TDOA-based passive localization of standard WiFi devices

Shenghong Li, Mark Hedley, Keith Bengston, Mark Johnson, David Humphrey, Alija Kajan, and Nipun Bhaskar

***Abstract*—Indoor location-based service has widespread applications. With the ubiquitous deployment of WiFi systems, it is of significant interest to provide location-based service using standard WiFi devices. Most of the existing WiFi-based localization techniques are based on Received Signal Strength (RSS) measurements. As the bandwidth of WiFi systems increases, it is possible to achieve accurate timing-based positioning. This work presents a WiFi-based positioning system that has been developed at CSIRO as a research platform, where target devices are located using passive sniffers that measure the Time Difference of Arrival (TDOA) of the packets transmitted by the target devices. This work describes the architecture, hardware, and algorithms of the system, including the techniques used for clock synchronizing and system calibration. It is shown experimentally that the positioning error is 23 cm in open spaces and 1.5 m in an indoor office environment for a 80MHz WiFi system. The system can be used to track standard WiFi devices passively without interfering with the existing WiFi infrastructure, and is ideal for security applications.**

I. Introduction

Wireless indoor positioning has attracted significant research interest due to its widespread applications in indoor navigation, asset tracking, location-based advertising, factory automation, security monitoring etc. With the ubiquitous deployment of WiFi systems, it is of significant interest to provide location-based service to standard WiFi devices (e.g., smart phone, laptop) based on the existing WiFi infrastructure.

Various techniques have been developed for indoor positioning, using measurements include Time-of-Arrival (TOA), Time-Difference-of-Arrival (TDOA), Angle-of-Arrival (AoA), and Received Signal Strength (RSS) [1]. Most of the existing WiFi-based localization techniques are based on RSS measurements, where the location of a device is obtained either by triangulation using distances estimated from RSS measurements according to a path loss model [2], or by matching the measured RSS values against those measured beforehand at various known locations (fingerprints) [1]. The triangulation-based approach suffers from low accuracy, while the fingerprint-matching-based approach relies on building and maintaining the fingerprint database which is a time consuming and labour-intensive process.

With the progress of standardization for high data rate communication, the radio bandwidth of WiFi systems has been significantly increased. Particularly, the late 802.11ac WiFi standard includes 80 MHz and 160 MHz transmission bandwidths, making it possible to achieve accurate timing-based positioning using WiFi signals.

The authors are with DATA61, Commonwealth Scientific and Industrial Research Organisation (CSIRO), Marsfield, NSW, 2122, Australia

In this article, we present a WiFi-based positioning system that has been developed at CSIRO as a research platform, where target devices are located using passive sniffers that measure the Time Difference of Arrival (TDOA) of the packets transmitted by the target devices. The features of the system include:

- It does not require site surveying as fingerprinting-based systems, and achieves higher positioning accuracy than systems using RSS-based triangulation.
- It is passive and can be deployed to track standard WiFi devices without compromising the performance of the WiFi network.
- The target is not required to interact with the sniffers to be located, making the system ideal for security applications.
- The system was designed as a flexible research platform which can collect and record WiFi traffic and position-related information for scientific research.

This work describes the architecture, hardware, and algorithms of the system, including the techniques used for anchor clock synchronizing and hardware delay calibration. It is shown experimentally that the positioning error is 23 cm in open spaces and 1.5 m in an indoor office environment for a 80MHz WiFi system.

II. System Architecture

The architecture of the system is shown in Fig. 1. The system consists of multiple custom-built WiFi sniffers deployed at known locations, which monitor the traffic in a WiFi network. The targets to be located are standard WiFi devices in the WiFi network, e.g., a smart phone communicating with an access point (AP). When the target device transmits a WiFi packet, the sniffers measure the time at which they receive the radio signal. The location of the target is then estimated in a PC based on the measured time stamps.

