

User Localization with HRIS and Backscatter Modulation for Next-Generation Networks

Mattia Piana and Stefano Tomasin

Dept. of Information Engineering, University of Padova, Italy
mattia.piana@studenti.unipd.it and stefano.tomasin@unipd.it

Abstract—Hybrid reflective intelligent surfaces (HRISs) can support localization in sixth-generation (6G) networks thanks to their ability to generate narrow beams and at the same time receive and process locally the impinging signals. In this paper, we propose a novel protocol for user localization in a network with an HRIS. The protocol includes two steps. In the first step, the HRIS operates in full absorption mode and the user equipment (UE) transmits a signal that is locally processed at the HRIS to estimate the angle of arrival (AoA). In the second step, the base station transmits a downlink reference signal to the UE, and the HRIS superimposes a message by a backscatter modulation. The message contains information on the previously estimated AoA. Lastly, the UE, knowing the position of the HRIS, estimates the time of flight (ToF) from the signal of the second step and demodulates the information on the AoA to obtain an estimate of its location. Numerical results confirm the effectiveness of the proposed solution, also in comparison with the Cramér Rao lower bound on the estimated quantities.

I. INTRODUCTION

Accurate user equipment (UE) localization is a key target for next-generation cellular networks [1] to provide new services to the UE. This target can be facilitated by new technologies that will be deployed in sixth-generation (6G) networks. In particular, reconfigurable intelligent surfaces (RISs) are seen as a transformative technology that can control the physical propagation environment in which they are embedded by passively reflecting radio waves in preferred directions [2]. UE localization and sensing are also among the applications that can benefit from RIS deployments. In particular, integrated sensing and communications (ISAC) systems can benefit from RISs as shaping the wireless environment can increase the target's illumination and facilitate its detection by the UEs in radar applications [3].

In this paper, we focus on the localization of the UE at the UE itself. Localization at the UE in RIS-aided scenarios was studied for base stations (BSs) and UEs with single antennas in [4], for BSs with multiple antennas and UEs with single antennas in [5], and for both BS and UE with multiple antennas in [6]. The localization of UE by the BS in a no line of sight (nLOS) scenario is particularly challenging due to the interaction of the RIS with the channel and the limited observation (channel matrix size) of the cascade channel through the RIS [7].

This work was partially supported by the European Union under the Italian National Recovery and Resilience Plan (NRRP) of NextGenerationEU, partnership on "Telecommunications of the Future" (PE00000001 - program "RESTART").

While RISs are equipped with a large number of elements and can create narrow electromagnetic beams, the channel seen by the RISs (and the entailed information on UE location) remains largely unknown to both the BS and the UE, as they are equipped with much fewer antennas. To overcome this issue, a new technological solution is provided by hybrid RISs (HRISs) that, beyond reflecting, also capture part of the impinging signal for local processing [8]. Early works have started exploring the use of HRISs for localization. In [9] the UE and HRIS positions are jointly estimated by the UE while in [10] both BS-HRIS and HRIS-UE channels are estimated by the BS, as well as the angle of arrival at the HRIS. In both works, the HRIS actively shares with the BS its locally gathered information to further process it, via a control link. It can be argued that while sharing the local information with the BS is easy, as an infrastructure connecting the HRIS to the BS is expected to be deployed (see for example [9]), sharing the local information with the UE is not straightforward.

In this paper, we propose a novel localization technique by the UE, which exploits the sensing capability of an HRIS. In our scheme, the UE transmits signals to the HRIS that operates in full absorption mode, i.e., the received signal is not reflected but fully processed locally to estimate the angle of arrival (AoA) at the HRIS. Then, after a preset time, the BS transmits a downlink signal through the HRIS that enables the UE to estimate the time of flight (ToF) from the HRIS. Moreover, in this second phase, the HRIS transmits to the UE the information on the AoA estimated in the first phase by a backscattered modulation superimposed on the signal transmitted by the BS. The UE, knowing the location of the HRIS, can then estimate its position. We denote the resulting localization protocol as localization with HRIS and backscattered signal (LHBS). LHBS exploits the control channel between the HRIS and the BS only to trigger the transmission of the downlink reference signal in the second phase. Lastly, the assumption that the UE knows the position of the HRIS is also reasonable since the HRIS is fixed and is part of the network infrastructure, thus being equivalent to that of knowing the position of BSs.

