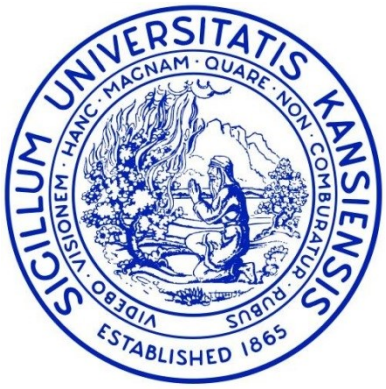
Exploiting Wireless Systems for Covert Communications

PhD. Dissertation

©2014

Zaid Hijaz



Exploiting Wireless Systems for Covert Communications

PhD. Dissertation

©2014

Zaid Hijaz

Submitted to the
Department of Electrical Engineering & Computer Science
and the Graduate Faculty of the University of Kansas
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy.

Dissertation Committee:

Dr. Victor S. Frost,
Chairperson

Dr. David Petr

Dr. Erik Perrins

Dr. Shannon Blunt

Dr. Jeffrey Lang

The Dissertation Committee for Zaid Hijaz certifies
that this is the approved version of the following dissertation:

Exploiting Wireless Systems for Covert Communications
PhD. Dissertation

Committee:

_____
Chairperson

_____

_____

_____

_____

_____
Date

Alhamdulilah

To my family for helping raise me up

To Dr. Frost for taking me under his wing

Acknowledgement

I would first and foremost like to thank God. He taught me what I knew not.

When one reflects upon his accomplishments he realizes that he is deserving of very little credit. And if it were not for those around him he would never have accomplished so much. Thanks Mom and Dad, I owe you everything. Thank you the love of my life and my daughters for patiently waiting. Thanks to my brother Zeyad for picking up the slack.

I greatly appreciate Professor Frost for taking me under his wing. Your guidance and supervision were as good as it gets.

Abstract

The desire to hide communications has existed since antiquity. This includes hiding the existence of the transmission and the location of the sender. Wireless networks offer an opportunity for hiding a transmission by placing a signal in the radio frequency (RF) occupied by a target network which also has the added benefit of lowering its probability of detection.

This research hides a signal within the RF environment of a packet based wireless (infrastructure) network. Specifically, in this research the interfering (covert) signal is placed in the guard band of the target network's orthogonal frequency division multiplexed (OFDM) signal. We show that the existence of adaptive protocols allow the target network to adjust to the existence of the covert signal. In

other words, the wireless network views the covert network as a minor change in the RF environment; this work shows that the covert signal can be indistinguishable from other wireless impairments such as fading.

The impact of the covert signal on the target system performance is discovered through analysis and simulation; the analysis and simulation begin at the physical layer where the interaction between the target and covert systems occurs. After that, analysis is performed on the impact of the covert link on the target system at the data-link layer. Finally, we analyze the performance of the target system at the transmission control protocol (TCP) layer which characterizes the end-to-end performance. The results of this research demonstrate the potential of this new method for hiding the transmission of information. The results of this research could encourage the creation of new protocols to protect these networks from exploitation of this manner.

Table of Contents

Acknowledgement iv

Abstract vi

Table of Contents viii

List of Figures xiii

List of Variables xx

Chapter 1 1

Introduction 1

Chapter 2 7

Contributions.....7

Chapter 3 13

Related Work and Roadmap 13

A. Covert Communications.....15

B. The Physical Layer 16

C. AMC and HARQ at the Data-Link Layer.....18

D. The TCP Layer.....19

E. Analysis Road Map 20

Chapter 4 21

The Physical Layer Interaction 21

A. Bit Error Rate at the Physical Layer 21

i. Introduction.....21

ii. Establish Concept of Feasibility 22

iii. Conclusions.....31

B. Probability Density Function of Received SNR with Interference...31

i. Introduction.....32

ii. Background 33

iii. Channel Modelling.....34

iv. Probability Density Function of SINR.....35

v. System Performance.....38

vi. Conclusions.....41

C. Predicting the Impact of a Covert Link on the BER of an OFDM System with Adaptive Modulation and Coding *41*

i. Introduction *42*

ii. Assumptions *43*

iii. Performance Analysis of Target System and Covert Link *44*

iv. Model Validation *49*

v. System Performance Tradeoffs *51*

vi. Conclusions *55*

D. Estimating the Average Packet Error Rate *56*

i. Introduction *56*

ii. System Configuration *58*

iii. Simulation of Packet Error Rates *59*

iv. Average Packet Error Rate with Fading and Interference *61*

v. Validation of Average Packer Error Rates *64*

vi. Conclusions *69*

Chapter 5 71

The Data-Link Layer 71

A. The Impact of Interference from a Covert Link on a Data-Link with OFDM, AMC, and ARQ *73*

i. Introduction *74*

ii. Assumptions *75*

iii. PER, Spectral Efficiency, and Outage Probability with Interference from the Covert Transmitter *79*

iv. Target System Performance....82

v. Performance Tradeoffs....88

vi. Comparing Hybrid and Truncated ARQ....92

vii. Conclusions....95

Chapter 6 97

Finite Length Queue 97

A. The Impact of a Covert Interferer on an Adaptive Modulation and Coding System with Hybrid ARQ and a Finite Queue....98

i. Introduction....98

ii. System Design and Assumptions....98

iii. Performance Analysis....100

iv. Numerical Results....105

v. Conclusions....111

Chapter 7 113

The TCP Layer....113

A. The Impact of Interference on an OFDM System with AMC, Hybrid ARQ, and a Finite Queue on End-to-End Performance....114

i. Introduction....114

ii. System Design and Assumptions....116

iii. Performance Analysis....117

iv. Numerical Results....119

v. Conclusions....128

Conclusions 130

Appendix 132

A. Mathematica *132*

B. Mat Lab *139*

C. Packet Error Rate Simulation Results *144*

References 146

List of Figures

Fig. 2.1. Computer network system with covert elements. 9

Fig. 4.1. Transmitter/receiver pairs and channels. 22

Fig. 4.2. Received PSD at the target receiver [18]. 25

Fig. 4.3. Comparison of BER curve with and without covert ($R_{b,covert}$ = 7.40 kbps, channel = -152 $E_{b,covert}/E_{b,target}$ = -10.83 dB, τ = 128 samples/symbol) [18]. . 25

Fig. 4.4. E_b/N_o Covert vs. BER target ($R_{b,target}$ = 7.40 kbps, τ= 128 samples/symbol) [18]. 27

Fig. 4.5. Target system BER vs. synchronous offset for sub-channel -105 ($E_{b,covert}/E_{b,targett}$ = -9.15 dB) [18]. 27

Fig. 4.6. Target system BER vs. synchronous offset for sub-channel -152

($E_{b,covert}/E_{b,targett}$ = -10.83 dB) [18]. 28

Fig. 4.7. Channel number vs. covert system BER [18]. 29

Fig. 4.8. Covert BER vs. synchronous offset for sub-channel -105 ($E_{b,covert}/E_{b,target}$ = -9.15 dB) [18]. 30

Fig. 4.9. Covert BER vs. synchronous offset for sub-channel -152 ($E_{b,covert}/E_{b,target}$ = -8.76 dB) [18]. 31

Fig. 4.10. PDF of SINR γ=30 dB, γc=6 dB, m_c =0.8. 37

Fig. 4.11. CDF of SINR γ=30 dB, γc=6 dB, m_c =0.8. 38

Fig. 4.12. Average PER of target system with γc==5dB. 39

Fig. 4.13. P_{out} for γc==5dB. 40

Fig. 4.14. P_{out} for γc==5dB. 41

Fig. 4.15. 16-QAM link with Nakagami-*m* fading: *m* = .75, 1.25, 1.75 and interference: SNR_{Covert} = -6 dB. 47

Fig. 4.16. 16-QAM link with Nakagami-*m* fading: *m* = .75, 1.25, 1.75 and interference: SNR_{Covert} = 6 dB. 47

Fig. 4.17. PSD of target OFDM system and covert link. 48

Fig. 4.18. 16-QAM OFDM system with QPSK covert link. 50

Fig. 4.19. Performance of OFDM system and covert link with SNR of the OFDM link = 25 dB. 51

Fig. 4.20. 16-QAM OFDM system with SNR = 26.15 dB and BPSK covert with variable bit rate. 52

Fig. 4.21. 16-QAM OFDM system with SNR = 26.15 dB and QPSK covert with

variable bit rate. 53

Fig. 4.22. 16-QAM OFDM system with SNR = 26.15 and BPSK covert with variable *m,* $r_{bc} = r_b/32$. 54

Fig. 4.23. 16-QAM OFDM system with SNR = 26.15 and BPSK covert with variable *m,* $r_{bc} = r_b/32$. 55

Fig. 4.24. System diagram with interfering transmitter. 60

Fig. 4.25. Packet error rate based on simulation of MCS (stars) and curve fitting to the simulation (line). 61

Fig. 4.26. Placement of the interfering signal in the guard band of the target down-link signal spectrum. 62

Fig. 4.27. Simulation of average PER (stars) and analytic prediction (line) for mode 5, Nakagami-*m* fading, interfering signal SNR = 5dB [21]. 65

Fig. 4.28. Simulation of average PER (stars) and analytic prediction (line) for all modes with covert signal SNR = 15 dB, Rayleigh fading. 66

Fig. 4.29. Simulation of average PER (stars) and analytic prediction (line), Rayleigh fading, interfering signal SNR = 5dB [21]. 67

Fig. 4.30. Simulation of average PER (stars) and analytic prediction (line) for mode 1, Nakagami-*m* fading, interfering signal SNR = 15dB [21]. 68

Fig. 4.31. Simulation of average PER (stars) and analytic prediction (line) for mode 5 with varying covert signal SNR, Rayleigh fading [21]. 69

Fig. 5.1. Design space variables. 73

Fig. 5.2. System model extended from [25] to include covert link. 74

Fig. 5.3. Mapping of bits to packets, frames, and symbols from [25] with modifications..... 77

Fig. 5.4. PER of target system with average covert SNR = 5 dB, Nakagami-*m* fading. 84

Fig. 5.5. Spectral efficiency of target system with average covert SNR = 5 dB, Nakagami-*m* fading..... 85

Fig. 5.6. P_{out} of target system with average target SNR = 26.15 dB, Nakagami-*m* fading. 85

Fig. 5.7. PER of 1st transmission of target system with average covert SNR = 5 dB, Nakagami-*m*=fading parameter..... 86

Fig. 5.8. Spectral efficiency of target system with $Nrmax = 3$. 87

Fig. 5.9. PER of target system with average target SNR = 26.15 dB, Nakagami-*m* fading. 89

Fig. 5.10. Spectral efficiency of target system with average target SNR = 26.15 dB, Nakagami-*m* fading..... 90

Fig. 5.11. PER of 1st transmission of target system resource block for increasing covert power..... 91

Fig. 5.12. Spectral efficiency of target system resource block for increasing covert power with $Nrmax = 3$. 91

Fig. 5.13. PER of target system with average covert SNR = 5 dB for truncated and hybrid ARQ, Rayleigh fading (*m* = 1). 93

Fig. 5.14. Spectral efficiency of target system with average covert SNR = 5 dB for

truncated and hybrid ARQ, m = 1. 94

Fig. 5.15. Difference of PER of target system with covert SNR=5 dB for truncated and hybrid ARQ, m = 1. 94

Fig. 5.16. Difference of PER of target system with covert SNR=15 dB for truncated and hybrid ARQ, m = 1. 95

Fig. 6.1. Target and covert networks. 99

Fig. 6.2. Throughput of target system with average covert SNR = 5 dB, Nakagami-m fading. 107

Fig. 6.3. Packet loss probability of target system with average covert SNR = 5 dB, Nakagami-m fading. 107

Fig. 6.4. Average spectral efficiency of target system with average covert SNR = 5 dB, Nakagami-m fading. 108

Fig. 6.5. Throughput of target system with average SNR = 26.15 dB vs. covert SNR, Nakagami-m fading. 108

Fig. 6.6. Packet loss probability of target system with average SNR = 26.15 dB vs. covert SNR, Nakagami-m fading. 109

Fig. 6.7. Average spectral efficiency of target system with average SNR = 26.15 dB vs. covert SNR, Nakagami-m fading. 109

Fig. 6.8. Throughput of target system with varying covert SNR, Nakagami-m fading. 110

Fig. 6.9. Packet loss probability of target system with varying covert SNR, Nakagami-m fading. 110

Fig. 6.10. Average spectral efficiency of target system with varying covert SNR, Nakagami-m fading. 111

Fig. 7.1. Target and covert networks with TCP parameters. 117

Fig. 7.2. Throughput of target system, Nakagami-m fading, interferer SNR = 5dB. 121

Fig. 7.3. Round-trip-time of target system , Nakagami-m fading, interferer SNR = 5dB. 121

Fig. 7.4. Packet loss rate (φ) of target system , Nakagami-m fading, interferer SNR = 5dB. 122

Fig. 7.5. Throughput of target system SNR= 26.15 dB vs. variable interferer SNR, Nakagami-m fading. 123

Fig. 7.6. Round-trip-time of target system SNR= 26.15 dB vs. variable interferer SNR, Nakagami-m fading. 123

Fig. 7.7. Packet loss rate (φ) of target system SNR= 26.15 dB vs. variable interferer SNR, Nakagami-m fading. 124

Fig. 7.8. Throughput of target system for interferer SNR 5 and 10 dB, Nakagami-m fading. 125

Fig. 7.9. Round-trip-time of target system for interferer SNR 5 and 10 dB, Nakagami-m fading. 125

Fig. 7.10. Packet loss rate (φ) of target system for interferer SNR 5 and 10 dB, Nakagami-m fading. 126

Fig. 7.11. Change in throughput ($\Delta\eta$) of target system, $\Delta\eta 1.0{,}0.5$ compared to $\Delta\eta 1.0{,}10\ dB$ 127

Fig. 7.12. Change in throughput ($\Delta\eta$) of target system, $\Delta\eta 2.0,1.0$ compared to $\Delta\eta 1.0,10\ dB$ 128

Fig. 7.13. Change in throughput ($\Delta\eta$) of target system, $\Delta\eta 3.0,2.0$ compared to $\Delta\eta 3.0,10\ dB$ 128

List of Variables

Variable	Description
i	Sub-carrier
I	No. of sub-carriers in an OFDM signal
M	No. of M-ary QAM constellation points
M_n	M_n-ary constellation assigned to mode n
k	Packet transmission attempt
K	Maximum no. of packet transmission attempts
n	AMC mode
N	No. of AMC modes
m	Fading parameter
m_c	Covert fading parameter
B	Sub-carrier bandwidth
B_c	Covert bandwidth
f_s	Sub-carrier spacing
f_{sc}	Covert center frequency
$H(f)$	Matched filter response
$S_i(f)$	OFDM sub-carrier PSD
$G_k(f)$	Jammer PSD
$P_{b,i}$	Bit error probability of i^{th} channel
B_i	Bits per channel
T	Synchronous offset

γ_{pn}	AMC curve fit maximum SNR where packet error rate is 1
$\bar{\gamma}$	Average target sub-carrier SNR
$\bar{\gamma}_c$	Average covert SNR
$\bar{\gamma}_r$	Average received SNR with covert interference
γ_k	Instantaneous packer SNR
a_n, g_n	PER mode curve fit parameters
N_f	Number of symbols per frame
N_c	Number of pilot symbols per frame
N_b	Number of bits per frame
N_p	Number of bits per packet
R_c	FEC coding rate
R_n	Information bits per symbol for mode *n*
r_i	Bit rate (bits/second)
φ	Packet loss rate
$\gamma_{T,n}$	Minimum SNR threshold meeting QoS constraint
$\gamma_{S,n}$	SNR threshold where spectral efficiency for mode *n* equals *n-1*
γ_n	Minimum SNR threshold where mode *n* is selected
$\bar{T}$	Average throughput at the queue
PER_n	Instantaneous PER for mode *n*
$p_\gamma(\gamma)$	PDF of SNR
$f_\gamma(\gamma)$	PDF of SNR with covert (SINR)
K_k	Modified Bessel function
ρ_i	Sub-carrier impact factor
$\mathrm{Pr}_c(n)$	Probability of mode *n*
P_c	Covert power
$\overline{PER}_{cn}$	Average PER of mode *n*
$\overline{PER}_c$	Average PER
$\bar{N}_a$	Average no. of packet transmission attempts
$\bar{S}_0$	Average spectral efficiency without retransmission
$\bar{S}_K$	Average spectral efficiency after K attempts
S	Spectral efficiency
P_{out}	Outage probability
RTT	Round trip time
b	No. of packets per frame
λ	Average TCP sending rate
β	TCP sending rate
N_r	No. of transmissions per segment
T_0	Average segment delay over wireline
T_s	Average segment transmission time over wireless channel
T_q	Average waiting time in base station queue
T_{wf}	ACK feedback delay over wireless channel
T_{wl}	$T_q + T_s$
η	TCP throughput
P_d	Packet dropping probability at the queue
P_0	Target packet error rate
A_t	Packet arrivals at time t
C_t	Queue server state at time t
U_t	Queue state at time t
T_f	Frame time, sever time unit
f_d	Doppler frequency
N_n	Cross rate of mode n

N_T	Covert in-band interference power
$P_{n,n}$	Probability of state transition
$\boldsymbol{P_c}$	State transition matrix
$\boldsymbol{P}$	State transition probability matrix
$\boldsymbol{A_{K,K}}$	State transition probability sub-matrix
D	Number of dropped packets
Q	Length of finite queue

Chapter 1

Introduction

As demand for wireless communication devices has grown substantially, so has the amount of information needed to be carried by service provider networks. Wireless carriers have also marketed smart phones as the device of choice [1]. These devices offer companies an opportunity for greater revenue by being able to charge for additional services such as email, internet access, and video. However, mobile devices put pressure on limited network resources, especially spectrum. Applications that run on these devices require substantially more network resources when compared to traditional voice services.

The increased number of users in addition to more bandwidth hungry applications has forced communication system designers to increase the capacity of

their wireless networks. The use of OFDM increases spectral efficiency when compared to Frequency Division Multiplexing (FDM). Adaptive coding and modulation (AMC) allow the system the ability to adapt to an ever changing fading environment and maintain a packet error rate (PER) while hybrid auto-repeat-request (HARQ) enables the system to recover from errors due to the wireless channel which results in a more efficient utilization of spectrum as do higher order modulation techniques such as quadrature phase shift keying (QPSK) or M_n-ary quadrature amplitude modulation (M-QAM). Coding methods such as convolutional codes and turbo codes also yield increased efficiencies.

The limited resource of spectrum has challenged engineers to invent solutions to the challenge of exponentially increasing demand. The "Shannon Limit" [2, 3] for channel capacity clearly demonstrates the amount of bits/second/channel theoretical capacity limit of a communication channel. OFDM, in combination with the aforementioned technologies, allows channels to achieve very high data rates (100 Mbps soft-input soft-output - SISO) [4] that are near capacity.

All fourth generation wireless communication systems (4G) currently being proposed use OFDM. Every major wireless carrier in the United States [1], Europe, and Asia [5] will migrate to Long Term Evolution-Advanced (LTE-Advanced). LTE technologies are expected to be staples for 4G and beyond networks [6]. Already, these standards are being applied to networks across the globe to help cope with the demand created by smart phones.

The purpose of covert communication is to hide, with a low probability of

detection (LPD), the transmission of information; sometimes the covert signal can be embedded within an existing non-covert communication. The desire to hide the transmission of information has existed for a long time. This includes the desire to hide the existence of the transmission. In [7] stenography is discussed as well as several covert methods of transmitting information. These methods vary greatly from ancient examples of using a human scalp to embed a hidden message to modern times where covert information can be hidden in the flow of data packets transmitted over the internet. Also discussed in [7] are some of the reasons behind covert communication as well as a few historical examples of covert communication. The reasons for covert communication can vary. Reasons include a desire to allow the sender to remain anonymous or hide the existence of the communication.

Encryption is not sufficient to hide the transmission of information. The hiding of information is usually associated with stenography while a covert channel is usually associated with embedding information within network protocols [8]. The DoD defines a covert channel as "{...} any communication channel that can be exploited by a process to transfer information in a manner that violates the system's security policy" [9]. The use of stenography or a covert channel requires common system elements so that the covert communication "hides" within normal communication. LPD communication systems have a history of providing a method for hiding RF transmissions [10], [11], and [12] in noise. LPD addresses the hiding of the signal while low probability of intercept (LPI) refers to denying the intercept system the ability to extract features of the signal; the combination of LPI and LPD is

referred to as low probability of exploitation (LPE) [10]. Here we are concerned with achieving LPD.

It has been reported that the US State Department is interested in the development of "stealth" wireless networks to assist activists in their endeavors [13]. Covert communication methods are of interest not only to those willing to exploit the characteristics of the communication system for these ends, but also to those managing the systems and protecting them from vulnerabilities or exploitation [8].

