RIScan: RIS-aided Multi-user Indoor Localization Using COTS Wi-Fi

Chenggao Li[1], Qianyi Huang[2], Yuxuan Zhou[1], Yandao Huang[1,3], Qingyong Hu[1], Huangxun Chen[3,4], Qian Zhang[1]
[1]The Hong Kong University of Science and Technology, Hong Kong SAR, China
[2]Sun Yat-sen University, Guangdong, China
[3]The Hong Kong University of Science and Technology (Guangzhou), Guangdong, China
[4]Huawei, Hong Kong SAR, China
{clicx,yzhoudo,yhuangfg,qhuag,qianzh}@cse.ust.hk,huangqy89@mail.sysu.edu.cn,huangxunchen@hkust-gz.edu.cn

ABSTRACT

Multi-user indoor localization is considered to be one of the most useful wireless applications. Low latency and high robustness to dynamic interference from surrounding people are essential requirements for multi-user localization. However, state-of-the-art (SOTA) indoor localization systems cannot satisfy both requirements at the same time. In this paper, we propose RIScan, a Reconfigurable Intelligent Surface (RIS)-aided localization system that can achieve both low latency and high reliability. We leverage RIS to perform Wi-Fi beam scanning so all clients can figure out their direction in a single scan. However, compared with traditional AP-based systems, the introduction of RIS creates a more complicated signal superposition at the receiver, preventing clients from directly obtaining target beams for direction derivation and localization. To overcome this challenge, we fully utilize the reconfigurability of RIS to endow target beams with distinguishing features, so that RIScan can extract stable and accurate direction information from complex and dynamic environments. RIScan is implemented in the real system with our own developed 16×16 RIS prototype and COTS Wi-Fi devices. Extensive experiments show that RIScan achieves a median localization error of 47cm and 71cm in static and dynamic environments with only two RIS anchors. Compared to the SOTA methods, RIScan reduces the localization latency by more than an order of magnitude.

CCS CONCEPTS

• **Networks** → **Location based services**.

KEYWORDS

Reconfigurable Intelligent Surface, Smart Surfaces, RIS-aided Wi-Fi Sensing, Multi-user Indoor Localization

Corresponding author: Qian Zhang.
Huangxun Chen participated in this research when she was a Researcher at Huawei. She now joins HKUST (GZ) as an Assistant Professor.

SenSys '23, November 12–17, 2023, Istanbul, Turkiye

ACM ISBN 979-8-4007-0414-7/23/11…$15.00
https://doi.org/10.1145/3625687.3625806

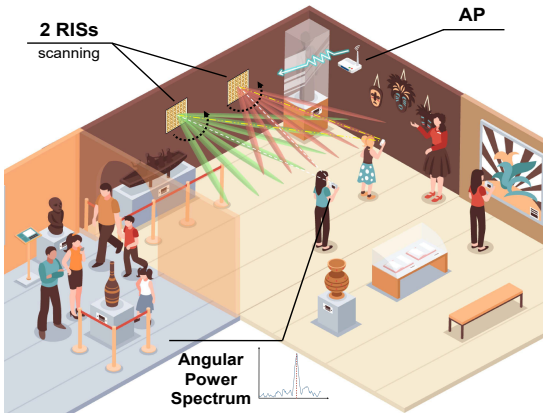


Figure 1: Illustration of RIScan system in the museum scenario.

ACM Reference Format:
Chenggao Li[1], Qianyi Huang[2], Yuxuan Zhou[1], Yandao Huang[1,3], Qingyong Hu[1], Huangxun Chen[3,4], Qian Zhang[1]. 2023. RIScan: RIS-aided Multi-user Indoor Localization Using COTS Wi-Fi. In *The 21st ACM Conference on Embedded Networked Sensor Systems (SenSys '23), November 12–17, 2023, Istanbul, Turkiye.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3625687.3625806

1 INTRODUCTION

Indoor localization is very helpful in many daily scenarios. For instance, in museums, localization services can provide many exciting functionalities. A group of visitors can quickly find the exhibits they are interested in with indoor navigation. In addition, when they walk to a certain showcase, the system can automatically display detailed information. To avoid providing visitors with outdated or even excessively wrong information, the system must be able to operate with low latency and robust to complicated interference caused by the movement of surrounding visitors.

Existing Wi-Fi localization systems can be broadly divided into two categories, Channel State Information (CSI) based [19, 25, 43] and Received Signal Strength Indicator (RSSI) fingerprint-based [7, 24, 47] approaches. For CSI-based systems, Angle of Arrival (AoA) and Time of Flight (ToF) are extracted from CSI with MUSIC algorithm [26]. As the AP usually has more antennas than the end device (2 antennas for the majority of smartphones), the CSIs are usually measured and processed at the AP side to get high angular

resolution. The processing capability of AP becomes a bottleneck when there are a large number of localization requests, which indicates that the latency will linearly increase with the number of clients. The time cost of UbiLocate to localize a client is 1.5s [25] with 3 APs, and the localization latency increases to 15s when there are 10 clients. For RSSI fingerprinting approaches, a RSSI map needs to be drawn through various measurements in space. Dynamic interference caused by surrounding movements will change the pre-measured RSSI map so that the performance will degrade significantly under complex interference. Overall, SOTA Wi-Fi indoor localization systems can achieve decimeter-level accuracy in a controlled lab setup, but to the best of our knowledge, none of the systems can satisfy both low latency and high robustness to environmental interference.

To bridge this gap, we present RIScan, a parallel multi-user indoor localization system with a pair of Reconfigurable Intelligent Surfaces (RIS). RIScan is inspired by the Radio Direction Finding (RDF) technology [36], which is widely used in the navigation of ships and emergency rescues. The working principle of RDF is to steer the directional antenna on the radar and find the direction with the highest signal strength at the receiver. In this paper, we leverage RIS, a passive reflecting antennas array in which each antenna can dynamically modulate the phases of reflected signals. As shown in Figure 1, with well-designed configurations, RIS can generate steerable Wi-Fi beams by reflecting radio waves emitted from the AP. With RIS beam scanning, the clients can extract CSIs from received packets to generate their own angular power spectrum (APS). Then the clients can indicate their directions viewed from the RIS by finding the highest peak in the APS. In RIScan, we call this direction as **RIS angle of departure (RAoD)**. Since all directions are scanned by the RIS each round, the RAoD of every client can be determined within a single scan, and thus the localization latency does not increase with the number of clients. Then, the clients' positions can be obtained by combining the direction estimation results from two RIS anchors.

Despite the enormous advantage of client scalability, RIS-based localization encounters more challenges than classical AP-based localization. There are three parties in traditional AP-based localization, the AP, the client, and the environment with static and moving objects, while in RIS-based localization, one more party, RIS, is involved. In principle, the key of localization is to accurately identify the anchor signal from superimposed signals at the receiver. The anchor signal is the AP-client direct path in AP-based case, while it is the RIS-client path in RIS-based case. It is noted that we need to handle more complicated signal superposition in RIS-based localization, including `AP-client` direct path, the traditional `AP-Env-client` multipath, the path caused by RIS configuration `RIS-client` and the RIS-induced multipath `RIS-Env-client`. We need to extract the `RIS-client` from the others to enable accurate RIS-based localization.

More specifically, to achieve this target, we have to address the following challenges. First, RIS-related paths are overwhelmed by `AP-client` path and `AP-Env-client` multipath, which leads to RIS beam direction finding failure, and we need to separate them out. However, existing techniques cannot fully address this problem. For example, SpotFi [19] extracts the anchor signal, `AP-client` path based on its smaller ToF compared to other paths. In RIS-based scenario, this method can not distinguish the anchor signal `RIS-client` and `AP-client` path. MetaSight [41] is a RIS-based solution to localize RFID tags. It modulates the `RIS-client` signal into another frequency band for separation. However, it will result in substantial channel switching overhead of clients and thus interrupt the communication between AP and clients. Thus, we need to design a systematic scheme to extract `RIS-client` path precisely. Second, there may be not only one path for the RIS beam to arrive at the clients due to reflection and scattering, especially in a complex environment. Some reflectors would redirect the signals from RIS to the client even when the RIS is not steering towards the client. In this paper, we call the `RIS-Env-client` path as RIS multipath. The RIS multipaths will result in many confusing peaks in the APS.

To tackle these challenges, our core idea is to leverage the configurability of RIS to make the `RIS-client` path more prominent than the others. Firstly, we design a pair of configurations with a 180-degree phase difference to separate `RIS-client` from the `AP-client` direct path and the static part of `AP-Env-client`. Then, we comprehensively analyze the dynamic part of `AP-Env-client` and design a RIS configuration sequence and a phase pattern detection mechanism to suppress their impact on RIS beam direction finding. Specifically, we classify the dynamic interferences into three categories, *i.e.*, surrounding interference, crossing the AP-client path, and crossing the RIS-client path, and then observe the difference between channel variation patterns caused by these interferences and that caused by RIS to drive the design. Finally, we delve into the formation of `RIS-Env-client` paths and design a special RIS configuration sequence to eliminate its effect. Specifically, we observe that RIS multipaths are created under a specific condition. Thus, we configure RIS strategically to destroy the conditions while preserving the stable `RIS-client` path across all configurations.

We implement RIScan using an AP, two customized RISs and several clients. The AP and clients are mini-PCs equipped with commodity Wi-Fi NICs. The key mechanisms are validated with extensive experiments in two different environments. The results show that RIScan achieves a median localization error of 47cm and 71cm in static and dynamic environments with only two RIS anchors. RIScan is at least 12.5× faster than the SOTA when simultaneously localizing more than ten users.

Our contributions can be summarized as follows:

- To the best of our knowledge, RIScan is the first Wi-Fi-based multi-user indoor localization system that has low latency and is robust to dynamic interference.
- We take full advantage of RIS's capability to customize the wireless environment. We design a novel algorithm to extract the RIS component from the superimposed channel and design mechanisms to suppress environmental disturbance, which makes the systems robust against dynamic interference and confusing multipaths. These mechanisms can inspire other Wi-Fi sensing applications and improve their robustness.
- We prototype RIScan with COTS Wi-Fi devices and customized RIS hardware. Extensive experiments in two indoor environments demonstrate excellent RIScan performance in multi-user scenarios.

