

# Wi-Fi Sensing Tool Release: Gathering 802.11ax Channel State Information from a Commercial Wi-Fi Access Point

Zisheng Wang<sup>1</sup>, Feng Li<sup>2</sup>, Hangbin Zhao<sup>2</sup>, Zihuan Mao<sup>1</sup>, Yaodong Zhang<sup>1</sup>, Qisheng Huang<sup>1</sup>, Bo Cao<sup>1</sup>, Mingming Cao<sup>1</sup>, Baolin He<sup>1</sup>, Qilin Hou<sup>1</sup>

**Abstract**—Wi-Fi sensing has emerged as a powerful technology, leveraging channel state information (CSI) extracted from wireless data packets to enable diverse applications, ranging from human presence detection to gesture recognition and health monitoring. However, CSI extraction from commercial Wi-Fi access point lacks and out of date. This paper introduces ZTECSITool, a toolkit designed to capture high-resolution CSI measurements from commercial Wi-Fi 6 (802.11ax) access points, supporting bandwidths up to 160 MHz and 512 subcarriers. ZTECSITool bridges a critical gap in Wi-Fi sensing research, facilitating the development of next-generation sensing systems. The toolkit includes customized firmware and open-source software tools for configuring, collecting, and parsing CSI data, offering researchers a robust platform for advanced sensing applications. We detail the command protocols for CSI extraction, including band selection, STA filtering, and report configuration, and provide insights into the data structure of the reported CSI. Additionally, we present a Python-based graphical interface for real-time CSI visualization and analysis.

**Index Terms**—Wi-Fi, Channel State Information, ZTECSITool

## I. INTRODUCTION

Wi-fi Sensing has been rapidly studied, using channel state information (CSI) obtained from the wireless data packets to enable a variety of applications from the most basic person present detection to gesture recognition and human heath monitoring. We proposed a toolkit (ZTECSITool) that records CSI measurements with a recent 802.11ax protocol and a larger number of subcarriers (up to 512 for 160MHz). The toolkit use the ZTE AX3000 series Wi-Fi Access Point (AP) products <sup>1</sup> with 3x Tx/Rx antennas for 5GHz and 2x Tx/Rx antenna for 2.4GHz. We provide a CSI toolkit to setup, record, and parse the CSI measurements for later analysis. In this paper, we also provide details of controlling methods and CSI structures so that users can design their own CSI applications.

## II. CSI EXTRACTION TOOL AND DATASETS

In current CSI-based Wi-Fi sensing technique, researchers typically utilize open-source CSI datasets and toolkits from various commercial Wi-Fi network adapters. In this section, we briefly introduce the widely used Wi-Fi CSI extraction tools and open-source CSI datasets for Wi-Fi sensing.

<sup>1</sup>Two types of AX3000 AP are supported. Production Type E2631 for AX3000 and ZXSLC SR6110 for AX3000 Pro. Both APs have the same Wi-Fi parameters where AX3000 Pro (SR6110) has two 2.5G ETH ports.

TABLE I  
CURRENT CSI EXTRACTION TOOLS COMPARED WITH ZTECSITOOL

Name	MIMO	802.11 Support	Sub-carriers	Bandwidth (MHz)	Resolution (bits)
CSITool	2x2	11n	60	40	8
Nexmon CSI Extractor	4x4	11n/ac		80	
Atheros CSI Tool	-	11n	114	40	8
ZTECSITool	3x2	11n/ac/ax	512	160	16

### A. CSI Extraction Tool

We first compiled a list of commonly used CSI extraction tools in current research, which is presented in Table I. The currently available and most widely used open-source CSI extraction tools includes CSITool [1], Nexmon CSI Extractor [2], Atheros CSI Tool [3], ESP32 CSI Toolkits [4], and the proposed ZTECSITool introduced in this work. A detailed comparison of the above tools, including Wi-Fi chipset architectures, operating system platforms, multi-input multi-output (MIMO) characteristics, 802.11 support, and additional parameters, is provided in the table. It is noteworthy that, compared to other CSI extraction tools, our proposed MT7916-based ZTECSITool supports both Linux and Windows Operating System platform and is compatible with the IEEE 802.11ax (WiFi 6) standard. Based on the 802.11ax standard and the advanced chipset design, ZTECSITool supports a bandwidth of up to 160 MHz and 512 subcarriers quantized with 16 bits. This capability provides more extensive and precise CSI information for Wi-Fi sensing.

