IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 6 March 2024, accepted 24 March 2024, date of publication 5 April 2024, date of current version 16 April 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3385630

APPLIED RESEARCH

Practical Trial for Low-Energy Effective Jamming on Private Networks With 5G-NR and NB-IoT Radio Interfaces

PAWEŁ SKOKOWSKI[1], **KRZYSZTOF MALON**[1], **MICHAŁ KRYK**[1], **KRZYSZTOF MAŚLANKA**[1], **JAN M. KELNER**[1], **(Member, IEEE), PIOTR RAJCHOWSKI**[2], **(Member, IEEE), AND JAROSŁAW MAGIERA**[2]

[1]Faculty of Electronics, Military University of Technology, 00-908 Warsaw, Poland
[2]Faculty of Electronics, Telecommunications and Informatics, Gdańsk University of Technology, 80-233 Gdańsk, Poland

Corresponding author: Paweł Skokowski (pawel.skokowski@wat.edu.pl)

This work was financed by the Military University of Technology under project no. UGB/22-748/2024/WAT on "Transmission properties of radio wave propagation environments in military applications."

ABSTRACT Fourth-generation (4G) mobile networks are successively replaced by fifth-generation (5G) ones, based on the new releases of the 3rd Generation Partnership Project (3GPP) standard. 5G generation is dedicated to civilian users and the conducted analytical work shows that it has numerous technological gaps that prevent its direct implementation in military communications systems. However, the recent armed world conflicts showed that closed or public mobile networks are willingly used by soldiers for both private and business communications, and to conduct defensive and offensive operations as well. From the military operation viewpoint, jamming both civil and military systems is one of the essential elements of electronic warfare. This paper focuses on the practical trial of low-energy and smart jamming on a 5G private network using narrowband signals, which facilitates the reduction of the available throughput, e.g. in the time division duplex - uplink (TDD-UL) by 99%, or by 82% in the frequency division duplex - downlink (FDD-DL). This type of jamming also allows for reaching up to 25 dB of energy gain comparing to barrage jamming. The authors moreover investigated jamming the Narrowband IoT radio interface using synchronized, selective jamming. The goal was to propose energy efficient methods that will allow the jammers to work longer and be mounted on a small unmanned aerial vehicle (UAV) that can operate near the gNB. The generation of low-power jamming signals in the gNB vicinity successfully hinders detecting the jammer by the enemy's electronic reconnaissance systems. The proposed solutions are compared with the test results for other types of jamming methods.

INDEX TERMS Electronic warfare, low-energy jamming, narrowband jamming, NB-IoT, 5G private network, smart jamming.

I. INTRODUCTION

In In the large majority of developed countries, the Long Term Evolution (LTE) with its enhancements LTE Advanced (LTE-A) and LTE-A Pro have become the standard for mobile communication. In comparison, older solutions based on the 2nd (2G) and 3rd generation (3G) technologies are slowly being withdrawn from the market. Mobile network operators (MNOs) resign from older systems and use released radio resources for newer standards networks instead. At the same time, in mobile networks, we witness a technological revolution related to the implementation of the 5th generation (5G) New Radio (NR) standard developed by the 3rd Generation Partnership Project (3GPP). Release 18 is being finalized, and the 5G Advanced standard specification will have been defined by 3GPP by 2028. Increasing the system efficiency in many areas involving LTE is one of the main goals set for 5G. In particular, the following are envisaged [1]:

The associate editor coordinating the review of this manuscript and approving it for publication was Wei-Wen Hu.

- improving the quality of service (QoS) by increasing throughput and capacity (i.e. enhanced mobile broadban d (eMBB) scenario),
- increasing number and density of the supported devices (i.e. massive machine type communications (mMTC) scenario, massive Internet of Things (IoT), ultra-dense network (UDN)),
- assuring reliability and reducing latency (i.e. ultra-reliable and low latency communications (URLLC) scenario, missioncritical applications).

Behind the success of 5G there are many modern radio and network technologies that have been developed for many years. For example, new modulation schemes or multiple access methods increase the spectral efficiency of the transmitted signals. Furthermore, using energy harvesting or green communication technologies improves the energy efficiency of 5G networks and reduces the energy consumption there [2]. On the other hand, implementing interference mitigation techniques increases the reliability and resilience of the 5G system which is targeted at unintentional interference [3]. Unfortunately, the civilian 5G standard is not designed to be resistant to jamming (intentional interference).

The enormous attractiveness and effectiveness of the 5G system utilizing modern technologies is recognized by various vendors of military communication equipment and international defence bodies such as European Defence Agency (EDA) [4], North Atlantic Treaty Organisation (NATO) Communications and Information Agency (NCIA) [5], NATO Science and Technology Organisation (NATO STO) [6]. Different use cases of the 5G technologies (including the Narrowband Internet of Things (NB-IoT) radio interface) are considered for military applications. These scenarios often use the private 5G network concept that operates in spatially limited areas, e.g. in large or small operational deployable headquarters, naval task force, etc. [5]. On the other hand, the analysis of the civilian 3GPP standard indicates numerous technological gaps that ought to be fixed before it can be used for military purposes [4]. A crucial issue is to increase its resilience to jamming which may occur during military operations [6], [7], [8].

A. RELATED WORKS

The classic definition of jamming describes it as intentional interference affecting radio signals, communication systems, or electronic devices, which is usually carried out by emitting radio frequency (RF) signals in the same frequency band as the attacked communication radio interface, aiming to overwhelm, block, or distort these signals. The primary purpose of jamming is to disrupt the regular operation of communication systems, radar systems, or other electronic devices. This technique is commonly employed in military, electronic warfare or security contexts [9], [10], [11]. On the other hand, the development of cybersecurity in the last decade has resulted in the perception of jamming as one of the types of cybersecurity attacks [12], [13]. This is also due to the blurring of boundaries between electronic and information warfare [14].

Until recently, the classical jamming approach was developed and considered in the context of military communication and radar systems. With the progress of mobile networks, the development of jamming techniques also applies to civilian and commercial systems. This is due to the fact that they are widely used for auxiliary communication in conflict areas. A decade earlier, the military doctrine assumed destruction or causing substantial damage to telecommunications infrastructure. Recent armed conflicts have shown that both their sides want to keep this infrastructure out of the occupied territory [15]. Therefore, effective methods for jamming cellular systems without causing permanent damage are indispensable. On the other hand, 5G technologies are being seriously considered for implementation in future military communication systems due to the benefits they offer [16], [17]. Therefore, developing 5G jamming techniques is crucial from the viewpoint of the potential 5G application in military operations [5], [6], [18].

The first works in the field of 5G jamming focused mainly on theoretical analysis [19], [20], [21]. This results from the signal structure of the 5G-NR standard and jamming techniques used in LTE and older generation networks, what can be seen in the surveys of 5G jamming methods [6], [7], [8], [22], [23], and this is additionally consistent with the classification of the techniques used in LTE [24], [25], [26], [27]. This convergence also results from the similarities in the physical layer, mostly due to the application of OFDM (Orthogonal Frequency Division Multiplexing) technique in both generations of mobile networks. On the other hand, the next 5G-NR generation introduces new technologies in the network and radio interface such as new modulations and coding schemes, and subcarrier spacing. A characteristic feature of LTE was the spread of Multiple-Input-Multiple-Output (MIMO) method [27], whereas massive MIMO and beamforming [28], [29] began to play an essential role in 5G-NR.

With greater availability of 5G equipment, more works present the practical implementation of jamming techniques, e.g. [30], [31], [32], [33], and [34]. The Norwegian Armed Forces plan to use 5G-NR connectivity in military operations carried out in congested urban environments, including electronic warfare applications. Hence, the Norwegian Defense Research Establishment (FFI) assessed technological gaps in 5G resistance to jamming and conducted a comprehensive study including a practical jamming experiment targeting the commercial 5G-NR system operating in the 3.6 GHz frequency band [32], [34]. The tests were conducted on a commercial 5G network operating in Non-Standalone (NSA) mode with Time Division Duplex (TDD). The research has shown weaknesses in the 3GPP standard, especially in the uplink (UL) signal due to limited user terminal transmit power. FFI has defined the threshold for jamming intensity and developed a model to estimate the distance and the jammer output power required for successful attacks. Additionally, practical countermeasures to enhance the robustness of 5G-NR radio interface, especially in the uplink, have been proposed in the report [32].

Similar studies of the resistance of the 5G TDD system operating in the 3.6 GHz band to jamming, but within a narrower scope, are presented in [30], [31], and [33]. In these cases, the tests concerned a 5G private network in the Standalone (SA) mode of operation. In [33], the authors used GNU Radio software and a SDR (Software Defined Radio) platform, USRP (Universal Software Radio Peripheral) B210 as a jammer to disrupt the 5G SA network. Three types of techniques, i.e. barrage, spot, and sweep jamming were tested. In [31], SDRs were used for jamming and emulating the gNB base station and the user equipment (UE). The authors examined the susceptibility of the 5G Physical Uplink Shared Channel (PUSCH) to a smart jamming attack as well as the impact of such an attack on the UE effective throughput. In [10] and [30], the authors additionally proposed mounting a jammer on an Unmanned Aerial Vehicle (UAV). This approach increases the jammer's mobility and allows it to be placed close to the gNB, making it more difficult to be detected and located.

