Effects of Radio Noise on 5G SA KPIs

Sándor Gyányi, Tibor Wührl, Márk Tamás Baross and Péter János Varga

Óbuda University, Kandó Kálmán Faculty of Electrical Engineering,
Bécsi út 96/b, H-1034 Budapest, Hungary;
gyanyi.sandor@kvk.uni-obuda.hu; wuhrl.tibor@kvk.uni-obuda.hu;
baross.mark@kvk.uni-obuda.hu; varga.peter@kvk.uni-obuda.hu

Abstract: The fifth-generation mobile network standards are designed in such a way that some Key Performance Indicators (KPI) values can show a significant improvement compared to the networks used so far. First, the low latency and its low jitter, as well as the high availability, create the possibility of certain previously impossible applications on mobile network infrastructure. However, a good KPI is not trivial, the whole network must be designed and implemented properly. When planning the network, the KPI expectations must be defined in advance and these must be taken into account in the hardware and configuration settings. This article presents a 5G SA network experiment, which highlights the potential problems of satisfying certain KPIs.

Keywords: 5G SA; KPI; SDR; jamming

1 Introduction

KPIs are a set of important parameters from the point of view of usability and applicability of the mobile network. Each use-case requires certain KPI limit values to be met. For an average mobile user – besides to stable operation – the most important quality indicators are the download and upload speeds, but the low latency is usually not a critical requirement. Only handful real-time applications require low latency, like Voice over IP, live video streaming, virtual reality or remote vehicle control. In the case of a high download speed, the user usually does not even detect packet losses, because they are retransmitted in higher layers. Sometimes the situation is very different. For example, in the case of vehicle control or vehicle safety communication, control and status information usually needs a small amount of data packet. In these applications, not the high data transfer speed in the download and upload direction is important, but the low latency and jitter. A low packet loss rate could also be important, even in a relatively noisy environment [1].

The above reasons caused significant modifications of the 4G LTE radio interface standard and the creation of 5G New Radio (5G NR). The flexible configurability as "numerology" makes the achievement of different KPIs possible, in contrast to the 4G LTE standard, where the low latency was not an important issue before.

A choice of subcarrier spacing provides the possibility of low-latency transmission on the radio channel. Larger subcarrier spacing means shorter OFDM symbol time, which means a lower delay in communication. In addition, the concept of "mini-slot" appeared which also supports the URLLC (Ultra-Reliable Low-Latency Communication) mode.

The following table shows the 5G NR numerology.

Table 1
5G NR numerology

Subcarrier spacing (SCS) [kHz]	**Number of subframes**	**Numers of slots in subframes**	**OFDM symbol/slot**	**Frequncy range**
15	10	1	14	FR1
30	10	2	14	FR1
60	10	4	14	FR1 and FR2
60	10	4	12	FR1 and FR2
120	10	8	14	FR2
240	10	16	14	FR2

In 5G SA networks the most important KPIs are the followings:

- One-way-latency
- Jitter
- Availability
- Reliability
- Packet Loss
- Connection Density
- Area Traffic Capacity
- User Experienced Data Rate
- Guaranteed Data Rate
- Data Volume
- Components Onboarding and Configuration
- Components
- Deployment Time
- Slice Creation/adaption Time
- Time to Scale

- Synchronization Signal Reference Signal Received Power
- CSI Reference Signal Received Power
- SS Reference Signal Received Quality
- CSI Reference Signal Received Quality
- SS Signal to Interference and Noise Ratio
- CSI Signal to Interference and Noise Ratio [2]

2 KPI Testing Environment – NR Configuration

Our test network is a 5G SA system. On the radio interface (5G NR) the communication frequency located in the FR1 band, with a bandwidth of 40 MHz. The spacing between the individual subcarriers is 30 kHz, the corresponding numerology index μ=1. The radio frame has a duration of 10ms, which is divided into 10 subframes. In the case of μ=1, a subframe consists of two slots. In this case, a slot is 0.5ms long and contains 14 symbols.

TDD is the duplexing method implemented on the radio interface of the test network. Figure 1 shows the 5G SA network environment.

