HELSINKI UNIVERSITY OF TECHNOLOGY
Department of Electrical and Communications Engineering
Communications Laboratory

Mika Husso

Performance Analysis of a WiMAX System under Jamming

Thesis submitted in partial fulfilment of the requirement for the degree of
Master of Science in Engineering in Espoo, Finland, December 20, 2006.

Supervisor: Professor Sven-Gustav Häggman

Instructor: Researcher Kari Pietikäinen, M.Sc.

HELSINKI UNIVERSITY OF TECHNOLOGY

ABSTRACT

Author: Mika Juhani Husso

Name of the Thesis: Performance Analysis of a WiMAX System under Jamming

Date: 20.12.2006 **Number of pages:** 84

Department: Department of Electrical and Communications Engineering

Professorship: S-72 Telecommunications

Supervisor: Prof. Sven-Gustav Häggman

Instructor: Kari Pietikäinen, M.Sc (Tech)

Worldwide techno-economical development has brought up an idea of offering wideband connections also to suburban and even rural areas. In Finland this has been conceptualised as national wideband strategy (Laajakaistastrategia). IEEE 802.16 WiMAX is a future technology which could provide users in rural areas with adequate connection speeds for basic wideband use with reasonable financial investments.

Being a developing technology, the research that focuses on studying the suitability of WiMAX in different operating environments is of great importance. In this thesis, a IEEE 802.16-2004 based system under jamming is evaluated in terms of the requirements set by the standard. The selection of the used jamming forms is justified by the easiness of generation, so that they could also exist in a natural environment.

The performance of the system was found out to greatly differ with the use of different jamming signals, allowing central areas to be identified, where system development should be focused on. In addition, from the basic theory point of view, rather surprising results where also found as some of the pilot subcarriers needed almost 10 dB less jamming power than others to cause the same portion of errors.

The work should give a clear picture of how the studied WiMAX system performs as well under jamming as without the presence of jamming. The results show that some forms of interference degrade the performance of the system rapidly, thus the form of incoming jamming should be known and considered before deploying the system.

Keywords: WiMAX, IEEE 802.16, WMAN, OFDM, Jamming, Interference

TEKNILLINEN KORKEAKOULU

TIIVISTELMÄ

Tekijä: Mika Juhani Husso

Työn nimi: WiMAX-järjestelmän suorituskyky häirinnän alaisena

Päivämäärä: 20.12.2006 **Sivumäärä:** 84

Osasto: Sähkö- ja tietoliikennetekniikan osasto

Professuuri: S-72 Tietoliikennetekniikka

Työn valvoja: Prof. Sven-Gustav Häggman

Työn ohjaaja: DI Kari Pietikäinen

Maailmanlaajuinen elintason nousu ja teknologinen kehitys ovat synnyttäneet idean laajakaistayhteyden tarjoamisesta myös harvaanasutuille alueille. Tämä tarve on nostettu esille myös Suomessa valtioneuvoston laajakaistastrategiassa. IEEE 802.16 standardin mukainen WiMAX on tulevaisuuden langaton teknologia, joka mahdollistaa perustason laajakaistakäyttöön riittävät yhteysnopeudet taloudellisessa mielessä kohtuullisin investoinnein.

WiMAX on kehittyvä teknologia, jonka soveltuvuuden tutkiminen erilaisiin käyttötarkoituksiin on keskeistä. Tässä diplomityössä tutkitaan skenaarioiden avulla yhden IEEE 802.16-2004 mukaisen järjestelmän toimivuutta häirinnän alaisena suhteessa standardin asettamiin vaatimuksiin. Häirintätyypit on valittu perusteena niiden helppo toteutettavuus, jolloin ne vastaavat myös luonnollisessa ympäristössä usein esiintyviä häiriösignaaleja.

Järjestelmän suorituskyvyn havaittiin poikkeavan selvästi eri häiriötyypeillä ja näin voitiin erottaa selkeästi ominaisuuksia, joihin järjestelmäkehityksessä tulisi tulevaisuudessa panostaa. Lisäksi järjestelmän toiminnasta löydettiin joitakin perusteorian kannalta tarkasteltuna yllättäviä ominaisuuksia, esimerkiksi pilottialikantoaaltojen häirintäherkkyyksissä havaittiin lähes 10 desibelin eroja.

Kokonaisuudessaan työ pyrkii antamaan selkeän kuvan järjestelmän tämän hetkisestä suorituskyvystä niin häirinnänalaisena, mutta myös toiminta häiriöttömässä ympäristössä selviää mittaustulosten analyysistä. Jotkin häirintätavat heikentävät järjestelmän toimintakykyä nopeasti, joten käyttöönottopäätöksen tekemiseksi tarvitaan etukäteistietoa mahdollisesti esiintyvistä häirintämuodoista.

Avainsanat: WiMAX, IEEE 802.16, WMAN, OFDM, Jamming, Interference

PREFACE

This thesis was carried out in the Communications Laboratory in Helsinki University of Technology as a part of a project funded by the Finnish Defence Forces.

I wish to express my gratitude to my supervisor Professor Sven-Gustav Häggman for showing great interest in my work and for all the guidance he has given me throughout the process. I also wish thank my instructor Kari Pietikäinen and Professor Riku Jäntti for their valuable advice and guidance.

I would like to thank all my colleagues, especially Seppo, Viktor, Mika N., Mikko and Michael for providing knowledge and support. Thanks also go to my friends for frequently giving me something else to think of.

Finally, I wish to thank my parents, who have always given me their unconditional caring and support.

In Otaniemi, Espoo,
December 20, 2006

Mika Husso

TABLE OF CONTENTS

List of abbreviations

ADC	Analog-to-Digital-Converter
AGC	Automatic Gain Control
ARB	Arbitrary Waveform Generator
AWGN	Additive White Gaussian Noise
BPSK	Binary Phase Shift Keying
BS	Base Station
BTC	Block Turbo Coding
BTS	Base Transmitter Station
BW	BandWidth
BWA	Broadband Wireless Access
COTS	Commercial Off The Shelf
CC	Convolutional Code
CPE	Customer Premises Equipment
CSI	Channel State Information
CTC	Convolutional Turbo Coding
DAC	Digital-Analog-Converter
DC	Direct Current
DINA	Direct Noise Amplification
DL	Downlink
DTE	Data Terminal Equipment
EIRP	Effective Isotropically Radiated Power
ERP	Effective Radiated Power
FDD	Frequency Division Duplexing
FEC	Forward Error Correction

FFT	Fast Fourier Transform
FICORA	Finnish Communications Regulatory Authority
GF	Galois Field
I/Q	In-phase / Quadrature
IEEE	Institute of Electrical and Electronics Engineers
IFFT	Inverse Fast Fourier Transform
ISI	InterSymbol Interference
LOS	Line-Of-Sight
MAC	Medium Access Control
MOTS	Modified Off The Shelf
NLOS	No-Line-Of-Sight
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
PER	Packet-Error-Ratio
PMP	Point-to-MultiPoint
PP	Point-to-Point
PRBS	PseudoRandom Bit Sequence
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RF	Radio Frequency
SC	Single Carrier
SINR	Signal-to-Interference-and-Noise-Ratio
SJR	Signal-to-Jamming-Ratio
SNR	Signal-to-Noise-Ratio

SS	Subscriber Station
RS	Reed-Solomon
TCP	Transmission Control Protocol
TDD	Time Division Duplexing
UDP	User Datagram Protocol
UL	UpLink
WGN	White Gaussian Noise
WiMAX	Worldwide interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network

List of symbols

A_{fixed}	Attenuation of the fixed attenuator
$A_{adj.}$	Attenuation of the adjustable attenuator
$A_{cables1}$	Attenuation caused by cables and connectors to the WiMAX signal
$A_{cables2}$	Attenuation caused by cables and connectors to the jamming signal
B_J	Bandwidth of the jamming signal
B_{VS}	Bandwidth of the victim system
BW	Nominal channel bandwidth
Δf	Subcarrier spacing
Fs	Sampling frequency
f_{pilot1}	The frequency of the 1st pilot
K	Number of data bytes after encoding
m	Number of information bits
N	Total number of bytes after encoding
N_{FFT}	Number of points used for FFT
$N_{suchannels}$	Number of allocated subchannels
n	Total number of bits after encoding
$n_{sampling}$	Sampling factor
$P_{t,jamming}$	Transmitted jamming power
$P_{t,signal}$	Transmitted signal power
SNR_{RX}	Minimum receiver Signal-to-Noise-Ratio
T	Number of data bytes which can be corrected using a code

1. Introduction

OFDM (Orthogonal Frequency Division Multiplexing) based IEEE 802.16 WiMAX has been widely accepted as the next generation wireless standard for providing wideband communications in rural areas. [1] Due to its reliability and flexibility, other applications e.g. in military communications have been proposed during the last few years.

Multicarrier systems such as WiMAX offer good functionality under heavy interference. Short interfering signals are countered using long symbol times, which are made possible by spreading data onto several subcarriers. These subcarriers are spread on a wide spectral range, which enables the system to effectively resist narrowband interference.

However, because of its wide operating bandwidth, WiMAX faces strong frequency selective fading. In order to combat the fading phenomena, the countermeasures need accurate and real-time knowledge of the transfer function of the radio channel. This so called CSI (Channel State Information) is a crucial factor concerning the true functionality of WiMAX. The fact that the system needs accurate information of the channel state makes it also vulnerable to systems that are able to prevent a WiMAX device from getting this information.

The ever going evolution of advanced wireless technologies makes it financially impossible for military organisations to completely manufacture their own equipment. This has raised growing interest in so called COTS (Commercial-Off-The-Shelf) and MOTS (Modified-Off-The-Shelf) equipment, the former meaning systems that can be utilised as they are in a store and the latter systems needing only small and low-cost modifications.

It is apparent that systems not designed to be used for example under jamming, may strongly degrade in performance when used in such an environment. This creates a need for research on how these devices can function or how simple modifications in their original setup could enable them to function in their area of applicability.

WiMAX system is a combination of complicated implementations of modern technologies and its true performance in a real noisy environment is obviously very difficult to draw from the basic radio communications theory. In [2] a simulation model is constructed for the IEEE 802.16-2004 based WiMAX, which will be used for comparison when analysing jamming measurement results. In [3] a somewhat similar measurement campaign was carried out which makes it possible in the future to compare OFDM technologies WLAN and WiMAX considering their jamming tolerance.

The goal of the thesis is to evaluate empirically how the measured WiMAX system functions when jamming is inserted on the connection and to conclude whether the system could be used in a typical hostile environment. The information derived from the study can be utilised not only for military purposes but it also gives an insight into the performance of the system in a natural, interference rich environment.

The scope of the thesis is limited to cover the measurement of the system with good received signal strength (sensitivity + 20 dB) under four typical jamming signals. The conclusions are based on basic telecommunications theory. More in-depth analysis would not be worthwhile since the IEEE 802.16-2004 standard leaves a large proportion of central issues to be decided by the manufacturer of a system. A brief comparison to a simulation based results is, however, performed.

In Chapter 2, the basic communications theory that the WiMAX is built on, is presented. Chapter 3 focuses on explaining the basic idea of jamming and illustrates the concepts of noise and carrier jamming signals. In Chapter 4, the different measurement setups are explained in detail and the measurement phases are presented. In Chapter 5, the measurement results are analysed and conclusions are drawn based on the principles presented in Chapter 2. Chapter 6 provides a summary and the main conclusions focusing on evaluating the overall performance of the measured system.

2. Introduction to WiMAX (physical layer operation)

IEEE 802.16 standard defines the air interface for fixed Broadband Wireless Access (BWA) systems to be used in WMANs (Wireless Metropolitan Area Networks), commonly referred to as WiMAX (Worldwide Interoperability for Microwave Access). The original standard IEEE 802.16 does not support mobility and for this purpose IEEE 802.16e-2005 was introduced. [1]

The original idea of WiMAX is to provide users in rural areas with high speed communications as an alternative for fairly expensive wired connections (e.g. cable or DSL). These so called last mile connections are not the only purpose for which WiMAX systems are thought to be used. WiMAX standard includes utilization of adaptive modulation and coding, which makes it possible to provide users with high connection speeds close to the BS (Base Station) and lower speeds when the radio channel is not as good. Thus, WiMAX can offer home and business users high data rates and QoS (Quality of Service) on dense areas and moderate connection speeds and still good QoS on rural areas. It is also designed to enable LANs to communicate with each other through a WMAN.

2.1. IEEE 802.16 standard family

This work relies on the IEEE 802.16 standard known as IEEE 802.16-2004, although 802.16e-2005 has already been published. This is due to the fact that the WiMAX equipment used in the measurements has been built according to 802.16-2004 and no update from the manufacturer is yet available. The 802.16 standard family comprises several related standards with the main functionalities described in Table 1. Standards 802.16a, 802.16c and 802.16d contain upgrades to the original standard and have been integrated into the 802.16-2004 standard.

Table 1. IEEE 802.16 standard family [1], [4], [11]

	Frequency band [GHz]	LOS/ NLOS	PP/ PMP	Duplex method	Modulation	Mobility?	PHY layer operation	Other
802.16	10-66	LOS	PP	TDD/ FDD	BPSK, QPSK, 16-QAM, 64-QAM (optional)	No	SC	complete standard, completed in 2001
802.16a	2-11	NLOS	PMP	TDD/ FDD	OFDM 256, BPSK, QPSK, 16-QAM, 64-QAM (opt.)	No	SC, SCa, OFDM, OFDMA	amendment
802.16c	Upgrades for the 10-66 GHz range							
802.16d	Upgrades for the 2-11 GHz range							
802.16-2004	2-11 and 10-66	LOS and NLOS	PMP	TDD/ FDD	OFDM 256, BPSK, QPSK, 16-QAM, 64-QAM (opt.)	No	SC, SCa, OFDM, OFDMA	complete standard
802.16e-2005	2-11 and 10-66	LOS and NLOS	PMP	TDD/ FDD	OFDM 256, BPSK, QPSK, 16-QAM, 64-QAM (opt.)	Yes	SC, SCa, OFDM, OFDMA	complete standard

- LOS/NLOS = Line-Of-Sight / Non-Line-Of-Sight
- PP / PMP = Point-to-Point / Point-to-MultiPoint
- TDD/FDD = Time Division Duplexing / Frequency Division Duplexing
- BPSK = Binary Phase Shift Keying
- QPSK = Quadrature Phase Shift Keying
- M-QAM = Quadrature Amplitude Modulation (M states)
- SC = Single Carrier
- OFDMA = Orthogonal Frequency Division Multiple Access

The newest complete version of the 802.16 standard is 802.16e-2005, whose main purpose is to introduce mobility making it possible for the DTE (Data Terminal Equipment) to move at about 120 km/h. Some corrections and amendments have also been made to the 2004 standard. [4]

The evolution of the standard is still far from complete and new versions are frequently published.

2.2 Technological aspects

WiMAX is a state-of-the-art wireless technology which utilizes adaptive modulation and coding, supports single carrier (SC) and orthogonal frequency division multiplexing techniques (OFDM) and several frequency bands for different operation environments. WiMAX system is able to constantly monitor the quality of the radio channel and change its operational parameters (e.g. modulation and coding) accordingly. In the following sections technological aspects are more profoundly dealt with.

In the following two subchapters, the basics of OFDM and OFDM transceiver are presented. The latter subchapters go deeper into issues that have relevancy when operating in a noisy or interference rich environment.

2.2.1 OFDM basics

Orthogonal frequency division multiplexing is a multicarrier technique, which splits the system bandwidth into orthogonal subchannels (Figure 1), each of which occupies only a narrow bandwidth and a separate subcarrier is assigned to each. Since the bandwidth of a single subchannel is generally smaller than the radio channel's coherence bandwidth, it can be treated as a flat fading channel. By means of guard interval and cyclic prefix, an OFDM system also achieves good resistance against multipath fading. [3]

The transmitted data is spread onto the subchannels' carriers, which makes it possible to transmit high data rates using rather modest per subcarrier data rates (long symbol times). Transmitting 1 Mbit/s using 200 data subcarriers, would thus mean a per subcarrier data rate of only 5 kbit/s. In transmission, data is mapped onto every subcarrier using basic modulation methods, such as BPSK, QPSK and M-QAM, where

M refers to the number of possible states (4, 16, …). Modulation methods are more profoundly dealt with in Section 2.2.3.

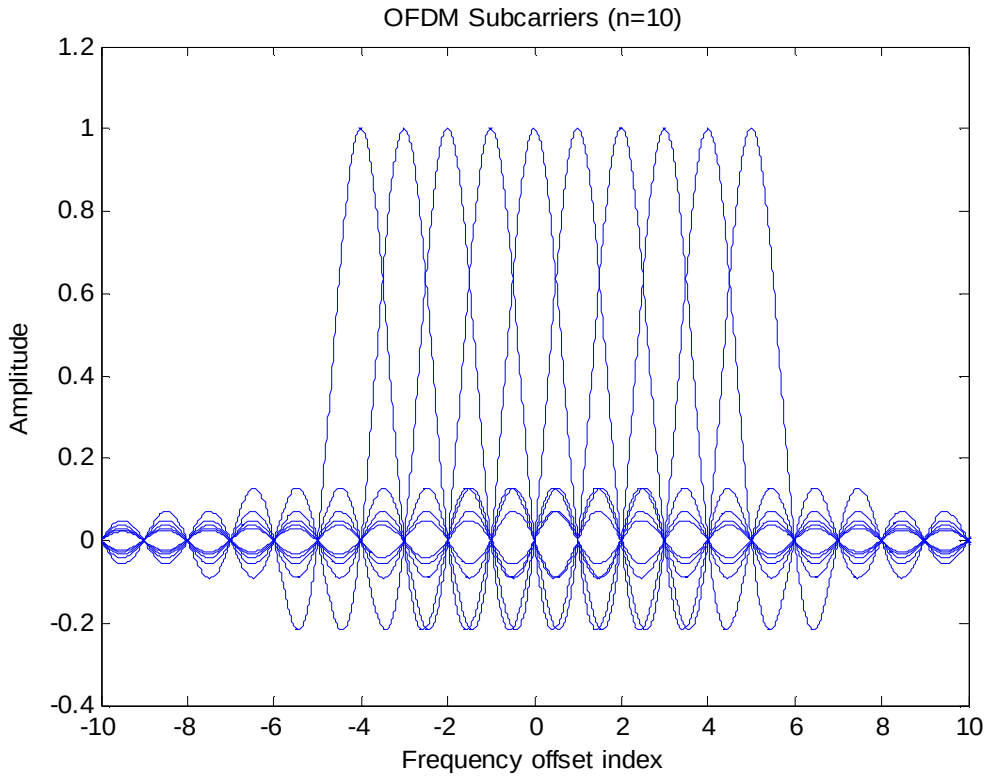

Figure 1. OFDM subcarriers

To reach good performance the transfer function of the channel need to be known and utilized in the receiver. The channel estimation process includes making an estimate of the channel by sending known signals (pilot subcarriers) at known frequencies and then mathematically obtaining the channel response by means of interpolation. The model obtained by these means is then used to remove effects of frequency selective fading from the data subcarriers. This is called channel equalisation.

2.2.2 OFDM transceiver: system architecture

OFDM transceiver (Figure 2) comprises two main blocks, transmitter and receiver, which are separated by a duplexer (TDD, FDD or half-duplex). The data coming from the Medium Access Control (MAC) layer is first channel coded, which includes randomization (scrambling), forward error correction (FEC) and interleaving. [5]

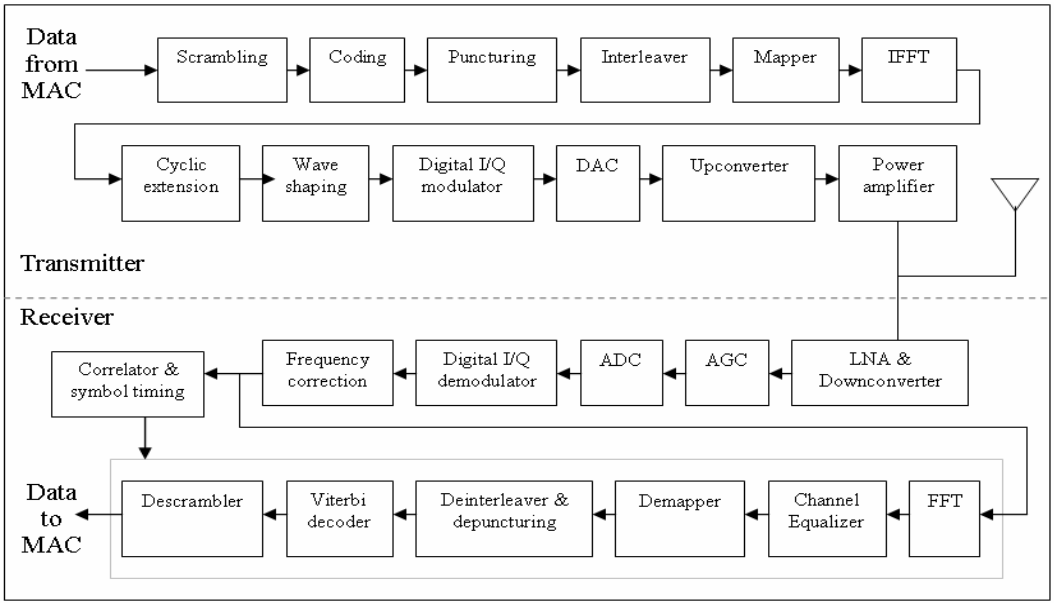

Figure 2. OFDM transceiver block diagram

The randomizer scrambles the transmitted bit sequence pseudorandomly, generating a sequence generally known as pseudorandom bit sequence (PRBS). It eliminates the possibility of transmitting series of all ones or zeros for a long period of time, which facilitates the work of adaptive circuits such as automatic gain control (AGC). It also efficiently removes the dependency between the transmitted data and the shape of the power spectrum, spreading the transmission equally on the used frequency band. [1] The block diagram of the PRBS generator used in WiMAX is presented in Figure 3.

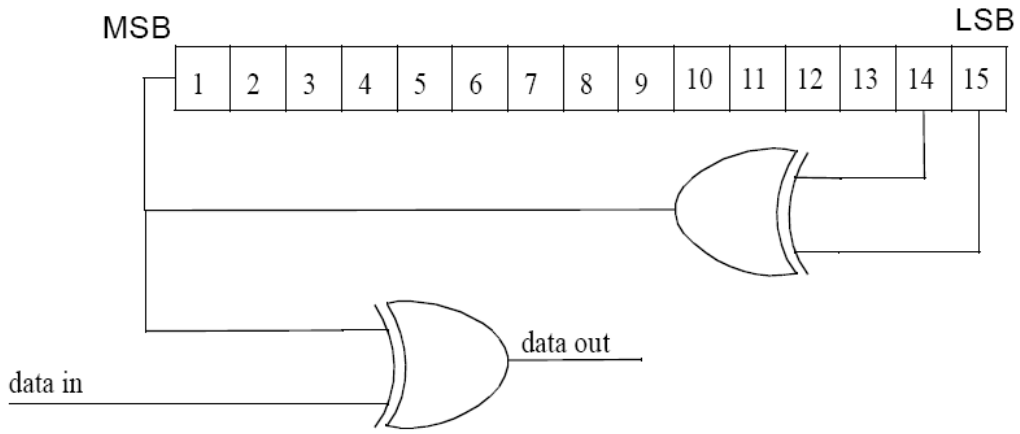

Figure 3. PRBS generator block diagram

Forward error correction is an error control code, which utilizes redundancy in finding errors and correcting them. In IEEE 802.16-2004, FEC consists of a concatenation of a Reed-Solomon outer code and a rate-compatible convolutional inner code. Puncturing removes some of the parity bits when using an error correction code. It affects in the same manner as having less redundancy or a higher coding rate, but enables us to use the same decoder regardless of the number of parity bits having been removed. This provides additional flexibility to the system. Implementation of block turbo coding (BTC) and convolutional turbo codes (CTC) is left optional in the standard and will not the treated in this thesis. Forward error correction will be more profoundly dealt with in Chapter 2.2.4. [1]

Interleaving is the process of transferring adjacent bits away from each other in time at transmission and deinterleaving combining them at reception. The process aims at weakening the destructive effect of short and strong interfering bursts. The idea is illustrated in Figure 4, which shows that when interleaving is used, the transmitted words (e.g. AAAA) can probably be recovered, while without interleaving the word BBBB is completely erased. [9]

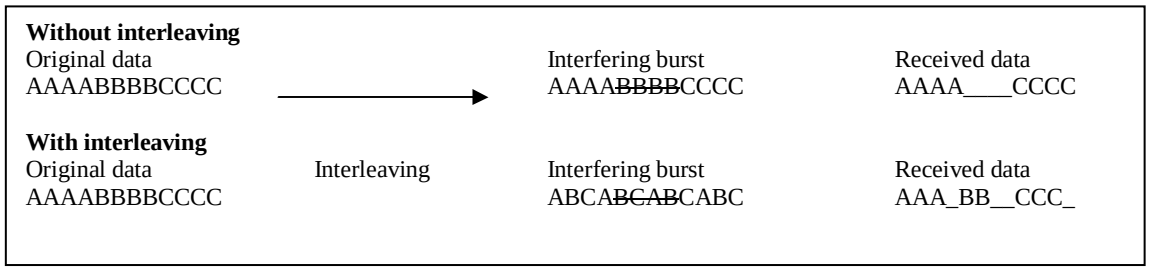

Figure 4. Interleaving

After interleaving, bits are fed to the constellation mapper, which assigns every fixed length series of bits (i.e. symbol) with a single complex value in a constellation. After mapping, the data stream is converted from serial to parallel and an inverse fast Fourier transform (IFFT) method is applied. IFFT transforms the parallel data streams from frequency to time domain.

