Vulnerabilities of LTE and LTE-Advanced Communication

White Paper

Long Term Evolution (LTE) technology has become the technology of choice for keeping up with the requirement of higher throughput in mobile communication in bands below 6 GHz. It is expected that within the next decade LTE will become the primary commercial standard. LTE is often used to broadcast emergency information in times of natural disasters and national crises and is under investigation for further end use application in government as well as military application fields.

Communication via LTE has some vulnerabilities. This drawback is a matter of concern since it is possible to completely take down the LTE network or at least partially block communication, intentionally with the help of jamming signals, or unintentionally through various forms of interference.

An example of unintentional interference issues is the frequently discussed co-existence issues with Air Traffic Control (ATC) S-band radar and Digital TV bands. The in-device co-existence challenge is also a potentially important issue with the rapid evolution of multi-standard radios.

This White Paper will focus on the vulnerabilities of LTE communication by explaining LTE jamming and unintentional interference problems, address the co-existence issues with other services, and discuss the mitigation options to build a broad perspective on the possible deployment of the LTE technology for future military and civil governmental applications.

Understanding the susceptance of new technologies to known and expected environments is critical to the adoption for defense applications

White Paper
Naseef Mahmud
9.2014 - 1MA245_2e

ROHDE&SCHWARZ

Table of Contents

1 Abstract

Demand for high-volume data streams in the current market for modern wireless communication systems is growing at a fast pace. In order to keep up with the trend to higher throughput requirements within unchanged bandwidth limitations, the Long Term Evolution (LTE) technology has become a popular solution for replacing the data transfer over 2G / 3G communication networks. It is expected that within the next decade LTE will become the primary cellular standard. The reason for this rapid increase in popularity of LTE, points to the low cost and high performance that is provided by this technology. It can potentially reach a raw bit rate of 300 Mbps in the downlink channel using advanced MIMO configurations. Furthermore, introduction of voice services to LTE is targeted for 2015. This would then allow complete substitution of all other cellular standards.

Other than providing the standard of choice for commercial networks, LTE is also often used to broadcast emergency information in times of natural disasters and national crisis situations. However, LTE has some vulnerabilities which is a matter of concern since it is possible to completely take down an LTE network or at least partially block communication network intentionally or unintentionally. Some of the defined LTE bands are prone to co-existence issues with the S-band radar frequencies as used by Air Traffic Control (ATC) and Air Traffic Surveillance (ATS) radars to look into the horizon up to 500 km range.

In the lower end of the frequency spectrum, LTE has co-existence issues at the Ultra High Frequency (UHF) and even in some cases with Very High Frequency (VHF) bands, which are used for transmitting digital television or commonly known as Digital Video Broadcasting-Terrestrial (DVB-T).

A clear understanding of the LTE technology and its vulnerabilities is very important for commercial, civil-governmental and defense applications. Rohde & Schwarz has published application notes which address the co-existence issues of LTE with the ATC S-band radar frequencies and DVB-T frequencies.

This white paper briefly touches relevant basics of LTE, highlights area of greatest susceptibility to interference and jamming of the LTE network as well as counter-measures. It also takes a look into the co-existence problem. The overall aim of this white paper is to help build a strong perspective on the possible deployment of the LTE technology for future commercial, civil-governmental and military applications.

2 Basics of LTE

Long Term Evolution (LTE) is a wireless communication standard developed by the 3rd Generation Partnership Project (3GPP). The concept was first introduced in the Release 8 document series of 3GPP in the 4th quarter of 2008. Further updates and modification were later made in Release 9 in 2009 and LTE Advanced introduced in Release 10 in 2011. Only 3GPP-Rel.10 fulfils requirements outlined by the International Telecommunications Union (ITU) for so-called 4th generation wireless communication systems. However, LTE Rel. 8 is also quite commonly referred to as "4G"

2.1 History of LTE

The "3G" Universal Mobile Telecommunications System (UMTS) network has seen a steady evolution over the years to keep up with the growing demand of higher data rate and capacity for packet data. High Speed Packet Access (HSPA) was first introduced to handle the demand in downlink (Rel.5) and later, uplink (Rel.6). The next significant step in the evolution was made in Release 7, with the introduction of HSPA+. Enhancements in terms of latency and peak data rate led to exploitation of the basic 5 MHz wide band operation which are not so different from what Release 8, the first step in LTE, would offer. The Rel.7 enhancements were realized by the introduction of downlink MIMO (Multiple Input Multiple Output), higher order modulation schemes for uplink (16QAM) and downlink (64QAM), Layer 2 protocol improvements and continuous packet connectivity.

To guaranty the competitiveness of UMTS for the next decade and beyond, the 3GPP introduced UMTS Long Term Evolution (LTE) in 2008 as part of its Release 8 document series. The proposed updates were higher data rates, lower latency on user side as well as the control side and a packet-optimized radio access technology. About 30 additional frequency band allocation of spectrum were assigned and channel bandwidths from 1.4 MHz to 20 MHz were defined for these bands. Commercial LTE network deployment started at the end of 2009.

3GPP in the following years, introduced additional enhancements on the LTE standard in the Release 9 and 10 publications. Improvements include the combination of 64 QAM and MIMO, up to four carrier operations for the downlink (without MIMO), and two carrier operation for the uplink. These updates made the theoretical downlink and uplink data rates, reach 168 Mbps and 23 Mbps, respectively.

At the moment, it is possible to obtain data rates of up to 300 Mbps in downlink and up to 75 Mbps in the uplink, depending on the complexity of the involved communication equipment. Networks using Rel.10-compatible equipment are also referred to as "LTE-Advanced"

2.2 Inside LTE

LTE is referred to as Evolved UMTS Terrestrial Radio Access (E-UTRA) or Evolved UMTS Terrestrial Radio Access Network (E-TRAN) in the industry. LTE uses two different multiple access schemes on the air interface for the downlink and the uplink. In the downlink, Orthogonal Frequency Division Multiple Access (OFDMA) is used and Single Carrier Frequency Division Multiple Access (SC-FDMA) is used in the uplink. MIMO antenna schemes play a major role in obtaining the high data rates in LTE.

LTE has two operational modes, the Frequency Division Duplex (FDD) mode of operation that requires pair of available spectrum, one assigned exclusively to uplink and the other to downlink use, or a Time Division Duplex (TDD) mode of operation operating in unpaired spectrum. Each LTE band supports a subset of bandwidths including 1.4, 3, 5, 10, 15 and 20 MHz or combinations of their integer multiples.

E-UTRA Operating Band	Uplink (UL) operating band BS receive UE transmit	Downlink (DL) operating band BS transmit UE receive	Duplex Mode
	F_{UL_low} – F_{UL_high}	F_{DL_low} – F_{DL_high}	
1	1920 MHz – 1980 MHz	2110 MHz – 2170 MHz	FDD
2	1850 MHz – 1910 MHz	1930 MHz – 1990 MHz	FDD
3	1710 MHz – 1785 MHz	1805 MHz – 1880 MHz	FDD
4	1710 MHz – 1755 MHz	2110 MHz – 2155 MHz	FDD
5	824 MHz – 849 MHz	869 MHz – 894MHz	FDD
6[1]	830 MHz – 840 MHz	875 MHz – 885 MHz	FDD
7	2500 MHz – 2570 MHz	2620 MHz – 2690 MHz	FDD
8	880 MHz – 915 MHz	925 MHz – 960 MHz	FDD
9	1749.9 MHz – 1784.9 MHz	1844.9 MHz – 1879.9 MHz	FDD
10	1710 MHz – 1770 MHz	2110 MHz – 2170 MHz	FDD
11	1427.9 MHz – 1447.9MHz	1475.9 MHz – 1495.9 MHz	FDD
12	699 MHz – 716 MHz	729 MHz – 746 MHz	FDD
13	777 MHz – 787 MHz	746 MHz – 756 MHz	FDD
14	788 MHz – 798 MHz	758 MHz – 768 MHz	FDD
15	Reserved	Reserved	FDD
16	Reserved	Reserved	FDD
17	704 MHz – 716 MHz	734 MHz – 746 MHz	FDD
18	815 MHz – 830 MHz	860 MHz – 875 MHz	FDD
19	830 MHz – 845 MHz	875 MHz – 890 MHz	FDD
20	832 MHz – 862 MHz	791 MHz – 821 MHz	FDD
21	1447.9 MHz – 1462.9 MHz	1495.9 MHz – 1510.9 MHz	FDD
22	3410 MHz – 3490 MHz	3510 MHz – 3590 MHz	FDD
23	2000 MHz – 2020 MHz	2180 MHz – 2200 MHz	FDD
24	1626.5 MHz – 1660.5 MHz	1525 MHz – 1559 MHz	FDD
25	1850 MHz – 1915 MHz	1930 MHz – 1995 MHz	FDD
26	814 MHz – 849 MHz	859 MHz – 894 MHz	FDD
27	807 MHz – 824 MHz	852 MHz – 869 MHz	FDD
28	703 MHz – 748 MHz	758 MHz – 803 MHz	FDD
29	N/A	717 MHz – 728 MHz	FDD[2]
30	2305 MHz – 2315 MHz	2350 MHz – 2360 MHz	FDD
31	452.5 MHz – 457.5 MHz	462.5 MHz – 467.5 MHz	FDD
...32	N/A	1452 MHz – 1496 MHz	FDD[2]
33	1900 MHz – 1920 MHz	1900 MHz – 1920 MHz	TDD
34	2010 MHz – 2025 MHz	2010 MHz – 2025 MHz	TDD
35	1850 MHz – 1910 MHz	1850 MHz – 1910 MHz	TDD
36	1930 MHz – 1990 MHz	1930 MHz – 1990 MHz	TDD
37	1910 MHz – 1930 MHz	1910 MHz – 1930 MHz	TDD
38	2570 MHz – 2620 MHz	2570 MHz – 2620 MHz	TDD
39	1880 MHz – 1920 MHz	1880 MHz – 1920 MHz	TDD
40	2300 MHz – 2400 MHz	2300 MHz – 2400 MHz	TDD
41	2496 MHz – 2690 MHz	2496 MHz – 2690 MHz	TDD
42	3400 MHz – 3600 MHz	3400 MHz – 3600 MHz	TDD
43	3600 MHz – 3800 MHz	3600 MHz – 3800 MHz	TDD
44	703 MHz – 803 MHz	703 MHz – 803 MHz	TDD

NOTE 1: Band 6 is not applicable
NOTE 2: Restricted to E-UTRA operation when carrier aggregation is configured. The downlink operating band is paired with the uplink operating band (external) of the carrier aggregation configuration that is supporting the configured Pcell.

