Bringing WiFi Localization to Any WiFi Devices

Tianxiang Li*[1], Haofan Lu*[1], Reza Rezvani[1], Ali Abedi[2], Omid Abari[1]
*Equal Contributions
[1]University of California, Los Angeles, [2]University of Waterloo

ABSTRACT

Recent years have seen significant advances in WiFi Localization. However, existing systems require either multiple access points to cooperate with each other or a single access point to have multiple antennas and transceiver chains. Therefore, they cannot be integrated into most IoT WiFi chipsets which have only a single transceiver chain. This paper presents WiSight, a novel approach to bringing WiFi localization to any WiFi devices, especially those with a single RF chain. We propose a WiFi antenna design and use the inherent properties of the 802.11 protocol to measure Angle-of-Arrival (AoA) and Time-of-Flight (ToF) using a single transceiver chain. Our proof-of-concept simulation and real world experiments promise the feasibility of this approach.

CCS CONCEPTS

• **Hardware** → *Wireless devices*; • **Networks** → *Wireless local area networks*;

KEYWORDS

Frequency Scanning Antenna, WiFi Localization

ACM Reference Format:
Tianxiang Li*[1], Haofan Lu*[1], Reza Rezvani[1], Ali Abedi[2], Omid Abari[1]. 2022. Bringing WiFi Localization to Any WiFi Devices. In *The 21st ACM Workshop on Hot Topics in Networks (HotNets '22), November 14–15, 2022, Austin, TX, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3563766.3564090

1 INTRODUCTION

Over the past decade, there has been a significant amount of work on WiFi localization. Despite impressive improvements in accuracy and robustness of WiFi localization systems, unfortunately, all existing approaches have a major limitation: they cannot be integrated into low-cost low-power WiFi devices which only have a single transceiver chain. In particular, existing WiFi localization systems can be divided into two categories: multi-device localization [5, 11, 18, 20] and single-device localization [15, 17]. Multi-device localization systems require multiple WiFi devices to cooperate and share their information to localize another device. These systems target environments such as enterprise networks where dense WiFi deployment exists. In contrast to multi-device localization systems, single-device localization systems require only a single WiFi device to locate other devices. These systems target small businesses and homes. Although these systems enable localization with a single Access Point (AP), they require the AP to have MIMO capability (i.e., multiple antennas with multiple transceiver chains). Unfortunately, most low-cost WiFi chipsets (in particular the ones used in IoT devices) have only a single transceiver chain due to cost and power consumption constraints.

To the best of our knowledge, none of the existing systems can enable WiFi localization on a low-power low-cost WiFi device with a single transceiver chain. For a single WiFi device to locate another device, it requires two parameters: (a) the distance between itself and the target device, and (b) the direction of the target device with respect to itself. To measure the distance, localization systems typically estimate the Time-of-Flight (ToF), and multiply it by the speed of light to obtain the distance. For the direction, existing systems use multiple antennas and measure the phase differences of the received signal at the antennas to compute the Angle-of-Arrival (AoA). In fact, this is exactly why today's single-device localization systems require multiple transceiver chains.

To solve this limitation and bring WiFi localization to any WiFi devices, especially those with a single transceiver chain such as low-cost IoT devices, we propose WiSight. WiSight is the first plug-and-play system that gives any WiFi device the ability to locate other WiFi devices. WiSight introduces a low-cost and passive WiFi antenna based on the Frequency Scanning Antenna (FSA) technique, and can be connected to any WiFi device without any modification to WiFi chipsets. Combining this antenna with the inherent properties of 802.11 protocol, WiSight enables any WiFi device to estimate the ToF and AoA of surrounding WiFi devices even if they are not part of the same network. Most importantly, WiSight does not require any cooperation with, software or hardware changes on target WiFi devices. In summary, we make the following contributions:

HotNets '22, November 14–15, 2022, Austin, TX, USA

ACM ISBN 978-1-4503-9899-2/22/11…$15.00
https://doi.org/10.1145/3563766.3564090

- We introduce the first system that enables WiFi localization on single-transceiver WiFi devices, without modification to the chipset or firmware.
- We design a novel WiFi antenna based on Frequency Scanning Antenna (FSA). Our design is passive and can be seamlessly connected to any WiFi chipset.
- We investigate the inherent properties of the 802.11 protocol and integrate them seamlessly with the FSA design to enable localization.
- We empirically evaluate the effectiveness of our approach using existing off-the-shelf WiFi devices. Our preliminary results show that our approach can enable low-cost low-power WiFi devices to estimate the ToF and AoA of the target devices accurately.

