Article

Enhancing Two-Step Random Access in LEO Satellite Internet An Attack-Aware Adaptive Backoff Indicator (AA-BI)

Jiajie Dong , Yong Wang * , Qingsong Zhao , Ruiqian Ma , Jiaxiong Yang

Posted Date: 11 September 2025

doi: 10.20944/preprints202509.0945.v1

Keywords: LEO satellite internet; Random Access; Backoff Algorithm; Network Security

Article

Enhancing Two-Step Random Access in LEO Satellite Internet An Attack-Aware Adaptive Backoff Indicator (AA-BI)

Jiajie Dong [1,2], Yong Wang [1,2,*], Qingsong Zhao [1,2], Ruiqian Ma [1,2] and Jiaxiong Yang [1,2]

[1] Anhui Province Key Laboratory of Electronic Restriction, Hefei 230037, China
[2] College of Electronic Engineering, National University of DefenseTechnology, Hefei 230037, China
* Correspondence: wyeei@126.com

Abstract

Low Earth Orbit Satellite Internet (LEO SI), with its capability for seamless global coverage, is a key solution for connecting IoT devices in areas beyond terrestrial network reach, playing a vital role in building a future ubiquitous IoT system. Inspired by the IEEE 802.15.4 Improved Adaptive Backoff Algorithm (I-ABA), this paper proposes an Attack-Aware Adaptive Backoff Indicator (AA-BI) mechanism to enhance the security and robustness of the two-step random access process in LEO SI. The mechanism constructs a composite threat intensity indicator that incorporates collision probability, Denial-of-Service (DoS) attack strength, and replay attack intensity. This quantified threat level is smoothly mapped to a dynamic backoff window to achieve adaptive backoff adjustment. Simulation results demonstrate that, with 200 user equipments (UEs), the AA-BI mechanism significantly improves the access success rate (ASR) and jamming resistance rate (JRR) under various attack scenarios compared to the I-ABA and Binary Exponential Backoff (BEB) algorithms. Notably, under high-attack conditions, AA-BI improves ASR by up to 25.1% and 56.6% over I-ABA and BEB, respectively. Moreover, under high-load conditions with 800 users, AA-BI still maintains superior performance, achieving an ASR of 0.42 and a JRR of 0.68, thereby effectively ensuring the access performance and reliability of satellite Internet in malicious environments.

Keywords: LEO satellite internet; Random Access; Backoff Algorithm; Network Security

1. Introduction

With the proposal of the 6G integrated space-air-ground-sea network vision, Non-Terrestrial Networks (NTN) have emerged as a critical technology for achieving global ubiquitous connectivity. Among these, satellite internet—characterized by its extensive coverage and high flexibility—is progressively becoming key infrastructure for enabling seamless worldwide coverage [1]. Compared to terrestrial cellular networks, LEO satellites offer advantages including wide-area coverage, independence from geographical constraints, and rapid deployment, providing continuous connectivity to regions beyond the reach of ground networks, such as oceans, deserts, and polar areas [2,3]. However, inherent challenges in LEO scenarios, such as long propagation delays and frequent beam handovers caused by high mobility, result in substantially higher retransmission costs—multiple times those of terrestrial systems—when collisions occur in the traditional 4-step Random Access procedure [4]. To alleviate these issues, 3GPP Release 19 has identified "Two-Step Random Access" as a direction for NTN standard evolution [5]. This approach reduces signaling overhead considerably by merging Msg1 and Msg3 into MsgA, and Msg2 and Msg4 into MsgB, and introduces a Backoff procedure for handling access collisions or failures [6].

In the two-step random access procedure adopted by LEO satellite internet, a UE must perform retransmissions based backoff window after an initial MsgA transmission failure, where the value of the backoff window is directly determined by the Backoff Indicator (BI). Thus, the selection of the BI becomes a critical bottleneck in access performance. In LEO-NTN environments, the primary challenge faced by conventional BI mechanisms is the coupling mismatch between the round-trip time (RTT) and the backoff window. The RTT of LEO satellites (15–40 ms) and the granularity of traditional BI values (e.g., 8 ms, 16 ms) are on the same order of magnitude, leading to two extreme scenarios. The first occurs when the BI value assigned by the network is smaller than the current link's RTT: the UE may receive a response message (MsgB) from the gNodeB before its backoff timer expires. In this case, the backoff process is prematurely terminated, resulting in channel resources being idle while the UE awaits the response, thereby reducing resource utilization. The opposite situation arises when the BI value exceeds the RTT: even after successfully receiving MsgB, the UE must wait through an extended backoff period before initiating the next access attempt. This excessive waiting causes significant "resource idling," particularly under favorable channel conditions with low collision probability, where an excessively long backoff window unnecessarily increases access latency and degrades user experience. Although traditional BI mechanisms are straightforward to implement, they struggle to adapt to the dramatic fluctuations in traffic load typical of LEO networks—undersized windows under high load induce persistent collisions, whereas oversized windows under low load lead to resource idling.[7].