Table 2-1: The operating frequency bands for an LTE-FDD and LTE-TDD base station (extracted from 3GPP TS36.141)

Table 2-1 shows the different LTE bands allocated for the two operating modes. Band 1 to band 28 are allocated for the FDD mode of operation and band 33 to band 44 are allocated for TDD mode of operation. As explained before, TDD spectra are the same for uplink and downlink as direction of communication alternates over time.

E-UTRA carrier aggregation (CA) is designed to operate in the operating bands defined in Table 2-2 to Table 2-4.

E-UTRA CA Band	E-UTRA Band	Uplink (UL) operating band BS receive / UE transmit F_{UL_low} – F_{UL_high}			Downlink (DL) operating band BS transmit / UE receive F_{DL_low} – F_{DL_high}			Duplex Mode
CA_2-2	2	1850 MHz	–	1910 MHz	1930 MHz	–	1990 MHz	FDD
CA_3-3	3	1710 MHz	–	1785 MHz	1805 MHz	–	1880 MHz	FDD
CA_4-4	4	1710 MHz	–	1755 MHz	2110 MHz	–	2155 MHz	FDD
CA_7-7	7	2500 MHz	–	2570 MHz	2620 MHz	–	2690 MHz	FDD
CA_23-23	23	2000 MHz	–	2020 MHz	2180 MHz	–	2200 MHz	FDD
CA_25-25	25	1850 MHz	–	1915 MHz	1930 MHz	–	1995 MHz	FDD
CA_41-41	41	2496 MHz	–	2690 MHz	2496 MHz	–	2690 MHz	TDD
CA_42-42	42	3400 MHz	–	3600 MHz	3400 MHz	–	3600 MHz	TDD

Table 2-2: Intra-band non-contiguous CA operating bands

E-UTRA CA Band	E-UTRA Band	Uplink (UL) operating band BS receive / UE transmit F_{UL_low} – F_{UL_high}			Downlink (DL) operating band BS transmit / UE receive F_{DL_low} – F_{DL_high}			Duplex Mode
CA_1	1	1920 MHz	–	1980 MHz	2110 MHz	–	2170 MHz	FDD
CA_3	3	1710MHz	–	1785MHz	1805MHz	–	1880MHz	FDD
CA_7	7	2500 MHz	–	2570 MHz	2620 MHz	–	2690 MHz	FDD
CA_23	23	2000 MHz	–	2020 MHz	2180 MHz	–	2200 MHz	FDD
CA_27	27	807 MHz	–	824 MHz	852 MHz	–	869 MHz	FDD
CA_38	38	2570 MHz	–	2620 MHz	2570 MHz	–	2620 MHz	TDD
CA_39	39	1880 MHz	–	1920 MHz	1880 MHz	–	1920 MHz	TDD
CA_40	40	2300 MHz	–	2400 MHz	2300 MHz	–	2400 MHz	TDD
CA_41	41	2496 MHz	–	2690 MHz	2496 MHz	–	2690 MHz	TDD
CA_42	42	3400 MHz	–	3600 MHz	3400 MHz	–	3600 MHz	TDD

Table 2-3: Intra-band contiguous CA operating bands

E-UTRA CA Band	E-UTRA Band	Uplink (UL) operating band BS receive / UE transmit F_{UL_low} – F_{UL_high}			Downlink (DL) operating band BS transmit / UE receive F_{DL_low} – F_{DL_high}			Duplex Mode
CA_1-5	1	1920 MHz	–	1980 MHz	2110 MHz	–	2170 MHz	FDD
	5	824 MHz	–	849 MHz	869 MHz	–	894 MHz	
CA_1-8	1	1920 MHz	–	1980 MHz	2110 MHz	–	2170 MHz	FDD
	8	880 MHz	–	915 MHz	925 MHz	–	960 MHz	
CA_1-11	1	1920 MHz	–	1980 MHz	2110 MHz	–	2170 MHz	FDD
	11	1427.9 MHz	–	1447.9 MHz	1475.9 MHz	–	1495.9 MHz	
CA_1-18	1	1920 MHz	–	1980 MHz	2110 MHz	–	2170 MHz	FDD
	18	815 MHz	–	830 MHz	860 MHz	–	875 MHz	
CA_1-19	1	1920 MHz	–	1980 MHz	2110 MHz	–	2170 MHz	FDD
	19	830 MHz	–	845 MHz	875 MHz	–	890 MHz	
CA_1-20	1	1920 MHz	–	1980 MHz	2110 MHz	–	2170 MHz	FDD
	20	832 MHz	–	862 MHz	791 MHz	–	821 MHz	
CA_1-21	1	1920 MHz	–	1980 MHz	2110 MHz	–	2170 MHz	FDD
	21	1447.9 MHz	–	1462.9 MHz	1495.9 MHz	–	1510.9 MHz	
CA_1-26	1	1920 MHz	–	1980 MHz	2110 MHz	–	2170 MHz	FDD
	26	814 MHz	–	849 MHz	859 MHz	–	894 MHz	
CA_2-4	2	1850 MHz	–	1910 MHz	1930 MHz	–	1990 MHz	FDD
	4	1710 MHz	–	1755 MHz	2110 MHz	–	2155 MHz	
CA_2-5	2	1850 MHz	–	1910 MHz	1930 MHz	–	1990 MHz	FDD
	5	824 MHz	–	849 MHz	869 MHz	–	894 MHz	
CA_2-12	2	1850 MHz	–	1910 MHz	1930 MHz	–	1990 MHz	FDD
	12	699 MHz	–	716 MHz	729 MHz	–	746 MHz	
CA_2-13	2	1850 MHz	–	1910 MHz	1930 MHz	–	1990 MHz	FDD
	13	777 MHz	–	787 MHz	746 MHz	–	756 MHz	
CA_2-17	2	1850 MHz	–	1910 MHz	1930 MHz	–	1990 MHz	FDD
	17	704 MHz	–	716 MHz	734 MHz	–	746 MHz	
CA_2-29	2	1850 MHz	–	1910 MHz	1930 MHz	–	1990 MHz	FDD
	29	N/A			717 MHz	–	728 MHz	
CA_3-5	3	1710 MHz	–	1785 MHz	1805 MHz	–	1880 MHz	FDD
	5	824 MHz	–	849 MHz	869 MHz	–	894 MHz	
CA_3-7	3	1710 MHz	–	1785 MHz	1805 MHz	–	1880 MHz	FDD
	7	2500 MHz	–	2570 MHz	2620 MHz	–	2690 MHz	
CA_3-8	3	1710 MHz	–	1785 MHz	1805 MHz	–	1880 MHz	FDD
	8	880 MHz	–	915 MHz	925 MHz	–	960 MHz	
CA_3-19	3	1710 MHz	–	1785 MHz	1805 MHz	–	1880 MHz	FDD
	19	830 MHz	–	845 MHz	875 MHz	–	890 MHz	
CA_3-20	3	1710 MHz	–	1785 MHz	1805 MHz	–	1880 MHz	FDD
	20	832 MHz	–	862 MHz	791 MHz	–	821 MHz	
CA_3-26	3	1710 MHz	–	1785 MHz	1805 MHz	–	1880 MHz	FDD
	26	814 MHz	–	849 MHz	859 MHz	–	894 MHz	
CA_3-27	3	1710 MHz	–	1785 MHz	1805 MHz	–	1880 MHz	FDD
	27	807 MHz	–	824 MHz	852 MHz	–	869 MHz	
CA_3-28	3	1710 MHz	–	1785 MHz	1805 MHz	–	1880 MHz	FDD
	28	703 MHz	–	748 MHz	758 MHz	–	803 MHz	
CA_4-5	4	1710 MHz	–	1755 MHz	2110 MHz	–	2155 MHz	FDD
	5	824 MHz	–	849 MHz	869 MHz	–	894 MHz	
CA_4-7	4	1710 MHz	–	1755 MHz	2110 MHz	–	2155 MHz	FDD
	7	2500 MHz	–	2570 MHz	2620 MHz	–	2690 MHz	
CA_4-12	4	1710 MHz	–	1755 MHz	2110 MHz	–	2155 MHz	FDD
	12	699 MHz	–	716 MHz	729 MHz	–	746 MHz	
CA_4-13	4	1710 MHz	–	1755 MHz	2110 MHz	–	2155 MHz	FDD
	13	777 MHz	–	787 MHz	746 MHz	–	756 MHz	
CA_4-17	4	1710 MHz	–	1755 MHz	2110 MHz	–	2155 MHz	FDD
	17	704 MHz	–	716 MHz	734 MHz	–	746 MHz	
CA_4-27	4	1710 MHz	–	1755 MHz	2110 MHz	–	2155 MHz	FDD
	27	807 MHz	–	824 MHz	852 MHz	–	869 MHz	

CA_4-29	4	1710 MHz	–	1755 MHz	2110 MHz	–	2155 MHz	FDD
	29	N/A			717 MHz	–	728 MHz	
CA_5-7	5	824 MHz	–	849 MHz	869 MHz	–	894 MHz	FDD
	7	2500 MHz	–	2570 MHz	2620 MHz	–	2690 MHz	
CA_5-12	5	824 MHz	–	849 MHz	869 MHz	–	894 MHz	FDD
	12	699 MHz	–	716 MHz	729 MHz	–	746 MHz	
CA_5-17	5	824 MHz	–	849 MHz	869 MHz	–	894 MHz	FDD
	17	704 MHz	–	716 MHz	734 MHz	–	746 MHz	
CA_5-25	5	824 MHz	–	849 MHz	869 MHz	–	894 MHz	FDD
	25	1850 MHz	–	1915 MHz	1930 MHz	–	1995 MHz	
CA_7-20	7	2500 MHz	–	2570 MHz	2620 MHz	–	2690 MHz	FDD
	20	832 MHz	–	862 MHz	791 MHz	–	821 MHz	
CA_7-28	7	2500 MHz	–	2570 MHz	2620 MHz	–	2690 MHz	FDD
	28	703 MHz	–	748 MHz	758 MHz	–	803 MHz	
CA_8-20	8	880 MHz	–	915 MHz	925 MHz	–	960 MHz	FDD
	20	832 MHz	–	862 MHz	791 MHz	–	821 MHz	
CA_8-40	8	880 MHz	–	915 MHz	925 MHz	–	960 MHz	FDD
	40	2300 MHz	–	2400 MHz	2300 MHz	–	2400 MHz	TDD
CA_11-18	11	1427.9 MHz	–	1447.9 MHz	1475.9 MHz	–	1495.9 MHz	FDD
	18	815 MHz	–	830 MHz	860 MHz	–	875 MHz	
CA_12-25	12	699 MHz	–	716 MHz	729 MHz	–	746 MHz	FDD
	25	1850 MHz	–	1915 MHz	1930 MHz	–	1995 MHz	
CA_19-21	19	830 MHz	–	845 MHz	875 MHz	–	890 MHz	FDD
	21	1447.9 MHz	–	1462.9 MHz	1495.9 MHz	–	1510.9 MHz	
CA_20-32	20	832 MHz	–	862 MHz	791 MHz	–	821 MHz	FDD
	32	N/A			1452 MHz	–	1496 MHz	
CA_23-29	23	2000 MHz	–	2020 MHz	2180 MHz	–	2200 MHz	FDD
	29	N/A			717 MHz	–	728 MHz	
CA_39-41	39	1880 MHz	–	1920 MHz	1880 MHz	–	1920 MHz	TDD
	40	2496 MHz	–	2690 MHz	2496 MHz	–	2690 MHz	

