Secrecy Rate Optimization for ISAC-UAV System via Joint Trajectory and Power Control

Xiao Tong¹, Xin Li¹, Wei Wang¹ and FuWang Dong¹
¹ College of Intelligent Systems Science and Engineering, Harbin Engineering University, Harbin, 150001, China.

Abstract: This letter investigates a secrecy rate maximum optimization problem of unmanned aerial vehicle (UAV) system with integrated sensing and communication (ISAC) function. To ensure the security of the ISAC-UAV system, we formulate a joint UAV trajectory and transmit power optimization problem to maximize the secrecy rate under the constraints of mobility restrictions, power budgets and sensing requirement. The block coordinate descent (BCD) method is employed to divide the original problem into two sub-problems. Then, the non-convex sub-problems are transformed to convex by the appropriate constraints relaxation and fractional programming method. Eventually, the simulation results verify the effectiveness of our proposed algorithm and demonstrate the trade-off performance between the secrecy and sensing.

Keywords: Integrated sensing and communication (ISAC), unmanned aerial vehicle (UAV), secrecy rate, joint trajectory and power optimization.

Classification: Wireless communication technologies

References

[1] Q. Wu et al., “A Comprehensive Overview on 5G-and-Beyond Networks With UAVs: From Communications to Sensing and Intelligence,” IEEE Journal on Selected Areas in Communications, vol. 39, no. 10, pp. 2912-2945, Oct. 2021, doi: 10.1109/JSAC.2021.3088681.
[2] Y. Wu et al., “Throughput Maximization of UAV-Enabled Wireless Network in the Presence of Jammers: Joint Trajectory and Communication Design,” IEICE Transactions on Communications, vol. E102.B no. 10 pp. 1983-1990, 2019, doi: https://doi.org/10.1587/transcom.2018DRP0034.
[3] G. Zhang, Q. Wu, M. Cui and R. Zhang, “Securing UAV Communications via Joint Trajectory and Power Control,” IEEE Transactions on Wireless Communications, vol. 18, no. 2, pp. 1376-1389, Feb. 2019, doi: 10.1109/TWC.2019.2892461.
[4] X. Hong, P. Liu, F. Zhou, S. Guo and Z. Chu, “Resource Allocation for Secure UAV-Assisted SWIPT Systems,” IEEE Access, vol. 7, pp. 24248-24257, 2019, doi: 10.1109/ACCESS.2019.2897226.
[5] J.-M. Kang and C.-J. Chun, “Joint Trajectory Design, Tx Power Allocation, and Rx Power Splitting for UAV-Enabled Multicasting SWIPT Systems,” IEEE Systems Journal, vol. 14, no. 3, pp. 3740-3743, Sept. 2020, doi: 10.1109/JSYST.2020.2966534.
1 Introduction

Recently, unmanned aerial vehicle (UAV) has attracted a great deal of research interests because of the flexible deployment and dominant line-of-sight (LoS) air-ground channel. The UAV can be leveraged as aerial sensing platforms to collect information on the ground as well as provide high-performance wireless communications [1]. Fortunately, the functionality of integrated sensing and communication (ISAC) system can perfectly match the UAV’s task, which motivates the researchers to develop ISAC-UAV system. However, the security of the information is overlooked in the current works on ISAC-UAV, which is important to ensure that the illegal receivers are blocked from the communication information.

In traditional UAV systems, the communication security can be guaranteed by optimizing the power allocation or the UAV’s trajectory [2]. Moreover, the work in [3] proposed to enhance the security by jointly optimizing the trajectory and power allocation of the UAV, whose performance outperforms the trajectory or power optimization method in both UAV-to-ground and ground-to-UAV cases. However, this approach is inapplicable for ISAC-UAV system. When the eavesdropper (Eve) is close to the sensing field interested (FI), there is a performance trade-off between sensing and secrecy rate. Specifically, the better sensing performance is achieved when the UAV fly closer to the FI (Eve), but the more information will be leaked. Therefore, security design problem in the ISAC-UAV is quite different from the traditional joint trajectory and power optimization problem for providing communication service only.

