Wi-Fi Ranging under Interference

Anatolij Zubow*, Christos Laskos*, Sascha Rösler*, Gerhard Wunder†, and Falko Dressler*
*School of Electrical Engineering and Computer Science, TU Berlin, Germany
†Cybersecurity and AI, FU Berlin, Germany
{zubow,laskos,roesler,dressler}@tkn.tu-berlin.de, g.wunder@fu-berlin.de

***Abstract*—The next generation of WiFi aims to deliver highly accurate location estimation through time-of-flight measurements. While initial results show promising performance, there is a lack of studies conducted under realistic, congested network conditions with significant cross-technology and co-channel interference. In this paper, we demonstrate that time of arrival (ToA)-based ranging, utilizing the MUSIC super-resolution algorithm, is severely impacted by interference. This is due to the fact that the channel state information (CSI) obtained in the presence of interference includes not only the characteristics of the channel but also the interference itself. This corrupted CSI leads to persistent ToA errors. Simulation results indicate that these errors are particularly pronounced in indoor scenarios with multipath propagation resulting in a ranging error of up-to 3 m which can only be mitigated by the usage of wider channels, e.g., 160 MHz, for ranging.**

***Index Terms*—Sensing, Interference, Ranging, Time of Arrival, 802.11, MUSIC**

I. Introduction

WiFi offers capabilities beyond traditional communication, making it an attractive choice for indoor positioning systems, particularly with the widespread support of the IEEE 802.11 standard in consumer devices like smartphones and tablets [1]. 802.11az aims to provide highly accurate location estimation, and initial results demonstrate promising performance [2]. However, studies under realistic conditions are still lacking. One major challenge is that WiFi operates in unlicensed spectrum bands, which are often crowded, leading to co-channel interference (CCI) from other WiFi networks. Additionally, WiFi must coexist with other wireless technologies such as Zigbee, Bluetooth, and LoRa in the 2.4 GHz band [3], and LTE-U/LAA in the 5 GHz band [4], making cross-technology interference (CTI) a potential issue that cannot be overlooked [5].

In this paper, we study the performance of Time of Arrival (ToA) estimation used in 802.11az under CTI. We therefore assume usage of the MUSIC super-resolution algorithm and examine the impact of CTI from IEEE 802.15.4 and CCI from other WiFi networks on it. The different scenarios are evaluated through link-level simulations conducted in MATLAB. Results reveal that even low levels of interference lead to inaccurate ToA and, hence, inaccurate distance estimation. The impact is particularly large in indoor environments with multipath propagation. However, the accuracy can be dramatically improved by using wider channels for ranging, i.e., 160 MHz instead of 20 MHz.

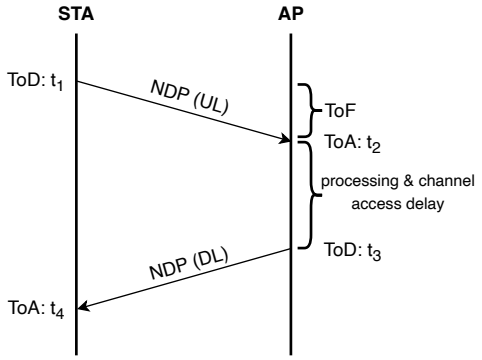


Figure 1. WiFi based distance ranging between STA and AP.