A guard interval is used between OFDM symbols in time domain to prevent overlapping of successive symbols caused by multipath propagation (intersymbol interference, ISI). Cyclic extension refers to the implementation of the guard interval by transferring a part from the symbol's end to the beginning of the same symbol. This creates adequate protection against multipath phenomena, while remaining orthogonality between symbols. [3]

Wave shaping (windowing) is the process of shaping the spectrum of the transmitted symbol so that the out-of-band spectrum usage of the subchannel is at small as possible. This is usually done by applying a passband filter, such as raised cosine window.

The digital I/Q modulator multiplies the in-phase (I) and quadrature (Q) control signals with sine and cosine functions respectively and sums them, creating the final baseband signal. The baseband signal is mixed to the wanted radio frequency (RF) and amplified to the desired power level (e.g. +10 dBm). Then the signal is finally fed through the duplexer to the antenna.

The receiver section of the transceiver comprises mostly corresponding blocks, but in the reverse order as presented in Figure 2. The main differences are the need for an AGC, channel equalization, frequency correction and symbol timing. These will be more thoroughly discussed in the following chapters.

2.2.3 Modulation

The selected modulation method affects how many bits can be transmitted in a symbol and how much fading and interference the system can tolerate without errors in transmission. In WiMAX, the (digital) modulation methods used are BPSK (Binary Phase Shift Keying), QPSK (Quadrature Phase Shift Keying), 16-QAM (Quadrature Amplitude Modulation) and 64-QAM.

The more advanced the modulation technique, the higher spectral efficiency (bit/s/Hz) can be reached and more bits can be sent in a given time. For every modulation method, there are areas in the constellation diagram, called decision regions, using which the

interpretation of a transmitted symbol is done. Since complex modulation techniques include several decision regions (Figure 5), adding noise to the signal easily leads to false interpretation of the transmitted symbol. If the received symbol, after channel estimation etc, falls into the box drawn in Figure 5, it is interpreted as 0000 ($b_0b_1b_2b_3$). [14]

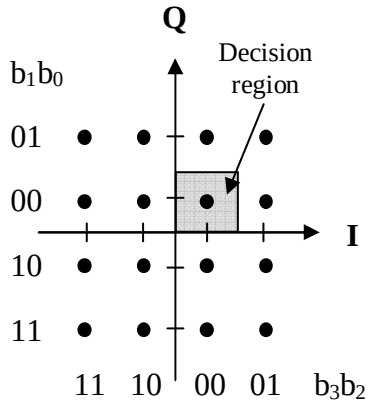

Figure 5. 16-QAM modulation decision region

However, in a realistic radio channel, additive white Gaussian noise (AWGN) and sources of interference are always present and sum to the signal as shown in Figure 6.

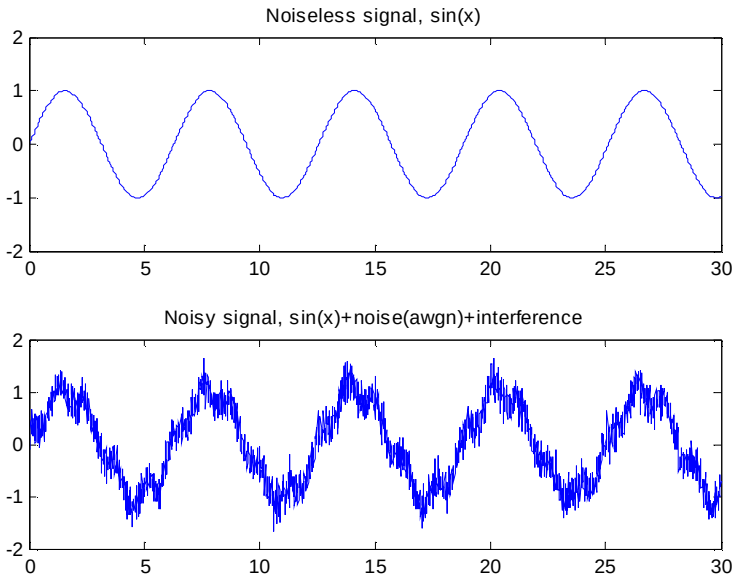

Figure 6. Noise adds to the signal

Since the amplitude and phase of additive noise are random in nature, channel equalisation is usually unable to correct their impact on the signal, which generally causes the symbol to move from its ideal position on the constellation diagram. If the signal-to-noise-ratio (SNR) is low as a result of a weak signal or intense noise, the symbol may move outside its decision region, causing the symbol to be falsely interpreted. Figure 7 represents false symbol decision caused by a change in amplitude and Figure 8 a change in phase.

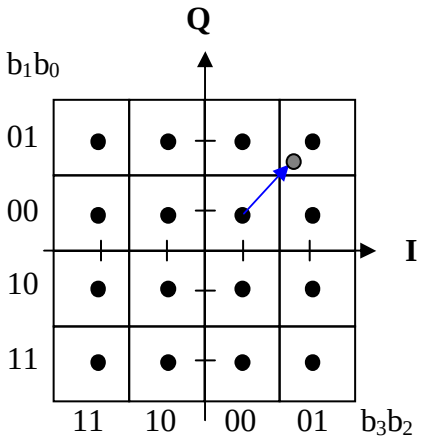

Figure 7. False symbol decision caused by amplitude noise

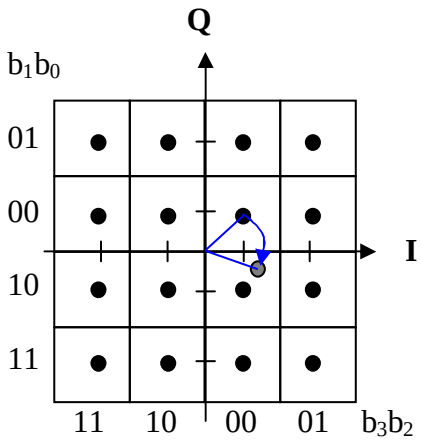

Figure 8. False symbol decision caused by phase noise

2.2.4 Forward Error Correction

An essential part of channel coding, forward error correction (FEC) is of great importance in WiMAX because, together with adaptive modulation, it enables effective link adaptation. In IEEE 802.16-2004, mandatory channel coding is implemented with concatenation of a Reed-Solomon (RS) outer code and a rate-compatible zero-terminating convolutional inner code (CC) as illustrated in Figure 9. The encoding of block formatted data is performed by first passing it through an RS-encoder and then through a convolutional encoder. The main reason for using encoders in this order is that convolutional coding with soft decision decoding operates well for low signal-to-noise ratios (SNR) and the hard-decision block (RS) decoder is able to correct the few errors left after convolutional decoding. [1]

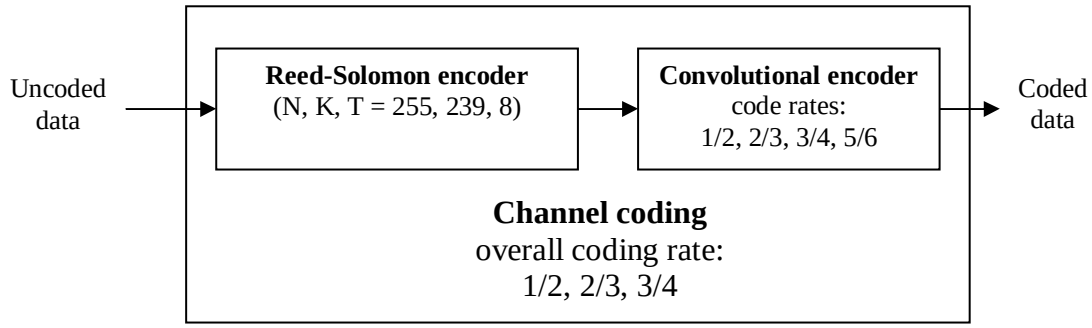

Figure 9. Channel coding in IEEE 802.16-2004

The RS encoding is derived from a systematic RS (N = 255, K = 239, T = 8) code using GF(2^8), where N is the overall number of bytes after encoding, K the number of data bytes before encoding and T the number of data bytes which can be corrected using the code. [13] The code rate of a convolutional encoder is defined as

$$\frac{m}{n} = \frac{number\ of\ information\ bits}{total\ number\ of\ bits\ after\ encoding} \quad (1)$$

The overall coding rate can be defined in a likewise manner

$$overall\ coding\ rate = \frac{total\ number\ of\ bits\ in\ uncoded\ data}{total\ number\ of\ bits\ in\ coded\ data} \quad (2)$$

In the standard, mandatory channel coding per modulation is defined and presented in Table 2.

Table 2. Modulation and coding methods in IEEE 802.16-2004 [1]

Modulation	Uncoded block size (bytes)	Coded block size (bytes)	Overall coding rate	RS code	CC code rate
BPSK	12	24	1/2	(12,12,0)	1/2
QPSK	24	48	1/2	(32,24,4)	2/3
QPSK	36	48	3/4	(40,36,2)	5/6
16-QAM	48	96	1/2	(64,48,8)	2/3
16-QAM	72	96	3/4	(80,72,4)	5/6
64-QAM	96	144	2/3	(108,96,6)	3/4
64-QAM	108	144	3/4	(120,108,6)	5/6

As can be seen in Table 2, high CC and low RS code rates are used for lower modulations, since e.g. for QPSK, we are generally operating in a low SNR environment. For BPSK, RS coder should be completely bypassed. [1]

2.2.5 Automatic Gain Control (AGC)

The main purpose of an automatic gain control (AGC) is to keep the input power level of the receiver on its optimal range. Generally WiMAX transceivers include AGCs that allow variations of approximately 50 dB in the power level received by the antenna. [6] Assuming that an optimal input power for the main receiver block would be -50 dBm, AGC (50 dB) would allow received powers in the range of -75 … -25 dBm. Should the power level exceed the range, the receiver may still work, but the performance is usually somewhat degraded. The main idea of AGC is illustrated in Figure 10.

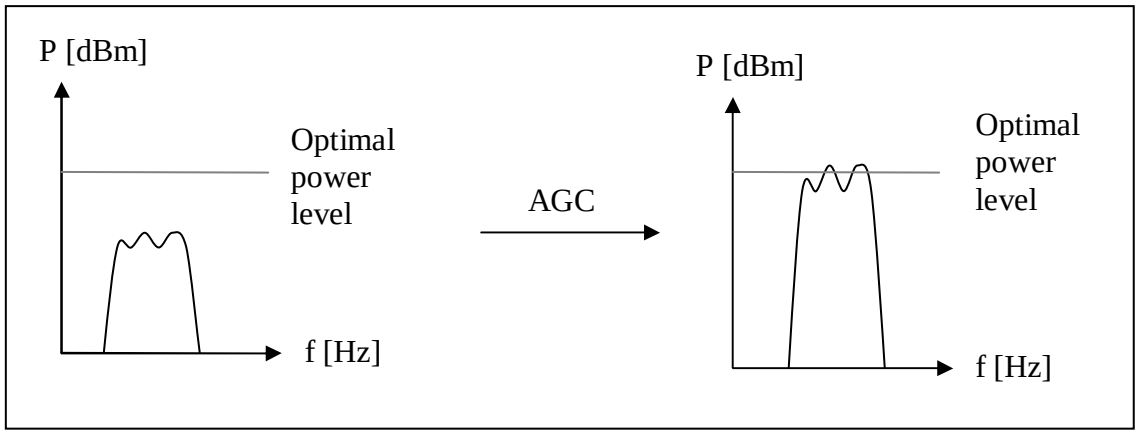

Figure 10. Automatic Gain Control (AGC)

However, if narrowband noise (i.e. interference) sums to the signal, AGC may not be able to raise the signal to the optimal power level. If the amplitude of the interfering signal is high enough, it may push the receiver off its functional range (Figure 11). This leads to a phenomenon generally known as receiver saturation.

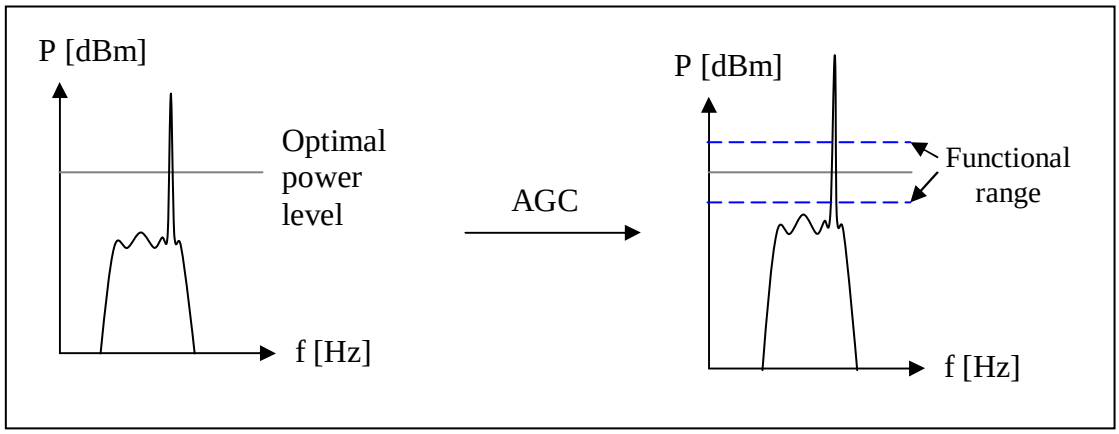

Figure 11. RX saturation caused by interference

The saturation of the receiver also affects the channel equalisation process, since the useful signal power is falsely evaluated due to an increase in the overall received power (sign. power + jamming power) caused by the jamming signal. This tightens the constellation as illustrated in Figure 12 and as the jamming power is increased, eventually leads to false interpretation of the transmitted symbols. In Figure 12, the symbols originally on the outer decision regions are now falsely interpreted
(e.g. 1011 -> 0001).

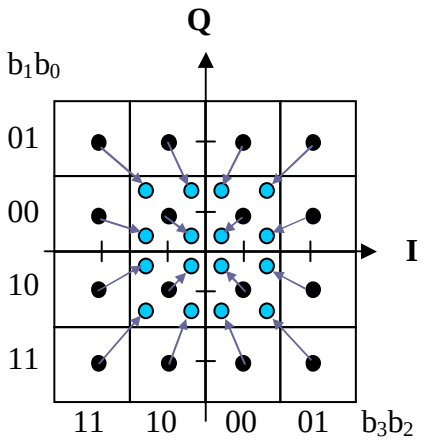

Figure 12: Tightening of the 16-QAM constellation caused by jamming signal

According to IEEE 802.16-2004 a WiMAX receiver should be capable of decoding a maximum input signal of -30 dBm and tolerate 0 dBm without damage to the system. Minimum input level (sensitivity) can be calculated from the equation

$$R_{SS} = -102 + SNR_{RX} + 10 \cdot \log\left(F_S \cdot \frac{N_{USED}}{N_{FFT}} \cdot \frac{N_{subchannels}}{16} \right) \quad (3)$$

where

SNR_{Rx}	the receiver SNR as per Table 7,
F_S	sampling frequency (4.0 MHz),
N_{USED}	number of used subcarriers (200),
N_{FFT}	number of points in FFT (256),
$N_{subchannels}$	the number of allocated subchannels (default 16, when no subchannelisation is used). [1]

2.2.6 Duplex methods

IEEE 802.16-2004 supports the duplex methods FDD (Frequency Division Duplexing) and TDD (Time Division Duplexing). TDD is to be used in license exempt bands and either TDD or FDD on licensed bands. However, this far all the WiMAX Forum -certified base stations operate in the FDD mode. In addition, FDD mode supports full duplex SSs (Subscriber Station) and half-duplex SSs, which do not receive and transmit

simultaneously. Half-duplex devices are normally used due to the lower implementation costs. In licensed bands TDD is normally used if the regulator (such as FICORA) supplies the operators with a relatively narrow operating bandwidth, which makes it hard to allocate enough bandwidth for both transmission bands (UL and DL). However, if operator has a large operating bandwidth, FDD operation is usually chosen due to its fundamentally higher capacity.

From interference point of view, operating in FDD mode should provide better protection against jamming, since jamming of the entire operational frequency band requires jamming of two individual bands (i.e. uplink and downlink). If only one of the bands would be jammed, the transmission in the remaining direction should still be possible, allowing that acknowledgements are not required or can still go through in the jammed transmission direction.

2.2.7 Channel equalization

Channel estimation is first performed to obtain adequate knowledge of the radio channel (channel state information, CSI). Channel equalization is then performed in order to compensate for the distortion and losses caused by the radio channel on the signal using the knowledge of the channel frequency response generated in the estimation process (CSI). [10] The general problem is reaching as complete and real-time CSI as possible with as little signalling as possible. In WiMAX, radio channel is measured by sending known signals at known frequencies (pilot subcarriers) and interpolating the frequency response of the channel thereof. (Figure 13)

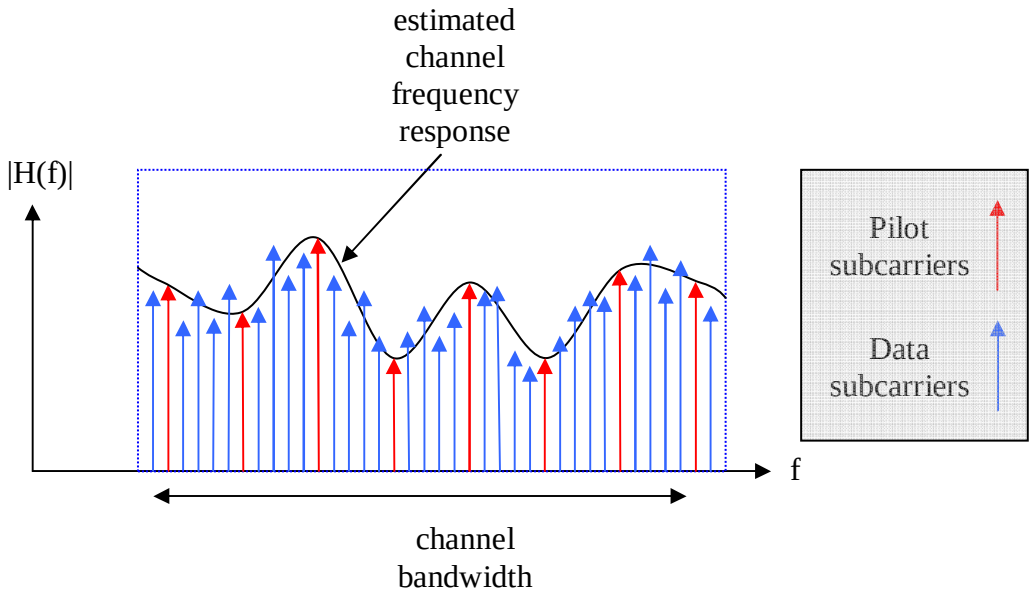

Figure 13. Channel estimation using pilot subcarriers

Since the radio channel is time-variant, the frequency response needs to be calculated frequently. The process of updating the receiver CSI is called training and the sent known information a training sequence. The more often the channel frequency response is derived the more accurate and real time CSI the receiver has. However, the process always consumes resources, which can be of importance especially when SSs are concerned.

Channel equalization is an important interference (or jamming) countermeasure, since it enables the system to adapt to changes in the operating conditions. On the other hand, it also provides an easy way to degrade the performance of the system by jamming the channel equalization mechanism. Jamming of the pilot subcarriers will be dealt with in Chapter 3.

2.2.8 Antennas

Antennas to be used with WiMAX are not defined in the standard, but have a crucial impact on the system operation especially in an interference rich environment. The basic sectorisation of the BTS provides some resistance against interference coming from directions other than that of the SS (Figure 14). Naturally, the more sectors we

use, the better the protection. Typically a WiMAX base station covering the entire radius (360 degrees), uses e.g. three (120 °) or four (90 °) sector antennas.

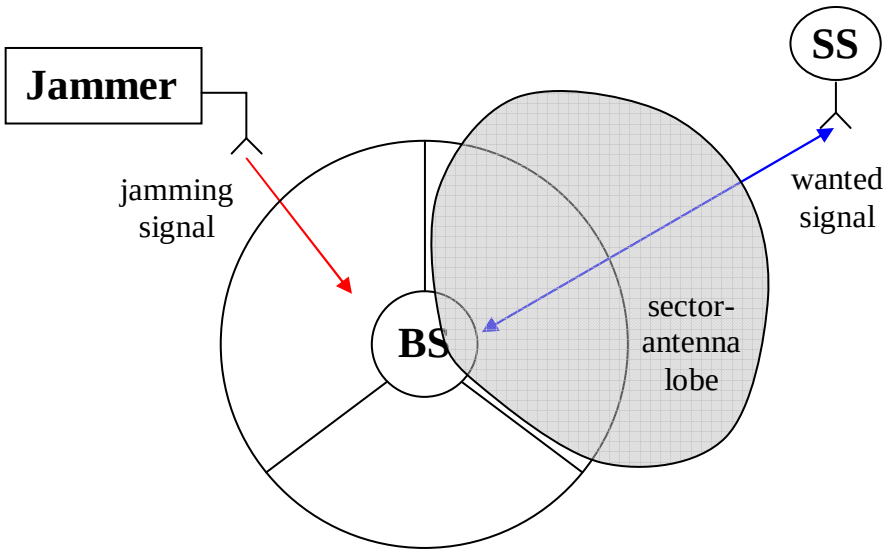

Figure 14: Sector antenna radiation pattern

Furthermore, by narrowing the lobe of the antenna vertically, we can reduce the harmful impact of interference coming for example from helicopters and other airborne jamming sources. For example, the sector antenna provided with the measured WiMAX system offers a gain of 16 dBi.

Other possibilities include high gain antennas (gain e.g. 50 dB), which are always aimed directly at the other part of the connection. (Figure 15) This usually requires both the BS and the SS not to move in order to stay within the lobe of the antenna. Smart antennas, where radiation pattern can be constantly electrically modified, are an important research topic especially in the field of military communications. [10] The process of controlling directionality of an antenna is generally called beamforming.

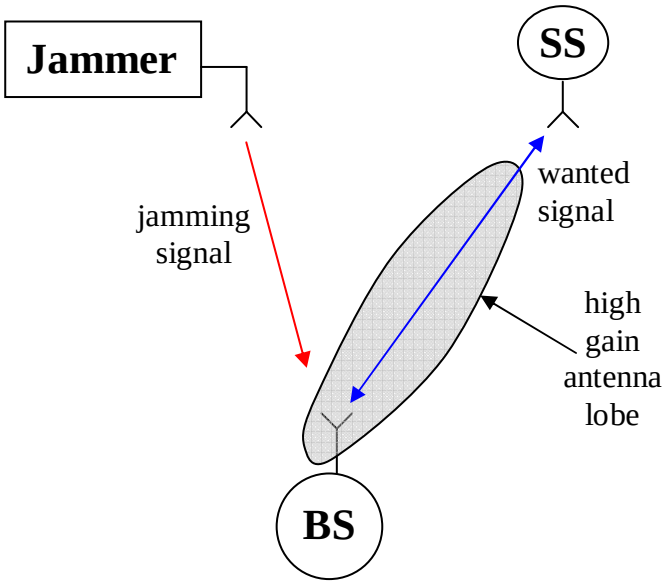

Figure 15: High gain antenna radiation pattern

2.3 WiMAX spectrum

The WiMAX system used in the measurements consists of an uplink band at 3.445 GHz ± 1.75 MHz and the downlink band 100 MHz above uplink at 3.545 GHz ± 1.75 MHz. The 3.5 MHz bandwidth is occupied with a total of 200 subcarriers, 192 of which are used for data transmission and 8 are pilot subcarriers used for channel estimation purposes. [1] The spectrum allocation for the entire BW is illustrated in Figure 16.

