CHALMERS
UNIVERSITY OF TECHNOLOGY

Leveraging Ris-Enabled Smart Signal Propagation for Solving Infeasible Localization Problems

Leveraging RIS-Enabled Smart Signal Propagation for Solving Infeasible Localization Problems

Kamran Keykhosravi, Benoît Denis, George C. Alexandropoulos,
Zhongxia Simon He, Antonio Albanese, Vincenzo Sciancalepore, and Henk Wymeersch

***Abstract*—Reconfigurable intelligent surfaces (RISs) have tremendous potential for both communication and localization. While communication benefits are now well-understood, the breakthrough nature of the technology may well lie in its capability to provide and support localization capabilities. We present an overview of RIS-enabled localization scenarios, considering various numbers of RISs, single- or multi-antenna base stations, narrowband or wideband transmissions, and near- and far-field operations. Based on this overview, we also highlight key research directions and open challenges specific to RIS-enabled localization and sensing.**

I. Introduction

Radio localization via wireless network infrastructure is a service stemming from governmental mandates on positioning emergency calls by network operators. Over time, especially after introducing dedicated signals and procedures in 3GPP R16, radio localization found many other applications, including navigation, network optimization, geo-targeting, and augmented reality [1], particularly for scenarios where the Global Positioning System (GPS) is insufficient (or not available), such as indoor environments, urban canyons, and tunnels. With cellular localization, the user equipment (UE) state (comprising UE location, time bias, but possibly also the orientation, velocity, etc.) can be estimated based on a variety of measurements from the received signal, including the signal strength, time-of-arrival (ToA), angle-of-arrival (AoA), and angle-of-departure (AoD). In the fifth generation (5G) of wireless systems, radio localization can be accurately performed thanks to a multitude of antennas and large radio bandwidth. In the future sixth generation (6G), radio localization is envisioned to be even more ubiquitous by utilizing reconfigurable intelligent surfaces (RISs) [2].

Typical communication services require predominantly a single base station (BS), whereas user localization often necessitates supplementary infrastructure, such as an additional multi-antenna BS, relay, or RISs. Compared with the former two options, the adoption of RISs provides a substantially more cost- and energy-efficient solution, thanks to their simpler hardware implementation as well as minimal deployment and maintenance efforts than multi-antenna BSs and relays [3]. Additionally, RISs can be easily installed on common surfaces, such as walls and billboards, and they are passive or have a few active elements (e.g., as with the RIS design in [4]). Due to their limited power consumption, they are even suitable for delivering 3D ubiquitous features being installed on board of unmanned aerial vehicles (UAVs) in emergency scenarios [5]. In Fig. 1, we compare two wireless systems with two single-antenna UEs (a car and a laptop). The position of the car can be estimated via the AoD and delay measurements from the two multi-antenna BSs, while the location of the laptop is estimated via the AoD and delay measurements from a single BS and an RIS. We note that if in Fig. 1 the RIS was not present, the laptop position could not be estimated via the reflection from the wall since the position of the wall is unknown.

In this article, we explore scenarios where localization is enabled by RISs, namely multiple-input multiple-output (MIMO), multiple-input single-output (MISO), single-input multiple-output (SIMO), and single-input single-output (SISO) setups with either wideband (WB) or narrowband (NB) signaling, which operate in the far- or near-field regimes. The investigated RIS-enabled scenarios rely on extremely limited BS infrastructure, thereby leading to significant cost and energy savings. These scenarios can be tailored to support various innovative use cases in the context of Industry 4.0, vehicular networks, and overall 6G networks, such as UAVs and automated guided vehicles (AGVs) localization and navigation, collaborative manufacturing, human-robot interaction and hazards mapping, radar detection and localization of passive objects, and so forth. While RIS-assisted localization systems have been studied in many papers (see, e.g., [6], [7], [8] and references therein), to the best of our knowledge, this is the first paper that treats the feasibility aspects of RIS-based localization in detail. We also support our discussion via a novel experimental localization example at 60 GHz for one of the considered RIS-enabled scenarios.

The remainder of this paper is organized as follows. We first provide some background on RIS operation, followed by an introduction to the fundamentals of wireless localization. The main part of this paper then covers the available RIS-enabled localization scenarios, one of which is experimentally evaluated. Finally, we list open research challenges.