### B. Opensource CSI Dataset

As WiFi sensing research advances, numerous open-source CSI datasets have become available. We categorize these datasets into three main types, based on their collection methods and data scale.

The first type of CSI dataset is collected by Wi-Fi systems with distributed antennas, e.g., WiSDAR [5], WiNDR [6] and WiCross [7]. Concretely, WiSDAR evaluates different distributed antenna topologies, such as line, hexagon, square, and random arrangements, which reveals the regions most

sensitive to human activities and achieves both high accuracy and reliability in Wi-Fi-based recognition. In order to design the placement of distributed antennas based on the principles of electromagnetic propagation, WiNDR and WiCross place three antennas for both the transmitter and receiver in a staggered and distributed manner around a 360° circle. Such configuration can effectively alleviate the confusion caused by the orientation according to the characteristics of the Fresnel region, and thus, enable the direction-agnostic gesture recognition.

The second type utilizes additional Wi-Fi devices to create a distributed system for CSI extraction. For example, the scenarios of single transmitter with multiple receivers are investigated in ReWiS [8], WiTraj [9], Widar 3.0 [10] and OneFi [11]. Through this distributed observation approach, the essential environment-independent information required for Wi-Fi sensing can be collected via CSI. Additionally, the theoretical relationship between sensing range and the transceivers distance is derived by Wang et al [12], which reveals that optimizing the layout of distributed devices can effectively enhance the sensing coverage and suppress environmental interference on sensing. The last type is the dataset with scaling up training data. In the context of data-driven Wi-Fi sensing methods, increasing the amount of training data is a vital method for enhancing the generalization capabilities of deep learning approaches. To this end, The representative methods, including Widar3.0 [10], MM-Fi [13], XRF55 [14] and CSI-PCNH [15], have all acquired large-scale CSI data for training. In the above work, the researcher researchers have found that training on tens of thousands of samples allows the sensing model to naturally achieve invariance to direction and position, while also supporting adaptation to new environments through learning from a small number of samples and fine-tuning model parameters.

### III. DETAILS ON ZTECSITOOL

In this section, we describe our contribution, ZTECSITOOL, which allows WLAN sensing researchers collect CSI raw data up to 512 sub-carriers for each chain from our commercial ZTE AX3000 APs. ZTECSITOOL consists of

- ZTE AX3000 Series AP: which accepts CSI configuration commands and uploads CSI raw data from and to LAN/WLAN.
- A PC software: which helps to control and parse the CSI raw data.

We first present the system architecture. Then, the CSI control commands and CSI data format are described in detail. Next, we present ZTECSITOOL software. Finally, essential usage notes for ZTECSITOOL are outlined. Anyone can access the latest information and access ZTECSITOOL from [https://github.com/WiFiZTE2025/ZTE\\_WiFi\\_Sensing.git](https://github.com/WiFiZTE2025/ZTE_WiFi_Sensing.git).

#### A. System Architecture

ZTECSITOOL maximizes usability by taking into account the diverse needs of different research scenarios. Hence, a CSI collection system using ZTECSITOOL consist of four parts:

- ZTE AP: The key part of the system. It estimates CSI from received PPDU preambles and uploads CSI accordingly.
- A Wi-Fi STA: usually a mobile phone. In WLAN sensing applications, Wi-Fi STAs typically transmit PPDU based on specific constraints or protocol-defined requirements.
- A CSI Controller: usually a computer. It sends CSI commands to the ZTE AP. It equips the software in ZTECSITOOL.
- A CSI Collector: usually a computer. It receives CSI from the ZTE AP after the AP is configured by the CSI controller.

