Users are Closer than they Appear: Protecting User Location from WiFi APs

Roshan Ayyalasomayajula, Aditya Arun, Wei Sun, and Dinesh Bharadia
UC San Diego

ABSTRACT

WiFi-based indoor localization has now matured for over a decade. Most of the current localization algorithms rely on the WiFi access points (APs) in the enterprise network to localize the WiFi user accurately. Thus, the WiFi user's location information could be easily snooped by an attacker listening through a compromised WiFi AP. With indoor localization and navigation being the next step towards automation, it is important to give users the capability to defend against such attacks. In this paper, we present MIRAGE, a system that can utilize the downlink physical layer information to create a defense against an attacker snooping on a WiFi user's location information. MIRAGE achieves this by utilizing the beamforming capability of the transmitter that is already part of the WiFi standard protocols. With this initial idea, we have demonstrated that the user can obfuscate his/her location from the WiFi AP always with no compromise to the throughput of the existing WiFi communication system through the real-world prototype, and reduce the user location accuracy of the attacker from 2.3m to more than 10m through simulation.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**; **Privacy-preserving protocols**; • **Computer systems organization → Sensor networks**.

KEYWORDS

Privacy, RF sensing, Localization, Wireless channel, Obfuscation

ACM Reference Format:
Roshan Ayyalasomayajula, Aditya Arun, Wei Sun, and Dinesh Bharadia. 2023. Users are Closer than they Appear: Protecting User Location from WiFi APs. In *The 24th International Workshop on Mobile Computing Systems and Applications (HotMobile '23), February 22–23, 2023, Newport Beach, CA, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3572864.3580345

1 INTRODUCTION

The proliferation of wireless sensing and localization has enabled the widely deployed WiFi APs to provide not only Internet connectivity but also sense the user's location. Specifically, location-based services in indoor settings have gained interest, especially in recent

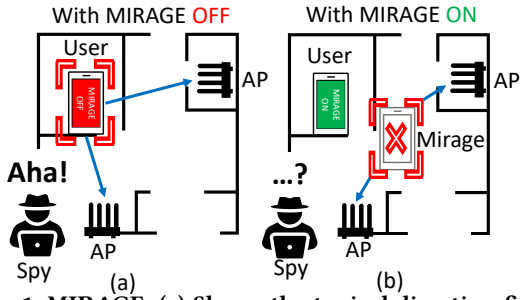


Figure 1: MIRAGE: (a) Shows the typical direction finding (e.g., AoA) based indoor device localization. (b) Shows the obfuscation that MIRAGE provides, which enables the users' location privacy.

times for contact tracing, indoor navigation, or density monitoring. For example, many WiFi vendors propose to deploy the Wi-Fi APs for joint wireless communication and sensing in the enterprise network [2–4, 20]. Furthermore, upcoming 5G deployments also claim to provide location services [8]. However, this would lead to potential breaches [26] of Wi-Fi users' private location information and other sensitive information (Fig. 1(a)). A simple example is the use of enterprise WiFi networks deployed in the malls to get accurate user locations [6, 25]. This location data collected in the malls can be used to stalk users, track a user's interactions with other users or even analyze their spending trends to infer private information (e.g., sex, age, personal preferences), violating the user's privacy. We present MIRAGE, an algorithm that the user can employ on their devices (e.g., smartphone) to maintain their location privacy if desired without compromising their WiFi's quality of service (Fig. 1(b)).

The typical enterprise networks estimate the user locations using a single access point (AP) to estimate the user's distance and direction. They can estimate user's range using existing 802.11mc [13] protocols that can estimate the received Wi-Fi signals Time-of-Flight (ToF). Additionally, these Wi-Fi APs, typically equipped with multiple antennas, can also measure the user's direction by estimating the received signals Angle-of-Arrival (AoA) using algorithms such as SpotFi/MUSIC [11]. ToF-based range estimates usually require multiple packet exchanges with the user and a simple defense is to not respond to these requests. Furthermore, Wi-Peep [7] demonstrates an attack against these 802.11 range estimation systems and proposes a few solutions for defense. Unfortunately, there seems to be no defense systems that can overcome the AoA algorithms-based direction estimation systems, as these are simply receiving the user's transmitted Wi-Fi signals.

Specifically, let us consider WiFi network-aided user localization in malls and other public spaces. Commonly, connecting the phone to free WiFi available at these venues exposes the user's location [26] unbeknownst to the user. Furthermore, some network providers utilize AoA to furnish these locations [5, 6], making it

