UAV-aided Optimal Physical Layer Security in Integrated Satellite and Terrestrial Networks

Tinh T. Bui*, Vishal Sharma†, Antonino Masaracchia‡, Trung Q. Duong*†
*Memorial University, Canada, (e-mail: {ttbui, tduong}@mun.ca)
†Queen's University Belfast, UK, (e-mail: {v.sharma, trung.q.duong}@qub.ac.uk)
‡Queen Mary University of London, UK, (e-mail: a.masaracchia@qmul.ac.uk)

***Abstract*—We investigate the secrecy performance of integrated satellite and terrestrial networks (ISTNs) with the support of a drone (aka UAV). An optimisation problem is formulated to maximise the secrecy rate while guaranteeing the quality of service, including the minimum secrecy rate of the legitimate user, the minimum data rate of normal users, and power consumption. A nested-loop algorithm including outer and inner loops is proposed to convert the initial non-convex problem into multiple convex problems, which are solved by the Dinkelbach algorithm. Simulation results prove the efficiency of our methods in terms of secrecy rate compared to traditional benchmarks.**

I. Introduction

With the increasing demand for global wireless connections, integrated satellite and terrestrial networkss (ISTNs) have become an important component of the sixth generation of networks (6G) [1]. However, due to their ubiquitous and broadcast nature, ISTNs are inherently vulnerable to security threats such as eavesdropping and unauthorised access. Therefore, ensuring security at the physical layer has become a fundamental challenge in ISTN design. To enhance the efficiency and flexibility of ISTNs, drones (aka UAVs) and high altitude platforms have been used as aerial base stations or relays, forming UAV-aided ISTNs [2]. UAVs provide on-demand connectivity with low latency and high-quality connections through line-of-sight (LoS) communications. In [3], [4], the network latency in satellite and cache-assisted UAV networks is reduced considerably by solving minimisation problem compared to traditional satellite networks. Additionally, thanks to their high flexibility, UAVs can be used in emergency scenarios such as disasters, rescues, safety missions, and public events to build or recover networks quickly. In [5], a system model combining a terrestrial network and a UAV network was proposed to provide wireless connections in a disaster area with minimum energy efficiency. Advanced physical layer security (PLS) techniques, including beamforming, artificial noise injection, and secure power allocation, have been extensively studied to improve security performance in ISTNs [6]. Despite these advancements, many existing approaches fail to optimise security and quality of service (QoS) requirements simultaneously. In practical ISTN scenarios, security optimisation must consider minimum secrecy rate constraints, data rate requirements for normal users, and power consumption limitations, making the problem highly complex.

The objective of this paper is to address these challenges by proposing an efficient optimisation framework for PLS in ISTNs. Specifically, we consider an ISTN scenario where an eavesdropper is positioned near a legitimate user, making secure communication more challenging. To mitigate this threat, a UAV acting as a movable radio jammer can confuse eavesdroppers. Then, we formulate an optimisation problem that aims to maximise the secrecy rate while ensuring QoS constraints for all users in the network. Due to the initial non-convex problem, we develop a nested-loop algorithm that transforms the optimisation problem into convex ones. This allows for efficient solving using the Dinkelbach algorithm in inner loops. Through extensive simulations, we demonstrate that our proposed approach outperforms traditional benchmarks in enhancing security and maintaining QoS in ISTNs.

II. System Model

In this paper, we propose a UAV-aided ISTN to enhance security where one satellite serves many ground users, including multiple normal users and one legitimate user, which is wiretapped by one close eavesdropper. The UAV confuses the eavesdropper by focusing a beam to transmit artificial noise, causing high interference received at the eavesdropper. In this setting, the satellite and the UAV are equipped with arrays of N_S antennas and N_U antennas, respectively. The set of normal users which are not wiretapped by the eavesdropper is represented $\mathcal{K}_N = \{1, \ldots, k_N, \ldots, K_N\}$. The legitimate user is denoted by k_W, while m represents the eavesdropper.