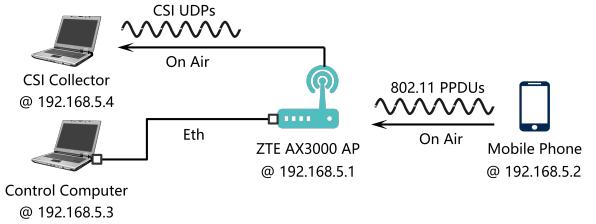


Fig. 1. An example system architecture of the CSI collection system using ZTECSITOOL.

Figure 1 shows an example system architecture of the CSI collection system using ZTECSITOOL. For the convenience, CSI Controller and Collector talks with the ZTE AP on IP protocol so that CSI controller and collector can use LAN or WLAN to finish their job once it obtains IP addresses from ZTE AP. The Controller and Collector can be the same computer. Note that, controller and collector require IP addresses assigned by ZTE AP, so it can't connect with ZTE AP using WAN. Which LAN port is WAN is subject to the user configuration. In the next section, we introduce how the CSI Controller should operate and how to issue CSI control commands.

#### B. CSI Commands

CSI Controller sends CSI command by using pre-defined UDP packets to the gateway of ZTE AP with port 8021. The UDP packets contains a magic number, command type and command data which is listed in TABLE II. ZTE AP listens UDP packets at 8021. Once ZTE AP parses correct magic number from captured UDP packets, it will start to parse the whole command and execute the corresponding job as per defined in this section. All field is little-end. The definition of CMD\_DATA field depends on CMD\_TYPE.

1) *CSI Report Enable Command (0x1)*: By setting CMD\_TYPE to 0x1 in the CSI Configuration UDP command, we can enable or disable the CSI report. The format of CSI Report Enable Command is defined in TABLE III.

2) *CSI STA Filter Command (0x2)*: ZTE AP might have many STA associated. By default, if CSI reporting is enabled, ZTE AP will report CSI based on PPDU's from every STA. Using CSI STA Filter Command, ZTE AP will only report CSI data from certain STAs. ZTE AP supports at most 5 STAs

TABLE II  
THE OVERALL FORMAT OF THE CSI CONFIGURATION UDP COMMAND

field	count	type	description
MAGIC_NUM	1	uint64_t	The magic num is set to 0xCAFE2025. ZTE AP use this field to validate the UDP packets
CMD_TYPE	1	uint8_t	The type of cmd.
CMD_DATA	various	-	CMD_DATA depends on the type of cmd.

TABLE III  
THE FORMAT OF THE CSI REPORT ENABLE COMMAND

field	count	type	description
MAGIC_NUM	1	uint64_t	The magic num is set to 0xCAFE2025. ZTE AP use this field to validate the UDP packets
CMD_TYPE	1	uint8_t	Set to 0x1 for CSI Report Enable Command
Enable	1	uint8_t	0 - for stopping CSI report 1 - for starting CSI report

TABLE IV  
THE FORMAT OF THE CSI STA FILTER COMMAND

field	count	type	description
MAGIC_NUM	1	uint64_t	The magic num is set to 0xCAFE2025. ZTE AP use this field to validate the UDP packets
CMD_TYPE	1	uint8_t	Set to 0x2 for CSI STA Filter Command. Suppose that the MAC address is 01:02:03:04:05:06
STA MAC 0	1	uint8_t	then, STA MAC 0 = 0x01
STA MAC 1	1	uint8_t	then, STA MAC 1 = 0x02
STA MAC 2	1	uint8_t	then, STA MAC 2 = 0x03
STA MAC 3	1	uint8_t	then, STA MAC 3 = 0x04
STA MAC 4	1	uint8_t	then, STA MAC 4 = 0x05
STA MAC 5	1	uint8_t	then, STA MAC 5 = 0x06

in the filter list. ZTE AP will not check if filtered STA has associated or if the STA mac is valid. The format of CSI STA Filter Command is defined in TABLE IV