The significant pressure on wireless networks that has been brought on by the exponential growth in mobile devices and their applications has led to increased frequency reuse and the advent of femtocells [14] which are potential sources for interference. Mobile ad hoc networks (MANETs) and a lack of available spectrum also contribute to the potential for interference which is one of the limiting factors of capacity in wireless networks. The ability to more accurately predict PER performance of multi-carrier systems when subject to interference from the aforementioned sources could lead to better spectrum management [15]. Therefore, the development of a method for predicting target network performance when a wireless link is impacted by interference when certain characteristics are known (e.g., spectral shape and power) can apply not only the covert link scenario, but also any form of interference. One of the challenges in finding the average PER is that the interference can impact each sub-carrier differently, i.e., each sub-carrier can have a different signal-to-noise-ratio (SNR). The calculation of the PER in systems with coding is not straightforward due to the fact that the bits of a packet are distributed

amongst multiple sub-carriers and the PER for single carrier systems differs from multi-carrier systems [16].

It is therefore beneficial to study the potential of covert ad hoc networks exploiting OFDM technology based wireless networks. Clearly there will be wide spread deployment of OFDM systems and the degree to which people will depend on them is destined to become significant. There has been little research in the area of covert ad hoc networks with regard to exploiting OFDM and 4G wireless networks [17].

Through this research we identify the characteristic technologies that make future wireless networks and their standards candidates for exploitation. This research has involved three separate aspects; 1) development of an analytic model that properly defines the interaction between the target and covert networks as well as the impacts on one another 2) a computer simulation of this interaction and exploitation by the covert network at the physical layer as previously reported in [18] and 3) analysis of the impact of the covert on end-to-end performance of the target network. This research quantifies the tradeoffs in exploiting an OFDM based wireless network for covert communication. The work here also demonstrates the effects of the covert network on the performance of the target OFDM 4G wireless system; it shows the effectiveness and throughput of the covert networks communication in the presence of the target OFDM network and examines the ability of the covert network to operate at a low power relative to the target network. We show that for effective covert link performance with relatively low SNR there is a decrease in the performance of the

target network that is practically indistinguishable from other wireless impairments such as fading.

This research demonstrates the impact of a covert link on a target wireless network and the impact of the target network on the covert link; it shows the potential for covert communications. Showing the ability of a covert network to operate effectively within the RF environment of a packet based wireless target network will encourage the development of protocols to prevent this type of exploitation. Also, this work offers the potential to contribute to the development of "stealth" wireless technologies that can assist others in the hiding of communication.

Chapter 2

Contributions

Fourth generation wireless networks take advantage of several technologies that allow them to cope with the demand of increasingly data hungry devices and allow for increased network capacity. Hence, a higher quality of experience (QoE) can be achieved by increasing throughput, reducing end-to-end delay, and reducing packet loss. AMC, OFDM, and HARQ increase overall throughput and reduce end-to-end delay.

Adaptive coding improves throughput by increasing the modulation order (4, 16, 64-QAM) on the sub-channels having a better channel quality. Adaptive modulation also increases throughput by increasing the coding rate based on the same condition. The combining of the two allows for different modulation and coding

schemes (MCS) that operate at the physical layer. The utilization of OFDM increases spectral efficiency when compared to FDM. These technologies when combined at the physical layer with HARQ at the data-link layer enable links to transmit more data thereby increasing throughput and reducing end-to-end delay under certain channel conditions.

The aforementioned system mechanisms respond as channel conditions, such as fading, change. We show that the introduction of a covert link exploiting a target network at the physical layer will affect the performance of the target network in a manner that is practically indistinguishable from fading when the covert has relatively low power [18-21]. Here the covert signal is placed in the guard band of the target OFDM signal which are required by the FCC for channel spacing. Target and covert network components are shown in Fig. 4.1.

As a first step to establish feasibility of the proposed concept we simulate the effects of inserting a narrow band signal that will be used for covert communication in one of the unused sub-carrier locations of the OFDM signal and analyze its influence on the target OFDM signal as well as determining the communications capabilities of the covert link. The covert signal inserted in an unused sub-carrier location, or frequency "slot", is no longer orthogonal to the target OFDM waveform. Thus, there is potential for the covert signal to impact the performance of the target link. Here we examine the effect of the covert signal on the target OFDM system as a function of the location of the covert signal, its power, and bit rate. The communications capability of the covert link is also studied. The amount of information that can be transmitted

covertly with minimal impact on the target OFDM system, i.e., a relatively low SNR of 5dB, is also presented. We show that a covert link with an average SNR of 5 dB can achieve an uncoded BER of approximately 10^{-2} while operating in the guard band of an OFDM target signal that has an average SNR of 26.15 dB and have an impact on the target link that is practically indistinguishable from fading. A target system with average SNR of 26.15 dB has a bit-error-rate (BER) that is 10^{-3} or better.

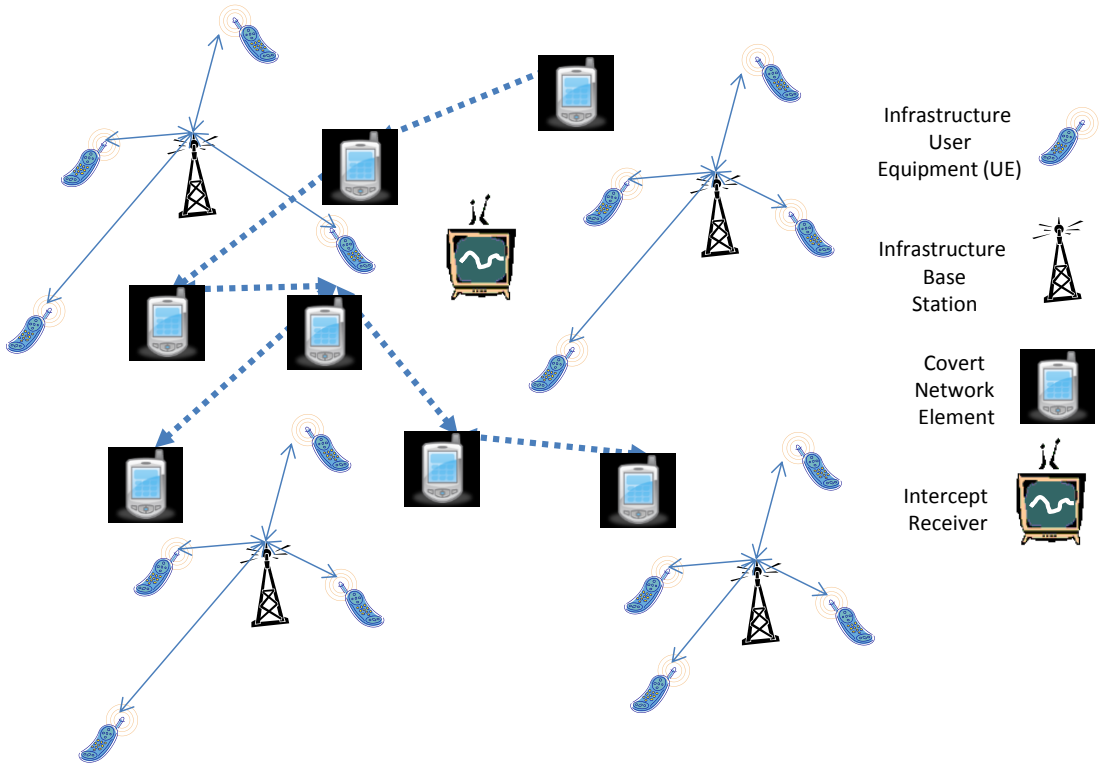


Fig. 2.1. Computer network system with covert elements.

To obtain the above result a probability density function (pdf) for the signal to interference plus noise ratio (SINR) was utilized. A separate pdf is used given the target and interfering signal have the same *m* fading parameter, target and interfering signals have different integer *m* fading parameter and different non-integer *m* fading

parameter. The pdf is used on the analysis to quantify the performance trade-offs for an OFDM system with interference from a covert transmitter. We utilize numerical integration for the prediction of the BER of an OFDM system with a covert interferer while both signals are subject to independent Nakagami-*m* fading and share the same *m* fading parameter; the performance of the covert interferer is also derived. An analytic model is used to show the trade-offs between the OFDM system BER versus covert link SNR and covert link BER versus target signal SNR. We then compare the analytic results to simulation which allows us to see how well the analysis performs in predicting the BER and confirm the approximation of interference to additive white Gaussian noise (AWGN).

We then propose a method for estimating the average PER of a coded OFDM system when the signal is subject to interference with a shaped spectral density (covert interferer). Thus the interference has a different impact on each sub-carrier. Typically, the PER is a function of the received SNR and the packet bits are distributed evenly amongst a fixed number of sub-carriers where each sub-carrier has the same SNR. The OFDM system under consideration utilizes convolutional coding for error correction and M-QAM for signaling. This method assumes that each sub-carrier is affected by a different interference power. The novelty of this contribution lies in equating the average interference power affecting each sub-carrier to an equivalent AWGN power. We compare PER prediction using this approach to simulation for a number of MCS to validate that the proposed approximation can be used to calculate the average PER.

The next contribution of this work is the prediction of the performance of the

target infrastructure network at the data-link layer. The PER and spectral efficiency of a packet based system that utilizes OFDM, AMC, and truncated-ARQ (TARQ) in the presence of a covert link while operating in a Nakagami-*m* fading environment is presented. The analytic model developed here demonstrates the tradeoffs between the target system performance at the data-link layer and increased covert link performance. These results also provide evidence to support the notion that the presence of the covert transmitter is practically indistinguishable from channel fading when one considers target system performance at the data-link layer. We then extend previous analysis and present results for networks that utilize HARQ. A comparison of HARQ data-link layer performance and TARQ in the presence of a covert link is also presented.

Analysis is then performed on the aforementioned system with the addition of a finite queue. The work here measures physical layer performance in terms of average spectral efficiency (ASE) and the queue's performance is measured in terms of throughput and packet loss rate versus increased covert signal power while assuming both signals are subject to independent Nakagami-*m* fading. The performance of this system is also shown to be practically indistinguishable from channel fading when HARQ is utilized.

Finally, end-to-end analysis is performed at the TCP layer. The work here shows the effect of a modulated interfering signal, i.e., the covert link, in the guard band of an OFDM system with AMC, HARQ, and a finite queue on the end-to-end TCP performance. In some cases, the impact from the interference with an average

SNR of 5 dB continues to be indistinguishable from the effects of channel fading in terms of TCP throughput and end-to-end delay.

This investigation shows the ability of the covert link to effectively communicate in the presence of the target infrastructure network. It quantifies the performance of the target network at every relevant layer and takes into consideration all relevant mechanisms of the target infrastructure network. This analysis shows that the covert link having an average SNR of 5 dB, utilizing 4-QAM signaling, and $1/8^{th}$ the symbol rate of the target system can have an impact on the target network performance that is practically indistinguishable from fading at all relevant layers up to the TCP layer where the covert link has an uncoded BER~10^{-2}.

Future work is needed to show the tradeoffs of covert network power and performance versus maintaining a LPD. The LPD advantage is gained by "hiding" the covert transmission in the allocated spectrum of the target network. Research is needed to quantify the probability of detection versus covert network throughput and power. Selection of a waveform for the covert signal is also a question for future endeavors.

Chapter 3

Related Work and Roadmap

The proposed study will show the impact of a covert link on a target network. Several technologies have been added in wireless network standards, such as 4G LTE-Advanced, to help cope with the exponential increase in demand on wireless networks. These technologies are implemented at the various internet protocol layers.

This research is aimed at discovering new approaches to covert communications that combines the attributes of LPD communication systems and covert channels by utilizing knowledge of the underlying protocols to enhance the transmission of covert communications ability to remain hidden.

These new standards also implement a cross layer optimization strategy. The cross layer strategy involves the sharing of information between the protocol layers in

order to achieve a target performance metric as opposed to each layer operating independently. This approach has the effect of increasing throughput, reducing delays, and improving the QoE for target network users. This research will show the effects of the covert network at the physical, data-link, and TCP layers of a target infrastructure network that employ cross layer optimization mechanisms

The work here uses existing analysis on the effects of partial band jamming of OFMD based WLAN at the physical layer in terms of BER performance [22, 23] to begin the assessment of the impact of the covert link on the target system. Work at the physical layer continues by assessing the impact of the covert link in terms of PER. The work in [24] utilized simulation and curve fitting to find the PER as a function of SNR for HiperLAN systems. A similar approach is used here to find the PERs as a function of SNR for an LTE "like" system. Moreover, [24] proposes a cross-layer mechanism to maximize the throughput of a HiperLAN system with OFDM and AMC. Next, TARQ is added to this system in [25]. Then, a finite queue and an additional cross layer mechanism is added in [26]. Finally, [27] takes the analysis of this system up to the TCP layer. The work in [28] performs analysis that calculates the average PER for a multi-carrier system with AMC, as in [24-27], that utilizes HARQ as opposed to TARQ. Covert channels in LTE-Advanced are investigated in [17]. Extensions and headers are analyzed where covert data can be hidden for covert communications.

The aforementioned works will provide a framework for analyzing the impact of interference with a shaped spectral density on a target 4G network that employs

OFDM, AMC, HARQ, and a finite queue.

A. Covert Communications

The hiding of information is usually associated with stenography while a covert channel is usually associated with embedding information within network protocols [8]. The DoD defines a covert channel as "{...} any communication channel that can be exploited by a process to transfer information in a manner that violates the system's security policy" [9]. The use of stenography or a covert channel requires common system elements so that the covert communication "hides" within normal communication. Here we are concerned with achieving LPD.

The covert link proposed here must maintain a LPD while also effectively communicating and having unnoticeable impact on the target network. This is achieved by exploiting the adaptive protocols used in all current and future wireless systems such as AMC and HARQ. Headers and extension fields in LTE-Advanced are examined in [17] where covert information can be placed. The covert channel capacity of the medium access (MAC), radio link control (RLC), and packet data convergence protocol (PDCP) layers for varying modulation, coding, and bandwidth are calculated in [17]. The trellis structure and adaptive modulation strategy is utilized in [29] to transmit a covert signal with the goal of designing an undetectable covert channel. The analysis in [29] reveals that the proposed covert communication scheme withstands extremely high levels of network noise and adversarial disruption, while it maintains a LPD. The threat of network based covert channel attacks, their classes and properties, are the subject of the study in [30]. Specifically, hardware and

operating system attacks are implemented and evaluated in [30] where significant differences in their properties and mechanisms are shown. The work in [31] discusses four ways to smuggle messages through the internet. Covert channels in computer network protocols, which attempt to hide the very existence of the communication in the high bandwidth environment, is the focus in [8, 32] where an overview of existing techniques for covert channels and their countermeasures is given. The aforementioned work on covert communications provides an overview of the varying methods and challenges that are faced by covert communications as well as their importance and capabilities. The covert communication presented here utilizes the target network spectrum and exploits the adaptive characteristics of the target network protocols to maintain a LPD. The adaptive protocols of the target network also allow the covert link to have little impact on the target network performance.

B. The Physical Layer

The physical layer is where the interaction between the covert link and the target network occur. The main goal in analyzing the effects of this interaction can be captured by deriving a received SNR which aids in the analysis of a BER as a function of SNR.

The work in [22] studies the effect of partial band jamming of an OFDM based 802.11G WLAN signal. It compares the effect of jamming on a coded versus an uncoded OFDM system. The jammer is assumed to have a square power spectral density (PSD). A received SNR is derived in [22] for a channel with AWGN and a co-channel interferer given by

$$\gamma_i = \frac{\int_{-\infty}^{\infty} |S_i(f)H(f)^2| df}{\int_{f-f_S/2}^{f+f_S/2} |G_k(f)H(f)^2| df + \frac{N_0}{2} \int_{-\infty}^{\infty} |H(f)^2| df}, \quad (1)$$

where (1) represents the received SNR for the *i*-th sub-carrier of the OFDM signal. Here, $S_i(f)$ represents the target signal sub-carrier PSD, $G_k(f)$ represents the covert signal PSD in the band of the OFDM sub-carrier, and $H(f)$ represents the matched filter response. Then, a PDF is derived for the received SNR given that both signals are subject to Rayleigh fading. Next, an average BER for the *i*-th sub-carrier is found based upon

$$P_{b,i} = \int_0^{\infty} p_i(\gamma) P_b(\gamma) d\gamma \quad (2)$$

The average BER for a given sub-carrier is found by integrating over all possible values of the received SNR, γ, the product of the pdf of the received SNR and probability of BER as a function of the received SNR, P_b. The average BER for the entire OFDM signal is found by

$$P_b = \frac{\sum_0^{N-1} P_{b,i} \cdot B_i}{\sum_0^{N-1} B_i}, \quad (3)$$

where B_i represents the bits-per-channel of the *i*-th sub-carrier.

This same approach is used to develop a received SNR here. Whereas the jammer in [22] is assumed to be rectangular, the covert signal considered is modulated and has a shaped spectrum that is $sinc^2$. The method for calculating the amount of power in the band of the target network's OFDM sub-carrier is done by setting the amount of power from the covert signal equal to a spectrally flat noise signal. This approach is utilized by [33] to find the BER.

C. AMC and HARQ at the Data-Link Layer

Wireless networks currently implement technologies that allow them to achieve improved spectral efficiency and increase the reliability of their connections. From amongst these technologies AMC is utilized at the physical layer while HARQ is utilized at the data-link layer.

The work in [24-27] deals with both the physical and data-link layers. Typically, these two layers operate independent of one another as the open systems interconnection model (OSI) stipulates. Traditionally, strict boundaries exist between these layers. In [25] a cross-layer design is developed which combines AMC at the physical layer with truncated ARQ at the data-link layer. The purpose of this design is to maximize spectral efficiency given delay and error performance constraints. The achieved spectral efficiency is derived in closed form assuming Nakagami-*m* block fading channels. The numerical results presented in [25] demonstrate that the joint AMC-ARQ design outperforms either AMC only at the physical layer or ARQ with a fixed modulation and coding at the data-link layer. Retransmissions at the data-link layer relieve stringent error control requirements at the physical layer.

The work in [24-27] assumes a that the channel is frequency flat and varies from frame to frame, that perfect channel state information (CSI) is available at the receiver, and that error detection based on cyclical redundancy check (CRC) is perfect. The system is constrained by a maximum number of packet retransmissions after which the packet is considered lost. The maximum packet loss probability is known which is set according to a performance requirement at the physical layer. The

AMC mode is set with the goal of maximizing the data rate while maintaining the performance requirement at the physical layer.

Work completed in [26] incorporates a finite queue at the base station. This allows the derivation of a closed form expression for the packet loss rate and the average throughput. A cross-layer design is introduced which optimizes the target PER in AMC at the physical layer and maximizes the average throughput when combined with a finite queue at the data-link layer. A finite queue and server states that are directly related to the AMC mode is represented by a finite state Markov chain (FMSC) with state pair containing both the queue and server state. This model is utilized to compute a stationary distribution for the queue and server states in [26].

The analysis in [24-27] guides the work here. The PER of a particular mode with interference is found and then the average PER over all AMC modes is calculated. The PER and finite queue analysis leads into the performance of HARQ at the data-link layer. Applying the cross-layer optimization method developed in [24-27] lead to a fuller understanding of the effects of the covert link on the physical and data-link layers.

The analysis in [28] examines a system with AMC and HARQ. The closed form expression for the average PER is derived in [28] for slow and fast varying channels.

D. The TCP Layer

The impact of the covert link on the end user, served by the target network,

will be quantified by the TCP performance. The work in [27] studies an end-to-end connection equipped with AMC at the physical layer and TCP protocol at the transport layer. By relying on a fixed-point procedure, a cross-layer design is presented in [27] that optimizes the target PER of AMC at the physical layer in order to maximize TCP throughput at the transport layer when coupled with a finite queue at the data-link layer.

E. Analysis Road Map

The first step of the work here establishes the feasibility of the proposed concept through simulation of the BER at the physical layer which was published in [18]. The work in [24-27] begins with the pdf of the received SNR in its analysis in order to find the system performance. Next, we validate the approximation of the interference for AWGN and find the PERs of our system as a function of the SNR which was published in [21]. Then, we used the pdf of the received SNR with interference which allows the approach in [24-27] to be followed. However, we modify the analysis in [24-27] for HARQ based on the work in [28]. A finite queue is added to the system as in [26] and finally we examine the TCP layer as in [27].

A unique aspect of this method of covert communication is the minimum impact on the target network in terms of PER, throughput, and spectral efficiency. This scheme has a potentially large design space; analysis and simulation at the physical layer lead to a focus on a part of the design space that is relevant in achieving goals.

