Reconfigurable Intelligent Surface Enhanced Wireless Localization: Phase Optimization for Malicious Interference Mitigation

Yi Zhang, *Member, IEEE,* Yajing Xie, Lijia Wang, Minghui Liwang, *Senior Member, IEEE,* and Xianbin Wang, *Fellow, IEEE*

***Abstract*—Recently, unmanned aerial vehicles (UAVs) and reconfigurable intelligent surfaces (RISs) have merged as important enabling technologies for localization coverage extension and localization accuracy improvement under signal blockage and malicious interference conditions. However, most existing works assume known locations of jammers, which is generally impractical in real-world networks. To overcome this challenge, we propose a novel RIS-enhanced wireless localization framework against malicious interference with the support of either narrowband or orthogonal frequency division multiplexing (OFDM) pilot signals. A two-stage anti-jamming localization approach is developed to first estimate the unknown channel and signal information of the jammer and then localize the user's position by eliminating the jamming signal. More importantly, we utilize the full potential of RIS to improve localization accuracy by optimizing the phase shift profile during the iterative process. Extensive simulation results demonstrate the commendable performance of our proposed framework, which can not only mitigate the jamming effect but also achieve better localization accuracy, offering a good reference for future heterogeneous and complex wireless networks.**

***Index Terms*—Wireless localization, malicious interference, reconfigurable intelligent surface (RIS), phase optimization.**

I. Introduction

LOCATION-based services (LBSs) have witnessed a growing importance across various sectors, such as intelligent transportation, public safety, social networks, etc. Recently, high-accuracy positioning services in typical urban areas with severe signal blockage have attracted increasing attention due to the ever-growing demands. Specifically, signal propagation from wireless infrastructures, e.g., base stations, roadside units, and Global Navigation Satellite Systems (GNSS), to ground users are prone to *partial or total blockage* by high-rise buildings in urban areas, significantly degrading localization performance [1, 2]. *Unmanned aerial vehicles (UAVs)* have brought an alternative to extend communication and localization coverage in blind areas, capitalizing on their high mobility, ease of deployment, and reliable line-of-sight (LoS) transmissions [3, 4]. Without relying on GNSS, UAV-assisted techniques can facilitate accurate and reliable localization by deploying the UAVs as aerial anchors, providing supplementary localization information [5, 6]. As a result, many efforts on UAV trajectory strategies have been put forward to enhance the localization performance [7].

As another promising solution for overcoming signal blockages caused by obstacles, *reconfigurable intelligent surface (RIS)* offers the capability of signal propagation environment reconfiguration through a reflection phase controllable plane, comprising a multitude of low-cost passive reflective elements. Thanks to the capability of independent phase control of incident signals, the RIS can alter the radio propagation in the desired direction for enhanced signal reception [8]. By controlling its reflection characteristics, the RIS phase-shift design has been extensively studied to support accurate localization and energy efficiency [9, 10]. For example, by leveraging indoor environments, the RIS can effectively convert the negative impacts of multipath propagation into exploitable multi-signal paths, thereby offering precise location services [11]. The RIS also allows conformal architectures and flexible deployments for outdoor environments [12]. As a result, the combinations of UAVs and RISs possess significant potential for facilitating high-accuracy localization of ground users in GNSS-denied regions [13].

In recent years, *malicious interference* have grown increasingly prevalent, driven by the declining cost and simplified design of jamming devices. These attacks pose a significant threat to both communication and positioning systems. For example, jamming attacks can effectively disrupt or block legitimate communication links by severely degrading the signal-to-interference-plus-noise ratio (SINR) of the received signals. However, when targeting positioning systems, the primary objective shifts from causing temporary service interruptions to deliberately misleading the localization function. Note that localization accuracy can be influenced by various factors, including geographic features, equipment conditions, and multipath effects. Among these, malicious interference involving the continuous emission of radio frequency (RF) signals by jamming devices plays a critical role in degrading localization accuracy [14]. For simplicity, throughout the rest

This work was supported in part by the National Natural Science Foundation of China under Grant No. 62401485 and 62271424, the Natural Science Foundation of Fujian Province of China under Grant No. 2022J01005, and in part by Shanghai Pujiang Programme under Grant No. 24PJD117. *(Corresponding author: Yi Zhang.)*

Yi Zhang, Yajing Xie and Lijia Wang are with the Department of Information and Communication Engineering, and also with the Key Laboratory of Multimedia Trusted Perception and Efficient Computing, Ministry of Education of China, Xiamen University, Xiamen, China (email: yizhang@xmu.edu.cn).

Minghui Liwang is with the Department of Control Science and Engineering, and also with the Shanghai Research Institute for Intelligent Autonomous Systems, Tongji University, Shanghai, China (email: minghuiliwang@tongji.edu.cn).

Xianbin Wang is with the Department of Electrical and Computer Engineering, Western University, Ontario, Canada (email: xianbin.wang@uwo.ca).

of this paper, the term *jamming* will be used to describe malicious interference, and *jammer* will refer to the device responsible for such interference.

To mitigate the effectiveness of malicious interference, several anti-jamming countermeasures are utilized at the transmitter, such as regulated transmitted power, frequency-hopping spread spectrum, antenna polarization, and so on. The most-used strategy at the receiver side is the filter design. Although some existing literature has highlighted the possibility of jamming and eavesdropping attacks in UAV-assisted localization scenarios [15, 16], however, their contributions mainly concentrate on cases where GNSS signals are disrupted, while rarely considering scenarios where the mixed positioning signals and jamming signals, leading to reduced localization accuracy.

Addressing the above-mentioned challenges represents our key motivation. In this paper, we propose a RIS-enhanced wireless localization framework in the presence of unknown malicious interference, which has been overlooked in most existing works [15]. Specifically, we pay attention to a GNSS-denied network environment, in which a hovering UAV can offer wireless localization services to ground user equipment (UE), but its direct communication links are blocked by high-rise buildings. Encouraged by the reflection capability, a RIS is deployed to provide a reflected path for pilot signals. Meanwhile, a malicious jammer positioned at an undisclosed location seeks to mislead the localization function by continuously emitting jamming signals with unknown constant transmission power. Since most conventional wireless localization technologies are susceptible to jamming, the unknown jamming attack considered in our work will further introduce new challenges to localization performance.

To this end, we utilize the full potential of the RIS and propose a two-stage anti-jamming localization approach. In the former stage, we investigate a jamming estimation approach to identify the unknown channel and signal information of the jammer. In particular, the jammer estimation problem is formulated as a two-dimensional maximization problem based on the maximum likelihood (ML) function and the least squares (LS) criterion. To cope with its hardness, the Jacobi-Anger expansion is utilized to approximate the original problem into two separated one-dimensional problems, which can be solved through linear search and further refined by using the Quasi-Newton method. In the latter stage, we present a UE localization approach to estimate the UE's position by eliminating the jamming signal constructed from the measured key information of the jammer. We also explore the distinctions between *narrowband* and *orthogonal frequency division multiplexing (OFDM)* pilot signals within the proposed localization framework. To further improve the localization accuracy, we develop a phase optimization algorithm for anti-jamming localization (POAJL) by iteratively adjusting the phase shifts of the RIS based on the previous estimation results. Our POAJL algorithm optimizes the phase shift profile to maximize the reflected channel gain during the jamming estimation stage, while simultaneously strengthening the received power of the pilot signal and weakening the jamming signal in the UE localization stages.

Our main contributions are summarized as follows:

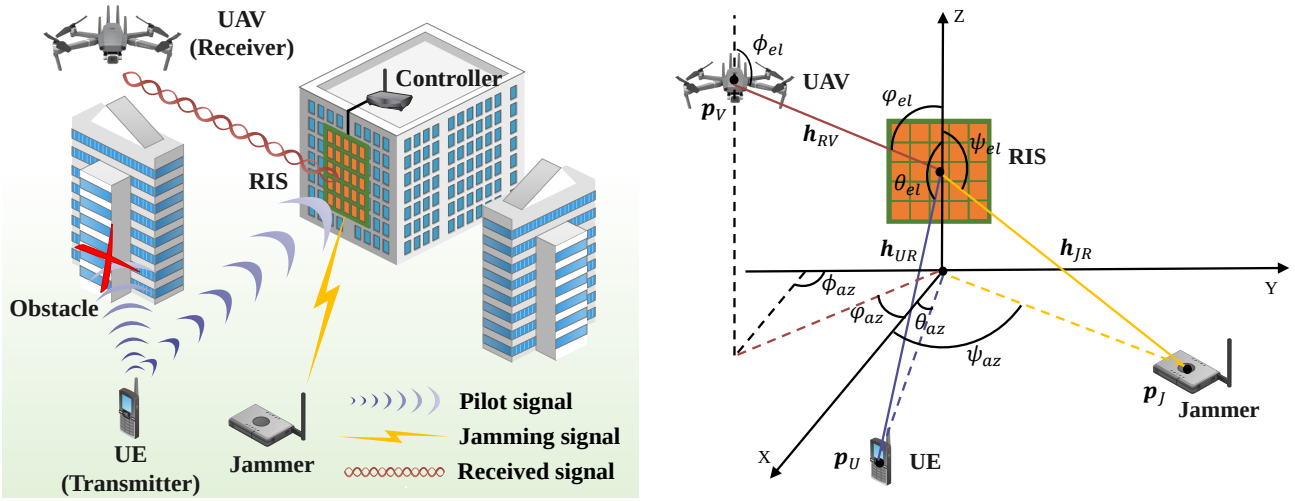
- Unlike most studies with accurately measured position of the malicious jammer, we formulate a RIS-enhanced anti-jamming localization framework and propose a two-stage localization approach for malicious interference elimination, where the unknown channel and signal information of the jammer is estimated in the former stage and then utilized to localize the user's position in the latter stage. Besides, two types of pilot signals, namely narrowband and OFDM, are studied in-depth to reveal their distinctions. Compared with the narrowband-based localization, the OFDM-based localization doesn't require any prior knowledge of the path fading factor.
- By fully exploiting the controllable phase shifts of the RIS, we propose a phase optimization algorithm for anti-jamming localization (POAJL) to alleviate the malicious interference caused by the jammer without disturbing the UE, meanwhile enhancing the received pilot signal throughout the iterative UE localization process, which can greatly improve the localization accuracy based on the historical estimation results.
- Through extensive simulations, we investigate the impact of the jammer's location and transmission power, while also discussing the localization performance based on narrowband and OFDM pilot signals. We further improve the proposed POAJL algorithm to overcome the drop in localization accuracy when the relative distance between the RIS and the jammer is similar to the distance between the RIS and the UE. Simulation results reveal that our proposed POAJL algorithm can outperform other approaches in terms of localization accuracy.

The rest of this paper is organized as follows. We summarize related works in Section II. The proposed RIS-enhanced localization system against jamming attacks is formulated in Section III and a two-stage anti-jamming localization approach is provided in Section IV. To further improve the estimation accuracy, we develop a RIS phase optimization process in Section V. We provide extensive evaluation results in Section VI and, finally, Section VII concludes this paper.

Notations : x, $\boldsymbol{x}$, and $\boldsymbol{X}$ denote scalars, column vectors, and matrices, respectively. The superscript T indicates the transpose operation ($(\boldsymbol{X})^{\mathsf{T}}$) and superscript H indicates the Hermitian transpose operationn ($(\boldsymbol{X})^{\mathsf{H}}$). $\odot$, $\times$, and $\cdot$ denote the Hadamard product, cross products, and vectorial dot, respectively. $\|\cdot\|$ is the 2-norm, $|\cdot|$ is the module, $\angle(\cdot)$ is the true phase, and $\mathrm{diag}(\cdot)$ is a diagonal matrix consisting of the elements of the parameter. $j = \sqrt{-1}$ represents the imaginary unit. $[\boldsymbol{X}]_{n,:}$ and $[\boldsymbol{X}]_{:,n}$ represent the n-th row and column of matrix $\boldsymbol{X}$, respectively. $\mathbf{0}_{m\times n}$ is the all-zeros matrices and $\boldsymbol{I}_n$ is the identity matrices. $\mathbf{1}_n$ and $\mathbf{0}_n$ are length n vectors of unity and zeros.

II. Related work

Due to their mobility and flexibility, UAVs have been widely utilized as aerial anchors or base stations, providing varying vertical heights to establish the LOS paths and improve the 3-D localization performance, especially in scenarios where GNSS is blocked [17–20]. To meet diverse communication



(a) RIS-enhanced wireless localization scenario

(b) 3D geometry model for wireless localization

Fig. 1. RIS-enhanced wireless localization system under malicious interference.

and localization service requirements for ground users, an integrated air-ground networking paradigm has become popular to minimize the deployment number of dual-functional UAVs [19]. In a UAV-enabled localization system, the lower bound of mean-square error (MSE) is derived and further minimized by considering the placement strategies of multiple UAV anchors. Semidefinite relaxation (SDR) technique and successive weighted least squares (SWLS) estimation are leveraged to a UAV-assisted multi-sensor localization system, addressing scenarios with unknown UAV parameters, e.g., unknown positions and velocities [6]. During this time, the parameters of users and UAVs should be simultaneously estimated, and the Cramér-Rao lower bound (CRLB) can be approximately achieved under mild Gaussian noise conditions. In addition, proper UAV trajectories are investigated to further enhance the localization accuracy [7, 21]. For example, a reinforcement learning-empowered multi-object localization framework [21] is proposed to autonomously optimize the trajectory of the UAV to improve the localization precision and reduce the UAV energy consumption.

As a promising technology for altering the radio propagation environment, the RIS has been extensively utilized to facilitate high-accuracy positioning services [22–30]. For instance, some research works analyze the RIS-enhanced localization from the perspective of the Fisher Information Matrix (FIM) [22, 23]. For near-field user localization, two practical signaling and positioning algorithms are proposed, addressing a synchronization mismatch problem in an OFDM downlink system, where only a single anchor node is adopted to localize the user with the assistance of a large RIS [25]. For far-field user localization, the fundamental limits of multiple RIS-aided OFDM localization systems are examined and the Bayesian bounds are derived to estimate the user's localization performance [27]. The potential benefits of the non-line-of-sight (NLOS) components in RIS-aided millimeter-wave (mmWave) communication systems have been explored in improving joint localization and environment sensing capabilities [28]. Besides, a low-complexity approximated mismatched maximum likelihood (AMML) estimator is developed to asymptotically tighten the lower bound on localization when the user is unaware of phase-dependent amplitude variations [29]. Moreover, the phase shift profile of the RIS can be optimized to enhance the received signal strength (RSS) and, consequently, improve the localization performance [9, 11, 13, 31]. A phase profile optimization algorithm based on gradient descent and alternative optimization methods is developed to obtain a more accurate wireless localization, which aims to minimize the CRLB [31]. For both near- and far-field localization and attitude (i.e., orientation) estimation, a close-form RIS phase profile is provided for joint communication and localization, demonstrating remarkable performance even in asynchronous signaling [9]. Distributed RISs are employed to manipulate multipath signals for indoor positioning and a two-step positioning approach is developed to timely update RIS reflection coefficients [11]. Combining UAV and RIS technologies, an integrated system for ground vehicles is proposed to strike a balance between communication and localization by solving the joint UAV trajectory planning and RIS phase-shift configuration problem [13].