3) *CSI Configuration Command (0x3)*: ZTE AP can report CSI of PPDUs from certain types. We can also configure the number of chains reported. The format of CSI Configuration Command is defined in TABLE V

4) *CSI Report Configuration Command (0x4)*: By default, CSI is reported by fragmented UDP packets sending to destination IP 192.168.X.2, destination port 8023 and source port 8024. The X in the destination IP depends on how the gateway of ZTE AP is set. But we allow user to change the destination IP to whichever they want. If this IP address is assigned to

TABLE V  
THE FORMAT OF THE CSI CONFIGURATION COMMAND

field	count	type	description
MAGIC_NUM	1	uint64_t	The magic num is set to 0xCAFE2025. ZTE AP use this field to validate the UDP packets
CMD_TYPE	1	uint8_t	Set to 0x3 for CSI Configuration Command.
FRAME_TYPE	1	uint8_t	The FRAME_TYPE are defined as per 9.2.4.13 Type and Subtype subfields (Draft P802.11 REVme_D7.0). For example, as per Table 9-1, QoS data is indicated by B3 B2 = 2b'10 B7 B6 B5 B4 = 4b'1000 Then FRAME_TYPE shall be set to 0 0 B7 B6 B5 B4 B3 B2 = 0x22 Note that ZTE won't guarantee that ppdus with any frame type can report valid CSI. We encourage user use QoS data (FRAME_TYPE = 0x22)

TABLE VI  
THE FORMAT OF THE CSI REPORT CONFIGURATION COMMAND

field	count	type	description
MAGIC_NUM	1	uint64_t	The magic num is set to 0xCAFE2025. ZTE AP use this field to validate the UDP packets
CMD_TYPE	1	uint8_t	Set to 0x4 for CSI Report Configuration Command.
TGT_IP	4	uint8_t	if target ip address is 192.168.1.1 TGT_IP[0] = 192 TGT_IP[1] = 168 TGT_IP[2] = 1 TGT_IP[3] = 1

a device which is a 802.11 STA connects to the ZTE AP, the CSI will be reported through WLAN interface. If this IP address is assigned to a devices which, for example, is a PC which connects to the ZTE AP by LAN, the CSI will be reported through the LAN connected. The format of CSI Report Configuration Command is defined in TABLE VI.

5) *CSI Band Configuration Command (0x5)*: The user can determine whether CSI is collected from 2.4G band or 5G band. Due to the limitation of system design, ZTE AP only supports one band a time. The format of CSI Band Command is defined in TABLE VII.

6) *Check Availability Command (0x6)*: We allow user to check if ZTE AP is ready for CSI report. After received Check Availability Command, ZTE AP will reply an UDP

TABLE VII  
THE FORMAT OF THE CSI BAND CONFIGURATION COMMAND

field	count	type	description
MAGIC_NUM	1	uint64_t	The magic num is set to 0xCAFE2025. ZTE AP use this field to validate the UDP packets
CMD_TYPE	1	uint8_t	Set to 0x5 for CSI Band Configuration Command
BAND	1	uint8_t	0 for 2.4G band 1 for 5G band

TABLE VIII  
THE FORMAT OF THE CHECK AVAILABILITY COMMAND

field	count	type	description
MAGIC_NUM	1	uint64_t	The magic num is set to 0xCAFE2025. ZTE AP use this field to validate the UDP packets
CMD_TYPE	1	uint8_t	Set to 0x6 for Check Availability Command

packet with "OK" in the data field if ZTE AP is ready for CSI Report. The format of Check Availability Command is defined in TABLE VIII

#### C. How to use command

In Section III-B, we introduce the commands supported by ZTE AP to start CSI report. These commands should be sent to ZTE AP in a required order so that ZTE AP can work correctly. To start the CSI report, the required order is

