Passive Side-Channel Interference Estimation for WiFi Networks

Aysun Gurur Onalan
Lifemote Networks
Istanbul, Turkey
aysun.onalan@lifemote.com

Mehmet Hakan Kurtoglu
Technical University of Berlin
Berlin, Germany
kurtoglu@campus.tu-berlin.de

Eren Soyak
Lifemote Networks
Istanbul, Turkey
eren.soyak@lifemote.com

***Abstract*—WiFi devices operating in the 2.4 GHz ISM band significantly suffer from the interference caused by overlapping side-channels. This paper proposes a metric to quantify the Quality of Experience (QoE) impact of side-channel interference based on passive, granular wireless driver parameter samples from consumer grade WiFi Access Points (APs). The variables of the metric are *BadPLCP, NoPkt,* and *Glitch* which are driver parameters determined in home environment experiments to be highly correlated to interference. Filed analysis of the proposed metric in 802.11ax and 802.11n deployments indicates that side-channel interference prevents medium access and causes frame losses, which are the main drivers of lowered QoE. Further, this paper proposes a Deep Neural Network (DNN) based algorithm to detect the interfering side-channel neighbour, where the wireless driver parameters are the input features. For 6 classes representing interference from different side-channels, we achieve 78% accuracy, 83% precision, 78% recall, and 79% f1-score.**

***Index Terms*—WiFi, WLAN, interference**

I. Introduction

Today, WiFi is one of the most prevalent technologies for broadband Internet access in the home. WiFi performance fluctuates quite often due to the varying and complex nature of the wireless medium. For instance, medium access conditions are affected by the location of WiFi APs and clients, WiFi contention, and non-WiFi interference sources [1], [2]. Therefore, quantifying WiFi performance and detecting WiFi problems are challenging, especially for home networks, where WiFi APs are randomly located.

Recently, the literature has focused on WiFi problem detection and performance estimation using continuously collected wireless driver parameters at a fine scale from commodity APs. In [3], the authors characterize the traffic activity and analyze the occurrence of the coverage problem. WiFi and non-WiFi (e.g., Microwave, Zigbee, etc.) interference sources are classified with various machine learning algorithms in [4]; whereas five different WiFi problems such as WiFi contention, non-WiFi interference, hidden terminal, capture effect, and coverage are identified with Neural Networks (NNs) in [5]. WiFi link capacity [6] and QoE [7] are also estimated based on passively collected wireless driver parameters.

None of the aforementioned works consider the WiFi interference from overlapping side-channels in 2.4 GHz WiFi, although it is a very significant problem. In the 2.4 GHz ISM band, there are 13 WiFi channels with 22 MHz bandwidth, among which only 3 channels, i.e., channels 1, 6, and 11, are non-overlapping in frequency [8]. Data traffic through neighbouring APs at overlapping side-channels cause interference on each other. The new standard IEEE 802.11ax, branded as WiFi6, with its faster data rates up to 9.6 Gbps, new medium access techniques such as OFDMA and its deployments in dense environments like stadiums, is even more prone to such interference [9]. As WiFi6 is expected to replace older standards such as 802.11n and 802.11ac in few years [10], the side-channel interference problem gain more importance.

Currently, based on an analysis of one day worth of data of 7084 Access Points (APs) of a Norwegian Internet Service Provider (ISP), among which 21% have WiFi6 clients.[1] %33 of these WiFi6 APs have neighbours at the overlapping side-channels and they use the 2.4 GHz band for data traffic for 35% of the time rather than 5 GHz. As the 2.4 GHz band and overlapping side-channels are preferred considerably in WiFi6, the analysis of the side channel interference is significant.

Side channel neighbors are only studied based on active WiFi scan results, which provide neighbour channel and Received Signal Strength (RSSI) information for channel selection mechanisms [11]. However, the scans are active measures disturbing user experience when executed; and the provided information by scans is not enough to quantify the QoE impact of actively interfering neighbors.

