Examination of 5G NR, LTE, and NB-IoT Radio Interfaces and Their Vulnerabilities to Interference

Piotr Rajchowski

Gdansk University of Technology, Gdańsk, Poland

https://doi.org/10.26636/jtit.2024.4.1960

Abstract — Modern cellular wireless communication systems of the fourth (4G) and fifth generation (5G) face a problem of various types of interference or intentional jamming. Consequently, a degradation of the services provided and an incorrect network operation may occur. In this paper, configuration of the networks' physical layer is investigated, with the said investigation preceded by the measurement of parameters of commercial networks operating in two different environments, to assess their vulnerabilities to interference or intentional jamming. Finally, a method for analyzing the radio signal received with the use of 5G New Radio (NR), Long Term Evolution (LTE), and Narrowband Internet of Things (NB-IoT) radio interfaces is proposed, to detect and mitigate the negative impact of unwanted signals. Software-based implementation of the proposed method allows one to detect and mitigate co-channel interference, intentional jamming and maintain compatibility of user equipment (UE) with the 3rd Generation Partnership Project (3GPP) standard, as it does not affect operations performed, for instance, at the time and frequency synchronization or channel parameter estimation phases.

Keywords — 5G NR, interference, jamming, NB-IoT, LTE

1. Introduction

The growing popularity of cellular communication systems, especially those of the fifth generation, stems from a rapid evolution in user habits and demands. The emergence of previous generation solutions (4G LTE [1]) and the new 5G networks addressed the needs of users taking advantage of popular services relying on mobile data transmission. Furthermore, other technologies, such as the Internet of Things (IoT), led to the development of new radio interfaces, e.g. Narrowband IoT (NB-IoT), which relied on a modified version of the LTE radio interface [2].

Regardless of the geographical region considered, an increase in the quantity of user equipment (UE) operating within increasingly dense networks may be observed in highly urbanized areas [3]. In many European countries, frequency range 1 (FR1) bands are reallocated from other systems to 4G and 5G solutions to ensure higher network capacity. Thus, the same radio interfaces, e.g. 5G NR, LTE and NB-IoT, operate together, in the same multiple bands, but with different physical layer configurations. Therefore, one may assume that network planning and optimization tasks have become, mostly in urban areas, more challenging due to co-channel interference (CCI).

It is worth mentioning that interference is not the only problem encountered by commercial and private networks. Intentional jamming is another issue of great importance. Beyond national networks, private companies or government entities create several private 5G/4G networks based on software-defined network cores and radio access networks (RAN) [4]. These networks may be the target of intentional attacks, especially when one considers the ease with which software defined radio (SDR) technology may be accessed, and the open-source nature of the software relied upon.

In this context, the paper addresses the problem of CCI and intentional jamming of signals transmitted in frequency bands that 4G and 5G cellular networks rely on. The proposed method is designed for implementation on the UE receiving path and is supported by measurements aimed at discovering the most common configuration of the network's physical layer.

The main goal of this paper is to present the concept of processing the downlink signal independently of operations performed during frequency and time synchronization, as well as decoding the messages broadcast. Furthermore, the author assumes that interaction between the proposed solution and the regular signal processing algorithms will additionally benefit the process of mitigating interference and jamming.

The key contributions of the paper can be summarized as follows:

- A literature review has been presented, focusing on the methodology of identifying the parameters of interference signals observed in real world networks and on testing vulnerability of 4G/5G networks to jamming.
- A physical layer of 4G/5G networks has been created to gather information on the configuration of time-frequency resources used, thus directly implying the potential sequences of interference and interference signals.
- A method for processing signals in along the 4G/5G UE receiving path is proposed, allowing us to implement interference and jamming detection and mitigation functionalities, while maintaining compliance with 3GPP standards. In addition, operational capabilities may be adjusted suit the computational resources available.

The rest of the paper is organized as follows. The state of the art regarding interference, jamming and jamming mitigation techniques is presented in Section 2. Section 3 describes the measurement campaign during which signals from real 4G and 5G NR commercial networks were analyzed in the context of the physical layer's configuration. Section 4 identifies the proposed method used for processing signals along the UE receiving path, intended to detect and mitigate the impact of interference or jamming. Finally, a summary of the research conducted is presented in Section 5.

2. Related Work on Interference and Jamming

This section addresses the main research problem, i.e. interference observed in 4G/5G networks and methods for mitigating its negative impact on signal reception. Detailed parameters of such interference are given as well.

2.1. Interference Detection and Mitigation

The typical method of jamming a radio system is based on the transmission of a wideband signal, with a frequency range equal or close to that of the affected radio interface [5]. Additive white Gaussian noise (AWGN) or quadrature phase shift keying (QPSK) modulated signals, relying on the orthogonal frequency division multiplexing (OFDM) technique, may be used as examples of such jamming signals.