Technologies on UAVs and RISs also specialize in wireless communication systems against jamming and eavesdropping attacks [32–35]. A threat model is discussed in a RIS-empowered multiple-input multiple-output (MIMO) system with multiple data streams, which aims to optimize the eavesdropper's receive combining matrix and the reflection coefficients of the malicious RIS [33]. To confront this threat, a physical layer security (PLS) scheme for secrecy rate maximization is proposed by jointly optimizing the legitimate precoding matrix and the number of data streams, the artificial noise (AN) covariance matrix, the receive combining matrix, and the reflection coefficients of the legitimate RIS [32, 33]. To facilitate the security of UAV networks in the presence of an eavesdropper, a RIS-assisted secure transmission design is proposed by maximizing the average secrecy rate, the trajec-

tory of UAV, the transmit beamforming, and the phase shift of RIS [36]. Simultaneous jamming and eavesdropping attacks are considered in a RIS-assisted multi-user cellular network with imperfect angular channel state information (CSI), and an alternative optimization (AO) method is proposed to improve both the spectrum efficiency and the security [37]. The feasibility of UAV-assisted anti-jamming localization is studied and evaluated to provide time-difference-of-arrival (TDoA) positioning service to ground users in jamming environments [15]. Specifically, the impacts of UAV self-localization uncertainty and synchronization errors caused by jamming are theoretically analyzed to demonstrate the feasibility of the proposed anti-jamming system. To protect the interests of operators and legitimate users, a UAV-enabled cooperative jamming framework is developed by optimizing the UAVs' locations and jamming power, and therefore preventing the unauthorized use of positioning services [16]. However, to the best of our knowledge, we are among the first to involve jamming attacks in the current RIS-assisted localization systems. Also, most existing anti-jamming approaches require knowledge of the exact location of the malicious jammer in advance, which can be impractical in real-world wireless mobile networks.

III. System Model

As illustrated in Fig.1(a), we consider a three-dimensional (3D) localization scenario in typical urban blind areas, where the conventional positioning technologies such as GNSS systems and terrestrial infrastructure-based positioning fail to meet the user's requirements. In this harsh environment, a hovering UAV (Receiver) equipped with a uniform planar array comprising $N_V = N_{Vx} \times N_{Vy}$ antennas in the x-y plane continuously offers wireless localization service to a single-antenna UE (Transmitter). As a service provider, the position of the UAV is known and represented by $\boldsymbol{p}_{_V} = (x_{_V}, y_{_V}, z_{_V})^{\mathsf{T}}$ in the Cartesian coordinate system. We assume that the distance between adjacent antennas is denoted by $\triangle d$ and satisfy $\triangle d = \frac{\lambda}{2}$, where λ denotes the carrier wavelength. Consequently, the positions of the UAV antennas (relative to the first one) can be expressed as $\boldsymbol{l}_{x,y} = [(x-1)\triangle d, (y-1)\triangle d, 0]^{\mathsf{T}}$, $x \in \{1, \ldots, N_{Vx}\}$, $y \in \{1, \ldots, N_{Vy}\}$. The position of the UE $\boldsymbol{p}_{_U} = (x_{_U}, y_{_U}, z_{_U})^{\mathsf{T}}$ is unknown and should be estimated.

Due to the obstruction of the direct communication link between the UE and the UAV, as shown in Fig. 1(a), a RIS assists in wireless localization by creating a reflected path for the pilot signals transmitted from the UE. The RIS located at $\boldsymbol{p}_{_R} = (x_{_R}, y_{_R}, z_{_R})^{\mathsf{T}}$ consists of $N_R = N_{Rx} \times N_{Ry}$ passive reflecting elements in the y-z plane and it is managed via a specialized controller. Similarly, the positions of RIS reflecting elements can be expressed as $\boldsymbol{u}_{v,h} = [0, (v-1)\triangle d, (h-1)\triangle d]^{\mathsf{T}}$, $v \in \{1, \ldots, N_{Ry}\}$, $h \in \{1, \ldots, N_{Rz}\}$, where $\triangle d$ is the distance between adjacent elements. We assume the physical size of the RIS constrained by N_R and $\triangle d$ is not very large in this work, which leads to small Fraunhofer distance and therefore electromagnetic near-field effects could be ignored [38, 39]. Unfortunately, the jamming signals emitted from a single-antenna **malicious jammer** with the **unknown position** $\boldsymbol{p}_{_J} = (x_{_J}, y_{_J}, z_{_J})^{\mathsf{T}}$ are reflected by the RIS toward the UAV and therefore lead to severe degradation in positioning accuracy. Specifically, we assume that the UAV, UE and RIS are synchronized to the same clock [40].

A. Channel Model

The geometry model of the wireless localization system is illustrated in Fig. 1(b). Let UR, RV and JR represent the links of UE→RIS, RIS→UAV and jammer→RIS. We denote the angle-of-arrival (AoA) in azimuth and elevation of the direct links UR and JR as $\boldsymbol{\theta} = [\theta_{az}, \theta_{el}]^{\mathsf{T}}$ and $\boldsymbol{\psi} = [\psi_{az}, \psi_{el}]^{\mathsf{T}}$, respectively. The angle-of-departure (AoD) and AoA in azimuth and elevation of the reflected link RV could be denoted by $\boldsymbol{\phi} = [\phi_{az}, \phi_{el}]^{\mathsf{T}}$ and $\boldsymbol{\varphi} = [\varphi_{az}, \varphi_{el}]^{\mathsf{T}}$, respectively.

Since the LoS path is much stronger than NLoS paths, within the far-field region of RIS, the channels $\boldsymbol{h}_{_{UR}} \in \mathbb{C}^{N_R \times 1}$ and $\boldsymbol{h}_{_{RV}} \in \mathbb{C}^{N_R \times N_V}$ of the links UR and RV are expressed as

$$\boldsymbol{h}_{_{UR}} = \rho_{_{UR}} e^{-j2\pi\tau_{_{UR}} f} \boldsymbol{a}(\boldsymbol{\theta}), \tag{1}$$

$$\boldsymbol{h}_{_{RV}} = \rho_{_{RV}} e^{-j2\pi\tau_{_{RV}} f} \boldsymbol{a}(\boldsymbol{\varphi}) \boldsymbol{b}^{\mathsf{T}}(\boldsymbol{\phi}), \tag{2}$$

where $\rho_{_{UR}}$ and $\rho_{_{RV}}$ represent the path loss, $\tau_{_{UR}}$ and $\tau_{_{RV}}$ indicate the corresponding transmission delay. The $\boldsymbol{a}(\boldsymbol{\theta})$ and $\boldsymbol{a}(\boldsymbol{\varphi})$ represent the response vectors of the direct link UR and the steering vector of the reflected link RV at the RIS, respectively. The vector $\boldsymbol{b}(\boldsymbol{\phi})$ denotes the response vector at the UAV. We further reformulate the vectors $\boldsymbol{a}(\boldsymbol{\theta})$, $\boldsymbol{a}(\boldsymbol{\varphi})$, and $\boldsymbol{b}(\boldsymbol{\phi})$ as

$$\boldsymbol{a}(\boldsymbol{\chi}) = \left[e^{-j\boldsymbol{w}^{\mathsf{T}}(\boldsymbol{\chi})\boldsymbol{u}_{1,1}}, \ldots, e^{-j\boldsymbol{w}^{\mathsf{T}}(\boldsymbol{\chi})\boldsymbol{u}_{N_{Ry},N_{Rz}}}\right]^{\mathsf{T}}, \boldsymbol{\chi} \in \{\boldsymbol{\theta}, \boldsymbol{\varphi}\} \tag{3}$$

$$\boldsymbol{b}(\boldsymbol{\chi}) = \left[e^{-j\boldsymbol{w}^{\mathsf{T}}(\boldsymbol{\chi})\boldsymbol{l}_{1,1}}, \ldots, e^{-j\boldsymbol{w}^{\mathsf{T}}(\boldsymbol{\chi})\boldsymbol{l}_{N_{Vx},N_{Vy}}}\right]^{\mathsf{T}}, \boldsymbol{\chi} \in \{\boldsymbol{\phi}\} \tag{4}$$

where $\boldsymbol{w}(\boldsymbol{\chi})$ is a wave vector and expressed as

$$\boldsymbol{w}(\boldsymbol{\chi}) = \frac{-2\pi}{\lambda} [\sin\chi_{el}\cos\chi_{az}, \sin\chi_{el}\sin\chi_{az}, \cos\chi_{el}]^{\mathsf{T}}. \tag{5}$$

Other specific channel parameters, if not mentioned, are provided in Appendix A. Furthermore, according to Eqs. (1) and (2), the cascade channel of the link UE→RIS→UAV, denoted by URV, at time slot t is formulated as

$$\boldsymbol{h}_{_{U,t}} = (\boldsymbol{h}_{_{UR}} \odot \boldsymbol{h}_{_{RV}})^{\mathsf{T}} \boldsymbol{\Phi}_t = \boldsymbol{h}_{_{RV}}^{\mathsf{T}} \mathrm{diag}(\boldsymbol{\Phi}_t) \boldsymbol{h}_{_{UR}}, \tag{6}$$

where $\boldsymbol{\Phi}_t \in \mathbb{C}^{N_R \times 1}$ represents the reflection coefficient matrix operated by the RIS. We have $\boldsymbol{\Phi}_t = \boldsymbol{\beta} e^{j\boldsymbol{\omega}_t}$, where $\boldsymbol{\omega}_t = \left[\omega_1, \ldots, \omega_{_{N_R}}\right]^{\mathsf{T}}$ and $\boldsymbol{\beta} = \left[\beta_1, \ldots, \beta_{_{N_R}}\right]$ with $\beta_i \in [0, 1]$ $\forall i$ represent the phase shift and the amplitude reflection coefficient of the N_R reflecting elements at the RIS [41]. For the ease of practical implementation, the phase shift values are obtained by uniformly spacing the interval $[0, 2\pi)$.

Similarly, let $\boldsymbol{h}_{_{JR}} \in \mathbb{C}^{N_R \times 1}$ be the channel of the direct link JR, we have

$$\boldsymbol{h}_{_{JR}} = \rho_{_{JR}} e^{-j2\pi\tau_{_{JR}} f} \boldsymbol{a}(\boldsymbol{\psi}), \tag{7}$$

where ρ_{JR} and τ_{JR} are the path loss and the corresponding transmission delay, respectively. Therefore, the cascade channel of the link jammer→RIS→UAV, denoted by JRV, can be calculated by

$$\boldsymbol{h}_{J,t} = \left(\boldsymbol{h}_{JR} \odot \boldsymbol{h}_{RV}\right)^{\mathsf{T}} \boldsymbol{\Phi}_t = \boldsymbol{h}_{RV}^{\mathsf{T}} \operatorname{diag}\left(\boldsymbol{\Phi}_t\right) \boldsymbol{h}_{JR}. \quad (8)$$

B. Signal Model

The UE can transmit either narrowband or OFDM pilot signals $x_t \in \mathbb{C}$ with the allocated power P_U at time slot t to perform wireless localization over a slotted transmission duration T. At the same time, the malicious jammer attempts to interfere with the received signal by emitting narrowband jamming signal $s_t \in \mathbb{C}$ with the constant power P_J continuously. Similar to [29, 42], the pilot signal x_t is assumed to be the power constraint, that is, $\mathbb{E}[x_t^2] = P_U$. For the sake of simplicity, x_t is treated to be 1 under the power constraint P_U. Unlike a stochastic jamming model purposefully disrupting or blocking the signal transmission, we assume a smarter jamming strategy by utilizing the effects of multipath propagation to introduce errors in localization measurements. Specifically, the jammer replays the target user's pilot sequences as the jamming pilot [43] to spoof the receiver with complex multipath environments.

1) Narrowband signals: If the UE transmits narrowband pilot signals at a carrier frequency f, the complex signal $\boldsymbol{y}_{N,t} \in \mathbb{C}^{N_R \times 1}$ received by the UAV at time slot t, which comprises the pilot signal and the jamming signal, can be expressed as

$$\begin{aligned}\boldsymbol{y}_{nrw,t} = &\underbrace{\sqrt{P_U}\left(\boldsymbol{h}_{UR} \odot \boldsymbol{h}_{RV}\right)^{\mathsf{T}} \boldsymbol{\Phi}_t x_t}_{pilot\ signal} \\ &+ \underbrace{\sqrt{P_J}\left(\boldsymbol{h}_{JR} \odot \boldsymbol{h}_{RV}\right)^{\mathsf{T}} \boldsymbol{\Phi}_t s_t}_{jamming\ signal} + \boldsymbol{n}_t. \end{aligned} \quad (9)$$

The independent and identically distributed (iid) additive white Gaussian noise $\boldsymbol{n}_t \in \mathbb{C}^{N_R \times 1}$ follows a normal distribution $\mathcal{CN}\left(0, \sigma^2\right)$.

2) OFDM signals: If the UE transmits OFDM pilot signals with N subcarriers, the effect of these delays on the signals can be captured by the subcarrier vector $\boldsymbol{d}\left(\tau_{UV}\right)$ as follows:

$$\begin{aligned}\boldsymbol{d}\left(\tau_{UV}\right) = \Big[&e^{-j2\pi\tau_{UV}(\triangle f - B/2)}, \ldots, \\ &e^{-j2\pi\tau_{UV}(N\triangle f - B/2)}\Big]^{\mathsf{T}}, \end{aligned} \quad (10)$$

where $\triangle f$ denotes the subcarrier spacing, B indicates the bandwith and τ_{UV} represents the transmission delay of URV. Therefore, the received signal $\boldsymbol{y}_{M,t} \in \mathbb{C}^{N_R \times N}$ at the UAV at time slot t is presented as

$$\begin{aligned}\boldsymbol{y}_{ofdm,t} = &\underbrace{\sqrt{E_U}\left(\boldsymbol{h}_{UR} \odot \boldsymbol{h}_{RV}\right)^{\mathsf{T}} \boldsymbol{\Phi}_t \left(\boldsymbol{d}^{\mathsf{T}}\left(\tau_{UV}\right) \odot x_t\right)}_{pilot\ signal} \\ &+ \underbrace{\sqrt{E_J}\left(\boldsymbol{h}_{JR} \odot \boldsymbol{h}_{RV}\right)^{\mathsf{T}} \boldsymbol{\Phi}_t s_t}_{jamming\ signal} + \boldsymbol{n}_t, \end{aligned} \quad (11)$$

where $E_U = P_U/N$ and $E_J = P_J/N$ represents the transmission power allocated to each subcarrier.

IV. Anti-Jamming Localization for Narrowband and OFDM Pilot Signals

The malicious jamming with unknown location and transmission power leads to uncertain wireless environments and therefore increases the difficulty of high-quality positioning services to the UE. In this section, we propose a two-stage anti-jamming localization approach to estimate the UE's position based on either narrowband or OFDM pilot signals in the presence of jamming attacks. The fundamental concept involves estimating the unknown channel and signal information of the jammer at the former stage (**Jamming Estimation**) and subsequently employing this acquired information for anti-jamming localization of the UE at the latter stage (**UE Localization**).

Jamming signal detection is the first step towards performing various anti-jamming strategies, which is beyond the scope of this paper, as some detection algorithms have been reported in the literature [44]. Generally speaking, one or multiple performance metrics, i.e., carrier sensing time and signal-to-noise ratio, are first measured and the existence of jammers is further detected through different techniques, such as machine learning, estimation-based method, and compressed sensing.