Standards such as IEEE 802.11 and LTE adopt the Binary Exponential Backoff (BEB) and its variants, which use an exponentially growing Contention Window (CW) to distribute retransmissions [8]. However, these algorithms exhibit large jitter, slow convergence, and—more critically—fail to adequately account for the coupling effects of high satellite mobility and RTT inherent in LEO environments. As a result, they remain unsuitable for direct application in the random access process of LEO satellite internet. To address these limitations, Khanafer et al. proposed I-ABA in 2024 [9], an adaptive backoff algorithm based on quadratic curve fitting. By mapping collision probability to a continuously varying contention window, I-ABA significantly improved channel utilization from 13.3% (with BEB) to 57.6% in a large-scale Wireless Body Area Network (WBAN) scenario with 340 nodes. Moreover, it provided, for the first time, an analytical model using a three-dimensional Markov chain to characterize throughput, delay, and energy consumption. Nevertheless, I-ABA still does not consider attack scenarios. In an open and resource-constrained environment like LEO-NTN, networks are more vulnerable to jamming attacks [10,11], such as DoS attacks and Replay attacks. DoS attackers can exhaust PRACH resources by flooding the channel with a large number of MsgA transmissions (random access preambles, RAP), thereby preventing legitimate UEs from accessing the network. Replay attackers, on the other hand, disrupt network operation by intercepting and retransmitting legitimate MsgA messages, creating artificial collisions. The design philosophy of traditional BI mechanisms is based on a "collision-backoff" closed loop, where the gNodeB adjusts the BI value according to the number of detected collisions. However, this approach has a fundamental flaw: it cannot distinguish between genuine random collisions and malicious collisions induced by attackers. Both normal high traffic load and malicious attack traffic are interpreted uniformly as channel congestion, triggering more aggressive backoff strategies [11]. This indiscriminate response not only fails to alleviate congestion under attack conditions but exacerbates network paralysis—legitimate UEs are forced into longer backoff periods after being attacked, while adversaries can ignore backoff constraints and continue their assaults unabated.

To address these challenges, this paper proposes an AA-BI mechanism. The core innovation of AA-BI lies in shifting the backoff decision paradigm from a conventional collision-driven to a threat-driven approach, enabling dynamic and adaptive backoff window adjustment tailored for two-step random access in LEO satellite networks. The main contributions are summarized as follows:

1. Threat-Aware Backoff Indicator Design: We propose a composite threat intensity metric (denoted as P_{eff}) that incorporates not only traditional collision probability (P_c), but also quantifies DoS attack intensity (P_{dos}) and replay attack intensity (P_{rep}). This enables accurate real-time network state assessment under malicious conditions.

2. Sigmoid-Based Adaptive Window Mapping: A lightweight Sigmoid mapping function is designed to translate P_{eff} into appropriate backoff window sizes, ensuring low latency under benign conditions and rapid attack suppression under high threats.

3. Low-Complexity Offline Optimization: Critical parameters including the sensitivity coefficient k and the trigger threshold x_0 of the mapping function are optimized via offline grid search, ensuring robust performance across diverse attack scenarios without introducing significant online computation.

2. Materials and Methods

2.1. Random Access Procedure

Current random access protocols in LEO satellite internet systems support two distinct procedures: the 4-step random access and the 2-step random access [12], as illustrated in Figure 1.

In the 4-step random access procedure, Msg1—the initial transmission from the UE to the network—consists of a preamble sent via the PRACH [13]. After transmitting Msg1, the UE monitors for a response, Msg2, from the LEO satellite base station within a preconfigured time window. Msg2 allocates a temporary identifier and grants resources on the Physical Uplink Shared Channel (PUSCH) for the UE to transmit Msg3 [14]. Msg3 serves as the UE's reply to Msg2 and includes a UE identifier for contention resolution. Finally, Msg4 is sent from the gNB to the UE in step 4, using the received UE ID to resolve contention that may arise when multiple UEs select the same preamble in step 1. Thus, the 4-step procedure entails two round-trip exchanges between the gNB and UE, implemented via carefully designed control signaling [14].

In contrast, the 2-step random access procedure combines the preamble and payload into a single initial transmission, MsgA, which is transmitted over the PRACH and PUSCH, respectively. After sending MsgA, the UE waits within a configured window for the response message MsgB. If the UE successfully receives MsgB and correctly decodes the contention resolution information intended for it, the random access is considered successful. If MsgB is not received within the stipulated time or contains incorrect information, the access attempt is deemed unsuccessful. The UE then performs a backoff procedure based on the Backoff Indicator (BI) broadcast by the gNodeB, waiting for a specified interval before reattempting access [15].In scenarios with a large number of UEs, random access failures frequently occur due to repeated preamble collisions during signal transmission, increasing overall latency under congested conditions [16].

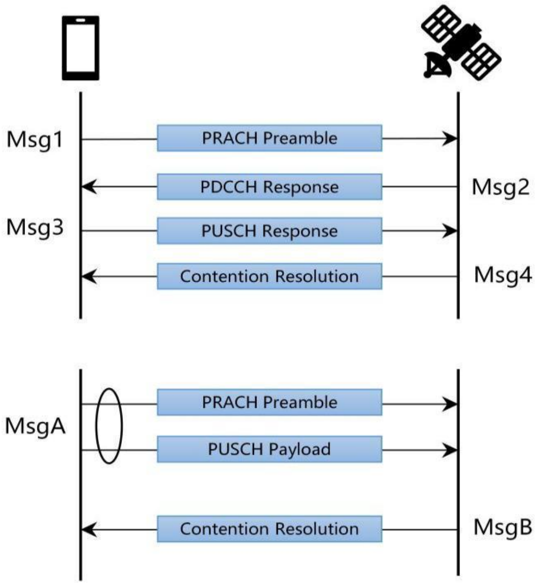


Figure 1. Schematic diagram of random access process.