The advancement of jamming techniques has spurred the search for methods to detect, avoid, and cancel both interference and jamming [32]. The use of 5G-NR technologies improves the network's resistance to unintentional interference. However, in the case of intentional interference, this is usually insufficient. Hence, novel jamming detection [35], [36], [37], [38] and mitigation [39], [40] techniques are also being researched and developed in relation to the 5G-NR standard. In [37], the author proposed a new metric for jamming detection in OFDM-based systems which may be used in both the time and frequency domains, and be implemented separately in each physical resource block. The effectiveness of the developed algorithm was estimated based on simulation tests. In another paper, [35], the authors highlight the benefits of using the Open Radio Access Network (O-RAN) architecture. It is suitable for detecting jamming events due to the open interfaces and the ability to analyze wireless traffic metrics. In this case, a statistical method is used for downlink jamming detection utilizing the link quality reports provided by the UE. The effectiveness of the proposed solution was verified through simulations. In [38], a novel method of detecting targeted interference in a NB-IoT network is proposed. The statistical anomaly detector algorithm is based on the analysis of the network performance data collected at the UE which aids reasoning about the current interference situation. The authors demonstrate that the detector can distinguish jamming attacks from unintentional interference occurring in cellular networks. Moreover, in [36], the authors propose exploitation of the principal direction of Physical Broadcast Channel (PBCH) demodulation reference signal space in order to detect PBCH intelligent jamming on the user side. This approach results from the fact that PBCH is used in smart jamming, e.g. [6], [22], and [7]. The effectiveness of this detection method is confirmed and assessed based on numerical analysis.

Artificial intelligence algorithms such as machine learning (ML) or deep learning (DeL) are some of the trends in the development of 5G-NR and beyond mobile networks. These methods can also be adopted in interference mitigation techniques. An example is [40], where a federated deep reinforcement learning (DRL)-based anti-jamming technique for two-tier 5G heterogeneous networks (HetNets) has been proposed. The presented concept involves a joint optimization problem of beamforming and power allocation at femto-stations (FSs) to improve the throughput for femto-users (FU), simultaneously mitigating the negative influence of a multi-antenna jammer. In another publication, [39], the authors explore the improvement of the throughput for a primary user (PU) facing a random jamming attack near the receiver within a cognitive radio network. They suggest a cooperative spectrum-sharing approach, involving a PU and a secondary user (SU) with limited energy resources, which harvests non-RF energy. The location of the SU is optimized to maximize the PU throughput. Notably, this approach operates under the assumption of no prior knowledge regarding the parameters controlling the random behaviour of the jammer, the energy harvesting process, and the sensing system. Bayesian reinforcement learning (BRL) is employed to both learn the unknown parameters and to optimize the PU decisions concurrently, which was proven to be an adaptive approach.

Our experimental studies presented in this paper are consistent with the contemporary trend in research on jamming topics, showing the results of empirical tests of selective and smart jamming on a private 5G-NR network and on the NB-IoT radio interface.

During the research, the authors used narrowband jamming signals in several variants, which is more subtle than burst jamming. During the real tests, it was possible to obtain high jamming efficiency, even up to 99% for 5G-TDD-UL or 82% for 5G-FDD-DL, compared to the mentioned burst jamming (84%). Moreover, the proposed jamming methodology is suitable for jamming only the selected subcarriers in the OFDM symbol, while barrage jamming is spread over all of them.

The selective (smart) jamming scenario was investigated for the second analyzed radio interface, NB-IoT. In this case, with a 3 dB jamming-to-signal peak power ratio and the interference focused solely on pilot resources, it was possible to substantially degrade the accuracy of the channel estimation. As a result, the percentage of successfully decoded MIBs (Master Information Blocks) was reduced to less than 50%.

The proposed technique is characterized by greater energy efficiency while blocking or significantly disturbing the connection between the UE and the 5G gNB base station. This approach is in line with the green communication trend and energy savings allow the jammer to work longer and be implemented on a small UAV, which prevents an uplink connection, when placed near the gNB, or a downlink connection, when placed close to the UE. Moreover, generation of low-power jamming signals in the DL frequency band in the gNB vicinity makes the jammer detection process challenging, also with the electronic reconnaissance systems. The proposed solution was compared with the test results for other types of jamming. This practical trial testifies to the paper's originality because most of the works in the literature are focused on theoretical or simulation considerations [6], [7], [8], [41].

The main contributions of this paper can be summarized as follows:

- The authors tested the influence of narrowband and barrage jamming on a 5G-NR SA private network based on the O-RAN concept;
- The efficiency of different jamming techniques was additionally studied on the NB-IoT radio interface, which is also treated as part of the next generation networks;
- The adopted energy efficient and smart jamming methods were proposed as solutions suitable for implementation on the UAV platform equipped with the SDR radio front-end.

The rest of the paper is organized as follows. The architecture of a 5G private network and the time-frequency structure of 5G and NB-IoT signals are shortly described in Sections II and III respectively. The low-energy effective jamming technique based on a 5G physical layer structure is explained in Section IV. Section V presents the jamming operational scenario, whereas the testbed and exemplary results of the practical trial are shown in Section VI. Finally, the research studies are completed with conclusions in Section VII.

II. 5G PRIVATE NETWORK

A. THE MAIN CONCEPT

The evolution of cellular networks can be perceived as a significant change in the set of services, the physical layer, and technical realization [42], [43]. Over the last years, 4G-LTE (Long Term Evolution) networks overlapped with the rapid growth of the 5G-NR (New Radio) concept. The main change in the physical realization of the new and next generation cellular networks can be seen in the software-defined elements in the network core and the RAN (Radio Access Network) part. Currently, many companies offer software packages for those 5G-Core and RAN components that are easily deployable and compliant with the 3GPP technical specification [44], [45], [46]. They can be purchased by any customer deploying a private or an R&D (Research and Development) 5G network. At this point it is worth mentioning that not all the implementations are capable of serving as large-scale networks, with many gNBs, but they are fully functional for stationary company networks, nomadic networks for critical communication, and for military applications [47], [48]. In this point it is worth mentioning that analogical software realization of the network core and RAN can be met for the 4G-LTE/NB-IoT networks.

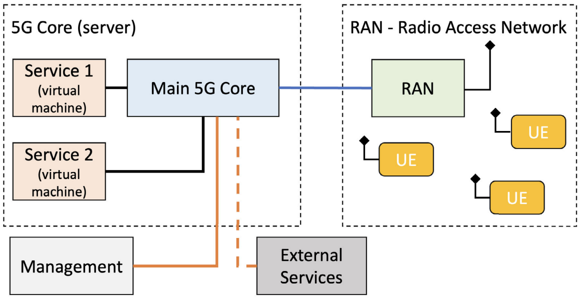

5G Core (server)
Service 1 (virtual machine)
Service 2 (virtual machine)
Main 5G Core
RAN - Radio Access Network
RAN
UE
UE
UE
Management
External Services

FIGURE 1. Block diagram of a 5G private network.

B. PRACTICAL REALISATION OF A 5G PRIVATE NETWORK

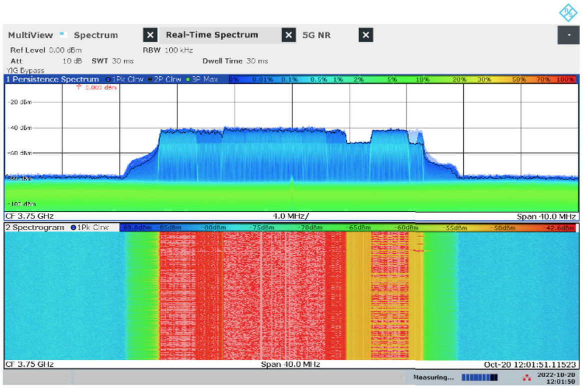
In Fig. 1, a block diagram of commercially available private networks is presented. In the figure two main components can be distinguished: the 5G-Core and the RAN part. The core is deployed on an industrial-class server as a software package based on the virtual machine and container structure. The connection between the core and the RAN utilizes a standard Ethernet link, which provides flexibility in selecting the radio heads. In the presented solution, the RAN component is implemented using SDR technology whereas the UL and downlink (DL) signals are received and transmitted by the wideband radio front-end and further processed by the software. In this case, the RAN was configured to operate in N7 and N77 bands.

As it has already been mentioned, the concept of easily deployable and flexible 5G private networks is usually based on virtual machines and the container structure. This approach has been adopted in the presented example (Fig. 1). This private 5G network is designed to serve, for instance, as a dispatch network. Thus, nontypical services ought to be implemented, like instant voice communication between the users. In this network implementation, the PTT (Push to Talk) service was realized as a virtual machine operating in the 5G-Core. From the user operation level, it is seen as an application that facilitates realisation of instant calls without the need to select the UE phone number. The presented service implies one of the major differences between a 5G private network and the commercial ones, which is the traffic scheme. When a 5G private network is used mainly for speech communication with a low duty cycle or short data transmission, most of the radio resources in the DL and UL are unoccupied. As the activity we can identify mainly the synchronization signals, broadcast messages, and RRC (Radio Resource Control) messages [42], [43].