II. Related Work

Frequency-domain super-resolution ToA estimation using MUSIC was first proposed by Li et al. [6]. Zhen et al. [7] analyzed the impact of interference on channel state information (CSI) measurements and proposed algorithms based on cyclostationary analysis enabling the identification of interfered CSI. Huang et al. [8] showed, that CSI based human activity recognition systems based on CSI are highly vulnerable to interference from jamming attacks. Additionally, the performance of WiFi is highly affected by CTI causing persistent decoding errors throughout the data payload and hence reduced throughput, as Son et al. [9] analyzed. The effect of extensive device-related noise on Time of Flight (ToF) measurements is studied by Rea et al. [10] in ranging experiments with COTS WiFi hardware. The noise makes it difficult to differentiate between direct and non-direct path signal components. Beko et al. [11] show that a two way handshake can help to detect malicious ToA measurements in a scenario of spoofing. Xiong et al. [12] proposed ToneTrack to target the problem of limited channel bandwidth in 802.11. The equivalent of a wideband channel was constructed by transmitting WiFi packets sequentially on multiple WiFi channels and stitching the received CSI together before performing the super-resolution MUSIC algorithm. Also ranging on non-WiFi technologies suffer from CTI, as Hechenberger et al. [13] and Sharma et al. [14] show for ultra wideband (UWB) ranging. For mitigation they introduce an interference filter based on linearly constrained minimum variance interference [13] and a first threshold crossing algorithm [14]. Vice versa, Hou et al. [15] use MUSIC to detect interference and optimize an intelligent reflecting surface (IRS) setup. Up to our knowledge there is no work analyzing the effect of CTI and CCI on MUSIC.

979-8-3315-2096-0/25/$31.00 ©2025 IEEE

III. Primer on WiFi Positioning

In this section we want to explain how MUSIC bases ToA estimation is used in modern WiFi ranging. Traditionally, WiFi networks have been used for positioning using techniques like Received Signal Strength Indicator (RSSI). However, these methods can be limited in accuracy due to environmental factors like shadowing and multipath. With 802.11mc Fine Time Measurement (FTM) was introduced into the 802.11 standard. FTM consists of multiple round trip time (RTT) handshakes. We will focus on one of these handshakes in the following study. A handshake allows two WiFi devices (access point (AP) and station (STA)) to measure the ToF, i.e., the time it takes for the WiFi signal to travel between them. The distance measurement is performed by capturing the timestamps of the down link (DL) and up link (UL) null data packet (NDP) packets (Figure 1). The STA records the time-of-departure (ToD) t_1 at which it transmits the UL NDP. The AP then estimates the ToA t_2 at which it receives the UL NDP and records the time t_3 at which it transmits the DL NDP packet. Finally, the STA then captures time t_4 representing the point in time at which it receives the DL NDP. The four different timestamps $t_1 - t_4$ are used afterwards to estimate the round trip time RTT:

$$\mathrm{RTT} = (t4 - t1) - (t3 - t2) \tag{1}$$

from which the distance is obtained as: $d = (\mathrm{RTT}/2) \cdot c$, where c is the speed of light.

The ranging accuracy in FTM highly depends on the precise estimation of the four timestamps, as even an error of 1 ns results in a distance error of 30 cm. For ToA, Li et al. [6] proposed the estimation of the timestamps t_2 and t_4 using MUSIC super-resolution algorithm as follows:

1) Estimate Channel Frequency Response (CFR), a complex vector depicting both gain and phase information of each OFDM subcarrier between each single transmit-receive antenna pair,
2) Interpolate across missing subcarriers in CFR,
3) Estimate CFR correlation matrix,
4) Perform spatial smoothing (decorrelate multipaths),
5) Perform MUSIC algorithm (Eigendecomposition of correlation matrix & estimation of time-domain delay profile) using knowledge about number of multipaths,
6) Estimate ToA as the first peak in time-domain delay profile.

In this paper, we want to study how this approach performs under the impact of radio frequency interference, i.e., CCI and CTI. Note, that by measuring distances towards multiple APs the STA can determine its position using trilateration.