HotMobile '23, February 22–23, 2023, Newport Beach, CA, USA

ACM ISBN 979-8-4007-0017-0/23/02…$15.00
https://doi.org/10.1145/3572864.3580345

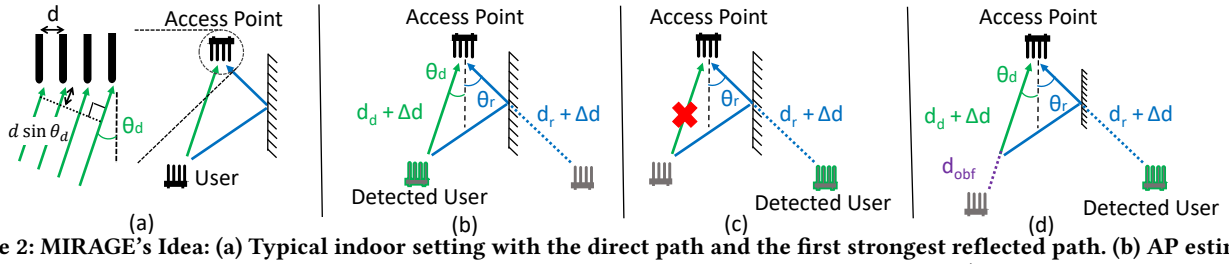


Figure 2: MIRAGE's Idea: (a) Typical indoor setting with the direct path and the first strongest reflected path. (b) AP estimates the angles of arrivals (AOAs) to be $\{\theta_d, \theta_r\}$ and relative time of flights (rToFs) as $\{d_d + \Delta d, d_r + \Delta d\}$[1]$(d_d < d_r)$. *Estimated AoA is* θ_d. (c) Shows beam-nulling towards θ_d. Estimated AoA (θ_r) is incorrect at the cost reduced SNR. (d) MIRAGE adds delay d_{obf} and makes $d_d + d_{obf} > d_r$. Estimated AoA is θ_r and no SNR reduction observed.

crucial to protect against AoA-based localization. To understand why defending against AoA-based localization algorithms is difficult, let us understand how AoA is measured at an AP. The WiFi signal arriving directly from a transmitter at the AP's antenna array traverses varying distances to each antenna (Fig. 2(a)). These small distances are observable from the phase of the signal across the receive antennas. These differential phases observed across the antennas vary in accordance to the AoA and hence can be used to estimate the AoA. However, in a typical indoor environment, this WiFi signal can bounce off various objects and arrive at the AP via multiple paths. These paths, dubbed multipath, can potentially corrupt the AoA of the direct path. Most localization systems [11] employ a simple heuristic – the straight-line direct path arriving at the AP travels the least distance – and separate the multipath from the direct path by measuring the relative time of flights. Consequently, obfuscating AoA is challenging as the signal accumulates phases by physically interacting with the environment and this phase can readily be measured by AP listening to the signal.

However, we develop a defense against this snooping attack via MIRAGE, and hence allow the user to protect their location by obfuscating primarily the direction of the user's location. The key idea is that users' direction or angle of arrival (AoA) information measured to perform localization is obfuscated by creating a 'mirage' such that the users' actual direction is along one of the reflected paths, i.e. making the reflected path look like the most direct path from the user to the AP. MIRAGE achieves this obfuscation without reducing the communication data rate, i.e. the communication between WiFi AP and user will not be affected. Finally, MIRAGE's mechanism for spoofing the AoA and creating a mirage also obscures the direct path's ToF information and protects against Chronos [29] and other ToF-based algorithms.

A naive way to create this mirage is to just simply beamform the signal transmitted by the user such that there is a null towards the access point and thus remove the direct path (Fig. 2(c)). This makes the path observed in the profile corresponding to the reflected path, which would obfuscate the attacker to accurately localize the user. Unfortunately, this beamforming comes at the cost of reduced SNR and hence the throughput of the network. Alternatively, in MIRAGE we develop a novel algorithm that enables us to add delay only to the direct path such that the direct path appears to have traveled more distance than the reflected path in the environment as shown in Fig. 2d. Employing MIRAGE hence takes away the user certainty in the AoA of the direct path and helps protect the locations of the user. And most importantly, by preserving the direct path, MIRAGE does not affect the signal's SNR and hence the throughput.

To demonstrate MIRAGE's feasibility, we have deployed it on WARP board [22] as the user device and commercially off-the-shelf (COTS) available ASUS device [17] that acts as the attacker AP. With this setup and a few experiments, we have shown

(a) The naive approach of nulling towards the direct path ensures that an attacker can practically never get accurate AoAs of the WiFi user, but it reduces the SNR by 6dB.
(b) Meanwhile, MIRAGE's design ensures obfuscation of the user's AoA by 46° on an average creating a localization error for AoA-based systems to up to 10 m on an average, while observing no degradation in SNR.
(c) MIRAGE follows Wi-Fi protocols by applying compliant precoding matrices which can be decoded by COTS APs.

2 PRIVACY ATTACKS

In this section, we first illustrate an attack model which will violate the WiFi user's location privacy. We also present a set of ideal defense model requirements, and define the assumptions under the pretext of which we present our defense solution, MIRAGE.