In the two-step random access procedure of LEO SI, preamble collision is a critical factor leading to network congestion. As shown in Figure 2, when multiple UEs select the same preamble in the same Random Access Opportunity (RO), the time-frequency resources occupied by these preambles overlap, resulting in a collision. This collision makes it impossible for the base station to distinguish between the identities of the UEs, thereby causing access failure. In such cases, the UE performs a backoff procedure according to the Backoff Indicator (BI) assigned by the base station and retries the access process after a randomly selected backoff time. However, when the number of UEs in the network is large, this collision-triggered backoff and retry mechanism leads to frequent preamble collisions, which in turn exacerbates congestion during the random access procedure.

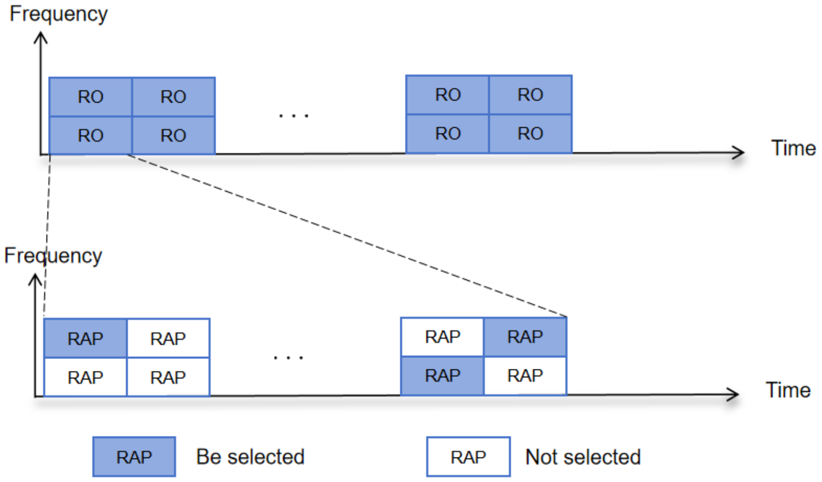


Figure 2. Schematic diagram of preamble selection within a random access opportunity.

2.2. DoS and Replay Attacks

To comprehensively evaluate the robustness of the proposed mechanism in hostile environments, two typical attacks targeting the random access procedure are considered in this work:

1. DoS Attack: Due to the limited computational power and bandwidth resources on satellites, DoS attacks can cause more severe damage—or even complete paralysis—to LEO satellite internet systems [17]. In this attack model, one or more malicious nodes (attackers) continuously transmit a large number of forged random access preambles over the PRACH. These preambles may be completely random or may mimic legitimate UEs. The primary goal is to exhaust the limited resources of the PRACH, causing access requests from legitimate UEs to fail due to either resource unavailability or collisions. In our model, the intensity of the DoS attack is quantified by P_{dos}, defined as the proportion of access requests sent by attackers within the total PRACH load. This attack significantly increases the collision probability on the channel, misleading conventional BI mechanisms into misjudging the network as experiencing high load, thereby inappropriately increasing the backoff window for all UEs.

2. Replay Attack: The replay attack is a more stealthy form of assault. The attacker first intercepts legitimate MsgA transmissions from UEs through eavesdropping or other means. At a later time, the attacker retransmits these intercepted legitimate messages into the PRACH. Since the MsgA itself is valid, this type of attack is more difficult to detect using traditional signature-based detection methods. The objective of the replay attack is to create artificial contention and collisions, disrupt the gNodeB's assessment of channel status, and cause legitimate UEs to fail during the contention resolution phase—thereby also increasing the channel collision rate. In our model, the intensity of the replay attack is quantified by P_{rep}, defined as the ratio of replayed access requests to the total PRACH load.

3. Attack-Aware Adaptive Backoff Indicator (AA-BI)

The core design principle of traditional backoff mechanisms can be summarized as a collision-backoff model. In the BEB algorithm, after each failed access attempt, the UE randomly selects a backoff interval based on the BI, resulting in an exponentially increasing backoff window. Before any transmission attempt, two parameters are initialized: the Contention Window (CW) and the Backoff Exponent (BE). Subsequently, the node's backoff window W is randomly chosen from the interval [W_{min}, W_{max}] [8]:

$$\begin{cases} W = 2\text{^} BE \in \left[W_{min}, W_{max}\right] \\ BE \in \left[BE_{min}, BE_{max}\right] \end{cases} \quad (1)$$

While this mechanism performs acceptably in stable network environments with low collision probability—as it reduces the likelihood of repeated collisions by randomizing retransmission times—it lacks adaptability under dynamic or malicious conditions. The I-ABA advances beyond standard BEB by continuously adjusting the contention window size in response to collisions on the wireless medium. Instead of using deterministic exponential increments, I-ABA employs the collision probability (P_c) as a feedback metric to proactively control the contention window size. The mathematical expression for updating the contention window is given as follows [9]:

$$\begin{cases} W = h\left(P_C\right) Wmax \\ h\left(P_C\right) = \left(5.18 \times P_C{}^2\right) - \left(0.65 \times P_C\right) + 0.05 \end{cases} \quad (2)$$

where h(P_c) is a curve-fitted function that maps the collision probability to a CW scaling factor, proposed in [9].