Such a method is usually effective in disrupting radio communication, but is energy-inefficient and easily detectable [6]. Therefore, some papers present jamming detection solutions based on estimating the received signal's power in the analyzed bandwidth, or the power of reference signals. Such an approach is taken, for instance, in [7], [8].

In contrast, in [9], the authors investigate a smart or adaptive jamming method in which the jamming signal is generated based on the configuration of the radio interface to be affected, i.e. as CCI. The problem of CCI cancelation was also investigated in [10], where the authors proposed the least mean squares-based method to reduce its negative impact in a multipath environment.

In [11], the authors proposed a method for minimizing LTE cell-specific reference signal (CRS) interference in cases in which interference is caused by another 5G network operating in the same area. In that paper, the authors estimated channel state information (CSI) based on zero-power resource elements and the CRS allocated according to pattern omitting 5G NR demodulation reference signal (DMRS). This assumption was made to detect interference.

Furthermore, the authors proposed multiple CRS rate matching patterns to mitigate the negative impact on DMRS interference. Despite the proved effectiveness of the solution, this method is not compatible with the physical layer defined by 3GPP and cannot be currently implemented in UE.

In article [12], the authors proposed an interference detection method based on analyzing a physical broadcast channel block of the synchronization signal (SS/PBCH). The authors assumed that DMRS resource components will be jammed by the attacker after the initial cell search procedure and while determining the DMRS pattern. The proposed detection mechanism is based on analyzing the failures in master information block (MIB) decoding, with adaptive threshold estimation, as not all MIBs are correctly decoded in non-jamming conditions.

The approach presented in [12] may be transferred to scenario involving LTE or NB-IoT radio interfaces, with a change to the signal processing methodology that is required due to the independent transmission of primary synchronization signal narrowband primary synchronization signal (PSS/NPSS) signals and broadcast messages.

Research has also been conducted that is not related to specific radio interfaces, but dealing with radio links relying on the OFDM technique to create the radio signal. In paper [13], the authors proposed a method for estimating narrowband interference using the subspace-based approach [14] and analyzing the cyclic prefix of the received signal. In the presented example, the authors proved that it is possible to reduce the bit error rate (BER) when the OFDM signal interferes with a single-tone sinusoidal waveform.

Furthermore, the simulations presented were performed with the signal-to-interference ratio (SIR) in a range of –25 to 25 dB. Despite significant effectiveness of the method, the research needs to be expanded by analyzing other scenarios, for instance those involving radio channels not modeled by AWGN noise only.

2.2. Parameters of Interference

The literature review revealed a few common approaches and main assumptions concerning the parameters of the simulation model used, regardless of the type of radio interference. During CCI analysis, the interference signal was usually of the same form as the impacted interface [15], [16]. However, in some publications, different numerical parameters, such as physical cell identity (PCI), number of antenna ports, or subcarrier spacing [17], [18], were taken into consideration.

In addition to CCI, in other research papers, interface affected narrowband [19] or wideband signals. In [20], a signal with a bandwidth of one physical resource block of 30 kHz was considered. The waveform was created using the OFDM technique, without complying with the 5G NR standard. Additionally, SNR was in the range of 0 to 6 dB. In another group of studies, interfering signals could be classified based on the synchronization of their frequency with the interface. In [5], the authors used an AWGN noise signal with a bandwidth of 1 MHz that was transmitted in a part of the interfered signal's band or swept over its entire frequency band. In papers [12], [21], initial time and frequency synchronization with next generation NodeB (gNB) was performed and parameters of the interfering signal, e.g. center frequency and transmission time, were adjusted.

Furthermore, in addition to analyzing interference and jamming attacks, there is another branch of research focused on

investigating the influence of the channel on the effectiveness of interference detection. This problem was mentioned, for instance, in papers [13], [22], where the authors assumed no channel impact or where the channel was modeled to comply with the AWGN profile. Such a simplification may be sufficient at the initial stage of research; in practice, the channel has to be modeled using profiles consistent with the environment under analysis. Moreover, it should be defined during the analysis whether channels existing between gNb/eNB (evolved NodeB), UE and the source of interference are correlated.

3. Measurement Studies of 4G/5G Radio Interfaces

In this section, the research methodology and the measurements are presented. Then, an analysis of the parameters of the physical layer of commercial and private networks is performed.

3.1. Test bed and Measurement Methodology

The physical layer is highly dependent on the network provider and on the assumptions made during the network planning and further optimization processes. The 3GPP specification contains detailed information on the potential configurations of the physical layer and on the dependencies between various modes of operation. These parameters are determined and interpreted on the UE platform, but are not reported to high-level user applications.

To reveal a detailed network configuration, the TSME6 SDR receiver (scanner) by Rohde&Schwarz was used for testing and measuring [22]. Moreover, using R&S ROMES software, it was possible to receive and analyze 5G NR, LTE and NB-IoT radio interface signals [23]. The block diagram of the test bed is presented in Fig. 1. The TSME6 scanner was connected to a wideband omnidirectional QRC antenna covering the 350 – 6000 MHz band [24]. It was also connected to a GPS antenna to determine the coordinates of the measurement position and enable synchronization of the scanner. The instrument was taken from the ROMES software.