The three-dimensional (3D) locations of the satellite, the UAV, and users are denoted by $\boldsymbol{q}_s, \boldsymbol{q}_u,$ and $\boldsymbol{q}_k \in \mathbb{R}^3$. We assume a deterministic LoS channel model between the satellite and each user, which accounts for both free-space path loss and phase shift.

The channel coefficient between the i-th antenna in the satellite and the k-th user is modeled as follows: $h_{i,k} = \lambda_c e^{-j\frac{2\pi}{\lambda_c}d_{i,k}}/(4\pi d_{i,k})$, where $d_{i,k} = \|\boldsymbol{q}_i - \boldsymbol{q}_k\|$ is the Euclidean distance between the i-th satellite antenna and the k-th user. Stacking the coefficients for all N_S antennas, the channel vector from the satellite to the k-th UE can be expressed as $\boldsymbol{h}_{s,k} = \left[h_{1,k}, h_{2,k}, \ldots, h_{N_S,k}\right]$.

The channel gain between the UAV and the k^{th} user is defined as [7]

$$\boldsymbol{h}_{u,k} = \boldsymbol{g}_{u,k}\left(\frac{\lambda_c}{4\pi d_{u,k}}\right)^{\frac{\alpha}{2}} 10^{-\frac{\eta^{\text{LoS}} Pr_{u,k}^{\text{LoS}} + \eta^{\text{NLoS}} Pr_{u,k}^{\text{NLoS}}}{20}}, \tag{1}$$

where $\boldsymbol{g}_{u,k} \in \mathbb{C}^{N_U}$ is the vector of small-scale fading components for the channel from the UAV and user k; α denotes path loss exponent; η^{LoS} and η^{NLoS} represent for the weighted constants of LoS and non LoS links; additionally, $Pr_{u,k}^{\text{LoS}}$ and $Pr_{u,k}^{\text{NLoS}}$ are the probability of LoS and non LoS links, respectively ($Pr_{u,k}^{\text{LoS}} + Pr_{u,k}^{\text{NLoS}} = 1$).

The satellite uses a large number of antennas to generate multiple narrow beams toward legitimate and normal users in the considered area simultaneously. The combined transmit signal at the satellite is formulated as

$$\boldsymbol{x}_s = \sum\nolimits_{k_N \in \mathcal{K}_N} \boldsymbol{w}_{s,k_N} s_{s,k_N} + \boldsymbol{w}_{s,k_W} s_{s,k_W}, \tag{2}$$

where $\boldsymbol{w}_{s,k_N} \triangleq \sqrt{p_{s,k_N}} \boldsymbol{h}_{s,k_N}^{\dagger} / \|\boldsymbol{h}_{s,k_N}\|$ and $\boldsymbol{w}_{s,k_W} \triangleq \sqrt{p_{s,k_W}} \boldsymbol{h}_{s,k_W}^{\dagger} / \|\boldsymbol{h}_{s,k_W}\|$ represent maximum ratio transmission (MRT) beamforming vectors at the satellite toward normal user k_N and legitimate user k_W, respectively; p_{s,k_N} and p_{s,k_W} are the satellite power allocated to serve users; $s_{s,k}$ is the required signal of user k with the assumption of $\|s_{s,k}\|^2 = 1$.

The transmitted artificial noise at the UAV is expressed as

$$\boldsymbol{x}_u = \boldsymbol{G}_{u,k_W} \boldsymbol{v}_u, \tag{3}$$

where $\boldsymbol{v}_u = [v_1, \ldots, v_{N_U}] \in \mathbb{C}^{N_U}$ is the vector of independent and identically distributed noises with $v_i \sim CN(0, 1/N_U)$; and the beamforming matrix at the UAV can be expressed as

$$\boldsymbol{G}_{u,k_W} = \sqrt{\beta_u} \text{Null}\{\boldsymbol{h}_{u,k_W}\} \boldsymbol{h}_{u,m}^{\dagger} / \|\boldsymbol{h}_{u,m}\|, \tag{4}$$

where β_u is the coefficient to allocate the power of the UAV; $\boldsymbol{h}_{u,k_W} \in \mathbb{C}^{N_U}$ is the channel matrix from the UAV to the legitimate user while $\boldsymbol{h}_{u,m}$ is the channel vector from the UAV to eavesdropper m which tries to receive signal s_{s,k_W}. The design of $\boldsymbol{G}_{u,k_W} \in \mathbb{C}^{N_U \times N_U}$ combines null-space of the channel to cancel the additional noise from the UAV to the legitimate user and MRT beamforming to enhance the noise toward the eavesdropper simultaneously.