- 1) CSI Band Configuration Command (0x5)
- 2) CSI Configuration Command (0x3)
- 3) CSI Report Enable Command (0x1)
- 4) CSI STA Filter Command (0x2)
- 5) CSI Report Configuration Command (0x4)

At least 500ms interval is required between each command. If there is STA sending PPDU to ZTE AP, after step 3, we will observe fragmented UDP packets from ZTE AP. A few rules should be obeyed,

- Steps 1–3 must be performed consecutively and not executed separately, as doing so may lead to unexpected errors.
- Only one band collection is supported at one time. If we already collect CSI from one band, before switching to another band, system reboot is required.

#### D. CSI Data Format

Once the ZTE AP is setup properly as per Section III-C, the raw CSI will be reported by UDP packets. Depends on the maximum transmission unit (MTU), the UDP packets might be fragmented. The users can listen on port 8023 with their local ip address. The CSI is saved in the data field of the UDP packets with little-end type. The format of CSI is defined in TABLE IX.

TABLE IX  
THE FORMAT OF THE CSI DATA

field	count	type	description
MAGIC_NUM	1	uint32_t	The high 2 bytes is 0xCAFE.
vendor	1	uint8_t	For ZTE AX3000, this value is 2
chip_id	1	uint32_t	For ZTE AX3000, this value is 1
timestamp	1	uint64_t	Timestamp when the CSI is collected in us.
resv	1	uint32_t	reserved for later use
bw	1	uint32_t	The bandwidth of the PPDU. 0-4 represent 20MHz to 160MHz
phy_mode	1	uint32_t	
resv_1	1	uint8_t	reserved for later use
resv_2	1	uint16_t	reserved for later use
peer_addr	6	uint8_t	The mac address of the PPDU which the CSI is estimated based on
rssi	16	int32_t	The rssi of the PPDU
resv_3	16	int32_t	reserved for later use
agc_gain	16	int8_t	The RF AGC gain when the PPDU is received.
mcs	1	int16_t	The MCS of the received PPDU
gi_type	1	int8_t	The Guard Interval of the received PPDU
coding	1	int8_t	The coding type of the received PPDU
stbc	1	int8_t	Whether the received PPDU is coded by stbc
resv_4	1	int8_t	reserved for later use
dcm	1	int8_t	Whether the received PPDU uses dual-carrier modulation
resv_5	1	int8_t	reserved for later use
resv_6	1	uint64_t	reserved for later use
csi_cnt	1	int16_t	The number of CSI in this packets
csi_i	512	int32_t	The I part of CSI
csi_q	512	int32_t	The Q part of CSI

#### E. Some Examples on Commands and CSI data

In Figure 2, we provide an example of a UDP packet which carries a CSI Band Command captured by Wireshark. The CSI Band Command requires ZTE AP report CSI from 5G band.

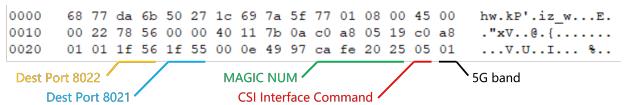


Fig. 2. An example of an UDP packet carrying CSI Band Command

In figure 3, we provide an example of UDP packets which carrier a CSI data. Note that, the CSI data is fragmented into 3 packets and it is reassembled by Wireshark. As show in Figure 3, the peer address is 0a:19:c6:51:00:12. The MCS of PPDU from which the CSI data is estimated is 9.