To fill the aforementioned research gap, we consider a ISAC-UAV system simultaneously senses the FI and communicates with the information receiver (IR) on the ground, while guaranteeing the information security under threat of the Eve around the FI. We formulate an average secrecy rate maximum problem with respect to trajectory and power, under the constraints of mobility restrictions, power budgets and sensing requirement. To solve the non-convex problem, we apply block coordinate descent (BCD) method to divide the original problem into two sub-problems. Then, the fractional programming (FP) method and Taylor expansion are employed to transform the sub-problem into convex. Finally, the simulation results verify the effectiveness of our proposed iterative algorithm and demonstrate there is a trade-off between the performance of secrecy and sensing.

2 System model and problem formulation

2.1 Signal model

We consider a ISAC-UAV system where a UAV base station flies at a fixed altitude of $H$ above ground. The UAV transmits information to the IR and senses the FI on the ground, at the presence of a potential Eve. Without
loss of generality, we consider a three-dimensional (3D) Cartesian coordinate system, where the IR, FI and Eve are located at \((x_B, y_B, 0)\), \((x_R, y_R, 0)\) and \((x_E, y_E, 0)\), respectively.

The UAV flies from the initial location \(A(x_0, y_0, H)\) to the final location \(B(x_F, y_F, H)\) within a given finite flight period \(T\) seconds. For convenience, we divide the period \(T\) into \(N\) time slots with equal length, \(T = Nd_t\). Furthermore, we chose a sufficiently small value of \(d_t\), the channels between the UAV and ground notes can be regarded as unchanged within each time slot. As a result, the UAV’s horizontal coordinate in time slot \(n\) can be denoted as \((x_n, y_n)\) (next, we use \([n]\) denotes the time slot \(n\)). The maximum flying distance in each slot is \(D = Vd_t\) with the maximize speed of \(V\). Therefore, the mobility constraints of the UAV should be satisfied as

\[
\|w[1] - w_0\| \leq D, \quad \|w_F - w[N]\| \leq D, \\
\|w[n + 1] - w[n]\| \leq D, n = 1, ..., N - 1,
\]

where \(w_n \triangleq (x[n], y[n]), n = 1, ..., N\) represents horizontal coordinate of the UAV. Furthermore, \(w_0\) and \(w_F\) are the horizontal coordinates of initial and final locations.

The channels between the UAV and ground nodes mainly consist of the LoS channels, where the channel gain follows the free-space path loss model, given by [3]

\[
g_{UG}[n] = \beta_0 d_G^{-1}[n],
\]

where \(d_G\) denotes the square of the distance from the UAV to the ground notes \(G\), which represents the set of IR(\(B\)), Eve(\(E\)) and FI(\(R\)). \(\beta_0\) denotes channel power gain at the reference distance \(d_0 = 1m\).

Let us denote \(p[n]\) as the transmit power, which subjects to the average and peak power limits, i.e.,

\[
\frac{1}{N} \sum_{n=1}^{N} p[n] \leq \bar{P}, \quad 0 \leq p[n] \leq P_{\text{peak}},
\]

where \(P_{\text{peak}}\) and \(\bar{P}\) denote the peak and average power. To make the power budgets non-trivial, we assume \(\bar{P} \leq P_{\text{peak}}\) in this paper.

