FFI Norwegian Defence Research Establishment

22/00906

FFI-RAPPORT

A study of 5G New Radio and its vulnerability to jamming

Agnius Birutis
Anders Mykkeltveit
Tore Ulversøy
Øystein Dag Borlaug
Jørn Kårstad

A study of 5G New Radio and its vulnerability to jamming

Agnius Birutis
Anders Mykkeltveit
Tore Ulversøy
Øystein Dag Borlaug
Jørn Kårstad

Norwegian Defence Research Establishment (FFI) 27 April 2022

Keywords
5G NR
Jamming
Mobilkommunikasjon
Radiokommunikasjon
Sårbarhetsanalyse

FFI report
22/00906

Project number
1556

Electronic ISBN
978-82-464-3406-3

Approvers
Åshild Grønstad Solheim, *Research Manager*
Jan Erik Voldhaug, *Director of Research*

The document is electronically approved and therefore has no handwritten signature.

Summary

Information and communication technology (ICT) is a critical factor needed by the Norwegian Armed Forces to succeed in their missions. Over the coming years, the Norwegian defence sector will invest heavily in new combat-near ICT solutions. Technologies developed for the civilian market are expected to be an integral part of this investment.

Commercial mobile technology is a technology that is developed for the commercial market and has gathered interest in the military worldwide as a cost-effective alternative to cover some of the military needs for communication services. The latest fifth generation of mobile communications (5G) can benefit the military in several domains, including radio communication. The 5G radio interface, called New Radio (NR), provides high transmission speeds and introduces some novelties like multi-antenna operation on high frequencies. However, a commercial technology like 5G NR is not explicitly designed to meet the military requirements for robustness. There is a lack of information on how well 5G NR performs when exposed to electronic warfare such as radio jamming. Insights into the effect of jamming are needed to assess operational scenarios in which 5G is safe for military use.

This report documents a study of the threat of radio jamming on the 5G NR. We introduce the necessary background on 5G NR. Then, we discuss 5G NR vulnerabilities to jamming based on theory and literature, but none of these previous studies have examined the effect of jamming on a complete and real-life 5G NR system. Therefore, we conducted a jamming experiment, creating a realistic scenario where a custom-made jammer aimed to disrupt a commercial 5G NR system that consisted of an off-the-shelf smartphone and a commercial base station antenna operating on the 3.6 GHz frequency band. The experiment showed that the uplink signal was the most vulnerable part of the radio communication, primarily because of the limited transmit power at the user terminal. The 5G radio system adapted to moderate jamming by lowering the modulation and coding scheme. However, in some cases, the 5G radio system struggled to find the optimal parameters. When the jamming signal was too strong, the 5G connection was terminated.

We identified a threshold (breaking point) at which a jamming signal was too strong for the 5G NR system to work. By combining our experimental results with theoretical propagation models, we developed a model that estimates the distance between a jammer and a base station and the jammer output power an adversary needs for a successful jamming attack. The model can help evaluate the threat level and decide whether or not 5G NR is suitable for a given military scenario.

We identified several practical mitigation measures that might make the 5G radio communication, especially the uplink transmission, more robust against radio jamming. Future studies should further investigate the implementation aspects of these jamming mitigation measures in the military use of 5G.

Sammendrag

Informasjons- og kommunikasjonsteknologi (IKT) er anerkjent av Forsvaret som en kritisk faktor for at de skal kunne løse sine oppgaver. De kommende årene vil forsvarssektoren investere store summer i kampnær IKT gjennom programmet Mime. Det forventes at mye av teknologien som tas i bruk er utviklet for det sivile markedet.

Kommersiell mobilteknologi er en slik teknologi som er utviklet for det sivile markedet og som de siste årene har fått mye oppmerksomhet fra forsvarssektoren i mange land som et kostnadseffektivt alternativ for å dekke noen militære behov for kommunikasjonstjenester. Femte generasjons mobilteknologi (5G) er nyeste generasjon mobilteknologi og kan utnyttes i militær sammenheng på flere måter, blant annet til radiokommunikasjon. Radiogrensesnittet i 5G, New Radio (NR), gir høy overføringshastighet samtidig som det tilbyr nye teknologiske løsninger som bruk av multi-antenner på høye frekvenser. Imidlertid er en kommersiell teknologi som 5G ikke spesifikt designet med tanke på å oppfylle militære krav til robusthet. Det er stor usikkerhet omkring hvordan 5G NR fungerer når det er utsatt for elektronisk krigføring slik som jamming. Innsikt i ytelsen til 5G NR under påvirkning av jamming er derfor viktig å ha for å kunne vurdere i hvilke operasjonelle scenarioer 5G er trygt å bruke under militære operasjoner.

Denne rapporten dokumenterer en studie av trusselen fra jamming mot 5G NR. Vi introduserer nødvendig bakgrunn om 5G NR. Deretter diskuterer vi sårbarheter 5G NR har for jamming, basert på teori og litteratur, men ingen av disse foregående studiene har undersøkt effekten av jamming på et virkelig 5G-system. Vi gjennomførte derfor et eksperiment der vi skapte et realistisk oppsett med en spesiallaget jammer og et kommersielt 5G NR-system som besto av en hyllevare-smarttelefon og en kommersiell antenne på en basestasjon som opererte på 3,6 GHz-frekvensbånd. Resultatene fra eksperimentet viste at signalet fra brukerutstyret til basestasjonen, kalt opplink, var mest sårbar, hovedsakelig på grunn av brukerutstyrets begrensede sendeeffekt. 5G-systemet viste seg å kunne tilpasses jamming med moderat effekt gjennom å redusere parameterne for koding og modulasjon. Imidlertid hadde 5G-systemet i noen tilfeller problemer med å finne riktige parameterverdier. Når signalet fra jammeren var for sterkt, ble 5G-forbindelsen terminert.

Ut fra resultatene fra eksperimentet identifiserte vi et jammenivå der jammestyrken var høy nok til å slå ut 5G-kommunikasjonen. Ved å kombinere resultatene med teoretiske propagasjonsmodeller utviklet vi en modell for å beregne den maksimale distansen en jammer kan ha til en basestasjon og likevel ødelegge 5G-kommunikasjonen med en gitt jammeeffekt. Denne modellen kan benyttes av Forsvaret til å evaluere jammetrusler mot 5G NR for å avgjøre om 5G er egnet for en spesifikk operasjon.

Vi identifiserte noen praktiske mottiltak som kan gjøre 5G-radiokommunikasjonen, spesielt overføringen i opplink, mer robust mot jamming. Fremtidige studier bør videre undersøke aspektene ved implementering av disse mottiltakene for jamming ved militær bruk av 5G.

Contents

1 Introduction

The Norwegian Armed Forces recognise information and communication technology (ICT) as a critical factor needed to solve their missions. The Norwegian Armed Forces also recognise that the fastest development of new technologies happens in the civilian sector [40].

One of the most advanced technological developments within the ICT domain occurs in the civilian commercial market for mobile communications. Specifically, the introduction of fifth-generation (5G) mobile technology in mobile networks brings new solutions that open up possibilities for new applications like communication between autonomous vehicles or support for virtual reality.

The Norwegian Armed Forces are interested in civilian communication systems, especially concerning new opportunities provided by 5G, which have the potential to fulfil the military ICT needs. The program *Mime* will renew the Norwegian Armed Forces' combat-near ICT systems in the coming years [42] and foresees widespread use of civilian ICT solutions [41]. Before commercial 5G technology can be integrated with the military communications networks, there is a need to disclose possibilities, limitations and vulnerabilities of 5G.

In the military domain, the electromagnetic spectrum may be contested by electronic warfare (EW). Traditional military communication systems are designed for use in situations where EW is a threat. One of the means in EW is radio jamming that has the intention to disrupt the radio communication of an opponent. A jammer tunes its frequency to the same frequency as targeted receiving equipment to corrupt the radio signal at the receiver. 5G is a civilian technology that has not been developed to withstand radio jamming. Figure 1.1 illustrates uplink and downlink jamming of a 5G radio system.

The objective of this report is to study the jamming vulnerabilities and resilience of the 5G radio interface called New Radio (NR). The report aims to determine the theoretical vulnerabilities of the 5G NR and the practical impact the jamming attacks might have on the 5G communication.

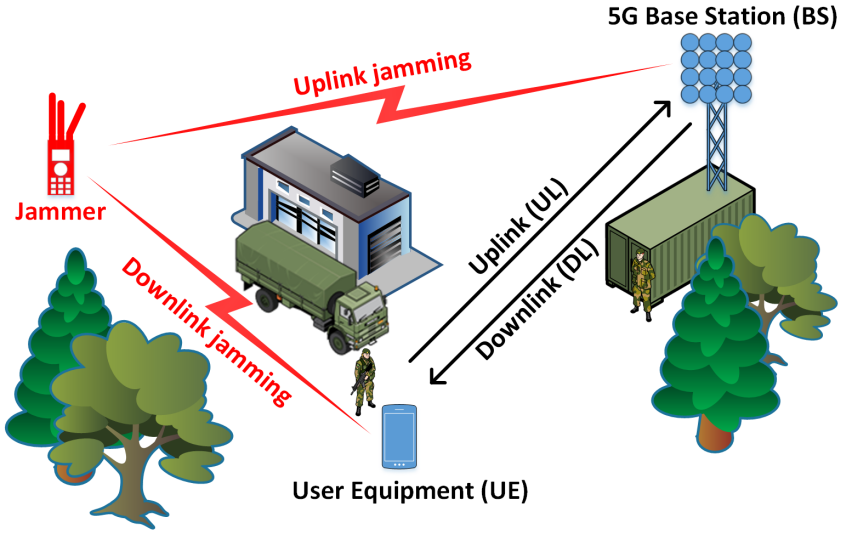


Figure 1.1 Illustration of uplink and downlink jamming of a 5G radio system.

1.1 Method

First, we studied the general theory and background of the 5G NR, focusing on relevant parts regarding vulnerabilities and robustness of the 5G waveform. We inspected types of jamming attacks and their effectiveness against 5G NR.

There are numerous theoretical studies of the vulnerability of mobile communications available. However, the literature contains few studies on experimental jamming of the 5G radio communication in a real-life scenario. Therefore, we designed a realistic jamming experiment to determine the characteristics of 5G NR in a contested radio frequency (RF) environment. The base station (BS) and user equipment (UE) were commercially available equipment providing a real-world scenario. The jamming equipment consisted of a signal generator, power amplifier and a custom-made antenna. We tested the 5G performance at various locations that vary in distance and line-of-sight (LOS)/non-line-of-sight (NLOS) propagation conditions between the UE, BS and jammer as different jamming set-ups were applied to disrupt the 5G communication.

Lastly, we analysed the measured data, generalised the results and modelled predictions for the jammer range. We also proposed some jamming mitigation measures worth further study to achieve more robust 5G radio communication.

1.2 Scope

The experiment was limited to a simple form of jamming. The entire or a part of the 5G band was filled with the interfering signal. This type of jamming was not explicitly designed for 5G. It was the easiest waveform to implement, but at the same time, its simplicity makes it a frequent choice for a jamming attack. The 5G equipment used in the experiment operated on a frequency band at 3.6 GHz.

1.3 Earlier work

FFI has conducted several studies of the mobile technology use for the military applications, mainly focusing on various aspects of 4G [25], [27], [28], [32]. The study in [50] conducts a vulnerability analysis of the 4G radio interface. When it comes to 5G, two FFI external notes have been published. The study in [24] provides an overview of the possibilities and security challenges of 5G adoption in the Norwegian Defence. The work in [21] presents early measurements of the 5G coverage and performance.

1.4 Research paper

As an output of this study of 5G NR and its vulnerability to jamming, the authors have also written a research paper titled "Practical Jamming of a Commercial 5G Radio System at 3.6

GHz", describing the jamming experiment and its results [16]. The paper has been accepted at the peer-reviewed conference International Conference on Military Communications and Information Systems (ICMCIS 2022).

The paper includes the main results of the experiment, while this report additionally presents the relevant theory of 5G NR and its vulnerability to various jamming attacks. The report also has a more detailed description of the experiment and presents broader results, including a model derived to predict the jammer range.

1.5 Outline

Chapter 2 introduces the relevant theory of 5G New Radio, which includes an overview of the physical layer specifications, antenna technology and radio communication procedures. Chapter 3 presents the theory of the 5G radio interface vulnerabilities to jamming. Chapter 4 describes the experiment set-up, including the specifications of the 5G base station, measurement equipment and jamming equipment. It also presents the jamming approach and the method of measuring the 5G performance. Chapter 5 presents the results of the measurements and introduces modelling of a successful jamming attack and operational jammer range. Chapter 6 discusses the results and provides some jamming mitigation measures for further studies. The conclusion of the report is given in Chapter 7.

2 5G New Radio (NR) theory relevant for jamming

5G is the fifth generation of mobile communication technology which is the basis for the services provided to billions of people globally. A complete 5G system consists of several components that deliver the data and voice services we use every day. The users have their user equipment (UE), e.g. a smartphone or broadband router. The UE connects to a base station (BS) over a radio interface named 5G New Radio (NR). The base stations connect to the 5G core network that handles user subscriptions and delivers data between users and external networks like the Internet. Figure 2.1 illustrates the key components of a standard 5G system.

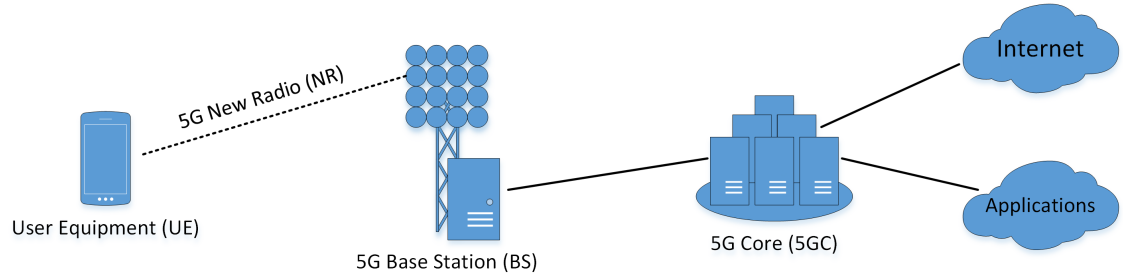


Figure 2.1 Key components of a standard 5G system.

This report focuses almost exclusively on the 5G NR, the UE and BS.

2.1 Frequency ranges

The data transmitted wirelessly occupies a certain bandwidth located at a certain carrier frequency in the frequency spectrum. The frequency spectrum is wide, but different frequencies have different characteristics. The spectrum that is suitable for mobile communications is limited, making it a finite, thus costly resource. National governmental authorities strictly regulate and license the frequency spectrum. The blocks of the frequency spectrum dedicated to mobile communications are usually auctioned and sold to the network operators.

The frequency spectrum used in the 5G NR is divided into frequency range 1 (FR1) and frequency range 2 (FR2). FR1 ranges over 410–7125 MHz, while FR2 covers a frequency interval of 24.25–52.6 GHz [13]. FR1 is known as the sub-6 frequency range in the 5G context, while FR2 is often called the millimetre wave frequency range (mmWave). Frequency ranges are further divided into smaller and well-defined frequency bands where an exact portion of the frequency spectrum is defined for the uplink and downlink. The name of a frequency band is given by "n" followed by a number. Table A.1 and A.2 in Appendix A provide a complete overview of all the NR frequency bands defined by 3GPP [2].

Not all frequency bands defined for 5G will be suitable to utilise in practice. Some bands are more relevant than others because of the frequency spectrum availability on the national or regional level. Also, different frequency bands have different characteristics suitable or not suitable for specific applications. Most globally popular bands can be found by exploring the market of user terminals.

Next Generation Mobile Network Alliance (NGMN) is a market representation partner for 3GPP, which ensures that the standards for the next generation network will meet the requirements of the operators and meet the end users' expectations [1]. NGMN has categorised 5G user equipment for different use cases [20]. The document contains technical requirements for mobile 5G devices such as mobile phones or tablets. The technical requirements include 5G frequency bands specified for 5G chipsets as either mandatory or recommended in the multi-band operation.

Table 2.1 provides an overview of frequency bands specified in [20] as mandatory for FR1 and recommended for FR2. For each frequency band in the table, a descriptive frequency, precise frequency ranges and duplex mode are given. The descriptive frequency acts as an additional name for the frequency band. Duplex mode specifies how the mobile network handles two-way communication in uplink and downlink. 5G NR supports two duplex modes, frequency-division duplexing (FDD) and time-division duplexing (TDD). FDD is a duplex mode where the uplink and downlink transmission occurs simultaneously using different frequencies. Therefore, separate frequency ranges must be specified for uplink and downlink. TDD is a duplex mode where uplink and downlink transmission occurs at different times but on the same frequency [17]. Therefore, only one frequency range is specified for the frequency bands in TDD mode.

Frequency range	Frequency band	Descriptive frequency	UL frequency range [MHz]	DL frequency range [MHz]	Duplex
FR1 below 1 GHz	n5	850 MHz	824–849	869–894	FDD
	n8	900 MHz	880–915	925–960	FDD
	n20	800 MHz	832–862	791–821	FDD
	n28	700 MHz	703–748	758–803	FDD
	n71	600 MHz	663–698	617–652	FDD
FR1 1–3 GHz	n1	2100 MHz	1920–1980	2110–2170	FDD
	n3	1800 MHz	1710–1785	1805–1880	FDD
	n7	2600 MHz	2500–2570	2620–2690	FDD
	n25	1900 MHz	1850–1915	1930–1995	FDD
	n40	2300 MHz	2300–2400		TDD
	n41	2500 MHz	2496–2690		TDD
	n66	1700 MHz	1710–1780	2110–2200	FDD
FR1 3–6 GHz	n77	3.7 GHz	3300–4200		TDD
	n78	3.6 GHz	3300–3800		TDD
	n79	4.7 GHz	4400–5000		TDD
FR2 24–30 GHz	n257	28 GHz	26500–29500		TDD
	n258	26 GHz	24250–27500		TDD
	n261	28 GHz	27500–28350		TDD

Table 2.1 The most relevant 5G frequency bands from the perspective of user equipment manufacturers. The bands given in FR1 are mandatory, while the bands given in FR2 are recommended for a 5G chipset to support [20].

The frequency bands given in Table 2.1 reflect which 5G frequencies manufacturers and mobile network operators (MNOs) focus on around the world. However, the frequency bands relevant

internationally do not necessarily have as much relevance nationally. MNOs in Norway must have a license to use a given part of the frequency spectrum for commercial mobile communications.

Some of the 5G frequency bands overlap with today's 4G bands, meaning that, potentially, the MNOs will retain the license to use these frequency blocks for the 5G communication. 5G brings a new technology called dynamic spectrum sharing (DSS). The DSS makes it possible to share a 4G frequency band between 4G and 5G services. An operator with a licence for 4G use in a specific frequency range can use this 4G frequency for 5G radio communication by utilising DSS, which adapts spectrum usage by demand.

Some of the new 5G frequency bands are temporarily licensed for testing purposes of early pilots and deployments. However, when the testing period is over, such frequency blocks will be divided and auctioned together with relevant 5G frequency bands. The auctions are held by the Norwegian Communications Authority (Nkom) that manages frequencies for mobile networks, radio and television in Norway [37].

Some 5G bands overlap with the spectrum reserved to military use in Norway. The use of the military bands is coordinated by the National Allied Radio Frequency Agency Norway (NARFA NOR).

By combining the frequency bands that manufacturers implement on user terminals worldwide and the frequency licences applicable in Norway, we can identify 5G frequency bands relevant in Norway. Table 2.2 provides an overview of the relevant frequencies for 5G use in Norway as of March 1, 2022. The table contains today's use, potential future use and 5G license of these most relevant frequency blocks. The information provided in the table is constantly changing and requires regular updates.

2.2 Physical layer

5G NR protocols include a user plane and a control plane, two widely used terms in radio communication. Data that a user sends to or receives from a network, for example, speech and multimedia, are carried through the user plane. The control plane passes the control traffic that carries signalling data necessary to initiate, authenticate, authorise and configure the connection between a user device and a network. Figure 2.2 provides an overview of the Open Systems Interconnection (OSI) model-based layers 1–3 and their services and protocols involved before the physical signal is emitted into the air and after it is received.

In this report, we focus on the physical layer. In the 5G communication between a base station and user equipment, the physical layer encodes raw data bits into a radio signal and transmits it over the air. The layer is also responsible for receiving the radio signal and decoding it back to the digital bits. The data that needs to be transmitted reaches the physical layer organised into so-called transport blocks. A transport block is simply a block of a fixed number of data bits. Figure 2.3 shows some of the key components of the physical layer in 5G NR, which are needed to convert the digital information into a radio signal at the transmitter and the inverse process of converting the radio signal back to the digital bits at the receiver. The process of modulating the digital bits on multiple carrier frequencies is based on orthogonal frequency-division multiplexing (OFDM).

Frequency	5G band	UL frequency [MHz]	DL frequency [MHz]	Duplex	Use today	Potential future use	License for 5G use
700 MHz	n28	703–784	758–803	FDD	4G and 5G pilots	4G/5G/DSS commercial	Will be retained by MNOs
800 MHz	n20	832–862	791–821	FDD	4G	4G/5G/DSS commercial	Will be retained by MNOs
900 MHz	n8	880–915	925–960	FDD	4G	4G/5G/DSS commercial	Will be retained by MNOs
1800 MHz	n3	1710–1785	1805–1880	FDD	4G	4G/5G/DSS commercial	Will be retained by MNOs
2100 MHz	n1	1920–1980	2110–2170	FDD	4G	4G/5G/DSS commercial	Will be retained by MNOs
2300 MHz	n40	2300–2400		TDD	Diverse	5G	Auction 2022
2600 MHz	n7	2500–2570	2620–2690	FDD	4G	4G/5G/DSS commercial	Sold to MNOs 2021
	n41	2570–2620		TDD	Diverse	4G/5G/DSS	Sold to MNOs 2021
3.6 GHz	n77 n78	3300–3400		TDD	Military	5G	NARFA NOR
	n77 n78	3400–3800		TDD	5G pilots	5G commercial	Sold to MNOs 2021
	n77	3800–4200		TDD	Free use licence	5G private networks	Auction 2022
4.7 GHz	n79	4400–5000		TDD	Military	5G	NARFA NOR
26 GHz	n257 n258	24250–27500		TDD	5G pilots and diverse	5G	Auction 2022

Table 2.2 Overview of relevant frequency blocks and their licences for 5G use in Norway as of March 1, 2022 [36], [38], [39], [53]. The information in the table is subject to future updates.

Some essential physical layer parameters and their configurations specified for 5G NR are given in Table 2.3. Some of the configurations are defined separately for FR1 and FR2.

All physical layer steps in Figure 2.3 and parameters in Table 2.3, except channel coding, are covered in the following subsections. Detailed exploration of the channel coding techniques is beyond the scope of this report. Briefly explained, channel coding encodes the data bits to enable error detection and correction. The polar coding technique is used for the control data, except for very small block lengths where repetition, simplex or Reed Muller coding may be used. Low-density parity-check (LDPC) coding is used for the user data [17].

Modulation is covered in Section 2.2.1. Resource element mapping and definitions and possible configurations for the radio frame, numerology and bandwidth are covered in Section 2.2.2. OFDM modulation and waveform design are covered in Section 2.2.3. Finally, layer mapping, data streams and beamforming are related to multiple antenna technology covered in Section 2.3.1.

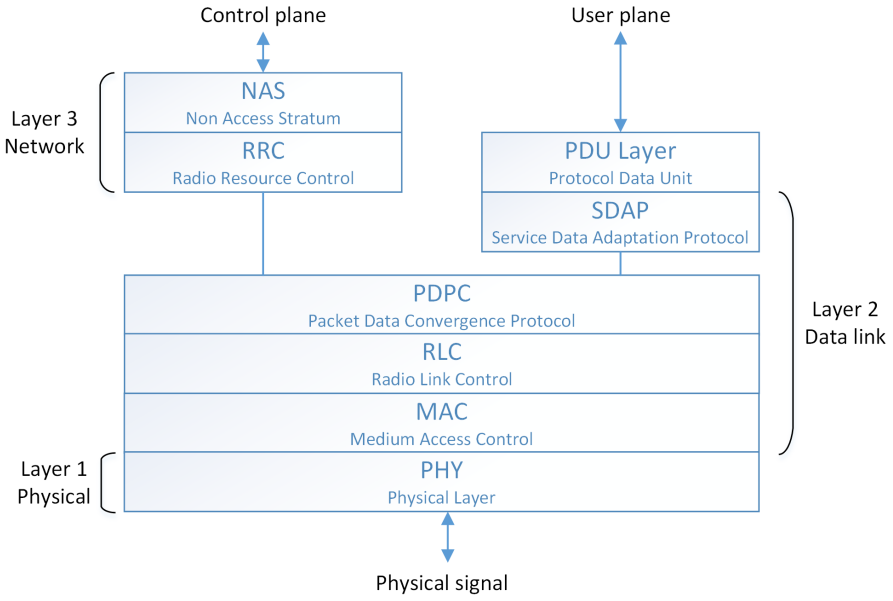


Figure 2.2 OSI model-based layers 1–3 and their services and protocols. Based on [17].

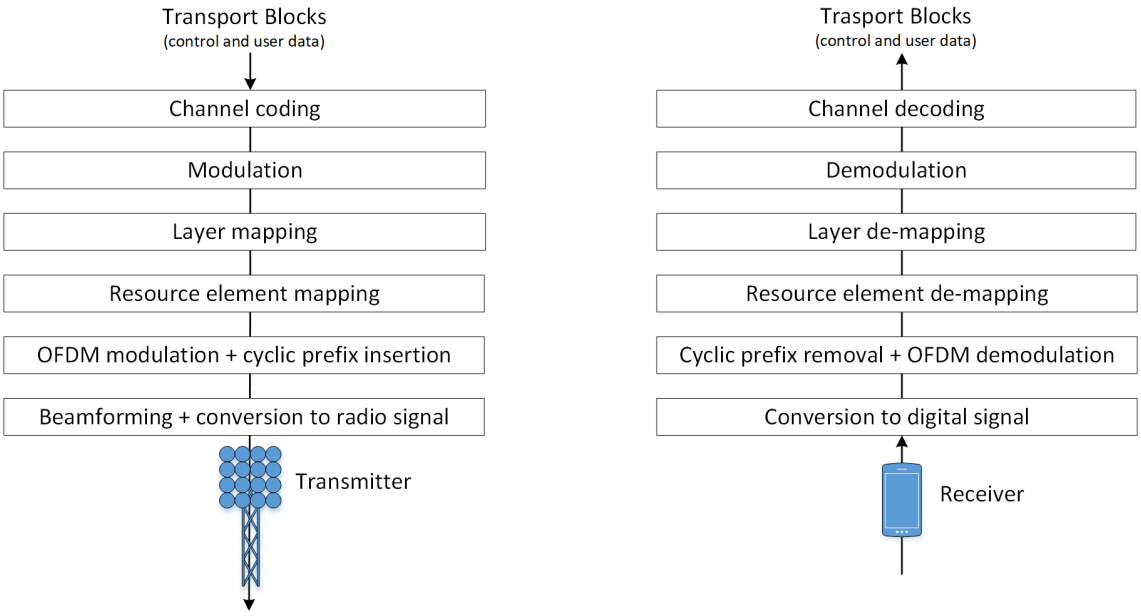


Figure 2.3 Key compenents of the physical layer in 5G NR. Based on [17].

2.2.1 Modulation

Modulation is a technique for converting digital bits into modulation symbols which are further encoded on frequency carriers. A modulation symbol (or just symbol) is a complex number (real and imaginary parts) representing a certain number of bits. The symbol can be represented by a point in a two-dimensional complex plane, where the point can be defined by an angle of rotation,

Parameter	FR1 (410 MHz–7125 MHz)	FR2 (24.25–52.6 GHz)
Channel coding	Polar coding, LDPC	
Modulation	π/2-BPSK (uplink only), QPSK, 16QAM, 64QAM, 256QAM	
Max data streams per user	4 in uplink, 8 in downlink	
Length of radio frame	10 ms	
Numerology	15, 30, 60 kHz	60, 120, 240 kHz
Bandwidth	5, 10, 15, 20, 25, 30, 40, 50, 60, 80, 90, 100 MHz	50, 100, 200, 400 MHz
Waveform	CP-OFDM (uplink/downlink), DFT-S-OFDM (uplink)	
Duplex	TDD, FDD	TDD

Table 2.3 Physical layer parameters and their configurations specified for 5G NR [2], [6], [13].

so-called phase, and a distance to the origin, so-called amplitude. The difference in phase and amplitude separates the symbols from each other.

5G NR supports modulation schemes where the symbols are given at different phases – quadrature phase-shift keying (QPSK) and binary phase-shift keying (π/2-BPSK) – and where the symbols are given at both phase and amplitude – quadrature amplitude modulation (QAM). 5G NR supports three configurations of QAM: 16QAM, 64QAM and 256QAM. All modulation schemes are shown in Figure 2.4. 3GPP defines feasible 5G modulation schemes for uplink and downlink in [6].

The modulation order of a modulation scheme determines the number of bits per symbol. More bits are carried on one symbol using higher modulation order, meaning that more bits are transmitted over the same bandwidth, increasing the bandwidth efficiency and total data rate. However, noise and interference in a radio channel limit the use of high modulation orders. The radio channel affects the phase and amplitude of the symbol, which can cause the symbol to be confused with another nearby symbol when the receiver demodulates the signal. Higher modulation orders result in shorter distances between symbols, which will lead to more detection errors. In case of poor signal quality (low signal-to-noise ratio), a lower modulation order must be used to avoid an unacceptable amount of bit errors.

2.2.2 Resource element mapping

Wireless signals must have an exact and well-defined allocation in the time and frequency domains so that a communication node knows precisely at what time and at what frequency to send or receive a signal. A resource grid provides the basis for allocating the time and frequency resources. A radio frame structure defines how these resources are mapped on the resource grid.

In 5G NR, the radio frame structure is strictly defined, where the time domain is divided into radio frames with a duration of 10 ms, and the frequency domain is defined for transmission bandwidth. A radio frame in the time domain is further divided into ten subframes of 1 ms. Each subframe is further divided into time slots. The number of time slots per subframe depends on the numerology

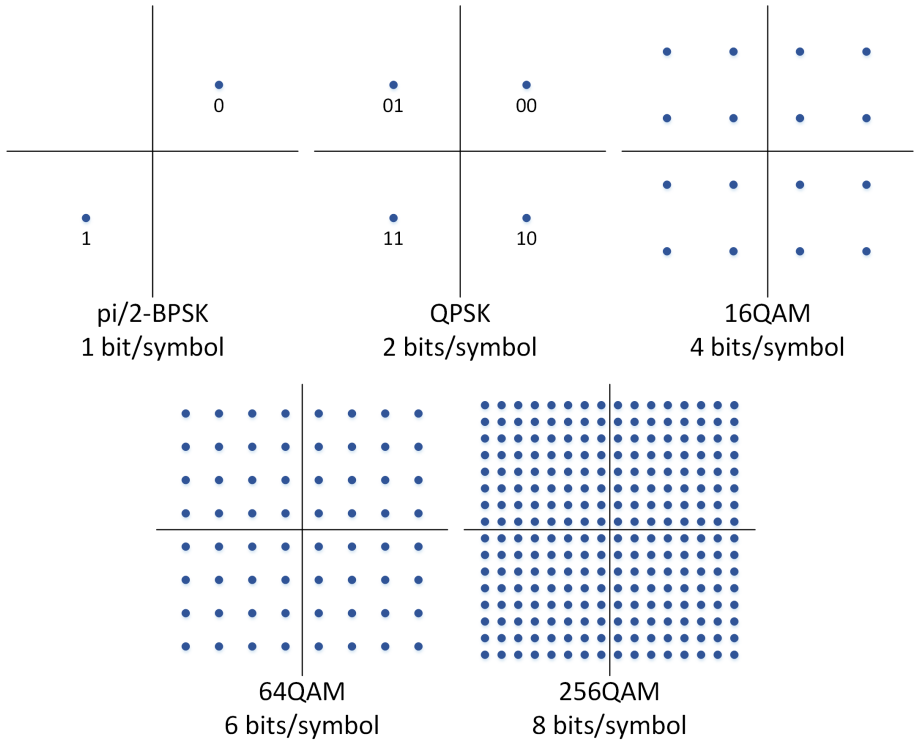


Figure 2.4 Graphic representation of modulation schemes used in 5G NR. Modulation rates are given by the number of bits per symbol.

used. Regardless of the numerology, each time slot consists of 14 OFDM symbols. In the frequency domain, the transmission bandwidth is divided into resource blocks (RB). Each RB consists of 12 orthogonal subcarriers. The bandwidth of a resource block also depends on the numerology [17].