III. TIME-FREQUENCY STRUCTURE OF THE 5G AND NB-IOT SIGNALS

A. 5G-NR RADIO INTERFACE

Smooth evolution from the 4G-LTE to 5G-NR technology implied inheritance of the key elements in the physical layer



MultiView Spectrum ☒ Real-Time Spectrum ☒ 5G NR ☒

Ref Level 0.00 dBm RBW 100 kHz
Att 10 dB SWT 30 ms Dwell Time 30 ms
YIG Bypass

FIGURE 2. 5G-NR downlink signal spectrum and the spectrogram without jamming.

with significant modifications for extended and heterogeneous usage of the radio network. 5G-NR uses the 10 ms frame structure divided into slots, grouping the subcarriers and symbols in OFDM resource blocks (RB). Nevertheless, a different pattern was proposed for carrier spacing and the symbol length. 5G-NR implements an extended set of subcarrier spacing defined by the value of μs parameter [43], from the set of [0, 1, 2, 3, 4], which corresponds to the subcarrier spacing of [15, 30, 60, 120, 240] kHz respectively. At this point it must be noted that the higher the subcarrier spacing, the shorter the length of the OFDM symbol, which implies a shorter duration of the slot, which, in this case, is in a range from 62,5 μs (240 kHz subcarrier spacing) to 1 ms (15 kHz subcarrier spacing). This new concept of slot timing and subcarrier spacing allows for adjusting the physical layer parameters to different applications (services) and for its coexistence with 5G-NR networks in the frequency bands of 4G-LTE networks [42], [43], [49]. The spectrum and spectrograms of the real signal of the gNB operating in the FDD (Frequency Division Duplex) mode is presented in Fig. 2. Compared to the LTE DL signal, a different occupation profile of the time-frequency resources can be observed. The presented spectrogram corresponds to the DL signal of the 5G SA gNB that was used as the testbed in the presented research studies.

Considering the main goal of the conducted research, the content of the 5G-NR radio frame needs to be briefly discussed. Physical channels and signals allocated in the time-frequency resources can be treated as similar with respect to 4G-LTE [42], [43]. In the DL, PBCH (Physical Broadcast Channel), PDCCH (Physical Downlink Control Channel), PDSCH (Physical Downlink Shared Channel) channels, PSS (Primary Synchronization Signal), and SSS (Secondary Synchronization Signal) signals are allocated. The channels are used to transmit the broadcast messages to the UE, such as the MIB as well as the user data. In the resource grid DMRS (Demodulation Reference Signal) signals used for channel parameters estimation are allocated in the RB assigned for the PDSCH. Analyzing the possible allocation of DMRS symbols in the two resource elements patterns, named type A and B in the 3GPP specification [43], can be pointed ou at. For instance, the basic configuration assumes the presence of DMRS symbols in the third (index ♯2) or fourth (index ♯3) OFDM symbol on 6 subcarriers, starting from subcarrier ♯0, and with 2 subcarrier spacing between the DMRS symbols (6 DMRS symbols in total). The allocation of additional DMRS symbols is optional and defined by a higher-layer parameter [43], [49].

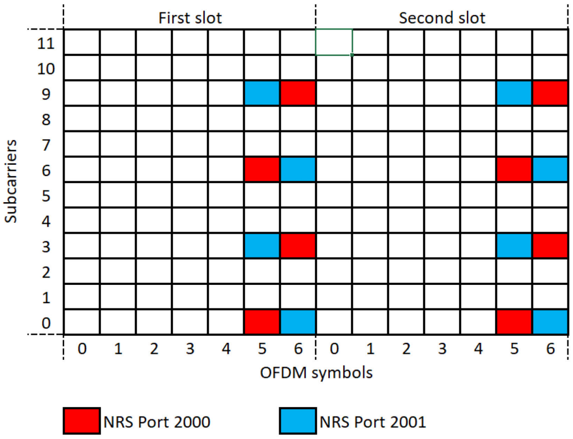


FIGURE 3. Example of resource allocation for an NRS signal in a single NB-IoT downlink subframe.

B. NB-IOT RADIO INTERFACE

NB-IoT is a communication standard defined by 3GPP for providing reliable, narrowband communication between IoT devices usually in frequency bands below 1 GHz. The radio interface between a NB-IoT device (UE) and a base station (eNodeB/gNodeB) implements a simplified version of the LTE protocol stack. Frequency resources allocated for NB-IoT may reside within the LTE band (in-band mode), between LTE FDD uplink and downlink (guard-band mode), or outside the LTE band (SA mode). Irrespective of the mode of operation, the NB-IoT downlink employs the OFDM transmission scheme in a single physical resource block (PRB) with a 180 kHz bandwidth (12 subcarriers with 15 kHz spacing). Downlink transmission is also organized in 10 ms frames, where one frame consists of 10 subframes and each subframe is divided into 2 slots containing 7 OFDM symbols. Characteristic static resource allocation is defined within the frame structure in the following ways [42]:

- Narrowband Primary Synchronization Signal (NPSS) occupies the resources of subframe ♯5 in each frame,
- Narrowband Secondary Synchronization Signal is present in subframe ♯9 of all even frames,
- Narrowband Physical Broadcast Channel (NPBCH) is transmitted in subframe ♯0 of each frame,
- NRS is transmitted in symbol ♯5 and ♯6 of each slot (except NPSS and NSSS subframes) and occupies two subcarriers according to the Cell ID specific pattern - an example of NRS resource allocation is depicted in 3.

Other subframes are reserved for the transmission of Narrowband Physical Downlink Control Channel

(NPDCCH) and Narrowband Physical Downlink Shared Channel (NPDSCH). The resources for these channels are allocated dynamically, depending on the cell configuration and traffic intensity, thus they are less prone to smart jamming. In contrast, subframes ♯0 and ♯5 as well as NRS resources are considered the most vulnerable components of NB-IoT downlink transmission.

IV. EFFECTIVE JAMMING

Each radio communication system operates in the presence of interference. In the case of civilian systems, we primarily consider intra- or inter-system unintentional interference [50], [51]. Military systems are additionally exposed to intentional interference, i.e. jamming [11]. Jamming is one of the essential elements of electronic warfare (EW) and it is designed to interrupt or prevent effective communications between enemy units [14], [52]. Hence, military wireless communication systems must be robust to interference and still provide reliable operational capability in a contested radio frequency (RF) environment. New jamming systems are being developed along with the use of new radio resources and technologies in military systems. On the other hand, new methods of counteracting and avoiding interference are investigated too. This last issue concerns both civilian and military systems, regarding unintentional and intentional interference respectively.

There are many jamming techniques with specific features. Every jammer unit differs from another in terms of power efficiency, signal parameters, complexity and vulnerability to detection. The most common types of jammers related to the most recent wireless communications systems are named as regular, delusive (deceptive), random, responsive, go-next (with frequency hopping) and control channels jammers (selective jammers) [7].

A regular jammer can be a contrast for the most advanced methods. In this case, the jamming radio signal is transmitted continuously, generally with high output power, resulting in short battery life of mobile devices. This type of jammer is also fairly easy to detect by the adversary's equipment for monitoring electromagnetic resources. Nevertheless, the main and significant advantage is its universality. Moreover, there is no need to possess precise knowledge about the parameters of the system that will be jammed. The only important thing in this case is the frequency range used. An example signal generated by this type of jammer is presented in Fig. 4.

More advanced jamming methods involve a'priori knowledge about the attacked system, such as the time-frequency structure of the physical layer. In this case, jamming signals are adjusted to a particular radio interface. For instance, the jamming signal can be periodical, with the duration of one slot. It may also occur during the transmisssion of the PSS/SSS synchronization signals, or it can occupy only the subcarriers allocated for the DMRS (Fig. 5) or NRS symbols.

In the case of simple barrage jamming (Fig. 4), the power of interference is spread across the entire frequency band of the signal, while a smart jammer may concentrate the power at specific frequency components. This improves the effectiveness or increases the range of jamming, assuming that the peak power of the interference is fixed. Moreover, the pulsed transmission pattern of a smart jammer reduces its power consumption. This adaptive approach can cause nontypical behaviour of the jammed system, e.g. the UE can detect and synchronize with the gNB but cannot correctly receive any data [6].

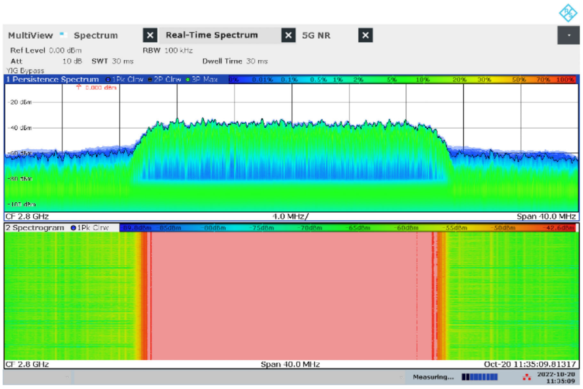

MultiView Spectrum | Real-Time Spectrum | 5G NR
Ref Level 0.00 dBm RBW 100 kHz
Att 10 dB SWT 30 ms Dwell Time 30 ms
YIG Bypass

FIGURE 4. Regular jammer - an example of a continuously transmitted jamming signal.