The rest of this work is organized as follows: Section II introduces the System model. The proposed LHBS protocol is described in Section III. The performance of the proposed solution is investigated in Section IV, where we also provide a comparison with the Cramér-Rao lower bound on the AoA, the range, and the position estimators. Lastly, in Section V we

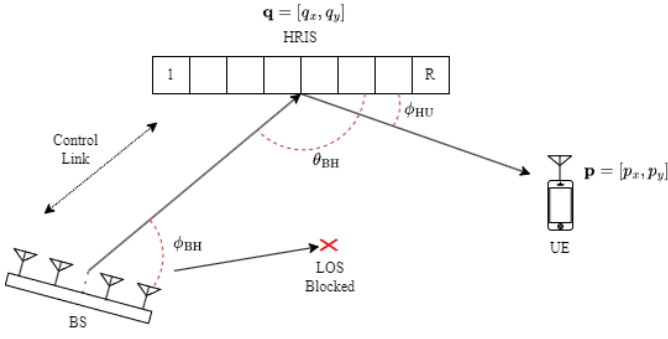


Fig. 1. Reference scenario: an UE at position \mathbf{p} localizes itself using an HRIS at position \mathbf{q} and a BS in a nLOS scenario. The AoA and AoD to and from the HRIS are θ_{BH} and ϕ_{HU} , respectively. The AoD from the BS is ϕ_{BH} .

draw the main conclusions.

II. SYSTEM MODEL

We consider the scenario of Fig. 1 in which a UE estimates its position in a cellular network assisted by a single BS. The estimation is assisted by an HRIS controlled by the BS.

The BS is located at the origin of our reference system. The HRIS is located at position $\mathbf{q} = [q_x, q_y]$, which is known to the UE. The UE aims at estimating its position $\mathbf{p} = [p_x, p_y]$.

The BS is equipped with a uniform linear array (ULA) with M antennas, while the UE is equipped with a single antenna. The HRIS comprises R evenly spaced elements organized along a line, each receiving and reflecting signals as an omnidirectional antenna while introducing a configurable phase shift. The HRIS is hybrid because it can also process impinging signals locally. The coefficient $\rho \in [0, 1]$ represents the fraction of the signal power that is reflected, while a fraction $(1 - \rho)$ of the signal power is absorbed for local processing purposes by each HRIS element. We assume that the HRIS has a direct/control link (e.g., via optical fiber) with the BS but it is not equipped with a transmitter. Consequently, the HRIS cannot directly communicate with the UE but it can only process locally the impinging signals and change its element phase shifts. We define two extreme operative modes of the HRIS, namely:

- *Full Absorption Mode*: in this case $\rho = 0$, meaning that the whole incoming signal is absorbed by the HRIS for local processing.
- *Fully Reflective Mode*: in this case $\rho = 1$, so the whole incoming signal is reflected by the HRIS.

We consider a scenario without strict synchronization between the BS, the HRIS, and the UE. In the following, time is referred to the system of the UE, without loss of generality. We denote with ϵ the normalized (to $\lambda/(2\pi c)$) time offset between the UE and the HRIS or BS clocks, where λ is the wavelength, and c is the speed of light in air.

A. Channel Model

Geometrical Properties of Signal Propagation: Considering a transmission at mmWaves, we assume that each channel

is characterized by a single path. The AoA and angle of departure (AoD) to and from the HRIS are denoted as θ_{BH} and ϕ_{HU} , respectively. The AoD from the BS is ϕ_{BH} . We define the ToF between the HRIS and the UE as τ_{HU} , consequently the distance between UE and HRIS is

$$r_{\text{HU}} = c\tau_{\text{HU}}. \quad (1)$$

Similarly, defining the ToF between the HRIS and the BS as τ_{HB} , the distance between BS and HRIS is $r_{\text{HB}} = c\tau_{\text{HB}}$. Let $d_{\text{tot}} = r_{\text{HU}} + r_{\text{HB}}$ be the total distance of the downlink path, i.e., the distance that the signal sent from the BS and reflected from the HRIS travels to reach the UE. We denote as $\tau = d_{\text{tot}}/c$ the ToF between the BS and the UE.

Baseband Channel Model: The free-space path loss between the UE and the HRIS is $\gamma = \left(\frac{\lambda}{4\pi r_{\text{HU}}}\right)^2$. We define the channel coefficient from the UE to the HRIS as $\xi_{\text{HU}} = \sqrt{\gamma}e^{-j(\epsilon + \frac{2\pi r_{\text{HU}}}{\lambda})}$, including the effect of path loss, group delay between the UE and the HRIS, and clock differences. Similarly, we define ξ_{BH} as the channel coefficient from the BS and the HRIS similarly defined (using r_{hb}). Lastly, we define the steering vector operator at the receiver as

$$\mathbf{a}_A(\theta) = [1, e^{-j\kappa \sin \theta}, \dots, e^{-j\kappa \sin \theta(A-1)}]^T, \quad (2)$$

where $\kappa = 2\pi d/\lambda$, d is the spacing between two adjacent antennas (or HRIS elements), $A \in \{M, R\}$ is the number of antennas (or elements), and θ represents the AoA. The baseband single-path channel matrix from the BS to the HRIS is therefore

$$\mathbf{H}_{\text{BH}} = \frac{1}{\sqrt{M}} \xi_{\text{BH}} \mathbf{a}_R(\theta_{\text{BH}}) \mathbf{a}_M^H(\phi_{\text{BH}}) \in \mathbb{C}^{R \times M}. \quad (3)$$

