RF Fingerprinting to Detect Beamstealing Attacks in mmWave 5G Communications

Martin KOUSAL, Josef VYCHODIL, Malek ALI, Roman MARSALEK

Dept. of Radio Electronics, Brno University of Technology FEEC, Technicka 12, 616 00 Brno, Czech Republic

martin.kousal@vut.cz

Submitted December 30, 2025 / Accepted February 5, 2026 / Online first February 13, 2026

Abstract. *5G mmWave networks rely on directional beamforming to ensure high-bandwidth connectivity, but the initial beam alignment process is vulnerable to beam–stealing attacks. In this scenario, an adversary transmits forged synchronization signals to hijack the receiver's connection, potentially leading to denial of service. This paper analyzes these threats and proposes a physical-layer detection mechanism based on radio frequency fingerprinting. Using a 60 GHz laboratory test-bed, we emulate legitimate and malicious transmission scenarios to evaluate specific hardware impairments. We investigate two primary detection metrics: power amplifier nonlinearities, analyzed via their Amplitude Modulation to Amplitude Modulation (AM/AM) characteristics, and local oscillator stability, quantified by carrier frequency offset drift. Experimental results demonstrate that these metrics can successfully distinguish among different transmitting devices based on their saturation levels and frequency stability profiles. The study confirms that lightweight radio frequency (RF) fingerprinting is a viable solution for hardening 5G beam management against spoofing.*

Keywords

Beam-stealing, 5G, mmWave, RF fingerprinting, nonlinearities, CFO

1. Introduction

The fifth generation (5G) of mobile networks is transforming connectivity by delivering gigabit-class data rates, millisecond-level latency, and enhanced reliability to support emerging sectors such as industrial automation, medical services, or autonomous transport. In industrial settings, the shift from fixed wired links to wireless infrastructures enables truly mobile automation. Mobile robots and autonomous vehicles can only realize their full productivity and flexibility when wireless links match the stability and throughput historically provided by cable links, such as Ethernet [1].

To satisfy these strict requirements, 5G networks increasingly exploit the millimeter wave (mmWave) bands, which offer very high bandwidth and capacity. In addition to the licensed Frequency Range 2 (FR2) which reaches up to a maximum of 33.4 GHz in Europe, a 60 GHz band has been attracting massive research interests, not only due to the wide available bandwidth, but also due to its unlicensed operation, where the coexistence of 5G and 60 GHz WiFi is expected [2]. Propagation at these frequencies is inherently lossy and sensitive to blockage and atmospheric effects. The wireless networks therefore need to concentrate energy using directional antennas and beamforming, producing narrow spatial lobes that restore link budget, but highly depend on precise alignment between transmitter and receiver [3].

This paper departs from the analysis of beam-stealing threats in 5G mmWave systems performed in [4]. The approach used falls within the domain of radio-frequency fingerprinting for physical-layer security, with a proliferation of contributions over the last decade. Among the related papers, it is worth mentioning some of the most recent or closest works. Authors of [5] provided an in-depth overview of the state-of-the-art in the RF fingerprinting for Internet of Things (IoT) devices, and classified the methods from various points of view, including used features (I/Q samples, spectrograms, Fourier coefficients), and they mostly focused on the specific IoT standards, not on 5G. The carrier frequency offset as a metric for authentication of the wireless devices for smart healthcare systems has been proposed in [6]. In contrast to our paper, the authors have not verified their approach on real data; instead, they modeled the frequency offset using a Markov process. Similarly, one of the early works that developed the carrier frequency offset as a suitable metric [7] assumed a Gaussian model, without prior verification of this hypothesis. The recent paper [8] considered the use of 5G New Radio (5G NR) waveforms and the fingerprints extracted from the pilot information (specifically Sounding Reference Symbols), and evaluated the developed metrics and methods on the dataset from low-cost ADALM-PLUTO devices operating in the 5G Frequency Range 1 (FR1). With the growing field of machine learning (ML) and artificial intelligence (AI), many studies have considered using such approaches to distinguish between legitimate and

DOI: 10.13164/re.2026.0129

rogue transmitters, including our previous contribution [9]. Despite the unprecedentedly high accuracy, explainability in ML/AI remains an important issue for safety-critical applications; thus, in contrast to [9], we focus on feature-based approaches hereinafter.

Main contributions of this paper can be summarized as follows:

- We formalize attacker capabilities and describe a representative attack strategy of beam-stealing in mmWave bands.
- We propose a signal processing chain to extract the fingerprinting metrics derived from 5G synchronization blocks.
- We evaluate the potential of lightweight, fingerprinting-based detection of beam-stealing attacks on data from real mmWave measurements in the unlicensed 60 GHz band.

The paper is structured as follows. Section 2 briefly discusses the beamforming technique and associated attacks, Section 3 describes our experimental mmWave test-bed, and is followed by a transmitter signal generation description in Sec. 4. Section 5 discusses suitable metrics for detecting such an attack, with further details on the signal processing chain provided in Sec. 6. Section 7 then presents the results for the specified detection metrics, while Section 8 concludes the paper.

2. 5G Beamforming Technique

Due to the narrow nature of mmWave beams, explicit beam management procedures are required to discover, select, and maintain optimal transmit–receive beam pairs. 3GPP New Radio (NR) specifies beam management mechanisms (sweeping, measurement, and reporting) that rely on synchronization and reference signals transmitted across candidate beam directions, as well as user feedback and network control, to select and switch beams [10]. Beam training and periodic or event-driven beam reporting are all used to reduce alignment time and overhead. Robust beam tracking is required for mobility and blockage recovery because small angular changes or blockage can rapidly degrade the performance of mmWave links.