2.1 Attack Model

A user connects to the Wi-Fi provided at common public spaces like shopping malls and airports. The snooping Wi-Fi APs (i.e., attackers) that are part of this enterprise network listen to the packets transmitted by the user for data communication and predict the user directions to each of the APs using state-of-the-art AoA algorithms (say SpotFi [11, 15]). The APs can use the AoAs either for (a)'single-AP Localization' by using the ToF measurements (from Wi-Peep [7] for example) for range and estimated AoA for direction or (b) 'Triangulation' by using AoAs across multiple APs to estimate user location. The AoA of the incoming Wi-Fi signal at the attacking AP can be extracted via Spotfi [11] as shown in Fig. 3(a). As discussed, the direct path (green box) arrives earlier than the reflected path (blue box) due to the shorter signal traversing path, and hence direct path's AoA can be reliably extracted even in multipath-rich environments. In this fashion, during protocol-compliant packet exchanges between a user and an enterprise AP, the user's location can be discerned within a meter level of accuracy. Thus we need a defense model against such attacks.

[1] Δd is the random distance error constant across all the paths for a given data packet, caused due to sampling frequency offsets (SFO).

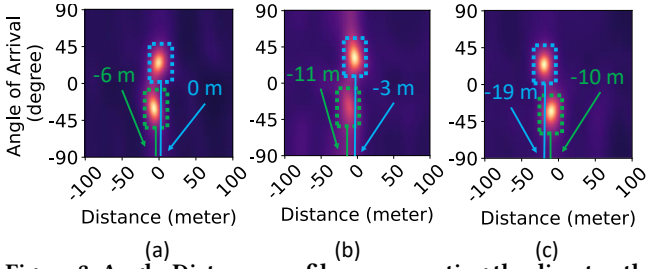


Figure 3: Angle-Distance profiles representing the direct path and reflected path angle of arrivals and their relative distance travelled. Measurement from COTS AP in (a) without MIRAGE, in (b) with nulling the direct path, in (c) with MIRAGE obfuscation applied.

2.2 Defense Model

MIRAGE seeks to protect a user from these snooping attacks during this connection period by fulfilling the following key requirements

(R.1) The transmitted packets from the user do not retain any user location artifacts.
(R.2) The user does not need any explicit collaboration from the connected APs.
(R.3) The defense works under the knowledge that the defense is applied
(R.4) The defense does not compromise the communication link, throughput, or network latency.
(R.5) The location should be recoverable for a benevolent application/AP

Assumptions for the solution: However, we make the following assumptions to provide the first of its kind defense solution for RF-privacy against the previously defined attack model.

- An active communication channel between the attacker and the user. We assume the AP is transmitting packets toward the user as well, a valid assumption as most user-side communication is preceded by either beacon or ACK packets [1].
- A linear, uniformly spaced, and at least 2-3 antennas on the device is assumed for this work. But the algorithm can be extensible to any antenna array as all we need to know are the corresponding steering vectors. Furthermore, no knowledge about AP location or antenna array is made.
- Channel reciprocity, where we assume that the channel measured at the user device could be used to compensate and apply MIRAGE's algorithm.
- The device is quasi-static or the direct path, and the first significant reflected path does not drastically change.

3 DESIGN

Based on these assumptions, we first propose a straightforward idea of beam nulling towards the direct path to protect the user's privacy comes at the cost of the user's throughput degradation. Finally, we propose the design of MIRAGE for WiFi user's location obfuscation, which makes the reflected path appear to be the direct path.

3.1 Nulling to the Direct Path

Hence, to obfuscate the AoA information at the WiFi user, a straightforward idea is to null this direct path to the AP. That is the user can beamform such that there is a null in the beamforming pattern in the direction of AP's direct path. Now the attacker WiFi AP will only observe the multipath and regard it as the direct path for localization. To perform this nulling, the WiFi user extracts the AoA of the direct path (i.e., θ_d) and AoA of the earliest reflected path (i.e., θ_r) from a downlink (AP to the user) channel measurement. For the sake of simplicity, we only consider two paths. To null the direct path, the WiFi user needs to apply the beamforming weights $N_d(f_i, k)$ to their data streams to null in the θ_d direction, where i indicates the subcarrier index and k indicates the antenna index. After we 'precode' the data stream $X(f_i, k)$ with nulling weights, the WiFi AP will receive the following signals:

$$\begin{aligned} Y(f_i,k) &= H(f_i,k)N_d(f_i,k)X(f_i,k) \\ &= (H_d(f_i,k) + H_r(f_i,k))N_d(f_i,k)X(f_i,k) \\ &= H_r(f_i,k)N_d(f_i,k)X(f_i,k) \end{aligned}$$

where $Y(f_i, k)$ and $H(f_i, k)$ indicate the received signal and wireless channel on k-th antenna and f_i subcarrier. $H(f_i, k) = H_d(f_k, k) + H_r(f_i, k)$ where H_d and H_r indicate the direct path and reflected path wireless channel. Note that $H_d(f_i, k)N_d(f_i, k) = 0$ as $N_d(f_i, k)$ is chosen to lie in the null space of $H_d(f_i, k)$ [12]. The WiFi AP will estimate the wireless channel as $H_r(f_i, k)N_d(f_i, k)$, which only contains the reflected path, thereby preventing the attacker from extracting the direct path AoA.

