Secure Transmission with Artificial Noise and Machine Learning in Low Earth Orbit Satellite Networks

Yongjae Lee[†], Emmanuel Kwaning Kwakye[†], Taehoon Kim[‡*], and Inkyu Bang[†*]
[†]Department of Intelligence Media Engineering, Hanbat National University, Daejeon 34158, South Korea
[‡]Department of Computer Engineering, Hanbat National University, Daejeon 34158, South Korea
Email: yjlee@edu.hanbat.ac.kr, ekwakye@edu.hanbat.ac.kr, thkim@hanbat.ac.kr, ikbang@hanbat.ac.kr

***Abstract*—Low Earth orbit (LEO) satellite communications face significant risks of eavesdropping in applications ranging from broadcasting to military operations. This paper investigates the potential of integrating machine learning techniques, specifically support vector machine (SVM)-based scheduling, with physical layer security (PLS) techniques in LEO satellite networks. Our proposed method leverages artificial noise (AN) and SVM to improve secrecy performance. Extensive simulations demonstrate that the proposed scheme closely matches optimal performance while being computationally efficient, significantly outperforming random scheduling.**

***Index Terms*—physical layer security (PLS), artificial noise, machine learning, low Earth orbit (LEO), satellite communication**

I. Introduction

In the 6G era, LEO satellite communications are crucial for global connectivity across various sectors like broadcasting, navigation, and military operations [1]. However, satellite communications are inherently vulnerable to eavesdropping by devices such as unmanned aerial vehicles (UAVs). The physical layer security (PLS) techniques have been studied to mitigate an eavesdropping attack on wireless signals. Further, exploiting machine learning and deep learning to enhance the performance of wireless communication at the physical layer has been highlighted recently [2]. However, its application in PLS remains underexplored. To the best of our knowledge, only a few studies investigated machine learning-based PLS techniques. In [3], He *et al.* only studied a transmit antenna selection scheme to enhance secrecy performance without considering an artificial noise technique.

In this paper, we study a PLS technique by jointly considering artificial noise and machine learning in LEO satellite networks, where LEO satellites consist of a cluster for cooperative communications. We summarize our main contributions as follows:

1) We investigate the potential benefits of machine learning for secure communications in satellite networks and propose a multi-satellite scheduling scheme that exploits the SVM algorithm and the AN technique;
2) We evaluate our proposed scheme through extensive simulations to verify its performance and provide fundamental intuition for exploiting machine learning algorithms on PLS techniques.

*Corresponding authors: Taehoon Kim and Inkyu Bang

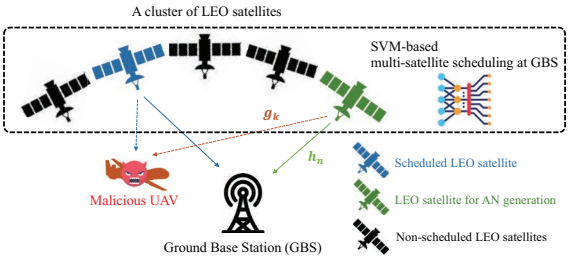

Fig. 1: An example of a system model that consists of one malicious UAV and a cluster of LEO satellites (i.e., $N = 5$) including one LEO satellite for downlink transmission and one additional LEO satellite for AN, scheduled by ground base station exploiting an SVM-based scheduling

II. System Model

Fig. 1 describes an example of our system model. We consider a downlink scenario where a cluster of N LEO satellites, a single ground base station (GBS), and a malicious UAV are considered. We assume every node (including the UAV) in the network is equipped with a single antenna.

We use an index $n \in \{1, \cdots, N\}$ to indicate each LEO satellite. Let $h_n \in \mathbb{C}$ denote the channel coefficient between GBS and LEO satellite n. Similarly, $g_n \in \mathbb{C}$ indicates the channel vector between malicious UAV and LEO satellite n. We assume a Rician fading channel where h_n (or g_n) follows Gaussian random variable with mean μ_h (or μ_g) and variance σ_h^2 (or σ_g^2), respectively. The GBS schedules two LEO satellites in the LEO cluster: one for data transmission and the other for AN generation, respectively. We assume that the channel state information (CSI) of the malicious UAV is not available at the GBS (i.e., the partial CSI case). Thus, the GBS performs multi-satellite scheduling only considering h_n. We consider secrecy outage probability $p_{so}(R_0)$ defined as the probability that secrecy rate R_s is no larger than a certain target secrecy rate R_0, given by

$$p_{so}(R_0) = \Pr[R_s \leq R_0]. \tag{1}$$

III. SVM-based Scheduling with Artificial Noise

In this section, we propose an SVM-based scheduling scheme that exploits AN to enhance the secrecy performance.

We employ an SVM algorithm to select two LEO satellites where one satellite is scheduled to transmit data and the other generates AN. For the training, we only consider CSI on the main link (i.e., the link between GBS and LEO satellites). We consider M training data $\left[\mathbf{H}^1, \mathbf{H}^2, \cdots, \mathbf{H}^M\right]$ where each training data (i.e., $\mathbf{H}^m$ for $m \in \{1, \cdots, M\}$) consists of a set of CSI for all LEO satellites.