The signal-to-interference-plus-noise ratio (SINR) of legitimate user k_W can be expressed as

$$\gamma_{k_W} = \frac{|\boldsymbol{h}_{s,k_W} \boldsymbol{w}_{s,k_W}|^2}{\sum_{k'_N \in \mathcal{K}_N} |\boldsymbol{h}_{s,k_W} \boldsymbol{w}_{s,k'_N}|^2 + \sigma_{k_W}^2}. \tag{5}$$

In addition, the SINR of eavesdropper m can be stated as

$$\gamma_m = \frac{|\boldsymbol{h}_{s,m} \boldsymbol{w}_{s,k_W}|^2}{\sum\limits_{k'_N \in \mathcal{K}_N} |\boldsymbol{h}_{s,m} \boldsymbol{w}_{s,k'_N}|^2 + |\boldsymbol{h}_{u,m} \boldsymbol{G}_{u,k_W} \boldsymbol{v}_u|^2 + \sigma_m^2}. \tag{6}$$

The achievable secrecy rate of legitimate user k_W is the amount of reliable information the user received in a unit of time and is defined as

$$SR_{k_W} = B[\log_2(1 + \gamma_{k_W}) - \log_2(1 + \gamma_m)]^+, \tag{7}$$

where B is the total bandwidth.

III. Problem Formulation and Power Allocation

A. Problem Formulation

The target is to maximise the secrecy rate of the legitimate user attacked through controlling the power of the satellite and the UAV under stringent constraints of maximum power and minimum rates, which is shown as

$$\max_{\boldsymbol{P}_s, \beta_u} \quad SR_{k_W} \tag{8a}$$
$$\text{s.t.} \quad \sum\nolimits_{k_N \in \mathcal{K}_N} p_{s,k_N} + p_{s,k_W} \leq P_s, \tag{8b}$$
$$\|\boldsymbol{G}_{u,k_W} \boldsymbol{v}_u\|^2 \leq P_u, \tag{8c}$$
$$SR_{k_W} \geq SR_{min}, \tag{8d}$$
$$R_{k_N} \geq R_{min}, \forall k_N \in \mathcal{K}_N \tag{8e}$$
$$\boldsymbol{P}_s, \beta_u \geq 0, \tag{8f}$$

where P_s and P_u is the maximum powers of the satellite and the UAV; $\boldsymbol{P}_s$ are the combination of p_{s,k_N} and p_{s,k_W}; R_{min} is the minimum data rate required for all users, and SR_{min} is the minimum secrecy rate required. In problem (8), constraints (8b), (8c), and (8f) guarantee the power allocated at the satellite and the UAV in the feasible ranges. Constraints (8d) and (8e) ensure the security and the QoS provided to the legitimate user and normal users.

B. Power Allocation using Approximation Method

Problem (8) is a non-convex problem due to the objective function (8a). First, we introduce a slack variable ζ_{k_W}. The initial problem (8) can be rewritten as

$$\max_{\boldsymbol{P}_s, \beta_u, \zeta_{k_W}} \quad [\log_2(1 + \gamma_{k_W}) - \log_2(1/\zeta_{k_W})]^+ \tag{9a}$$
$$\text{s.t.} \quad \log_2(1 + \gamma_m) \leq \log_2(1/\zeta_{k_W}), \tag{9b}$$
$$\log_2(1 + \gamma_{k_W}) - \log_2(1/\zeta_{k_W}) \geq SR_{min}/B, \tag{9c}$$
$$(8b), (8c), (8e), (8f). \tag{9d}$$