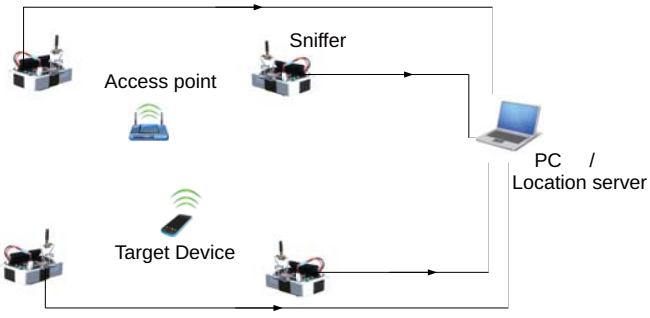

Fig. 1. Structure of the TDOA-based passive WiFi localization system.

978-1-5386-3755-5/18/$31.00

Since the sniffers are passive, they can be deployed alongside existing WiFi networks to provide location-based services. Alternatively, the sniffers can be integrated with APs in a WiFi network, e.g., by augmenting APs with the capability of measuring packet arrival time. In either case, the traffic throughput in existing WiFi networks is not impaired. In addition, the targets is not required to interact with the sniffers, making the system ideal for security applications.

Denote the locations of the sniffers and that of the target as $\boldsymbol{a}_j = [x_j, y_j, z_j]^T$ $(j = 1, ..., N)$ and $\boldsymbol{x} = [x, y, z]^T$, respectively, where N is the number of sniffers. Each sniffer in the system has a local clock that is not synchronized to each other or to any external reference. The reading of the clock at time instant t is given by [3]

$$t_j = (1 + \alpha_j)(t + \beta_j), \tag{1}$$

where α_j and β_j denote the clock skew and clock offset of sniffer j, respectively. Suppose the target transmits a packet at t_{Tx}, the arrival time of the corresponding radio signal measured by each sniffer is given by[1]

$$r_j = (1 + \alpha_j)\left(t_{\text{Tx}} + \frac{d_j}{c} + \beta_j + \Delta t_j + z_j\right), \quad j = 1, ..., J, \tag{2}$$

according to (1), where

$$d_j \triangleq |\boldsymbol{a}_j - \boldsymbol{x}| \tag{3}$$

denotes the distance between the target and sniffer j, c is the speed of light, Δt_j is the hardware delay (e.g., delay caused by radio frequency (RF) circuitry), z_j is the time measurement error. The impacts of α_j, β_j, and Δ_j needs to be compensated before the target position can be estimated. In the following sections, we will describe the hardware platform of the sniffer, followed by the techniques/algorithms used for obtaining r_j, α_j, β_j, and Δ_j.

III. Hardware Platform

The sniffers are implemented based on commercial MicroZed development boards and custom-designed AD9361 [4] software defined radio (SDR) modules. The block diagram of the sniffer is shown in Fig. 2. Since the bandwidth of AD9361 is limited to 56 MHz, two SDR modules are tuned to overlapping frequency bands to cover a 80 MHz WiFi channel. The FPGA firmware in the sniffer continuously monitors the output of SDR receivers and captures raw I/Q samples into the DRAM upon detecting a WiFi packet. A time stamp based on a hardware clock is also recorded to indicate the time at which the packet is received. The data is then transferred via network cables to a PC for processing. Fig. 3 shows the photo of a sniffer

[1]Eqn. (2) holds if the target and the sniffer are within line-of-sight of each other. The accuracy of a positioning system is deteriorated significantly under none-line-of-sight (NLOS) conditions. Addressing NLOS propagation and improving the positioning accuracy is an important research subject that is beyond the scope of this paper.