This paper aims to quantify the performance degradation caused by side-channel interference and to detect the neighbouring APs causing the interference based on the wireless driver parameters passively collected from consumer grade APs. The major contributions of the paper are as follows:

- We conduct experiments in a home environment to observe the QoE impact of side-channel interference and determine the wireless driver parameters indicating the interference.
- We propose a metric to quantify the impact of side-channel interference on WiFi QoE based on the experiment results.
- We use the proposed metric for a field study in 802.11n and 802.11ax deployments of the Norwegian ISP to indicate that side-channel interference causes medium

[1]Anonymized data used in this study done so with permission from the service provider, a Lifemote customer under a Data Processor Agreement.

access and frame delivery problems, which are the two main reasons of WiFi QoE degradation [6].
- We propose a novel interfering side-channel neighbour detector based on Deep Neural Networks (DNNs) for which the features are extracted from the wireless driver parameters.

This paper is organized as follows: Section II presents the measurement setup, procedure, data, and results. Section III introduces the metric to quantify side-channel interference effect on QoE. Section IV presents the field study results and compare the side-channel interference impact on 802.11ax and 802.11n APs. Section V proposes a DNN based architecture to detect the interfering neighbour. Finally, Section VI concludes the paper.

II. Experiments

A. Experimental Setup

In this section, we describe the setup of our experiments to observe the side-channel interference effects on WiFi QoE and the wireless driver parameters indicating the interference. We conducted experiments in a home environment with a broadband xDSL downlink speed of 59Mbps. We used two APs featuring the Broadcom BCM43217 2x2 802.11n chipset, two Ubuntu laptops with 2x2 802.11n WiFi interfaces as clients (one HP and one Dell) and an Apple Mac-mini desktop PC as the automation controller of the measurements. The setup is depicted in Fig. 1. The APs were connected to the controller Mac-Mini via Ethernet, and the laptops were connected to different APs as WiFi clients. One AP-client pair was used only to utilize a specified channel and shall be named the *traffic pair*. The other AP-client pair was used to conduct the tests and shall be named the *test pair*.

B. Experimental Procedure

We collected wireless driver parameters and rates measured by the Ookla Speedtestand [12] and Iperf [13] under different side-channel interference conditions for several cases, where physical locations of test and traffic pairs are changed.

Five different cases were created based on the locations of the test and traffic pairs. We placed the test client at different distances to the test AP to create high, medium, and poor coverage conditions under side-channel interference. In the first case, which could be thought as the reference case, both pairs were positioned in the same room, where the clients were closer to their corresponding APs than the other AP. For cases 2 and 3, the APs and the traffic client were positioned at the same place, but the test client was located in different rooms corresponding to the medium and poor coverage points, respectively. Moreover, APs were also located at different distances between them to control the interference level. In cases 4 and 5, the test pair was placed in its location in Case 1; while the traffic pair was moved to the next room and a room farther away, respectively. The RSSI values between two APs and between the test pair from the test AP's perspective are given in Table I.

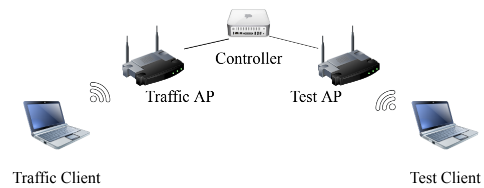


Fig. 1. Experimental setup

TABLE I
RSSI values for different cases

	Case 1	Case 2	Case 3	Case 4	Case 5
AP - AP	-40 dBm	-40 dBm	-40 dBm	-60 dBm	-70 dBm
Test pair	-30 dBm	-60 dBm	-70 dBm	-30 dBm	-30 dBm

TABLE II
Tests

Test	side-channel	Util.	Test	side-channel	Util.	Test	side-channel	Util.
1	0	15%	7	2	15%	13	4	15%
2	0	50%	8	2	50%	14	4	50%
3	0	75%	9	2	75%	15	4	75%
4	1	15%	10	3	15%	16	5	15%
5	1	50%	11	3	50%	17	5	50%
6	1	75%	12	3	75%	18	5	75%

A single test consists of 10 Speedtests, and a single pair TCP Iperf run of 60 seconds. Speedtests were conducted to measure download and upload limits by using Python's speedtest-cli tool, which tests Internet bandwidth via speedtest.net. Then, Iperf TCP traffic was generated from the controller to the test client to test the Wireless Local Area Network (WLAN) bandwidth. During each test, wireless driver parameters of the test AP were sampled at 1 second intervals. We collected wireless driver parameters with the "wl" application provided by Broadcom.

