Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 205 (2022) 258–267

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Military Communications and Information Systems (ICMCIS 2022)

Jamming and jamming mitigation for selected 5G military scenarios

Paweł Skokowski[a]*, Jan M. Kelner[a], Krzysztof Malon[a], Krzysztof Maślanka[a], Agnius Birutis[b], Miguel A. Vazquez[c], Souradip Saha[d], Warren Low[e], Agnieszka Czapiewska[f], Jarosław Magiera[f], Piotr Rajchowski[f], Sławomir Ambroziak[f]

[a]*Military University of Technology, gen. Sylwestra Kaliskiego 2 street, Warsaw, 00-908, Poland*
[b]*Norwegian Defence Research Establishment, Instituttveien 20, Kjeller, NO-2007, Norway*
[c]*Centre Tecnològic de Telecomunicacions de Catalunya, Avinguda Carl Friedrich Gauss 7, Castelldefel , 08-860, Spain*
[d]*Fraunhofer FKIE, Fraunhoferstraße 20, Wachetberg, 53-343, Germany*
[e]*NATO Allied Command Transformation (ACT), 7857 Blandy Rd STE 100, Norfolk, VA 23-551, USA*
[f]*Gdańsk University of Technology, Gabriela Narutowicza 11/12 street, Gdańsk, 80-233, Poland*

Abstract

This paper presents jamming and jamming mitigation techniques, which can be used in relation to emerging military systems based on fifth-generation (5G) technology. Nowadays, 5G technology provides incremental improvements over Long Term Evolution (LTE) networks resulting in the enhancement of civilian communications. Considering enormous possible applications of this new technology, it is feasible to use them in military utilities. The authors want to introduce the most important aspects related to the 5G system vulnerability in the context of its use in military scenarios. We also present a quality analysis of adequate solutions for 5G to mitigate the jamming and improve the system immunity. The description of use case scenarios depicts how 5G applications can fit in typical use cases.

Keywords: : jamming; jamming mitigation; 5G technology; military communications; military scenarios; technological gaps.

* Corresponding author. Tel.: +48 261 837 622.
E-mail address: pawel.skokowski@wat.edu.pl

10.1016/j.procs.2022.09.027

1. Introduction

Civilian wireless networks are designed to maximize the overall throughput and coverage yet maintaining a low communication latency. These systems do not consider the tentative transmission of malicious radio signals to preclude the connectivity of the user terminals. As a result, general cellular communication standards such as long-term evolution (LTE), LTE Advanced (LTE-A), LTE-A Pro, and current fifth-generation New Radio (5G-NR) suffer from certain vulnerabilities whenever jamming signals are present in the available spectrum [1–5].

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 [6,7]. Military systems are additionally exposed to intentional interference, i.e., jamming [8]. Jamming is one of the essential elements of electronic warfare (EW) and is designed to interrupt or prevent effective communications by enemy troops [9,10]. Hence, military wireless communication systems must be designed to provide major resistance to interference and to still provide reliable operation in a contested electromagnetic 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 also being developed. This last issue concerns both civilian and military systems regarding unintentional and intentional interference, respectively.

Currently, one can observe the implementation of 5G systems in civilian markets. 5G technologies provide significant improvements, such as increasing bandwidth and reliability, reducing delays, and increasing network density [11,12]. The use of higher frequency ranges, i.e., millimeter-waves (mmWave) in 5G and terahertz (THz) frequencies in the upcoming sixth-generation (6G) [13] offers the possibility of significantly increasing wireless capacity and solving critical problems related to radio resource management. However, the introduction of a higher frequency of radio waves is accompanied by an increase in attenuation and range degradation. It turns out that from the military point of view, this aspect may also have a positive consequence. In the 5G systems, new and older radios and networking technologies are used, such as massive multiple-input-multiple-output (massive MIMO), Internet of Things (IoT), massive-IoT, full-duplex, device-to-device (D2D) communications, software-defined networking (SDN), network functions visualization (NFV), mobile edge computing (MEC), fog computing (FC), open- (O-RAN) and cloud - (C-RAN), ultra-dense network (UDN), or self-organizing network (SON), and other multiple access (MA) techniques like pattern division MA (PDMA) or non-orthogonal MA (NOMA) [11,12]. 5G revolution is being considered to be implemented for military communications systems within the next decade [14–16]. Activities are undertaken by the national companies and research centers as well as within the framework of international cooperation, such as