The downlink (DL) signals of 5G NR, LTE, and NB-IoT radio interfaces were recorded at two fixed locations and in different environmental conditions. The Gdańsk University Campus and the suburbs of Gdańsk City were selected to represent urban and suburban cases, respectively. Such a choice was characterized by large and variable number of pieces of UE with different network traffic characteristics, and by various distances to nearest eNBs/gNBs. Moreover, a large variety of cell sizes, numbers and configurations was expected at those locations [25].

At each measurement location, eNBs and gNBs data were recorded for 15 minutes and measurement reports were generated afterwards. The set of measurement data contained detailed information about the configuration of the physical layer, radio interface operation mode, decoded MIB, and (in selected cases) the system information block no. 1 (SIB-1)

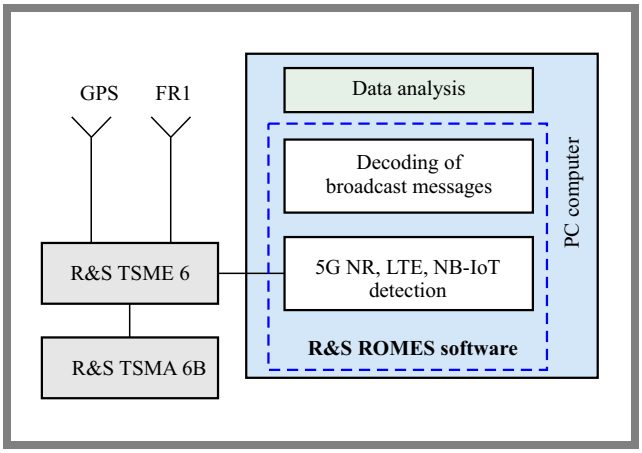

Fig. 1. Block diagram of the test bed used to reveal the parameters of the physical layer and decode messages broadcast using 5G NR, LTE and NB-IoT radio interfaces.

broadcast messages. One should notice that for a 5G NR radio interface operating in the non-standalone (NSA) mode, the SIB1 message cannot be decoded receiving signal only in the n77 band.

3.2. Analysis of 4G/5G Network Configuration

The radio signals transmitted by gNBs and eNBs were recorded in all frequency bands assigned to network operators in Poland [26]. The data was analyzed statistically and numerically in the Matlab environment. The exported data files were filtered to extract numerical parameters for each radio interface and to determine empirical cumulative distribution functions (CDFs) of the signal-to-interference and noise ratio (SINR) in various frequency bands and environments. For the 5G NR radio interface, DMRS SINR presented as the SS/PBCH block is the only element assumed to be present in the DL, regardless of interface load [25], [27].

The 4G LTE radio interface was deployed in six frequency bands (ranging from 0.8 to 2.7 GHz), with resources for the NB-IoT radio interface assigned in the 800 and 900 MHz bands (n8, n20). A detailed configuration of the radio interfaces under investigation is presented in Tab. 1, where the data are grouped for each radio interface, highlighting the key parameters closely related to detection and mitigation of interference.

The 5G network in the investigated environments was configured to operate in the NSA mode. It was discovered that 5G NR radio signals were transmitted in two basic configurations, as co-existing in the LTE bands: n1, n38, n65 in the frequency division duplex (FDD) mode or in a separated n77 frequency band. The sharing of resources with the LTE interface is explained in the following subsection. For the n77 band, the interface operated in the time division duplex (TDD) mode with a channel bandwidth of 100 MHz. Additionally, gNB transmission was carried out by means of smart radio heads with a multiple input multiple output (MIMO) antenna array – a configuration used by operators to form three radio beams, all having the same cell number, in the sector of a given cell. Bearing in mind the main scope

of the research conducted, such an approach to transmitting signal via the interface increases the number of the receiver's processing operations, as it is necessary to separately distinguish each beam and perform a more extensive analysis of the SSB transmission's configuration (transmission period and repetition). Moreover, in each environment, multipath propagation will result in the reception of numerous reflected signals which may unintentionally result in CCI. To visualize this phenomenon, in Fig. 2, the empirical CDFs of DMRS SINR are plotted for different gNBs, the n77 band, and the suburban scenario. Notice that each color in the figure presents one PCI number.

From Fig. 2, one may observe that despite the long distance to the closest gNB (1.2, 1.7, and 2.6 km) [28], it was possible to receive and identify many sectors (or sector beams) from 3 physical gNBs, each with 3 sectors [28]. During this discovery process, the SINR of the DMRS was far below –10 dB for 50% of the cases in the case of most received DL signals, and the estimated received DMRS reference signal receive power (RSRP) was in a range of –125 to –80 dBm.