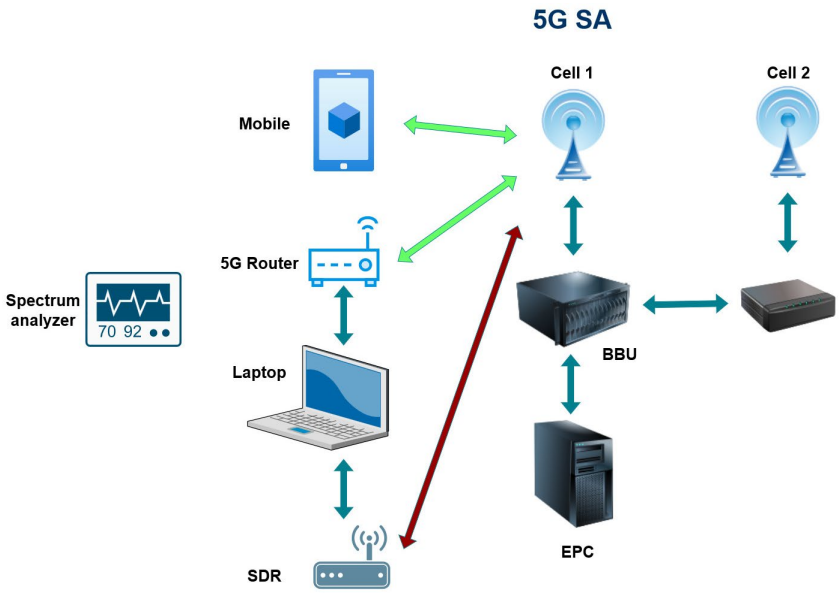

Figure 1
5G SA network environment

The experimental environment consisted of one wired (Ethernet II) and two radio sections, on which the transmission of packets was tested. During the test, a Linux-based computer generated the needed network traffic, sending ICMP “Echo request” packets to the radio direction and in response ICMP “Echo reply” messages sent by the smartphone connected to the 5G network. In this way, the delay of packets can be determined by measuring the time of successful exchange of these messages. This so-called "roundtrip time" therefore cannot be directly used to accurately measure one-way latency, because it also includes the uplink latency of the network, the response time caused by the operating system of the remote device, and the downlink latency. The network bandwidth during the measurement was symmetrical, which means the uplink and downlink delay times were roughly the same. The responding device had sufficient capacity and was not under any other heavy load, so the packet delay time is roughly half the roundtrip time. During the experiments, the primary goal was not to measure the absolute and precise value of the latency, but to examine the possible deterioration of KPI values due to jamming, therefore the approximation does not affect the interpretation of the measured values.

To performing the test, the "ping" command of the Linux system generated the necessary packets and also measured the time elapsed between the sent requests and the reception of the responses. After sending packets for 10 seconds with the speed of 10 packets per second and collecting the roundtrip time values, the evaluation was performed.

During the measurements, the unjammed environment was used as a reference. After that the measurements repeated by using various jamming methods. The value of the delays and packet losses are graphically illustrated in the next chapter [3].

3 Tests

In the tests, two parameters were examined: latency and packet loss caused by too large delay in transport. Packets were delivered through the network via 3 hops: computer to 5G router, 5G router to EPC, EPC to 5G terminal. Figure 2 shows these 3 hops.

The first hop between the laptop and 5G router is a wired network connection. The second and third hops were using wireless connection therefore the jamming affected only these connections.

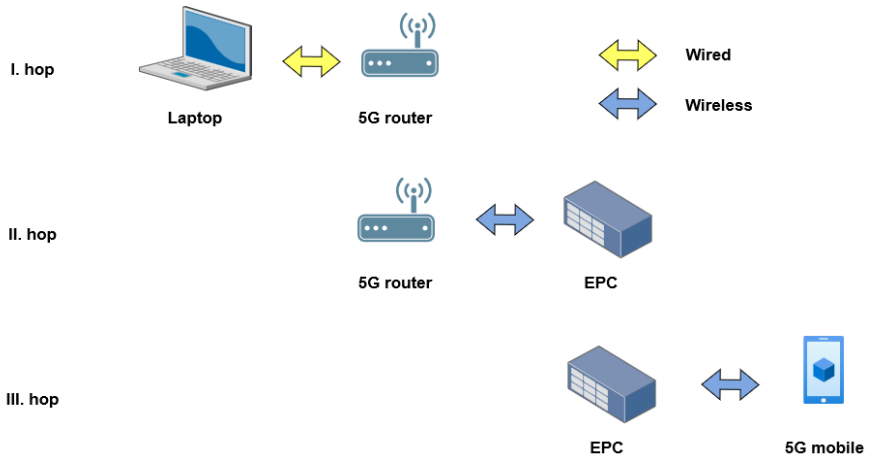

Figure 2
Packet transfer topology

Table 2 shows the test cases and the packet losses experienced during the jamming periods.

Table 2
Test cases

	To 5G router (I.hop)	5G Router to EPC (II.hop)	EPC to 5G mobile (III.hop)
Noiseless environment			
Noise at the beginning of the spectrum			
Noise in the middle of the spectrum		Packet loss	Packet loss
Noise at the end of the spectrum			
Sweep in the spectrum		Packet loss	Packet loss
Noise in full spectrum		Packet loss	Packet loss

Red-colored cells indicate packet losses during the jamming in the tested network sections.