Chapter 4

The Physical Layer Interaction

A. Bit Error Rate at the Physical Layer

i. Introduction

To demonstrate the feasibility of the proposed concepts, preliminary research related to the physical layer has been completed in [18]. The interaction between the target network and the covert link occur at the physical layer. The first aspect of completed work involved a “proof of concept” that simulated a single covert signal exploiting an OFDM wireless signal [18]. The second part of preliminary work involves the development of an analytic expression for the PDF of a received SNR and a simulation to verify its validity.

ii. Establish Concept of Feasibility

The work in [18] involved studying the effects of inserting a narrow band signal to be utilized for covert communication in one of the unused sub-carrier locations of the OFDM signal and analyzing its influence on the target OFDM signal as well as determining the communications capabilities of the covert link. The non-utilized sub-channels occur due to either guard bands or poor channel characteristics. The covert signal when inserted in a single unused sub-carrier location or frequency "slot" is no longer orthogonal to the target OFDM waveform. The effect of the covert signal on the target OFDM system as a function of the location of the covert signal, power, and bit rate were simulated. The communications capability of the covert link was also simulated. The amount of information that can be transmitted covertly with minimal impact on the target OFDM user (i.e., relatively low probability of detection) was also presented.

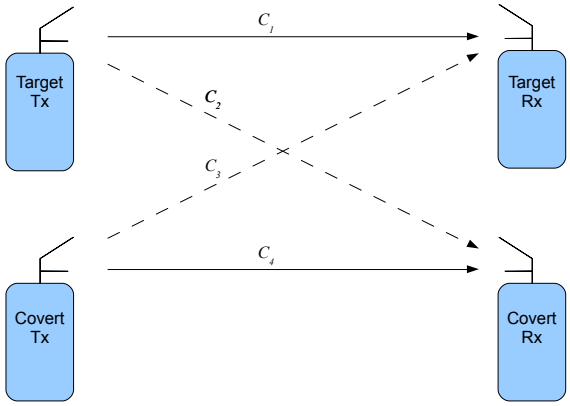


Fig. 4.1. Transmitter/receiver pairs and channels.

The work in [18] assumes ideal CSI at the receiver. The four channels in Fig. 4.1 are simulated: 1) target transmitter to target receiver 2) target transmitter to covert receiver 3) covert transmitter to target receiver and 4) covert transmitter to covert receiver. It is also assumes that the covert transmitter has knowledge of the target network's non-utilized sub-channels.

Table I gives target OFDM system parameters. Fig. 4.2 is an example of the received PSD at the target receiver. The channel noise power is set to N_o = 0.0002 W/Hz. The covert communications system uses BPSK signaling and 6 samples/symbol cyclic prefix (CP). The parameters of the covert communications system were varied as part of this study. The covert system is specified in terms of its bit rate-$R_{b\text{-}covert}$, spectral location-i, relative power-$E_{b,covert}/E_{b,target}$ dB, and synchronous offset- τ.

TABLE I

TARGET OFDM SYSTEM PARAMETERS

Modulation	QPSK, 16-QAM, 64-QAM
RF Bandwidth	5MHz
Sub-carrier spacing	15 kHz
Number of sub-carriers	512 (512 FFT)
Cyclic Prefix	6 samples/symbol
Number of samples/symbol + CP	518
Symbol Time	13.5 (msec)
Number of modulated sub-carriers	301
Normalized Power	1 Watt
Target SER	10^{-4}

The first case simulated the effect of increasing the noise power while maintaining constant signal power on the target system in the presence of the covert link. We would expect that the BER increases with increasing noise power (N_o). The target OFDM signal power will remain constant while the noise power increases, thereby decreasing the E_b/N_o. The covert will occupy spectrum in a selected unused "slot" adjacent to the sub-carriers occupied by the OFDM signal and be held at constant power. Here, sub-channel -152, a guard band sub-channel, was chosen as the covert sub-channel. It can be seen in Fig. 4.3 that the presence of the covert signal has little effect on the target non-covert system for this case as the two lines follow the same path.

Fig. 4.4 demonstrates the increase of target system BER as the covert signal power increases for several spectral locations. The dashed line is inserted for comparison. It provides us with a reference for the BER of the target system without a covert signal present. The BER rate increase is comparable for a $E_{b,covert}/N_o$ less than 9 dB when placed in channel -152. This is the power required to achieve a desired SER equal to that of the non-covert system of 10^{-4}. Beyond that, the BER for the non-covert OFDM becomes more noticeable as covert power increases.

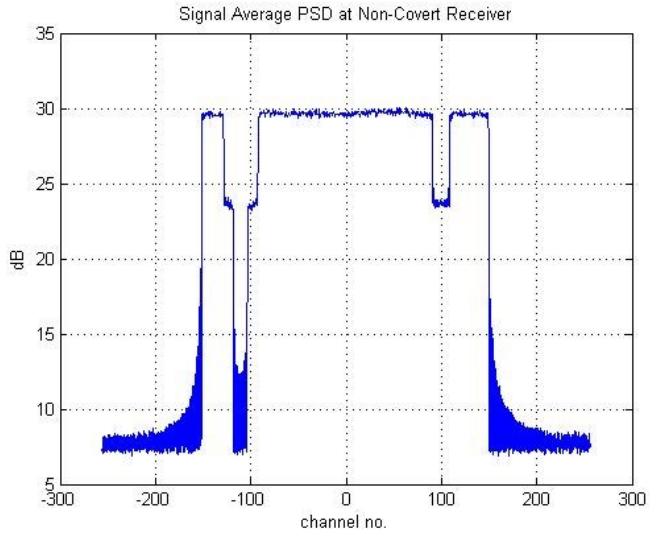


Fig. 4.2. Received PSD at the target receiver [18].

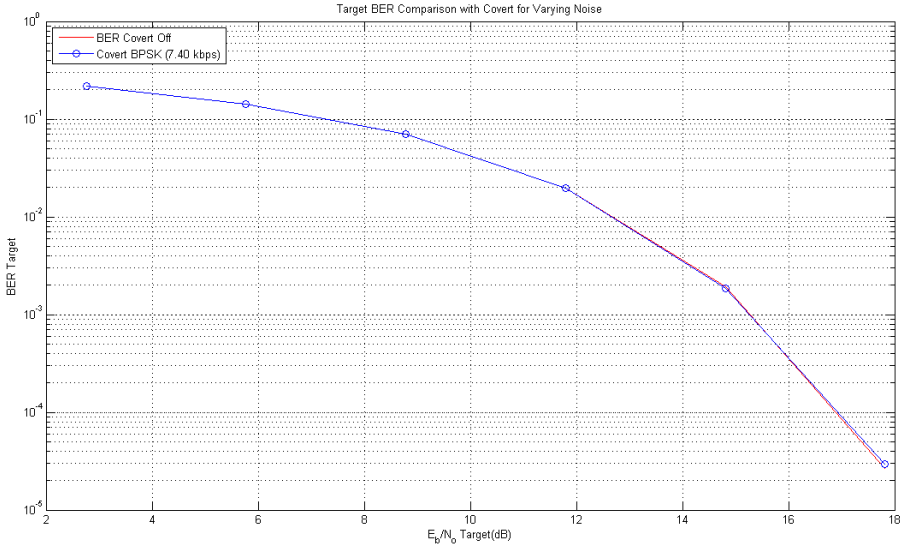


Fig. 4.3. Comparison of BER curve with and without covert ($R_{b,covert}$ = 7.40 kbps, channel = -152 $E_{b,covert}/E_{b,target}$ = -10.83 dB, τ = 128 samples/symbol) [18].

Another of the variables that was examined is the synchronous offset between the two signals, τ. The OFDM signal sub-carriers are orthogonal to one-another. However, the non-covert will only achieve this orthogonality if its timing is perfectly in line with the OFDM symbols. In other words, the covert symbol must arrive at the receiver at precisely the same instant as the non-covert symbol. This is very unlikely and may not be possible to achieve in practice.

Figs. 4.5 and 4.6 show the simulated effects of a synchronous offset in terms of the samples per symbol. When the covert signal is offset, it loses its orthogonality with respect to the other OFDM sub-carriers thereby resulting in co-channel interference. We examined the effects of this interference on the target OFDM signal for synchronous offsets of 0, 1, 4, 8, 16, 32, 64, 128, and 256 samples per symbol. The power of the signals and the noise power were held constant throughout this part of the study. We must note that there is a set of sub-carriers around i = -105 inside the utilized spectrum of the target OFDM signal that are unused. This result also demonstrated that the covert communication signal does not impact the overall target system BER even when the covert signal is embedded inside the modulated OFDM spectrum.

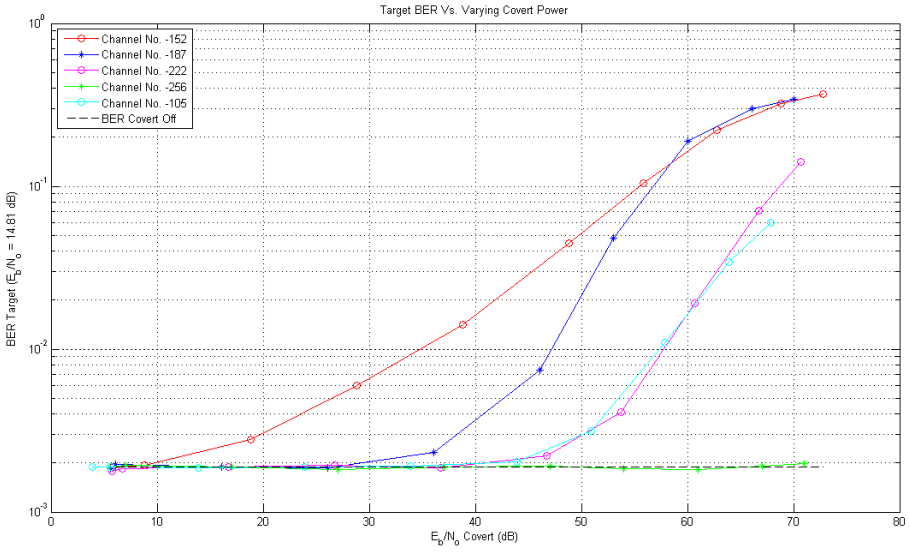


Fig. 4.4. E_b/N_o Covert vs. BER target ($R_{b,target}$ = 7.40 kbps, τ= 128 samples/symbol) [18].

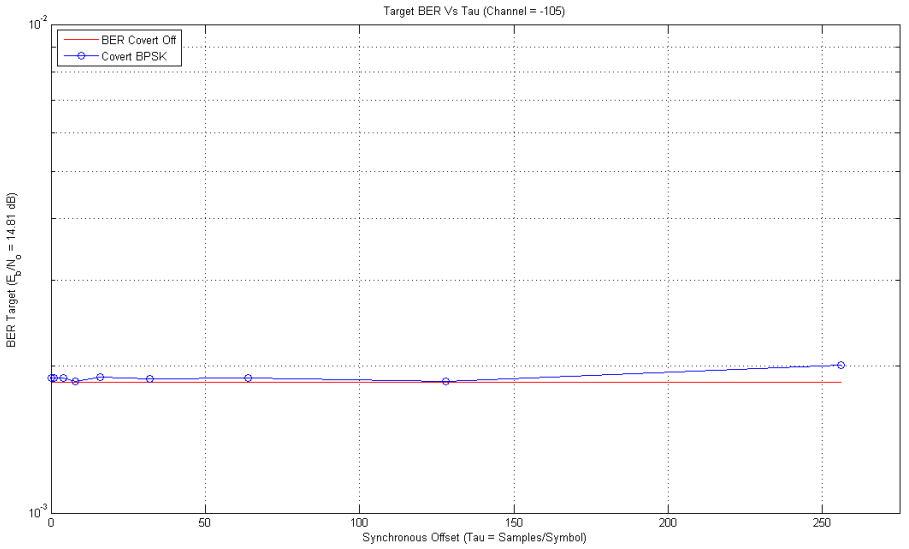


Fig. 4.5. Target system BER vs. synchronous offset for sub-channel -105 ($E_{b,covert}/E_{b,targett}$ = -9.15 dB) [18].

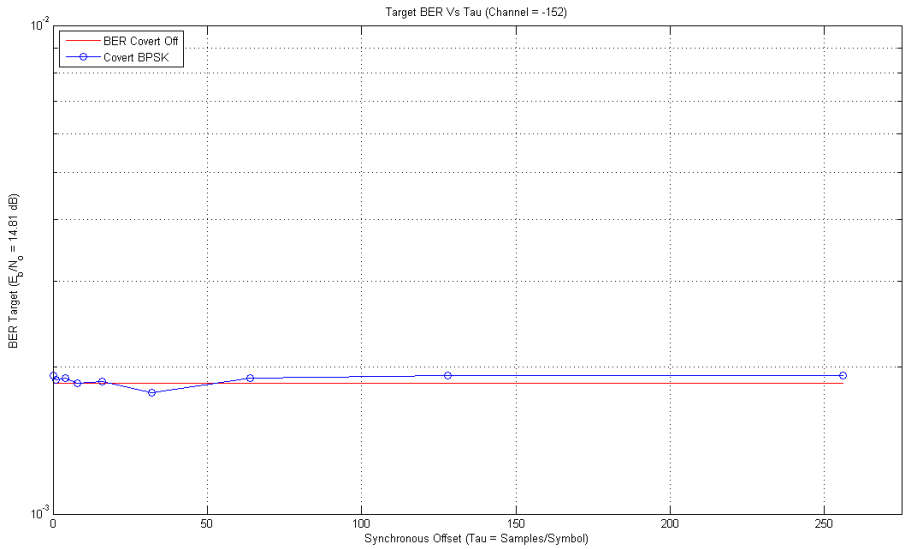


Fig. 4.6. Target system BER vs. synchronous offset for sub-channel -152 ($E_{b,covert}/E_{b,targett}$ = -10.83 dB) [18].

We next examined the communications capability of the covert system. For this part of the study the covert signal was placed in one of the guard band sub-channels designated for the OFDM signal. It was moved from the left most sub-channel (channel no. -256 @ f_c = -3.8325 MHz) until it reached the sub-channel which lies next to the first sub-channel utilized by the OFDM waveform (channel no. -152 @ f_c = -2.2725 MHz). A synchronous offset of 128 symbols/second was used. The rate of the covert transmitter was also varied from 1.85 to 7.40 kb/s. Note that 7.40 kb/s is the maximum rate of the covert system for this scenario and was the maximum allowed bit-rate of the 15 kHz sub-channel when taking into account CP. The rate was then lowered in order to achieve an improved BER for the covert communications system. In Fig. 4.7, we see that the rates of each individual curve,

starting from the top curve, is the full rate (7.4 kbps), half the full rate, one third the full rate, and one quarter the full rate for a bandwidth of 15 kHz respectively.

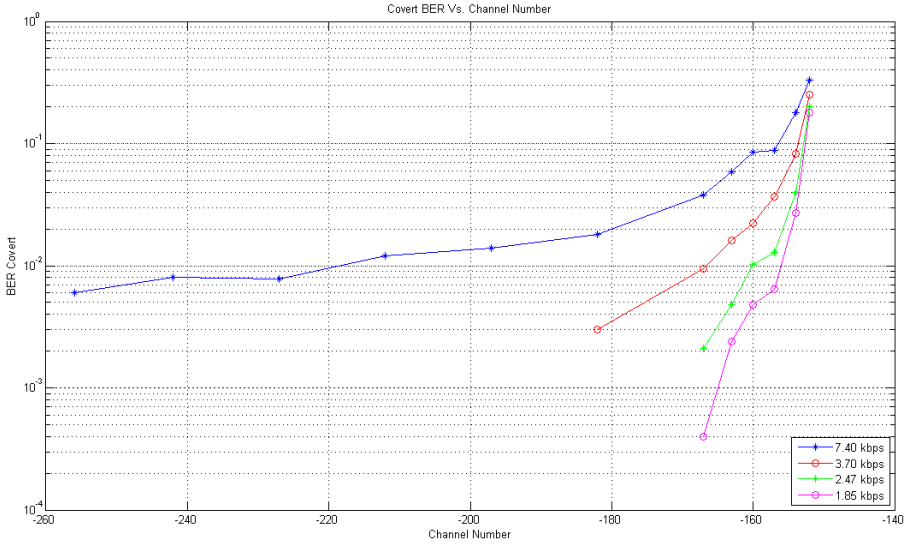


Fig. 4.7. Channel number vs. covert system BER [18].

As expected, when the distance from the utilized sub-carriers of the OFDM signal increases, the BER of the covert system decreases. For example, if an acceptable BER is 10^{-2} and we have a bit rate of 1.85 kbps, then the covert can reside as close as sub-channel -157. If our rate is 2.47 kbps, then we need to be as far out as channel -160. It is also worth noting that the lower the channel number, the further in the spectrum the covert signal is from the non-covert signal while the detectability of the covert communications increases.

Finally, we examined the effect of synchronous offset on the covert system BER. Using the first sample as a reference out of the *I* samples per symbol for the

covert and target signals, if both are received at the same sample time at the receiver, there is no synchronous offset. If the covert sample is received i samples later, then the synchronous offset (τ) is equal to i.

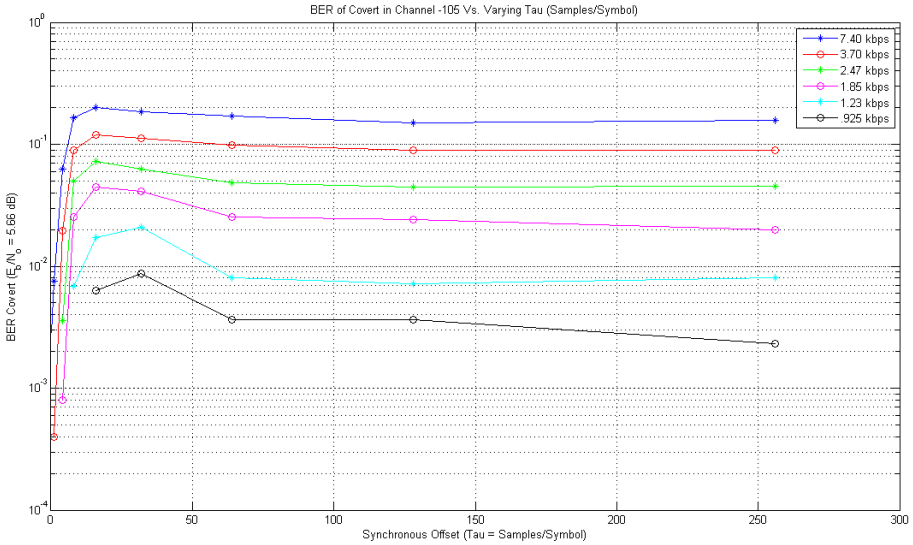


Fig. 4.8. Covert BER vs. synchronous offset for sub-channel -105 ($E_{b,covert}/E_{b,target}$ = -9.15 dB) [18].

For Figs. 4.8 and 4.9, we placed the covert in sub-channel number -105 and -152, respectively. It was assumed that the covert transmitter had knowledge of the non-utilized sub-channels. The BER increases for the covert with loss of orthogonality ($\tau > 0$).

iii. Conclusions

It was concluded that by inserting the covert signal in one of the unused sub-channels of the OFDM channel, the signal is potentially hidden or difficult to detect by the target network. In order to remain undetected, the covert signal must have little to no effect on the OFDM signal. This work demonstrates the potential and feasibility of the concept with respect to the impact in the target OFDM down-link.

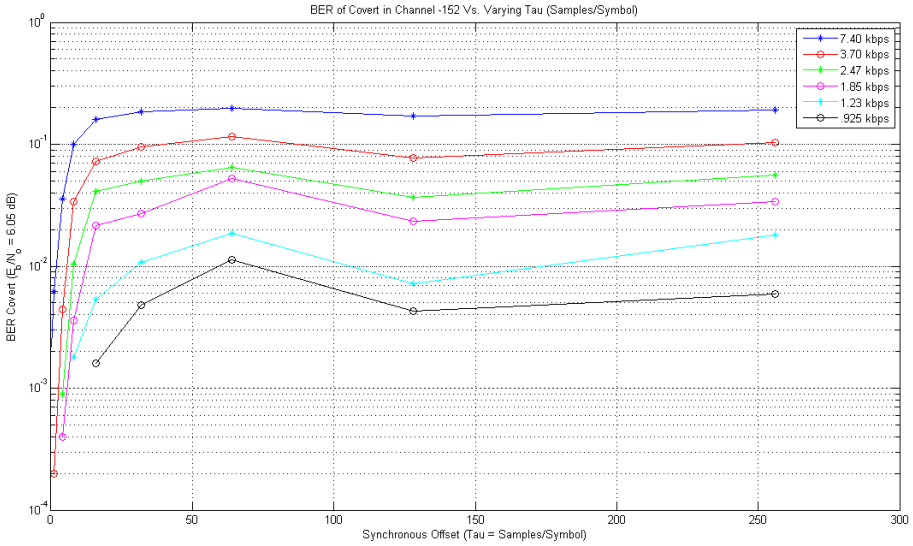


Fig. 4.9. Covert BER vs. synchronous offset for sub-channel -152 ($E_{b,covert}/E_{b,target}$ = -8.76 dB) [18].