A. Jammer Estimation

At this stage, the UE is expected to remain silent so that the UAV can identify the information of the jammer. Derived from Eqs. (7) and (9), the received signals at the UAV can be reformulated and stacked into a vector as below:

$$\underbrace{\begin{bmatrix}\boldsymbol{z}_1 \\ \vdots \\ \boldsymbol{z}_T\end{bmatrix}}_{\boldsymbol{Z} \in \mathbb{C}^{TN_V \times 1}} = \alpha_{JR} \underbrace{\begin{bmatrix}\boldsymbol{\Lambda}_1 \\ \vdots \\ \boldsymbol{\Lambda}_T\end{bmatrix}}_{\boldsymbol{\Lambda} \in \mathbb{C}^{TN_V \times N_R}} \boldsymbol{a}\left(\boldsymbol{\psi}\right) + \underbrace{\begin{bmatrix}\boldsymbol{n}_1 \\ \vdots \\ \boldsymbol{n}_T\end{bmatrix}}_{\boldsymbol{N} \in \mathbb{C}^{TN_V \times 1}}, \quad (12)$$

where $\alpha_{JR} = \sqrt{P_J}\rho_{JR}e^{-j2\pi\tau_{JR}f}$, $\boldsymbol{\Lambda}_t = \boldsymbol{h}_{RV}^{\mathsf{T}} \operatorname{diag}\left(\boldsymbol{\Phi}_t\right)$, and $\boldsymbol{z}_t \in \mathbb{C}^{N_R \times 1}$ is the received jamming signal at time slot t.

Note that the transmission power P_J, channel parameters ρ_{JR}, τ_{JR}, and $\boldsymbol{\psi} = [\psi_{az}, \psi_{el}]^{\mathsf{T}}$ are unknown, it is difficult to obtain all exact information of the jammer at the UAV. Alternatively, the UAV in this stage only needs to measure the key parameters $\boldsymbol{\eta}_J = [\alpha_{JR}, \boldsymbol{\psi}]^{\mathsf{T}}$ of the jammer based on the *maximum likelihood (ML)* function, that is,

$$\begin{aligned}\left[\hat{\alpha}_{JR}, \hat{\boldsymbol{\psi}}\right] &= \arg\max f\left(\boldsymbol{Z} \mid \alpha_{JR}, \boldsymbol{\psi}\right) \\ &= \arg\min \left\|\boldsymbol{Z} - \alpha_{JR}\boldsymbol{\Lambda}\boldsymbol{a}\left(\boldsymbol{\psi}\right)\right\|^2. \end{aligned} \quad (13)$$

Using the *least squares (LS)* criterion, the α_{JR} can be estimated and expressed as a function of $\boldsymbol{\psi}$:

$$\hat{\alpha}_{JR}\left(\boldsymbol{\psi}\right) = \frac{\left(\boldsymbol{\Lambda}\boldsymbol{a}\left(\boldsymbol{\psi}\right)\right)^{\mathsf{H}} \boldsymbol{Z}}{\left\|\boldsymbol{\Lambda}\boldsymbol{a}\left(\boldsymbol{\psi}\right)\right\|^2}. \quad (14)$$

Substituting (14) in (13), the $\hat{\boldsymbol{\psi}}$ can be estimated by

$$\hat{\boldsymbol{\psi}} = \arg\min \left\| \boldsymbol{Z} - \frac{\left(\boldsymbol{\Lambda}\boldsymbol{a}\left(\boldsymbol{\psi}\right)\right)^{\mathsf{H}} \boldsymbol{Z}\left(\boldsymbol{\Lambda}\boldsymbol{a}(\boldsymbol{\psi})\right)}{\left\|\boldsymbol{\Lambda}\boldsymbol{a}\left(\boldsymbol{\psi}\right)\right\|^2} \right\|^2, \quad (15)$$

which is a minimization problem with the complex periodic function $\boldsymbol{a}\left(\boldsymbol{\psi}\right)$ and $\boldsymbol{\psi} = [\psi_{az}, \psi_{el}]^{\mathsf{T}}$.

Furthermore, we introduce the *Jacobi-Anger expansion* [29], which can approximate the complex periodic function as a linear combination of a series of simple sinusoidal functions, simplifying the analysis and computation process to tackle the difficulty of the problem in Eq. (15). Hence, each term in $\boldsymbol{a}(\boldsymbol{\psi})$ for $i = 1, \ldots, N_R$ can be represented as

$$\begin{aligned}[\boldsymbol{a}(\boldsymbol{\psi})]_i &= e^{j\frac{2\pi}{\lambda}\cos\psi_{el}\boldsymbol{u}_{i,h}} e^{j\frac{2\pi}{\lambda}\sin\psi_{az}\sin\psi_{el}\boldsymbol{u}_{i,v}} \\ &\approx e^{j\frac{2\pi}{\lambda}\cos\psi_{el}\boldsymbol{u}_{i,h}} \sum_{n=-N_A}^{N_A} j^n J_n\left(\frac{2\pi}{\lambda}\sin\psi_{el}\boldsymbol{u}_{i,v}\right) e^{jn\left(\frac{\pi}{2}-\psi_{az}\right)},\end{aligned} \tag{16}$$

where $J_n(\cdot)$ denotes the n-th order Bessel function of the first kind. Note that $J_n(\cdot)$ tends to zero as the increase of $|n|$, we omit the terms with $|n| > N_A$ for a given N_A. In this case, the function $[\boldsymbol{a}(\boldsymbol{\psi})]_i$ can be approximated by $[\boldsymbol{a}(\psi_{az}, \psi_{el})]_i \approx \boldsymbol{f}_i^{\mathsf{T}}(\psi_{el})\,\boldsymbol{g}(\psi_{az})$, where

$$[\boldsymbol{f}_i(\psi_{el})]_n = e^{j\frac{2\pi}{\lambda}\cos\psi_{el}\boldsymbol{u}_{i,z}} j^n J_n\left(\frac{2\pi}{\lambda}\sin\psi_{el}\boldsymbol{u}_{i,y}\right), \tag{17}$$

$$[\boldsymbol{g}(\psi_{az})]_n = e^{jn\left(\frac{\pi}{2}-\psi_{az}\right)}, \tag{18}$$

with $n = -N_A, \ldots, N_A$ and $i = 1, \ldots, N_R$. We further have $\boldsymbol{a}(\psi_{az}, \psi_{el}) \approx \boldsymbol{F}^{\mathsf{T}}(\psi_{el})\,\boldsymbol{g}(\psi_{az})$ with $\boldsymbol{F}(\psi_{el}) = [\boldsymbol{f}_1(\psi_{el}), \ldots, \boldsymbol{f}_{N_R}(\psi_{el})] \in \mathbb{C}^{(2N_A+1)\times N_R}$. Then, Eq. (12) can be rewritten as

$$\boldsymbol{Z} = \alpha_{JR}\boldsymbol{\Lambda}\boldsymbol{F}^{\mathsf{T}}(\psi_{el})\,\boldsymbol{g}(\psi_{az}) + \boldsymbol{N}. \tag{19}$$

By introducing $\boldsymbol{v}(\psi_{az}) = \alpha_{JR}\boldsymbol{g}(\psi_{az})$, we have an estimation of $\boldsymbol{v}(\psi_{el})$ according to LS criterion:

$$\hat{\boldsymbol{v}}(\psi_{el}) = \frac{\left(\boldsymbol{\Lambda}\boldsymbol{F}^{\mathsf{T}}(\psi_{el})\right)^{\mathsf{H}}\boldsymbol{Z}}{\left\|\boldsymbol{\Lambda}\boldsymbol{F}^{\mathsf{T}}(\psi_{el})\right\|^2}. \tag{20}$$

In the same way, substituting (20) into (19), the two-dimensional ML estimation problem in (15) can be transformed into two simple one-dimensional problems of solving ψ_{el} and ψ_{az}, respectively. That is, the optimal value of ψ_{el} can be found out through linear search as follows:

$$\hat{\psi}_{el} = \arg\min \left\|\boldsymbol{Z} - \boldsymbol{\Lambda}\boldsymbol{F}^{\mathsf{T}}(\psi_{el})\,\hat{\boldsymbol{v}}(\psi_{el})\right\|^2. \tag{21}$$

Specifically, the measured $\hat{\psi}_{el}$ is considered as the initial point to refine the estimation accuracy by using the *Quasi-Newton method*, which can compensate for the errors introduced by the on-grid effect. And then, the ψ_{az} will be further estimated by taking $\hat{\alpha}_{JR}\left(\psi_{az}, \hat{\psi}_{el}\right)$ into (15):

$$\hat{\psi}_{az} = \arg\min \left\|\boldsymbol{Z} - \hat{\alpha}_{JR}\left(\psi_{az}, \hat{\psi}_{el}\right)\boldsymbol{\Lambda}\boldsymbol{F}^{\mathsf{T}}\left(\hat{\psi}_{el}\right)\boldsymbol{g}(\psi_{az})\right\|^2. \tag{22}$$

Accordingly, the value of ψ_{az} could be further refined by using the Quasi-Newton method as well.

Based on the angle information $\hat{\boldsymbol{\psi}} = \left[\hat{\psi}_{az}, \hat{\psi}_{el}\right]^{\mathsf{T}}$, the α_{JR} can be further calculated according to Eq. (14). The overall description of the proposed jammer estimation approach is shown in Algorithm 1. It can be observed that the computational complexity of Algorithm 1 is dominated by the estimation of $\boldsymbol{v}(\psi_{el})$. According Eq. (20), the estimation of $\boldsymbol{v}(\psi_{el})$ depends on the calculation of $\left(\boldsymbol{\Lambda}\boldsymbol{F}^{\mathsf{T}}(\psi_{el})\right)$ as well as the pseudo-inverse of $\left(\boldsymbol{\Lambda}\boldsymbol{F}^{\mathsf{T}}(\psi_{el})\right)$, that is, $\mathcal{O}\left(TN_VN_R(2N_A+1)\right) + \mathcal{O}\left(TN_V(2N_A+1)^2\right)$. Then, the linear search with discretized grids of size K_1 is applied to achieve the initial point of ψ_{el} in Eq. (21) and the Quasi-Newton method with the number of iterations K_2 is utilized to refined and updated ψ_{el}. Therefore, the overall computational complexity of Algorithm 1 is given by $\mathcal{O}\left(TN_VN_R(2N_A+1)(K_1+K_2)\right)$ plus $\mathcal{O}\left(TN_V(2N_A+1)^2(K_1+K_2)\right)$ and further simplified as $\mathcal{O}\left(TN_V(K_1+K_2)(2N_A+1)\max\{N_R, 2N_A+1\}\right)$.

Algorithm 1: Jammer Estimation (**Former Stage**)

1. **Initialization:** Phase shift profile $\boldsymbol{\omega} = \{\boldsymbol{\omega}_t\}$, AoA of the reflected link RV $\boldsymbol{\varphi}$.
2. Estimate the initial point of $\hat{\psi}_{el}$ by linear search according to Eq. (21).
3. Refine and update $\hat{\psi}_{el}$ by the Quasi-Newton method.
4. Estimate the initial point of $\hat{\psi}_{az}$ by linear search according to Eq. (22).
5. Refine and update $\hat{\psi}_{az}$ by the Quasi-Newton method.
6. Based on $\hat{\boldsymbol{\psi}} = \left[\hat{\psi}_{az}, \hat{\psi}_{el}\right]^{\mathsf{T}}$, calculate $\hat{\alpha}_{JR}$ according to Eq. (14).
7. **Output:** The jammer estimation results $\hat{\boldsymbol{\eta}}_J = \left[\hat{\alpha}_{JR}, \hat{\boldsymbol{\psi}}\right]^{\mathsf{T}}$.

B. Narrowband UE Localization

We first analyze the UE transmitting narrowband pilot signals at this stage. Derived from Eqs. (1) and (9), the complex received signals at the UAV can be vectorized into $\boldsymbol{Y}_{nrw} \in \mathbb{C}^{N_VT\times 1}$ as follows:

$$\boldsymbol{Y}_{nrw} = \boldsymbol{\Lambda}\boldsymbol{A}\boldsymbol{\alpha}_{nrw} + \boldsymbol{N}, \tag{23}$$

where $\boldsymbol{\Lambda} = \boldsymbol{h}_{RV}^{\mathsf{T}}\,\mathrm{diag}(\boldsymbol{\Phi})$, $\boldsymbol{A} = \left[\boldsymbol{a}(\boldsymbol{\theta}) \quad \boldsymbol{a}(\boldsymbol{\psi})\right]$ and $\boldsymbol{\alpha}_{nrw} = \left[\alpha_{UR} \quad \alpha_{JR}\right]^{\mathsf{T}}$ with $\alpha_{UR} = \sqrt{P_U}\rho_{UR}e^{-j2\pi\tau_{UR}f}$. Note that the UE's transmission power P_U and the jammer's key information $\boldsymbol{\eta}_J = [\alpha_{JR}, \boldsymbol{\psi}]^{\mathsf{T}}$ are known, the target at this stage is to estimate $\boldsymbol{\eta}_U = [\tau_{UR}, \boldsymbol{\theta}]^{\mathsf{T}}$.

Given $\hat{\alpha}_{JR}$ and $\hat{\boldsymbol{\psi}}$, the ML estimation problem is formulated as

$$\left[\hat{\boldsymbol{\alpha}}_{nrw}, \hat{\boldsymbol{\theta}}\right] = \arg\min \left\|\boldsymbol{Y}_{nrw} - \boldsymbol{\Lambda}\boldsymbol{A}\boldsymbol{\alpha}_{nrw}\right\|^2. \tag{24}$$

Using the least squares (LS) criterion, $\boldsymbol{\alpha}_{nrw}$ can be estimated and expressed as a function of $\boldsymbol{\theta}$:

$$\hat{\boldsymbol{\alpha}}_{nrw}(\boldsymbol{\theta}) = \frac{\left(\boldsymbol{\Lambda}\boldsymbol{A}(\boldsymbol{\theta})\right)^{\mathsf{H}}\boldsymbol{Y}_{nrw}}{\left\|\boldsymbol{\Lambda}\boldsymbol{A}(\boldsymbol{\theta})\right\|^2}. \tag{25}$$

Substituting (25) in (24), the $\boldsymbol{\theta}$ can be estimated by

$$\hat{\boldsymbol{\theta}} = \arg\min \left\|\boldsymbol{Y}_{nrw} - \frac{\left(\boldsymbol{\Lambda}\boldsymbol{A}(\boldsymbol{\theta})\right)^{\mathsf{H}}\boldsymbol{Y}_{nrw}\left(\boldsymbol{\Lambda}\boldsymbol{A}(\boldsymbol{\theta})\right)}{\left\|\boldsymbol{\Lambda}\boldsymbol{A}(\boldsymbol{\theta})\right\|^2}\right\|^2. \tag{26}$$

Similar to the derivations in Section IV-A, we have $\boldsymbol{A} \approx$

$\boldsymbol{F}_{nrw}^{\mathsf{T}}\boldsymbol{G}_{nrw}$ based on the Jacobi-Anger expansion, where

$$\boldsymbol{F}_{nrw} = \begin{bmatrix} \boldsymbol{F}(\theta_{el}) \\ \boldsymbol{F}(\psi_{el}) \end{bmatrix} \in \mathbb{C}^{(4N_A+2)\times N_R}, \tag{27}$$

$$\boldsymbol{G}_{nrw} = \begin{bmatrix} \boldsymbol{g}(\theta_{az}) & \boldsymbol{0}_{(2N_A+1)\times 1} \\ \boldsymbol{0}_{(2N_A+1)\times 1} & \boldsymbol{g}(\psi_{az}) \end{bmatrix} \in \mathbb{C}^{(4N_A+2)\times 2}. \tag{28}$$

Then, Eq. (23) can be rewritten as

$$\boldsymbol{Y}_{nrw} = \boldsymbol{\Lambda}\boldsymbol{F}_{nrw}^{\mathsf{T}}\boldsymbol{G}_{nrw}\hat{\boldsymbol{\alpha}}_{nrw}(\boldsymbol{\theta}) + \boldsymbol{N}. \tag{29}$$

We introduce $\boldsymbol{v}_{nrw} = \boldsymbol{G}_{nrw}\hat{\boldsymbol{\alpha}}_{nrw}(\boldsymbol{\theta})$ and transform it by LS estimation, that is, $\hat{\boldsymbol{v}}_{nrw} = \left(\boldsymbol{\Lambda}\boldsymbol{F}_{nrw}^{\mathsf{T}}\right)^{\mathsf{H}}\boldsymbol{Y}_{nrw}/\left\|\boldsymbol{\Lambda}\boldsymbol{F}_{nrw}^{\mathsf{T}}\right\|^2$. Currently, the original problem in Eq. (26) can be split into two low-complexity ML estimators

$$\hat{\theta}_{el} = \arg\min \left\|\boldsymbol{Y}_{nrw} - \boldsymbol{\Lambda}\boldsymbol{F}_{nrw}^{\mathsf{T}}\hat{\boldsymbol{v}}_{nrw}\right\|^2, \tag{30}$$

$$\hat{\theta}_{az} = \arg\min \left\|\boldsymbol{Y}_{nrw} - \boldsymbol{\Lambda}\hat{\boldsymbol{F}}_{nrw}^{\mathsf{T}}\boldsymbol{G}_{nrw}\hat{\boldsymbol{\alpha}}_{nrw}\right\|^2, \tag{31}$$

which can be separately solved by linear search and further refined by the Quasi-Newton method.