The column-vector channel from the UE to the HRIS is

$$\mathbf{h}_{\text{UH}} = \xi_{\text{UH}} \mathbf{a}_R(\phi_{\text{HU}}) \in \mathbb{C}^{R \times 1}. \quad (4)$$

The BS-HRIS channel \mathbf{H}_{BH} is assumed to be known both at the BS and at the HRIS as it is fully determined by their positions. Let $\mathbf{b}_{\text{BS}} \in \mathbb{C}^M$ be the beamforming vector at the BS.

HRIS Model: We characterize the effect of the HRIS by the diagonal matrix $\mathbf{\Omega} \in \mathbb{C}^{R \times R}$, where each element introduces the following gain and phase shift

$$\Omega_{ii} = \sqrt{\rho} e^{j\alpha_i}, \quad \alpha_i \in [0, 2\pi), \quad i = 0, \dots, R-1. \quad (5)$$

We assume that the line of sight (LOS) between the UE and the BS is blocked, so the communication is assisted by an HRIS.

III. LOCALIZATION WITH HRIS AND BACKSCATTERED SIGNAL

In this section, we describe the localization with HRIS and backscattered signal (LHBS) at the UE. Our approach is based on the estimation of two quantities: the AoD at the HRIS ϕ_{HU} and the ToF τ_{HU} . From this information, the UE will estimate its position. Our algorithm is divided into three phases, which are first briefly outlined and then explained in detail:

where $w'(t)$ is the AWGN and both AoA and ToF appear. This model will be used in Section III-D to assess the AoA and range estimator performance. Then the UE filters the received signal by $q(-t)$ and upsamples the filter output with oversampling period $T_s = \frac{T_c}{u_f}$, where u_f is the oversampling factor. Let us define

$$s_i = R\xi_{\text{BH}}\xi_{\text{UH}}e^{j\hat{\phi}_{\text{HU}}} \sum_{n=0}^{N-1} x_n \tilde{q}(iT_s - nT_c - 2\tau_{\text{HU}} - T - \tau_1), \quad (11)$$

for $i = 0, \dots, Nu_f - 1$, where $\tilde{q}(t)$ is the convolution between $q(t)$ and $q(-t)$, and τ_1 is a suitable delay so that the maximum of the convolution is one of the samples of s_i and all non-zero terms fall in the considered window of i . The oversampled signal model is

$$\mathbf{r} = \mathbf{s} + \mathbf{w}, \quad (12)$$

where entries of \mathbf{r} are $r_i = s_i + w(iT_s)$ and $w(iT_s) \sim \mathcal{CN}(0, \sigma_w^2)$ for $i = 0, \dots, Nu_f - 1$. Note that, $\sigma_w^2 = u_f \sigma^2$ as up sampling the received signal also increases the noise variance. Recalling (1), we notice that $\mathbf{r} \sim \mathcal{CN}(\mathbf{s}(\hat{\phi}_{\text{HU}}, r_{\text{HU}}), \sigma_u^2 \mathbf{I}_{Nu_f})$, i.e., the range and AoA information is contained in the mean of a Gaussian vector.

Note that we could obtain the same goal via digital modulation of the HRIS elements. As an example, in [13] a passive (non-hybrid) RIS is exploited and the state of its elements (on/off) is used to convey its local information via a spatial modulation scheme.

The estimation of the AoA at the HRIS in phase 1 is crucial, as it will affect the modulation that HRIS will apply in phase 2. Since the path loss of the signal received by the HRIS when estimating the UE AoA is much lower than the one that affects the BS-HRIS-UE path, we can take the estimation at the HRIS as perfect. In other words, due to the large number of HRIS elements and the mmWave frequencies, if we want our algorithm to work then the estimation error at the HRIS can be made much smaller with respect to the end-to-end one. Hence, the bottleneck of the system is the estimation at the UE of the AoA with the signal coming from the BS and reflected by the HRIS.