To solve problem (9), we use a nested-loop algorithm which consists of outer loops and inner loops. The outer loops are used for solving problem (9) with variable ζ_{k_W} while the inner loops are to optimise variables $\boldsymbol{P}_s$ and $\boldsymbol{\beta}_u$. By fixing $\boldsymbol{P}_s$ and $\boldsymbol{\beta}_u$, the outer problem can be given as

$$\max_{\zeta_{k_W}} \quad [\log_2(\zeta_{k_W} + \psi_{k_W}(\zeta_{k_W}))]^+ \tag{10a}$$
$$\text{s.t.} \quad 0 \leq \zeta_{k_W} \leq 1, \tag{10b}$$

where $\psi_{k_W}(\zeta_{k_W})$ is defined as a function of ζ_{k_W} in an inner problem. The inner problem can be formulated as

$$\psi_{k_W}(\zeta_{k_W}) \triangleq \max_{\boldsymbol{P}_s, \beta_u} \quad \zeta_{k_W} \gamma_{k_W} \tag{11a}$$
$$\text{s.t.} \quad (9b), (9c), (8b), (8c), (8e), (8f). \tag{11b}$$

To solve outer problem (10), a Bayesian optimisation method, which is suitable for problems with complex objective functions, is used. The functions $\psi_{k_W}(\zeta_{k_W})$ with the user k_W are obtained by solving inner problem (11). To solve the inner problem (11), we use the Dinkelbach algorithm by adding

a new fractional variable λ. The optimisation problem in an iteration where λ is fixed can be expressed as

$$\max_{\boldsymbol{P}_s,\beta_u} \quad \zeta_{k_W}|\boldsymbol{h}_{s,k_W}\boldsymbol{w}_{s,k_W}|^2 - \zeta_{k_W}\lambda\left(\sum\nolimits_{k'_N\in\mathcal{K}_N}|\boldsymbol{h}_{s,k_W}\boldsymbol{w}_{s,k'_N}|^2+\sigma^2_{k_W}\right) \quad (12a)$$

$$\text{s.t.} \quad (9b),(9c),(8b),(8c),(8e),(8f). \quad (12b)$$

The constraint (9b), (9c), and (8e) can be easily transformed as $\gamma_m \leq 1/\zeta_{k_W} - 1$, $\gamma_{k_W} \geq 2^{\log_2(\frac{1}{\zeta_{k_W}})+\frac{SR_{min}}{B}} - 1$, and $\gamma_{k_N} \geq 2^{\frac{R_{min}}{B}} - 1$, respectively. By this way, problem (12) can be converted into a series of linear problems that can be solved efficiently by CVXPY in Python.

IV. Simulation Results

An area of 100×100 km^2 is considered with the location of the satellite at $[50, 50, 780]$ km and the location of the UAV at $[0, 0, 1]$ km. We assume that the altitude of 9 normal users, 1 legitimate user, and 1 eavesdropper equals 0, the eavesdropper and the legitimate user are located on the x-axis with a distance of 8 km. The number of antennas on the satellite, the UAV and users are 128, 64, 1, respectively. The operating carrier frequency is 2 GHz with the bandwidth of 0.5 MHz and the noise power density of -174 dBm/Hz. Additionally, the maximum power of the satellite and the UAV are 20 and 1 watts, while the minimum secrecy rate and normal data rate is required by 0.1 Mbps.

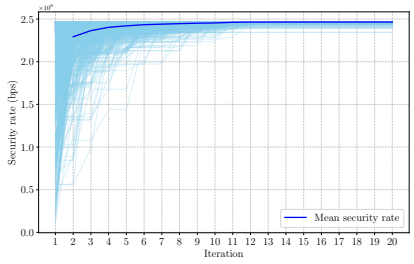

Fig. 1. The average convergence capacity of outer loops in 20 iterations under 1000 Monte Carlo simulations.