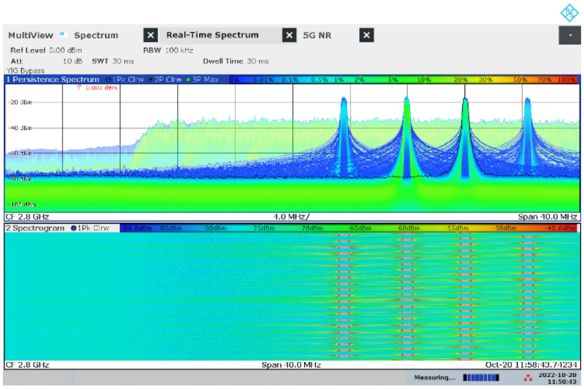

MultiView Spectrum | Real-Time Spectrum | 5G NR
Ref Level 0.00 dBm RBW 100 kHz
Att 10 dB SWT 30 ms Dwell Time 30 ms
YIG Bypass

FIGURE 5. Effective jamming - an example of a narrowband jamming signal.

In odrer to operate properly, a smart jammer must maintain time synchronization between its transmission and the rate of the jammed signal. One way to acheive this is to equip the jammer with an appropriate receiver with time synchronization output which could be used as a triggering clock source for jamming transmission. However, this approach is not recommended for two reasons. Firstly, when the jammer is active, it may not be possible to receive the signal, which is required to keep the jammer synchronized with the attecked system. Secondly, the jammer location is limited by the range of the useful signal. This excludes the scenario where a jamming source with a highly directional antenna is at a coniderable distance from the target receiver. Due to these limitations, another solution has been proposed, based on the assumption that network nodes are synchronized

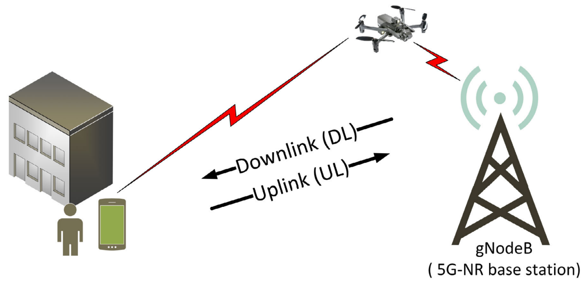


FIGURE 6. Low-energy jamming operational scenario.

with respect to Global Navigation Satellite Systems' (GNSS) signals. In such a case, the jammer transmitter may be synchronized with GNSS signals as well, thus excluding the need to receive the jammed radio interface signal.

V. JAMMING OPERATIONAL SCENARIO

The operational scenario of the proposed jamming test is presented in Fig. 6. The aim is to prevent data transmission or significantly degrade the quality of service in the target 5G private network. The given scenario assumes placing a jamming device on a UAV. During operation, the UAV gets close to the 5G-NR base station (gNB) so that the generated jamming signals can be transmitted with as low power as necessary. Thanks to the reduced energy consumption, it is possible to operate the UAV and the jammer for a longer period of time. Besides, a significant benefit while using the proposed solution in military scenarios is reducing the probability of detecting the operation of such a jammer by the enemy. At this point it is worth mentioning that the methods of jamming UAV control signals are not the point of interest, especially if a military UAV can operate in an SA mode with a predefined route, e.g. based on GNSS (Global Navigation Satellite Systems) signals.

In the second investigated scenario, verification of smart jamming effectiveness on the NB-IoT radio interface was possible by using a testbed whose scheme is presented in Fig. 7. The jammer generates OFDM signals in which the locations of jamming-intended time-frequency resources are occupied by the pulses of unit magnitude and random phase shift. In other locations of the OFDM resource grid the pulses are muted. This transmission pattern is stored as a waveform on a PC class computer. When jamming is initiated, samples are cyclically transferred to a USRP X310 front-end, whose TX path generates an RF signal at the desired carrier frequency. The USRP internal clock and oscillator are synchronized with the PPS signal provided by the embedded GPS receiver.

Instead of using a laboratory radio communication tester, the jammed transmission was an actual NB-IoT signal received from a nearby eNodeB station, operating in LTE band 8. The purpose of using the real signal source was to verify whether the LTE/NB-IoT base station is actually synchronized with the GNSS reference signals. The received RF signal was combined with the generated interference one.

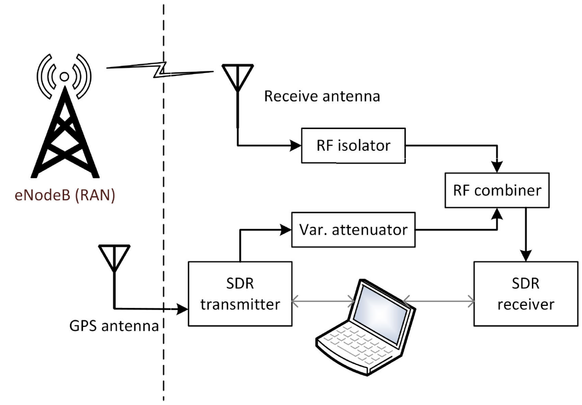


FIGURE 7. NB-IoT Smart jamming testbed scenario.

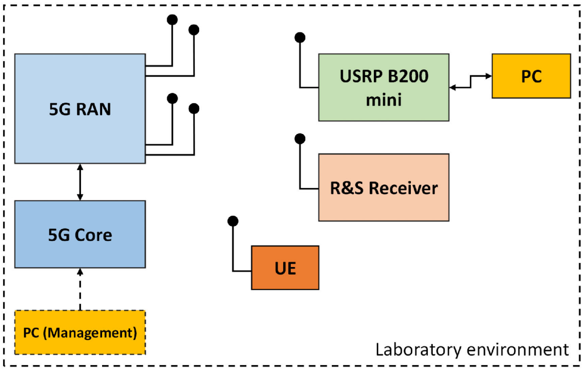


FIGURE 8. Laboratory testbed for the jamming practical trial - flowchart.

A variable attenuator was placed between the transmitter and the combiner in order to acheive the desired jammer-to-signal power ratio. Additionally, an RF isolator was plugged between the receive antenna and the combiner so that the interference was not radiated outside the testbed. The RF combiner output was directed to the RX path input of the USRP device, which allowed for recording the received signals. The samples of the jammed NB-IoT signal were further post-processed using developed Matlab scripts for analysis and decoding NB-IoT radio interface signals.

VI. PRACTICAL TRIALS

A. TESTBED

In order to conduct the measurements of 5G private network jamming, a dedicated and isolated laboratory stand was built, including a software and a hardware layer (Fig. 8). Using a base station for 5G private networks in the study allowed the authors to analyse the 5G SA standard. The presented approach can also be applied to LTE and 5G NSA base stations after considering the time-frequency structure of their signals. At this stage, the authors did not have the opportunity to test the system at a commercial base station. Discussions are being held with one of the operators so that such tests can be conducted in a real environment. In addition, an isolated laboratory 5G network is being built to implement

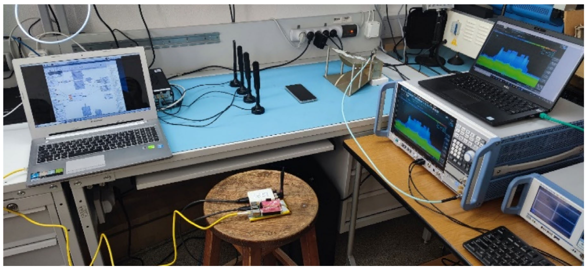


FIGURE 9. Laboratory testbed for the 5G jamming practical trial - photo of the stand.

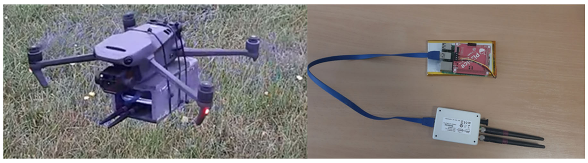


FIGURE 10. Real photo of the integrated UAV RF jammer: DJI Mavic 3 + USRP B200mini + RaspberyPi 4.

the research experiments in cooperation with several research centres and it is planned to be used for future work as well.

As a 5G private network, the device provided by Athonet company was used. It consists of an SA 5G-Core and a 5G-RAN developed by Amarisoft. The set operates in two FR1 frequency bands, N77 - 3.75 GHz for TDD, and N7 - 2.68 GHz for FDD operation, with occupied 20 MHz bandwidth and MIMO 2 × 2 connection. It must be pointed out that the hardware realization of the RAN part is dedicated to indoor environments considering its output power (below 10 dBm), but it can easily be employed to perform the assumed test case. As the UE, a Xiaomi Mi11 smartphone was used. Moreover, a USRP B200 mini (adapted for mounting on and powered from the UAV platform) was selected as the source of jamming signals. The last element of the testbed was a Rohde&Schwarz receiver used to monitor the spectrum during the tests.

Fig. 9 and Fig. 10 present the actual views of the laboratory testbed, and the integrated UAV jammer respectively.