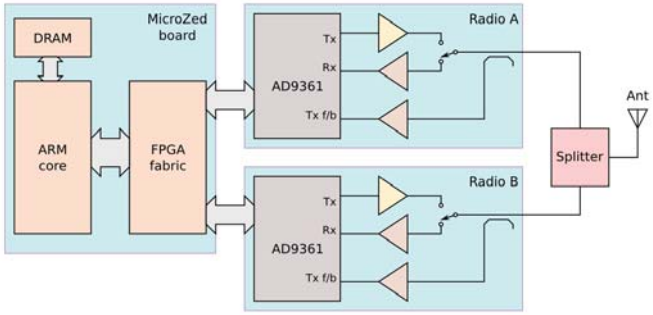

Fig. 2. Block diagram of the sniffer.

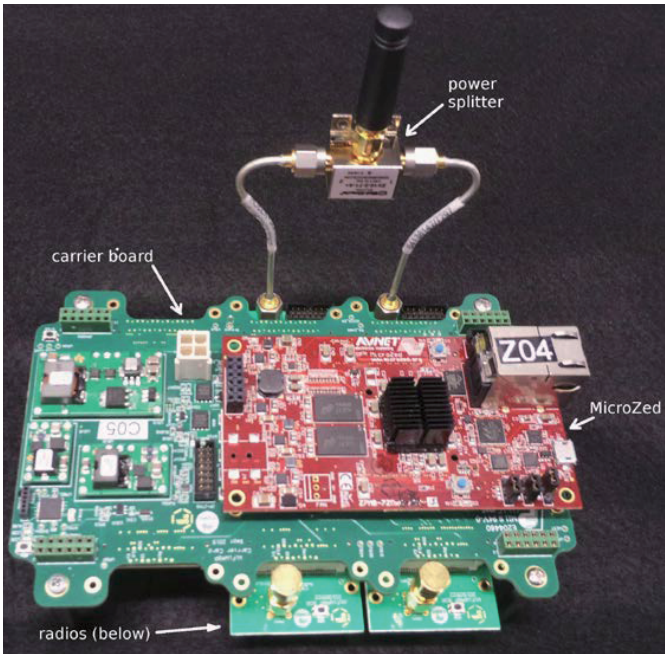

Fig. 3. A photo of the sniffer, which shows the Microzed, carrier board, and SDR modules sharing a single antenna.

IV. WiFi Packet Decoding and Packet Arrival Time Estimation

The captured I/Q samples are decoded to retrieve the information required for positioning, which include the source of each WiFi packet and the corresponding fine-grained arrival time at each sniffer.

A. Packet Source Determination

Since the sniffer is equipped with a single antenna, the payload of the packets encoded with multiple-input-multiple-output (MIMO) technology cannot be decoded. To address this issue, the sources of such packets are determine based on the context of the WiFi traffic. For example, the transmitter of a MIMO-encoded packet is identical to that of the accompanying Request-To-Send (RTS) packet or the destination of the associated Acknowledgement (ACK) packet.

B. Fine-grained Time Stamp Estimation

The precision of the measured packet arrival time (r_j in (2)) is critical to the position accuracy. The time stamp recorded by the sniffer has a coarse granularity determined by the sampling frequency of the radio, which s not enough for accurate positioning. For example, the time stamp is precise to 12.5 ns for a sampling frequency of 80 MHz, which corresponds to 3.75 m in distance. To improve the precision of the packet arrival time, the recorded time stamps are refined using the channel state information (CSI) obtained from the captured packets. Specifically, each WiFi packet contains channel training fields to estimate the channel response required for packet decoding. The CSI is obtained using the VHT long training field (VHT-LTF) in 802.11ac packets or the HT long training field (HT-LTF) in 802.11n packets [5], which are shown in Fig. 4. The excessive delay of the first signal path (relative to first sample of the packet) can be subsequently estimated from the CSI using super-resolution spectral estimation algorithms. The excessive delay is then added to the time stamp recorded by the hardware to obtain fine-grained packet arrival time measurements.