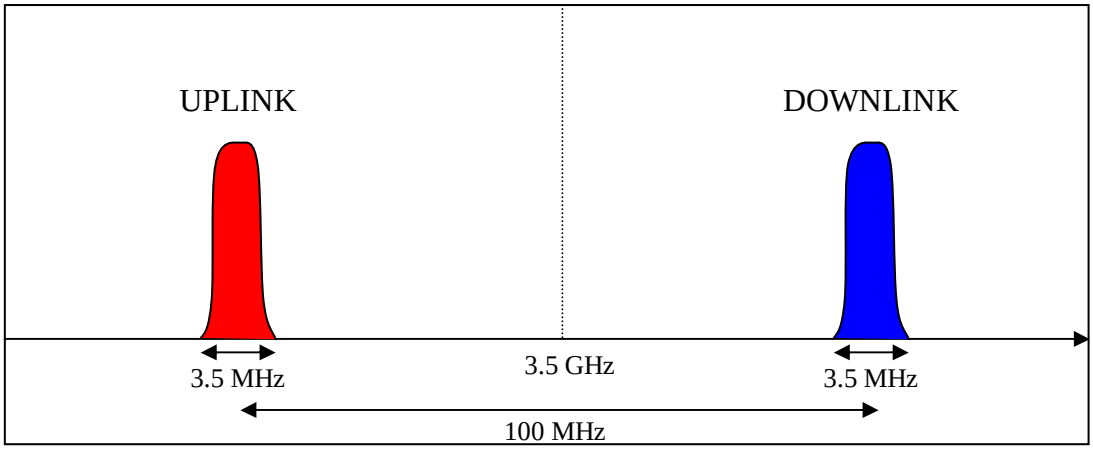

Figure 16. WiMAX spectrum in FDD operation

Compared to a single carrier (SC) system, using a large number of narrowband subchannels results to a very sudden power density drop at the border of the transmission band. This makes efficient use of the entire allocated band possible, as is typical for OFDM systems.

The carriers of the entire transmission band of a single transmission direction (UL or DL) are shown in Figure 17.

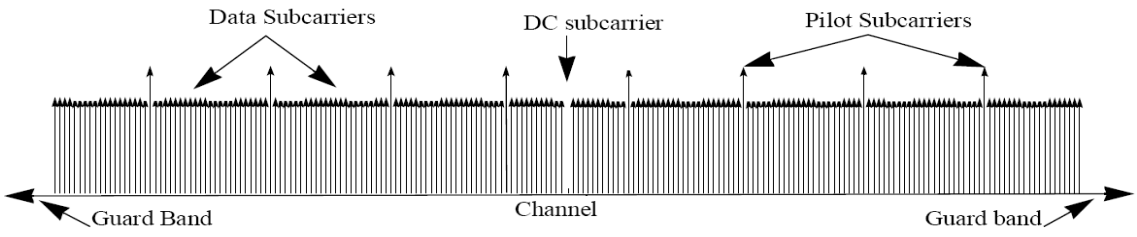

Figure 17. WiMAX subcarriers on the spectrum (UL/DL) [1]

According to [1] the subcarrier spacing for the system can be calculated from the equation

$$\Delta f = \frac{F_S}{N_{FFT}} = \frac{floor\left(\frac{n_{sampling} \cdot BW}{8000}\right) \cdot 8000}{N_{FFT}} \qquad (4)$$

where

F_S	sampling frequency (4.0 MHz),
N_{FFT}	number of points if FFT (256),
$n_{sampling}$	sampling factor (8/7 for channel bandwidths multiple of 1.75 MHz) and
BW	nominal channel bandwidth (3.5 MHz).

For the measured system, this results in subcarrier spacing of 15.625 kHz. The exact positions of the subcarriers can be determined using the frequency offset indices from the Table 3.

Table 3. WiMAX subcarriers

Subcarrier index	Other
-128 … -101	Guard
-100 … -89	Data
-88	Pilot
-87 … -64	Data
-63	Pilot
-62 … -39	Data
-38	Pilot
-37 … -14	Data
-13	Pilot
-12 … -1	Data
0	DC subcarrier
1 … 12	Data
13	Pilot
14 … 37	Data
38	Pilot
39 … 62	Data
63	Pilot
64 … 87	Data
88	Pilot
89 … 100	Data
101 … 127	Guard

For example the first pilot subcarrier of the downlink band can be found at the frequency

$$f_{pilot1} = (3545000 - 88 \cdot 15.625)\ \text{kHz} = 3.543625\ \text{GHz}\ . \qquad (5)$$

2.4 Chapter summary

In this chapter an overview of the basics of IEEE 806.16-2004 based WiMAX technology was presented. The standard family is still constantly evolving and now seems to have its major breakthrough as the mobile IEEE 802.16-2005 based WiMAX hits the market.

OFDM based systems offer efficient use of regulator allocated bandwidth due to the orthogonality of subcarriers and effective link adaptation with the standard defined capability of intelligibly adjusting modulation and coding. They also offer efficient

coding methods and channel equalisation to provide high speed, errorless connections. When operating with higher modulations (16-QAM ->), the channel equalisation process needs accurate channel state information as an input. Thus, the efficient implementation of channel estimation is of great importance in WiMAX.

On many parts, the implementation of the above mentioned features in commercial WiMAX systems has been left open in the standard, which can be seen not only as a factor giving desired freedom in design, but also as a future challenge what comes to compatibility of differently implemented devices.

3. Introduction to jamming

Due to the development of highly sophisticated encryption techniques, the decryption of enemy's messages is getting practically impossible. Since recovering the message is no longer possible, the only practical option left is to make it impossible for the enemy parties to communicate.

Jamming could be defined as the process of deliberately inserting man-made interference onto a medium, with the purpose of paralysing or destroying enemy's equipment. In this sense, paralysing can simply mean inserting enough interference onto the connection, so that adequate signal-to-noise-and-interference-ratio (SINR-ratio) can no longer be reached and the system can not function.

Jamming signals can be sent from whatever suitable device, for example from helicopter, airplane, car etc. The further away from the jamming target the jammer is, the more equivalent isotropic radiated power (EIRP) must be used. Hence, one of the key factors in successful jamming is to get the jammer close to the jamming target.

The basic idea is thus to accurately locate the jamming target and then use high gain antennas, high transmit powers and a suitable waveform to disrupt enemy communication. Accurately stated, the denial of accurate information consists of deception, disruption and destruction of information. [12] In the following subchapter the effect of the earlier mentioned parameters are more profoundly dealt with.

3.1 Jamming types

In the thesis two main jamming types are used: noise and multicarrier jamming. Noise jamming can be further divided into wide- and narrowband jamming according to on how large a fraction of the communication system frequency band the jamming is applied onto. Multicarrier jamming aims at jamming certain preselected carriers that have the most effect on the overall performance of the system.

3.1.1 Noise jamming

The goal of noise jamming is to insert an interference signal into the enemy communication system so that the wanted signal is completely submerged by the interference. This form of jamming is also known as denial jamming or obscuration jamming. The main idea of noise jamming is illustrated in Figure 18.

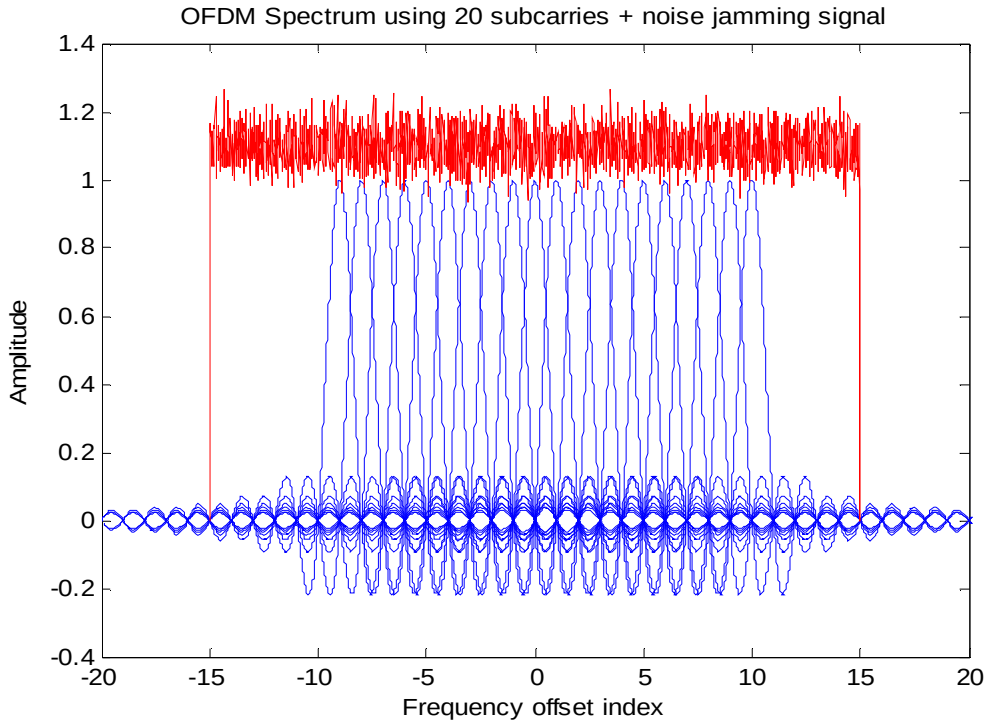

Figure 18. Wideband noise jamming

The optimal jamming waveform is intuitively white Gaussian noise (WGN), since from the information theory point of view, it has maximum entropy. [8] This conclusion can also be drawn from the fact that the receiver can not distinguish between jammer injected noise and its own. Based on the relationship between jammer bandwidth and that of the equipment, noise jamming can be categorised into narrow- (spot) and wideband (barrage) jamming. The relationship is conveniently expressed as

$$\frac{B_J}{B_{VS}} = \frac{Jammer\ bandwidth}{Victim\ system\ bandwidth}. \qquad (6)$$

Typically, if the ratio B_J/B_{VS} is less than 0.2 jamming is considered to be spot jamming and if greater than 1, barrage jamming.

The main advantage noise jamming has, is that very little about the enemy's equipment need to be known. However, there are great many factors, which make the performance of a noise jammer to drop below its theoretical capability. The fact that a noise jammer has to function on victim systems using arbitrary polarisations, generally leads to usage of either 45 degrees slant polarised or circularly polarized jammer radiations. This causes a rather modest ERP (Effective Radiated Power) drop of typically 3 dB, but more serious losses in the order of tens of dBs occur as a result of bad noise quality and e.g. orthogonal polarization between jammer and victim antennas. [7]

The easiest way of creating an effective noise jammer is to pass band-limited noise through an RF-amplifier and to the transmitting antenna. This method is also known as direct noise amplification (DINA). In the noise jamming measurements described in the following chapter, a WGN signal is first created in baseband, then modulated onto the selected RF and transmitted.

3.1.2 Multicarrier jamming

Multicarrier jamming differs from noise jamming by being suitable only for jamming the very system it is designed for. The general idea is to determine the most critical vulnerability of the victim system in terms of the carriers used and then inject a very narrowband signal, e.g. zero bandwidth sine signal, onto the those carriers. The idea is illustrated in Figure 19.

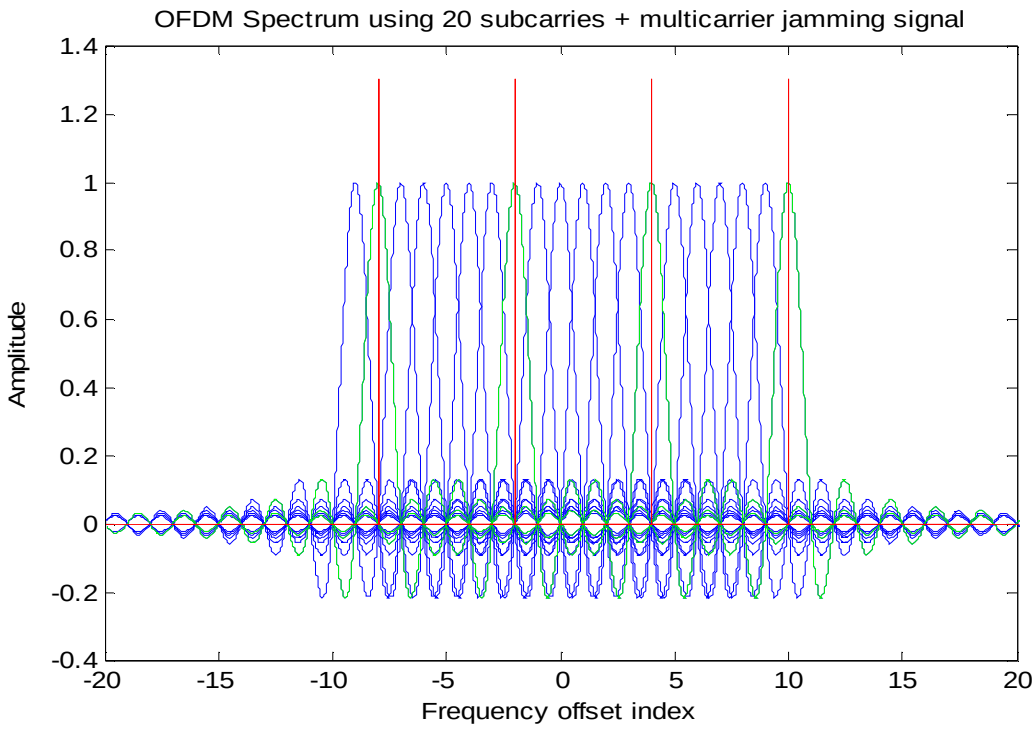

Figure 19. Multicarrier jamming signal injected on an OFDM signal

In Figure 19, a 20-carrier OFDM system with 4 pilot subcarriers (green) is used. The multicarrier jamming signal (red) is inserted onto the pilot subcarriers with frequency offset indices -8, -2, +4 and +10. In Figure 19, it is assumed that pilots are the critical vulnerability of the jammed system. In this case, the jamming signal is a zero bandwidth sine signal, which is also used in the measurement described in Chapter 4.

In WiMAX, channel equalisation is performed using 8 pilot subcarriers, which makes it intuitively one of the critical vulnerabilities of the WiMAX. The jamming of these subcarriers prevents the victim system from adequately correcting the effects of the channel on the signal. A successful channel equalisation is shown in Figure 20 and the effects of jamming on the 16-QAM constellation in Figure 21. It is assumed that only 0001 symbols are sent over the channel.

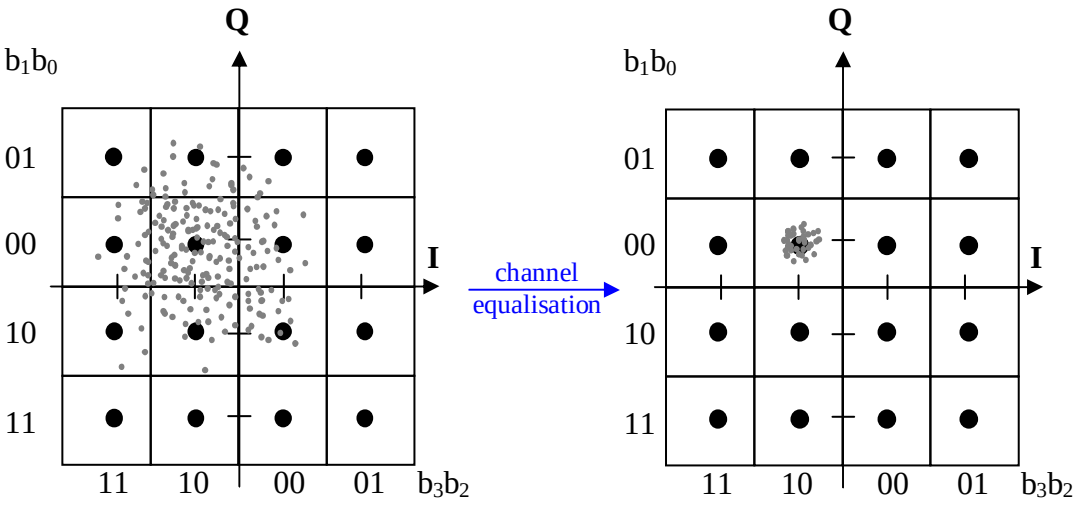

Figure 20. Successful channel equalisation

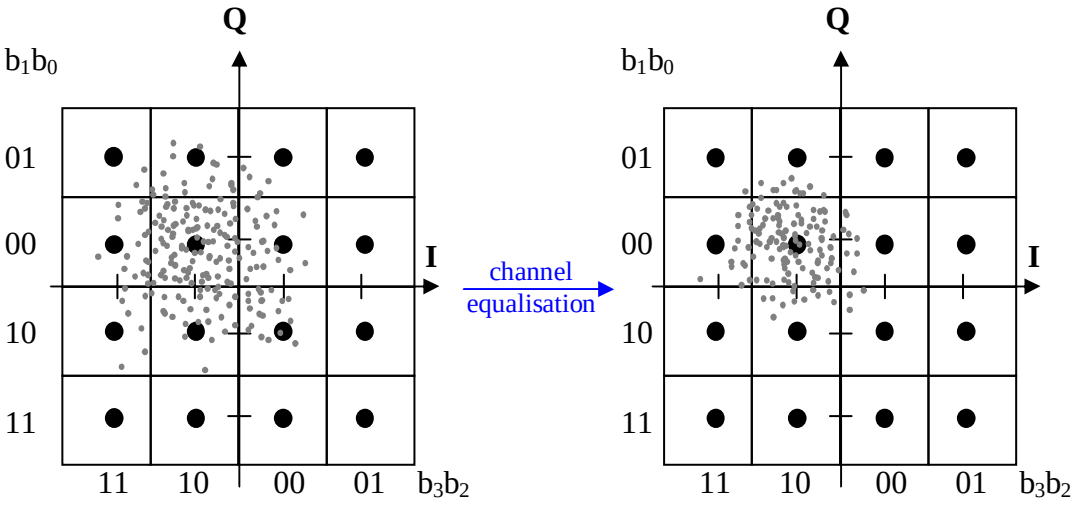

Figure 21. Unsuccessful channel equalisation caused by jamming

As can be noticed in Figure 21, the jamming of the victim system led to a number of false symbol decisions. Increasing the power of the multicarrier jamming signal increases the spread of the constellation and leads to a further degradation in the symbol error probability.

3.3 Chapter summary

In Chapter 3, the basic jamming types and their usage principles were presented. If no specific knowledge of the attacked system is available, noise jamming should generally be used. Its efficiency is based on the fact that white noise has maximum entropy, which makes it practically impossible for the victim system to separate noise from the desired signal.

If the attacked system is already known in detail, there may be other, more efficient ways of deteriorating the performance of the system. One such method, in the case of WiMAX, is jamming its pilot subcarriers. For other systems there can be other vulnerabilities and of course differently implemented WiMAX transceivers may not be as vulnerable to pilot jamming as the one analysed in Chapter 5.

4. Measurement setup

The measurement setup used in the jamming measurements consists of a WiMAX base transmitter station (BTS), customer premises equipment (CPE), cables, attenuators, directional coupler, spectrum analyzer and signal generator. For the downlink jamming measurements the setup is illustrated in Figure 22 and for the uplink in Figure 23.

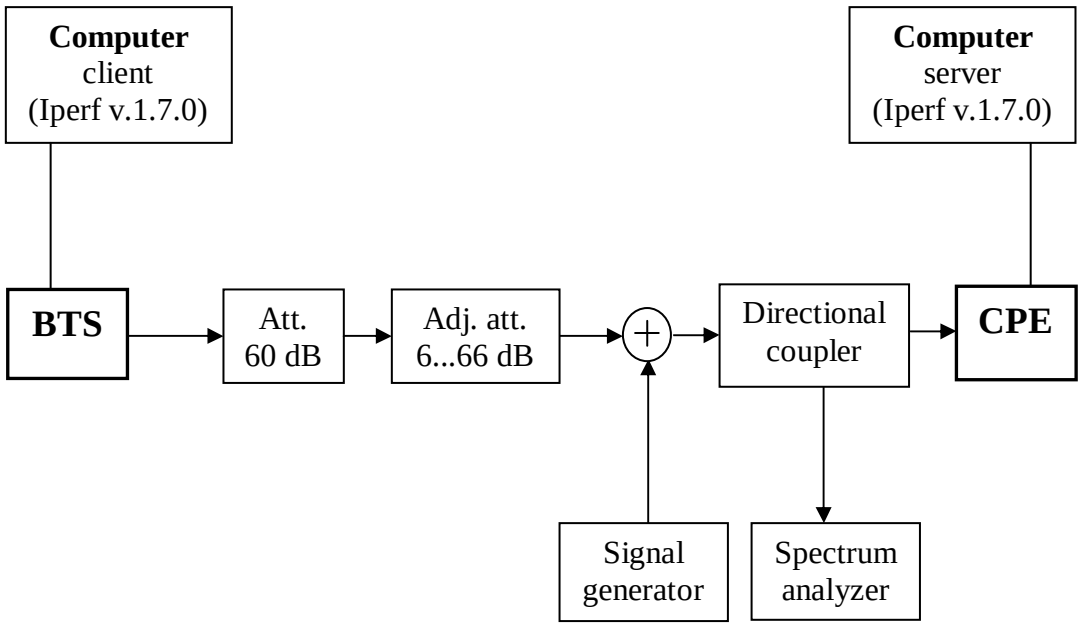

Figure 22. Measurement setup (Downlink measurement)

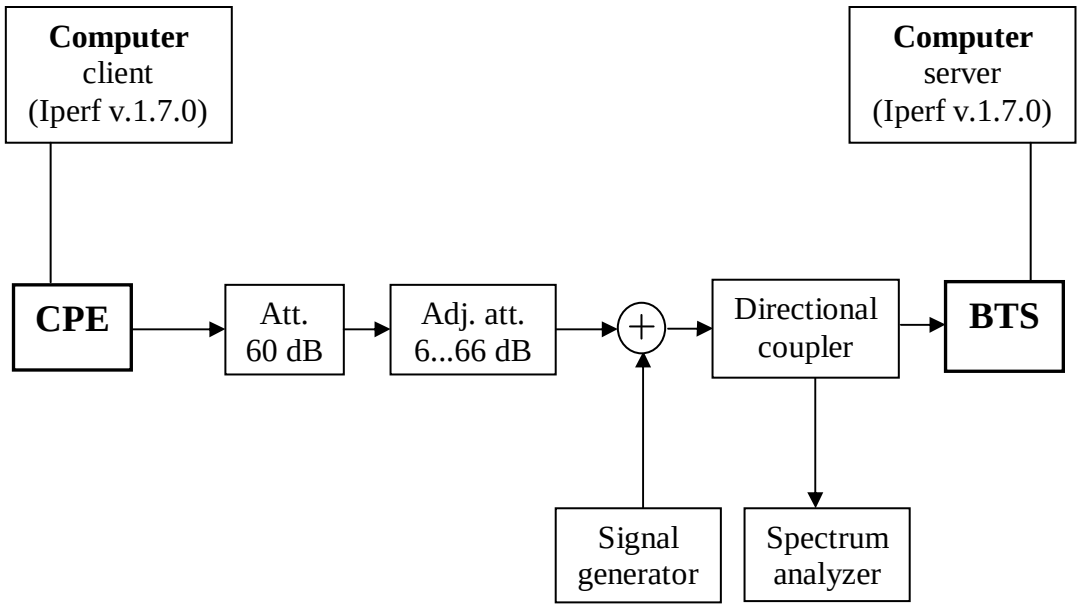

Figure 23. Measurement setup (Uplink measurement)

The attenuation normally caused by the additive white Gaussian noise (AWGN) radio channel is generated using two attenuators, a fixed attenuator of 60 dB and an adjustable attenuator (6 … 66 dB). The adjustable attenuator is used to create a typical operating condition for each modulation, which can be expressed as

$$\textit{typical received power level} = \textit{rec. sensitivity (standard)} + \textit{fade margin}. \quad (7)$$

In the measurement, the typical received power level is calculated using the sensitivity requirements defined in the standard and adding a 20 dB fade margin. For instance, for QPSK 3/4 standard defines a sensitivity of -86 dBm, thus the signal is attenuated so that the power level of -66 dBm is received. For a Rayleigh fading channel, the 20 dB fade margin would correspond to time availability of about 99 %. [13]

Cables are radio frequency coaxial cables, whose overall attenuation with connectors, the spectrum analyzer and signal generator in different measurement settings is calculated in Section 4.4.

Spectrum analyzer is connected in parallel to the radio path using a directional coupler in order to observe the changes in the system's operational state and to verify that the jamming signal is of the correct bandwidth and accurately located on the transmission band. Signal generator is used to create the jamming signal and to inject it onto the jammed band.

4.1 Generation of jamming signals

The jamming signals were created using a Rohde & Schwarz SMJ100A signal generator (Figure 24) and the base band white Gaussian noise signal with WinIQSIM v. 4.30 software (Figure 25) created by Rohde & Schwarz.