This is illustrated in the angle-distance profile in Fig. 3(b). Note the reduced power of the direct path. However, this simple idea has two key flaws. First, nulling to the direct path will decrease the signal strength at the Wi-Fi AP and degrade the network throughput. Second, in case the nulling angle is predicted incorrectly by the user, nulling will be ineffective and a residual peak of the direct path will remain exposing the user's location. Clearly, this solution is impractical and we propose MIRAGE for user location obfuscation to eliminate this side effect.

3.2 Beamforming and Delaying

To overcome this user's throughput degradation we need to ensure the direct path is preserved, as the direct path contributes to the majority of the channel diversity. However, the presence of the direct path will appear as a strong signal at the Wi-Fi AP and an attacker can easily extract the AoA. However, to disambiguate the effects of the inevitable reflected paths, the attacker relies on the simple heuristic that the direct path always travels the shortest path. Specifically, for a distance traveled d, the phases accumulated across the various subcarriers are given by $e^{-2\pi f_c \frac{d}{c}}$. By leveraging super-resolution localization algorithms [11], the attacker can hence separate the various paths in the time domain and predict the direct path.

Here we provide a key insight – delaying only the direct path signal invalidates the foundational heuristic to select the correct AoA. With this in mind, we propose to beamform to the direct path and multipath and add delay to the direct path. This ensures communication throughput will be preserved over the beamforming and the user's location will be obfuscated by adding the delay to the direct path. This is qualitatively illustrated in Fig. 3(c). The WiFi user adds a delay of 15 m in the direction of the direct path and

successfully pushes the direct path peak (green box) predicted by SpotFi to the right of the multipath peak (blue box).

Specifically, to beamform to the direct path and multipath, we need to have the beamforming vectors, $S_d(f_i,k)$ and $S_r(f_i,k)$ for direct path and reflected path respectively [16].

$$S_d(f_i,k) = \left[1, e^{-j2\pi f_i \frac{d_d + Dsin\theta_d}{c}}, \cdots, e^{-j2\pi f_i \frac{d_d+(n-1)Dsin\theta_d}{c}}\right]^T,$$
$$S_r(f_i,k) = \left[1, e^{-j2\pi f_i \frac{d_r + Dsin\theta_r}{c}}, \cdots, e^{-j2\pi f_i \frac{d_r+(n-1)Dsin\theta_r}{c}}\right]^T$$

Note, d_d and d_r indicate the direct path and reflected path distance between the Wi-Fi AP to the user's reference antenna respectively. θ_d and θ_r indicate the angle-of-departure at the user for the direct path and reflected path. D indicates the antenna separation at the antenna array. So, these steering vectors are only determined by the downlink channel between WiFi AP and the user, which is independent of WiFi AP. The specific beamforming angles are predicted via a downlink channel measurement at the user. Hence, the Wi-Fi user will use the precoding weight of $S_d(f_i,k)e^{-j2\pi f_i d_{\text{obf}}/c} + S_r(f_i,k)$, where d_{obf} indicates the additional path length that WiFi user wants to add to obfuscate its location for WiFi AP as shown in Fig. 2(d). We ensure that $d_{\text{obf}} > d_{\text{multipath}} - d_{\text{direct}}$ via the same downlink channel measurements. Then, the WiFi AP will receive the following signals:

$$\begin{aligned} Y(f_i,k) &= H(f_i,k)(S_d(f_i,k)e^{-j2\pi f_i \frac{d_{\text{obf}}}{c}} + S_r(f_i,k))X(f_i,k) \\ &= (H_d(f_k,k) + H_r(f_i,k))(S_d(f_i,k)e^{-j2\pi f_i \frac{d_{\text{obf}}}{c}} \\ &\quad + S_r(f_i,k))X(f_i,k) \\ &= (H_d(f_k,k)S_d(f_i,k)e^{-j2\pi f_i \frac{d_{\text{obf}}}{c}} \\ &\quad + H_r(f_i,k)S_r(f_i,k))X(f_i,k) \end{aligned} \quad (1)$$

Beamforming in the directions of the direct path ensures weaker energy directed towards the strongest multipath and vice versa. Hence, in Eqn. 1, the cross terms $H_d(f_k,k)S_r(f_i,k)$ and $H_r(f_i,k) * S_d(f_i,k) * e^{-j2\pi f_i d_{\text{obf}}/c}$ are ignored. Thus, the wireless channel is $H_d(f_k,k) * S_d(f_i,k) * e^{-j2\pi f_i d_{\text{obf}}/c} + H_r(f_i,k)S_r(f_i,k)$, which will only contain direct path with delay of d_{obf} and multipath without any delay. Note that there is only one direct path and multiple reflected paths in the multipath-rich environment.Since the direct path has been deliberately delayed with MIRAGE, it's impossible to recognize this delayed direct path from all the other multipaths. As a result, the attacker will never recover the delayed direct path even if they know that MIRAGE has altered the channel.