Note that $\rho_{UR} = \sqrt{g_0}/\left\|\boldsymbol{p}_U - \boldsymbol{p}_R\right\|$ is the free-space path loss, where g_0 is the path loss at a reference distance $d_0 = 1$m. The propagation distance between the UE and the RIS $\left\|\boldsymbol{p}_U - \boldsymbol{p}_R\right\|$ can be estimated by $c \cdot \tau_{UR}$, where c is the speed of light. To focus on the anti-jamming localization, we share a similar idea of [45] and assume that there is prior knowledge of g_0 in the user's region because the perfect CSI can be obtained by various existing channel estimation methods [46, 47] and remain unchanged for a relatively long time. In this way, $\boldsymbol{\alpha}_{nrw}$ formulated in Eq. (23) can be viewed as a function of transmission delay τ_{UR}, where $\alpha_{UR} = \sqrt{P_U}[\sqrt{g_0}/(c\cdot\tau_{UR})]e^{-j2\pi\tau_{UR}f}$. Finally, the $\hat{\tau}_{UR}$ is calculated by

$$\hat{\tau}_{UR} = \arg\min \left\|\boldsymbol{Y}_{nrw} - \boldsymbol{\Lambda}\boldsymbol{F}_{nrw}^{\mathsf{T}}\hat{\boldsymbol{G}}_{nrw}\boldsymbol{\alpha}_{nrw}(\tau_{UR})\right\|^2. \tag{32}$$

C. OFDM UE Localization

The UE localization based on OFDM pilot signals is slightly different from narrowband signals due to the subcarrier vector $\boldsymbol{d}(\tau_{UV})$. Similar to the derivations in Section IV-B, derived from Eq. (11), the complex signal can be vectorized into $\boldsymbol{Y}_{ofdm} \in \mathbb{C}^{N_V T\times N}$ as follows:

$$\boldsymbol{Y}_{ofdm} = \boldsymbol{\Lambda}\boldsymbol{A}\boldsymbol{\alpha}_{ofdm} + \boldsymbol{N}, \tag{33}$$

where $\boldsymbol{\alpha}_{ofdm} = \begin{bmatrix}\alpha_{UR}\boldsymbol{d}(\tau_{UV}) & \boldsymbol{\alpha}_{JR}\boldsymbol{1}_N\end{bmatrix}^{\mathsf{T}} \in \mathbb{C}^{2\times N}$. The ML estimation problem is formulated as

$$\left[\hat{\boldsymbol{\alpha}}_{ofdm}, \hat{\boldsymbol{\theta}}\right] = \arg\min \left\|\boldsymbol{Y}_{ofdm} - \boldsymbol{\Lambda}\boldsymbol{A}\boldsymbol{\alpha}_{ofdm}\right\|^2. \tag{34}$$

The calculation of $\hat{\boldsymbol{\theta}}$ is the same as the ML estimators in Eqs. (30) and (31).

Given the measured $\hat{\boldsymbol{\theta}}$, the $\hat{\boldsymbol{\alpha}}_{ofdm}$ can be solved as a function of $\boldsymbol{\theta}$ using the LS criterion:

$$\hat{\boldsymbol{\alpha}}_{ofdm}(\boldsymbol{\theta}) = \frac{\left(\boldsymbol{\Lambda}\boldsymbol{A}(\boldsymbol{\theta})\right)^{\mathsf{H}}\boldsymbol{Y}_{ofdm}}{\left\|\boldsymbol{\Lambda}\boldsymbol{A}(\boldsymbol{\theta})\right\|^2}. \tag{35}$$

Furthermore, it could be observed that only the first row of $\boldsymbol{\alpha}_{ofdm}$ is related to the delays. Substituting $[\boldsymbol{\alpha}_{ofdm}]_{1,:} = \alpha_{UR}\boldsymbol{d}^{\mathsf{T}}(\tau_{UV})$ into Eq. (35), we have

$$\hat{\boldsymbol{\alpha}}_{UR} = \frac{\boldsymbol{d}(\tau_{UV})^{\mathsf{H}}\left[\hat{\boldsymbol{\alpha}}_{ofdm}(\hat{\boldsymbol{\theta}})\right]_{1,:}^{\mathsf{T}}}{\boldsymbol{d}(\tau_{UV})^{\mathsf{H}}\boldsymbol{d}(\tau_{UV})}. \tag{36}$$

Combining Eqs. (35) and (36), τ_{UV} can be calculated by

$$\hat{\tau}_{UV} = \arg\min \left\| \left[\hat{\boldsymbol{\alpha}}_{ofdm}(\hat{\boldsymbol{\theta}})\right]_{1,:}^{\mathsf{T}} - \hat{\boldsymbol{\alpha}}_{UR}\boldsymbol{d}(\tau_{UV})\right\|^2. \tag{37}$$

Then, $\hat{\tau}_{UR}$ can be estimated by $\hat{\tau}_{UR} = \hat{\tau}_{UV} - \tau_{RV}$.

The overall description of the proposed user localization approach suitable for both narrowband and OFDM pilot signals is shown in Algorithm 2. Given the measured $\hat{\boldsymbol{\eta}}_U = \left[\hat{\tau}_{UR}, \hat{\boldsymbol{\theta}}\right]^{\mathsf{T}}$, the UE's position $\boldsymbol{p}_U$ can be computed by

$$\hat{\boldsymbol{p}}_U = \boldsymbol{p}_R + c\cdot\hat{\tau}_{UR}\left[\sin\hat{\theta}_{el}\cos\hat{\theta}_{az}, \sin\hat{\theta}_{el}\sin\hat{\theta}_{az}, \cos\hat{\theta}_{el}\right]^{\mathsf{T}}. \tag{38}$$

Compared with narrowband-based localization, we can find out that the proposed OFDM-based localization doesn't require any prior knowledge of the path fading factor g_0 because the CSI can be estimated by solving $\hat{\boldsymbol{\alpha}}_{ofdm}$ in Eq. (35). The computational complexity of Algorithm 2 primarily depends on the estimation of $\boldsymbol{v}_{nrw}$. Similar to the complexity analysis in Algorithm 1, the computational complexity of Algorithm 2 is given by $\mathcal{O}\left(TN_V(K_1+K_2)(2N_A+1)\max\{N_R, 4N_A+2\}\right)$ for either narrowband or OFDM pilot signals.

So far, the two-stage anti-jamming localization approach has been introduced to localize the user's position by eliminating the jamming signal. Specifically, once the unknown channel and signal information of the jamming have been estimated

Algorithm 2: UE Localization (**Latter Stage**)

Initialization: RIS' position $\boldsymbol{p}_R$ and phase shift profile $\boldsymbol{\omega} = \{\boldsymbol{\omega}_t\}$, UE's transmission power P_U, AoA of the reflected link RV $\boldsymbol{\varphi}$, the measured jammer information $\hat{\boldsymbol{\eta}}_J = \left[\hat{\alpha}_{JR}, \hat{\boldsymbol{\psi}}\right]^{\mathsf{T}}$.
Estimate the initial point of $\hat{\theta}_{el}$ by linear search according to Eq. (30).
Refine and update $\hat{\theta}_{el}$ by the Quasi-Newton method.
Estimate the initial point of $\hat{\theta}_{az}$ by linear search according to Eq. (31).
Refine and update $\hat{\theta}_{az}$ by the Quasi-Newton method.
switch *Type of pilot signals* **do**
  case *Narrowband* **do**
    Based on $\hat{\boldsymbol{\theta}} = \left[\hat{\theta}_{az}, \hat{\theta}_{el}\right]^{\mathsf{T}}$, calculate $\hat{\tau}_{UR}$ according to Eq. (32).
  end
  case *OFDM* **do**
    Based on $\hat{\boldsymbol{\theta}} = \left[\hat{\theta}_{az}, \hat{\theta}_{el}\right]^{\mathsf{T}}$, calculate $\hat{\boldsymbol{\alpha}}_{ofdm}(\boldsymbol{\theta})$ according to Eq. (35).
    Based on $\hat{\boldsymbol{\alpha}}_{ofdm}(\boldsymbol{\theta})$, calculate $\hat{\tau}_{UR}$ according to Eq. (37).
  end
end
Based on $\hat{\boldsymbol{\eta}}_U = \left[\hat{\tau}_{UR}, \hat{\boldsymbol{\theta}}\right]^{\mathsf{T}}$, calculate $\hat{\boldsymbol{p}}_U$ according to Eq. (38).
Output: The UE estimation results $\hat{\boldsymbol{\eta}}_U$ and $\hat{\boldsymbol{p}}_U$.

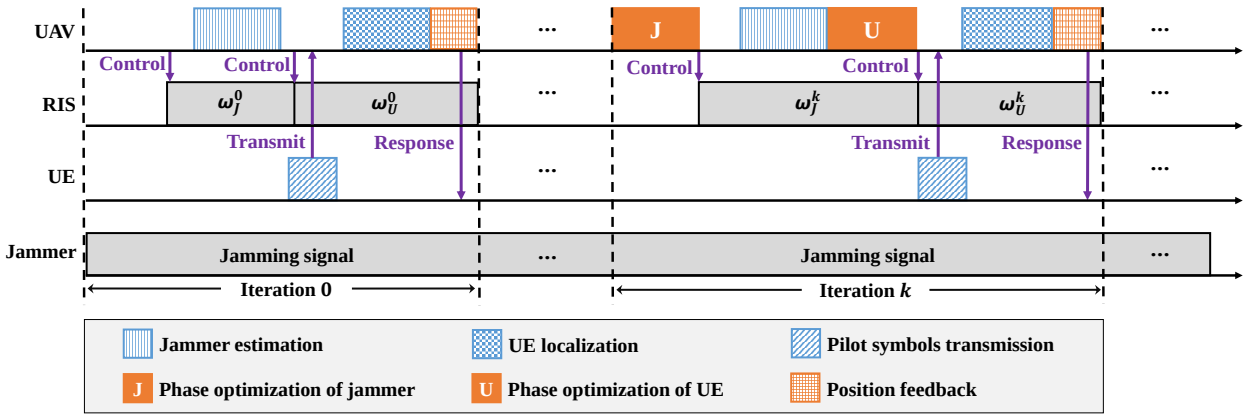


Fig. 2. Phase optimization process for the anti-jamming localization.

by Algorithm 1, the UE's position can be further measured by Algorithm 2 according to the type of pilot signals. It should be noted that both Algorithm 1 and Algorithm 2 are one-shot algorithms but their performance is limited to the transmission duration T. A larger transmission time means more training overhead but less estimation error.

V. RIS Phase Optimization

A two-stage anti-jamming localization approach has been proposed to estimate the UE's position. However, to cope with the estimation error of the unknown channel and signal information of the jammer, how to fully utilize the potential of the RIS to further enhance localization accuracy is still a challenging issue. In this section, we improve the estimation accuracy by optimizing the phase shifts of the RIS during the localization process. The proposed RIS phase optimization process works in an **iterative manner** based on the historical estimation results, as shown in Fig. 2. In each iteration, two-phase optimization stages are carried out to iteratively update the RIS phase shift profiles before the jamming estimation and UE localization stages, respectively. One is to maximize the reflected channel gain of the link RV, and the other aims to enhance the received power of the pilot signal transmitted by the UE and meanwhile mitigate the malicious interference caused by the jammer.

A. Phase Design for Jammer Estimation

Note that the estimation error of the jammer's key information will affect the accuracy of the anti-jamming UE localization result. In the k-th iteration of the jammer estimation stage, derived from Eqs. (2) (7), and (9), we would like to find a RIS phase shift profile $\boldsymbol{\omega}_{J,t}^k = \left[\omega_{J,t,1}^k, \quad \ldots \quad, \omega_{J,t,N_R}^k\right]^{\mathsf{T}}$ to maximize the channel gain of the propagation path JRV at time slot t:

$$\max_{\boldsymbol{\omega}_{J,t}^k} \left\| \boldsymbol{h}_{RV}^{\mathsf{T}} \operatorname{diag}\left(\boldsymbol{\Phi}_{J,t}^k\right) \boldsymbol{h}_{JR} \right\| = \Big\| \rho_{JR}\rho_{RV} e^{-j2\pi(\tau_{JR}+\tau_{RV})f} \boldsymbol{b}\left(\boldsymbol{\phi}\right) \boldsymbol{a}^{\mathsf{T}}\left(\boldsymbol{\varphi}\right) \operatorname{diag}\left(\boldsymbol{\Phi}_{J,t}^k\right) \boldsymbol{a}\left(\boldsymbol{\psi}\right) \Big\|, \quad (39)$$

where $\boldsymbol{\Phi}_{J,t}^k = \boldsymbol{\beta} e^{j\boldsymbol{\omega}_{J,t}^k}$. We observe that $\boldsymbol{a}\left(\boldsymbol{\psi}\right)$ is defined by Eq. (3) and only the term $\boldsymbol{a}^{\mathsf{T}}\left(\boldsymbol{\varphi}\right) \operatorname{diag}\left(\boldsymbol{\Phi}_{J,t}^k\right) \boldsymbol{a}\left(\boldsymbol{\psi}\right)$ are influenced by $\boldsymbol{\Phi}_{J,t}^k$. By ignoring these terms that do not depend on $\boldsymbol{\Phi}_{J,t}^k$, the problem in Eq. (39) is equivalent to

$$\begin{aligned} &\max_{\boldsymbol{\omega}_{J,t}^k} \left\| \boldsymbol{a}^{\mathsf{T}}\left(\boldsymbol{\varphi}\right) \operatorname{diag}\left(\boldsymbol{\Phi}_{J,t}^k\right) \boldsymbol{a}\left(\boldsymbol{\psi}\right) \right\| \\ &= \left| \sum_{i=1}^{N_R} \beta_i e^{j\omega_{J,t,i}^k} e^{-j[\boldsymbol{w}(\boldsymbol{\psi})+\boldsymbol{w}(\boldsymbol{\varphi})]\boldsymbol{u}_i} \right| \\ &\le \sum_{i=1}^{N_R} \beta_i \left| e^{j\omega_{J,t,i}^k - j[\boldsymbol{w}(\boldsymbol{\psi})+\boldsymbol{w}(\boldsymbol{\varphi})]\boldsymbol{u}_i} \right|. \end{aligned} \quad (40)$$

Therefore, the maximum value of the problem in Eq. (40) is achieved when the phase shifts of the i-th RIS element $\hat{\omega}_{J,i}^k$ satisfy

$$\hat{\omega}_{J,t,i}^k = \hat{\omega}_{J,i}^k = \left[\boldsymbol{w}\left(\hat{\boldsymbol{\psi}}^{k-1}\right) + \boldsymbol{w}\left(\boldsymbol{\varphi}\right)\right] \boldsymbol{u}_i, \quad \forall t \quad (41)$$

where $\boldsymbol{\varphi}$ is known and $\hat{\boldsymbol{\psi}}^{k-1}$ has been estimated in the last iteration.