However, in highly dynamic and vulnerable environments such as LEO-NTN, the limitations of the collision-backoff model become evident. Most notably, it fails to distinguish the root cause of collisions. An access failure may result either from accidental collisions between legitimate UEs or from fabricated conflicts generated by malicious attackers. Treating these two scenarios identically leads to inappropriate responses: under attack conditions, legitimate UEs are misguided into excessive backoff periods, while attackers can exploit this behavior to persistently generate collisions and disrupt network access.

To overcome this fundamental flaw, the proposed AA-BI mechanism introduces a Threat-Backoff model. The core idea is to base backoff decisions not solely on the singular and ambiguous metric of collision, but on a more comprehensive and dynamic threat-aware system. To enable holistic assessment of the network state, an Effective Threat Intensity, denoted as P_{eff} is defined. This metric integrates three core components: the collision probability P_c, the DoS attack intensity P_{dos}, and the replay attack intensity P_{rep}. The mathematical expression is given as follows:

$$P_{eff}\left(t\right) = P_c\left(t\right) + P_{dos}\left(t\right) + P_{rep}\left(t\right) \quad (3)$$

The gNB broadcasts this quantified threat intensity, enabling all UEs to dynamically adjust their backoff window size accordingly. To achieve a smooth and responsive mapping, a Sigmoid function is adopted as the core mapping model. By taking P_{eff} as input, the mapping model operates as follows: when the network threat is low (P_{eff} close to 0), the backoff window remains at a small baseline value to ensure low access latency; as the threat intensity exceeds a certain threshold, the backoff window increases rapidly to effectively mitigate congestion and attacks; under very high threat intensity, the backoff window approaches its maximum value to protect the network to the greatest extent. The mapping function can be expressed as:

$$f\left(P_{eff}\right) = \frac{1}{\left(1 + exp\left(-k * \left(P_{eff} - x_0\right)\right)\right)} \quad (4)$$

where k is the sensitivity coefficient that determines how rapidly the backoff window increases with the threat intensity—a larger k results in a faster expansion of the backoff window for the same increase in threat level. The parameter x_0 represents the activation threshold, indicating the critical point at which the system transitions from a light-load to a heavy-load state. When the comprehensive threat intensity remains below x_0, the backoff window stays close to its minimum value. Once the intensity exceeds x_0, the window increases sigmoidally with the threat level, enabling a smooth transition that ensures low latency under low threat and strong backoff under high threat. The final backoff window is thus given by:

$$W = W_{min} + \left(W_{max} - W_{min}\right) \times P_{eff} \tag{5}$$

This shift from a collision-based to a threat-driven approach equips the backoff mechanism with context-awareness. It enables the system to understand the current network condition and respond more intelligently: under normal high-load scenarios, it moderately increases backoff, while under attack conditions, it rapidly and decisively elevates backoff intensity. This effectively suppresses malicious traffic and safeguards the random access process for legitimate users.

4. Performance Evaluation and Simulation Analysis

4.1. Simulation Environment and Parameter Design

To validate the effectiveness of the proposed AA-BI mechanism, a simulation platform was constructed based on the provided MATLAB code. The platform emulates a LEO-NTN scenario involving multiple UEs and conducts a comparative analysis of the performance of different backoff mechanisms under both DoS and Replay attacks. Key parameters used in the simulations are summarized in Table 1.

Table 1. Simulation Parameters.

Parameter	Description	Value
N	Total number of UEs in the network	200-800
BE	Backoff Exponent	3-11
W_{min}	Minimum backoff window	8
W_{max}	Maximum backoff window	2048
k	Sensitivity coefficient	0-20
x_0	Activation threshold	0-0.05
P_{dos}	DoS attack intensity	0-0.3
P_{rep}	replay attack intensity	0-0.1

4.2. Evaluation Metrics

The Access Success Rate (ASR) is defined as the probability that a UE successfully accesses the satellite internet network upon its first attempt. This metric is crucial for evaluating access efficiency and user experience, requiring the simultaneous fulfillment of two conditions: 1) winning the channel contention, and 2) avoiding any malicious attacks. A high ASR indicates that UEs can access the network quickly and reliably. In the simulation, the ASR is calculated using the following formula:

$$ASR=\left(1-P_c-P_{rep}\right)*\left(1-P_j\right) \tag{6}$$

where the channel collision probability P_c is expressed as:

$$P_c=1-(1-\tau)^{N-1} \tag{7}$$

In this expression, τ represents the transmission probability of a node (determined by the steady-state equation under different network conditions), and N denotes the total number of nodes.