A total of 18 tests were conducted for each of the five cases, given in Table I, whose specifications are tabulated in Table II. In each case, both pairs started at the same channel, which was WiFi Channel 1. The test pair performed 3 tests; while the traffic pair filled the air incrementally going through 15%, 50% and 75% with Iperf UDP corresponding to the requirement of each test. Then, the test pair moved to the next channel, i.e., WiFi Channel 2, and performed 3 more tests under 3 different channel utilizations. This procedure was repeated by setting the test pair's channel to the next WiFi channel every 3 tests, until reaching Channel 6. Note that, the traffic pair always stayed at the WiFi Channel 1 and filled the air with UDP traffic creating side-channel interference for the the traffic pair. The side-channel causing interference is referred according to the channel difference between the pairs, e.g., if the test pair is on Channel 4 and the traffic pair on Channel 1, interference is said to be caused by the 3rd side-channel, and 0th side-channel if both pairs on Channel 1.

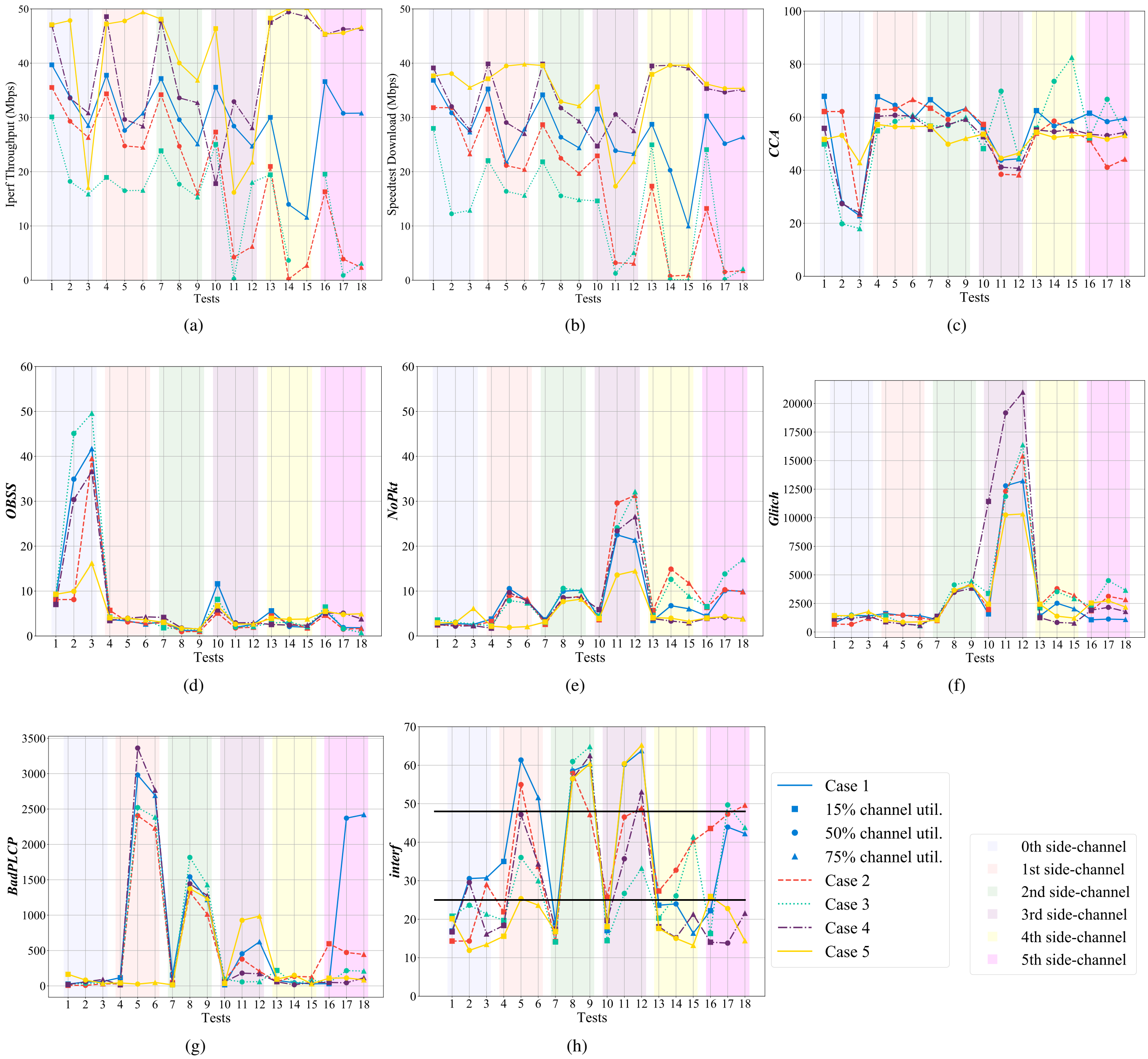


Fig. 2. Average (a) Iperf Throughput, (b) Speedtest download rate, (c) *CCA*, (d) *OBSS*, (e) *NoPkt*, (f) *Glitch* (g) *BadPLCP* and (h) *interf* values for each test.

C. Experimental Data

Experiment data consist of Speedtest rates and Iperf TCP logs from the test client, and wireless driver parameters of the test AP. Especially, the parameters related to the channel statistics of the AP are collected with the “wl chaim_stats” command. Note that due to the text length limitations, we only present the driver parameters highly related to the side channel interference, i.e., *OBSS* — percentage of time while receiving packets from an overlapping basic service set, *NoPkt* — percentage of time while receiving non-WiFi packets, *BadPLCP*— counter for packets whose PLCP header cannot be decoded, and *Glitch* — counter for noisy packets.

