanisms. The triple attack combination represents the most severe threat environment, with the system's comprehensive resilience falling to 0.2540, and all resilience dimensions suffering severe impacts. Particularly, system stability drops to 0.0401, indicating that under simultaneous multiple threats, the system almost loses its ability to maintain stable performance.

4.4 Performance Verification of Resilience Assessment Method

To verify the technical feasibility and practicality of the proposed resilience assessment method, this paper conducts in-depth performance verification analysis from two key dimensions: computational

ISSN 2616-5775 Vol. 8, Issue 7: 105-114, DOI: 10.25236/AJCIS.2025.080713

complexity and parameter sensitivity.

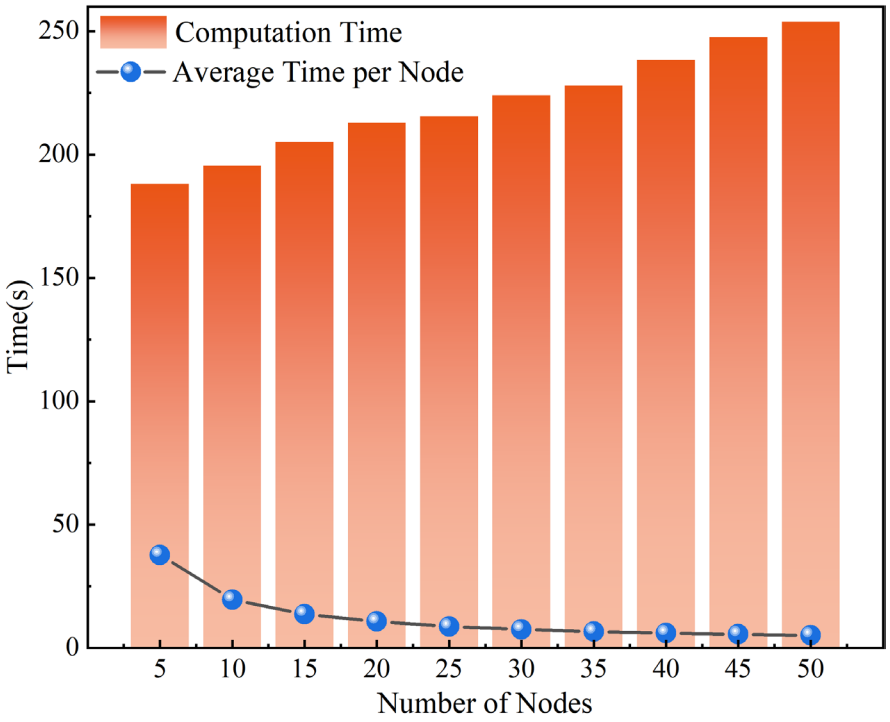

Figure 3 Computational Scalability for Different System Scales (Number of Access Terminals)

Figure 3 shows computational performance under different system scales, verifying the good scalability of the resilience assessment algorithm. Results indicate that as the number of access terminals increases from 5 to 50, total computation time grows from 188.1 milliseconds to 253.7 milliseconds, an increase of approximately 35%. Notably, average computation time per node decreases significantly as system scale expands, dropping from 37.62 milliseconds for 5 nodes to 5.07 milliseconds for 50 nodes, a reduction of 86.5%. This phenomenon indicates that the resilience assessment algorithm has good computational efficiency optimization characteristics, effectively utilizing batch processing advantages when handling large-scale systems and achieving effective allocation of computational resources. The rapid decline trend in average time per node shows that the algorithm's fixed overhead components can be effectively amortized in multi-node processing. From a practical perspective, even in large-scale systems with 50 nodes, total computation time is only 253.7 milliseconds, fully meeting real-time assessment requirements. This performance level enables the resilience assessment method to be deployed in actual LEO satellite IoT systems, providing timely decision support for system operations and security management.

Table 2 Impact of different baseline data point numbers on assessment results

Baseline Points	ADC Value	ADP Value	STS Value	Comprehensive Resilience	Computation Time (s)
30	0.3482	0.5213	0.0477	0.3057	249.164
35	0.3753	0.5681	0.0515	0.3317	251.301
40	0.3622	0.5462	0.0497	0.3194	252.450
45	0.3651	0.5510	0.0501	0.3221	239.005
50	0.3865	0.5857	0.0530	0.3417	246.134
55	0.4097	0.6203	0.0560	0.3620	245.386
60	0.4474	0.6701	0.0923	0.4032	248.121
65	0.4327	0.6514	0.0742	0.3861	246.374
70	0.4808	0.7090	0.1317	0.4405	239.678

The experimental results in Table 2 reveal the impact of baseline data point numbers on resilience assessment results. As baseline points increase from 30 to 70, various resilience indicators show a trend of first rising then stabilizing. The ADC indicator gradually rises from 0.3482 to 0.4808, ADP indicator rises from 0.5213 to 0.7090, and comprehensive resilience improves from 0.3057 to 0.4405. This trend reflects the statistical stability requirements for baseline performance calculation. When baseline data points are few (30-40 points), insufficient statistical samples lead to low reliability in baseline

ISSN 2616-5775 Vol. 8, Issue 7: 105-114, DOI: 10.25236/AJCIS.2025.080713

performance estimation, thereby affecting the accuracy of resilience indicators. As data points increase to 50-60, various indicators gradually stabilize, indicating achievement of statistically reliable levels. When data points exceed 60, the variation amplitude of resilience indicators decreases significantly, indicating that continuing to increase baseline length has limited marginal effects on improving assessment accuracy. Notably, computation time remains relatively stable under different baseline point settings, all fluctuating within the 239-252 millisecond range with a coefficient of variation of only 2.1%. This indicates that baseline point adjustment has minimal impact on algorithm computational efficiency, providing flexibility for parameter optimization in practical applications. Based on sensitivity analysis results, 50-60 data points can be selected as the baseline calculation window in practical applications, which can ensure assessment accuracy while avoiding representativeness problems that overly long baseline windows might bring. For systems with high data collection frequency, baseline points can be appropriately increased to improve statistical stability; for application scenarios requiring high real-time performance, relatively fewer baseline points can be chosen to accelerate response speed.