Table 2-4: Inter-band CA operating bands (extracted from 3GPP TS36.141)

2.2.1 LTE Downlink

Orthogonal Frequency Division Multiple Access (OFDMA) scheme is the transmission scheme used for LTE-FDD and LTE-TDD operational modes in the downlink. In an OFDM system, the total available spectrum is divided into multiple carriers. These carriers are called subcarriers. Each of these subcarriers is independently modulated by a low rate data stream. This implies that each subcarrier carries a separate stream of information which causes the information to be mapped in both the time and frequency domains. The OFDM time-frequency lattice, a two-dimensional grid used to represent how information is mapped to both, the subcarrier and the OFDM symbol are shown in Fig. 2-1. The channel delay spread causes inter-symbol-interference (ISI). The guard intervals are added to each symbol in the time domain to tackle the ISI problem.

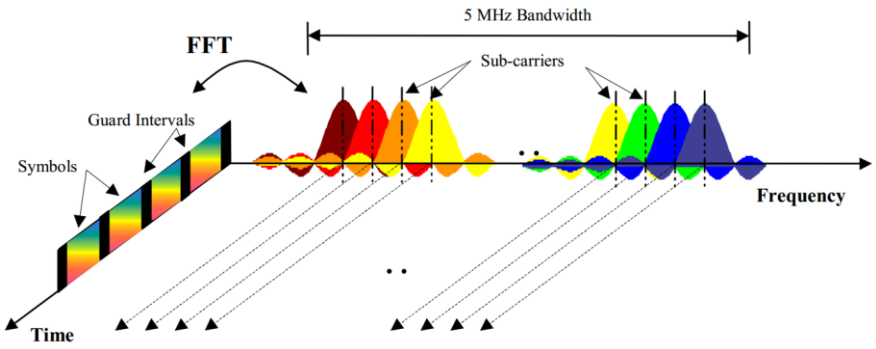

Fig. 2-1: Frequency- Time representation of an OFDM signal [2]

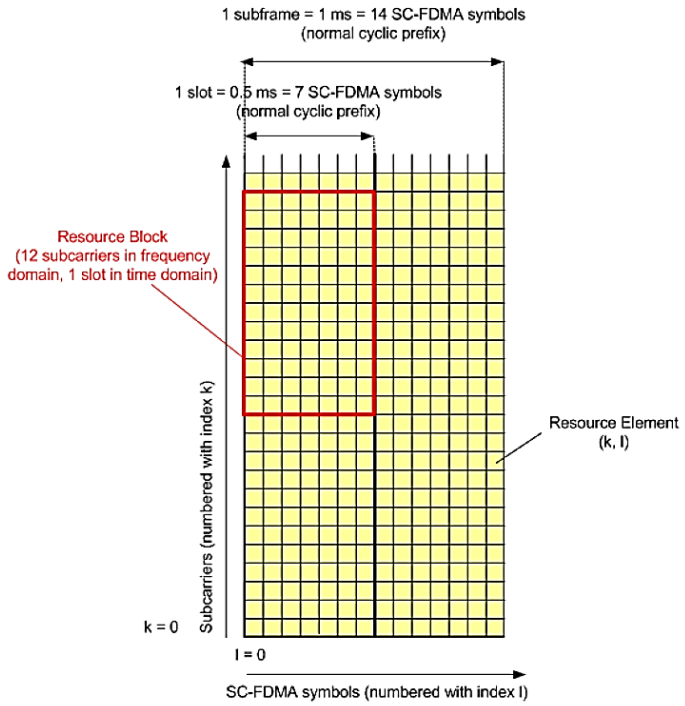

Fig. 2-2: Formation of a resource grid [1]

Fig. 2-2 shows the content of a resource grid. Each single element in the resource block is called a Resource Element (RE). A resource block consists of 12 consecutive subcarriers in the frequency domain and 7 OFDM symbols in the time domain [3]. This technique of mapping information into blocks with regard to time and frequency makes it possible for the interference or jamming to be selective with regards to information.

2.2.1.1 OFDM Signal Generation

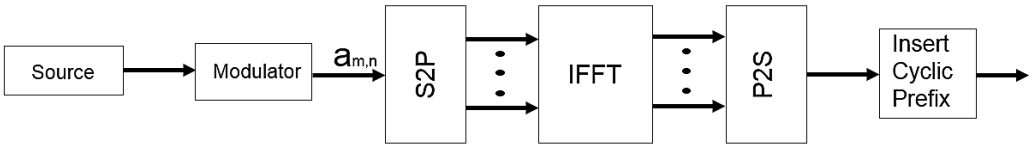

Fig. 2-3: Block diagram of OFDM signal generation

The OFDM signal is generated using Inverse Fast Fourier Transform (IFFT) digital signal processing. The IFFT converts a number N of complex data symbols used as frequency domain bins into the time domain signal. In Fig. 2-3, the serial stream of modulated signals ($a_{m,n}$) are mapped to N parallel streams by the S2P block and are used as frequency domain bins for the IFFT. The parallel stream of N sources of data, each one independently modulated, a waveform composed of N orthogonal subcarriers is obtained. Each subcarrier has the shape of a frequency sinc (sin(x) / x) function as shown in Fig. 2-1.

The N-point time domain blocks obtained from the IFFT are then serialized (by P2S block) to create a time domain signal. To each OFDM symbol, a cyclic prefix (CP) (Fig. 2-3) is appended as guard interval (Fig. 2-1), to avoid the effect of the previous symbol partially still arriving at the receiver during reception of the following symbol, CP are used. The length of the CP depends on delay spread which in turn is roughly a function of the cell size. The "Extended Cyclic Prefix" is able to cover larger cell sizes with higher delay spread of the radio channel.

2.2.1.2 OFDMA Parameterization

Two frame structure types are defined for E-UTRA: frame structure type 1 for FDD mode, and frame structure type 2 for TDD mode. The E-UTRA frame structures are defined in [3]. For the frame structure type 1, the 10 ms radio frame is divided into 20 equally sized slots of 0.5 ms. A subframe consists of two consecutive slots, so one radio frame contains ten sub frames. This is illustrated in Fig. 2-4.

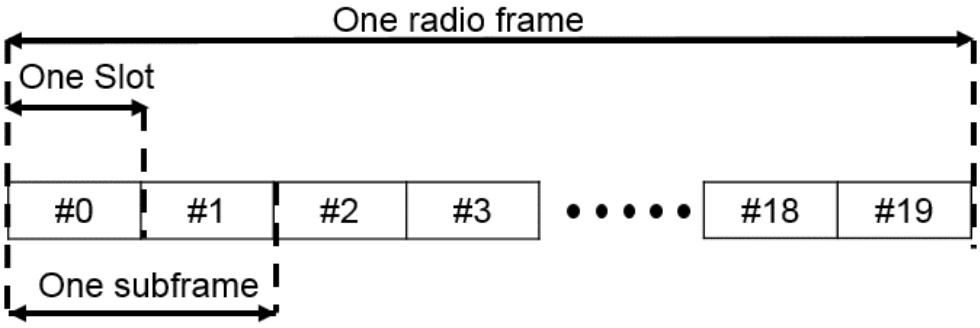

Fig. 2-4: Frame structure type 1 [3]

For the frame structure type 2, the 10 ms radio frame consists of two half-frames of length 5 ms each. Each half-frame is divided into five sub-frames of each 1 ms, as shown in Fig. 2-5 below. All sub-frames which are not special sub-frames are defined as two slots of length 0.5 ms in each subframe. The special sub-frames consist of the three fields DwPTS (Downlink Pilot Timeslot), GP (Guard Period), and UpPTS (Uplink Pilot Timeslot). DwPTS, GP and UpPTS have configurable individual lengths and a total length of 1ms.

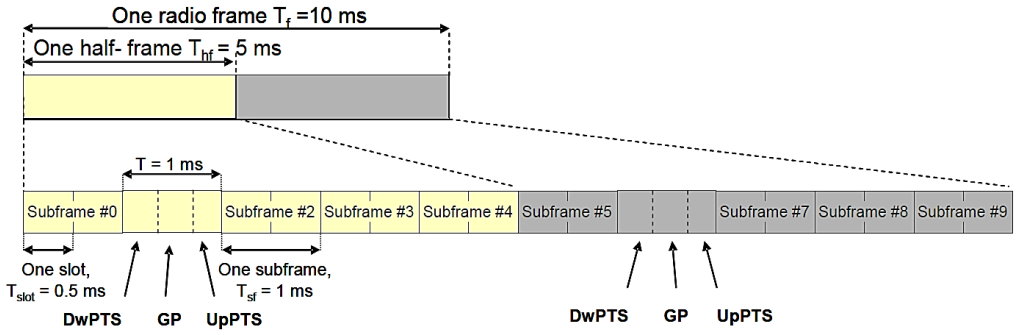

Fig. 2-5: Frame Structure Type 2 [3]

2.2.1.3 Downlink Data Transmission

Data is allocated to a device (User Equipment, UE) in terms of resource blocks, i.e. one UE can be allocated integer multiples of one resource block in the frequency domain. These resource blocks do not have to be adjacent to each other. In the time domain, the scheduling decision can be modified every transmission time interval of 1

ms. All the scheduling decisions for downlink and uplink are done in the base station (enhanced NodeB, eNodeB or eNB). The scheduling algorithm has to take into account the radio link quality situation of different users, the overall interference situation, Quality of Service requirements, service priorities, etc. and is a vendor-specific implementation [4].