II. RIS Operation Mode Supporting Localization

A planar array of elementary ultra-thin and ultra-low power electronic circuits or metamaterials, each capable of realizing distinct electromagnetic (EM) states, is known as reflective RIS [9], [10]. Its dynamic reconfigurability according to desired wireless networking objectives is enabled by a multitude of unit elements, such as positive intrinsic negative (PIN) diodes or varactors, which are usually managed by a microcontroller that communicates with the rest of the

Fig. 1: RIS-enabled localization: without RIS, several BSs are needed for localization, while with RIS, localization is possible with less infrastructure. The symbols τ, ϕ, θ are used to indicate ToAs, AoDs, and AoAs, respectively.

network infrastructure in- or out-of-band [2], [3]. For example, by appropriately configuring the state of the PIN diodes or the bias voltage of the varactors, the resulting macroscopic transformations of the radio waves impinging at the RIS can be controlled, offering desired reflective beamforming towards intended receivers. This beamforming mechanism is cost- and power-efficient compared to multi-antenna BSs and relays, which include transceiver radio-frequency chains (consisting of signal converters and amplifiers, as well as frequency mixers) and possibly networks of phase shifters, while imposing certain installation constraints due to their large sizes.

In geometric propagation environments with mmWave and sub-THz frequency bands, which are the focus of this article, fine-grained control over the reflected EM field is essential for accurate reflective beamforming, enabled by RIS elements of sub-wavelength sizes (e.g., $\lambda/10$ with λ being the wavelength), despite inevitable strong inter-element mutual coupling and possibly gray-scale-tunable EM properties. In contrast, in stochastic sub-6 GHz rich scattering environments, half-wavelength-sized elements suffice for supporting EM wave fingerprinting in conjunction with supervised learning for localization [11]. The channel modeling of RIS-enabled smart wireless environments is an active area of research [3]. For localization purposes, sparse parametric models are often used, where the channel is represented via a few geometric components. The received signal in the downlink (DL) can be calculated as a sum of individual rays reflected from each RIS element at the UE location. When the UE is in the geometric near-field of the RIS, this signal is a function of the transmitted symbols, the BS position, the positions of the RIS elements, and the UE position, among which only the last one is unknown and needs to be estimated [12]. When the BS and UE are in the far field of the RIS, i.e., when the distances between the UE, BS, and RIS are much larger than the RIS size, the wireless channel to the UE can be described by the AoD, which consists of elevation and azimuth components.

III. Wireless Localization Fundamentals

Radio localization methods are based on the premise that received waves convey geometric information about the propagation channel, which can be in turn used to determine the locations of the wirelessly connected devices (i.e., UEs). Broadly speaking, radio localization methods can be categorized as *data-driven* and *model-driven*. In the former category, we have methods such as fingerprinting and artificial-intelligence-assisted localization, which rely on rich features of the received radio signal, but without a structure that is easy to model [11]. In this context, RISs generate richer multipath and thus more effective radio signatures. The latter category of model-driven methods harnesses approximate statistical relations between the received radio signal and the signal propagation geometry (including the UE location), and form the bulk of radio localization techniques used in practice. Model-based methods have a large number of benefits over data-driven methods. They rely on decades of signal processing methods and optimization techniques, usually offering lower complexity than data-driven approaches, and are accompanied by performance bounds that provide strong guarantees of optimality and reliability [6], [12].

In the following, we focus our attention on model-driven approaches and study the feasibility of localization problems from a geometric standpoint by analyzing scenarios that would be infeasible for conventional non-RIS techniques. As visualized in Fig. 2, practical radio-based localization methods in 5G systems rely on time-based measurements from several BSs, where the propagation time of the direct line-of-sight (LOS) signal path to or from a BS is proportional to the distance between the UE and BS, but also includes an unknown clock bias of the UE with respect to the BS. As a specific example, under time-difference-of-arrival (TDoA), measurements from 4 synchronized BSs are needed to solve the 3D positioning and 1D clock bias estimation problem out of one-way transmissions (i.e., uplink (UL) or downlink). In contrast, under two-way round-trip time (RTT) measurements, when signal exchanges between BS and UE naturally remove the timing uncertainty, 3 BSs are sufficient for UE localization. To

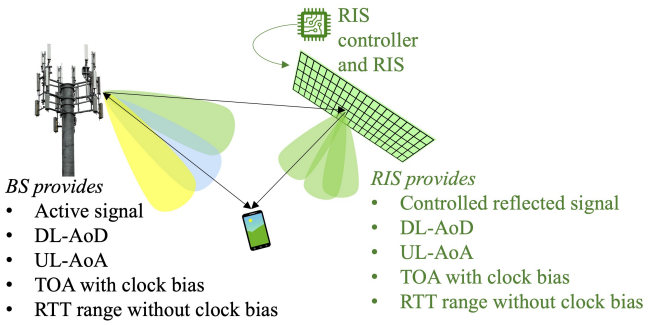


Fig. 2: An overview of the different location-relevant measurements under standard 5G systems (in black) and potential RIS-enabled systems (in green).

complement delay-based measurements, angle measurements (AoA and AoD) are employed, which, based on a codebook of directional beams, constrain the UE to lie within an angular sector. The sector size depends on the beamwidth, with the latter being inversely proportional to the array size. We refer the interested reader to [1] for a more detailed study on the conventional localization methods and history.