2 BACKGROUND AND RELATED WORK

Past work can be divided into three groups:

(a) Multi-Device Localization: Multi-device localization systems mostly target enterprises and large buildings where multiple access points can cooperate to find the location of a WiFi device. These systems assume dense deployment of WiFi access points where a target device is in the communication range of multiple of them. In these systems, the access points measure the distance or direction to the target devices cooperatively and infer the position of the target device by trilateration or triangulation [5, 9, 11, 12, 20]. Some other systems use fingerprinting based methods to infer the unknown target location by matching the signal patterns learned from multiple Access Points in prior [6, 16, 19].

(b) Single-Device Localization Single-device localization systems try to enable WiFi localization using a single WiFi device. These systems are more appealing for the relatively small environment such as homes and small businesses. For these systems, the WiFi device needs to estimate both ToF and AoA to obtain the distance and direction of the target device [15, 17]. The closest work to ours is [10], which uses an RF switch that quickly switches the connection between a single transceiver and multiple antennas to emulate the effect of multiple transceiver chains. However, this approach requires the active control of the RF switch, which calls for modification to the WiFi chipset and firmware. Moreover, since all measurements are not taken at the same time, their phase will not be accurate due to Carrier Frequency Offset (CFO) which will impact on the accuracy of AoA estimation.

(c) Leaky Wave Antenna (LWA): Finally our work builds on past work on LWA[7, 13, 14]. However, in contrast to past work which uses LWA for direction finding at THz and mmWave bands, our goal is to design a frequency scanning antenna which operates in WiFi frequency band. This involves unique challenges, such as limited Field-of-View (FoV) constrained by available bandwidth and the number of emitting elements within a reasonable size.

3 WISIGHT OVERVIEW

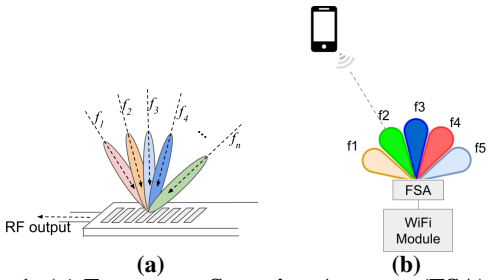
WiSight is a localization system applicable to any WiFi device with even a single transceiver chain. It utilizes the inherent properties of the 802.11 and a specially designed antenna to collect the two essential pieces of information for localization: Angle of Arrival (AoA), and Time of Flight (ToF).

AoA is typically measured using an antenna array. The phase differences of the received signal across antennas are used to compute AoA [3]. However, this approach requires multiple antennas and a complete transceiver chain for each antenna, which is not available in most low-cost IoT devices. Even for devices with multiple antennas, the AoA estimation accuracy is still constrained by the limited number of antenna elements, and the synchronization accuracy between multiple transceiver chains [10]. To solve this issue and enable AoA estimation with a single transceiver chain, we design a novel antenna based on the Frequency Scanning Antenna (FSA) technique. Our antenna design can be seamlessly connected to any WiFi module as a substitute for its original antenna. FSA is a passive structure whose beam forms in different directions based on the signal frequency. WiSight integrates our antenna design with the inherent probing process of the IEEE 802.11 protocol to measure the Received Signal Strength Indicator (RSSI) of a WiFi device at different frequency channels (beam directions). This enables WiSight to estimate the AoA of other WiFi devices using a single RF chain, without any modification to the WiFi chipset or firmware.

The time-of-flight (ToF) is typically measured between a WiFi client device and its access point by exchanging WiFi packets and measuring the time it takes for a packet to reach the other device. For example, a client device sends a data packet to its access point and measures the time it takes to receive the ACK for that packet. The limitation of this technique is that it works only between a client device and its access point. Specifically, a client device cannot send a packet directly to another client device to measure the ToF, because all traffic must go through the access point. In WiSight, our goal is to measure the ToF to all nearby devices, even those not in our network. To do so, we inject a fake packet to a target device pretending the packet is coming from a legitimate source like the access point. Although this fake packet has no encryption, it still triggers a physical-layer ACK from the target. In fact, our past work has tested more than 5000 WiFi devices from 186 vendors, and shown that they all respond ACK to even fake packets [4]. Hence, this behavior is widespread and can be used by a WiFI device to measure the ToF to any other WiFi device in its communication range.