2.2.2 LTE Uplink

Extensive research has been carried out to find the optimum uplink transmission scheme. OFDMA has shown to satisfy the downlink requirements with good performance but unfortunately was less favorable for the uplink channels. The problem is mainly because OFDMA comes with a high peak-to-average power ratio (PAPR). The high peak power demands large RF output stages even for medium average output. That is less suited to battery powered devices. Smaller amplifiers satisfy battery runtime constraints, but then average power is too low to allow for a good uplink coverage area.

The chosen LTE uplink transmission scheme for FDD and TDD mode of operation is based on SC-FDMA (Single Carrier Frequency Division Multiple Access) with cyclic prefix. SC-FDMA signals have lower PARP compared to an OFDMA signal. SC-FDMA signal processing has some similarities with OFDMA signal processing, so parameterization of downlink and uplink can be harmonized.

2.2.2.1 SC-FDMA Signal Generation

There are different ways of generating an SC-FDMA signal. Discrete Fourier Transform-spread-OFDM (DFT-s-OFDM) has been selected for E-UTRA. The principle is illustrated in Fig. 2-6. For DFT-s-OFDM, a size-M DFT is first applied to a block of M modulation symbols. QPSK, 16QAM and 64QAM are used as uplink E-UTRA modulation schemes, the latter being optional for the user equipment (UE). The DFT transforms the modulation symbols into the frequency domain. The result is mapped onto the available number of subcarriers. An N-point IFFT where N>M is then performed as in OFDM. This step is followed by the addition of the cyclic prefix and parallel to serial conversion.

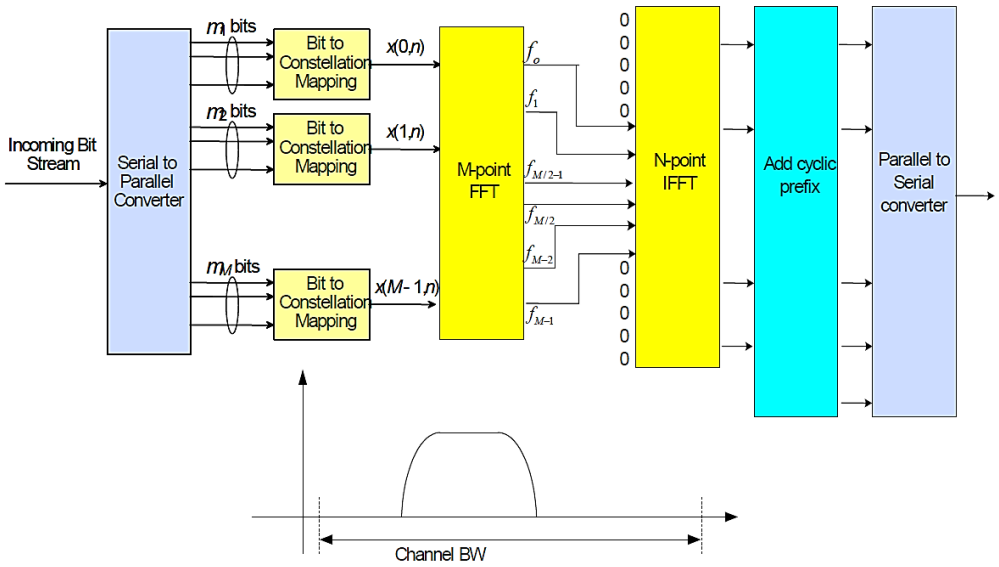

Fig. 2-6: Block diagram of DFT-s-OFDM

The DFT processing is therefore the fundamental difference between SC-FDMA and OFDMA signal generation. This is indicated by the term "DFT-spread-OFDM". In an SC-FDMA signal, each subcarrier used for transmission contains information of all transmitted modulation symbols, since the input data stream has been spread by the DFT transformation over the available subcarriers. In contrast to this, each subcarrier of an OFDMA signal only carries information related to specific modulation symbols. This spreading is a central reason for lower the PAPR compared to OFDMA.

2.2.2.2 SC-FDMA parameterization

The LTE uplink structure is similar to the downlink. In frame structure type 1, an uplink radio frame consists of 20 slots of 0.5 ms each, and one subframe consists of two slots. Frame structure type 2 consists also of ten sub-frames with special sub-frames. They include DwPTS, GP and UpPTS fields as shown in Fig. 2-5. Each slot carries 7 SC-FDMA symbols in case of normal cyclic prefix configuration and 6 SC-FDMA symbols in case of extended (large cell) cyclic prefix configuration. SC-FDMA symbol number 3 (i.e. the 4th symbol in a slot) carries the demodulation reference signal (DMRS), being used for coherent demodulation at the eNodeB receiver as well as channel estimation.

2.2.2.3 Uplink Data Transmission

Scheduling of uplink resources is done by eNodeB. The eNodeB assigns certain time/frequency resources to the UEs and informs UEs about transmission formats to be used. The scheduling decisions may be based on QoS parameters, UE buffer status, uplink channel quality measurements, UE capabilities, UE measurement gaps, etc. In the uplink, data is allocated in multiples of one resource block. Uplink resource block size in the frequency domain are 12 subcarriers, i.e. the same as in downlink. However, not all integer multiples are allowed in order to simplify the DFT design in the uplink signal processing and so only factors 2, 3, and 5 are allowed.

2.2.3 LTE Control and Signaling

It is possible to disturb LTE service intentionally and also unintentionally (interference). Interference can be from sources fully adhering to national or regional emission limits, as e.g. from hardware operated in license-free bands, or by means of radiation from malfunctioning equipment. No matter whether a task is to defend or manipulate LTE communication, it is important to know about LTE physical channels and physical signals in order to more efficiently address the challenge. There are many ways of unintentionally jamming LTE signals or jamming them with brute force attacks. Smarter jamming techniques can only be applied when information about the channel and the signal are available. The same goes for a responsible risk evaluation.

To get a mathematical value on the efficiency of a jamming technique, two figures of merit are important. One is the jammer-to-signal ratio (J/S). In case of smart jamming, only certain subcarriers and certain OFDM symbols where the data traffic is high are jammed. In this case, it is useful to measure the jammer-to-signal ratio per resource element ($J/S_{Resource\text{-}element}$) instead of the more general J/S. A highly efficient jammer would have a lower J/S ratio compared to the J/S for barrage jamming (explained in section 3.1). This means a signal does not need to have a high signal power to block LTE communication.

The second figure of merit is the Bit Error Rate (BER) or Block Error Rate (BLER). The BLER required in order to corrupt a received LTE channel is worth a more in-depth look.

2.2.3.1 Physical Channels

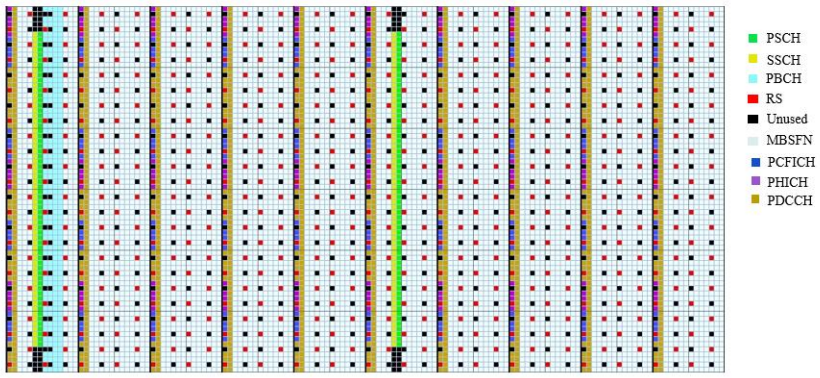

Fig. 2-7: Resource grid for the downlink of LTE [19]

Fig. 2-7 illustrates the positioning of all the physical control channels in the downlink of LTE.

1. Physical Downlink and Uplink Shared Channel

The user data is carried to the eNodeB on the Physical Downlink Shared Channel (PDSCH) and from the eNodeB on the Physical Uplink Shared Channel (PUSCH). Adaptive modulation and coding scheme are used by both channels [3].

The authors in [6] have shown in case there is a presence of an interferer or a jammer, even with a coding rate of 1/15, the BLER is calculated to be 0.1 and the Signal to Noise (SNR) ratio is -7 dB. This means the number of retransmissions will be significant.

QPSK modulation scheme was used for both OFDM and SC-FDMA case in [6] for a typical urban channel with the threshold of $J/S_{Resource\text{-}element}$ estimated at 7 dB.

2. Physical Control Format Indicator Channel

The UE information regarding the location of the Physical Downlink Control Channel (PDCCH), in the frequency-time lattice is sent via the Physical Control Format Indicator Channel (PCFICH). In the case that there was a problem with the decoding of this information, the UE will not be able to locate the PDCCH and so it becomes impossible to get the resource allocation information of the UE.

The PCFICH is transmitted only one symbol per subframe and 16 sub carriers are oiccupied. Jamming the PCFICH successfully would means to transmit on top of the 16 subcarriers. The location of the subcarriers are not static, it is determined by the eNodeB's complete cell ID [3]. This id is embedded in the Primary Synchronization Signal (PSS) and Secondary Synchronization Signal (SSS). And therefore selectively jamming the PCFICH means that the jammers needs to synchronize to both of the downlink synchronization signals. The PCFICH jamming attack can be performed to only a single cell [5].

A two bit indicator information is carried on the PCFICH and the encoder uses a coding rate of 1/16. A successful jamming attack would require the transmitted a signal with

power level to be high enough to cause a BER near 0.5 [5]. A study [7] has shown that, by using BPSK as the modulation scheme in AWGN channel, with a code rate of 1/16, a block code can be decoded at a SNR of at least -1.5 dB. So the threshold of $J/S_{Resource\text{-}element}$ needs to be at least 1.5 dB.

3. Physical Uplink Control Channel

Hybrid Automatic Repeat Request (HARQ) acknowledgements and channel quality indicators (CQI) are transmitted to the base station via the Physical Uplink Control Channel (PUCCH). The PUCCH is normally assigned almost at the end of the system bandwidth for every resource block [5]. Thus making it possible for the PUCCH jamming only when there is a priori knowledge of the LTE system bandwidth and center frequency.

If an uplink channel with a BW of 10 MHz is considered, around 192 subcarriers or about 16 resource blocks is assigned to PUCCH. Around 30% of the uplink bandwidth needs to be jammed for a successful attack.

The authors of [8], have shown an AWGN channel with BPSK modulation and 1/3 coding rate, around 2 dB of SNR and a BER of 0.1 can be reached. The threshold of $J/S_{Resource\text{-}element}$ needs to be at least -2 dB.