2 SYSTEM MODEL AND CHANNEL MODEL

2.1 System Model

RIScan comprises three entities: a Wi-Fi AP, two RISs, and several clients. The Wi-Fi AP and clients are mini-PCs equipped with commodity Intel 5300 NICs. RISs reflect and modulate the radio wave transmitted by the AP. With proper configurations, RISs can generate steerable reflective beams and execute a RIS beam scanning mechanism. Then the clients receive these packets and extract CSIs. Based on a series of CSI, the clients can determine their RAoDs. Then clients can estimate their locations by combining the RAoDs from two RISs with triangulation.

2.2 Channel Model

The channel model here is to reveal how RIScan can assist the localization. In this paper, we introduce a RIS with M columns and N rows of reflecting antennas. For simplicity, we first consider the RIS with only one row. Each antenna element will produce a controllable transmission path, called a RIS path. Considering the i-th antenna element, a RIS path consists of three stages: as shown in Figure 2, the signal first travels from the AP to this element, which is called the AP-RIS path or AR path; then it is reflected by the antenna element, where the reflection loss is denoted by Γ which is the same for each element; at the same time, each element will shift reflected signal a configurable phase offset $\phi_c(i)$; at last, it travels from this RIS element to the client, called the RC path. We can express the channel of the i-th RIS path as:

$$\begin{aligned} h_{RIS}(i) &= A_{AR}(i)e^{-jkd_{AR}(i)}\Gamma e^{j\phi_c(i)}A_{RC}(i)e^{-jkd_{RC}(i)} \\ &= A_{AR}(i)A_{RC}(i)\Gamma e^{-jk(d_{AR}(i)+d_{RC}(i))}e^{j\phi_c(i)}, \end{aligned} \tag{1}$$

where $A_{AR}(i)$ and $A_{RC}(i)$ are the attenuation factor of the AR path and RC path for the i-th RIS path, respectively; $d_{AR}(i)$ and $d_{RC}(i)$ is the length of these paths; k is the wave number, i.e., $k = 2\pi/\lambda$. Let $A(i) = A_{AR(i)}A_{RC(i)}\Gamma$ denote the amplitude of i-th RIS path. Then we can model the whole RIS channel as:

$$h_{RIS} = \sum_{i=1}^{M} A(i)e^{-jk(d_{AR}(i)+d_{RC}(i))}e^{j\phi_c(i)}. \tag{2}$$

Without loss of generality, we assume the distance between RIS and client is far, which meets the requirement of far-field conditions [18]. Then we can assume that the RC paths of all RIS elements are parallel. Under this assumption, the difference in path length between two adjacent RC paths is $d\sin(RAoD)$, where d is the spacing between the elements on RIS. Then the phase of i-th RIS path can be written as:

$$\phi_{RIS}(i) = -k(d_{AR}(i) + d_{RC}(1) - (i-1)dsin(RAoD)) + \phi_c(i). \tag{3}$$

Obviously, if we align the phases of all RIS paths, the amplitude of h_{RIS} becomes maximum which can be achieved by setting a set of appropriate ϕ_c.

In practical deployment, the location of the AP and RIS are fixed so we can easily obtain d_{AR}. Hence, we can derive the RAoD by maximizing $|h_{RIS}|$. However, for a b-bit RIS, there are 2^{bMN} different configurations, which is a huge search space. Thus, an exhaustive search is not a feasible solution. Besides, the target of RIScan is to localize multiple clients simultaneously, which makes it impractical to search for an optimal RIS configuration for each client device.

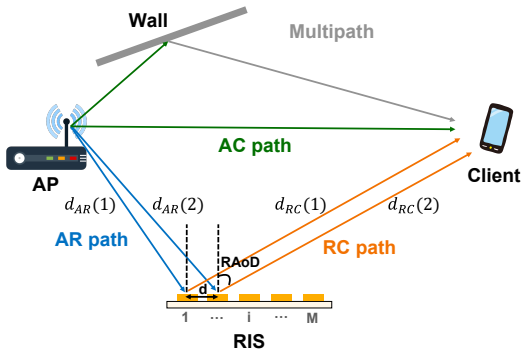


Figure 2: The channel model in RIScan.

To make things worse, the indoor wireless channel is made up of multiple propagation paths in the environment. Besides the AP-client (AC) direct path, radio waves can also arrive at the receiver by reflection, diffraction or scattering. Hence, the composite channel observed by the client can be expressed as:

$$h_{received} = h_{AC} + h_{multipath} + \sum_{i=1}^{M} A(i)e^{j\phi_{RIS}(i)}, \tag{4}$$

where h_{AC} is the direct channel from AP to client, $h_{multipath}$ is the combination of all multipath signals. Therefore, the RIS component is buried in other propagation paths. In addition, the AC path and multipath profile will change with the user position and other dynamic interferences in the environment. Hence, we cannot directly estimate the RAoD by maximizing the received signal strength.

3 SYSTEM OVERVIEW OF RISCAN

The overall procedure of RIScan is shown in Figure 3. First, a host sends a synchronization signal to the AP and a RIS. Then, the AP starts broadcasting packets, and the RIS modulates the incoming radio waves and generates reflective beams with well-designed configurations. These steerable Wi-Fi beams sequentially scan the environment and induce channel changes. During the scanning, the clients extract and process a series of CSI from received packets simultaneously. The overwhelmed RIS components can be extracted from the superimposed channels by calculating the difference of CSI affected by a pair of special configurations. Hence, the clients can obtain their own APSs.

To improve the system robustness in multi-user scenarios, the dynamic interferences need to be suppressed. To achieve that, a special configuration sequence is designed. With it, weak interferences can be suppressed by channel differences directly. In terms of severe interferences (e.g., users crossing the AC path), we design a phase pattern detection mechanism for it. This mechanism can distinguish the desired RAoD estimate from multiple misleading RAoD estimates due to interferences.

However, reflections in the environment can also cause confusing RIS multipaths. A special beam scanning sequence is designed to destroy the formation conditions of these reflections. If the clients detect more than one RIS-related path signals with the phase pattern

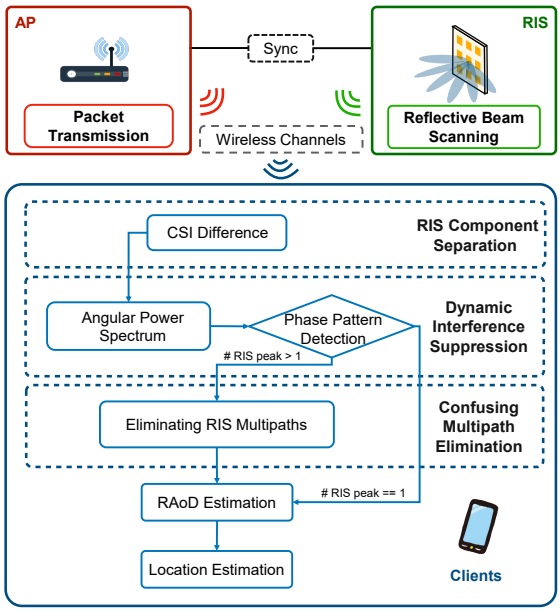


Figure 3: The system overview of RIScan.

detection mechanism, the system will apply this beam scanning sequence to eliminate the undesired RIS multipaths.

To avoid interference between RISs, RISs cannot operate beam scanning at the same time. Therefore, when the localization service begins, the host will notify the first RIS to start beam scanning and wait for it to complete before telling the next RIS to start. For each client, the location can be determined by combining the estimated RAoDs from two separate RISs with triangulation. The details of the key mechanisms will be mentioned in the following section.

4 ROBUST DIRECTION ESTIMATION

In this section, we will first introduce how RIScan achieves direction (RAoD) estimation in a static environment. Next, a special set of configurations and a phase pattern detection mechanism are proposed to improve RIScan's robustness to dynamic interference. At last, we eliminate confusing RIS multipaths caused by reflection.

4.1 RIS Beam Scanning

Here, we illustrate how RIScan performs RAoD estimation. For simplicity, we first consider there is only the RIS component arriving at the user device. In Section 2.2, we mentioned that the search space of maximizing $|h_{RIS}|$ is huge, which will cause a large localization latency. Inspired by direction finding technology [36], we can shrink the search space by executing beam scanning. The idea is that we do not derive RAoD by finding the optimal configuration but search through all possible directions θ to generate an APS and determine which is the RAoD. In this way, we reduce the search space from 2^{bMN} to $2\beta+1$, if we search among $[-\beta, \beta]$ at 1° granularity. Furthermore, the search time does not increase with the number of clients, which brings RIScan the benefits of finding RAoDs for multiple clients at one round of scan.

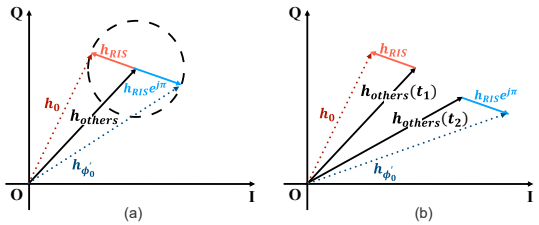


Figure 4: The IQ diagram of channel in (a) static environment and (b) environment with dynamic interference.

To achieve RIS beam scanning (RBS), we align the phase of all RIS paths at a certain direction θ. For 2D beam scanning, the RBS-codebook of a 2-dimension RIS is:

$$\phi_c(m,n) = k\left[d_{AR}(m,n) + d_{RC}(n/2,1) - (m-1)dsin\theta\right] + \phi_0 \quad (5)$$

where $1 \le m \le M, 1 \le n \le N$ and ϕ_0 is a phase constant that does not affect the corresponding $|h_{RIS}|$ (it will be used in the later section). When the RIS steers the beam direction from $-\beta$ to β, the clients measure the signal strength and determine the direction θ with the largest signal strength to be its RAoD, i.e., $RAoD = max_\theta(|h_{RIS}(\theta)|)$.