Figure 24: Rohde & Schwarz SMJ100A signal generator

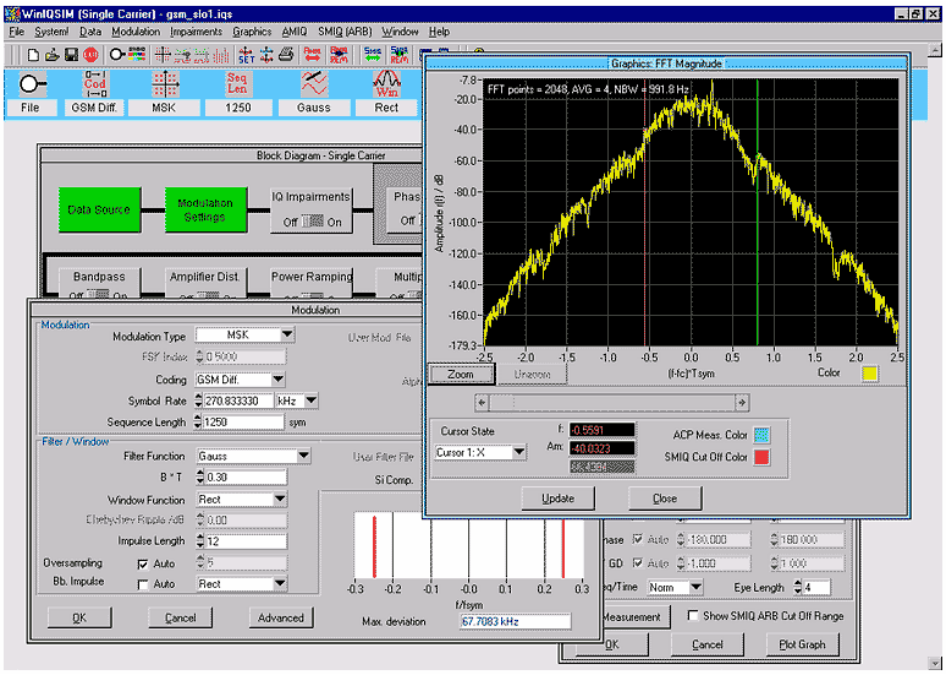

Figure 25: Rohde & Schwarz WinIQSim program

The parameters of the different types of jamming signals are presented in Table 4 and a graphical illustration in Figure 26. In Sections 4.1.1 and 4.1.2, the generation of different jamming signals used in the measurement will be explained in greater detail.

Table 4. Jamming scenarios used in the measurement

Jamming scenario	Noise/pilot jamming	Bandwidth (%)	Other
1	Noise	10	Narrowband (spot)
2	Noise	50	
3	Noise	120	Wideband (barrage)
4	Pilot	Zero-BW sine signal	Pilot 4 (UL), Pilot 7 (DL)
~~5~~	~~Pilot~~	~~4 Zero-BW sine signals~~	~~4 pilots~~
~~6~~	~~Pilot~~	~~8 Zero-BW sine signals~~	~~All 8 pilots~~

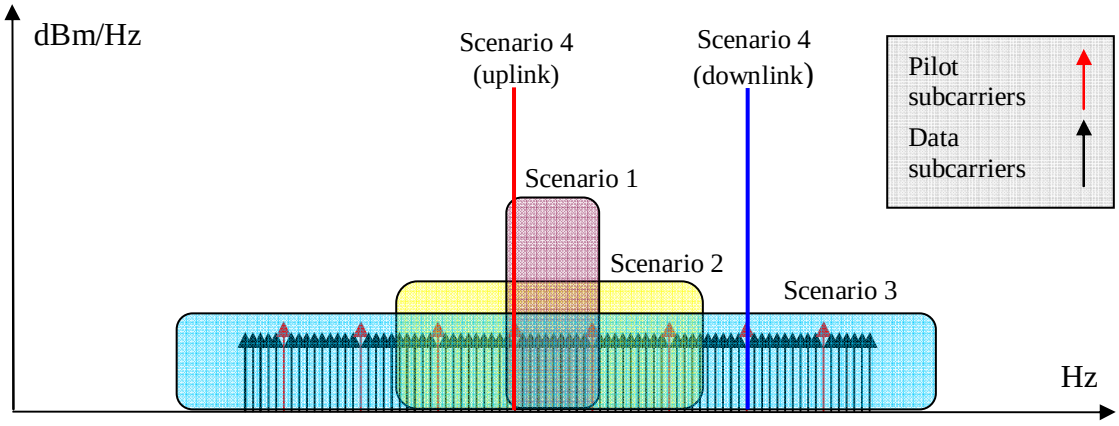

Figure 26: Jamming scenarios

4.1.1 Noise jamming

For the jamming Scenarios 1-3, a white Gaussian noise (WGN) signal was first created in base band with the WinIQSIM software and modulated onto RF using signal generator's integrated I/Q-modulator.

The bandwidth of the noise signal was selected by altering the clock frequency of the arbitrary waveform generator (ARB) of the signal generator and verified with the spectrum analyzer (Figure 27). The base band noise signal consists of 12000 samples and can thus be considered satisfactorily random in nature.

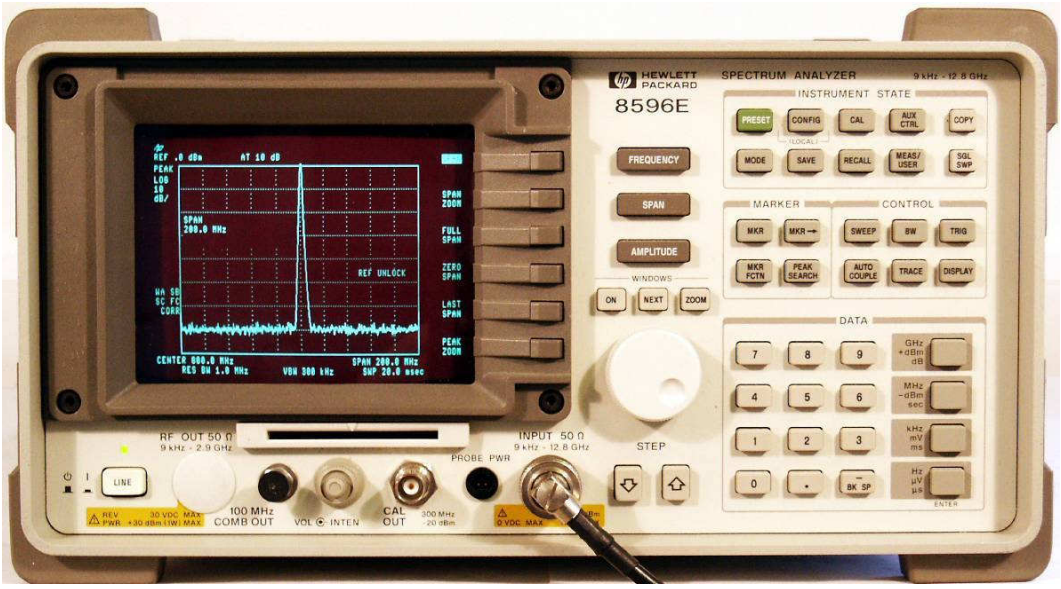

Figure 27: Hewlett Packard 8596E spectrum analyzer

The centre frequency of the jamming signal was chosen to be the same as that of the WiMAX system. Of course, especially for the spot jamming case, if the noise jamming would be set to optimally overlap certain pilot subcarriers, the effect on the system might be more significant. However, noise jamming is usually used when no specific knowledge or equipment is available to attack the victim system and on the other hand, jamming of the pilots is already studied in another measurement.

The idea of studying the impact of the bandwidth of the noise jamming signal on the performance of the system is conducted to study the compromise needed to be done between the spectral power density (dBm/Hz) of the jamming signal and its spectral coverage (percentage of the system BW). For narrowband jamming (Scenario 1), the achieved spectral power density is high, but the covered fraction of the system BW is modest. The system could therefore possibly transmit data using the subchannels not covered by the jamming signal. On the other hand, using a wideband jamming signal (Scenario 3) makes it possible to cover the entire operational BW, but the spectral power density with the same jamming power remains low.

4.1.2 Pilot jamming

Multicarrier jamming signal was planned to be studied in jamming Scenarios 5 and 6 (Table 4) but due to the limitations of the used signal generator this could not be performed. Scenario 6 with 8 jamming carriers could not be studied, because of the different distance between the 5th and the 6th pilot subcarrier.

Scenario 5 could not be actualised because the multicarrier jamming signal created using the signal generator integrated signal creation tool did not place the carriers at their exact intended positions. Adjusting the distance manually with the help of the spectrum analyzer did not help, since there seemed to be discreteness in the possible positions of the carriers in the order of a few kHz. Because of the very high accuracy needed to make jamming effective, proceeding would have given false conception of the performance of the multicarrier jamming signal.

The only studied pilot jamming scenario now includes jamming of individual pilots. The jamming signal is a pure sine signal located exactly at the frequencies of the pilot subcarriers, which are given in Table 5. Because of the additional DC subcarrier, the frequency gap between 4th and 5th subcarrier is 406.25 kHz while for other it is 390.625 kHz.

Table 5. Pilot and DC subcarrier frequencies

Uplink frequency (Hz)	Downlink frequency (Hz)	
3443625000	3543625000	1st pilot
3444015625	3544015625	2nd pilot
3444406250	3544406250	3rd pilot
3444796875	3544796875	4th pilot
3445000000	3545000000	DC subcarrier
3445203125	3545203125	5th pilot
3445593750	3545593750	6th pilot
3445984375	3545984375	7th pilot
3446375000	3546375000	8th pilot

4.2 Packet error ratio measurement

The effect of jamming was conceptualized using a typical measure known as packet error ratio (PER), which can be expressed as

$$PER = \frac{Number\ of\ erronous\ packets}{Number\ of\ packets\ sent} \quad . \tag{8}$$

The measurement was conducted by transmitting constant length (8 kb) UDP (User Datagram Protocol) packets over the connection (Figures 28 and 29), with a constant transmission rate of 95 % of the measured maximum throughput allowed by the selected modulation/coding combination. The transmission rate was selected 5 % lower than the maximum to make sure that no errors occur because of the small fluctuations in the system capacity caused by the software, computers, network adapters etc. UDP packets very chosen to minimize the signalling traffic over the connection so that only real effects on the transmission rate could be monitored. Of course, effects of jamming on a connection with a need for 0 % PER (such as TCP) also have great significance, but are completely of different nature and therefore not covered in this thesis.

The measurement was performed using iPerf v.1.7.0, which is considered a good measurement tool due to its simplicity and the fact that it consumes very little resources. First the receiving end of the connection was initialized as the server (Figure 28) and the transmitting end as the client (Figure 29).

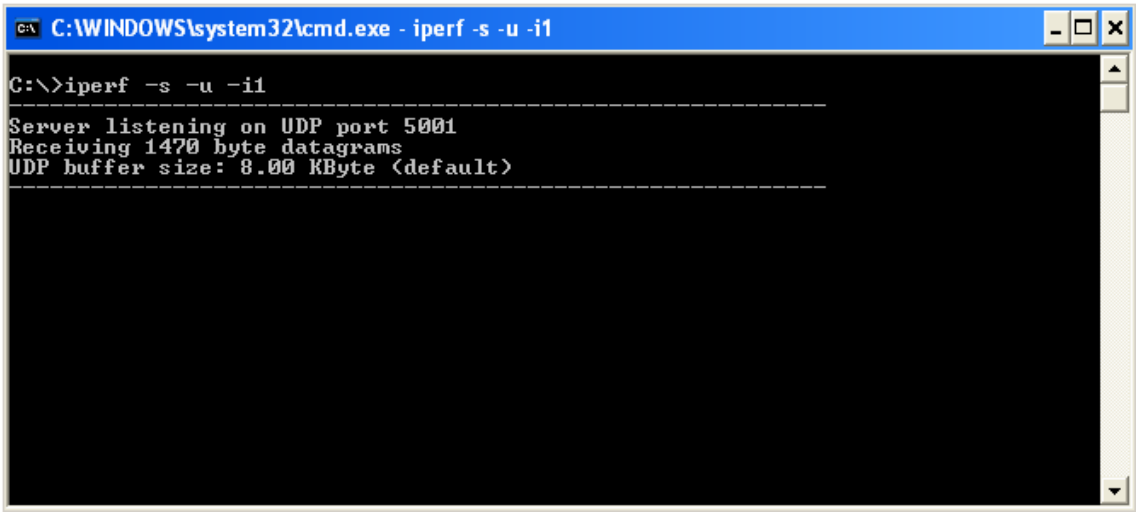

Figure 28: Iperf v.1.7.0 running in server mode

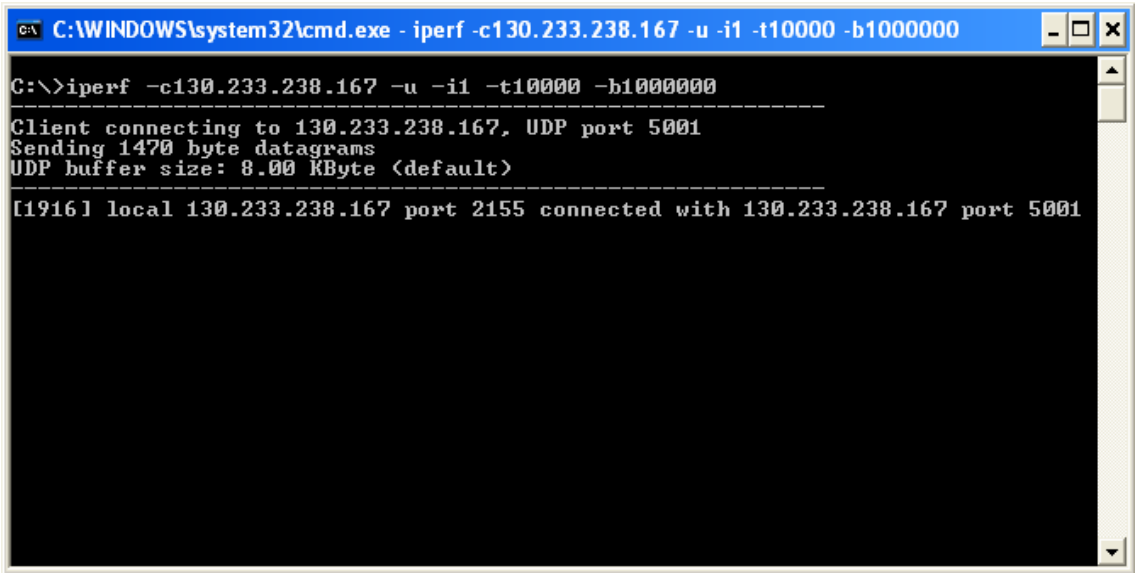

Figure 29: Iperf v.1.7.0 running in client mode

The server was set to report the transmission PER every second and the jamming power needed to reach certain PER was written down. Due to the large number of measurements (~500), the jamming power values were taken as the PER value mostly stabilized between the values shown in the Table 6 having its average with good accuracy at the intended PER for a period of 10 seconds.

Table 6. Packet Error Ratio ranges used in the measurements

PER (%)	0	5	30	60	100
PER range (%)	0	3…7	20…40	50…70	100

An example of on ongoing 16-QAM 3/4 downlink PER-measurement aiming at 30 % PER is illustrated in Figure 30.

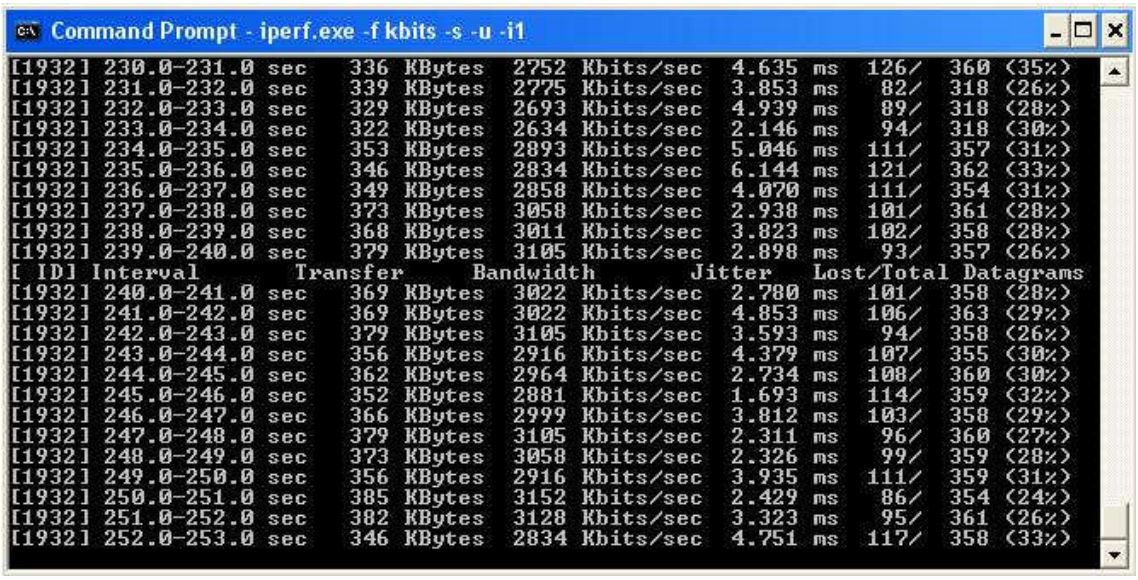

Figure 30: 16-QAM 3/4 PER measurement (PER = 30 %)

In Figure 30 on the right the PER value is shown (24 % … 35 %), which falls in the range (20 % … 40 %) defined in Table 6. The average of the PER values in the window is 29.1, which can be considered to be sufficiently near PER = 30 % that was the target value. The measurements targeting at other PERs (e.g. 60 %) were performed in a similar manner.

4.3 Receiver sensitivity measurement

Receiver sensitivity measurement is performed to see how well the requirements set by IEEE 802.16-2004 standard have been met. Should the sensitivity exceed the requirements, the functionality of the receiver at the standard sensitivity defined coverage area borders can be expected to be good.

The measurement is performed by transmitting UDP packets at 95 % of the modulation and coding enabled maximum throughput separately for both transmission directions.

The connection is then attenuated using the adjustable attenuator until transmission errors start to occur or the system drops the connection.

Measured receiver sensitivity can now be calculated from the equation

$$rec.\ sensitivity = transmitted\ power - fixed.\ att. - adj.\ att. - cable\ att. \quad (9)$$

where
transmitted power = power transmitted by CPE (uplink) or BTS (downlink) in dBm,
fixed att. = attenuation caused by fixed attenuator (60 dB),
adj. att. = attenuation caused by adjustable attenuator (6 … 66 dB),
cable att. = attenuation caused by cables (≈ 0.5 dB).

4.4 Cable attenuation measurement

Cables and connectors used in the measurement are RF-components, but at frequencies high as 3.5 GHz, they cause significant attenuation to the signal. In order to calculate PER vs. SJR (Signal-to-Jamming-Ratio) curves correctly, the impact of these and that of the signal generator and spectrum analyzer have to be carefully taken into account.

In the PER measurement BTS and CPE were at the ends of the connection (Figures 22 and 23). Here, they have been replaced by the signal generator and the spectrum analyzer. The spectrum analyzer and the signal generator as they were in the PER measurement, are here replaced by 50 Ohm loads. The attenuation caused by cables, connectors, directional coupler, signal generator and spectrum analyzer is measured by feeding a 3.5 GHz sine signal through the measurement system and measuring the input power with the spectrum analyzer. The whole setup is illustrated in Figure 31.

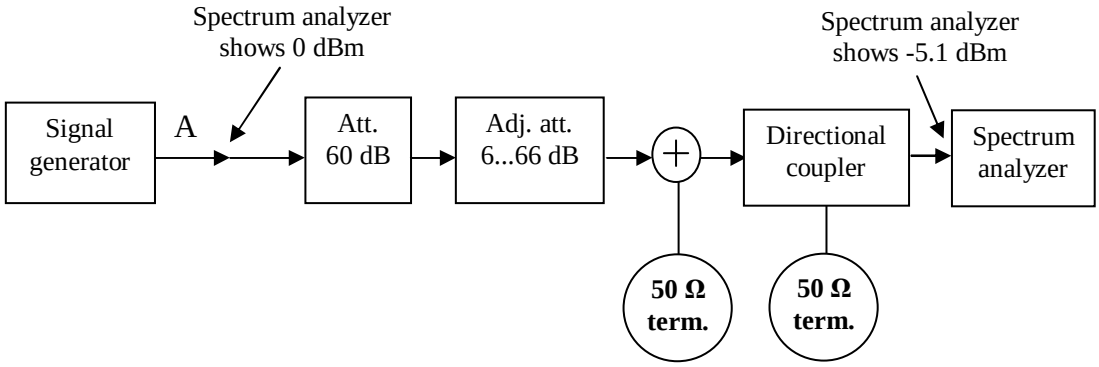

Figure 31. Cable attenuation measurement setup

Before the actual measurement a short, 30 cm, cable (A) is connected between the signal generator and the spectrum analyzer and the received power by the spectrum analyzer is set to 0 dBm by adjusting signal generator transmitted power (Figure 32). In this case, the signal generator transmitted signal needed was 0.2 dBm.

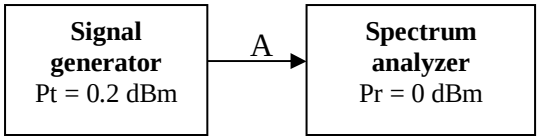

Figure 32. Cable A attenuation measurement

The same cable (A) is used when measuring the attenuation of the whole setup allowing its effect to be cancelled. While keeping the transmitted power at 0.2 dBm, the attenuation of the whole system without cable A can now be simply expressed by the Equation 10.

Total attenuation (dB) = received power (dBm) (10)

Now the spectrum analyzer received signal power was –5.1 dBm, meaning simply that the attenuation of the rest of the measurement system was 5.1 dB. Since the setup without cable A is used in the jamming measurements, this value can also be considered total attenuation of the measurement system.

4.5 Chapter summary

In this chapter, the measurement setup used in jamming, cable attenuation and sensitivity measurements was presented and the procedure for measuring packet-error-ratio was explained. For verification, the attenuation caused by components in the measurement system was measured for both the WiMAX signal and the injected jamming signal.

The generation of different jamming signals was illustrated and the limitations of the generator resulting in fewer jamming scenarios than planned were presented. The waveform and bandwidth of the jamming signal were verified with the spectrum analyzer connected parallel to the measurement system.

5. Measurement results analysis

Four different jamming scenarios were measured, three being noise jamming scenarios and one targeted at jamming individual pilots. Multipilot jamming scenarios were planned to be measured, but could not be realised due to limitations of the software of the signal generator described in Chapter 4.

In the following sections, the results are graphically presented e.g. by using signal-to-jamming-ratio (SJR) vs. packet-error-ratio (PER) curves. First the downlink measurement results are analyzed with all the possible modulation/coding combinations for different jamming scenarios. In Chapter 5.4 uplink is analysed for BPSK ½ and downlink jamming scenarios are summarized. Uplink modulation could not be kept constant, since jamming the connection always led to the system dropping modulation. Thus, the data for uplink consist only of BPSK ½ measurements and therefore no deep downlink vs. uplink analysis will be performed. All the measurement based curves are presented in Appendixes I and II and the measurement data in Appendixes III and IV.

In Table 7, minimum receiver signal-to-noise-ratio (SNR) required for BER = 10^{-6} after forward error correction (FEC) is presented assuming 7 dB noise figure and 5 dB implementation margin. The SNR values given in Table 7 can be used to evaluate the performance of the system especially under wideband noise jamming, since its effect can simply be considered as an increase in noise level (or drop in SNR). Other types of jamming signals can then be compared to the performance under wideband jamming.

Table 7. Required receiver SNR to reach BER = 10^{-6} after FEC [1]

Modulation	Coding rate	Receiver SNR (dB)
BPSK	1/2	6.4
QPSK	1/2	9.4
	3/4	11.2
16-QAM	1/2	16.4
	3/4	18.2
64-QAM	2/3	22.7
	3/4	24.4

Here signal-to-jamming-ratio is defined as

$$Signal\text{-}to\text{-}Jamming\text{-}Ratio = \frac{Signal\ Power\ (W)}{Jamming\ Power(W)} \quad (11)$$

and in decibels as

$$Signal\text{-}to\text{-}Jamming\text{-}Ratio\ [dB] = Signal\ Power\ [dBm] - Jamming\ Power\ [dBm] \quad (12)$$

where

Signal Power= Signal power received by BTS (uplink) or CPE (downlink),

$= P_{t,\,signal} - A_{fixed} - A_{adj.} - A_{cables1}$,

where

$P_{t,\,signal}$ = Transmitted signal power by BTS (DL) or CPE (UL)

A_{fixed} = Fixed attenuator attenuation (60 dB)

$A_{adj.}$ = Adjustable attenuator attenuation (6 … 66 dB)

$A_{cables1}$ = Attenuation caused by cables and connectors (5.1 dB) and

Jamming Power = Jamming power received by BTS or CPE.

$= P_{t,\,jamming} - A_{cables2}$,

where

$P_{t,\,jamming}$ = Transmitted signal power by the signal generator

$A_{cables2}$ = Attenuation caused by cables and connectors (4.5 dB)

The packet-error-ratio values are calculated as defined by Equation 8.

5.1 Downlink noise jamming (scenarios 1-3)

In downlink measurements for Scenario 1 (Figure 33), a narrowband (B_J/B_{VS} = 10%) jamming signal was summed to the WiMAX signal having a centre frequency of 3.545 GHz. For modulation methods QPSK ¾ to 64-QAM ¾ it seems that the SJRs follow the SNRs given in Table 7, but for the two lowest modulations BPSK ½ and QPSK ½ the jamming is not as effective.