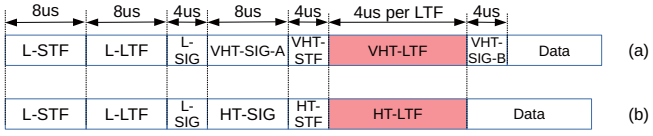

Fig. 4. Physical layer frame format of a WiFi packet [5]. (a): 802.11ac packet, (b): 802.11n packet.

Popular super-resolution estimation algorithms include MUSIC (Multiple Signal Classification) [6] or ESPRIT (Estimation of Signal Parameters via Rotational Invariance Technique) [7]. However, the performance of these approaches is significantly compromised in indoor environments due to the abundance of multi-path and non-line-of-sight (NLOS) propagations. In our system, the packet arrival time is estimated using the pattern matching algorithm described in [8]. Specifically, the frequency domain channel responses are firstly converted to the time domain to obtain the channel impulse response. The packet arrival time is then estimated by matching the leading edge of the channel impulse response against a database of leading edge templates and picking the delay information associated with the closest database entry. This is based on the discovery that all the information pertaining to the arrival time of the first path is contained in the leading edge of the channel impulse response. The accuracy of this approach in realistic indoor applications is significantly higher than the approaches based on MUSIC or ESPRIT, as has been demonstrated in [3].

V. Clock Synchronization

The clocks of the sniffers are post-synchronized by estimating and compensating for the clock skew and clock offset (α_j and β_j respectively in (1)), so that the packet arrival time are measured against a common reference clock.

A. Clock Skew Estimation

Suppose a standard WiFi device transmits two packets in succession at t_n and t_{n+1} respectively. The time period between the two transmissions ($t_{n+1} - t_n$) is sufficiently small (e.g., less than 0.5s), such that α_j and β_j can be considered as invariant during the period. The location of WiFi device is assumed to be unchanged, e.g., the device is stationary or the change is negligible. According to (2), the arrival times of the transmit packets at each anchor j are given by $r_j^n = (1+\alpha_j)\left(t_n + \frac{d_j}{c} + \beta_j + z_j^n\right)$ and $r_j^{n+1} = (1+\alpha_j)\left(t_{n+1} + \frac{d_j}{c} + \beta_j + z_j^{n+1}\right)$, respectively[2]. The difference between r_j^{n+1} and r_j^n is then given by

$$\begin{aligned} r_j^{n+1} - r_j^n =& (1+\alpha_j)(t_{n+1} - t_n) + \\ & (1+\alpha_j)(z_j^{n+1} - z_j^n). \end{aligned} \tag{4}$$

Similarly, for a different anchor k, the difference between the two recorded arrival time is given by

$$\begin{aligned} r_k^{n+1} - r_k^n =& (1+\alpha_k)(t_{n+1} - t_n) + \\ & (1+\alpha_k)(z_k^{n+1} - z_k^n). \end{aligned} \tag{5}$$

The relationship between α_j and α_k is thus obtained by dividing (4) by (5) as follows

$$\frac{1+\alpha_j}{1+\alpha_k} \approx \frac{r_j^{n+1} - r_j^n}{r_k^{n+1} - r_k^n}. \tag{6}$$

Multiplying both the numerator and denominator on the LHS of (6) by $(1-\alpha_k)$ gives

$$\frac{(1+\alpha_j - \alpha_k - \alpha_j\alpha_k)}{1-\alpha_k^2} \approx \frac{r_j^{n+1} - r_j^n}{r_k^{n+1} - r_k^n}. \tag{7}$$

$\alpha_j\alpha_k$ and α_k^2 can be ignored since α_j and α_k are in the order of 10^{-6} for typical crystal oscillators [9], and (7) can be rewritten approximately as

$$\alpha_j - \alpha_k \approx \frac{r_j^{n+1} - r_j^n}{r_k^{n+1} - r_k^n} - 1. \tag{8}$$

By assigning one of the sniffers as reference clock (i.e., $\alpha_j = 0$), the clock skews of other sniffers can be obtained from (8). Note that the only information required in this process is the recorded packet arrival time, while the location of the transmitter and the transmit time are not required.

