Project Report: Batch localization based on OFDMA backscatter

Fengyuan Zhu

I. Introduction

Recent years have witnessed rapid increment of Internet-of-Things (IoT) devices [1], which provide numerous novel applications typically consisting of mainly two parts, one is communication-based applications such as real-time environment monitoring [2]–[4], and the other is location-aware applications such as object searching [5], [6]. Since ubiquitous IoT devices are usually in small size and sensitive to energy, it is necessary to design IoT devices with low energy consumption. Thus, the recently proposed works [7]–[10] leverage the backscatter techniques to enable low-power communication and some other works [6], [11] focus on locating backscatter tag using channel state information (CSI).

As presented in existing works, backscatter brings backscatter system brings more benefits to the location-aware application in IoT networks. However, as the number of IoT devices increases, the method already proposed severely lowers the efficiency of wireless channel, which is not acceptable. On the other hand, existing methods [6], [16]–[20] try to improve localization accuracy via sending more localization packets continuously, which makes the situation only worse. The solution to this problem lies in the promotion of multiple access method.

OFDMA is a multiple access technique that is based on orthogonal frequency division multiplexing (OFDM). This technique is of high spectrum efficiency and will be applied in next generation of Wi-Fi, 802.11ax [23]–[26]. The basic idea of OFDMA is to divide the channel to subchannels, which are orthogonal in frequency domain. Thus, multiple users can modulate their data on the assigned subchannels to use channel simultaneously.

In this paper, we for the first time propose a scheme to locate multiple tags concurrently based on OFDMA backscatter. Our design realizes at least $48\times$ efficiency of existing low-power localization system. The key technique used in this work is the utilization of channel response (CR), which provides a symbol-level view of the channel. We made three main contributions.

First, we for the first time realize OFDMA in backscatter localization system, which leads to at least 48× efficient compared to current works. Second, we propose a new algorithm to dynamically eliminate the random phase offset on the receiver side without extra calibration process. Third, we propose the MUSIC extension scheme to to locate target with limited sub-carriers, antennas and packets.

As far as I am concerned, I am in charge of the OFDMA system and wrote all the codes for communication and CR (channel response) collection. It should be noted that the original OFDMA system was realized by the team led by R.J.Zhao. I was also a member of the team. The original system was used for communication. In this work, I modified the system so that it can realize localization when it communicates. Besides, I proposed the dynamic calibration method which can effectively eliminate the random phase offset on the receiver side. Furthermore, I did a survey on the random phase offset and proposed the detailed derivation of it. Finally, I checked the detailed information of OFDMA system, and suggested the three-dimension MUSIC algorithm (symbol domain, frequency domain and spatial domain). And the three-dimension MUSIC algorithm was finally realized by my partner, Xinyu Tong. The system overview as well as my contributions will be illustrated in this report.

II. Preliminaries

A. Framework

Our localization system works in a OFDMA backscatter framework. It is basically composed of three components, i.e. transmitter, tags with FPGA, and receiver. Fig. 1(a) is an illustration of how the system works. Firstly, the transmitter sends preamble and PHY header to synchronize with the receiver. Secondly, the transmitter sends a to-tag frame to the backscatter tags which synchronizes with the tags. Thirdly, the transmitter began to transmit a RF pure tone, while the tags triggered by the to-tag frame begin to backscatter the pure tone to send data. It should be noted that each tag can do different frequency shifting to realize sub-channel selection. To be specific, after the tags are assigned with a certain sub-channel, it adjust the backscatter frequency, and then begins to backscatter the pure tone to its assigned channel. Since these backscattered signals are synchronized, they make up a OFDM symbol, as shown in Fig. 1(b). Such a combined message can be separated and decoded on the receiver side using FFT.