The performance of model-based localization methods depends on several fundamental metrics: *identifiability*, *ambiguity*, *resolution*, *precision*, and *accuracy*. Note that this does not correspond to an exhaustive list of metrics (which would include latency, update rate, integrity, etc.), but merely to convey the fundamentals.

- **Precision and accuracy** refer, respectively, to the spread and bias of localization errors, but are usually treated jointly (with either term being commonly used, though we will use accuracy herein) through the localization error statistics (e.g., mean or median error, 90% confidence interval). In principle, the accuracy can be arbitrarily improved by increasing the signal-to-noise ratio (SNR). In addition to link-level SNR, accuracy is also determined by the deployment geometry (i.e., UE relative position with respect to BSs), also referred to as Geometric Dilution of Precision (GDoP) (e.g., in the GPS community). Accuracy is arguably the definitive metric for any localization method, as it accounts for both resolution and identifiability.
- **Resolution** in our context refers to the separability of perfectly correlated radio propagation paths in at least one domain (which could be delay/Doppler, as commonly used in radar, but also angle or polarization). Signal paths that are not resolvable will be interpreted as a single path, thus limiting the accuracy (irrespective of the SNR), and leading to worse performance than predicted by analytical bounds. The resolution is bounded by the available physical resources, i.e., bandwidth for delay/distance resolution (and conversely time for frequency/Doppler resolution), and antenna array aperture for angle resolution. Accordingly, aiming at achieving better resolution (rather than better accuracy), more bandwidth and larger arrays are, in general, required to improve localization.
- **Ambiguity and non-identifiability** may still occur, even with very high resolution. In particular, the solution to the localization problem may be ambiguous (i.e., there are several distinct solutions) or the problem may not be identifiable (i.e., there exists a continuous space of solutions). This happens, for instance, when the LOS signal from one BS is missing due to an obstruction or when the infrastructure deployment/coverage is not sufficient. Ambiguity can generally be resolved by prior information (e.g., an ambiguous GPS solution far away from the earth's surface can readily be discarded) and occur generally intermittently. On the other hand, identifiability is more harmful, as there are many equally valid solutions to the localization problem, most of which cannot be discarded based on external information. We note that identifiability is related to, but distinct from observability in control theory, where observability refers to the ability to estimate the user location over time.

There are several (equivalent) approaches to assess identifiability, including geometry and Fisher information analysis. The geometric approach is generative, in the sense that, it constructs the manifold that constrains the solution based on each measurement, and then, determines the dimensionality of the intersection of these manifolds. An identifiable problem would thus have a zero-dimensional manifold as the solution. Instead, a Fisher information analysis aims at characterizing the amount of location information conveyed by measurements, given both the known statistics of the latter and the true UE location. More specifically, it determines the local curvature of the likelihood function. This curvature is described by a matrix, called the Fisher information matrix. When this matrix is not full-rank, the likelihood is locally flat along at least one dimension in the vicinity of the true location, rendering the problem infeasible. An example of an infeasible localization problem is TDoA-based localization with 2 BSs (the intersection of two hyperboloids is a 1D manifold).

In the following section, we discuss the expected advantages of RIS-empowered settings in terms of localization feasibility, when compared to conventional settings in similar scenarios and operating contexts.

IV. RIS-enabled localization scenarios

In this section, we present several localization scenarios wherein UE 3D positioning can be achieved. In addition to positioning, we discuss whether the UE velocity, clock bias, and orientation are identifiable. We focus on the downlink direction since it facilitates the positioning of multiple UEs at once. We consider minimal localization scenarios, meaning that if a single BS or RIS is removed, 3D positioning is no longer possible. Besides, we assume that all the BSs are synchronized with each other, while the UE is not.

We consider both NB and WB signals, where only in the latter case the ToA estimation can be performed. Moreover, depending on the scenario, the BSs and the UE are equipped with either a single or multiple antennas, where angle measurements are only possible in the latter case. We list relevant scenarios in Table I, which are also illustrated in Fig. 3.