B. Phase Design for Narrowband UE Localization

In the k-th iteration of the UE localization stage, derived from Eq. (9), we would like to find a RIS phase shift profile $\boldsymbol{\omega}_{U,t}^k = \left[\omega_{U,t,1}^k, \quad \ldots \quad, \omega_{J,t,N_R}^k\right]^{\mathsf{T}}$ to strengthen the received power of the narrowband pilot signal and weaken the jamming signal at time slot t:

$$\max_{\boldsymbol{\omega}_{U,t}^k} \left\| \sqrt{P_U} \left(\boldsymbol{h}_{UR} \odot \boldsymbol{h}_{RV}\right)^{\mathsf{T}} \boldsymbol{\Phi}_{U,t}^k - \sqrt{P_J} \left(\boldsymbol{h}_{JR} \odot \boldsymbol{h}_{RV}\right)^{\mathsf{T}} \boldsymbol{\Phi}_{U,t}^k \right\|. \quad (42)$$

Similar to the derivations in Section V-A, we can simplify the problem in Eq. (42) as

$$\begin{aligned} &\max_{\boldsymbol{\omega}_{U,t}^k} \left\| \left(\sqrt{P_U}\boldsymbol{h}_{UR} \odot \boldsymbol{a}\left(\boldsymbol{\varphi}\right) - \sqrt{P_J}\boldsymbol{h}_{JR} \odot \boldsymbol{a}\left(\boldsymbol{\varphi}\right)\right)^{\mathsf{T}} \boldsymbol{\Phi}_{U,t}^k \right\| \\ &= \left\| \left(\left(\boldsymbol{S}_U - \boldsymbol{S}_J\right) \odot \boldsymbol{a}\left(\boldsymbol{\varphi}\right)\right)^{\mathsf{T}} \boldsymbol{\Phi}_{U,t}^k \right\| \\ &= \left| \sum_{i=1}^{N_R} \beta_i \left|\boldsymbol{S}_{U,i} - \boldsymbol{S}_{J,i}\right| \cdot e^{j\angle\left(\boldsymbol{S}_{U,i} - \boldsymbol{S}_{J,i}\right)} e^{j\omega_{U,t,i}^k} e^{-j\boldsymbol{w}(\boldsymbol{\varphi})\boldsymbol{u}_i} \right| \\ &\le \sum_{i=1}^{N_R} \beta_i \left|\boldsymbol{S}_{U,i} - \boldsymbol{S}_{J,i}\right| \cdot \left| e^{j\omega_{U,t,i}^k - j\boldsymbol{w}(\boldsymbol{\varphi})\boldsymbol{u}_i + j\angle\left(\boldsymbol{S}_{U,i} - \boldsymbol{S}_{J,i}\right)} \right|, \end{aligned} \quad (43)$$

where $\boldsymbol{S}_U = \sqrt{P_U}\boldsymbol{h}_{UR}$ and $\boldsymbol{S}_J = \sqrt{P_J}\boldsymbol{h}_{JR}$. Therefore, the optimal phase shifts of the i-th RIS element $\omega_{U,i}^k$ can be written in close-form as

$$\hat{\omega}_{U,t,i}^k = \hat{\omega}_{U,i}^k = \boldsymbol{w}(\boldsymbol{\varphi})\boldsymbol{u}_i - \angle(\boldsymbol{S}_{U,i} - \boldsymbol{S}_{J,i}), \quad \forall t \tag{44}$$

where $\boldsymbol{\varphi}$ is known. The $\boldsymbol{S}_U$ and $\boldsymbol{S}_J$ can be calculated using $\hat{\boldsymbol{\eta}}_U^{k-1}$ and $\hat{\boldsymbol{\eta}}_J^k$.

C. Phase Design for OFDM UE Localization

Differing from the analysis of the narrowband pilot signal, the influence of the OFDM subcarriers should be taken into consideration. For the OFDM pilot signals, in the k-th iteration, the phase optimization problem for the anti-jamming UE localization at time slot t can be written as

$$\begin{aligned}\max_{\boldsymbol{\omega}_{U,t}^k} \Big\| & \sqrt{E_U}\boldsymbol{h}_{RV}^{\mathsf{T}}\operatorname{diag}\left(\boldsymbol{\Phi}_{U,t}^k\right)\boldsymbol{h}_{UR}\boldsymbol{d}^{\mathsf{T}}(\tau_{UV}) \\ & -\sqrt{E_J}\boldsymbol{h}_{RV}^{\mathsf{T}}\operatorname{diag}\left(\boldsymbol{\Phi}_{U,t}^k\right)\boldsymbol{h}_{JR}\mathbf{1}_N^{\mathsf{T}}\Big\|\end{aligned} \tag{45}$$

Similarly, the problem in (45) is equivalent to

$$\begin{aligned}&\max_{\boldsymbol{\omega}_{U,t}^k} \Big\|\boldsymbol{a}(\boldsymbol{\varphi})\operatorname{diag}\left(\boldsymbol{\Phi}_{U,t}^k\right)\cdot \\ &\qquad \left(\sqrt{E_U}\boldsymbol{h}_{UR}\boldsymbol{d}^{\mathsf{T}}(\tau_{UV}) - \sqrt{E_J}\boldsymbol{h}_{JR}\mathbf{1}_N^{\mathsf{T}}\right)\Big\| \qquad (46)\\ &= \left\|\boldsymbol{a}(\boldsymbol{\varphi})\operatorname{diag}\left(\boldsymbol{\Phi}_{U,t}^k\right)\cdot\left(\boldsymbol{L}_U d^{\mathsf{T}}(\tau_{UV}) - \boldsymbol{L}_J\mathbf{1}_N^{\mathsf{T}}\right)\right\| \\ &= \left|\sum_{i=1}^{N_R}\sum_{n=1}^{N}\beta_i\left|\boldsymbol{L}_{U,i}e^{j\Psi_n} - \boldsymbol{L}_{J,i}\right|\cdot\right. \\ &\qquad \left. e^{j\angle\left(\boldsymbol{L}_{U,i}e^{j\Psi_n}-\boldsymbol{L}_{J,i}\right)}e^{-j\boldsymbol{w}(\boldsymbol{\varphi})\boldsymbol{u}_i}e^{j\omega_{U,t,i}^k}\right| \\ &= \left|\sum_{i=1}^{N_R}\beta_i|D_i|\,e^{j\angle D_i}e^{-j\boldsymbol{w}(\boldsymbol{\varphi})\boldsymbol{u}_i}e^{j\omega_{U,t,i}^k}\right| \\ &\le \sum_{i=1}^{N_R}\beta_i|D_i|\cdot\left|e^{j\omega_{U,t,i}^k - j\boldsymbol{w}(\boldsymbol{\varphi})\boldsymbol{u}_i + j\angle D_i}\right|,\end{aligned}$$

where $\Psi_n = -2\pi\tau_{UV}(n\triangle f - B/2)$, $\boldsymbol{L}_U = \sqrt{E_U}\boldsymbol{h}_{UR}$, $\boldsymbol{L}_J = \sqrt{E_J}\boldsymbol{h}_{JR}$ and $D_i = \sum_{n=1}^{N}\left|\boldsymbol{L}_{U,i}e^{j\Psi_n} - \boldsymbol{L}_{J,i}\right| e^{j\angle\left(\boldsymbol{L}_{U,i}e^{j\Psi_n}-\boldsymbol{L}_{J,i}\right)}$. Then, the optimal phase shifts of the i-th RIS element will be

$$\begin{aligned}\hat{\omega}_{U,t,i}^k &= \hat{\omega}_{U,i}^k \\ &= \boldsymbol{w}(\boldsymbol{\varphi})\boldsymbol{u}_i \\ &\quad - \angle\left(\sum_{n=1}^{N}\left|\boldsymbol{L}_{U,i}e^{j\Psi_n} - \boldsymbol{L}_{J,i}\right| e^{j\angle\left(\boldsymbol{L}_{U,i}e^{j\Psi_n}-\boldsymbol{L}_{J,i}\right)}\right),\end{aligned} \tag{47}$$

where $\boldsymbol{\varphi}$ is known. The $\boldsymbol{L}_U$ and $\boldsymbol{L}_J$ can be calculated using $\hat{\boldsymbol{\eta}}_U^{k-1}$ and $\hat{\boldsymbol{\eta}}_J^k$.

The overall description of the proposed phase optimization for anti-jamming localization (POAJL) is provided in Algorithm 3. More specifically, at the initial stage, i.e., $k = 0$, the two-stage anti-jamming localization consisting of Algorithm 1 and Algorithm 2 is leveraged to obtain the initial parameters of both the jammer and the UE with random RIS phase shift profiles $\hat{\omega}_J^0$ and $\hat{\omega}_U^0$. In the k-th iteration, the UAV first optimizes the RIS phase shift profile $\hat{\omega}_J^k$ according to the last iteration information and then performs the jamming estimation in Algorithm 1 based on the optimal phases. After the jamming estimation stage, the RIS phase shift profile for the UE $\hat{\omega}_U^k$ is further improved according to the type of pilot signals. At the end of pilot symbols transmission, the UE localization is executed by Algorithm 2. The measured position of the UE $\hat{\boldsymbol{p}}_U^k$ will be replied at the end of each iteration and the localization process terminates when the value of $\hat{\boldsymbol{p}}_U^k$ converges. Note that Algorithm 3 works in an iterative manner, its computational complexity is not only dominated by the cost of the jammer estimation and UE localization but also affected by the number of iterations. We assume that Algorithm 3 stops in K_P iterations, then the overall computational complexity will be $\mathcal{O}\left(TN_V(K_1+K_2)K_P(2N_A+1)\max\{N_R, 2N_A+1\}\right)$ plus $\mathcal{O}\left(TN_V(K_1+K_2)K_P(4N_A+2)\max\{N_R, 2N_A+1\}\right)$ and further simplified as $\mathcal{O}(TN_V(K_1+K_2)K_P(2N_A+1)\max\{N_R, 4N_A+2\})$.

Algorithm 3: Phase Optimization for Anti-Jamming Localization (**POAJL**)

Initialization: RIS' position $\boldsymbol{p}_R$ and phase shift profiles $\hat{\omega}_J^0 = \{\hat{\omega}_{J,i}^0\}$ and $\hat{\omega}_U^0 = \{\hat{\omega}_{U,i}^0\}$, UE's transmission power P_U, AoA of the reflected link RV $\boldsymbol{\varphi}$.
Obtain the initial $\hat{\boldsymbol{\eta}}_J^0 = \left[\hat{\alpha}_{JR}^0, \hat{\boldsymbol{\psi}}^0\right]^{\mathsf{T}}$ by Algorithm 1.
The UE transmits pilot symbols.
Obtain the initial $\hat{\boldsymbol{\eta}}_U^0 = \left[\hat{\tau}_{UR}^0, \hat{\boldsymbol{\theta}}^0\right]^{\mathsf{T}}$ and $\hat{\boldsymbol{p}}_U^0$ by Algorithm 2.
Reply $\hat{\boldsymbol{p}}_U^0$ to the UE.
while $\hat{\boldsymbol{p}}_U^k$ *does not converge* **do**
  Based on $\hat{\boldsymbol{\psi}}^{k-1}$, obtain the optimal phase shift profile $\hat{\omega}_J^k = \{\hat{\omega}_{J,i}^k\}$ according to Eq. (41).
  Control the RIS phase shifts with $\hat{\omega}_J^k$ and then update $\hat{\boldsymbol{\eta}}_J^k$ by Algorithm 1.
  switch *Type of pilot signals* **do**
    case *Narrowband* **do**
      Based on $\hat{\boldsymbol{\eta}}_U^{k-1}$ and $\hat{\boldsymbol{\eta}}_J^k$, obtain the optimal phase profile $\hat{\omega}_U^k = \{\hat{\omega}_{U,i}^k\}$ according to Eq. (44).
    end
    case *OFDM* **do**
      Based on $\hat{\boldsymbol{\eta}}_U^{k-1}$ and $\hat{\boldsymbol{\eta}}_J^k$, obtain the optimal phase profile $\hat{\omega}_U^k = \{\hat{\omega}_{U,i}^k\}$ according to Eq. (47).
    end
  end
  Control the RIS phase shifts with $\hat{\omega}_U^k$ and then the UE transmits pilot symbols.
  Update $\hat{\boldsymbol{\eta}}_U^k$ and $\hat{\boldsymbol{p}}_U^k$ by Algorithm 2.
  Reply $\hat{\boldsymbol{p}}_U^k$ to the UE.
end
Output: UE's position $\hat{\boldsymbol{p}}_U^k$, the optimal RIS phase shift profiles $\hat{\omega}_J^k$ and $\hat{\omega}_U^k$.

VI. Evaluations

In this section, we evaluate the performance of the proposed anti-jamming localization framework through extensive simulations as shown in Fig. 3. In our considered scenario, the RIS is located at $(0, 0, 15)^{\mathsf{T}}$ in meter (m), the hovering UAV equipped with 2×2 antennas is randomly and uniformly

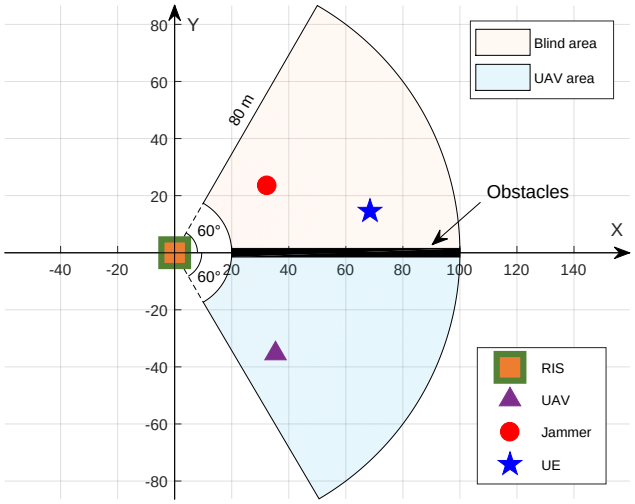
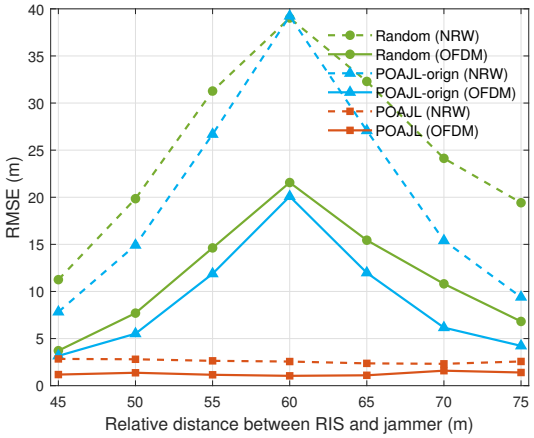


Fig. 3. Simulation scenario for anti-jamming localization.