Packet losses are caused by bit errors. In our test system, the NR interface had the highest sensivity to the effects of jamming at the center of the spectrum, which can be traced back to the given numerology (μ=1) and the corresponding Resource Grid configuration. In our test case, the Sychronisation Signal Burst (SS-Burst) is transmitted on the carriers in the middle of the spectrum. Disturbing these signals can cause a higher number of bit errors which are cannot be repaired, this can result dropped data frames.

In the next sections the tests descriptions are described along with the jamming methods and corresponding GNU Radio blocks. For comparison, the spectrum is shown measured by a spectrum analyzer [4].

3.1 Unjammed Radio Environment

Figure 3 shows the radio spectrum of the 5G SA network in an unjammed "clean" environment. That is the reference use-case for comparison, the bandwidth is 40 MHz in all of tests.

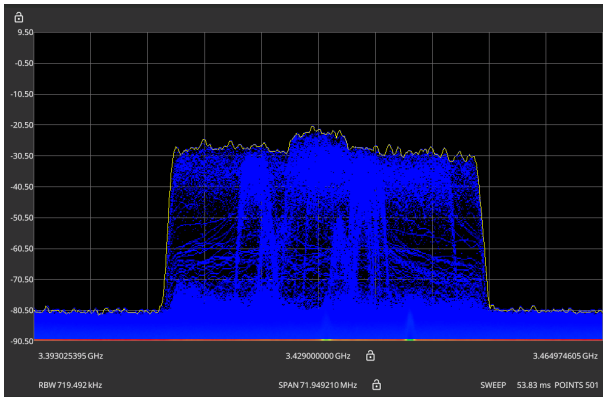

Figure 3
Reference radio spectrum

3.2 Jamming at the Start of 5G SA Band

The jammer device in all test cases was a Software Defined Radio (USRP B210 SDR). Jammer software was implemented in GNU Radio, run by a Dragon OS-based computer. The SDR device was connected to the computer via USB, its antennas placed within 5 meters to the 5G SA antenna [5].

Hyperlog 4060 broadband antenna was used which has 5dBi gain at the jamming frequency spectrum. This parameter is quite stable on the selected frequency range used in the tests. Figure 4 shows the gain diagram.

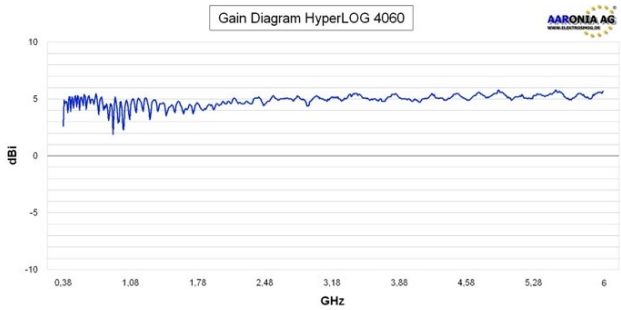

Figure 4
Antenna gain in dBi of HyperLOG broadband antenna [11]

Nominal impedance is 50 Ohm, the connection to the SDR implemented using 50 Ohm common impedance coupling. SMA (f) connectors were used in the test.

Figure 5 shows the horizontal and vertical radiation pattern plots of the antenna. On the applied frequency the antenna azimuth is 45 degrees but it can be different on other frequencies which must be corrected when targeting the jammed receiver. During the tests the antenna was placed around 5 meters from the target.

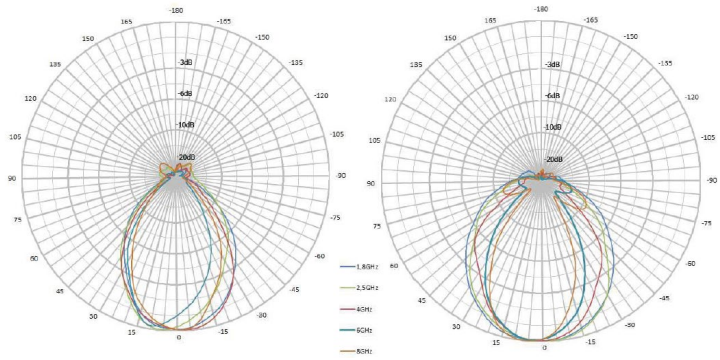

Figure 5
Antenna horizontal and vertical radiation pattern plots of HyperLOG 4060[6]

First test used jamming at a frequency which was near to the start of the 5G SA band. Figure 6 shows the GNU Radio schema for this experiment.