2.1 Beam-Stealing Attack

Beamforming in mmWave communications is usually maintained by applying discrete antenna array settings from a predefined steering codebook (so-called beamboook). Each entry in this codebook is referred to as a sector and creates such a beam. For optimal establishment of the mmWave link, the transmitter and receiver must select the codebook entries that yield the highest received signal strength [11]. Because the connection has not yet been established at this early stage of communication, the beam alignment process is insecure and can be easily compromised.

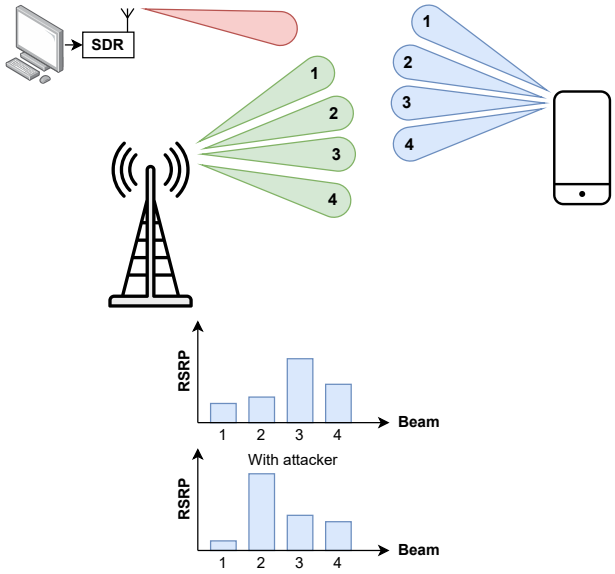


Fig. 1. Beam alignment procedure with beam-stealing attack.

As described in [12], the Man-In-The-Middle (MITM) attack can be performed to forge a legitimate transmitter and receiver to steer their beams at an attacker, who resends packets with possible eavesdropping. A simpler version of this attack can be implemented solely at the transmitter, without forwarding packets. Such a transmitter would send only malicious synchronization signals, just with a higher power than the legitimate ones. This situation will lead the receiver to evaluate the counterfeit beam as the strongest, based on the Reference Signal Received Power (RSRP), and thus the best beam. This may cause the receiver to get looped in the beam alignment process and potentially Denial of Services (DoS), as shown in Fig. 1.

With the expected massive deployment of millimeter-wave communications, the research of attack countermeasures is of utmost importance. As the attacks on the beam management target the initial phase of the connection, it is advantageous to focus on the physical layer security techniques. In the following chapter, we describe our experimental setup.

3. Hardware Setup

The measurement was performed in a laboratory environment to ensure a controlled setup. Throughout the experiment, the vector signal analyzer Rohde&Schwarz FSW85 [13] was used as the reference receiver. It is assumed to be the most linear and stable over time and thus will not introduce signal distortions nor offsets into the received signal. Directly at the input RF port, an adapter from waveguide to coaxial QWA-15R18FE [14] was connected. At the waveguide side, a horn antenna SAR-2013-15-S2 [15] with 20 dBi gain was used. This setup remains the same throughout all measurements. The role of the signal analyzer is primarily to store the In-phase and Quadrature (I/Q) samples with a sampling rate of 491.52 MHz for future processing in the connected computer.

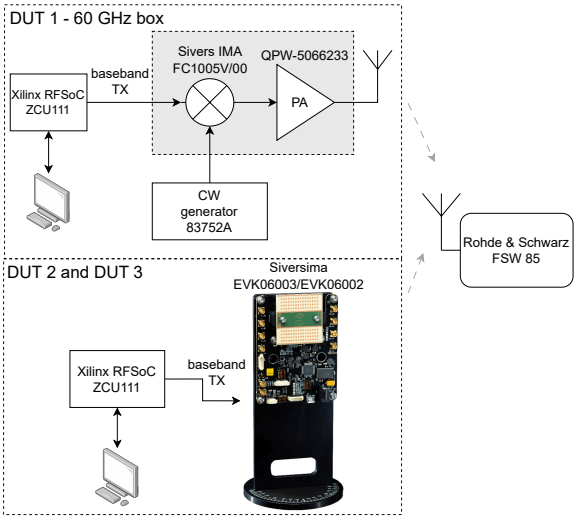


Fig. 2. Measurement system schematic diagram.

A total of three distinct transmitting devices were measured: some of them could represent legitimate devices, while the others serve as attacker devices. Our primary objective was to determine whether it is possible to distinguish one of these devices from another. Only one of the devices was transmitting at the same time. The block schematic of the measurement setup is shown in Fig. 2. All transmission in the baseband is realized with the development board ZCU111 from Xilinx equipped with Zynq UltraScale+ RFSoC [16]. The I and Q baseband components are generated by fast 14-bit DACs clocked at 6.554 GSPS connected to VLFX-2500+ low-pass filters, which are used to prevent aliasing.