The channel obfuscation solution provided by MIRAGE eliminates the direct path, making it impossible for an attacker to determine the user's location (R1); it does not require any participation from the connected network (R2); and even with knowledge of MIRAGE's implementation, the attacker cannot obtain the user's location (R3), meeting many of the requirements outlined in section 2.2. Additionally, because only normalized phase vectors are multiplied, the overall signal strength remains unchanged as the added phase does not affect the interference pattern at the receiver. This is further supported by the results in section 4 (Table 4b), showing that MIRAGE's implementation does not negatively impact the communication link and only obscures the user's location (R4). While the current implementation of MIRAGE does not address (R5), potential future research directions are discussed in section 7.2.

4 IMPLEMENTATION

Setup. For the proof of concept, we deploy a commercially-off-the-shelf (COTS) AP and a WARP as a user device in a cluttered indoor scenario as shown in Fig. 4(a). In this scenario, there are mainly two paths (i.e., direct path and multipath) between the Wi-Fi AP and the user. The multipath gets reflected by the reflector (purple box) shown in the figure. WiFi user (black circle) will communicate with Wi-Fi AP (red box) using 802.11n protocol with a bandwidth of 20MHz at the center frequency of 5180MHz. In this scenario, we have added a metal reflector as shown in Fig. 4(a), to ensure a known multipath, and in a generic indoor environment, there would be more naturally occurring multipath in the environment. That is we assume a multipath-rich environment.[2]

Real-world deployment is done as a proof of concept and for more large-scale testing of MIRAGE's effect on user localization performance by an attacker, we have simulated 10k user locations in an indoor simulation of 40 m×30 m, with 4 APs at the center of each wall, where each wall behaves as a perfect reflector and there are additional reflectors placed within the environment to create multipath for significant data points. With this setup, we test the obfuscation MIRAGE provided to AoA and thus the user location.
WiFi AP. We use ASUS RT-AC86U [17] WiFi AP as the compromised snooper for WiFi user's location. The WiFi AP is instrumented with a uniform linear array of four antennas with a spacing of 0.026 m. The WiFi AP can estimate the uplink channel for indoor localization with the SpotFi algorithm. Specifically, WiFi AP will create an angle-distance profile via SpotFi for localization by identifying AoA of the direct path with the least traveled distance.
WiFi User. We use WARP software-defined radio [22] as the WiFi user, which is also instrumented with four antennas. The antenna spacing at the WiFi user is 0.026m to achieve accurate nulling and beamforming for the WiFi user. After WiFi user obtains the downlink channel, they will 'precode' the data stream for location obfuscation with MIRAGE as discussed in Sec. 3.2.

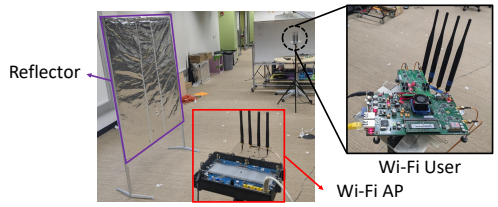
5 EVALUATION

We evaluate MIRAGE with the above implementation and demonstrate through real-world experiments and some simulations the capabilities of MIRAGE's obfuscation of users' AoA and locations.

5.1 MIRAGE's Performance

We first demonstrate that MIRAGE will disable the WiFi AP to localize the WiFi user, while MIRAGE will not degrade the normal communication throughput between the WiFi AP and the user. As shown in Table 4b, with nulling to the direct path approach, SpotFi algorithm will not identify the direct path correctly due to the AoA error of 62°. However, nulling the direct path will decrease RSSI by 6dBm in comparison to the standard communication with no obfuscation. So, nulling the direct path will degrade the network

[2]Multipath-rich indoor environment is the basic assumption made by any MIMO architecture design.



(a)

	No obf.	Nulling	MIRAGE with delay of			
			0 (m)	20 (m)	30 (m)	40 (m)
AoA error	0°	62°	0°	58°	61°	53°
RSSI (dBm)	-65	-71	-64	-64	-64	-62

(b)

Figure 4: (a) Hardware setup showcasing the ASUS WiFi-AP, WARP client and reflector. (b) AoA error and RSSI measured without obfuscation; with nulling; and using MIRAGE to delay the path by varying amounts

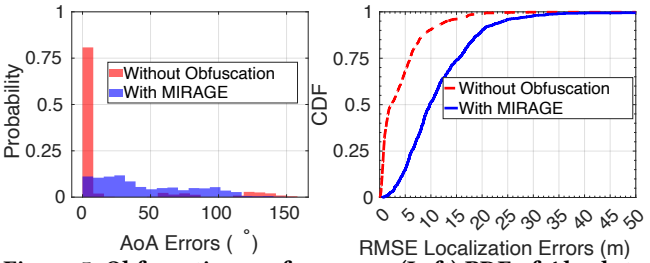


Figure 5: Obfuscation performance: (Left) PDF of Absolute AoA prediction errorswith and without MIRAGE. (Right) RMSE Localization CDF with and without MIRAGE.

throughput. When we employ MIRAGE and add different delays to the direct path (i.e., 20m, 30m, and 40m), the AoA error becomes significant (i.e., 58°, 61° and 53°) which will disable SpotFi for accurate localization. Additionally, the RSSIs do not change significantly in comparison to the beamforming without delay and standard communication without MIRAGE.