In contrast, Fig. 3 presents the empirical CDFs of 5G NR DMRS SINR for the urban scenario. In this case, one may notice that the test bed was located, during the measurements, within the beam of one sector of the closest gNB (line-of-sight conditions and distance of 215 m). Therefore, the determined DMRS SINR is higher than 22 dB for 50% of the cases (as shown on the right, purple curve) and the DMRS RSRP reached –69 dBm. Moreover, in Figs. 2 and 3, few empirical distributions are affected by non-Gaussian, rapid changes in the distribution, i.e. step-shaped SINR change. This phenomenon may be caused by the transmission of data on the DL and the adjustment of the gNB's DMRS power, as the measurements were performed in a stationary environment, with no moving objects in its proximity.

From the analysis of the measurement dataset, we concluded that the configuration of the LTE radio interface is highly dependent on the frequency band used by the network. For n8 and n22 (800, 900 MHz) bands, the radio interface was configured to use 1 (1 eNB, 5 MHz DL bandwidth) or 2 antenna ports (regardless of the network operator) for different DL bandwidths (5, 10, and 20 MHz). For higher frequencies, i.e. n1 – 2.1 GHz, n3 – 1.8 GHz, n7 – 2.7 GHz, eNBs transmitted the DL signal using 4 antenna ports.

Another important aspect of the physical layer's configuration is dynamic spectrum sharing (DSS), a service that is supported by up to 50% of the identified eNBs. This functionality was noticed in the operation of eNBs in the n1 band. From the main scope of the research this implies further analysis of LTE downlink signals to classify multicast-broadcast single frequency network (MBSFN) and non-MBSFN radio frames to minimize the possibility of false interference detection caused by overlapping SSB and CRS resource components [25], [27]. It is also worth pointing out that some eNBs transmitted the LTE-M radio interface signal (four eNBs in the suburban environment) that is not considered in the presented research.

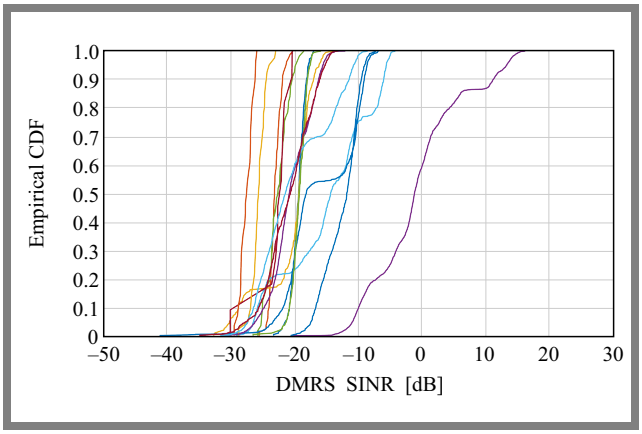

Fig. 2. Empirical CDFs of the DMRS SINR in the 5G NR radio interface for the n77 band in a suburban environment.

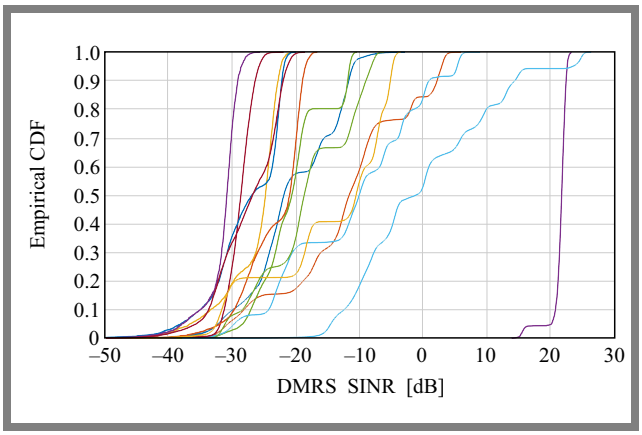

Fig. 3. Empirical CDFs of the DMRS SINR in the 5G NR radio interface for the n77 band in an urban environment.

The CDFs of estimated SINR in the LTE radio interface are presented in Fig. 4. The CDFs shown are representative for measurements performed in the urban environment and eNBs transmitting in the n8 band (900 MHz). In Fig. 4, one may notice that signals were received from four nearby eNB sectors, where SINR was in a range of 6 to 14 dB for more than 50% of cases, with the received signal power equaling up to –41 dBm. Furthermore, 12 other DL signals were received with significantly lower SINR (–19 to –11 dB for 50% of the cases).

In the case of the NB-IoT radio interface, the configuration of the physical layer is not dependent on the type of environment (urban or suburban). For both cases, the radio signal is transmitted by eNBs using one or two antenna ports, both for network operators A and B. The measurement result show a difference in the configuration of the physical layer, as reported in MIB messages. For network operator A, the NB-IoT radio interface is configured to operate in the standalone mode (for both environments). This implies a simplified time-frequency resource grid configuration, without the transmission of LTE CRS symbols. The NB-IoT radio interface of network operator B is configured to operate in the guard band mode, with an additional 2.5 kHz frequency shift. Similarly to previous investigations, the empirical CDFs of SINR for urban environment are presented in Fig. 5.

