Integrated Sensing and Communication (ISAC) in Secured Wireless Powered IoT Networks

Abid Afridi[1], Iqra Hameed[2], Insoo Koo[1]
[1] Department of Electrical/Electronic and Computer Engineering, University of Ulsan, South Korea
[2] Department of Electronic Engineering, Hanyang University, South Korea
(aafridi157@gmail.com, iqrahameed@hanyang.ac.kr, iskoo@ulsan.ac.kr)

Abstract

In this paper, we investigate physical layer security within an integrated sensing and communication (ISAC) framework in a wireless powered IoT network (WPIN). Our study focuses on optimizing transmit beamforming and time allocation in an ISAC system to minimize transmit power while ensuring a secrecy throughput threshold in the presence of an eavesdropper. We used convex optimization techniques and bisection search in an iterative manner to jointly optimize the beamforming vector and downlink/uplink time. Simulation results validate the effectiveness of our approach, demonstrating a significant improvement in the minimization of the transmit power.

I. Introduction

Wireless powered IoT networks (WPINs) have emerged as a promising solutions for energy-limited devices. Radio frequency (RF) enabled energy harvesting has played a significant role in battery-powered wireless devices in communication networks [1]. In the context of 6G networks, secure communications are crucial due to increasingly complex environments that threaten the privacy and security of user data. Since perfect channel state information (CSI) is hard to obtain, especially with unknown eavesdropper locations and no cooperation with legitimate users, imperfect CSI can degrade beamforming and system performance [2]. Integrated sensing and communications (ISAC) is a new technology that enhances spectral and energy efficiency in next-generation wireless systems. Beamforming design has been extensively studied in full-duplex ISAC systems, where the base station (BS) detects targets and communicates with multiple downlink and uplink users simultaneously [3]. In ISAC, the transmitted signal contains both sensing and communication information, and radar-like sensing allows detection of potential eavesdroppers to enhance physical layer security [4].

II. System Model and Problem Formulation

We consider an ISAC system as depicted in Fig. 1, where a dual-functional FD base station (BS) is equipped with multiple transmit/receive antennas N. The system also includes a single-antenna target, which acts as a potential eavesdropper, and one legitimate user U with a single antenna. We assume the coherence time interval as T=1. The network employs a harvest-then-transmit mechanism, where the initial slots are designated for sensing. At first, the ISAC-BS senses the target to estimate the channel in the preserved slots τ_s and subsequently sends an energy signal in the downlink to charge the user in time τ. After harvesting the required energy, the user transmits information in the uplink using the time $(1-\tau-\tau_s)$ allocated for uplink wireless information transfer (WIT).

Radar Sensing Model:

ISAC-BS transmits a radar signal $\boldsymbol{x_0} \in \mathbb{C}^{N\times 1}$ with zero mean and variance $R_X = \mathrm{E}(\boldsymbol{x_0}\,\boldsymbol{x_0^H}) \succeq 0$, where $\boldsymbol{x_0} = \sum_{i=1}^{N} \boldsymbol{v_i^r}\boldsymbol{x_i^r}$. In addition, $\boldsymbol{x_i^r}$ shows random (0,1) radar signal while $\boldsymbol{v_i^r}$ denotes the beamformers for radar. In the considered scenario, the echo signal is reflected by the target which is received at ISAC-BS and can be expressed as:

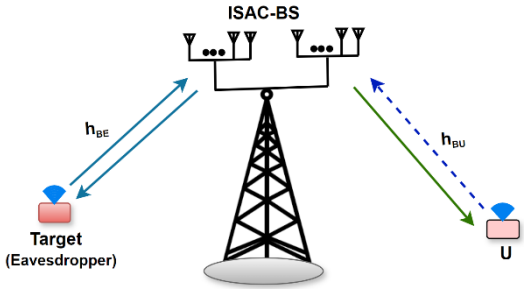

Fig. 1 : System Model

$$\gamma = \alpha\, a_T(\theta) a_R^T(\theta)\boldsymbol{x_0} + \boldsymbol{z} \qquad (1)$$

where α is a complex valued reflection coefficient, θ denotes the angle-of-departure (AoD) of a radar wave. $a_T(\theta)$ shows a transmitter steering vector which is written as $a_T(\theta) = \left[1 + e^{j\frac{2\pi}{\lambda}dsin(\theta)}, \dots, e^{j\frac{2\pi}{\lambda}d(N-1)sin(\theta)}\right]$. When the echo signal is received at the same BS then $a_T(\theta) = a_R(\theta)$, hence we can estimate the θ using MUSIC algorithm.