B. THE 5G-NR JAMMING SCENARIO

The scenario to evaluate the effectiveness of 5G radio interface jamming utilized the following signals generated by the software-defined radio platform (USRP B200 mini + RaspberyPi 4):

- AWGN (Additive White Gaussian Noise) signal with a 20 MHz bandwidth,
- Four narrowband (62,5 kHz) signals generated simultaneously (the total signals bandwidth was 250 kHz),
- Four narrowband (62,5 kHz) signals generated sequentially (slow hopping - 1 hop/s),
- Four narrowband (62,5 kHz) signals generated sequentially (medium hopping - 5 hops/s).
- Four narrowband (62,5 kHz) signals generated sequentially (fast hopping - 10 hops/s).

The tests were conducted for two duplex modes of operation: FDD (Frequency Division Duplex) and TDD (Time Division Duplex) in two different frequency bands regarding 3GPP regulations. In the FDD mode, jamming signals were generated on DL frequencies. In contrast, in the case of the TDD mode, the jamming affected both DL and UL transmissions. The quality of service in the presence of jamming signals was tested for data transmission. The laboratory stand allowed us to run DL and UL data benchmarks from the UE to the 5G-Core (Service number 2 in Fig. 1).

C. THE NB-IOT JAMMING SCENARIO

The experiments were conducted in two test cases: barrage jamming and NRS jamming. It is worth mentioning that in the literature the impact of selective jamming on an NRS signal was not investigated widely, in contrast to NB-IoT synchronization signals jamming [53]. In each scenario the same source of NB-IoT downlink signal was used, which was the eNodeB located at the campus of Gdańsk University of Technology. This is a public base station belonging to a commercial provider, operating in the SA mode on 935.10 MHz carrier frequency. The first test was intended to verify if the downlink transmision is synchronized with the GPS system clock. More precisely, the test was expected to prove that the beginning of each GPS clock second (the pulse per second signal) coincides with the beginning of an even NB-IoT frame. In order to verify this statement, a test signal with a specific temporal pattern was generated and recorded simultaneously with NB-IoT signal. Next, the spectrograms of the two signals were compared.

In the second step, selective jamming effectiveness was compared with barrage jamming, i.e. a continuous jamming signal covering the entire 180 kHz NB-IoT frequency band. The tests focused on jamming the NPBCH channel which carries MIBs which provide initial information acquired by the UE during the cell attachment procedure.

The selective interference consisted of pulses jamming only the NRS resource elements in subframe ♯0 and the NRS resources occurring before subframe ♯0 (i.e. the NRS in the second slot of subframe ♯8 or ♯9, depending on the frame oddity). In contrast, barrage interference covered the whole NB-IoT band in all the subframes, except those carrying NPSS and NSSS, in order to avoid the jamming impact on the UE synchronization performance needed for a proper jamming effectiveness analysis.

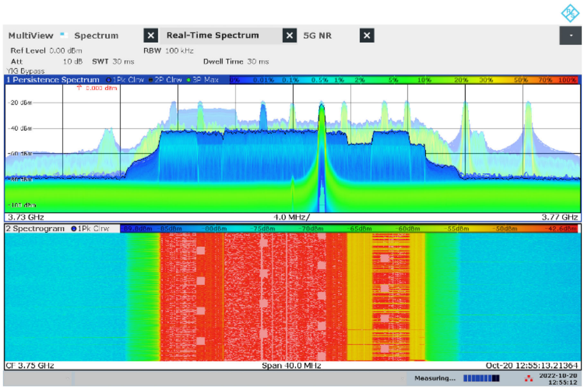
D. SELECTED RESULTS OF 5G RADIO INTERFACE JAMMING

The results of the test scenario are presented in Table 1. It also contains reference values acquired for the donwlink and uplink transmission when no jamming signals were generated.

In the TDD mode, jamming in the hopping mode by four narrowband signals made it impossible to perform

TABLE 1. Data rates measured for downlink and uplink transmission.

Jamming signal	Operation mode	Downlink speed [Mb/s]	Uplink speed [Mb/s]
—	FDD	212.00	27.80
—	TDD	149.80	22.90
AWGN, 20 MHz	FDD (DL)	33.96	23.99
Four simultaneous narrowband signals	FDD (DL)	103.73	25.26
Four sequentially generated narrowband signals (fast frequency hopping)	FDD (DL)	37.98	23.49
Four simultaneous narrowband signals	TDD	43.40	0.22



MultiView Spectrum | Real-Time Spectrum | 5G NR

Ref Level 0.00 dBm RBW 100 kHz

Att 10 dB SWT 30 ms Dwell Time 30 ms

YIG Bypass

1 Persistence Spectrum ●1Pk Clrw ●2P Clrw ●3P Max

3.73 GHz 4.0 MHz/ 3.77 GHz

2 Spectrogram ●1Pk Clrw

CF 3.75 GHz Span 40.0 MHz Oct-20 12:55:13.21364

Measuring... 2022-10-20 12:55:12

FIGURE 11. 5G signal spectrum and spectrogram with a narrowband jamming signal (medium frequency hopping).

benchmark tests. Based on the results, it can be inferred that each proposed jamming signal disrupts 5G radio interface transmission. Therefore, an essential aspect of the proposed jamming solution effectiveness is the energy required to disable 5G-based communication. For example, a quantitative analysis shows that in the case of a signal interfering selectively in sub-bands occupying 62.5 kHz each (250 kHz total) and compared to a 20 MHz width signal from a regular jammer, the energy gain reaches 19 dB. It is worth noting that the effect of blocking communications is also possible for selective interference with only one sub-band out of four with a width of 62.5 kHz according to the set scheme (Fig. 11).

In this case, the energy is consumed for only one selectively chosen sub-band at a time, reducing the total energy consumption (the required necessary radiation power) four times (6 dB). Moreover, compared to a regular jammer, in one sub-band jamming scenario the gain of 25 dB can be achieved. Thanks to the jammer's efficiency, we can assume obtaining these potential benefits: a larger operational range of the jammer, reduction in the required radiated power, longer operating time of the device due to lower power consumption, and/or minimization of the detection probability in the military context. In addition to this, following the obtained results, when a DL is jammed the source of the jamming signal should be as close as possible to the UE to maximize the jamming effectiveness.

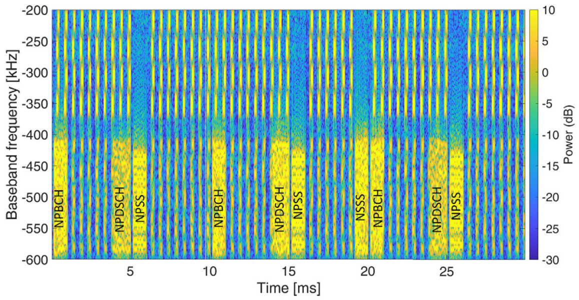


FIGURE 12. Spectrogram for illustrating signal synchronization.

E. SELECTED RESULTS OF NB-IOT RADIO INTERFACE JAMMING

The test signal in the first step was generated as an OFDM waveform which consisted of pulses located only in symbols and subcarriers allocated for NRS signal transmission (in order to determine the NRS location, the eNodeB cell identifier was found first). Next, based on this waveform, an RF signal was generated at a center frequency of 935.3 MHz, with +200 kHz offset from the received NB-IoT signal.

The 400 kHz wide spectrogram of both signals recorded simultaneously is presented in Fig. 12. The spectrum of the NB-IoT signal from the eNodeB is visible in the lower part, centered around the baseband frequency of −500 kHz. The time axis was limited so that its beginning coincides with the beginning of the NB-IoT frame and spans three subsequent frames (30 ms duration). The spectrogram clearly shows characteristic components corresponding to specific signals and physical channels. In the 1^{st}, 11^{th} and 21^{st} millisecond, NPBCH transmission is visible. Similarly, NPSS is transmitted in the 6^{th}, 16^{th} and 26^{th} millisecond. NSSS is present in the 20^{th} millisecond, which means that the first frame of the spectrogram is odd. Moreover, NPDSCH resources carrying a System Information Block (SIB) are present in the 5^{th}, 15^{th} and 25^{th} millisecond. Isolated pulses observed at four subcarriers correspond to the NRS signal components. NRS is present in subframes $\sharp 0$ and $\sharp 4$ as well, but cannot be distinguished from other resources in the spectrogram.

The upper part of Fig. 12 shows the spectrogram of the generated test signal, centered at −300 kHz baseband frequency. It can be seen that time intervals, when the test signal is active, coincide with OFDM symbols carrying the NRS signals in NB-IoT downlink. Moreover, longer periods of the test signal inactivity correspond to the segments of the NB-IoT signal when synchronization signals (NPSS and NSSS) are transmitted. These results prove that the NB-IoT signal transmitted by eNodeB is synchronized with the GPS clock.

In the second phase of the tests, the effectiveness of jamming the NPBCH channel was investigated. Jamming effectiveness is considered here to be the percentage of not decoded Master Information Blocks (MIB). MIB decoding is

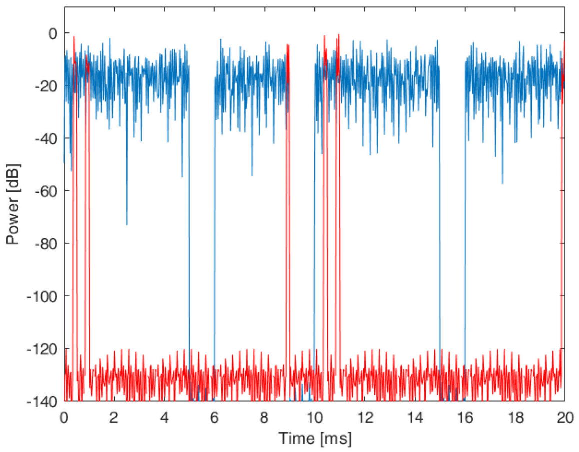


FIGURE 13. Instantaneous powers of barrage and selective jamming.