4 MEASURING ANGLE OF ARRIVAL (AOA)

We first describe the working principle of FSA, then we explain how we build on it to measure AoA in WiFi devices.



(a) (b)

Figure 1: (a) Frequency Scanning Antenna (FSA), and (b) Measuring AoA of WiFi Device using FSA.

4.1 Frequency Scanning Antenna (FSA)

FSA is a passive structure (similar to a patch antenna) that is mostly used in multi-dimensional radar image scanning [21]. However, in contrast to a typical patch antenna, FSA receives and transmits a signal toward a specific direction, where the direction depends on the frequency of the signal, as shown in Figure 1(a).

The FSA structure consists of an array of elements (copper traces) which are known as slots as shown in Figure 1(a). In the case of transmitting, when a signal is fed to this structure, the signal gradually leaks from the structure into the air at different slots. Therefore, this structure works similarly to an array of emitting elements where the phase shift of the signal at each element is a function of the distance of the element from the signal feed and the wavelength of the signal. This natural phase shift enables the structure to act as an antenna array and transmit a signal toward a direction. However, since the amount of phase change at each element is a function of the signal's wavelength, the transmitting direction is a function of the signal's wavelength or frequency. FSA works in a similar way when receiving signals. Each radiating slot of the FSA receives signals with different phase shifts, which causes the signal to combine constructively in a certain direction. The phase shift is dependent on the frequency of the received signal, which means that the signals of different frequencies will combine constructively in different directions. We build on the principle of FSA and design a FSA operating in the WiFi ISM band. However, instead of using an array of slots (a typical approach for designing FSAs), we design a FSA where its elements are dipole antennas printed on a PCB.

4.2 Measuring AoA using FSA

We develop an FSA-based antenna for WiFi that can easily connect to a WiFi chipset instead of their typical antennas. The localizing WiFi device (equipped with our FSA antenna) then measures the RSSI of another WiFi device (target device) in different WiFi channels. Since the mapping between the beam direction and the frequency is known and fixed for an FSA, the channel which has the highest RSSI corresponds to the AoA. However, the question is how can we measure the RSSI of a target WiFi device in different channels?

To measure the RSSI at different WiFi channels, our idea is to use the WiFi Probing feature. WiFi probe request packets are broadcast by each WiFi device in every frequency channel periodically for the purpose of discovering available networks in its communication range. Note that the probe request packets are sent even when the device is connected to a network, in order to update its list of available access points. As the probe request packet is transmitted on every frequency channel, it provides a perfect tool for us to measure AoA using our FSA approach. In particular, FSA passively beam-forms in different directions based on the signal frequency. Hence, the probe request packet of a certain frequency channel will have a strong signal strength only if it arrives from a particular direction. This enables WiSight to measure the RSSI at different frequency channels and use it to estimate the AoA.

Figure 1(b) shows a simple example of how our approach works where we have a WiFi module (localizing device) and a phone (target device). Assume we have an FSA whose beam forms in five different directions based on the signal frequency (i.e., f_1 to f_5). These frequencies are matched with WiFi channel center frequencies. The FSA is attached to a WiFi module as the substitute for the original antenna. As the phone transmits WiFi probe requests in frequencies f_1, f_3, f_4, and f_5, the WiFi module will receive the probe request with relatively low RSSI because the FSA's beams of those frequencies are pointing to the other directions. On the other hand, when the phone transmits a WiFi probe request in frequency f_2, the WiFi module will receive it with high RSSI because the FSA's beam direction at f_2 is pointing to the direction of the phone. Hence, by just comparing the five RSSI measurements, the WiFi device can estimate the AoA. Note, in this example the phone direction is perfectly aligned with the direction of one of the beams (i.e., beam f_2). However, in reality, there is a chance that the direction of the target devices is not perfectly aligned with any of the beam directions. In these cases, WiSight can still use the RSSI profile from multiple frequencies (different beam directions) to interpolate and estimate the correct AoA.