2.2.2.1 Numerology

5G NR defines a family of scalable OFDM numerologies to support different services and solve specific physical layer challenges at high frequencies. Numerology is denoted as a variable $\mu = \{0, 1, 2, 3, 4\}$ and is defined by subcarrier spacing (SCS) which is a distance in frequency between two subcarriers. Defined SCSs are 15, 30, 60, 120 and 240 kHz. Different numerologies lead to different bandwidths of resource blocks and different numbers of time slots per subframe. The higher the SCS, the more time slots can be placed in one subframe, thus the shorter the duration of one OFDM symbol. Figure 2.5 illustrates the radio frame structure for different numerologies.

Table 2.4 summarises the relevant parameters and configurations of the numerologies defined in 5G NR. Not all numerologies are supported by a given frequency and channel bandwidth. FR1 only supports 15, 30 and 60 kHz SCS, while FR2 supports 60, 120 and 240 kHz. The 60 kHz numerology does not support the transmission of synchronisation signals and can only be used for data carrying. In contrast, 240 kHz can only be used for synchronising signals [2].

Supported numerology also depends on a given frequency band. Table 2.5 shows which numerology is supported for data and synchronisation signals for four selected frequency bands.

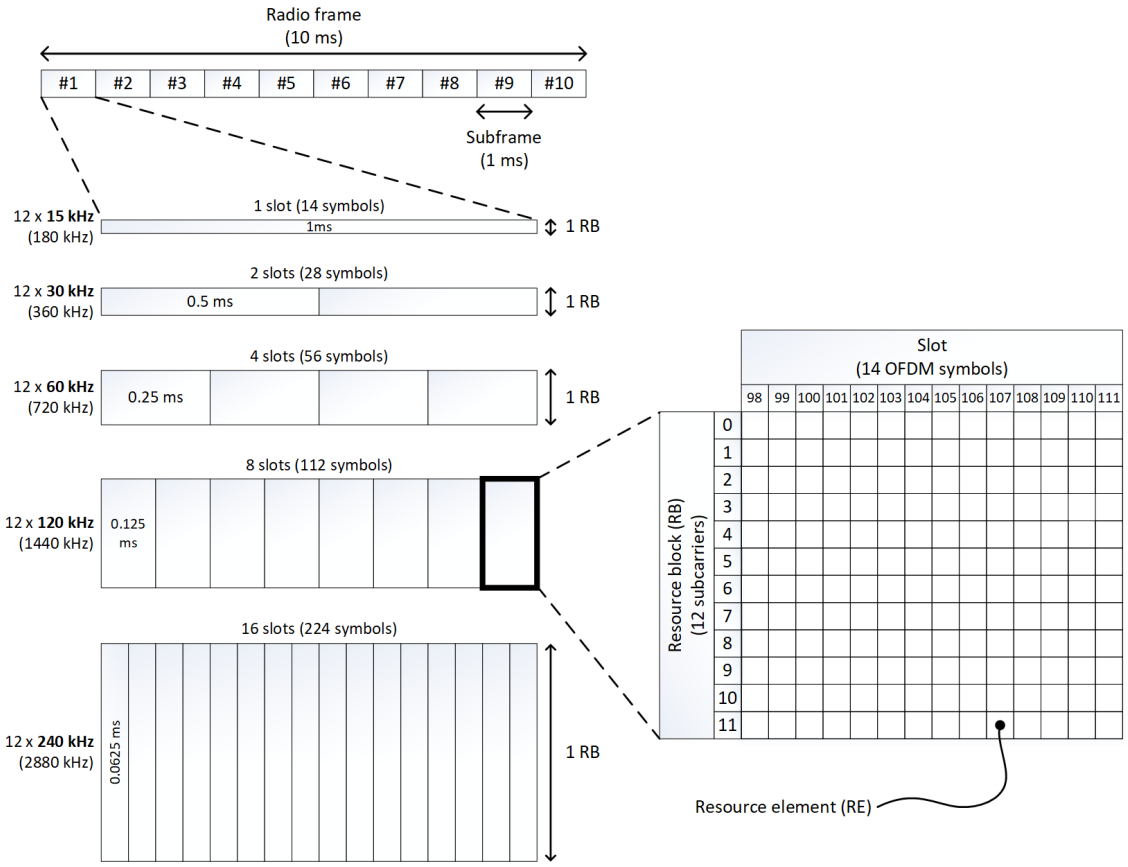


Figure 2.5 Radio frame structure and its configurations depending on a given numerology.

Numerology μ	Subcarrier spacing (SCS)	RB bandwidth	Slots per subframe	OFDM symbol length	Frequency range	Channel bandwidth	Adoption
0	15 kHz	180 kHz	1	66.67 μs	FR1	5–50 MHz	Data & sync
1	30 kHz	360 kHz	2	33.33 μs	FR1	5–100 MHz	Data & sync
2	60 kHz	720 kHz	4	16.67 μs	FR1 & FR2	10–200 MHz	Data
3	120 kHz	1440 kHz	8	8.33 μs	FR2	50–400 MHz	Data & sync
4	240 kHz	2880 kHz	16	4.17 μs	FR2	-	Sync

Table 2.4 Characterisation of numerologies defined in 5G NR [17], [2].

	Numerology for data				Numerology for synchronisation signals			
5G band	15 kHz	30 kHz	60 kHz	120 kHz	15 kHz	30 kHz	120 kHz	240 kHz
n28 (700 MHz)	✓	✓			✓			
n78 (3.6 GHz)	✓	✓	✓			✓		
n79 (4.7 GHz)	✓	✓	✓			✓		
n258 (26 GHz)			✓	✓			✓	✓

Table 2.5 Supported numerology by frequency band and function [2].

2.2.2.2 Physical channels and signals

The resource grid is made up of resource elements (REs). One RE allocates a modulation symbol modulated on a single subcarrier in the frequency domain and a single OFDM symbol in the time domain (see Figure 2.5, 2.6 and 2.7). In other words, resource elements on a radio frame carry information. This information can be in the form of user data, control data, reference signals or synchronisation signals. The user and control data allocated on the REs form so-called physical channels, while the reference and synchronisation signals form physical signals. All physical channels and signals and their functions defined in 5G NR are presented separately for downlink in Table 2.6 and for uplink in Table 2.7.

Downlink physical channels and signals	Abbreviation	Function
Physical downlink shared channel	PDSCH	Carry user data in downlink
Demodulation reference signal for PDSCH	PDSCH DM-RS	Channel estimation to demodulate PDSCH
Phase-tracking reference signal for PDSCH	PDSCH PT-RS	Track and compensate for phase errors in PDSCH
Physical downlink control channel	PDCCH	Carry control data in downlink
Demodulation reference signal for PDCCH	PDCCH DM-RS	Channel estimation to demodulate PDCCH
Physical broadcast channel	PBCH	Carry information required for initial access
Demodulation reference signal for PBCH	PBCH DM-RS	Channel estimation to demodulate PBCH
Primary synchronisation signal	PSS	Synchronisation, physical cell ID
Secondary synchronisation signal	SSS	Synchronisation, physical cell ID, signal quality measurements
Channel state information reference signal	CSI-RS	Downlink channel estimation, signal quality measurements and beam management
Positioning reference signal	PRS	Positioning measurements

Table 2.6 Downlink physical channels and signals in 5G NR [6], [17].

Uplink physical channels and signals	Abbreviation	Function
Physical uplink shared channel	PUSCH	Carry user data in uplink
Demodulation reference signal for PUSCH	PUSCH DM-RS	Channel estimation to demodulate PUSCH
Phase-tracking reference signal for PUSCH	PUSCH PT-RS	Track and compensate for phase errors in PUSCH
Physical uplink control channel	PUCCH	Carry control data in uplink
Demodulation reference signal for PUCCH	PUCCH DM-RS	Channel estimation to demodulate PUCCH
Sounding reference signal	SRS	Uplink channel estimation and beam management
Physical random-access channel	PRACH	Carry user's initial access message to the BS

Table 2.7 Uplink physical channels and signals in 5G NR [6], [17].

3GPP specifies which REs in a radio frame are allocated to carry which physical channel or signal. Compared with 4G, the allocation is much more flexible in 5G as many different configurations are allowed. However, it becomes complicated and unclear what configurations are implemented in an

existing 5G radio system, making it challenging to know the exact location of every physical channel and signal in time and frequency. Which configurations manufacturers are implementing are often commercially confidential. Figure 2.6 gives an example of how the key physical channels and signals can be allocated on a radio frame operating in the TDD mode with the 30 kHz numerology. This configuration is based on 3GPP standards [6], [8], [9] and can only be used as an educational illustration.

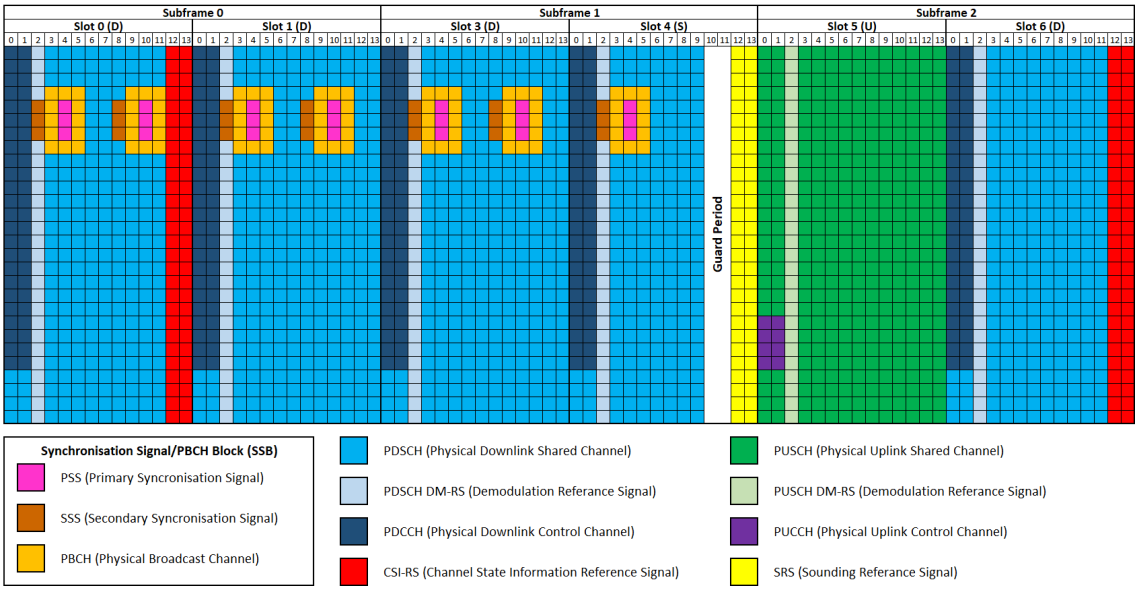


Figure 2.6 Illustration of the presumed allocation of physical channels and signals on a radio frame. Based on [6], [8], [9].

The given radio frame is an example of a so-called DDDSU slot configuration, where "D" stands for *Downlink*, "S" stands for *Special* and "U" stands for *Uplink*. The DDDSU configuration means that three slots are dedicated to downlink communication, one slot has a special configuration, and one slot is dedicated to uplink communication. The slot with the special configuration is a transition slot between the downlink and uplink transmissions and contains time symbols dedicated to both downlink communication, guard period, and uplink communication. The DDDSU configuration is downlink-centred as more time resources are given for the downlink transmission. The guard period is the time between the downlink and uplink transmissions. Its purpose is to avoid interference within a cell and ensure coexistence among cells by compensating for propagation delays [26].

2.2.3 Orthogonal frequency-division multiplexing (OFDM) signal

5G NR is a technology that transfers digital information bits between a base station and user equipment. Before information bits can be transmitted wirelessly, these digital bits must be converted to an analog signal. For this purpose, orthogonal frequency-division multiplexing (OFDM) is used to encode digital information into an OFDM signal. The OFDM signal consists of modulated subcarriers in the frequency domain and OFDM symbols in the time domain. The OFDM signal can be converted to an analog signal and transmitted over the air at an assigned carrier frequency.

Figure 2.7 illustrates the process of modulation symbols being converted into an OFDM signal, also referred to as an OFDM waveform. The resource element mapping procedure is responsible for allocating the modulation symbols to the subcarriers. The sum of all the modulated subcarriers using inverse fast Fourier transform (IFFT) produces an OFDM symbol. Further, a portion at the start of the symbol is copied and attached to the end of the symbol. This procedure is called cyclic prefix (CP). The CP makes the OFDM communication more robust to timing synchronisation errors and inter-symbol interference. The type of waveform presented in the example is called CP-OFDM.

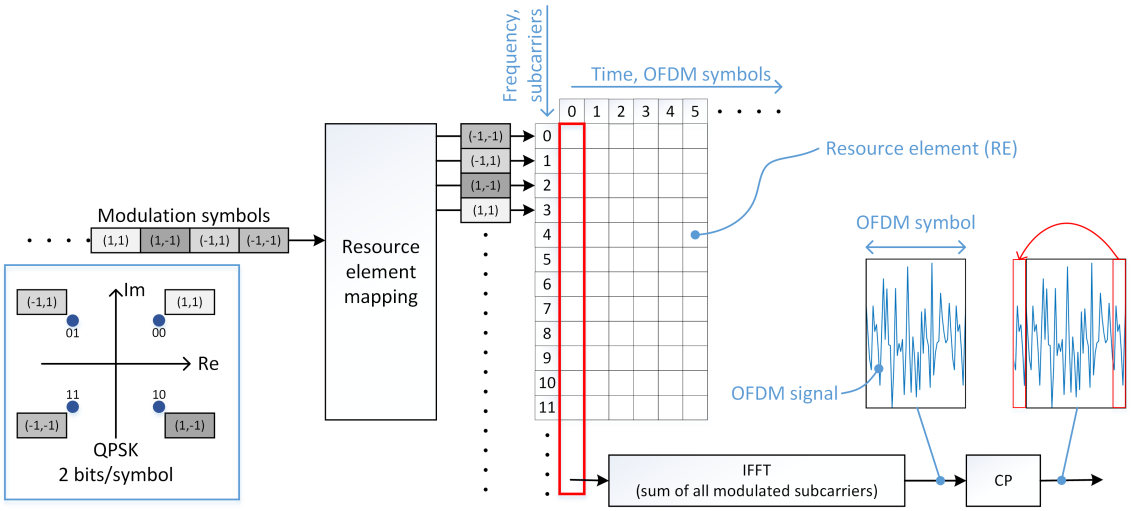


Figure 2.7 Illustration of the process of modulation symbols being converted into an OFDM signal.

Another waveform used in 5G NR for uplink transmissions is discrete Fourier transform spread OFDM (DFT-S-OFDM). The process of building the OFDM signal in DFS-S-OFDM is the same as for CP-OFDM but with an additional step of DFT. The DFT-S-OFDM is more power-efficient, an essential aspect for a user terminal. However, the DFT-S-OFDM waveform cannot offer dynamic spectrum utilisation, compatibility with multi-antenna systems and robustness to frequency-selective channels on the same level as the CP-OFDM waveform can [29].

An OFDM-based waveform is used in wireless technologies such as 4G Long-Term Evolution (LTE), Wi-Fi or DAB radio and will continue to be used in 5G NR. OFDM has an advantageous ability to cope with poor radio channel conditions such as narrowband interference or frequency selective fading in multipath channels. Channel estimation and equalisation are simplified because OFDM can be seen as a set of many orthogonal (non-interfering with each other) narrowband signals instead of one broadband signal [17].

2.3 Antenna technology

This section covers the relevant theory of multi-antenna operation and beamforming. Possibilities and expectations regarding the practical use of base station antennas and user equipment antennas are also presented.

2.3.1 Multiple-input multiple-output (MIMO)

Radio resources must be distributed between the users when a cell serves several users simultaneously. Different generations of mobile technologies use different methods to multiplex data transmission between the users. In 2G, the radio resources are distributed either in time using time-division multiple access (TDMA) or in frequency using frequency-division multiple access (FDMA). 3G uses a special encoding mechanism, called code-division multiple access (CDMA), to separate users. 4G and 5G use the OFDM waveform, allowing easy distribution of time and frequency resources over several users. The multi-access method in 4G and 5G is thus called orthogonal frequency-division multiple access (OFDMA) [52].

In addition to OFDMA, multiple-input multiple-output (MIMO) technology is used in both 4G LTE and 5G NR to distribute radio resources in domains other than time and frequency. MIMO in radio communications is a multiplexing technique that uses multiple antennas to transmit and receive several data streams simultaneously by exploiting the fact that each antenna has a separate and independent radio channel [54]. With MIMO, multiple data streams can be transmitted and received on the same time and frequency resources, which increases both data speed for the end-user and total capacity for the network. Data streams refer to either many users' data or a single user's data divided into streams of bits to be transmitted and received in parallel.

Separate and independent radio channels can be achieved by, i.e., utilising antenna polarisation diversity or spatial multiplexing. Antenna polarisation diversity exploits independent radio channels on different orthogonal antenna polarisations, like vertical and horizontal polarisation or cross polarisation. Spatial multiplexing can be achieved by utilising multipath propagation, beamforming or both. Different data streams transmitted on different antennas might have different physical propagation paths, also known as multipath propagation. Multipath propagation is more likely to occur in an environment rich in reflective objects like trees, buildings and mountains. If the radio signals arrive at the receiver antennas with sufficiently different spatial signatures, the receiver can separate those signals and, thus, receive multiple data streams simultaneously.

MIMO, exploiting antenna polarisation diversity and multipath propagation, is used in 4G LTE and will continue to be used in 5G NR. However, spatial multiplexing achieved by beamforming is a new 5G NR feature, which is often referred to as massive MIMO. Beamforming and massive MIMO are covered in the following subsections.

Figure 2.8 shows the principle of radio resources distribution in an OFDM system with and without MIMO enabled spatial multiplexing. Without MIMO, the radio resources between the users are multiplexed in time and frequency. With MIMO, spatial multiplexing is enabled, allowing the transmission of several data streams on the same time-frequency resources.

A conventional radio communication system that uses one antenna to transmit and one antenna to receive is called single-input single-output (SISO) and, therefore, cannot transmit and receive multiple data streams simultaneously [54]. Figure 2.9 shows an example of a SISO system, where the transmitter uses only one antenna for data transmission. If there are several users in a cell that require communication at the same time, the SISO system must distribute the radio resources in time, frequency or by coding. Before a digital data stream can be transmitted as a radio signal, it must be digitally processed on a baseband unit and converted into an analog signal on a so-called radio frequency (RF) chain. The digital baseband processing includes all the steps on a physical

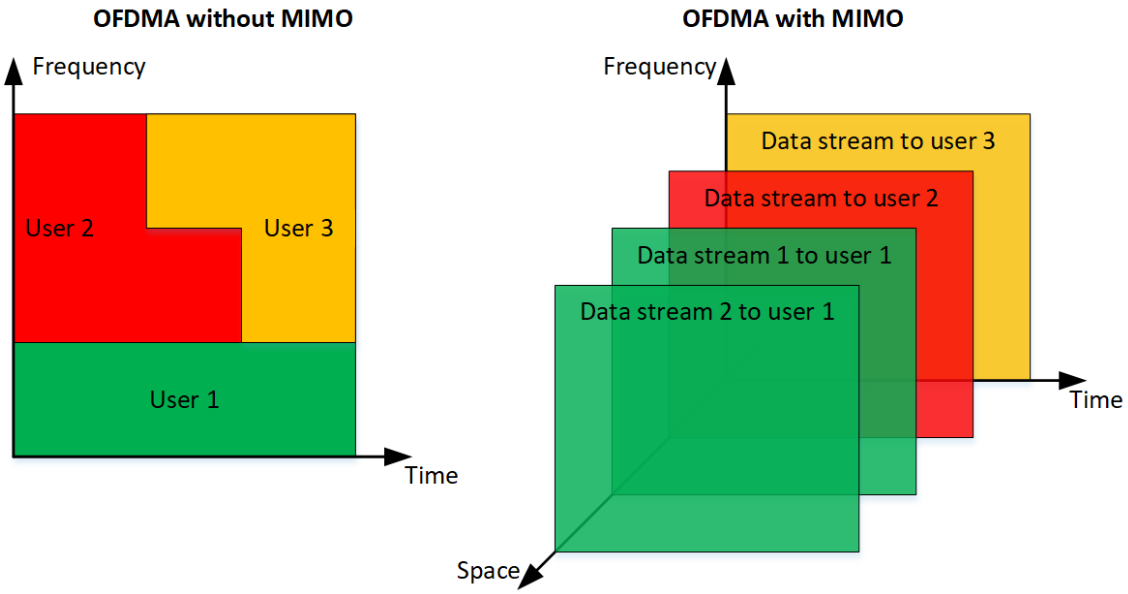


Figure 2.8 Radio resource multiplexing between the users in an OFDM system without and with MIMO enabled spatial multiplexing. MIMO allows simultaneous transmission of several data streams on the same time-frequency resources.

layer from coding to OFDM modulation described in Section 2.2. The RF chain manages steps like digital-to-analog conversion, filtering and carrier frequency modulation.

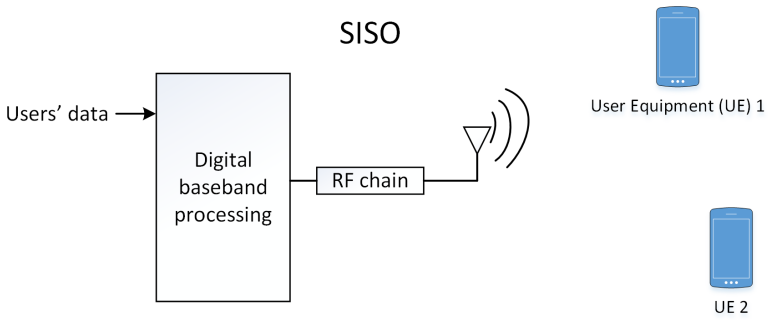


Figure 2.9 Illustration of a single-input single-output (SISO) system.

The case in which a user transmits or receives several data streams simultaneously is called single-user MIMO (SU-MIMO) [23]. Figure 2.10 shows a high-level example of a radio system that exploits two pairs of antennas and multipath propagation to deliver two data streams in parallel. The layer mapping procedure of the physical layer uses MIMO precoding techniques to distribute the data streams to the physical antennas. The number of separate radio channels cannot be higher than the number of antennas equipped at the transmitter and receiver. In the case of two parallel data streams, the user equipment must also be equipped with at least two receiving antennas. This is called 2x2 MIMO because two antennas are used at the transmitter, and two antennas are used at the receiver to transfer two separate data streams.

In 5G NR, it is defined that the maximum number of data streams per user is eight in downlink (8x8 MIMO) and four in uplink (4x4 MIMO) [13].

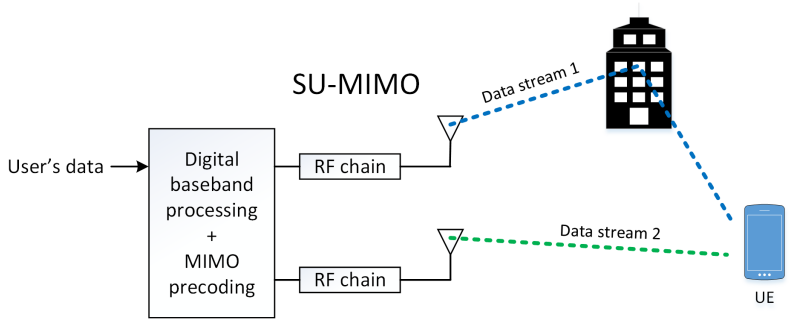


Figure 2.10 Illustration of a single-user MIMO (SU-MIMO) system.

In multi-user MIMO (MU-MIMO), the data streams are distributed among multiple users [23]. Figure 2.11 shows an example of MU-MIMO with a 4x4 MIMO setup, where four transmitting antennas are used to transmit four data streams. This 4x4 MIMO system has to have four receiving antennas – two at UE 1 and one each at UE 2 and UE 3 in this case. The equivalent MIMO communication can be utilised in uplink where the base station can receive multiple data streams on multiple antennas from multiple users simultaneously.

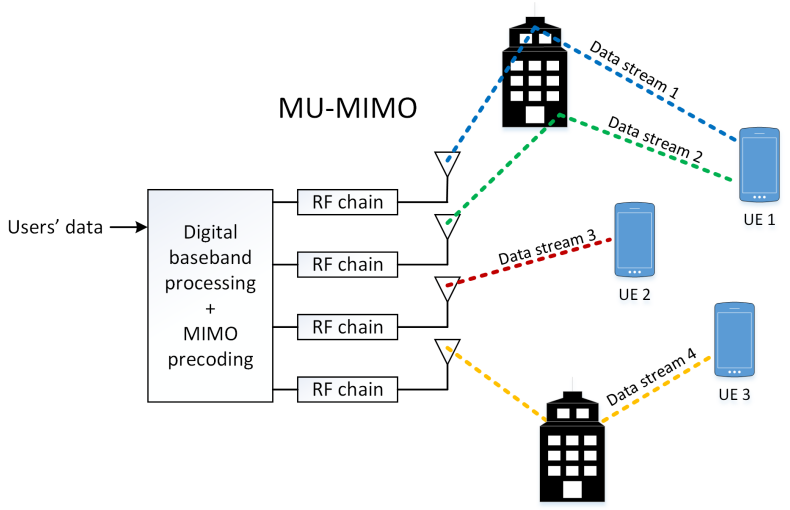


Figure 2.11 Illustration of a multi-user MIMO (MU-MIMO) system.

2.3.2 Beamforming

An antenna that radiates the output power concentrated in a specific direction creates a so-called beam. The beams are formed using an array antenna consisting of a number of antenna elements. The more antenna elements are connected, the narrower and more concentrated beam can be formed. An illustration of an array antenna and a beam is shown in Figure 2.12. A communication system that utilises beams can increase received signal power, leading to higher signal quality than an omnidirectional antenna.

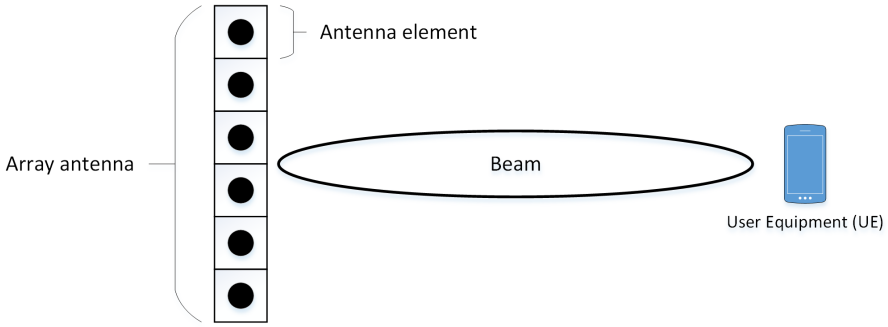


Figure 2.12 Illustration of an array antenna forming a beam.

Forming a beam and steering its direction by constructively changing the amplitude and phase of every antenna element in an array antenna is called beamforming. Beamforming can be

- analog, where antenna elements are controlled in the antenna's hardware
- digital, where antenna elements are controlled by digital signal processing
- hybrid, where both analog and digital beamforming are utilised

Figure 2.13 shows a typical example of a transmitter that utilises analog beamforming. The digital signal is converted to a transmission-ready analog signal in the RF chain. Then, it passes through an analog phase shifter and is emitted through an antenna element. The phase shifter provides a certain shift in phase so that the beam is directed in the desired direction.

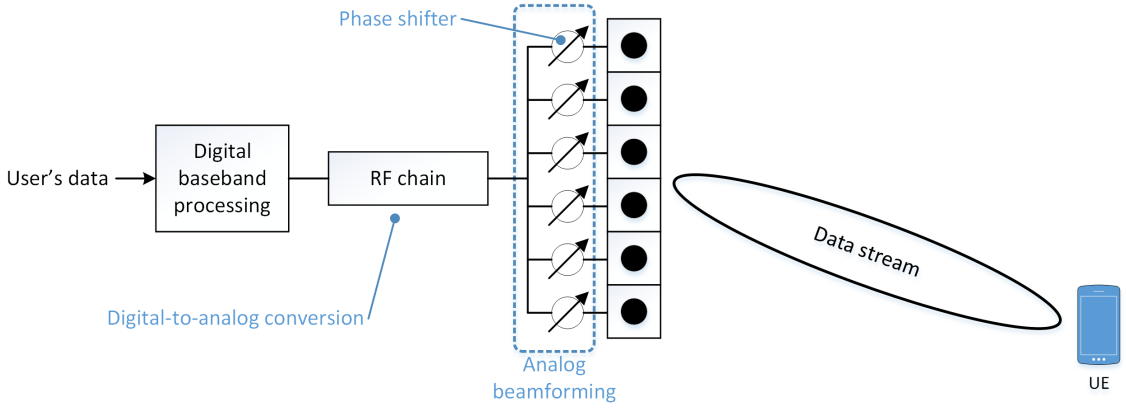


Figure 2.13 Analog beamforming architecture. Based on [17].

Analog beamforming can, in principle, support many antenna elements, provide narrow beams and have sufficient beam steering. However, a system with only analog beamforming is generally limited to one data stream at a time because the group antenna is connected to one RF chain, and the same signal (only phase-shifted) is fed to each antenna element.

Digital beamforming, on the other hand, provides a multi-beam operation that enables the transmission and reception of several data streams that simultaneously serve several users. Figure 2.14 shows a high-level architecture of a transmitter that uses digital beamforming. In digital beamforming, the phase and amplitude of the signal are adjusted in the digital domain before the

signal is sent to the RF chains for digital-to-analog conversion. A unique signal is generated for each antenna element using special precoding matrices, and therefore each antenna element must have its own RF chain. The digital control of each separate antenna element allows the system to form several beams, where each beam carries a unique data stream. Beamforming in the digital domain also provides high flexibility in the directional steering of one or multiple beams, making it possible to have user-specific beams following the users.

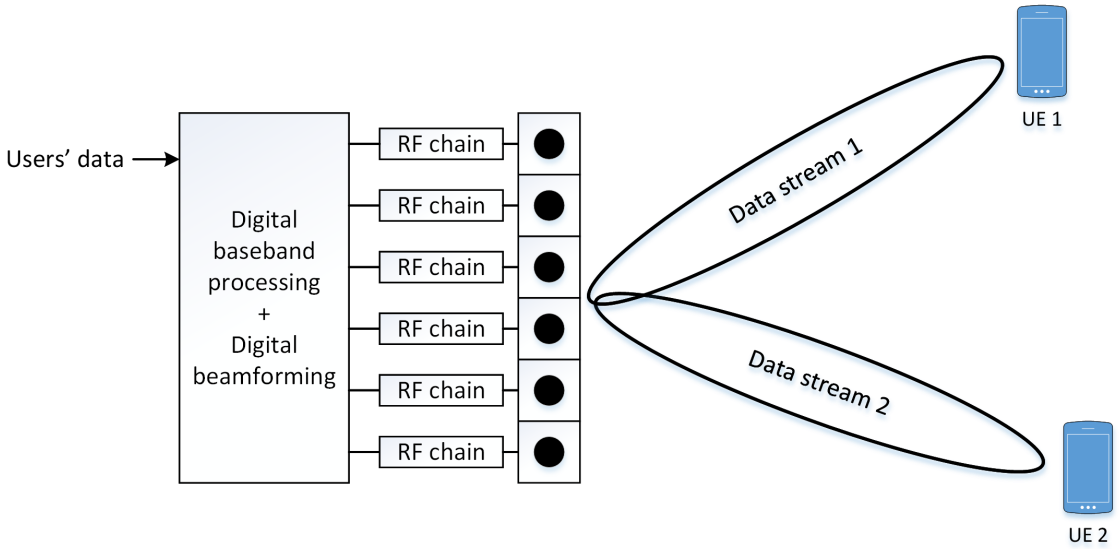


Figure 2.14 Digital beamforming architecture. Based on [17].

However, digital beamforming is not always an ideal solution when it comes to practical implementation. High complexity in signal processing and a high number of RF chains can lead to increased costs and high energy consumption.

Hybrid beamforming combines the benefits of both digital and analog beamforming. Figure 2.15 provides an example of how digital and analog beamforming can be combined in a hybrid system. A small group of antenna elements connected in the analog domain contributes to narrowing the beams and, at the same time, saves the number of necessary RF chains. However, digital control over the RF chains provides flexible beam steering and enables multi-user operation.