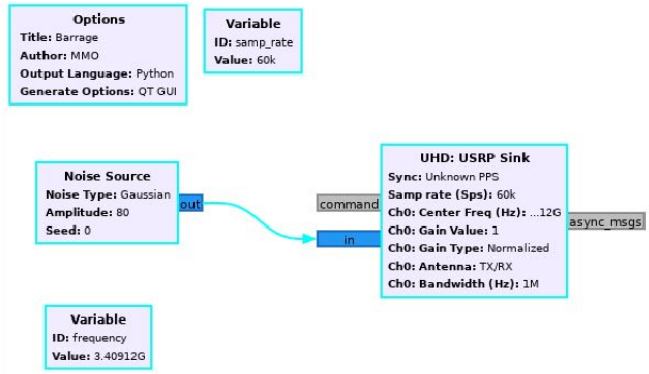

Figure 6
Jamming at 3.40912 GHz (start of the band)

Figure 7 shows the 5G spectrum during the jamming. In this test case no packet loss occurred.

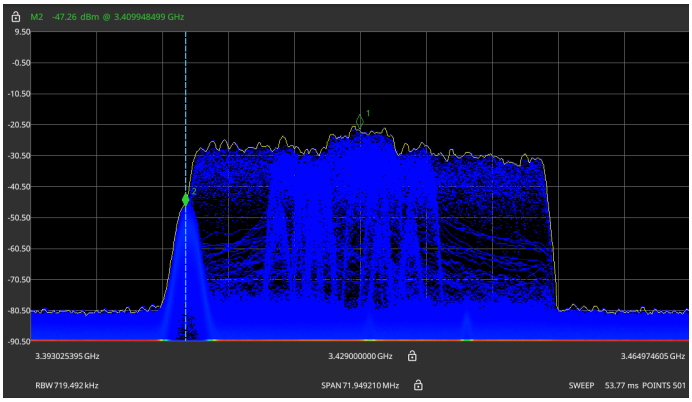

Figure 7
Spectrum during the jamming (start of the band)

3.3 Jamming at the Middle of 5G SA Band

In the next test the jamming was targeted the middle of the 5G SA band. Figure 8 shows the GNU Radio schema for this method.

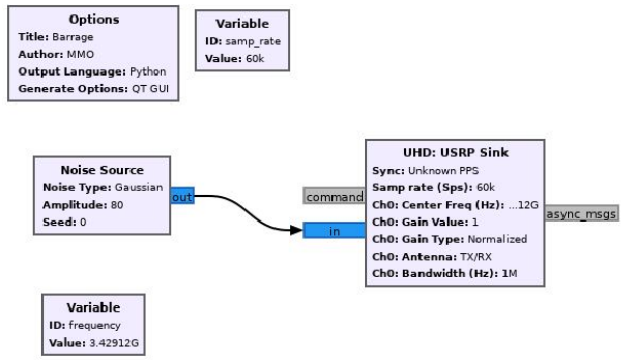

Figure 8
Jamming at 3.42912 GHz (middle of the band)

Figure 9 shows the spectrum during the jamming.

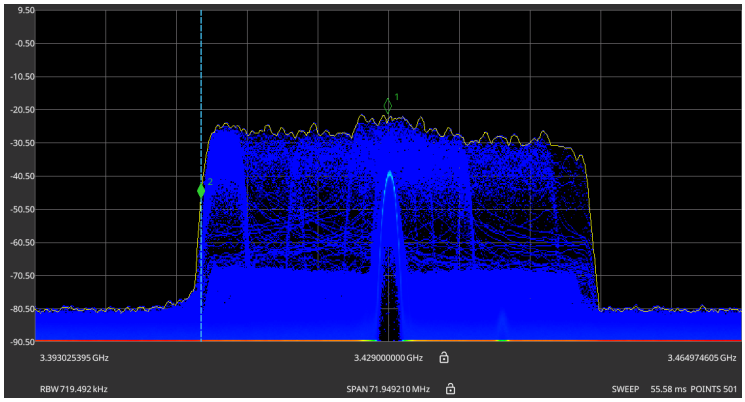

Figure 9
Spectrum during the jamming (middle of the band)

In this test, packet losses occurred in the second and third hop (radio interfaces). The following two graphs indicates the changes in latency and eventually the inevitable packet losses.

