UDC 621.396.8

ARTIFICIAL NOISE AIDED PHYSICAL LAYER SECURITY FOR LOW EARTH ORBIT SATELLITE COMMUNICATIONS

CAN WANG

Belarusian State University of Informatics and Radioelectronics, Republic of Belarus

Received March 18, 2026

Abstract. Low Earth Orbit (LEO) satellite communications are vulnerable to eavesdropping due to open wireless links. To address this issue, a simplified artificial noise (AN)-aided physical layer security scheme is proposed. A practical system model including a multi-antenna LEO satellite, a single-antenna ground user, and multiple eavesdroppers is established, considering shadowed-Rician fading and imperfect channel state information (CSI). The AN is projected into the null space of the legitimate user's channel to avoid interference, while suppressing eavesdroppers. A fixed power allocation strategy is adopted for easy implementation. Simulation results show that the proposed scheme outperforms traditional methods in secrecy rate and secrecy outage probability (SOP) with low computational complexity, making it suitable for resource-constrained LEO satellite systems.

Keywords: LEO satellite communication, physical layer security, artificial noise, null space projection, power allocation.

Introduction

LEO satellite networks have gained significant attention for global connectivity, offering low latency and wide coverage [1]. However, their open wireless links expose data transmission to eavesdropping threats. Traditional upper-layer encryption is impractical for LEO satellites due to limited on-board resources [2].

Physical layer security (PLS) leverages wireless channel characteristics to achieve secure communication without complex key management [3]. Artificial noise (AN) is a promising PLS technique: AN is transmitted to interfere with eavesdroppers while not affecting legitimate users [4]. Existing AN schemes for satellites often involve complex optimizations [5][6], which increase implementation difficulty.In particular, [5] employs iterative beamforming design with high computational overhead, while [6] optimizes power allocation under multiple eavesdroppers but requires global CSI. To address these limitations,this paper proposes a simplified artificial noise-aided physical layer security scheme for LEO satellite communications. Characterized by clear and intuitive principles and low implementation complexity, the scheme combines technical innovation with engineering feasibility, and can effectively adapt to the resource-constrained characteristics of LEO satellites.

System Model

1. Network Architecture

The system consists of three components (Fig 1):

LEO satellite: Equipped with 4 transmit antennas, transmits information signals and AN. It leverages multi-antenna beamforming to enhance legitimate reception while confusing eavesdroppers with artificial noise. Ground user (GU): Single antenna, receives secure data. It only processes useful information and suppresses interference through reasonable receiving filtering and signal detection mechanisms.Eavesdroppers (Eve): 2 passive single-antenna nodes intercepting signals.

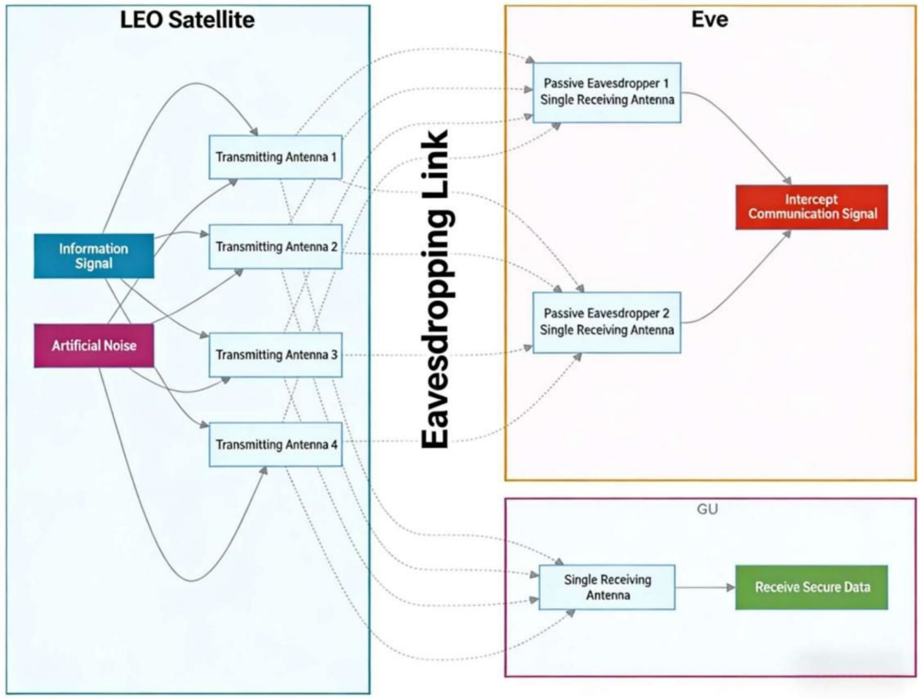

Figure 1.The system consists of three components (Fig 1)

2. Channel and Signal Models

Channels: Legitimate (satellite-GU) and eavesdropper (satellite-Eve) channels follow shadowed-Rician fading [1]. Channel characteristics: Both the legitimate link (satellite–user) and the eavesdropping link (satellite–eavesdropper) follow shadowed-Rician fading. Imperfect channel state information is modeled using estimation errors.

Transmit signal: The information symbol is modulated with QPSK and combined with maximum ratio transmission (MRT) beamforming. Artificial noise is a complex Gaussian random variable, and the noise vector is orthogonal to the channel vector of the legitimate user.