The joint attack probability P_j, which combines the intensity of DoS attacks P_{dos} and Replay attacks P_{rep}, is defined as:

$$P_j=P_{dos}+P_{rep}\times(1-P_{dos}) \tag{8}$$

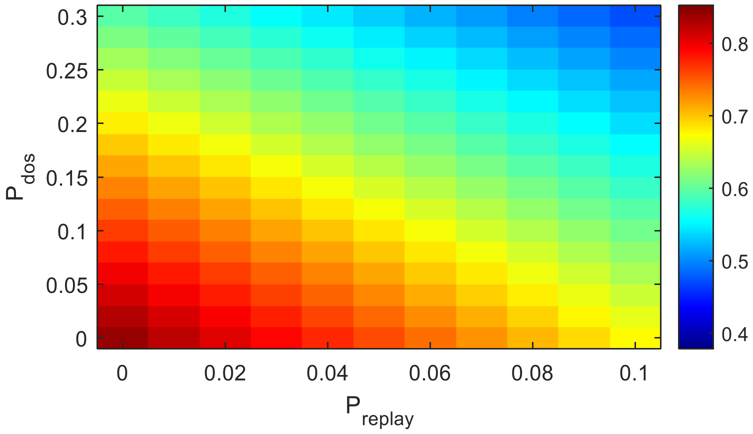
The Jamming Resilience Rate (JRR) is an evaluation metric built upon the ASR that further incorporates network jitter and stability. It employs an exponential decay factor to adapt to high-collision and high-attack scenarios, making it more sensitive to fluctuations in network performance. A high JRR value indicates not only a high access success rate but also a relatively stable network environment. In the simulation, the JRR is calculated as follows:

$$JRR=exp\left(-P_c-P_{dos}\right)*\left(1-P_{rep}\right) \tag{9}$$

4.3. Analysis of Simulation Results

To provide a comprehensive analysis of the performance of the AA-BI algorithm and the I-ABA algorithm under different attack combinations, this section presents heatmaps illustrating the ASR and JRR. These heatmaps reflect the variations in ASR or JRR under different DoS attack probabilities (P_{dos}) and Replay attack probabilities (P_{rep}).

Figures 3 and 4 present heatmaps of the ASR for the AA-BI and I-ABA algorithms, respectively. The color bar represents the value of the performance metric, with a transition from blue to red indicating an increase in the metric value. The color gradient in the heatmaps reveals the vulnerability of the network under varying attack intensities. Specifically, the AA-BI algorithm maintains high ASR values under low to moderate Replay attack probabilities (P_{rep} from 0 to 0.06) and DoS attack probabilities (P_{dos} from 0 to 0.2), with the corresponding regions in the heatmap predominantly appearing red and yellow. In contrast, the heatmap for the I-ABA algorithm is primarily dominated by blue and green hues, indicating lower performance. Under the specific condition of P_{rep} = 0.02 and P_{dos} = 0.05, the ASR of AA-BI reaches approximately 0.8, while that of I-ABA decreases to 0.55. Furthermore, AA-BI demonstrates significantly superior performance compared to I-ABA even under extreme conditions with higher attack probabilities.



doi:10.20944/preprints202509.0945.v1

Figure 3. Heatmap of Access Success Rate (ASR) for AA-BI.

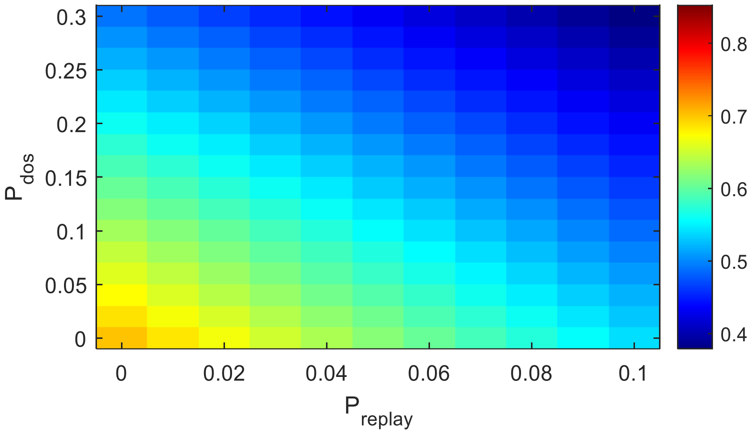


Figure 4. Heatmap of Access Success Rate (ASR) for I-ABA.

Figures 5 and 6 present heatmaps of the JRR for the AA-BI and I-ABA algorithms under varying attack probabilities. In regions with low attack probability (P_{rep} < 0.04 and P_{dos} < 0.15), the JRR values of AA-BI generally exceed 0.7, while those of I-ABA remain around 0.6. Under high attack probability conditions (P_{rep} approaching 0.1 and P_{dos} approaching 0.3), the JRR of AA-BI decreases to approximately 0.45, whereas that of I-ABA drops further to 0.4.These results demonstrate that the AA-BI algorithm achieves a higher JRR across a wide range of attack probabilities, maintaining stronger interference resistance under more challenging conditions. This capability is crucial for enhancing network stability and reliability.

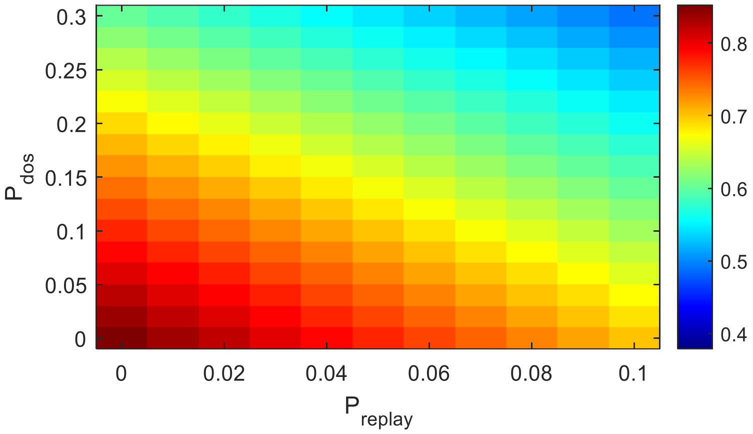


Figure 5. Heatmap of Jamming Resilience Rate (JRR) for AA-BI.