4. Physical Broadcast Channel

The UE first synchronizes with the Primary Synchronization Signal (PSS) and Secondary Synchronization Signal (SSS). After that, the UE receives information about the cell by decoding the Master Information Block (MIB). The MIB is transmitted on the Physical Broadcast Channel (PBCH). The PBCH is transmitted using QPSK modulation scheme. A combination of repetition coding and convolutional coding, generates four self-decodable units, each with a coding rate of 1/12 and a combined coding rate of 1/48 [5].

The authors in [7], have shown an AWGN channel with un-coded QPSK signal reach a BER of 0.1 at 0 dB SNR. Therefore, the $J/S_{Resource\text{-}element}$ threshold for the PBCH is estimated to be 0 dB. Fig. 2-8 and Fig. 2-9 shows the position of the PBCH, PSS and SSS in the frame for both FDD and TDD types.

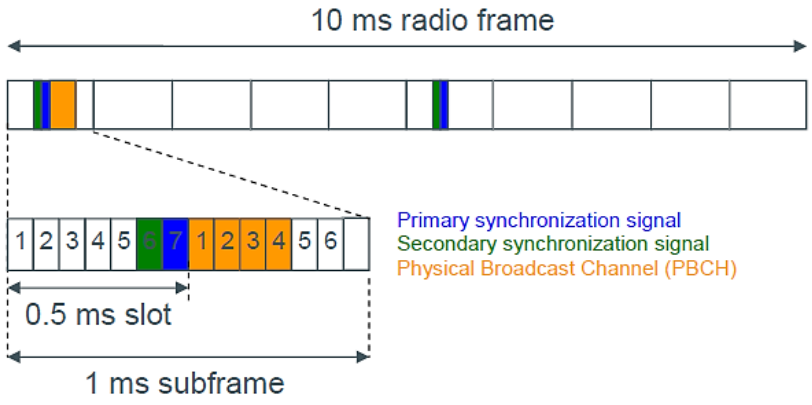

Fig. 2-8: PSS, SSS and PBCH structure (frame structure type 1 / FDD with normal CP)

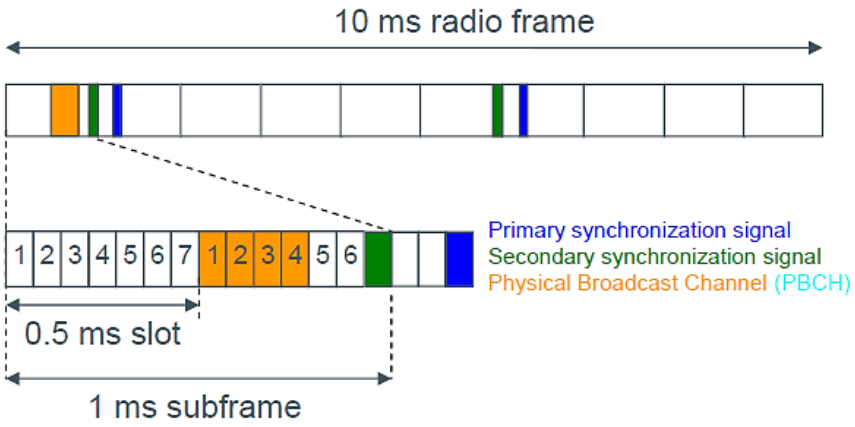

Fig. 2-9: PSS, SSS and PBCH structure (frame structure type 2 / TDD with normal CP)

5. Physical Hybrid-ARQ Indicator Channel

According to the 3GPP technical report, the BPSK is used by PHICH in combination to repetition-3 coding [3]. A BER of 0.1 and an SNR of 2 dB was obtained with the threshold of the $J/S_{Resource\text{-}element}$ being roughly at -2 dB [5, 7].

2.2.3.2 Physical Layer Signals

1. **Primary and Secondary Synchronization Signals**

In accessing a cell, the UE first synchronizes with the Primary Synchronization Signal (PSS) and Secondary Synchronization Signal (SSS). A complex-valued Zadoff-Chu (ZC) sequence is used for the generation of the PSS [10]. There are three PSS sequences used in LTE. The requirement of the power level of the jamming signal in order to jam the PSS is high, since the PSS can be detected even at high levels of interference. The intention is that the UE can be detected by the neighboring cells. A smarter PSS jamming strategy is to transmit all of the three PSS sequence, making the UE unable to synchronize with the eNb. If the power level of the jammer at the receiver of the UE is larger than the power level of the real LTE base station, the UE will connect to the bogus base station. This gives rise to the concept of spoofing. According to the author in [5], around 3 dB of $J/S_{Resource\text{-}element}$ is enough to corrupt the synchronization of UE. This technique of spoofing does not mean that this cause a denial of service (DOS) to the UE in operation in the cell. However, the new UE that enters the cell or the UEs in idle state will synchronize with the bogus base station.

UEs are designed to recognize bogus PSS signals because of the blacklisting mechanism that is installed in them. However, it is still possible to “confuse” the UE by corrupting the SSS. This is because after synchronizing with the valid PSS, the UE needs to also synchronize with the SSS to access the LTE network. The SSS is a BPSK modulated signal providing information such as TDD/FDD configuration, cell group ID, timing information and CP length. Jamming the SSS is not an optimum jamming strategy as it requires synchronizing with a cell, figuring out the SSS transmit sequence and them transmitting the bogus SSS sequence for launching a successful jamming attack.

2. **Downlink Reference Signals**

Pilot tones or reference symbols are periodically transmitted in LTE in order to perform channel estimation and frequency-domain equalizations. According to the 3GPP technical specifications for LTE, these signals are known as Reference Signals (RSs). Both frequency and time domain multiplexing are performed in the downlink for RSs (Fig. 2-7). In a frame, about 14% of the RE is filled up by the reference signals [5]. The cell ID determines the time and frequency domain locations QPSK modulated RSs. A study has shown, in order to obtain higher BER, it is more effective to jam a subcarrier containing RSs rather than a subcarrier that carries only data [11]. For successful RS jamming, synchronization with the base station is required. A simulation of this kind of jamming attack is described in [11], where the authors obtained a BER of 0.1 by using $J/S_{Resource\text{-}element}$ of -5 dB. The simulated system uses a QPSK signal with a pilot density of 1/8.

3 Jamming Techniques

Wireless communication systems are not deployed in ideal environment. The channels are subject to unwanted interference from other services operating in the adjacent frequency bands. There are also cases of jamming attempts on the network. This causes the performance of the network to degrade. In this chapter certain conventional jamming techniques, as well as certain new, smarter and more power efficient jamming techniques have been discussed.

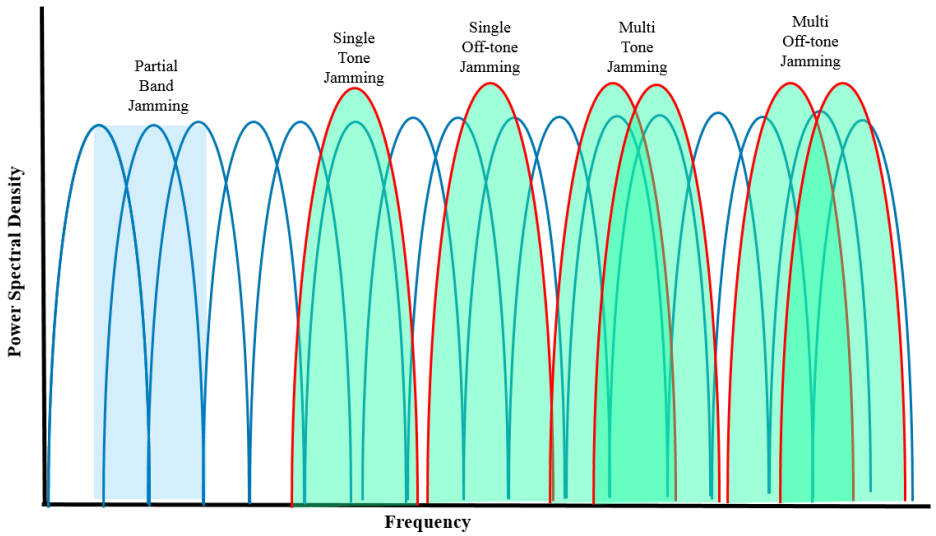

Fig. 3-1: Different jamming attacks on LTE downlink [13]

3.1 Barrage Jamming (BJ)

Barrage jamming is the most basic form of jamming technique. This is very effective when there is no a-priori knowledge of the network. The entire spectrum of the target signal is jammed by transmitting band-limited noise to the system. This means that the SNR decreases over the entire bandwidth. BJ is the most in-efficient method of jamming as this requires a lot of power, but is taken as a baseline for comparing the efficiency of other forms of jamming attacks and the corresponding effectiveness. More information on BJ analysis can be found in [12]. Fig. 3-1 presents the spectrum for barrage jamming attack.

3.2 Partial Band Jamming (PBJ)

Partial band jamming is a technique where a certain portion of the entire system bandwidth (BW) is targeted and jammed by transmitting AWGN over this specific BW. When the power of the jamming signal is constant, the effectiveness of the jamming depends directly on the fraction of jamming BW and the signal BW. More information on PBJ can be found in [12, 13]. In Fig. 3-1 , the part of the spectrum effected by PBJ can be seen.

3.3 Single Tone Jamming (STJ)

In single tone jamming (STJ), a single high powered impulse of AWGN noise is transmitted to the jam only a certain band of interest. In the LTE downlink, only single subcarriers can be jammed using STJ technique.

Fig. 3-1 shows the effect of STJ on the spectrum. STJ can also be considered as a special case of PBJ. A more analytical investigation of the STJ can be found in [12]. In STJ, the knowledge of the target systems carrier frequency is required in order to jam the target signal.

3.4 Multi Tone Jamming (MTJ)

Multi tone jamming (MTJ) is another form of PBJ. Unlike STJ, multiple numbers of equally powered noise are transmitted in order to take down a multiple number of frequency subcarriers within the LTE bands. MTJ attack is highly effective when there is a power limitation on the transmit side. This means if there is a strict limitation on the transmit power, an increase in the number of transmitted tones will decrease the power associated with the individual transmitted jamming tones. A detailed analysis of the effect of MTJ on OFDM can be found in [14].

Fig. 3-1 shows an illustration of the MTJ attack on the spectrum. In MTJ, the knowledge of the target systems carrier frequency is required.