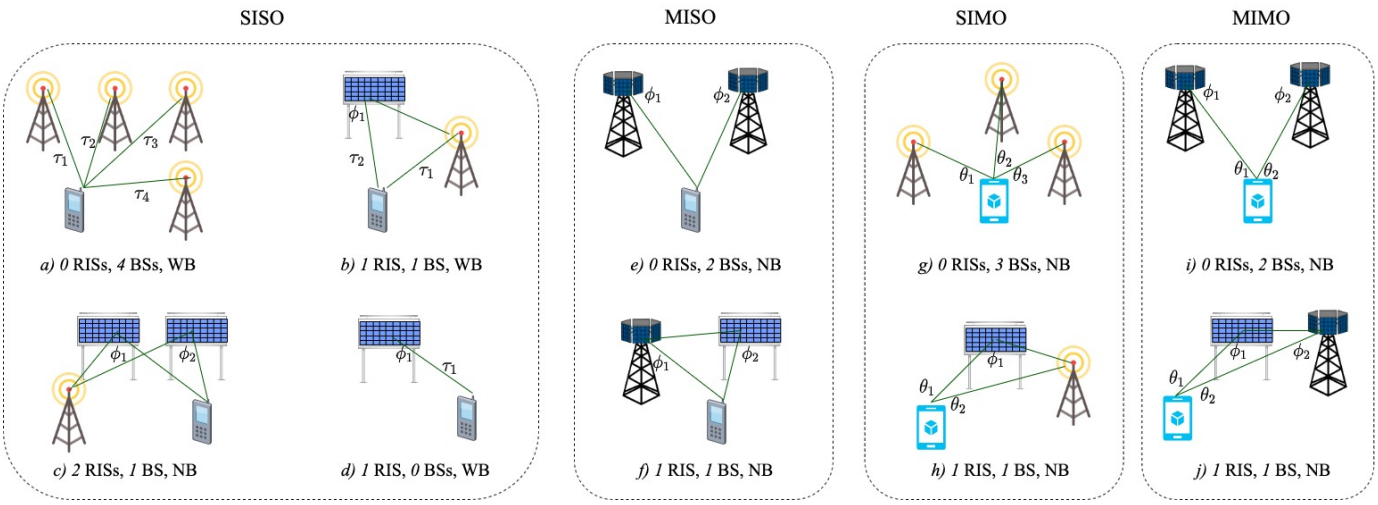


Fig. 3: Scenarios of feasible 3D UE positioning. The symbols τ, ϕ, and θ indicate ToAs, AoDs, and AoAs, respectively.

TABLE I: Identifiability analysis of 3D UE positioning in the downlink. The abbreviations pos, vel, and ori stand for position, velocity, and orientation, respectively.

	Scenario/example paper	Signaling	Measurements	Identifiable State	Positioning is possible also
SISO	0 RISs, 4 BSs	WB	TDoA	3D pos, clock, 3D vel	with 3 BSs and RTT measurements
SISO	1 RIS, 1 BS [13]	WB	TDoA, AoD	3D pos, clock, 2D vel	in near-field w/o LOS to BS
SISO	2 RISs, 1 BS	NB	AoD	3D pos, 3D vel	w/o LOS to BS
SISO	1 RIS, 0 BSs [14]	WB	RTT, AoD	3D pos, 1D vel	N/A
MISO	0 RISs, 2 BSs	NB	AoD	3D pos, 2D vel	N/A
MISO	1 RIS, 1 BS [15]	NB	AoD	3D pos, 2D vel	in near-field w/o LOS to BS
SIMO	0 RISs, 3 BSs	NB	AoA	3D pos, 3D vel, 3D ori	N/A
SIMO	1 RIS, 1 BS	NB	AoD, AoA	3D pos, 2D vel, 3D ori	N/A
MIMO	0 RISs, 2 BSs	NB	AoD, AoA	3D pos, 2D vel, 3D ori	N/A
MIMO	1 RIS, 1 BS	NB	AoD, AoA	3D pos, 2D vel, 3D ori	in near-field w/o LOS to BS

A. SISO localization

SISO with 4 BSs in the absence of an RIS (Fig. 3 (a)): We consider the standard cellular localization protocol with four synchronized BSs transmitting WB pilots and generating three TDoAs or four ToAs. The UE position can be estimated by intersecting the three hyperboloids corresponding to the three TDoA measurements. Next, based on the UE position estimate and the measured ToAs, we can obtain the clock bias allowing the UE to be synchronized to the BSs. By measuring the RTTs instead of the TDoAs, UE localization becomes feasible even with three BSs via intersecting the three spheres identified by the three RTTs and centered in the corresponding BSs. Lastly, we can derive the UE velocity vector in 3D via four measured Doppler shifts (i.e., radial velocities).

SISO with 1 RIS and 1 BS (Fig. 3 (b)): We assume a SISO system with a single RIS as in [13]. By using WB pilots, we can obtain the ToAs for the direct (i.e., the path BS-UE) and the reflected (i.e., the path BS-RIS-UE) paths, from which we calculate the resulting TDoA, which corresponds to a hyperboloid in 3D space. By using different RIS phase profiles for different transmissions, the AoD from the RIS to the UE can be estimated, which geometrically translates to a half-line. Therefore, we can calculate the UE position by intersecting this half-line and the above-mentioned hyperboloid, while deriving the clock bias from the UE position estimate and the measured ToAs. Moreover, we can exploit the Doppler shifts on the direct and the reflected paths to estimate the UE 2D velocity. Furthermore, if the UE is in the near-field of the RIS, its position can be found by leveraging on the wavefront curvature, even with a blocked direct path.