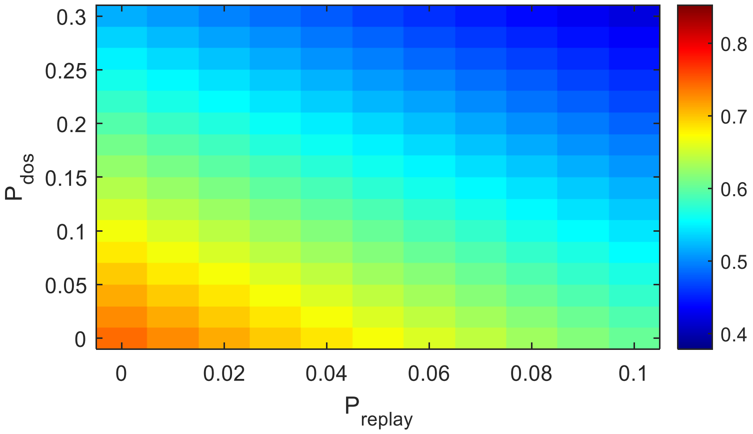


Figure 6. Heatmap of Jamming Resilience Rate (JRR) for I-ABA.

Subsequently, this section compares the performance of four different backoff mechanisms under varying attack intensities. The attack scenario is configured such that the Replay attack intensity is one-third of the DoS attack intensity, with the DoS attack intensity P_{dos} increasing gradually from 0 to 0.3. Figures 7 and 8 illustrate the trends in ASR and JRR, respectively, as functions of P_{dos} for the AA-BI algorithm (including two curves: "opt" representing optimal sensitivity coefficient and activation threshold, and "def" representing default parameters), the I-ABA algorithm, and the BEB algorithm.

Figure 7 demonstrates that the AA-BI(opt) algorithm achieves the highest ASR)across all tested conditions, with its curve consistently remaining above the other three, indicating a significant advantage in random access performance. In contrast, the I-ABA and BEB algorithms exhibit lower ASR values, revealing their vulnerability under attack conditions. At low DoS attack probabilities, such as P_{dos} = 0.05, the ASR of AA-BI(opt) reaches 0.776, while the ASR values of AA-BI(def), I-ABA, and BEB are 0.723, 0.639, and 0.526, respectively. This indicates that AA-BI(opt) achieves ASR values 7.3%, 21.4%, and 47.5% higher than AA-BI(def), I-ABA, and BEB, respectively, under low-attack conditions. As P_{dos} increases to 0.3, the ASR of AA-BI(opt) remains at 0.473, while the ASR of AA-BI(def) and I-ABA decline to 0.465 and 0.378, respectively, and the ASR of BEB further decreases to 0.302. Under this high-attack condition, the ASR of AA-BI(opt) is 1.7%, 25.1%, and 56.6% higher than that of AA-BI(def), I-ABA, and BEB, respectively.

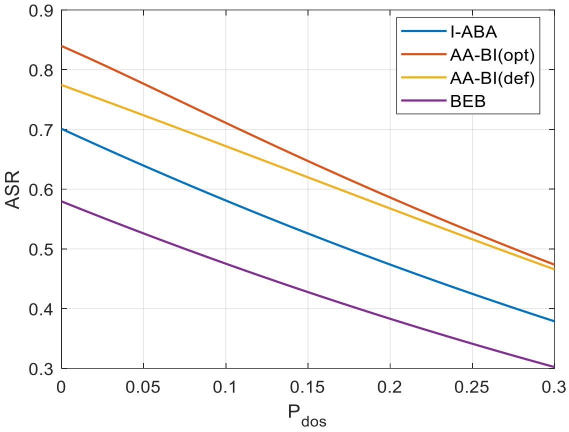


Figure 7. Access Success Rate (ASR) vs. DoS attack intensity.

Figure 8 further confirms the superior performance of the AA-BI(opt) algorithm in terms of JRR. Under low P_{dos} conditions, such as P_{dos} = 0.05, the JRR of AA-BI(opt) reaches 0.852, while the JRR values of AA-BI(def), I-ABA, and BEB are 0.798, 0.742, and 0.657, respectively. This indicates that AA-BI(opt) achieves a JRR that is 6.8%, 14.8%, and 29.7% higher than that of AA-BI(def), I-ABA, and BEB under low-attack conditions. As P_{dos} increases to 0.15, the JRR of AA-BI(opt) remains at 0.662, while the JRR of I-ABA and AA-BI(def) decrease to 0.640 and 0.569, respectively, and the JRR of BEB further declines to 0.504. Under high-attack conditions (P_{dos} = 0.3), the JRR of AA-BI(opt) is approximately 1.2%, 16.3%, and 31.3% higher than that of AA-BI(def), I-ABA, and BEB, respectively.

With the number of random access users fixed at N=200, the AA-BI(opt) algorithm demonstrates significant advantages in both key performance metrics—Access Success Rate and Jamming Resilience Rate—particularly under high-attack scenarios, where the performance improvement is most pronounced. These results underscore the potential and importance of AA-BI(opt) in the design of secure and reliable wireless communication networks.