The design of MIRAGE does not change the RSSI of the existing communication channel, so it does not affect the overall communication or data-rate. Additionally, even if an attacker is aware of MIRAGE's implementation, they are unable to re-estimate the direct path due to lack of prior knowledge of the channel, making the user's location impossible to determine while preserving the quality of the original communication link.

5.2 Location Obfuscation Performance

Finally, it is important to understand how much location and angular obfuscation MIRAGE provide for a large deployment scenario. To understand them, we have deployed MIRAGE in a simulated environment of 40 m×30 m, with 4 APs at the center of each wall, where each wall behaves as a perfect reflector and there are additional reflectors placed within the environment to create multipath for significant data points. With this setup, we test the obfuscation MIRAGE provided to AoA and thus the user location.

AoA accuracy: We have computed the AoAs of the users moved to 500 random positions within this environment and observed the absolute AoA errors' distribution as shown in Figure 5(left). We can see that the AoA error distributions before Obfuscation had an average error of 20°. These AoA errors increase 2×, as shown in the blue histogram with a mean of 46°. Demonstrating that MIRAGE's AoA obfuscation is successful.

Localization accuracy: We use the above AoAs to perform both triangulation and AoA+ToF-based user localization and present the errors for both the algorithms together for before (in red) and after (in blue) obfuscation as shown in Figure 5(right), where we can see that while before obfuscation the attacker could get the user location with an average precision of 2.3m and 10 m after obfuscation the average precision of the user's location known to the attacker, a 5× poorer location accuracy. With an error of this magnitude, the attacker cannot extract any meaningful information either, showing the strengths in MIRAGE's AoA obfuscation techniques.

6 RELATED WORK

The most commonly employed location obfuscation technique is to randomize the user device's MAC address to prevent an attacker from uniquely identifying a user. However, these MAC address randomization approaches can either be easily broken or disabled by the user device [14].

Hence, many works look towards disabling an AP's ability to localize users. For signal-strength-based techniques, obfuscating the strength of wireless signals is used. Authors in [28, 31] introduce several approaches (i.e., geofencing with electromagnetic shielding paint on the walls and jamming with extra signal generators), however, this interrupts ongoing wireless communication between the WiFi AP and user. These techniques hence comprise a weak defense against location snooping. On the other hand, Fine Timing Measurement (FTM) [10] based localization, introduced in 802.11 standards, considered to be secure [21, 23], can also be leveraged for privacy-invasive localization [7].

Considering the poor defenses against signal strength or FTM-based localization techniques, some prior works look towards modifying the wireless sensing environment. However, these systems deploy additional hardware in the environment affecting widescale adoption. For example, PhyCloak [18] requires a full duplex radio co-located with the user for location obfuscation; IRShield [27] requires to deploy a smart surface in the wireless sensing environment to distort the wireless channel for location obfuscation. Additionally, PhyCloak and IRSheild may interrupt user communication. RF-Protect [24] deploys a reflector in the environment to obfuscate the wideband FMCW signals; Aegis [30] deploys an additional radio instrumented with amplifier and antennas to obfuscate the wireless signals.

To overcome the limitations of prior work, MIRAGE simply uses the beamforming capability of end-user devices (e.g., smartphones) to obfuscate the user location without affecting the ongoing wireless communication.

7 DISCUSSION AND FUTURE WORK

In this section, we discuss the implications and limitations of MIRAGE's current implementation and propose the future research direction for privacy-preserving wireless sensing.

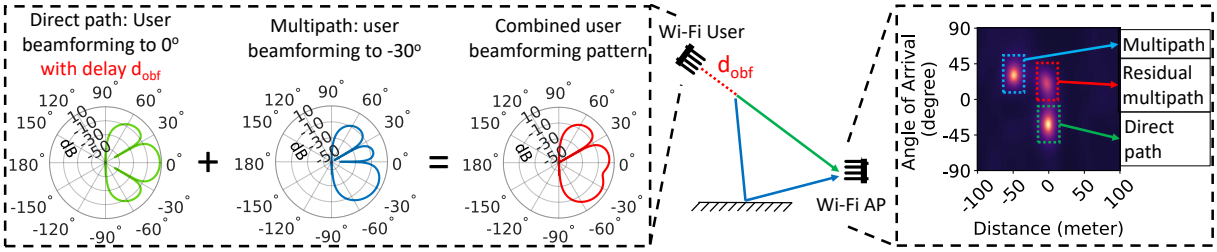


Figure 6: Imperfect beamforming introduces residual peak in angle-distance profile (red dotted box) due to the power leakage from the side lobe of the direct path beamforming. *(left inset)* Antenna beamforming patterns transmitted by the user; *right inset* received SpotFi profile at a commodity Wi-Fi AP

7.1 Discussion

Resolving Multipath in Indoor Wireless Environment. Indoor communication is deployed with the assumption of a multipath-rich environment, and we also rely on this assumption. Note that the indoor wireless environment is multipath-rich due to the nature of the indoor environment with different kinds of reflectors (e.g., chairs, walls, ceilings, desks, etc.). The heart of the wireless sensing-based indoor environment is resolving the multipath, where the direct path should be identified to localize the object of interest. When there is no direct path, the localization will be failed, as we cannot characterize the reflectors in an unknown wireless environment. There are algorithms like MUSIC, RAP-MUSIC, and SpotFi [11, 15] that can help identify both the direct and the first reflected path. The direct path is easy to obtain based on the least signal traversing path thus the shortest time of flight. Then, we can extract one reflected path easily based on the second shortest time of flight, which is constrained by the bandwidth, antenna array, etc.