SISO with 2 RISs and 1 BS (Fig. 3 (c)): Let us assume a SISO system with two RISs. In this scenario, we can perform UE positioning even with NB signaling, which does not allow ToA estimation. Indeed, the UE position can be estimated by intersecting the two half-lines corresponding to the AoDs from the RISs. The direct BS-UE path does not carry any position information, thus localization can be performed even when the direct path is blocked. Nonetheless, the direct path provides Doppler information and enables us to estimate the UE velocity in 3D. Later in this paper, we perform experimental measurements to further investigate this scenario.

SISO with 1 RIS in the absence of a BS (Fig. 3 (d)): A single-antenna full-duplex UE can estimate its own location by transmitting WB pilots to the RIS and processing the reflected signals, thus (strictly) not requiring any BS (see [14]). In this scenario, we can measure the RTT and the AoD from the RIS to the UE. Geometrically, they respectively correspond to a sphere centered in the RIS and a half-line originated in the RIS, whose intersection returns the UE position estimate. As the Doppler shifts can only be measured along the RIS-UE direction, the UE velocity can be estimated in 1D. However,

if the UE motion direction is a priori known, the 1D estimate fully identifies the UE velocity vector (e.g., for UEs moving along a highway).

B. MISO localization

We consider a MISO system, where multi-antenna BSs allow estimating the respective AoD towards the UE (see e.g., [15]). Here, we can perform UE positioning with only 2 BSs and no RIS as shown in Fig. 3 (e). Here, the UE position can be estimated by intersecting the two half-lines corresponding to the two AoDs from the BSs. Since ToAs measurements are not required, we can employ NB pilots. Similarly, UE localization can be achieved by replacing one of the BSs with an RIS as shown in Fig. 3 (f), thus obtaining a MISO system with 1 RIS and 1 BS, and leveraging on the AoDs from the BS and the RIS.

C. SIMO localization

In a SIMO system, it is possible to estimate the AoAs from the BSs at the UE in the UE's frame of reference, which depends on its orientation. We first consider a scenario with no RIS and 3 BSs using NB pilots as shown in Fig. 3 (g). To show that the user position is identifiable, we define $\theta_{i,j}$ to be the angle between the direction of arrival from the ith BS and that of the jth one. Note that $\theta_{i,j}$ can be calculated based on the measured AoAs and does not depend on the UE's orientation. Now consider any arbitrary plane that includes the ith and the jth BS. If the user is in this plane, then it should create a $\theta_{i,j}$ angle with these BSs. One can show that the locus of these points is described by an arc of a circle containing the two BSs and its reflection by the line that passes through the two BSs. Since this argument holds for all the planes that contain ith and jth BSs, to obtain all the points that create $\theta_{i,j}$ angle with the two BSs, we should rotate this curve around the line that connects them. The generated surface is either the inner or the outer part of a spindle torus. Observe that the user should locate on the intersection of the three surfaces corresponding to $\theta_{1,2}$, $\theta_{1,3}$, and $\theta_{2,3}$, which, in general, has dimension zero (is a set of finite points). Therefore, the problem of user localization is identifiable. After estimating the UE position the UE orientation also can be found by means of any two AoAs.

Furthermore, localization is possible with 1 RIS and 1 BS as illustrated in Fig. 3 (h). In this scenario, we can measure two AoAs and one AoD from the RIS. Using the two AoAs, we can locate the user on (part of) a spindle torus, whose intersection with the line corresponding to the AoD locates the UE. Then the UE orientation can be estimated via the two AoAs.

D. MIMO localization

In MIMO systems, both AoAs and AoDs can be estimated. Therefore, UE localization is possible with no RIS and 2 BSs (Fig. 3 (i)) or with 1 RIS and 1 BS (Fig. 3 (j)). In both cases, the UE position can be estimated via the two AoDs (by intersecting the two corresponding half-lines) while the UE orientation can be derived from the two AoAs.

E. Conventional vs RIS-enabled localization

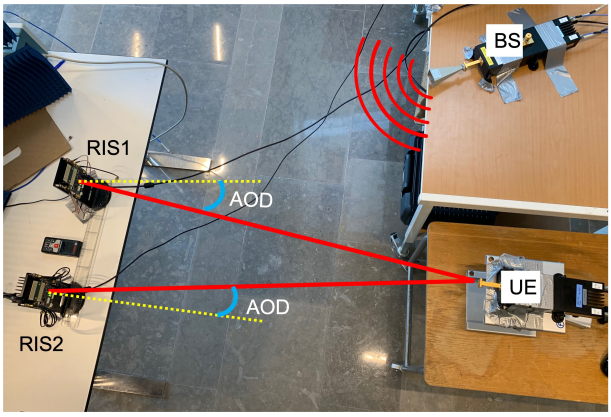
We now provide a qualitative comparison between two of the aforementioned scenarios: *Scenario 1: SISO with* 2 *RISs and* 1 *BS* and *Scenario 2: MISO with* 0 *RISs and* 2 *BSs*. Although both scenarios use two AoDs to localize the UE, in the former case, the AoDs are measured from the RISs, while in the latter one they are measured from the BSs. We compare the two methods in terms of cost, energy consumption, and accuracy. RISs have lower manufacturing and installation costs than multi-antenna BSs. Furthermore, since RISs are almost passive devices, they consume much less energy than BSs. Therefore, *Scenario 1* is preferable to *Scenario 2* in terms of cost and power consumption. As far as localization accuracy goes, we need to consider two countering effects: the number of antennas and cascaded path loss. As RISs can have many more reflecting elements than the BSs antennas, they can produce narrower beams and higher beam resolution. However, compared to the signal received directly from the BS, the reflected signal through an RIS suffers from a much larger path loss, which reduces the SNR and subsequently the localization accuracy. Therefore, the comparison in terms of localization accuracy depends on several factors, such as the RIS and BS array sizes, carrier frequency, and network geometry (e.g., BSs and RISs placement), which are tied to the specific parameters of the localization system.