- research task group (RTG) IST-187-RTG on “5G Technologies Application to NATO Operations” operating within the Information Systems Technology (IST) Panel at the NATO Science & Technology Organization (NATO STO) [17];
- 5G Military Security Workshop hosted by the NATO Allied Command Transformation (ACT) and Cooperative Cyber Defence Centre of Excellence (CCDCOE) in 2021 [18];
- workshops on “5G for Defense” (2019-2021) organized by CapTech Communication Information Systems and Networks (CapTech Information in short), the result of which was the development of “5G technologies for defence. White paper” [19];
- IEEE Workshop on 5G Technologies for Tactical and First Responder Networks (2018–2021, the 4th edition in 2021) [20].

The introduction of 5G applications to military communication systems is also associated with new jamming and anti-jamming techniques. In [21], the authors present the concept of using 5G technology for increasing soldier survival on the battlefield. The idea is to monitor the soldiers’ psychophysical states and collect this information by the commander. Based on this, the commander may take specific actions to save the life and health of soldiers. An important thing that should be considered is the presence of jammers, which can distort ongoing communication. For example, a battlefield situation with a jammer is presented in Fig. 1.

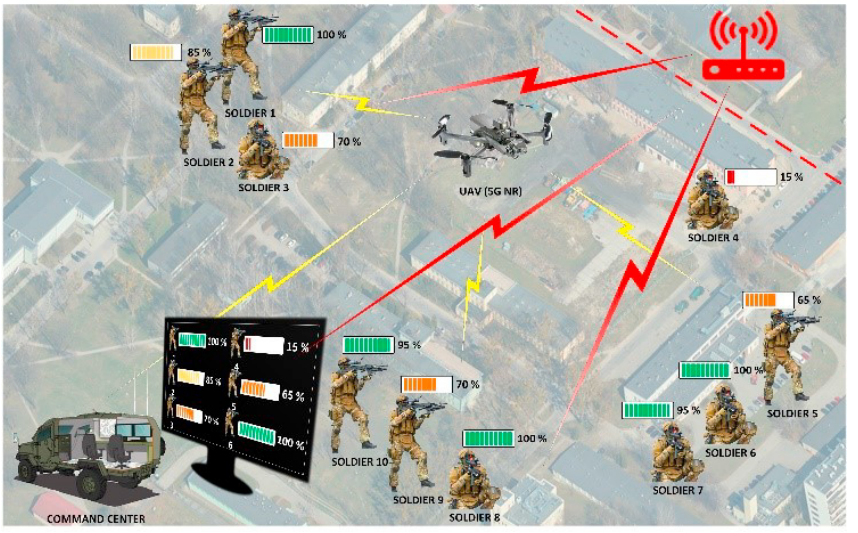

Fig. 1. Example battlefield situation with jammer.

In the literature, one can find a description of modern jamming techniques, e.g., [5,22,23]. However, the previous works on the jamming techniques are being analyzed in civilian systems because military 5G systems do not exist. This paper shows possible trends in jamming and jamming mitigation techniques in the context of selected technologies and 5G military scenarios (i.e., use cases). From this viewpoint, this approach can be considered innovative. The presented analysis is the result of the preliminary work of one of the IST-187 teams.The remainder of the paper is organized as follows. In Section II, the possible use of the 5G technology in the military scenarios is described. In Sections III and IV, jamming and jamming mitigation techniques are presented, respectively. Section V covers 5G analysis in jamming environments for the proposed military scenarios. Finally, we summarize the paper in Section VI.

2. 5G military scenarios

In the literature, one can find a description of modern jamming techniques, e.g., [5,22,23]. However, the previous works on the jamming techniques are being analyzed in civilian systems because military 5G systems do not exist. This paper shows possible trends in jamming and jamming mitigation techniques in the context of selected technologies and 5G military scenarios (i.e., use cases). From this viewpoint, this approach can be exist. This paper shows possible trends in jamming and jamming mitigation techniques in the context of sel In this section, a brief description of use case scenarios with high relevance to military requirements is provided. For example, wireless communications required by multinational joint forces of a coalition of different military bodies can include command and control (C2) capabilities supporting [24,25]:

- Land operations;
- Naval operations and;
- Air-based or non-terrestrial operations.