B. Probability Density Function of Received SNR with Interference

In this section we calculate the average PER and packet outage probability when the target and interfering signals experience Nakagami-*m* fading with different channel parameters. The PER for an M-QAM convolutionally coded system is

considered. The approach required the development of the pdf for the signal to interference plus noise ratio (SINR). A separate pdf is developed given the target and interfering signal have the same *m* fading parameter, target and interfering signals have different integer *m* fading parameter and different non-integer *m* fading parameter.

i. Introduction

A commonly used approximation for the PER for M-QAM convolutionally coded communication links is based on curve fitting the exact expression for PER [24-27]

$$G(\gamma) \approx \begin{cases} 1, & if\ 0 < \gamma < \gamma_p, \\ ae^{-g\gamma}, & if\ \gamma \geq \gamma_p, \end{cases} \tag{4}$$

where γ is the instantaneous SNR, γ_p, a, and g are the fitting parameters. Values for these parameters for 1080 bits/packet are found in [24-27]. The average PER is then

$$PER(\bar{\gamma}, \bar{\gamma}_c, m, m_c) = \int_0^\infty G(\gamma) f_\gamma(\gamma; \bar{\gamma}, \bar{\gamma}_c, m, m_c)\, \mathrm{d}\gamma \tag{5}$$

where $f_\gamma(\gamma; \bar{\gamma}, \bar{\gamma}_c, m, m_c)$ is the pdf of the instantaneous SINR, $\bar{\gamma}$ = average SNR of the target link, $\bar{\gamma}_c$= average SNR of the interfering link, *m* and m_c are the Nakagami fading parameters for the target and interfering channels respectively. The function represented in (4) provides the basis for determining the SNR thresholds $\gamma_0, \gamma_1, \ldots \gamma_N$ used in AMC schemes to select the transmission mode, i.e., *n* and coding rate which will be addressed in more detail later. If the instantaneous SNR is between γ_0 and γ_1 the channel is in a deep fade and no packets are transmitted. Thus a packet outage

probability is defined here as

$$P_{out} = \int_0^{\gamma_1} f_\gamma(\gamma, \bar{\gamma}, \bar{\gamma}_c, m, m_c) d\gamma. \quad (6)$$

Here we derive the pdf $f_\gamma(\gamma; \bar{\gamma}, \bar{\gamma}_c, m, m_c)$ which is then applied to finding the average PER and P_{out} in the presence of interference.

ii. Background

Much work has been done on determining the system performance for fading channels [34]. A closed form solution for the BER of M-QAM when the target and interfering signals experience Nakagami-*m* fading with different channel parameters is given in [35] . However, the approach given in [35] does not use the pdf of the instantaneous SINR and cannot be applied to the case with coding and hence to finding the PER. The BER for communications links in interference limited scenarios is given in [16] and [36] while the interference plus noise scenario is considered in [37]. These reported BER results do not directly calculate the system performance using the pdf for the instantaneous SINR. Outage probability for fading systems is commonly defined [34] as "when either the carrier-to-interference ratio (CIR) or the carrier-to-noise ratio (CNR) is less than its respective predetermined threshold value". Given this definition [34] the outage probability for interference limited scenarios is reported in [38] and [39] , and interference plus noise limited scenarios in [40] and [16]. However, the outage probability definition in [34] is different than the packet outage probability for AMC systems considered here as given in (6).

The above mentioned works use methods that find the quantities of interest

(BER and P_{out}) without considering interference, i.e., the covert link. Here we first find the pdf of the SINR and then directly calculate average PER and P_{out} with interference.

The central approximation made in finding this solution lies in modeling the in-band interference as additional AWGN with an equivalent power. Similar assumptions are used in the analysis given in [22, 37, 41, 42] . In [37] only a Rayleigh interference channel is considered.

iii. Channel Modelling

The pdf of a signal's instantaneous SNR in Nakagami-*m* fading is well known and given as [34]

$$f_\gamma(\gamma) = \frac{m^m \gamma^{m-1} e^{-\frac{m\gamma}{\bar{\gamma}}}}{\bar{\gamma}^m \Gamma(m)}. \tag{7}$$

With interference the received SINR at the receiver is modeled by

$$\gamma = \frac{\alpha^2 E_s}{N_o + \beta^2 P_c}, \tag{8}$$

where E_s is the average transmitted symbol energy, N_0 is the noise power, and P_c is the amount of power from the interfering signal in the bandwidth of the target system which is modeled as white Gaussian noise. The random variables α and β represent the channel gain due to Nakagami fading for the target and interfering signals, respectively. The power from the interfering signal that exists in the pass-band of target signal's receiver is needed in this analysis. It is assumed here that the impact of the interference on the target link can be found through modeling the interference as

white Gaussian noise with an equivalent amount of interference power as was used in [22, 33, 37]. This model is general and can be applied to a wide range of interference including co-channel, adjacent channel, and intentional interference conditions.

iv. Probability Density Function of SINR

After some rearranging, (3) becomes

$$\gamma = \frac{\left(\frac{E_S}{N_O}\right)\alpha^2}{1+\left(\frac{P_C}{N_O}\right)\beta^2} = \frac{\bar{\gamma}*W}{1+\bar{\gamma}_c*R}, \tag{9}$$

where $\bar{\gamma}_c = \frac{P_c}{N_o}$ is the interference-to-noise ratio. For Nakagami-*m* fading with this normalization, *W* and *R* are unit mean gamma random variables with parameters *m* and m_c, respectively.

Finding the pdf of γ requires deriving the distribution of the quotient of two random variables [43] . Now let

$$\gamma = \frac{U}{V}, \tag{10}$$

with

$$U = \bar{\gamma}\, W \quad U > 0 \;\; and \; V = 1 + \bar{\gamma}_c R \quad V > 1.$$

Now

$$f_U(u) = \frac{f_W\left(\frac{u}{\bar{\gamma}}\right)}{\bar{\gamma}} \text{ and } f_V(v) = \frac{f_R\left(\frac{v}{\bar{\gamma}_c}-\frac{1}{\bar{\gamma}_c}\right)}{\bar{\gamma}_c}.$$

Using the quotient distribution of two random variables, the pdf of the instantaneous SINR at the desired receiver is given by (11). The function ${}_1F_1(\mathrm{a}; b; z)$ is the confluent hypergeometric function. However, when *b* is a negative integer,

${}_1F_1(\mathrm{a};b;z)$ is undefined (also $\Gamma(-m)$ is unbounded for integer m) [44] . Therefore, $f_\gamma(\gamma;\ \bar{\gamma},\bar{\gamma}_c,m,m_c)$ given in (12) is not defined when m and m_c are simultaneously integers. For the integer m and m_c case the above integral is solved separately with the resulting pdf given by (13). Solving this integral when $m_c = m$ yields a pdf for the instantaneous SINR, where K_k is the modified Bessel function of the second kind [45] and is given by (8).

$$f_\gamma(\gamma;\ \bar{\gamma},\bar{\gamma}_c,m,m_c) = \int_1^\infty v f_V(v) f_U(v\gamma)\, dv =$$

$$\left(\frac{m^m}{\Gamma(m)}\frac{\gamma^{m-1}}{\bar{\gamma}^m}\frac{{m_c}^{m_c} e^{\frac{m_c}{\bar{\gamma}_c}}\left(\frac{1}{\bar{\gamma}_c}\right)^{m_c}}{\Gamma(m_c)}\right)\left(\Gamma(m+m_c)\left(\frac{m_c}{\bar{\gamma}_c}+\frac{\gamma m}{\bar{\gamma}}\right)^{-m_c-m}{}_1F_1\left(1-m_c;-m-m_c+1;-\frac{m\gamma}{\bar{\gamma}}-\frac{m_c}{\bar{\gamma}_c}\right)+\frac{1}{\Gamma(-m)}\Gamma(-m-m_c)\Gamma(m_c)\,{}_1F_1\left(m+1;m+m_c+1;-\frac{m\gamma}{\bar{\gamma}}-\frac{m_c}{\bar{\gamma}_c}\right)\right) \tag{11}$$

$$\left(\frac{m^m {m_c}^{m_c} e^{\frac{-m*\gamma}{\bar{\gamma}}}\gamma^{m-1}\bar{\gamma}^{m_c}\bar{\gamma}_c{}^m}{(m-1)!(m_c\bar{\gamma}+m\gamma*\bar{\gamma}_c)^{m+m_c}}\right)\left(\sum_{n=0}^{m}\left(\frac{m!}{n!(m-n)!}\right)\left(\frac{(m_c+m-n-1)!}{(m_c-1)!}\right)\left(\frac{(m_c\bar{\gamma}+m\gamma\bar{\gamma}_c)^n}{(\bar{\gamma}\bar{\gamma}_c)^n}\right)\right) \tag{12}$$

$$f_\gamma(\gamma;\ \bar{\gamma},\bar{\gamma}_c,m) = \frac{1}{2\sqrt{\pi}\gamma\,\Gamma(m)} m^{2m}\left(\frac{1}{\bar{\gamma}_c}\right)^m\left(\frac{\gamma}{\bar{\gamma}}\right)^m e^{\frac{m(\bar{\gamma}-\bar{\gamma}_c\gamma)}{2\bar{\gamma}\,\bar{\gamma}_c}}$$

$$\left(m\left(\frac{\gamma}{\bar{\gamma}}+\frac{1}{\bar{\gamma}_c}\right)\right)^{\frac{1}{2}-m}\left(K_{\frac{1}{2}-m}\left(\frac{m(\bar{\gamma}+\bar{\gamma}_c\gamma)}{2\bar{\gamma}\,\bar{\gamma}_c}\right)+K_{-m-\frac{1}{2}}\left(\frac{m(\bar{\gamma}+\bar{\gamma}_c\gamma)}{2\bar{\gamma}\bar{\gamma}_c}\right)\right) \tag{13}$$

A form of (11), (12), and (13) is found in [33]. Fig. 4.10 shows the pdf and Fig. 4.11 the cumulative distribution function for the SINR. As the channel parameter m surpasses 1, the characteristic shape of the pdf for the SINR changes.

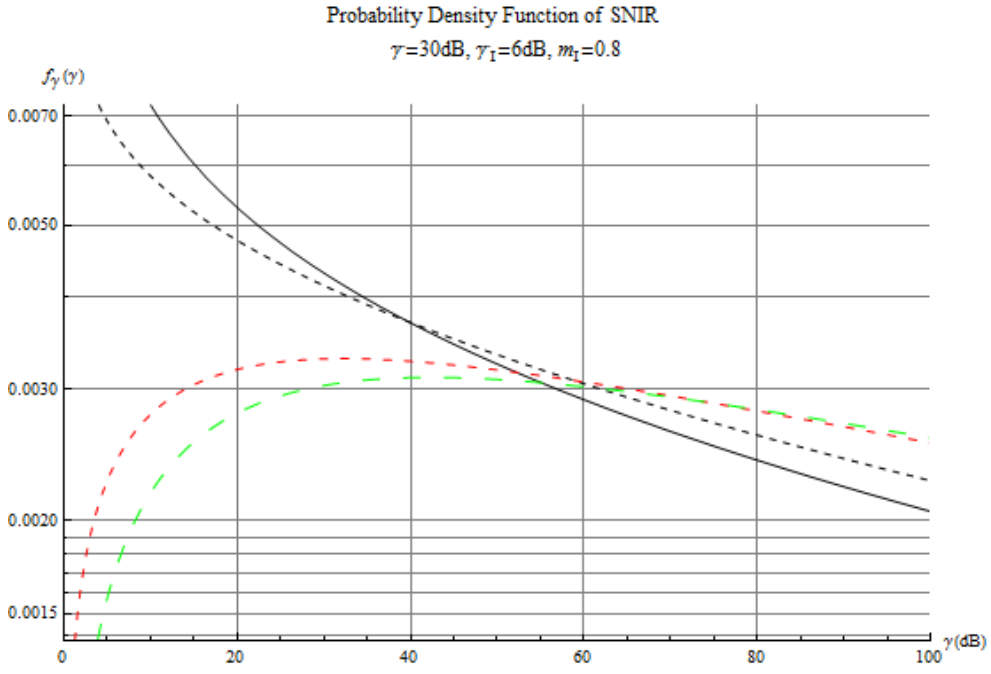


Fig. 4.10. PDF of SINR $\bar{\gamma}$=30 dB, $\bar{\gamma}_c$=6 dB, m_c =0.8.

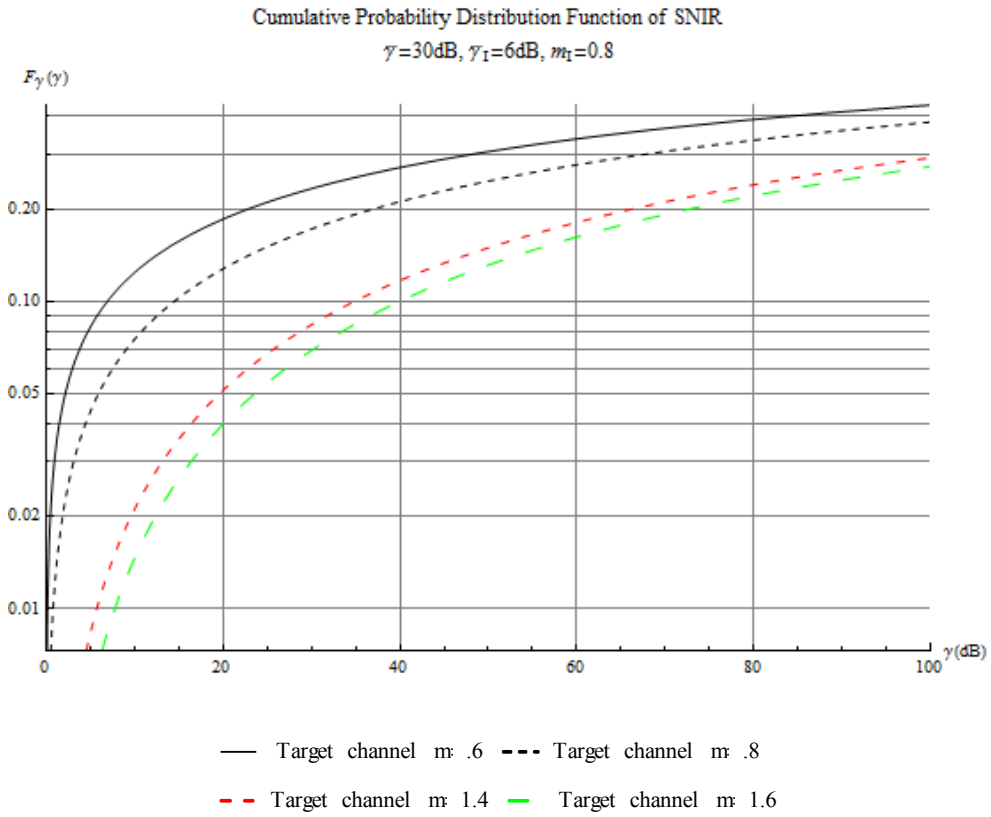


Fig. 4.11. CDF of SINR $\bar{\gamma}$=30 dB, $\bar{\gamma}_c$=6 dB, m_c =0.8.

v. System Performance

Fig. 4.12 shows the average PER versus the target system SNR for rate ½ convolutionally coded 4-QAM system with 1080 bits per packet and an interference power of 5 dB, from [25] a=90.2514, g=3.4998, and γ_p=1.0942. The Nakagami fading parameter for the target and interfering channels is shown in the legend of Fig. 4.12. As expected, the PER of the target system decreases as the m fading parameter of the target system increases.

Fig. 4.13 shows that for a fixed m_c, as the m parameter of the target system

increases the P_{out} decreases as expected. We now define another metric for measuring the impact of the fading parameter on the performance of the target system.

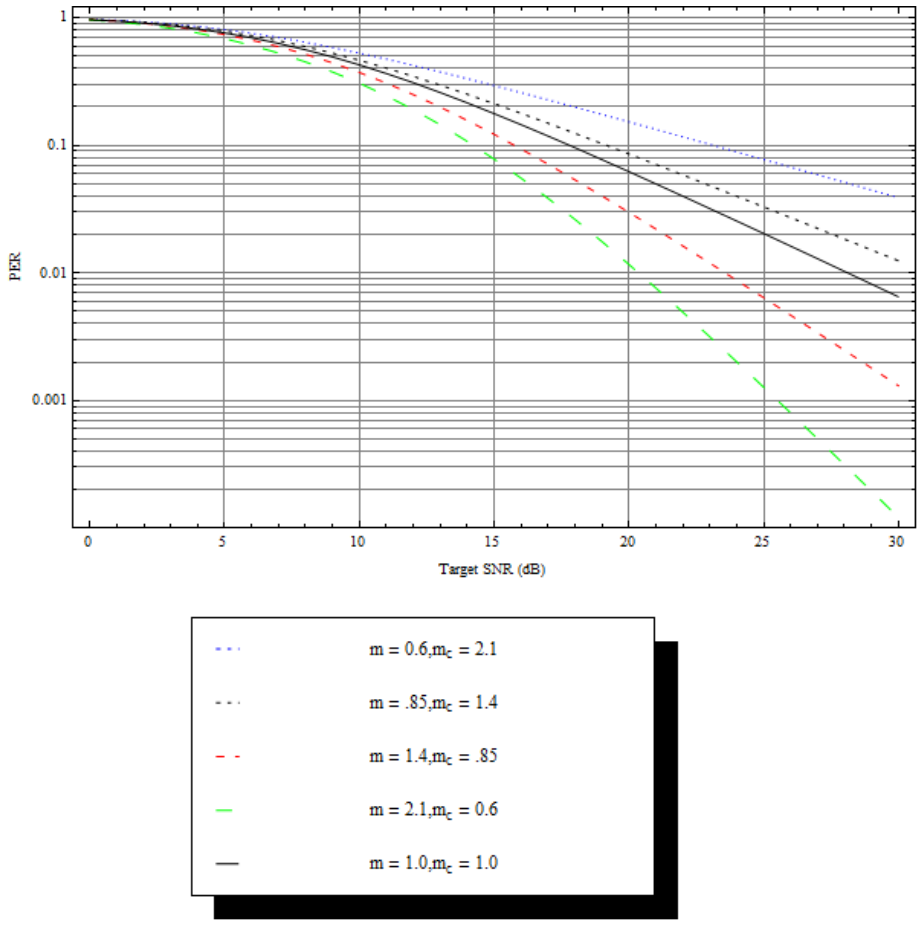


Fig. 4.12. Average PER of target system with $\bar{\gamma}_c$==5dB.

$$P_{out,Relative}(m_c; \bar{\gamma}, \bar{\gamma}_c, m) = \frac{P_{out}(\bar{\gamma},\bar{\gamma}_c,m,m_c)}{P_{out}(\bar{\gamma},\bar{\gamma}_c,m,m)}. \quad (14)$$

$P_{out,Relative}$ is shown in Fig. 4.14. For fixed interference power, the interfering channel fading parameter can have a degrading influence (here over 60%) on the target system P_{out}. The different shape of the performance characteristics for the m<1 and m>1

cases follows from the nature of $f_\gamma(\gamma)$ shown in Fig. 4.10.

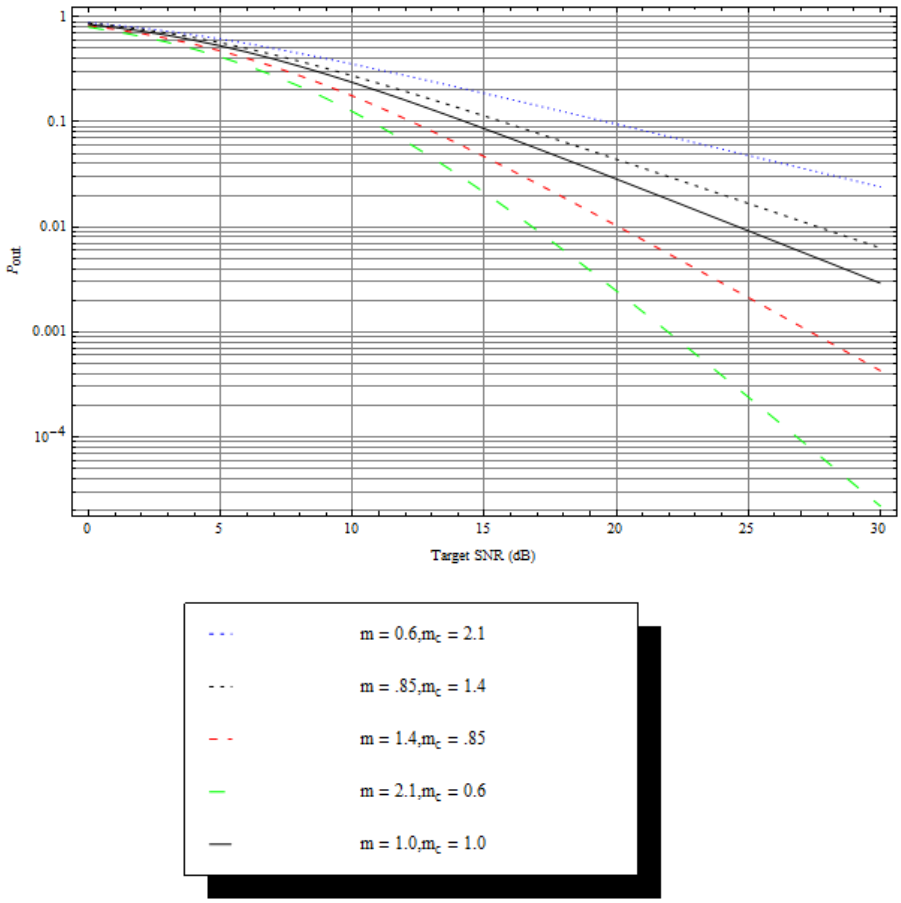


Fig. 4.13. P_{out} for $\bar{\gamma}_c$==5dB.