V. An Experimental Localization Case

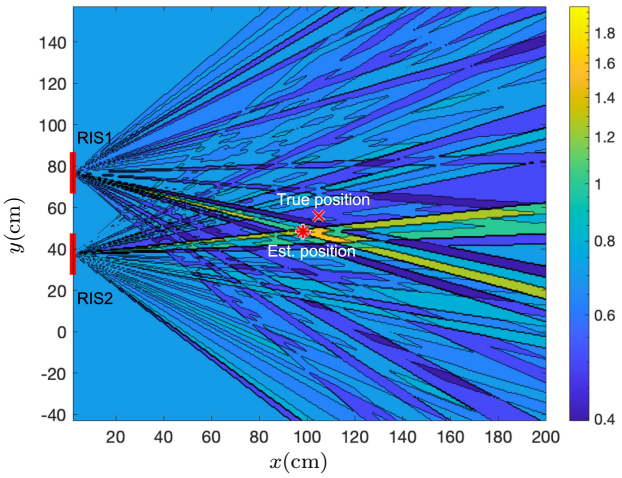
In this section, we experimentally validate the SISO localization scenario with 1 *BS and* 2 *RISs*, as described earlier. The laboratory experimental setup operating at 60 GHz is illustrated in Fig. 4 (a). As real RIS hardware prototypes are still under development (and hence, not yet available), we deploy two commercial transceivers as RISs and a two-port millimeter-wave vector network analyzer (VNA). We configure one of the VNA ports as the transmitter, i.e., the BS, and the other port as the receiver, i.e., the UE. Two transceiver modules BFM6010 from SiversIMA, operating over the 57–71 GHz frequency band, are used to emulate the two RISs. Each module contains a transmitter and a receiver, which are equipped with an antenna array of size 16×4. To emulate an RIS with those modules, we loop the receiver I and Q signals back to the transmitter I and Q ports and apply the desired beamforming (in terms of relative phase shifts) before transmitting the up-converted signal. A common local oscillator is used by the transmitter and the receiver for signal up- and down-conversion to avoid frequency offsets.

To perform localization in 2D, each of the two RISs iteratively sets 63 beampattern configurations, which generate different azimuth AoDs. The received power to the UE is recorded for each of the beams and each of the RISs. Fig. 4 (b) illustrates the received power from the two RISs in a 2D plane by assigning the crossing point of each pair of beams (i.e., 63^2 points), the sum of normalized[1] received powers. The estimation of the AoDs at the UE side is performed by selecting the beam that provides the largest received power for

[1]The values are normalized by the maximum received power from each RIS.



(a)



(b)

Fig. 4: (a) The experimental localization setup at 60 GHz and (b) the normalized received power for different possible UE positions. The true and estimated UE positions are shown by a cross and a star, respectively.

each RIS. Hence, the UE position is given by the intersection of such two beams, which corresponds to the point with maximum value in Fig. 4 (b), marked by a red star. It can be seen that the estimation is within the 10-cm radius of the ground truth value (marked by a red cross).

It should be noticed that the UE can receive a certain power even when the beam is not directed towards it. Apart from the imperfect beams, localization error is caused by limited beam resolution, power measurement errors, and geometrical factors. In terms of the last point, for any AoD estimation routine, the localization error increases with UE distance. Furthermore, if real RISs are used instead of the transceivers, additional impairments (e.g., losses) could reduce the localization accuracy.

VI. Conclusions and Research Challenges

We have argued that a decisive breakthrough of RISs lies in their capacity to make localization feasible in lightweight operating contexts, where conventional systems would fail or necessitate more physical resources. The qualitative analysis conducted in this paper confirms that the introduction of RISs can significantly reduce the requirements on the infrastructure, by replacing BSs with RIS, thus reducing cost and power consumption. The use of RIS for lightweight localization introduces a multitude of related research questions.