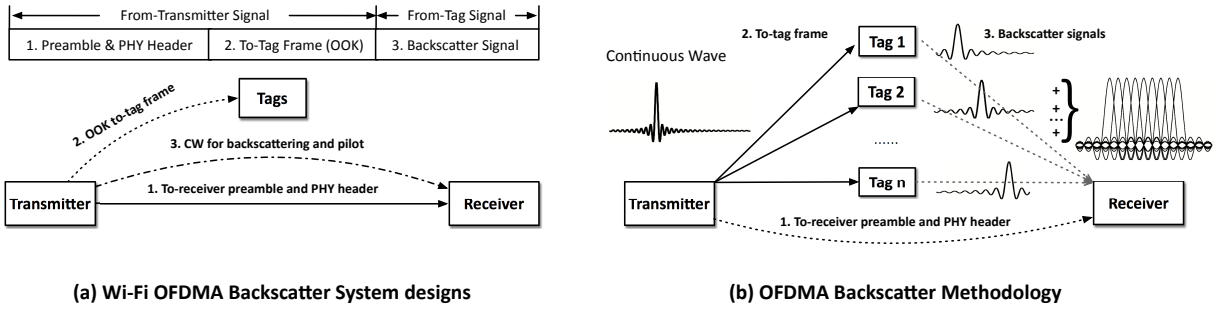

Fig. 1: Wi-Fi OFDMA Backscatter System Design.

B. Challenges

Based on such a architecture, we design a concurrent localization system. Before we introduce how this system works, we first list the challenges to our system.

a) ***Challenge 1: Collection of available CSI****:* In contrast to other CSI localization works [20], [29], we did not use Intel 5300 [27] which can provide 30 CSI measurements for each packet. We use Warp as our transceiver, therefore the channel estimation part should be realized on our own to obtain CSI. Besides, in our OFDMA architecture, the frame is composed of three parts, and the estimation of CSI is of great challenge because the preamble and to-tag frame come from the transmitter while backscatter signal comes from different tags in different places.

b) ***Challenge 2: Elimination of Phase Offsets****:* Phase offsets can significantly affect communication and localization [28], [30]. There are at least two important phase offsets to deal with in this work. They are continuous dynamic phase offset and down conversion phase offset. ***Continuous dynamic phase offset*** is a classic problem in communication. The receiver has a local oscillator with a slightly different frequency compared to the transmitter, which causes the symbols to have a increasing or decreasing angle. In our system, the tags perform frequency shifting, therefore incur additional frequency offset. If this combined frequency offset is not corrected, it will cause a continuous phase offset in the symbol domain, i.e. even in the same sub-carrier, different symbols will have different angles. Due to the fact that the phase difference between any two adjacent symbols is a small constance, we call it *Continuous dynamic phase offset*. Since we apply three-dimension MUSIC algorithm which includes symbol dimension, this problem has to be addressed. ***Downconversion phase offset*** is a phase offset caused by down conversion step on the receiver side. Different from the continuous phase offset, which is a offset in frequency level, downconversion phase offset is a offset in spatial level. Specifically,

different antennas are connected to different down-converters. Though these down-converters share the same reference frequency provided by crystal oscillator, they are independently locked to random phases after setting the working frequency. These random phases will be transferred to symbols in the baseband after downconversion. Since our localization algorithm includes spatial dimension, which utilize the phase difference of symbols between antennas, such random phase offsets would corrupt the results and therefore must be addressed.

c) ***Challenge 3: Locating with limited subcarriers****:* Form Fig. 1(b), we observe that limited subcarriers could be assigned to one tag. This is rooted in the design of OFDMA backscatter system, where different subcarriers have been assigned to different tags. Since the amount of subcarriers is constant, with the increase of tags to be located, the number of subcarriers for one certain tag decreases. In fact, such a problem would make prior low-power localization system depending on multiple subcarriers inapplicable. For example, RF-Echo and WiTag [6], [11] parse ToF based on multi-subcarrier CSI. When limited subcarriers could be employed, these systems cannot provide satisfing solution. Another possible scheme against limited subcarriers is to utilize numerous packets to improve reliability [20]. However, such frequent communication is energy-consuming and might not be satisfied in practical low-power backscatter system. Since 3D-CSI collected is exactly unstable and therefore leads to inaccurate AoA, this challenge is necessary to be addressed in our system. However, OFDMA backscatter mechanism limits the employment of multiple subcarriers while low-power communication mechanism makes continuous massive packets inoperable. Thus, it is challenging to locate target accurately with limited subcarriers and packets.