3.5 Asynchronous Off-Tone Jamming (AOTJ)

There is two types of Asynchronous Off-Tone Jamming (AOTJ). The first type is called single off-tone jamming and the second type is multiple off-tone jamming attack. The operational concept of this technique is to transmit asynchronous off-tones which are not perfectly periodic or have an offset at the sampling frequencies. As a result, the energy gets smeared from the true frequency into the adjacent frequency bins and thus creating inter channel interference (ICI) of the OFDM signal at the receiver [13]. Also the side-lobes of the signal (sinc function) not aligned with the orthogonal OFDM subcarriers due to frequency offset can have non-zero components at the sampling period that can be a source of ICI . One advantage of AOTJ is that the jamming signal does not need frequency matching with target signal and any channel state information (CSI). AOTJ has much more superior performance than BJ, STJ and MTJ. The example of the two types of AOTJ can be seen in Fig. 3-1.

3.6 Pilot Tone Jamming and Pilot Tone Nulling

In pilot tone jamming, the jammer needs to be perfectly synchronized with the target signal. This is done through observation of communication between all the parties involved in the network. A vector jammer signal Zi where Zi = 0 for the non-pilot sub carriers and for the pilot tones, Zi = qi, which is an independent and identically distributed (i.i.d) AWGN [11]. If this AWGN sequence is coherently transmitted on all pilots simultaneously, then the noise is not averaged out for linear combinations.

In case of pilot tone nulling, it is also important to know the channel. The transmitter transmits a signal which is channel-corrected, π-radian phase shifted of the pilot tone. This causes the original pilot tone to cancel out and thus degrades the performance of the network.

4 Co-existence with other services

4.1 Co-existence of LTE and S-band Radar

Air traffic control (ATC) radar, military Air Traffic Surveillance (ATS) radar and meteorological radar operate in the S-band frequency range. In fact 4G communication system (LTE) make also the same frequencies. Test and measurement of their co-existence is absolutely essential as performance degradation of mobile device and networks have been proven.

Table 2-1 lists the LTE frequency bands for FDD and TDD mode of operation.
The bands 1, 4, 7, 10, 22, 23 and 30 are fairly close to any operational S-Band radar system.

LTE base stations (eNodeB) may be disturbed through radar systems. Depending on the ATC or ATS radar system, a power of up to 7000 MW EIRP is transmitted. The blocking requirements of the LTE base stations and UEs have to also comply with these figures, by taking into account the distance of the BS or UE. TS36.141 defines the blocking performance requirement for wide area BS as described Table 4-1.

Operating Band	Centre Frequency of Interfering Signal [MHz]	Interfering Signal mean power [dBm]	Wanted Signal mean power [dBm]	Interfering signal centre frequency minimum frequency offset from the channel edge of the wanted signal [MHz]	Type of Interfering Signal
1-7, 9-11, 13-14, 18,19,21, 24, 33-43	(F_{UL_low} -20) to (F_{UL_high} +20)	-35	$P_{REFSENS}$ +6dB*	See table 7.6-2	See table 7.6-2
	1 to (F_{UL_low} -20) (F_{UL_high} +20) to 12750	-15	$P_{REFSENS}$ +6dB*	—	CW carrier

Table 4-1: Blocking performance requirement for Wide Area BS [16]

The user equipment (UE) may even be closer to a radar system. According to [16], out-of-band blocking parameters are defined as shown in Table 4-2.

E-UTRA band	Parameter	Units	Frequency			
			range 1	range 2	range 3	range 4
	$P_{interferer}$	dBm	-44	-30	-15	-15
1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43	$F_{interferer}$ (CW)	MHz	F_{DL_low} -15 to F_{DL_low} -60	F_{DL_low} -60 to F_{DL_low} -85	F_{DL_low} -85 to 1 MHz	-
			F_{DL_high} +15 to F_{DL_high} + 60	F_{DL_high} +60 to F_{DL_high} +85	F_{DL_high} +85 to +12750 MHz	-
2, 5, 12, 17	$F_{interferer}$	MHz	-	-	-	F_{UL_low} - F_{UL_high}
Note: For the UE which supports both Band 11 and Band 21 the out of blocking is FFS.						

Table 4-2: Out-of-band blocking parameters [16]

In 3GPP TS36.521-1 [16] the test purpose of "TC 7.6.2 Out-of-band blocking" is described with an "Unwanted CW interfering signal falling more than 15 MHz below or above the UE receive band, at which a given average throughput shall meet or exceed

the requirement…". Under minimum conformance requirements the throughput is mentioned to be "≥95% of the maximum throughput of the reference measurement channel".

As shown in several measurements, disturbance of LTE networks occurs through S-Band radar, such as degradation of performance due to lower throughput indicated by an increasing block error rate (BLER). Throughput reduction is unlikely, but not a major drawback. However spectral efficiency, power reduction and costs are of great importance for any mobile network operator. Therefore disturbance through other signals is therefore of great interest.

Unlike mobile communication, radar is not defined by a global specification. Thus, many different systems applying different waveforms, frequencies and bandwidth are deployed and operate nearly autonomously to detect the desired kind of target. For a radar engineer, bandwidth is also one of the key parameters when defining the radar system, as bandwidth defines range resolution. Depending on the radar, bandwidth can range from nearly zero (just a carrier frequency, CW radar) to measure radial velocity up to several GHz for high resolution range measurements (e.g. Ultra Wideband Radar, UWB).

The 2.7 GHz to 2.9 GHz frequency band is primarily allocated to aeronautical radio navigation, i.e. ground based fixed and transportable radar platforms for meteorological purposes and aeronautical radio navigation services. Operating frequencies of these radars are assumed to be uniformly distributed throughout S-Band [4]. The two frequency bands for mobile communication and aeronautical radio navigation are very closely located and so the coexistence problem also needs special attention.

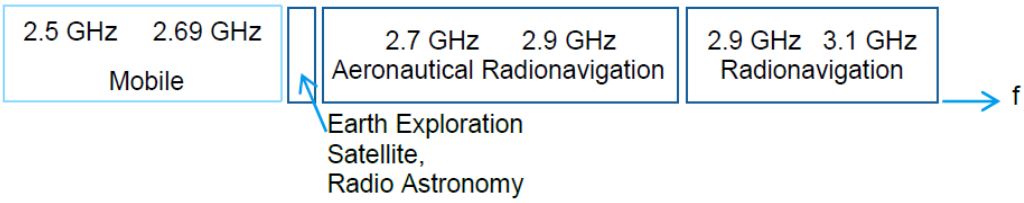

Fig. 4-1: International Telecommunication Union Radio (ITUR) regulations in the band of 2.5 GHz to 3.1 GHz [3]

In the application note 1MA211 [4], a more detailed investigation of the co-existence problem has been described. It also talks about the potential issues concerning S-Band radar systems and LTE signals from base stations / mobile devices operating close-by. It addresses frequency allocation of these systems, explains the performance degradation or malfunction that can be expected and describes test and measurement solutions for interference test of radar and LTE networks in detail.

4.2 Co-existence with LTE and Digital TV

LTE operates alongside with broadcast applications in the same frequency range. As a result, numerous coexistence scenarios are possible. So network operators and manufacturers from both the mobile radio and the broadcast sector have a vital interest in avoiding any interference and performing in-depth testing of their products.

Digital broadcast TV standards typically occupy the frequency ranges from 174 MHz to 230 MHz (VHF) and 470 MHz to 862 MHz (UHF). They can be roughly classified in three different areas:

- Mobile broadcast
- Terrestrial broadcast
- Cable broadcast

Table 4-3 shows the current status of the digital TV frequency bands. In order to achieve the data rates needed, e.g., for high definition (HD) television, today's

Overview of digital TV standards						
Technology		Frequency range				Region
		174 MHz to 230 MHz VHF	470 MHz to 862 MHz UHF	1452 MHz to 1492 MHz L-Band	S-Band	
Mobile	DVB-H, DVB-SH	X	X		2170 MHz to 2220 MHz	Europe
	ISDB-T1 Seg	X	X			Japan South America
	MediaFLO™		X			USA
	T-DMB		X	X		Korea
	ATSC-M/H		X			USA
	CMMB	X	X		2635 MHz to 2660 MHz	China
Terrestrial	ATSC		X			USA, Korea
	DVB-T/T2	X	X			Europe
	DTMB	X	X			China
	ISDB-T		X			Japan South America
Cable	DVB-C/C2	X	X			Europe
	J.83/B	X	X			USA
	ISDB-C	X	X			Japan

Table 4-3: Overview of digital TV standards

standards use orthogonal frequency division multiplexing (OFDM), higher-order modulation from 16QAM up to 256QAM (with even higher orders planned), channel bandwidths of up to 8 MHz and encoding techniques such as MPEG-4 and H.264.

LTE also operates in the frequency bands that are already available for existing 3G networks. Moreover, additional ranges such as the 2.5 GHz to 2.7 GHz band (Europe/Asia) and the 700 MHz band (USA) are available for use. LTE bands 5, 12, 13, 14, 17, 19 and 20 overlaps with digital TV bands and should be checked for vulnerabilities. In this coexistence scenario, the digital TV transmitter may act as interferer on the cellular system LTE. Depending on the spectrum situation, the LTE base station receiver or the LTE terminal receiver could be impacted. If the LTE system and the digital TV system are operated in different frequency bands, this coexistence scenario will never be a co-channel scenario. A more detailed discussion on the issue can be found in [17].

4.3 In-Device Interference and Co-existence

With the ever growing usage of various wireless technologies and services, the UE are integrated with multiple radio transceivers designed to operate with multiple standards such as LTE, Wi-Fi, Bluetooth (BT) and Global Navigation Satellite Systems (GNSS), simultaneously. This means, the in-device co-existence interference becomes a matter of concern due to the extreme proximity of multiple transceivers within the same device which can potentially interfere with each other.

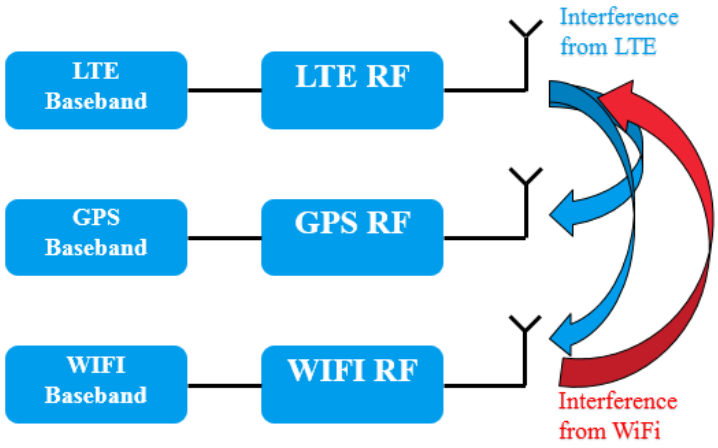

Fig. 4-2: Co-existence interference in a UE device supporting LTE, GPS and WI-FI

The extreme proximity of collocated radios due to small form factor of the UE and the scarcity of spectrum are the main points that account for this problem. When these radio technologies within the same UE are working on adjacent frequencies or sub-harmonic frequencies, interference power due to out-of band emission from a transmitter of one radio may be much higher than the signal strength of the desired signal for a receiver of a collocated radio. This situation is known as in-device co-existence interference [18].