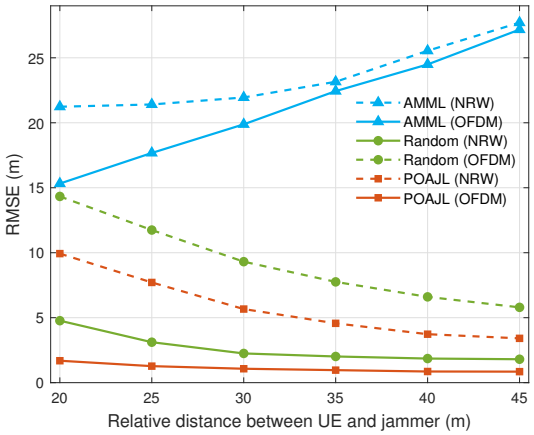
TABLE I
LIST OF KEY SIMULATION PARAMETERS

Parameter	Value
Height of UAV and RIS, $\{z_V, z_R\}$	20m, 15m
Number of RIS elements, N_R	$36\,(6\times 6)$ or $64\,(8\times 8)$
Number of UAV antennas, N_V	$4\,(2\times 2)$
Approximation factor of Jacobi-Anger expansion, N_A	25
Transmission power, $\{P_U, P_J\}$	10dBm [42]
Carrier frequency, f	28GHz
Wavelength, λ	1cm
Light speed, c	3×10^8m/s
Path loss at 1m, g_0	-31dBm [13]
Noise figure, n_f	3dB [9]
Power spectral density (PSD) of noise, N_0	-174dBm/Hz
Narrowband pilot signal:	
Noise variance $\sigma^2 = n_f N_0 B$	
i) Bandwidth, B	12×240kHz
OFDM pilot signal:	
Noise variance per subcarrier $\sigma^2 = n_f N_0 \triangle f$	
i) Subcarrier space, $\triangle f$	240kHz
ii) Number of subcarriers, N	12 [9]

distributed within the semi-annular region, with height 20 m highlighted in light blue (called UAV area), covering the sector with central angle from 0° to 60° between the inner and outer circles with the radius of 20m and 100m, respectively. Similarly, the single-antenna UE and the single-antenna jammer are randomly and uniformly distributed within the blind area highlighted in light orange. Specifically, we assume that the distance between the UE and the jammer should be within $[20, 50]$m to ensure that the jammer can remain hidden and not be captured. The RIS is empowered for anti-jamming localization due to the disconnection of the direct communication link between the UE and the UAV, e.g., blocked by the obstacles marked in black. Key parameters are summarized in Table I. We assume unit-amplitude RIS element response for simplicity, i.e., the amplitude reflection coefficient $\beta_i = 1\ \forall i$ [48]. We set $N_A = 25$ for Jacobi-Anger expansion in Eq. (16) according to [29]. To quickly obtain an initial position of the UE and meanwhile decrease the training



(a) Relative distance between RIS and jammer



(b) Relative distance between UE and jammer

Fig. 4. Localization performance versus the jammer's location: $N_R = 64$.

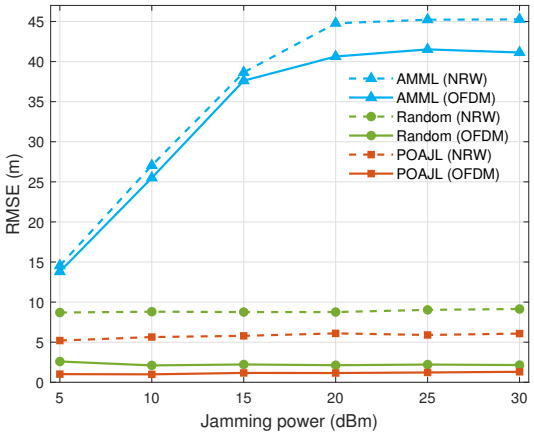
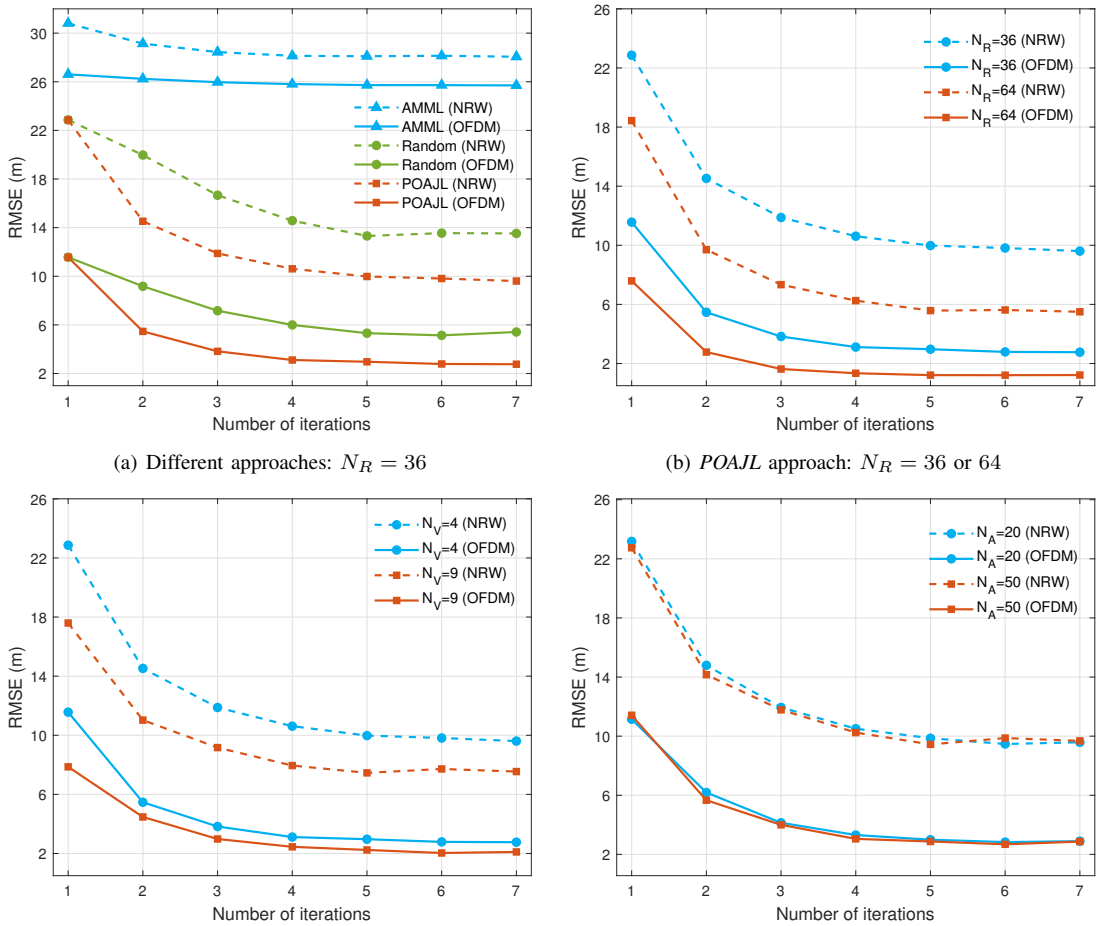


Fig. 5. Localization performance versus transmission power of jammer: $N_R = 64$.

overhead during the iterative process, the transmission duration T is allowed to gradually increase until it reaches a sufficient level to meet the application requirements of the Jacobi-Anger expansion [29], i.e., T is initialized by 15 with its upper bound set by 50.

We compare three approaches for the RIS-enhanced wireless localization: *1) Random*, where the RIS phase shifts are



(a) Different approaches: $N_R = 36$

(b) *POAJL* approach: $N_R = 36$ or 64

(c) *POAJL* approach: $N_V = 4$ or 9

(d) *POAJL* approach: $N_A = 20$ or 50

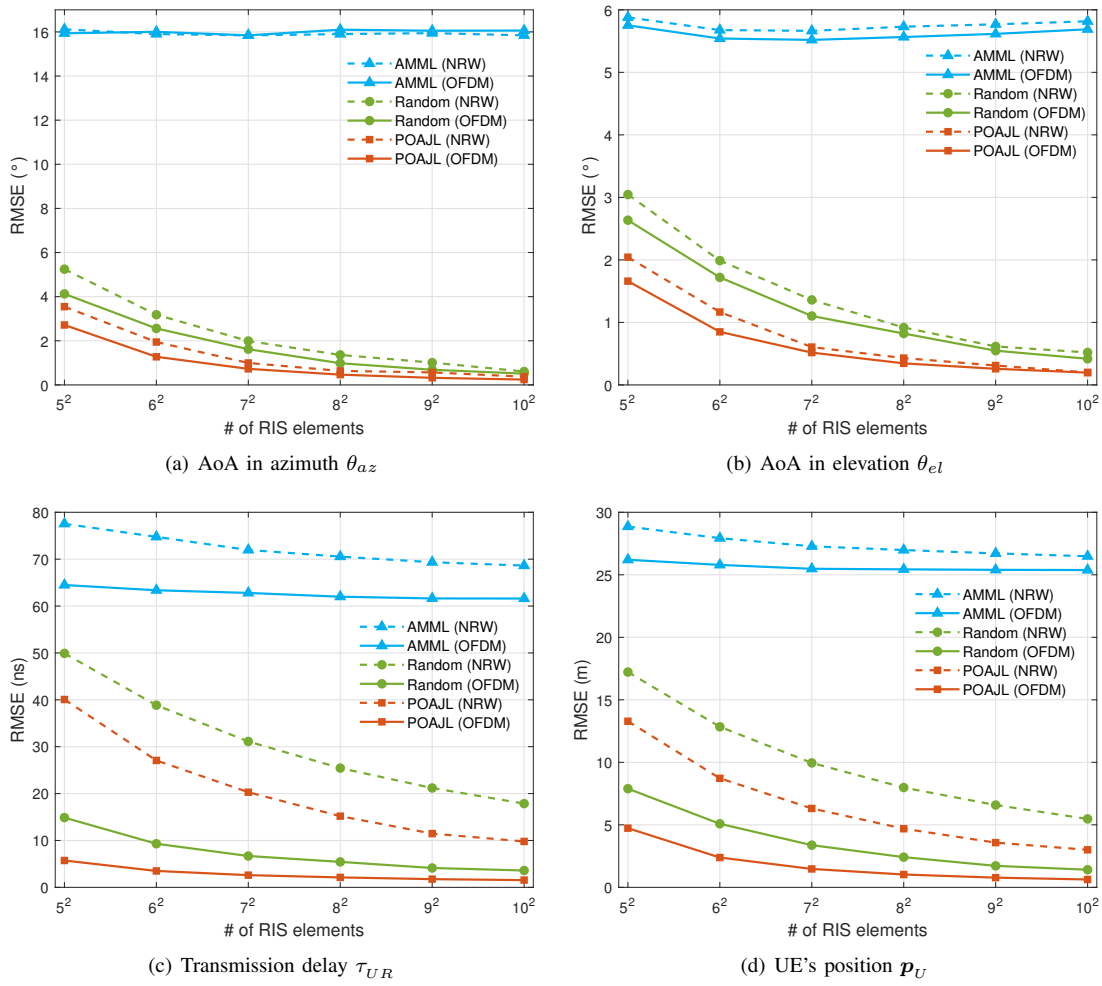
Fig. 6. Localization performance versus the number of iterations.

randomly initialized by uniformly spacing the interval $[0, 2\pi)$ and are always fixed during the whole iterative process; *2) AMML*, which is the approximated mismatched maximum likelihood (AMML) approach proposed in [29] without considering the impact of the jammer; *3) POAJL*, which refers to the iterative phase optimization approach in Algorithm 3. Note that both the *Random* and our proposed *POAJL* approaches apply the two-stage anti-jamming localization as investigated in Algorithm 1 and Algorithm 2. We use *NRW* and *OFDM* to represent the wireless localization techniques based on narrowband and OFDM pilot signals, respectively. Besides, we introduce a common measurement tool, namely *root mean square error (RMSE)*, in estimating the differences between true values and observed values [10, 12], as the localization performance metric, which is defined by

$$RMSE = \sqrt{\frac{1}{M}\sum_{m=1}^{M}(\hat{x} - x)^2}, \tag{48}$$

where M is the number of simulations, x and $\hat{x}$ denote the real value and estimated value of a specific parameter. More specifically, the RMSE is utilized to evaluate not only the estimated position of the UE $\boldsymbol{p}_U$ but also those key impact factors, which are estimated during the localization process and will affect the final localization performance, such as transmission delay τ_{UR}, AoA in azimuth θ_{az}, and AoA in elevation θ_{el}.

1) Jammer's Location: We first discuss the impact of the jammer's location. The relative distance between the RIS and the jammer is demonstrated in Fig. 4(a), where the UE is randomly located with 60m relative distance to the RIS. We can observe that there exists a significant peak in RMSE for UE localization with both the *Random* approach and the original POAJL approach called *POAJL-orign*. This is primarily due to the similarity in relative distance to the RIS, i.e., 60m, leading to a comparable approximation of AoA in elevation ψ_{el} and θ_{el}, which will increase the estimation error when differentiating θ_{el} by Eq. (30). To address this issue, we further **improve** the proposed UE localization approach in Section IV-B. We use $\pi/180$ as a finite resolution to sample θ_{el} within the range of $(-\pi/2, -\pi)$ and then obtain a series of angel pairs by plugging each sampled value into Eq. (31) to calculate the corresponding θ_{az}. In this way, the optimal pair $(\theta_{el}, \theta_{az})$ with minimum value of Eq. (26) can be found through linear search. Furthermore, the refined UE localization approach could be also applied to our proposed *POAJL* approach in the rest of the simulations. Fig. 4(a) illustrates that the improved *POAJL* approach can greatly eliminate the adverse impact of the