Communication Model:

During the downlink phase, the ISAC-BS sends an energy signal to the user U in the assigned time τ. Hence, the amount of energy harvested by the user U on downlink can be expressed with E_U as follows:

$$E_U = \xi_U \tau ||\boldsymbol{w}_e^H\, \mathbf{h}_{BU}||^2 \qquad (2)$$

where $0 < \xi_U < 1$, is the energy harvesting efficiency at user U and $\boldsymbol{w_e}$ shows the energy beamformer in downlink. During the uplink phase, we assume (N-1) antennae for communication while the N^{th} antenna for sending the jamming signal towards the eavesdropper. The achievable uplink throughput for user U in the assigned time can be defined as:

$$R_U = (1-\tau) log_2\left(1 + \frac{\boldsymbol{p}_U |(\boldsymbol{h}_{BU}^H \boldsymbol{r})|^2}{||\boldsymbol{r}||^2 \boldsymbol{\sigma}^2}\right) \qquad (3)$$

where $\mathbf{r} \in \mathrm{C}^{N\times 1}$ denotes the received beamforming vector for decoding the information signal at the BS and $\boldsymbol{p}_U$ shows the uplink transmit power.

Now, the achievable rate for the Eavesdropper can be expressed as:

$$R_E = (1- \tau-\tau_s) log_2 \left(1+ \frac{p_U |h_{EU}^H|^2}{p_j |h_{BE}^H|^2+\sigma^2}\right) \quad (4)$$

By knowing the channel of Eavesdropper $\boldsymbol{h}_{BE}$, BS also send the jamming signals towards the target (potential Eavesdropper). In this paper, we aim to minimize the transmit power of ISAC-BS while maintaining the secrecy throughput threshold in the presence of an Eavesdropper by jointly optimizing the transmit beamforming $\boldsymbol{w}$ and downlink/uplink time $\boldsymbol{\tau}$.

$$\min_{(\boldsymbol{W},\boldsymbol{p_j},\boldsymbol{\tau})} \quad ||\boldsymbol{W}||^2 \quad (5a)$$

subject to:

$$C_1 : R_U - R_E \geq R_{Thr} \quad (5b)$$

$$C_2 : \boldsymbol{p_j} + ||\boldsymbol{W}||^2 \leq P_{max} \quad (5c)$$

$$C_3 : 0 \leq \boldsymbol{\tau}_s + \boldsymbol{\tau} \leq 1 \quad (5d)$$

where the constraint C_1 and C_3 satisfy the secrecy throughput and maximum power constraint at ISAC-BS, respectively. C_3 satisfies the normalization of allocation time on the frame length. First we fix $\boldsymbol{\tau}$ and rewrite the problem into P1.

$$\textbf{P1:} \quad \min_{(\boldsymbol{W},\boldsymbol{p_j})} \quad ||\boldsymbol{W}||^2 \quad (6a)$$

$$0 \geq 2^{\frac{R_{Thr}}{1-\tau}} (1+ y)-1-x \quad (6b)$$

$$0 \geq \frac{\boldsymbol{A}\, ||w^H \mathbf{h}_{BU}||^2}{\boldsymbol{x}} \quad (6c)$$

$$0 \geq \frac{\boldsymbol{B}\, ||w^H \mathbf{h}_{BU}||^2}{\boldsymbol{y}} - \boldsymbol{p_j} |\boldsymbol{h}_{BE}^H|^2 - \boldsymbol{\sigma}^2 \quad (6d)$$

$$0 \geq \boldsymbol{p_j} + ||\boldsymbol{W}||^2 - P_{max} \quad (6e)$$

Now the problem **P1** is convex, so using iterative method we can solve it using CVX tool. Subsequent to this, we use bisection search method to find optimal $\boldsymbol{\tau}$.