4.2 RIS Component Separation

In Section 4.1, we only consider the RIS channel. However, in practical situations, the received signals also contain the AC direct path and multipaths. Therefore, the received signal strength may not be maximum when the RIS steers at the RAoD. Our key insight is extracting RIS components by altering RIS configurations and canceling the invariant components. Here we assume that the environment is static where the AC and multipath signals are stable (we leave the dynamic interference case to Section 4.3). Remember the phase constant ϕ_0 in Section 4.1. It's a phase constant adding to all RIS elements and notes that no matter what its value is, it won't affect the alignment of the RIS paths and the corresponding $|h_{RIS}|$. We let the AP send two packets to the client which we set ϕ_0 to 0 and ϕ_0', respectively. Then the client estimates the channel h_0 and $h_{\phi_0'}$, which are as follows:

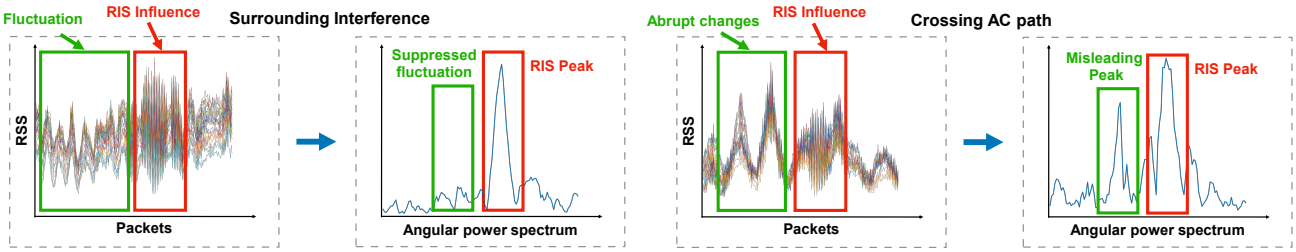
$$\begin{aligned} h_0(\theta) &= h_{AC} + h_{multipath} + h_{RIS}(\theta) \\ h_{\phi_0'}(\theta) &= h_{AC} + h_{multipath} + h_{RIS}(\theta)e^{j\phi_0'} \end{aligned} \quad (6)$$

As the static environment assumption, h_{AC} and $h_{multipath}$ won't change. By subtracting $h_{\phi_0'}(\theta)$ from $h_0(\theta)$, we can cancel the AC and multipath components and get the differential of RIS component:

$$|\Delta h(\theta)| = \left|h_0(\theta) - h_{\phi_0'}(\theta)\right| = |h_{RIS}(\theta)|\left|1 - e^{j\phi_0'}\right|. \quad (7)$$

For a given ϕ_0', $\left|1 - e^{j\phi_0'}\right|$ is a constant. $\Delta h(\theta)$ has the maximum magnitude when $|h_{RIS}(\theta)|$ is maximized. Then, RIScan can steer signals at different directions θ and each client can find the θ that maximizes $|\Delta h(\theta)|$.

A remaining problem is how to choose the best ϕ_0'? In RIScan, we set ϕ_0' to π for two reasons. The first reason is that the channel difference $|h_0(\theta) - h_{\phi_0'}(\theta)|$ has the maximum value $2|h_{RIS}(\theta)|$ when $\phi_0' = \pi$. As shown in Figure 4 (a), changing ϕ_0' is equivalent to vector rotation, and its rotation trajectory forms a circle with $|h_{RIS}|$ as the radius. Since the other components h_{others} (including h_{AC} and



(a) Surrounding interference (b) Crossing AC path

Figure 5: The RSS of raw channel estimates for 30 subcarriers and the corresponding final APS.

$h_{multipath}$) in the received channel are the same, the amplitude of the differential channel is the length of the chord of the circle. When the phase is set to π, its value reaches the maximum which is the diameter of the circle. The larger $|h_0(\theta) - h_{\phi_0'}(\theta)|$ means RIScan can better combat electromagnetic noise in actual deployment and improve the working range. Second, almost all phase-shifting-based RIS designs support the two configurations of 0 and π.

4.3 Dynamic Interference Suppression

However, in the multi-user scenario, the movement of surrounding persons will change the wireless environment. These movements will create some dynamic, unpredictable multipaths which will introduce unwanted interferences. Assume we set ϕ_0' to 0 at time t_1 and π at time t_2, then we separate the RIS component as the following equation:

$$|\Delta h(\theta)| = |h_{AC}(t_1) - h_{AC}(t_2) + h_{multipath}(t_1) - h_{multipath}(t_2) + 2h_{RIS}(\theta)|. \quad (8)$$

As shown in Figure 4(b), in this situation, the other path components can't be canceled and $|h_{RIS}(\theta)|$ is not directly correlated with $|\Delta h(\theta)|$.

In order to achieve a robust localization system, we classify the dynamic interferences into three categories, including surrounding interference, crossing AC path, and crossing RC path. Then we analyze their characteristics and design the corresponding algorithms.

4.3.1 Surrounding interference. Surrounding interference is caused by people walking near the system but not crossing the AC or RC path. Our key observation is that surrounding interference will not cause abrupt channel changes. There are two reasons for this. First, this interference is caused by the variations of multipath reflected by people walking around. Compared with the AC path, multipaths have longer transmission distances and larger reflection loss, so they have a weaker influence and won't cause large changes in channel estimates. Second, compared with the packet rate of Wi-Fi devices, human motion is slow. In other words, $|h_{multipath}(t_1) - h_{multipath}(t_2)|$ is very small when $|t_1 - t_2|$ is small. Based on this observation, we design a special configuration sequence to eliminate the surrounding interference.

Since the surrounding interference does not change $|h_{AC}|$, we only need to minimize $h_{multipath}(t_1) - h_{multipath}(t_2)$, then $|\Delta h(\theta)| \approx 2|h_{RIS}(\theta)|$. In order to achieve this goal, we arrange the two RIS phase configurations for θ ($\phi_0 = 0$ and $\phi_0 = \pi$) consecutively. The optimal configuration sequence of beam scanning among $[-\beta, \beta]$ at 1° granularity is shown in Figure 6. Since a packet corresponds

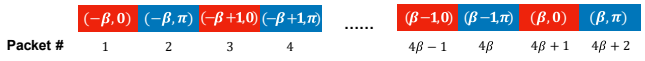


Figure 6: The optimal configuration sequence.

to a configuration, the time interval of these two configurations $|t_1 - t_2|$ is just the 1/packet rate.

Figure 7(a) shows the relationship between packet rate and the interference suppression performance. The blue points are the raw channel estimations and differential channels of two adjacent packets with a packet rate of 50Hz, 100Hz, and 1000Hz are shown in green, yellow, and red points, respectively. In the IQ diagram, the closer a point is to the origin, the smaller its magnitude. We can see that the points (except for blue) are centered near the origin, and the higher the packet sending rate, the closer they are to the origin, and thus the weaker the impact of surrounding interference on our system. In RIScan, we set the packet rate to 1000Hz, which can be achieved by commercial COTS Wi-Fi NIC. Hence, the multipath profile can be considered to be stable within 1ms and $h_{multipath}(t_1) - h_{multipath}(t_2) \approx \vec{0}$. As shown in Figure 5 (a), affected by surrounding interference, the received signal strength (RSS) fluctuates. In the APS, this interference is well suppressed by our designed configuration sequence. Here, we add up the APS of all 30 subcarriers as the final APS.

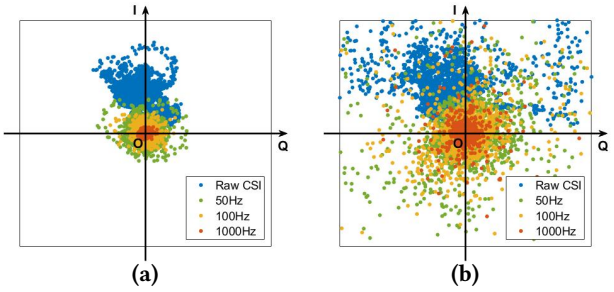


Figure 7: The relationship between the interference suppression performance and packet rate. (a) Surrounding interference. (b) Crossing AC path.

4.3.2 Crossing the AC path. Different from the surrounding interference, walking across the AC path will bring drastic channel change. Since the AC path is usually the strongest component in the

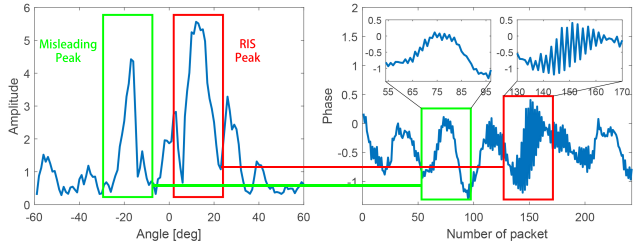


Figure 8: Eliminating the misleading peak based on the phase pattern characteristics.

combined channel, blocking it will vary the phase and amplitude significantly in a very short time. Therefore, as shown in Figure 7(b), though most points are still concentrated near the origin, some aberrant points cannot be removed. According to Equation 8, this drastic change in AC path will increase the magnitude of the differential channel and produce a misleading peak in APS which confuses the direction estimation (as shown in Figure 5 (b)).

To deal with this case, we observe that the misleading peaks and RIS peak have different phase patterns. Recall the optimal RIS configuration sequence in Figure 6, ϕ_0 is set to 0 and π alternately. For a certain beam direction, two configurations with the ϕ_0 of 0 and π will cause the superimposed channel to rotate at a certain angle in the IQ diagram (Figure 4(a)), that is, the phase of the superimposed channel will change. As shown in Figure 8, this pattern is especially noticeable when the beam is scanned close to the client because the energy of the RIS component gets maximum at that time. However, the phase patterns of misleading peaks are usually random. Thus, we apply phase pattern detection to recognize the RIS peak. First, we select 3 peaks with the largest amplitude in the APS. For each peak, to detect its phase pattern, we extract channel estimations around this peak with a length of N and then calculate the phase difference between the adjacent phases. Next, we just count the number of alternative signs in this phase difference sequence and denote it by l. If the ratio of l to N is larger than a threshold (80% in RIScan), then this peak is considered a RIS peak.

4.3.3 Crossing RC path. For the interference caused by crossing the RC path, the human body will absorb part of the RF energy reflected by the RIS and introduce dynamic disturbance. In this case, the RIS peak will be destroyed and lead to direction estimation failure. Note that only when the beam steers close to the client, persons moving across the RC path will disturb direction estimation. Thus, the probability of this interference is low. What's more, since the user will not move a large distance in a short period of time, the RAoD will not change greatly. Therefore we can apply a clustering algorithm to exclude invalid measurements.