(a) AoA in azimuth θ_{az}

(b) AoA in elevation θ_{el}

(c) Transmission delay τ_{UR}

(d) UE's position $\boldsymbol{p}_U$

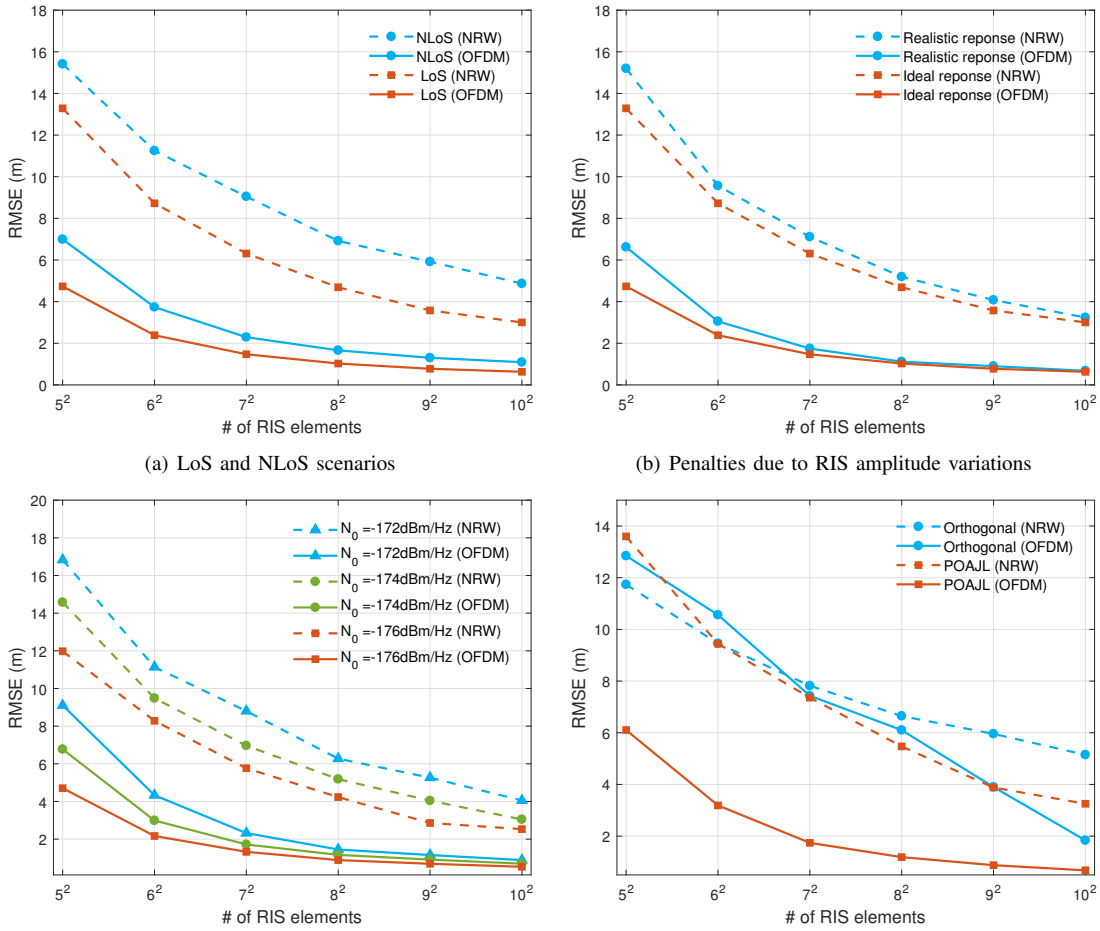
Fig. 7. Performance comparisons versus different number of RIS reflecting elements.

jammer's location and is applicable for both narrowband and OFDM pilot signals.

Fig. 4(b) demonstrates the localization RMSE versus the relative distance between the UE and the jammer. In general, higher localization accuracy could be achieved with OFDM pilot signals compared to narrowband pilot signals. The RMSE decreases with the increased relative distance when using the *Random* and our proposed *POAJL* approaches. The reason is that a closer relative distance between the UE and the jammer leads to similar channel conditions and therefore degrades the localization accuracy when applying the proposed two-stage anti-jamming localization algorithm. On the contrary, the RMSE in the *AMML* approach decreases with the increased relative distance because the jamming attack remains to be solved. Compared with the *Random* approach, our proposed *POAJL* approach can achieve better localization accuracy thanks to the well-designed iterative phase optimization algorithm.

2) Jamming Power: We then investigate the localization accuracy versus the jamming power, i.e., the transmission power of the jammer, as shown in Fig. 5. In other words, the increased jammer power implied an increased jammer-user power ratio when the transmission power of the UE is fixed. Thanks to the proposed two-stage anti-jamming localization algorithm, we observe that both the *Random* and our proposed *POAJL* approaches can achieve significant improvements in the localization accuracy against jamming attacks as compared to the *AMML* approach. Specifically, the proposed *POAJL* approach remains unaffected by the increased jamming power and therefore can achieve an average RMSE of 5.07 meters and 1.40 meters when using narrowband and OFDM pilot signals, respectively. In other words, compared with the *Random* approach, our proposed *POAJL* approach can reduce the localization RMSE by 36.31% and 48.84% accordingly.

3) Iterative Process: The localization performance during the iterative process is shown in Fig. 6. In Fig. 6(a), due to the increased transmission times T, the RMSE of both the *Random* and the proposed *POAJL* approaches could be iteratively improved through the proposed two-stage anti-jamming localization algorithm, whereas the *AMML* approach does not benefit from the iterative process. Besides, the proposed *POAJL* approach outperforms the *Random* approach by optimizing the RIS phase shift profiles. The performance of the proposed *POAJL* approach with different reflecting elements N_R and UAV antennas N_V are demonstrated in Fig. 6(b) and Fig. 6(c), respectively. We can observe that more reflecting



(a) LoS and NLoS scenarios

(b) Penalties due to RIS amplitude variations

(c) Against noise level

(d) Compare with the *Orthogonal* approach

Fig. 8. Localization Performance of *POAJL* approach.

elements or UAV antennas are used lower localization RMSE is achieved and fewer iterations are required for convergence. Nevertheless, note that more reflecting elements or UAV antennas meanwhile will introduce higher computing requirements for user localization. Moreover, to verify the approximation effect of the Jacobi-Anger expansion, the performance of the proposed *POAJL* approach with different values of N_A is illustrated in Fig. 6(d). The results show that the localization performance has little enhancement when the approximation factor N_A increases from 20 to 50. Namely, sufficient localization accuracy can be achieved if the constraint of N_A is satisfied.

4) RIS Elements: Finally, as shown in Fig. 7, we demonstrate the localization performance with the increased RIS reflecting elements N_R from the perspective of the UE's estimated position $\boldsymbol{p}_U$ and other intermediate parameters of the directed link UR, that is, the transmission delay τ_{UR}, the AoA in azimuth θ_{az} and elevation θ_{el}. In general, jamming signals cause significant errors in angle estimation when using the *AMML* approach, as shown in Fig. 7(a) and Fig. 7(b). Nevertheless, both the *Random* and the proposed *POAJL* approaches demonstrate an improved ability to mitigate the jamming effect with the increased RIS reflecting elements. The performance gap between the two approaches with large RIS reflecting elements is not obvious because sufficiently large RIS elements will give no extra benefit to the estimation improvement. Additionally, in Fig. 7(c), we find out that the RMSE of transmission delay τ_{UR} based on OFDM pilot signals is greatly smaller than that of narrowband pilot signals, which is because the multiple OFDM subcarriers can provide more information for transmission delay estimation. The estimation improvement of transmission delay τ_{UR} based on narrowband pilot signals makes the biggest contributions to the localization accuracy when using both the *Random* and the proposed *POAJL* approaches. With large RIS elements, the proposed *POAJL* approach still can achieve more estimation improvement of transmission delay τ_{UR} , especially when narrowband pilot signals are applied.

Overall, the proposed *POAJL* approach can outperform other approaches in terms of localization RMSE, especially the estimated position of the UE in Fig. 7(d), which represents the final localization accuracy. For example, when the number of RIS elements N_R is 6×6, the proposed *POAJL* approach can reduce the localization RMSE by 32.07% and 53.06% compared with the *Random* approach when using narrowband and OFDM pilot signals, respectively. Even with large RIS elements 10×10, the proposed *POAJL* approach still can reduce the localization RMSE by 45.16% and 55.32%, respectively.

5) Other Factors: Note that so far only the LOS path has been involved in the simulations, we further consider a more realistic Rician fading model in Appendix B, i.e., LoS links coexist with NLoS, for the received signals through the wireless links UR, RV and JR, where the Rician factors K_{UR}, K_{RV}, and K_{JR} are set to 31.3. The localization performance of the proposed *POAJL* approach in both LOS and NLoS scenarios is shown in Fig. 8(a). We can observe that the localization accuracy with the Rician fading model is deteriorated by NLoS propagation. Still, the proposed *POAJL* approach based on OFDM pilot signals can perform better against the influence of NLoS when the RIS elements become large.

We quantify performance penalties due to RIS amplitude variations [49], as shown in Fig. 8(b), where the ideal response is the unit-amplitude RIS element response. The realistic RIS amplitude model is provided in Appendix C, where $\bar{\beta}_{\min} = 0.7$, $\bar{\vartheta}0$, and $\bar{\kappa} = 1.5$ [50, 51]. Note that β_i is a function of the applied phased shift ω_i, our *POAJL* approach utilizes the applied phase profile in the last iteration to calculate the amplitude responses for phase optimization. The results show that the phase-dependent amplitude variations degrade the localization accuracy but more RIS elements can mitigate this performance loss, i.e., 8×8 RIS elements based on OFDM pilot signals.

Furthermore, we discuss how the proposed *POAJL* approach confronts the noise level at the jammer side. According to Eqs. (9) and (11), the noise integrating with the jamming signal can be regarded as a component of $\boldsymbol{n}_t$. Note that the received noise at the UE side is connected with the location of the jammer and the RIS phase shift profile, we provide the performance with the increased PSD of noise N_0 to simplify. As shown in Fig. 8(c), the localization performance decreases with the increased noise level because the noise $\boldsymbol{n}_t$ is treated to 0 throughout the derivations of the proposed *POAJL* approach. Still, the OFDM pilot signals have better performance to eliminate the adverse impact of noise level and more RIS elements can greatly overcome the drop in estimation error.

Based on the jammer estimation in the former stage, an intuitive approach denoted by *Orthogonal* is to exploit the orthogonal RIS phase shift profile to eliminate the jamming signal in the latter stage. As shown in Fig. 8(d), we can observe that the proposed *POAJL* approach has better localization accuracy than the *Orthogonal* approach. The reason is that the *Orthogonal* approach aims at eliminating the jamming signal but at the same time may reduce the received power of the pilot signal transmitted by the UE. However, the proposed *POAJL* approach optimizes the RIS phase shift profiles to not only enhance the UE's pilot signal but also mitigate the malicious interference caused by the jammer.

VII. Conclusions

This paper investigates a RIS-enhanced wireless localization framework, where a two-stage anti-jamming algorithm is investigated to mitigate the malicious interference caused by jamming attacks and a phase optimization algorithm is further utilized to iteratively improve the localization accuracy. We discuss the localization performance based on narrowband and OFDM pilot signals. Overall, the proposed POAJL approach can iteratively optimize the RIS phase shift profiles and outperform other approaches in terms of localization RMSE. Although our proposed framework offers certain contributions, we may face limitations when comparing with practical jamming attacks, which can transmit the jamming signals with time-varying power and random pilot sequences. Thus, as a future direction, we expect to tackle this difficulty by proposing reinforcement learning-based approaches. There are also several future research avenues considering the jammer with multiple antennas and the multi-jammer scenario.

References

[1] Y. Liu, J. Bai, G. Wang, X. Wu, F. Sun, Z. Guo, and H. Geng, "Uav localization in low-altitude gnss-denied environments based on poi and store signage text matching in uav images," *Drones*, vol. 7, no. 7, 2023.

[2] Y. Lee, P. Wang, and B. Park, "Nonlinear regression-based gnss multipath dynamic map construction and its application in deep urban areas," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 5, pp. 5082–5093, 2023.

[3] Z. Ullah, F. Al-Turjman, and L. Mostarda, "Cognition in uav-aided 5g and beyond communications: A survey," *IEEE Trans. Cogn. Commun. Netw.*, vol. 6, no. 3, pp. 872–891, 2020.

[4] L. Xiao, H. Li, S. Yu, Y. Zhang, L.-C. Wang, and S. Ma, "Reinforcement learning based network coding for drone-aided secure wireless communications," *IEEE Trans. Commun.*, vol. 70, no. 9, pp. 5975–5988, 2022.

[5] W. Zhang and W. Zhang, "An efficient uav localization technique based on particle swarm optimization," *IEEE Trans. Veh. Technol.*, vol. 71, no. 9, pp. 9544–9557, 2022.

[6] S. Bayat and R. Amiri, "Advances in uav-assisted localization: Joint source and uav parameter estimation," *IEEE Trans. Veh. Technol.*, vol. 72, no. 11, pp. 14 268–14 278, 2023.

[7] Y.-J. Chen, D.-K. Chang, and C. Zhang, "Autonomous tracking using a swarm of uavs: A constrained multi-agent reinforcement learning approach," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13 702–13 717, 2020.

[8] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming," *IEEE Trans. Wireless Commun.*, vol. 18, no. 11, pp. 5394–5409, 2019.

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

[10] M. Luan, B. Wang, Y. Zhao, Z. Feng, and F. Hu, "Phase design and near-field target localization for ris-assisted regional localization system," *IEEE Trans. Veh. Technol.*, vol. 71, no. 2, pp. 1766–1777, 2022.

[11] T. Ma, Y. Xiao, X. Lei, W. Xiong, and M. Xiao, "Distributed reconfigurable intelligent surfaces assisted indoor positioning," *IEEE Trans. Wireless Commun.*, vol. 22, no. 1, pp. 47–58, 2023.

[12] Y. Lin, S. Jin, M. Matthaiou, and X. You, "Conformal irs-empowered mimo-ofdm: Channel estimation and envi-

ronment mapping," *IEEE Trans. Commun.*, vol. 70, no. 7, pp. 4884–4899, 2022.

[13] J. Luo, T. Liang, C. Chen, and T. Zhang, "A uav mounted ris aided communication and localization integration system for ground vehicles," in *2022 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2022, pp. 139–144.

[14] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 767–809, 2022.

[15] Z. Wang, R. Liu, Q. Liu, L. Han, and J. S. Thompson, "Feasibility study of uav-assisted anti-jamming positioning," *IEEE Trans. Veh. Technol.*, vol. 70, no. 8, pp. 7718–7733, 2021.

[16] Z. Wang, R. Liu, Q. Liu, L. Han, and W. Mu, "Controllable positioning service with uav-enabled cooperative jamming," *IEEE Wireless Commun. Lett.*, vol. 10, no. 9, pp. 1929–1933, 2021.

[17] B. Liu, X. Zhu, Y. Jiang, Z. Wei, and Y. Huang, "Uav and piecewise convex approximation assisted localization with unknown path loss exponents," *IEEE Trans. Veh. Technol.*, vol. 68, no. 12, pp. 12 396–12 400, 2019.

[18] Z. Wang, R. Liu, Q. Liu, L. Han, J. S. Thompson, Y. Lin, and W. Mu, "Toward reliable uav-enabled positioning in mountainous environments: System design and preliminary results," *IEEE Trans. Rel.*, vol. 71, no. 4, pp. 1435–1463, 2022.

[19] Z. Yang, S. Bi, and Y.-J. A. Zhang, "Deployment optimization of dual-functional uavs for integrated localization and communication," *IEEE Trans. Wireless Commun.*, vol. 22, no. 12, pp. 9672–9687, 2023.

[20] F. Zhou, L. Fan, J. Tang, and W. Chen, "Placement and concise mse lower-bound for uav-enabled localization via rss," *IEEE Trans. Veh. Technol.*, vol. 71, no. 2, pp. 2209–2213, 2022.

[21] D. Ebrahimi, S. Sharafeddine, P.-H. Ho, and C. Assi, "Autonomous uav trajectory for localizing ground objects: A reinforcement learning approach," *IEEE Trans. Mobile Comput.*, vol. 20, no. 4, pp. 1312–1324, 2021.

[22] J. He, H. Wymeersch, L. Kong, O. Silvén, and M. Juntti, "Large intelligent surface for positioning in millimeter wave mimo systems," in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, 2020, pp. 1–5.

[23] H. Wymeersch and B. Denis, "Beyond 5g wireless localization with reconfigurable intelligent surfaces," in *2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1–6.