IV. System Model

Figure 2 shows our system model. Without loss of generality, we study the ToA estimation of one packet in a FTM handshake. Therefore, we simulate the transmission of one NDP UL frame, as a STA performs ranging towards the AP following the 802.11az standard. Both STA and AP are SISO systems with a configurable channel width $B = 20, 40, 80, 160$ MHz. In addition there is a co-located interferer operating in the same radio spectrum. The interferer is either an 802.15.4 (ZigBee) node or a legacy 802.11a node. The channel, i.e., center frequency, used by the interferer is assumed to be random within the spectrum used by the ranging setup. Any activity contributes to interference in form of either CTI or CCI. As the channel model we consider two different propagation scenarios as described by the IEEE 802.11ax group [16]:

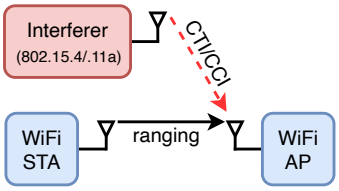


Figure 2. System model for WiFi ranging under interference.

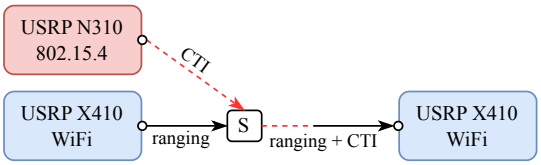


Figure 3. SDR setup for ranging under interference.

- **Model-A**: propagation with line-of-sight (LOS) only (single tap, frequency flat channel),
- **Model-B**: indoor in residential building with LOS and non-LOS (NLOS) (selective channel, 9 taps, 2 clusters, RMS delay spread of 15 ns).

In absence of CCI and CTI the SNR on the WiFi link is $\gamma = 35$ dB representing very good channel quality. During the evaluation the signal-to-interference ratio (SIR) from CCI/CTI is controlled by changing the distance of the interferer node towards the WiFi AP. The ToA is estimated at the WiFi AP from a single WiFi packet according to the method described in the previous section.

V. CFR under Interference

The CFR estimated at the WiFi receiver (AP) being impacted by interference (CCI or CTI) is given as [7]:

$$\hat{H} = \frac{Y + Y_{\mathrm{int}}}{X} \tag{2}$$

where X and Y denote the transmitted and received WiFi signal respectively, whereas Y_{int} represents the received interference signal. Denote the CFR corresponding to the WiFi signal as H and of the interference as H_{int}, the above equation can be converted into [7]:

$$\hat{H} = H + \frac{H_{\mathrm{int}} X_{\mathrm{int}}}{X} \tag{3}$$

where X_{int} represents the transmitted signal of the interferer. Hence the subcarriers in the CFR which are overlapping with the channel of the interference will be impacted provided that the interference power is sufficient high.

For validation we performed measurements using a Software-defined Radio (SDR) in an experiment shown in Figure 3. We

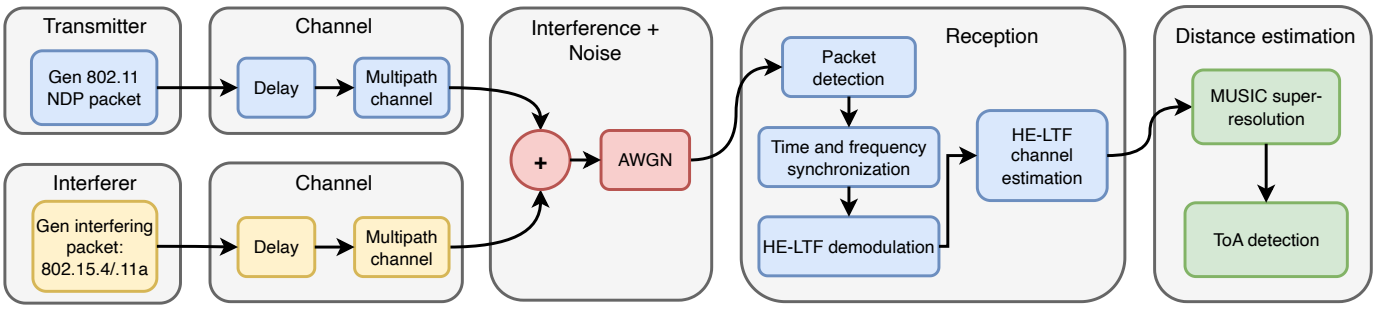


Figure 4. Simulation methodology.