Tab. 1. Physical parameters of 5G NR, LTE and NB-IoT network interfaces determined during the measurement campaign.

Parameter	Urban	Suburban 1	Suburban 2
5G NR			
Subcarrier spacing [kHz]	15/30		
DMRS mapping	A		
DMRS position	2/3		
Frequency band [GHz]	2.1, 2.6, 3.5, 3.6, 3.7		
Number of PCIs	43	59	86
LTE			
Antenna ports	1, 2, 4	2, 4	
DL bandwidth [MHz]	5, 10, 15, 20		
Frequency band [GHz]	0.8 – 2.7	0.8, 0.9, 1.8, 2.1, 2.6	
Number of PCIs	29	44	71
NB-IoT			
Antenna ports	1, 2		
Frequency band [GHz]	0.8, 0.9	0.8, 0.9, 1.8, 2.2	
Number of PCIs	4	15	20

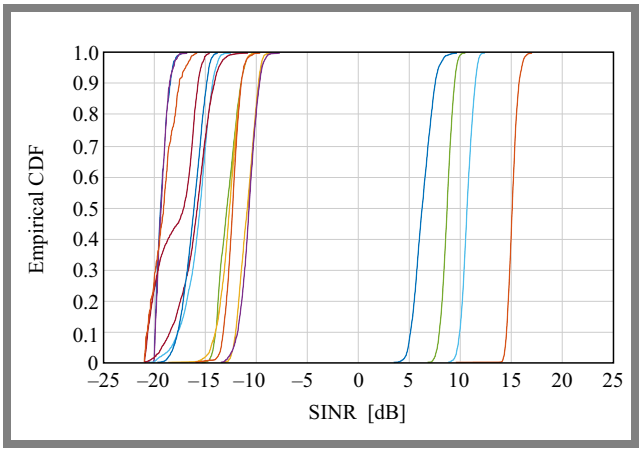

Fig. 4. Empirical SINR CDFs in LTE radio interface for 900 MHz frequency channel (n8 band) in urban environment.

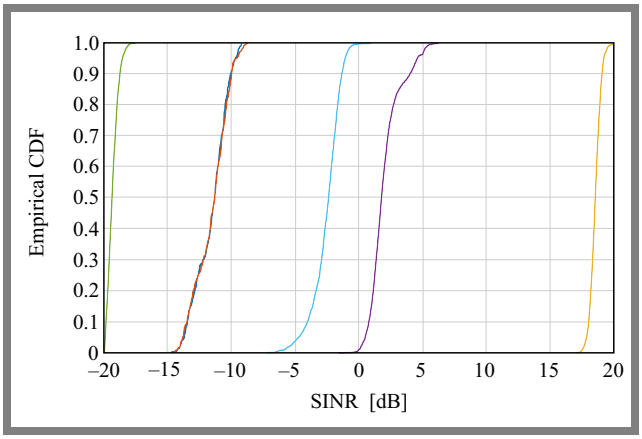

Fig. 5. Empirical SINR CDFs in NB-IoT radio interface for 800 MHz frequency channel (n20 band) in urban environment.

From Fig. 5 one may conclude that while performing the measurements in the urban environment (n20 band), a good quality NB-IoT DL signal (SINR equaling 18.5 dB for 50% of the cases) was received from one nearest eNB. A similar result can be provided for DL in the n8 band (900 MHz). The remaining detected signals come from other sectors, with different azimuths of physical eNBs and eNBs located outside the measurement area.

In Fig. 6, CDFs of SINR for a suburban environment are presented. For this scenario, there are 8 DL NB-IoT signals, with 4 of them potentially causing CCI, as they are identified by the same PCI from the same network operator.

The RSSI of the NB-IoT DL signal in bands n8 and n20 was similar and remained in the range of –71 to –66 dBm.

3.3. Vulnerability of Radio Interfaces to Interference and Jamming

The analysis presented in Subsection 3.2. The physical layer parameters related to 5G NR, LTE, and NB-IoT can be summarized in light of key vulnerabilities to interference, especially with the main scope of this research borne in mind. The first aspect to be mentioned is the simple grid configuration in all radio interfaces analyzed. The interface configuration parameters may be easily disclosed after receiving the synchronization signals and broadcast messages. Afterwards, a jamming signal waveform may be generated to match, e.g., the CRS or DMRS reference symbol allocation in LTE or 5G NR interface.