D. Experimental Results

Figs. 2a-2g present the measurement results as the mean values of Iperf throughput, Speedtest download rates and wireless driver parameters collected during each test. Each sub-figure includes the mean values of the corresponding parameter for 18 tests in all five cases given in Table I. In each sub-figure, different background colors indicate different side-channels that the test AP was operating on, leftmost pale blue indicates the 0th side-channel and rightmost pale purple indicates the 5th side-channel. Square, circle, and triangle markers represent the 15%, 50% and 75% channel utilization, respectively. Different lines indicate different test cases.

The Iperf and Speedtest download rates depicted in Figs. 2a and 2b are used as indicators of user Quality of Experience (QoE). In general, QoE is affected the most when the test client is far away from but the traffic AP is close to the test AP, i.e. Cases 2 and 3. The QoE degradation decreases as the distance between the APs increases, as expected. Increasing channel utilization results in lower rates, as expected. Even if the APs are distant, i.e., Cases 4 and 5, 3rd side-channel interference causes dramatic rate decreases so it has the worst impact on QoE.

Fig. 2c depicts the mean CCA, i.e. Clear Channel Assessment, values during the tests. CCA is a commonly used parameter to determine the channel availability. CCA clearly decreases with the presence of 0th side channel interference. However, it cannot sufficiently detect the effect of other side-channels. This is our main motivation in proposing a new metric for side-channel interference in Section III.

The mean values of *OBSS*, *NoPkt*, and *Glitch* for each test are shown in Figs. 2d, 2e, and 2f, respectively. We observe a great increase of *OBSS* when both pairs are operating on the same channel. *NoPkt*, and *Glitch* highly increase under 3rd side-channel interference. *Glitch* has slight increases also under 2nd side-channel interference.