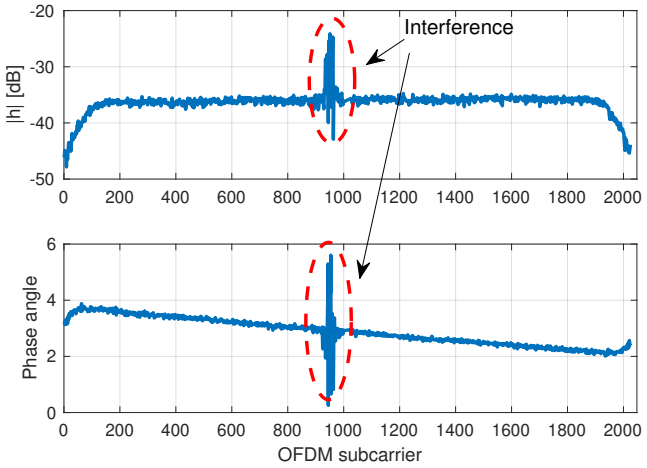


Figure 5. Experimental result for CFR (magnitude and phase angle) obtained under CTI ($B = 160$ MHz).

connected three SDRs via cables and a splitter (S), where the two X410 perform ranging and the N310 transmits 802.15.4 frames causing CTI. The result is presented in Figure 5, where in terms of the amplitude the impact of narrow-band CTI (802.15.4 ZigBee signal) is visible with a narrow and high peak at the affected subcarriers. Moreover, the corresponding phase is distorted.

VI. Performance Evaluation

In the following, we presented selected results from our experiments, which underline the impact of interference on WiFi ranging.

A. Methodology

In order to assess the impact of interference on 802.11-based ranging we performed link-level simulations in MATLAB using the WiFi toolbox. Therefore the transmission and reception of ranging packets was simulated from which the distance was estimated. Specifically, the steps are (Figure 4):

1) Waveform generation: a. 802.11 ranging null data packet (NDP, BPSK 1/2) and b. interfering data packet (IDP, 802.15.4 or 802.11a (20 MHz) packet),
2) Delaying the NDP and IDP packets according to the simulated distance, i.e., distance between the two WiFi nodes involved in ranging and distance between interferer and the WiFi RX node (AP),
3) Passing the two waveforms through an TGax channel (Model-A/B) [16]. Note, that the IDP waveform is resampled in order to meet the sampling rate of WiFi,
4) Adding up the two waveforms and adding additive white Gaussian noise (AWGN) to get the received waveform,
5) Performing synchronization and frequency correction on the received waveform,
6) Demodulating the HE-LTF from the WiFi preamble and estimating the CFR from the HE-LTF,
7) Estimating the ToA by using the MUSIC super-resolution algorithm.

For the evaluation we selected the distance between the WiFi nodes performing ranging, i.e., STA and AP, to be $d = 6$ m. Moreover, the distance from the interferer node towards the WiFi receiver (AP) node was varied. For each placement a single NDP ranging packet was transmitted from which the ToA was derived. Note, that in case of unsuccessful transmission no ToA could be determined. Finally, for the TGax channel we analyzed the two propagation scenarios (Model-A and B).