The NSA operation mode of the 5G NR radio interface can also be classified as a hypothetical vulnerability loophole. UE data transmission in the n77 band is followed by the cell attachment process and by the decoding of control messages

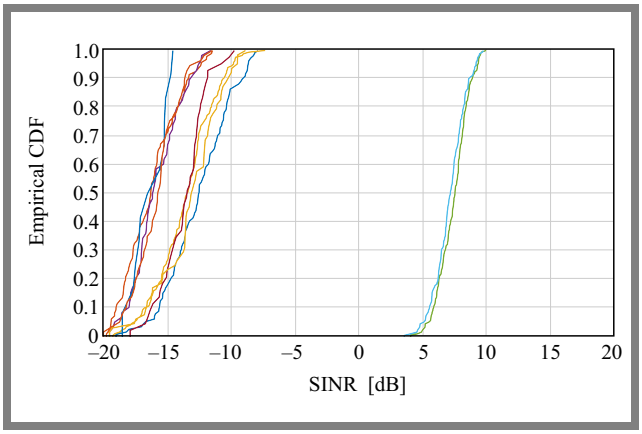

Fig. 6. SINR measured CDFs at NB-IoT radio interface for 800 MHz frequency channel (n20 band) in suburban environment.

that are processed in the lower LTE bands. Thus, one could prepare an attack vector in which only the LTE bands, i.e. the synchronization signals, will be impacted. Therefore, the UE will not be able to connect with the eNB and will further switch to the 5G-NR NSA n77 band. Another threat is linked to the time synchronization of the gNBs and the eNB. In various studies, radio frames of the 4G/5G radio interfaces were synchronized in time [21]. This simplifies the jamming attack, as the jamming signal may be transmitted only at the frequency and time typical of the resource component present in the attacked radio interface. Moreover, it is not necessary to initially synchronize the jammer with gNB/eNB using DL synchronization signals, which simplifies such an attack.

4. Detecting and Mitigating Interference and Jamming

In this section, a concept of a DL signal processing method for 5G NR, LTE, and NB-IoT radio interfaces is introduced for implementation in the receiver in order to detect and mitigate interference. The block diagram of the proposed method is presented in Fig. 7.

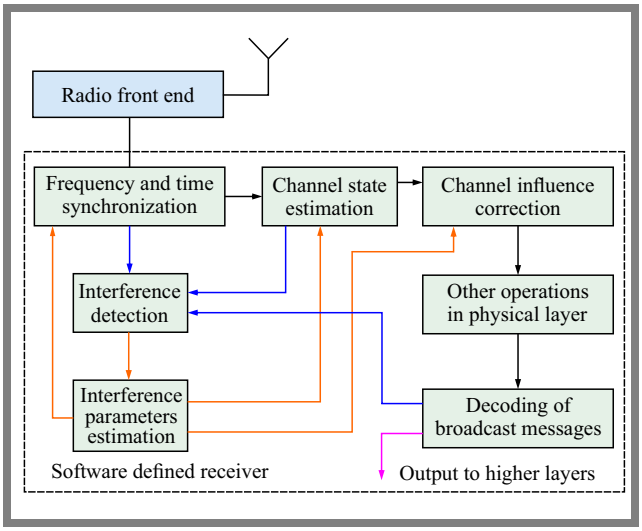

Fig. 7. Block diagram of the proposed DL signal processing method designed to detect and mitigate interference in 5G NR, LTE, NB-IoT radio interfaces.

In general, the concept assumes interception, from the radio transmission, of the investigated radio interface, e.g. using the SDR front end, and initiates an operation performed during the cell attachment process [26]. At this point, it should be mentioned that the methods described in the literature assume complete initial time and frequency synchronization of UE with eNB/gNB or even full UE cell attachment [25], [27]. This assumption may limit the operational abilities of these methods, especially when the networks are highly affected by interfering signals (low value SINR), as described in Subsection 3.2.

On the contrary, the interference detection process should be initiated at the level of physical signal detection, i.e. PSS/SSS for 5G NR, LTE and NPSS/NSSS for NB-IoT. The detection of primary and secondary signals is followed by decoding the broadcast messages, MIB and SIB. Therefore, it implies the second stage of signal analysis in the proposed method. To correctly decode the transmitted messages and transmitted data in other physical channels, it is necessary to estimate channel state parameters and use them to compensate for the negative impact of the channel on the received radio signal.

To make this operation possible, reference symbols are located on the time-frequency resource grid [27]. Their allocation depends on the configuration of the physical layer and on the type of radio interference [27]. There is a possibility that reference signals will be analyzed to detect anomalies, e.g. a phase error characterized by a large degree of variance or constant deviation from the mean over time or over subcarriers.

Moreover, in Fig. 7 the blocks entitled “Interference detection” and “Interference parameters estimation” receive feedback from modules concerned with the estimation of time/frequency synchronization and the once related to channel state parameters. This logical connection between the blocks will allow them to transfer data, e.g. in the form of a resource element grid or OFDM symbols that should be neglected during channel state estimation due to their disruption by interference. This offers the possibility of changing the operating mode of the adaptive receiver, and it will be investigated during future research work. Additionally, the proposed method does not assume the introduction of additional signals to waveforms defined by 3GPP [27] to facilitate the applicability of this method in software-defined UEs.