Therefore, the achievable rate from the UAV to the G can be expressed as

\[
R_{UG}[n] = \log_2(1 + \frac{p[n]g_{UG}[n]}{\sigma^2}) = \log_2(1 + \frac{\gamma_0 p[n]}{d_G[n]})
\]

where \(\sigma^2\) is the additive white Gaussian noise (AWGN) power at the receiver and \(\gamma_0 = \beta_0/\sigma^2\) is the reference signal-to-noise ratio (SNR). Then, we can formulate the average secrecy rate as [3]

\[
SR = \frac{1}{N} \sum_{n=1}^{N} \left[ \log_2(1 + \frac{\gamma_0 p[n]}{d_B[n]}) - \log_2(1 + \frac{\gamma_0 p[n]}{d_E[n]}) \right]^+.
\]

In order to satisfy the sensing performance, the average SNR at the FI has to be greater than a certain threshold, which given by

\[
\frac{1}{N} \sum_{n=1}^{N} \frac{p[n]\gamma_0}{d_R[n]} \geq \eta.
\]
2.2 Problem formulation

In this letter, we aim to maximize the average secrecy rate by jointly optimizing the UAV’s transmit power $p \in \mathbb{R}^N$ and trajectory in terms of its horizontal coordinates $x \in \mathbb{R}^N$ and $y \in \mathbb{R}^N$ over all $N$ time slots. The optimization problem can be formulated as

$$\max_{x,y,p} \sum_{n=1}^{N} \left[ \log_2(1 + \frac{\gamma_0 p[n]}{d_B[n]}) - \log_2(1 + \frac{\gamma_0 p[n]}{d_E[n]}) \right]$$

subject to (1), (3), (6).

In (7), we ignore the operator $[,]^+$ to make the problem smooth without changing the optimal value [3]. However, the problem is still difficult to tackle since that the objective function and constraint (6) are non-convex with respect to either $x$, $y$ or $p$.

3 Proposed algorithm

In this section, we develop an iterative algorithm to obtain a suboptimal solution with good performance. We divide the problem (7) into two sub-problems and transform each sub-problem into solvable convex form. What’s more, we assume the FI and the Eve are in the same position, $d_E[n] = d_R[n]$. On the one hand, this more practical situation can be regarded as that the Eve is close to the FI where our solution will be the lower bound of the system secrecy rate. On the other hand, this assumption can similarly represent the simultaneous wireless information and power transmission (SWIPT) system, where the Eve can be treated as the energy receiver [4].

3.1 Transmit power optimization

For given UAV trajectory $(x,y)$, sub-problem 1 can be expressed as

$$\max_{p} \sum_{n=1}^{N} \left[ \log_2(1 + a_n p[n]) - \log_2(1 + b_n p[n]) \right]$$

subject to (3), (6),

where $a_n = \gamma_0/d_B[n]$, $b_n = \gamma_0/d_E[n]$. In order to deal with the non-convexity caused by the cost function, the Taylor expansion is used. We can transform the cost function into

$$\sum_{n=1}^{N} \frac{1}{\ln 2} \left[ \ln(1 + a_n p[n]) - \ln(1 + b_n p_{\text{feas}}[n]) - \frac{b_n}{1 + b_n p_{\text{feas}}[n]}(p[n] - p_{\text{feas}}[n]) \right]$$

The problem becomes convex and can be solved by the CVX tool after the transform.

3.2 UAV trajectory optimization

For given transmit power $p$, by letting $P_n = \gamma_0 p[n]$ and introducing slack variables $t \in \mathbb{R}^N$, $u \in \mathbb{R}^N$ and $\alpha \in \mathbb{R}^N$ over all $N$ time slots, the problem

© IEICE 2022
can be reformulated as [3], [5]

\[
\max_{x,y,t,u} \sum_{n=1}^{N} \left[ \log_2(1 + \frac{P_n}{u[n]}) - \log_2(1 + \frac{P_n}{t[n]}) \right]
\]

s.t. \( H^2 \leq t[n] \leq d_E[n], \forall n \) \hfill (10a)
\( d_B[n] \leq u[n], \forall n, \text{ and } (1) \) \hfill (10b)
\( \frac{1}{N} \sum_{n=1}^{N} F(x[n], y[n], \alpha[n]) \geq \eta, \) \hfill (10c)

where \( F(x[n], y[n], \alpha[n]) = 2\alpha[n]\sqrt{p[n]} - \alpha^2[n]d_E[n] \) and the \( \alpha \) can be updated by setting \( \partial F/\partial \alpha = 0 \) [5].