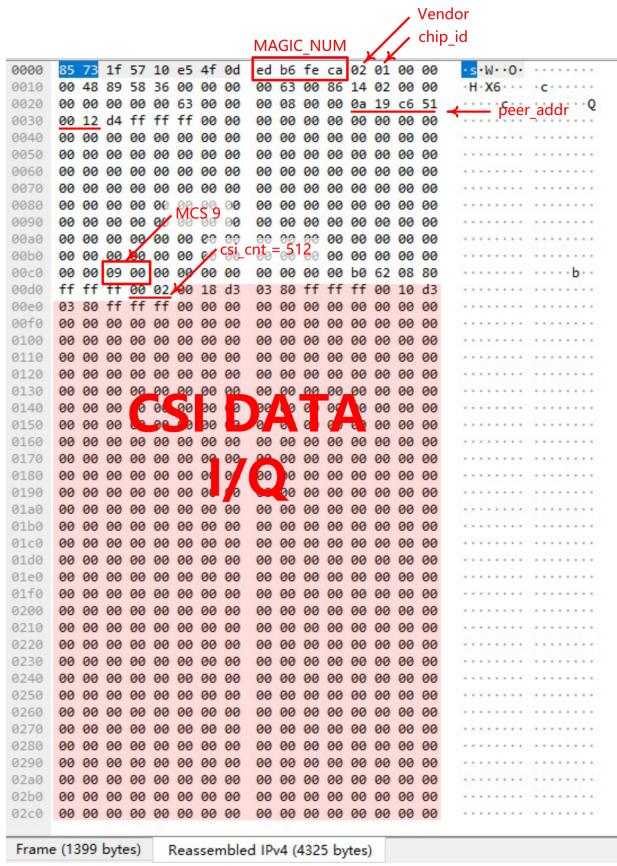


Fig. 3. An example of an UDP packet carrying CSI data format.

#### F. PC Software

We provide then PC software "ZTECSITool" which integrates control, data collection, and statistics. ZTECSITool serves as a best-practice implementation for both the commands and CSI parsing methods presented in this paper. Users can adapt and extend its framework to develop their own customized applications. Figure 4 shows the main page of the ZTECSITool. The main interface is divided into three sections: CSI Configuration Control, Real-time CSI Visualization, and Statistics Display.

- CSI Configuration Control: All UDP commands discussed in Section III-B have been deployed. Just click "Configure CSI Report" button.
- Real-time CSI Visualization: The magnitude, phase, and original I/Q data will be drawn.
- Statistics: The number of CSI is counted according to bandwidth and MCS. The average RSSI is also computed.

#### G. ZTE AP Firmware

Before using ZTECSITool, the firmware of ZTE AX3000 AP should be updated to the CSI-updated experimental version, which supports all functions described in this paper. The firmware is deployed on the cloud. User can request this experimental version on the management web page of the ZTE

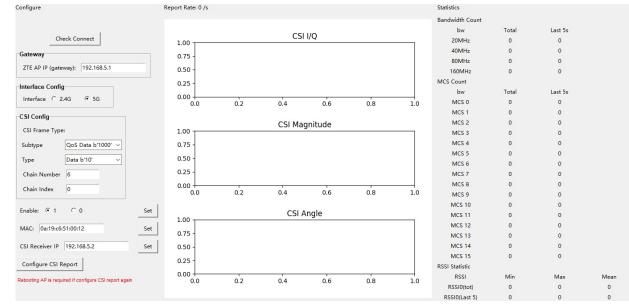


Fig. 4. The home page of ZTECSITool.

AP. To update ZTECSITool firmware, the following step needs to be done:

- 1) Login to the management web page of ZTE AP (by default 192.168.5.1). On the bottom of the main page, record the sequence number.
- 2) Send an email to the corresponding author and attach the sequence number.
- 3) Users will receive confirmation from the author and your device will be ready for the experimental test.
- 4) Connect your ZTE AP to Internet through WAN. Login to the management web page. On the system - upgrade, click "request update" bottom. Your ZTE AP will download the experimental firmware and reboot.
- 5) Use ZTECSITool PC software to collection CSI Information.

Figure 5 shows the example of web pages.



Fig. 5. The home page of web pages.