III. System Overview

Our localization system can realize concurrent localization for OFDMA backscatter tags. The entire process can be divided into the following modules:

a) ***OFDM Burst Processing Module:****:* In this part, we process the received signal to obtain multi-dimension CSI. Firstly, we apply the matched filter to received signal. Secondly, we perform cross-relation to find the LTS peak, which indicates the starting point of the frame. This process is based on the property of preamble. According to the starting point of the frame, we can divide the frame into three parts, i.e. preamble with PHY header, to-tag frame and backscatter signal. Thirdly, we eliminate the cyclic prefix (CP) of each OFDM symbol. Fourthly, we perform FFT to transform the time domain signal to frequency domain. We can distinguish the signals

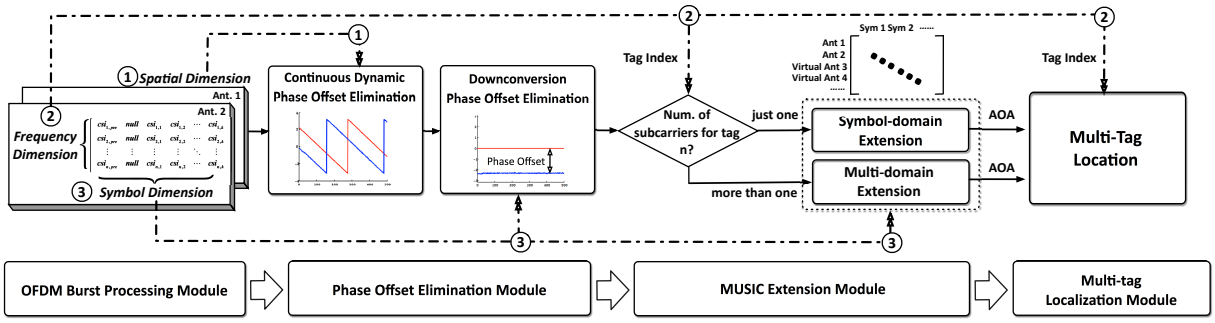

Fig. 2: System Overview.

in different sub-channels by the index of 64-point FFT. Finally, we divide each symbol by the generated symbol, which has a normalized phase, and then we obtain the channel response, i.e. the CSI.

b) ***Phase Offset Elimination Module:*** As described in *challenge 2*, there are two main phase offsets in our system which can significantly affect the performance of localization. For continuous dynamic phase offset, we process the CSI in spatial domain, because the frequency offsets of all antennas are equivalent. Note that the AOA localization requires the difference of angles of CSIs of different antennas. Therefore, we design a scheme to eliminate the phase offset utilizing the CSI in spatial domain. This step is illustrated in the Fig.2. The other phase offset is the downconversion phase offset. Since the CSI in our system includes the information from transmitter and from tag, i.e. from different propagation paths, this phase offset can be automatically eliminated since we know the positions of the APs. In contrast to previous works, we for the first time remove this phase offset without interruptting normal communication, which is more and more necessary with the increase of connected IoT devices. Besides, since our phase offset elimination module works in a real-time manner (frame-level), the performance evaluation and re-calibration processes mentioned in previous work [29] are also unnecessary.

c) ***MUSIC Extension Module:*** To address *challenge 3*, our MUSIC Extension algorithm consists of ***symbol-domain extension*** and ***multi-domain extension***. As shown in Fig. 2, we first determine the number of subcarriers assigned to given tag and then perform corresponding MUSIC extension. Symbol-domain extension and multi-domain extension share the same basic idea, i.e., improving performance by establishing virtual antenna array. Mathematically, we extend the dimensions of traditional MUSIC matrix to obtain more accurate AOA measurement. In particular, our 3D-CSI collected provides us with fine-grained channel state depiction and around