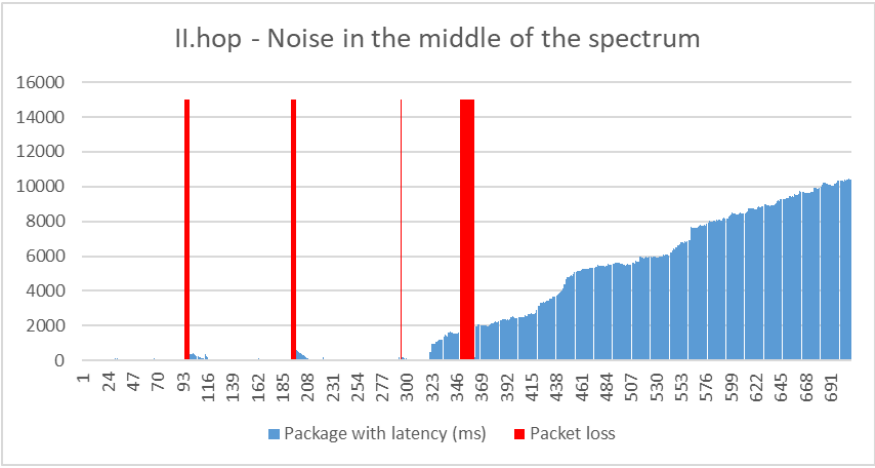

Figure 10
II.hop - Noise in the middle of the spectrum

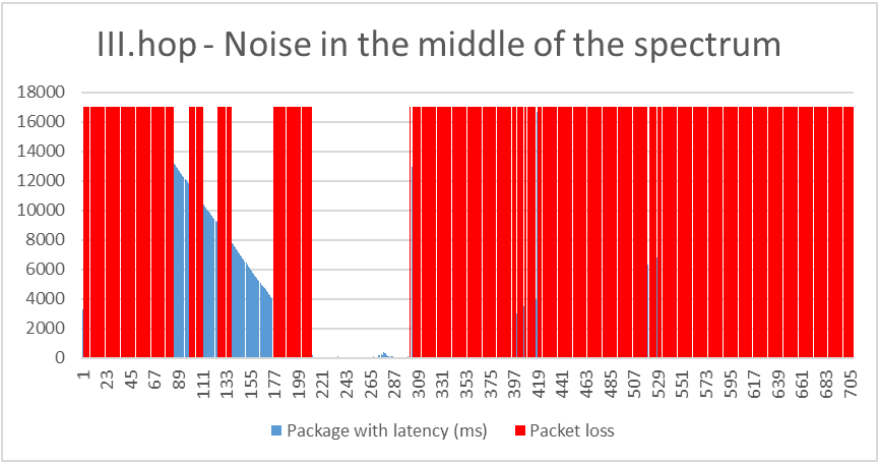

Figure 11
III.hop - Noise in the middle of the spectrum

3.4 Jamming at the End of the 5G SA Band

The next test used jamming targeted the end of the radio band. Figure 12 shows the GNU Radio schema for this method.

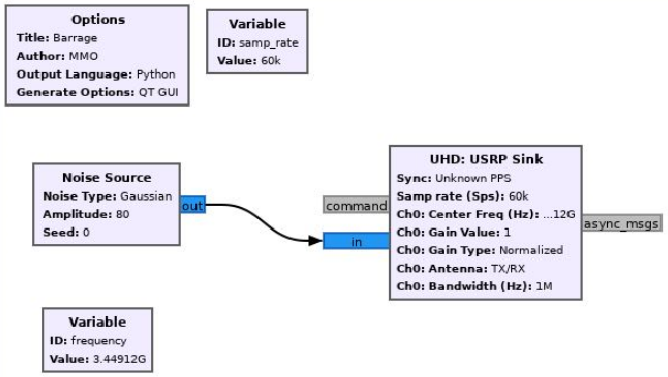

Figure 12
Jamming at 3.44912 GHz (end of band)

Figure 13 shows the spectrum during the jamming. In this test case no packet loss occurred.

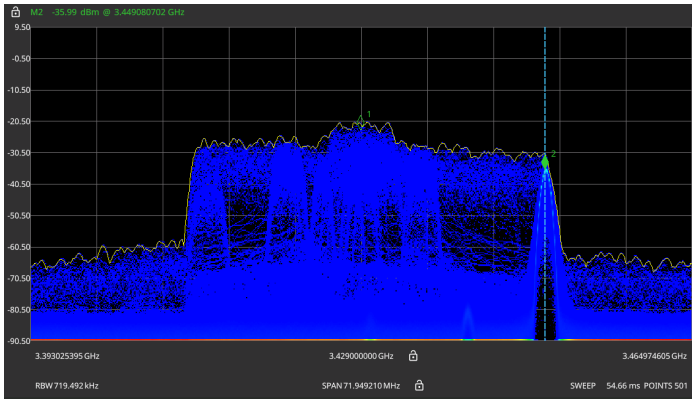

Figure 13
Spectrum during jamming (end of the band)

3.5 Sweep Jamming in the Whole 5G SA Band

In this test a sweeping jamming method was used in the whole 40 MHz 5G SA band. During this test, the jammer used the generated noise for a few milliseconds in a certain frequency, and changed this frequency afterward. Figure 14 shows the GNU Radio schema for this method [7, 8].