Fig. 4-2 shows one situation where a UE supports multiple standards. The LTE signals undergo interference between different co-located radio transceivers. The WIFI does not interfere with GPS but has interference with Band 7 and 41 of LTE.

5 Mitigation Techniques

As discussed in the previous section, there are various jamming techniques as well as unwanted interference that plays a role in the degradation of the performance of the LTE communication system. This is important to know when looking at civil-governmental as well as military communication systems, which must be robust both in circumstantial as well as in hostile jamming scenarios. Therefore, keeping all the discussed techniques in mind, a few schemes already exist or offer themselves for jamming mitigation.

5.1 Jamming Mitigation

One of the most basic way of mitigating the unwanted interference is to rely on radio frequency (RF) techniques, such as sufficient filtering or isolation. Unfortunately, the current state-of-the-art filter technology cannot provide sufficient interference rejection. This gives rise to necessity to find better mitigation schemes.

Certain interference and jamming mitigation schemes such as Frequency Division Multiplexing (FDM) based solutions, Time Division Multiplexing (TDM) based solutions, transmit power control solutions and frequency hopping solutions are very popular.

5.1.1 FDM based solution

The basic idea is to shift LTE or ISM signals away from an interfering band via the frequency domain. This can be done by performing inter-frequency handover within E-UTRAN or by removing secondary cells (SCells) from the set of serving cells as shown in Fig. 5-1.

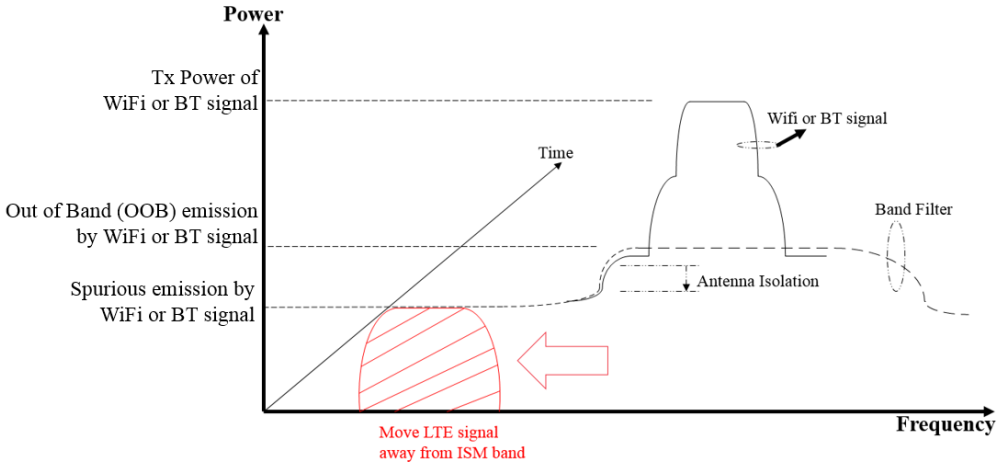

Fig. 5-1: Moving LTE signal away from ISM band [18]

5.1.2 TDM based solution

The basic idea is shown in Fig. 5-2. This solution relies on avoiding the overlapping of signal transmission in the time domain. In LTE, a discontinuous reception (DRX) mechanism can provide TDM patterns for the scheduling of LTE transmissions.

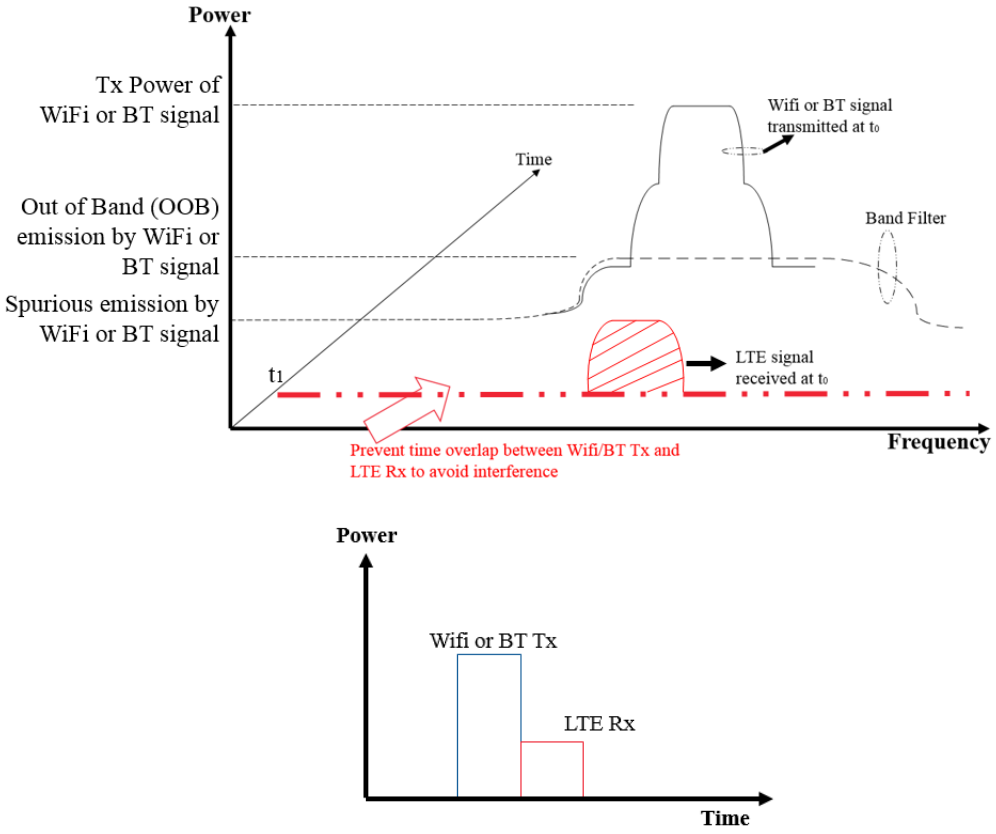

Fig. 5-2: Time division multiplexing for co-existence interference avoidance

5.1.3 Transmit Power Control Solution

This solution relies on reducing the power of the transmitting signal (LTE or ISM) in order to mitigate interference on the other receivers. Fig. 5-3 shows a graphical depiction of the solution. Reducing the transmit power also means a reduction in the size of the coverage area.

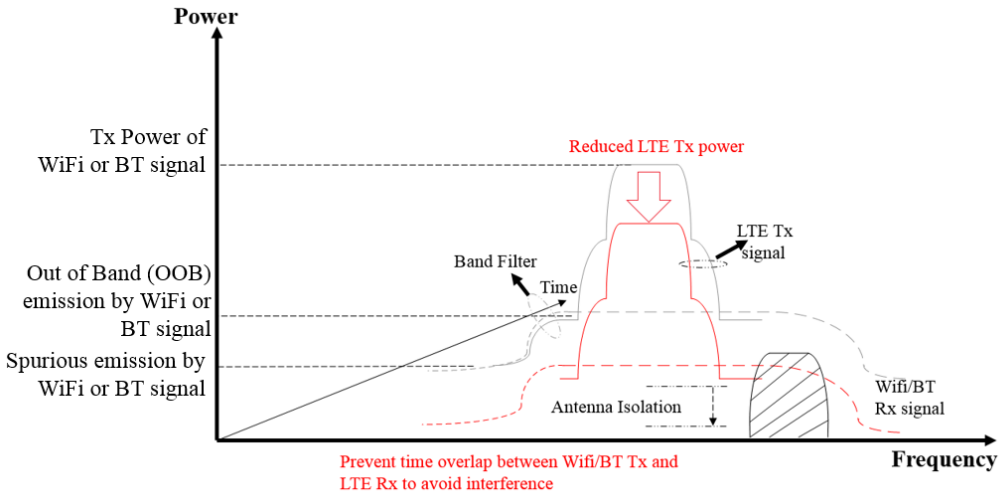

Fig. 5-3: LTE power control for co-existence interference mitigation

Furthermore, in some cases the UE can autonomously deny ISM transmission in order to protect important LTE signaling (e.g. RRC connection configuration).

5.1.4 Frequency Hopping (FH) Solution

Frequency hopping (FH) system is widely used to mitigate the effects of hostile jamming. FH is mainly limited by the collision effect and the spectral efficiency of the FH system is very low. In order to develop the spectrally efficient of the FH systems, a space-time coded collision-free frequency hopping scheme based on the OFDM framework and a secure subcarrier assignment algorithm exists where each user hops to a different set of subcarriers in a pseudo-random manner at the beginning of each new symbol period and at each symbol period, different users always transmit on non-overlapping sets of subcarriers thus making the FH scheme collision-free.

Frequency hopping has also been considered in cases where there is significant additional available bandwidth for use. However, it is very difficult to overcome the impact of active jamming, especially when jammers acquire the inherent properties of MAC layer protocols. There is a mitigation scheme known as the subcarrier-level radio agility. This is based on the concept that jamming signals are likely to experience varying levels of fading on different OFDM subcarriers. As a result, some subcarriers may not be significantly affected by the malicious power emission. As long as a transceiver pair is made aware of which these subcarriers are, these subcarriers could be temporarily used for legitimate packet transmissions,

Thus, a framework is created that allows a transceiver pair to exchange information about these unaffected subcarriers in the available spectrum, where the jamming signal experiences significant fading. Once such subcarriers are identified, the maximum allowed transmit power are assigned to these channels, and utilize them for packet transmissions to increase the probability of successful packet delivery and thereby increasing the long-term throughput (while being actively jammed).

5.2 Co-existence Problem Mitigation Techniques

Different approaches can mitigate disturbances on radar and 4G base stations. One approach is to reduce transmit power at the base station and radar. Also increasing frequency separation or distance between the two services is a solution. However, these two ideas reduce maximum range of the radar and coverage of the base station and frequency selection may be impossible due technical restrictions. Avoiding to let mobile service base station antennas point at towards S-Band radar is one approach to mitigate. Also, the improvement of receiver selectivity, filtering of transmitter signals, and reduction of unwanted spurious emissions on both sides allows coexistence.