Combination of these operations includes amphibious or coastal operations, air support for extending coverage range beyond-line-of-sight (BLOS) communications, intelligence or information gathering, and reconnaissance. These operations can be considered from different operational levels like operational and tactical levels.

Additionally, sustainment operations like logistics and asset tracking, enhanced mobile training, resource transportation, management, etc., also require robust communication systems. The enhancement of existing technologies or entirely novel features that 5G networks could provide can include a variety of applications in the aforementioned scenarios.

Down selecting from the wide range of choices of military use cases, we focus only on the tactical land operations, including C2 headquarters (HQs), vehicular (tanks/mechanized infantry), and infantry units and support units. Special cases include deployable headquarters (DHQs), segregated into large DHQ and small DHQ with differing network requirements. These use cases are used to identify how jamming mitigation techniques based on 5G can aid in military operations.

2.1. Land tactical operations

The lower echelon units (including vehicular or infantry units) in tactical land operations need to communicate with their command posts or headquarters, which need to communicate back to the subordinate troops or joint force command HQ. For such operations, uninterrupted, low latency, high quality-of-service (QoS) network infrastructure is necessary for which robust tactical waveforms and network protocols are required. During mission-critical situations, the EW threat levels are deemed high with the presence of active jammers by the adversarial forces.

Multiple 5G-based concepts can be employed to augment the performance of tactical land networks and associated waveforms, as follows,

- A fixed private macro 5G-NR cell (at sub–1 GHz, particularly ~700 MHz band or sub–6 GHz, particularly ~3.6–3.8 GHz, i.e., C band) deployed at an HQ level to provide reach-back connectivity to sub-ordinate units.
- In the presence of 5G non-terrestrial networks (NTNs), reach-back connectivity can be provided to increased coverage range in challenging topographical conditions. NTN can also support communications in the C band and mmWave Ka band (i.e., ~26 GHz).
- Connectivity using sidelink or integrated access backhaul (IAB) for a distributed/meshed topology reduces the vulnerabilities of a centralized network (single point of failure) architecture while providing an extended coverage range
- Beamforming gains spatial diversity and provides better QoS on limited link/power budget and spectral diversity for opportunistic utilization of licensed/shared spectral bands. It is complemented by massive MIMO modules, which improve the resource management aspects and diminishes the risks of being eavesdropped upon by adversarial radios.
- Enhanced mobile broadband (eMBB) channel type can provide increased throughput to accommodate multimedia services for remote nodes, particularly in benign electromagnetic environments. In addition, robust multiplexing techniques can easily re-direct resource utilization to ultra-reliable low latency channel (uRLLC) type communications in combat scenarios.

5G technologies offer opportunities to design cost-effective, interoperable, resilient network architectures required by military applications and standards. However, to deploy the 5G technologies, resistance to jamming must be incorporated either through standard or non-standard 3rd Generation Partnership Project (3GPP) 5G specifications.

2.2. Brigade-size deployable HQ

In this sub-section, we describe a brigade-sized DHQ as shown in Fig. 2, which is a small tactical land unit composed of one main communication information system (CIS) unit, tents or shelters (static units) housing the command and HQ staff, and some mobile (vehicular or infantry) units supporting potentially several hundred militaries. The DHQ is expected to be within a small operational area with a maximum required transmission range of hundreds of meters. In addition, this DHQ needs to have a small electromagnetic (EM) footprint owing to its proximity to the actual battlefield area.

During the initial stages of a conflict, this DHQ encounters a relatively benign EM environment in spite of close proximity to projected combat areas. Therefore, a private, single-tier, high capacity, 5G-NR base stations with combined wireless local area network (WLAN) – wireless metropolitan area network (WMAN), ideally operating in the C band (mainly 4.4–5.0 GHz, also referred to as NATO Band IV), from a single wireless point-to-multi-point (PTMP) system connecting the CIS to network terminals, is a quick and convenient option for operational Headquarters that is expected to move depending on the operations. Although the NATO Band IV is not ideal for

wireless communications, it is desirable for spectral management. When combined with 5G NR features like beamforming, massive MIMO, and dynamic/adaptive non-orthogonal modulation schemes, it can provide the desired QoS and limit the spillage of the radio signatures. Further, to a lower capacity, a coverage layer network at the sub–1 GHz frequency is also required to provide information exchange with subordinate Battalion Headquarters (BH).