2.3.3 Massive MIMO

Massive MIMO is an extension of MU-MIMO, which exploits even greater numbers of antennas than previous generation antenna technologies and utilises beamforming, enabling an even higher number of simultaneous MIMO streams. Massive MIMO does not have a universal definition, but the authors in [47] provide an accurate proposal on how massive MIMO should be defined. Based on this proposal, we define massive MIMO as follows.

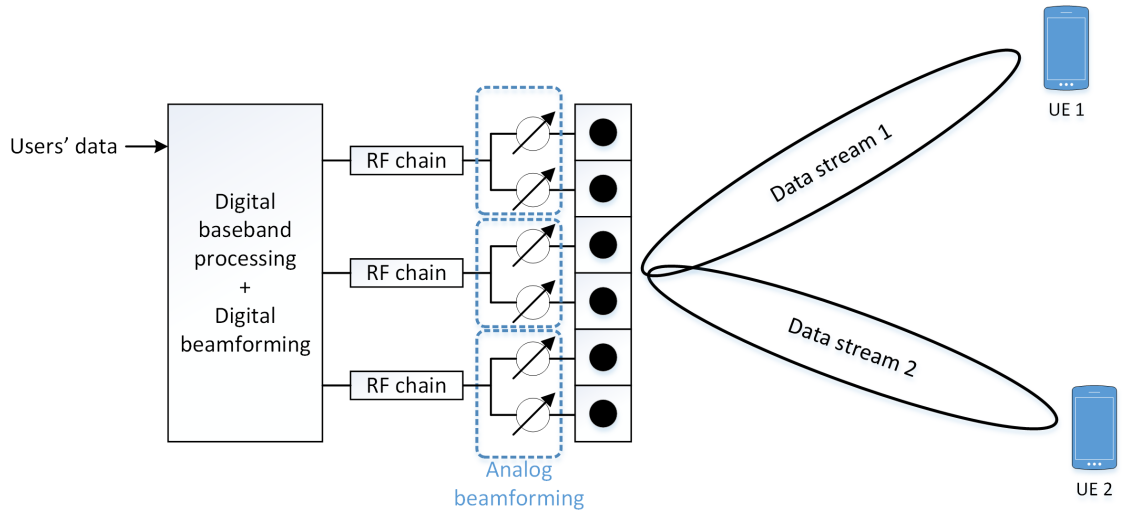


Figure 2.15 Hybrid beamforming architecture. Based on [17].

Massive MIMO is a wireless technology aiming to improve spectral efficiency (bits/s/Hz/cell). This physical-layer technology equips a base station with an array of many active antennas, which are used to spatially multiplex signals of many user terminals; that is, to communicate with them on the same time-frequency resource.

An *active antenna* in this context is an antenna element (or a group of antenna elements connected in the analog domain) that has its own RF chain and is digitally controlled to enable spatial multiplexing. The word *massive* in massive MIMO stands for many (a massive number of) active antennas. The number of active antennas required for an antenna to be considered a massive MIMO antenna is not strictly defined. Researchers often consider that a massive MIMO antenna should consist of at least 64 fully digital active antennas [47]. However, vendors of base station equipment often promote antennas with 16 or 32 active antennas as massive MIMO antennas. Either way, the number of active antennas is higher in a massive MIMO system than in conventional MU-MIMO systems, enabling beamforming and enhancing spatial multiplexing.

The difference between the massive MIMO and conventional MU-MIMO systems is that massive MIMO is less dependent on a reflective radio environment to achieve multiple separate radio channels and provide service to multiple users simultaneously. An array antenna with many antenna elements combined with hybrid beamforming, many RF chains and proper radio channel estimation allows the base station to estimate the user's direction. In the downlink, beamforming creates a separate radio channel in a specific direction sufficiently independent from other users' radio channels. In the uplink, the massive MIMO antenna is able to receive multiple data streams from multiple users and separate them spatially since the radio signals will arrive at the base station at different angles and have different propagation channels. However, to provide multiple SU-MIMO data streams, the massive MIMO still needs to operate in a multipath propagation environment or utilise antenna polarisation diversity [23].

Figure 2.16 shows a principle of a radio communication system with a massive MIMO antenna. In addition to hybrid beamforming and many RF chains, a typical massive MIMO antenna will utilise many antenna elements with orthogonal polarisation. Dual-polarisation allows transmitting a separate data stream on each polarisation as each group of polarised antenna elements has a separate RF chain.

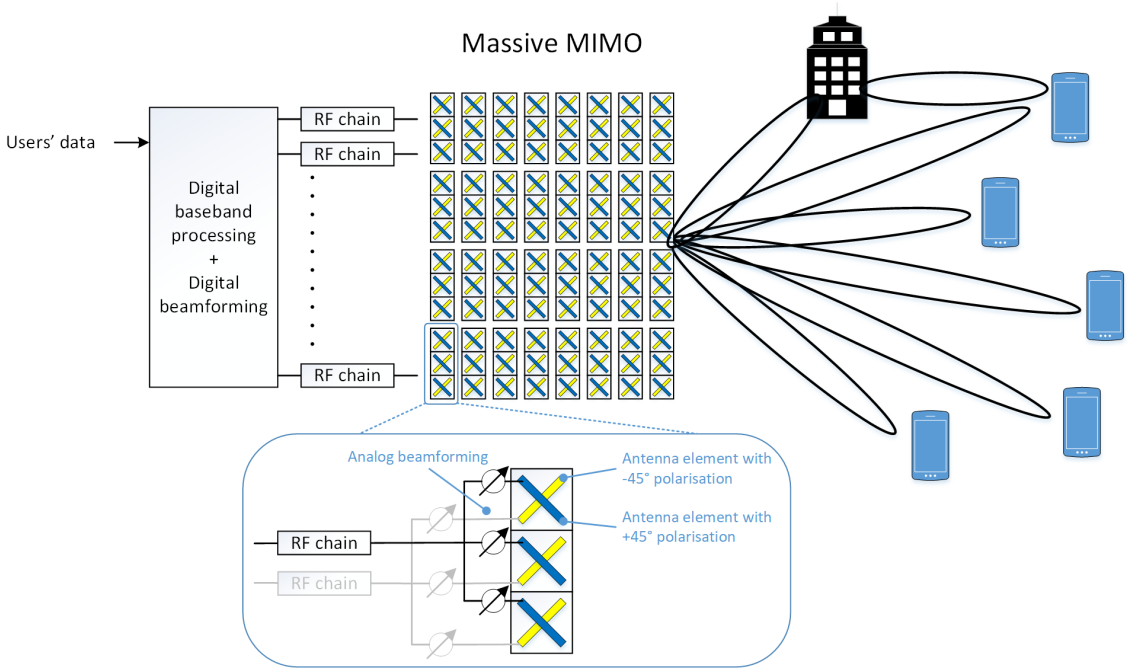


Figure 2.16 Massive MIMO system providing multiple MIMO streams by utilising beamforming and antenna polarisation. Based on [17], [23].

One RF chain can be connected to multiple antenna elements with analog steering. An array antenna can have many antenna elements connected in the analog domain to narrow the beams. However, it is the digital control over RF chains that enables the multi-beam operation. The maximum number of simultaneous data streams the massive MIMO antenna can handle equals the number of digitally controlled RF chains. Authors in [47] suggest that a real massive MIMO antenna should have at least 64 digitally controlled RF chains. The notation of such configuration is 64T64R, where "T" stands for *Transmitter* and "R" stands for *Receiver*. In theory, an array antenna with 64 RF chains can transmit and receive 64 parallel data streams. In practice, it is challenging to utilise all 64 digital channels fully, so the maximum number of simultaneously multiplexed data streams can go down to, for example, 16. The maximum number of parallel data streams can then be noted as 16x16 MIMO.

2.3.4 Base station antennas

The choice of antenna type at a base station depends on the frequency band and the service a cell is required to provide. As described in Section 2.1, currently the most relevant frequency bands in initial commercial rollouts of 5G in Norway are 700 MHz, 3.6 GHz, and 26 GHz.

The 700 MHz frequency bands provide area coverage in open rural areas, where an extended coverage radius is achieved because of low free space loss, and urban areas, where good propagation

through walls provides sufficient indoor coverage. Advanced beamforming at these frequencies is not practical due to long wavelengths at the low frequencies. The longer the wavelength, the greater the distance between antenna elements in a group antenna, which would lead to an oversized physical antenna at the base station. Antennas operating at frequencies below 1 GHz support up to 8x8 MIMO in practice. In principle, such antennas can utilise a simple form of beamforming to concentrate the radiated energy towards the serving sector. Antennas operating at low frequencies usually operate in FDD mode.

Higher frequencies in 5G NR provide a practical opportunity to utilise massive MIMO array antennas. At frequencies as high as 3.6 GHz, an array antenna with hundreds of antenna elements is ideally suited for commercial 5G mobile networks. Massive MIMO antennas are particularly suitable for urban areas, where capacity is more important than a large coverage area. The use of spatial multiplexing in a massive MIMO antenna makes it possible to serve several users sending or receiving user data simultaneously. In addition, the use of beamforming to concentrate the signal power in the desired direction compensates, to some extent, for the increased free space loss the higher frequencies are experiencing. Frequency bands above 3 GHz operate primarily in TDD mode.

Base station antennas that operate at millimetre-wave (mmWave) frequencies can be even smaller, even with the number of antenna elements increased to thousands. Digital control over this many antenna elements in a massive MIMO antenna provides even narrower and more precise user-specific data beams. Highly concentrated beams compensate for significant free space losses experienced at frequencies as high as 26 GHz. Small obstacles such as trees or the human body reduce the high-frequency signal; thus, the connection is highly dependent on line-of-sight (LOS). In commercial mobile networks, massive MIMO antennas on mmWave frequencies will be used in scenarios with high user density, such as city centres, train stations, concert halls, stadiums, offices and similar gathering places because the mmWave frequency range can offer large bandwidths while a massive MIMO antenna can simultaneously serve many UEs. All frequency bands in the millimetre-wave spectrum operate in TDD mode.

2.3.5 User equipment antennas

Based on categorisation done by NGMN (introduced in Section 2.1), 5G user equipment can be grouped into three types:

- broadband devices like smartphones, tablets, laptops and mobile hotspot routers
- outdoor and indoor customer premises equipment (CPE) for 5G fixed wireless access (FWA)
- different types of 5G modules for industrial applications, Internet of things (IoT) or vehicle-to-vehicle (V2V) applications

Antenna design for mobile phones has always been challenging for engineers, and designing antennas to support the new 5G frequency bands will further raise the bar. 5G will be used alongside existing 4G, 3G, 2G and Wi-Fi communication channels. This increases the number of antennas to be integrated into the smartphone, especially since most of these standards also include support for MIMO multi-antenna operation [46]. NGMN sets requirements for the order of MIMO a 5G broadband device must support. The requirements for what is mandatory and recommended depend on the frequency range and are given in Table 2.8.

Frequency range	MIMO downlink	MIMO uplink
FR1 below 1 GHz	2x2 mandatory 4x4 recommended	1x1 mandatory 2x2 recommended
FR1 above 1 GHz	4x4 mandatory	1x1 mandatory 2x2 recommended
FR2	2x2 mandatory 4x4 recommended	2x2 mandatory

Table 2.8 Order of MIMO mandatory and recommended for a broadband device to support [20].

User equipment antennas at 5G frequencies below 6 GHz will have no fundamental differences from antennas used in 4G LTE. However, antennas at millimetre-wave frequencies (above 24 GHz) have to overcome new challenges. One of the challenges is integrating the antenna inside the housing components, cover or screen. On mmWave frequencies, these components are no longer electrically thin and thus have a substantial effect on the radiating performance of the antenna [46].

2.3.5.1 Output power

The 5G standards restrict user equipment transmit power (output power). 3GPP defines the maximum allowed output power for every frequency band using power classes.

Power classes 1, 1.5, 2 and 3 are defined for FR1. The maximum output power is given by total radiated power (TRP). The maximum TRP value for every power class in FR1 is given in Table 2.9. Power classes 1, 1.5 and 2 can only be used with the given frequency bands. Power class 3 is a default for all frequency bands in FR1.

Power Class FR1	Max TRP [dBm]	Frequency band
1	31	n14 (700 MHz)
1.5	29	n41 (2500 MHz)
2	26	n40 (2300 MHz), n41 (2500 MHz), n77 (3.6 GHz), n78 (3.7 GHz), n79 (4.7 GHz)
3	23	default for all bands

Table 2.9 Power classes specified for FR1 [11].

Power classes 1, 2, 3 and 4 are defined for FR2. 3GPP specifies the power classes for FR2 based on the assumption of certain UE types given in Table 2.10.

In addition to the TRP, the effective isotropic radiated power (EIRP) is also used to define the output power limits for user equipment in FR2. EIRP is a measure for directional radiated power, which takes into account the gain obtained by beamforming and represents the antenna's strongest beam. Each power class has a defined value for maximum TRP, minimum EIRP and maximum EIRP. The minimum and maximum output values for different frequency bands in FR2 are given in Table 2.11.

Power Class FR2	UE type
1	Fixed wireless access (FWA)
2	Vehicular
3	Handheld
4	High power non-handheld

Table 2.10 User equipment (UE) type for a given power class in FR2 [12].

Frequency band	Power Class FR2	Max TRP [dBm]	Min EIRP [dBm]	Max EIRP [dBm]
n257, n258, n261 (24.25–29.5 GHz)	1	35	40	55
	2	23	29	43
	3	23	22.4	43
	4	23	34	43
n260 (37–40 GHz)	1	35	38	55
	3	23	20.6	43
	4	23	31	43
n259 (35.5–43.5 GHz)	3	23	18.7	43

Table 2.11 Power classes specified for FR2 [12].

2.4 Radio communication

This section covers aspects of 5G radio communication regarding interworking with 4G, downlink synchronisation, mobility measurements, radio connection establishment procedures and beam management.

2.4.1 Downlink synchronisation signals

In order to attach to the network, a UE must perform an initial cell search and downlink synchronisation. The objective of the initial cell search is to find a strong cell signal for connection establishment, obtain an estimate of frame timing, obtain cell identification, and find the reference signals for demodulation of the physical channels. For this purpose, a primary synchronisation signal (PSS) and secondary synchronisation signal (SSS) are used. The PSS and SSS, together with the physical broadcast channel (PBCH) and its demodulation reference signal (PBCH DM-RS), are transmitted on a synchronisation signals/physical broadcast channel block abbreviated as SS/PBCH block or SSB [17].

Physical-layer cell identity (PCI) is scrambled on and carried by PSS and SSS. There are 1008 possible combinations of different PSS and SSS sequences representing the PCI. UEs use PCI to correctly identify the cell on the physical layer level to decode the received data.

PBCH carries the master information block (MIB), which contains system information necessary for initial access. MIB carries parameters such as frame number, frequency offset for SSB, and

other configurations necessary for the process of connection establishment [10]. PBCH also carries an SSB index that is encoded as part of channel coding of PBCH [4].

2.4.1.1 Synchronisation signals block (SSB)

An SSB spans 20 resource blocks (240 subcarriers) in the frequency domain and 4 OFDM symbols in the time domain. SSB can be broadcasted from the BS several times in a row in a so-called SS burst. The purpose of an SS burst is to enable beamforming, where each SSB in an SS burst is transmitted on a separate beam. The technique of transmitting several consecutive beams, one beam at a time, is called beam sweeping. The beam carrying the SSB is called an SSB beam. The intention of broadcasting the synchronisation signals and PBCH in beams is to achieve better cell coverage. The SSB beams can be transmitted in different direction patterns to adapt the coverage to a specific scenario. For example, the SSB beams can be transmitted vertically to provide better coverage for a tall building with tens of floors. The SSB beams can also be directed to cover a specific ground area. The beam patterns are flexible and can be configured in antenna settings.

Figure 2.17 shows a set-up of an SS burst with seven SSBs in a radio frame, as well as an example of beam sweeping. SSBs in an SS burst contain identical information except for the unique SSB index, which helps differentiate the SSB beams. The figure also contains an example of the configuration of PSS, SSS and PBCH mapped on a resource grid.

The highest number of SSBs per SS burst depends on the frequency range and duplex mode. Table 2.12 gives an overview of the maximum number of SSBs per SS burst for a given frequency range and duplex mode [13]. An SSB or SS burst is transmitted periodically, where the periodicity can vary between 5, 10, 20, 40, 80 or 160 ms. The periodicity of 20 ms is the default [8].

Frequency range		Max number of SSBs in SS burst
FR1	below 3 GHz in FDD below 2.4 GHz in TDD	4
	above 3 GHz in FDD above 2.4 GHz in TDD	8
FR2		64

Table 2.12 Maximum number of SSBs per SS burst for a given frequency range and duplex mode [13].

The exact allocation of the SSB on time and frequency resources is configurable in 5G NR, whereas in 4G LTE, the allocation of the synchronisation signals is static. The synchronisation signals in 4G are always placed in the middle of the transmission bandwidth and have a fixed periodicity of 5 ms. In 5G NR, the synchronisation signals can be placed nearly anywhere within the transmission bandwidth. Which OFDM symbols in a radio frame the SSB can be carried on, and where on the transmission bandwidth the SSB can be placed, depend on several settings. The exact configurations of the possible SSB allocation are given in Appendix B.

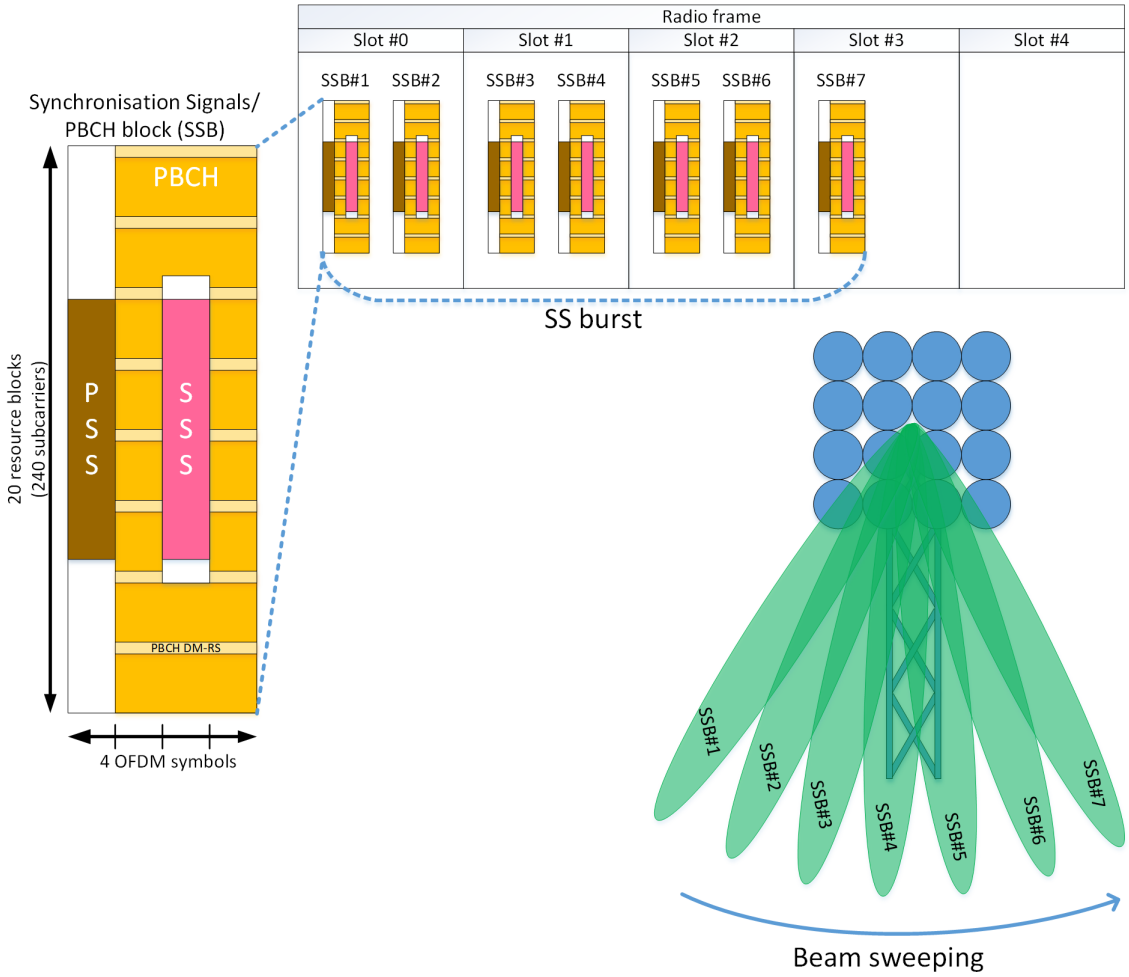


Figure 2.17 Set-up of an SSB on a resource grid and SS burst on a radio frame. SSBs in an SS burst are transmitted in a beam sweeping fashion [13].

2.4.2 Mobility measurements

Measurements of the radio signal strength and quality done by the BS or UE to establish and manage the radio communication link are called mobility measurements. 3GPP specifies three main mobility measures for 5G NR [7]:

- Reference signal received power (RSRP) is defined as the linear average over the power contributions of the resource elements that carry reference signals configured for RSRP measurements. The averaging results in RSRP represent the average wanted signal strength of a single resource element.
- Reference signal received quality (RSRQ) represents the ratio of the RSRP and the average total received power, including noise and interference, of a single resource block (12 resource elements).
- Signal-to-noise and interference ratio (SINR) represents the ratio of the RSRP and the average noise and interference power contribution of a single resource element.

These parameters can be measured in resource elements carried by SSB and CSI-RS. SSB based mobility measures are called SS-RSRP, SS-RSRQ and SS-SINR and are measured in resource elements that carry the secondary synchronisation signal (SSS). If needed, PBCH DM-RS can also be used in addition to SSS. CSI-RS based mobility measures are called CSI-RSRP, CSI-RSRQ and CSI-SINR.

2.4.3 Non-Stand Alone (NSA) and Stand Alone (SA)

As a first and temporary step towards deploying the "complete 5G", an architecture option called Non-Stand Alone (NSA) is introduced by 3GPP. The NSA can use a 5G base station with 5G NR in conjunction with the 4G radio interface (LTE) and the 4G core network (EPC). This type of NSA is known as E-UTRA-NR Dual Connectivity (EN-DC) or Architecture Option 3. Stand Alone (SA) architecture can be seen as the "complete 5G deployment" that does not require any part of a 4G system to operate [13].

Figure 2.18 illustrates how the traffic between a UE and a core network flows in the NSA and SA. In the NSA scenario, the 4G base station acts as a primary node while the 5G BS operates as a secondary node. Control plane signalling goes through the 4G base station, or a so-called 4G anchor, where the LTE radio interface is used. The 4G anchor is connected to a 5G BS to configure the transmission of the user plane. After the successful connection between the UE and the 5G BS is configured, the user data can be transferred on 5G NR. In the SA scenario, all traffic passes through the 5G BS and into the 5G core network (5GC) [3].

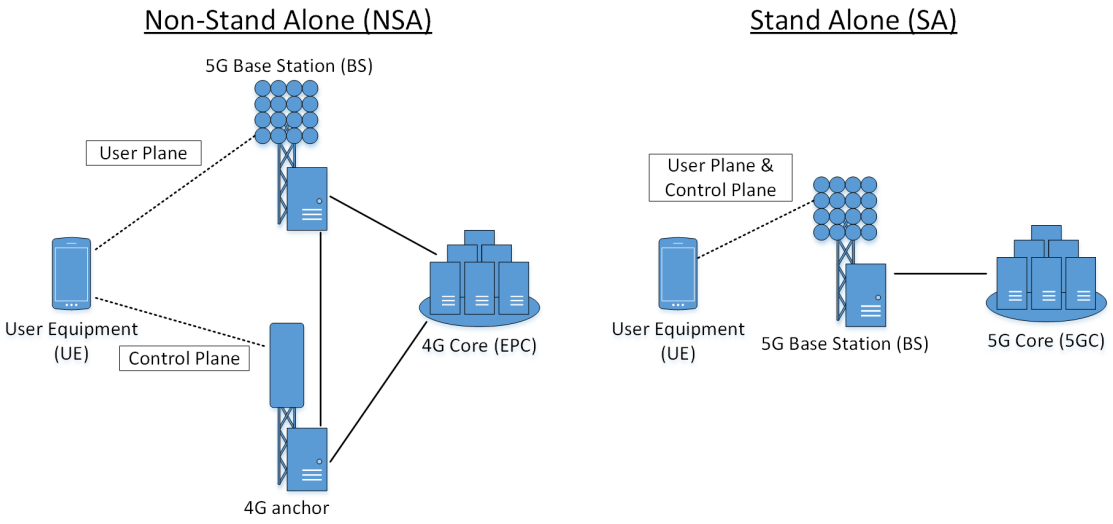


Figure 2.18 Non-Stand Alone (NSA) and Stand Alone (SA) deployment scenarios. Based on [3].

The collaboration with the 4G in NSA makes the 5G NR technology available by making some minor adjustments to the 4G core network. This easy integration of 5G NR is an attractive option for mobile operators who want to offer 5G as early as possible. Large amounts of available bandwidths at higher frequencies can be utilised using 5G NR, which leads to an increased data rate compared

to 4G LTE. However, the use of NSA brings along some disadvantages compared to SA. Firstly, 5G coverage is dependent on 4G coverage since the 4G anchor is necessary to control the 5G communication. Secondly, functionalities like extremely low latency or network slicing cannot be offered using the 4G core. Only the standalone SA version can provide all the new, exciting capabilities promised in 5G.

2.4.4 Radio connection establishment in SA

A new device that wants to connect to the network must first establish a radio connection with the base station. The procedure of the radio connection establishment between the user equipment (UE) and the 5G base station (BS) operating with the SA architecture is given in Figure 2.19. The steps of the connection establishment procedure presented in the figure are described in more detail below based on [5], [8] and [10].

1) The synchronisation block SSB contains PSS, SSS and PBCH and is periodically broadcasted by the BS. PSS and SSS are used for time and frequency synchronisation in the downlink, while PBCH carries the master information block (MIB). MIB contains configurations necessary for the further process of the connection establishment. The information that MIB carries includes system frame number (SFN), frequency offset of SSB, instructions for finding control resource set #0 (CORESET#0) on PDCCH, and subcarrier spacing of system information block 1 (SIB1). SFN is a number from 0 to 1023 that identifies the radio frame [10].
2) CORESET#0, sent on the PDCCH, contains scheduling information of PDSCH to receive SIB1. SIB1 specifies basic parameters that determine the exact time and frequency resources for the UE to transmit uplink data. In the connection establishment phase, SIB1 configures parameters for the initial random-access message transmitted on PRACH.
3) The UE's introduction to the BS is called random-access because the BS is not aware when the new UE will respond to the broadcasted messages and send a request to connect. Therefore, for the BS, the first contact from the UE is perceived as random. The first message from the UE is called Random Access Preamble and can be seen as the signature of the UE. The signature is transmitted over PRACH and is also used for uplink synchronisation.
4) The BS responds with a Random Access Response, which verifies the Random Access Preamble and configures data transmission on the PUSCH.
5) The first message on the uplink data channel from the UE to the BS is called *RRCSetupRequest*, precisely because the message contains a request to Radio Resource Control (RRC) for radio resources. RRC is a layer 3 (Network Layer) protocol that controls and manages the connection aspects of the physical layer.
6) The BS approves the request sending a confirmation called *RRCSetup* with the configurations required to complete the radio connection.
7) The UE sends a message called *RRCSetupComplete* confirming that the radio connection has been established.

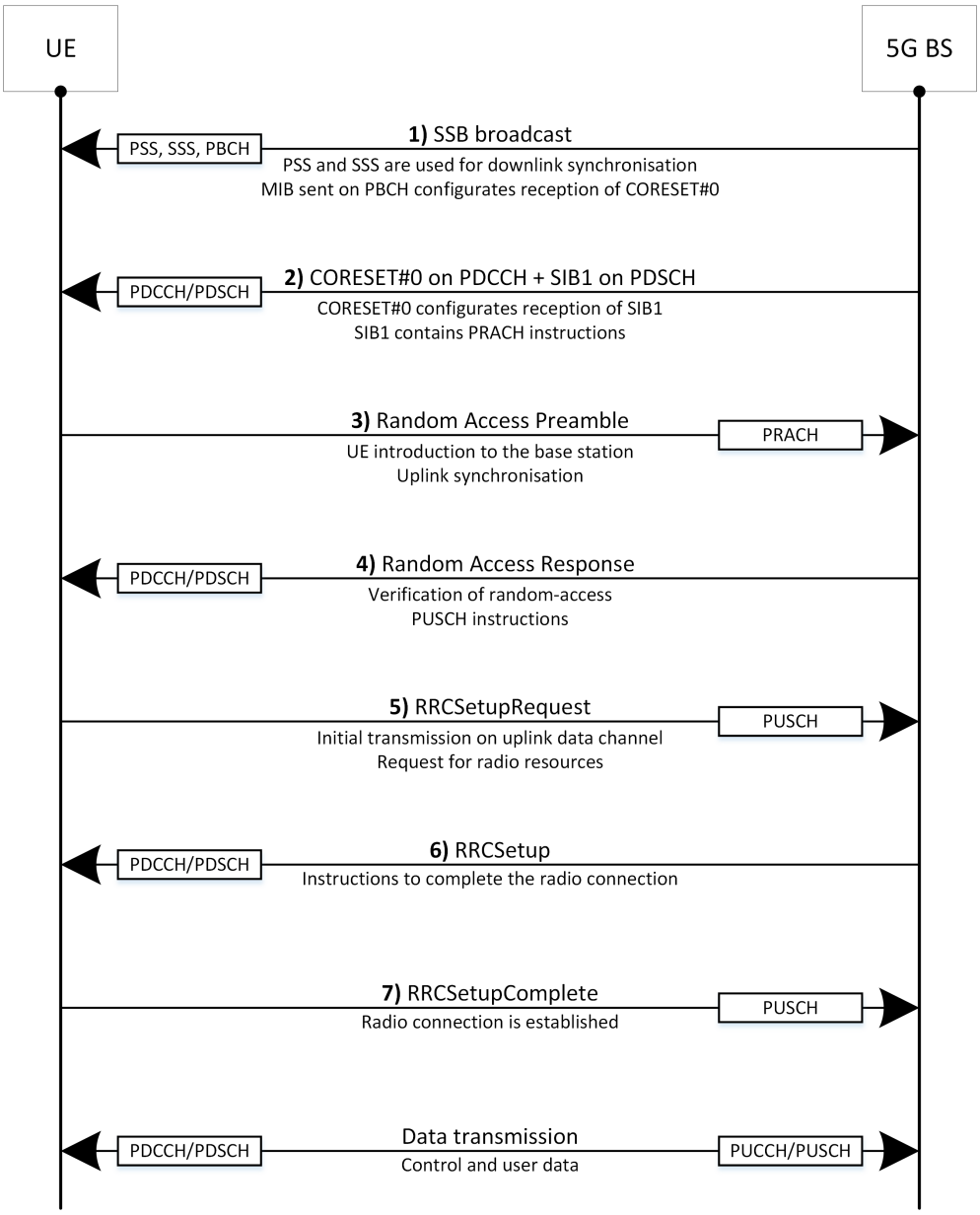


Figure 2.19 Radio connection establishment between user equipment (UE) and a 5G base station (BS) in the Stand Alone (SA) architecture. Based on [5], [8] and [10].

2.4.5 Radio connection establishment in NSA

The procedure of the radio connection establishment between the UE and the 5G BS involves a 4G anchor in an NSA architecture. The 4G anchor manages the radio resources (RRC) and allows the UE to connect to the 5G BS. Figure 2.20 shows the flow of signalling messages that are needed to establish the radio connection between the UE and the 5G BS.

