ARTIFICIAL NOISE AIDED PHYSICAL LAYER SECURITY FOR LEO SATELLITE COMMUNICATIONS

Can Wang

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Jun Ma – Assistant

Abstract. Low Earth Orbit (LEO) satellite communications are vulnerable to eavesdropping over open wireless links. This paper proposes a simplified artificial noise (AN)-aided physical layer security scheme. A system model with a multi-antenna LEO satellite, a single-antenna ground user, and multiple eavesdroppers is built under shadowed-Rician fading and imperfect channel state information. AN is projected into the null space of the legitimate channel to avoid interference, and fixed power allocation is adopted for low complexity. Simulations show the scheme achieves better secrecy rate and secrecy outage probability than traditional methods, 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 provide low-latency global coverage but are vulnerable to eavesdropping. Traditional encryption is impractical due to limited on-board resources [1, 2]. Physical layer security (PLS) using artificial noise can achieve secure transmission without complex key management [3]. However, existing AN schemes are overly complex for LEO platforms [4]. This paper presents a low-complexity AN-aided PLS scheme for LEO satellites.

System Model

The system consists of a 4-antenna LEO satellite, a single-antenna ground user, and two single-antenna eavesdroppers. Channels follow shadowed-Rician fading with imperfect channel state information:

$$\widehat{h_b} = h_b + e \ , \sigma_e{}^2 = 0.01 \tag{1}$$

The transmitted signal is expressed as：

$$\boldsymbol{x} = \boldsymbol{w}s + \boldsymbol{v}n \tag{2}$$

where s is the information symbol, w is the MRT beamforming vector, n is the artificial noise, and v is the AN vector orthogonal to the legitimate channel.

Artificial Noise Scheme Design. Null Space AN Generation:The AN vector v is constructed in the null space of $\widehat{\mathbf{h_b}}$, satisfying $\widehat{\mathbf{h_b^H}}\mathbf{v} = \mathbf{0}$. For 4 transmit antennas, the null space has 3 dimensions:

$$v = U_{null}\, u \tag{3}$$

where U_{null} is the null space matrix of $\widehat{\mathrm{h_b}}$, and u is a random vector.

Power Allocation:Total satellite power constraint: $\| \mathbf{w} \|^2 + \| \mathbf{v} \|^2 \leq \mathbf{P_{max}}$. Fixed power allocation ($\boldsymbol{\alpha} = \mathbf{0.5}$):

$$\| \mathrm{w} \|^2 = 0.5\mathrm{P_{max}}, \| \mathrm{v} \|^2 = 0.5\mathrm{P_{max}} \tag{4}$$

This strategy ensures low computational complexity and easy implementation.

Performance Evaluation

The main metrics are secrecy rate and SOP. Simulation parameters: LEO altitude 1000 km, Pmax=23 dBm, carrier frequency 2 GHz.

Table 1 – Simulation parameters

Parameter	Value
LEO altitude	1000 km
Pmax	23 dBm
Carrier frequency	2 GHZ
Noise spectral density	-174 dBm/Hz

The proposed scheme is compared with “Traditional AN” and “No AN”. Results (Fig. 1) show it achieves higher secrecy rate and lower SOP with lower computational cost.

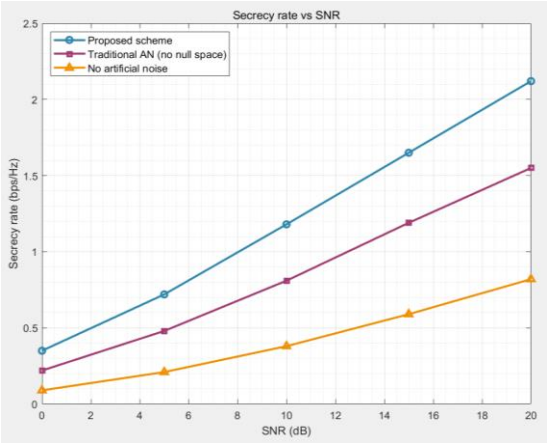

Figure 1 – Secrecy rate vs SNR

The secrecy outage probability (SOP) performance of the three schemes is presented in Figure 2.

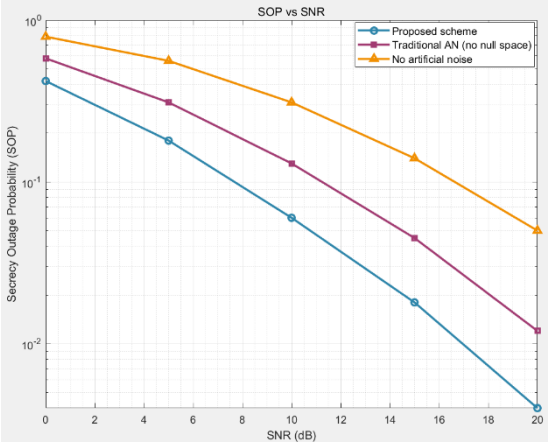

Figure 2 – SOP vs SNR

As shown in the figures, the proposed scheme achieves the highest secrecy rate across all SNR values and the lowest SOP, outperforming both traditional AN and no-AN baselines. The fixed power allocation ensures low computational complexity, making the scheme suitable for resource-constrained LEO satellite systems.

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. doi: 10.3390/electronics13224414.
4.Talgat A., Wang R., Kishk M. A., Alouini M.-S. // 2024.