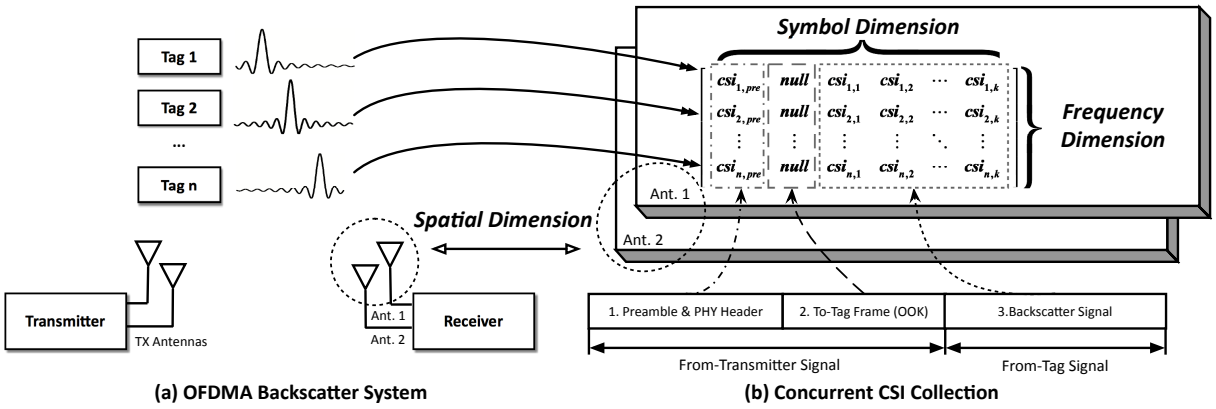

Fig. 3: Concurrent CSI Collection.

$500\times$ samples for each communication compared with packet-level CSI. Therefore, we can utilize symbol-dimension CSI to build up symbol-domain extension matrix while employ both symbol-dimension and frequency-dimension CSI to build up multi-domain extension matrix for MUSIC algorithm.

IV. OFDM Burst Processing and Localization Principles

In this work, CSI collection is my main work, i.e. obtaining CSI through baseband processing. The whole process consists some knowledge of 802.11g, because our OFDMA framework is a stimulation of this protocol although 802.11g itself does not realize OFDMA. The main hardware that I use is Warp, which is installed with WarpLab, a officially provided Warp code for the on-chip FPGA. After setting some parameters in initialization, we can use digital signal processing to obtain the required 3D-CSI.

A. 3D-CSI Analysis

There are several steps before we can obtain the raw CSI. First, as a typical step in communication, we need to apply the matched filter to the received signal in time domain. This step can eliminate inter-symbol interference (ISI) as much as possible. Then the time-domain signal is sent to the 64-point FFT module. In this module, the signal is transformed into frequency domain, i.e, we get $S_r(f)$. After that, we obtain one sample for each symbol. And the FFT index indicates the number of the sub-carrier. So far, we have not obtained CSI. Since $H(f) = S_r(f)/S_t(f)$, and CSI is factually channel response $H(f)$, we need to obtain $S_t(f)$ to get CSI. Here the $S_r(f)$ denotes the received symbol in frequency domain, and $S_t(f)$ denotes the transmitted symbol in

frequency domain. Since we can decode the received signal to obtain transmitted bits, and we can map the transmitted bits to frequency-domain symbols based on the modulation type, we can therefore obtain $S_t(f)$ after some signal processing. Finally, apply $H(f) = S_r(f)/S_t(f)$, then the multi-dimension CSI is obtained. The above signal processing and decoding steps are the same for each subcarrier. The above steps are the same for each antenna as well, i.e., all the above steps are identical to different antennas because different antennas receive signals independently. After these processing, as Fig.3 shows, the CSIs of each time slot (symbol) and of each tag and of each antenna are obtained.

B. Phase offsets and localization principles

It should be noted that so far we have not distinguished CSIs in three different frame parts. However, the difference of CSIs among these parts is the key part of our batch localization scheme. This difference is important because we have not dealt with the two main phase offsets listed in the introduction part. Now we consider the CSIs in the preamble and to-tag frame part. These CSIs belong to the transmitter, and they are corrupted by a random phase ϕ_0 and a dynamic phase offset $\phi(t) = \Delta f t$. It should be emphasized that for each antenna, the random phase offset ϕ_0 is the same in the time domain (symbol domain), but they are different between antennas. On the contrary, dynamic phase offset is the same for the symbols sampled at the same time even if they belong to different antennas, but they are different in different time slots. The localization result lies in the differences among the CSIs of different antennas.