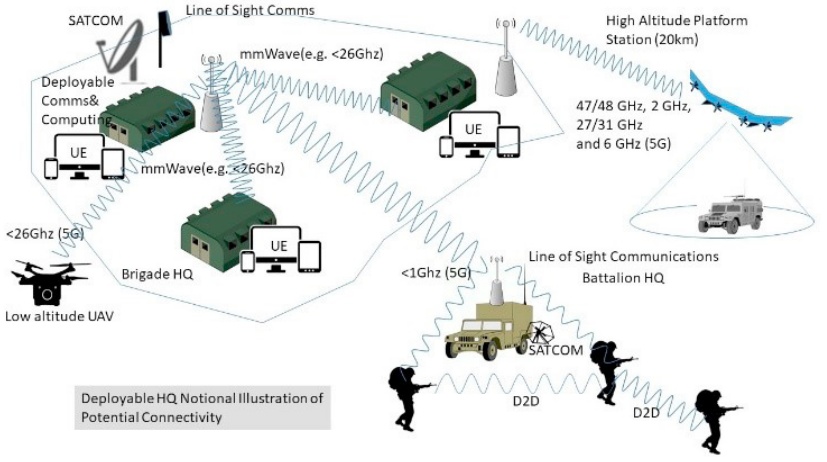

Fig. 2. Example of brigade-size DHQ unit in tactical land operations.

Over time, at the height of the conflict, however, such DHQs are subject to high levels of the EW with the presence of active jammers over multiple frequency bands. The remainder of the paper proposes several methods to mitigate or reduce the effects of jamming on the performance of the deployed HQ.

3. Jamming techniques

There are many jamming techniques with specific features. Every jammer type differs from each other while considering power efficiency, complexity, probability of detection vulnerability.

The most current and common kinds of jammers related to the newest wireless communications systems are [5]:

- Regular jammer:
  - continuous transmission of a jamming radio signal (legitimate bit sequences or random bit sequences);
  - the high amount of power is needed (short battery life);
  - knowledge about the medium access control (MAC) layer protocol of the jammed system is not required;
  - easy to detect.
- Delusive (deceptive) jammer:
  - continuous transmission of a jamming radio signal (legitimate bit sequences);
  - the high amount of power is needed (short battery life);
  - goal – mislead the receiver and force it to wait in the listening state;
  - harder to detect than the regular jammer.
- Random jammer
  - active and idle states;
  - regular or deceptive jamming during the active states;
  - reduced power consumption (sleep mode).
- Responsive jammer:
  - monitoring of the communication channel;
  - transmission of a jamming radio signal only if the transmitter is active;
  - power-efficient.

- Go-next jammer:
  - selective jamming (one frequency channel at a time);
  - follows the transmitter frequency channel;
  - power-efficient, but it depends on the frequency hopping rate of the transmitter.
- Control channel jammers:
  - targets the control channel;
  - acts before initiation of the communication;
  - cause denial of service.

Considering how and when the radio signal may be jammed, we can focus on the corresponding 5G technology.

3.1. Physical layer vulnerabilities of 5G NR

Jamming vulnerability analysis of each specific channel and signal of the 5G-NR is crucial. According to [26], the extent to which a channel or signal is susceptible to jamming is highly influenced by the sparsity of that channel or signal concerning all resources (time and frequency grid). One of the factors that can reduce the potential vulnerability of resources is their mapping on the time-frequency grid using a dynamic scheme that involves higher-layer parameters. In these cases, a jammer does not know about such a structure.

The most effective jamming attacks on the 5G physical layer (PHY), considering the complexity and attack efficiency (jamming-to-signal ratio for given radiated power), are those that may interfere [22]:

- Synchronization Signals:

To jam the Primary Synchronization Signal (PSS) and Secondary Synchronization Signal (SSS), one must synchronize to the cell in time and identify the subcarrier spacing (which might already be known beforehand using publicly available band plans) and then transmit/radiate interference selectively in time.