Second Transmission: In the transmission of the second acknowledgment signal, the HRIS optimally aligns the channel between BS and UE and creates a virtual LOS between the two. To do that, the HRIS sets its phase shifters as

$$\Omega_{ii} = e^{jk[\sin \hat{\phi}_{\text{HU}} - \sin \theta_{\text{BH}}]i}. \quad (13)$$

In this case, no additional modulation is added by the HRIS. The second transmission starts immediately after the first and the received discrete-time signal at the UE (after filtering and sampling) can be written similarly to (12) as

$$\mathbf{r}' = \mathbf{s}' + \mathbf{w}', \quad (14)$$

where \mathbf{w}' is the AWGN vector and entries of \mathbf{s}' are

$$s'_i = R\xi_{\text{BH}}\xi_{\text{UH}} \sum_{n=0}^{N-1} x_n \tilde{q}(iT_s - nT_c - 2\tau_{\text{HU}} - T - \tau_1 - NT_c), \quad (15)$$

for $i = 0, \dots, Nu_f - 1$.

The UE demodulates $\hat{\phi}_{\text{HU}}$ by aligning in time the two signals, and then combining them as follows

$$z = \frac{1}{Nu_f} \sum_{n=0}^{Nu_f-1} r_n^* r'_n \simeq \|\xi_{\text{BH}}\xi_{\text{UH}}\|^2 R^2 e^{-j\hat{\phi}_{\text{HU}}}. \quad (16)$$

The approximation in (16) arises from the large number theorem as we substituted the average with the expectation operator when N is sufficiently large. The UE can now obtain the analog demodulated AoA at the HRIS as

$$\dot{\phi}_{\text{HU}} = -\angle z. \quad (17)$$

Note that in both transmissions we use a CAZAC sequence of length N . In principle, we could use a general pilot sequence not necessarily known at the UE to estimate the AoA, as (16) holds when we use the same sequence in both transmissions. Still, we will use these two sequences also in Section III-C for the range estimation.

C. UE Position Estimation

In the third phase of LHBS, the UE computes its position. In particular, the UE knows the time of its transmission (time zero) and also the fixed time T . Consequently, the UE can extract the ToF τ_{HU} from both the received signals of the first and second transmission by the BS, and then take the average. Note the estimate of the delay cannot be done on the two sequences together, since they have an unknown phase shift, due to backscatter modulation.

In detail, the UE correlates the over-sampled signal with a local replica of the over-sampled transmitted sequence. The relation between the transmitting and arrival times at the UE is (e.g., for the first sequence)

$$t_{\text{RX}} = 2\tau_{\text{HU}} + T, \quad (18)$$

and so a first estimate of the ToF at the UE is

$$\tilde{\tau}_{\text{HU}} = \frac{t_{\text{RX}} - T}{2}. \quad (19)$$

Similarly, we obtain the second estimation $\tilde{\tau}'_{\text{HU}}$ from the second transmission. Lastly, the estimation of the range at the UE is obtained by computing

$$\dot{r}_{\text{HU}} = c \left(\frac{\tilde{\tau}_{\text{HU}} + \tilde{\tau}'_{\text{HU}}}{2} \right). \quad (20)$$

Note that estimating the range in this way relies only on the absolute times at the UE and is not affected by clock misalignment between UE and BS.

With the AoA and range estimations $\dot{\phi}_{\text{HU}}$ and \dot{r}_{HU} , and the known HRIS position \mathbf{q} , the UE estimates its position $\dot{\mathbf{p}}$. In particular, defining $\boldsymbol{\theta} = [\phi_{\text{HU}}, r_{\text{HU}}]^T$, we have

$$\begin{bmatrix} \dot{p}_x \\ \dot{p}_y \end{bmatrix} = \mathbf{g}(\dot{\boldsymbol{\theta}}) = \mathbf{q} + \begin{bmatrix} \dot{r}_{\text{HU}} \cos \dot{\phi}_{\text{HU}} \\ -\dot{r}_{\text{HU}} \sin \dot{\phi}_{\text{HU}} \end{bmatrix}. \quad (21)$$

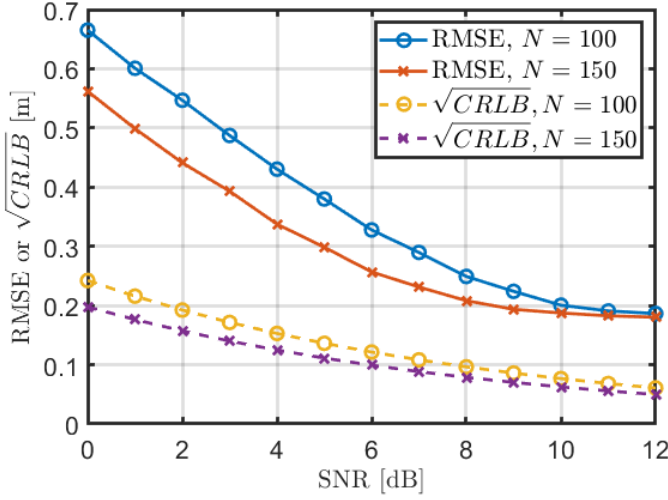


Fig. 3. RMSE and \sqrt{CRLB} of the ranging estimate vs the SNR for a sequence length $N = 100$ or 150 .