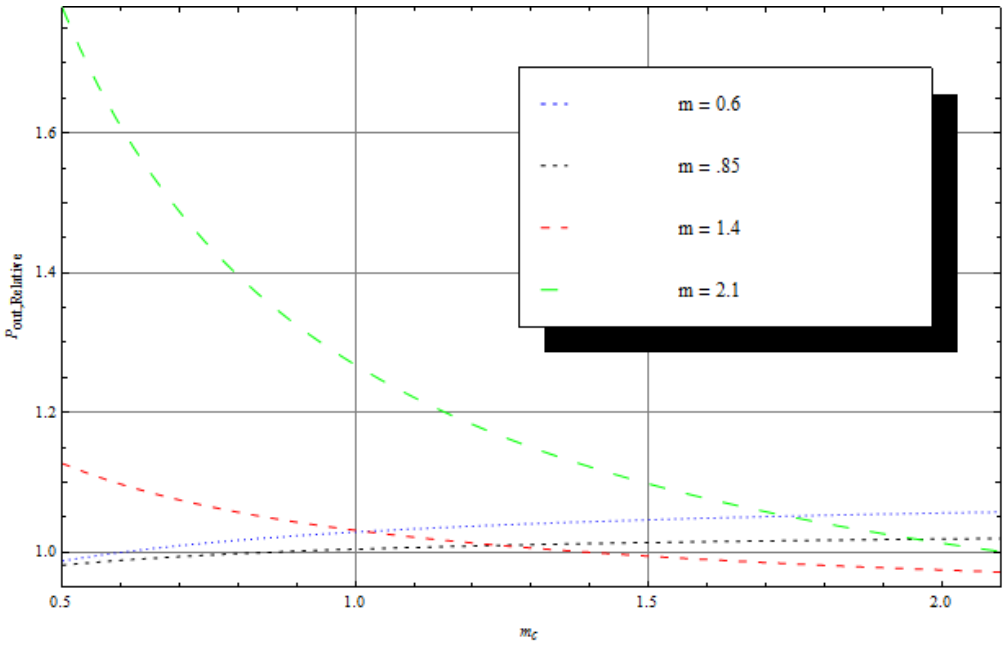


Fig. 4.14. P_{out} for $\bar{\gamma}_c$==5dB.

vi. Conclusions

Probability density functions are derived for the instantaneous received SINR when the target and interfering signals are transmitted through Nakagami-*m* channels with different fading parameters. The derived pdfs were used to calculate the average PER and P_{out}. This work shows that the performance of the target link is influenced by changes in the interference channel characteristics. Also, the shape of the pdf of the SINR fundamentally changes as *m* crosses the boundary of *m*=1.

C. Predicting the Impact of a Covert Link on the BER of an OFDM System with Adaptive Modulation and Coding

This section quantifies the performance trade-offs for an OFDM system with

interference from a covert transmitter. Knowledge of these system trade-offs is next step toward evaluating the potential of covert communication within the RF environment created by packet-based broadband wireless (infrastructure) networks, like LTE. Adaptivity is integral to broadband wireless network protocols and makes them vulnerable to exploitation. The contribution of this section is the prediction of the BER of an OFDM with a covert interferer in Nakagami-*m* fading; the performance of the covert interferer is also derived. The analytic model is used to show trade-offs between the OFDM system and covert link performance. These results extend the proof of concept simulation where fading was not considered.

i. Introduction

This section takes the first step in the process of learning the performance impact on an infrastructure network using OFDM and AMC by quantifying the physical layer performance trade-offs for an OFDM system with interference from a covert transmitter. While there has been much work done on the impact of interference on OFDM systems, here we focus on the special case of physical layer performance trade-offs between the OFDM system and covert transmitter.

In [18] we used simulation to predict the physical layer performance of the covert link as well as the target OFDM infrastructure system. The BER of the target system as a function of the covert's power, bandwidth and spectral location was presented. The BER of the covert link was also shown as a function of its spectral location. The contributions presented here are the analytic prediction of the covert link BER as well as the target OFDM infrastructure system BER performance in the

presence of Nakagami-*m* fading and evaluation of the associated system trade-offs. Here, we examine the impact of the interference from the covert link on the physical layer of the target system through the BER while later we will address the AMC and HARQ aspects.

ii. Assumptions

As in [18] there are two sets of transmitters/receivers; a transmitter and receiver for the target communication system and a transmitter and receiver for the covert communication link. There are four channels that must be represented in the model as shown in Fig. 4.1. Here we assume Nakagami-*m* fading for all the channels with a common Nakagami-*m* fading parameter of *m* and flat fading. At 900 MHz measurements were reported in [46] of channel characteristics in an urban environment where the most likely values of *m* ranged from 0.5 to 3.5 with an average of m =1.56. While at 870.9 MHz in an urban environment in [47] an *m* = 2.38 was reported. Here *m* = 0.5, 1 (Rayleigh fading), 1.56, and 2.38 are used in the tradeoff analysis.

The analysis presented here can be used for any modulation format, however, for the tradeoff analysis presented here the target OFDM signals uses 16-QAM with rectangular pulse shaping. The covert link uses BPSK or QPSK. Un-coded transmission is assumed; the results presented here will be the basis for the work that will include coding, adaptive modulation as well as HARQ which is discussed in Chapter 5. Optimum receiver structures are utilized; perfect CSI for each transmitter/receiver pair and ideal phase and frequency synchronization is assumed.

While the analysis framework developed here is more general, for this section we assume that the covert signal is placed in frequency in the guard band adjacent to the target OFDM signal. The target OFDM and covert systems are not in synchronization; thus the covert and target signals are not orthogonal. To facilitate the analysis it is assumed that the interference generated by the undesired signal (the covert signal in the case of the target receiver and the target signal in the case of the covert receiver) can be modeled by white Gaussian noise with a noise power equal to the in-band interference power. A similar approach was used in [33] and [34], while in [35] a general approach to finding the BER is presented. We define in-band power as the power within the zero-to-zero crossings of the signal spectrum, here a $\sim sinc^2(f/\mathrm{BW})$. The impact of modeling the interfering signal as white noise for this environment is discussed later. While in the analysis presented here the covert signal is placed in the guard band of the OFDM system, the approach is more general and can be applied to other covert waveforms, e.g., time or frequency hopping where the LPD performance for the covert link can be improved.

iii. Performance Analysis of Target System and Covert Link

The development of the pdf of the received SNR with interference while both target and interfering signals are subject to independent Nakagami-*m* fading was developed in the previous section. The BER for M-QAM given an SNR of γ is needed to calculate the average BER. Here we use eq. (8-15) from [45] that improves the prediction for both low and high SNR regimes defined as

$$BER(\gamma) = \frac{4(\sqrt{M}-1)\sum_{i=0}^{\frac{\sqrt{M}}{2}-1} Q\left((2i+1)\sqrt{\frac{3\gamma}{M-1}}\right)}{\sqrt{M}log_2(M)}, \quad (14)$$

where $Q(\cdot)$ is the tail probability of the standard normal Q-function and M is the number of constellation point in M-QAM signaling. Now the BER can be found from [48]

$$BER = \int_0^\infty BER(\gamma) f_\gamma(\gamma)\, d\gamma. \quad (15)$$

Here the BER is found by numerical integration. Fig. 4.15 shows the BER performance of a 16-QAM link as a function of its SNR with a small covert link power (SNR_{Covert} = -6 dB) under three channel conditions, m = 0.75, 1.25 and 1.75. The performance shown in Fig. 4.15 compares favorably to the BER without interference given in [46] for m = 0.75, 1.25 and 1.75 and 16-QAM modulation. As expected, the performance improves as m increases. Fig. 4.16 shows the performance for a 6 dB SNR_{Covert}.

Consider the case shown in Fig. 4.17 where only three OFDM subcarriers (-1, 0, 1) are shown. Each subcarrier has a normalized power of 1 and bandwidth of 2; the covert is operating at 1/2 of the bit rate of each sub-carrier and has a normalized power of 0.1. Here the bandwidth of the covert is 1. Note the covert signal will impact each subcarrier differently. In this figure the covert signal is 10 dB below the target, however we will show later that the covert link can operate at ~21 dB below the OFDM sub-carrier power. For the sub-carrier i = 1 the normalized in-band interference power is

$$\rho_1 = \int_0^2 sinc^2(\pi(f-2))\, df, \tag{16}$$

and in this case $N_I = .1\ \rho_1$. Then to calculate the BER in general for each subcarrier, i, a different normalization factor is needed and can be found by

$$\rho_i = \frac{1}{B_c} \int_{f_i - \frac{f_S}{2}}^{f_i + \frac{f_S}{2}} sinc^2\left(\pi \frac{f - k f_S}{B_c}\right) df, \tag{17}$$

where f_S is the subcarrier spacing (in this case f_s = 1) and B_c is the bandwidth of the covert signal. With a covert signal power of P_c the in-band interference for sub-carrier i is $N_i = \rho_i\ P_c$. The BER for the i^{th} subcarrier is defined as BER_i and can be found using (15) with $N_I = N_i = \rho_i\ P_c$. Note each sub-carrier can have a different modulation and bit rate (bits/s), r_i. With r_i = bit rate, when the AMC is in mode i, the total BER for the target OFDM system is given by

$$BER = \frac{\sum_{k=-N}^{N} r_i \mathrm{BER}_i}{\sum_{k=-N}^{N} r_i}. \tag{18}$$

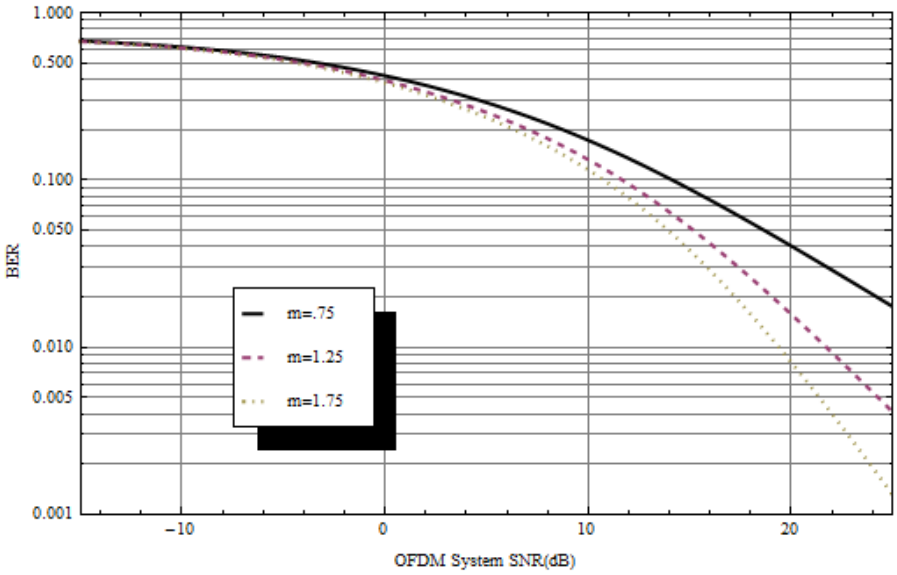


Fig. 4.15. 16-QAM link with Nakagami-*m* fading: *m* = .75, 1.25, 1.75 and interference: SNR_{Covert} = -6 dB.

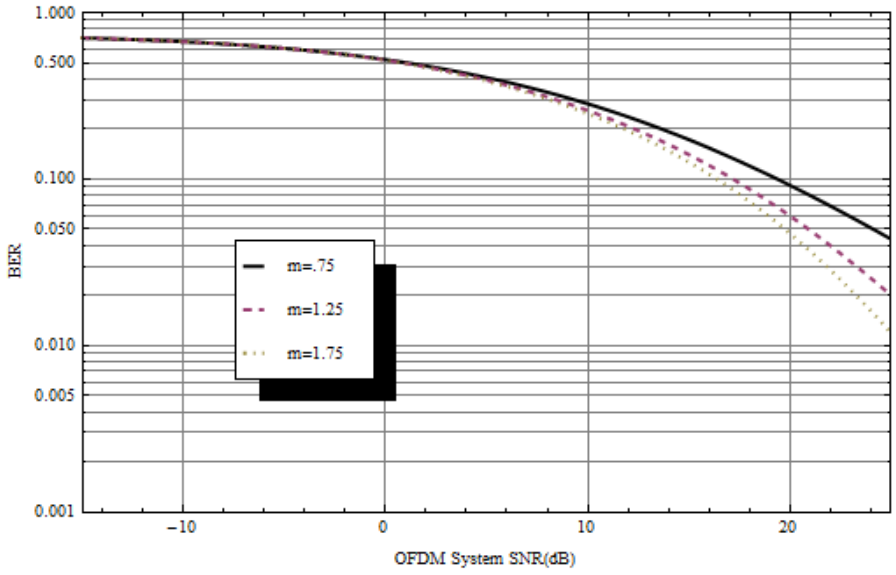


Fig. 4.16. 16-QAM link with Nakagami-*m* fading: *m* = .75, 1.25, 1.75 and interference: SNR_{Covert} = 6 dB.

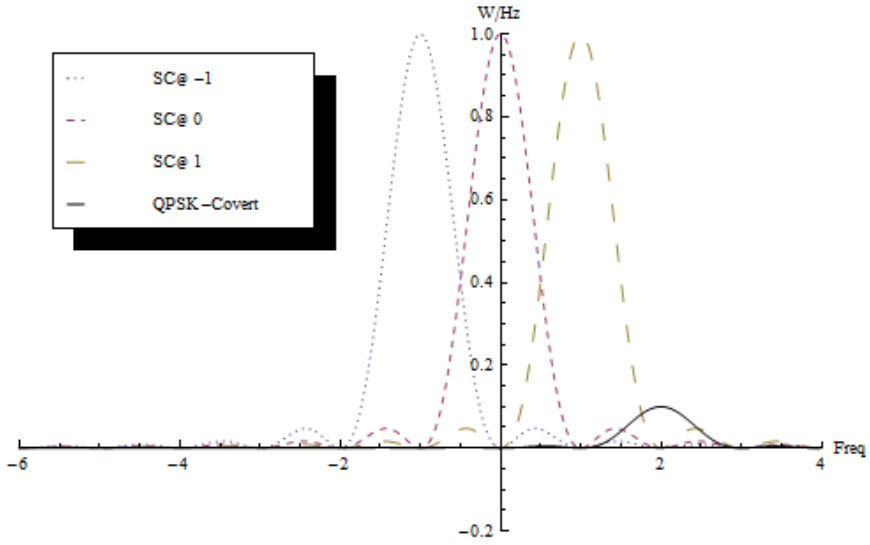


Fig. 4.17. PSD of target OFDM system and covert link.

However, for the cases of interest the covert signal will impact only a few adjacent sub-carriers.

Again referring to Fig. 4.17, the total interference the covert receiver sees is

$$N_T = \int_2^3 (sinc[\pi * (f+1)]^2 + sinc[\pi * f]^2 + sinc[\pi * (f-1)]^2)\, df. \quad (19)$$

In general

$$N_T = \sum_{k=1}^{N} \frac{P_i}{f_s} \int_{f_{sc}-\frac{B_c}{2}}^{f_{sc}+\frac{B_c}{2}} sinc^2\left(\pi \frac{f-if_s}{f_s}\right) df, \quad (20)$$

where P_i is the power in the i^{th} sub-carrier and f_{sc} is the center frequency of the covert signal. The BER of the covert link can be found utilizing (15) with $N_I = N_T$. Again, for cases of interest only the first few sub-carriers of the OFDM system will be considered in impacting the covert link.

The outage probability, P_{out}, of the target system is defined as the probability

the SNR will fall below a BER constraint. We set the threshold, γ_T, equal to the SNR that results in a BER of 10^{-2}. We find this threshold using (14). The outage probability is then given by

$$P_{out} = \int_0^{\gamma_T} f_\gamma(\gamma) d\gamma. \quad (21)$$

iv. Model Validation

This section quantifies the impact of modeling the interfering signal as white noise with a noise equivalent to the in-band interference power. Parameters are selected and the BER of the OFDM target system and covert link is calculated utilizing (14) through (20). These same parameters are utilized in simulation. The covert link is placed in the guard band of the OFDM signal. Here we only take into account the impact of the first three OFDM sub-carriers on the covert link and the impact of the covert link on the first three OFDM sub-carriers. This is due to the fact that the impact of the systems on one another is significantly reduced as the distance in the spectrum increases.

The OFDM system utilizes 16-QAM. Rayleigh fading (m = 1) and additive white Gaussian noise (AWGN) are assumed. The SNR for the OFDM sub-carriers is varied from -15 to 27 dB. The covert link utilizes QPSK signaling. Both systems are un-coded.

Fig. 4.18 compares the analytic results to the simulated results for a covert link SNR of 0, 10, and 20 dB. An analytic curve is included for when no covert is present as a baseline comparison. The simulated curves follow the analytic curves. It

is to be noted that the analytic curves are more conservative than the simulated ones at all points. This means we can expect better performance than predicted by the analysis.

Fig. 4.19 compares analytic results to simulated results for the target OFDM system and covert link. Here we can see the tradeoff in performance of the OFDM system for covert system as the covert link SNR increases. The performance of both predicted by the analysis is an adequate and a conservative estimate.

The difference between the simulated and analytic results shows that white noise can be used to approximate the impact of in-band power of interference power. It also shows that this estimate conservatively predicts the associated performance.

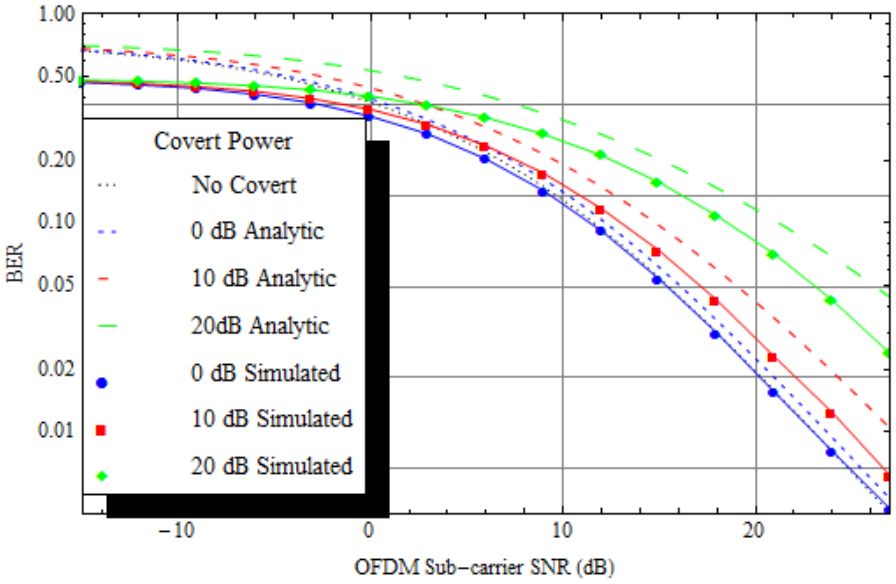


Fig. 4.18. 16-QAM OFDM system with QPSK covert link.