4.3 Measuring AoA of Multiple Devices

The next question is how can we extend our approach to localizing multiple WiFi devices. In particular, since WiSight needs to perform multiple RSSI measurements across different channels to estimate the AoA, it needs to differentiate probe request packets received from different devices. Our solution to solve this issue is to first identify the target devices based on their unique MAC addresses. Although this solution works for most WiFi devices (such as IoT and most laptops), it is not effective for Apple and Android phones. This is due to the fact that these WiFi devices perform MAC address randomization. Hence, WiSight cannot simply use MAC addresses to differentiate RSSI measurements of a specific device from that of other devices in the area.

To solve this problem, we studied the behavior of Android and iOS WiFi devices in more detail. For Android devices, we found that the device probes with the same random MAC address on different channels as long as it is connected to an

AP. However, for iOS devices, the story is slightly different. we found that when an iOS WiFi device is associated with an AP, it probes with the same MAC address only in the channel on which the AP is operating, and it uses other random MAC addresses for sending probe request packets on other channels. This is known as a *directed probe request*. Interestingly, we observed that this behavior is not dependent on the MAC address of the AP but on the SSID broadcast of the AP. In particular, in the channels where there is no AP with that specific SSID, the WiFi device still probes with randomized MAC addresses. On the other hand, in the channels where there is an AP with that specific SSID, the WiFi device probes with the same MAC address.

WiSight leverages this property to push the target WiFi devices to use the same MAC addresses instead of randomizing them. In particular, the localizing device forges a beacon frame, and put the SSID of the AP in its field[1] and broadcast it on every channel. This makes the target WiFi device assume there are multiple APs with the same SSID working on every single channel. As a result, the probing packets will always use the same source MAC address which helps WiSight to identify each target device consistently. Finally, it is worth mentioning that we found that this technique not only works for target devices that are connected to a specific AP but also works for devices that were once associated with the AP and still have the SSID saved in their list of connected APs. Although these devices are no longer associated with that AP, they still probe with the same source MAC address on the channels where the AP's SSID is broadcasted.

In summary, WiSight's localizing device broadcasts fake Beacons using the SSID of an AP. The WiFi devices which are in the range respond to this by sending Probe Requests on different channels with the same MAC address (i.e., without randomizing their MAC address). The localizing device which is equipped with an FSA antenna measures the RSSI of these probe request packets at different channels. Since the FSA's beam direction changes as a function of the frequency, the channel (beam direction) with the highest RSSI presents the direction of the AoA.

5 MEASURING TIME OF FLIGHT (TOF)

In order to estimate the distance of the target device from the localizing device, WiSight first needs to measure ToF. WiSight measures ToF using DATA-ACK frame exchange. Specifically, the localizing WiFi device sends fake data packets to the target devices. The target device responds to these packets with ACK packets. The localizing WiFi device records the timestamps at which a fake packet is sent and the corresponding ACK is received. The difference between these two timestamps is the sum of round-trip signal propagation delay (round-trip ToF), Short Inter-Frame Space (SIFS), and the transmission duration of the ACK frame. Note, the duration of SIFS, t_{SIFS}, is defined by the WiFi standard and is $10\mu s$ and $16\mu s$ in the 2.4 and 5 GHz ISM bands, respectively. Moreover, the duration of the ACK, t_{ACK}, is constant for a given modulation scheme. Hence, the ToF can be calculated by subtracting the SIFS and ACK duration from the timestamp difference, Δt . Finally, distance is calculated by multiplying one-way ToF with the speed of light C. However, since timestamp measurements are noisy, we take the average over multiple measurements to reduce noise, as shown in the following equation.

$$d = \frac{C}{2} \times \mathbb{E}[\Delta t - t_{ACK} - t_{SIFS}] \quad (1)$$

It is worth mentioning that traditional ToF measuring techniques which also use DATA-ACK traffic [8, 9] work only for devices that are connected to the same wireless network. In other words, only authenticated devices can send packets to each other. Hence, two devices operating in different WiFi networks could not locate each other using the typical DATA-ACK approach. Even within the same WiFi network, the devices communicate with each other through the access point. This limitation prevents us from measuring ToF between the WiFi devices directly. To solve this problem, we leverage the fact that all WiFi devices respond with an ACK to any WiFi data packets sent to them [4], even when they are not part of the same network. This enables the localizing device to send fake packets to the target device and get the ACK frame without setting up any connections, which enables WiSight to perform direct device-to-device ToF and distance measurement.