Note that the interference caused by crossing AP-RIS (AR) path is similar. Since the locations of AP and RISs are fixed, in actual deployment, we can place the AP at a higher position to avoid blocking the AR path, such as installing the AP and RISs on the ceiling.

4.4 Confusing RIS multipath Elimination

The RC path is not always the only path from RIS to the client. For example, some reflectors in the environment would redirect the

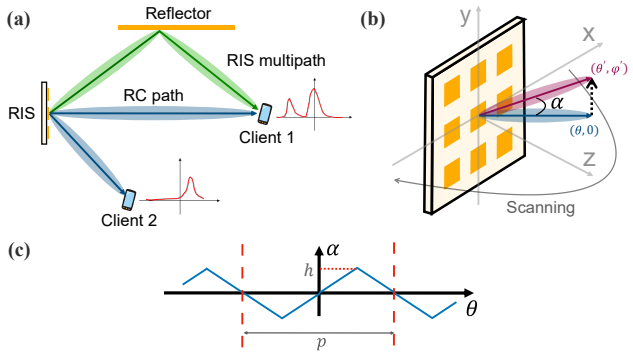


Figure 9: (a) Illustration of RIS multipath. (b) The pitch angle α which lifts the beam up along the y-axis. (c) The variation of the pitch angle α.

signals from RIS to the client even when the RIS is not steering towards the client, as shown in Figure 9 (a). To differentiate this type of multipath from the multipath signals in Figure 2, we call it RIS multipath. In the indoor environment, small spaces and various furniture create conditions for RIS multipath. These RIS multipaths will generate confusing peaks in the APS. In the worst case, one RIS multipath may have the largest amplitude when the RC direct path between the RIS and the client is blocked by some obstacles. Note that phase pattern detection in the previous section cannot be used to eliminate them because RIS multipaths also have the same phase pattern as the RC path.

To suppress RIS multipaths, we are inspired by the observation in ArrayTrack [42] that when the transmitter, the receiver, or the objects between them move slightly, the reflection path usually changes significantly while the direct path is stable. The main reason for this phenomenon is that the condition to generate a stable reflection path is hard to satisfy in a real deployment. What's more, the conditions to generate stable RIS multipaths are even stricter. Recall that the RIS beam is composed of many phase-aligned paths reflected by antenna elements on RIS, and thus its pattern is fragile. In general, to create strong RIS multipaths, it needs to meet two conditions simultaneously. The first is that the reflecting surface should be smooth. When the RIS beam strikes an uneven surface, scattering will destroy its directivity. The second is that the position of the RIS, reflector, and client device needs to satisfy the law of reflection, that is, the incident angle is equal to the reflection angle.

Based on this observation, we proactively change the configurations of RIS to eliminate RIS mulipaths. We prevent the formation of strong RIS multipaths by applying some special perturbations during beam scanning. Then, we could identify the RC path by finding almost invariant peaks in the two measurements. More specifically, in the previous sections, the RIS beam is scanned in the horizontal plane, and now we introduce a pitch angle α which lifts the beam up along the y-axis, as shown in Figure 9 (b). And the pitch angle varies with beam scanning direction θ (Figure 9 (c)). It is a triangle wave with a maximum h and a period p. In RIScan, we set h and p to 5° and 20°, respectively. This scheme has two advantages. First, different from ArrayTrack [42], RIScan does not require the user to actively cooperate with the system to move a certain distance to

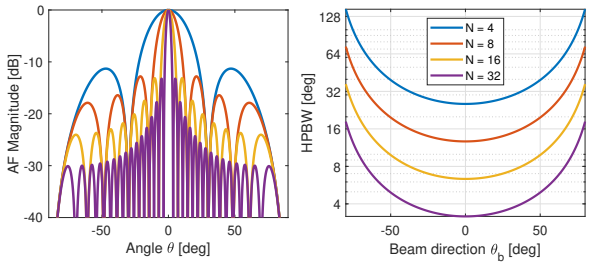


Figure 10: The impact of the number of RIS element

distinguish RIS multipaths. Second, the pitch angle does not change the projection on the horizontal plane, which indicates that this scheme will not distort the RAoD.

5 PRACTICAL ISSUES OF RISCAN DESIGN

5.1 RIS Element Number Trade-off

The number of RIS elements significantly impacts the angular resolution of RAoD estimation. For a N element linear array with uniform spacing, the array factor(AF) [8] can show the RIS beam pattern and the relationship between the half-power bandwidth (HPBW) and beam direction θ_b. The simulation results depicted in Figure 10 indicate that when the number of RIS elements increases, the HPBW decreases, and the angular resolution improves. Additionally, more RIS elements will enhance the energy of the RIS path and expand the working range. However, it also escalates the complexity of the control circuit and the overall manufacturing cost. Therefore, to strike a balance, 16 elements are chosen for each dimension of the RIS.

In addition, though RIS can generate beams covering the whole 180°, it is observed that the HPBW expands as the beam direction $|\theta_b|$ increases, and becomes excessively large at certain extreme beam directions (for instance, those greater than 60°). Besides, although the localization delay of RIScan will not increase with the number of clients, it will increase with the number of scanned beam directions. Consequently, to enhance the precision of RAoD estimation and reduce the time overhead, the beam scanning direction is restricted to a range of $[-60°, 60°]$ at 1° granularity. It is worth noting that most beamforming-related works[12, 41] limit the beam angle to this range to obtain greater gain.

5.2 RIS Quantization Error

In the previous sections, we assume that RIS can provide continuous phase control. Although smart surfaces that can achieve continuous phase control [31] have been proposed, they have large response latency and increase the complexity of control circuit design, making them less practical. Therefore, many prototypes with discrete phase configurations [12, 13, 53] have attracted the attention of researchers. Nevertheless, these designs will introduce quantization errors. For RIScan, we need to consider two factors, the directivity reduction and beamforming error caused by quantization error. The reduction of directivity for 1- to 3-bit designs is 3.87dB, 0.88dB, and 0.21dB, respectively [39]. The 2-bit setting offers the largest marginal gain with an acceptable loss. In addition, the quantization error will not lead to an apparent angular resolution degradation [38] when there are 16 elements on each RIS dimension. Since more discrete configurations will increase the cost of the control circuit, we choose to design a 2-bit smart surface.

5.3 Elminate Phase Distortions for COTS Wi-Fi Device

RIScan aims to achieve multi-user indoor localization on commodity user devices. However, in practical deployments, the CSI extracted by receivers carries a time-varying random phase offset $e^{-j\theta_{offset}}$ due to the lack of accurate synchronization between the transmitter and receiver. This makes the RIS component separation mentioned in Section 4.2 fail. The distorted CSI can be expressed as:

$$h_{distorted} = e^{-j\theta_{offset}}(h_{AC} + h_{multipath} + h_{RIS}). \quad (9)$$

Observing that this random phase offset is equal on different antennas of the same receiver, the works [35] and [50] use a phase difference to cancel it. The authors of [50] have demonstrated that when there is only one length-varying reflected path in the environment and its attenuation is stable, the variation of this phase difference of the overall channel roughly matches changes in the length of this path. However, there is more than one reflection path in our situation. Without loss of generality, we can approximate that the path reflected by each RIS antenna has the same attenuation due to their close path lengths and identical reflection loss. Then these RIS element paths can be considered as a combined reflection path. Then recall the configurations pair used in Section 4.2, they differ only in phase and have the same attenuation.

Hence, we can use the phase difference between two antennas as the corrected phase. Note that $e^{-j\theta_{offset}}$ will not distort the amplitude of the overall channel. So we modify distorted CSI as:

$$h_{modified} = |h_{distorted}(RX_1)|e^{j(\theta(RX_1)-\theta(RX_2))}, \quad (10)$$

where RX_1 and RX_2 are two antennas of the receiver. Then, the energy of the RIS component can be extracted successfully from commercial Wi-Fi devices.

6 IMPLEMENTATION

6.1 RIScan Hardware

RIScan hardware comprises customized RISs and FPGA-based control circuits, as shown in Figure 11. We design the RIS according to the design principle in [12]. We implement our smart surface with 2-bit phase configurations. Each antenna element has a three-layer structure, the upper patch, the slot-loaded layer, and the ground. The key component is the middle layer which contains five Skyworks $SMP1340-040LF$ PIN diodes operating at frequencies from 10MHz to 10GHz. By setting the voltage of two DC biasing lines to -0.9V or 0.9V, these PIN diodes switch between ON and OFF states and provide four different phase offsets (i.e., 0, $\pi/2$, π, and $3\pi/2$). We manufactured our smart surface with a standard $Rogers4350B$ substrate. The central frequency is 5.5GHz. The three-layer structure enlarges the bandwidth to 600MHz, which makes the working band cover the whole 5GHz Wi-Fi band. The size of our smart surface is $31cm \times 31cm \times 0.4cm$, which allows it to be hidden behind upholstery (e.g., paintings).

There are 16×16 antenna elements in our smart surface, and it needs $16 \times 16 \times 2 = 512$ control signals. We customized and implemented an FPGA-based control circuit with 512 independent

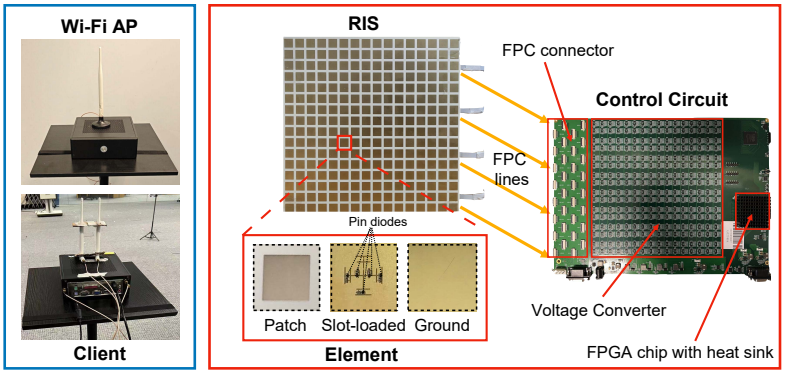


Figure 11: Prototype of RIScan.