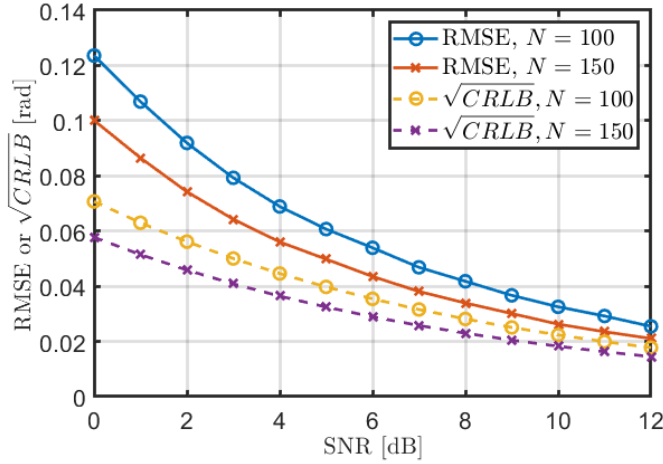


Fig. 4. RMSE and \sqrt{CRLB} of the AoA estimate vs the SNR for a sequence length $N = 100$ or 150 .

D. Cramér-Rao Lower Bounds

To assess the performance of the LHBS algorithm, we compared the MSE of the range r_{HU} and the demodulated AoA $\hat{\phi}_{\text{HU}}$ with their Cramér Rao lower bounds (CRLB) that give a lower bound on the error variance of all the possible unbiased estimators of the parameters. Due to space limitations, the algebraic operations to compute the quantities in the following can be found in the Appendix.

CRLB of the Received AoA: We assume that the estimate of the AoA at the HRIS is without error, while we take into account the error introduced in the transmission from the BS to the UE through the HRIS. From [14, Sec. 15.7] we compute

$$\frac{\partial^2 \ln p(\mathbf{r}|\hat{\phi}_{\text{HU}}, r_{\text{HU}})}{\partial^2 \hat{\phi}_{\text{HU}}} = \frac{2}{\sigma_u^2} \frac{\partial}{\partial \hat{\phi}_{\text{HU}}} \Re \left[(\mathbf{r} - \mathbf{s}(\hat{\phi}_{\text{HU}}, r_{\text{HU}}))^H \times \frac{\partial \mathbf{s}(\hat{\phi}_{\text{HU}}, r_{\text{HU}})}{\partial \hat{\phi}_{\text{HU}}} \right] = \frac{2}{\sigma_u^2} \Re[-\mathbf{r}^H \mathbf{s}]. \quad (22)$$

The CRLB on the AoA is then

$$CRLB_{\phi_{\text{HU}}} = - \left[\mathbb{E} \left(\frac{\partial^2 \ln p(\mathbf{r}|\hat{\phi}_{\text{HU}}, r_{\text{HU}})}{\partial^2 \hat{\phi}_{\text{HU}}} \right) \right]^{-1} = \frac{\sigma_u^2}{2\|\mathbf{s}\|^2}. \quad (23)$$

CRLB of the Ranging Estimation at the UE: We also compute the CRLB of the estimate of the ranging using the results of [15, Sec. 2.4.6] that provide

$$CRLB_{r_{\text{HU}}} = \frac{c^2}{8 \cdot 2B_2^2 \frac{E_s}{N_0}}, \quad (24)$$

where E_s is the total energy used for the correlation, B_2 is the root mean square bandwidth, and $N_0 = \sigma_u^2 T_s$. The coefficient 8 at the denominator of (24) is due to our use of two sequences to perform the estimation of the ToF and both of them estimate $2\tau_{\text{HU}}$.

CRLB of the Position Estimation: To obtain the CRLB of the position estimation we first compute the Fisher information matrix (FIM) on the AoA and range. In detail, the FIM is

$$\mathbf{I} = \begin{bmatrix} CRLB_{\phi_{\text{HU}}}^{-1} & \alpha \\ \alpha & CRLB_{r_{\text{HU}}}^{-1} \end{bmatrix}. \quad (25)$$

where

$$\begin{aligned} \alpha &= -\mathbb{E} \left(\frac{\partial^2 \ln p(\mathbf{r}|\hat{\phi}_{\text{HU}}, r_{\text{HU}})}{\partial \hat{\phi}_{\text{HU}} \partial r_{\text{HU}}} \right) \\ &= -\frac{2}{\sigma_u^2} \Re \left[\mathbf{s}^H \frac{\partial \mathbf{s}}{\partial r_{\text{HU}}} \right]. \end{aligned} \quad (26)$$