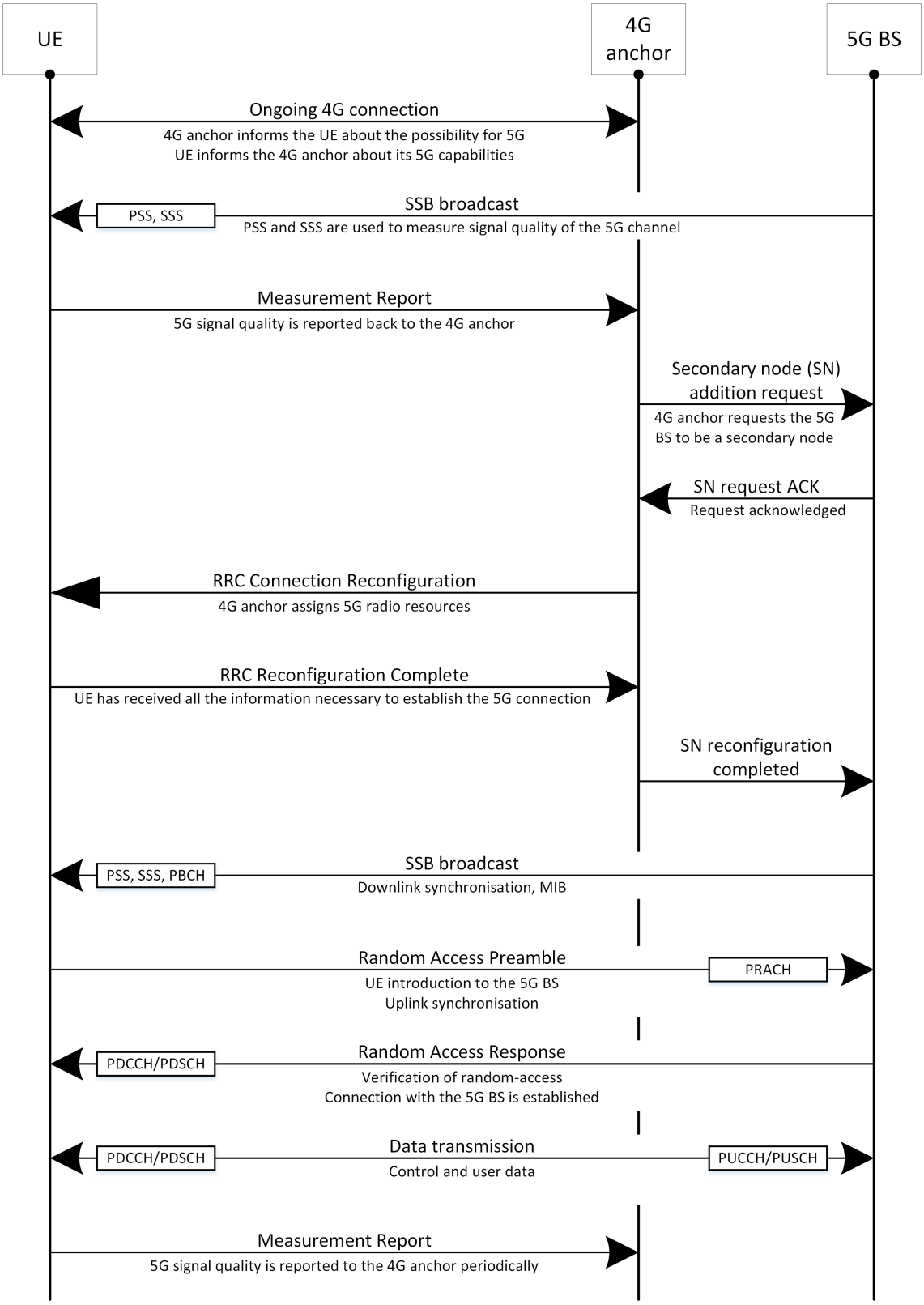


Figure 2.20 Radio connection establishment between user equipment (UE) and a 5G base station (BS) controlled by a 4G anchor in the Non-Stand Alone (SA) architecture. Based on [3].

2.4.6 User data flow

After a successful radio connection establishment, the data can be transmitted from and received by the user. Figure 2.21 shows the procedures that are carried out between a UE and a 5G BS during the dynamically scheduled transmission of user data [9].

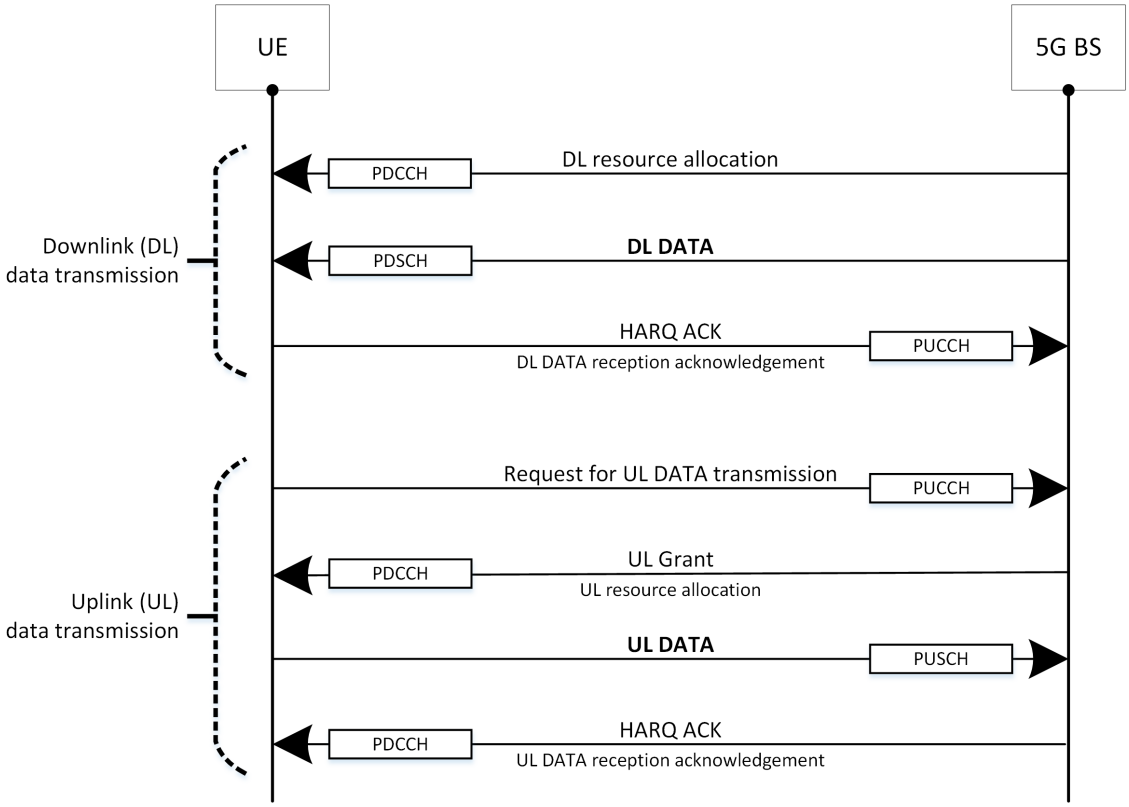


Figure 2.21 Procedures carried out between a UE and a 5G BS during the transmission of user data in uplink (UL) and downlink (DL). Based on [9].

In the downlink (DL), the time-frequency resources for DL data are allocated, and the UE receives the configurations through the control channel PDCCH. The DL data is transmitted on the data channel PDSCH. The UE responds with a hybrid automatic repeat request (HARQ) acknowledgement (ACK) through the control channel PUCCH to inform the BS about the successful data reception or ask for retransmission in case of a failure.

In the uplink (UL), the UE may request the BS for time-frequency resources for a user data transmission. If the request is granted, the radio resources are allocated, and the UE can transmit its UL data on PUSCH. The BS responds with the HARQ ACK to confirm whether or not the data was received successfully.

The uplink and downlink transmissions depend on each other. Control information concerning resource scheduling and acknowledgements must be exchanged on the physical control channels both in the uplink and downlink in order to transmit data successfully.

2.4.7 Beam management in downlink

5G NR supports multi-beam operation where every physical channel and signal is transmitted on a directional beam [13]. By utilising the massive MIMO technology, the user data can be transmitted on user-specific beams directed towards the UE. Directional links require fine beam alignment that can only be achieved through a procedure known as beam management. Beam management is defined as the process of acquiring and maintaining a set of beams, which can be used for data transmission and reception. The beam management operation, in general, is based on the reference signals and control messages which are periodically exchanged between the BS and users. The reference signals used for beam management are the channel state information reference signal (CSI-RS) and the sounding reference signal (SRS) used in the downlink and uplink, respectively [17].

To transmit DL data in user-specific beams, the BS needs to find the direction towards the UE. For this purpose, the BS applies beamforming to CSI-RS transmissions. The massive MIMO antenna at the BS transmits multiple CSI-RS beams creating a beam grid over the coverage area. The UE measures the RSRP of the strongest CSI-RS beams and reports the values to the BS. Based on the information of which CSI-RS beams were the strongest at the UE, the BS can estimate the direction of the UE and direct the beam carrying the data towards the user. If the UE moves, the reported CSI-RSRP values will change, and the BS can adjust the beamforming accordingly, creating the data beams that follow the user.

In addition, SRS can be used to estimate the radio channels of the UEs. The UE transmits the SRS so that the BS receiving this reference signal can estimate the characteristics of the uplink radio channel. The channel estimation is also valid for the downlink because of so-called channel reciprocity. Channel reciprocity means that the uplink and downlink radio channels are identical since, in TDD mode, they are using the same frequency channel and thus will be evenly affected by the radio channel environment. The BS utilises the uplink channel estimation obtained from the SRS to estimate the user's direction and direct the beams carrying downlink data towards the desired user.

3 5G NR vulnerabilities and resilience to jamming

This chapter describes jamming attacks relevant in targeting the 5G radio communication, discloses the essential vulnerabilities that the 5G radio interface has for jamming, compares jamming in NSA and SA, and compares the 5G robustness with the robustness of 4G LTE.

3.1 Radio jamming attacks

There are many types of jamming in terms of complexity, power efficiency, waveform, detectability and impact on the 5G radio communication. The jamming techniques vary from a simple noise transmission on the target bandwidth to an advanced jammer that has knowledge of the target system architecture and exploits its vulnerabilities.

Barrage jamming, also known as broadband noise jamming, is the most straightforward kind of jamming attack in which the jammer jams the entire bandwidth of the target system. It is shown to be the optimal jamming strategy in the absence of any knowledge of the target signal. In barrage jamming, the noise is transmitted in an effort to increase the noise floor at the receiver degrading its signal-to-noise ratio. Barrage jamming is typically used as the baseline when evaluating other kinds of jamming attacks [48].

In *partial-band jamming*, a certain fraction of the occupied bandwidth is jammed with noise. The partial-band jamming might be used to conserve power while still causing a denial of service [48]. This type of jamming is especially effective when a vulnerable part of the bandwidth is targeted to disrupt subcarriers critical to the communication system to function.

The 5G system design is based on open standards, so the specifications and configurations of the NR architecture are available, making 5G NR vulnerable to a jammer that is able to exploit this knowledge and attack the vital spots of the target communication system. This jamming technique is known as *smart jamming*. Smart jamming aims to increase jamming efficiency – more damage with less power. Another aim of a smart jammer might be to operate undercover so that the target system would struggle to detect the jamming activity.

A smart jammer can target individual physical channels and signals of a 5G radio communication system. This type of attack requires that the jammer is aware of the exact time-frequency allocation of the target channels and signals and is time-synchronised to the target system. The efficiency and level of sophistication of the jammer come at the cost of high complexity. However, open-source libraries and low-cost software-defined radio (SDR) make the implementation of the smart jamming attacks feasible [33]. Specially designed destructive signals to target some explicit physical channels or signals can cause severe damage using minimal power [48].

Another type of smart jamming attack is *spoofing*. Spoofing refers to the transmission of a fake signal meant to masquerade as a legitimate signal [34]. For instance, a jammer may be more efficient in transmitting fake primary and secondary synchronisation signals (PSS and SSS) rather than attempting to inject noise on top of the resource elements carrying the PSS and SSS. A UE that uses fake PSS and SSS to establish a radio connection will experience a denial of service. Spoofing

can be taken further by transmitting fake control information on the PBCH and PDCCH in an attempt to lure the UE to connect to a non-existing cell. Moreover, by transmitting large quantities of random-access preambles on the PRACH, the operation of the BS might be interrupted as the BS would try to handle many fake connection requests [33]. The complexity of this type of jammer varies depending on the extent of spoofing.

Table 3.1 sums up the most common types of jamming and their features and effect on 5G radio.

Attack type	Attack feature	Effect on 5G NR
Barrage jamming – intentional interference across the entire target bandwidth	Simplest kind of jamming attack, no knowledge of the target system is required	All physical channels and signals have to contest with jamming signal
Partial-band jamming – intentional interference across a certain part of the target bandwidth	Low complexity, can be used to target vulnerable parts of the bandwidth	Selected (parts of) physical channels and signals have to contest with jamming signal
Targeted attack on explicit resource elements in time and frequency	Efficient but high complexity, requires knowledge of the exact location of the target channel/signal and time synchronisation	Explicit channels and signals have to contest with specially designed destructive jamming signals
Spoofing – transmission of fake signals	Efficient, various levels of complexity, require knowledge of target system, might require time synchronisation	The 5G system is disturbed by fake signals that masquerade the legit communication

Table 3.1 Types of jamming, features and effect on 5G NR. Based on [33],[48].

3.2 Jamming impact on physical channels and signals

5G physical channels and signals were introduced in Section 2.2.2.2. This section covers the impact and damage that jamming can cause to these physical channels and signals. Downlink synchronisation and synchronisation signals block (SSB) were introduced in Section 2.4.1.

5G NR data channels, on which user data is transmitted and received, are the physical downlink shared channel (PDSCH) and the physical uplink shared channel (PUSCH). While jamming explicitly the resource elements (REs) carrying user data is possible, an attacker might also jam the entire uplink and downlink transmission bandwidth using barrage jamming since the data channels occupy the largest part of the time-frequency resources on a radio frame. The disrupted user data reception leads to corrupted data demodulation resulting in reduced or unavailable service [33].

Control channels in 5G NR are the physical downlink control channel (PDCCH) and the physical uplink control channel (PUCCH). Control information exchanged on the control channels between the UE and BS includes HARQ acknowledgements, resource allocation, slot format, modulation and coding format, and channel quality reports [5]. The functions of the control channels are vital for the communication system to operate successfully. Corrupted channel information results in reduced performance quality or connection loss [48].

5G NR uses demodulation reference signal (DM-RS) for channel estimation and equalisation to demodulate the received data correctly. The DM-RS is a sequence known to both transmitter

and receiver. The receiver can estimate how the communication channel distorted the transmitted signal by comparing the received and predefined reference signals. The estimate is then used to reduce noise and interference effects introduced by the radio channel. It has been shown that jamming the REs carrying DM-RS leads to a higher error rate than jamming the data channels separately. Disrupted channel estimation leads to poor demodulation of the received data. However, to surgically transmit noise on top of the REs carrying DM-RS requires knowledge or detection of the DM-RS allocation and synchronisation to the target system, which drastically increases the jamming complexity [34].

Other types of reference signals that can be jammed are the channel state information reference signal (CSI-RS) and the sounding reference signal (SRS). In the downlink, the CSI-RS can be used to estimate radio signal quality to select an optimal modulation scheme. In addition, CSI-RS assists in resource allocation, beam management, MIMO order selection, and time/frequency tracking. In the uplink, a UE can be configured to transmit SRS to enable the BS to estimate the uplink channel and provide functionalities similar to CSI-RS [17]. A sophisticated jammer can utilise this knowledge and attack on these reference signals, resulting in rapidly vanished benefits of MIMO and beamforming and significant reduction of the achievable data rates [48], [22], [18].

5G NR uses an OFDM waveform that consists of multiple subcarriers where each subcarrier carries a small amount of data. The OFDM waveform may be seen as a waveform composed of many slowly modulated narrowband signals rather than one rapidly modulated wideband signal. An OFDM symbol has a relatively long duration, making it capable of combating the distortions caused by multipath propagation. Another advantage of using multiple narrowband subcarriers is the resilience against a narrowband interferer that can degrade only a limited portion of the signal, leaving the rest of the subcarriers undamaged. In addition, wireless broadband standards such as LTE and NR include adaptive modulation, which allows subcarriers under poor conditions to fall back to a lower order modulation scheme. However, a notable drawback of OFDM is its sensitivity to timing and frequency synchronisation. Mismatch in synchronisation can cause severe issues in receiving and decoding the data correctly [48].

In 5G NR, the primary synchronisation signal (PSS) and secondary synchronisation signal (SSS) are used for frame/slot/symbol timing. PSS and SSS are formed using specific correlation sequences. The sequence correlated with itself at the receiver provides an exact peak in time to establish the time synchronisation. The sequence has a low correlation with other sequences, allowing the UE to distinguish between nearby base stations operating on the same carrier frequency. The fact that synchronisation signals are correlation-based sequences makes them more resilient to basic interference. Therefore, to jam PSS and SSS requires either sufficient jamming power or an explicitly designed signal to corrupt the correlation. In addition, to jam the PSS and SSS selectively in time requires synchronisation to the cell. Therefore, it would be more effective for an adversary to transmit fake PSS and SSS signals (spoofing), requiring less output power and no synchronisation to the cell [33]. Fake PSS and SSS can either disrupt the correlation of the legit synchronisation signals or confuse the UE and make it connect to a non-existing cell [48], [34].

The physical broadcast channel (PBCH) is broadcasted by the BS together with the PSS and SSS on the SSB. The information carried on the PBCH is essential to a UE attaching to a cell. A jammed PBCH would prevent new UEs from accessing the cell. PBCH jamming can be performed in a time-selective manner if the jammer can synchronise to the target cell. Otherwise, the jammer could disrupt the resource blocks that contain the PBCH [33]. While jamming the PBCH is of concern, spoofing might also cause a denial of access if the UEs are lured to connect to a non-existing cell.

A UE uses the physical random access channel (PRACH) to deliver its initial message to a BS in the radio connection establishment or re-establishment procedures. In order to corrupt this initial message, a jammer would firstly need the information about the allocation of the physical channel on the radio frame. This information can be obtained by decoding the SIB1 message broadcasted on the PDSCH. A jammed PRACH can cause a denial of service to the new users attaching to the cell or prevent an existing user from transitioning from an idle to an active state. The UE goes to an idle state when no mobile services like calling or data are needed. In the idle state, the UE is still camping on the cell without consuming any radio resources. The UE must enter the active state to get the radio resources assigned and access the mobile services. The UE uses the PRACH to initiate the transition to an active state, and if that transition is blocked, the user experiences denial of service. Eventually, all users in the cell can lose the connection as the mobile devices enter the idle state and can not go back to the active state. The random-access preamble transmitted on PRACH is a correlation-based sequence, which, similarly as with PSS and SSS, requires relatively strong interference to be disrupted. However, a custom-designed waveform that targets the random-access preambles or flooding of fake random-access preambles to confuse the BS is feasible [33], [34].

Table 3.2 sums up the impact that jamming has on the separate 5G physical channels and signals and the damage such impact could cause for the 5G radio communication. Every 5G physical channel and signal would require different jamming power to be disrupted and different complexity when building a smart jammer that targets that individual physical channel or signal. The authors of [33] have introduced an analysis of jamming complexity versus attack efficiency on separate 5G physical channels and signals.

Disrupted physical channel/signal	Impact	Damage
Data channels PDSCH and PUSCH	Increased error rate in modulation symbols detection, data demodulation is corrupted	Reduced or unavailable service
Control channels PDCCH and PUCCH	Vital control information managing the connection fails to be delivered	Reduced or unavailable service
Reference signal DM-RS	Channel estimation and equalisation is disrupted, data demodulation is corrupted	Reduced or unavailable service
Reference signals CSI-RS and SRS	Inefficient MIMO and beamforming performance	Reduced service quality
Synchronisation signals PSS and SSS	Blocked cell detection, disrupted time and frequency synchronisation	New connections cannot be established, active connections are lost
Broadcast channel PBCH	Prevented attachment to a cell	New connections cannot be established
Random-access channel PRACH	Request to connect or re-connect to a cell is disrupted	New connections cannot be established, active connections are eventually lost

Table 3.2 Impact and damage on 5G radio communication caused by disrupting a physical channel or signal. Based on [33], [34], [48].

3.3 Jamming of Non-Stand Alone (NSA) and Stand Alone (SA)

Jamming of 5G NR can have a different impact on the total system performance depending on whether the radio communication operates in Stand Alone (SA) or Non-Stand Alone (NSA) mode. SA and NSA were presented in Section 2.4.3. Radio connection establishment in SA and NSA were presented in Section 2.4.4 and Section 2.4.5, respectively.

In SA, all control signalling and data traffic are transmitted on 5G NR. In NSA, a 4G anchor manages the connection on 5G NR and uses the 5G channel as a supplementary data carrier. The management from the 4G side involves radio connection establishment and maintenance controlled by the RRC protocol on layer 3 (Network Layer). The 4G anchor assigns 5G radio resources to the UE and monitors the connection between the UE and 5G BS in case the connection needs to be terminated or handed over. Compared to SA, part of the information carried on MIB and SIBs and some RRC instructions are carried on 4G LTE in NSA [3]. Thus, when the 5G channel is jammed in NSA, all the messages necessary for the connection establishment will not be disrupted. Therefore, the connection establishment procedure might go smoother in NSA compared to SA when the 5G channel is jammed.

Physical layer procedures and user data transmission on physical control and data channels are the same in SA and NSA operations. When the 5G BS has established the connection with the UE, the 5G BS manages the radio transmission on 5G NR itself in NSA, the same way the 5G BS would do in SA [9]. Therefore, the jamming of the data transmission on 5G NR should have the same consequences, whether it is SA or NSA.

However, if the 5G channel is corrupted in NSA, the UE can be downgraded to operate on an uninterrupted 4G channel. In SA, this option is not available. Given that there are no neighbour cells, the UE might be forced to operate on a 5G channel of poor quality or terminate the connection and go into "no service" mode.

3.4 5G NR robustness in comparison with 4G

It is anticipated that 5G NR is relatively vulnerable to electronic warfare, given that commercial mobile technology is not designed to operate in a challenging electromagnetic environment. Nevertheless, the fifth generation technology has improved on some radio aspects compared to the previous generations. Some of the improvements can enhance robustness to jamming attacks.

5G NR can operate on higher frequencies than 4G LTE can. Operating in a high-frequency range, especially mmWave, reduces the cell coverage area because of the increased signal path loss. A short-range cell creates a small communication "bubble" with reduced unwanted radio emissions outside this "bubble".

Another factor in 5G NR that reduces unwanted radio emissions is the massive MIMO technology. The antenna array at the BS enables beamforming, leading to the signal energy being concentrated towards the user, thus reducing the emissions in unwanted directions. Less exposure in the frequency spectrum makes it more difficult for the jammer to detect, identify, eavesdrop and exploit the radio communication.

Another advantage of directing the signal energy towards the UE is a stronger received signal in the downlink, which is beneficial when combating interference.

Furthermore, compared to 4G LTE, 5G NR is less vulnerable to electronic warfare because of its dynamic nature in the physical layer design. Static allocation of a physical channel or signal in the time and frequency domain makes it easier for a jammer to find, exploit and attack that specific physical channel or signal. But, this is not the case with 5G NR. The allocation of the 5G NR physical channels and signals on the radio frame is highly flexible and configurable. For example, synchronisation signals must no longer be allocated at the centre of the transmission bandwidth, as it is done in 4G LTE. The SSB in 5G NR can be placed across the entire transmission bandwidth following the synchronisation raster described in Appendix B. Another example is the uplink control channel, PUCCH, which is especially vulnerable to jamming. In 5G NR, PUCCH can be mapped more dynamically so that it cannot be jammed simply by transmitting the energy on the outer edges of the uplink transmission bandwidth, as was the case in 4G LTE [33].

Lastly, less information is broadcasted in 5G NR than in 4G LTE, which means less information can be intercepted and exploited to disrupt the communication. In 4G LTE, the physical control format indicator channel (PCFICH) is vulnerable to jamming. In 5G NR, this channel is not needed and has been removed [33]. Another improvement relative to 4G LTE is the support of on-demand SIB transmission that enables the UE to request specific SIBs instead of them being periodically broadcasted [17].

4 Experiment set-up

The jamming experiment took place at Rygge Air Station, which is operated by the Norwegian Armed Forces. The 5G infrastructure was provided through the 5G-VINNI project funded by the EU [15]. The 5G-VINNI network at Rygge is operated by Telenor Research. The testing activities are coordinated by the Norwegian Defence Material Agency (FMA).

This section presents the 5G base station set-up, measurement equipment, jamming equipment, jamming approach, selected measurement and jammer positions, and the approach of measuring the 5G performance.

4.1 5G base station

The network providing 5G coverage contained a 5G base station (BS) placed in the premises of Rygge Air Station and a 4G core network placed at Fornebu. The BS was connected to the core network via fibre and Telenor's transport network. The radio communication system operated on the Non-Stand Alone (NSA) architecture. As described in Section 2.4.3, in NSA, the 5G radio communication relies on and is managed by a 4G LTE radio, the so-called anchor, while the 5G NR band is used as a data carrier. Detailed specifications of the 5G BS and radio communication used in the experiment are given in Table 4.1. Figure 4.1 shows the BS at the test site with both 4G and 5G antennas.

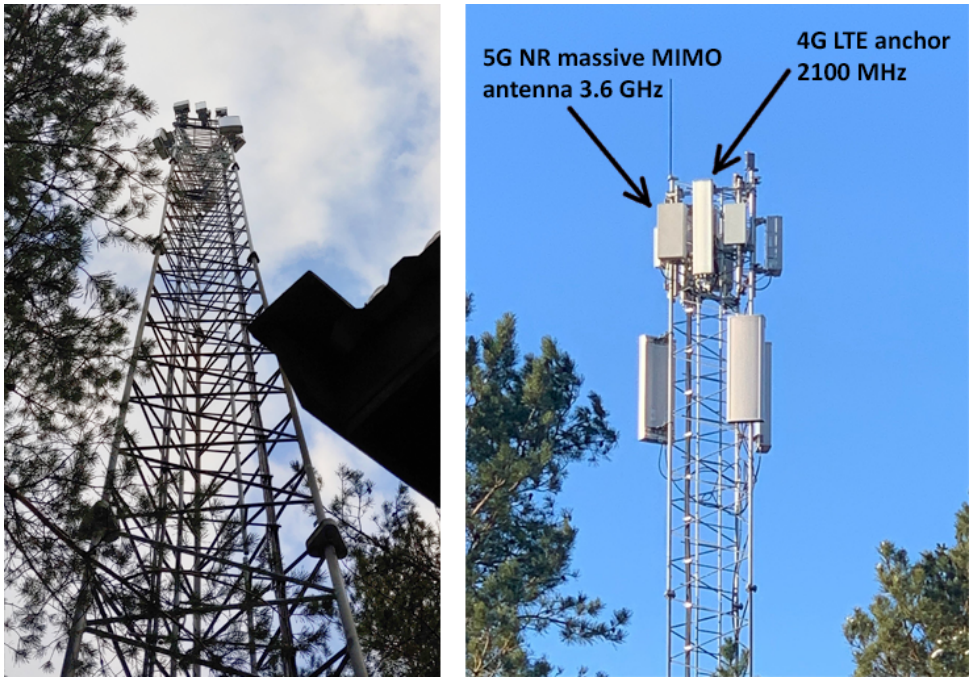


Figure 4.1 Base station at the 5G test site at Rygge (photos: Kennet Nomeland/FMA).

Feature		Specification
5G BS	Height	24 meters
	Serving sectors	2 (105 and 205)
	Antenna	Huawei AAU5613
	Technology	Massive MIMO 64T64R
	Max antenna gain	25 dBi
	Max EIRP	68 dBm
	Polarisation	Cross (+45° and -45°)
5G radio communication	Frequency band	n77/n78 (3.6 GHz, C band)
	Operational frequency	3.62–3.70 GHz
	Bandwidth	80 MHz
	Number of SSB beams	7 (default)
	Duplex	TDD
	Modulation	QPSK, 16QAM, 64QAM
	Subcarrier spacing	30 kHz
	Slot configuration	DDDSU (4:1)
	Max SU-MIMO streams	4 in downlink, 1 in uplink
	Architecture option	Non-Stand Alone (EN-DC, option 3)
	4G anchor band	B1 (2100 MHz)

Table 4.1 Specifications of the 5G base station (BS) and radio communication at the test site at Rygge.

4.2 Measurement equipment

Equipment for the 5G physical layer measurements included a Sony smartphone with customised software from Rohde and Schwarz (R&S), a fixed wireless access (FWA) terminal from Huawei, and a spectrum analyser from Keysight.

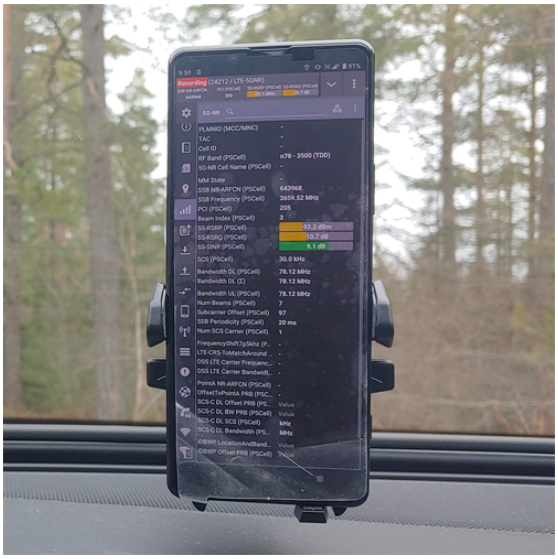
A Sony Xperia 1 II (XQ-AT51) smartphone with Android 10 had a measurement tool, called QualiPoc, installed. The QualiPoc is a mobile application from R&S that monitors and stores many physical layer parameters that are not available to a regular Android user [45]. The smartphone was the primary measurement equipment for the experiment.

An attempt to use an FWA terminal, or so-called customer premises equipment (CPE) device, was made to determine any difference in performance between a smartphone and a CPE device when the devices operate in a contested RF environment. Huawei 5G Outdoor CPE (N5368X) was used for this purpose.

A spectrum analyser, or an RF scanner, measures the magnitude of incoming radio signals at a given frequency spectrum. A spectrum analyser N9914B FieldFox from Keysight was used to measure the activity on the 3.6 GHz frequency band [49]. In addition, the analyser had a built-in 5G NR mode that could recognise and decode the broadcasted SSBs. By using this function, all the available SSB beams could be measured simultaneously, providing the measurements of their SS-RSRP,

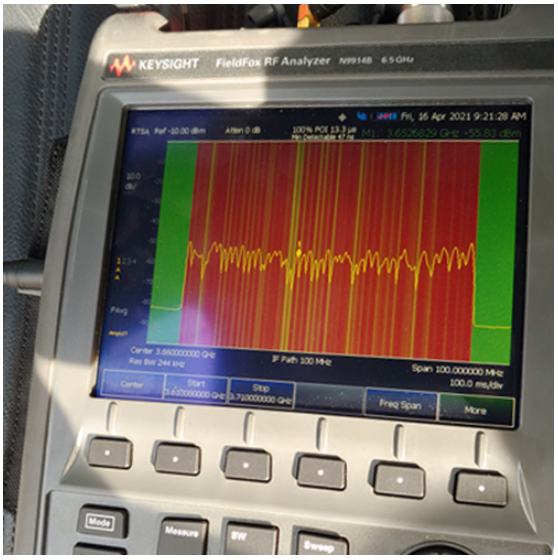
SS-RSRQ and SS-SINR. An external omnidirectional antenna Pointing A-OMNI-0296-V1 was used with the RF scanner [44].

Figure 4.2 shows the measurement equipment used in the experiment. The measurement equipment was mounted at fixed positions in the car to achieve consistent results.



(a) Sony Xperia 1 II smartphone with the QualiPoc measurement tool.

(b) Huawei 5G Outdoor CPE.



(c) N9914B FieldFox spectrum analyser from Keysight.

(d) External omnidirectional antenna for the spectrum analyser.

Figure 4.2 Measurement equipment used for the experiment.

4.3 Jamming equipment and waveform

The jamming equipment consisted of a commercial high-bandwidth signal generator, a commercial power amplifier, and a custom-made helix antenna. Figure 4.3 shows the overview diagram of the jamming equipment modules.