The first Device Under Test (DUT), hereinafter called the 60 GHz box, is a part of our mmWave test-bed previously used for channel sounding or vehicular communications experiments [17]. It is built from Sivers IMA FC1005V/00 upconverter, which raises the baseband signal to the required mmWave frequency. The upconverter can be used in the range of 57 – 66 GHz. The local oscillator signal is generated by a frequency-stable, low-phase-noise generator, Agilent 83752A. The upconverted signal then drives the QuinStar QPW-5066233 power amplifier with 30 dB gain and 23 dBm P1dB power, to boost the power of the RF signal, which is then transmitted using the horn antenna of the same type as used at the receiver side. Distance between DUT and FSW is 150 cm and does not change during the experiment.

The second and third DUTs are Sivers IMA beamforming kits, specifically EVK06003 and EVK06002 [18]. They were placed 80 cm from FSW. Those kits have all the required RF hardware for transmitting in 60 GHz band (exact frequency range of 57 – 71 GHz); there is only a need to supply a differential baseband I/Q signal, and connect them via USB interface to the PC for remote setup and control. To ensure the conversion of single-ended I/Q data from the RFSoC platform to the differential pair, the balun board ADC-WB-BB from Texas Instruments is used.

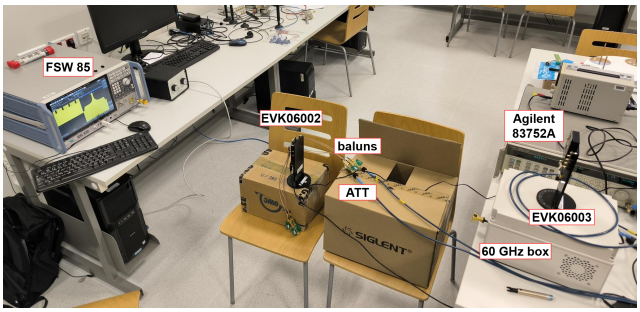


Fig. 3. Transmitters and receiver in laboratory.

Both kits are equipped with the same motherboard, which provides a local oscillator, control circuits, etc., and the difference between them lies only in the populated RF module. Beamforming is performed through the integrated codebook with 63 fixed steps, alternatively, there is an option for the omnidirectional mode. The first-mentioned kit is equipped with the RFM06009 module, which supports beamforming in azimuth by ±54 degrees and in elevation by ±25 degrees, and the output RF power reaches up to 40 dBm. The second-mentioned kit is equipped with the RFM06010 module, which allows only azimuth beamforming in the range ±45 degrees, again with 63 fixed steps. The entire test bed during the laboratory measurements is shown in Fig. 3.

4. Signal Generation

For a realistic emulation of the beamforming procedure in the 5G system, it is necessary to generate a corresponding signal to be transmitted through the DUTs. Throughout our experiment, we have generated the signal resource grid using the MATLAB 5G Toolbox [1] to maintain the 5G standard rules as close to the real situation.

In order to correctly perform the initial access by the User Equipment (UE), the base station, in the 5G terminology denoted as the next generation Node B (gNB) transmits the beams burst in all possible directions at defined intervals. These synchronization bursts consist of the Synchronization Signal Blocks (SSB) containing the Primary Synchronization Sequence (PSS), the Secondary Synchronization Sequence (SSS), the Physical Broadcast Channel (PBCH) and the Demodulation Reference Signals (DMRS). The single synchronization block occupies 4 OFDM symbols and 20 Resource Blocks (RB), which is equal to the 240 subcarriers as shown in Fig. 4. Depending on the transmission frequency, there is a maximum number of those synchronization blocks that are repeated and together form a synchronization burst. For the 5G mmWave frequency range (FR2), there is a limit of 64 SSB blocks per burst, which forms 5 ms window periodically repeated in time. This period is usually set to 20 ms, but in order to reduce amount of received I/Q samples to process throughout our experiment, we have repeated these windows one next to each other.

[1] https://www.mathworks.com/products/5g.html

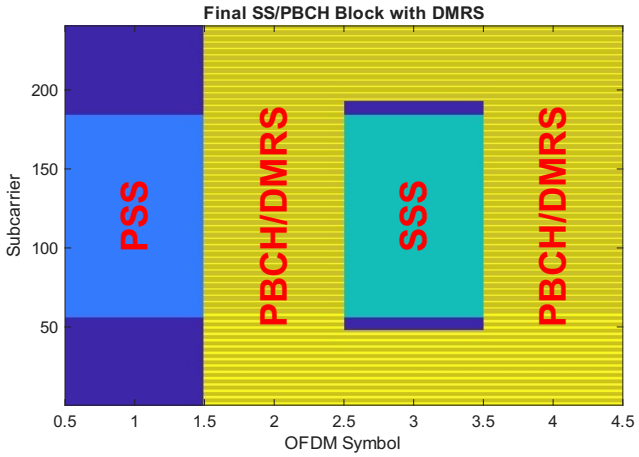


Fig. 4. Structure of generated synchronization block.

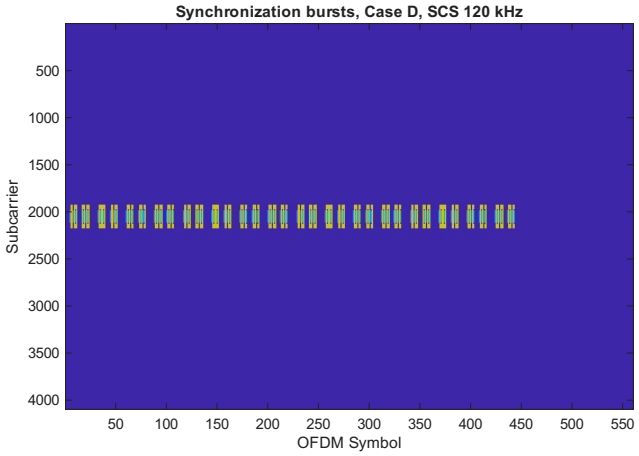


Fig. 5. Resource grid of final synchronization burst with SCS 120 kHz, FFT size 4096, occupied bandwidth 28.8 MHz.