For example, there are two antennas for Warp, noted as A and B. Antenna A suffers a random phase offset ϕ_1, and antenna B suffers a random phase offset ϕ_2. At the same time, they also suffer a dynamic phase offset in time domain, i.e. $\phi(t) = \Delta f t$. In reality, since the received signal is discrete, the dynamic phase offset is also in a discrete form; however, for the convenience of illustration, we use the continuous form. Then, for symbol n of antenna A, the total phase offset is $\Phi(n) = \phi_1 + \Delta f \Delta t n$. Here Δt is the symbol duration, which is a constant value for a given communication protocol. Similarly, we can obtain the phase offset for antenna B: $\Phi(n) = \phi_2 + \Delta f \Delta t n$. ϕ_2 is the random phase offset for antenna B. Since there are only two antennas, we can immediately obtain a series of localization result (AOA) by subtracting the phase of each symbol of A from corresponding symbols of B. Then the phase offsets also experience such a operation. The remaining phase offset in the obtained AOA is $\Delta\Phi(n) = \phi_1 - \phi_2 = \phi$. Here ϕ is the difference between two random variables and is

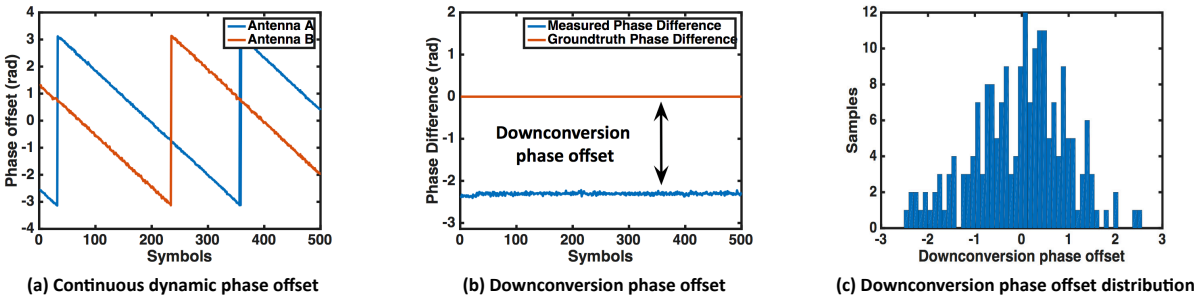

Fig. 4: Phase offset elimination.

therefore also a random variable. Therefore, in the localization result, the dynamic phase offset is automatically eliminated because we perform subtraction in the same time slot. Nevertheless, there is still a unknown random phase offset ϕ, which causes trouble to our localization. If this value is not determined, then all the AOAs calculated are all random, i.e. they are all meaningless. Now we note that there are two kinds of CSI in our sight: one from the preamble/to-tag frame, and the other from the backscatter signal. In correspondence, we get two kinds of AOA. The first kind of AOAs means the true AOA of transmitter plus the random phase ϕ, while the second kind of AOAs means the true AOA of each backscatter tag working in different subcarriers plus the random phase ϕ. Now that we already know the position of the transmitter, we substract these two kinds of AOAs. After this operation, we obtain the $relative$ AOAs of tags from transmitter, and the random phase offset ϕ is totally eliminated. Due to the fact that we know the real absolute AOA of transmitter (because we know the position of transmitter), we can therefore obtain the real absolute AOAs of the tags. These are the principles of our localization. So far, we have not considered how to determine the final AOA since we have so many AOAs of tags in each frame. The final determination of AOA experiences a multi-dimension MUSIC algorithm. Since this part is realized by Xinyu Tong, this report does not cover this part.

V. Conclusion

In this paper, we have presented how to enable batch localization in OFDMA backscatter. Instead of utilizing multiple antennas, subcarriers and packets for pure accuracy improvement, we appropriately utilized fine-grained 3D-CSI to enable system concurrency, energy conservation, communication compatibility and accuracy. First, we utilized frequency-dimension to collect multi-tag CSI concurrently based on OFDMA. Then, we employed spatial-dimension CSI and

symbol-dimension CSI to remove phase offsets. Finally, we performed our MUSIC extension scheme and locate multiple tags concurrently. Experimental results show that our system can achieve 50× valid concurrency compared with the existing design. Meanwhile, our system can realize average localization errors within 0.28m while the tag consumes 55-81.3W active power.