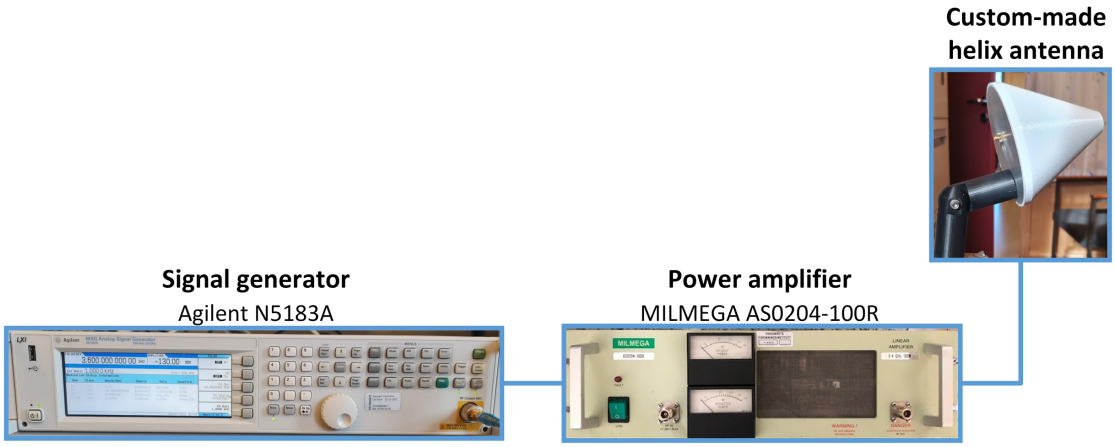


Figure 4.3 Overview diagram of the jamming equipment modules.

The signal generator Agilent N5183A was used to generate a jamming waveform. The jamming waveform was a frequency-modulated sinusoidal signal. The sweeping frequency of the modulated sinusoidal signal was set to 1 kHz, meaning that the sinusoidal waveform was sweeping back and forth across the targeted bandwidth 1000 times per second. According to [51], jamming, in which a narrow frequency band of jamming energy is repeatedly swept over a relatively wide frequency band, and the sweep rate is high enough to accomplish its jamming task, may be considered as a barrage or partial-band jamming. Figure 4.4 shows the envelope of the 80 MHz wide jamming signal.

The power amplifier MILMEGA AS0204-100R was used to amplify the jamming signal power to the desired level. The amplifier's incident power meter was used to monitor and determine the output power delivered by the amplifier.

A custom-made[1] directional wideband helix antenna was used for the jamming signal radio transmission. A helix-type antenna radiates circularly polarised radio waves. The reason for using a circular polarisation (right-hand) antenna for the experiment was to be independent of the polarisation of the targeted 5G system. The circularly polarised jamming waveform targeted all possible linear polarisations (horizontal, vertical and crossed). The maximum gain of the antenna at 3.5 GHz is 10.7 dBi with a 3 dB opening angle of +/- 22 degrees. This gain value was considered applicable for the jamming frequency range at 3.6 GHz. The modelled antenna pattern in the horizontal plane is given in Figure 4.5.

The total system loss, including the loss in the cables, connectors and antenna radome, was estimated to be 4.7 dB.

[1] Designed by Asbjørn Kleivstul/FFI.

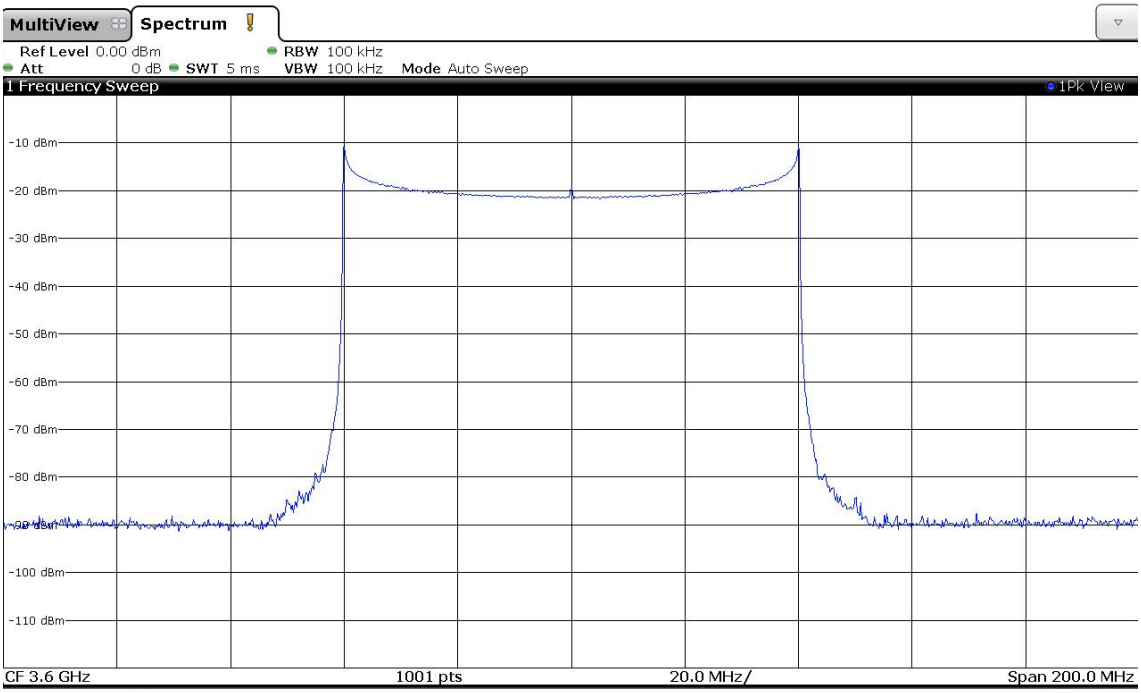


Figure 4.4 The envelope of the 80 MHz wide jamming signal.

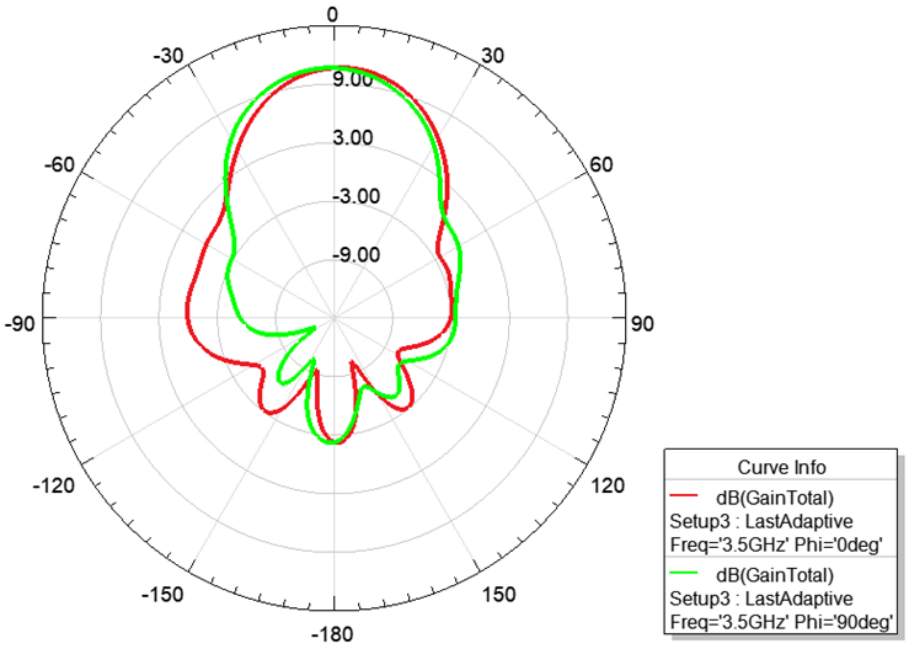


Figure 4.5 The modelled helix antenna pattern in the horizontal plane.

The antenna was mounted on a rotor attached to the top of a 10-meter high mast (AB-175N). The rotor simplified the physical pointing of the antenna towards the target objects. A picture of the antenna setup is provided in Figure 4.6.

Figure 4.6 Antenna installation on a 10-meter high mast.

4.4 Jamming approach

There are many ways to jam a radio signal. The following sections describe the jamming approach used to attack the radio communication on 5G NR in the experiment.

4.4.1 Barrage jamming and partial-band jamming

Two different types of jamming attacks were applied in the experiment: barrage jamming and partial-band jamming. The barrage jamming attack targeted the entire 80 MHz bandwidth of the 5G system operating at the 3.62–3.70 GHz frequency range. The partial-band jamming attack targeted part of the band carrying the SSB signal. The targeted bandwidth, in this case, was 7.2 MHz wide, with the centre frequency at 3659.52 MHz. Since this type of partial-band jamming aimed to interfere with the synchronisation signals on the SSB, we refer to this jamming attack as *SSB jamming* in this report.

The bandwidth of an SSB can be calculated by multiplying the number of subcarriers it contains with the frequency distance between the subcarriers. One SSB spans 20 resource blocks or 240 subcarriers (one resource block contains 12 subcarriers). The distance between the subcarriers is specified by the numerology and was 30 kHz in our case. Thus, in the test set-up, the SSB spanned $240 \times 30 = 7200$ kHz or 7.2 MHz of bandwidth.

There are several ways of finding the exact frequency where the SSB is positioned. Since the SSB is periodically broadcasted on the cell, the RF spectrum can be inspected with a spectrum analyser

to find a power level that exposes the SSB. This method does not require being a legit user on the network. In case the user is a legit subscriber, the UE will need to find the SSB to obtain the synchronisation with the BS. The UE finds the SSB by using the global synchronisation channel number (GSCN). This number can be read on a measurement tool like QualiPoc and converted to the exact frequency. More information on the GSCN and the exact location of the SSB, both in time and frequency, can be found in Appendix B.

4.4.2 Uplink and downlink jamming

The 5G radio communication on the 3.6 GHz frequency band operates in TDD mode, meaning that the uplink and downlink channels use the same frequency channel. In our test set-up, the uplink jamming and downlink jamming could not be completely separated because both the uplink channel and the downlink channel, in other words, the BS and UE, were always jammed. However, we picked some specific measurement locations and jammer directions in order to separate the analysis of the jamming effect on uplink and downlink as much as possible. Thus, we introduced separate scenarios for uplink jamming and downlink jamming.

In the uplink jamming scenario, the jammer aimed to attack the BS. The directive jammer antenna was physically rotated to point its maximum gain towards the BS to disrupt the uplink signal. The jammer was always in LOS with the BS. The UE received interference only from the side lobes of the jammer. Also, the BS could transmit the downlink signal with an EIRP of 68 dBm, which was 45 dB higher compared with the 23 dBm TRP of the uplink signal transmitted by the UE. Barrage jamming was applied in the uplink jamming scenario.

In the downlink jamming scenario, the jammer aimed to attack the user equipment. The jammer was in LOS with the UE and NLOS with the BS. While some of the interference was still present at the BS, it was the closest we could get to a scenario where only the UE was jammed. Both barrage jamming and SSB jamming were applied in the downlink jamming scenario.

4.4.3 Jamming signal power

Different types of jammers will have different maximum output power levels for transmitting the jamming signal. To model different types of jammers, the tests were conducted with different power settings on the jammer.

The signal power transmitted on the directional antenna can be represented as effective isotropic radiated power (EIRP). The EIRP in our case was calculated by

$$\text{EIRP}_{[\text{dBm}]} = \text{Power amplifier output}_{[\text{dBm}]} - \text{Total system loss}_{[\text{dB}]} + \text{Antenna gain}_{[\text{dBi}]}.$$

As presented in Section 4.3, the total system loss was 4.7 dB, and the antenna gain was 10.7 dBi. Three different power output levels at the jamming signal power amplifier were set up for the experiment: 0.5, 5 and 50 W, which resulted in the jamming signal EIRP levels of approximately 33, 43 and 53 dBm, respectively.

4.5 Measurement and jammer positions

5G NR performance testing included tests that had to be manually started and monitored on the smartphone. Some fixed measurement positions had to be selected where the car could be parked, and the tests could be conducted. The connection stability was also taken into account when selecting the measurement positions. Even though the selected positions met varying LOS/NLOS propagation conditions and had different distances to the BS, they were all selected to have a stable and persistent connection to the cell.

Figure 4.7 shows the selected measurement positions (M1–M9) and jammer positions (J1–J3). The figure also provides the cell sectors, the cell range, the LOS/NLOS propagation conditions between the UE and BS, and the jammer direction. At J1 and J2, the uplink jamming was applied as the jammer aimed directly towards the BS. The measurements were taken at M1–M4 with the jammer placed at J1 (Figure 4.7a). With the jammer placed at J2, the measurements were taken at M5–M8 (Figure 4.7b). With the jammer placed at J3, the downlink jamming was applied as the jammer aimed towards the UE at M9 (Figure 4.7c).

4.5.1 Path loss

An estimate of the path loss between the UE and BS and between the jammer and its target was needed to compare the signal strengths of the 5G signal and the jamming signal. Two existing path loss models fitted the test environment and set-up: the path loss exponent model [55] and the path loss model for Rural Macro (RMa) scenario defined by 3GPP [14]. The 3GPP RMa path loss model was applicable for 5G radio communication (except for one measurement position, where the path loss exponent model was applied). For the jamming signal path loss, the path loss exponent model was applied.

The path loss exponent model is defined as

$$L = 10n\log(d) + C$$

where L is the path loss measured in dB, n is the path loss exponent, d is the air distance between the transmitter and receiver measured in meters, and C is a constant. With $n = 2$ and $C = 20\log(40\pi f/3)$ where f is the carrier frequency measured in GHz, we get the model for the free space loss (FSL). With an increased value of n, the model considers for higher losses, for example, taking into account the obstructions in an NLOS scenario.

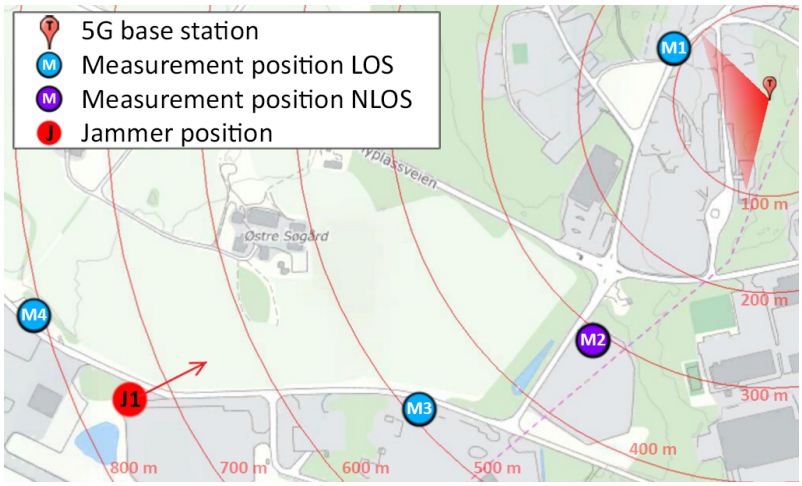
The 3GPP RMa path loss model is relatively complex. The complete equations of the model and the derivation of applying the model to our test environment are given in Appendix C. The applied 3GPP RMa path loss model became

$$L = 20\log(40\pi f/3) + 20.5\log(d) + 0.0014d - 0.7$$

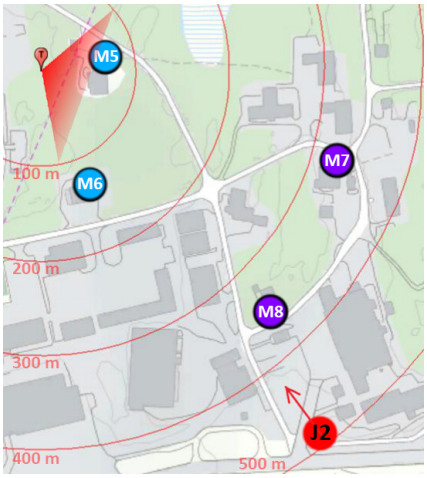
for LOS and

$$L = 20\log(f) + 39.1\log(d) + 7.2$$

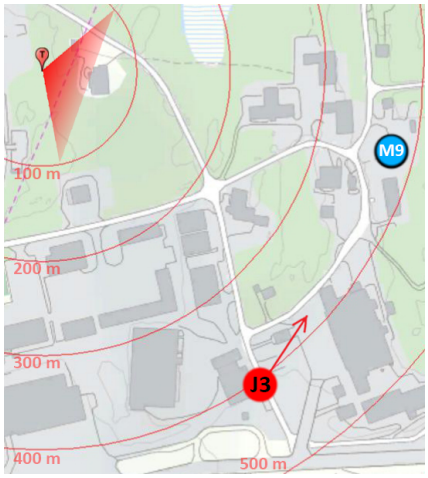
for NLOS where L is given in dB, d is given in meters, and f is given in GHz. The given RMa LOS path loss model was valid within a 2 km distance between the UE and BS. The given RMa NLOS model was valid within a 5 km distance.



(a) M1–M4 and J1. Uplink jamming.



(b) M5–M8 and J2. Uplink jamming.



(c) M9 and J3. Downlink jamming.

Figure 4.7 Measurement positions (M1–M9) and jammer positions (J1–J3).

In Figure 4.8, the path loss was calculated within a 2 km distance between the transmitter and receiver using the given path loss models. The RMa LOS model complied with the FSL model, while the RMa NLOS model complied with the path loss exponent $n = 3$.

For clear LOS and clear NLOS scenarios, the RMa LOS and RMA NLOS models were used to calculate the path loss between the UE and BS. The path loss exponent model with $n = 2.5$ was used for measurement position M7 where the obstacles were only partially blocking the link between the user and the base station, and thus the model in-between the LOS and NLOS was needed. Table 4.2 provides the characteristics of every measurement position in terms of the serving sector physical-layer cell identity (PCI), the air distance between the UE and BS, the LOS/NLOS propagation conditions, the applied path loss model, and the calculated path loss. The smartphone was placed inside a vehicle during the measurements, which could cause additional radio signal attenuation. However, the vehicle was always directed towards the BS so that the only obstruction would be the front windscreen. The attenuation of the signal penetrating the front windscreen was assumed to be insignificant and, thus, could be neglected.

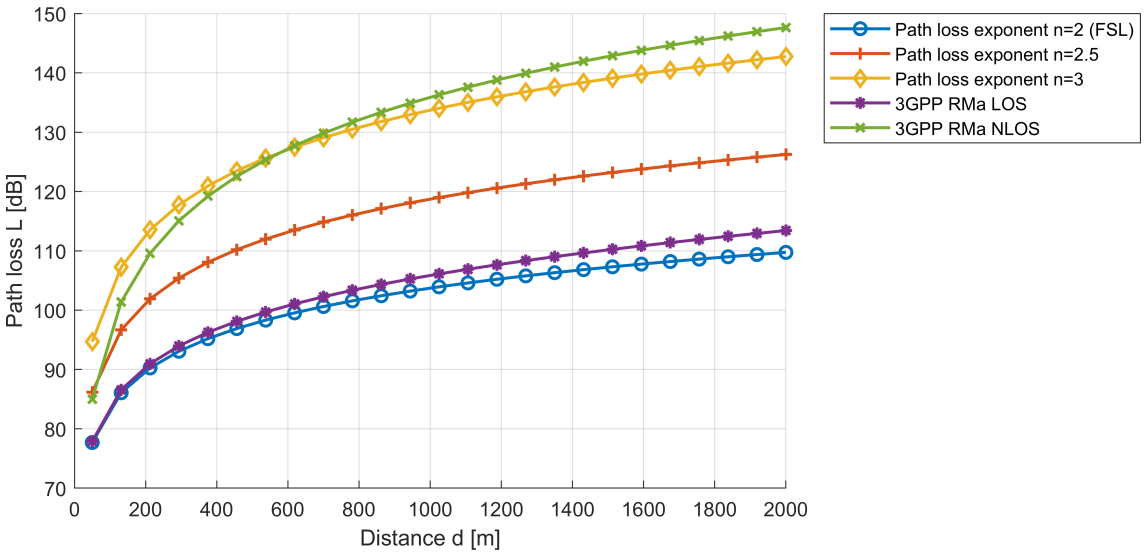


Figure 4.8 Path loss calculations for 3.66 GHz frequency using different path loss models.

Meas. position	Serving sector PCI	Air distance between UE and BS [m]	LOS/NLOS propagation conditions	Path loss model	Path loss [dB]
M1	105	116	LOS	RMa LOS	85
M2		315	NLOS, blocked by buildings	RMa NLOS	116
M3		498	LOS	RMa LOS	99
M4		806	LOS, between some trees	RMa LOS	104
M5	205	79	LOS	RMa LOS	82
M6		125	LOS, between some trees	RMa LOS	86
M7		324	NLOS, partly blocked by tree tops	Path loss exponent $n = 2.5$	106
M8		344	NLOS, blocked by buildings and trees	RMa NLOS	118
M9		389	LOS	RMa LOS	97

Table 4.2 Characterisation of measurement positions.

For the jamming signal, the path loss exponent model was selected. Since the jammer was always in LOS with the target, the FSL model was applied. Table 4.3 provides the characteristics of every jammer position in terms of the pointing direction of the jammer's antenna, the air distance between the jammer and the target, the LOS/NLOS propagation conditions, the applied path loss model, and the calculated path loss.

4.6 Performance measurements

This section describes the parameters measured on the physical layer, explains the dynamic nature of the physical layer, presents how the throughput measurements were interpreted, describes in detail

Jammer position	Target and pointing direction	Air distance to target [m]	LOS/NLOS propagation conditions	Path loss model	Path loss [dB]
J1	BS	751	LOS	FSL	101
J2	BS	487	LOS	FSL	98
J3	UE	288	LOS	FSL	93

Table 4.3 Characterisation of jammer positions with respect to its target.

the metrics retransmission rate and block error rate, and introduces a jamming-to-uplink-signal ratio used to characterise the jamming effect.

4.6.1 Measured physical layer parameters

As previously explained, the primary measurement equipment in the experiment was a smartphone pre-installed with the QualiPoc mobile application. The UE was used to monitor and store the physical layer parameters of the 5G communication. The measured values were stored every time there was a change in value in one of the monitored parameters. Often, this led to 5–20 samples per second. The key parameters for the 5G performance analysis are given in Table 4.4. The table also describes each parameter.

Parameter	Description	Units	Range	UL/DL
Beam Index	Beam index of the serving SSB beam	-	0–6	DL
SS-RSRP	Reference Signal Received Power measured in SSB	dBm	-	DL
SS-RSRQ	Reference Signal Receive Quality measured in SSB	dB	-	DL
SS-SINR	Signal-to-Noise and Interference Ratio measured in SSB	dB	-	DL
Throughput	Physical layer throughput	Mbps	-	UL/DL
MCS Index	Modulation Coding Scheme index averaged over 500 ms. The index converts to modulation scheme according to Table 4.5	-	0–31	UL/DL
MIMO Rank	Number of serving SU-MIMO data streams in DL	-	1–4	DL
BLER	Block Error Rate – the rate of received erronous transport blocks	%	0–100	DL
Retransmission rate	The rate of retransmitted transport blocks	%	0–100	UL

Table 4.4 Parameters measured and stored on the UE side.

QualiPoc monitors the throughput of the 5G communication on the physical layer. This metric includes all the headers, so the actual user data rate is lower.

Modulation and coding scheme (MCS) Index is an indicator of the modulation scheme and the code rate used for the data transmission. The MCS Index, defined by 3GPP in [6], can be translated into the exact values of the modulation scheme and coding rate. The simplified version of the relation between the index and the modulation scheme that applies to the 5G communication in our test

MCS Index	Modulation scheme	Bits/symbol
0 <= index <10	QPSK	2
10 <= index <17	16QAM	4
17 <= index <= 31	64QAM	6

Table 4.5 Conversion table from the MCS Index to the modulation scheme that applies to the measurements.

set-up is given in Table 4.5. As the MCS Index varies between 0 and 31, the modulation scheme alters between QPSK, 16QAM and 64QAM.

The parameter MIMO Rank monitored the number of parallel MIMO data streams received in the downlink by the single user (SU-MIMO). This parameter was only given for the downlink because the value of the MIMO Rank in the uplink was constantly equal to one, meaning that the UE transmitted only one data stream, and the SU-MIMO was not used in the uplink.

4.6.2 Dynamic test environment

The physical layer of a mobile communication system is dynamic and can adapt to various radio environments. A base station and a user in the cell exchange information about the quality of the radio link. The UE measures the radio channel and constantly reports the results to the BS. The radio channel quality can be determined by measuring the reference signals or monitoring the occurred errors in transmission. Depending on the radio channel quality, the physical layer parameters like modulation and coding scheme can be adjusted dynamically to achieve optimal throughput and spectral efficiency performance.

The dynamic and automated nature of the physical layer settings in the 5G communication system made our test environment slightly uncontrolled. We did not have an option to lock the mobile phone to communicate on the 5G channel regardless of the radio channel quality, nor we could lock the mobile phone to use a specific modulation scheme or code rate. The radio access technology (4G LTE or 5G NR) and physical layer parameters were selected automatically depending on the radio channel quality measured by the BS and UE.

4.6.3 Throughput and service quality

Our user terminals were the only users in the cell, and only one terminal was connected at a time. Any instabilities and changes of the 5G performance could not be caused by the network load or radio resource sharing.

The user data throughput depends on the selection of the physical layer parameters like modulation scheme, coding rate, and MIMO Rank. Higher signal quality allows higher order of modulation or can lead to a lower rate of errors, thus providing higher throughput. Since the measured throughput

depends on several physical layer parameters that dynamically adapt to the radio environment and radio channel quality, we selected the throughput as a primary performance indicator of the 5G communication.

The smartphone was pushed to send and receive as much data as possible to measure the maximal capacity of the communication link. Speed test applications from Ookla [43] and iPerf3 [30] were used to generate the data traffic and measure the throughput on uplink and downlink. Every speed test was started manually. One speed test lasted for, on average, around 10 seconds.

As described in section 4.6.2, the dynamic parameter selections made on the 5G physical layer could determine the throughput performance or even force the UE to downgrade to 4G. The dynamic nature of the physical layer in our test environment made the throughput results uncontrollably varying and unstable. In other words, the throughput performance depended not only on the radio channel quality but also on the physical layer parameter adjustments made to adapt to the radio environment dynamically.

Multiple consecutive speed tests were conducted at each measurement position and jamming set-up. Because of the uncontrolled test environment, the outputs of the speed tests were inconsistent in the presence of interference. The speed test with the highest throughput represented the 5G system's best adaptation to the contested RF environment compared with the rest of the tests and, therefore, was considered the optimal response to jamming. When measuring the effect of jamming at any given measurement position and jamming set-up, we used these optimal 5G performance results in the analysis, isolating the effect of physical layer parameters selection. The performance indicators like the MCS Index and MIMO Rank were calculated over the interval of samples obtained during this optimal, highest-throughput speed test.

The 5G performance at each measurement position and jamming set-up could not be characterised only by the optimal performance. In reality, when the interference was present, the service delivered by 5G could become unstable and unreliable. Four different service quality levels were introduced to characterise the results of the 5G performance in terms of service stability: stable, acceptable, unreliable and no service. The categorisation of the service quality levels is described in Table 4.6. The service quality was described in terms of 5G connection stability, expected user experience and service delivery, and variations in measured throughput. Each level was given a specific colour.

Service quality	5G connection	Service and throughput
Stable	Stable connection	Stable throughput used for reference measurements without any interference
Acceptable	Persistent and non-breaking connection on 5G with reduced service quality	Varying throughput, but stable enough to have an acceptable communication
Unreliable	Unstable 5G connection that could either break at any time or became too degraded to deliver any service	Unstable and unpredictable throughput enough to deliver the service to some extent
No service	Unserviceable 5G connection often downgraded to 4G	Obtained throughput was not enough to deliver any basic service

Table 4.6 Description and representative colour of different service quality levels.

4.6.4 Retransmission rate and block error rate (BLER)

Retransmission rate measured on the physical layer is the percentage of the transport blocks that failed to be delivered correctly in uplink and needed to be retransmitted from the UE. Block error rate (BLER) is the transport blocks that failed to be delivered correctly in the downlink and must be retransmitted from the BS. The retransmission rate and BLER are measures of the radio link quality that can help the 5G system select the physical layer parameters for optimal communication.

However, the radio channel quality can not be evaluated by only looking at the retransmission rate and BLER because these error rates are relative to the selected physical layer parameters like the modulation scheme. For example, a high order modulation scheme can lead to a higher retransmission rate if more errors in modulation symbol detection occur. However, that would not necessarily mean that the channel quality is poor. If the increased modulation order leads to a higher retransmission rate but still provides increased throughput, the retransmission rate can be considered acceptable, and the radio link can be considered favourable. Since there is a relation between the modulation order and the error rates, the retransmission rate and BLER were analysed separately for a given modulation scheme.

4.6.5 Jamming-to-uplink-signal ratio (J/S)

In uplink jamming, the jammer transmits its signal towards the BS and aims to interrupt the signals arriving from the UE. We introduced a jamming-to-uplink-signal ratio (J/S) to characterise the jamming effect with respect to the received uplink signal. Every measurement and jammer position differed in terms of distance and path loss to the BS. Additionally, the jammer had different set-ups of the transmit power. The J/S ratio covered all the scenarios.

We defined J/S as the ratio of the jammer signal power at the BS and the UE signal power at the BS. The signal power that reaches the BS is defined by the transmit power and the path loss. The J/S ratio can be expressed as

$$\text{J/S} = \frac{\text{Jammer signal power at the BS}}{\text{UE signal power at the BS}}.$$

J/S expressed in decibels can be calculated by

$$\text{J/S}_{[\text{dB}]} = (\text{EIRP}_{\text{Jammer}} - \text{L}_{\text{Jammer}}) - (\text{TRP}_{\text{UE}} - \text{L}_{\text{UE}})$$

where $\text{EIRP}_{\text{Jammer}}$ is the EIRP of the jammer, L_{Jammer} is the path loss of the jamming signal, TRP_{UE} is the transmit power of the UE, and L_{UE} is the path loss of the 5G uplink signal. The values for $\text{EIRP}_{\text{Jammer}}$ were given in Section 4.4.3. The TRP_{UE} was 23 dBm defined for Power Class 3, as described in Section 2.3.5.1. The path loss for every measurement and jammer position was given in Section 4.5.1.

The higher the J/S value, the higher the impact of the jamming on the uplink channel. Higher power of the jamming signal and lower path loss between the jammer and the BS lead to an increased J/S ratio. Higher power from the UE and lower path loss between the UE and the BS lead to a decreased J/S ratio, lowering the impact of the jamming.

5 Results

This section presents the data analysis results of the reference measurements, uplink jamming measurements and downlink jamming measurements. An example of the 5G system's behaviour in the contested radio environment is given. Also, modelling of a successful jamming attack and jammer range is introduced.

5.1 Reference performance

The performance of the 5G communication was first measured without interference. These measurements were a reference point for comparison with the performance of the disrupted communication link. Figure 5.1 shows the reference 5G performance in terms of uplink and downlink throughput and service quality measured at all nine measurement positions. More detailed reference performance characteristics are given in Table 5.1 as the table additionally includes the path loss, the MCS Index and the MIMO Rank obtained at every measurement position.

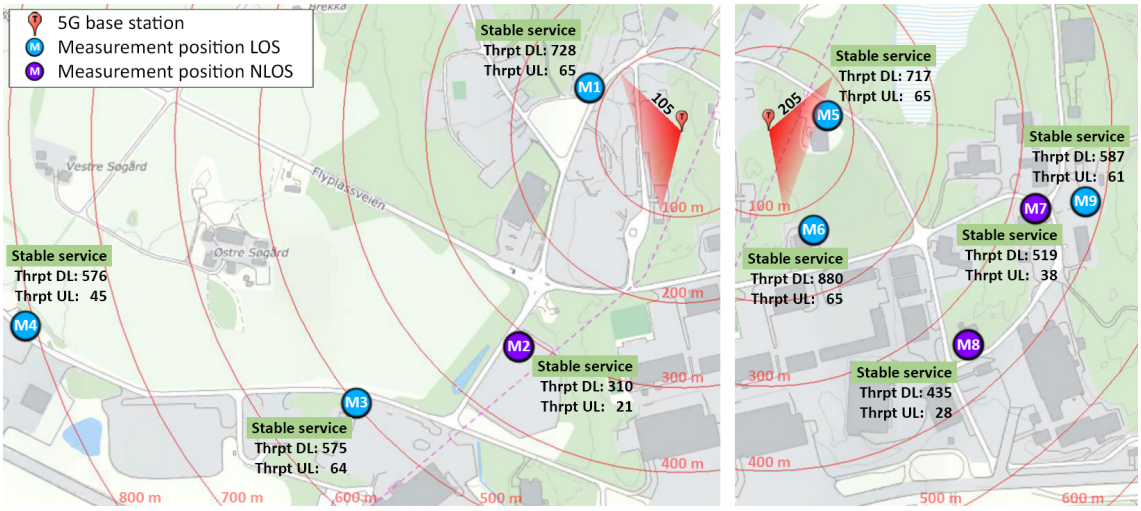


Figure 5.1 Reference downlink (DL) and uplink (UL) throughput (thrpt) and service quality at every measurement position.