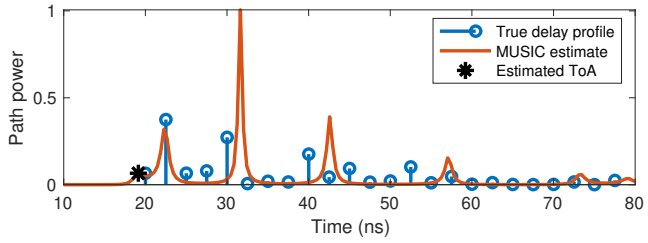
As metric we computed the ToA error ϵ between the estimated and the ground truth ToA:

$$\epsilon = |\theta_{\text{est}} - \theta_{\text{real}}| \tag{4}$$

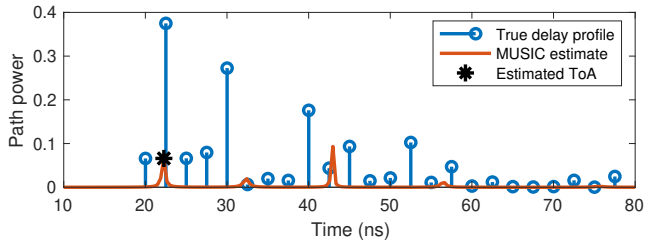
B. Results

1) Illustrative Example on Impact from CTI: As an illustrative example we consider a WiFi transmission on an 160 MHz channel in the indoor residential environment, i.e., Model-B. Figure 6a shows the pseudo power delay profile (PDP) estimated by MUSIC in case of a clear channel, i.e., no CTI. The estimated ToA was 19.14 ns which comes very close to the ground truth of 20.01 ns. Under CTI from 802.15.4 (ZigBee) the estimated PDP was different (Figure 6b). Here, the estimated ToA is 22.27 ns resulting in an error of 2.25 ns compared to only 0.87 ns in case of a clear channel without CTI. This is because the CSI used by MUSIC was estimated under interference and differs from the one obtained on a clear channel (Figure 7).

2) Impact of CTI/CCI on PER: As a preliminary investigation, we like to understand up to which level of SIR NDP packets are still decodable by the AP, such that the interfered CSI is used for ranging. Hence, the WiFi decoder works as a filter, as corrupted packets are sorted out and not used for ranging. In this study, we evaluate the impact of both CTI and



(a) clear channel



(b) with CTI

Figure 6. Power delay profile (Model-B, $B = 160\,\text{MHz}$).

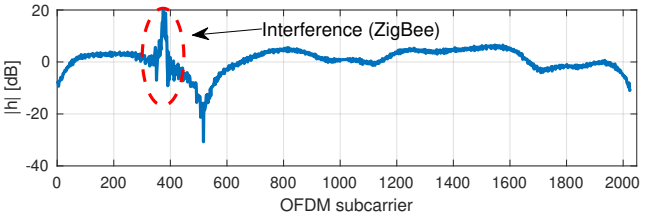


Figure 7. CFR obtained under CTI (Model-B, $B = 160\,\text{MHz}$).

CCI on the packet error rate (PER) and compute the SIR for each node placement.

Figure 8 shows the results. We can observe that even at very high level of interference, i.e., low SIR, WiFi NDP packets can still be received although at very high PER. However, from such interfered packets it is very likely that an incorrect CSI and, hence, incorrect ToA is estimated afterwards.

3) Impact of Propagation Scenario: In the following we analyzed the impact of CTI for the two different propagation scenarios (Model-A and B) on the estimated ToA. As for some node placements, the level of interference was too high for successful NDP packet reception and it was not possible to estimate a ToA. Hence, the following results contain only the estimations of ToA of successful NDP transmissions.

Figure 9 shows the ToA error ϵ in case of Model-A propagation, i.e., channel with LOS only. We can observe

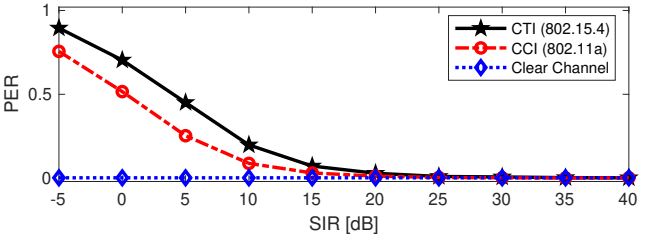


Figure 8. SIR vs. PER (Model-A scenario, $B = 20\,\text{MHz}$).