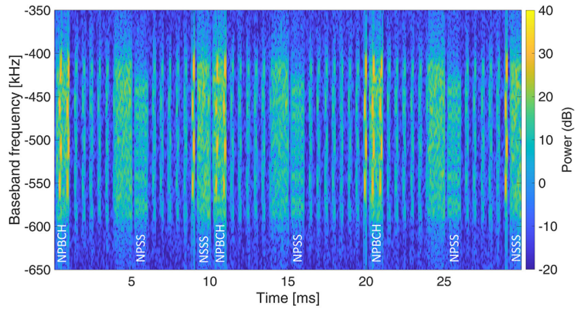


FIGURE 14. Spectrogram for selective NRS jamming.

considered successful if the cyclic redundancy check (CRC) of the respective transport block is passed.

Fig. 13 shows variations in instantaneous power for barrage jamming (blue) and selective NRS jamming (red). As can be seen, peak relative power levels of both signals are roughly the same. This is essential for fair comparison of jamming effectiveness for which the transmitter peak power is considered to be the main limiting factor. The spectrograms of the NB-IoT signal in the presence of both types of jamming, with a jamming-to-signal peak power ratio of 3 dB, are shown in Fig. 14 and Fig. 15. For readers' convenience, the positions of characteristic subframes were labeled at the bottom. In the case of selective interference, stronger pulses (yellow color) are visible in the locations of NRS symbols in the NPBCH (subframe ♯0) or they precede the NRS symbols (subframe ♯8 or ♯9). In contrast, barrage jamming covers the whole NB-IoT signal except for the NPSS and NSSS subframes which begin with the period of inactivity in the first three OFDM symbols, which is characteristic for the NB-IoT SA operation mode.

The comparison of NPBCH jamming effectiveness is presented in Fig. 16. The tests were conducted for jamming-to-signal peak power ratios of −6 dB, −3 dB, 0 dB, and 3 dB. In each case, 500 trials of MIB decoding were performed. The results show that barrage jamming barely affects the possibility of decoding the MIBs, regardless of the power ratio. Only a few MIB decoding failures were observed, which is likely even for no-jamming conditions (e.g. because of the negative influence of the channel conditions). Different results were obtained for selective jamming, where a strong relationship between jamming effectiveness and jammer power was observed. When the jamming-to-signal power ratio was 3 dB, less then half the MIBs were successfully decoded.

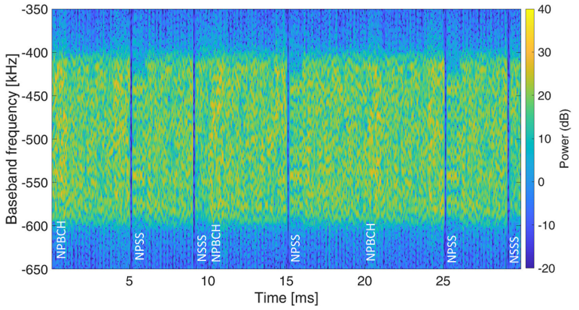


FIGURE 15. Spectrogram for barrage jamming.

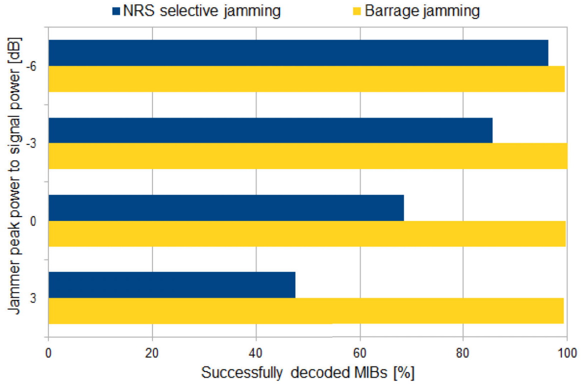


FIGURE 16. Effectiveness of jamming the NPBCH.

VII. CONCLUSION

In the presented research studies, it was proven that narrowband jamming signals can be used to disturb or disable communication in a 5G private network for the FDD and TDD modes of operation. The obtained jamming efficiency, reaching up to 99% for the TDD-UL or 82% for the FDD-DL, can be compared to broadband jamming (84%), also in the context of power gain. In the proposed use case, the power gain can reach up to 25 dB when one narrowband sub-band is jammed. Based on the obtained results, the authors assume similar effectiveness of the jamming technique for other gNB operation configurations, i.e. 200/100 MHz bandwidths. Because of the 5G physical Layer EW resistant weakness, it seems that 5G private networks should be carefully selected in the context of operational activities on the battlefield in the presence of strong radio interference and/or intentional jamming. This issue does not narrow down the application of

5G to isolated, controlled military environments, but it offers space for further research studies.

Moreover, the results of smart jamming prove that performing selective and efficient jamming of the NB-IoT radio interface is feasible. Since the base stations' clocks are synchronized with the GNSS signal, this offers the opportunity to use the signal to synchronize the jamming source as well, thus avoiding the necessity to receive and detect the attacked radio interface signal beforehand. Based on the obtained results, it can be concluded that significantly greater effectiveness of selective jamming stems mainly from the fact that jamming signal power is focused on selected resource elements. In the analyzed case, the interference was active only at two subcarriers in the OFDM symbol, while barrage jamming was spread over all the twelve subcarriers. In addition to this, with the 3 dB jamming-to-signal peak power ratio and the signal focused on NRS resources it was possible to degrade the accuracy of the channel estimation for subframe ♯0. This negatively affected the reception of MIB transport blocks (successful decoding ratio below 50%), which is crucial during the UE attachment procedure.

In the paper it was demonstrated that narrowband jamming signals can be used to disturb or disable communication in a 5G private network for the FDD and TDD modes of operation. Owing to the proposed energy-efficient and flexible 5G private networks jammer, it is possible to use it to prevent or disturb communications in the area of interest, minimizing the risk of possible detection. The significant advantage of the developed jammer is its high mobility and the possibility of being steered from a remote location (in the case of armed conflicts, the risk of the system operators' localization can be subtantially reduced). Furthermore, using the commercial SDR platform and UAV equipment allows for a quick increase in the number of jammers and for adapting the solution to the current operational requirements. The assumed future works might aim to develop other smart methods of jamming and to verify their practical implementations. In addition, the authors are considering using commercial LTE and 5G NSA base stations for future tests and performing experiments on an emerging isolated 5G network.

ACKNOWLEDGMENT

The authors would like to thank Systemics-PAB Company, especially Leszek Wojdalski, for lending the 5G standalone private networks developed by Athonet. This article is a collaborative work of research task group (RTG) members from the IST-187-RTG on "5G Technologies Application to NATO Operations" operating within the Information Systems Technology (IST) Panel at the NATO Since and Technology Organization (NATO STO).

REFERENCES

[1] *IMT Vision—Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond*, document ITU-R Recommendation M.2083-0, 2015.

[2] X. Huang, R. Yu, J. Kang, Y. Gao, S. Maharjan, S. Gjessing, and Y. Zhang, "Software defined energy harvesting networking for 5G green communications," *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 38–45, Aug. 2017, doi: 10.1109/MWC.2017.1600360.

[3] H. Kim, J. Kim, and D. Hong, "Dynamic TDD systems for 5G and beyond: A survey of cross-link interference mitigation," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2315–2348, 4th Quart., 2020, doi: 10.1109/COMST.2020.3008765.

[4] V. Conan, "5G technologies for defence," EDA CapTech Inf., Eur. Defence Agency, Rue des Drapiers, Ixelles, Belgium, White paper 1.0, Jan. 2021.

[5] L. Bastos, G. Capela, A. Koprulu, and G. Elzinga, "Potential of 5G technologies for military application," in *Proc. Int. Conf. Mil. Commun. Inf. Syst. (ICMCIS)*, The Hague, The Netherlands, May 2021, pp. 1–8, doi: 10.1109/ICMCIS52405.2021.9486402.

[6] P. Skokowski, J. M. Kelner, K. Malon, K. Maslanka, A. Birutis, M. A. Vazquez, S. Saha, W. Low, A. Czapiewska, J. Magiera, P. Rajchowski, and S. Ambroziak, "Jamming and jamming mitigation for selected 5G military scenarios," *Proc. Comput. Sci.*, vol. 205, pp. 258–267, Jan. 2022, doi: 10.1016/j.procs.2022.09.027.

[7] Y. Arjoune and S. Faruque, "Smart jamming attacks in 5G new radio: A review," in *Proc. 10th Annu. Comput. Commun. Workshop Conf. (CCWC)*. Las Vegas, NV, USA, Jan. 2020, pp. 1010–1015, doi: 10.1109/CCWC47524.2020.9031175.

[8] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 767–809, 2nd Quart., 2022, doi: 10.1109/COMST.2022.3159185.