With the given feasible initial points \( x_{fea}, y_{fea}, u_{fea} \text{ and } t_{fea} \), we use the Taylor expansion to reformulate the non-convex terms. Then, we have

\[
H^2 \leq t[n] \leq -\left( x_{fea}^2[n] - 2x_{fea}[n]x[n] + 2x_Ex[n] - x_E^2 + y_{fea}^2[n] - 2y_{fea}[n]y[n] + 2y_Ey[n] - y_E^2 - H^2 \right), \forall n,
\]

SR\([n]\) \( \triangleq \log_2(1 + \frac{P_n}{u_{fea}[n]}) - \frac{P_n(u[n] - u_{fea}[n])}{\ln 2(u_{fea}[n]^2 + P_nu_{fea}[n])} \)

\( -\log_2(1 + \frac{P_n}{t_{fea}[n]}) + \frac{P_n(t[n] - t_{fea}[n])}{\ln 2(t_{fea}[n]^2 + P_nt_{fea}[n])} \).

Finally, the problem (10) is transformed into

\[
\max_{x,y,t,u} \sum_{n=1}^{N} SR[n]
\]

s.t. \( (10b), (10c), (11) \).

Problem (13) is a convex and can be solves though CVX tool. Since the problem is non-decreasing over iterations and the optimal value is upper-bounded by a finite value, the convergence is guaranteed.

4 Simulation results

In this section, we conduct simulations to verify the effectiveness of the proposed optimization algorithm, which is labelled as Proposed. Unless otherwise stated, we adopt all parameters in Fig. 1. Besides, for initial feasible UAV trajectory, we use the best-effort approach, which can be labelled as Baseline 1. Baseline 2 represents joint trajectory and power optimization algorithm without sensing requirement in [3].

Fig. 2 shows the trajectories of the UAV by applying different algorithms with different flight period. We use circle and square represent the IR and Eve, respectively. When \( T > 50s \), compared with the Baseline 1, the Baseline 2 shows that the UAV flies as close as possible to the IR and as farther as possible from Eve to achieve the best secrecy rate. What’s more, it can be seen in the Fig. 2 that the increase of the sensing SNR threshold makes the UAV fly closer to the FI(Eve). It means that we have to sacrifice some secrecy performance to satisfy the sensing requirement.

© IEICE 2022
Fig. 1. Simulation parameters

| Parameter | $w_0$ | $w_f$ | $w_B$ |
|-----------|-------|-------|-------|
| Value     | (50,50) | (50,50) | (0,0) |

Fig. 2. Trajectories of UAV

Fig. 3. SNR of FI versus time

Fig. 4. Average SR versus $\eta$.

Fig. 3 shows the SNR of FI versus time in different algorithms. Compared with the Baseline 1, Baseline 2 shows that the secrecy rate is increased and the SNR of FI is decreased. This is because the objective of [3] is maximizing the secrecy rate. However, in order to meet the sensing requirement in our study, we have to sacrifice the secrecy performance as the Proposed shows. Moreover, more power should be transmitted when the UAV is close to the FI for better sensing performance. Therefore, the SNR at the both ends is greater than the other time slots.

Fig. 4 shows the average secrecy rate versus sensing SNR with different transmit power and fight period. Consistent with the above analysis, the increase of sensing SNR threshold decreases the secrecy rate. However, we can increase the transmit power or fight period to increase the secrecy rate.

5 Conclusion

In this letter, we have studied the secrecy rate maximization problem of ISAC-UAV system. Specifically, we maximize the average secrecy rate by jointly optimizing the UAV trajectory and transmit power under the mobility constraints, power budgets and sensing requirement. In order to solve the original problem, we divide it into two sub-problems, which are transformed into convex by using Taylor expansion and fractional programming. Simulation results verify the effectiveness of our proposed algorithm and demonstrate there is a compromise between the secrecy and sensing performance.