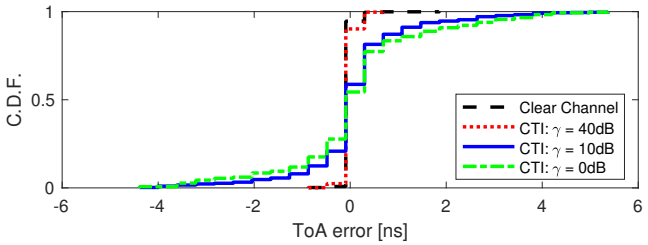


Figure 9. CDF of ToA error under CTI (Model-A scenario, $B = 20\,\text{MHz}$).

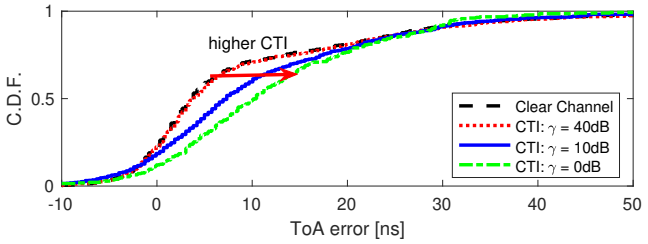


Figure 10. CDF of ToA error under CTI (Model-B scenario, $B = 20\,\text{MHz}$).

that at low SIR the dispersion of ϵ increases. This is visible from the interquartile range (IQR) which is: $\text{IQR}_{\text{clear}} = 0.0\,\text{ns}$, $\text{IQR}_{\gamma=40\,\text{dB}} = 0.14\,\text{ns}$, $\text{IQR}_{\gamma=10\,\text{dB}} = 1.16\,\text{ns}$, $\text{IQR}_{\gamma=0\,\text{dB}} = 1.48\,\text{ns}$. However, a bias cannot be observed as the expectation value for ϵ is zero regardless of the SIR, $\mathbb{E}(\epsilon) = 0$.

In a multipath propagation scenario (Model-B) the impact of CTI is much larger. As can be seen from Figure 10, CTI leads not only to higher dispersion of ϵ but also to a bias towards overestimation of the true distance. The distribution of ϵ is no longer Gaussian. The median value for the clear channel is $3.42\,\text{ns}$ and it increases to $10.45\,\text{ns}$ for SIR $\gamma = 0\,\text{dB}$. Note, that this corresponds to a distance error of $\approx 3.13\,\text{m}$ which cannot be ignored as the true distance was only 6 m.

4) Impact of WiFi Channel Width: Impact of both CTI/CCI can be significantly decreased by using a larger channel bandwidth for the WiFi ranging which is possible as 802.11ax offers flexible channel width from 20 to 160 MHz. This is because a ToA estimation from a wideband transmission is less affected by narrow-band interference. Note, that when using a 160 MHz WiFi channel the number of OFDM subcarriers affected by the interfering 802.15.4 waveform having a bandwidth of $5\,\text{MHz}$ is only $\approx 3\,\%$ vs. $\approx 25\,\%$ when using 20 MHz WiFi.

Figure 11 shows the impact of CTI from 802.15.4 in the multipath scenario (Model-B). The median value for ϵ is $11.63\,\text{ns}$ and $1.08\,\text{ns}$ for 20 MHz and 160 MHz respectively. Also the dispersion of ϵ is dramatically reduced with increased bandwidth, i.e., $\text{IQR}_{\text{CB20}} = 12.99\,\text{ns}$ vs. $\text{IQR}_{\text{CB160}} = 1.56\,\text{ns}$. Hence, the decrease in ϵ is approximately proportional to the used channel bandwidth.

Figure 12 shows the same study, however, with CCI from legacy WiFi (802.11a). Due to increased channel width the impact is higher as compared to the CTI study. However, the overall picture is the same and clearly showing the advantage of using wider channel for ranging.