REFERENCES

[1] Behind The Numbers: Growth in the Internet of Things. https://www.ncta.com.

[2] Q. Chi, H. Yan, C. Zhang, Z. Pang and L. Da Xu, "A reconfigurable smart sensor interface for industrial WSN in IoT environment," in *IEEE transactions on industrial informatics*, pp. 1417-1425, 2014.

[3] N. Vijayakumar and R. Ramya, "The real time monitoring of water quality in IoT environment," in *ICCPCT*, pp. 1-4, 2015.

[4] L. Dan, C. Xin, H. Chongwei and J. Liangliang, "Intelligent agriculture greenhouse environment monitoring system based on IOT technology," in *ICITBS*, pp. 487-490, 2015.

[5] J. Wang and D. Katabi, D, "Dude, where's my card?: RFID positioning that works with multipath and non-line of sight," in *ACM SIGCOMM*, pp. 51-62, 2013

[6] M. Kotaru, P. Zhang and S. Katti, "Localizing Low-power Backscatter Tags Using Commodity WiFi," in *ACM CoNEXT*, pp. 251-262, 2017.

[7] A. Wang, V. Iyer, V. Talla, J. R. Smith and S. Gollakota, "FM Backscatter: Enabling Connected Cities and Smart Fabrics," in *NSDI*, pp. 243-258, 2017.

[8] B. Kellogg, V. Talla, J. R. Smith and S. Gollakot, "Passive Wi-Fi: bringing low power to wi-fi transmissions," in *NSDI*, 2016.

[9] P. Zhang, C. Josephson, D. Bharadia and S. Katti, "FreeRider: Backscatter Communication Using Commodity Radios," in *ACM CoNEXT*, pp. 389-401, 2017.

[10] P. Zhang, D. Bharadia, K. Joshi and S. Katti, "HitchHike: Practical backscatter using commodity WiFi," in *Proc. ACM SenSys*, 2016.

[11] L. X. Chuo, Z. Luo, D. Sylvester, D. Blaauw and H. S. Kim, "RF-Echo: A Non-Line-of-Sight Indoor Localization System Using a Low-Power Active RF Reflector ASIC Tag," in *ACM MobiCom*, pp. 222-234, 2017.

[12] J. Ou, M. Li and Y. Zheng, "Come and be served: Parallel decoding for COTS RFID tags," in *Proc. ACM MobiCom*, 2015.

[13] P. Hu, P. Zhang, D. Ganesan, "Leveraging interleaved signal edges for concurrent backscatter," in *Proc. ACM HotWireless*, 2014

[14] P. Hu, P. Zhang, D. Ganesan, "Laissez-faire: Fully asymmetric backscatter communication," in *Proc. ACM SIGCOMM*, 2015.

[15] O. Abari, D. Vasisht, D. Katabi and A. Chandrakasan, "Caraoke: An E-toll transponder network for smart cities," in *Proc. ACM SIGCOMM*, 2015.

[16] 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 *ACM MobiCom*, pp. 243-256, 2016.

[17] K. Qian, C. Wu, Z. Yang, Y. Liu and K. Jamieson, "Widar: Decimeter-Level Passive Tracking via Velocity Monitoring with Commodity Wi-Fi," ," in *ACM MobiHoc*, 2017.

[18] X. Li, D. Zhang, Q. Lv, J. Xiong, S. Li, Y. Zhang and H. Mei, "IndoTrack: Device-Free Indoor Human Tracking with Commodity Wi-Fi," in *ACM Ubicomp*, pp. 1-22, 2017.

[19] X. Li, S. Li, D. Zhang, J. Xiong, Y. Wang, and H. Mei, "Dynamic-MUSIC: Accurate Device-free Indoor Localization," in *ACM UbiComp*, pp. 196-207, 2016.