- Physical Broadcast Channel:

To block UEs to access critical information, which is needed to connect to a cell, one must jam the physical broadcast channel (PBCH) (preventing new UEs from accessing one or more cells). When the jammer can synchronize to the target cell, then it may distort PBCH in a time-selective manner. The other solution is that the jammer can easily jam the PBCH subcarriers (i.e., PBCH uses 100% duty cycle).

- Physical Downlink Control Channel"

First, the physical downlink control channel (PDCCH) appears on any subcarrier, so the jammer shall decode the parameter CORESET-freq-dom [22,27]. Second, the parameter CORESET-time-dur indicates the numbers of orthogonal frequency division multiplexing (OFDM) symbols the PDCCH occupies in each slot [22,27]. The PDCCH channel starts in the first symbol of each slot and is modulated using a quadrature phase-shift keying (QPSK) scheme with polar coding. Assuming knowledge of CORESET-freq-dom, the jammer would have to jam all of those subcarriers to jam all possible PDCCH locations in the time-frequency grid [22].

3.2. Vulnerableness of massive MIMO to jamming

Massive MIMO is vulnerable to jamming attacks. Jamming MIMO systems targets the channel estimation process realized by these systems. Targeting the channel estimation procedure launch active jamming attacks against unsuspecting users. Those attacks are feasible by way of analysis, simulations, and real-world experimentation. Therefore, accurate channel estimation under jamming attacks is essential to get the desired performance by the massive MIMO. Therefore, finding proper techniques for accurate channel estimation is essential. Developing a channel estimator for which performance is not affected by jammers or consider their impact is fundamental.

4. Jamming mitigation techniques

Focusing on the 5G-NR downlink transmission, the anti-jamming techniques must consider the supporting air interface, MIMO, and OFDM. This PHY enabling technology supports a well-known anti-jamming strategy: frequency hopping. In this modulation, the communication is done over a specific subcarrier whose location in the

frequency domain changes temporally. Therefore, both transmitter and receiver must know in advance the temporal subcarrier hops.

Despite the fact that frequency hopping modulation eliminates the impact of the wideband jamming attacks (the jamming signal does not occupy the entire available bandwidth), frequency hopping might fail if the jammer is narrowband and follows the legitimate transmission subcarrier. In other words, whenever the jammer can detect the useful subcarrier and transmit in the same frequency band, the frequency hopping resilience is dramatically decreased.

However, if the receiver is equipped with multiple antennas, spatial filtering can be used to mitigate the jamming signal if the receiver knows its spatial signature. Indeed, the MIMO filtering success relies on the receiver capability to acquire the jamming spatial covariance matrix. Fortunately, since the follower jamming signal has a certain delay between the hops, the receiver can use this silent time to determine the jammer spatial covariance matrix and compute the spatial receiver filter. In [28], this technique has been developed considering that the legitimate transmitter performs a narrowband communication. Other narrowband anti-jamming schemes can be found in [29–31].

More and more advanced beamforming techniques are being implemented into 5G radio systems, especially at the Base Station (BS) side. Beamforming is primarily implemented to increase the spectral efficiency for a 5G network, but it might naturally provide some additional robustness to the communication system simply because the downlink signal is directed and concentrated towards the users. Thus, the received signal at the UE is strengthened. This is beneficial when the downlink signal has to compete with a jamming signal to achieve an acceptable signal-to-interference-plus-noise ratio (SINR).

Another aspect to consider is limited transmit power in the uplink. Uplink transmission is much weaker than downlink transmission, where BS provides transmit powers in hundreds of watts supplemented with directive beams. In contrast, present-day commercial UEs transmit uplink data through omnidirectional antennas with less than one watt total radiated power (TRP). A weak uplink signal makes it difficult for the communication system to compete with a jammer transmitting strong interference in the uplink towards the BS. The UE transmit signal must be made more robust by either operating with external antennas, implementing beamforming to increase directivity, or revising the standards to allow higher uplink power for some exceptional use cases. However, inter-cell and inter-user interference could increase and must be considered.