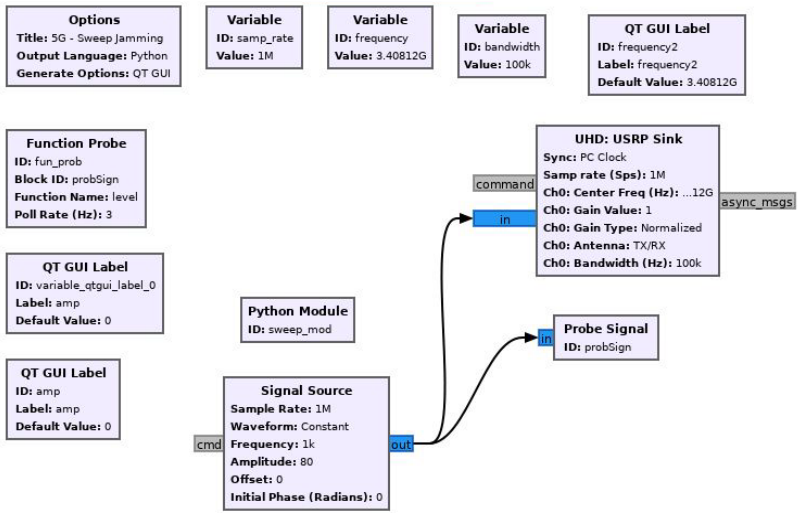

Figure 14
Sweep jamming method

Figure 15 shows the spectrum during this jamming.

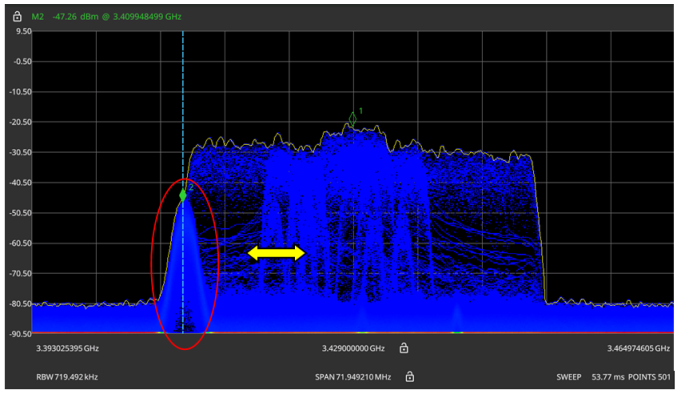

Figure 15
Snapshot of the sweep jamming

In this test packet losses occurred in the second and third hops. The next two graphs indicate the latency and packet loss.

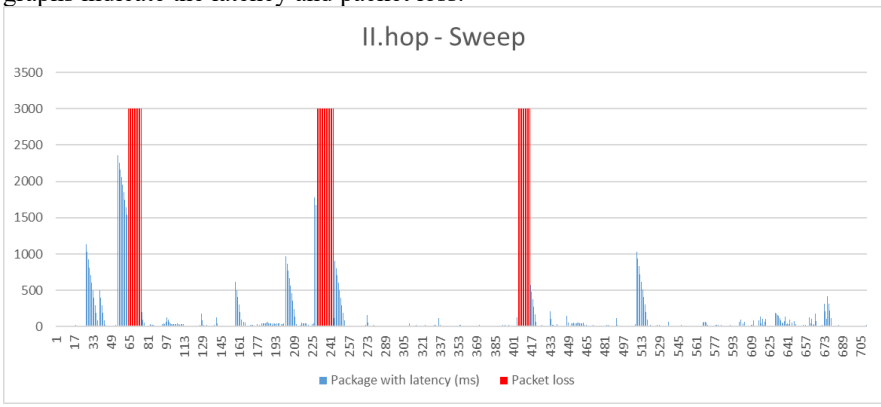

Figure 16
II.hop – Sweep noise

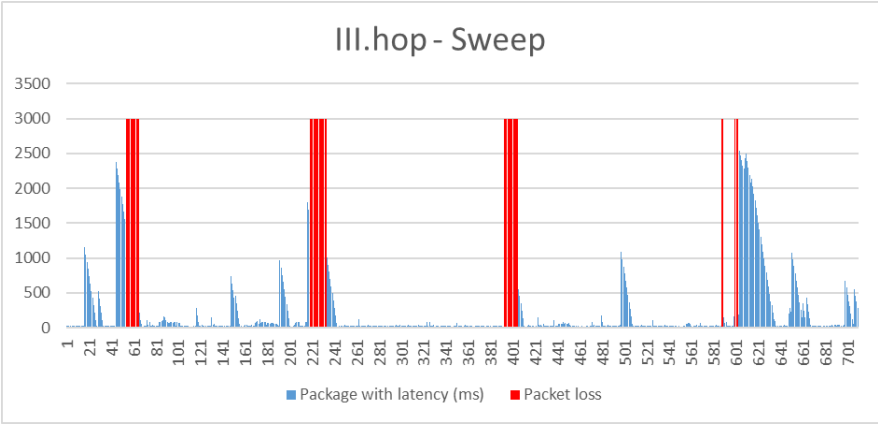

Figure 17
III.hop – Sweep noise

3.6 Jamming the Whole 5G SA Band

Preliminary tests clearly indicated that this method would be the most effective. In this test case the jammer generated noise in the whole 40 MHz band [9].