The 5G cell provided coverage up to 2 km in LOS. The services at the edge of the cell were unstable, so the measurement positions were picked to be within a few hundred meters from the BS. Inside 500 meter radius and in LOS, the uplink throughput performance was the highest, providing 61–65 Mbps. At the 800 meter LOS range, the uplink throughput went down to 45 Mbps. In complete NLOS, the uplink throughput went down to 21–28 Mbps.

Meas. position	Path loss [dB]	Throughput DL [Mbps]	Throughput UL [Mbps]	MCS Index DL	MCS Index UL	MIMO Rank	Service quality
M1	85	728	65	26	28	4.0	Stable
M2	116	310	21	18	15	3.0	Stable
M3	99	575	64	26	28	3.0	Stable
M4	104	576	45	23	24	4.0	Stable
M5	82	717	65	25	28	4.0	Stable
M6	86	880	65	27	28	4.0	Stable
M7	106	519	38	24	22	3.1	Stable
M8	118	435	28	22	19	3.0	Stable
M9	97	587	61	27	28	3.0	Stable

Table 5.1 Reference measurements of the 5G performance characteristics at every measurement position.

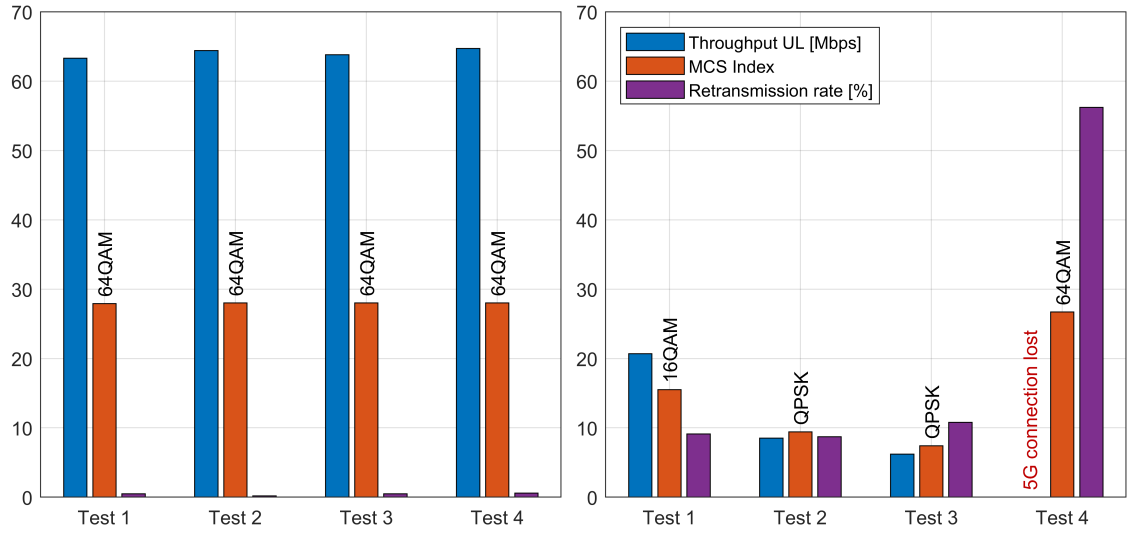
5.2 An example of the 5G system's response to jamming

As described in Section 4.6.2, the 5G radio system dynamically adjusts the physical layer parameters according to the radio channel quality to adapt to the radio environment and efficiently transmit data. As the channel was disrupted, the 5G system lowered the MCS to minimize the errors in signal decoding and demodulation. However, the 5G system often struggled to find the optimum settings for the physical layer parameters, which led to a high number of retransmissions and the 5G connection being terminated and downgraded to 4G.

This section provides a typical example of the 5G system's reaction to the jamming experienced during the experiment. Figure 5.2 shows the results of four consecutive speed tests conducted at measurement position M5 without jamming (Figure 5.2a) and during uplink jamming of 43 dBm (Figure 5.2b). The 5G performance in the uplink is given in terms of throughput, MCS index, and retransmission rate.

Without jamming, as shown in Figure 5.2a, the uplink throughput during the speed tests was stable and reached 65 Mbps, the maximum total capacity in the uplink. The MCS index was always at maximum, meaning that the 64QAM modulation scheme was used. The retransmission rate stayed below 1%.

During jamming, as shown in Figure 5.2b, the throughput in the uplink was reduced and became highly varying from test to test until, at the start of the fourth speed test, the 5G connection was lost and went down to 4G. During Tests 1–3, the 5G system adapted to the contested radio channel by lowering the modulation order. A decent throughput with an acceptable level of retransmissions was achieved. During Test 4, the data transmission started on 64QAM, the averaged retransmission rate went up to 56%, and the connection was lost. Many errors in data transmission suggest that the modulation order of 64QAM was too high in this contested RF environment, which led to the connection being terminated. Selecting the 64QAM modulation scheme on this disrupted radio channel was not a sufficient response from the 5G system. On the contrary, the 5G system's performance during Test 1 may be considered an optimal adaptation to the jamming since, compared with the results from the rest of the speed tests, the throughput during Test 1 was the highest.



(a) Reference measurements without jamming.

(b) Measurements with uplink jamming of 43 dBm with the jammer in position J2.

Figure 5.2 The 5G system's performance and reaction to jamming at measurement position M5.

Even though the 21 Mbps throughput was reached on the disrupted channel during Test 1, the overall 5G service quality at measurement position M5 during the uplink jamming of 43 dBm was classified as unreliable since the 5G connection was unstable and, finally, lost during the measurements.

5.3 Uplink jamming

The uplink jamming impact on the 5G throughput, service quality, modulation scheme and retransmission rate is analysed in this section. The 5G performance is also analysed with respect to the J/S ratio.

5.3.1 Throughput, service quality and modulation

Figure 5.3 illustrates the 5G performance under the influence of different uplink jamming signal power levels. The 5G performance is given in terms of throughput and service quality as described in Section 4.6.3. The results were plotted on a map to provide a complete picture of the

- geographical area and terrain
- location of the BS and the measurement and jammer positions
- UE angle, distance and LOS/NLOS propagation condition towards the BS and jammer
- direction of the jammer and the cell sectors

More detailed performance characteristics, including MCS Index and MIMO Rank for every measurement position, are given in Appendix D.

(a) Jamming signal EIRP of 33 dBm.

(b) Jamming signal EIRP of 43 dBm.

(c) Jamming signal EIRP of 53 dBm.

Figure 5.3 5G performance in terms of throughput and service quality under the influence of three different uplink jamming signal power levels.

The results show that the increased jamming power reduced 5G performance both in throughput and service quality. The radio communication struggled to surpass the jamming signal when the UE was in NLOS with the BS or further away from the BS.

Because of the contested RF environment, the 5G communication was forced to use lower modulation schemes to reduce the errors in the modulation symbol detection. Lower modulation schemes led to fewer bits per symbol transmitted, thus lower throughput. Figure 5.4 shows the correlation between the throughput and MCS Index (presented in Section 4.6.1) measured both with no jamming and with uplink jamming.

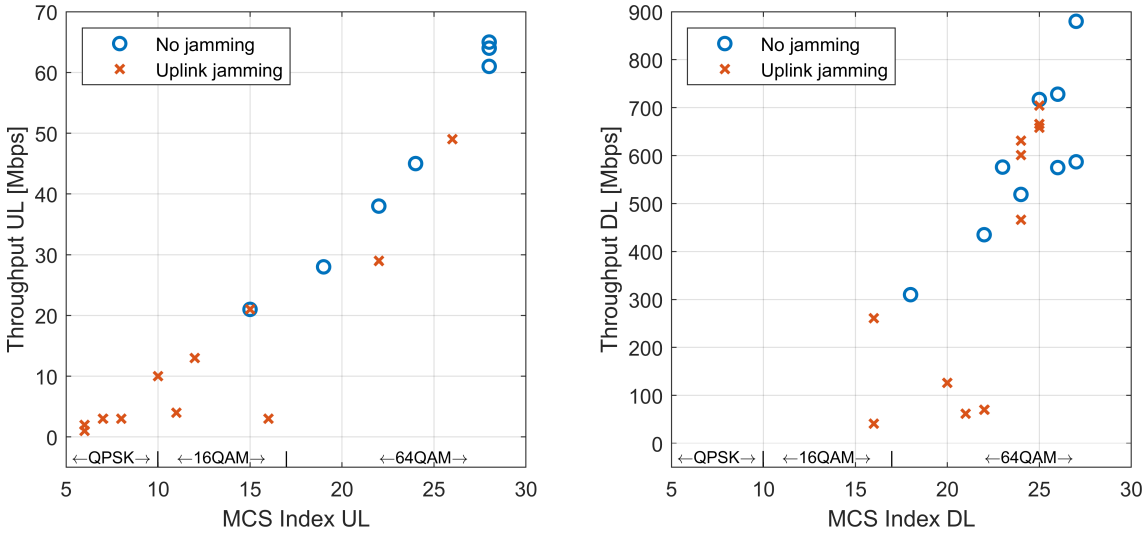


Figure 5.4 Correlation between 5G throughput and modulation scheme, without and with uplink jamming (all jamming signal power levels).

The uplink modulation scheme went down from 64QAM to 16QAM or QPSK in most cases during uplink jamming. Accordingly, the downgrade in modulation led to a reduced throughput.

The downlink modulation scheme in most cases stayed on 64QAM, yet sometimes it went down to 16QAM, but never to QPSK. Even though the downlink modulation order was relatively high during the uplink jamming, the downlink throughput was still significantly reduced in some cases. Since the uplink (not downlink) jamming was applied, the impact on the downlink radio signal quality was minimal, so the downlink modulation was not reduced to a minimum. The reduced downlink throughput can then be explained by disrupted uplink data transmission since the uplink and downlink transmissions depend on each other.

5.3.2 Retransmission rate

The retransmission rate metric was presented in Section 4.6.4. Figure 5.5 shows the distribution of retransmission rate of all of the samples logged at measurement position M1 during the different jamming set-ups. The retransmission rate is given separately for QPSK, 16QAM and 64QAM. The distribution is given in box plots that are explained in Appendix E.

Without jamming applied, the UE transmitted data with 64QAM. The retransmission rate was, on average, below 2%, and the throughput reached 65 Mbps, which is the maximum total capacity

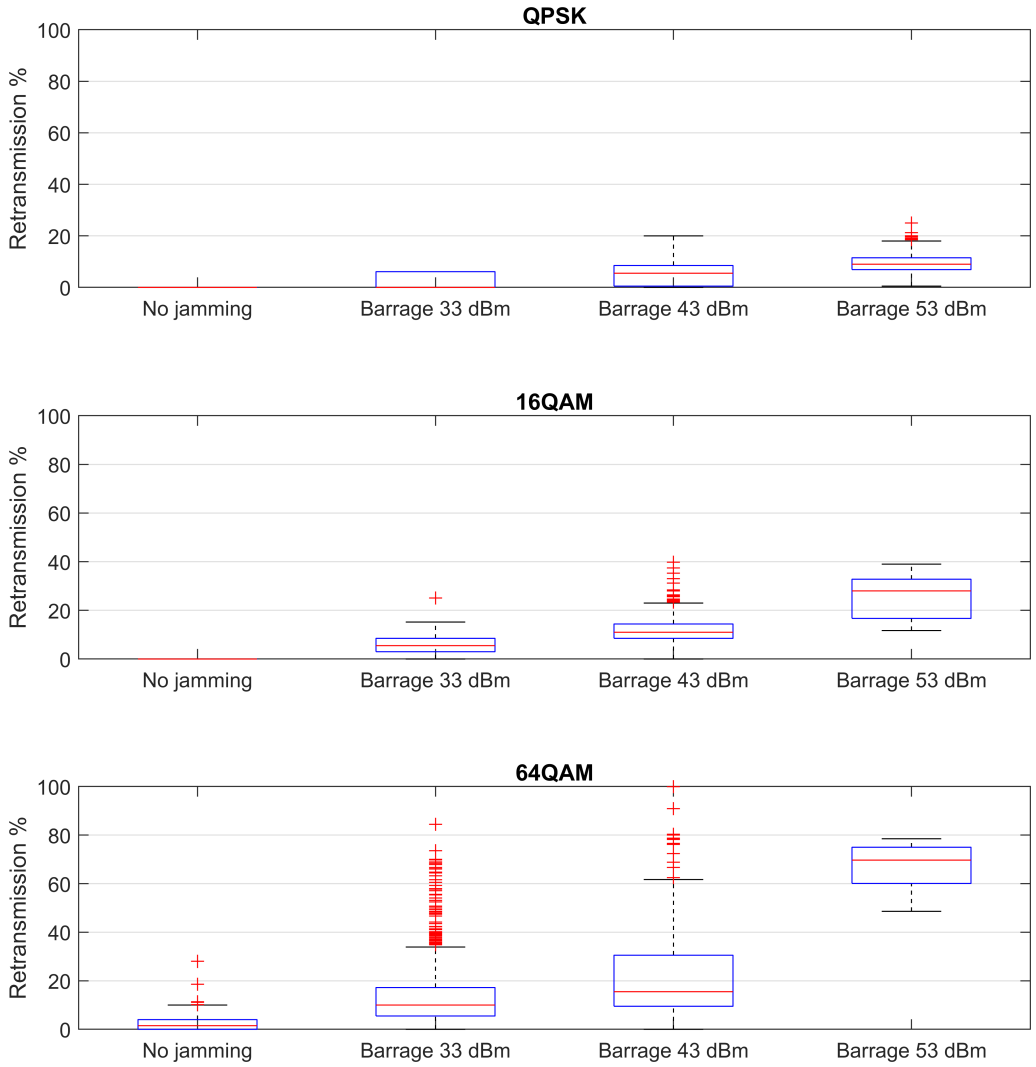


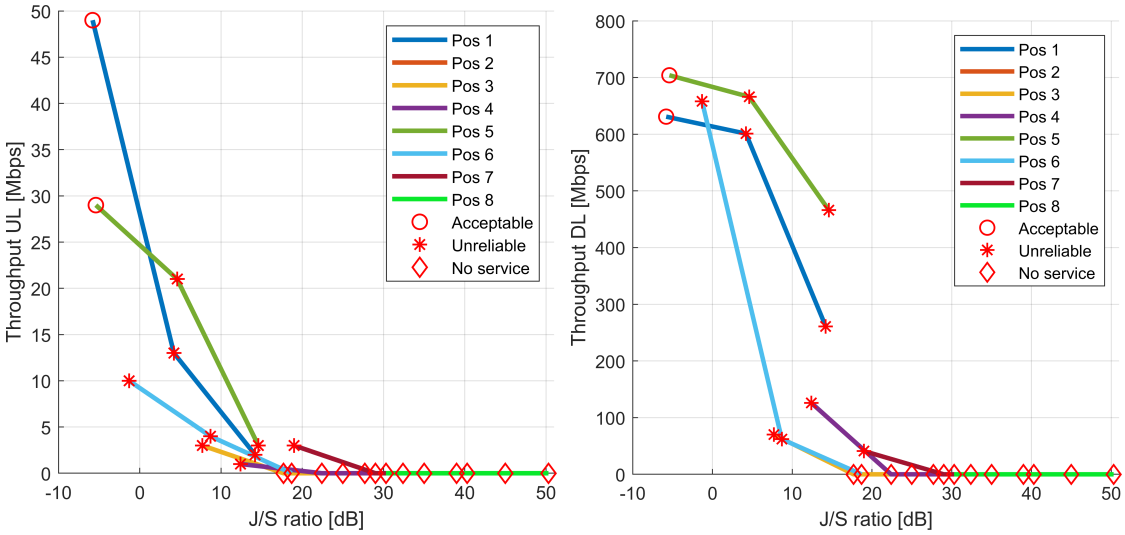
Figure 5.5 Retransmission rate distribution obtained at measurement position M1 during uplink jamming.

in the uplink. The highest number of retransmissions occurred during jamming with the highest power, while the UE attempted to transmit on the highest modulation order. During the 53 dBm barrage jamming, the UE transmitted mostly with QPSK since higher modulation schemes led to a high retransmission rate. The service was unreliable, and the throughput in uplink was not higher than 2 Mbps. Lower jamming power, on average, led to fewer retransmissions for all types of modulation schemes. In the case of jamming EIRP of 43 dBm, the UE transmitted mainly with 16QAM, and the service was unreliable with a maximum of 13 Mbps of uplink throughput. The lowest jamming power reduced the uplink throughput to 49 Mbps with acceptable service quality. The UE transmitted mostly with 64QAM.

It was also observed that a high percentage of retransmissions affected the 5G system's decision of dropping the 5G connection. In cases where the 5G connection was lost, the retransmission rate was often above 80%.

5.3.3 J/S ratio

The J/S ratio metric was presented in Section 4.6.5. The relation between the J/S ratio and the 5G throughput gave a clear picture of the jamming effect on the 5G radio communication. The plots in 5.6 show how the throughput in uplink and downlink decreased with the increasing J/S ratio. The plots contain throughput results from all eight measurement positions (M1–M8) with all three jamming signal power levels. Every measurement also includes information about the service quality.



(a) Uplink throughput versus J/S ratio. *(b) Downlink throughput versus J/S ratio.*

Figure 5.6 Uplink jamming impact on the uplink and downlink throughput. The J/S ratio is given for the uplink jamming signal and the uplink UE signal.

Even though the uplink jamming was applied, the throughput in the downlink was also reduced. Since the uplink and downlink signals were transmitted on the same frequency (TDD), the jamming signal also disrupted the radio signal in the downlink to some extent. Also, the downlink and uplink transmissions depend on each other, so the disrupted communication in the uplink impacted the downlink performance.

However, since the plotted measurements were taken during the uplink jamming, this section focuses on the uplink performance. We can see that when the J/S ratio was less than -5 dB (meaning that the uplink signal was 5 dB stronger than the jamming signal at the BS), the 5G performance was at an acceptable level of stability and data throughput. When the J/S ratio was between -5 and 5 dB, the service quality provided by 5G dropped significantly but still managed to achieve 10–20 Mbps of uplink throughput. Above the 5 dB J/S ratio (meaning that the jamming signal was 5 dB stronger than the uplink signal at the BS), the 5G service was either very poor or unavailable.

5.4 Downlink jamming

This section analyses the downlink jamming impact on the 5G throughput, service quality, modulation scheme, block error rate (BLER) and radio signal quality parameters.

5.4.1 Throughput, service quality and modulation

Figure 5.7 shows how the 5G performance was influenced by the different downlink jamming types and signal power levels. The 5G performance is given in terms of throughput and service quality (colour), described in Section 4.6.3, and modulation and coding scheme index, described in 4.6.1.

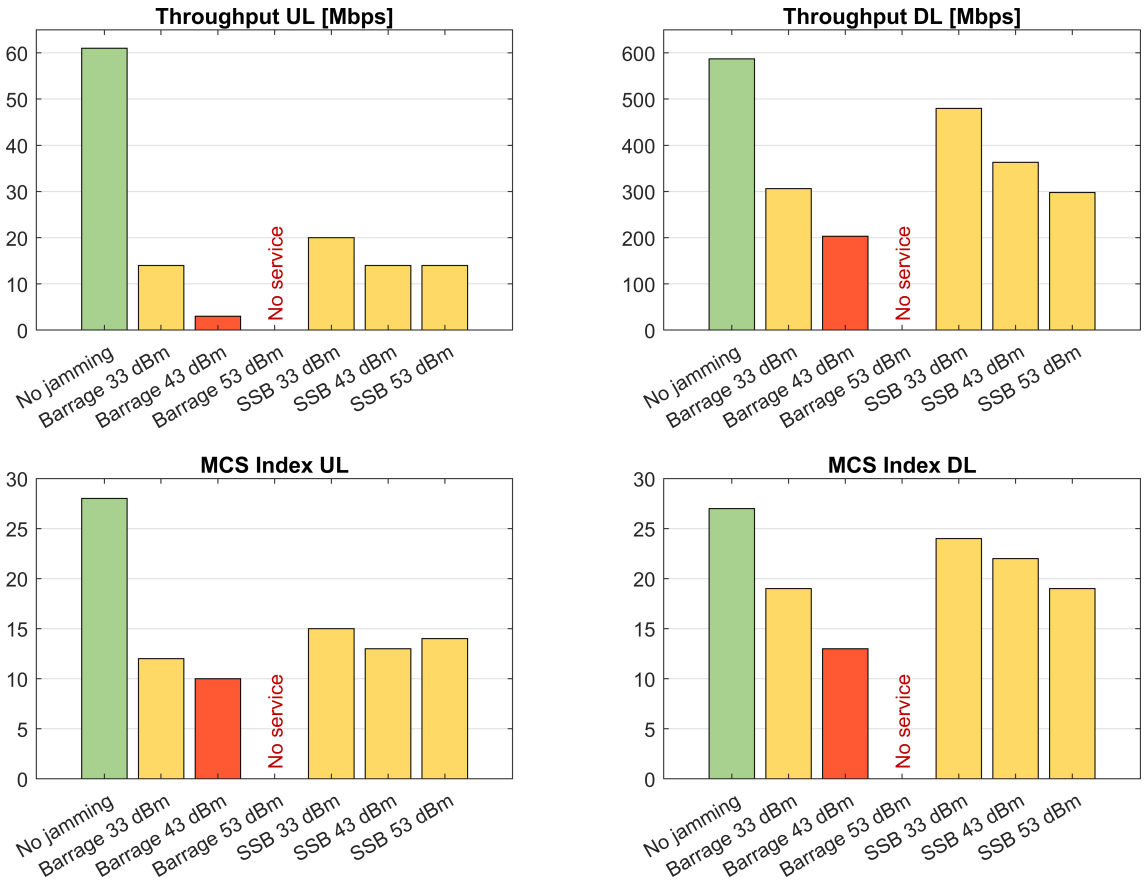


Figure 5.7 Throughput and MCS performance at measurement position M9. The service quality is given by the colour specified in Table 4.6.

Barrage jamming with high power was the most effective in disrupting the 5G communication as no service could be delivered when the jamming of 53 dBm EIRP was applied. Even though this set-up was focused on jamming the downlink channel, the 5G performance in the uplink was also significantly affected. The reduced uplink performance suggests that either the communication in uplink was strongly dependent on the downlink performance or that a significant amount of interference still reached the BS even though the jammer was in NLOS with the BS or both.

The 5G transmission would break down if the UE's synchronisation with the BS were lost. In the case of the SSB jamming, the jamming power was concentrated on the synchronisation signals. However, this type of jamming signal was not enough to completely disrupt the synchronisation and break the 5G connection. The 5G system operated with reduced throughput and acceptable quality of service during the SSB jamming.

5.4.2 Block error rate

The block error rate (BLER) metric was presented in Section 4.6.4. Figure 5.8 shows the distribution of BLER of all of the samples logged at measurement position M9 during the downlink barrage jamming. The BLER is given separately for QPSK, 16QAM and 64QAM. The distribution is given in box plots that are explained in Appendix E. The BLER is not presented for the SSB jamming because this type of jamming had a minimal impact on the total BLER.

The 5G connection exposed to the 53 dBm barrage jamming was too poor to transfer any considerable amount of data. There were short attempts to transmit downlink data with 16QAM and 64QAM, resulting in BLER as high as 30–40% and 50–60%, respectively. Because of the high error rate, the modulation order stayed mostly on QPSK when the highest jamming power was applied. During the barrage jamming of 43 dBm, no attempt to transmit data with 64QAM was registered, whereas the unreliable service quality was delivered using QPSK and 16QAM. The BLER noticeably increased compared with the uninterrupted channel performance. With the 33 dBm barrage jamming, the service quality was acceptable, all modulation orders were available, and the jamming impact on the BLER was minimal.

The 5G system's response to the barrage jamming of 43 dBm was not to transmit with 64QAM, the highest modulation scheme supported. This adaptation to the contested RF environment was sufficient as the 5G service could still be delivered only with reduced throughput and stability.

5.4.3 Radio signal quality

The UE performs mobility measurements to determine the downlink radio channel quality. When it comes to jamming, SS-SINR (synchronisation signal signal-to-noise and interference ratio) is a radio signal quality parameter of interest for two reasons. Firstly, the SS-SINR is a ratio between the power contributions from the wanted signal and the noise and interference, taking into account both the 5G signal received power and the jamming signal received power. Secondly, a 5G radio system measures the SS-SINR on the synchronisation signal block (SSB), which the partial-band downlink jamming (SSB jamming) aimed to disrupt. Mobility measurement parameters, including SS-SINR, were introduced in Section 2.4.2.

As explained in Section 4.2, in addition to the smartphone, the SS-SINR was also measured and stored with the spectrum analyser. Figure 5.9 shows the SS-SINR at measurement position M9. The distribution of the SS-SINR is given in box plots. SS-SINR was measured on SSB beam #2, the strongest beam at M9.

High jamming signal power and jamming signal concentrated to target SSB led to decreased SS-SINR. The SSB jamming with the highest (53 dBm) EIRP reduced the SS-SINR, on average,

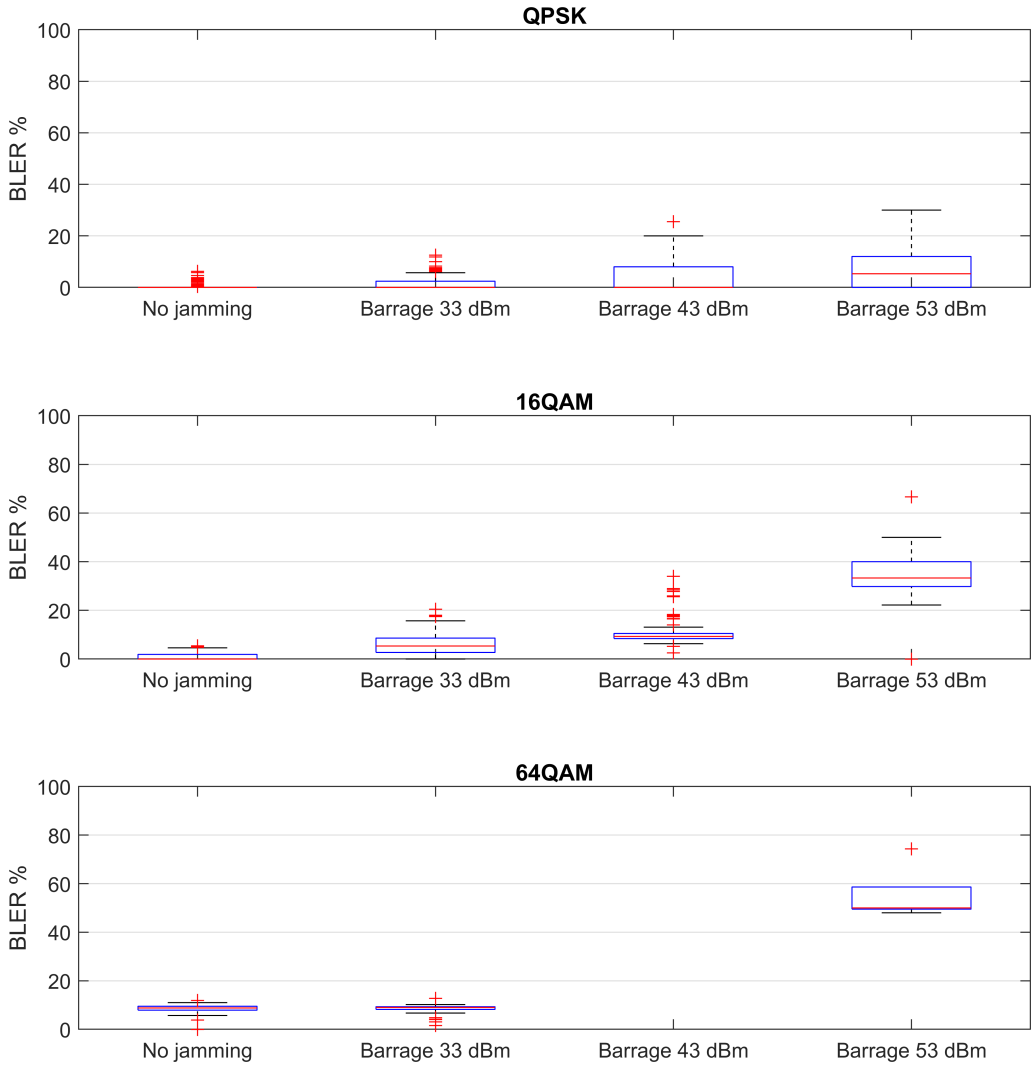


Figure 5.8 Block error rate (BLER) distribution obtained at measurement position M9 during the downlink barrage jamming.

by 20 dB on the smartphone and by 38 dB on the spectrum analyser compared with the SS-SINR measured without jamming. Even when the average SS-SINR on the smartphone was as low as 5 dB at 53 dBm SSB jamming, the service quality was still acceptable, and the communication was not breaking down. The difference between the SS-SINR measurements taken with the smartphone and spectrum analyser can be explained by differences in receiving antennas, leading to different receiver sensitivity.

Also, the variation of the SS-SINR increased when the jamming was applied. The high variation could be explained by the sweeping nature of the jamming signal. The measured value of the SS-SINR might depend on how, where, and when the sweeping sinusoidal jamming signal collided with the reference signal from which the SS-SINR was calculated.

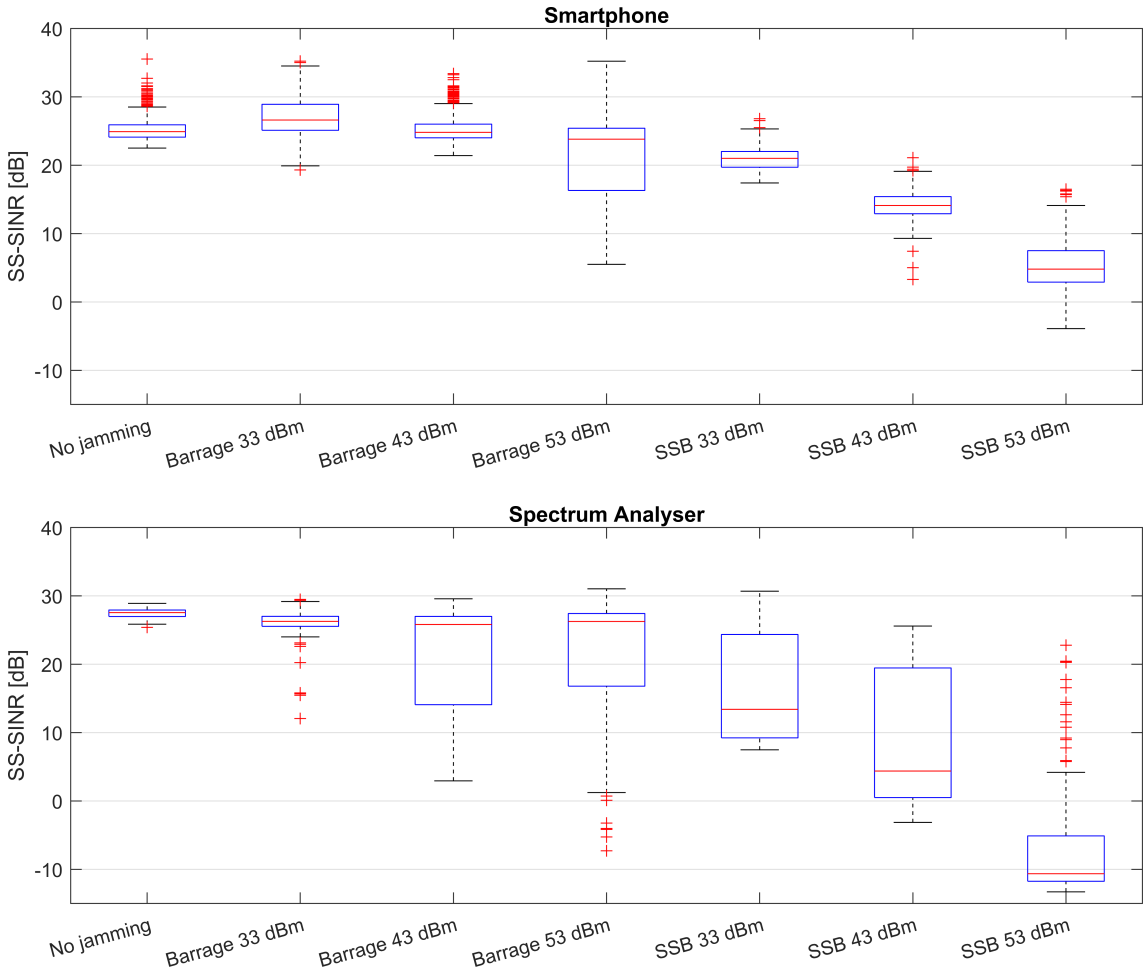


Figure 5.9 SS-SINR measured on the smartphone and the spectrum analyser at measurement postion M9 during the downlink jamming.