Fig. 2g demonstrates the mean *BadPLCP* values in each test case. *BadPLCP* increase dramatically under 1st and 2nd side-channel interference among which the effect of 1st side-channel is stronger than the 2nd. *BadPLCP* may also increase slightly when there is interference from the 3rd side-channel.

III. INTERF METRIC

A. Formula

Based on the results explained in Section II-D, we propose a new metric, *interf*, to quantify the effect of side-channel interference on Wi-Fi QoE as follows:

$$interf = \left\lfloor \frac{\frac{B \times B_w}{B_{th}} + \frac{G \times Gw}{G_{th}} + \frac{N \times N_w}{N_{th}}}{B_w + G_w + N_w} * 100 \right\rceil \qquad (1)$$

where B, G and N denote the values of *BadPLCP, Glitch* and *NoPkt*, respectively. Subscript *th* and *w* denote scaling threshold and weight values, respectively, for corresponding parameters and $\lfloor . \rceil$ denotes rounding the input to the nearest integer. Eq. (1) is the weighted average of the scaled values of *BadPLCP, Glitch* and *NoPkt*. We do not consider *OBSS* as the 0th side-channel impact has already been considered in *CCA* which is a commonly used metric for WiFi channel availability.

We apply min-max scaling to the parameters, where the minimum values of these parameters are 0. To determine the maximums, we observe these parameters in the field with over $1M$ samples collected in 1 min intervals from the APs in the field. As the parameter mean values are significantly lower compared to the maximums as seen in Table III, we use the 95th percentile of the max values for scaling. This 95th percentile coefficient is intended to discard outlier results in the normal distribution of samples. Note that the thresholds are rounded up for simplicity.

TABLE III
POPULATION MEANS, MAXIMUMS, THRESHOLDS, FACTORS

	Mean	Max	Threshold	Weight
BPlcp	33	1845	130	3.66
NPkt	5	59	20	5.05
Glitch	1791	65006	4930	1.34

The weights aim to quantify how much one unit increase of the corresponding parameters impacts QoE. We applied linear regression between the mean download rates and mean parameter values of each test run, and used the resulting slope as the weight of the parameter. The weight values are also shown in Table III. Note that the threshold and weight values are obtained for the AP model being used and may need to be adjusted for the other AP models.

B. Evaluation

Fig. 2h depicts the average *interf* values for 18 consecutive tests for all five cases. When compared with the mean Iperf throughput and download rates in Figs. 2a and 2b, jumps in *interf* value coincide with the decreases in the Iperf throughput and download rates. In this sense, our proposed metric captures the QoE impact of the side-channel interference.

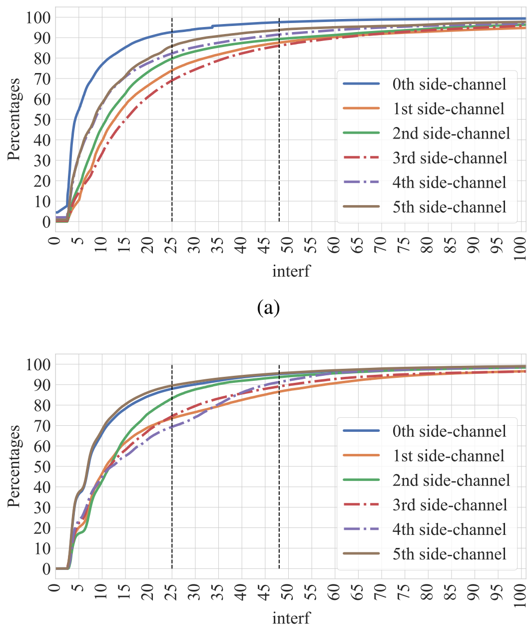
We determine two thresholds to divide the [0,100] *interf* range into three zones, namely high, mid and low interference zones. These thresholds are adjusted so that the highest jumps of mean *interf* in Fig. 2h lie in the high zone, and relatively smaller jumps are in the mid zone. The thresholds, *interf* values of 25 and 48, are depicted in Fig. 2h with dashed black horizontal lines. A client having *interf* values greater than 48 are in the range of high interference, which means that there appears to be a severe interference problem and visible QoE decrease. On the other hand, a client in the low interference zone, whose *interf* is lower than 25, would not be expected to have any visible QoE decrease due to side-channel interference.