Figure 18 shows the GNU Radio schema for this method.

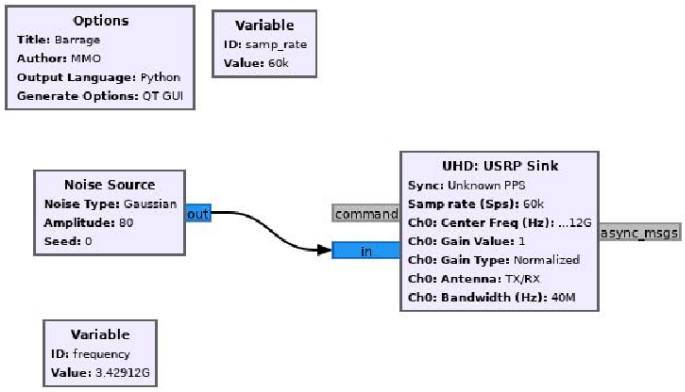

Figure 18
III.hop – Sweep noise

Figure 19 shows the spectrum during this jamming.

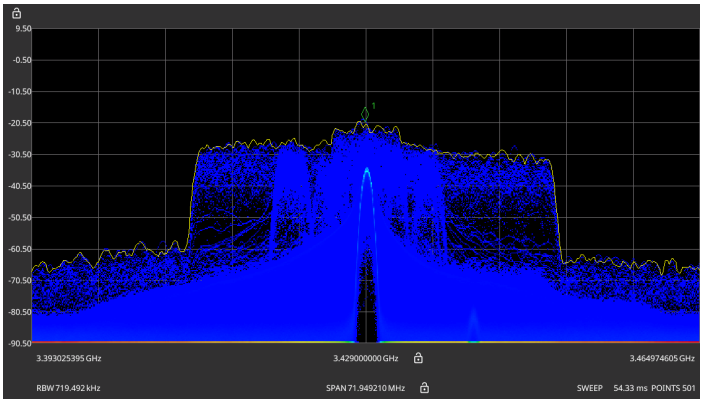

Figure 19
Spectrum of the jamming in the whole 5G SA band

Of course, in this test the packet losses occurred in the second and third hops too. When jamming is ongoing, it affects both radio sections, therefore, when packet loss occurs in the second hop, the third hop is also affected. In the third hop the jamming effect probability is higher because the third hop uses two radio sections. The following two graphs show the latency and packet loss tendency [10, 11].