5.5 Jammer power and range modelling

Based on the experiment results, this section determines the jamming power needed for a successful jamming attack on 5G NR. Further, a model is developed, which translates the threshold of a successful jamming attack into the expected jammer range.

5.5.1 Breaking point

By inspecting the jamming-to-uplink-signal (J/S) ratio, we can identify a successful jamming attack in terms of the power needed to completely disrupt the 5G service. In Section 5.3.3 we presented the results of the 5G uplink performance versus the J/S ratio measured in various locations during different jamming power set-ups. In Figure 5.10, those results are plotted with a logistic curve fit function. In addition, the figure includes a threshold line that separates a jammed radio channel that could not provide any service from a radio channel that managed to provide services to some extent.

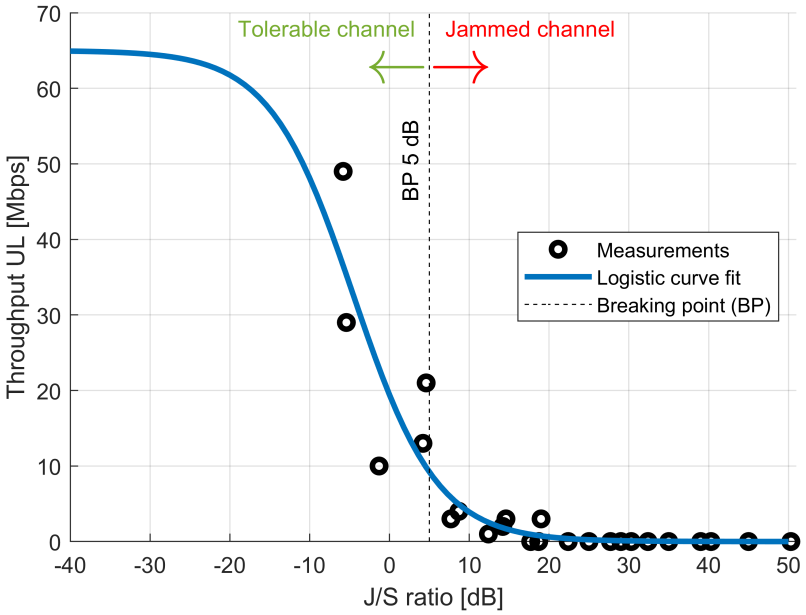


Figure 5.10 The results of the jamming-to-uplink-signal (J/S) ratio presented in Section 5.3.3 with an added logistic curve fit function and identified breaking point (BP).

A logistic curve fit function was applied to the measurements to provide a model for the drop in throughput caused by jamming. The applied logistic curve fit function is expressed as

$$y = \frac{65}{1 + 2.344 \exp[0.1899x]}$$

where the variable y represents the uplink throughput in Mbps, while x corresponds to the J/S ratio in dB. The value of 65 is a constant and represents the maximum uplink throughput obtained during the reference measurements. The values computed with a curve fitting tool were $a = 2.344$ and $b = 0.1899$.

In this report, we call the value of the J/S ratio, at which a jamming signal was too destructive for a 5G system to work, a breaking point (BP). The BP is a threshold separating a tolerable channel from a jammed channel. The BP tells how much stronger the jamming signal received power compared with the uplink signal received power to achieve a successful jamming attack.

Our results show that, with the J/S ratio higher than 5 dB, the 5G performance was too poor to deliver any service. Therefore, we identified the BP to be 5 dB, which means that if the jamming signal that reached the BS was at least 5 dB stronger than the uplink signal at the BS, the jamming attack was successful.

5.5.2 Jammer range

Jammer range is the longest distance between the jammer and the jammer's target, which results in a successful jamming attack. When it comes to 5G radio communication, the jammer range depends on various factors like

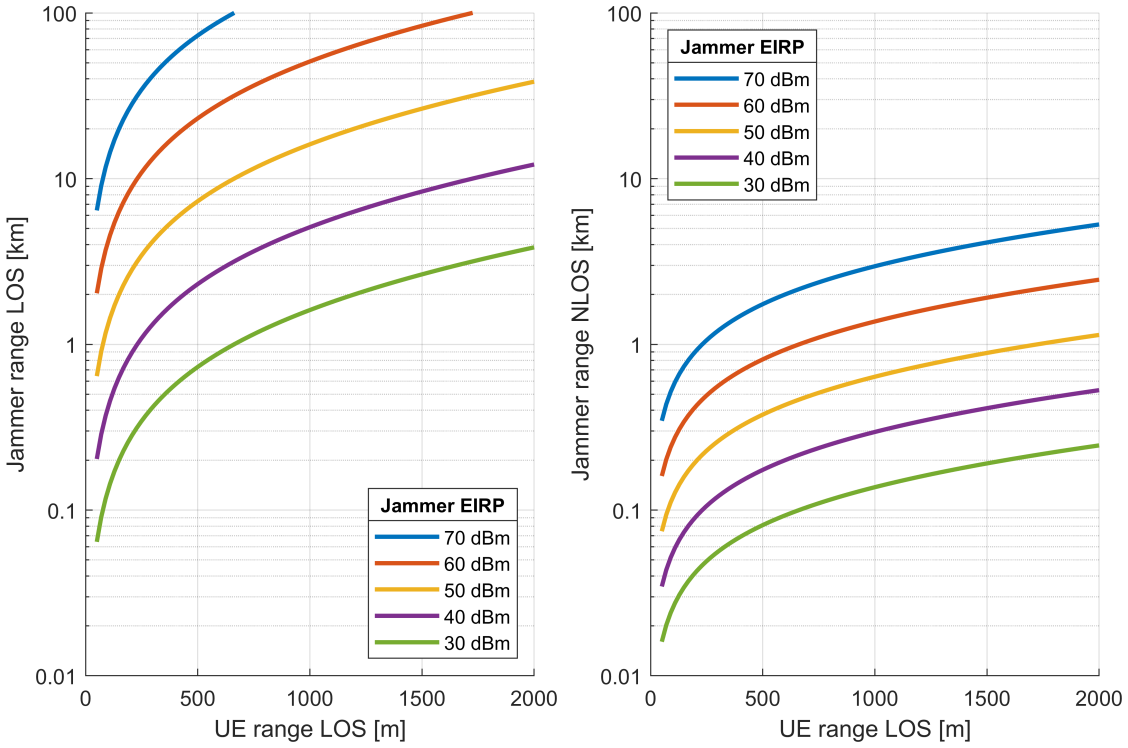
- frequency range
- targeted system's sensitivity, output power and directivity
- targeted system's antenna height and direction of the sector
- distance beween the UEs and the BS
- surroundings, terrain, LOS/NLOS propagation conditions
- jamming waveform (barrage or smart jamming)
- jammer's output power and directivity
- uplink/downlink jamming

We modelled the expected jammer range between a jammer and a BS based on the J/S ratio obtained from the measurements during the uplink jamming. The model provides the jammer range based on a given jamming signal power, UE output power, breaking point (BP) of the J/S ratio, the distance between the UE and BS and LOS/NLOS condition between the jammer and BS. The signal power that arrives at the BS depends on the transmit power and path loss. The path loss expressions contain the distance between the transmitter and receiver. By inserting the transmit powers, path losses and 5 dB BP into the J/S ratio expression, the distance between a jammer and a BS can be derived. The derivation of the expression for the jammer range is given in Appendix F.

Figure 5.11 shows the plots of the modelled jammer range for a given distance between the UE and BS, jamming signal power and LOS/NLOS propagation condition of the jamming signal. The transmit power of the jammer is given in EIRP, which specifies the radiated power in the strongest direction measured in dBm. 30 dBm of EIRP is equivalent to 1 watt and represents a small size jamming equipment. 70 dBm of EIRP is equivalent to 10000 watts and represents heavy jamming equipment, possibly armed with highly directive antennas. The jammer range was modelled with the UE output power of 23 dBm and the J/S ratio of 5 dB (the breaking point (BP)). The model was calculated for the UE being in LOS with the BS as it is expected that LOS would be available within a relatively short cell radius.

Figure 5.11a can, for instance, be interpreted as follows. A jammer, which has 30 dBm output power directed towards the BS and is in LOS with the BS, has to be within 700 meters to the BS to knock out the 5G radio communication of a user terminal that is 500 meters away from and in LOS with the BS.

Figure 5.11b can, for instance, be interpreted as follows. A jammer, which has 60 dBm output power directed towards the BS and is in NLOS with the BS, has to be within 800 meters to the BS to knock out the 5G radio communication of a user terminal that is 500 meters away from and in LOS with the BS.



(a) Jammer in LOS with the BS. *(b) Jammer in NLOS with the BS.*

Figure 5.11 Modelled jammer range depending on jamming signal power, distance between the UE and BS (UE range) and LOS/NLOS propagation condition between the jammer and BS.

6 Discussion

This section discusses differences in response to jamming between a 5G radio operating on NSA and SA, identifies the weaknesses of the 5G radio system regarding resilience to jamming, and interprets the modelled jammer range. We also suggest some theoretical and practical measures worth studying and considering to mitigate the effect jamming has on 5G NR.

6.1 Resilience to jamming in NSA and SA

Non-Stand Alone (NSA) and Stand Alone (SA) architectures were described in Section 2.4.3. In NSA, some part of the higher layer signalling goes through a 4G radio channel instead of a 5G radio channel. If interference is present on the 5G frequency channel, the signalling on the 4G frequency channel would not be interrupted. The signalling includes messages needed for radio connection establishment. In the case of jamming a SA system, the radio connection establishment procedure would be more disrupted than in NSA as all the connection establishment instructions would go through the jammed 5G radio channel in SA. However, as described in Section 3.3, the 5G physical layer is controlled by the 5G BS both in NSA and SA, so, from the radio perspective, the data transmission on the 5G radio channel is identical whether it is NSA or SA.

Therefore, we consider the difference between the jamming impact on data transmission on 5G NR in NSA and the jamming impact on data transmission on 5G NR in SA to be minimal. Our measurements were conducted on the 5G system operating in NSA, but since the 5G resilience to jamming is expected to be similar in NSA and SA, the analysis results are also assumed to be valid for a 5G system operating in SA.

As described in section 5.5.1, the disrupted 5G radio channel that could not provide any service was characterised as a jammed radio channel. The experiment results showed that a 5G system operating in NSA responds to a jammed 5G channel by shifting the communication to an undisrupted 4G (anchor) channel. In the case of a jammed 5G channel of a 5G radio system operating in SA, the UE would first try to search for any other available and undisrupted radio channel. If no other cells were available, the UE would be forced to operate on the jammed 5G channel of poor quality or terminate the connection and go into "no service" mode.

6.2 Vulnerable uplink

In time-division duplexing (TDD), where the uplink and downlink are transmitted on the same frequency band, the barrage jamming will affect both the uplink and downlink channels. Nevertheless, the jammer is more likely to direct its attack towards the BS, knowing that it can affect the uplink channels of all users in the cell, while the downlink jamming disrupts only the users that are in the jammer's range. Also, the attacker is aware that the uplink signal power is minimal compared to the downlink signal and thus easier to contest.

The experiment results also imply that the uplink was more sensitive to jamming than the downlink. The vulnerability of the uplink was particularly observed in the downlink jamming scenario, where the jamming power was focused on jamming the downlink communication, but the uplink channel was still strongly disrupted. Since the uplink channel is easier and more effective to disrupt than the downlink channel, and since the performance in uplink decides the system's overall performance, we consider the uplink channel as a weak spot of the 5G radio communication.

In Section 5.5.1, we determined the power needed for a successful jamming attack on the uplink channel based on the results of the experiment. The jamming power was expressed relative to the power of the uplink signal using the J/S ratio. We presented a breaking point (BP) of the J/S ratio, which is a threshold that separates a tolerable channel from a jammed channel. The BP was identified to be 5 dB, which means that if the jamming signal that reaches the BS was stronger than the uplink signal at the BS by 5 dB or more, the jamming attack was successful.

Different studies can have different definitions for a jammed channel and thus different selections of the BP threshold, which further defines the jammer power needed to disrupt the targeted radio communication. However, in general, the reduction in throughput as the J/S ratio increased and the BP of 5 dB observed in the experiment results are in agreement with the vulnerability studies found in the literature. According to the logistic curve fit model in Figure 5.10, for a J/S ratio of 0 dB and 5 dB, the throughout was reduced to 30% and 14% of the maximum capacity, respectively. The authors in [33] suggest that the BP for a successful jamming attack on 5G NR physical data channels would be 0 dB. The authors in [22] suggest that the achievable data rate of a regular massive MIMO system would be reduced to 40% and 12% of the maximum capacity at a J/S ratio of 0 dB and 5 dB, respectively.

The authors in [34] suggest that a 0 dB BP is also valid for the physical data channels in 4G LTE, meaning that there is no significant difference between 4G LTE and 5G NR when it comes to jamming resilience. Our experiment confirmed this fact, at least for the uplink transmissions. The 5G uplink signal did not show any more resilience to jamming than what would be expected from the 4G uplink signal. Both technologies are based on the OFDM waveform, and, as with 5G NR, the standard UE output power in 4G LTE is also limited to 23 dBm. The massive MIMO technology and beamforming might boost the 5G radio signal in the downlink. However, when it comes to the uplink, the BS antenna showed no additional resilience to jamming in the signal reception.

The fact that the uplink signal is relatively low in power and that the jamming power needs to be equal to or just a few decibels higher than the uplink signal to achieve a successful jamming attack makes the 5G radio communication vulnerable to jamming.

6.3 Jammer range

The model for the jammer range, the longest distance between the jammer and the jammer's target, which results in a successful jamming attack, was introduced in Section 5.5.2. The model suggests that the jammer's operational radius increases with higher jamming power and lower received 5G signal in the uplink. However, an increased UE power, a higher breaking point (BP) of the J/S ratio, and higher jamming signal path loss decrease the operational range of the jammer.

Even though in the derivation of the jammer range model (Appendix F), the carrier frequency of the communication system and jammer cancelled out, the carrier frequency can influence the jammer

range. 5G NR can operate on relatively high-frequency bands in, for example, 3.6 GHz, 4.8 GHz or 26 GHz frequency range. Higher frequency leads to higher path loss. Higher path loss leads to a shorter operational cell radius. So, according to the jammer range model, a shorter distance between a UE and BS also requires a jammer to be closer to the BS.

Whether the jammer has LOS towards its target or not has a significant impact on the jammer range. However, it is not realistic to believe that the jammer will not have LOS when it is in the vicinity of a BS. Likewise, it is not realistic to believe that a large ground-based jammer will have LOS to a BS at distances greater than a few tens of kilometres because of the horizon or, in some cases, hilly terrain.

Smart jamming techniques might increase the jammer range. A smart jammer can exploit the knowledge about 5G NR and attack the vital spots of radio communication, increasing jamming efficiency. The increased jamming efficiency would lead to a lower BP of the J/S ratio. Also, a smart jammer might operate without exposing itself on the frequency spectrum, making the jammer harder to detect and eliminate even in the vicinity of the cell.

6.4 Jamming mitigation measures

The potential threat of being jammed while using commercial mobile technology is evident. However, there will always be measures to mitigate the threat as much as practically possible. Such measures can reduce the jammer range, force the jammer to be more exposed, lower the probability of the 5G communication being detected and intercepted, and enhance the service quality in a contested RF environment. As an output of the experience gained during the jamming experiment, we propose four jamming mitigation measures that are worth consideration and should be researched in more detail:

- Boosted uplink output power for user equipment (UE)
- Improved utilisation of a massive MIMO system to detect and suppress the uplink interference
- Optimised 5G physical layer to operate in highly challenging radio environments
- Supplementary frequency bands

6.4.1 Boosted uplink output power for user equipment (UE)

The uplink transmission is much weaker in power than the downlink transmission, where BS provides transmit powers in hundreds of watts supplemented with directive beams. In contrast, today's commercial UEs transmit uplink data through omnidirectional antennas with a total radiated power of less than one watt. It is difficult for a communication system with low output power to compete with a jammer transmitting a strong interfering signal. More resilience to uplink jamming can be achieved by boosting the transmit power of a UE, either by using external antennas, implementing beamforming to some extent, or revising the standards to allow higher uplink power in exceptional use cases. Increased uplink power would be beneficial only if it is not causing any additional issues like increased inter-user or inter-cell interference. Increased radiated energy in the uplink must also comply with safety guidelines and requirements set by governmental institutions.

As higher and higher frequencies are enabled in mobile communications, and the radio signal attenuation is growing, the high-power uplink transmission gets more and more attention from the 3GPP. The 5G NR standards take into account the directive gain of a UE that operates in the mmWave frequency bands. That is new compared to the frequency bands below 6 GHz, where total radiated power is limited without any options for additional antenna gain. However, more and more bands in the frequency range 2–5 GHz are allowed to use the uplink output power of 26 or 29 dBm, which is an increase compared to the default value of 23 dBm. For comparison, a handheld UE operating above 24 GHz can achieve up to 43 dBm of EIRP. A fixed wireless access terminal can support up to 55 dBm of EIRP. All specifications of the uplink output power were presented in Section 2.3.5.1.

6.4.2 Improved utilisation of a massive MIMO system to detect and suppress the uplink interference

An important difference between 4G and 5G is that 5G NR utilises massive MIMO technology. By definition, a massive MIMO antenna can spatially separate multiple users because they have different radio channel properties [47]. A BS equipped with this type of antenna can then estimate and separate the different radio channels, thus, separating the users, which allows the simultaneous reception of radio signals from multiple users. Naturally, a question arises whether a massive MIMO antenna can distinguish a jamming signal's radio channel and, consequently, suppress the interference. The authors in [22] and [31] show that potentially, if the base station can accurately estimate the jamming signal and its radio channel, then a massive MIMO system can use this estimate to suppress the jamming signal significantly, making the system resilient to interference.

However, the results from our experiment showed that a regular commercial massive MIMO antenna had no advantage against the uplink jamming signal. The BS had no functionality to estimate and suppress the uplink jamming signal. The jamming suppression would require some resource elements dedicated to the jamming channel estimation and digital signal processing techniques to filter out the interference. The analysis in [19] and [22] show that, ideally, it is possible to obtain a massive MIMO system that is completely resilient to the jamming signal independently of the jamming power. Aspects of implementing such techniques are worth further investigation.

Even without the jamming suppression, the ability to detect the presence and the direction of a jamming signal would be a valuable measure against jamming. A massive MIMO antenna could be set up to use some time-frequency resources to estimate the direction of the jamming signal. This information could assist in identifying and neutralising the threat.

6.4.3 Optimised 5G physical layer to operate in highly challenging radio environments

A 5G radio system is designed to dynamically adjust the physical layer parameters for optimal operation in various radio channel conditions. The system's ability to automatically adapt to a poor radio channel is advantageous against interference. However, when the radio environment was highly contested in the experiment, the 5G radio system struggled to find the optimal parameters for communication on 5G and often shifted to 4G to avoid a bad user experience. Some military applications such as friendly (blue) force tracking and messaging services might work even if the

radio link is unstable and the throughput is highly reduced. The tolerance for transmission errors might be high as long as the radio link completes the task. A 5G radio system could be optimised at the physical layer to handle these challenging radio environments. For example, supporting increased tolerance for high retransmission rates before terminating the connection could give the 5G system more time to adapt and provide reduced but tolerable service quality.

6.4.4 Supplementary frequency bands

Commercial mobile networks have, over the years, successfully adopted the technologies for handover, multi-band operation and carrier aggregation. As the user moves, the UE is handed over to the cell with the strongest signal. A regular mobile phone supports multiple frequency bands, which increases service availability and allows the use of several frequency bands simultaneously, so-called carrier aggregation, to increase the bandwidth. In case one of the cells or frequency bands is jammed, the ability for a UE to automatically switch to another cell or frequency band that is available and undisrupted can be seen as a measure to increase redundancy. We observed this behaviour during the experiment. The smartphone switched to 4G if the 5G channel was too corrupted. The CPE terminal was also able to switch to the uninterrupted mmWave band. In this case, the system multi-band operation gave the 5G communication advantage in combating the jammer. The implementation aspects of multi-band 5G military systems should be further investigated.

7 Conclusion

The Norwegian Armed Forces are interested in fifth-generation (5G) mobile technology because of new opportunities provided by 5G, which has the potential to cover military ICT needs. However, 5G is a civilian commercial mobile communication technology that is not designed to be fully resistant to jamming. Before adapting 5G in military use cases, it is crucial to evaluate the vulnerabilities and possible disruptions to the radio communication system, which can help evaluate the threat level and the possibility of being jammed.

This report documents a theoretical and practical study of the 5G radio interface, New Radio (NR), performance in the presence of interference from a jammer. The theoretical study introduced the necessary background on 5G NR and then discussed 5G NR vulnerabilities to jamming based on theory and literature. The theoretical study gave relevant information but did not give us the necessary knowledge about jamming in a real-world commercial 5G system. We, therefore, created a real-life attack scenario by conducting a radio jamming experiment on a commercial 5G radio system that consisted of an off-the-shelf smartphone and a commercial base station antenna operating on the 3.6 GHz frequency band.

The 5G radio system responded to the contested RF environment by lowering the modulation and coding scheme and operated with reduced capacity when the jamming signal was tolerable. However, the results also showed that, in some cases, the 5G radio system struggled to find the optimal parameters for the communication under workable conditions. When the interference was too strong, leading to many errors in data transmission, the 5G session was terminated, and the connection tended to go down to an uninterrupted 4G channel.

Because of the limited user equipment (UE) output power, we consider the base station (BS) an attractive target and the uplink transmission a vulnerable 5G radio communication component. When the barrage jamming signal power received at the BS was at least 5 dB higher than the UE signal power received at the BS, the 5G connection could not provide tolerable services, indicating a successful jamming attack. Based on this 5 dB threshold (breaking point), we developed a model that determines the expected jammer range and power needed to disrupt the 5G services at a given cell radius. The model can help the armed forces evaluate the threat level and decide whether or not 5G NR is suitable for a given military scenario. For further studies, we proposed some jamming mitigation techniques that might make the 5G radio communication, especially the uplink transmission, more robust against radio jamming.

The 5G radio communication can improve capacity, broaden functionality, simplify interoperability and enable cost-effective scalability. Even though 5G NR can be jammed with enough jamming power, a 5G radio system can adapt to a moderately contested RF environment or switch to a frequency channel that is available and not disrupted. In addition to various jamming mitigation techniques, the security and robustness of mobile radio communications are upgraded with every new release of 3GPP standards. During this study of 5G jamming, we did not identify any critical drawbacks that should hinder the process of adopting 5G NR and benefiting from its advantages in military applications.

A Frequency bands

Table A.1 gives an overview of the frequency bands defined for frequency range 2 (FR2), while Table A.2 gives an overview of the frequency bands defined for frequency range 1 (FR1). The tables contain additional information about the duplex and possible bandwidths.

Band	Duplex	Frequency [GHz]	Uplink/Downlink [GHz]	Bandwidth [MHz]
n257	TDD	28	26.50–29.50	50, 100, 200, 400
n258	TDD	26	24.25–27.50	50, 100, 200, 400
n259	TDD	40	35.50–43.5	50, 100, 200, 400
n260	TDD	39	37.00–40.00	50, 100, 200, 400
n261	TDD	28	27.50–28.35	50, 100, 200, 400

Table A.1 Overview of all the frequency bands in FR2 [2].

Band	Duplex	Frequency [MHz]	Uplink [MHz]	Downlink [MHz]	Bandwidth [MHz]
n1	FDD	2100	1920–1980	2110–2170	5, 10, 15, 20
n2	FDD	1900	1850–1910	1930–1990	5, 10, 15, 20
n3	FDD	1800	1710–1785	1805–1880	5, 10, 15, 20, 25, 30
n5	FDD	850	824–849	869–894	5, 10, 15, 20
n7	FDD	2600	2500–2570	2620–2690	5, 10, 15, 20, 25, 30, 40, 50
n8	FDD	900	880–915	925–960	5, 10, 15, 20
n12	FDD	700	699–716	729–746	5, 10, 15
n14	FDD	700	788–798	758–768	5, 10
n18	FDD	850	815–830	860–875	5, 10, 15
n20	FDD	800	832–862	791–821	5, 10, 15, 20
n25	FDD	1900	1850–1915	1930–1995	5, 10, 15, 20, 25, 30, 40
n26	FDD	800	814–849	859–894	5, 10, 15, 20
n28	FDD	700	703–748	758–803	5, 10, 15, 20
n29	SDL	700	N/A	717–728	5, 10
n30	FDD	2300	2305–2315	2350–2360	5, 10
n34	TDD	2100	2010–2025		5, 10, 15
n38	TDD	2600	2570–2620		5, 10, 15, 20, 40
n39	TDD	1900	1880–1920		5, 10, 15, 20, 25, 30, 40
n40	TDD	2300	2300–2400		5, 10, 15, 20, 25, 30, 40, 50, 60, 80
n41	TDD	2500	2496–2690		10, 15, 20, 30, 40, 50, 60, 80, 90, 100
n46	TDD	5500	5150–5925		5, 10, 15, 20, 40, 50, 60, 80
n48	TDD	3500	3550–3700		5, 10, 15, 20, 40, 50, 60, 80, 90, 100
n50	TDD	1500	1432–1517		5, 10, 15, 20, 30, 40, 50, 60, 80
n51	TDD	1500	1427–1432		5
n53	TDD	2400	2483,5–2495		5, 10
n65	FDD	2100	1920–2010	2110–2200	5, 10, 15, 20
n66	FDD	1700	1710–1780	2110–2200	5, 10, 15, 20, 40
n70	FDD	2000	1695–1710	1995–2020	5, 10, 15, 20, 25
n71	FDD	600	663–698	617–652	5, 10, 15, 20
n74	FDD	1500	1427–1470	1475–1518	5, 10, 15, 20
n75	SDL	1500	N/A	1432–1517	5, 10, 15, 20, 25, 30, 40, 50
n76	SDL	1500	N/A	1427–1432	5
n77	TDD	3700	3300–4200		10, 15, 20, 25, 30, 40, 50, 60, 70, 80, 90, 100
n78	TDD	3500	3300–3800		10, 15, 20, 25, 30, 40, 50, 60, 70, 80, 90, 100
n79	TDD	4700	4400–5000		40, 50, 60, 80, 100
n80	SUL	1800	1710–1785	N/A	5, 10, 15, 20, 25, 30
n81	SUL	900	880–915	N/A	5, 10, 15, 20
n82	SUL	800	832–862	N/A	5, 10, 15, 20
n83	SUL	700	703–748	N/A	5, 10, 15, 20
n84	SUL	2100	1920–1980	N/A	5, 10, 15, 20
n86	SUL	1700	1710–1780	N/A	5, 10, 15, 20, 40
n89	SUL	850	824–849	N/A	5, 10, 15, 20
n90	TDD	2500	2496–2690		10, 15, 20, 30, 40, 50, 60, 80, 90, 100
n91	FDD	800/1500	832–862	1427–1432	5, 10
n92	FDD	800/1500	832–862	1432–1517	5, 10, 15, 20
n93	FDD	900/1500	880–915	1427–1432	5, 10
n94	FDD	900/1500	880–915	1432–1517	5, 10, 15, 20
n95	SUL	2100	2010–2025	N/A	5, 10, 15
n96	TDD	6500	5925–7125		5, 10, 15

Table A.2 Overview of all the frequency bands in FR1 [2].

B Allocation of synchronisation signals block (SSB)

The exact SSB location on a radio frame depends on the frequency band and numerology used to transmit the SSB. In Tables B.1 and B.2, all possible SSB subcarrier spacing (SCS) configurations are specified for every frequency band. Tables also contain an SSB pattern necessary for the SSB allocation in time and range of global synchronization channel number (GSCN) necessary for the SSB allocation in frequency.

Table B.3 defines all the SSB pattern cases from A to E. Depending on the case and frequency range, the index of the start symbol of the SSB in a radio frame can be calculated. The given equation covers the use of beamforming, where several SSBs in an SS burst are used. One SSB spans 4 OFDM symbols in the time domain.

A UE uses a frequency raster to find the SSB position in a given frequency band in order to establish a connection with the cell. This frequency raster is the GSCN. As shown in Tables B.1 and B.2, the range of GSCN is defined with a step size for every frequency band. A given GSCN can be translated into an exact centre frequency of the SSB using Table B.4. One SSB spans 20 resource blocks in the frequency domain.

Frequency band	SSB SCS	SSB pattern	Range of GSCN (First - <Step size>- Last)
n1	15 kHz	Case A	5279 - <1>- 5419
n2	15 kHz	Case A	4829 - <1>- 4969
n3	15 kHz	Case A	4517 - <1>- 4693
n5	15 kHz	Case A	2177 - <1>- 2230
	30 kHz	Case B	2183 - <1>- 2224
n7	15 kHz	Case A	6554 - <1>- 6718
n8	15 kHz	Case A	2318 - <1>- 2395
n12	15 kHz	Case A	1828 - <1>- 1858
n14	15 kHz	Case A	1901 - <1>- 1915
n18	15 kHz	Case A	2156 - <1>- 2182
n20	15 kHz	Case A	1982 - <1>- 2047
n25	15 kHz	Case A	4829 - <1>- 4981
n26	15 kHz	Case A	2153 - <1>- 2230
n28	15 kHz	Case A	1901 - <1>- 2002
n29	15 kHz	Case A	1798 - <1>- 1813
n30	15 kHz	Case A	5879 - <1>- 5893
n34	15 kHz	Case A	5030 - <1>- 5056
n38	15 kHz	Case A	6431 - <1>- 6544
n39	15 kHz	Case A	4706 - <1>- 4795
n40	15 kHz	Case A	5756 - <1>- 5995
n41	15 kHz	Case A	6246 - <3>- 6717
	30 kHz	Case C	6252 - <3>- 6714
n48	30 kHz	Case C	7884 - <1>- 7982
n50	15 kHz	Case A	3584 - <1>- 3787
n51	15 kHz	Case A	3572 - <1>- 3574
n53	15 kHz	Case A	6215 - <1>1 6232
n65	15 kHz	Case A	5279 - <1>- 5494
n66	15 kHz	Case A	5279 - <1>- 5494
	30 kHz	Case B	5285 - <1>- 5488
n70	15 kHz	Case A	4993 - <1>- 5044
n71	15 kHz	Case A	1547 - <1>- 1624
n74	15 kHz	Case A	3692 - <1>- 3790
n75	15 kHz	Case A	3584 - <1>- 3787
n76	15 kHz	Case A	3572 - <1>- 3574
n77	30 kHz	Case C	7711 - <1>- 8329
n78	30 kHz	Case C	7711 - <1>- 8051
n79	30 kHz	Case C	8480 - <16>- 8880
n90	15 kHz	Case A	6246 - <1>- 6717
	30 kHz	Case C	6252 - <1>- 6714
n91	15 kHz	Case A	3572 - <1>- 3574
n92	15 kHz	Case A	3584 - <1>- 3787
n93	15 kHz	Case A	3572 - <1>- 3574
n94	15 kHz	Case A	3584 - <1>- 3787

Table B.1 Applicable SSB entries per frequency band in FR1. More detailed information, including exceptions, can be found in Table 5.4.3.3-1 in [2].

Frequency band	SSB SCS	SSB pattern	Range of GSCN (First - <Step size>- Last)
n257	120 kHz	Case D	22388 - <1>- 22558
	240 kHz	Case E	22390 - <2>- 22556
n258	120 kHz	Case D	22257 - <1>- 22443
	240 kHz	Case E	22258 - <2>- 22442
n259	120 kHz	Case D	23140 - <1>- 23369
	240 kHz	Case E	23142 - <2>- 23368
n260	120 kHz	Case D	22995 - <1>- 23166
	240 kHz	Case E	22996 - <2>- 23164
n261	120 kHz	Case D	22446 - <1>- 22492
	240 kHz	Case E	22446 - <2>- 22490

Table B.2 Applicable SSB entries per frequency band in FR2. More detailed information, including exceptions, can be found in Table 5.4.3.3-2 in [2].