Received signals:

Ground user: Artificial noise is completely canceled due to orthogonality, with only additive white Gaussian noise superimposed.

Eavesdropper: Artificial noise causes interference, with additive white Gaussian noise superimposed.

AN Scheme Design

1. Null Space AN Generation

The artificial noise vector is constructed in the null space of the legitimate user's channel (satisfying orthogonality with the legitimate channel). For a satellite with 4 transmit antennas, the null space is 3-dimensional and is generated by multiplying the null-space matrix of the legitimate channel with a random vector.

2. Power Allocation

The total transmit power constraint of the satellite is satisfied, and fixed power allocation is adopted: power is allocated to the information signal and artificial noise at a fixed ratio.

Performance Evaluation

1. Metrics and Parameters

Secrecy rate: Calculated jointly by the signal-to-noise ratio (SNR) of the legitimate user and the signal-to-interference-plus-noise ratio (SINR) of the eavesdropper.

Secrecy outage probability (SOP): The probability that the secrecy rate falls below 0.5 bps/Hz.

Table 1. **Simulation parameters**

Parameter	Value
LEO altitude	1000km
P_{max}	23dBm
Carrier frequency	2GHz
Noise spectral density	-174dBm/Hz

2. Results

Fig 2 and Fig 3 show the performance compared with two baseline schemes: 1) "Traditional AN" (AN transmitted without null-space projection, as in [6]); 2) "Without AN" (only MRT beamforming, no artificial noise). The proposed scheme achieves the highest secrecy rate (1,2 bps/Hz at SNR=15 dB) and lowest SOP (0,02 at SNR=15 dB), outperforming the comparison schemes.

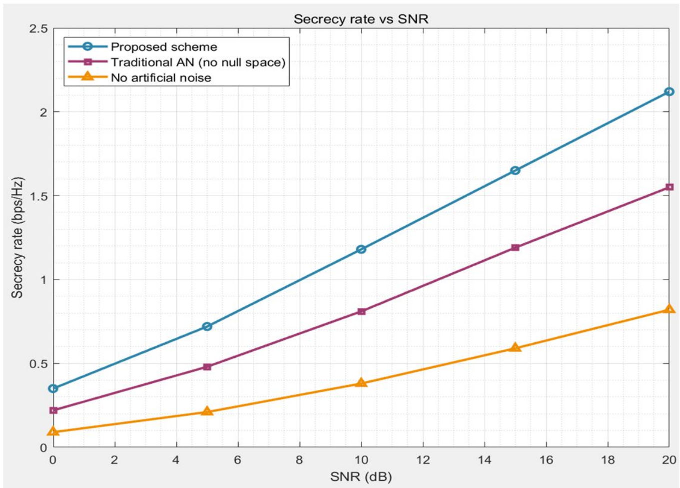

Figure 2. Secrecy rate vs SNR

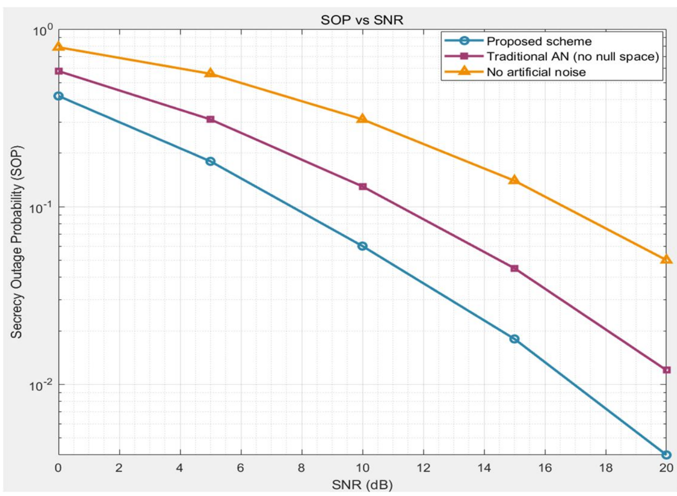

Figure 3. SOP vs SNR

Conclusion

This paper proposes a simplified artificial noise-aided physical layer security scheme suitable for LEO satellite communications. Aiming at the problems of limited resources and vulnerable eavesdropping of open wireless links in LEO satellites, the scheme projects artificial noise into the null space of the legitimate user's channel, which can effectively suppress eavesdroppers while avoiding interference to legitimate communications. Meanwhile, a fixed power allocation strategy is adopted to simplify the implementation process of the scheme, which significantly improves the physical layer security of communication links on the premise of ensuring low computational complexity. Simulation results verify the performance superiority of the proposed scheme over the traditional schemes without artificial noise and with artificial noise without null space projection from two core indicators of secrecy rate and secrecy outage probability. The scheme can be effectively adapted to resource-constrained LEO satellite communication systems and has good engineering application value.

References

1.Niu H. et al. // 2025.
2.Kim S. H., Lee J. W., Lee I. T. // Proc. IEEE Int. Conf. Inf. Commun. Technol. Converg. (ICTC). 2024. P. 112–116.
3.Kumar R., Arnon S. // Electronics. 2024. Vol. 13. No. 22.
4.Talgat A., Wang R., Kishk M. A., Alouini M.-S. // 2024.
5.Zhang P., Gao J. // PLoS One. 2025. Vol. 20. No. 8.
6.Lu W., Liang T., An K., Yang H. // IEEE Access. 2018. Vol. 6. P. 65760–65771.