- *Integrated communication and localization*: The provision of distinct services in an RIS-enabled wireless environment raises novel challenges in terms of multi-purpose RIS optimization (e.g., localization-optimized vs. communication-optimized configurations), protocols (e.g., in-band vs. out-of-band control, RIS resource sharing in complex multi-user multi-operator ecosystems, BS-RIS synchronization) and architectures (e.g., seamless integration within open RAN).
- *Mobility support*: The continuous tracking of mobile UEs would benefit from both NLoS channel detection (for proper RIS activation) and low-latency location-based RIS control capabilities (thus requiring prior UE location and uncertainty at any time).
- *Uncontrolled multipath - robustness and exploitation*: In practice, apart from the LOS path, other signal components reach the UE after being scattered by the surrounding objects. If such components are not resolved at the UE, they interfere with the LOS signal and deteriorate the localization accuracy. If the NLOS components are resolvable in at least one domain (angle, delay, or Doppler), they can be separated from the LOS signal, but, more importantly, they can contribute to UE localization and environmental mapping.
- *RIS deployment*: Both RIS cardinality and placement must be optimized with respect to both communication metrics and localization/sensing accuracy and coverage, while being competitive in comparison with conventional BSs deployment (in terms of overall power consumption and coordination efforts). This also relates to the issue of RIS location and orientation calibration.
- *RIS operating modes*: Alternative RIS usages are also being considered to support localization and sensing functionalities with minimal deployment costs (e.g., vehicle-mounted reflective RISs, BS-free or multi-static radar-like approaches, hybrid RISs supporting also the Rx mode for sensing both connected UEs and passive objects).
- *Estimation algorithms*: Dedicated location/speed/attitude state estimators for UEs and passive objects (i.e., up to 9D), as well as source separation and data association schemes (e.g., between measured radio variables and controlled multipath components), should enable efficient channel-based simultaneous localization and mapping, while benefiting from the geometric near-field propagation properties offered by large RISs.
- *Security*: While RIS-aided integrated communications and localization can be inherently secured through controlled spatial filtering, they can also contribute to channel-based physical-layer security through enhanced multipath diversity. On the other hand, passive reflective RISs can be used for undetectable location-based attacks against legitimate communication links.

Acknowledgment

The authors would like to thank Hugo Ssi Yan Kai and Viet Lê for their contributions in the the experimental setup

and Gonzalo Seco Granados for the insightful discussions. This work was supported by the EU H2020 RISE-6G project under grant 101017011 and the Chalmers Transport Area of Advance.

REFERENCES

[1] J. A. del Peral-Rosado, R. Raulefs, J. A. López-Salcedo, and G. Seco-Granados, "Survey of cellular mobile radio localization methods: From 1G to 5G," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 1124–1148, 2018.

[2] E. Calvanese Strinati, G. C. Alexandropoulos, H. Wymeersch, B. Denis, V. Sciancalepore, R. D'Errico, A. Clemente, D.-T. Phan-Huy, E. D. Carvalho, and P. Popovski, "Reconfigurable, intelligent, and sustainable wireless environments for 6G smart connectivity," *IEEE Commun. Mag.*, vol. 59, no. 10, pp. 99–105, Oct. 2021.

[3] M. Jian, G. C. Alexandropoulos, E. Basar, C. Huang, R. Liu, Y. Liu, and C. Yuen, "Reconfigurable intelligent surfaces for wireless communications: Overview of hardware designs, channel models, and estimation techniques," *Intell. Converged Netw.*, vol. 3, no. 1, pp. 1–32, Mar. 2022.

[4] I. Alamzadeh, G. C. Alexandropoulos, N. Shlezinger, and M. F. Imani, "A reconfigurable intelligent surface with integrated sensing capability," *Scientific Reports*, vol. 11, no. 1, p. 20737, 2021.

[5] A. Albanese, V. Sciancalepore, and X. Costa-Pérez, "First responders got wings: UAVs to the rescue of localization operations in beyond 5G systems," *IEEE Commun. Mag.*, vol. 59, no. 11, pp. 28–34, Nov. 2021.

[6] H. Wymeersch, J. He, B. Denis, A. Clemente, and M. Juntti, "Radio localization and mapping with reconfigurable intelligent surfaces: Chal-lenges, opportunities, and research directions," *IEEE Veh. Technol. Mag.*, vol. 15, no. 4, pp. 52–61, Dec. 2020.

[7] E. Björnson, H. Wymeersch, B. Matthiesen, P. Popovski, L. Sanguinetti, and E. de Carvalho, "Reconfigurable intelligent surfaces: A signal processing perspective with wireless applications," *IEEE Signal Process. Mag.*, vol. 39, no. 2, pp. 135–158, Mar. 2022.

[8] C. Pan, G. Zhou, K. Zhi, S. Hong, T. Wu, Y. Pan, H. Ren, M. Di Renzo, A. L. Swindlehurst, R. Zhang *et al.*, "An overview of signal processing techniques for RIS/IRS-aided wireless systems," *IEEE Journal of Selected Topics in Signal Processing*, 2022.