Vulnerable transmission in uplink might become more resilient by utilizing massive MIMO technology. A BS equipped with a Massive MIMO system can receive multiple streams from multiple users simultaneously and separate those streams by the direction from which they arrive. The UEs transmit pilot signals during the training phase so that the BS can estimate their radio channels and then apply the spatial multiplexing. Authors in [4,32–34] suggest that with a proper radio channel estimation of the legitimate users and the jammer, the jamming signal, arriving from a given direction, could be detected, separated and suppressed by the array antenna in massive MIMO. If the legitimate pilot signals are contested, and the BS has no estimate of the jamming signal radio channel, the BS will not be able to suppress jamming efficiently. To fully utilize antenna array features of the Massive MIMO in suppressing the jamming, authors in [32–34] suggest exploiting the unused time-frequency resources to channel estimation of the jamming signal. During this phase, none of the users is transmitting, so the BS can detect jamming, estimate its radio channel and nullify it in the digital signal-processing phase.

5. 5G in jamming environments for presented military scenarios

The scenarios described in Section II proposed to use the following 5G technologies in military applications: mmWave, MIMO, NTN, IAB, beamforming, eMBB. For example, in the brigade-size DHQ unit in the tactical land operations depicted in Fig. 2, one must take care not only for keeping services, when the EW is considered.

We cannot rule out opponents having all types of jammers (see Section III). Furthermore, depending on the used 5G technology, its susceptibility to interference varies. Therefore, it is necessary to consider such methods of avoiding interference tailored to a specific use case and application.

As can be noticed, D2D communication may be easily jammed due to the near proximity of possible jammer (battlefield or just out of the board of our basecamp). In this particular case, if we want to increase the resistance to

interference, we can, e.g., switch to mmWaves - this will reduce the range within, e.g., the platoon (although communication should be maintained anyway), but potentially prevent transmission interference. In these cases, it is the need to place the jammer closer to the radiation sources due to higher attenuation of high frequency.

For all types of jammers – MIMO enables the avoidance of intentional interference through spatial filtering, which can be used, e.g., in communication inside basecamp between BS and UEs (brigade HQ).

For more energy-efficient jammers (e.g., responsive jammers), it is necessary to monitor the enemy's radio activity. During using beamforming, monitoring of energy for a directed narrow beam of the electromagnetic wave is significantly difficult. The location of the jammer is essential in this case – if it is in the wrong place – the level of received power will be too low to detect the radio activity.

Similar considerations could be made for all technologies used in the presented scenarios. However, due to the limited scope of this paper, they will not be referenced here. The most important conclusion that seems to be the basis for considering the use of 5G technology in military applications is as follows: known solutions for jamming mitigation should be considered in the new 5G release.

6. Conclusions

5G technology is showing promise as a critical enabler for many civil market applications. The possibility analysis of this technology prompts for real consideration of its implementation in future military communication systems. However, it requires searching for and patching weaknesses and technological gaps in the civilian standard to adapt it to combat conditions. In this case, resilience and counteracting intentional interference that is a part of EW is one of the crucial issues. This paper is devoted to jamming and jamming mitigation techniques in forthcoming 5G military systems. This analysis was carried out in relation to selected scenarios of the 5G technology use in future military communication systems. In the description of the use cases, we indicated important technologies that should be used in military systems. On the other hand, we have shown how critical technology gaps in the civilian standard can be exploited in the jamming of such communication systems. Hence, we finally proposed possible jamming mitigation techniques. The presented analysis may be the basis for the development of future solutions that are more resistant to intentional interference.

Further work by the IST-187-RTG will allow for identifying the potential areas of 5G-NR applications in the military domain and which elements of the systems require improvement or modification to meet the requirements of operational activities. We also plan to conduct a similar analysis for a wider spectrum of potential military use cases.

Acknowledgements

This paper is a collaborative work of members from the IST-187-RTG on “5G Technologies Application to NATO Operations” operating within the IST Panel at the NATO STO.

This work received funding by:

- •the Spanish Ministry of Science and Innovation under project: IRENE(PID2020-115323RB-C31/AEI/10.13039/501100011033) and grant from the Spanish ministry of economic affairs and digital transformation and of the European union – NextGenerationEU [UNICO-5G I+D/AROMA3D-Space (TSI-063000-2021-70);
- the Polish Ministry of Defense under research grant: UGB 22-740 “Modern technologies of wireless communication and emission sources localization in various system applications”.