IV. FIELD STUDY

In this section, we present the results of the field study with the Norwegian ISP regarding the side-channel interference effect on 802.11ax and 802.11n deployments. For this study, over 2M samples is collected from 1003 802.11ax and 966 802.11n APs in 1min interval during one day.

Fig. 3 shows the cumulative distribution function (CDF) of *interf* values of the APs in the 802.11ax and 802.11n deployments. Each line denotes the samples belonging to the APs with at least one neighbor on the specified side-channel. In both deployments, APs with neighbors on 1st and 3rd side-channels, being in mid or high interference zones for approximately 30% of the time, suffer most. 802.11n APs with 4-th side-channel neighbours also experience high *interf* values.

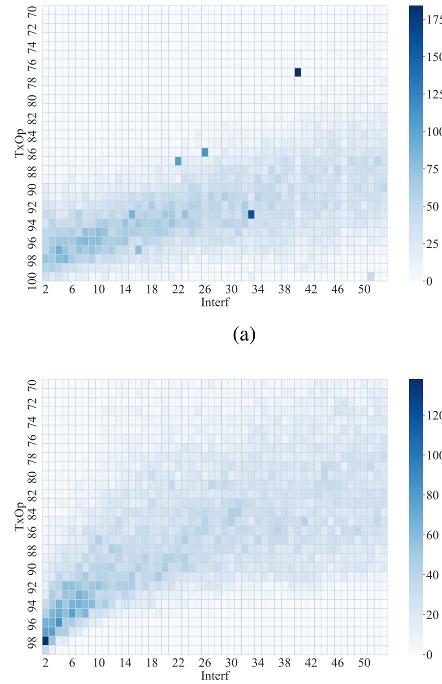
Fig. 4 demonstrates the relation between *txop* and *interf* as a heatmap for 802.11ax and 802.11n APs. The *txop*



(a)

(b)

Fig. 3. CDF of *interf* values for (a) 802.11ax APs and (b) 802.11n APs



(a)

(b)

Fig. 4. *TxOp* vs.*interf* heatmap for (a) 802.11ax APs and (b) 802.11n APs where the color bar indicates number of samples

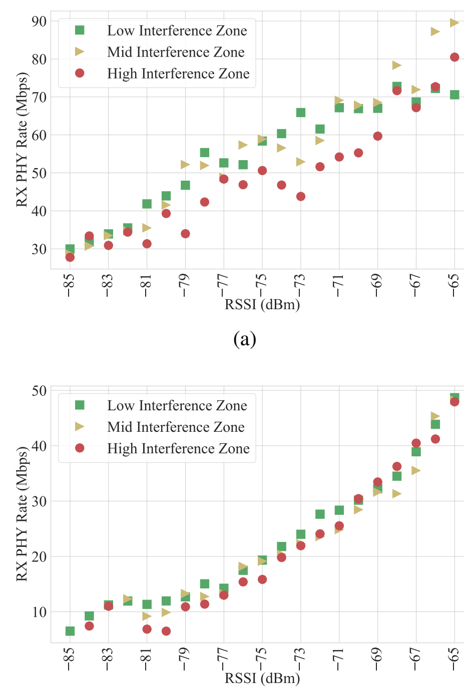
parameter indicates transmit opportunity sensed by the APs. For both type of APs, higher *interf* values correlate with the lower transmit opportunity. This indicates that the side-channel interference may limit medium access, as the chipset carrier sensing mechanism marks the medium as unavailable during times of high interference. 802.11n APs suffer from this medium access issue more than 802.11ax APs since their *txop* decreases to lower values compared to 802.11ax APs.