Improving User Location Obfuscation: We have demonstrated MIRAGE's obfuscation for the WiFi user's location through beamforming and delaying through a few examples. However, in MIRAGE's design I, we make a critical assumption. We ignore the cross terms in Eqn. 1 when adding delay to the direct path due to weaker energy directed towards the reflected path. However, in some cases where there is a strong reflection in the environment, these cross terms cannot be ignored. An exemplary case is shown in Fig. 6. In this scenario, we beamform towards 0° and add a delay of $d_{\text{obf}} = 40m$ to the direct path (green pattern) and simultaneously beamform towards the multipath at $-30°$ (blue pattern). This creates a combined beamforming pattern (red) shown in the left inset. However, due to some side-lobe leakage in the direction of multipath and the presence of a strong reflector, we inadvertently add delay to the multipath as well. This creates a residual peak (in red dotted box) along with the delayed direct path peak (green box). This abnormal angle-distance profile will expose MIRAGE's spoofing and an attacker can potentially extract the correct direct path.

Dynamic User and/or Wireless Environment: To accurately obfuscate AoA information, the WiFi user needs to accurately estimate the wireless channel either with CSI feedback from the WiFi AP which will require the collaboration of the attacker (i.e., WiFi AP) and introduce the overhead due to the downlink communication of feedback, or leveraging the property of wireless channel reciprocity. From another perspective, the dynamic environment will decrease the accuracy of wireless localization due to the dynamic clutters in the environment, which will require frequent channel estimation.

How Much Location Obfuscation is Needed?: MIRAGE is designed to defend against the fine-grained wireless localization algorithms (e.g., Spotfi [11]), which can provide the localization error of decimeters. Therefore, any location obfuscation that can make the localization error more than a decimeter will disable the WiFi AP to accurately localize the WiFi user and derive the context-sensing information from the user's location. However, the WiFi AP may just employ the coarse-grained localization algorithms (e.g., RSSI-based indoor localization [9]) to localize the WiFi user for context sensing (e.g., to know if people are at home or not). In this case, WiFi user can leverage the nulling technique illustrated in Section 3.1 to hide his/her location or beamform to a far distance, while it will degrade the network throughput as the signal strength will be significantly degraded.

7.2 Future Directions

Wi-Fi User's Beamforming/Nulling Capability: The performance of our obfuscation depends on the WiFi user's beamforming/nulling capability. More antennas for the Wi-Fi user, a more accurate estimation of AoA. This is because the Wi-Fi user can always shine the narrow beam toward the Wi-Fi user for the purpose of obfuscation without interfering with the reflected path. The commodity smartphones are usually instrumented with three or more antennas [19], which are enough for our user location obfuscation. For example, iPhone 13 supports 4x4 MIMO for 5G and 2x2 MIMO for Wi-Fi 6 (802.11ax), which will enable them to leverage MIRAGE for location obfuscation.

Multiple Collaborative Wi-Fi APs: Currently, MIRAGE only considers one WiFi AP deployed in the environment to steal the WiFi user's location information. In the enterprise network, there are multiple WiFi APs deployed in the building to achieve larger coverage and better service. These WiFi APs can collaborate with each other to localize the WiFi user, which will significantly improve localization accuracy. To defend against multiple APs, the WiFi user needs to obfuscate AoA information extracted by each of them, which will require the WiFi user to create more fine-grained beams with more antennas and eliminate interference across different beams.

Recovering the User's Location at the benevolent AP. Someone may wonder that MIRAGE will disable the context-based sensing at the benevolent AP due to the obfuscation. Therefore, we need to design an algorithm that will only obfuscate the attacker but not the benevolent AP. To do so, we have to make sure, the direct path signal seen by the benevolent AP has not been delayed and

the direct path signal seen by the attacker AP is delayed properly. This will be left for our future work.

REFERENCES

[1] 802.11 frame exchanges. https://howiwifi.com/2020/07/16/802-11-frame-exchanges/. Accessed: 20123-01-10.

[2] Aruba localization services. https://www.arubanetworks.com/en-in/products/location-services/. Accessed: 20123-01-10.

[3] Cisco dna spaces. https://spaces.cisco.com/indoor-navigation/. Accessed: 20123-01-10.

[4] Juniper localization services. https://www.juniper.net/us/en/solutions/indoor-location.html. Accessed: 20123-01-10.