B. Clock Offset Estimation

The clock offsets of the sniffers are estimated based on WiFi packets transmitted by standard WiFi devices at known locations, e.g., the AP. Since the locations of the sniffers are also known, the distance between the transmitter and the sniffer (d_j in (2)) can be readily obtained. Dividing both sides of (2) by $(1+\widehat{\alpha}_j)$, where $\widehat{\alpha}_j$ denotes the estimated clock skew using the approach described in Section V-A, one obtains

$$\frac{r_j}{1+\widehat{\alpha}_j} \approx t_{\text{Tx}} + \frac{d_j}{c} + \beta_j + z_j. \tag{9}$$

[2]Throughout Section V, the hardware delay Δt_j is assumed to have been compensated and therefore is omitted.

Similarly, for a different anchor k,

$$\frac{r_k}{1+\widehat{\alpha}_k} \approx t_{\text{Tx}} + \frac{d_k}{c} + \beta_k + z_k. \tag{10}$$

Subtracting (10) by (9) gives

$$\beta_k - \beta_j \approx \frac{r_k}{1+\widehat{\alpha}_k} - \frac{r_j}{1+\widehat{\alpha}_j} - \frac{d_k}{c} + \frac{d_j}{c}. \tag{11}$$

The clock offsets of the sniffers can then be obtained according to (8) by assigning the clock offset of the reference sniffer as 0.

Given the estimated clock skews and clock offsets, the measured packet arrival time are then corrected so that they are all measured against the clock of the reference sniffer. However, it should be noted that α_j and β_j drift with time and can be considered to be invariant only for a short time period (e.g., 0.5s). Therefore the transmissions used for clock synchronization and those for localization need to be proximate to each other in time for the model in (2) to hold.

VI. Hardware Delay Calibration

The hardware delay Δt_j represents the time required for the signal to propagate from the antenna of the sniffer to the Analog-Digital Converter (ADC) circuitry. The delay is dependent on the receiver state in practice, which degrades the positioning accuracy if unaccounted for. Particularly, we discovered that the hardware delay varies significantly with the receiving gain, i.e., the setting of the Automatic Gain Control (AGC) circuit [3][3]. Since the characteristic of AGC circuit varies with hardware, it is hard to model the hardware delay empirically.

To improve the accuracy of the measured packet arrival time, the variation of Δt_j is calibrated under different AGC settings in our system. Particularly, the sniffer was modified such that both SDR modules were fed radio signals from the same source through coaxial cables, with the signal power kept constant for one SDR module and varied for the other over a range of 90 dB using an attenuator. The differences between the receive time stamps obtained by the two SDR modules under different attenuator settings (therefore different AGC settings for the second SDR module) were recorded. A look up table that indicates the variation of the hardware delay under different AGC settings is then built. Fig. 5 shows the variation of the hardware delay with AGC settings for our sniffers. It can be seen that the hardware delay varies by as much as three nanoseconds, which corresponds to one meter in distance if not accounted for.

During system operation, the measured packet arrival time is corrected according to the associated AGC settings. Particularly, since the values of both α and Δt_j are small, (2) can be rewritten as

$$r_j = \Delta t_j + (1+\alpha_j)\left(t_{\text{Tx}} + \frac{d_j}{c} + \beta_j + z_j\right). \tag{12}$$

Therefore the excessive hardware delay can be subtracted from r_j directly.

[3]Note that AGC is critical for radio receivers. By adjusting the receive gain automatically, it ensures that the amplitude of the baseband signal is at an optimal level for digitization.