The subcarrier spacing (SCS) is selected according to Case D in the 3GPP specifications, which is 120 kHz [10], appropriate for mmWave bands. For such a burst configuration, the minimum sampling frequency is 30.72 MHz (note that in our experiment, without loss of generality, we do not transmit any data as we expect the initial access phase). Due to the hardware limitations of the clock settings in the used RFSoC platform, we can not set such very low ADCs sampling frequencies, and thus we have chosen the sampling frequency of 491.52 MHz, corresponding to the product of the optimal FFT length of 4096 and 120 kHz SCS. Such sampling frequency is comparable to one we used in our previous experiments [17]. The unused part of the time-frequency resource grid is set to zero, so nothing is transmitted there, as illustrated by a blue color in Fig. 5.

5. Suitable Detection Metrics

The use of low-cost, widely available Software-Defined Radio (SDR) technology by the attacker is usually considered. Every transmitting hardware has some imperfections, such as nonlinearities, mismatches, or leakages, and these create a specific kind of distortion to the transmitted signal, unique to every single device, as we discussed previously for sub-6 GHz frequencies in [19]. When observing raw sampled I/Q data, there are several RF fingerprinting [20] options to distinguish which transmitter we are actually receiving data from.

There are several basic assumptions we consider in our experiment to identify the individual devices:

- The attacker's device is usually not equipped with very precise (and thus expensive) pieces of hardware, such as the ultra-linear power amplifiers (PA), nor the precise signal upconverters with an ultra-stable local oscillator.
- The attacker usually operates from a larger distance to the victim UE, than the legitimate gNB. Moreover, in order to perform a successful attack, the power level from the attacker at the location of UE must be higher than the power level from the legitimate user.

  Therefore, the attacker usually has to transmit at a higher power level, reaching the amplifier's limits and causing its output to saturate easily. Operating the PA in the highly linear regime would, on the other hand, require much higher energy from the power supply.

The power amplifier nonlinearity and the local oscillator frequency offset are two examples of impairments whose effects on the signal are relatively easy to distinguish from one another and from those of other impairments. Exploiting additional impairments, such as phase noise [21], or I/Q imbalance [22] can be considered in future work.

5.1 Transmitter Nonlinearities

The first suitable metric leverages the second-mentioned assumption and extends the concept of RF fingerprinting by identifying AM/AM characteristics of the power amplifier. Note that the Amplitude Modulation to Phase Modulation (AM/PM) distortion of the state-of-the-art solid state PA's is usually considered negligible, in contrast to e.g. traveling tube amplifiers used in SatCom applications.

In order to estimate the AM/AM curve, there is a need to know both the received and the transmitted signal. This may be challenging for general data transmission, but in our case we rely on processing SSB signals, as defined by 3GPP, which are present in any standard-compliant gNB transmission. In real applications, it is thus possible to generate a synthetic copy of synchronization bursts after receiving the real, legitimate ones and decoding the required information, such as PSS and SSS.

After the synthetic copy is created, the AM/AM characteristic, which describes the (non)linearity of the transmitter, can be estimated. If the attacker's PA operates in saturation, the received signal will be accordingly distorted. To distinguish among the individual transmitters, a suitable metric could be the Normalized Mean Squared Error (NMSE) between the measured AM/AM and the perfectly linear AM/AM response.

5.2 Local Oscillator Imperfections

The second metric is based on imperfections in the transmitter's upconverter and the connected local oscillator, which have previously been identified as a suitable fingerprinting feature [19]. Every oscillator drifts over time and, if not compensated, its frequency is also highly dependent on temperature [23]. Those imperfections are much stronger in mmWave bands because the upconverter will multiply their effect.

In general, it is assumed that legitimate gNBs are using the high-precision, and thus expensive, hardware components, for which such described frequency drifting is kept pretty small, and the attacker's oscillator hardware is usually much less stable. Even if this is not the case, the frequency drift across transceivers will vary. Fingerprinting transmitters with this method is based on estimating the Carrier Frequency Offset (CFO) from PSS and Cyclic Prefixes (CP) of OFDM symbols and comparing the deviation of CFO both by its distribution and over time.

6. Signal Processing Chain

The received signal at carrier frequency 58.576 GHz with subcarrier spacing 120 kHz and occupied bandwidth 28.8 MHz is recorded using a signal analyzer sampling at frequency 491.52 MHz with a record length corresponding to a duration of 20 ms, which is sufficient to capture at least three repetitions of the transmitted sequence, each with a duration of 5 ms. The I/Q samples are stored on an SSD drive and transferred to MATLAB for further processing. The size of the 20 ms file is 150 MB, for the long-term CFO estimation approximately 1.5 s were recorded and this file is 10.9 GB in size. The block schematic of the processing chain is shown in Fig. 6.