SSB pattern	Frequency range		Index of first OFDM-symbol of SSB	Max SSBs in SS burst
Case A: 15 kHz	FR1	<3 GHz	$\{2, 8\} + 14 \cdot n, \quad n = 0, 1$	4
		>3 GHz	$\{2, 8\} + 14 \cdot n, \quad n = 0, 1, 2, 3$	8
Case B: 30 kHz		<3 GHz	$\{4, 8, 16, 20\} + 28 \cdot n, \quad n = 0$	4
		>3 GHz	$\{4, 8, 16, 20\} + 28 \cdot n, \quad n = 0, 1$	8
Case C: 30 kHz		<2.4 GHz TDD <3 GHz FDD	$\{2, 8\} + 14 \cdot n, \quad n = 0, 1$	4
		>2.4 GHz TDD >3 GHz FDD	$\{2, 8\} + 14 \cdot n, \quad n = 0, 1, 2, 3$	8
Case D: 120 kHz	FR2		$\{4, 8, 16, 20\} + 28 \cdot n$, $n = 0, 1, 2, 3, 5, 6, 7, 8, 10, 11, 12, 13, 15, 16, 17, 18$	64
Case E: 240 kHz			$\{8, 12, 16, 20, 32, 36, 40, 44\} + 56 \cdot n$, $n = 0, 1, 2, 3, 5, 6, 7, 8$	64

Table B.3 Time symbol allocation of SSB collected from [8].

Frequency range		SSB centre frequency position	GSCN
FR1	<3 GHz	$N \cdot 1200$ kHz + $M \cdot 50$ kHz, $N = \{1 : 2499\}, \quad M \in \{1, 3, 5\}$ ($M = 3$ standard)	$3N + (M - 3)/2$
	>3 GHz	3000 MHz + $N \cdot 1.44$ MHz, $N = \{0 : 14756\}$	$7499 + N$
FR2		24250.08 MHz + $N \cdot 17.28$ MHz, $N = 0 : 4383$	$22256 + N$

Table B.4 GSCN parameters for the frequency raster [2].

C Rural Macro (RMa) path loss model

3GPP has defined several path loss models for outdoors and indoors [14]. We selected a path loss model called Rural Macro (RMa) to calculate the 5G signal path loss between the UE and BS. The RMa path loss model fitted our test environment because the model covers the rural deployment scenario and focuses on large and continuous coverage. This appendix introduces the RMa path loss model and applies it to the 5G test set-up at Rygge by inserting corresponding model parameters. Table C.1 describes all the parameters used in the RMa path loss model.

Parameter	Description	Units	Default value	Applicability range
d_{2D}	Ground distance (2D) between UE and BS	m	-	10 m $\leq d_{2D} \leq$ 10 km for LOS 10 m $\leq d_{2D} \leq$ 5 km for NLOS
d_{BPT}	Break point (BPT) distance	m	-	-
f	Carrier frequency	GHz	-	$0.5 < f < 30$ GHz
h_{BS}	Base station (BS) height	m	35 m	$10 \leq h_{BS} \leq 150$ m
h_{UE}	User equipment (UE) height	m	1.5 m	$1 \leq h_{UE} \leq 10$ m
d	Air distance (3D) between UE and BS	m	-	-
h	Average building height	m	5 m	$5 \leq h \leq 50$ m
W	Average street width	m	20 m	$5 \leq W \leq 50$ m

Table C.1 Parameters of the RMa path loss model.

The RMa path loss model is defined separately for LOS and NLOS scenarios. In the case of LOS, the model is defined as follows:

$$L_{\text{LOS}} = \begin{cases} L_1, & 10 \text{ m} \leq d_{2D} \leq d_{BPT} \\ L_2, & d_{BPT} \leq d_{2D} \leq 10 \text{ km} \end{cases}$$

where d_{BPT} is a break point (BPT) distance, which is a constant defined as

$$d_{BPT} = 20\pi h_{BS} h_{UE} f/3.$$

The LOS RMa path loss model is either calculated using the equation for L_1 or L_2, depending on whether the given ground distance between the UE and BS (d_{2D}) is shorter or longer than the given BPT distance. The L_1 is defined as

$$L_1 = 20\log(40\pi df/3) + \min(0.03h^{1.72}, 10)\log(d) - \min(0.044h^{1.72}, 14.77) + 0.002\log(h)d$$

while the L_2 is defined as

$$L_2 = L_1(d_{BPT}) + 40\log(d/d_{BPT}).$$

In the case of NLOS, the model is defined as

$$L_{\text{NLOS}} = \max(L_{\text{LOS}}, L'_{\text{NLOS}})$$

which means that the path loss for NLOS is either given by the LOS RMa path loss model or calculated using the equation for L'_{NLOS}, depending on whichever results in the highest value. The L'_{NLOS} is calculated by

$$\begin{aligned} L'_{\text{NLOS}} = {} & 161.04 - 7.1\log(W) + 7.5\log(h) - (24.37 - 3.7(h/h_{\text{BS}})^2)\log(h_{\text{BS}}) + \\ & (43.42 - 3.1\log(h_{\text{BS}}))(\log(d) - 3) + 20\log(f) - (3.2(\log(11.75h_{\text{UE}}))^2 - 4.97). \end{aligned}$$

The RMa path loss model was simplified by inserting the model parameters. The model parameters were either given by the test set-up or selected to be the default values. The centre carrier frequency (f) was 3.66 GHz. The height of the BS (h_{BS}) was 24 meters. The height of the UE (h_{UE}) was approximately 1.1 meters. For the average building height (h) and the average street width (W), the default values of 5 and 20 meters, respectively, were selected. The BPT distance then becomes

$$d_{\text{BPT}} = 20 \cdot \pi \cdot 24 \cdot 1.1 \cdot 3.66/3 \; m \approx 2022 \text{ m} \approx 2 \text{ km}.$$

The d_{BPT} value of 2 km means that within a 2 km distance between the UE and BS, the equation for L_1 could be used to calculate the path loss for the LOS propagation. By inserting the default value for h, the RMa path loss model for LOS becomes

$$L_{\text{LOS}} = 20\log(40\pi f/3) + 20.5\log(d) + 0.0014d - 0.7.$$

With the inserted values for h_{BS}, h_{UE}, h and W, the equation for L'_{NLOS} in the RMa path loss model for NLOS becomes

$$L'_{\text{NLOS}} = 20\log(f) + 39.1\log(d) + 7.2.$$

The output of the RMa path loss model is given in dB.

D Uplink jamming results

Meas. position	J/S ratio [dB]	Throughput DL [Mbps]	Throughput UL [Mbps]	MCS Index DL	MCS Index UL	MIMO Rank	Service quality
1	-6	631	49	24	26	4.0	Acceptable
2	25	-	-	-	-	-	No service
3	8	70	3	22	7	2.0	Unreliable
4	12	126	1	20	6	2.6	Unreliable
5	-5	704	29	25	22	4.0	Acceptable
6	-1	658	10	25	10	4.0	Unreliable
7	19	41	3	16	8	3.0	Unreliable
8	30	-	-	-	-	-	No service

Table D.1 Detailed 5G performance characteristics under the infuence of the barrage jamming signal of 33 dBm EIRP.

Meas. position	J/S ratio [dB]	Throughput DL [Mbps]	Throughput UL [Mbps]	MCS Index DL	MCS Index UL	MIMO Rank	Service quality
1	4	601	13	24	12	3.8	Unreliable
2	35	-	-	-	-	-	No service
3	18	-	-	-	-	-	No service
4	22	-	-	-	-	-	No service
5	5	666	21	25	15	4.0	Unreliable
6	9	62	4	21	11	4.0	Unreliable
7	29	-	-	-	-	-	No service
8	40	-	-	-	-	-	No service

Table D.2 Detailed 5G performance characteristics under the infuence of the barrage jamming signal of 43 dBm EIRP.

Meas. position	J/S ratio [dB]	Throughput DL [Mbps]	Throughput UL [Mbps]	MCS Index DL	MCS Index UL	MIMO Rank	Service quality
1	14	261	2	16	6	3.1	Unreliable
2	45	-	-	-	-	-	No service
3	28	-	-	-	-	-	No service
4	32	-	-	-	-	-	No service
5	15	466	3	24	16	4.0	Unreliable
6	19	-	-	-	-	-	No service
7	39	-	-	-	-	-	No service
8	50	-	-	-	-	-	No service

Table D.3 Detailed 5G performance characteristics under the infuence of the barrage jamming signal of 53 dBm EIRP.

E Box plot

The definition of a box plot can be found in [35]. A box plot, shown in Figure E.1, provides a visualisation of summary statistics for sample data and contains the following features:

- The bottom and top of each box are the 25th and 75th percentiles of the samples, respectively.
- The red line in the middle of each box is the sample median. If the median is not centered in the box, the plot shows sample skewness.
- The whiskers are lines extending above and below each box. Whiskers go from the minimum value to the 25th percentile and from the 75th percentile to the maximum value.
- Observations beyond the whisker length are marked as outliers.

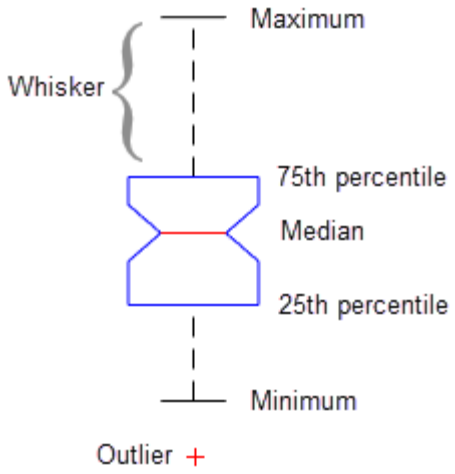


Figure E.1 Visualisation of statistics represented by a box plot [35].

F Jammer range derivation

The expression for the jammer range is derived from the definition of the J/S ratio, which is the ratio between the jammer signal power at the BS and the UE signal power at the BS. The signal power that reaches the BS is defined by the transmit power and the path loss between the transmitter and BS. The J/S ratio in dB can then be expressed as

$$\mathrm{J/S}_{[\mathrm{dB}]} = (P_{\mathrm{J}} - L_{\mathrm{J}}) - (P_{\mathrm{UE}} - L_{\mathrm{UE}})$$

where P_{J} is the jammer's transmit power, L_{J} is the jamming signal path loss, P_{UE} is UE's transmit power and L_{UE} is the uplink signal path loss. We want to find the expression for L_{J} because the jamming signal path loss contains the jammer range. In this report, a determined value of the J/S ratio for a successful jamming attack is called breaking point (BP). Inserting BP into the expression gives

$$\begin{aligned} BP &= (P_{\mathrm{J}} - L_{\mathrm{J}}) - (P_{\mathrm{UE}} - L_{\mathrm{UE}}) \\ L_{\mathrm{J}} &= P_{\mathrm{J}} - P_{\mathrm{UE}} + L_{\mathrm{UE}} - \mathrm{BP}. \end{aligned} \tag{F.1}$$

Now we insert the corresponding expressions for the path losses L_{J} and L_{UE}. We assume LOS between the UE and BS and use the RMa LOS path loss model introduced in Appendix C:

$$L_{\mathrm{UE}} = \begin{cases} L_1, & 10\ \mathrm{m} \leq d_{\mathrm{2D}} \leq d_{\mathrm{BPT}} \\ L_2, & d_{\mathrm{BPT}} \leq d_{\mathrm{2D}} \leq 10\ \mathrm{km} \end{cases}$$

where d_{BPT} is defined as

$$d_{\mathrm{BPT}} = 20\pi h_{\mathrm{BS}} h_{\mathrm{UE}} f/3.$$

The d_{BPT} is given in meters, h_{BS} and h_{UE} are the hights of the BS and UE, respectively, given in meters, and f is the carrier frequency given in GHz. L_1 can be expressed as

$$L_1 = 20\log(40\pi f/3) + 20.5\log(d) + 0.0014d - 0.7$$

when the default value for average building height is used. L_2 is defined as

$$L_2 = L_1(d_{\mathrm{BPT}}) + 40\log(d/d_{\mathrm{BPT}}).$$

For the jamming signal, we use the path loss exponent model introduced in Section 4.5.1:

$$L_{\mathrm{J}} = 10n\log(d) + 20\log(40\pi f/3).$$

If the ground distance between the UE and BS ($d_{2\mathrm{D}}$) is less than d_{BPT}, L_1 is used to calculate L_{UE}. Inserting L_{UE} and L_{J} in F.1 gives

$$10n\log(d_{\mathrm{J}})+20\log(40\pi f/3) = P_{\mathrm{J}}-P_{\mathrm{UE}}+20\log(40\pi f/3)+20.48\log(d_{\mathrm{UE}})+0.0014d_{\mathrm{UE}}-0.7-\mathrm{BP}$$

where n is the path loss exponent of the jamming signal, d_{J} is the distance between the jammer and the BS, d_{UE} is the distance between the UE and the BS. The carrier frequency f is given in GHz. The distances d_{J} and d_{UE} are given in meters. P_{J} and P_{UE} are given in dBm. BP is given in dB. The carrier frequency f is common for the jammer and the UE; thus, it cancels out in the equation. The equation for the jammer range becomes

$$\mathrm{d_J} = 10^{(P_{\mathrm{J}}-P_{\mathrm{UE}}-\mathrm{BP}+20.48\log(d_{\mathrm{UE}})+0.0014d-0.7_{\mathrm{UE}})/(10n)}$$

$$\text{where } n = \begin{cases} 2, & \text{for jammer in LOS with the BS} \\ 3, & \text{for jammer in NLOS with the BS.} \end{cases}$$

If the $d_{2\mathrm{D}}$ is greater than d_{BPT}, L_2 is used to calculate L_{UE}. With L_2, the jammer range becomes

$$\mathrm{d_J} = 10^{(P_{\mathrm{J}}-P_{\mathrm{UE}}-\mathrm{BP}+20.48\log(d_{\mathrm{BPT}})+0.0014d_{\mathrm{BPT}}-0.7+40\log(d_{\mathrm{UE}}/d_{\mathrm{BPT}}))/(10n)}$$

$$\text{where } n = \begin{cases} 2, & \text{for jammer in LOS with the BS} \\ 3, & \text{for jammer in NLOS with the BS.} \end{cases}$$

The d_{BPT} was 2 km for the 5G test set-up at Rygge. The distance between the UE and BS in the jammer range model presented in Section 5.5.2 did not exceed this value. Therefore, only the expression for the jammer range derived from L_1 was used in this report.

Abbreviations

3GPP	3rd Generation Partnership Project
4G	4th Generation mobile network
5G	5th Generation mobile network
5GC	5G Core Network
5G-VINNI	5G Vertical Innovation Infrastructure
ACK	Acknowledgement
BLER	Block Error Rate
BP	Breaking Point
BPSK	Binary Phase-Shift Keying
BPT	Break Point
BS	Base Station
CDMA	Code-Division Multiple Access
CORESET	Control Resource Set
CP	Cyclic Prefix
CPE	Customer Premises Equipment
CRS	Cell-specific Reference Signal
CSI	Channel State Information
CSI-RS	Channel State Information Reference Signal
DAB	Digital Audio Broadcasting
DFT-S-OFDM	Discrete Fourier Transform Spread OFDM
DL	Downlink
DM-RS	Demodulation Reference Signal
DSS	Dynamic Spectrum Sharing
EIRP	Effective Isotropic Radiated Power
EN-DC	E-UTRA-NR Dual Connectivity
eNodeB	E-UTRAN Node B
EPC	Evolved Packet Core
EU	European Union
E-UTRA	Evolved Universal Mobile Telecommunications System (UMTS) Terrestrial Radio Access
EW	Electronic Warfare
FDD	Frequency-Division Duplexing
FDMA	Frequency-Division Multiple Access
FFI	Norwegian Defence Research Establishment
FMA	Norwegian Defence Material Agency
FR1	Frequency Range 1
FR2	Frequency Range 2
FSL	Free Space Loss
FWA	Fixed Wireless Access
gNodeB	next Generation Node B
GSCN	Global Synchronisation Channel Number
HARQ	Hybrid Automatic Repeat Request
ICT	Information and Communication Technology
ID	Identification

IKT	Informasjons- og kommunikasjonsteknologi
IoT	Internet of Things
J/S ratio	Jamming-to-uplink-Signal ratio
LDPC	Low-Density Parity-Check
LOS	Line-Of-Sight
LTE	Long-Term Evolution
MCS	Modulation Coding Scheme
MIB	Master Information Block
MIMO	Multiple-Input Multiple-Output
MNO	Mobile Network Operator
MU-MIMO	Multi-User MIMO
NARFA NOR	National Allied Radio Frequency Agency Norway
NGMN	Next Generation Mobile Network Alliance
Nkom	Norwegian Communications Authority
NLOS	Non-Line-Of-Sight
NR	New Radio
NSA	Non-Stand Alone
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency-Division Multiple Access
OSI	Open Systems Interconnection
PBCH	Physical Broadcast Channel
PCFICH	Physical Control Format Indicator Channel
PCI	Physical-layer Cell Identity
PDCCH	Physical Downlink Control Channel
PDSCH	Physical Downlink Shared Channel
PRACH	Physical Random-Access Channel
PRS	Positioning Reference Signal
PSS	Primary Synchronisation Signal
PT-RS	Phase-Tracking Reference Signal
PUCCH	Physical Uplink Control Channel
PUSCH	Physical Uplink Shared Channel
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase-Shift Keying
R&S	Rohde and Schwarz
RB	Resource Block
RE	Resource Element
RF	Radio Frequency
RMa	Rural Macro
RRC	Radio Resource Control
RS	Reference Signal
RSRP	Reference Signals Received Power
RSRQ	Reference Signal Received Quality
RSSI	Received Signal Strength Indicator
SA	Stand Alone
SCS	Subcarrier Spacing
SDR	Software-Defined Radio

SFN	System Frame Number
SIB	System Information Block
SINR	Signal-to-Noise and Interference Ratio
SISO	Single-Input Single-Output
SMA	SubMiniature version A
SN	Secondary Node
SRS	Sounding Reference Signal
SS	Synchronisation Signal
SSB	Synchronisation Signals/Physical Broadcast Channel Block
SSS	Secondary Synchronisation Signal
SU-MIMO	Single-User MIMO
TDD	Time-Division Duplexing
TDMA	Time-Division Multiple Access
TRP	Total Radiated Power
UE	User Equipment
UL	Uplink
V2V	Vehicle-to-Vehicle
Wi-Fi	Wireless Fidelity

Bibliography

[1] 3GPP. *NGMN Alliance Joins 3GPP as Partner*. [Internet].
URL: https://www.3gpp.org/news-events/partners-news/1362-NGMN-Alliance-Joins-3GPP-as-Partner.

[2] 3GPP. *NR; Base Station (BS) radio transmission and reception*.
Technical specification (TS) 38.104. Version 16.7.0.
3rd Generation Partnership Project (3GPP), Apr. 2021.
URL: https://3gpp.org/dynareport/38104.htm.

[3] 3GPP. *NR; Multi-connectivity; Overall description; Stage-2*.
Technical specification (TS) 37.340. Version 16.5.0.
3rd Generation Partnership Project (3GPP), Mar. 2021.
URL: https://3gpp.org/dynareport/37340.htm.

[4] 3GPP. *NR; Multiplexing and channel coding*. Technical specification (TS) 38.212.
Version 16.5.0. 3rd Generation Partnership Project (3GPP), Mar. 2021.
URL: https://3gpp.org/dynareport/38212.htm.

[5] 3GPP. *NR; NR and NG-RAN Overall description; Stage-2*.
Technical specification (TS) 38.300. Version 16.6.0.
3rd Generation Partnership Project (3GPP), July 2021.
URL: https://3gpp.org/dynareport/38300.htm.

[6] 3GPP. *NR; Physical channels and modulation*. Technical specification (TS) 38.211.
Version 16.5.0. 3rd Generation Partnership Project (3GPP), Mar. 2021.
URL: https://3gpp.org/dynareport/38211.htm.

[7] 3GPP. *NR; Physical layer measurements*. Technical specification (TS) 38.215.
Version 16.4.0. 3rd Generation Partnership Project (3GPP), Jan. 2021.
URL: https://3gpp.org/dynareport/38215.htm.

[8] 3GPP. *NR; Physical layer procedures for control*. Technical specification (TS) 38.213.
Version 16.5.0. 3rd Generation Partnership Project (3GPP), Mar. 2021.
URL: https://3gpp.org/dynareport/38213.htm.

[9] 3GPP. *NR; Physical layer procedures for data*. Technical specification (TS) 38.214.
Version 16.5.0. 3rd Generation Partnership Project (3GPP), Mar. 2021.
URL: https://3gpp.org/dynareport/38214.htm.

[10] 3GPP. *NR; Radio Resource Control (RRC); Protocol specification*.
Technical specification (TS) 38.331. Version 16.4.1.
3rd Generation Partnership Project (3GPP), Mar. 2021.
URL: https://3gpp.org/dynareport/38331.htm.

[11] 3GPP.
NR; User Equipment (UE) radio transmission and reception; Part 1: Range 1 Standalone.
Technical specification (TS) 38.101-1. Version 16.7.0.
3rd Generation Partnership Project (3GPP), Apr. 2021.
URL: https://3gpp.org/dynareport/38101-1.htm.

[12] 3GPP.
NR; User Equipment (UE) radio transmission and reception; Part 2: Range 2 Standalone.
Technical specification (TS) 38.101-2. Version 16.7.0.
3rd Generation Partnership Project (3GPP), Apr. 2021.
URL: https://3gpp.org/dynareport/38101-2.htm.

[13] 3GPP. *Release description; Release 15*. Technical report (TR) 21.915. Version 15.0.0.
3rd Generation Partnership Project (3GPP), Oct. 2019.
URL: https://3gpp.org/dynareport/21915.htm.

[14] 3GPP. *Study on channel model for frequencies from 0.5 to 100 GHz*.
Technical report (TR) 38.901. Version 16.1.0.
3rd Generation Partnership Project (3GPP), Jan. 2020.
URL: https://3gpp.org/dynareport/38901.htm.

[15] 5G-VINNI. *5G Verticals Innovation Infrastructure - Concept*. [Internet]. 2021.
URL: https://www.5g-vinni.eu/concept-approach/.

[16] Anders Mykkeltveit Agnius Birutis.
Practical Jamming of a Commercial 5G Radio System at 3.6 GHz.
Proceedings of ICMCIS 2022. Udine, Italy, May 17-18, 2022.

[17] Sassan Ahmadi. *5G NR: Architecture, Technology, Implementation, and Operation of 3GPP New Radio Standards*. Academic Press, 2019.

[18] Berk Akgun, Marwan Krunz and O. Ozan Koyluoglu.
Vulnerabilities of Massive MIMO Systems to Pilot Contamination Attacks. Article. 2019.
DOI: 10.1109/TIFS.2018.2876750.

[19] Hossein Akhlaghpasand, Emil Björnson and S. Mohammad Razavizadeh.
Jamming Suppression in Massive MIMO Systems. Article. 2020.
DOI: 10.1109/TCSII.2019.2902074.

[20] NGMN Alliance. *5G Devices Categorization*. Final Deliverable. Version 1.2.
Next Generation Mobile Networks (NGMN), Mar. 2020.
URL: https://www.ngmn.org/publications/5g-devices-categorization.html.

[21] Agnius Birutis and Anders Mykkeltveit. *5G New Radio – oversikt og foreløpige målinger*.
FFI-eksternnotat 20/02198. 2020.

[22] Tan Tai Do et al. *Jamming-Resistant Receivers for the Massive MIMO Uplink*. Article. 2018.
DOI: 10.1109/TIFS.2017.2746007.

[23] Ericsson. *Advanced antenna systems for 5G networks*. Technical White Paper. Nov. 2018.
URL: https://www.ericsson.com/en/reports-and-papers/white-papers/advanced-antenna-systems-for-5g-networks.

[24] Bodil Hvesser Farsund and Anne Marie Hegland.
5G i Forsvaret – Muligheter og sikkerhetsutfordringer. FFI-eksternnotat 20/01206. 2020.

[25] Bodil Hvesser Farsund, Anne Marie Hegland and Frode Lillevold.
LTE i Forsvaret – sårbarheter knyttet til ulike forretningsmodeller. FFI-rapport 16/00808.
2016.

[26] GSMA. *5G TDD synchronisation*. [Internet]. 2020. URL: https://www.gsma.com/spectrum/resources/3-5-ghz-5g-tdd-synchronisation.

[27] Anne Pernille Hveem.
Mobilt bredbånd med LTE: teknologi, sikkerhet, tjenester og utbygging.
FFI-rapport 2011/00709. 2011.

[28] Anne Pernille Hveem. *Samhandling mellom autonome taktiske LTE-noder i nettverk*.
FFI-rapport 18/01601. Unntatt offentlighet. 2019.

[29] National Instruments. *5G New Radio: Introduction to the Physical Layer*.
Technical White Paper. URL: https://www.ni.com/en-no/innovations/wireless/5g/new-radio.html#whitepaper.

[30] iPerf3. *iPerf3*. [Internet]. 2021. URL: https://iperf.fr/.

[31] Asanka Kekirigoda et al.
Massive MIMO for Tactical Ad-hoc Networks in RF Contested Environments. Article. 2019.
DOI: 10.1109/MILCOM47813.2019.9020756.

[32] Petter Kristiansen and Anders Mykkeltveit.
Muligheter og sårbarheter ved bruk av kommersiell mobilteknologi i Forsvaret.
FFI-rapport 18/01708. BEGRENSET. 2019.

[33] Marc Lichtman et al.
5G NR Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation. Article. 2018.
DOI: 10.1109/ICCW.2018.8403769.

[34] Marc Lichtman et al.
LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation. Article. 2016.
DOI: 10.1109/MCOM.2016.7452266.

[35] MathWorks. *Boxplot*. [Internet]. 2021.
URL: https://se.mathworks.com/help/stats/boxplot.html.

[36] Nkom. *Frekvensportalen*. [Internet]. 2021. URL: https://frekvens.nkom.no/.

[37] Nasjonal kommunikasjonsmyndighet (Nkom). *About Nkom*. [Internet]. 2021.
URL: https://www.nkom.no/english/about-nkom.

[38] Nasjonal kommunikasjonsmyndighet (Nkom). *Frekvenser til mobilkommunikasjon og 5G*.
[Internet]. 2021. URL: https://www.nkom.no/frekvenser-og-elektronisk-utstyr/frekvenser-til-mobilkommunikasjon-og-5g.

[39] Nasjonal kommunikasjonsmyndighet (Nkom). *The Norwegian 5G auction has concluded*.
[Internet]. 2021. URL:
https://www.nkom.no/aktuelt/the-norwegian-5g-auction-has-concluded.

[40] Norwegian Armed Forces.
Forsvarets IKT-strategi. Økt operativ effekt gjenom robust IKT i kontinuerlig utvikling - IKT for morgendagens forsvar (Norwegian Armed Forces' ICT strategy). Article. 2021.

[41] Norwegian Defence Materiel Agency. *Program Mime*. [Internet]. 2022.
URL: https://www.fma.no/anskaffelser/virksomhetsprogrammet-mime.

[42] Norwegian Ministry of Defence.
Future Acquisitions For the Norwegian Defence Sector 2021–2028. [Internet]. 2021.
URL: https://www.regjeringen.no/contentassets/09d83a5cbefd4fb68064e6ca871acccb/faf-2021-2028-engelsk-versjon-__.pdf.

[43] Ookla. *Speedtest*. [Internet]. 2021. URL: https://www.speedtest.net/about.

[44] Poynting. *OMNI-296*. [Internet]. 2021. URL: https://poynting.tech/antennas/omni-296/.

[45] Rohde and Schwarz. *QualiPoc Android – The premium handheld troubleshooter*. [Internet]. 2021. URL: https://www.rohde-schwarz.com/no/product/qualipoc_android-productstartpage_63493-55430.html.

[46] Marc Rutschlin. *5G Antenna Design for Mobile Phones*. [Internet]. 2018. URL: https://blogs.3ds.com/simulia/5g-antenna-design-mobile-phones/.

[47] Luca Sanguinetti, Emil Björnson and Jakob Hoydis. *Toward Massive MIMO 2.0: Understanding Spatial Correlation, Interference Suppression, and Pilot Contamination*. Article. 2020. DOI: 10.1109/TCOMM.2019.2945792.

[48] Chowdhury Shahriar et al. *PHY-Layer Resiliency in OFDM Communications: A Tutorial*. Article. 2015. DOI: 10.1109/COMST.2014.2349883.

[49] Keysight technologies. *N9914B FieldFox Handheld RF Analyzer, 6.5 GHz*. [Internet]. 2021. URL: https://www.keysight.com/zz/en/product/N9914B/fieldfox-b-handheld-rf-analyzer-6-5-ghz.html.

[50] Thomas Thoresen, Jørn Kårstad and Tore Ulversøy. *Sårbarhetsvurdering av LTE radiogrensesnitt*. FFI-rapport 18/00617. BEGRENSET. 2018.

[51] Martin H Weik. *Communications standard dictionary*. Van Nostrand Reinhold, 1983.

[52] Wikipedia. *Comparison of mobile phone standards – Wikipedia*. [Internet]. 2021. URL: https://en.wikipedia.org/w/index.php?title=Comparison_of_mobile_phone_standards&oldid=1033411136.

[53] Wikipedia. *Liste over frekvenser for telekommunikasjon i Norge – Wikipedia*. [Internet]. 2021. URL: https://no.wikipedia.org/w/index.php?title=Liste_over_frekvenser_for_telekommunikasjon_i_Norge&oldid=21474067.

[54] Wikipedia. *MIMO*. [Internet]. 2021. URL: https://en.wikipedia.org/w/index.php?title=MIMO&oldid=1033152220.

[55] Wikipedia. *Path loss*. [Internet]. 2021. URL: https://en.wikipedia.org/w/index.php?title=Path_loss&oldid=1024387324.

About FFI

The Norwegian Defence Research Establishment (FFI) was founded 11th of April 1946. It is organised as an administrative agency subordinate to the Ministry of Defence.

FFI's mission

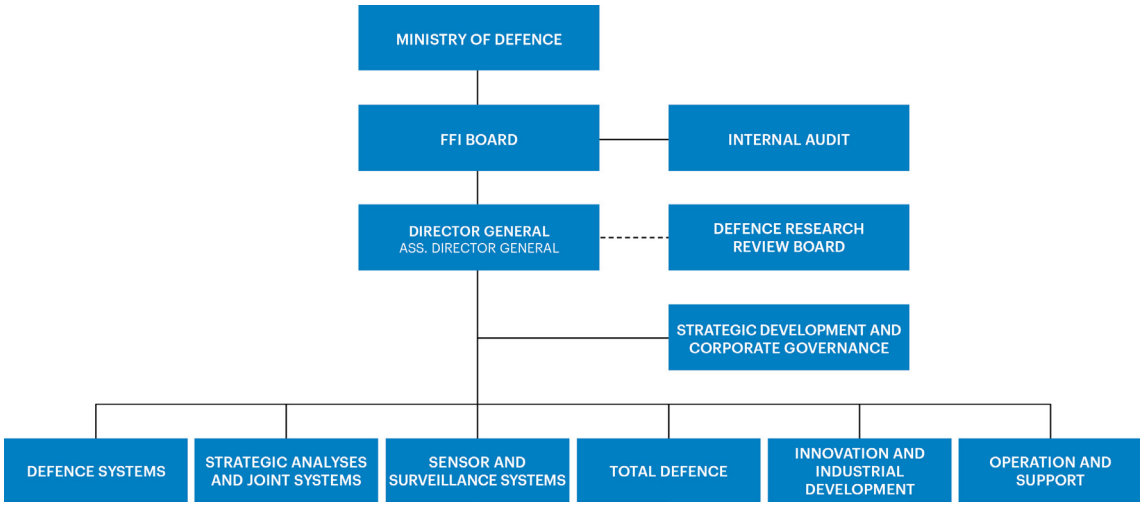
FFI is the prime institution responsible for defence related research in Norway. Its principal mission is to carry out research and development to meet the requirements of the Armed Forces. FFI has the role of chief adviser to the political and military leadership. In particular, the institute shall focus on aspects of the development in science and technology that can influence our security policy or defence planning.

FFI's vision

FFI turns knowledge and ideas into an efficient defence.

FFI's characteristics

Creative, daring, broad-minded and responsible.



Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

Telefon: 63 80 70 00
Telefaks: 63 80 71 15
Epost: post@ffi.no

Norwegian Defence Research Establishment (FFI)
P.O. Box 25
NO-2027 Kjeller

Office address:
Instituttveien 20
N-2007 Kjeller

Telephone: +47 63 80 70 00
Telefax: +47 63 80 71 15
Email: post@ffi.no