In the case of the distance between the legitimate user and the UAV being 10 km (2 km with the eavesdropper), Fig. 1 shows the convergence capacity of outer loops through the mean secrecy rate of 1000 Monte Carlo simulations. The outer algorithm converges after 10 iterations where the secrecy rate reaches the top of 2.47 Mbps. This proves the efficiency of adding the slack variable ζ_{k_W} to the initial problem (8) to create a bound for the data rate of the eavesdropper.

To evaluate the performance of our method, we introduce three conventional benchmarks, including Max-SNR, Random, and No UAV. Max-SNR focuses on maximise the data rate of the legitimate user without considering the eavesdropper, while the power is randomly allocated using Random method. In addition, No UAV is where secrecy rate is maximised without the support from the UAV. In Fig. 2, the distance from the UAV to the legitimate user is in range from 10 to 50 km.

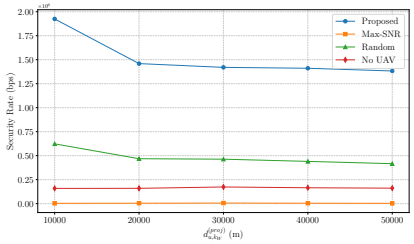

Fig. 2. The secrecy rate of our method and three conventional methods with different distances between the UAV and legitimate user-eavesdropper.

Overall, our method outperforms the other in terms of secrecy rate. In detail, the secrecy rate of our method is 0.966 to 1.3 Mbps higher than the one of Random method, while Max-SNR and No UAV shows inefficiency in security by low secrecy rate. Additionally, with the support of the UAV, the security performance of the network is better than ISTNs without the UAV. Therefore, in case of eavesdropping, UAV-aided ISTNs are suitable to be applied to improve the security capacity.

V. Conclusions

Our proposed nested-loop algorithm has outperformed the other traditional methods by the highest secrecy rate shown in simulation results. Therefore, the proposed method has offered a scalable and computationally efficient solution to protect wireless transmissions from the eavesdropper, ensuring reliable and secure communication in ISTNs.

Acknowledgment

This work was supported in part by the Canada Excellence Research Chair (CERC) Program CERC-2022-00109 and in part by the Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery Grant Program RGPIN-2025-04941.

References

[1] T. Q. Duong, L. D. Nguyen, T. T. Bui, K. D. Pham, and G. K. Karagiannidis, "Machine learning-aided real-time optimized multibeam for 6G integrated satellite-terrestrial networks: Global coverage for mobile services," *IEEE Netw.*, vol. 37, no. 2, pp. 86–93, Mar./Apr. 2023.

[2] C. T. Nguyen *et al.*, "Emerging technologies for 6G non-terrestrial-networks: From academia to industrial applications," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 3852–3885, Jun. 2024.

[3] D.-H. Tran, S. Chatzinotas, and B. Ottersten, "Satellite-and cache-assisted UAV: A joint cache placement, resource allocation, and trajectory optimization for 6G aerial networks," *IEEE Trans. Open J. Veh. Technol.*, vol. 3, pp. 40–54, Jan. 2022.

[4] M.-H. T. Nguyen, T. T. Bui, L. D. Nguyen, E. Garcia-Palacios, H.-J. Zepernick, H. Shin, and T. Q. Duong, "Real-time optimized clustering and caching for 6G satellite-UAV-terrestrial networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 3, pp. 3009–3019, Mar. 2024.

[5] T. Do-Duy, L. D. Nguyen, T. Q. Duong, S. Khosravirad, and H. Claussen, "Joint optimisation of real-time deployment and resource allocation for UAV-aided disaster emergency communications," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 11, pp. 3411–3424, Nov. 2021.

[6] S. Han, J. Li, W. Meng, M. Guizani, and S. Sun, "Challenges of physical layer security in a satellite-terrestrial network," *IEEE Netw.*, vol. 36, no. 3, pp. 98–104, May/Jun. 2022.

[7] R. I. Bor-Yaliniz, A. El-Keyi, and H. Yanikomeroglu, "Efficient 3-D placement of an aerial base station in next generation cellular networks," in *Proc. IEEE ICC*, Kuala Lumpur, Malaysia, May 2016, pp. 1–5.