[9] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, *A Comprehensive Guide to 5G Security*. Hoboken, NJ, USA: Wiley, 2018, pp. 117–141, doi: 10.1002/9781119293071.ch6.

[10] M. Arif and A. Shakoor, "Clustered jamming and antenna beam-width fluctuations for UAV-assisted cellular networks," *Comput. Netw.*, vol. 240, Feb. 2024, Art. no. 110171, doi: 10.1016/j.comnet.2024.110171.

[11] R. A. Poisel, *Modern Communications Jamming. Principles and Techniques*, 2nd ed. Boston, MA, USA: Artech House, 2011.

[12] J. Sliwa and M. Suchanski, "Security threats and countermeasures in military 5G systems," in *Proc. 24th Int. Microw. Radar Conf. (MIKON)*, Gdansk, Poland, Sep. 2022, pp. 1–6, doi: 10.23919/MIKON54314.2022.9924818.

[13] J. P. Mohan, N. Sugunaraj, and P. Ranganathan, "Cyber security threats for 5G networks," in *Proc. IEEE Int. Conf. Electro Inf. Technol. (eIT)*, Mankato, MN, USA, May 2022, pp. 446–454, doi: 10.1109/eIT53891.2022.9813965.

[14] R. Poisel, *Introduction to Communication Electronic Warfare Systems*, 2nd ed. Boston, MA, USA: Artech House, 2008.

[15] S. J. B. Babu and H. Williams. *Ukraine Conflict: Ukraine's Electronic Warfare Systems in Focus*. Accessed: Feb. 4, 2024. [Online]. Available: https://www.janes.com/defence-news/news-detail/ukraine-conflict-ukraines-electronic-warfare-systems-in-focus

[16] A. Bhardwaj, "5G for military communications," *Proc. Comput. Sci.*, vol. 171, pp. 2665–2674, Jan. 2020, doi: 10.1016/j.procs.2020.04.289.

[17] J. F. Harvey, M. B. Steer, and T. S. Rappaport, "Exploiting high millimeter wave bands for military communications, applications, and design," *IEEE Access*, vol. 7, pp. 52350–52359, 2019, doi: 10.1109/ACCESS.2019.2911675.

[18] D. Zmyslowski, P. Skokowski, K. Malon, K. Maslanka, and J. Kelner, "Naval use cases of 5G technology," *TransNav, Int. J. Mar. Navigat. Saf. Sea Transp.*, vol. 17, no. 3, pp. 595–603, Sep. 2023, doi: 10.12716/1001.17.03.11.

[19] F. Tian, P. Zhang, and Z. Yan, "A survey on C-RAN security," *IEEE Access*, vol. 5, pp. 13372–13386, 2017, doi: 10.1109/ACCESS.2017.2717852.

[20] P. Schneider and G. Horn, "Towards 5G security," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, vol. 1, Helsinki, Finland, Aug. 2015, pp. 1165–1170, doi: 10.1109/Trustcom.2015.499.

[21] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011, doi: 10.1109/MWC.2011.5751298.

[22] M. Lichtman, R. Rao, V. Marojevic, J. Reed, and R. P. Jover, "5G NR jamming, spoofing, and sniffing: Threat assessment and mitigation," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Kansas City, MO, USA, May 2018, pp. 1–6, doi: 10.1109/ICCW.2018.8403769.

[23] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2734–2771, 3rd Quart., 2019, doi: 10.1109/COMST.2018.2865607.

[24] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic, and J. H. Reed, "LTE/LTE-A jamming, spoofing, and sniffing: Threat assessment and mitigation," *IEEE Commun. Mag.*, vol. 54, no. 4, pp. 54–61, Apr. 2016, doi: 10.1109/MCOM.2016.7452266.

[25] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016, doi: 10.1109/JPROC.2016.2558521.

[26] C. Yu, S. Chen, F. Wang, and Z. Wei, "Improving 4G/5G air interface security: A survey of existing attacks on different LTE layers," *Comput. Netw.*, vol. 201, Dec. 2021, Art. no. 108532, doi: 10.1016/j.comnet.2021.108532.

[27] A. Jagannath, J. Jagannath, and A. Drozd, "High rate-reliability beamformer design for 2×2 MIMO-OFDM system under hostile jamming," in *Proc. 29th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Aug. 2020, pp. 1–9, doi: 10.1109/ICCCN49398.2020.9209635.

[28] A. Kekirigoda, K.-P. Hui, Q. Cheng, Z. Lin, J. A. Zhang, D. N. Nguyen, and X. Huang, "Massive MIMO for tactical ad-hoc networks in RF contested environments," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Norfolk, VA, USA, Nov. 2019, pp. 658–663, doi: 10.1109/MILCOM47813.2019.9020756.

[29] H. Akhlaghpasand, E. Bjornson, and S. M. Razavizadeh, "Jamming suppression in massive MIMO systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 1, pp. 182–186, Jan. 2020, doi: 10.1109/TCSII.2019.2902074.

[30] P. Skokowski and J. Dulowicz, "Autonomous mobile system for detecting and jamming cellular network signals using a software defined radio integrated into a UAV platform," in *Proc. Signal Process. Symp. (SPSympo)*, Karpacz, Poland, Sep. 2023, pp. 149–151, doi: 10.23919/SPSympo57300.2023.10302702.

[31] M. E. Flores, D. D. Poisson, C. J. Stevens, A. V. Nieves, and A. M. Wyglinski, "Implementation and evaluation of a smart uplink jamming attack in a public 5G network," *IEEE Access*, vol. 11, pp. 75993–76007, 2023, doi: 10.1109/access.2023.3296701.

[32] A. Birutis, A. Mykkeltveit, T. Ulversoy, O. D. Borlaug, and J. Karstad. (2022). *A Study of 5G New Radio and Its Vulnerability to Jamming*. Accessed: May 21, 2023. [Online]. Available: https://ffi-publikasjoner.archive.knowledgearc.net//handle/20.500.12242/3022

[33] P. J. Varga, T. Wührl, S. Gyányi, M. T. Baross, and A. Németh, "Jamming attacks in 5G NR FR1," in *Proc. IEEE 5th Int. Conf. Workshop Obuda Elect. Power Eng. (CANDO-EPE)*, Budapest, Hungary, Nov. 2022, pp. 175–180, doi: 10.1109/CANDO-EPE57516.2022.10046381.

[34] M. A. Birutis and A. Mykkeltveit, "Practical jamming of a commercial 5G radio system at 3.6 GHz," *Proc. Comput. Sci.*, vol. 205, pp. 58–67, Jan. 2022, doi: 10.1016/j.procs.2022.09.007.

[35] P. Kryszkiewicz and M. Hoffmann, "Open RAN for detection of a jamming attack in a 5G network," in *Proc. IEEE 97th Veh. Technol. Conf. (VTC-Spring)*, Florence, Italy, Jun. 2023, pp. 1–2, doi: 10.1109/vtc2023-spring57618.2023.10201067.

[36] S.-D. Wang, H.-M. Wang, W. Wang, and V. C. M. Leung, "Detecting intelligent jamming on physical broadcast channel in 5G NR," *IEEE Commun. Lett.*, vol. 27, no. 5, pp. 1292–1296, May 2023, doi: 10.1109/LCOMM.2023.3260194.

[37] K. Wesolowski, "A simple algorithm for jamming detection in OFDM systems," in *Proc. IEEE 97th Veh. Technol. Conf. (VTC-Spring)*, Florence, Italy, Jun. 2023, pp. 1–5, doi: 10.1109/vtc2023-spring57618.2023.10200416.

[38] G. Morillo, U. Roedig, and D. Pesch, "Detecting targeted interference in NB-IoT," in *Proc. 19th Int. Conf. Distrib. Comput. Smart Syst. Internet Things (DCOSS-IoT)*, Pafos, Cyprus, Jun. 2023, pp. 475–482, doi: 10.1109/dcoss-iot58021.2023.00080.

[39] A. N. Elbattrawy, A. H. Abd El-Malek, S. I. Rabia, and W. K. Zahra, "Model-based Bayesian reinforcement learning for enhancing primary user performance under jamming attack," *Ad Hoc Netw.*, vol. 148, Sep. 2023, Art. no. 103206, doi: 10.1016/j.adhoc.2023.103206.

[40] H. Sharma, N. Kumar, and R. Tekchandani, "Mitigating jamming attack in 5G heterogeneous networks: A federated deep reinforcement learning approach," *IEEE Trans. Veh. Technol.*, vol. 72, no. 2, pp. 2439–2452, Feb. 2023, doi: 10.1109/TVT.2022.3212966.

[41] O. A. Topal, S. Gecgel, E. M. Eksioglu, and G. K. Kurt, "Identification of smart jammers: Learning-based approaches using wavelet preprocessing," *Phys. Commun.*, vol. 39, Apr. 2020, Art. no. 101029, doi: 10.1016/j.phycom.2020.101029.

[42] *LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Channels and Modulation*, 3rd Gener. Partnership Project, Tech. specification, document TS 36.211, V14.14.0, 3GPP, 2020.

[43] *5G; NR; Physical Channels and Modulation*, 3rd Generation Partnership Project, Tech. Specification document TS 38.211, V16.2.0, 3GPP, 2020.