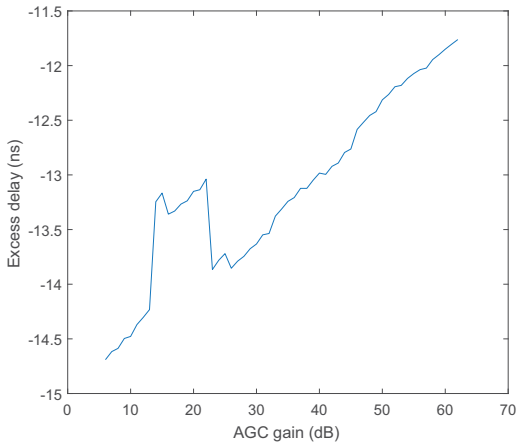

Fig. 5. Hardware delay variation under different AGC settings.

VII. Experiment Results

The system performance was evaluated under both outdoor line-of-sight (LOS) conditions and indoor NLOS conditions. A 802.11ac wireless local area network was set up during each experiment, which operate in channel 149 with 80MHz bandwidth. A laptop with a WiFi USB dongle was used as the target device, which pings the AP regularly to generate WiFi traffic. The packets transmitted by the APs were used for synchronizing the sniffers.

A. Outdoor Test

Fig. 6 shows the positioning result of the outdoor experiment, where six sniffers were deployed in a hexagonal arrangement around the WiFi network. The target was placed at 25 different locations to evaluate the overall positioning accuracy across the test area. It can be seen that the estimated target locations are consistent with the true locations. The

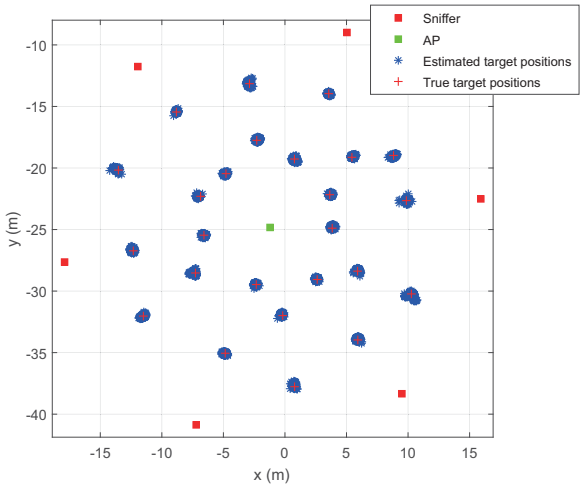

Fig. 6. Estimated target locations in the outdoor experiment.

cumulative distribution function (CDF) of the positioning errors is shown in Fig. 7. It can be seen that 90% of positioning errors are less than 0.23m.

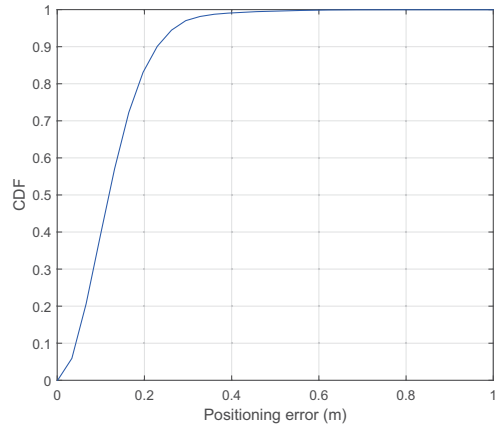

Fig. 7. Cumulative distribution of the positioning errors in the outdoor experiment.

B. Indoor Test

For the indoor experiment, we deployed 10 sniffers in an office, covering a area of around 700 square meters. Six standard Wi-Fi devices were placed at known locations for synchronizing the sniffer clocks. The target was moved across the test area along the centers of corridors. Fig. 8 shows the path the target and the estimated trajectory. It can be seen that the estimated trajectory is generally consistent with the true path. Given the width of the corridors is 1.1m, it can be observed that the positioning error is less than 1.5 m, which is sufficient for many indoor applications.