The latter would be the most straightforward mitigation measure, both at the radar and base station (BS) side. To avoid receiver saturation through inter-modulation and blocking a filter can be placed on the radar's receiver before the Low Noise Amplifier (LNA). At the BS side, a filter can be placed on the transmitter close to the antenna to suppress the out-of-band (OOB) LTE emissions in the spurious domain. Furthermore, a revision of the ETSI 3GPP technical specifications TS 136.101 (UE) and TS 136.104 (BS) is recommended. Currently, these standards impose flexible power levels for Spurious Emissions in non-protected bands, while these levels are much more stringent in the protected bands. Because the S-band (and also the L-band) is used for security and safety services a more stringent maximum power level for Spurious Emissions should be defined.

In any case, test and measurement of radar, LTE base stations and user equipment is necessary to confirm spectral emission masks and prove robustness against other co-existing signals [4]. Off-the shelf test & measurement equipment as well as dedicated test systems to characterize susceptibility to interference and jamming exists, and can aid in the development of more robust communication equipment or design of more efficient targeted jamming scenarios.

6 Integration 4G LTE with Tactical Network

Advanced communication technology is a key component of military success. The integration of 4G LTE network allows the dissemination of secured mission command data, imagery, streaming video and voice transmission between dismounted soldiers and command centers. The availability of real time complete situational awareness (SA) of the surrounding gives the combat soldiers a clear advantage. Military mobile communications need to keep up with the innovations occurring in the commercial space. LTE offers lower latency, faster speeds and a more efficient architecture than the latest wireless military network technology when it comes to two-way communication.

Mobilization of a military 4G LTE network can be done by installing the base stations on a moving vehicle or an Unmanned Aerial Vehicle (UAV) overhead or even on satellites operating at UHF (300 MHz – 3 GHz). Streaming video feeds from various individual endpoints and from UAV cameras can be transmitted on this 4G network safely. Depending on the frequency band, LTE service is supported for terminals moving at up to 350 km/h (220 mph) or 500 km/h (310 mph).

4G LTE makes it possible for the military to set up beyond-line-of-sight radio communication at a low cost. The low frequency bands (i.e. 700 MHz) makes it possible for deployment in rural areas as the signal travels further and provide better in-building coverage. This means fewer base stations are required to serve the same area. On the other hand, with 700 MHz in urban areas, there is a higher possibility of running into capacity issues, as there are more user per cell. Typically the higher frequencies (such as 2.6 GHz) are used for small cells (micro, pico, femto etc.) to increase system capacity in hotspot areas. Users are handed over to these cells to free up resources on the macro cell. It's basically an overlay to the macro layer which typically uses lower frequencies to provide wide-area coverage..

With 3GPP Release 12, two essential features will be added to the LTE standard. First, there is Device-to-Device (D2D) communication. Here two or more devices can directly communicate with each other, using uplink spectrum (FDD mode) at certain periodically occurring moments in time, or uplink subframes (TDD mode). This feature will be defined for in-coverage scenarios, where these devices are still served by a base station. But also for out-of-coverage scenarios, where no network is available. Second, there is Group Communication on top of D2D, which enables these devices to establish, for instance, a voice communication throughout the group using the D2D functionality. Release 12 shall be finished by the standardization team end of December 2014.

With Release 13, the standard will be even further enhanced to support, for instance, Mission Critical Push-To-Talk (MCPTT) services, utilized by all types of terminals, ranging from popular smartphone to ruggedized devices. The current time plan is to finish Release 13 by March 2016. All these features and applications are of interest in the case of public safety. When an emergency, disaster or any unexpected event occurs, communication infrastructure is very important and plays a vital role. The terrestrial communication infrastructure, especially core network functionality, might be in many cases seriously compromised and would fail to guarantee a reliable communication for rescue teams. In times like these, the isolated EUTRAN operations,

also part of Release 13, might be an interesting and effective solution to the problem. This feature enables the local routing of the communication (i.e. via base station only), when the interface to the core network is harmed or not available.

All-in-all the features that are coming along with Release 12 and 13 make LTE an interesting candidate for tactical communications as the underlying technology for next generation battlefield communications.

LTE Network emulation and tests up to 3GPP Release 10 can be performed with the R&S®CMW500 Wideband Communication Tester. The LTE base station can be configured and a mobile connected to perform several tests as explained in e.g. application notes 1MA211 [4] or 1MA176 [17].

7 Conclusion

This white paper is aimed at pointing out vulnerabilities of LTE and LTE Advanced. An inside look into LTE technology can also be found. All relevant parts of the LTE communication system has been discussed including LTE downlink and uplink channels as well as control channels.

Some commonly used traditional as well as more recent "smart" jamming techniques have been discussed, such as barrage jamming, partial band jamming, single tone jamming, multi tone jamming , asynchronous off-tone jamming and pilot tone jamming and nulling. Even though every jamming scheme comes with its own set of advantages and disadvantages, the asynchronous off-tone jamming has shown to be the more efficient jamming scheme in terms of figure of merit compared to the other schemes.

This paper also has a discussion about the unwanted interference and jamming mitigation schemes. A few solution has proposed which includes frequency division multiplexing based solution, time division multiplexing based solution, transmit power control based solution and the popular frequency hopping based solution.

The co-existence issue of LTE with S-band frequencies and Digital TV bands have been emphasized as well. The co-existence issue of LTE and S-band frequency is highly critical and requires constant attention because Air Traffic Control Radar and Air Traffic Surveillance Radars operate in the S-band. A coupling of the LTE transmitted power in the receiver of the radar may cause a rise in the noise floor and result in a failure of detecting an object in the sky.

The focus of this white paper is not only to draw attention to vulnerabilities of the technology but also how to address them. It goes without mentioning, that the UE and the eNodeB needs to be more robust in design. Both of them for use in security-relevant applications, should be designed in a way so that they are "self-aware" of interference and jamming cases and ideally are programmed to take actions in maintaining un-degraded communication.

Test and measurement is a key component in all steps of the development and maintenance process to ensure proper communication even in environments with high interference.

Further reading is compiled for the reader in the reference section.

8 Reference

1. Rohde & Schwarz, Application Note 1MA111, LTE Technology Introduction; retrieved from http://www.rohde-schwarz.com/appnote/1MA111

2. 3GPP TR 25.892, Feasibility Study for Orthogonal Frequency Division Multiplexing (OFDM) for UTRAN enhancement (Rel. 6); available at www.3gpp.org

3. 3GPP TS 36.211; Physical Channels and Modulation (Rel. 8); available at 3gpp.org

4. Rohde & Schwarz, Application Note 1MA211, Coexistence Test of LTE and Radar systems; retrieved from http://www.rohde-schwarz.com/appnote/1MA211

5. M. Lichtman, J. Reed, M. Norton, T. Clancy, "Vulnerability of LTE to Hostile Interference", IEEE Global Conference on Signal and Information Processing (GlobalSIP), Dec 2013.

6. K. Miwa, N. Miki, T. Kawamura, and M. Sawahashi, “Performance of decision-directed channel estimation using low-rate turbo codes for DFT-recoded OFDMA”; in Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th, 2012, pp. 1–5

7. J. G. Proakis, Digital communications, 4th edition, New York, New York: McGraw Hill, 2000

8. E. Malkamaki and H. Leib, “Evaluating the performance of convolutional codes over block fading channels,” Information Theory, IEEE Transactions on, vol. 45, no. 5, pp. 1643–1646, 1999.

9. M. Baker and T. Moulsley, “Downlink physical data and control channels,” in LTE, The UMTS Long Term Evolution: From Theory to Practice, 2nd ed., S. Sesia, I. Toufik, and M. Baker, Eds. Chichester, West Sussex, United Kingdom: John Wiley & Sons Ltd, 2011, ch. 9.

10. F. Tomatis and S. Sesia, “Synchronization and cell search,” in LTE, The UMTS Long Term Evolution: From Theory to Practice, 2nd ed. S. Sesia, I. Toufik, and M. Baker, Eds. Chichester, West Sussex, United Kingdom: John Wiley & Sons Ltd, 2011, Ch. 7.

11. T. Clancy, “Efficient OFDM denial: Pilot jamming and pilot nulling,” in Communications (ICC), 2011 IEEE International Conference on, June 2011, pp. 1 – 5.

12. J. Luo, J. Andrian, and C. Zhou, “Bit error rate analysis of jamming for OFDM systems,” in Wireless Telecommunications Symposium, 2007. WTS 2007, pp. 1 –8, april 2007

13. Chowdhury Shariar, Shabnam Sodagari, Robert McGwier and T. Charles Clancy, "Performance Impact of Asynchronous Off-tone Jamming Attacks against OFDM".

14. S. Chao, W. Ping, and S. Guozhong, “Performance of OFDM in the presence of multitone jamming,” in Robotics and Applications (ISRA), 2012 IEEE Symposium on, pp. 118 –121, June 2012.

16. 3GPP TS 36.141 version 10.1.0 Release 10, LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) conformance testing.

17. Rohde & Schwarz, Application Note 1MA176, Coexistence of Digital TV and LTE retrieved from http://www.rohde-schwarz.com/appnote/1MA176

18. Zhenping Hu, Riikka Susitaival, Zhuo Chen, I-Kang Fu, Pranav Dayal, Sudhir Kumar Baghel, “Interference Avoidance for In-Device Coexistance in 3GPP LTE-Advanced: Challenge and Solutions”; IEEE Communication Magazine, November 2012

19. Tutorial website for LTE resource grid generator, retrieved from http://www.pewscorner.host-ed.me/LTE/lte_resource_grid.html

About Rohde & Schwarz

Rohde & Schwarz is an independent group of companies specializing in electronics. It is a leading supplier of solutions in the fields of test and measurement, broadcasting, radio monitoring and radiolocation, as well as secure communications. Established more than 75 years ago, Rohde & Schwarz has a global presence and a dedicated service network in over 70 countries. Company headquarters are in Munich, Germany.

Regional contact

Europe, Africa, Middle East
+49 89 4129 12345
customersupport@rohde-schwarz.com

North America
1-888-TEST-RSA (1-888-837-8772)
customer.support@rsa.rohde-schwarz.com

Latin America
+1-410-910-7988
customersupport.la@rohde-schwarz.com

Asia/Pacific
+65 65 13 04 88
customersupport.asia@rohde-schwarz.com

China
+86-800-810-8228 /+86-400-650-5896
customersupport.china@rohde-schwarz.com

Environmental commitment

- Energy-efficient products
- Continuous improvement in environmental sustainability
- ISO 14001-certified environmental management system

Certified Quality System
ISO 9001

Rohde & Schwarz GmbH & Co. KG
Mühldorfstraße 15 | D - 81671 München
Phone + 49 89 4129 - 0 | Fax + 49 89 4129 – 13777

www.rohde-schwarz.com