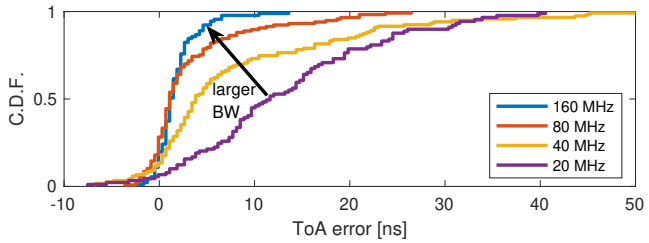


Figure 11. Impact of WiFi bandwidth under CTI (Model-B scenario).

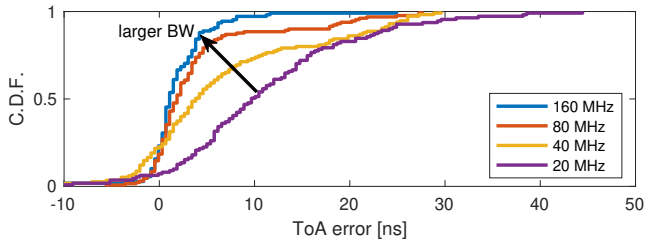


Figure 12. Impact of WiFi bandwidth under CCI (Model-B scenario).

VII. Discussion

Our results lead to the following conclusions. A scheme for detection of highly-interfered channels could improve localization as the WiFi network could switch to a different channel with lower load and interference. However, such an approach has limits as the ISM/U-NII bands are becoming increasingly crowded with diverse technologies, and hence it may not be possible to find an interference-free channel. Another approach would be the identification and exclusion of interfered CSI during ranging. This could improve ranging accuracy and positioning at the cost of higher latency and usage of radio resources, i.e., more ranging attempts need to be performed. Designing good filters is a challenging task, as there is a region of interference power where WiFi packets are received without corruption but the obtained CSI is still highly distorted by interference. Hence, there is a need to either find good filtering algorithms for excluding contaminated CSI as proposed in [7] or to develop error correction techniques for contaminated CSI to derive the correct CSI. The latter opens a new field of research.

VIII. Conclusion

In this work, we have shown the significant impact of interference (CCI and CTI) on the ranging accuracy of the MUSIC super-resolution algorithm as it is used in WiFi. Especially in scenarios with multipath propagation we observe large errors in the ToA estimation. The reason for this is the usage of MUSIC on a CSI estimated under interference. We clearly see how using a wider bandwidth improves the estimation of ToA under CCI and CTI conditions. As future work we plan to perform experiments with real 802.11az hardware (COTS, SDR) to study the impact under real channel and interference conditions. Moreover, we want to introduce an interference model to FTM-ns3 [17] which is a software module implementing the 802.11 ranging protocol in the ns3 network simulator.

Acknowledgements

This work was supported by the Federal Ministry of Education and Research (BMBF, Germany) within the 6G Research and Innovation Cluster 6G-RIC under Grant 16KISK020K, German Research Foundation (DFG) within the project ML4WiFi under grant DR 639/28-1, and Federal Ministry for Economics and Climate Action (BMWK) under grant 01MT22001G.

References

[1] F. Liu, J. Liu, Y. Yin, W. Wang, D. Hu, P. Chen, and Q. Niu, "Survey on WiFi-based indoor positioning techniques," *IET Communications*, vol. 14, no. 9, pp. 1372–1383, Jun. 2020.

[2] IEEE, "802.11az-2022 - Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 4: Enhancements for Positioning," IEEE, Std 802.11az-2022, Mar. 2023.

[3] A. Hithnawi, H. Shafagh, and S. Duquennoy, "Understanding the impact of cross technology interference on IEEE 802.15.4," in *20th ACM International Conference on Mobile Computing and Networking (MobiCom 2014), 9th ACM International Workshop on Wireless Network Testbeds, Experimental evaluation and Characterization (WiNTECH 2014)*, Maui, HI: ACM, Sep. 2014.