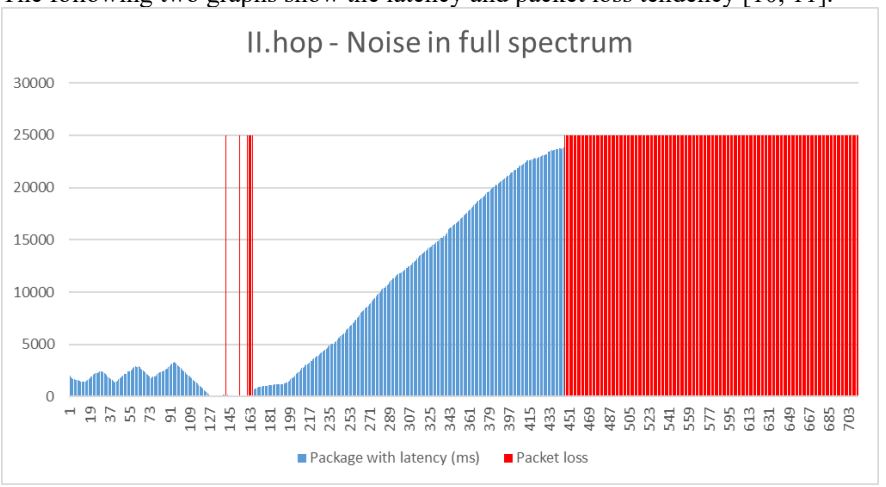

Figure 20
II.hop - Noise in full spectrum

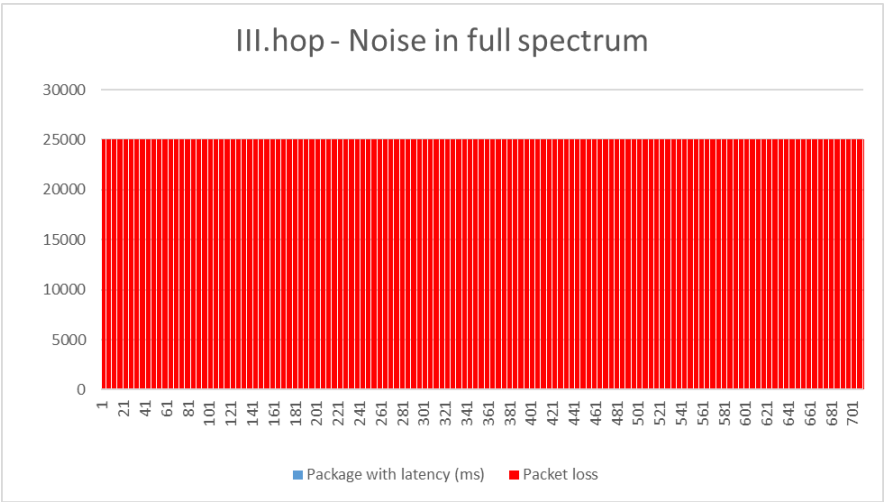

Figure 21
III.hop - Noise in full spectrum

Conclusions

In this experiment, multiple jamming methods were used to examine how the noise in the radio band affects the network communication. The radio communication is quite robust but certain noise types could cause problems. These problems mean increased latency and in some cases packet losses.

The radio interface can prevent the effects of narrow-band noises at both ends of the band but wide-band or hopping frequency noises cause a problem in low-level transmission. These problems can be sensed in the upper-level data structures and eventually cause packet losses. These effects cause significant increase in latency and can prevent the proper working of certain real-time applications.

Table 3
Packet losses in the examined network sections in percentage

	To 5G router (I.hop)	5G Router to EPC (II.hop)	EPC to 5G mobile (III.hop)
Noiseless environment	0%	0%	0%
Noise at the beginning of the spectrum	0%	0%	0%
Noise in the middle of the spectrum	0%	16,5%	82,0%
Noise at the end of the spectrum	0%	0%	0%
Sweep in the spectrum	0%	5,3%	6,3%
Noise in full spectrum	0%	35,4%	100%

In the article, only the KPI of latency and packet loss was evaluated with the help of the radio channel jamming. In the future, it is also possible to carry out tests of other KPIs with other attacking methods.

Acknowledgement

The research was supported by the Ministry of Culture and Innovation NRDI Office within the framework of the Infocommunication and Information Technology National Laboratory Program.

References

[1] G. Soós, D. Ficzere, P. Varga and Z. Szalay, "Practical 5G KPI Measurement Results on a Non-Standalone Architecture," NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary (2020) pp. 1-5, doi: 10.1109/NOMS47738.2020.9110457

[2] 5G PPP White Paper, "KPIs Measurement Tools – From KPI definition to KPI validation enablement", TMV WG (2023) https://doi.org/10.5281/zenodo.7683903

[3] T. Wührl, P. J. Varga, S. Gyányi, M. Baross and A. Németh, 5G RAN synchronization vulnerability IEEE 20th Jubilee International Symposium on Intelligent Systems and Informatics (SISY 2022) Subotica, Serbia, IEEE (2022) 457 p. pp. 139-144, 6 p.

[4] M. Bogdanoski, T. Shuminoski, M. Hadji-Janev, A. Risteski and T. Janevski, Future 5G Mobile Broadband Networks Using Cloud-based Services with Advanced Security and QoS Framework, Acta Polytechnica Hungarica, Vol. 17, No. 10 (2020)

[5] Ettus Research, GNURadio, Online, Available: https://www.ettus.com/sdr-software/gnu-radio/ [Accessed: 05.01.2024]

[6] AARONIA, Logper Antennas – HYPERLOG catalogue, Online, Available: https://aaronia.com/en/breitband-messantennen-hyperlog4060 [Accessed: 05.01.2024]

[7] Zs. Haig, Zs. Illési and P. J. Varga, Possibilities of Electronic Jamming of WLAN Networks in the Physical Layer, HADMÉRNÖK 17: 3 pp. 133-152, 20 p. (2022)

[8] M. Bogdanoski, T. Shuminoski, M. Hadji-Janev, A. Risteski and T. Janevski, Future 5G Mobile Broadband Networks Using Cloud-based Services with Advanced Security and QoS Framework, Acta Polytechnica Hungarica, Vol. 17, No. 10 (2020)

[9] P. J. Varga, T. Wührl, S. Gyányi, M. T. Baross and A. Németh, "Jamming Attacks in 5G NR FR1," 2022 IEEE 5th International Conference and Workshop Óbuda on Electrical and Power Engineering (CANDO-EPE), Budapest, Hungary (2022) pp. 000175-000180, doi: 10.1109/CANDO-EPE57516.2022.10046381

[10] T. Wührl, Pilot Signal Removal, Digital Signal Processing Algorithm and it's Practical Implementation, Acta Polytechnica Hungarica, Vol. 20, No. 7, (2023)

[11] P. P. Bakucz and J. Z. Szabó, Determining the Embedded Key Performance Indicator (KPI), based on a Fuzzy FxLMS Algorithm, Acta Polytechnica Hungarica, Vol. 18, No. 9 (2021)