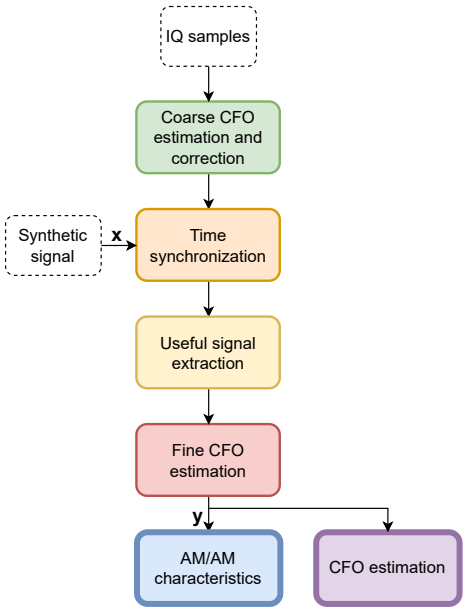


Fig. 6. Received signal processing chain in MATLAB.

The first step is to compute a coarse CFO estimate from PSSs via correlation. As defined in 5G standard [10], there are three possible PSSs. We synthesize all of them, shift each by half the SCS in the range of $\pm 6 \times$ SCS, and correlate with the received signal. The PSS index and corresponding coarse frequency offset are then selected based on the highest identified correlation peak. After the coarse CFO calculation is completed, the frequency correction is applied to the whole received waveform. The next step is to synchronize in time with the known SSB sequence and extract all repetitions of synchronization bursts which have been captured, similar to the process described in [24]. This is done by using integer sample synchronization by correlating a known transmitted synchronization burst with the received waveform. Then the process continues with fine CFO estimation and correction, which is calculated using CP for each OFDM symbol separately. The CFO estimate $\hat{\epsilon}$ is calculated from the phase difference between CP and the corresponding tail part of the OFDM symbol as described in [25] using (1), where M is the length of CP and N is the size of the FFT :

$$\hat{\epsilon} = (1/2\pi)\arg\left\{\sum_{n=1}^{M} y_1^*[n]\, y_1[n+N]\right\}. \tag{1}$$

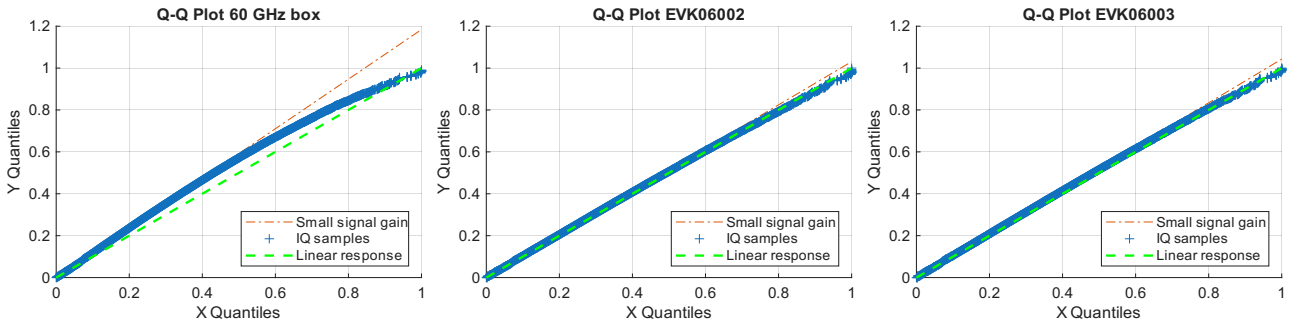
Such calculated CFOs are stored and processed as the suitable fingerprinting metrics. The synchronized and frequency-corrected signal is then used to obtain AM/AM characteristics estimates.

7. Results

This section presents the results of measurement and further analysis of the described detection metrics to unveil their potential to detect the beam stealing attack.

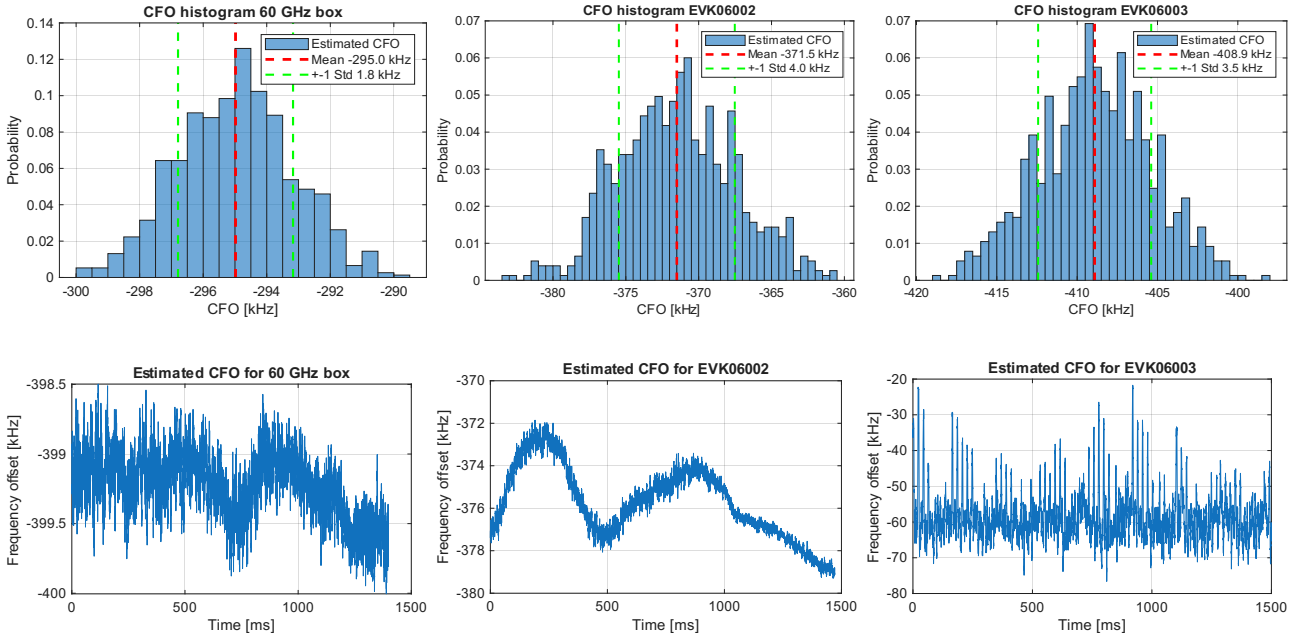
The first method, relying on the modeling of PA nonlinearities, makes use of a quantile-quantile data transformation, that has effectively been used in various applications, ranging from traffic modeling [26] to digital predistortion adaptation [27]. The quantile-quantile transformation, expressed using a quantile-quantile plot (Q-Q plot), is a graphical tool used to compare the distribution of a dataset to a reference distribution. In the case of PA modeling, the Q-Q plot serves to visualize how the quantiles of the PA output and the quantiles of the PA input are related. Note that in the 5G context, the PA input signal has the complex zero-mean Gaussian distribution, and its amplitude thus follows the Rayleigh distribution.