[20] M. Kotaru, K. Joshi, D. Bharadia and S. Katti, "Spotfi: Decimeter level localization using wifi," in *ACM SIGCOMM*, pp. 269-282, 2015.

[21] D. Vasisht, S. Kumar and D. Katabi, "Decimeter-Level Localization with a Single WiFi Access Point," in *NSDI*, pp. 165-178, 2016.

[22] S. Kumar, S. Gil, D. Katabi and D. Rus, "Accurate indoor localization with zero start-up cost," in *ACM MobiCom*, pp. 483-494, 2014.

[23] 802.11ax - 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 Amendment Enhancements for High Efficiency WLAN, Available Online: http://standards.ieee.org/develop/wg/WG802.11.html.

[24] 802.11ax: Transforming Wi-Fi to bring unprecedented capacity and efficiency, Qualcomm Technologies, Available Online: https://www.qualcomm.com/solutions/networking/features/80211ax.

[25] 802.11ax: Next generation Wi-Fi for the Gigabit home, Broadcom white paper, Available Online: https://www.mobileworldlive.com/broadcom-whitepaper-802-11ax-next-generation-wi-fi-for-the-gigabit-home/.

[26] Introduction to 802.11ax, National Instruments white paper, Available Online: http://www.ni.com/80211ax/.

[27] D. Halperin, W. Hu, A. Sheth and D. Wetherall, "Tool release: Gathering 802.11n traces with channel state information," in *ACM SIGCOMM*, 2011.

[28] J. Xiong and K. Jamieson, "ArrayTrack: A fine-grained indoor location system," in *NSDI*, pp. 71-84, 2013.

[29] J. Gjengset, J. Xiong, G. Mcphillips and K. Jamieson, "Phaser:enabling phased array signal processing on commodity wi-fi access points," in *ACM MobiCom*, 2014.

[30] Z. Chen, Z. Li, X. Zhang, G. Zhu, Y. Xu, J. Xiong, X. Wang, "AWL: Turning Spatial Aliasing From Foe to Friend for Accurate WiFi Localization,"in *ACM CoNEXT*, pp. 238-250, 2017.

[31] J. Xiong, K. Sundaresan and K. Jamieson, "ToneTrack: Leveraging Frequency-Agile Radios for Time-Based Indoor Wireless Localization," in *ACM MobiCom*, pp. 537-549, 2015.

[32] Z. Yang, Z. Zhou and Y. Liu, "From rssi to csi: indoor localization via channel response," in *ACM Computing Surveys*, pp. 1-32, 2014.

[33] J. Xiao, Z. Zhou, Y. Yi and L. M. Ni, "A survey on wireless indoor localization from the device perspective," in *ACM CSUR*, 2016.

[34] Y. Wang, Q. Ye, J. Cheng and L. Wang, "RSSI-based bluetooth indoor localization," in *MSN*, pp. 165-171, 2015.

[35] Y. Zeng, P. H. Pathak and P. Mohapatra, "WiWho: wifi-based person identification in smart spaces," in *IEEE IPSN*, 2016.

[36] W. Wang, A. X. Liu and M. Shahzad, "Gait recognition using wifi signals," in *ACM Ubicomp*, pp. 363-373, 2016.

[37] R. O. Schmidt, "Multiple emitter location and signal parameter estimation," in *IEEE Trans. on Antennas and Propagation*, 1986.

[38] R. Behzad, "RF Microelectronics, second edition", pp. 161-179, 2012.

[39] WARP Project, Available Online: http://warpproject.org

[40] Power splitter/combiner, BP2U+ by Mini-Circuits, https://www.minicircuits.com/pdfs/BP2U+.pdf

[41] SPST reflective switch, ADG902 by ADI, http://www.analog.com/media/en/technical-documentation/data-sheets/ADG901 902.pdf

[42] FPGA development board, NEXYS4 by DIGILENT, https://reference.digilentinc.com/media/reference/programmable-logic/nexys-4-ddr/nexys4ddr rm.pdf

[43] Linux 802.11n CSI Tool, http://dhalperi.github.io/linux-80211n-csitool/faq.html