Fig. 5 depicts the mean RX PHY-rates of the samples with the same RSSI for 802.11ax and 802.11n APs. The samples in the high interference zone generally have lower PHY-rates than samples in the mid and low zones at the same RSSI. As WiFi PHY-rates are adaptively adjusted based on the frame losses [14], we conclude that the APs decrease the PHY-rates to cope with the frame losses caused by the side-channel interference. Especially 802.11ax APs, whose mean RX PHY-rates are almost two times higher than 802.11n APs, experience a significant decrease in their PHY-rates.

V. Interfering Neighbor Detection

In this section, we propose a DNN architecture to detect the actively interfering side-channel neighbours.

We use a DNN with 3 hidden layers which consist of 32, 16, and 8 neurons, respectively. The input features are *OBSS*, *NoPkt*, *BadPLCP*, *Glitch*, and *interf*. The 6 outputs represent the classes of neighbours operating on 0th-4th side channels or no interfering neighbour. All neuron weights are initialized randomly from a Gaussian distribution with 0 mean and 0.05 standard deviation. Standard scaling is applied on input features. $tanh$ and $softmax$ activation functions are preferred at the hidden and output layers, respectively. The DNN is implemented in Python using *Keras* with *Tensorflow* backend and trained with an Adam optimizer to minimize categorical cross entropy loss. In the training, class weights inversely proportional to the class sample sizes are used.



(a)

(b)

Fig. 5. Mean RX PHY-rates of samples at the same RSSI values for (a) 802.11ax APs and (b) 802.11n APs .

TABLE IV
CONFUSION MATRIX ON THE TEST SET (%)

	No	0th	1st	2nd	3rd	4th
No	**97.26**	2.25	0	0	0	0.48
0th	1.14	**98.81**	0	0	0.01	0.04
1st	0.32	18.46	**51.76**	0.89	0.19	27.38
2nd	1.82	0.93	0.30	**92.27**	0.62	4.06
3rd	2.63	0.10	0	0.38	**88.31**	8.59
4th	**70.01**	10.98	2.34	0.11	0.08	16.47

TABLE V
PRECISION, RECALL AND F1-SCORES ON THE TEST SET

	precision	**recall**	**f1-score**	**support**
accuracy			0.78	31432
macro avg	0.69	0.74	0.66	31432
weighted avg	0.83	0.78	0.79	31432

Note that 5th side-channel neighbours are not considered since WiFi Channels 1 and 6, or Channels 6 and 11, are non-overlapping in frequency and their impact on each other is only observed when the APs are located in the same room, which is not common in the field.

We consider training, validation, and test sets with 29724, 7431, and 31432 samples, respectively. The training and validation sets are constructed by randomly dividing the data samples collected in the experiments described in Section II. The test set is created by another set of experiments with the same AP but several different clients. For the test set, the wireless driver parameters are again collected in 1s intervals while either the positions of the AP and clients, the side-channel generating the interference, or utilization of the side-channel are changed every 30s.

The DNN performance is presented in Table IV, which shows the confusion matrix, and in Table V, in terms of precision, recall and f1-scores of all classes. The classification results with 78% accuracy, 83% precision, 78% recall, and 79% f1-score. The main reason decreasing the performance is 4th side-channel neighbours who confused with no interference case. This confusion is expected since the wifi driver parameters of both classes are similar, as seen in measurement results in Section II-D. Similar to the no interference case, neighbours at the 4th side-channel do not have negative effect on QoE, except when the APs are located in the same room, which is not common in the field. Hence, not being able to detect 4th side-channel neighbours will not have significant consequences for real life applications.