References

[1] R. P. Jover, J. Lackey, and A. Raghavan, “Enhancing the security of LTE networks against jamming attacks,” EURASIP J. Inf. Secur., vol. 2014, no. 1, p. 7, Apr. 2014, doi: 10.1186/1687-417X-2014-7.

[2] Q. Yan, H. Zeng, T. Jiang, M. Li, W. Lou, and Y. T. Hou, "MIMO-based jamming resilient communication in wireless networks," in 2014 IEEE Conference on Computer Communications (INFOCOM), Toronto, ON, Canada, Apr. 2014, pp. 2697–2706. doi: 10.1109/INFOCOM.2014.6848218.
[3] L. Sanguinetti, E. Björnson, and J. Hoydis, "Toward massive MIMO 2.0: Understanding spatial correlation, interference suppression, and pilot contamination," IEEE Trans. Commun., vol. 68, no. 1, pp. 232–257, Jan. 2020, doi: 10.1109/TCOMM.2019.2945792.
[4] Y. O. Basciftci, C. E. Koksal, and A. Ashikhmin, "Securing massive MIMO at the physical layer," in 2015 IEEE Conference on Communications and Network Security (CNS), Florence, Italy, Sep. 2015, pp. 272–280. doi: 10.1109/CNS.2015.7346837.
[5] Y. Arjoune and S. Faruque, "Smart jamming attacks in 5G New Radio: A review," in 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, Jan. 2020, pp. 1010–1015. doi: 10.1109/CCWC47524.2020.9031175.
[6] K. Bechta, J. M. Kelner, C. Ziółkowski, and L. Nowosielski, "Inter-beam co-channel downlink and uplink interference for 5G New Radio in mm-wave bands," Sensors, vol. 21, no. 3, Art. no. 3, Jan. 2021, doi: 10.3390/s21030793.
[7] 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.
[8] R. A. Poisel, Modern communications jamming. Principles and techniques, 2nd ed. Boston, MA, USA: Artech House Publishers, 2011.
[9] R. Poisel, Introduction to communication electronic warfare systems, 2nd ed. Boston, MA, USA: Artech House, 2008.
[10] R. Inkol, "Electronic warfare," Defence Research and Development Canada, Ottawa, ON, Canada, DRDC-OTTAWA-SL-2008-019, Oct. 2013. Accessed: Jul. 12, 2021. [Online]. Available: https://pubs.drdc-rddc.gc.ca/BASIS/pcandid/www/engpub/DDW?W%3Dadddate+ge+%2720130601%27+sort+by+adddate+descend%26M%3D783%26K%3D806524%26U%3D1
[11] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," IEEE Commun. Surv. Tutor., vol. 18, no. 3, pp. 1617–1655, 2016, doi: 10.1109/COMST.2016.2532458.
[12] A. Gupta and R. K. Jha, "A survey of 5G network: Architecture and emerging technologies," IEEE Access, vol. 3, pp. 1206–1232, 2015, doi: 10.1109/ACCESS.2015.2461602.
[13] W. Jiang, B. Han, M. A. Habibi, and H. D. Schotten, "The road towards 6G: A comprehensive survey," IEEE Open J. Commun. Soc., vol. 2, pp. 334–366, 2021, doi: 10.1109/OJCOMS.2021.3057679.
[14] F. T. Johnsen et al., "Application of IoT in military operations in a smart city," in 2018 19th International Conference on Military Communications and Information Systems (ICMCIS), Warsaw, Poland, May 2018, pp. 1–8. doi: 10.1109/ICMCIS.2018.8398690.
[15] 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.
[16] A. Bhardwaj, "5G for military communications," Procedia Comput. Sci., vol. 171, pp. 2665–2674, Jan. 2020, doi: 10.1016/j.procs.2020.04.289.
[17] "IST-187-RTG on 5G Technologies Application to NATO Operations," Technical Activities of the NATO Science & Technology Organization (NATO STO), 2020. https://www.sto.nato.int/Lists/test1/activitydetails.aspx?ID=16937&Sou (accessed Jul. 12, 2021).
[18] "First joint 5G military security workshop hosted by ACT and CCDCOE," CCDCOE. https://ccdcoe.org/news/2021/first-joint-5g-security-workshop-hosted-by-act-and-ccdcoe/ (accessed Jun. 19, 2021).
[19] V. Conan, R. Djapic, T. Ehlersson, T. Haas, H. Saarnisaari, R. Siekmeyer, et al., "5G technologies for defence," EDA CapTech Information, White paper 1.0, Jan. 2021.
[20] "2021 First Responder and Tactical Networks Workshop - IEEE Future Networks." https://futurenetworks.ieee.org/conferences/2021-first-responder-and-tactical-networks-workshop (accessed Jun. 19, 2021).
[21] P. Skokowski and K. Malon, "5G technology application for increasing soldiers' survival on the battlefield," in 2021 37th International Business Information Management Conference (IBIMA), Cordoba, Spain, May 2021, pp. 1–4. [Online]. Available: https://ibima.org/accepted-paper/5g-technology-application-for-increasing-soldiers-survival-on-the-battlefield/
[22] M. Lichtman, R. Rao, V. Marojevic, J. Reed, and R. P. Jover, "5G NR jamming, spoofing, and sniffing: Threat assessment and mitigation," in 2018 IEEE International Conference on Communications 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. Surv. Tutor., vol. 21, no. 3, pp. 2734–2771, 2019, doi: 10.1109/COMST.2018.2865607.
[24] L. Bastos, G. Capela, and A. Koprulu, "Potential of 5G technologies for military application," NATO Communications and Information Agency (NCIA), Hague, the Netherlands, Working paper NCIA/2020/NCB014792/03, Sep. 2020.
[25] L. Bastos and G. Capela, "Potential of 5G technologies for land and maritime tactical networks," presented at the 2020 3rd Workshop on 5G Technologies for First Responder and Tactical Networks, Oct. 2020.
[26] 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.
[27] 3GPP, "5G; NR; Physical channels and modulation (3GPP TS 38.211 version 16.6.0 Release 16)," European Telecommunications Standards Institute (ETSI), Sophia-Antipolis, France, ETSI TS 138 211 V16.6.0, Jun. 2021. [Online]. Available: https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=63346
[28] M. Nájar, X. Mestre, and M. A. Lagunas, "Two-stage code reference beamformer for the reception of frequency hopping modulated signals," Signal Process., vol. 80, no. 12, pp. 2623–2632, Dec. 2000, doi: 10.1016/S0165-1684(00)00144-4.
[29] L. Acar and R. T. Compton, "The performance of an LMS adaptive array with frequency hopped signals," IEEE Trans. Aerosp. Electron. Syst., vol. AES-21, no. 3, pp. 360–371, May 1985, doi: 10.1109/TAES.1985.310566.