[24] H. Zhang, H. Zhang, B. Di, K. Bian, Z. Han, and L. Song, "Metalocalization: Reconfigurable intelligent surface aided multi-user wireless indoor localization," *IEEE Trans. Wireless Commun.*, vol. 20, no. 12, pp. 7743–7757, 2021.

[25] D. Dardari, N. Decarli, A. Guerra, and F. Guidi, "Los/nlos near-field localization with a large reconfigurable intelligent surface," *IEEE Trans. Wireless Commun.*, vol. 21, no. 6, pp. 4282–4294, 2022.

[26] Z. Abu-Shaban, K. Keykhosravi, M. F. Keskin, G. C. Alexandropoulos, G. Seco-Granados, and H. Wymeersch, "Near-field localization with a reconfigurable intelligent surface acting as lens," in *2021 IEEE International Conference on Communications (ICC)*, 2021, pp. 1–6.

[27] D.-R. Emenonye, H. S. Dhillon, and R. M. Buehrer, "Fundamentals of ris-aided localization in the far-field," *IEEE Trans. Wireless Commun.*, vol. 23, no. 4, pp. 3408–3424, 2024.

[28] Y. Huang, J. Yang, W. Tang, C.-K. Wen, S. Xia, and S. Jin, "Joint localization and environment sensing by harnessing nlos components in ris-aided mmwave communication systems," *IEEE Trans. Wireless Commun.*, vol. 22, no. 12, pp. 8797–8813, 2023.

[29] C. Ozturk, M. F. Keskin, H. Wymeersch, and S. Gezici, "Ris-aided near-field localization under phase-dependent amplitude variations," *IEEE Trans. Wireless Commun.*, vol. 22, no. 8, pp. 5550–5566, 2023.

[30] Q. Cheng, L. Li, M.-M. Zhao, and M.-J. Zhao, "Cooperative localization for reconfigurable intelligent surface-aided mmwave systems," in *2022 IEEE Wireless Communications and Networking Conference (WCNC)*, 2022, pp. 1051–1056.

[31] Y. Liu, E. Liu, R. Wang, and Y. Geng, "Reconfigurable intelligent surface aided wireless localization," in *2021 IEEE International Conference on Communications (ICC)*, 2021, pp. 1–6.

[32] G. C. Alexandropoulos, K. Katsanos, M. Wen, and D. B. Da Costa, "Safeguarding mimo communications with reconfigurable metasurfaces and artificial noise," in *2021 IEEE International Conference on Communications (ICC)*, 2021, pp. 1–6.

[33] G. C. Alexandropoulos, K. D. Katsanos, M. Wen, and D. B. Da Costa, "Counteracting eavesdropper attacks through reconfigurable intelligent surfaces: A new threat model and secrecy rate optimization," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 1285–1302, 2023.

[34] H. Yang, Z. Xiong, J. Zhao, D. Niyato, Q. Wu, H. V. Poor, and M. Tornatore, "Intelligent reflecting surface assisted anti-jamming communications: A fast reinforcement learning approach," *IEEE Trans. Wireless Commun.*, vol. 20, no. 3, pp. 1963–1974, 2021.

[35] Z. Ji, W. Yang, X. Guan, X. Zhao, G. Li, and Q. Wu, "Trajectory and transmit power optimization for irs-assisted uav communication under malicious jamming," *IEEE Trans. Veh. Technol.*, vol. 71, no. 10, pp. 11 262–11 266, 2022.

[36] X. Pang, N. Zhao, J. Tang, C. Wu, D. Niyato, and K.-K. Wong, "Irs-assisted secure uav transmission via joint trajectory and beamforming design," *IEEE Trans. Commun.*, vol. 70, no. 2, pp. 1140–1152, 2022.

[37] Y. Sun, K. An, Y. Zhu, G. Zheng, K.-K. Wong, S. Chatzinotas, H. Yin, and P. Liu, "Ris-assisted robust hybrid beamforming against simultaneous jamming and eavesdropping attacks," *IEEE Trans. Wireless Commun.*, vol. 21, no. 11, pp. 9212–9231, 2022.

[38] K. T. Selvan and R. Janaswamy, "Fraunhofer and fresnel distances: Unified derivation for aperture antennas,"

IEEE Antennas and Propagation Magazine, vol. 59, no. 4, pp. 12–15, 2017.

[39] W. Liu, C. Pan, H. Ren, F. Shu, S. Jin, and J. Wang, "Low-overhead beam training scheme for extremely large-scale ris in near field," *IEEE Transactions on Communications*, vol. 71, no. 8, pp. 4924–4940, 2023.

[40] A. Fascista, A. Coluccia, H. Wymeersch, and G. Seco-Granados, "Millimeter-wave downlink positioning with a single-antenna receiver," *IEEE Trans. Wireless Commun.*, vol. 18, no. 9, pp. 4479–4490, 2019.

[41] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming," *IEEE Trans. Wireless Commun.*, vol. 18, no. 11, pp. 5394–5409, 2019.

[42] J. He, A. Fakhreddine, C. Vanwynsberghe, H. Wymeersch, and G. C. Alexandropoulos, "3d localization with a single partially-connected receiving ris: Positioning error analysis and algorithmic design," *IEEE Trans. Veh. Technol.*, vol. 72, no. 10, pp. 13 190–13 202, 2023.

[43] H. Akhlaghpasand, E. Björnson, and S. M. Razavizadeh, "Jamming-robust uplink transmission for spatially correlated massive mimo systems," *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3495–3504, 2020.

[44] X. Wei, Q. Wang, T. Wang, and J. Fan, "Jammer localization in multi-hop wireless network: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 765–799, 2017.

[45] Y. Cai, M.-M. Zhao, K. Xu, and R. Zhang, "Intelligent reflecting surface aided full-duplex communication: Passive beamforming and deployment design," *IEEE Trans. Wireless Commun.*, vol. 21, no. 1, pp. 383–397, 2022.

[46] Y. Wei, M.-M. Zhao, M.-J. Zhao, and Y. Cai, "Channel estimation for irs-aided multiuser communications with reduced error propagation," *IEEE Trans. Wireless Commun.*, vol. 21, no. 4, pp. 2725–2741, 2022.

[47] Y. Lin, S. Jin, M. Matthaiou, and X. Yi, "Circular ris-enabled channel estimation and localization for multi-user isac systems," *IEEE Trans. Wireless Commun.*, vol. 23, no. 8, pp. 8730–8743, 2024.

[48] S. Hu, Z. Wei, Y. Cai, C. Liu, D. W. K. Ng, and J. Yuan, "Robust and secure sum-rate maximization for multiuser miso downlink systems with self-sustainable irs," *IEEE Trans. Commun.*, vol. 69, no. 10, pp. 7032–7049, 2021.

[49] K. D. Katsanos, N. Shlezinger, M. F. Imani, and G. C. Alexandropoulos, "Wideband multi-user mimo communications with frequency selective riss: Element response modeling and sum-rate maximization," in *2022 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2022, pp. 151–156.

[50] S. Abeywickrama, R. Zhang, Q. Wu, and C. Yuen, "Intelligent reflecting surface: Practical phase shift model and beamforming optimization," *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5849–5863, 2020.

[51] C. Ozturk, M. F. Keskin, H. Wymeersch, and S. Gezici, "Ris-aided near-field localization under phase-dependent amplitude variations," *IEEE Trans. Wireless Commun.*, vol. 22, no. 8, pp. 5550–5566, 2023.

APPENDIX A
GEOMETRY

The channel parameters are given below. The c is the speed of light.

$$\tau_{UR} = \|\boldsymbol{p}_U - \boldsymbol{p}_U\|/c, \tau_{RV} = \|\boldsymbol{p}_V - \boldsymbol{p}_R\|/c, \tag{49}$$

$$\tau_{JR} = \|\boldsymbol{p}_J - \boldsymbol{p}_U\|/c, \tag{50}$$

$$\theta_{az} = arctan\left(\frac{y_U - y_R}{x_U - x_R}\right) \in (-\pi/2, \pi/2), \tag{51}$$

$$\varphi_{az} = arctan\left(\frac{y_V - y_R}{x_V - x_R}\right) \in (-\pi/2, 0), \tag{52}$$

$$\psi_{az} = arctan\left(\frac{y_J - y_R}{x_J - x_R}\right) \in (-\pi/2, 0), \tag{53}$$

$$\phi_{az} = \pi + \varphi_{az} \in (\pi/2, \pi), \tag{54}$$

$$\theta_{el} = arccos\left(\frac{z_U - z_R}{\|\boldsymbol{p}_U - \boldsymbol{p}_R\|}\right) \in (0, \pi), \tag{55}$$

$$\varphi_{el} = arccos\left(\frac{z_V - z_R}{\|\boldsymbol{p}_V - \boldsymbol{p}_R\|}\right) \in (0, \pi/2), \tag{56}$$

$$\psi_{el} = arccos\left(\frac{z_J - z_R}{\|\boldsymbol{p}_J - \boldsymbol{p}_R\|}\right) \in (0, \pi), \tag{57}$$

$$\phi_{el} = \pi - \varphi_{el} \in (0, \pi), \tag{58}$$

$$\rho_{UR} = \frac{\sqrt{g_0}}{\|\boldsymbol{p}_U - \boldsymbol{p}_R\|}, \rho_{RV} = \frac{\sqrt{g_0}}{\|\boldsymbol{p}_V - \boldsymbol{p}_R\|}, \tag{59}$$

$$\rho_{JR} = \frac{\sqrt{g_0}}{\|\boldsymbol{p}_J - \boldsymbol{p}_R\|}. \tag{60}$$

APPENDIX B
RICIAN FADING MODEL

By applying the Rician fading model, the channel of links UR, RV, and JR can be respectively given by

$$\tilde{\boldsymbol{h}}_{UR} = \rho_{UR}\left(\sqrt{\frac{K_{UR}}{K_{UR}+1}}\boldsymbol{h}_{UR}^{LoS} + \sqrt{\frac{1}{K_{UR}+1}}\boldsymbol{h}_{UR}^{NLoS}\right), \tag{61}$$

$$\tilde{\boldsymbol{h}}_{RV} = \rho_{RV}\left(\sqrt{\frac{K_{RV}}{K_{RV}+1}}\boldsymbol{h}_{RV}^{LoS} + \sqrt{\frac{1}{K_{RV}+1}}\boldsymbol{h}_{RV}^{NLoS}\right), \tag{62}$$

$$\tilde{\boldsymbol{h}}_{JR} = \rho_{JR}\left(\sqrt{\frac{K_{JR}}{K_{JR}+1}}\boldsymbol{h}_{JR}^{LoS} + \sqrt{\frac{1}{K_{JR}+1}}\boldsymbol{h}_{JR}^{NLoS}\right), \tag{63}$$

where K_{UR}, K_{RV}, and K_{JR} are the Rician factors. The $\boldsymbol{h}_{UR}^{LoS} = e^{-j2\pi\tau_{UR}f}\boldsymbol{a}(\boldsymbol{\theta})$, $\boldsymbol{h}_{RV}^{LoS} = e^{-j2\pi\tau_{RV}f}\boldsymbol{a}(\boldsymbol{\varphi})\boldsymbol{b}^{\mathsf{T}}(\boldsymbol{\phi})$ and $\boldsymbol{h}_{JR}^{LoS} = e^{-j2\pi\tau_{JR}f}\boldsymbol{a}(\boldsymbol{\psi})$ are the LoS components of the UR, RV and JR links, respectively. The $\boldsymbol{h}_{UR}^{NLoS}$, $\boldsymbol{h}_{RV}^{NLoS}$ and $\boldsymbol{h}_{JR}^{NLoS}$ are the NLoS components and follow the zero-mean circularly symmetric complex Gaussian (CSCG) distribution with unit-variance.

APPENDIX C
RIS AMPLITUDE MODEL

In the realistic RIS amplitude model, the amplitude reflection coefficient of each RIS element is expressed as

$$\beta_i(\omega_i) = (1 - \bar{\beta}_{\min})\Big(\frac{\sin(\omega_i - \bar{\vartheta}) + 1}{2}\Big)^{\bar{\kappa}} + \bar{\beta}_{\min}, \qquad (64)$$

where $\bar{\beta}_{\min} \geq 0$, $\bar{\vartheta} \geq 0$, and $\bar{\kappa} \geq 0$ are the constants related to the specific circuit implementation. The ω_i is the applied phase shift of the corresponding RIS element.

Yi Zhang (Member, IEEE) received the B.S. degree in software engineering from Software College, Xiamen University in 2014. He received the M.S. and the Ph.D. degree from Graduate Institute of Communication Engineering, National Taiwan University in 2016. He has been an assistant engineer in Quanzhou Institute of Equipment Manufacturing, Haixi Institutes, Chinese Academy of Sciences, during 2016-2017. He is currently an Assistant Professor with Department of Information and Communication Engineering, Xiamen University. His research interests include mobile and wireless networking, fog/edge computing, and game theoretical models for communications networks.

Yajing Xie received the B.S. degree in Electronic and Information Engineering from Fuzhou University in 2021 and the M.S. degree from the Department of Information and Communication Engineering, Xiamen University in 2024. Her research interests are wireless communications and RIS optimization.

Lijia Wang received the B.S. degree in communication engineering from Changsha University of Science and Technology, Changsha, China in 2022. She is currently pursuing a M.S. degree with the Department of Information and Communication Engineering, Xiamen University. Her research interests include wireless communications and maritime communications.

Minghui Liwang (Senior Member, IEEE) is currently an associate professor with the Department of Control Science and Engineering, the National Key Laboratory of Autonomous Intelligent Unmanned Systems, and also with Frontiers Science Center for Intelligent Autonomous Systems, Ministry of Education, Tongji University, Shanghai, China. Her research interests include multi-agent systems, edge computing, distributed learning, as well as economic models and applications.

Xianbin Wang (Fellow, IEEE) received his Ph.D. degree in electrical and computer engineering from the National University of Singapore in 2001.

He has been with Western University, Canada, since 2008, where he currently serves as a Distinguished University Professor and a Tier-1 Canada Research Chair in Trusted Communications and Computing. Prior to joining Western University, he was with the Communications Research Centre Canada as a Research Scientist and later a Senior Research Scientist from 2002 to 2007. From 2001 to 2002, he was a System Designer at STMicroelectronics. His current research interests include 5G/6G technologies, Internet of Things, machine learning, communications security, digital twin, and intelligent communications. He has over 600 highly cited journals and conference papers, in addition to over 30 granted and pending patents and several standard contributions.

Dr. Wang is a Fellow of the Canadian Academy of Engineering and a Fellow of the Engineering Institute of Canada. He has received many prestigious awards and recognitions, including the IEEE Canada R. A. Fessenden Award, Canada Research Chair, Engineering Research Excellence Award at Western University, Canadian Federal Government Public Service Award, Ontario Early Researcher Award, and ten Best Paper Awards. He is currently a member of the Senate, Senate Committee on Academic Policy and Senate Committee on University Planning at Western. He also serves on NSERC Discovery Grant Review Panel for Computer Science. He has been involved in many flagship conferences, including IEEE GLOBECOM, ICC, VTC, PIMRC, WCNC, CCECE, and ICNC, in different roles, such as General Chair, TPC Chair, Symposium Chair, Tutorial Instructor, Track Chair, Session Chair, and Keynote Speaker. He serves/has served as the Editor-in-Chief, Associate Editor-in-Chief, Area Editor, and editor/associate editor for over ten journals. He was the Chair of the IEEE ComSoc Signal Processing and Computing for Communications (SPCC) Technical Committee and is currently serving as the Central Area Chair of IEEE Canada.