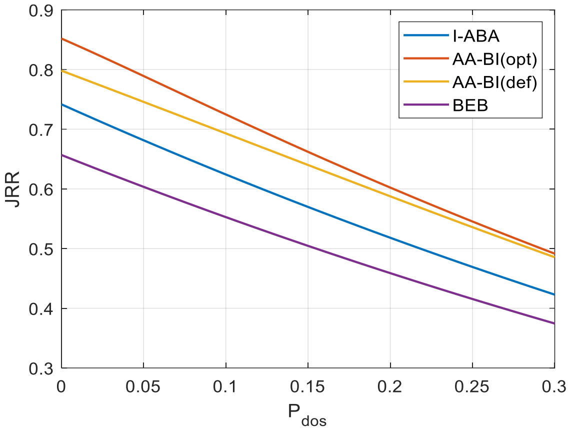


Figure 8. Jamming Resilience Rate (JRR) vs. DoS attack intensity.

Figures 9 and 10 present the variation curves of the ASR and JRR for the four backoff algorithms—I-ABA, AA-BI(opt), AA-BI(def), and BEB—as the number of UE increases from 100 to 800, under fixed attack intensities (P_{dos} = 0.15, P_{rep} = 0.05).

Figure 9 shows that as the number of UEs increases, the ASR of all algorithms exhibits a monotonic decreasing trend, reflecting the combined impact of intensified channel contention and rising collision probability. Notably, AA-BI(opt) consistently maintains the highest ASR. Particularly when the number of UEs reaches 800, its ASR remains at 0.498, outperforming I-ABA (0.486), AA-BI(def) (0.446), and BEB (0.161). This result demonstrates that AA-BI(opt), leveraging its threat-aware dynamic window adjustment mechanism, sustains superior access success rates even under high user load.

In terms of JRR performance, as illustrated in Figure 10, AA-BI(opt) also exhibits outstanding stability, leading across the entire range of UE numbers. When the number of UEs reaches 500, the JRR of AA-BI(opt) is 0.588, approximately 10.1%, 2.4%, and 37.1% higher than that of I-ABA (0.534), AA-BI(def) (0.574), and BEB (0.429), respectively. Moreover, as the number of UEs continues to increase, the decline rate of JRR for I-ABA and AA-BI(def) is significantly steeper than that of AA-BI(opt), further highlighting the latter’s comprehensive advantage in jointly addressing network congestion and malicious attacks.

In summary, the AA-BI(opt) algorithm achieves optimal performance in both ASR and JRR, with its advantages becoming more pronounced as the user scale expands. By integrating multi-source threat indicators and a non-linear mapping strategy, it effectively enhances both access success and system robustness, providing a reliable solution for LEO satellite internet access scenarios characterized by high user load and strong attack intensity.

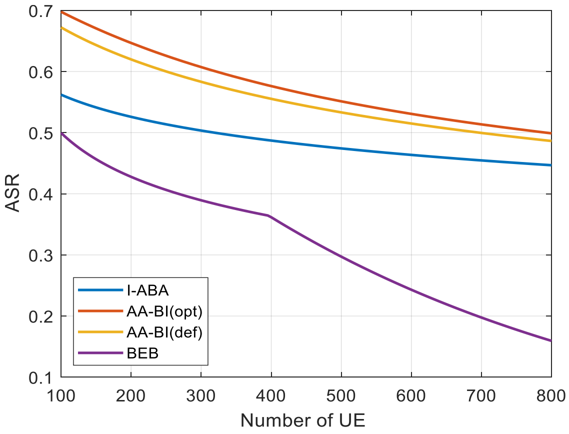


Figure 9. Access Success Rate (ASR) vs. Number of UEs.

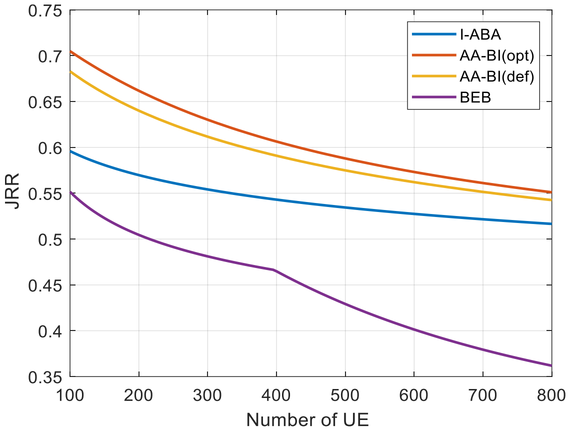


Figure 10. Jamming Resilience Rate (JRR) vs. Number of UEs.

5. Conclusions

This paper addresses key challenges in the random access process of LEO-SI, including mismatched backoff strategies, poor tolerance to malicious attacks, and limited scalability, by proposing an AA-BI mechanism. By constructing a composite threat metric Peff that integrates collision probability (P_c), DoS attack intensity (P_{dos}), and replay attack intensity (P_{rep}), and employing a Sigmoid function to achieve a nonlinear and smooth mapping to the backoff window. In contrast to conventional collision-dependent backoff mechanisms, the proposed AA-BI accomplishes a paradigm shift towards threat-awareness, demonstrating superior performance not only under malicious attacks but also in large-scale network scenarios.