From [14, Sec. 3.8] we obtain the CRLB on the position estimation at the UE as

$$CRLB_{\text{pos}} = \text{tr} \left[\frac{\partial \mathbf{g}(\boldsymbol{\theta})}{\partial \boldsymbol{\theta}} \mathbf{I}^{-1} \frac{\partial \mathbf{g}(\boldsymbol{\theta})^T}{\partial \boldsymbol{\theta}} \right]. \quad (27)$$

IV. NUMERICAL RESULTS

In this section, we assess the performance of the proposed LHBS protocol and compare it with the obtained CRLBs. The transmit power is $\mathbb{E}(|x_n|^2) = 1$, the carrier frequency is $f_c = 25$ GHz, the distance HRIS-UE is $r_{\text{HU}} = 100$ m, the distance BS-HRIS is $r_{\text{BH}} = 100$ m, the sequence length is $N = 100$ or 150 , the signal bandwidth is $B = 20$ MHz, the roll-off factor is $\beta = 0.8$, and the up sampling factor is $u_f = 10$.

We define the signal-to-noise ratio (SNR) on the received signal as

$$\text{SNR} = \frac{\|\xi_{\text{BH}} \xi_{\text{UH}}\|^2 R^2}{\sigma^2}. \quad (28)$$

Fig. 3 shows the root mean square error (RMSE) of the ranging r_{HU} as a function of the SNR. We also plot the

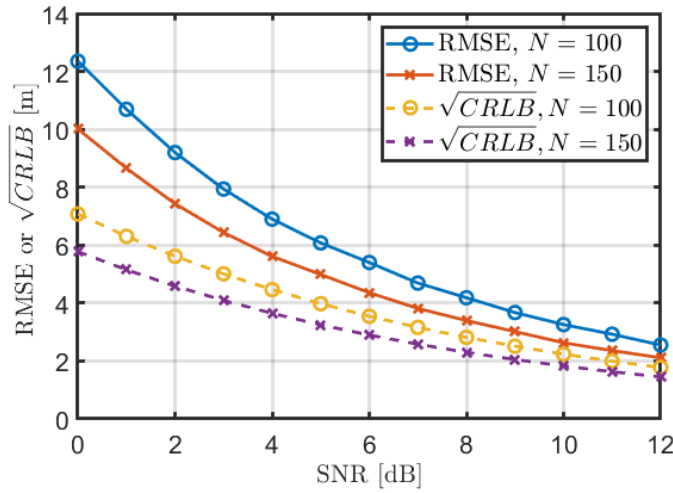


Fig. 5. RMSE or \sqrt{CRLB} of the position estimation vs SNR for a sequence length of $N = 100$ or 150 .

corresponding square root of CRLB (24). We observe that the RMSE of the ranging error is in the range of tens of centimeters and for high SNR values the performance of the estimator gets close to the CRLB. Also, we observe that increasing the sequence length (N) provides a performance improvement. We also observe that the improvement saturates at high SNR: this is due to the time quantization. Upsampling even more the received signal would lower the saturation level.

Fig. 4 shows the RMSE of the AoA estimated at the HRIS as a function of the SNR, again in a comparison with the square root of the CRLB (23). We note that in this case, the estimator achieves a performance that is closer to the CRLB.

Lastly, Fig. 5 shows the RMSE of the estimated UE position as a function of the SNR. We observe that in the considered scenario we can achieve a positioning precision in the range of meters.

V. CONCLUSIONS

In this paper, we presented a novel protocol for HRIS-aided user localization. We exploited the sensing property available at the HRIS to locally process the incoming signal from the UE and estimate the AoA of the signal. The UE then computes its position from two signals transmitted from the BS and reflected by the HRIS. They encode by a differential

backscatter modulation the AoA information. We proved the effectiveness of our approach via simulation and compared the performances with the Cramér Rao lower bounds.