The main goal of using the proposed method is to shorten the lead time required to obtain the correct time and frequency synchronization of the UE terminal with the eNB/gNB, especially when the radio interfaces are affected by interference signals. Furthermore, increasing the reliability of the cell attachment processes is crucial to minimize computational cost and thus energy consumption, and to ensure the proper operation of all components of the receiving path. Consequently, mitigating the negative influence of the interfering signal may allow to maintain the assumed level of data transmission quality or increase the quality of service (QoS) compared to the scenario in which the proposed approach is not used.

It should also be taken into account that at multiple locations, despite the interference, the NB-IoT terminal will be forced to operate in one frequency channel, due to the lack of alternative communication methods, e.g. other interface operating bands. This situation can also be observed in the case of 5G NR and LTE radio interfaces used in private networks or in suburban areas, where only one eNB/gNB is deployed.

5. Conclusions

It should be mentioned that the presented approach offers only preliminary results of the research and development project pursued.

It clearly identifies a priority configuration which should be investigated further during the development process (Fig. 7) in which a large set of potential physical layer parameters and their combinations will be examined. Additionally, the measurement results serve as reference data for radio channel profile parameters, which will give credibility to further research.

The analysis presented in Subsection 3.2 shows the numerical assessment of DL signal quality, i.e., DMRS SINR and RSSI, which provides information about the state of the interfaces when no intentional jamming signals are transmitted and only signals from other gNBs/eNBs may be classified as CCI. The measurement data, as well as the results presented, will be further investigated during the practical implementation of the proposed DL signal processing method to adjust its sensitivity and minimize the probability of a false alarm.

Acknowledgments

This work was carried out as part of the research and development project entitled "Software-Defined Device for Detecting and Mitigating Inner, Outer System Interference and Hidden Transmissions in 4G-LTE, 5G NR radio interfaces", financed by the National Research and Development Center under the LIDER XIV program, agreement no. LIDER14/0116/2023 signed on 13.02.2024.

References

[1] ETSI, "Evolved Universal Terrestrial Radio Access (E-UTRA) Physical Channels and Modulation", *3GPP 3rd Generation Partnership Project*, 3GPP, TS 36.211, V8.8.0, 2009.

[2] ETSI, "LTE, Evolved Universal Terrestrial Radio Access (E-UTRA) Physical Channels and Modulation", *3GPP 3rd Generation Partnership Project*, 3GPP, TS 36.211, V13.4.0, 2017.

[3] K. Cheon, S. Park, J. Jahng, and J.K. Choi, "Methodology for Network Capacity Assessment of 5G NSA EN-DC Network", *2021 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju Island, South Korea, 2021 (https://doi.org/10.1109/ICTC52510.2021.9620984).

[4] A. Wulandari, M. Hasan, and A. Hikmaturokhman, "Private 5G Network Capacity and Coverage Deployment for Vertical Industries: Case Study in Indonesia", *2022 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT)*, Solo, Indonesia, 2022 (https://doi.org/10.1109/COMNETSAT56033.2022.9994332).

[5] P.J. Varga, T. Wuhrl, S. Gycnyi, M.T. Baross, and A. Nameth, "Jamming Attacks in 5G NR FR1", *2022 IEEE 5th International Conference and Workshop Obuda on Electrical and Power Engineering (CANDO-EPE)*, Budapest, Hungary, 2022 (https://doi.org/10.1109/CANDO-EPE57516.2022.10046381).

[6] P. Skokowski, K. Malon, M. Kryk, K. Maslanka, J.M. Kelner, P. Rajchowski, and J. Magiera, "Practical Trial for Low-Energy Effective Jamming on Private Networks With 5G-NR and NB-IoT Radio Interfaces", IEEE Access vol. 12, pp. 51523–51535, 2024 (https://doi.org/10.1109/ACCESS.2024.3385630).

[7] J. Ming *et al.*, "A 5G Noise and Interference Power Estimation Method Based on the Fusion of Time-Frequency Acquisition Information", *2023 IEEE 11th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*, Chongqing, China, 2023 (https://doi.org/10.1109/ITAIC58329.2023.10408885).

[8] A. Usman, B.A. Salihu, and K.P. Dawar, "Interference Mitigation Using Enhanced Active Power Control Technique for 5G Downlink Transmission of Macro-femto Cellular Networks", *2021 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, Cape Town, South Africa, 2021 (https://doi.org/10.1109/ICECET52533.2021.9698634).

[9] H. Li, X. Zhang, L. Cao, X. Hu, and D. Yang, "Performance Evaluation of Interference Coexistence in Dense Urban Scenario for 5G NR System", *2018 IEEE 4th International Conference on Computer and Communications (ICCC)*, Chengdu, China, 2018 (https://doi.org/10.1109/CompComm.2018.8780903).