Algorithm 1 WiSight localization algorithm

```
Initialize to sniffing mode, record SSIDs in set S, target MAC addresses in set M
Switch to AP mode
for ssid in S do
    Broadcast fake beacons with SSID = ssid
end for
Switch to sniffing mode
for mac in M do
    for ch in WiFi Channels do
        Measure RSSI for probe request packets in ch
    end for
    AoA[mac] = argmax_ch RSSI(ch)
end for
for mac in M do
    Inject fake packets to measure ToF
end for
```

6 LOCALIZATION ALGORITHM

In this section, we summarize the techniques developed in previous sections and formalize the localization algorithm. The pseudo-code is presented in Algorithm 1. In the bootstrap phase, the localizing WiFi device first works in the sniffing mode to collect target MAC addresses and the SSIDs of the

[1] Note, since the SSID field of an AP is not encrypted, it can be easily obtained by sniffing the traffic.

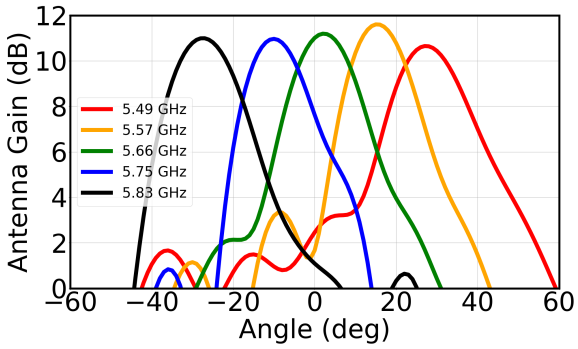


Figure 2: Our Designed FSA Performance

APs with which they are associated. Then it switches to broadcast mode to send fake beacon frames with collected SSIDs. This step is for creating the illusion that there are APs with the same SSID working on all the channels to handle MAC randomization in some devices. Then it switches to the sniffing mode again for listening to the probe request packets in different channels and recording the RSSI for each packet. In this phase, the localizing device quickly switches between channels. Once the RSSI for each channel is collected, the channel (FSA's beam) with the highest RSSI pinpoints the AoA. Finally, the localizing device measures ToF to each target device using the DATA-ACK exchange approach as explained before. The beauty of WiSight is that it requires no modification on target devices.

7 EVALUATION

We evaluate WiSight's performance using simulations and experiments.

7.1 FSA Performance

We design an FSA antenna operating at the 5.8 GHz WiFi band. Our design can also be extended to the 2.4 GHz WiFi band. However, we choose the 5.8 GHz band since there are more channels and bandwidth available than the 2.4 GHz band. In particular, larger bandwidth enables wider field of view (i.e. more steering angles). Hence, an FSA operating at 5.8 GHz will have a larger FOV than an FSA operating at 2.4 GHz band. The form factor of our design is $10\,cm \times 20\,cm$ for a 8-element FSA, where elements are half-wavelength spaced. We evaluate the performance of our design using the HFSS simulator. Figure 2 shows the antenna gain of our FSA at five different frequencies. The operating frequency range is $5.49 - 5.835$ GHz, which covers a continuous part of the 5.8 GHz band. The figure shows that our FSA achieves a directional beam with around 10 dB gain for different frequencies in the WiFi band. The 3 dB beamwidth for the beams is around 12 degrees which is narrow enough to enable accurate AoA estimation.

7.2 Experiment Setup

For the target device, we use an iPhone X mobile phone without any hardware or software modification. We use an ESP32 WiFi module [2] as the localizing WiFi device. Note, that this module costs only $10, and has a single transceiver chain. In fact, the WiFi chipset used in this module is the same as the one used in many IoT devices. This module has an antenna connector which can be easily used to connect an FSA to it. To emulate our FSA design, we use five directional indoor panel WiFi antennas [1] and connect them to the same ESP32 module. We arrange them in a circular layout, with each antenna's beam pointing to a specific direction ($-45°$, $-22.5°$, $0°$, $22.5°$, and $45°$). The fake beacon and data packets are generated via the API provided by the Software Development Kit (SDK) of ESP32 [2]. The sampling rate of ESP32 is set to 240 MHz, which translates to a two-way ranging resolution of 0.625 m. Note, to simplify our measurements and have better control over experiments, instead of using one ESP32 module, we use two co-located modules; one for sending beacon packets and another one for sniffing. However, our ideas can be implemented using a single module too.