Simulation results demonstrate that in a scenario with 200 UEs, as P_{dos} increases from 0 to 0.3 and P_{rep} increases proportionally at a ratio of 1/3, AA-BI consistently maintains an Access Success Rate (ASR) above 0.47, outperforming I-ABA and BEB by 25.1% and 56.6%, respectively. Furthermore, its Jamming Resilience Rate (JRR) remains above 0.65, significantly exceeding I-ABA and BEB by approximately 16.3% and 31.3%. More importantly, in high-load experiments where the number of UEs increases to 800, AA-BI also exhibits exceptional scalability and stability, with both ASR and JRR comprehensively surpassing those of comparative algorithms, confirming the strong adaptability of the mechanism under varying network scales.

Heatmap analysis further indicates that AA-BI maintains high performance across moderate to high attack intensity ranges. Without requiring complex computations, the mechanism provides an efficient and reliable random access solution for building highly secure and low-latency 6G integrated space-air-ground-sea networks. Future work will focus on online adaptive optimization of key parameters and the design of cross-layer collaborative defense mechanisms.

Author Contributions: Conceptualization, J.D. and Y.W.; methodology, J.D.and J.Y.; software,J.D., Y.W. and Q.Z.; validation, J.D. and Q.Z.; writing—original draft preparation, J.D. and Y.W; writing—review and editing, J.D., Y.W.,R.M. and Q.Z. All authors have read and agreed to the published version of the manuscript.

Funding: The National Natural Science Foundation of China under Grant 62405371

Data Availability Statement: No new dataset was created in this study, and the acquisition methods for all relevant data have been detailed in the paper.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Zhou, Y.; Chen, H.; Dou, Z. MOLM: Alleviating Congestion through Multi-Objective Simulated Annealing-Based Load Balancing Routing in LEO Satellite Networks. Future Internet 2024, 16, 109.

2. Lin, Z.; Niu, H.; An, K.; et al. Refracting RIS-Aided Hybrid Satellite-Terrestrial Relay Networks: Joint Beamforming Design and Optimization. IEEE Trans. Aerosp. Electron. Syst. 2022, 58, 3717–3724.
3. Iglesias-Sanuy, P.; López-Ardao, J.C.; Rodríguez-Pérez, M.; et al. An Efficient Location-Based Forwarding Strategy for Named Data Networking and LEO Satellite Communications. Future Internet 2022, 14, 285.
4. Althumali, H.D.; Othman, M.; Noordin, N.K.; et al. Dynamic Backoff Collision Resolution for Massive M2M Random Access in Cellular IoT Networks. IEEE Access 2020, 8, 201345–201359.
5. Non-Terrestrial Networks (NTN). Available online: https:// www.3gpp.org/technologies/ntn-overview (accessed on 24 August 2025).
6. 3GPP. Solutions for NR to Support Non-Terrestrial Networks (NTN); TR 38.821, Version 19.0.0; 3GPP: Sophia Antipolis, France, 2019.
7. Guidotti, A.; Cioni, S.; et al. Architectures, Standardisation, and Procedures for 5G Satellite Communications: A Survey. Comput. Netw. 2020, 183, 107588.
8. IEEE 802.15.4-2020; IEEE Standard for Low-Rate Wireless Networks; IEEE: Manhattan, NY, USA, 2020.
9. Khanafer, M.; Guennoun, M.; El-Abd, M. Improved Adaptive Backoff Algorithm for Optimal Channel Utilization in Large-Scale IEEE 802.15.4-Based Wireless Body Area Networks. Future Internet 2024, 16, 313.
10. Halloush, R.D. Transmission Early-Stopping Scheme for Anti-Jamming Over Delay-Sensitive IoT Applications. IEEE Internet Things J. 2019, 6, 7891–7906.
11. Yan, P.; Chu, F.; Jia, L.; et al. A Cross-Layer Anti-Jamming Method in Satellite Internet. IET Commun. 2023, 17, 121–133.
12. Liu, J.; Zhao, X.; Wang, Y.; Liu, H.; Zhang, Y.; Wang, X.; Gan, J.; Li, D. A Resource Optimization for Two-Step Random Access in 5G New Radio. J. Phys. Conf. Ser. 2023, 2625, 012063.
13. Krummacker, D.; Veith, B.; Lindenschmitt, D.; Schotten, H.D. Radio Resource Sharing in 6G Private Networks: Trustworthy Spectrum Allocation for Coexistence through DLT as Core Function. In Proceedings of the 1st International Conference on 6G Networking (6GNet 2022), Paris, France, 6–8 July 2022.
14. Mozaffari, M.; Saad, W.; Bennis, M.; Nam, Y.H.; Debbah, M. A Tutorial on UAVs for Wireless Networks: Applications, Challenges, and Open Problems. IEEE Commun. Surv. Tutor. 2019, 21, 2334–2360.
15. Kim, T.; Chae, S.H.; Bang, I. Two-Step Random Access With Message Replication for Low-Earth Orbit Satellite Networks. IEEE Wireless Commun. Lett. 2025, 14, 1.
16. Dawy, Z.; Saad, W.; Ghosh, A.; et al. Toward Massive Machine Type Cellular Communications. IEEE Wireless Commun. 2017, 24, 120–128.
17. Guo, W.; Xu, J.; et al. A Distributed Collaborative Entrance Defense Framework Against DDoS Attacks on Satellite Internet. IEEE Internet Things J. 2022, 9, 15497–15510.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.