#### IV. CONCLUSION

In this paper, we present ZTECSITool, a toolkit allowing commercial ZTE AX3000 Series AP uploading CSI informa-

tion. ZTECSITool supports CSI parameters that, to the best of our knowledge, represent the highest known specifications to date, with support for up to 160MHz bandwidth, 512 subcarriers, and 6 chains. We believe that this tool can facilitate the advancement of research in WLAN sensing, especially in areas such as deployment and through-wall detection, and promote the development of the industry

## REFERENCES

- [1] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, “Tool release: Gathering 802.11n traces with channel state information,” *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 1, pp. 53, 2011.
- [2] M. Schulz, D. Wegemer and M. Hollick, “Nexmon: The C-based Firmware Patching Framework,” 2017. [Online]. Available: <https://nexmon.org>
- [3] Y. Xie, Z. Li and M. Li, “Precise Power Delay Profiling with Commodity WiFi,” in *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking (MobiCom)*, ACM, 2015, pp. 53–64.
- [4] S.M. Hernandez and E. Bulut, “Lightweight and Standalone IoT Based WiFi Sensing for Active Repositioning and Mobility,” in *Proceedings of the 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, IEEE, 2020, pp. 277–286.
- [5] F. Wang, W. Gong and J. Liu, “On spatial diversity in WiFi-based human activity recognition: A deep learning-based approach,” *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 133–136, 2019.
- [6] Y. Qin, S. Sigg, S. Pan and Z. Li, “Direction-agnostic gesture recognition system using commercial WiFi devices,” *Computer Communications*, vol. 216, pp. 34–44, 2024.
- [7] Y. Qin, S. Pan and Z. Li, “Cross-domain extendable gesture recognition system using WiFi signals,” *Electronics Letters*, vol. 59, no. 16, pp. 133–136, 2023.
- [8] N. Bahadori, J. Ashdown and F. Restuccia, “ReWiS: Reliable Wi-Fi sensing through few-shot multi-antenna multireceiver CSI learning,” in *2022 IEEE 23rd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, IEEE, 2022, pp. 50–59.
- [9] D. Wu, Y. Zeng, R. Gao, S. Li, Y. Li, R. C. Shah, H. Lu, D. Zhang “WiTraj: Robust indoor motion tracking with WiFi signals,” *IEEE Transactions on Mobile Computing*, vol. 22, no. 5, pp. 3062–3078, 2021.
- [10] Y. Zheng, Y. Zhang, K. Qian, G. Zhang, Y. Liu, C. Wu and Z. Yang “Zero-effort cross-domain gesture recognition with Wi-Fi,” in *2022 Proceedings of the 17th annual international conference on mobile systems, applications, and services (MobiSys)*, ACM, 2019, pp. 313–325.
- [11] R. Xiao, J. Liu, K. Qian, J. Han and K. Ren “Onefi: One-shot recognition for unseen gesture via cots wifi,” in *2021 Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems (SenSys)*, ACM, 2021, pp. 206–219.
- [12] X. Wang, K. Niu, J. Xiong, B. Qian, Z. Yao, T. Lou and D. Zhang “Placement matters: Understanding the effects of device placement for WiFi sensing,” in *2022 Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, ACM, 2022, pp. 1–25.
- [13] J. Yang, H. Huang, Y. Zhou, X. Chen, Y. Xu, S. Yuan, H. Zou, C.X. Lu and L. Xie “Mm-fi: Multi-modal non-intrusive 4d human dataset for versatile wireless sensing.” *Advances in Neural Information Processing Systems*, vol. 36, pp. 18756–18768, 2023.
- [14] F. Wang, Y. Lv, M. Zhu, D. Han and J. Han “XRF55: A Radio Frequency Dataset for Human Indoor Action Analysis,” *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 8, no. 1, pp. 1–34, 2024.
- [15] Y. Zhang, Y. Yin, Y. Wang, J. Ai and D. Wu “CSI-based location-independent Human Activity Recognition with parallel convolutional networks,” *Computer Communications*, vol. 197, pp. 87–95, 2023.