III. Results and Discussion

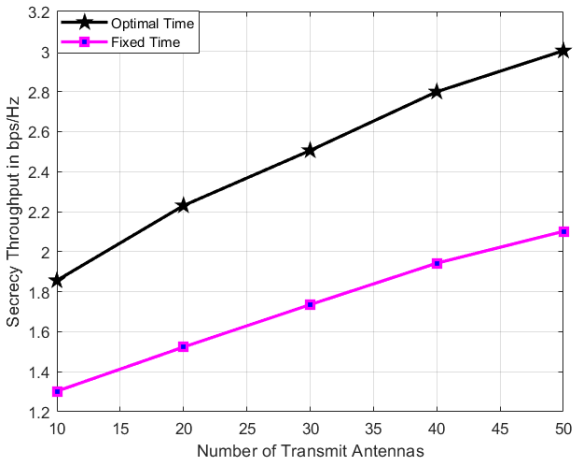

Fig. 2 : Secrecy Throughput vs. Number of Antennas

Fig. 2 illustrates the secrecy throughput of the user U with respect to different values of transmit antennas (N), while considering the fixed and optimal time. Moreover, Fig. 3 describes the transmit power at BS with respect to different values of N. The transmit power graph shows continuous decrease as the number of transmit antennas increases at BS for different scenarios.

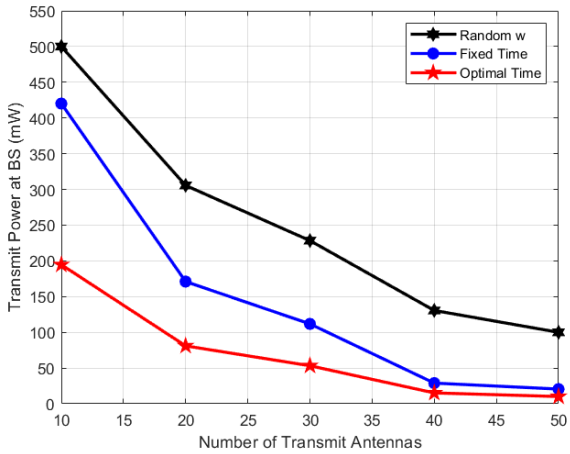

Fig. 3 : Transmit Power vs. Number of Antennas

IV. Conclusion

This paper introduces an approach to optimize the beamforming vector and downlink/uplink time in ISAC system for secured WPIN with the objective minimize the transmit power of ISAC-BS while maintaining the secrecy throughput threshold. We employed convex optimization techniques and the bisection search method iteratively to jointly optimize the beamforming vector and downlink/uplink time allocation. Throughout this process, we ensure that the downlink power budget of the Base Station (BS) and Quality of Service (QoS) requirements user are safeguarded. The simulation results validate the effectiveness and significance of our proposed approach to minimize the transmit power at base station.

ACKNOWLEDGMENT

This work was supported by Regional Innovation Strategy (RIS) through the National Research Foundation of Korea (NRF) funded by the Ministry of Education(MOE) 2021RIS-003.

REFERENCES

[[1] Y. Ko, S.-H. Kim, and J.-S. No, "Uplink Time Scheduling With Power Level Modulation Scheme in Wireless Powered Communication Networks," *IEEE Access*, vol. 7, pp. 11187–11194, 2019, doi: 10.1109/ACCESS.2018.2890721.

[[2] Q. Wang, F. Zhou, R. Q. Hu, and Y. Qian, "Energy Efficient Robust Beamforming and Cooperative Jamming Design for IRS-Assisted MISO Networks," *IEEE Trans Wirel Commun*, vol. 20, no. 4, pp. 2592–2607, Apr. 2021, doi: 10.1109/TWC.2020.3043325.

[[3] Z. He, W. Xu, H. Shen, D. W. K. Ng, Y. C. Eldar, and X. You, "Full-Duplex Communication for ISAC: Joint Beamforming and Power Optimization," *IEEE Journal on Selected Areas in Communications*, vol. 41, no. 9, pp. 2920–2936, Sep. 2023, doi: 10.1109/JSAC.2023.3287540.

[[4] N. Su, F. Liu, and C. Masouros, "Sensing-Assisted Eavesdropper Estimation: An ISAC Breakthrough in Physical Layer Security," *IEEE Trans Wirel Commun*, vol. 23, no. 4, pp. 3162–3174, Apr. 2024, doi: 10.1109/TWC.2023.3306029.