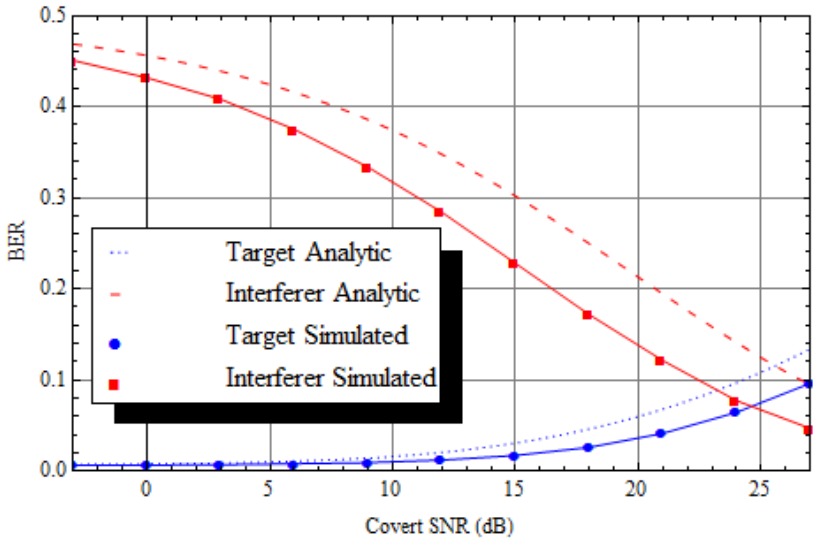


Fig. 4.19. Performance of OFDM system and covert link with SNR of the OFDM link = 25 dB.

v. System Performance Tradeoffs

As the SNR of the covert increases the negative impact on the OFDM system increases but the performance of the covert link improves; this section explores this trade-off. A goal of this trade-off analysis is to determine an operating point for the covert link, that is, its data rate, $r_{bc,}$ and transmit power such that the impact on the OFDM system is "small". With fixed power, as the data rate decreases the covert link performance increases. There is negligible change in impact on sub-carrier *i* of the OFDM system when the modulation of the covert link is changed. In these results the OFDM system uses 16-QAM on each sub-carrier and the SNR was set such that the BER= $5x10^{-3}$ in Rayleigh fading with no interference. Therefore, when the covert system uses QPSK, its data rate is ½ the data rate per sub-carrier in the OFDM

system. When BPSK, with the same symbol time as the 16-QAM OFDM sub-carrier is utilized, the covert data rate is ¼ the rate of an OFDM sub-carrier. For a sub-carrier bandwidth of 15 kHz with 16-QAM the data rate is 30 kb/s and with BPSK the covert link has a data rate of 7.5 kb/s. The data rate of the covert link can be further reduced by increasing its symbol time; this improves its BER performance while not increasing its influence on the target OFDM system. Let r_b be the OFDM per sub-carrier bit rate. Figs. 4.20 and 4.21 show the system trade-off for covert link bit rates, $r_{bc,}$ ranging from $r_b/2$ to $r_b/32$.

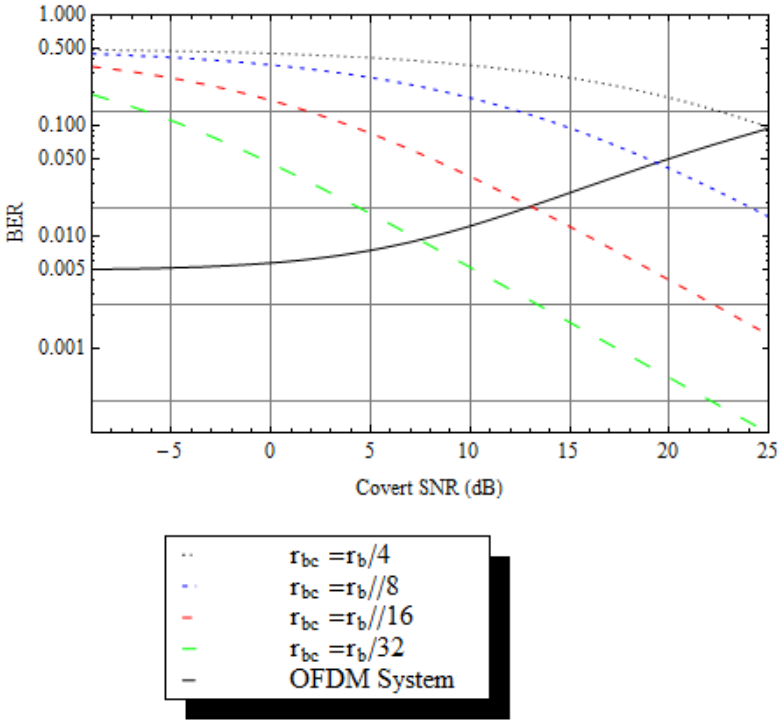


Fig. 4.20. 16-QAM OFDM system with SNR = 26.15 dB and BPSK covert with variable bit rate.

In order to see the impact of changing the channel fading characteristics, Fig. 4.22 shows the trade-off between covert and OFDM system performance for different values of the fading parameter *m*. The symbol rate of the covert link is $1/8^{th}$ of the target OFDM system which results in an overall bit rate for the covert link that is $1/32^{nd}$ of an OFDM sub-carrier. The BER performance improves as the Nakagami-*m* fading parameter increases as expected.

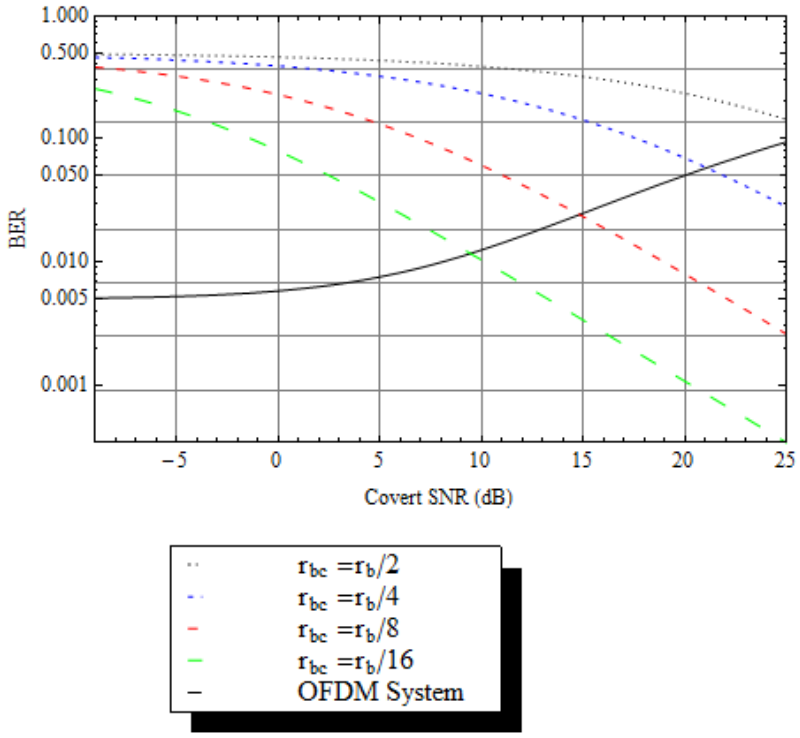


Fig. 4.21. 16-QAM OFDM system with SNR = 26.15 dB and QPSK covert with variable bit rate.

There is a small impact on the OFDM system when the SNR of the covert link operates at approximately 5 dB. The covert link also performs well, achieving a BER $< 10^{-2}$, for $r_{bc} = r_b/32$ operating at 5 dB SNR. Here the covert signal is approximately

21 dB below the OFDM sub-carrier power. It can be seen from Fig. 4.21 that the increase in BER for the OFDM system could easily be attributed to fading. For example, the increase in BER for the OFDM system is greater when the *m* parameter decreases from 2.38 to 1.56 than when covert link is present with a SNR ratio of 5 dB. Fig. 4.23 shows the impact of the interference from the covert link on the target OFDM system outage probability. There also is a knee in the outage probability curves at about 5dB.

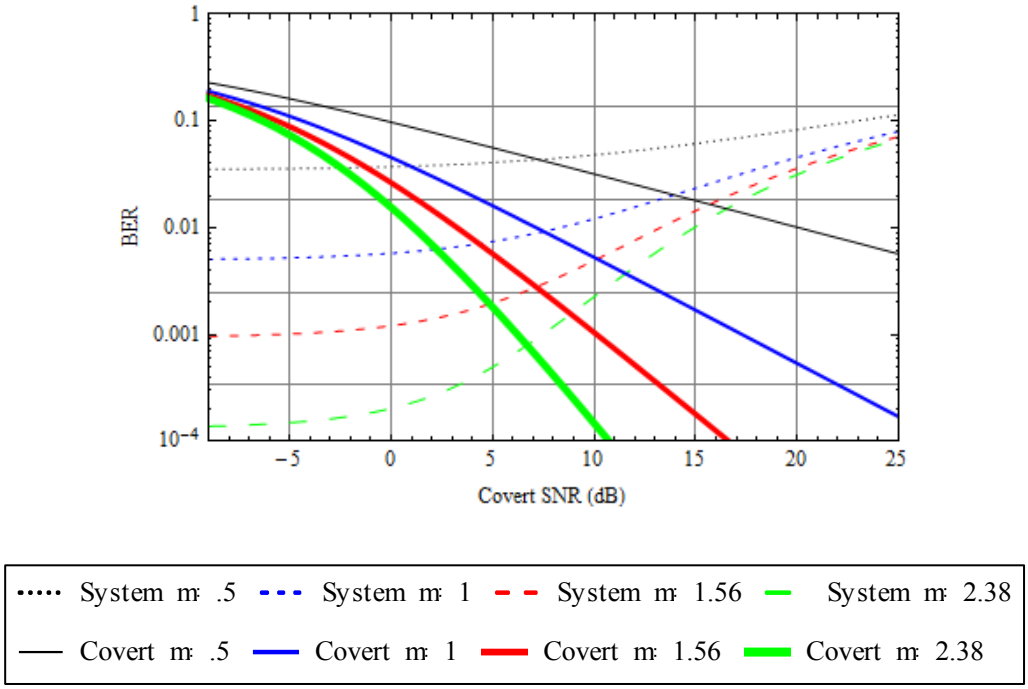


Fig. 4.22. 16-QAM OFDM system with SNR = 26.15 and BPSK covert with variable *m*, $r_{bc} = r_b/32$.

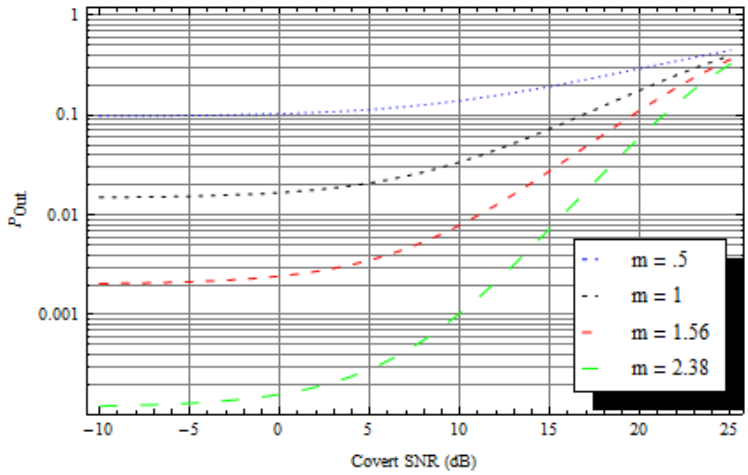


Fig. 4.23. 16-QAM OFDM system with SNR = 26.15 and BPSK covert with variable *m,* $r_{bc} = r_b/32$.

vi. Conclusions

In this section we developed and validated an analytic model that characterizes the interaction between the target OFDM system and the covert link in Nakagami-*m* fading at the physical layer. Specifically, the BER was determined for an OFDM system with a covert interferer as well as the performance of the covert link in Nakagami-*m* fading. The analytic model developed here was used to illustrate trade-offs between the OFDM system and covert link performance under different channel conditions, i.e., different *m*. For the cases discussed here, a covert link utilizing BPSK in Nakagami-*m* fading is feasible. That is, low bit rate communications is possible over the covert link with insignificant degradation caused by the covert link on the infrastructure system; this degradation likely being handled by AMC and HARQ.

Next steps are needed to quantify and demonstrate how AMC and HARQ in the target system effectively conceal this degradation. The probability density function for the instantaneous SNR derived here and given in (13) is a required first step in such an analysis and will play an important role in determining the influence of the covert transmitter. This probability density function (13) used in conjunction with the analysis in [24-27] is needed to determine the packet level effects. In the analysis reported here the covert transmitter is hidden in the guard band.

D. Estimating the Average Packet Error Rate

We propose a method for estimating the average PER of a coded OFDM system when the signal is subject to interference with a shaped spectral density. Thus the interference has a different impact on each sub-carrier. Typically, the PER is a function of the received SNR and the packet bits are distributed evenly amongst a fixed number of sub-carriers where each sub-carrier has the same SNR. The OFDM system under consideration here utilizes convolutional coding for error correction and M-QAM for signaling. The proposed method assumes that each sub-carrier is affected by a different interference power. The novelty in the analysis lies in equating the average interference power affecting each sub-carrier to an equivalent AWGN power. We compare PER prediction using this approach to simulation for a number of MCSs to validate that the proposed approximation can be used to calculate the average PER.

i. Introduction

LTE is a wireless packet based (infrastructure) network technology [49] that has become the prevalent choice in wireless networks and will continue to remain a staple for the foreseeable future. The ability to more accurately predict PER performance of multi-carrier systems could lead to better spectrum and interference management [15]. Therefore, it is of value to develop a method for calculating the average PER when a wireless link is impacted by interference with a shaped spectral density. Previously, simulation was used to find the BER of an uncoded multi-carrier system when subject to a fixed channel [18] and the impact a covert interferer with a shaped spectral density could potentially have on a packet-based broadband wireless network, like LTE. The work here first finds the PER, as a function of SNR, for an OFDM system with 12 sub-carriers like a resource block (RB) in LTE. Knowledge of the PER as a function of SNR for each the MCS is a prerequisite for analyzing the impact of interference. The interaction between the target and interfering signals occurs at the physical layer and the PER analysis developed here provides the basis for performance analysis at higher layers.

Much work has been done studying the effects of interference on the error rates of single carrier systems [33], [35], and [16]. It is well documented that PERs of single carrier systems are different than multi-carrier systems [50]. The work in [24-27] examines the PER of multi-carrier OFDM systems without interference. The work in [51] examines the PER of multi-carrier OFDM systems with fading but does not examine interference.

One of the challenges in finding the average PER is that the interference can

impact each sub-carrier differently, i.e., each sub-carrier can have a different SNR. Therefore, the calculation of the PER in systems with coding is not straightforward due to the fact that the bits of a packet are distributed amongst multiple sub-carriers and the PER for single carrier systems is different for multi-carrier systems [16].

Closed form expressions for PERs of each MCS under consideration here are currently unavailable. Therefore, for the case without interference we utilize simulation to collect data of the PER for a set of SNRs over a RB for each MCS mode; then apply curve fitting to find a functional relationship between PERs and SNR for each MCS similar to [24-27]. However, here we focus on a RB of 12 sub-carriers as in LTE. It is to be noted that all sub-carriers in a RB utilize the same MCS, i.e., mode, based on CSI. Therefore, we present results for each AMC mode. Here we show the average SNR over all sub-carriers in a RB can be used as an approximation to determine the impact of interference generated by a signal with a shaped spectral density. The SNR each sub-carrier experiences is calculated first and then averaged. This average SNR is then used to analytically calculate the average PER for each MCS mode with Nakagami-*m* fading and interference. To validate this approach, we simulate the average PER of each scheme with interference and fading and compare it to the analytic result.

ii. System Configuration

Adaptive mechanisms, such as AMC, allow the communications link the ability to meet a performance target, such as PER, in a changing fading environment while maximizing throughput. AMC achieves this by pairing a specific signal

modulation, M-QAM in this case, with a coding rate that meets or exceeds the PER requirement. The selection of the particular MCS is based upon the SNR at the receiver. The work here considers a system similar to an LTE system. LTE specifies a 12 sub-carrier RB and has 16 AMC modes with turbo codes for error correction [49]. LTE utilizes 4, 16, and 64-QAM signaling. The system considered here (Fig. 4.24) follows [24-27]. However, in this work we utilize a 12 sub-carrier RB, 6 AMC modes, and convolutional codes in order to simplify the analysis. As in [24-27] the work here considers coding rates of ½, 9/16, and ¾. The number of bits per packet is 1080 and is distributed evenly amongst the 12 sub-carriers that comprise the RB. No bits are sent when the received SNR falls below the minimum SNR threshold for mode 1, $\gamma < \gamma_1$. The convolutional encoder, with generator polynomials $g_1 = 133$ and $g_2 = 171$, is terminated at the zero state by appending six zeros to the uncoded packet bits. Hard decision decoding is used at the Viterbi decoder. The puncture pattern for the rate ½, 9/16, and ¾, respectively, are [1 1], [1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1 0 1], and [1 1 1 0 0 1].

iii. Simulation of Packet Error Rates

The PER, as a function of SNR, is utilized to find the expected value of the PER when the system is subject to fading and interference for each MCS. A closed form expression for the PER of each of the MCS in the proposed system is not available. Similarly, work in [51] finds the PER functions for convolutionally coded OFDM-based WLANs in fading and finds, through analysis, the average PER with and without fading. The work in [24] finds the PER functions of HiperLAN systems

which are then utilized to find the average PER of a single carrier system when AMC and fading is considered.

Here we utilize simulation to collect data of the PER for a set of SNRs over a RB for each MCS and then curve fitting is applied to find a functional expression relating PER to SNR as in [24]. The simulation results from these simulations are then used to predict the average PER of the multi-carrier RB. The results given in Fig. 4.25, denoted by a star, were obtained by processing 10,000 packets at each SNR. The least squares method was utilized to fit the data to an analytic expression for each mode.

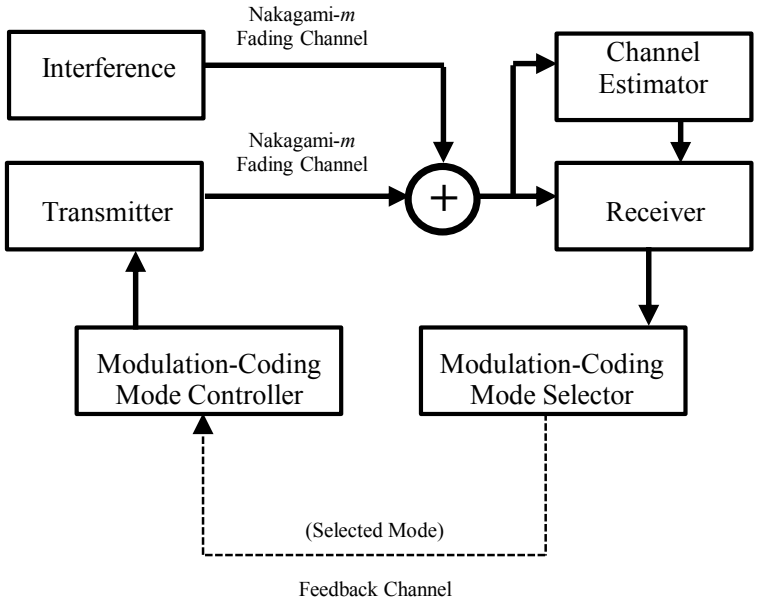


Fig. 4.24. System diagram with interfering transmitter.

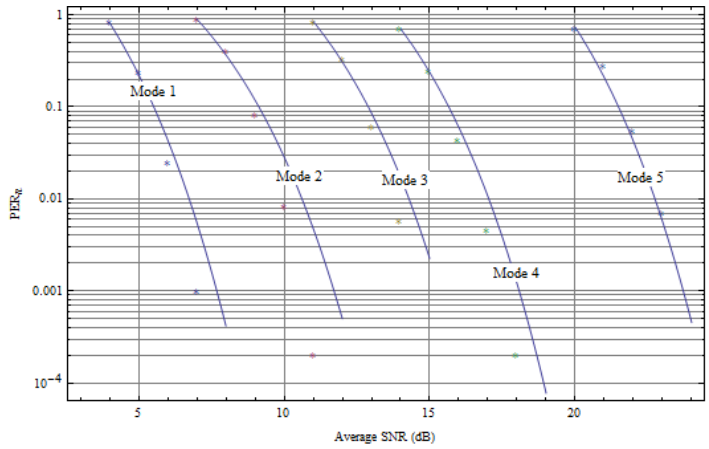


Fig. 4.25. Packet error rate based on simulation of MCS (stars) and curve fitting to the simulation (line).

As in [24-27], the functional form for fitting is

$$PER_n(\gamma) \approx \begin{cases} 1, \ if \ 0 < \gamma < \gamma_{pn}, \\ a_n e^{-g_n \gamma}, \ if \ \gamma \geq \gamma_{pn}, \end{cases} \tag{22}$$

where n represents the mode and γ is the received SNR. The parameters a_n,g_n, and γ_{pn} are the curve fitting parameters and given in Table II.

iv. Average Packet Error Rate with Fading and Interference

We use the PER as a function of SNR (22) to predict the system performance when the received signal is subject to interference and fading. Both the target and interfering signals are subject to independent Nakagami-*m* fading with the same *m* fading parameter and flat fading is assumed. Optimum receiver structures are utilized; perfect channel state information (CSI) for the target transmitter/receiver pair and ideal phase and frequency synchronization is presumed. Since each RB uses the same

mode, this analysis is performed per mode. The interfering signal utilizes 4-QAM signaling and has the same bandwidth as a target system sub-carrier. We place the interfering signal in the guard band of the target signal as in Fig. 4.26. However, the methodology developed here can be applied to any placement of the interfering signal including frequency hopping interference.