REFERENCES

- [1] A. Behravan, V. Yajnanarayana, M. F. Keskin, H. Chen, D. Shrestha, T. E. Abrudan, T. Svensson, K. Schindhelm, A. Wolfgang, S. Lindberg, and H. Wymeersch, "Positioning and sensing in 6G: Gaps, challenges, and opportunities," *IEEE Vehicular Technology Magazine*, vol. 18, no. 1, pp. 40–48, Mar. 2023.
- [2] H. Wymeersch, J. He, B. Denis, A. Clemente, and M. Juntti, "Radio localization and mapping with reconfigurable intelligent surfaces: Challenges, opportunities, and research directions," *IEEE Vehicular Technology Magazine*, vol. 15, no. 4, pp. 52–61, Dec. 2020.
- [3] R. Liu, M. Li, H. Luo, Q. Liu, and A. L. Swindlehurst, "Integrated sensing and communication with reconfigurable intelligent surfaces: Opportunities, applications, and future directions," *IEEE Wireless Commun.*, vol. 30, no. 1, pp. 50–57, Feb. 2023.
- [4] K. Keykhosravi, M. F. Keskin, G. Seco-Granados, and H. Wymeersch, "SISO RIS-enabled joint 3D downlink localization and synchronization," in *Proc. IEEE Int. Conf. on Commun. (ICC)*, 2021, pp. 1–6.
- [5] A. Fascista, A. Coluccia, H. Wymeersch, and G. Seco-Granados, "RIS-aided joint localization and synchronization with a single-antenna mmwave receiver," in *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, 2021, pp. 4455–4459.
- [6] J. He, H. Wymeersch, L. Kong, O. Silvén, and M. Juntti, "Large intelligent surface for positioning in millimeter wave MIMO systems," in *Proc. IEEE Vehicular Technology Conf. (VTC2020)*, 2020, pp. 1–5.
- [7] A. L. Swindlehurst, G. Zhou, R. Liu, C. Pan, and M. Li, "Channel estimation with reconfigurable intelligent surfaces—a general framework," *Proceedings of the IEEE*, vol. 110, no. 9, pp. 1312–1338, Sep. 2022.
- [8] G. C. Alexandropoulos, N. Shlezinger, I. Alamzadeh, M. F. Imani, H. Zhang, and Y. C. Eldar, "Hybrid reconfigurable intelligent metasurfaces: Enabling simultaneous tunable reflections and sensing for 6G wireless communications," *IEEE Vehicular Technology Magazine*, pp. 2–11, Dec. 2023.
- [9] R. Ghazalian, H. Chen, G. C. Alexandropoulos, G. Seco-Granados, H. Wymeersch, and R. Jäntti, "Joint user localization and location calibration of a hybrid reconfigurable intelligent surface," *IEEE Trans. on Vehicular Technology*, vol. 73, pp. 1435–1440, Jan. 2023.
- [10] J. He, A. Fakhreddine, and G. C. Alexandropoulos, "Joint channel and direction estimation for ground-to-UAV communications enabled by a simultaneous reflecting and sensing RIS," in *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, 2023, pp. 1–5.
- [11] A. Albanese, P. Mursia, V. Sciancalepore, and X. Costa-Pérez, "Papar: Practical RIS-aided localization via statistical user information," in *Proc. Int. Workshop on Signal Proc. Advances in Wireless Commun. (SPAWC)*, 2021, pp. 531–535.
- [12] M. H. Hayes, *Statistical digital signal processing and modeling*. John Wiley & Sons, 1996.
- [13] W. Yan, X. Yuan, and X. Kuai, "Passive beamforming and information transfer via large intelligent surface," *IEEE Wireless Commun. Letters*, vol. 9, no. 4, pp. 533–537, Apr. 2020.
- [14] S. M. Kay, *Fundamentals of statistical signal processing: estimation theory*. Prentice-Hall, Inc., 1993.
- [15] U. Mengali, *Synchronization techniques for digital receivers*. Springer Science & Business Media, 2013.

VI. APPENDIX

A. CRLB of the Received AoA

In this section, the CRLB of the Received AoA will be derived.

$$\begin{aligned}
\frac{\partial^2 \ln p(\mathbf{r}|\hat{\phi}_{\text{HU}}, r_{\text{HU}})}{\partial^2 \hat{\phi}_{\text{HU}}} &= \frac{2}{\sigma_u^2} \frac{\partial}{\partial \hat{\phi}_{\text{HU}}} \Re \left[(\mathbf{r} - \mathbf{s}(\hat{\phi}_{\text{HU}}, r_{\text{HU}}))^H \frac{\partial \mathbf{s}(\hat{\phi}_{\text{HU}}, r_{\text{HU}})}{\partial \hat{\phi}_{\text{HU}}} \right] \\
&= \frac{2}{\sigma_u^2} \frac{\partial}{\partial \hat{\phi}_{\text{HU}}} \Re \left[(\mathbf{r}^H - \mathbf{s}^H(\hat{\phi}_{\text{HU}}, r_{\text{HU}})) j \mathbf{s}(\hat{\phi}_{\text{HU}}, r_{\text{HU}}) \right] \\
&= \frac{2}{\sigma_u^2} \frac{\partial}{\partial \hat{\phi}_{\text{HU}}} \Re \left[j \mathbf{r}^H \mathbf{s}(\hat{\phi}_{\text{HU}}, r_{\text{HU}}) \right] \\
&= \frac{2}{\sigma_u^2} \Re[-\mathbf{r}^H \mathbf{s}(\hat{\phi}_{\text{HU}}, r_{\text{HU}})].
\end{aligned} \tag{29}$$

If we take the expectation of (29) we simply substitute \mathbf{r} with $\mathbf{s}(\hat{\phi}_{\text{HU}}, r_{\text{HU}})$, and from that the CRLB immediately follows.