The better performance using lower modulations can be explained by the fact that they don't need as efficient channel equalisation as the higher ones. For BPSK and QPSK there are no multiple amplitude levels in the constellation, which makes them rather insensitive to AGC saturation. In this case, the jamming signal was located at the centre of the downlink band, which makes it overlap pilot subcarriers 4 and 5. Due to its high spectral density, the jamming signal was able to detoriate the channel equalisation process effectively, but didn't overlap enough data subcarriers to be efficient when using lower modulations.

The effect of moving the jamming signal to another part of the WiMAX spectrum was not studied, but is worth noting. In Section 5.2, where pilot jamming is studied, it is noticed that jamming the pilot subcarriers is the most efficient form of jamming studied here. Naturally, should the jamming signal overlap only one pilot which is possible, the impact on the performance of the victim system would not probably be as severe.

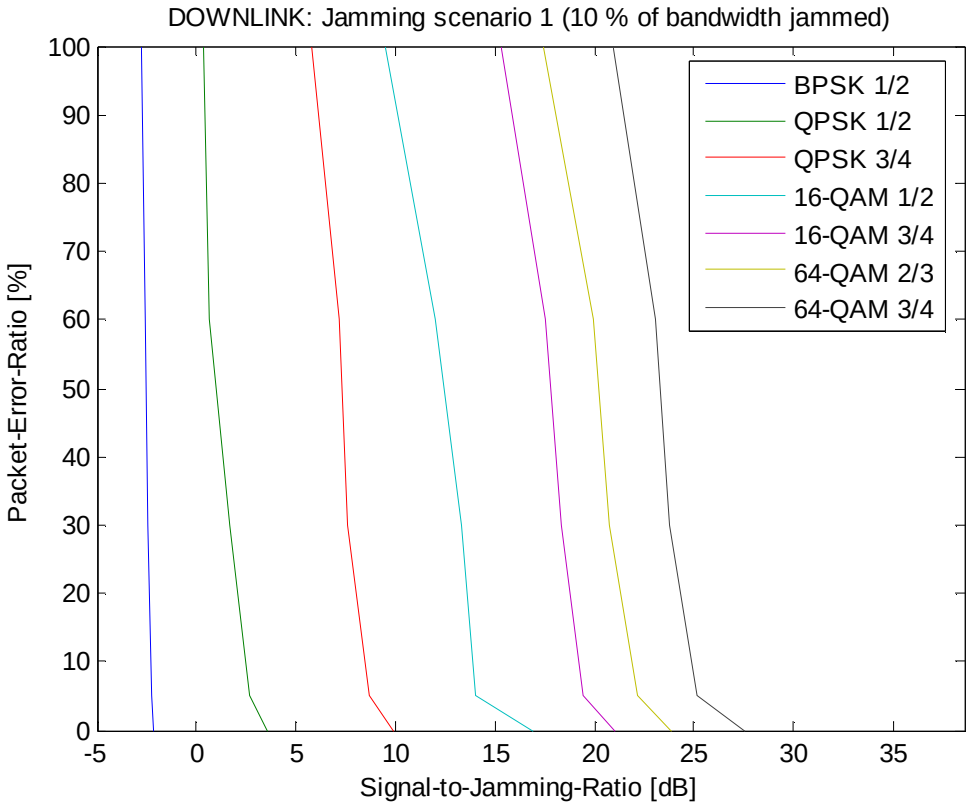

Figure 33: Downlink jamming (Scenario 1)

In Scenario 2 (Figure 34), a jamming signal with 50 % of the bandwidth of the WiMAX system was used centred at the centre frequency of the victim system. The downlink measurements show that, compared to Scenario 1 (Figure 33), the jamming now affects the lowest modulations rather effectively. This leads to the conclusion that the system is not resistant to the jamming form, even if it does not need very good channel estimation. This can be justified by thinking that, leaving channel equalisation aside, the noise occupies enough of the whole band making it impossible for the system to ignore it.

However, now that the jamming power is spread on a wider frequency range, the pilots can form a good channel estimate, which is the crucial especially when operating with 16- and 64-QAM modulations. This can easily be seen by comparing 64-QAM ¾ curves in both the Scenarios 1 and 2.

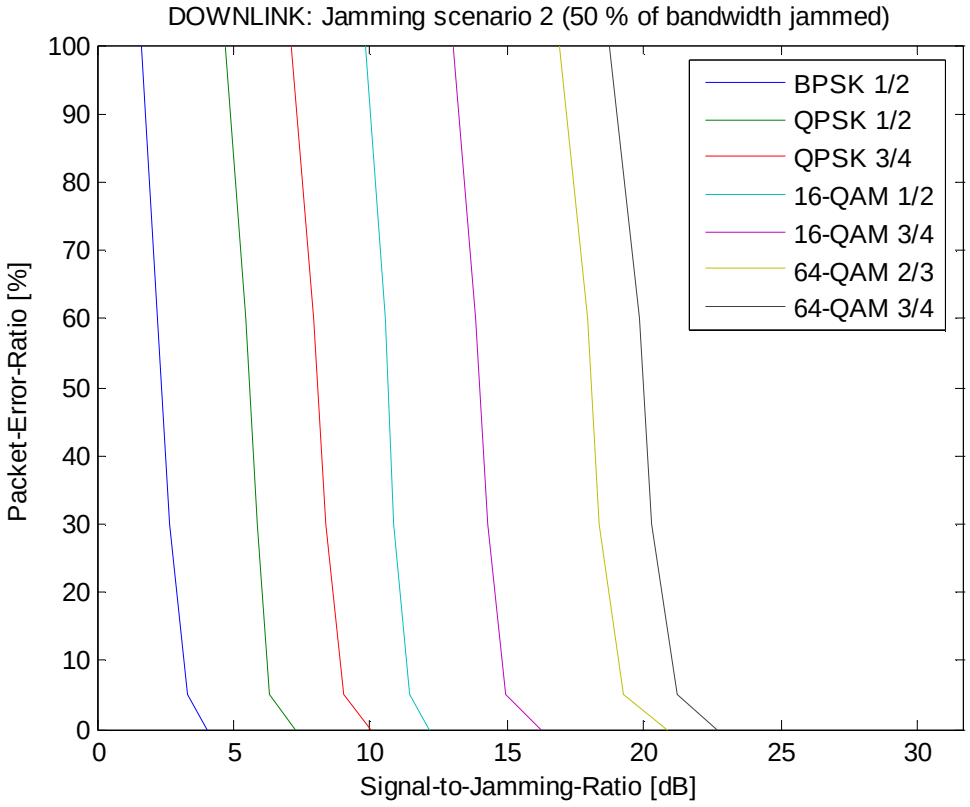

Figure 34: Downlink jamming (Scenario 2)

In the wideband jamming case (Figure 35), a noise jamming signal occupying 120 % of the system bandwidth was inserted onto the transmission medium. Compared to Scenario 2, the results seem to be rather similar. To reach the same performance the system now seems to need a bit lower SJR, which can partly be explained by the fact that the jamming signal now occupies 20 % more bandwidth than would have been needed and about 16.7 % of the jamming power is therefore wasted.

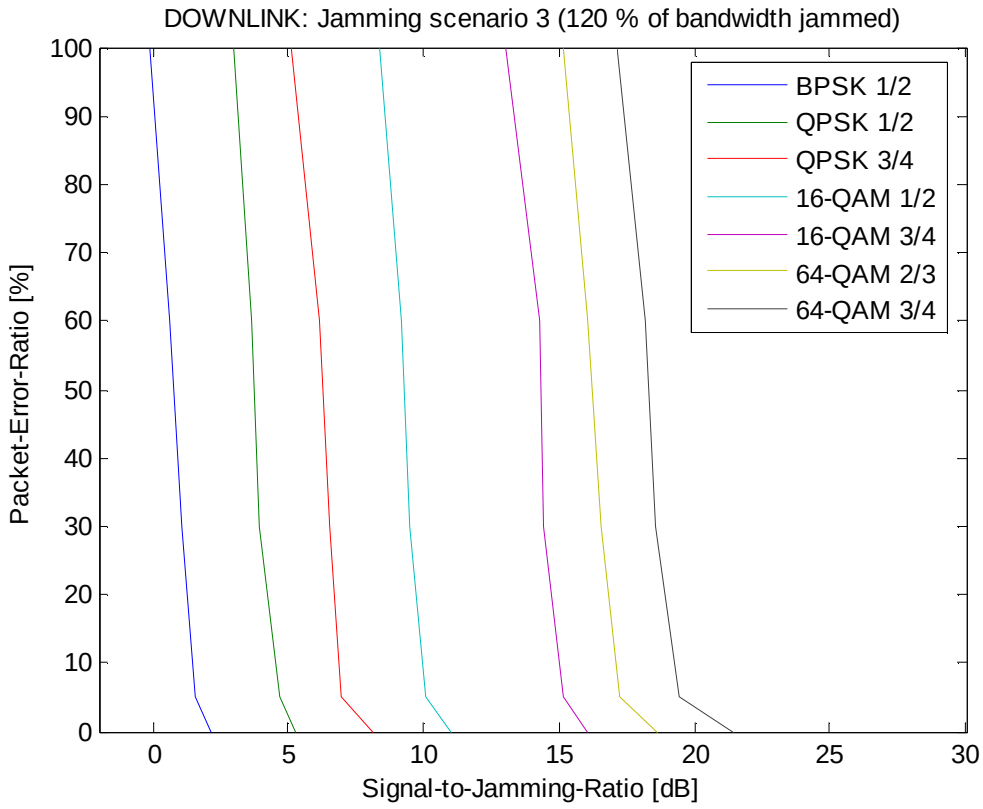

Figure 35: Downlink jamming (Scenario 3)

5.2. Downlink pilot jamming (scenario 4)

In jamming Scenario 4, a sine signal was inserted at the centre frequency of one pilot at a time, and their relative vulnerability was determined by comparing the needed jamming power. The most vulnerable pilot subcarrier appeared to be 7th for the downlink and 4th for the uplink jamming. The needed jamming power to reach PER = 5% for each of the pilot subcarriers is illustrated in Figure 36.

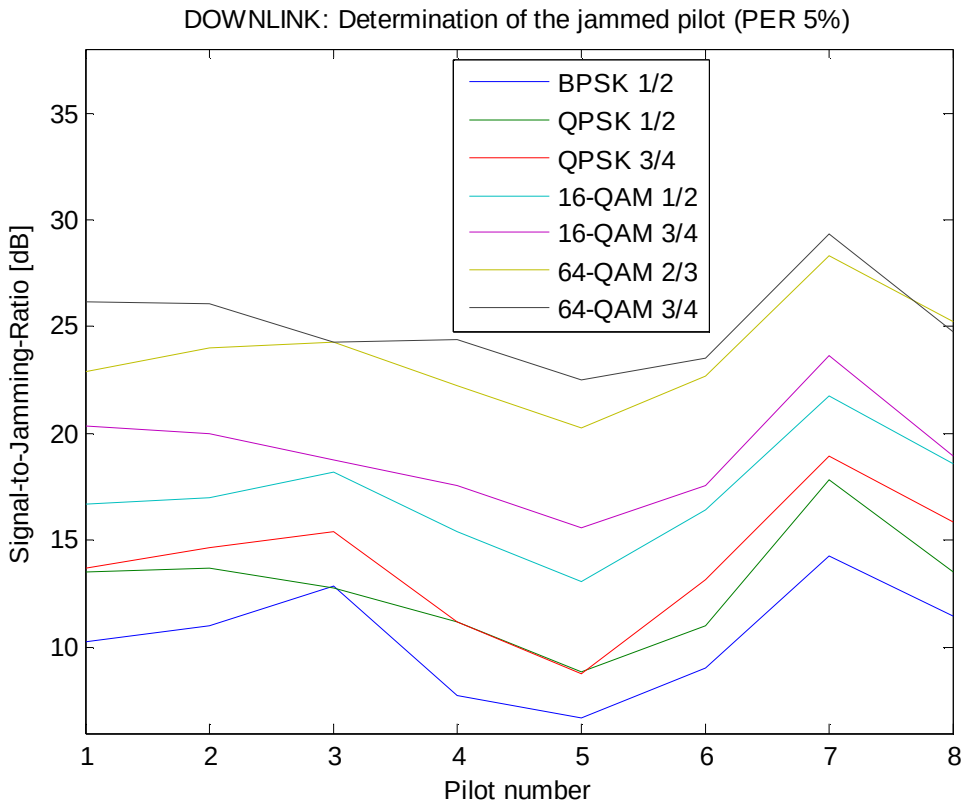

Figure 36: Determination of the jammed pilot (Downlink)

What is somewhat surprising is the difference in the jamming power needed to detoriate system performance by jamming individual pilot subcarriers. For example, when operating with BPSK ½ the difference in the needed jamming power when jamming different pilot subcarriers can be up to 7.5 dB (pilots 5 and 7). One could also expect that there would be some symmetry what comes to the vulnerability of the pilots, i.e. pilots 1 and 8, 2 and 7, and so on, would act in a similar manner. This appears not to be true, either.

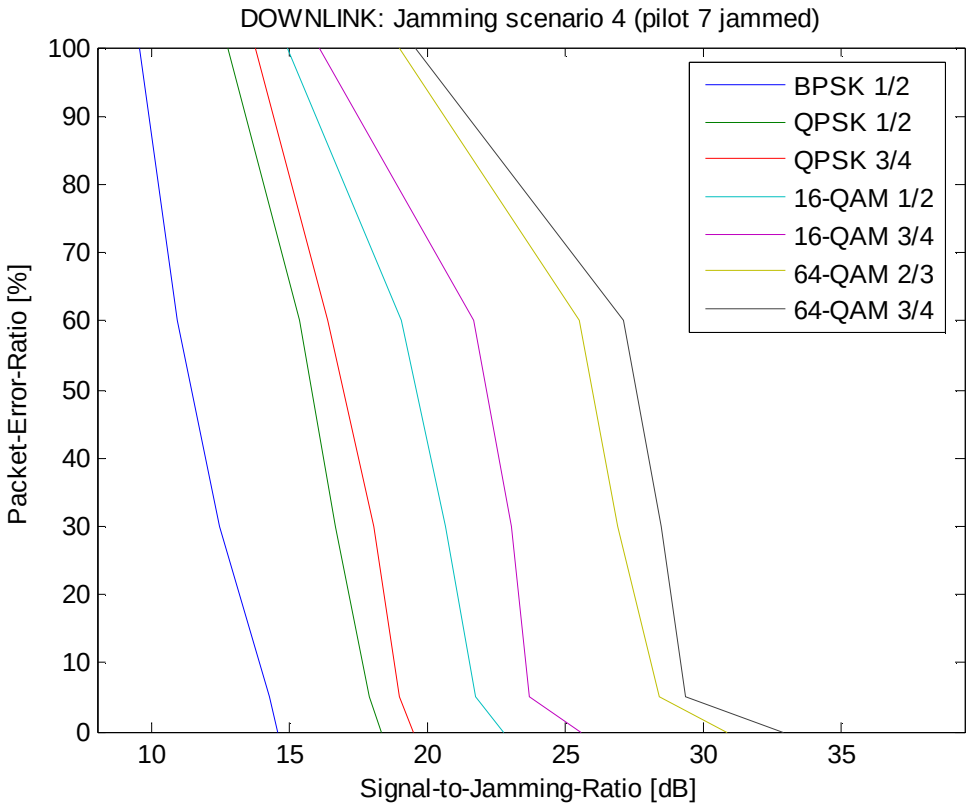

Figure 37: Downlink jamming (Scenario 4)

As the weakest pilot was determined, a similar PER measurement as with Scenarios 1-3 was performed. The result shows clearly that jamming the 7th pilot is a far more efficient way of attacking the system than the ones used in Scenarios 1-3. The jamming power needed is now about 10 dB less, than with the second most efficient scenario (i.e. Scenario 2). However, since the implementation of the channel equalisation is vendor specific, the results shown here apply only for the very system studied.

It can also be noticed that the performance (i.e. PER) does not go down as quickly as in Scenarios 1-3. Using the highest modulations, the difference of the 0 % and 100 % PER is now about 14 dB as with earlier scenarios it was only about 4 dB. The phenomenon could be explained by the receiver saturation which, however, is not very likely since, by changing the transmission frequency of the signal generator, it was noticed that moving the jamming signal away from its exact intended position on the transmission band reduced the measured PER significantly. Therefore, it is concluded that the channel equalisation is not possible for the data subcarriers closest to the jammed pilot.

Thus, the theory based assumption of the pilots being the system's weak spot can be considered to have been justified. The reasoning is clarified in Figure 38.

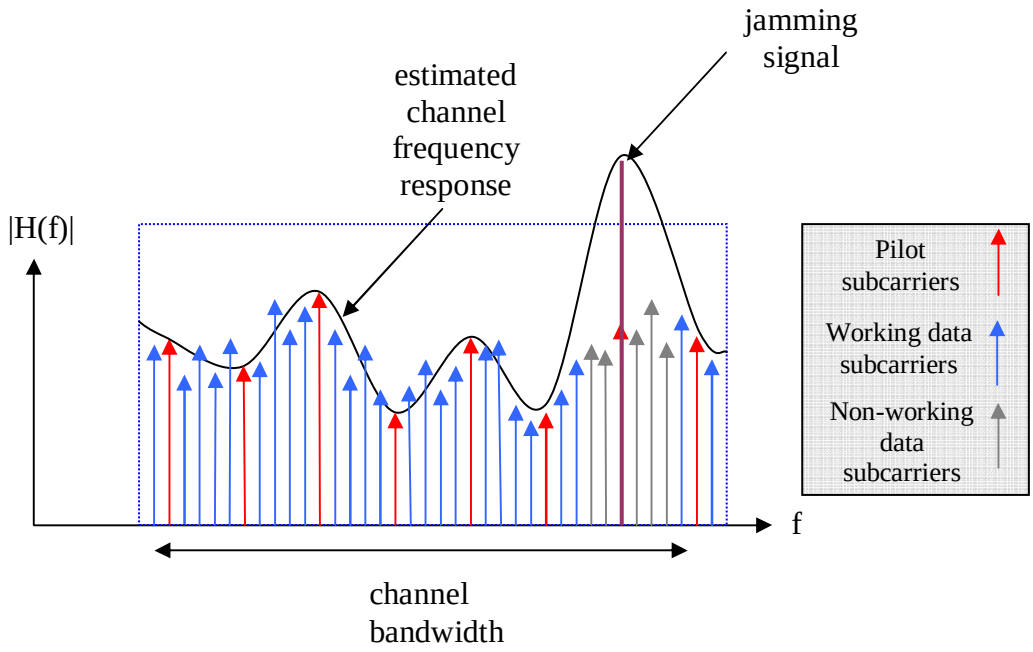

Figure 38: The effect of pilot jamming on system performance

Figure 38 now illustrates how the performance of the system drops as more and more data subcarriers stop to function as the jamming power increases. Had it been possible to inject a multipilot jamming signal to the system, a more sudden decrease in performance would probably have happened.

5.3 Comparison of jamming scenarios (UL and DL)

The comparison of jamming modes in downlink jamming provides some insight into how the system actually functions. With the lowest modulations not needing accurate CSI, it seems that narrowband jamming can be easily ignored. Jamming a larger fraction of the system bandwidth is more effective, but the only fairly easy way to deteriorate system performance is to jam a pilot subcarrier, especially the 7^{th} (Figure 39). Naturally, this is a system specific feature and thus the jamming performance of another system can be different.

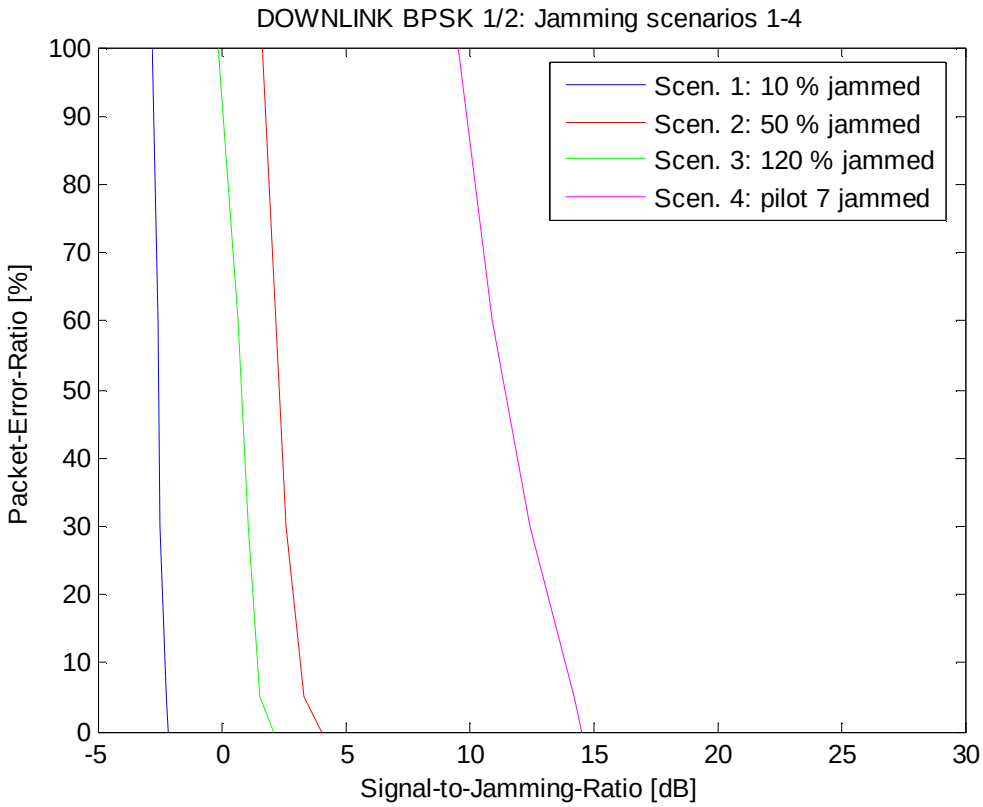

Figure 39: Comparison of DL jamming scenarios (BPSK 1/2)

As we move to jamming the system operating with more advanced modulations (Figure 40), jamming the 7th pilot is still clearly the most effective type of jamming. However, the increased need for accurate channel estimation becomes clear, since the narrowband jamming is now getting more effective compared to the ones jamming a larger bandwidth. Thus, it is concluded that the narrowband jamming actually starts to function as if it was a form of pilot jamming by overlapping pilot subcarriers 4 and 5. The reason it is still far more inefficient compared to Scenario 4, is the fact that it wastes most of its power on the data subcarriers.

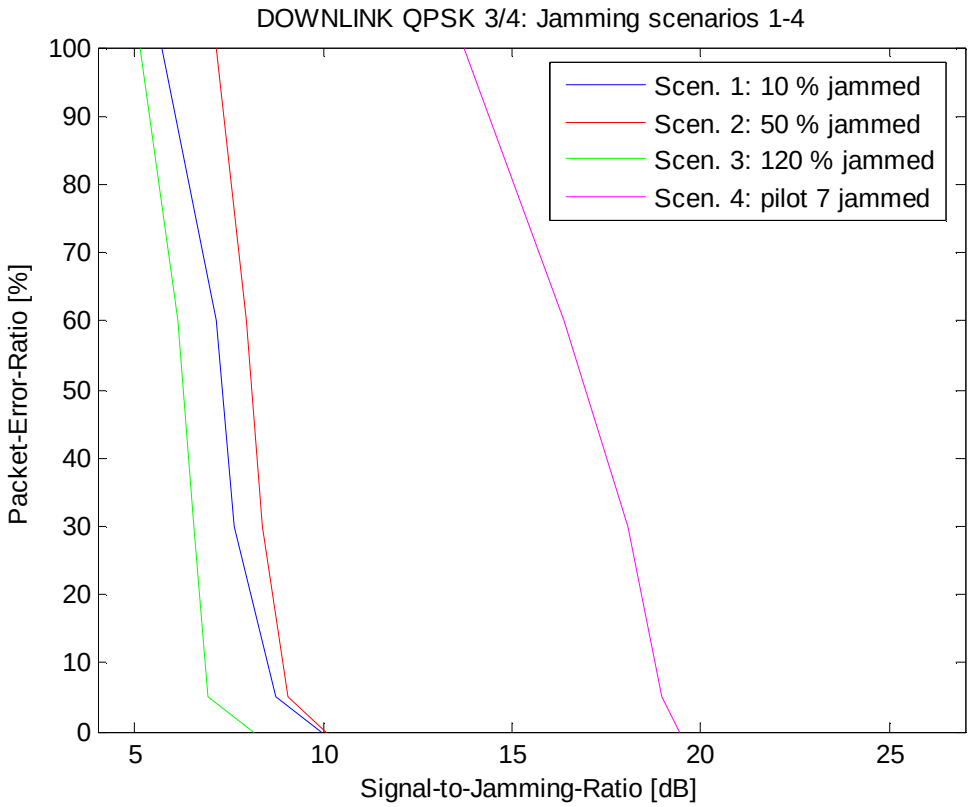

Figure 40: Comparison of DL jamming scenarios (QPSK 3/4)

What was earlier presumed about the increasing efficiency of narrowband jamming when operating with higher modulations shows inevitably with 64-QAM 2/3 (Figure 41). Narrowband jamming has now risen as the second most efficient jamming form and is now more efficient than jamming some of the pilots (not the 7th). The relative difference of the second best jamming type to the pilot jamming has dropped from about 10 dB to 6 dB when comparing the required jamming power causing errors on connection.