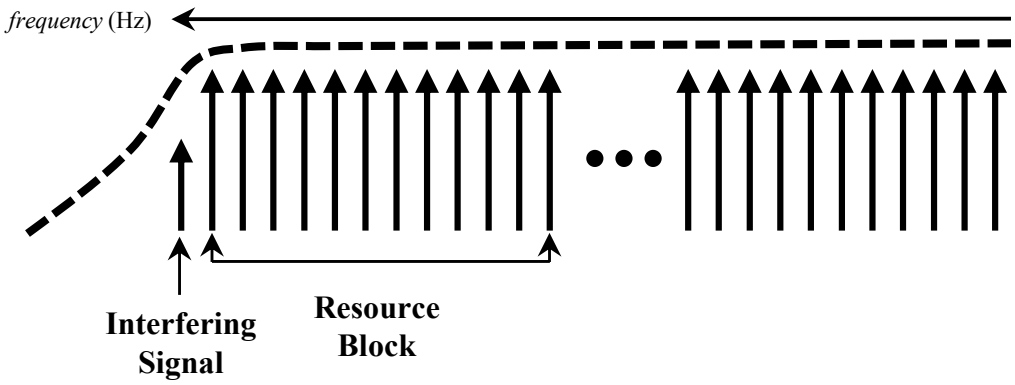


Fig. 4.26. Placement of the interfering signal in the guard band of the target down-link signal spectrum.

TABLE II

CURVE FITTING PARAMETERS

	Mode 1	Mode 2	Mode 3	Mode 4	Mode 5
Modulation (M_n)	QPSK	QPSK	16-QAM	16-QAM	64-QAM
Coding Rate R_c	1/2	3/4	9/16	3/4	3/4
Rate (bits/sym)	1.00	1.50	2.25	3.00	4.50
a_n	124.9390	28.8989	42.9191	47.9713	97.5387
g_n	1.9992800	0.6920240	0.3116290	0.1679410	0.0488942
γ_{pn} (dB)	3.82877	6.86698	10.81470	13.62620	19.71630

The target OFDM and interfering systems are not in synchronization. Therefore, the interfering and target signals are not orthogonal. The in-band interference is set equivalent to white Gaussian noise with a noise power equal to the in-band interference power; the main purpose of this study is to validate this equivalence. A similar approach was used in [33], [34], and [35] to find BER for uncoded systems. We define in-band interference power as the power within the zero-to-zero crossings of the spectrum of the interfering signal, here ~sinc^2(*f*/BW).

The pdf of the instantaneous received SNR when the target and interfering signals experience independent Nakagami-*m* fading was developed in [16]. A form of the resulting pdf [20] is given as

$$f_\gamma(\gamma) = \frac{1}{2\sqrt{\pi}\gamma\,\Gamma(m)} m^{2m} \left(\frac{1}{\bar{\gamma}_c}\right)^m \left(\frac{\gamma}{\bar{\gamma}}\right)^m e^{\frac{m(\bar{\gamma}-\bar{\gamma}_c\gamma)}{2\bar{\gamma}\bar{\gamma}_c}} \left(m\left(\frac{\gamma}{\bar{\gamma}}+\frac{1}{\bar{\gamma}_c}\right)\right)^{\frac{1}{2}-m} \left(K_{\frac{1}{2}-m}\left(\frac{m(\bar{\gamma}+\bar{\gamma}_c\gamma)}{2\bar{\gamma}\bar{\gamma}_c}\right) + K_{-m-\frac{1}{2}}\left(\frac{m(\bar{\gamma}+\bar{\gamma}_c\gamma)}{2\bar{\gamma}\bar{\gamma}_c}\right)\right), \quad (23)$$

where K_k is the modified Bessel function of the second kind [45] and $\bar{\gamma}_c$ is the average in-band transmitted SNR of the interfering signal. Recall that (13) is identical to (23) and is repeated for its importance in the development of the analysis going forward. The OFDM signal is comprised of multiple carriers organized into RBs as in LTE [49] where each RB contains 12 sub-carriers. The different impact of the interfering signal on each sub-carrier in the target system must be taken into account. The influence of the interfering signal on a sub-carrier decreases as the spectral distance between the interfering signal and each sub-carrier increases. To account for

the different interference power on each sub-carrier, i, a different normalization (impact) factor is needed and can be found as in [22] by (17). We approximate the impact of the interference over the entire RB by using the average in-band transmitted SNR over all sub-carriers in a RB and setting it equal to $\bar{\gamma}_c$ in equation (23), i.e.,

$$\bar{\gamma}_c = P_c \frac{\sum_{i=1}^{I} \rho_i}{I}. \tag{24}$$

The contribution of the work here is the application of (24) to predicting the PER over a RB and its validation. If the PER of a coded multi-carrier system without interference is known, then the impact of interference with a shaped spectral density can be found using (24).

The work here considers a slow fading channel model as in [24-27]. This means the channel does not change from the time the channel is measured until the packet is received. Therefore, the average PER for a given mode in the presence of an interferer with a shaped spectral density over a RB as a function of the average transmitted target system power is defined to be [48]

$$\overline{PER}_n(\bar{\gamma}) = \int_0^\infty PER_n(\gamma) f_\gamma(\gamma) d\gamma, \tag{25}$$

where $\bar{\gamma}_c$ from (24) is used in $f_\gamma(\gamma)$ and $PER_n(\gamma)$ for each mode n is from (22).

v. Validation of Average Packer Error Rates

In this section we present results that validate the analysis in the previous section. The purpose of the first study was to compare the average PER predicted using (24) and (25) for all the modes of the proposed system with simulation. We first set the Nakagami-m fading parameter to m = 1 (Rayleigh fading) for all modes. The

interfering signal has an average transmitted SNR of 5 dB. Fig. 4.27 shows that analytic curves follow the simulation closely and are more conservative than the analysis predicts. The study is repeated in Fig. 4.28 where the interfering signal has an average SNR of 15 dB. Fig. 4.28 produces results similar to Fig. 4.27.

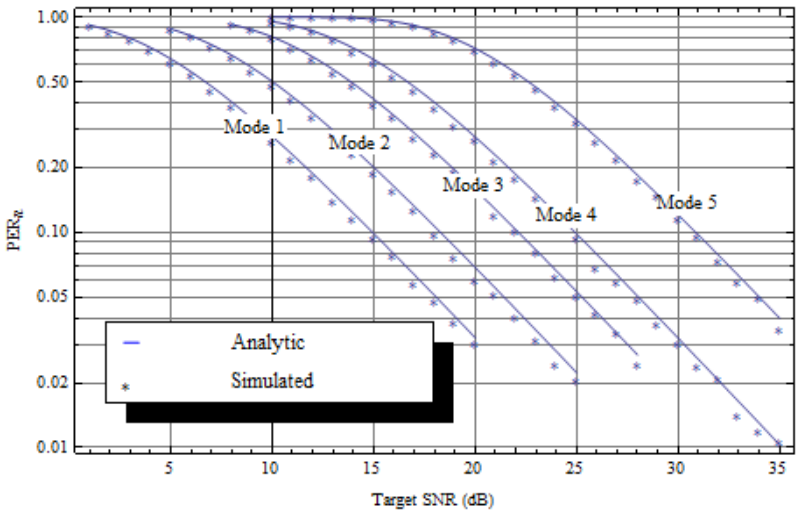


Fig. 4.27. Simulation of average PER (stars) and analytic prediction (line) for mode 5, Nakagami-*m* fading, interfering signal SNR = 5dB [21].

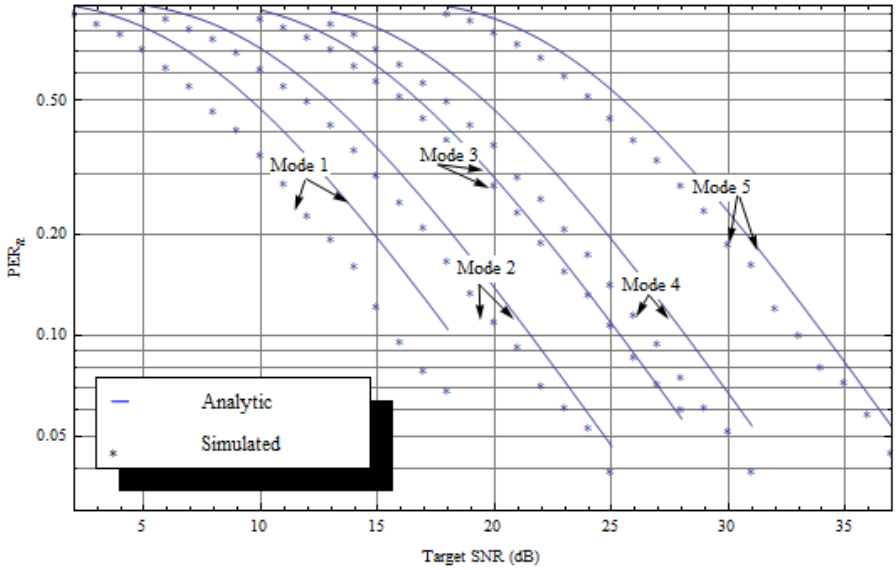


Fig. 4.28. Simulation of average PER (stars) and analytic prediction (line) for all modes with covert signal SNR = 15 dB, Rayleigh fading.

The second study looks at the impact the channel has on the ability of the analysis to predict average PER performance. We select mode 5 and simulate Nakagami-*m* fading for m = 0.5, 1.0, 2.0, and 3.0 for comparison. Fig. 4.29 shows that the analysis performs in a fashion similar to Fig. 4.27; the simulated curves follow the analytic curves with only a small difference. The proposed approximation predicts worse performance for the target system than what the simulation revealed.

In the next study we utilize mode 1 and hold the interferer SNR steady throughout the simulation at 15 dB. We can see from Fig. 4.30 that as m increases the difference between the analytic prediction and the simulation increases.

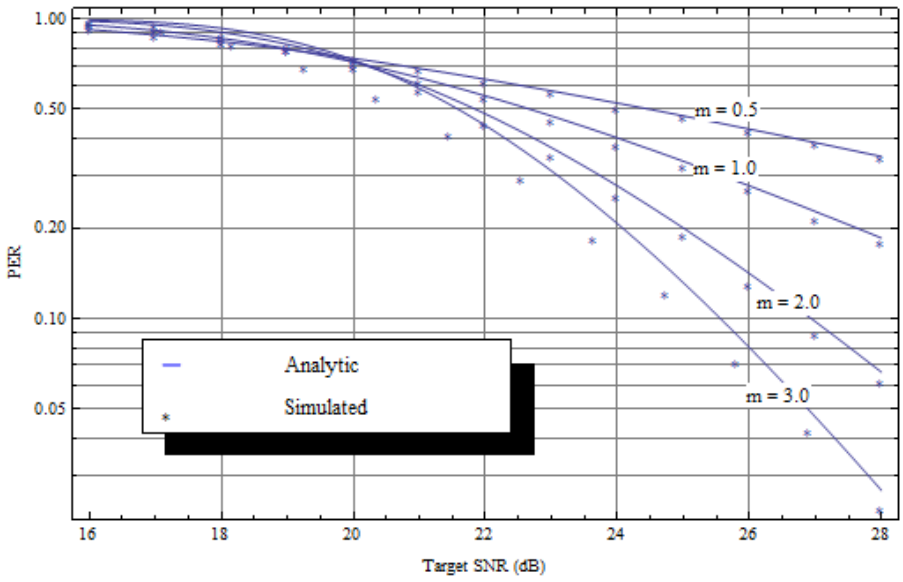


Fig. 4.29. Simulation of average PER (stars) and analytic prediction (line), Rayleigh fading, interfering signal SNR = 5dB [21].

The final study broadens the design space by considering other interfering signal powers. We compare the ability of the analysis to predict the target system performance when interfering signal SNR is increased from 5 to 15 and then 25 dB for mode 5. Fig. 4.31 reveals that the calculated performance of the target system is again a more conservative prediction of PER. The difference between the analytic and simulated curves increases as the interfering SNR increases; at an interfering signal SNR of 25 dB the analytic prediction is off by 3 dB.

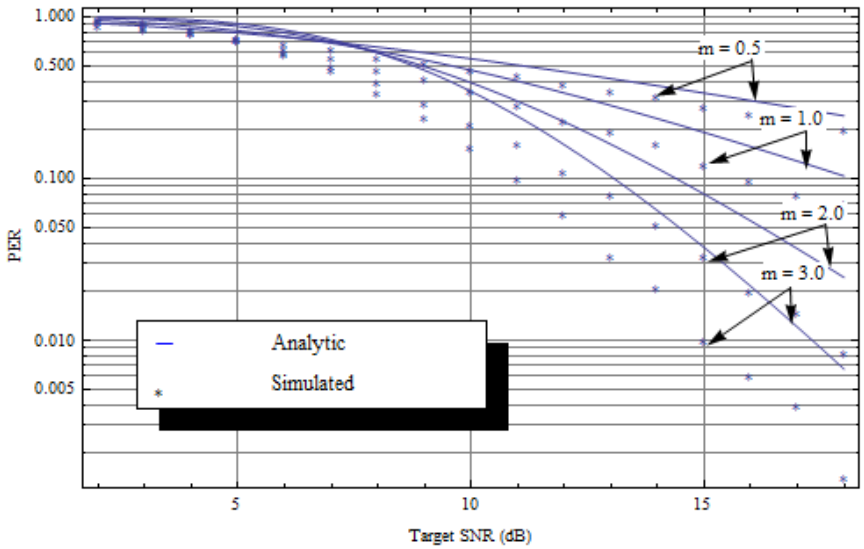


Fig. 4.30. Simulation of average PER (stars) and analytic prediction (line) for mode 1, Nakagami-*m* fading, interfering signal SNR = 15dB [21].

These results show that the proposed method closely predicts the PER performance when the interference power is 5 dB; the difference between the simulated and analytic prediction is less than 1 dB. Thus in this case the impact of the interferer is mostly on the 1st sub-carrier. As the interference power increases the effect on subsequent sub-carriers increases and hence the estimate becomes less accurate however the proposed method always provides a conservative prediction of PER performance. This means that equating the in-band interference to white noise is overestimating the effect of the interference; white noise of the same power as in-band interference impacts the target signal worse than a shaped power spectrum. So the actual performance will be better than the predicted by the analysis.

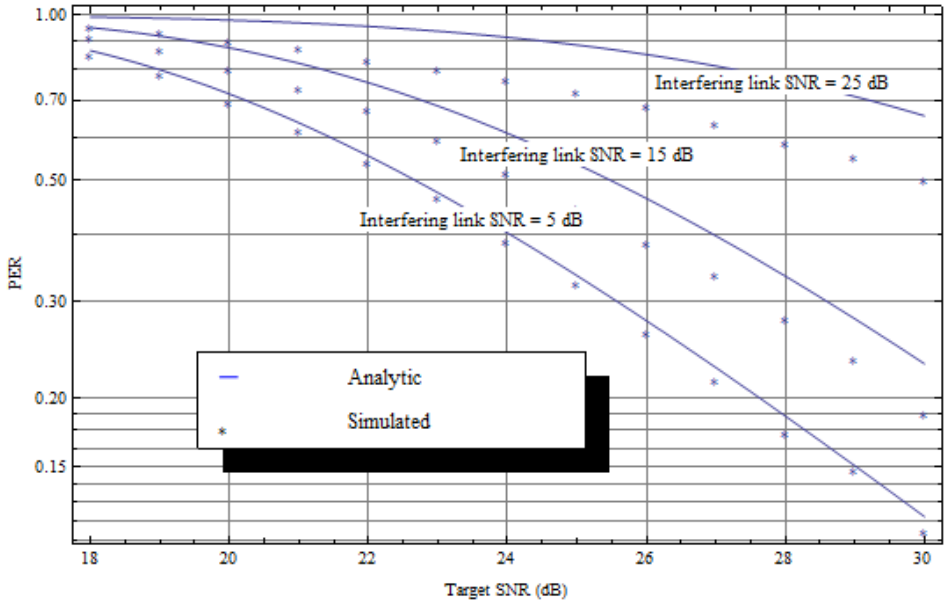


Fig. 4.31. Simulation of average PER (stars) and analytic prediction (line) for mode 5 with varying covert signal SNR, Rayleigh fading [21].

vi. Conclusions

A new method for estimating the average PER of a coded OFDM system subjected to interference with a shaped spectral density was proposed and validated. Results were presented that compared the performance of the proposed method for PER estimation to simulation. These results validated using the average in-band transmitted SNR over all sub-carriers as an approximation to determine the average PER. The method presented is a conservative predictor of performance and in all cases presented is conservative, i.e., one can expect better target system performance than predicted by the analysis. The prediction of PER performance using the proposed approach could contribute to better spectrum and interference management schemes. Also, this method can provide the basis to predict end-to-end performance including

impacts on higher network layers, e.g., TCP, when a wireless hop is exposed to interference with a shaped spectral density.

Chapter 5

The Data-Link Layer

In this chapter we show the impact of interference generated by a covert link on the data-link layer of a packet based (infrastructure) wireless network. Infrastructure networks employ OFDM, AMC, and ARQ to allow them to achieve higher data rates and increase capacity; the adaptive characteristics of these networks make them susceptible to exploitation. Performance was measured in terms of PER and spectral efficiency (throughput) versus increased covert signal power while assuming both signals are subject to independent Nakagami-*m* fading. The performance at the data-link layer was shown to be practically indistinguishable from channel fading when ARQ is used. This chapter gives similar results for networks that utilize HARQ or TARQ and compares the data-link layer performance in the presence of a covert link.

The design space that will be examined going forward can be viewed as consisting of three variables; target SNR, covert (interferer) SNR, and the fading environment. A visualization of this concept can be seen in Fig. 5.1. In order to validate the conclusions, a broad range of the design space must be analyzed. Measurement of channel characteristics at 900 MHz in an urban environment were reported in [46] where the most likely values of m ranged from 0.5 to 3.5 with an average of m= 1.56. While in [47] m= 2.38 was reported at 870.9MHz in an urban environment. Note that these measurements indicate that the fading parameter m can vary widely. However, m= 1.56 and 2.38 are incompatible with the method of calculation used here. Thus values of m = 0.5, 1.0, 2.0, and 3.0 were selected which covers the range of m measured in [46] and [47]. We focus on SNRs in the approximate range of 0 to 30 dB for the interfering and target signal so that we cover both high and low SNR cases. In Chapter 4 the physical layer tradeoffs reveled that a covert link with an average SNR of 5 dB, utilizing 4-QAM signaling, and operating at $1/8^{th}$ the symbol rate of the target OFDM system with an average SNR of 26.15 dB could achieve an uncoded BER ~ 10^{-2}.

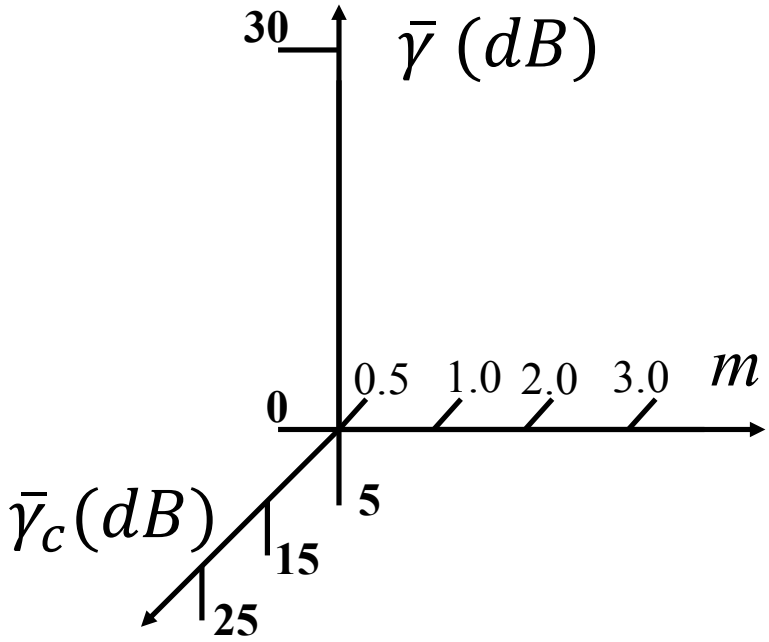


Fig. 5.1. Design space variables.

A. The Impact of Interference from a Covert Link on a Data-Link with OFDM, AMC, and ARQ

This section addresses the data-link layer performance in the presence of interference generated by a covert transmitter as in Fig. 5.2. Performance is measured in terms of PER and spectral efficiency versus increased covert signal power while assuming both signals are subject to independent Nakagami-*m* fading.