B. Off-diagonal coefficient

In this section, the off-diagonal coefficient

$$\alpha = -\mathbb{E} \left(\frac{\partial^2 \ln p(\mathbf{r}|\hat{\phi}_{\text{HU}}, r_{\text{HU}})}{\partial \hat{\phi}_{\text{HU}} \partial r_{\text{HU}}} \right) \tag{30}$$

is derived. We start by computing

$$\frac{\partial^2 \ln p(\mathbf{r}|\hat{\phi}_{\text{HU}}, r_{\text{HU}})}{\partial \hat{\phi}_{\text{HU}} \partial r_{\text{HU}}} = \frac{2}{\sigma_u^2} \frac{\partial}{\partial \hat{\phi}_{\text{HU}}} \Re \left[(\mathbf{r} - \mathbf{s}(\hat{\phi}_{\text{HU}}, r_{\text{HU}}))^H \frac{\partial \mathbf{s}(\hat{\phi}_{\text{HU}}, r_{\text{HU}})}{\partial r_{\text{HU}}} \right]. \tag{31}$$

Knowing that $\partial r_{\text{HU}} = c \partial \tau_{\text{HU}}$, we rewrite (31) as

$$\frac{\partial^2 \ln p(\mathbf{r}|\hat{\phi}_{\text{HU}}, r_{\text{HU}})}{\partial \hat{\phi}_{\text{HU}} \partial r_{\text{HU}}} = \frac{2}{\sigma_u^2} \frac{\partial}{\partial \hat{\phi}_{\text{HU}}} \Re \left[(\mathbf{r} - \mathbf{s}(\hat{\phi}_{\text{HU}}, r_{\text{HU}}))^H \frac{\partial \mathbf{s}(\hat{\phi}_{\text{HU}}, r_{\text{HU}})}{c \partial \tau_{\text{HU}}} \right]. \tag{32}$$

We compute \check{s} with entries

$$\check{s}_i = \left[\frac{\partial \mathbf{s}(\hat{\phi}_{\text{HU}}, r_{\text{HU}})}{\partial \tau_{\text{HU}}} \right]_i = -2R\xi_{\text{BH}}\xi_{\text{UHE}} e^{j\hat{\phi}_{\text{HU}}} \sum_{n=0}^{N-1} x_n \tilde{q}'(iT_s - nT_c - 2\tau_{\text{HU}} - T - \tau_1), \tag{33}$$

where $\tilde{q}'(\cdot)$ is the raised cosine derivative. We notice that $\mathbf{s}(\hat{\phi}_{\text{HU}}, r_{\text{HU}})^H \frac{\partial \mathbf{s}(\hat{\phi}_{\text{HU}}, r_{\text{HU}})}{\partial \tau_{\text{HU}}}$ does not depend on $\hat{\phi}_{\text{HU}}$, consequently its derivative with respect to $\hat{\phi}_{\text{HU}}$ is zero. Thus, we rewrite (32) as

$$\begin{aligned}
\frac{\partial^2 \ln p(\mathbf{r}|\hat{\phi}_{\text{HU}}, r_{\text{HU}})}{\partial \hat{\phi}_{\text{HU}} \partial r_{\text{HU}}} &= \frac{2}{\sigma_u^2} \frac{\partial}{\partial \hat{\phi}_{\text{HU}}} \Re \left[\mathbf{r}^H \frac{\partial \mathbf{s}(\hat{\phi}_{\text{HU}}, r_{\text{HU}})}{c \partial \tau_{\text{HU}}} \right] \\
&= \frac{2}{\sigma_u^2} \Re \left[j \mathbf{r}^H \frac{\partial \mathbf{s}(\hat{\phi}_{\text{HU}}, r_{\text{HU}})}{c \partial \tau_{\text{HU}}} \right].
\end{aligned} \tag{34}$$

Finally, we find

$$\begin{aligned}
\alpha &= -\mathbb{E} \left(\frac{\partial^2 \ln p(\mathbf{r}|\hat{\phi}_{\text{HU}}, r_{\text{HU}})}{\partial \hat{\phi}_{\text{HU}} \partial r_{\text{HU}}} \right) \\
&= -\frac{2}{\sigma_u^2} \Im [\mathbf{s}^H \check{\mathbf{s}}] = -\frac{2}{\sigma_u^2} \Im \left[\mathbf{s}^H \frac{\partial \mathbf{s}(\hat{\phi}_{\text{HU}}, r_{\text{HU}})}{\partial r_{\text{HU}}} \right].
\end{aligned} \tag{35}$$