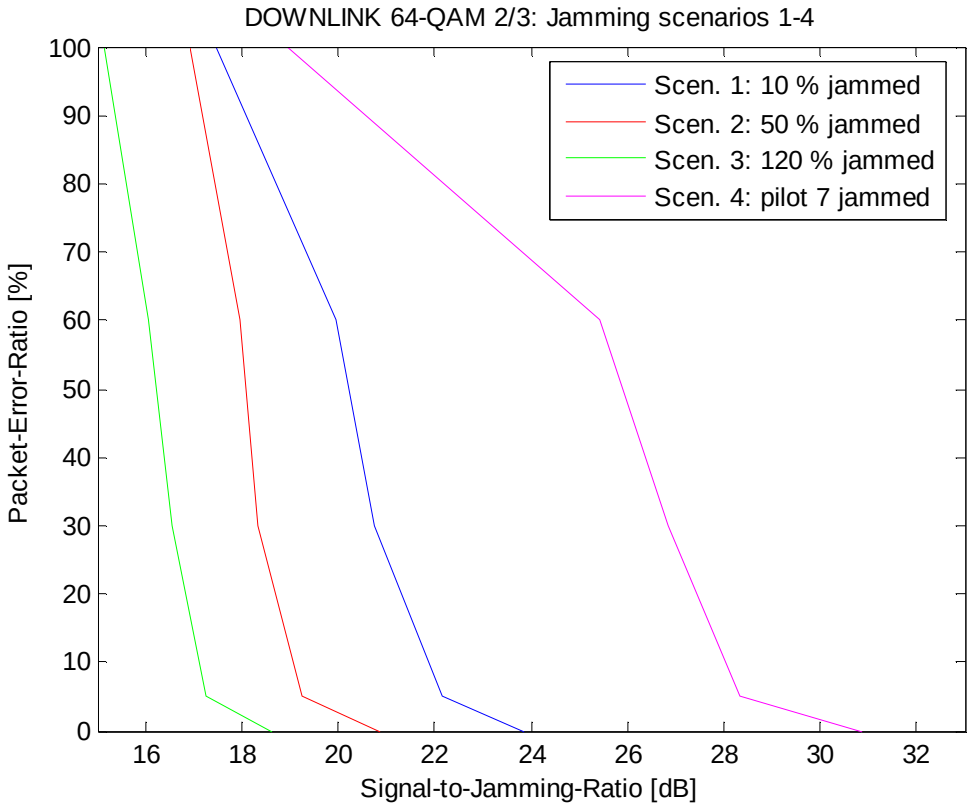

Figure 41: Comparison of DL jamming scenarios (64-QAM 2/3)

A distinctive feature noticed, is that the PER curves of the wideband noise jamming signals come down from 0 % to 100 % PER far more rapidly than those of the narrowband and pilot jamming. This result can be justified with the reasoning already presented in Figure 38. As data subcarriers start to drop as a result of increased narrowband jamming power, the PER value slowly starts to increase. For Scenarios 2 and 3, such a phenomenon doesn't occur due to the lighter impact of jamming on channel estimation (i.e. the pilot subcarrier).

The uplink jamming measurements were performed in a similar way as the downlink measurements. For Scenario 4, the jammed pilot was chosen to be the 4th due to its highest relative sensitivity to jamming (Figure 42). What can clearly be noticed is the more profound difference in the vulnerability of the different pilots in terms of jamming. It almost seems that only four pilots are used for channel estimation. Of course, this can also have something to do with the fact that the measurement was only done with BPSK not needing very accurate channel estimation. However, the difference

to the downlink measurements is that there is now apparent symmetry to be seen in Figure 42.

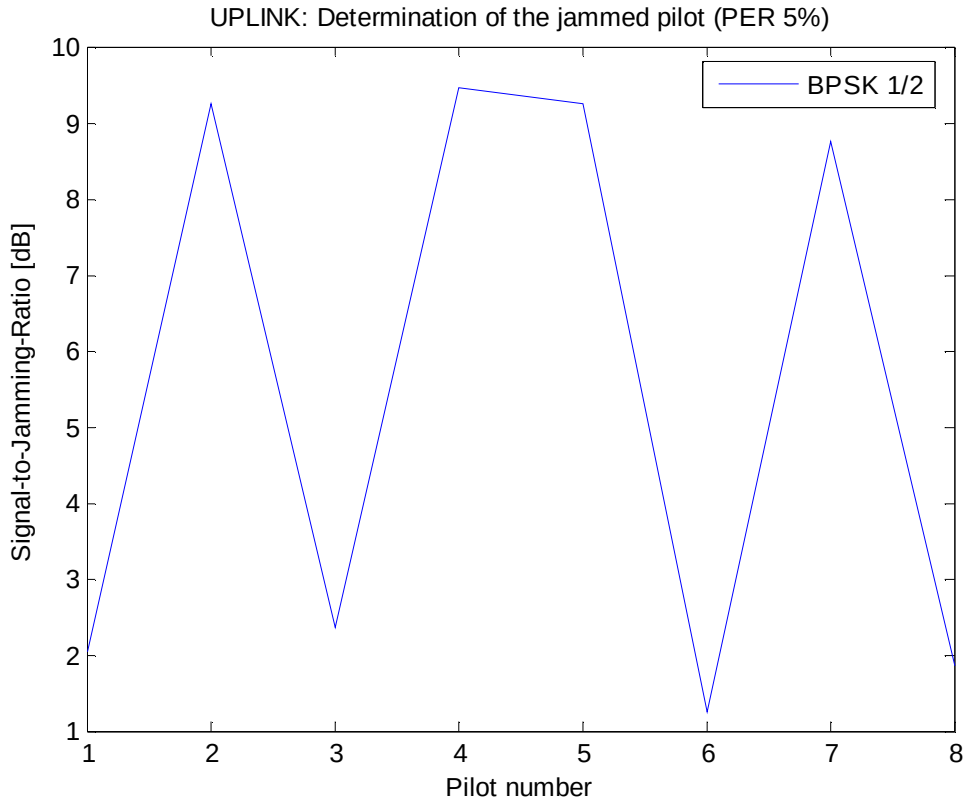

Figure 42: Selection of the jammed pilot (Uplink)

The result obtained from the uplink measurements (Figure 43) for BPSK have some rather similar features compared to those for downlink. The PER curves of Scenarios 2 and 3 are much more steep than for the other two scenarios. What is different, however, is the fact that the narrowband jamming signal (Scenario 1) is already almost as efficient as the pilot jamming for BPSK jamming. Another difference is that to completely prevent transmission in uplink direction, it seems to be reasonable to use Scenarios 2 and 3. However, the differences of uplink and downlink jamming results can't easily be justified theoretically, since the standard doesn't go into the implementation of the transceivers at both ends of the connection.

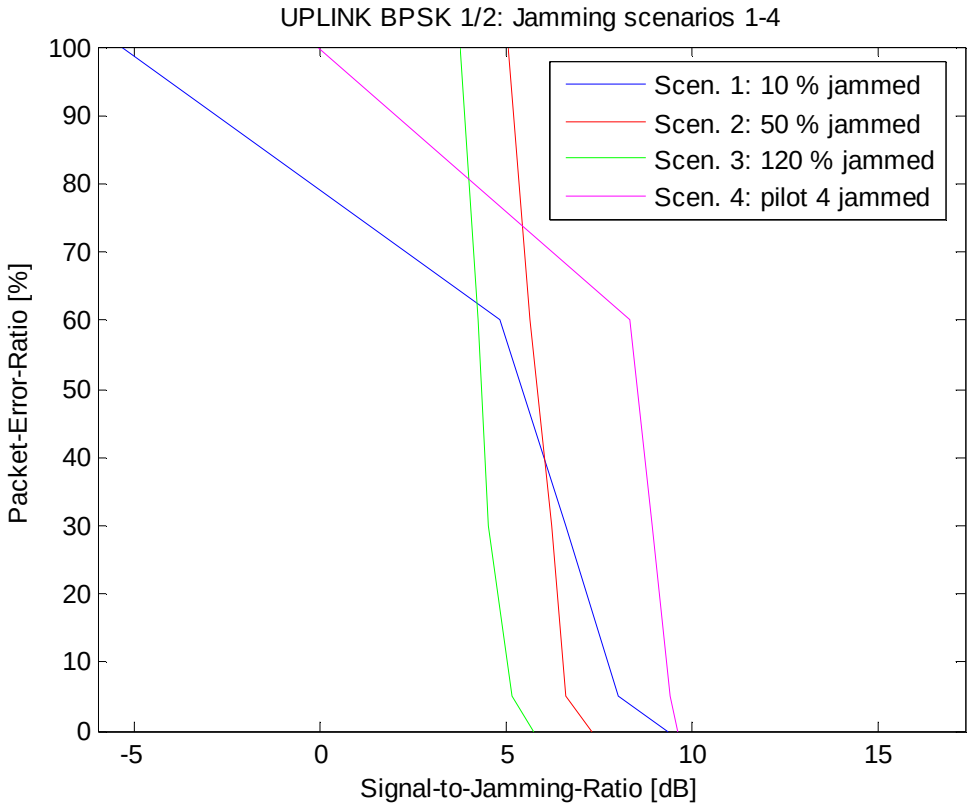

Figure 43: Comparison of uplink jamming scenarios

5.4 Comparison to the simulated results

In [2] a simulator was built to predict the effects of jamming on an IEEE 802.16-2004 based WiMAX system. The results are not completely comparable, since the jamming scenarios are slightly different and a Rayleigh fading channel is used. However, in [2] the user is moving only 1.5 m/s, so the channel is not very rapidly changing and the results should therefore have similar features. The channel parameters (Table 8) correspond to flat terrain type and moderate-to-heavy tree density.

Table 8: Rayleigh channel parameters

Operating Band	2.4 GHz
Channel Bandwidth	7 MHz
Channel Path Gains	[0 -4 -8] dB
Channel Path Delays	[0 1.5 4] µs
Max. Doppler spread	12 Hz (at 1.5 m/s)

In the following, the simulation results for 1 pilot jamming (Figure 44) and 50 % partial jamming (Figure 45) are compared to the measured results, since the jamming forms should perfectly match the ones used in the measurements.

According to [2], jamming an individual pilot subcarrier should not have much of an effect on the performance of the system (Figure 41). However, the results obtained by measuring the system (Figure 37) show that even BPSK requires a SJR of almost 15 dB to reach maximum throughput (or PER = 0 %) when jamming the 7th pilot subcarrier. This contradiction can result from the way the measured system is implemented, since the pilots don't even seem to act similarity in channel estimation. For higher modulations (e.g. 64-QAM ¾) a similar kind of behaviour can be noticed when comparing the measured and simulated results, but there is still a notable difference in the needed SJR to reach a certain level of performance.

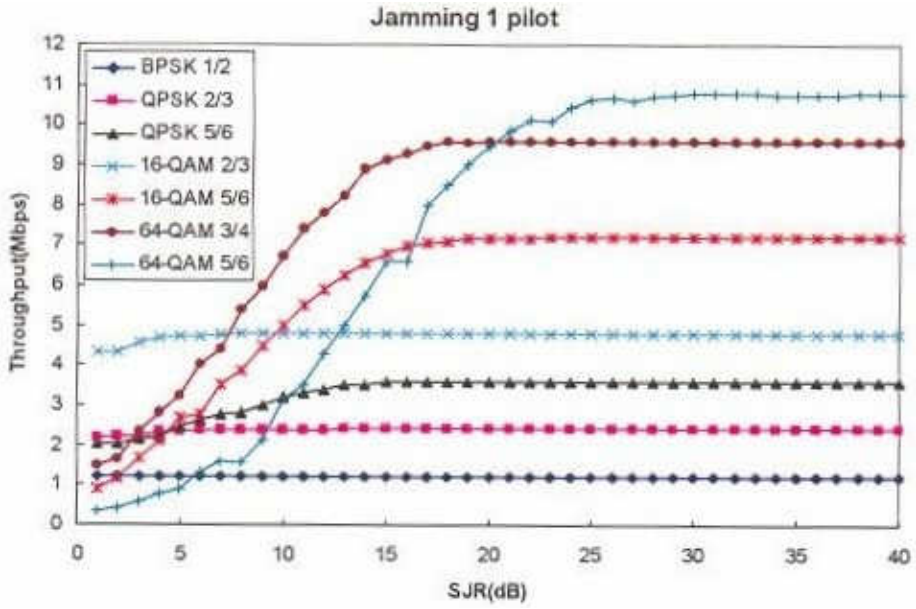

Figure 44: Jamming 1 pilot (simulation [2])

For the 50 % partial jamming scenario the measured (Figure 34) and simulated (Figure 45) results are now presumably a lot closer to one another. To reach PER = 0 % for 64-QAM 3/4, a SJR of about 25 dB (simulated) and 23 dB (measured). Similarly, for BPSK ½ a SJR of about 4 dB is required according to both the simulated and measured results.

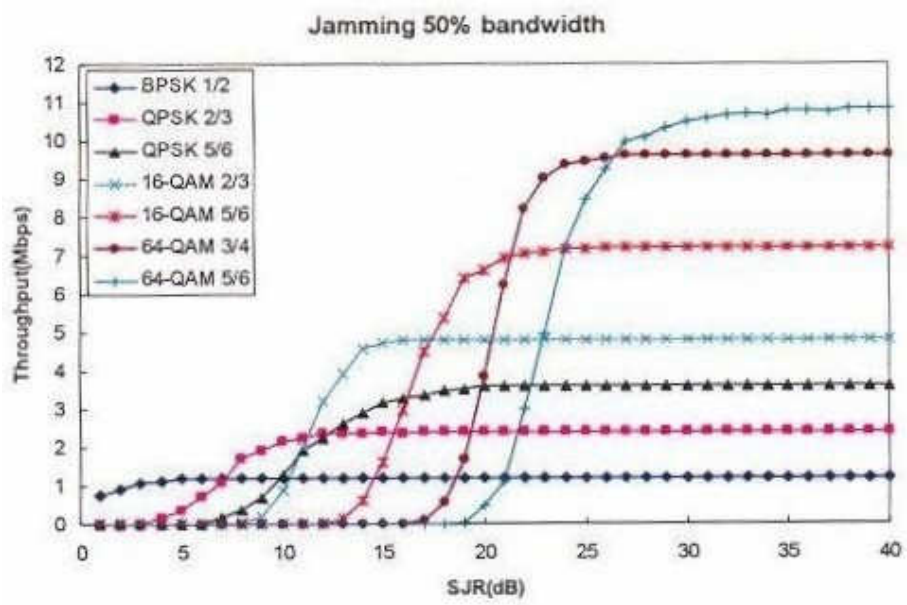

Figure 45: Jamming 50 % of the bandwidth (simulation [2])

The reason, why the simulation results are now very similar to the measured ones can be justified by the fact that the implementation of the channel estimation and equalisation does not have as crucial a role. When summing additional noise to the signal, it adds to the pilot subcarriers in the same manner as to the data subcarriers. This does not prevent the system from making an accurate channel estimate and mainly functions as natural noise the system is already designed to tolerate up to a certain level. Thus, the measurements support the simulator and vice versa.

5.5 Receiver sensitivity measurement

According to [1], standard defined minimum receiver sensitivity can be calculated from Equation 3 and is presented in Table 8. For standard defined sensitivity values it is assumed that BER < 10^{-6} after FEC.

The measurement was performed as described in Chapter 4.3 and the final sensitivity value was calculated using Equation 9. The results were rounded down to the nearest integer value, not to give too good a conception of the performance of the system. Since it was not possible to measure BER with the given equipment, the sensitivity values obtained from the measurement are given with the assumption of PER = 0 % for a period of 30 seconds. This resulted in values some 2 - 5 dB better than standard defined.

For uplink only BPSK ½ could be measured, due to the automatic modulation drop resulting from attenuating the connection. Should the points where modulation change occurred be used as sensitivity values, a false view of the uplink performance would be given. In addition, there seemed to be significant variance in the received power values where modulation drop occurred, which is likely to be caused by the chosen channel quality measurement algorithm. However, it appeared that the modulation changes occurred close to the sensitivity values measured for downlink and since the value for BPSK ½ was the same, it can be assumed that the values for uplink are most likely rather similar.

Table 9: Receiver sensitivity (standard defined and measured)

	Receiver sens. (standard):	Rec.sens.(meas.) DL	Rec.sens.(meas.) UL
BPSK 1/2	-91	-96	-96
QPSK 1/2	-88	-91	-
QPSK 3/4	-86	-88	-
16 QAM 1/2	-81	-84	-
16 QAM 3/4	-79	-82	-
64 QAM 2/3	-74	-78	-
64 QAM 3/4	-73	-75	-

The measurement allows the conclusion that, in terms of sensitivity, the system at least meets the standard defined values. For the lowest modulations, the system seems to even function with somewhat weaker signals.

5.6 Chapter summary

In Chapter 5, the results of the four measured jamming scenarios and the receiver sensitivity measurement were presented. Since the uplink modulation could not be locked, uplink measurements consist only of BPSK measurements and were presented together with the downlink jamming mode comparison in Section 5.3.

Downlink jamming measurement indicated clearly that the jamming of an individual pilot is the most effective way of attacking the system. It was also noticed that narrowband jamming forms start to act like pilot jamming as higher modulations are chosen. For the studied system, wideband jamming signals function naturally like a raise in the noise floor and are not very powerful.

The results from the uplink jamming measurement are not all the way similar to the results from downlink jamming. To cause some errors on the uplink connection, the pilot jamming scenario was the most efficient. However, in order to raise the PER value up to 80 % and higher, Scenarios 2 and 3 proved to be more powerful, which wasn't the case for downlink. Still, it can't be explicitly stated which transmission direction is the most vulnerable due to fact that not all uplink modulations could be analysed and because of the relative difference in the effectiveness of the different jamming forms.

Although the jamming of pilots generally seems to be the best way to attack the system, the differences in the vulnerability between individual pilot subcarriers is very significant. For both downlink and uplink, the differences between pilots were remarkable, but the real reason for this can't be known without additional knowledge of the implementation of the channel equalisation process. The conclusion can be drawn that the effectiveness of pilot jamming is very likely to depend greatly on the WiMAX system used.

A comparison to the simulated results was also made, evidently supporting the measurement results for the noise jamming scenarios. However, single pilot jamming was predicted to be rather inefficient in the simulations, which was not the case in the measurements. This could result from the implementation of the measured system or from the presumed parameters in the setup of the simulations.

In terms of sensitivity, the system clearly meets the requirements set by the standard as can be noticed in Figure 60 in Appendix II.

6. Summary and conclusions

The goal of this thesis was to evaluate how an IEEE 802.16-2004 based WiMAX system operates in a hostile environment, where different kinds of intentional interference exist. Due to the ever increasing complexity and cost of manufacturing state-of-the-art equipment only for military purposes, much interest has also raised in, what is known as, commercial-off-the-shelf (COTS) and modified-off-the-shelf (MOTS) devices.

WiMAX supports orthogonal frequency division multiplexing (OFDM), which should make the system fairly resistant against e.g. interference and different fading phenomena. To correctly interpret the information carried by the data subcarriers, 8 pilot subcarriers are inserted along the spectrum to facilitate efficient channel estimation and equalisation. In jamming scenarios, the vulnerability of the system, when attacking pilot subcarriers and the whole spectrum was tested.

The measurements were conducted using a flat-fading AWGN channel, since the system does not yet support mobility (i.e. IEEE 802.16e-2005). In the measurements, four different jamming signals were separately inserted onto the connection and the required jamming powers were recorded. Signal-to-jamming-ratio (SJR) values were compared with the general conclusion that the easiest and most powerful way to jam the measured system is to insert a single sine wave onto the centre frequency of a pilot subcarrier. All the other measured interference scenarios generally needed more power to reach similar system performance degradation.

It was also noticed that the system tolerates jamming of different pilot subcarriers in a very different manner, which can not be explained by the standard. This practically means that the results obtained in this thesis apply directly only to the very system studied. Also, the simulated results support that another approach in system design might have made the system rather insensitive to single pilot jamming. In that case, more advanced jamming signals (i.e. noise or multipilot jamming) should be used.

Although the system does not appear to be very resistant against a simple interfering sine signal, an easy fix could be applied. The channel estimation algorithm could simply

be modified to detect if a certain pilot subcarrier seems to be under jamming and ignore it when estimating the frequency response of the channel. In the case of a strong constant interfering sine signal, the presence of jamming should not be very hard to discover. This would now turn the system from COTS to MOTS, but the cost of modification should remain on a reasonable level. Modifying the system to tolerate multipilot jamming would require that the locations of the pilots on the frequency band could be dynamically altered allowing for the system to escape jamming. However, this would require an operation mode contradicting with the requirements of the standard and would thus be possible only when normal regulations would not apply.

It should be noted that in this thesis the system downlink modulation was kept constant by disabling adaptive modulation and coding, and for uplink only BPSK was studied. However, the performance of the system under jamming also greatly depends on its ability to adapt to the environment, which to a large degree is dictated by the performance of the adaptive modulation and coding. The fact that the system does lower the modulation/coding when a jamming signal is injected, actually makes the system a lot more resistant to jamming than what could be stated simply be looking at the graphs. Although not included in the scope of this thesis, studying the functionality of adaptive modulation/coding and combining the results with those presented in this thesis would be worthwhile.

At the moment, it can stated that the measured system does not tolerate jamming the way it should when operating in a hostile environment. However, the performance under jamming in not strictly dictated by the standard and it is thus possible to further develop the system to better resist jamming. The practical limits that currently restrict development for military environment are the fixed operating frequency and the fixed positions of the subcarriers.

In the future, the performance of IEEE 802.16e-2005 would make an interesting topic for further studies. Due to its standard built requirement to tolerate phenomena related to mobility, the performance of the system in an interference rich Rayleigh fading environment should also be on a better level.

References

[1] IEEE std 802.16-2004, IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access, 857 pp., 2004

[2] Juan Li, Performance of IEEE802.16-2004 based System in Jamming Environment and its improvement with Link Adaptation, Licentiate's thesis, 76 pp., 2006

[3] Kari Pietikäinen, Jamming Tolerance of Orthogonal Frequency Division Multiplexing Based System, Master's thesis, 101 pp., 2005

[4] IEEE std 802.16e-2005, Amendment to IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems – Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands, The Institute of Electrical and Electronic Engineers, Inc., 864 pp., 2006

[5] http://www.us.design-reuse.com/articles/article10358.html, Aseem Pandey, Shyam Ratan Agrawalla, Shrikant Manivannan, VLSI implementation of OFDM modem, D&R Industry Articles, Wipro Technologies, 13.11.2006

[6] http://www.intel.com/technology/itj/2004/volume08issue03/ art02_rfsystem/p05_wimax_specs.htm, RF System and Circuit Challenges for WiMAX, 13.11.2006

[7] D. Curtis Schleher, Electronic Warfare in the Information Age, Artech House, 605 pp.,1999

[8] S. A. Vakin, L. N. Shuston, R. H. Dunwell, Fundamentals of Electronic Warfare, Artech House, 384 pp., 2001

[9] William Webb, Introduction to Wireless Local Loop, Artech House Publishers, 1999, 319 pp., U.S.A.