Alternatively, a standard approach to estimate AM/AM characteristics through least squares-based polynomial fitting can be used, but with difficulties in determining the optimal order of the polynomial, which can cause either underfitting and loss of information or overfitting of the PA characteristic.



(a) DUT 1: 60 GHz box, NMSE: −16.2 dB (b) DUT 2: EVK06002, NMSE: −22.8 dB (c) DUT 3: EVK06003, NMSE: −23.8 dB

Fig. 7. Measured AM/AM characteristics using Q–Q plot.



(a) DUT 1: 60 GHz box (b) DUT 2: EVK06002 (c) DUT 3: EVK06003

Fig. 8. CFO estimation histograms and long time measurement for DUTs (each column represents one DUT).

	60 GHz box	EVK06002	EVK06003
NMSE [dB]	−16.2	−22.8	−23.8
CFO deviation [kHz]	1.8	4.0	3.5

Tab. 1. AM/AM characteristics NMSE from linear gain.

The Q-Q plots at Fig. 7 show that the 60 GHz box (acting as a far-distance jammer) is in saturation, whereas the two beamforming kits behave almost linearly. To quantify the nonlinearity, NMSE is calculated as the error between the ideal linear gain curve and AM/AM I/Q samples from Q-Q plot with the equation:

$$\mathrm{NMSE}_{\mathrm{dB}} = 10\log_{10}\left(\frac{\sum_n |x(n)-y(n)|^2}{\sum_n |y(n)|^2}\right) \qquad (2)$$

where x is ideal linear response and y is measured I/Q samples from Q-Q plot. NMSE results for all three measured transmitting devices are presented in Tab. 1.

The second metric, evaluating the stability of the local oscillator and resulting CFO is characterized by the statistical distribution of the instantaneous CFO estimates $\hat{\epsilon}$. The results are expressed at Fig. 8 showing the CFO histograms with bin width of 500 Hz. In addition, a standard deviation from the mean value is calculated to compare individual transmitters and presented in Tab. 1. These results are the outcomes of 3 synchronization bursts measurements with a total length of 15 ms.

The AM/AM shape could depend on the target output power of PA, and in some scenarios, the nearby attacker can still work in a relatively linear regime. In such a case, it could be advantageous to base the fingerprinting classification on CFO estimation. Among our tested devices, the 60 GHz box has a precise and stable local oscillator, with a standard deviation of ±1.8 kHz. In contrast to this device, the beamforming kits have much more unstable local oscillators, which manifests in higher standard deviation of CFO, equal to ±4 kHz for EVK06002 and ±3.5 kHz for EVK06003. Those results do not depend on the set PA gain/output power, so they represent a more promising way to distinguish among these devices.

Figure 8 then shows the results of the CFO estimation for a longer period of time (almost 1.5 s), from which the trend in CFO stability of each DUT can be seen. The most stable is again the 60 GHz box, where only minimal fluctuations are observed; on the other hand, the beamforming kits have their local oscillators relatively unstable. Note that it is not possible to distinguish between devices solely on the basis of the mean value of the CFO, because the beamforming kits exhibit different values after each power-on cycle. By comparing the measured results with previous work, e.g., from our measurement campaign in the FR1 band presented in [19], our study confirms the expected greater CFO deviations in mmWaves. Due to a lack of data, we are unable to directly compare NMSEs of AM/AM characteristics; however, given the variety of power amplifier technologies, generalization is not straightforward.

8. Conclusions

Shifting communications to the millimeter-wave spectrum offers increased capacity and inherently more secure links, enabled by unprecedented bandwidth and highly directional propagation. Conversely, the beam search process introduces additional vulnerabilities. Similar to other stages of network initial access, it remains unencrypted and may therefore be exposed to new attack vectors, including beam stealing and beam manipulation.