[44] T. Cheng and F. Zhou, "5G virtual private network planning methodology analysis," in *Proc. 14th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Nanjing, China, Nov. 2022, pp. 1–4, doi: 10.1109/WCSP55476.2022.10039428.

[45] C. Lee, J. Park, T. Park, J. Kwon, H. Lee, and M. Yoon, "An efficient networks operation system for private 5G networks," in *Proc. 13th Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Nov. 2022, pp. 1794–1796, doi: 10.1109/ICTC55196.2022.9952871.

[46] *Open5Gcore, Open5GCore—5G Core Network for Research, Testbeds and Trials*. Accessed: Apr. 14, 2023. [Online]. Available: https://www.open5gcore.org

[47] A. Aijaz, B. Holden, and F. Meng, "Open and programmable 5G network-in-a-box: Technology demonstration and evaluation results," in *Proc. IEEE 7th Int. Conf. Netw. Softwarization (NetSoft)*, Tokyo, Japan, Jun. 2021, pp. 369–371, doi: 10.1109/NetSoft51509.2021.9492719.

[48] E. Palacios-Morocho, P. Picazo-Martinez, S. Inca, and J. F. Monserrat, "Open source 5G-NSA network for Industry 4.0 applications," in *Proc. IEEE 32nd Annu. Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Helsinki, Finland, Oct. 2021, pp. 1–6, doi: 10.1109/PIMRC50174.2021.9569481.

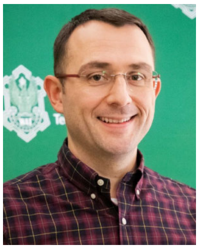
[49] E. Garro, M. Fuentes, J. L. Carcel, H. Chen, D. Mi, F. Tesema, J. J. Gimenez, and D. Gomez-Barquero, "5G mixed mode: NR multicast-broadcast services," *IEEE Trans. Broadcast.*, vol. 66, no. 2, pp. 390–403, Jun. 2020, doi: 10.1109/tbc.2020.2977538.

[50] 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, p. 793, Jan. 2021, doi: 10.3390/s21030793.

[51] S. Kim, E. Visotsky, P. Moorut, K. Bechta, A. Ghosh, and C. Dietrich, "Coexistence of 5G with the incumbents in the 28 and 70 GHz bands," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 6, pp. 1254–1268, Jun. 2017, doi: 10.1109/JSAC.2017.2687238.

[52] R. Inkol, "Electronic warfare," in *Wiley Encyclopedia of Computer Science and Engineering*, B. W. Wah, Ed. Hoboken, NJ, USA: Wiley, 2008, doi: 10.1002/9780470050118.ecse135.

[53] G. Morillo and U. Roedig, "Jamming of NB-IoT synchronisation signals," in *Proc. 26th Eur. Symp. Res. Comput. Secur. (ESORICS)*, Oct. 2021, pp. 1–5.



PAWEŁ SKOKOWSKI was born in Poland, in 1983. He received the M.Sc. (Eng.) and Ph.D. degrees in wireless communications systems from the Military University of Technology (MUT), Warsaw, Poland, in 2007 and 2019, respectively. He is currently an Assistant Professor with the Department of Radiocommunications, MUT Institute of Communications Systems. Since 2007, he has been involved in many research and development projects for Polish Ministry of Defence, European Defence Agency (EDA), and the National Centre for Research and Development. His main research interests include signal processing, wireless communication systems, cognitive radios, situation awareness building, electronic warfare, and data fusion. He also participates in the NATO-STO IST-187 RTG working group "5G Technologies Application to NATO Operations." He was awarded first prize in the ABB Award Competition (the main goal of the competition is to promote and support talented people passionate about advanced technologies) and third prize in the Ministry of Defense competition (a competition for the best doctoral dissertation in the field of modern technologies in communications, with potential application in the area of national defense or security).

KRZYSZTOF MALON was born in Poland, in 1987. He received the E.Eng., M.Sc., and Ph.D. degrees in telecommunications systems from the Military University of Technology (MUT), Warsaw, Poland, in 2010, 2011, and 2019, respectively. He is currently an Assistant Professor with the Department of Radiocommunications, MUT Institute of Communications Systems. Since 2010, he has been actively participated in national and international research and development projects for European Defence Agency (EDA) and the National Center for Research and Development. His main research interests include modern wireless communication systems, software-defined and cognitive radios, dynamic spectrum access, electronic warfare, and radio spectrum monitoring. He also participates in the NATO IST-187 RTG working group on using civilian 5G standards in military operations (5G Technologies Application to NATO Operations). He was awarded first prize in the Ministry of Defence competition (a competition for the best doctoral dissertation in the field of modern technologies in communications, with potential application in the area of national defence or security) and third prize in the National Competition for the Best Doctoral Dissertation in Radio Communication and Multimedia Techniques.

MICHAŁ KRYK was born in Poland, in 1986. He received the M.Sc. (Eng.) degree in wireless communications systems from the Military University of Technology (MUT), Warsaw, Poland, in 2011. He is currently an Assistant Professor with the Department of Radiocommunications, MUT Institute of Communications Systems. Since 2010, he has been actively participated in national and international research and development projects for European Defence Agency (EDA) and the National Center for Research and Development. His current research interests include modern wireless communication systems, simulations, modeling, measurements of channels and propagation, signal-processing, software-defined radio, electronic warfare, and radio spectrum monitoring.

KRZYSZTOF MAŚLANKA was born in Poland, in 1974. He received the M.S. and Ph.D. degrees in telecommunications systems from the Military University of Technology (MUT), Warsaw, Poland, in 1999 and 2017, respectively. He is currently an Assistant Professor with the Institute of Communications Systems, Faculty of Electronics, MUT. He engages in problems of communications and information systems (CIS), modeling and simulation of computer networks, IP networks problems, and telecommunication systems engineering. Since 2000, he has been actively participating in national and international research and development projects for Polish Ministry of Defence, NATO, EDA, and the National Center for Research and Development. He is also involved in, among others, the NATO IST-187 RTG working group on using civilian 5G standards in military operations (5G Technologies Application to NATO Operations).

JAN M. KELNER (Member, IEEE) was born in Poland, in 1977. He received the M.Sc. degree (Hons.) in applied physics and the Ph.D. degree in telecommunications from the Military University of Technology (MUT), Warsaw, Poland, in 2001 and 2011, respectively, and the D.Sc. (Habilitation) degree in information and communication technology from the AGH University of Science and Technology, Krakow, Poland, in 2020. He is currently an Associate Professor with the Institute of Communications Systems (ICS), Faculty of Electronics, MUT, where he started working, in 2003. Since January 2021, he has been the Institute Director. Since 2017, he has been a Principal Voting Member with the Information Systems Technology Panel operating within the NATO Science and Technology Organization. He has been an Expert of European Defence Agency (EDA) CapTech Information and the Office of Electronic Communication, since 2019 and 2022, respectively. Since 2001, he has been involved in many research and development projects for Polish Ministry of Defence, EDA, National Centre for Research and Development, and National Science Centre. Currently, he is the Manager of four research projects and the supervisor for ten Ph.D. students. He has authored or coauthored more than 200 articles in peer-reviewed journals and conferences. He is a reviewer for 35 scientific journals and about 20 conferences. His current research interests include wireless communications, simulations, modeling, measurements of channels and propagation, quality of services, signal-processing, navigation, and localization techniques.

PIOTR RAJCHOWSKI (Member, IEEE) was born in Poland, in 1989. He received the E.Eng., M.Sc., and Ph.D. degrees in radio communication from Gdansk University of Technology (Gdansk Tech), Poland, in 2012, 2013, and 2017, respectively. Since 2013, he has been with the Department of Radiocommunication Systems and Networks, Faculty of Electronics, Telecommunications and Informatics, Gdansk University of Technology, as an IT Specialist, from 2013 to 2017, a Research Assistant, from 2017 to 2019, and has been an Assistant Professor, since 2019. Since 2020, he has been the Deputy Head of the Department. His research and science activity include being the Contractor of six research and development projects related to homeland security, radiolocalization, and modern wireless networks. From 2019 to 2020, he was the Early Career Investigator Representative of the COSTIRACON CA-15104 Action, now he participates the CA20120 Action. His main research interests include radiolocalization in modern sensor and cellular networks and aspects of the synchronization in the NB-IoT and 5G networks, especially in the harsh propagation conditions. He received the Young Scientists Award of URSI, in 2020, and some domestic awards like the Annual Award of the President of the City of Gdansk and Gdansk Scientific Society for Young Scientists.

JAROSŁAW MAGIERA received the Ph.D. degree (Hons.) from the Faculty of ETI, in 2015, and the Graduate degree from the Faculty of Electronics, Telecommunications and Informatics, Gdansk University of Technology, in 2009. His Ph.D. thesis: "Analysis and research on anti-spoofing system for GPS." Currently, he is an Assistant Professor with the Department of Radio Communication Systems and Networks, Gdask Tech. His research interests include digital signal processing, multi-antenna systems, physical layer security, and electronic warfare. From 2008 to 2023, he was engaged in ten research and development projects supported by EU and Polish National Centre for Research and Development. He is involved in NATO IST-187 working group and COST CA20120 INTERACT action.