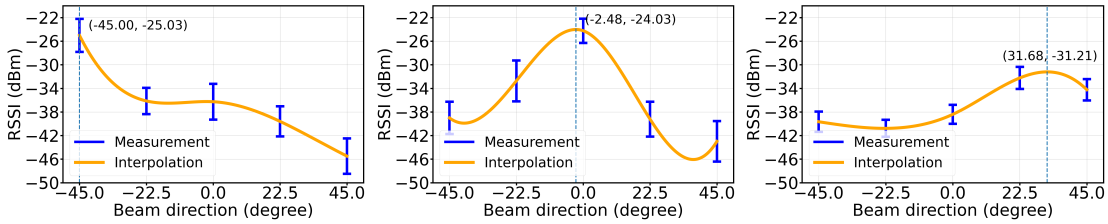
7.3 Angle of Arrival Measurements

To measure AoA, the WiFi module measures the RSSI of probe request packets at different WiFi channels where each channel has its own beam direction. Figure 3 shows the RSSI measurements across five different beam directions ($-45°$, $-22.5°$, $0°$, $22.5°$, and $45°$) for three different scenarios: (a) the target device is at $-45°$, (b) the target device is at $0°$, and (c) the Target device is at $30°$. When the target direction is exactly aligned with the direction of a beam (such as in scenarios (a) and (b)), the RSSI measurement of that channel has the highest energy. Hence, since each channel has a one-to-one mapping to a direction, WiSight accurately estimates the AoA. However, when the direction of the target device falls between two beams (such as scenario (c) in Figure 3), there will be an ambiguity in estimating the AoA. In this case, we first interpolate the raw RSSI measurements with a cubic function and then use the maximum RSSI to find the Angle-of-Arrival (AoA). The solid orange lines in the figures show the results after interpolation. As can be seen, the estimated AoA using the interpolation technique is $-45°$, $-2.48°$, and $31.68°$ when the ground truth direction of the target is $-45°$, $0°$, and $30°$. Hence, WiSight achieves high accuracy in detecting the AoA.

To better evaluate WiSight performance in estimating AoA, we perform more experiments in different target directions. Figure 4a presents the results for these experiments. The Root Mean Square Error (RMSE) between the estimated AoA and ground truth is $5°$, and in most cases, the estimated direction is just a few degrees off from the ground truth.

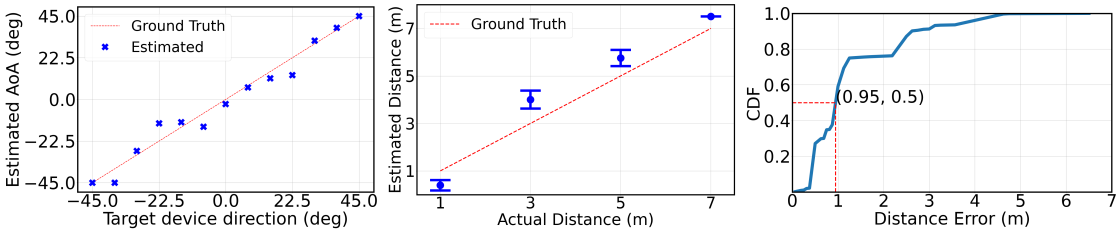
7.4 Time-of-Flight Measurements

To measure ToF, the WiFi module sends fake data packets to the target devices. The target device responds to these packets with ACK packets. The WiFi module records the timestamps at which a fake packet is sent and the corresponding ACK is received. As explained before, these timestamps are used to estimate the ToF and the distance of the target device from the localizing WiFi module.



(a) Target at -45 degrees **(b) Target at 0 degrees** **(c) Target at 30 degrees**

Figure 3: RSSI Measurements for Three Different Target Locations.