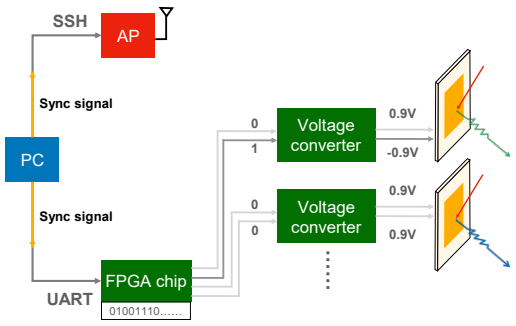


Figure 12: Illustration of RIScan's circuit architecture.

control ports. We use a *Kintex* 7*K*325 FPGA chip to generate the control signal of each IO port. The latency for this FPGA chip to update all the IO ports is at a microsecond level and guarantees the fast configuration switch in Section 4.3. Since the output voltage of the FPGA chip does not match with the PIN diodes, we design a voltage conversion circuit, on which the key components are two transistors, *MMBT*3904 and *MMBT*3906. The smart surface is connected to the control circuit via FPC lines.

For power consumption, since the smart surface is a passive device that only reflects RF energy from the environment, all the power consumption comes from the FPGA-based control board. The static control board draws around 90mA from 12V (the power is around 1.08W). When providing 512 independent control signals, the measured average power is about 2W, which is about 1/6 of the power consumption of a typical AP[1, 2]. The cost to manufacture a RIS system (including the control circuit) is around $350, of which the IC components and PCB manufacturing each cost about $175. Hence, the total system which includes two RISs costs around $700. However, the cost of PCB manufacturing can be significantly reduced by using *FR*4 substrate instead of *Rogers*4350*B*. For a RIS, the PCB manufacturing cost can be reduced to $58. For large-scale production, the manufacturing cost of PCB and the price of IC components will be greatly reduced, and the cost of the entire system will be reduced to approximately $340 (the cost of each RIS is approximately $170). Although the cost of deploying RIS is somewhat high, it is worth noting that RIS is proposed as an important technology in 6G communication, which means that it will be a common communication infrastructure in the future. Therefore, RIScan can reuse RISs deployed for communication purposes to achieve multi-user localization.

6.2 Client and AP

The clients and AP are implemented via min-PCs with commercial Intel 5300 network cards. In RIScan, we only require that the AP has one antenna and the clients have two antennas. Note that the most common commercial Wi-Fi devices (e.g., smartphones) are equipped with two antennas. We collect the CSI of each packet with the CSI Tool [14]. We evaluate RIScan and baselines in Wi-Fi channel 140, with a central frequency of 5.7GHz and a bandwidth of 20MHz. The results can be generalized to other channels.

6.3 Synchronization

Since RIScan collects a series of CSI under different RIS configurations to estimate RAoD, the clients should be synchronized with the RIS so that they are aware of the current configuration. In our implementation, a PC connects with the AP via gigabit Ethernet and communicates to the RIS control circuits with UART. The clients are set in listening mode. When the PC sends a trigger signal to the AP and the RIS controller simultaneously, the AP begins to send Wi-Fi packets and the RIS starts to execute a preset configuration sequence with the same rate of 1000Hz. Therefore, when the first packet is received by the clients, it indicates the start of the RIS configuration sequence, and then the following packages and RIS configurations are corresponding.

7 EVALUATION

In this section, we conduct extensive experiments to demonstrate the effectiveness of RIScan. First, we introduce the detailed experimental setting and the baselines we compared. Then, we evaluate the end-to-end performance of RIScan in the static environment. Next, we evaluate how well RIScan handles interferences that are unique to multi-user scenarios. Specifically, we verify RIScan's performance against interference among users' Wi-Fi devices in Section 7.3 and interference caused by other users (humans) in Section 7.4, respectively. Finally, we assess the RIScan's localization latency in multi-user scenarios in Section 7.5.

7.1 Experiment Setup

Experiment Scenarios: To evaluate RIScan, we deploy our system in two different spaces. The first space is an ideal one where all testing positions have the Line-of-Sight (LoS) paths. As shown in Figure 13 (a), the 6.5 × 13 m room is spacious and has a minor multipath effect. One AP and two RISs are deployed on one side of the room. These two RISs are separated by 2 m and placed 2 m away from the AP on both sides. The client device is iteratively deployed at 40 different testing locations covering an area of $4 \times 7m$ for data collection. The spacing of testing locations is set to 1m, and the maximum distance between the client and a RIS is 10 m. Note that we also evaluate the system performance with interference among users' Wi-Fi devices and interference caused by other users (humans) in this room under different settings which will be specified in corresponding sections.

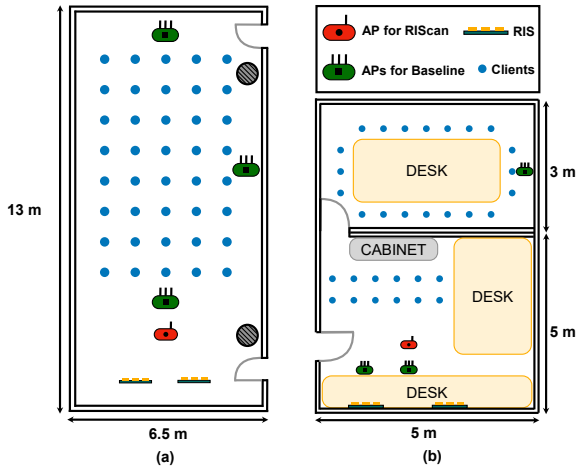


Figure 13: Experiment setup. (a) A simple spacious space that spans 84.5 m^2. (b) A complex messy space that spans 40 m^2.

As shown in Figure 13 (b), the second space is much more challenging, which contains two small rooms separated by a wall. In both rooms, there are various furniture and sundries that create rich multipaths. We deploy the RIScan system in the outer room with 12 testing locations while the other 20 testing locations is set in the inner room. The spacing of testing locations is set to 0.5 m. The inner room can be considered as a typical NLoS scenario.

Comparison with Baselines: We reproduce two SOTA indoor localization systems, SpotFi [19] and UbiLocate [25], as our baselines. Both of them leverage Wi-Fi CSI to estimate the client's location. Spotfi applies a 2D MUSIC algorithm to estimate AoA and achieve decimeter-level localization with at least 3 APs. UbiLocate combines AoA and ToF to achieve localization with an improved AoA estimation algorithm and a modified Fined Timing Measurement(FTM) protocol. Without modifying hardware and protocols, their localization algorithm can run with only AoA information. In our experiments, both baselines are implemented using several mini-PCs equipped with Intel 5300 NICs. As shown in Figure 13, both Spotifi and UbiLocate employ 3 APs to localize clients, while RIScan only employs one AP.

7.2 RIScan's Overall Performance

In this section, we first demonstrate RIScan's overall end-to-end performance in two static scenarios and compare its performance with baselines.

7.2.1 LoS Scenario. We first evaluate our system under the LoS scenario as shown in Figure 13 (a). The cumulative distribution functions (CDF) of the angular estimation errors and localization errors for all systems are shown in Figure 14 (a) and Figure 14 (b), respectively. For angular estimation, RIScan achieves a median error of 1.3 degrees, while UbiLocate and Spotfi have a significantly higher median error of 5.2 and 5.4 degrees, respectively. In addition, we can observe that RIScan gets a more stable performance where the maximum error of 90% measurements is less than 3.9 degrees compared to that of UbiLocate and Spotfi at 18 degrees and 24 degrees, respectively. We attribute the improvement to the high angle resolution beam created by all reflective RIS antennas, as

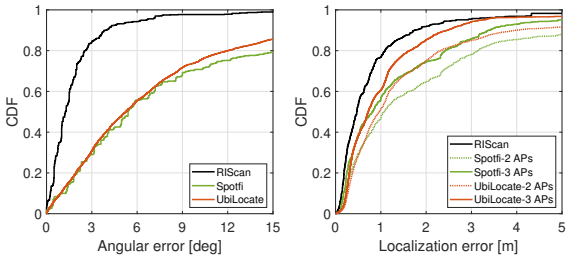


Figure 14: Overall performance comparison with SOTA Wi-Fi localization systems in LoS scenario.

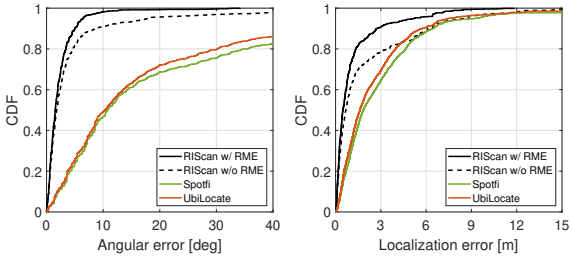


Figure 15: Overall performance when different baselines go against multipath and NLoS conditions.

described in Section 4.1. Based on the precise angle estimation, RIScan achieves a median localization error of 47 cm. On the other hand, UbiLocate and Spotfi have a median error of 73 cm and 82 cm, respectively. Note that RIScan only uses two pieces of angle information while baselines combine three. Under the setting with two APs, the median error of UbiLocate and Spotfi will increase to 97 cm and 109 cm, respectively.

7.2.2 Impact of Multipath and NLoS Conditions. We further conduct an experiment on a more complex scenario, as shown in Figure 13 (b). It is challenging for all localization systems to get a good localization performance because this scenario is rich in multipath and blockage. Although we eliminate the multipath components as discussed in Section 4.2, this complex environment will still lead to many confusing peaks in the APS, as the reflection will make the RIS beam have more than one path to the client.

The results are shown in Figure 15. We can see that RIScan achieves a similar median angular error of 1.6 degrees and 1.8 degrees when turning on/off the RIS multipath elimination (RME) scheme. The 95th percentile angular error declines from 17.9 to 6.5 degrees when eliminating confusing paths. These results demonstrate that our algorithm is effective in recognizing the direct RIS path. In contrast, UbiLocate and Spotfi, which uses relative ToF to distinguish the LoS path achieve a median angular error of 10.3 degrees and 11 degrees, respectively.