[4] V. Sathya, M. I. Rochman, and M. Ghosh, "Hidden-nodes in coexisting LAA & Wi-Fi: a measurement study of real deployments," in *IEEE International Conference on Communications (ICC 2021), Workshop on Spectrum Sharing Technology for Next Generation Communications*, Virtual Conference: IEEE, Jun. 2021.

[5] S. Bayhan, G. Gür, and A. Zubow, "The Future is Unlicensed: Coexistence in the Unlicensed Spectrum for 5G," arXiv, cs.NI 1801.04964, Jan. 2018.

[6] X. Li and K. Pahlavan, "Super-Resolution TOA Estimation With Diversity for Indoor Geolocation," *IEEE Transactions on Wireless Communications*, vol. 3, no. 1, pp. 224–234, Jan. 2004.

[7] Y. Zheng, C. Wu, K. Qian, Z. Yang, and Y. Liu, "Detecting radio frequency interference for CSI measurements on COTS WiFi devices," in *IEEE International Conference on Communications (ICC 2017)*, Paris, France: IEEE, May 2017, pp. 1–6.

[8] P. Huang, X. Zhang, S. Yu, and L. Guo, "IS-WARS: Intelligent and Stealthy Adversarial Attack to Wi-Fi-Based Human Activity Recognition Systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 6, pp. 3899–3912, Nov. 2022.

[9] Y. Son and S. Bahk, "Revisiting Wi-Fi Performance under the Impact of Corrupted Channel State Information," in *23rd ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM 2020)*, Alicante, Spain: ACM, Nov. 2020, pp. 83–92.

[10] M. Rea, A. Fakhreddine, D. Giustiniano, and V. Lenders, "Filtering Noisy 802.11 Time-of-Flight Ranging Measurements From Commoditized WiFi Radios," *IEEE/ACM Transactions on Networking*, vol. 25, no. 4, pp. 2514–2527, Aug. 2017.

[11] M. Beko and S. Tomic, "Toward Secure Localization in Randomly Deployed Wireless Networks," *IEEE Internet of Things Journal*, vol. 8, no. 24, pp. 17 436–17 448, Dec. 2021.

[12] J. Xiong, K. Sundaresan, and K. Jamieson, "Tonetrack: Leveraging frequency-agile radios for time-based indoor wireless localization," in *21st ACM International Conference on Mobile Computing and Networking (MobiCom 2015)*, Paris, France, Sep. 2015, pp. 537–549.

[13] S. Hechenberger, S. Tertinek, and H. Arthaber, "Low-Complexity Wideband Interference Mitigation for UWB ToA Estimation," *Sensors*, vol. 23, no. 13, pp. 1–21, Jun. 2023.

[14] S. Sharma, A. Gupta, and V. Bhatia, "Joint Estimation of ToA and Data Symbols in UWB Communication in Presence of Impulsive Interference," in *IEEE Global Communications Conference (GLOBECOM 2017)*, Singapore, Singapore: IEEE, Dec. 2017, pp. 1–7.

[15] Y. Hou, K. Yano, N. Suga, J. Webber, S. Denno, and T. Sakano, "MUSIC Spectrum Based Interference Detection, Localization, and Interference Arrival Prediction for mmWave IRS-MIMO System," *IEEE Access*, vol. 12, pp. 142 592–142 605, 2024.

[16] J. Liu and R. Porat, "TGax Channel Model," IEEE, IEEE IEEE 802.11-14/0882r4, Sep. 2014, pp. 1–10.

[17] A. Zubow, C. Laskos, and F. Dressler, "Toward the Simulation of WiFi Fine Time Measurements in NS3 Network Simulator," *Elsevier Computer Communications*, vol. 210, pp. 35–44, Oct. 2023.