(a) AoA Estimation Accuracy **(b) Distance Estimation Accuracy** **(c) Distance Estimation Accuracy**

Figure 4: WiSight Measurement Results.

We place the target device 1, 3, 5, and 7 meters away from the localizing device. The localizing device sends 100 fake data packets per second and measures the ToF. Samples collected within 1 second (100 DATA-ACK pairs) are chosen as a sample group. The median value of the sample group is taken for the distance estimation. We collected 150 sample groups for each ground truth distance. Figure 4b shows the distance measurement error at each ground truth position. The error bars represent the 95% confidence interval. Figure 4c shows the Cumulative Distribution Function (CDF) of error in estimating the distance. We note that 80% of the estimated distances have an error of fewer than 2.5m and the median error is 0.95m. It is worth mentioning that although past work has achieved higher accuracy in distance measurement, they require much more complex WiFi devices. The main contribution of WiSight is to enable WiFi localization using low-power WiFi devices which have only one transceiver chain. Moreover, WiSight's accuracy is sufficient for many WiFi localization applications.

8 DISCUSSION AND CONCLUSION

This paper presents WiSight which brings localization functionality to any WiFi devices, especially those with a single RF chain. However, to enable a complete end-to-end localization system, the following questions require further study:

FSA Scan Range. Our current FSA design can steer its beam across only 60 degrees. Although this might be enough when the localizing WiFi device is installed on a wall or at a corner, we believe designing an FSA which provides a wider scan range is an interesting research direction. To have a large scan angle, the phase variation must be large within the operating bandwidth. One potential solution is using passive phase shifters with large phase shifts, and integrating them in the FSA design.

SIFS and RSSI Measurements. Although SIFS are defined by the WiFi standard, we found that there is some variation across different WiFi chipsets which results in an error in the distance estimation. Moreover, since our AoA estimation is relying on the probe requests, our WiFi device needs to learn a strategy to hop among channels such that it can receive the probe request packets sent by the same target device on each frequency channel. Therefore, Exploring methods to estimate SIFS accurately and learn to adapt to different probing behaviors are interesting research directions.

Normal WiFi Operation. Our FSA antenna creates a directional beam in different directions depending on the operating channel frequency. Therefore, during the normal operation (i.e., the localizing device communicating with its AP), there is a chance that the FSA beam is not aligned directly to the AP. Hence, this may result in degradation in the signal power and SNR. We believe a more extensive evaluation is required to verify this and evaluate its impact on the communication range and data rate.

Multipath. Multipath is a common issue for all the AoA-based localization system. While our system provides a new approach to passively estimate AoA, it may still suffer from the multipath issue. How to build upper-level algorithms to mitigate this issue is an open and interesting research direction. One potential solution is to mitigate the multipath problem by monitoring the AoA profile over multiple frames in the mobile settings. In this case, AoAs of multipath reflections change over time, while the AoA of direct path AoA remains relatively stable.

ACKNOWLEDGMENTS

We thank UCLA and CISCO for partially funding this project. We also thank the anonymous reviewers, and our shepherd, Swarun Kumar, for their helpful feedback.

REFERENCES

[1] Alfa network 2.4ghz/5ghz 10dbi high gain directional indoor panel antenna. https://www.wifi-stock.com/details/alfa-dual-band-indoor-panel-apa-m25.html. Accessed: 2022-06-10.

[2] Espressif systems. ESP32 datasheet. https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf, 2022. Accessed: 2022-06-13.

[3] O. Abari, D. Vasisht, D. Katabi, and A. Chandrakasan. Caraoke: An e-toll transponder network for smart cities. In *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, pages 297–310, 2015.

[4] A. Abedi and O. Abari. Wifi says "hi!" back to strangers! In *Proceedings of the 19th ACM Workshop on Hot Topics in Networks*, HotNets '20, page 132–138, New York, NY, USA, 2020. Association for Computing Machinery.

[5] R. Ayyalasomayajula, A. Arun, C. Wu, S. Sharma, A. R. Sethi, D. Vasisht, and D. Bharadia. *Deep Learning Based Wireless Localization for Indoor Navigation*. Association for Computing Machinery, New York, NY, USA, 2020.