With RME, RIScan's median localization error is 50 cm. In contrast, the median error of UbiLocate and Spotfi is 161 cm and 184 cm, respectively. Note that the accuracy of RIScan in the NLoS scenario is close to the LoS scenario because of the stronger energy and higher angular resolution of RIS beams. In other words, RIScan

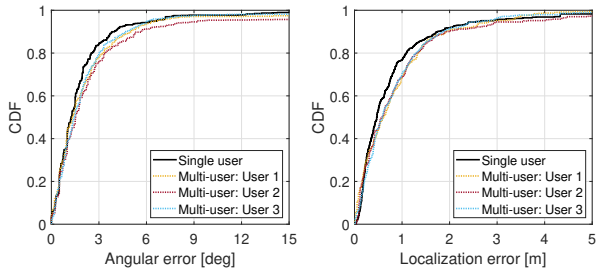


Figure 16: Robustness analysis for mutual interference among client devices.

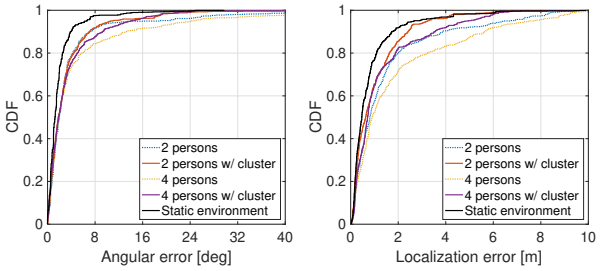


Figure 17: Robustness analysis for different degrees of dynamic interference.

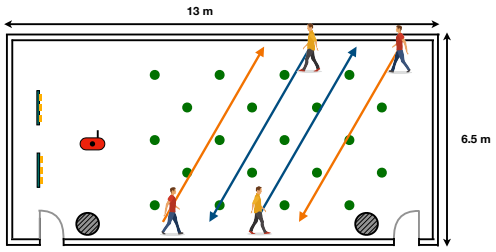


Figure 18: Experiment setup for the dynamic interference scenario.

is not sensitive to multipaths and blockages, while the performance of baselines degrades significantly in the same scenario.

7.3 Robustness to Devices' Interference

In previous sections, all experiments are conducted with only one client. Different from baseline systems, the clients in RIScan act as receivers and enjoy the localization service in parallel. It is intuitive that there will be no mutual interference among receivers, but we still want to verify if it will compromise the system's performance when localizing multiple users. To this end, we conduct this experiment by placing a group of three user devices at the 20 locations marked with green points in Figure 18. The three devices in the group are placed very close to each other, with a spacing of 0.5m, as this is the scenario where interference is most likely to occur. The environment is static without human interference. The angle estimation and localization results are shown in Figure 16. It is obvious that the performance of the three-user scenario is almost the same as the single-user scenario in both graphs.

7.4 Robustness to Humans' Interference

All the experiments discussed above are conducted under a static environment without humans' interference. However, in multi-user scenarios, we cannot ignore the dynamic interference caused by the movements of other RIScan users or other people in the environment. Here, we will verify the effectiveness of the dynamic interference suppression schemes in RIScan. As discussed in Section 4.3, we consider three types of dynamic interferences: (1)Surround: moving around clients but not crossing AC or RC path; (2)AC: crossing AC path only; (3)RC: crossing RC path only; We first independently show RIScan's suppression of each type of dynamic interference. Then a general experiment mixing all types of interference is demonstrated. Furthermore, we also evaluate our system in mobile client scenarios.

Suppress each type of interference: The RIScan system is deployed in a spacious space with 20 testing locations, as shown in Figure 18. To independently create dynamic AC interference, a person is asked to frequently walk across the midpoint of the AC path back and forth. What's more, we also consider static cases where the person stands at the midpoint of the AC path. RC interference is created in the same way. The angular estimation results in terms of static and moving cases are shown in Figure 20. For moving situations, with the optimal configuration sequence, the phase pattern detection mentioned in Section 4.3, the interferences caused by the surrounding movement and crossing AC path are well suppressed. Their median angular errors are 2 degrees and 2.1 degrees, respectively, which is very close to the error of 1.5 degrees in the situation without interference (i.e., No Inft.). As for crossing the RC path, there are more outliers, and the median angular error increases to 3 degrees. In the stationary situation, the results show that standing either around clients or in the LoS path will not affect our system. But the median error of standing at the RC path increases slightly to 2.8 degrees

Mix all interferences: Then we evaluate our system in a more general scenario where each type of dynamic interferences can be mixed with each other. As shown in Figure 18, the experiments are carried out in two cases: a two-person case (orange routes) and a four-person case (orange and blue routes), respectively. For each testing location, we let RIScan consecutively execute 30 times of location estimation (≈15 s in total) while people are walking along the parallel routes back and forth from different starting points. These people walk across the testing area and introduce dynamic interferences, which indicates that multiple types of interferences may co-occur in one measurement. As shown in Figure 17, the median angular error of the two-person and four-person cases is around 2 degrees. However, when zooming into the CDF interval from 0.8 to 1, we can observe that the result of the four-person case contains more outliers. The reason is that more people cause more complex interferences. With two RISs, RIScan achieves a median localization error of 81 cm and 90cm for the static and moving cases, respectively. Furthermore, we apply the K-means clustering algorithm to process four consecutive measurements. Then the maximum localization error of 80% measurements is less than 2 m for both cases.

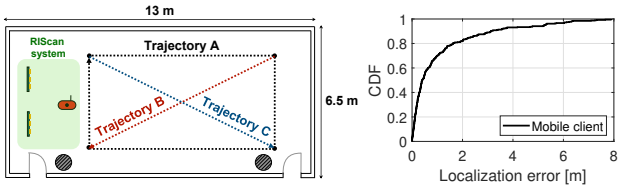


Figure 19: Positioning mobile clients with RIScan

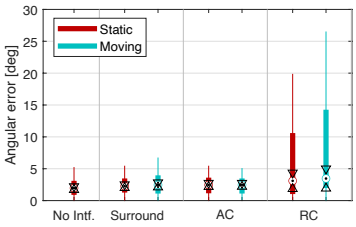


Figure 20: Error analysis for different types of dynamic interferences.

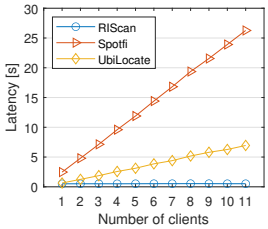


Figure 21: Comparison of localization latency.

Positioning mobile clients: We also evaluate RIScan's localization performance for moving clients. As shown in Figure 19, a person holding a receiver walks along three trajectories in a room. The moving speed is about $0.5m/s$, a typical indoor walking speed. The results demonstrate that RIScan achieves a median localization error of 52cm when the client is moving, slightly worse than the 47cm in the static scenario. Moreover, 80% of the localization errors are lower than 2m. The reason is that the change of the AC and multipath components on the client's channel caused by moving is very tiny in a short period (i.e, the time between two RIS configurations), and these interferences can be suppressed by the mechanism in Section 4.3.1. The main impact comes from the asynchronous RAoD estimation of two RISs. Since the time required for one RAoD estimation is very short (within $0.25s$), during which the client will not move a lot, RIScan is still robust in the mobile client scenario.

7.5 Localization Latency

RIScan is designed for multi-user localization with low latency. The latency of single location estimation contains the time cost of CSI collection and algorithm execution. RIScan steers the reflective beam from -60° to 60° with 1° granularity, and each direction has two configurations (Section 4.2). In total, there are 242 configurations for each scan round. Hence, RIScan will cost $484ms$ for data collection with a packet rate of 1000Hz for two RISs. Because the baselines only need one packet to estimate AoA, the time cost of their data collection can be ignored. Thus, we only consider the algorithm execution time as the latency for baselines.

We use MATLAB R2021a to run the algorithms in a PC which are equipped with a 2.7 GHz Intel Core i5 CPU and 8GB RAM, and the average execution time for one direction estimation is 30ms, 220ms, and 800ms for RIScan, UbiLocate [25], and Spotfi [19], respectively. Furthermore, in Spotfi and UbiLocate, a central server is deployed to process the data. To achieve decimeter-level accuracy, three APs are needed, which means their algorithms need to be executed three times for single location estimation. So the time required for single location estimation is 544ms, 660ms, and 1600ms for RIScan, UbiLocate, and SpotFi, respectively. The relationship between the localization latency and the number of users is shown in Figure 21. Note that both baseline systems process users' localization requests in serial, while RIScan responds to requests in parallel. When there are 5 clients, the latency of RIScan is around 0.5s, while UbiLocate requires 3.3s and SpotFi even requires 8s. When the number of clients grows to 10, RIScan can respond 12.5× faster than UbiLocate (6.27s). RIScan's latency does not increase with the number of users (or requests), making it very suitable for multi-user scenarios.

8 RELATED WORK

8.1 Device-based Indoor Localization

WiFi-based indoor localization has been extensively studied in the past decades. Here, we mainly focus on device-based indoor localization systems that estimate the location of Wi-Fi devices. Fingerprint-based indoor localization systems characterize each location using RSSI [7, 11, 46, 49] or CSI [33, 34, 40] patterns, but the proposed systems suffer unacceptable performance degradation in dynamic environments.

Model-based approaches can estimate a variety of channel parameters (e.g., AoA [19, 21, 28, 42] and ToF [16, 17, 23, 32, 48]) using multiple APs with antenna arrays and perform triangulation algorithms (e.g., 2D MUSIC [19]) for localization. Most of them rely on large antenna arrays [10, 42] and frequency hopping [30, 32, 44] for achieving decimeter-level precision under the ideal experimental setup. For those works [19, 25] built on COTS NIC, they must undergo complex and frequent device calibration, making them impractical. In addition, UbiLocate [25] builds an IEEE 802.11ac-based WiFi localization system that enjoys wider bandwidth and more antennas to improve AoA estimation accuracy. However, to obtain accurate ToF estimation, they modify the 802.11 Fine Timing Measurement (FTM) protocol [16]. In contrast, RIScan builds upon COTS APs and does not require any modification on both hardware and protocols. In addition, RIScan can provide localization services for multiple users simultaneously with low latency.