Comprehensive performance verification results indicate that the proposed multi-dimensional resilience assessment method not only has scientific and comprehensive theoretical foundations but also possesses good feasibility and practicality in technical implementation, providing effective technical tools for security assessment and resilience management of LEO satellite IoT systems.

5. Conclusion and Future Work

This paper addresses the resilience assessment challenges of LEO satellite IoT under complex security threats and proposes a security assessment method based on multi-dimensional resilience indicators. The core of the research lies in decomposing system resilience into three quantifiable, measurable, and mutually orthogonal dimensions, thereby comprehensively characterizing the dynamic response characteristics of LEO satellite IoT systems when facing complex security threats. Through introducing indicators such as performance retention rate, coefficient of variation, and performance degradation frequency to accurately quantify the three dimensions of ADC, ADP, and STS, while employing weighted geometric mean to fuse the three-dimensional indicators for calculating comprehensive resilience. This method can effectively reflect the significant impact of any dimensional performance degradation on overall resilience, avoiding assessment bias that linear weighting might bring, better conforming to the systemic characteristics of resilience. In experimental verification, this paper comprehensively validates the effectiveness and practicality of the resilience assessment method through large-scale simulation experiments. The experiments cover multiple typical attack scenarios, including single attacks, combined attacks, and attacks of different intensities, verifying the applicability and effectiveness of the resilience assessment method in complex threat environments.

The assessment method proposed in this paper not only considers the passive ability of systems to resist attacks but also fully embodies the system's proactive adaptive capability and rapid recovery ability, providing a more scientific and complete theoretical foundation for resilience assessment of LEO satellite IoT systems. However, this method is based on simulation data and needs further verification in real LEO satellite systems. Future work could consider utilizing deep learning technologies to automatically extract system state features, improving the accuracy of threat identification and resilience prediction. Furthermore, the real-time assessment results of this framework can serve as input states for reinforcement learning agents, driving systems to perform actions such as dynamically adjusting protocol parameters, intelligently switching communication frequencies, or reconfiguring network routing, ultimately forming an intelligent resilience closed-loop system that integrates "perception-assessment-decision-response."

References

[1] Zheng J, Luan T H, Li G, et al. Low Earth Orbit Satellite Networks: Architecture, Key Technologies, Measurement, and Open Issues[J]. IEEE Network, 2025.

[2] De Sanctis M, Cianca E, Araniti G, et al. Satellite communications supporting internet of remote things[J]. IEEE Internet of Things Journal, 2015, 3(1): 113-123.

[3] Yang Z, Shaofeng L, Chenyang T. Research on Security Protection of Space-Earth Integrated Network Wireless Link Based on Consortium Blockchain Technology and Application[C]//2023 IEEE 2nd International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA). IEEE, 2023: 1455-1458.

[4] Li K, Zhou H, Tu Z, et al. Distributed network intrusion detection system in satellite-terrestrial

ISSN 2616-5775 Vol. 8, Issue 7: 105-114, DOI: 10.25236/AJCIS.2025.080713

integrated networks using federated learning[J]. IEEE Access, 2020, 8: 214852-214865.
[5] Babu B N, Gunasekaran M. An Analysis of Insider Attack Detection Using Machine Learning Algorithms[C]//2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC). IEEE, 2022: 1-7.
[6] Ansong S, Rankothge W, Sadeghi S, et al. Role of cybersecurity for a secure global communication eco-system: A comprehensive cyber risk assessment for satellite communications[J]. Computers & Security, 2024: 104156.
[7] Zhang Y, Wang Y, Hu Y, et al. Security performance analysis of leo satellite constellation networks under ddos attack[J]. Sensors, 2022, 22(19): 7286.
[8] Tran H T, Balchanos M, Domerçant J C, et al. A framework for the quantitative assessment of performance-based system resilience[J]. Reliability Engineering & System Safety, 2017, 158: 73-84.
[9] Yamagata Y, Maruyama H. Urban resilience[M]. Berlin/Heidelberg, Germany: Springer, 2016.
[10] Tan Z, Wu B, Che A. Resilience modeling for multi-state systems based on Markov processes[J]. Reliability Engineering & System Safety, 2023, 235: 109207.
[11] Erol O, Henry D, Sauser B. 3.1. 2 Exploring resilience measurement methodologies[C]//INCOSE international symposium. 2010, 20(1): 302-322.
[12] Weerackody V. Satellite diversity to mitigate jamming in LEO satellite mega-constellations[C]//2021 IEEE International Conference on Communications Workshops(ICC). IEEE, 2021: 1-6.
[13] Kalambe D, Sharma D, Kadam P, et al. A comprehensive plane-wise review of DDoS attacks in SDN: Leveraging detection and mitigation through machine learning and deep learning[J]. Journal of Network and Computer Applications, 2024: 104081.
[14] Zhu M, Martinez S. On the performance analysis of resilient networked control systems under replay attacks[J]. IEEE Transactions on Automatic Control, 2013, 59(3): 804-808.