Our paper presents the results of a practical experiment that aims to enhance the security of the beam search procedure through radio-frequency fingerprinting. On the practical examples of commercially available beamformers, we demonstrate the ability to detect the identity impersonation of the transmitter by analyzing two selected metrics - the normalized mean squared error of the power amplifier nonlinearity from the linear gain, and the deviation of the transmitter's local oscillator carrier frequency offset. As shown in Tab. 1, the measured devices can be distinguished by a combination of these two metrics. We have shown that the transmitter architecture plays a crucial role in classification, with the standard beamforming-free transmitter being readily distinguishable from beamforming kits. Nevertheless, despite the identical architectures of the two beamforming devices, they can still be distinguished when the combination of NMSE and CFO deviation metrics is used. On the other hand, the CFO mean value is not a suitable metric, as it varies substantially after a transmitter reset and may also depend on the Doppler frequency induced by user motion.

Despite the promising results, there remains a long path to reliable implementation in real-world settings. The behavior as a function of transmitter-receiver distances, beam index, power amplifier operating point, or the wide center-frequency sweep can be investigated in future research. Moreover, the design of a lightweight automatic classifier that is not dependent on high-end measurement equipment, but can be implemented using commercial off-the-shelf components could be of further interest.

All measured data are also available in the form of an open access dataset[2].

Acknowledgments

This work has been funded by the Ministry of the Interior of the Czech Republic, program IMPAKT 1, project No. VJ03030044 *Robust 5G networks*. We would also like to thank for the support from the internal project of Brno University of Technology, FEKT-S-20-6325.

References

[1] AGIWAL, M., ROY, A., SAXENA, N. Next generation 5G wireless networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 2016, vol. 18, no. 3, p. 1617–1655. DOI: 10.1109/COMST.2016.2532458

[2] KIM, S., VERBOOM, J. On the coexistence of WiGig and NR-U in 60 GHz band. In *Proceedings of the 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*. Helsinki (Finland), 2021, p. 1–5. DOI: 10.1109/VTC2021-Spring51267.2021.9448837

[3] RAPPAPORT, T. S., SUN, S., MAYZUS, R., et al. Millimeter wave mobile communications for 5G cellular: It will work! *IEEE Access*, 2013, vol. 1, p. 335–349. DOI: 10.1109/ACCESS.2013.2260813

[4] HARVANEK, M., BOLCEK, J., KUFA, J., et al. Survey on 5G physical layer security threats and countermeasures. *Sensors*, 2024, vol. 24, no. 17, p. 1–40. DOI: 10.3390/s24175523

[5] ZHANG, J., SHEN, J., SAAD, W., et al. Radio frequency fingerprint identification for device authentication in the Internet of Things. *IEEE Communications Magazine*, 2023, vol. 61, no. 10, p. 110–115. DOI: 10.1109/MCOM.003.2200974

[6] TENG, Y., SHI, H., ZHANG, P., et al. PHY-layer authentication exploiting CFO for smart healthcare systems with mmWave communication technology. *Ad Hoc Networks*, 2023, vol. 140, p. 1–10. DOI: 10.1016/j.adhoc.2022.103075

[7] HOU, W., WANG, X., CHOUINARD, J.-Y., et al. Physical layer authentication for mobile systems with time-varying carrier frequency offsets. *IEEE Transactions on Communications*, 2014, vol. 62, no. 5, p. 1658–1667. DOI: 10.1109/TCOMM.2014.032914.120921

[8] ZHA, H., WANG, H., WANG, Y., et al. Enhancing security in 5G NR with channel-robust RF fingerprinting leveraging SRS for cross-domain stability. *IEEE Transactions on Information Forensics and Security*, 2025, vol. 20, p. 3429–3444. DOI: 10.1109/TIFS.2025.3551638

[9] BOLCEK, J., KUFA, J., HARVANEK, M., et al. Deep learning-based radio frequency identification of false base stations. In *Proceedings of the Workshop on Microwave Theory and Technology in Wireless Communications (MTTW)*. Riga (Latvia), 2023, p. 45–49. DOI: 10.1109/MTTW59774.2023.10320078

[2] KOUSAL, M., VYCHODIL, J., ALI, M., et al. RF fingerprinting in mmWave 5G communications. Zenodo, 2026. DOI: 10.5281/zenodo.18481702

[10] 3GPP. *TS 38.213: 5G; NR; Physical Layer Procedures for Control*.

[11] THE MATHWORKS, INC. *Understanding 5G Beam Management*. 13 pages. [Online] Cited 2025-12-06. Available at: https://www.mathworks.com/content/dam/mathworks/mathworks-dot-com/images/responsive/supporting/campaigns/offers/5g-beam-management-white-paper/5g-beam-management-white-paper.pdf

[12] STEINMETZER, D., YUAN, Y., HOLLICK, M. Beam-stealing: Intercepting the sector sweep to launch man-in-the-middle attacks on wireless IEEE 802.11ad networks. In *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec '18)*. New York (USA), 2018, p. 12–22. DOI: 10.1145/3212480.3212499

[13] ROHDE & SCHWARZ USA, INC. *FSW Signal and Spectrum Analyzer*. [Online] Cited 2025-12-01. Available at: https://www.rohde-schwarz.com/us/products/test-and-measurement/benchtop-analyzers/fsw-signal-and-spectrum-analyzer_63493-11793.html