[5] Retail tracking firm settles ftc charges it misled consumers about opt out choices. https://www.ftc.gov/news-events/news/press-releases/2015/04/retail-tracking-firm-settles-ftc-charges-it-misled-consumers-about-opt-out-choices. Accessed: 20123-01-10.

[6] Retailnext occupancy services. https://retailnext.net/product/occupancy. Accessed: 20123-01-10.

[7] A. Abedi and D. Vasisht. Non-cooperative wi-fi localization & its privacy implications. In *Proceedings of the 28th Annual International Conference On Mobile Computing And Networking*, pages 126–138. ACM, 2022.

[8] N. Alliance. 5g white paper. *Next generation mobile networks, white paper*, 1(2015), 2015.

[9] V. Bahl and V. Padmanabhan. RADAR: An In-Building RF-based User Location and Tracking System. INFOCOM, 2000.

[10] M. Ibrahim, H. Liu, M. Jawahar, V. Nguyen, M. Gruteser, R. Howard, B. Yu, and F. Bai. 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*, pages 417–427, 2018.

[11] M. Kotaru, K. Joshi, D. Bharadia, and S. Katti. SpotFi: Decimeter Level Localization Using Wi-Fi. SIGCOMM, 2015.

[12] M. Li and Y. Lu. Null-steering beamspace transformation design for robust data reduction. In *2005 13th European Signal Processing Conference*, pages 1–4. IEEE, 2005.

[13] I. Martin-Escalona and E. Zola. Ranging estimation error in wifi devices running ieee 802.11 mc. In *GLOBECOM 2020-2020 IEEE Global Communications Conference*, pages 1–7. IEEE, 2020.

[14] C. Matte and M. Cunche. *Spread of MAC address randomization studied using locally administered MAC addresses use historic*. PhD thesis, Inria Grenoble Rhône-Alpes, 2018.

[15] J. C. Mosher and R. M. Leahy. Source localization using recursively applied and projected (rap) music. *IEEE Transactions on signal processing*, 47(2):332–340, 1999.

[16] Natalia Schmid. beamforming weight design . https://safe.nrao.edu/wiki/pub/Beamformer/WebHome.

[17] A. B. Pizarro, J. P. Beltrán, M. Cominelli, F. Gringoli, and J. Widmer. 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*, pages 241–254, 2021.

[18] Y. Qiao, O. Zhang, W. Zhou, K. Srinivasan, and A. Arora. {PhyCloak}: Obfuscating sensing from communication signals. In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*, pages 685–699, 2016.

[19] Qualcomm. Iphone antennas . https://discussions.apple.com/thread/1334188.

[20] Qualcomm. Qualcomm Enterprise Network . https://www.qualcomm.com/products/application/wireless-networks/wi-fi-networks/networking-pro-series.

[21] Qualcomm and Android FTM MAC address randomizatoin. CVE-2020-11287 Detail . https://nvd.nist.gov/vuln/detail/CVE-2020-11287.

[22] rice university. WARP software defined radio . https://warpproject.org/trac/wiki/about.

[23] D. Schepers and A. Ranganathan. Privacy-preserving positioning in wi-fi fine timing measurement. *Proceedings on Privacy Enhancing Technologies*, 2022(2):325–343, 2022.

[24] J. Shenoy, Z. Liu, B. Tao, Z. Kabelac, and D. Vasisht. Rf-protect: privacy against device-free human tracking. In *Proceedings of the ACM SIGCOMM 2022 Conference*, pages 588–600, 2022.

[25] I. Solomiia Ryfiak. Indoor Positioning Technologies as a Rising Force in Retail Sales. https://intellias.com/indoor-positioning-technologies-as-a-rising-force-in-retail-sales/.

[26] A. Soltani. Privacy trade-offs in retail tracking. *Federal Trade Commision*.

[27] P. Staat, S. Mulzer, S. Roth, V. Moonsamy, M. Heinrichs, R. Kronberger, A. Sezgin, and C. Paar. Irshield: A countermeasure against adversarial physical-layer wireless sensing. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 1705–1721. IEEE, 2022.

[28] W. Sun, T. Chen, and N. Gong. Sok: Inference attacks and defenses in human-centered wireless sensing. *arXiv preprint arXiv:2211.12087*, 2022.

[29] D. Vasisht, S. Kumar, and D. Katabi. Decimeter-Level Localization with a Single Wi-Fi Access Point. NSDI, 2016.

[30] Y. Yao, Y. Li, X. Liu, Z. Chi, W. Wang, T. Xie, and T. Zhu. Aegis: An interference-negligible rf sensing shield. In *IEEE INFOCOM 2018-IEEE conference on computer communications*, pages 1718–1726. IEEE, 2018.

[31] Y. Zhu, Z. Xiao, Y. Chen, Z. Li, M. Liu, B. Y. Zhao, and H. Zheng. Et tu alexa? when commodity wifi devices turn into adversarial motion sensors. *arXiv preprint arXiv:1810.10109*, 2018.