[9] C. Huang, A. Zappone, G. C. Alexandropoulos, M. Debbah, and C. Yuen, "Reconfigurable intelligent surfaces for energy efficiency in wireless communication," *IEEE Trans. Wireless Commun.*, vol. 18, no. 8, pp. 4157–4170, Aug. 2019.

[10] Q. Wu, S. Zhang, B. Zheng, C. You, and R. Zhang, "Intelligent reflecting surface aided wireless communications: A tutorial," *IEEE Trans. Commun.*, vol. 69, no. 5, pp. 3313–3351, May 2021.

[11] G. C. Alexandropoulos, N. Shlezinger, and P. del Hougne, "Reconfigurable intelligent surfaces for rich scattering wireless communications: Recent experiments, challenges, and opportunities," *IEEE Commun. Mag.*, vol. 59, no. 6, pp. 28–34, Jun. 2021.

[12] A. Elzanaty, A. Guerra, F. Guidi, and M.-S. Alouini, "Reconfigurable intelligent surfaces for localization: Position and orientation error bounds," *IEEE Transactions on Signal Processing*, vol. 69, pp. 5386–5402, 2021.

[13] K. Keykhosravi, M. F. Keskin, G. Seco-Granados, P. Popovski, and H. Wymeersch, "RIS-enabled SISO localization under user mobility and spatial-wideband effects," *IEEE Journal of Selected Topics in Signal Processing*, 2022.

[14] K. Keykhosravi, G. Seco-Granados, G. C. Alexandropoulos, and H. Wymeersch, "RIS-enabled self-localization: Leveraging controllable reflections with zero access points," in *Proc. IEEE ICC*, Seoul, South Korea, Jun. 2022, [available on arXiv:2202.11159].

[15] A. Fascista, M. F. Keskin, A. Coluccia, H. Wymeersch, and G. Seco-Granados, "RIS-aided joint localization and synchronization with a single-antenna receiver: Beamforming design and low-complexity estimation," *IEEE Journal of Selected Topics in Signal Processing*, 2022.

Kamran Keykhosravi was a postdoctoral researcher with the Department of Electrical Engineering at Chalmers University of Technology, Sweden. He is currently working as a researcher with Ericsson AB in Sweden. His research interests include radio localization, reconfigurable intelligent surfaces, and 5G core network.

Benoît Denis is a senior researcher with the Department of Wireless Technologies at CEA-Leti, Grenoble, France. His main research interests concern wireless localization and location-enabled networks, with a focus on cooperative, multipath-aided and data fusion approaches, as well as on enabling technologies such as ultra-wideband radio, millimeter waves, and reconfigurable intelligent surfaces.

George C. Alexandropoulos is Assistant Professor for wireless communication systems and signal processing with the Department of Informatics and Telecommunications, National and Kapodistrian University of Athens, Greece. His research interests span the general areas of algorithmic design and performance analysis for wireless networks with emphasis on multi-antenna transceiver hardware architectures, active and passive metasurfaces, full duplex radios, and high-frequency communications, as well as distributed machine learning algorithms.

Zhongxia Simon He received the M.Sc. degree from the Beijing Institute of Technology, Beijing, China, and the Ph.D. degree from the Chalmers University of Technology, Gothenburg, Sweden, in 2008 and 2014, respectively. He is currently an Associate Professor with the Microwave Electronics Laboratory, Department of Microtechnology and Nanoscience (MC2), Chalmers University. His current research interests include high data rate wireless communication, modulation and demodulation, mixed-signal integrated circuit design, radar, and packaging. He is also jointly working at SinoWave AB, Sweden.

Antonio Albanese received the M.Sc. degree in Telecommunications Engineering from Politecnico di Milano, Italy, in 2018. Currently, he is pursuing his Ph.D. in Telematic Engineering at Universidad Carlos III de Madrid, Spain, while being appointed as Research Scientist at NEC Laboratories Europe GmbH, Heidelberg, Germany. His research field covers millimeter waves, reconfigurable intelligent surfaces, applied mathematical optimization and machine learning techniques, with a particular interest in localization and prototyping.

Vincenzo Sciancalepore received his M.Sc. degree in Telecommunications Engineering and Telematics Engineering in 2011 and 2012, respectively, whereas in 2015, he received a double Ph.D. degree. Currently, he is a Principal Researcher at NEC Laboratories Europe in Heidelberg, focusing his activity on network virtualization and network slicing challenges. He is the Chair of the ComSoc Emerging Technologies Initiative (ETI) on Reconfigurable Intelligent Surfaces (RIS) and an editor of IEEE Transactions on Wireless Communications.

Henk Wymeersch is Professor at Chalmers University of Technology, Sweden, active in the area of 5G and beyond 5G radio localization and sensing.