8.2 RIS-aided Localization System

The emerging RIS technology is capable of customizing the wireless environment, which shows potential advantages in addressing the open issues of wireless localization. However, most of the research only stops at the simulation stage and does not consider the actual dynamic environments [3, 4, 6, 45, 52]. MetaRadar [51] presents a metasurface-aided RSS fingerprint-based indoor localization system, which leverages different configurations to generate different RSS maps, improving the RSS specificity of each point in 3D space. The system most similar to ours is MetaSight [41], which deploys multiple metasurfaces on the roof to localize RFID objects in the NLOS scenario. The metasurface reflects the RF signals from the RFID tags and creates an MS path that goes around blockages. Then the system modulates the frequency to separate the MS path for direction estimation. However, frequency modulation is inapplicable in Wi-Fi systems because it will occupy other channels and interrupt communication. In contrast, RIScan uses only a pair of configurations and is suitable for Wi-Fi devices.

8.3 RIS-aided Sensing Applications

The emergence of RIS changes the passive sensing paradigm to a proactive sensing paradigm due to its wireless channel customization. The new capability of producing a controllable transmission path and amplifying the key signal makes the RIS suitable to improve the sensing resolution and thus enable many novel attractive applications [9, 15, 20, 27, 29, 54]. [20] exploits deep learning to develop a RIS-aided Wi-Fi imaging system. [15] leverages some well-designed RIS configurations to acquire redundant information about the ROI to infer the posture. [54] and [9] improve the performance of respiration monitoring by boosting the signal reflected from the user's chest. [29] and [27] actively change the wireless channel to defend the adversary motion sensing.

9 DISCUSSION

RIS Placement: Proper placement will strengthen the ability of RIScan to extend the localization range and resist interference. Ideally, the distance between the AP and RISs should be kept to a minimum to enhance the power of the RIS component. However, the two RISs should not be placed too close to each other, as this will result in only one angle estimation. In this paper, we deploy the RISs $2m$ away from the AP (as shown in Figure 13). In addition, RIS is not recommended to be placed in the proximity of obstacles, as the nearby obstacles will block an extensive angular range of RIS beam scanning. For instance, in the museum, RISs should be placed a certain distance from the exhibits as visitors are usually crowded around the exhibits.

Deployment of More RISs: This paper conducts all experiments with two RISs. Although RIScan only needs two RISs to achieve decimeter-level accuracy, deploying more RISs can further improve the accuracy and combat more serious interferences. We can deploy more RISs and control them in a time-division multiplexing manner to avoid mutual influence. What's more, in actual deployment, one AP may not be able to cover all areas requiring location services. Since RISs are paired with an AP in RIScan, when the user leaves the range of the first AP, he will automatically connect to another AP with stronger signal strength and be localized by the RISs paired with the new AP.

RIS-client Synchronization: The key point of the synchronization issue is to let the clients know which RIS configuration each packet corresponds to. In Section 6.3, we present the synchronization method in our laboratory environments. In practical situations, it can be achieved in two steps. First, the RIS should inform the AP of the configuration being executed, and then, the AP will inform the clients of the current RIS configuration. For the first step, AP and RISs should be synchronized within 1ms (1/maximum packet rate). Ethernet or Bluetooth can be used for AP-RIS communication since their delay is in microseconds[13, 37]. In the second step, when the AP starts a localization service, it will broadcast a service packet containing active RIS information, including ID, location, orientation, and configuration. If the AP's channel is preempted due to CSMA, the AP will notify the RIS to stop working and record the current RIS configuration. When communication is restored, the AP will resend the service information packet, containing the RIS configuration before the interruption, and resume the localization service. In this way, the clients can know which RIS configuration each packet corresponds to.

Effect on Communication: RIScan's positioning process will not harm normal Wi-Fi communication. RIScan does not need to modify the physical layer and link layer of the current Wi-Fi protocol. Although it needs to add some control packets (discussed in RIS-client synchronization) at the application layer, the overhead they introduce is very small. Because these packets will only be sent when a positioning service starts, when positioning is restored after being interrupted, and when switching RIS. Besides, the RIS beam scanning will not negatively impact Wi-Fi's physical layer. The reason is that RIScan only uses RIS to create RIS paths and existing communication systems only need to treat them as multipath. Furthermore, the user's directional information (RAoD) provided by RIScan is also very beneficial for RIS-assisted communication scenarios [5, 22]. In these scenarios, how to find the optimal RIS configuration to maximize the client's SNR (or accurately point the beam toward the client) is one of the key challenges.

10 CONCLUSION

In this paper, we present RIScan, a RIS-aided multi-user indoor localization system that has low latency and is robust to dynamic interference. A RIS beam scanning mechanism is used to achieve a parallel direction estimation. In addition, we adequately leverage the capability of RIS to suppress dynamic interference. Evaluation results show that RIScan achieves a median error of 47cm and 71cm in the static and dynamic environment with only two RISs as anchors. The localization latency of RIScan is around 0.5s and not increases with the number of users. When responding to 10 clients' requests, RIScan gains a 12.5× acceleration compared to the SOTA Wi-Fi indoor localization system. The biggest advantage of RIScan lies in responding to location service requests in parallel. This advantage will be more pronounced with more users. We envision that RIScan can simultaneously provide real-time localization services for a number of people in shopping malls, airports, and hospitals.

ACKNOWLEDGMENTS

We are grateful to all anonymous reviewers and our shepherd for their constructive feedback on this paper. We also thank Yujie Zhang and Ross MURCH for their support on RIS testing. This research is supported in part by the Key-Area Research and Development Program of Guangdong Province (No. 2020B0101390001), in part by RGC under Contract CERG 16204820, 16206122, AoE/E-601/22-R, Contract R8015, and 3030_006, in part by the National Natural Science Foundation of China (No. 62002150).

REFERENCES

[1] 2021. HUAWEI WiFi AX3 Pro Access Points. https://consumer.huawei.com/en/routers/ax3-pro/specs/
[2] 2023. TP-Link Archer AX55 Pro Access Points. https://www.tp-link.com/hk/home-networking/wifi-router/archer-ax55-pro/v1/#specifications
[3] Zohair Abu-Shaban, Kamran Keykhosravi, Musa Furkan Keskin, George C Alexandropoulos, Gonzalo Seco-Granados, and Henk Wymeersch. 2021. Near-field localization with a reconfigurable intelligent surface acting as lens. In *ICC 2021-IEEE International Conference on Communications*. IEEE, 1–6.
[4] Nooshin Afzali, Mohammad Javad Omidi, Keivan Navaie, and Naghmeh Sadat Moayedian. 2022. Low Complexity Multi-User Indoor Localization Using Reconfigurable Intelligent Surface. In *2022 30th International Conference on Electrical Engineering (ICEE)*. IEEE, 731–736.

[5] Venkat Arun and Hari Balakrishnan. 2020. {RFocus}: Beamforming using thousands of passive antennas. In *17th USENIX symposium on networked systems design and implementation (NSDI 20)*. 1047–1061.

[6] Augusto Aubry, Antonio De Maio, and Massimo Rosamilia. 2021. Reconfigurable intelligent surfaces for N-LOS radar surveillance. *IEEE Transactions on Vehicular Technology* 70, 10 (2021), 10735–10749.

[7] Paramvir Bahl and Venkata N Padmanabhan. 2000. RADAR: An in-building RF-based user location and tracking system. In *Proceedings IEEE INFOCOM 2000. Conference on computer communications. Nineteenth annual joint conference of the IEEE computer and communications societies (Cat. No. 00CH37064)*, Vol. 2. Ieee, 775–784.

[8] Constantine A Balanis. 2015. *Antenna theory: analysis and design*. John wiley & sons.

[9] Lili Chen, Wenjun Hu, Kyle Jamieson, Xiaojiang Chen, Dingyi Fang, and Jeremy Gummeson. 2021. Pushing the Physical Limits of IoT Devices with Programmable Metasurfaces. In *18th USENIX Symposium on Networked Systems Design and Implementation, NSDI 2021, April 12-14, 2021*, James Mickens and Renata Teixeira (Eds.). USENIX Association, 425–438. https://www.usenix.org/conference/nsdi21/presentation/chen

[10] Guoxuan Chi, Zheng Yang, Jingao Xu, Chenshu Wu, Jialin Zhang, Jianzhe Liang, and Yunhao Liu. 2022. Wi-drone: wi-fi-based 6-DoF tracking for indoor drone flight control. In *Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services*. 56–68.

[11] Krishna Chintalapudi, Anand Padmanabha Iyer, and Venkata N Padmanabhan. 2010. Indoor localization without the pain. In *Proceedings of the sixteenth annual international conference on Mobile computing and networking*. 173–184.

[12] Linglong Dai, Bichai Wang, Min Wang, Xue Yang, Jingbo Tan, Shuangkaisheng Bi, Shenheng Xu, Fan Yang, Zhi Chen, Marco Di Renzo, et al. 2020. Reconfigurable intelligent surface-based wireless communications: Antenna design, prototyping, and experimental results. *IEEE access* 8 (2020), 45913–45923.

[13] Manideep Dunna, Chi Zhang, Daniel Sievenpiper, and Dinesh Bharadia. 2020. ScatterMIMO: Enabling virtual MIMO with smart surfaces. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*. 1–14.

[14] Daniel Halperin, Wenjun Hu, Anmol Sheth, and David Wetherall. 2011. Tool release: Gathering 802.11 n traces with channel state information. *ACM SIGCOMM computer communication review* 41, 1 (2011), 53–53.

[15] Jingzhi Hu, Hongliang Zhang, Boya Di, Lianlin Li, Kaigui Bian, Lingyang Song, Yonghui Li, Zhu Han, and H. Vincent Poor. 2020. Reconfigurable Intelligent Surface Based RF Sensing: Design, Optimization, and Implementation. *IEEE J. Sel. Areas Commun.* 38, 11 (2020), 2700–2716. https://doi.org/10.1109/JSAC.2020.3007041

[16] Mohamed Ibrahim, Hansi Liu, Minitha Jawahar, Viet Nguyen, Marco Gruteser, Richard Howard, Bo Yu, and Fan Bai. 2018. Verification: Accuracy evaluation of WiFi fine time measurements on an open platform. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*. 417–427.

[17] Mohamed Ibrahim, Ali Rostami, Bo Yu, Hansi Liu, Minitha Jawahar, Viet Nguyen, Marco Gruteser, Fan Bai, and Richard Howard. 2020. Wi-go: accurate and scalable vehicle positioning using wifi fine timing measurement. In *Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services*. 312–324.