[14] QUINSTAR TECHNOLOGY, INC. *Waveguide to Coax Adapters QWA*. 4 pages. [Online] Cited 2025-11-30. Available at: https://quinstar.com/wp-content/uploads/2023/02/QUINSTAR-QWA-DATA-SHEETS.pdf

[15] ERAVANT. *WR-15 Pyramidal Horn Antenna, 20 dBi Gain*. 5 pages. [Online] Cited 2025-11-30. Available at: https://sftp.eravant.com/content/datasheets/SAR-2013-15-S2.pdf

[16] XILINX. *ZCU111 Evaluation Kit*. 1 page. [Online] Cited 2025-12-02. Available at: https://www.amd.com/content/dam/amd/en/documents/products/adaptive-socs-and-fpgas/boards-kits/product-briefs/zcu111-product-brief.pdf

[17] MARSALEK, R., BLUMENSTEIN, J., VYCHODIL, J., et al. Real-world OTFS channel estimation performance evaluation on mmWave vehicular channels. In *Proceedings of the 27th International Workshop on Smart Antennas (WSA)*. Dresden (Germany), 2024, p. 1–7. DOI: 10.1109/WSA61681.2024.10512001

[18] SIVERS SEMICONDUCTORS. *Product Brief – Wireless*. 2 pages. [Online] Cited 2025-11-28. Available at: https://www.sivers-semiconductors.com/wp-content/uploads/2022/03/Product-Brief-EVK06002_03-02001_-220224.pdf

[19] POSPISIL, M., MARSALEK, R., POMENKOVA, J. Wireless device authentication through transmitter imperfections—measurement and classification. In *Proceedings of the IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. London (UK), 2013, p. 497–501. DOI: 10.1109/PIMRC.2013.6666187

[20] YUAN, H., BAO, Z., HU, A. Power ramped-up preamble RF fingerprints of wireless transmitters. *Radioengineering*, 2011, vol. 20, no. 3, p. 703–709. ISSN: 1210-2512

[21] LOMAYEV, A., KRAVTSOV, V., GERNOSSAR, M., et al. Method for phase noise impact compensation in 60 GHz OFDM receivers. *Radioengineering*, 2020, vol. 29, no. 1, p. 159–173. DOI: 10.13164/re.2020.0159

[22] JOVANOVIC, B., MILENKOVIC, S. Transmitter IQ imbalance mitigation and PA linearization in software defined radios. *Radioengineering*, 2022, vol. 31, no. 1, p. 144–155. DOI: 10.13164/re.2022.0144

[23] POSPISIL, M., MARSALEK, R., GOTTHANS, T. Wireless device classification through transmitter imperfections—evaluation of performance degradation due to the chip heating. In *Proceedings of the IEEE Radio and Wireless Symposium (RWS)*. Phoenix (USA), 2017, p. 169–172. DOI: 10.1109/RWS.2017.7885978

[24] BLOESSL, B., SEGATA, M., SOMMER, C., et al. Performance assessment of IEEE 802.11p with an open-source SDR-based prototype. *IEEE Transactions on Mobile Computing*, 2018, vol. 17, no. 5, p. 1162–1175. DOI: 10.1109/TMC.2017.2751474

[25] MOOSE, P. H. A technique for orthogonal frequency division multiplexing frequency offset correction. *IEEE Transactions on Communications*, 1994, vol. 42, no. 10, p. 2908–2914. DOI: 10.1109/26.328961

[26] LANER, M., SVOBODA, P., RUPP, M. Parsimonious network traffic modeling by transformed ARMA models. *IEEE Access*, 2014, vol. 2, p. 40–55. DOI: 10.1109/ACCESS.2013.2297736

[27] BARRADAS, F. M., LAVRADOR, P. M., CUNHA, T. R., et al. Using statistical information for fast static DPD of RF PAs. In *Proceedings of the IEEE Topical Conference on RF/Microwave Power Amplifiers for Radio and Wireless Applications (PAWR)*. Phoenix (USA), 2017, p. 11–13. DOI: 10.1109/PAWR.2017.7875560

About the Authors ...

Martin KOUSAL was born in Brno. He received his M.Sc. degree in Electronics and Communication Technologies from the Brno University of Technology, Brno, Czech Republic, in 2024. He is currently pursuing his Ph.D. degree with a focus on physical layer security of mobile networks. His research interests include signal processing and digital communication systems.

Josef VYCHODIL received the master's and Ph.D. degrees from Brno University of Technology, in 2013 and 2022, respectively. His research interests include ultra-wideband and millimeter wave band channel measurement techniques and channel emulation. His other interests are signal processing and RFID systems.

Malek ALI received the B.Sc. degree in Computer and Communication Engineering from the Faculty of Engineering and IT, Taiz University, Yemen, in 2012, and the M.Sc. degree in Infocommunication Technologies and Communication Systems from Ryazan State Radio Engineering University, Russia, in 2020. He is currently pursuing the Ph.D. degree in Sensing Systems at Brno University of Technology, Czech Republic.

Roman MARSALEK (Member, IEEE) received the Ing. degree from the Brno University of Technology, Brno, Czech Republic, in 1999, and the Ph.D. degree from the Université de Marne-La-Vallée, France, in 2003. In 2013, he was a Teaching and Research Fellow with Johannes Kepler University, Linz, Austria. He is currently a Full Professor with the Department of Radio Electronics, Brno University of Technology. His research interests include wireless communications theory and applied digital signal processing.