[6] V. Bahl and V. Padmanabhan. Radar: An in-building rf-based user location and tracking system. In *Proceedings of IEEE INFOCOM 2000*. Institute of Electrical and Electronics Engineers, Inc., March 2000. ACM SIGMOBILE Test-of-Time Paper Award, 2016.

[7] Y. Ghasempour, C.-Y. Yeh, R. Shrestha, D. Mittleman, and E. Knightly. Single shot single antenna path discovery in thz networks. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*, pages 1–13, 2020.

[8] D. Giustiniano, T. Bourchas, M. Bednarek, and V. Lenders. Deep inspection of the noise in wifi time-of-flight echo techniques. In *Proceedings of the 18th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, MSWiM '15, page 5–12, New York, NY, USA, 2015. Association for Computing Machinery.

[9] J. Gjengset, J. Xiong, G. McPhillips, and K. Jamieson. Phaser: Enabling phased array signal processing on commodity wifi access points. In *Proceedings of the 20th Annual International Conference on Mobile Computing and Networking*, MobiCom '14, page 153–164, New York, NY, USA, 2014. Association for Computing Machinery.

[10] Z. Gu, T. He, J. Yin, Y. Xu, and J. Wu. Tyrloc: a low-cost multi-technology mimo localization system with a single rf chain. In *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services*, pages 228–240, 2021.

[11] M. Kotaru, K. Joshi, D. Bharadia, and S. Katti. Spotfi: Decimeter level localization using wifi. In *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, SIGCOMM '15, page 269–282, New York, NY, USA, 2015. Association for Computing Machinery.

[12] S. Kumar, E. Hamed, D. Katabi, and L. Erran Li. Lte radio analytics made easy and accessible. *ACM SIGCOMM Computer Communication Review*, 44(4):211–222, 2014.

[13] T. Li, M. H. Mazaheri, and O. Abari. 5g in the sky: the future of high-speed internet via unmanned aerial vehicles. In *Proceedings of the 23rd Annual International Workshop on Mobile Computing Systems and Applications*, pages 116–122, 2022.

[14] H. Saeidi, S. Venkatesh, X. Lu, and K. Sengupta. Thz prism: One-shot simultaneous localization of multiple wireless nodes with leaky-wave thz antennas and transceivers in cmos. *IEEE Journal of Solid-State Circuits*, 56(12):3840–3854, 2021.

[15] S. Sen, J. Lee, K.-H. Kim, and P. Congdon. Avoiding multipath to revive inbuilding wifi localization. In *Proceeding of the 11th Annual International Conference on Mobile Systems, Applications, and Services*, MobiSys '13, page 249–262, New York, NY, USA, 2013. Association for Computing Machinery.

[16] S. Sen, B. Radunovic, R. R. Choudhury, and T. Minka. You are facing the mona lisa: Spot localization using phy layer information. In *Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services*, MobiSys '12, page 183–196, New York, NY, USA, 2012. Association for Computing Machinery.

[17] D. Vasisht, S. Kumar, and D. Katabi. Decimeter-level localization with a single wifi access point. In *Proceedings of the 13th Usenix Conference on Networked Systems Design and Implementation*, NSDI'16, page 165–178, USA, 2016. USENIX Association.

[18] J. Wang, H. Jiang, J. Xiong, K. Jamieson, X. Chen, D. Fang, and B. Xie. Lifs: Low human-effort, device-free localization with fine-grained subcarrier information. In *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking*, MobiCom '16, page 243–256, New York, NY, USA, 2016. Association for Computing Machinery.

[19] Z.-H. Wu, Y. Han, Y. Chen, and K. J. R. Liu. A time-reversal paradigm for indoor positioning system. *IEEE Transactions on Vehicular Technology*, 64(4):1331–1339, 2015.

[20] J. Xiong and K. Jamieson. ArrayTrack: A Fine-Grained indoor location system. In *10th USENIX Symposium on Networked Systems Design and Implementation (NSDI 13)*, pages 71–84, Lombard, IL, Apr. 2013. USENIX Association.

[21] S. Zhan-shan, R. Ke, C. Qiang, B. Jia-jun, and F. Yun-qi. 3d radar imaging based on frequency-scanned antenna. *IEICE Electronics Express*, 14(12):20170503–20170503, 2017.