Before the training, we preprocess the training data to create a feature vector suitable for machine learning. Each feature vector consists of the absolute values of CSI in $\mathbf{H}^m$ and are normalized as in [3], it is given by

$$t_k^m = \frac{d_k^m - \mathbb{E}[\mathbf{d}^m]}{\max(\mathbf{d}^m) - \min(\mathbf{d}^m)} \tag{2}$$

where t_k^m indicates the k-th element of the normalized feature vector $\mathbf{t}^m$, d_k^m is the k-th element of the vector $\mathbf{d}^m$, which consists of absolute values of CSI in $\mathbf{H}^m$.

The feature vector $\mathbf{t}^m$ is then used in the SVM model training. Each vector is associated with a unique class label corresponding to a specific pairing of two different satellites, (n, a) where the class label is obtained by $l_{n,a} = (n-1)\times(N-1)+a$. For a given $l_{n,a}$, we train an SVM model to consider the data transmission rate $R_d(l_{n,a})$ defined as follows:

$$R_d(l_{n,a}) = \log_2\left(1 + \frac{\|\mathbf{h}_n\|^2}{\|\mathbf{h}_a\|^2 + 1/\rho}\right), \tag{3}$$

where $\|\mathbf{h}_n\|^2$ and $\|\mathbf{h}_a\|^2$ indicate the channel gains of satellite 'n' for data transmission and satellite 'a' for AN generation, respectively, and ρ is the transmit SNR (Signal-to-Noise Ratio).

We train a multi-class SVM classifier considering a radial basis function (RBF) kernel and optimize the classification performance by tuning parameters. Finally, we employ the trained SVM model for multi-satellite scheduling. Using the measured CSI at GBS, GBS predicts the pair of two satellites for data transmission and AN generation. The predicted class $l_{n,a}$ determines the selected satellite pair, and the data transmission rate $R_d(l_{n,a})$ on the main channel is then calculated.

IV. Numerical Results

In this section, we evaluate the performance of the proposed SVM-based scheduling scheme through extensive simulations. For performance comparison in terms of secrecy outage probability, we consider three schemes as follows: (1) 'random AN scheduling' which selects the best one LEO satellite for downlink transmission and randomly selects another satellite for generating AN without considering channel conditions; (2) 'optimal AN scheduling' selects the LEO satellite with the best channel quality for downlink transmission and optimally selects another satellite for generating AN; (3) 'SVM-based scheduling' uses a machine learning model to select the pair of LEO satellites for both downlink transmission and AN generation.

Fig. 2 shows the secrecy outage probability for varying SNR when $N = 8$, $\sigma_h^2 = \mu_h^2 = 0.5$, $\sigma_g^2 = \mu_g^2 = 0.5$, and SNR $= 0$ dB (for malicious UAV). The proposed scheme

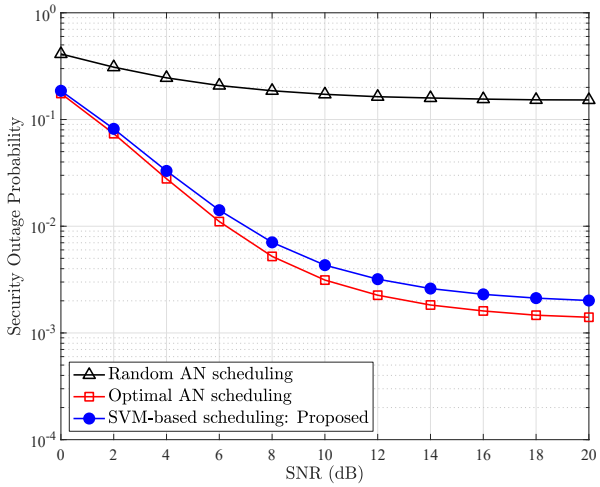

Fig. 2: Secrecy outage probability for varying SNR when $N = 8$, $\sigma_h^2 = \mu_h^2 = 0.5$, $\sigma_g^2 = \mu_g^2 = 0.5$, and SNR $= 0$ dB (for malicious UAV)

closely approximates the performance of the optimal AN scheduling while significantly outperforming the random AN scheduling. This demonstrates that the SVM-based approach effectively learns and utilizes channel conditions, providing a balance between performance and computational efficiency.

V. Conclusion

In this paper, we proposed an SVM-based scheduling scheme incorporating AN to enhance secrecy performance in LEO satellite networks, which can achieve near-optimal secrecy performance. Our findings show the potential of applying machine learning techniques to physical layer security and provide an intuition for designing satellite networks considering secrecy.

Acknowledgment

This research was partially supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2024-RS-2024-00437886) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation), and by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2022R1F1A1076126).

References

[1] X. Zhu and C. Jiang, "Integrated satellite-terrestrial networks toward 6G: Architectures, applications, and challenges," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 437–461, 2021.

[2] K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y.-J. A. Zhang, "The roadmap to 6G: AI empowered wireless networks," *IEEE Communications Magazine*, vol. 57, no. 8, pp. 84–90, 2019.

[3] D. He, C. Liu, T. Q. Quek, and H. Wang, "Transmit antenna selection in MIMO wiretap channels: A machine learning approach," *IEEE Wireless Communications Letters*, vol. 7, no. 4, pp. 634–637, 2018.