[10] Simon Haykin, Michael Moher, Modern Wireless Communications, Prentise-Hall, U.S.A, 560 pp., 2005

[11] IEEE std 802.16a-2003 (Amendment to IEEE Std 802.16-2001), IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access, 318 pp., 2003

[12] Edward Waltz, Information warfare: principles and operations, Artech House, pp.26, U.S.A, 397 pp., 1998

[13] Roger L. Freeman, Radio System Design for Telecommunications 2nd edition, John Wiley & Sons, Inc, 887 pp., U.S.A, 1997

[14] A. B. Carlson, P. B. Crilly, J. C. Rutledge, Communication systems: An introduction to signals and noise in electrical communication, 4th edition, 850 pp., McGraw-Hill, U.S.A, 2002

Appendix I - Noise and pilot jamming results

DOWNLINK JAMMING MEASUREMENT

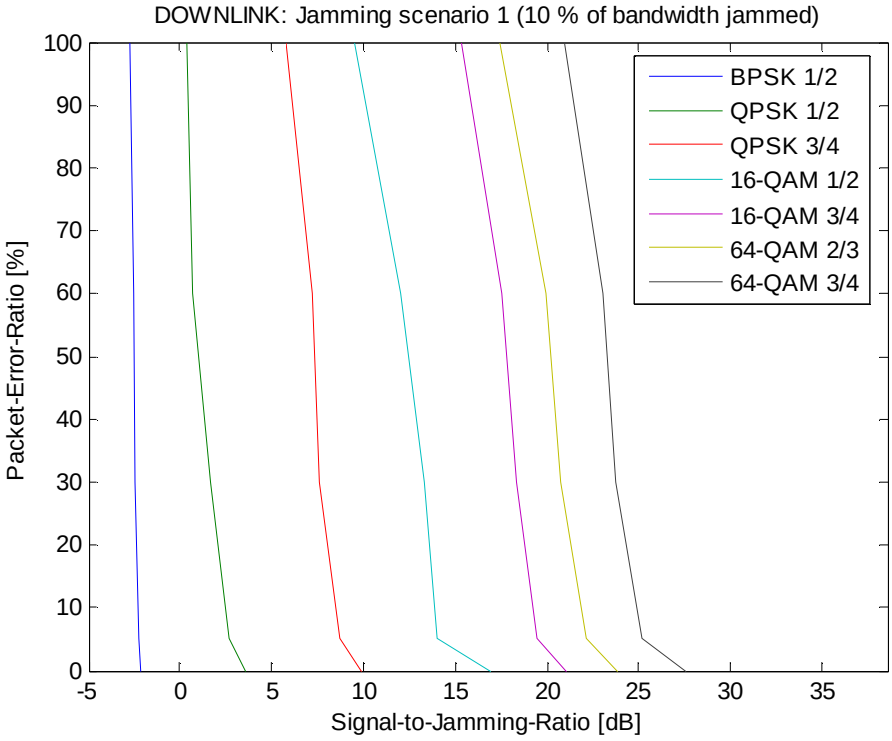

Figure 46: 10 % of bandwidth jammed (DOWNLINK)

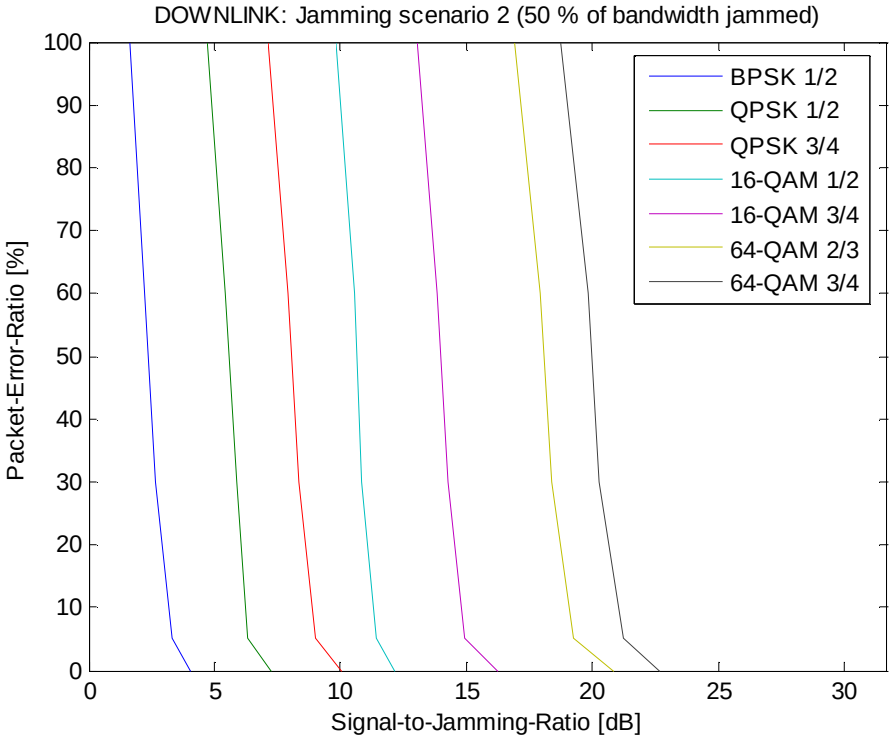

Figure 47: 50 % of bandwidth jammed (DOWNLINK)

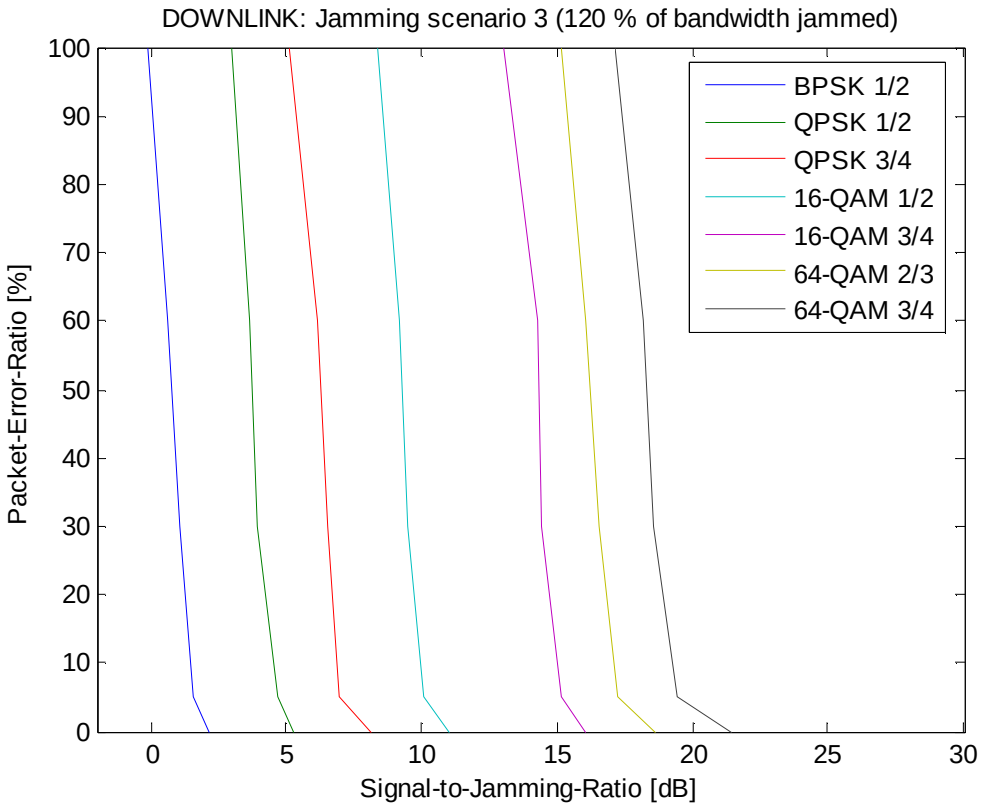

Figure 48: 120 % of bandwidth jammed (DOWNLINK)

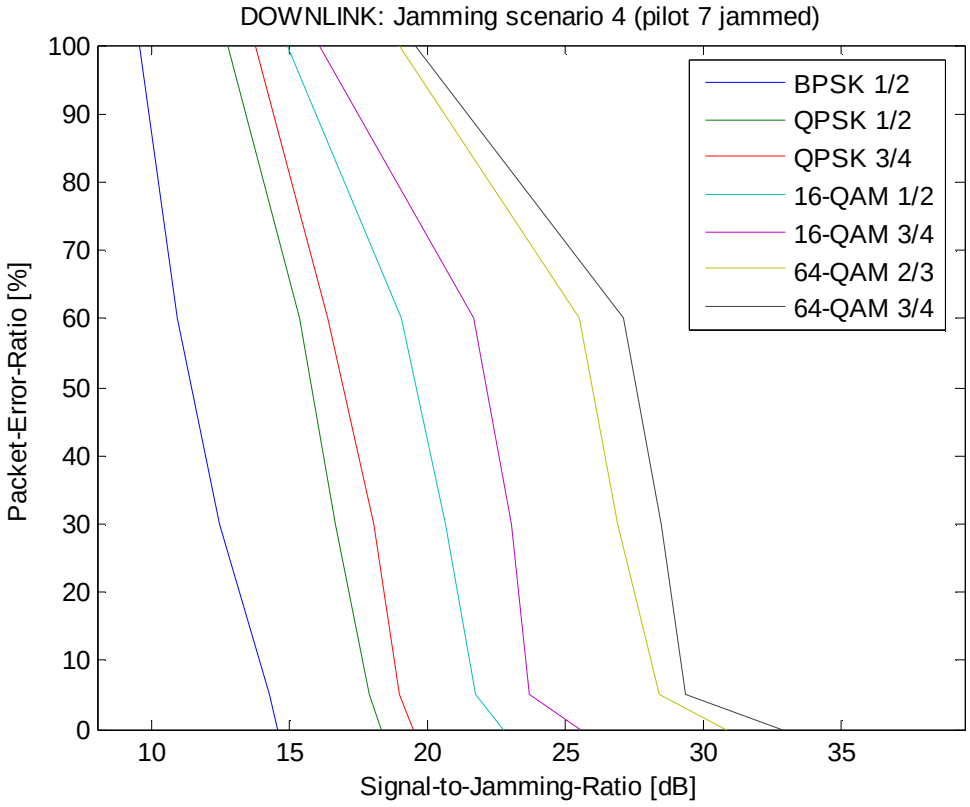

Figure 49: Pilot 7 jammed (DOWNLINK)

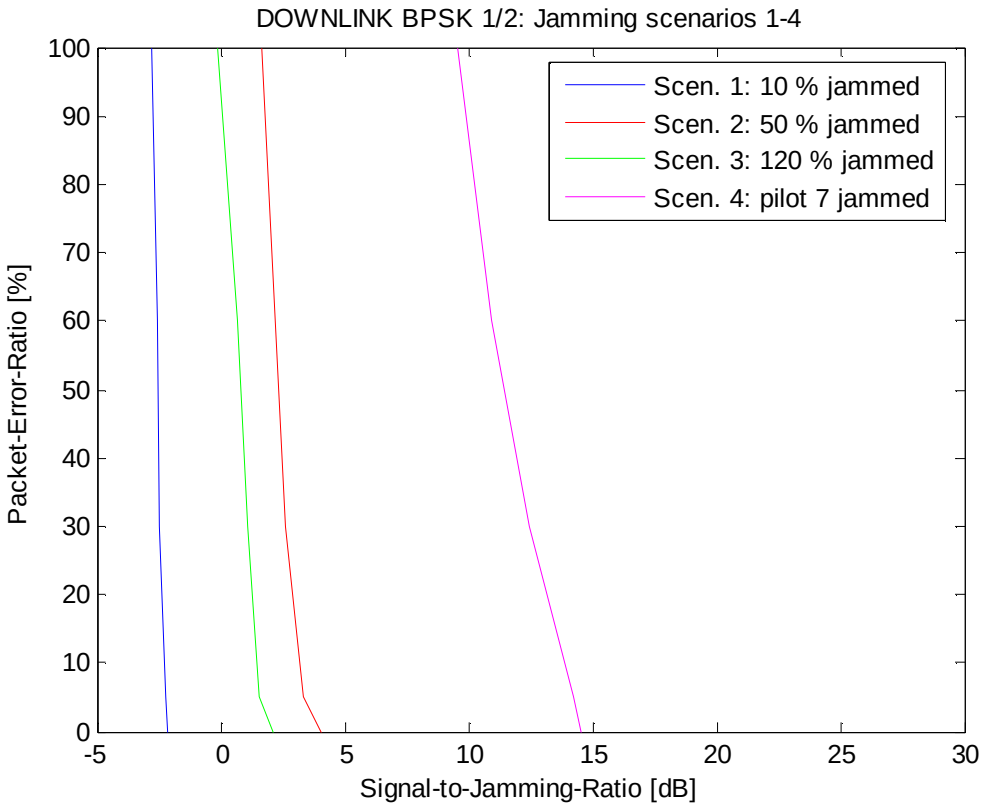

Figure 50: Jamming modes comparison (BPSK 1/2, DL)

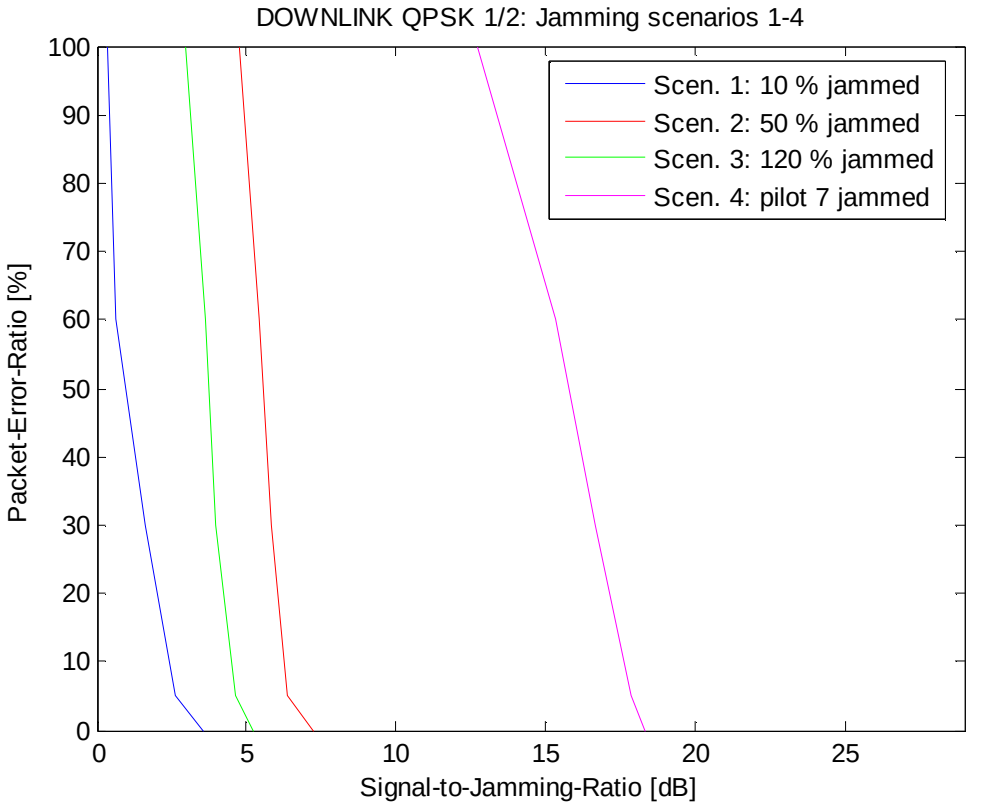

Figure 51: Jamming modes comparison (QPSK 1/2, DL)

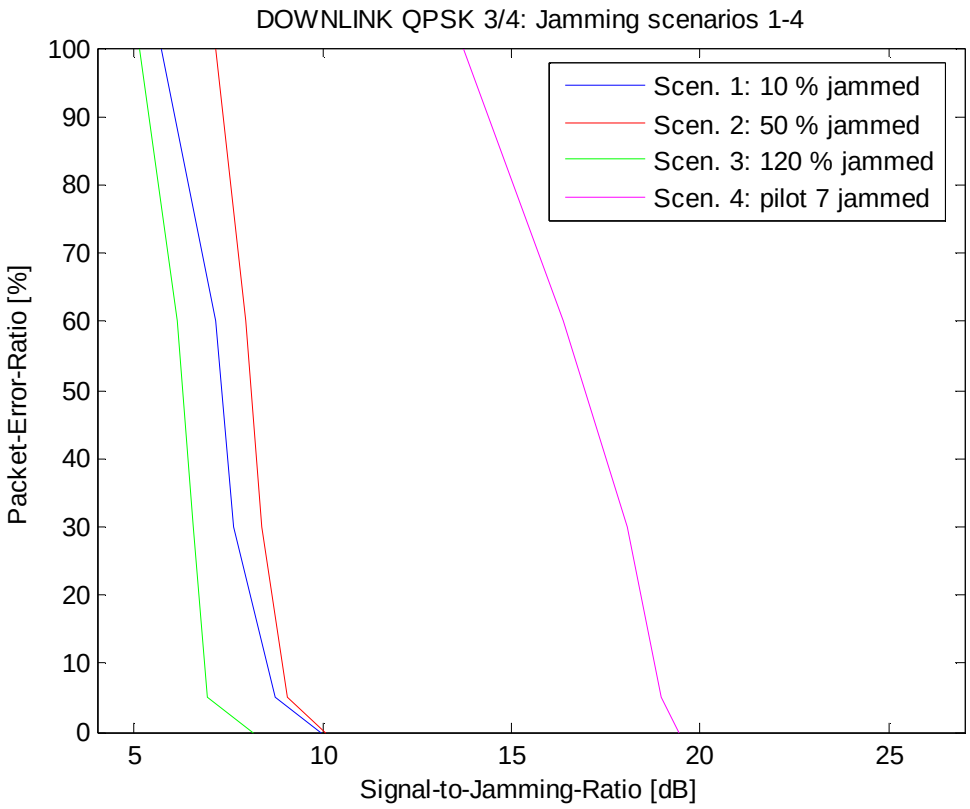

Figure 52: Jamming modes comparison (QPSK 3/4, DL)

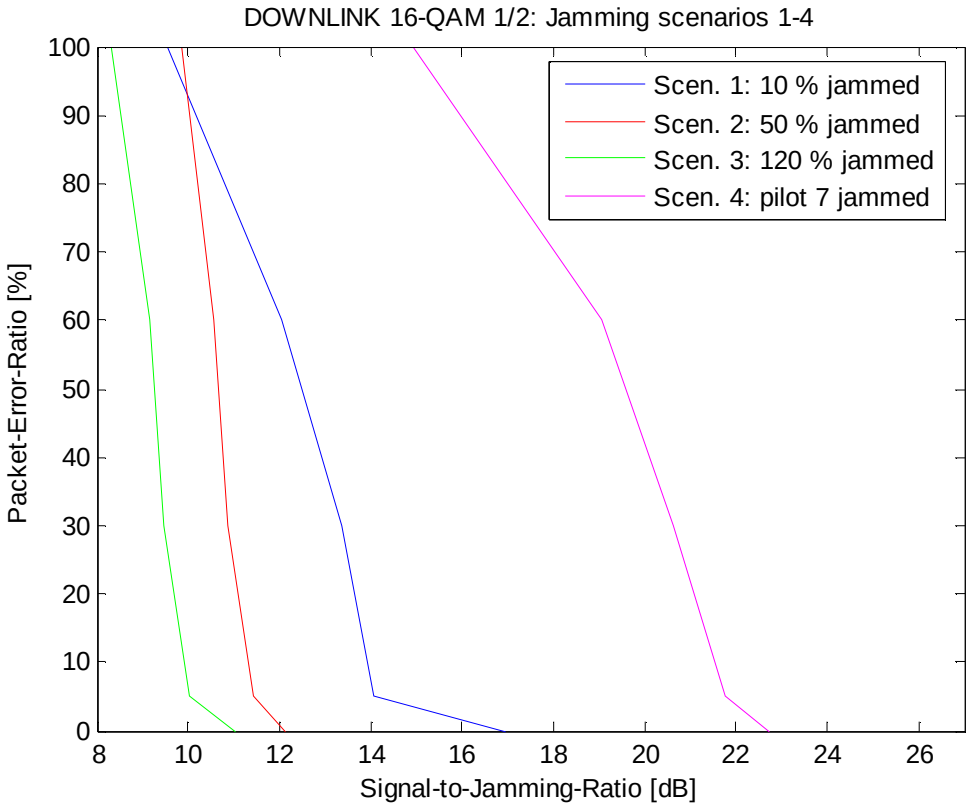

Figure 53: Jamming modes comparison (16-QAM 1/2, DL)

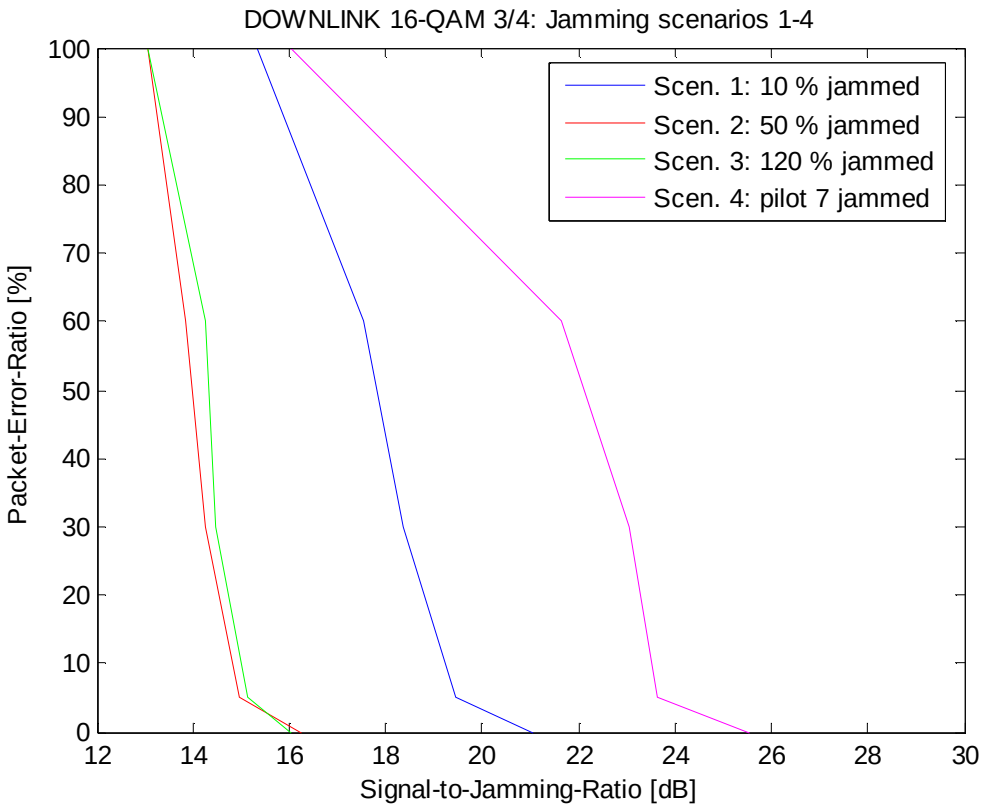

Figure 54: Jamming modes comparison (16-QAM 3/4, DL)

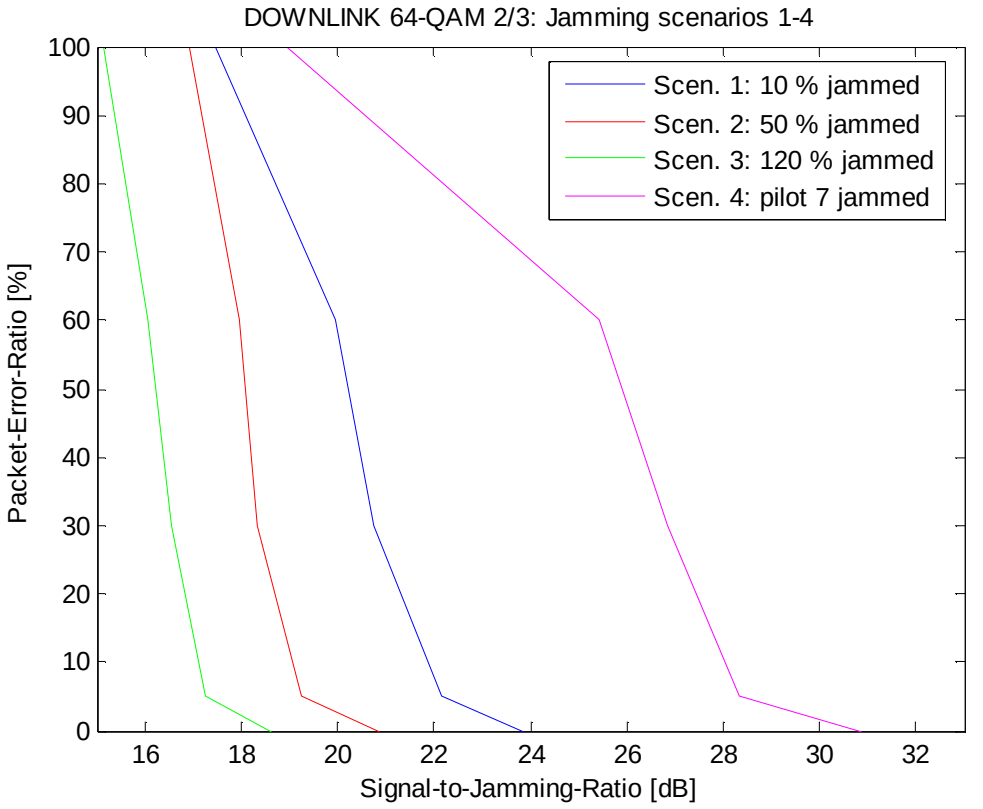

Figure 55: Jamming modes comparison (64-QAM 2/3, DL)