[10] S. Xu, J. Xin, S. Xiong, and Z. Sun, "Performance Analysis of CRS Interference Mitigation Algorithm in LTE and NR Coexistence Scenario", *2021 2nd Information Communication Technologies Conference (ICTC)*, Nanjing, China, 2021 (https://doi.org/10.1109/ICTC51749.2021.9441653).

[11] S.D. Wang, H.M. Wang, W. Wang, and V.C.M. Leung, "Detecting Intelligent Jamming on Physical Broadcast Channel in 5G NR", IEEE Communications Letters, vol. 27, no. 5, pp. 1292–1296, 2023 (https://doi.org/10.1109/LCOMM.2023.3260194).

[12] C. de Frein, M. Flanagan, and A. Fagan, "OFDM Narrowband Interference Estimation Using Cyclic Prefix Based Algorithm", *University College Dublin*, 2006 [Online].

[13] P. Stoica, *Spectral Analysis of Signals*, Hoboken: Pearson/Prentice Hall, 2005 (ISBN: 9780131139565).

[14] G. Morillo, U. Roedig, and D. Pesch, "Detecting Targeted Interference in NB-IoT", *2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT)*, Pafos, Cyprus, 2023 (https://doi.org/10.1109/DCOSS-IoT58021.2023.00080).

[15] K. Bechta, J.M. Kelner, C. Ziółkowski, and L. Nowosielski, "Inter-beam Co-channel Downlink and Uplink Interference for 5G New Radio in mm-Wave Bands", *Sensors*, vol. 21, no. 3, art. no. 793, 2021 (https://doi.org/10.3390/s21030793).

[16] J. Wu *et al.*, "CRS Interference Handling on NR and LTE Overlapping Spectrum: Analysis on Performance and Standard Impact", *2022 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*, Sanshui, China, 2022 (https://doi.org/10.1109/ICCCWorkshops55477.2022.9896636).

[17] A. Ghiulai, G. Barb, F. Alexa, and M. Otesteanu, "Downlink Interference Measurement in 4G/5G Systems with Dynamic Spectrum Sharing", *2022 14th International Conference on Communications (COMM)*, Bucharest, Romania, 2022 (https://doi.org/10.1109/COMM54429.2022.9817351).

[18] G. Morillo, U. Roedig, and D. Pesch, "Detecting Targeted Interference in NB-IoT", *2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT)*, Pafos, Cyprus, 2023 (https://doi.org/10.1109/DCOSS-IoT58021.2023.00080).

[19] K. Wesołowski, "A Simple Algorithm for Jamming Detection in OFDM Systems", *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*, Florence, Italy, 2023 (https://doi.org/10.1109/VTC2023-Spring57618.2023.10200416).

[20] J. Magiera and P. Rajchowski, "Intentional Pilot Contamination in 5G NR Uplink", *Przegląd Telekomunikacyjny – Wiadomości Telekomunikacyjne*, vol. 2024, no. 4, 2024 (https://doi.org/10.15199/59.2024.4.43) (in Polish).

[21] C. Shahriar *et al.*, "PHY-layer Resiliency in OFDM Communications: A Tutorial", *IEEE Communications Surveys and Tutorials*, vol. 17, no. 1, pp. 292–314, 2015 (https://doi.org/10.1109/COMST.2014.2349883).

[22] "TSME6 Ultracompact Drive Test Scanner", Rohde & Schwarz, V17.00, 2024.

[23] "ROMES Drive Test Software, Mobile Coverage and QoS Measurements in Mobile Networks", Rohde & Schwarz, v.31.00, 2024.

[24] "Wideband Antenna User Guide", QRC Technologies, v.004, Fredericksburg, VA, USA, 2015.

[25] M. Kottkamp, A. Pandey, A. Roessler, R. Stuhlfauth, and D. Raddino, "5G New Radio Fundamentals, Procedures, Testing Aspects", Munich: Rohde & Schwarz, 450 p., 2019 (ISBN: 9783939837152).

[26] "Information on Spectrum Occupancy in the 420 MHz, 450 MHz, 800 MHz, 900 MHz, 1800 MHz, 2100 MHz, 2600 MHz, 3600 MHz bands", *Office of Electronic Communications*, 2024 (in Polish).

[27] ETSI, "5G, NR, Physical Channels and Modulation", *3GPP 3rd Generation Partnership Project*, 3GPP, TS 38.211, V18.2.0, 2024

[28] "Electromagnetic Field Map", *SI2PEM* [Online] Available: (https://si2pem.gov.pl) (in Polish).

Piotr Rajchowski, Ph.D.
Department of Radio Communication Systems and Networks
https://orcid.org/0000-0002-7736-3526
E-mail: piorajch@pg.edu.pl
Gdansk University of Technology, Gdańsk, Poland
https://pg.edu.pl