VI. CONCLUSION

This paper aims to quantify QoE degradation caused by 2.4 GHz WiFi side-channel interference, and detect the interfering neighbour based on passively sampled wireless driver parameters of consumer grade APs. First, experiments are conducted in a home environment, whose results indicate that *OBSS, BadPLCP*, *NoPkt* and *Glitch* are the driver parameters which signify interference from different side-channels. Based on these parameters, we propose a metric, *interf*, which quantifies side-channel interference impact on QoE. Observation of *interf* values in the field shows that side-channel interference prevents medium access and causes frame losses, which are the main drivers of lowered QoE. Under side-channel interference, APs in 802.11n deployments suffer medium unavailability more than ones in 802.11ax deployments. PHY-rates of 802.11ax APs, on the other hand, are affected by the interference conditions more than PHY-rates of 802.11n APs .

Further, a DNN-based algorithm to detect actively interfering neighbors, where the driver parameters are inputs and the side-channel causing the interference is the output, is proposed. Our proposed algorithm reaches 78%, 83%, 78%, and 79% accuracy, precision, recall and f1-score, respectively. As future work, we aim to extend this DNN-based algorithm to provide a channel selection mechanism.

REFERENCES

[1] E. Stancu, S. Halunga, O. Fratu, C. Florea, M. G. Berceanu, and C. Cristian, “Spectral analysis in the 2.4 ghz wifi band in bucharest,” in *2020 13th International Conference on Communications (COMM)*, 2020, pp. 435–438.

[2] W. N. Fatihah Wan Mustapha, M. A. Abdul Aziz, M. Masrie, R. Sam, and M. N. M. Tan, “Wifi approximated strength measurement method with brute force algorithm for a minimum number of ap and maximum wifi coverage,” in *2020 IEEE 10th Symposium on Computer Applications Industrial Electronics (ISCAIE)*, 2020, pp. 180–185.

[3] I. Pefkianakis, H. Lundgren, A. Soule, J. Chandrashekar, P. Le Guyadec, C. Diot, M. May, K. Van Doorselaer, and K. Van Oost, “Characterizing home wireless performance: The gateway view,” in *2015 IEEE Conference on Computer Communications (INFOCOM)*, 2015, pp. 2713–2731.

[4] N. Inzerillo, D. Croce, D. Garlisi, F. Giuliano, and I. Tinnirello, “Error-based interference detection in WiFi networks,” in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*. IEEE, dec 2017.

[5] I. Syrigos, N. Sakellariou, S. Keranidis, and T. Korakis, “On the employment of machine learning techniques for troubleshooting WiFi networks,” in *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, jan 2019.

[6] D. Neves da Hora, K. Van Doorselaer, K. Van Oost, R. Teixeira, and C. Diot, “Passive Wi-Fi Link Capacity Estimation on Commodity Access Points,” in *Traffic Monitoring and Analysis Workshop (TMA) 2016*, Louvain-la-Neuve, Belgium, Apr. 2016. [Online]. Available: https://hal.inria.fr/hal-01292633

[7] D. da Hora, K. van Doorselaer, K. van Oost, and R. Teixeira, “Predicting the effect of home wi-fi quality on qoe,” in *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, 2018, pp. 944–952.

[8] “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, 2016.

[9] E. Khorov, A. Kiryanov, A. Lyakhov, and G. Bianchi, “A tutorial on ieee 802.11ax high efficiency wlans,” *IEEE Communications Surveys Tutorials*, vol. 21, no. 1, pp. 197–216, 2019.

[10] B. Bellalta, “Ieee 802.11ax: High-efficiency wlans,” *IEEE Wireless Communications*, vol. 23, no. 1, pp. 38–46, 2016.

[11] K. Mathur, D. Jena, S. Agrawal, S. Baburaj, S. Kondabathini, and V. Tyagi, “Throughput improvement by using dynamic channel selection in 2.4ghz band of ieee 802.11 wlan,” in *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)*, 2018, pp. 805–810.

[12] Speedtest. Online. Ookla. [Online]. Available: speedtest.net

[13] Iperf. Online. ESnet / Lawrence Berkeley National Laboratory. [Online]. Available: iperf.fr

[14] S. Biaz and S. Wu, “Rate adaptation algorithms for ieee 802.11 networks: A survey and comparison,” in *2008 IEEE Symposium on Computers and Communications*, 2008, pp. 130–136.