[18] Richard C Johnson, H Allen Ecker, and J Searcy Hollis. 1973. Determination of far-field antenna patterns from near-field measurements. *Proc. IEEE* 61, 12 (1973), 1668–1694.

[19] Manikanta Kotaru, Kiran Joshi, Dinesh Bharadia, and Sachin Katti. 2015. Spotfi: Decimeter level localization using wifi. In *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*. 269–282.

[20] Lianlin Li, Ya Shuang, Qian Ma, Haoyang Li, Hanting Zhao, Menglin Wei, Che Liu, Chenglong Hao, Cheng-Wei Qiu, and Tie Jun Cui. 2019. Intelligent metasurface imager and recognizer. *Light: science & applications* 8, 1 (2019), 1–9.

[21] Xiang Li, Shengjie Li, Daqing Zhang, Jie Xiong, Yasha Wang, and Hong Mei. 2016. Dynamic-music: accurate device-free indoor localization. In *Proceedings of the 2016 ACM international joint conference on pervasive and ubiquitous computing*. 196–207.

[22] Zhuqi Li, Yaxiong Xie, Longfei Shangguan, Rotman Ivan Zelaya, Jeremy Gummeson, Wenjun Hu, and Kyle Jamieson. 2019. Towards programming the radio environment with large arrays of inexpensive antennas. In *16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19)*. 285–300.

[23] Alex T. Mariakakis, Souvik Sen, Jeongkeun Lee, and Kyu-Han Kim. 2014. SAIL: Single Access Point-Based Indoor Localization. In *Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, and Services* (Bretton Woods, New Hampshire, USA) *(MobiSys '14)*. Association for Computing Machinery, New York, NY, USA, 315–328. https://doi.org/10.1145/2594368.2594393

[24] Jiazhi Ni, Fusang Zhang, Jie Xiong, Qiang Huang, Zhaoxin Chang, Junqi Ma, BinBin Xie, Pengsen Wang, Guangyu Bian, Xin Li, et al. 2022. Experience: pushing indoor localization from laboratory to the wild. In *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*. 147–157.

[25] Alejandro Blanco Pizarro, Joan Palacios Beltrán, Marco Cominelli, Francesco Gringoli, and Joerg Widmer. 2021. Accurate ubiquitous localization with off-the-shelf IEEE 802.11 ac devices. In *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services*. 241–254.

[26] Ralph Schmidt. 1986. Multiple emitter location and signal parameter estimation. *IEEE transactions on antennas and propagation* 34, 3 (1986), 276–280.

[27] Jayanth Shenoy, Zikun Liu, Bill Tao, Zachary Kabelac, and Deepak Vasisht. 2022. RF-protect: privacy against device-free human tracking. In *Proceedings of the ACM SIGCOMM 2022 Conference*. 588–600.

[28] Elahe Soltanaghaei, Avinash Kalyanaraman, and Kamin Whitehouse. 2018. Multipath triangulation: Decimeter-level wifi localization and orientation with a single unaided receiver. In *Proceedings of the 16th annual international conference on mobile systems, applications, and services*. 376–388.

[29] Paul Staat, Simon Mulzer, Stefan Roth, Veelasha Moonsamy, Markus Heinrichs, Rainer Kronberger, Aydin Sezgin, and Christof Paar. 2022. IRShield: A Countermeasure Against Adversarial Physical-Layer Wireless Sensing. In *43rd IEEE Symposium on Security and Privacy, SP 2022, San Francisco, CA, USA, May 22-26, 2022*. IEEE, 1705–1721. https://doi.org/10.1109/SP46214.2022.9833676

[30] Sheng Tan, Linghan Zhang, Zi Wang, and Jie Yang. 2019. MultiTrack: Multi-User Tracking and Activity Recognition Using Commodity WiFi. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300766

[31] Xin Tan, Zhi Sun, Josep M Jornet, and Dimitris Pados. 2016. Increasing indoor spectrum sharing capacity using smart reflect-array. In *2016 IEEE International Conference on Communications (ICC)*. IEEE, 1–6.

[32] Deepak Vasisht, Swarun Kumar, and Dina Katabi. 2016. {Decimeter-Level} Localization with a Single {WiFi} Access Point. In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*. 165–178.

[33] Xuyu Wang, Lingjun Gao, and Shiwen Mao. 2016. CSI Phase Fingerprinting for Indoor Localization With a Deep Learning Approach. *IEEE Internet of Things Journal* 3, 6 (2016), 1113–1123. https://doi.org/10.1109/JIOT.2016.2558659

[34] Xuyu Wang, Lingjun Gao, Shiwen Mao, and Santosh Pandey. 2017. CSI-Based Fingerprinting for Indoor Localization: A Deep Learning Approach. *IEEE Transactions on Vehicular Technology* 66, 1 (2017), 763–776. https://doi.org/10.1109/TVT.2016.2545523

[35] Xuyu Wang, Chao Yang, and Shiwen Mao. 2017. PhaseBeat: Exploiting CSI phase data for vital sign monitoring with commodity WiFi devices. In *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 1230–1239.

[36] Wikipedia contributors. 2022. Direction finding — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Direction_finding&oldid=1114428562. [Online; accessed 24-November-2022].

[37] Wikipedia contributors. 2023. NearLink — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=NearLink&oldid=1177630496. [Online; accessed 3-October-2023].

[38] Cornelis Rossouw Wilke. 2018. *Quantization effects on beamforming in dense phased arrays*. Ph. D. Dissertation. Stellenbosch: Stellenbosch University.

[39] Billy Wu, Adrian Sutinjo, Mike E Potter, and Michal Okoniewski. 2008. On the selection of the number of bits to control a dynamic digital MEMS reflectarray. *IEEE antennas and wireless propagation letters* 7 (2008), 183–186.

[40] Kaishun Wu, Jiang Xiao, Youwen Yi, Dihu Chen, Xiaonan Luo, and Lionel M. Ni. 2013. CSI-Based Indoor Localization. *IEEE Transactions on Parallel and Distributed Systems* 24, 7 (2013), 1300–1309. https://doi.org/10.1109/TPDS.2012.214

[41] Dianhan Xie, Xudong Wang, and Aimin Tang. 2022. MetaSight: localizing blocked RFID objects by modulating NLOS signals via metasurfaces. In *Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services*. 504–516.

[42] Jie Xiong and Kyle Jamieson. 2013. ArrayTrack: A Fine-Grained Indoor Location System. In *10th USENIX Symposium on Networked Systems Design and Implementation (NSDI 13)*. 71–84.

[43] Jie Xiong, Karthikeyan Sundaresan, and Kyle Jamieson. 2015. Tonetrack: Leveraging frequency-agile radios for time-based indoor wireless localization. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*. 537–549.

[44] Jie Xiong, Karthikeyan Sundaresan, and Kyle Jamieson. 2015. ToneTrack: Leveraging Frequency-Agile Radios for Time-Based Indoor Wireless Localization. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking* (Paris, France) *(MobiCom '15)*. Association for Computing Machinery, New York, NY, USA, 537–549. https://doi.org/10.1145/2789168.2790125

[45] Ziang Yang, Haobo Zhang, Hongliang Zhang, Boya Di, Miaomiao Dong, Lu Yang, and Lingyang Song. 2022. MetaSLAM: Wireless Simultaneous Localization and Mapping Using Reconfigurable Intelligent Surfaces. *IEEE Transactions on Wireless Communications* (2022).

[46] Zuwei Yin, Chenshu Wu, Zheng Yang, and Yunhao Liu. 2017. Peer-to-peer indoor navigation using smartphones. *IEEE Journal on Selected Areas in Communications* 35, 5 (2017), 1141–1153.

[47] Moustafa Youssef and Ashok Agrawala. 2005. The Horus WLAN location determination system. In *Proceedings of the 3rd international conference on Mobile systems, applications, and services*. 205–218.

[48] Moustafa Youssef, Adel Youssef, Chuck Rieger, Udaya Shankar, and Ashok Agrawala. 2006. PinPoint: An Asynchronous Time-Based Location Determination System. In *Proceedings of the 4th International Conference on Mobile Systems, Applications and Services* (Uppsala, Sweden) *(MobiSys '06)*. Association for Computing Machinery, New York, NY, USA, 165–176. https://doi.org/10.1145/1134680.1134698

[49] Gergely V Zàruba, Manfred Huber, FA Kamangar, and Imrich Chlamtac. 2007. Indoor location tracking using RSSI readings from a single Wi-Fi access point. *Wireless networks* 13, 2 (2007), 221–235.

[50] Youwei Zeng, Dan Wu, Jie Xiong, Enze Yi, Ruiyang Gao, and Daqing Zhang. 2019. FarSense: Pushing the range limit of WiFi-based respiration sensing with CSI ratio of two antennas. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 3, 3 (2019), 1–26.

[51] Haobo Zhang, Jingzhi Hu, Hongliang Zhang, Boya Di, Kaigui Bian, Zhu Han, and Lingyang Song. 2020. Metaradar: Indoor localization by reconfigurable metamaterials. *IEEE Transactions on Mobile Computing* (2020).

[52] Haobo Zhang, Hongliang Zhang, Boya Di, Kaigui Bian, Zhu Han, and Lingyang Song. 2021. Metalocalization: Reconfigurable intelligent surface aided multi-user wireless indoor localization. *IEEE Transactions on Wireless Communications* 20, 12 (2021), 7743–7757.

[53] Ming-Tao Zhang, Steven Gao, Yong-Chang Jiao, Ji-Xiang Wan, Bu-Ning Tian, Chun-Bang Wu, and Andrew-John Farrall. 2016. Design of novel reconfigurable reflectarrays with single-bit phase resolution for Ku-band satellite antenna applications. *IEEE Transactions on Antennas and Propagation* 64, 5 (2016), 1634–1641.

[54] Yangfan Zhang, Xiaojing Wang, Chao Feng, Xinyi Li, Yuan-Ming Cai, Yuhui Ren, Fuwei Wang, and Ke Li. 2021. Pushing the Limits of Respiration Sensing with Reconfigurable Metasurface. In *SenSys '21: The 19th ACM Conference on Embedded Networked Sensor Systems, Coimbra, Portugal, November 15 - 17, 2021*. ACM, 367–368. https://doi.org/10.1145/3485730.3492873