[30] D. Torrieri, "An anticipative adaptive array for frequency-hopping communications," in 1987 IEEE Military Communications Conference (MILCOM), Washington, DC, USA, Oct. 1987, vol. 1, pp. 0276–0282. doi: 10.1109/MILCOM.1987.4795195.
[31] Y. Bresler, V. U. Reddy, and T. Kailath, "Optimum beamforming for coherent signal and interferences," IEEE Trans. Acoust. Speech Signal Process., vol. 36, no. 6, pp. 833–843, Jun. 1988, doi: 10.1109/29.1594.
[32] A. Kekirigoda et al., "Massive MIMO for tactical ad-hoc networks in RF contested environments," in 2019 IEEE Military Communications Conference (MILCOM), Norfolk, VA, USA, Nov. 2019, pp. 658–663. doi: 10.1109/MILCOM47813.2019.9020756.
[33] T. T. Do, E. Björnson, E. G. Larsson, and S. M. Razavizadeh, "Jamming-resistant receivers for the massive MIMO uplink," IEEE Trans. Inf. Forensics Secur., vol. 13, no. 1, pp. 210–223, Jan. 2018, doi: 10.1109/TIFS.2017.2746007.
[34] H. Akhlaghpasand, E. Björnson, and S. M. Razavizadeh, "Jamming suppression in massive MIMO systems," IEEE Trans. Circuits Syst. II Express Briefs, vol. 67, no. 1, pp. 182–186, Jan. 2020, doi: 10.1109/TCSII.2019.2902074.