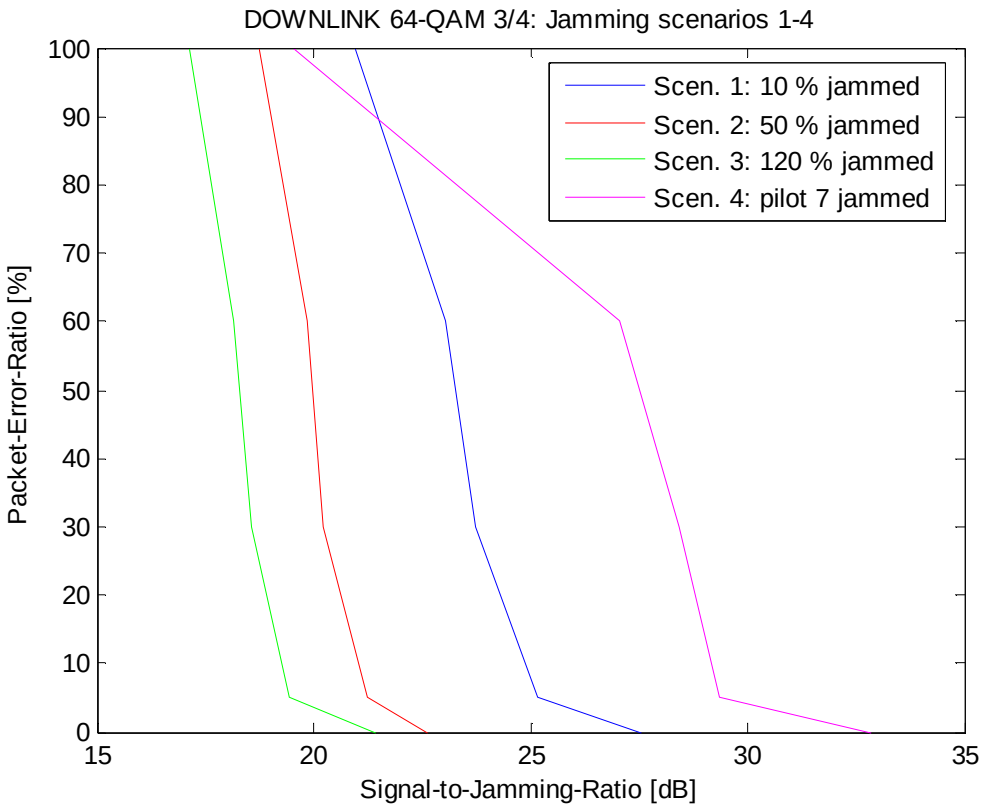

Figure 56: Jamming modes comparison (64-QAM 3/4, DL)

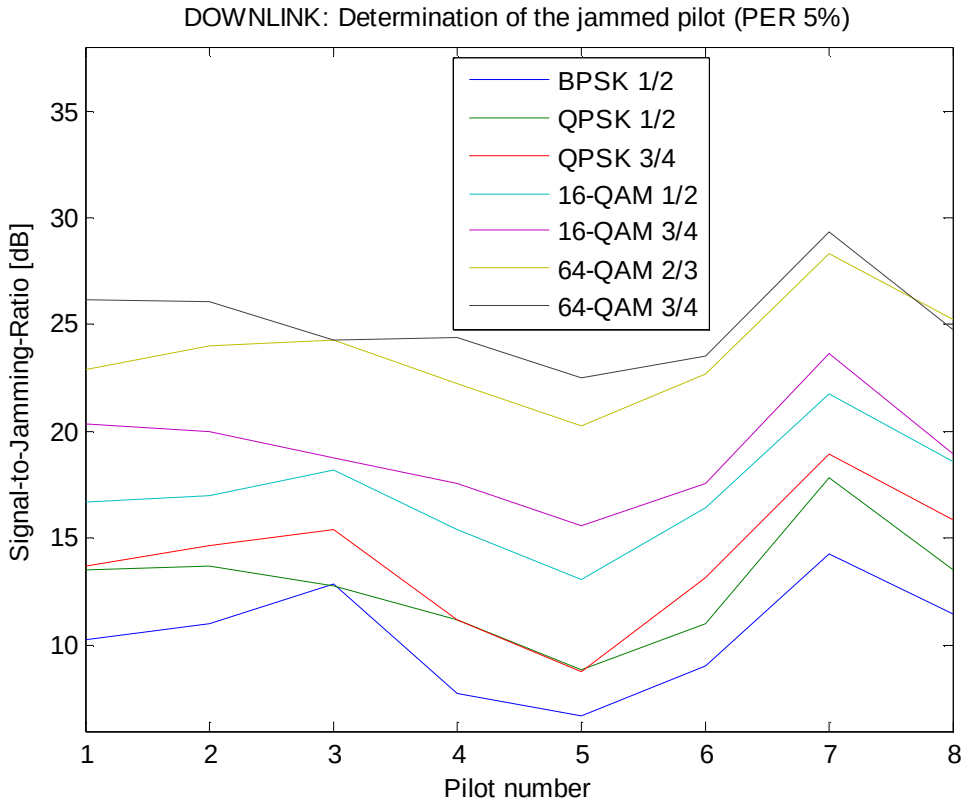

Figure 57: Determination of the jammed pilot

UPLINK JAMMING MEASUREMENT

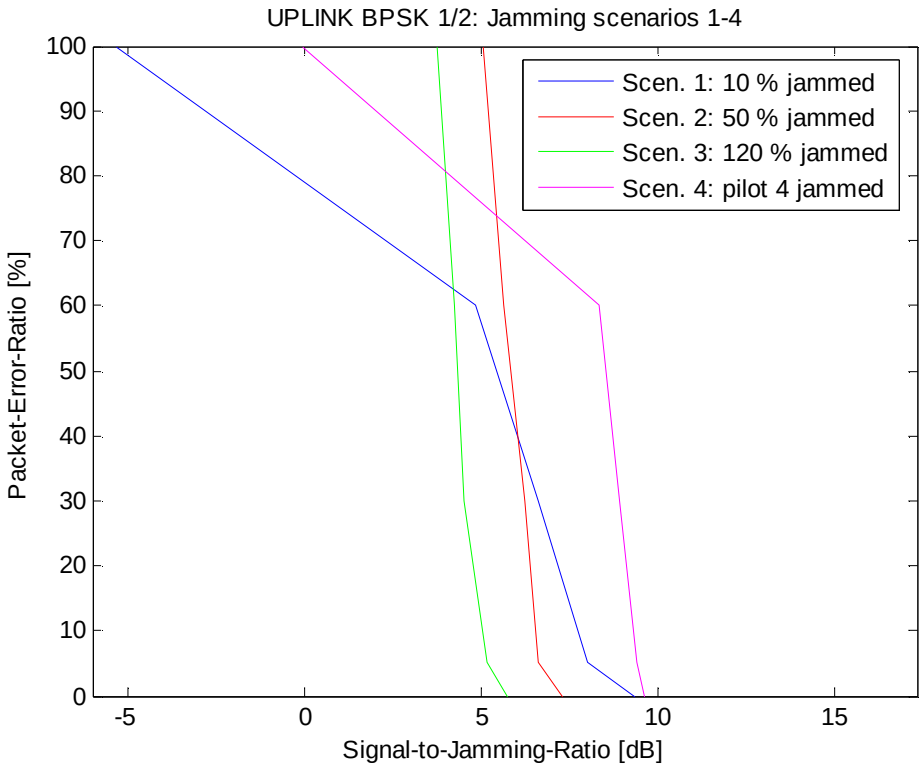

Figure 58: Jamming modes comparison (BPSK 1/2, DL)

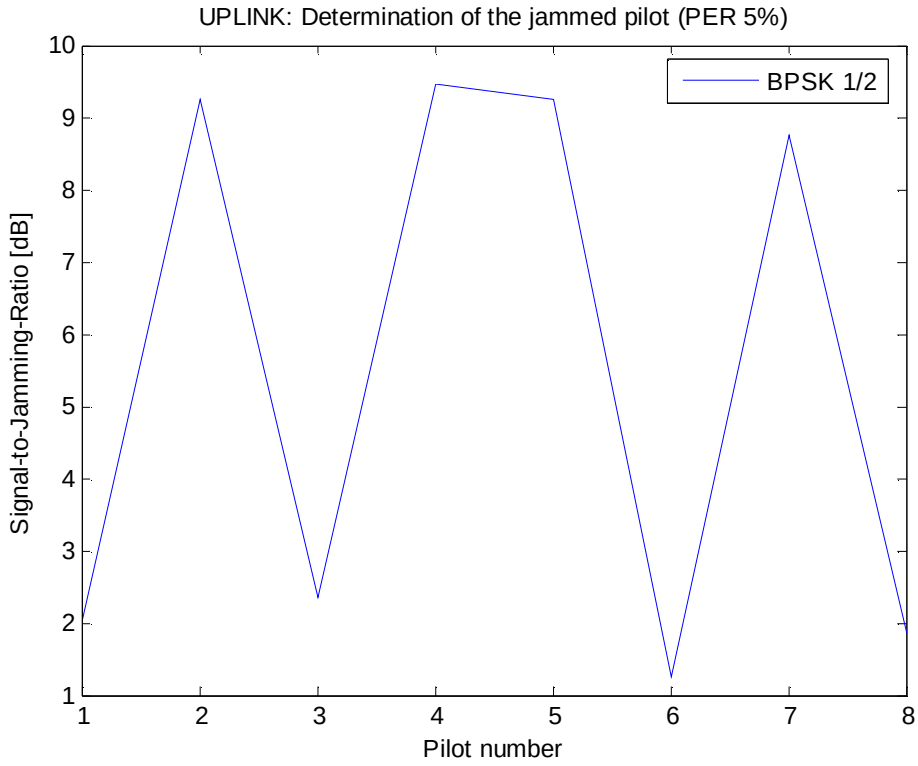

Figure 59: Determination of the jammed pilot

Appendix II - Sensitivity measurement

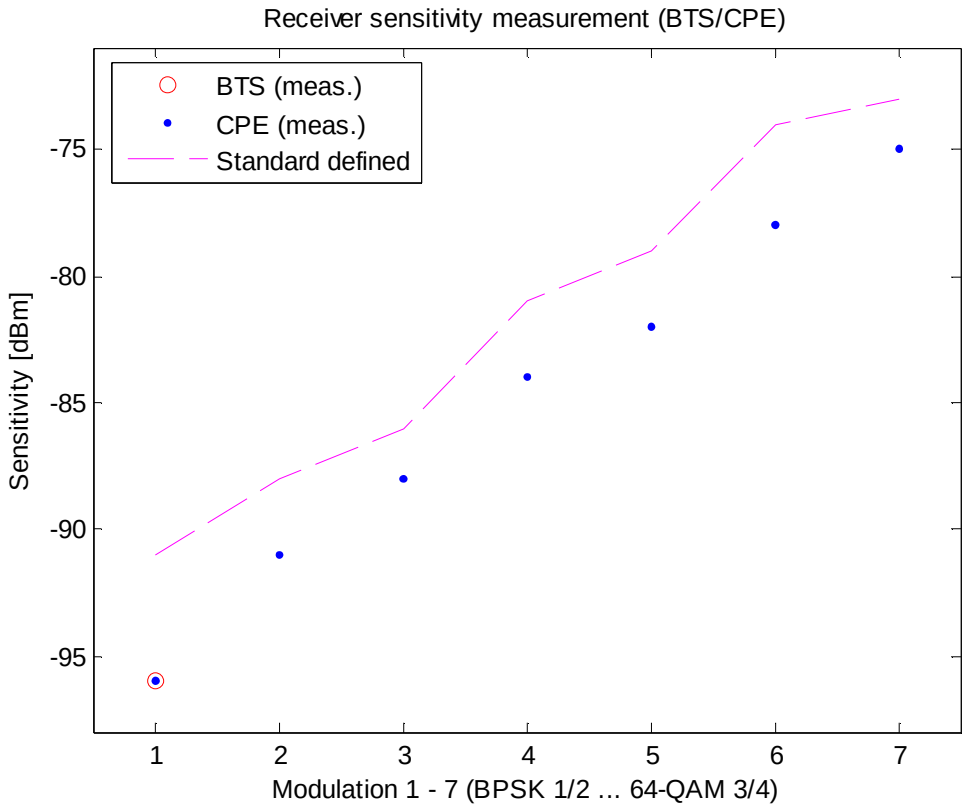

Figure 60: Receiver sensitivity measurement (CPE and BTS)

Appendix III - WiMAX Jamming Measurements

25.10.2006 / Mika Husso

Adj. att. settings:	Adj. att setting (DL)	Adj. att. sett. (UL)	Rec. sens. (stand.)
BPSK 1/2	-35,6	-25,6	-91
QPSK 1/2	-32,6	-22,6	-88
QPSK 3/4	-30,8	-20,8	-86
16 QAM 1/2	-25,6	-15,6	-81
16 QAM 3/4	-23,8	-13,8	-79
64 QAM 2/3	-19,3	-9,3	-74
64 QAM 3/4	-17,6	-7,6	-73

Scenario number	**Jamming signal**	**Jammed BW (Hz)**
1	10 % of bandwidth	350000
2	50 % of bandwidth	1750000
3	120 % of bandwidth	4200000
4	pilot 7 (DL) / pilot 4 (UL)	-
5	pilots: 1,2,3,4	not possible
6	8 pilots	not possible

Throughput measurement (kbit/s)

			95% of max tp.			95% of max tp.
	Meas. max. tp /DL		Used data rate /DL	Meas. max. tp /UL		Used data rate /UL
BPSK 1/2	687		653	635		603
QPSK 1/2	1400		1330	1290		1226
QPSK 3/4	2100		1995	1920		1824
16 QAM 1/2	2800		2660	2580		2451
16 QAM 3/4	4210		4000	3860		3667
64 QAM 2/3	5620		5339	5160		4902
64 QAM 3/4	6340		6023	3860		3667

SCENARIO 1

Jamming power measurement (dBm)

UPLINK					
	PER 0% until	**PER 5 %**	**PER 30 %**	**PER 60 %**	**PER 100 % from**
BPSK 1/2	-75,5	-74,2	-72,8	-71	-60,8
QPSK … 64 QAM	-	-	-	-	-
DOWNLINK					
	PER 0% until	**PER 5 %**	**PER 30 %**	**PER 60 %**	**PER 100 % from**
BPSK 1/2	-64	-63,9	-63,7	-63,6	-63,4
QPSK 1/2	-66,7	-65,8	-64,8	-63,8	-63,5
QPSK 3/4	-71,3	-70,1	-69	-68,5	-67,1
16 QAM 1/2	-73,1	-70,2	-69,5	-68,2	-65,7
16 QAM 3/4	-75,4	-73,8	-72,7	-71,9	-69,7
64 QAM 2/3	-73,7	-72	-70,6	-69,8	-67,3
64 QAM 3/4	-75,7	-73,3	-71,9	-71,2	-69,1

SCENARIO 2

Jamming power measurement (dBm)

UPLINK	**PER 0% until**	**PER 5 %**	**PER 30 %**	**PER 60 %**	**PER 100 % from**
BPSK 1/2	-73,5	-72,8	-72,4	-71,8	-71,2
QPSK … 64 QAM	-	-	-	-	-
DOWNLINK	**PER 0% until**	**PER 5 %**	**PER 30 %**	**PER 60 %**	**PER 100 % from**
BPSK 1/2	-70,2	-69,5	-68,8	-68,4	-67,8
QPSK 1/2	-70,4	-69,5	-69	-68,6	-67,9
QPSK 3/4	-71,4	-70,4	-69,7	-69,3	-68,5
16 QAM 1/2	-68,3	-67,6	-67	-66,7	-66
16 QAM 3/4	-70,6	-69,3	-68,6	-68,2	-67,4
64 QAM 2/3	-70,7	-69,1	-68,2	-67,8	-66,8
64 QAM 3/4	-70,8	-69,4	-68,4	-68	-66,9

SCENARIO 3

Jamming power measurement (dBm)

UPLINK					
	PER 0% until	**PER 5 %**	**PER 30 %**	**PER 60 %**	**PER 100 % from**
BPSK 1/2	-71,9	-71,3	-70,7	-70,4	-69,9
QPSK … 64 QAM	-	-	-	-	-
DOWNLINK					
	PER 0% until	**PER 5 %**	**PER 30 %**	**PER 60 %**	**PER 100 % from**
BPSK 1/2	-68,3	-67,7	-67,2	-66,8	-66
QPSK 1/2	-68,4	-67,8	-67,1	-66,8	-66,1
QPSK 3/4	-69,5	-68,3	-67,9	-67,5	-66,5
16 QAM 1/2	-67,2	-66,2	-65,6	-65,3	-64,5
16 QAM 3/4	-70,4	-69,5	-68,8	-68,6	-67,4
64 QAM 2/3	-68,5	-67,1	-66,4	-65,9	-65
64 QAM 3/4	-69,6	-67,6	-66,7	-66,3	-65,3

Selection of the jammed pilot (the most critical)

Jamming power measurement (dBm)

PER 5 %, Data rates and attenuation as usual, downlink jamming power

UPLINK	Pilot1	Pilot 2	Pilot3	**Pilot4**	Pilot5	Pilot6	**Pilot7**	Pilot 8
BPSK 1/2	-68,2	-75,4	-68,5	**-75,6**	-75,4	-67,4	-74,9	-68,0
QPSK … 64 QAM	-	-	-	-	-	-	-	-
DOWNLINK								
BPSK 1/2	-76,4	-77,2	-79,0	-73,9	-72,9	-75,2	**-80,4**	-77,6
QPSK 1/2	-76,7	-76,9	-75,9	-74,3	-72,0	-74,2	**-81,0**	-76,7
QPSK 3/4	-75,1	-76,0	-76,8	-72,5	-70,1	-74,5	**-80,3**	-77,2
16 QAM 1/2	-72,9	-73,1	-74,4	-71,6	-69,2	-72,6	**-77,9**	-74,7
16 QAM 3/4	-74,7	-74,3	-73,1	-71,9	-69,9	-71,9	**-78,0**	-73,3
64 QAM 2/3	-72,7	-73,9	-74,1	-72,1	-70,1	-72,6	**-78,2**	-75,1
64 QAM 3/4	-74,3	-74,2	-72,4	-72,5	-70,7	-71,7	**-77,5**	-72,9

SCENARIO 4 (DL: pilot 7/ UL: pilot 4)

Jamming power measurement (dBm)

UPLINK					
pilot 4	**PER 0% until**	**PER 5 %**	**PER 30 %**	**PER 60 %**	**PER 100 % from**
BPSK 1/2	-75,8	-75,6	-75,1	-74,5	-66,1
QPSK … 64QAM	-	-	-	-	-
DOWNLINK					
pilot 7	**PER 0% until**	**PER 5 %**	**PER 30 %**	**PER 60 %**	**PER 100 % from**
BPSK 1/2	-80,7	-80,4	-78,6	-77,1	-75,7
QPSK 1/2	-81,5	-81	-79,8	-78,5	-75,9
QPSK 3/4	-80,8	-80,3	-79,4	-77,7	-75,1
16 QAM 1/2	-78,9	-77,9	-76,8	-75,2	-71,1
16 QAM 3/4	-79,9	-78	-77,4	-76	-70,4
64 QAM 2/3	-80,7	-78,2	-76,7	-75,3	-68,8
64 QAM 3/4	-81	-77,5	-76,6	-75,2	-67,7

Sensitivity measurement

sending at 95 % of max. tp

	Rec. sens. (std.):	SNRRX	rec.sens.(meas.) /CPE	rec.sens.(meas.) /BTS
BPSK 1/2	-91	6,4	-96	-96
QPSK 1/2	-88	9,4	-91	-
QPSK 3/4	-86	11,2	-88	-
16 QAM 1/2	-81	16,4	-84	-
16 QAM 3/4	-79	18,2	-82	-
64 QAM 2/3	-74	22,7	-78	-
64 QAM 3/4	-73	24,4	-75	-

Appendix IV - SJR vs. PER calculations

27.10.2006 / Mika Husso

SJR [dB] = (Ptx + Gatt,fixed + Gatt,adj. + Gcables1) - (Ptx,sign.gen., + Gcables2)

Ptx	20 dBm (CPE) / 30 dBm (BTS)		Transmitted signal power	
Ptx,sign.gen.	See Appendix III		Transmitted jamming power	
Gatt,fixed	-60	dB		
Gatt,adj.	See Appendix III			
Gcables1	-5,1	dB		
Gcables2	-4,5	dB		

Signal-to-Jamming-Ratios (SJR)

Values in dB are calculated using the formula above

SCENARIO 1 (10 % jamming)

PER (%)	**0**	**5**	**30**	**60**	**100**
UPLINK	PER 0% until	PER 5 %	PER 30 %	PER 60 %	PER 100 % from
BPSK 1/2	9,35	8,05	6,65	4,85	-5,35
QPSK … 64 QAM					
DOWNLINK	PER 0% until	PER 5 %	PER 30 %	PER 60 %	PER 100 % from
BPSK 1/2	-2,15	-2,25	-2,45	-2,55	-2,75
QPSK 1/2	3,55	2,65	1,65	0,65	0,35
QPSK 3/4	9,95	8,75	7,65	7,15	5,75
16 QAM 1/2	16,95	14,05	13,35	12,05	9,55
16 QAM 3/4	21,05	19,45	18,35	17,55	15,35
64 QAM 2/3	23,85	22,15	20,75	19,95	17,45
64 QAM 3/4	27,55	25,15	23,75	23,05	20,95

SCENARIO 2 (50 % jamming)

PER (%)	**0**	**5**	**30**	**60**	**100**
UPLINK	PER 0% until	PER 5 %	PER 30 %	PER 60 %	PER 100 % from
BPSK 1/2	7,35	6,65	6,25	5,65	5,05
QPSK … 64 QAM					
DOWNLINK	PER 0% until	PER 5 %	PER 30 %	PER 60 %	PER 100 % from
BPSK 1/2	4,05	3,35	2,65	2,25	1,65
QPSK 1/2	7,25	6,35	5,85	5,45	4,75
QPSK 3/4	10,05	9,05	8,35	7,95	7,15
16 QAM 1/2	12,15	11,45	10,85	10,55	9,85
16 QAM 3/4	16,25	14,95	14,25	13,85	13,05
64 QAM 2/3	20,85	19,25	18,35	17,95	16,95
64 QAM 3/4	22,65	21,25	20,25	19,85	18,75

SCENARIO 3 (wideband jamming 120%)

PER (%)	**0**	**5**	**30**	**60**	**100**
UPLINK	PER 0% until	PER 5 %	PER 30 %	PER 60 %	PER 100 % from
BPSK 1/2	5,75	5,15	4,55	4,25	3,75
QPSK … 64 QAM					
DOWNLINK	PER 0% until	PER 5 %	PER 30 %	PER 60 %	PER 100 % from
BPSK 1/2	2,15	1,55	1,05	0,65	-0,15
QPSK 1/2	5,25	4,65	3,95	3,65	2,95
QPSK 3/4	8,15	6,95	6,55	6,15	5,15
16 QAM 1/2	11,05	10,05	9,45	9,15	8,35
16 QAM 3/4	16,05	15,15	14,45	14,25	13,05
64 QAM 2/3	18,65	17,25	16,55	16,05	15,15
64 QAM 3/4	21,45	19,45	18,55	18,15	17,15

Selection of the jammed pilot (the most critical)

PER 5 %

Pilot	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
UPLINK								
BPSK 1/2	2,05	9,25	2,35	9,45	9,25	1,25	8,75	1,85
QPSK … 64QAM	-	-	-	-	-	-	-	-
DOWNLINK								
BPSK 1/2	10,25	11,05	12,85	7,75	6,75	9,05	14,25	11,45
QPSK 1/2	13,55	13,75	12,75	11,15	8,85	11,05	17,85	13,55
QPSK 3/4	13,75	14,65	15,45	11,15	8,75	13,15	18,95	15,85
16 QAM 1/2	16,75	16,95	18,25	15,45	13,05	16,45	21,75	18,55
16 QAM 3/4	20,35	19,95	18,75	17,55	15,55	17,55	23,65	18,95
64 QAM 2/3	22,85	24,05	24,25	22,25	20,25	22,75	28,35	25,25
64 QAM 3/4	26,15	26,05	24,25	24,35	22,55	23,55	29,35	24,75

SCENARIO 4 (pilot jamming)

PER (%)	0	5	30	60	100
UPLINK (pilot 4)	PER 0% until	PER 5 %	PER 30 %	PER 60 %	PER 100 % from
BPSK 1/2	9,65	9,45	8,95	8,35	-0,05
QPSK … 64 QAM					
DOWNLINK (pilot 7)	PER 0% until	PER 5 %	PER 30 %	PER 60 %	PER 100 % from
BPSK 1/2	14,55	14,25	12,45	10,95	9,55
QPSK 1/2	18,35	17,85	16,65	15,35	12,75
QPSK 3/4	19,45	18,95	18,05	16,35	13,75
16 QAM 1/2	22,75	21,75	20,65	19,05	14,95
16 QAM 3/4	25,55	23,65	23,05	21,65	16,05
64 QAM 2/3	30,85	28,35	26,85	25,45	18,95
64 QAM 3/4	32,85	29,35	28,45	27,05	19,55