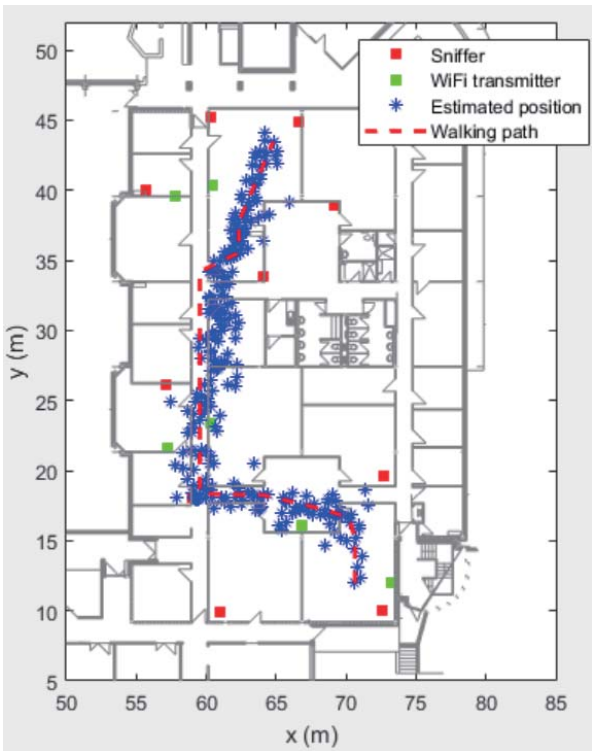

Fig. 8. Estimated target locations in the indoor experiment.

VIII. Conclusion

This work presents a research platform for WiFi-based positioning, where standard WiFi devices are located passively based on TDOA measurements. The architecture, hardware, and algorithms of the system are described, including the techniques used for anchor clock synchronizing and hardware delay calibration. It is shown experimentally that the positioning error is 23 cm in open spaces and 1.5 m in an indoor office environment for a 80 MHz WiFi system.

References

[1] H. Liu, H. Darabi, P. Banerjee, and J. Liu, "Survey of wireless indoor positioning techniques and systems," *IEEE Trans. Syst., Man, Cybern.*, vol. 37, no. 6, pp. 1067–1080, Nov. 2007.

[2] N. Patwari, J. Ash, S. Kyperountas, A. Hero, R. Moses, and N. Correal, "Locating the nodes: Cooperative localization in wireless sensor networks," *IEEE Signal Processing Mag.*, vol. 22, no. 4, pp. 54–69, Jul. 2005.

[3] T. Sathyan, D. Humphrey, and M. Hedley, "WASP: A system and algorithms for accurate radio localization using low-cost hardware," *IEEE Trans. Syst., Man, Cybern. C*, vol. 41, no. 2, pp. 211–222, 2011.

[4] [Online]. Available: http://www.analog.com/en/products/rf-microwave/integrated-transceivers-transmitters-receivers/wideband-transceivers-ic/ad9361.html

[5] "IEEE standard for information technology–telecommunications and information exchange between systems local and metropolitan area networks–specific requirements - part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications," *IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)*, pp. 1–3534, Dec 2016.

[6] R. O. Schmidt, "Multiple emitter location and signal parameter estimation," vol. 34, pp. 276 – 280, Apr. 1986.

[7] R. Roy and T. Kailath, "ESPRIT-estimation of signal parameters via rotational invariance techniques," *IEEE Trans. on Acoustics, Speech, and Signal Proc.*, vol. 37, no. 7, pp. 984–995, Jul. 1989.

[8] D. Humphrey and M. Hedley, "Prior models for indoor super-resolution time of arrival estimation," in *Proc. IEEE Veh. Technol. Conf. (VTC)*, 2009, pp. 1–5.

[9] J. Elson, L. Girod, and D. Estrin, "Fine-grained network time synchronization using reference broadcasts," *SIGOPS Oper. Syst. Rev.*, vol. 36, no. SI, pp. 147–163, Dec. 2002. [Online]. Available: http://doi.acm.org/10.1145/844128.844143