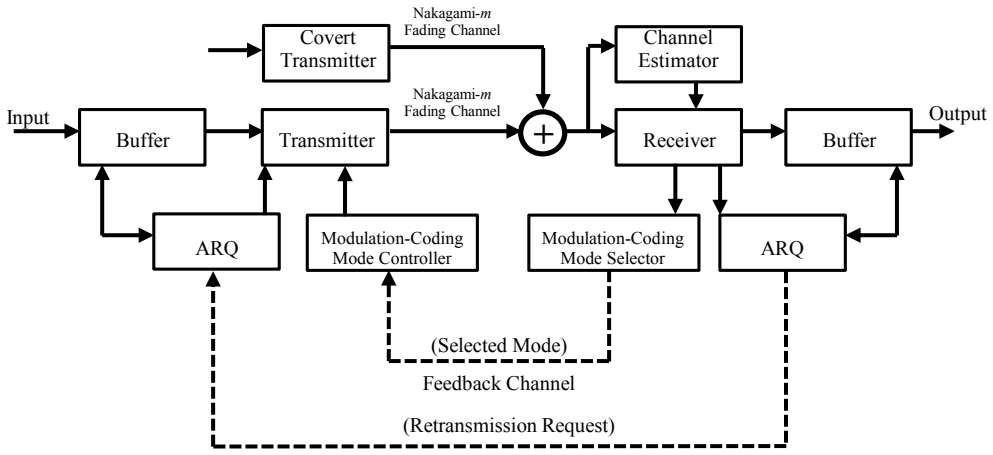


Fig. 5.2. System model extended from [25] to include covert link.

i. Introduction

The work in previous chapters addressed the interaction between the covert and target signals at the physical layer and quantified the performance of both by measuring the uncoded BER; it showed that a covert link with an average SNR of 5 dB, utilizing QPSK signaling, and operating at $1/8^{th}$ the symbol rate one sub-carrier of the target OFDM system with an average SNR of 26.15 dB could achieve a BER ~ 10^{-2}. The analytic methods used to find the BER were verified through simulation. The work presented here shows the impact of a covert signal on a target network that utilizes AMC at the physical layer and ARQ at the data-link layer. The work in this chapter also compares the impact of a covert signal on a target network that utilizes either HARQ with a target network that utilizes TARQ. It is to be noted that while the analysis presented here models a covert link placed in the guard band of the target OFDM system, the analysis is general and can be applied to any type of interference, i.e., intentional, unintentional, co-channel, or adjacent channel interference.

ii. Assumptions

a. Physical Layer

Many of the assumptions here follow from Chapter 4. The physical layer model consists of a target transmitter/receiver pair and a covert transmitter. Standards that utilize OFDM, such as LTE [49], allocate sub-carrier frequencies on the edges as a guard band. This model assumes that the covert transmitter is operating in the guard band closest to the sub-carriers transmitting information in the target OFDM signal as in Fig. 4.26. The covert and the target OFDM signal are subject to independent Nakagami-*m* fading and share the same *m* fading parameter. Here we consider *m* fading parameters of 0.5, 1.0 (Rayleigh fading), 2.0, and 3.0. The channel is frequency flat. Therefore, the channel does not appreciably change from the time the channel is measured until after the first packet is transmitted.

The target OFDM signal consists of *I* orthogonal sub-carriers. In LTE, twelve sub-carriers typically comprise a resource block. A UE can be assigned one or more resource block [49]. The modulation on each sub-carrier of the target OFDM signal is selected based on the channel quality indicator (CQI) feedback to be 4, 16, or 64-QAM signaling with rectangular pulse shaping. The transmission mode, *n*, is defined by a coding rate, R_n, and a modulation, M_n. All sub-carriers in a resource block utilize the same AMC mode. We assume packet bits are distributed evenly among the sub-carriers of a single resource block. While the analysis presented here is general and can be applied to wide range of interference, the covert transmitter utilizes QPSK signaling with $sinc^2$ power spectrum. Receiver structures are optimum with ideal

phase and frequency recovery. The target and covert signals are not orthogonal due to the non-synchronization of the signals at the target receiver. This analysis models the in-band interference from the covert as white Gaussian noise. The power from the covert interferer that lies in the target sub-carriers frequency band is set equal to white Gaussian noise. A similar approach was used in [22] and [33]. The work in Chapter 4 simulated the scenario discussed here and compared the results with analytic results in order to verify the validity of this assumption. It was found that setting the interference power equivalent to white Gaussian noise was a conservative estimate of the impact of the interference on the target system.

b. Data-Link Layer

The analysis follows [24-27] where streams of bits from the physical layer are fed to the data-link layer and mapped to packets as in Fig. 5.3. The number of packets (N_b) at the data-link layer combined with the necessary pilot symbols (N_c) comprise a frame at the physical layer. The mapping of this relationship can be found in [24-27]. Using the notation from [25], a frame is comprised of N_f symbols. Each packet contains N_p bits. Some of these bits are used for error checking. We assume ideal error checking which triggers retransmission of the packet as part of the ARQ protocol.

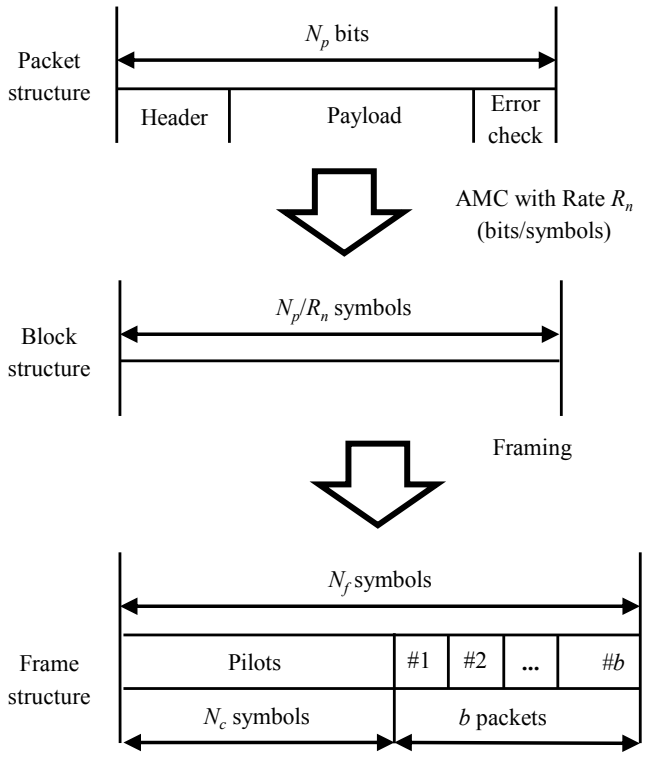


Fig. 5.3. Mapping of bits to packets, frames, and symbols from [25] with modifications.

If a packet is received in error a retransmission request is sent through the feedback channel. When TARQ is utilized a packet is discarded if it is received in error. The packet is then retransmitted using the same AMC mode as the first packet transmission attempt. Here HARQ with Chase combining (CC) [52] is implemented at the data-link layer. The packet received in error is saved and combined with the next packet [28]. Retransmitting, and combining with prior packets for HARQ only, continues until either the packet is received correctly or the maximum number of transmissions is reached. We set the maximum number of transmissions to be K for HARQ and N_r^{max} for TARQ. If a packet has been transmitted K or N_r^{max} times and

received unsuccessfully, then a packet error is declared. The probability of a packet error event is P_{loss}. Note that in the case of a packet error event the transport layer will be affected.

c. Cross-Layer Modelling

Exact closed form expressions for PER of coded modulations are not available. Therefore, we utilize the PER functions from Chapter 4 in the form of (22) whose parameters are given in Table II.

The cross-layer model developed in [25] utilizes TARQ at the data-link layer. The analysis in [28] alters the model in [25] for HARQ. The work here extends the model in [28] to include interference from a covert transmitter. The probability of packet loss after k transmissions is set to be no greater than P_{loss} in order to satisfy the QoS constraint. The loss probability for the k^{th} transmission in HARQ is approximated by [28, eq. (26)]

$$P_{loss} = e^{-g_n(\frac{k(k+1)}{2}\gamma - k\gamma_{pn})}. \tag{26}$$

The thresholds for mode switching, γ_n, are found using the approach in [28]. Here calculation of the SNR switching thresholds is optimized for each AMC mode and minimum PER requirement without consideration or knowledge of the covert signal. There are N transmission modes available to the target system. We assume constant power transmission. The total SNR range is partitioned into $N+1$ consecutive non-overlapping intervals γ_0 to γ_N. The channel is not utilized when $\gamma < \gamma_1$. The system curve fit parameters used here are given in Table II.

iii. PER, Spectral Efficiency, and Outage Probability with Interference from the Covert Transmitter

The pdf of the instantaneous received SNR of a target signal with no interference from the covert link in Nakagami-*m* fading is characterized by (7). The thresholds for AMC mode selection are calculated without consideration of the interference from the covert link.

a. Hybrid ARQ

The thresholds used in the AMC mode selection for HARQ $\{\gamma_n\}_{n=0}^{N+1}$ are calculated using the approach presented in [28]. Note $\{\gamma_n\}_{n=0}^{N+1}$ are determined without consideration of the interference generated by the covert signal. The pdf of the instantaneous received SNR when the target and covert signals experience independent Nakagami-*m* fading was is given by (23).

The OFDM signal is comprised of multiple carriers organized into resource blocks. The impact of the covert link on each sub-carrier in the target system must be taken into account. The influence of the covert link on a sub-carrier decreases as the spectral distance between the covert signal and each sub-carrier increases. For each sub-carrier, *i*, a different normalization (impact) factor is needed and can be found as in (17). We approximate the PER of a resource block by using the average in-band transmitted SNR over all sub-carriers in a resource block and setting (24) equal to $\bar{\gamma}_c$ in (23). This approximation enables us to directly extend the analysis in [25] to the analysis of OFDM with HARQ and AMC in the presence of an interferer.

Now following [25], the probability that mode *n* will be selected with the interference generated by the covert transmitter taken into account is given by [48, eq. (34)]

$$\Pr_c(n) = \int_{\gamma_n}^{\gamma_{n+1}} f_\gamma(\gamma) d\gamma. \tag{27}$$

As in [28], the per packet SNR is i.i.d. for a fast block fading channel. Each packet transmission experiences a new i.i.d. SNR which is in the range of $\gamma \in [0, \infty)$. A fast block fading channel is assumed in [28] which results in an average PER for a given mode in the presence of a covert interferer for a resource block as [28, eq. (8)]

$$\overline{PER}_{cn}(\mathrm{K}) = \frac{1}{\Pr_c(n)} \int_0^\infty \dots \int_0^\infty \int_0^\infty \prod_{k=1}^{K} \begin{matrix} PER_n\left(\sum_{q=1}^{k} \gamma_q\right) f_\gamma(\gamma_1) \dots \\ \dots f_\gamma(\gamma_K)\, d\gamma_1 \dots d\gamma_K \end{matrix}. \tag{28}$$

Using the above equation and without interference, a closed form solution for the average PER is given in [28].

However, this work considers a slow block fading channel model as in [24-27]. Here the channel does not appreciably change from the time the channel is measured until after the first packet is transmitted. Assuming that the channel does not significantly change from the time the channel is measured until the first packet transmission means that the SNR of the first packet transmission utilizing mode *n* lies in the SNR region for mode *n*, i.e., for the first packet transmission the Prob$\{\gamma \in [\gamma_n, \gamma_{n+1})\}$ = 1. The SNR of all other subsequent packet retransmissions are i.i.d. and can have any value $\gamma \in [0, \infty)$, i.e., from the time the channel is measured until the packet is retransmitted is long enough such that the retransmission experiences a new i.i.d. SNR in the range of $\gamma \in [0, \infty)$. Therefore, the average PER for a given mode in

the presence of a covert interferer for a resource block is defined here to be

$$\overline{PER}_{cn}(\mathrm{K}) = \frac{1}{\Pr_c(n)} \int_0^{\infty} \dots \int_0^{\infty} \int_{\gamma_n}^{\gamma_{n+1}} \prod_{k=1}^{K} \begin{matrix} PER_n\left(\sum_{q=1}^{k} \gamma_q\right) f_\gamma(\gamma_1) \dots \\ \dots f_\gamma(\gamma_K)\, d\gamma_1 \dots d\gamma_K \end{matrix}. \quad (29)$$

The average PER with the covert link given all *N* modes of AMC transmission can be found as the total number of packets transmitted in error over the total number of packets transmitted which is given by [25, eq. (8)]

$$\overline{PER}_c(\mathrm{K}) = \frac{\sum_{n=1}^{N} R_n \Pr_c(n) \overline{PER}_{cn}(K)}{\sum_{n=1}^{N} R_n \Pr_c(n)}. \quad (30)$$

Having utilized HARQ at the data-link layer, the maximum number of transmissions of a packet is *K*. Here, including the covert link in the analysis, the average number of transmissions per packet is [28, eq. (17)]

$$\bar{N}_a = 1 + \sum_{k=1}^{K-1} \overline{PER}_c(k). \quad (31)$$

Each transmitted symbol will carry $R_n = R_c log_2(M_n)$ information bits when mode *n* is utilized. M_n refers to the QAM constellation for mode *n* and R_c is the FEC code rate. The average spectral efficiency, without retransmission, is [25, eq. (12)]

$$\bar{S}_0 = \sum_{n=1}^{N} R_n \Pr_c(n). \quad (32)$$

Including retransmissions with the covert link present and taking into account the HARQ protocol, the average spectral efficiency is [25, eq. (13)]

$$\bar{S}_K = \frac{\bar{S}_0}{\bar{N}_a} = \frac{1}{\bar{N}_a} \sum_{n=1}^{N} R_n \Pr_c(n). \quad (33)$$

The pdf of the instantaneous SINR is utilized to calculate the packet outage probability (P_{out}). The P_{out} is defined as the probability the instantaneous SINR falls below γ_1 for the AMC system, which is defined as

$$P_{out} = \int_0^{\gamma_1} f_\gamma(\gamma) d\gamma. \quad (34)$$

For hybrid ARQ systems, P_{out} becomes [53]

$$P_{out-HARQ} = \bar{N}_a \cdot P_{out}. \quad (35)$$

b. Truncated ARQ

The mode switching thresholds for TARQ, γ_n, are found by inverting (22). The average PER of mode *n* over a resource block with covert interferer for TARQ is [25, eq. (8)]

$$\overline{PER}_{cn} = \frac{1}{\Pr_c(n)} \int_{\gamma_n}^{\gamma_{n+1}} PER_n(\gamma) f_\gamma(\gamma) d\gamma. \quad (36)$$

Having utilized truncated-ARQ at the data-link layer, the maximum number of times a packet may be retransmitted is N_r^{max}. Here, including the covert link, the average number of transmissions per packet is [25, eq. (10)]

$$\bar{N}_c = \frac{1-\overline{PER}_c{}^{N_r^{max+1}}}{1-\overline{PER}_c}. \quad (37)$$

Including retransmissions with the covert link present and taking into account the truncated-ARQ protocol, the average spectral efficiency is [25, eq. (13)]

$$\bar{S}_{N_r^{max}} = \frac{\bar{S}_0}{\bar{N}_c} = \frac{1}{\bar{N}_c} \sum_{n=1}^{M} R_n \Pr_c(n). \quad (38)$$

iv. Target System Performance

In this section we present the target system performance when impacted by a covert link based on the previous analysis for HARQ and TARQ.

a. HARQ System Performance

To evaluate the target system performance the numerical results presented

here considers the case where the mode switching thresholds for the link adaptive system, γ_n, is set to satisfy $P_{loss} = 0.01$ and K=3. A resource block is comprised of 12 sub-carriers; each sub-carrier has a symbol rate of 15,000 *symbols/sec*. The covert signal is placed 15 kHz from the first sub-carrier and is characterized by a $sinc^2$ power spectrum operating at 5 dB average transmitted SNR. The covert link utilizes QPSK signaling. The symbol rate of the covert link is $1/8^{th}$ of the target OFDM system which results in an overall bit rate for the covert link that is $1/8^{th}$ of an individual OFDM sub-carrier utilizing identical M-QAM signaling constellation. The parameters of the covert link were selected to enable the covert link to operate at BER $< 10^{-2}$ in the presence of the target link as found in the trade-off analysis conducted in Chapter 4.

Fig. 5.4 and Fig. 5.5 include a performance comparison with and without the covert link present for m = 1 (Rayleigh fading). With and without the covert link present, the OFDM performance in terms of PER and spectral efficiency follow the same trend and only show a slight deviation from the line without interference. Results are also included for other channel conditions, i.e., for different values of the Nakagami fading parameter m. The performance of the target system changes more as the channel conditions change from m = 1 to .5 or when the fading parameter goes from m = 1 to 2 compared to the performance degradation introduced by adding the covert link with a SNR of 5 dB. At 20 dB the target system has a PER of 10^{-4} for m = 1 with or without interference compared to a PER of 10^{-3} for m = .5 with interference. Fig. 5.4 shows the PER for when m = 1 with and without covert presence having a

difference of less than 10^{-4} while changing the m to .5 or 1 has a much greater impact; at 15 dB the PER is approximately 10^{-4} for m = 1.0 and approximately 10^{-2} for m = 0.5. The same is also true in relation to spectral efficiency when one takes into account Fig. 5.5. The spectral efficiency is approximately 4 *bits/symbol* for m =1 and 3.5 and 4.25 *bits/symbol* when m = .5 and 2, respectively. Fig. 5.6 shows P_{out} for average target SNR of 26.15 dB. We can see that P_{out} increases for lower values of SNR as m increases. For example, when m = 3 P_{out} begins to increase at approximately 5 dB whereas when m = .5 it begins to increase at approximately 15 dB. Also, the rate of increase is greater as m increases. The four lines converge to approximately P_{out} = 0.1 at high SNR while they begin at approximately 10^{-1}, 10^{-3}, 10^{-5}, and 10^{-6} for m = 0.5, 1.0, 2.0, and 3.0, respectively, at low SNR.

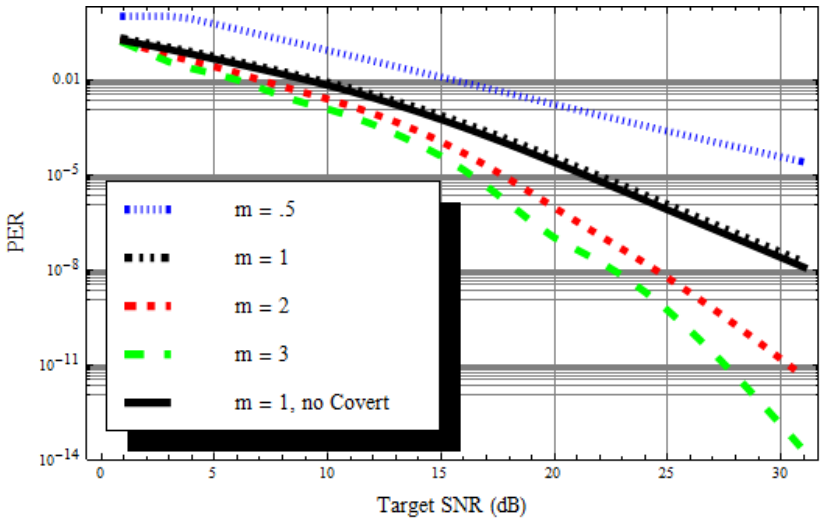


Fig. 5.4. PER of target system with average covert SNR = 5 dB, Nakagami-*m* fading.

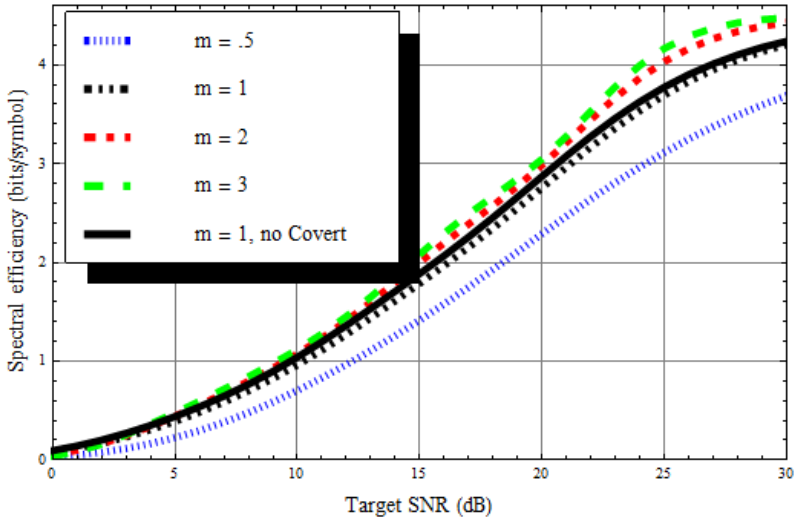


Fig. 5.5. Spectral efficiency of target system with average covert SNR = 5 dB, Nakagami-*m* fading.

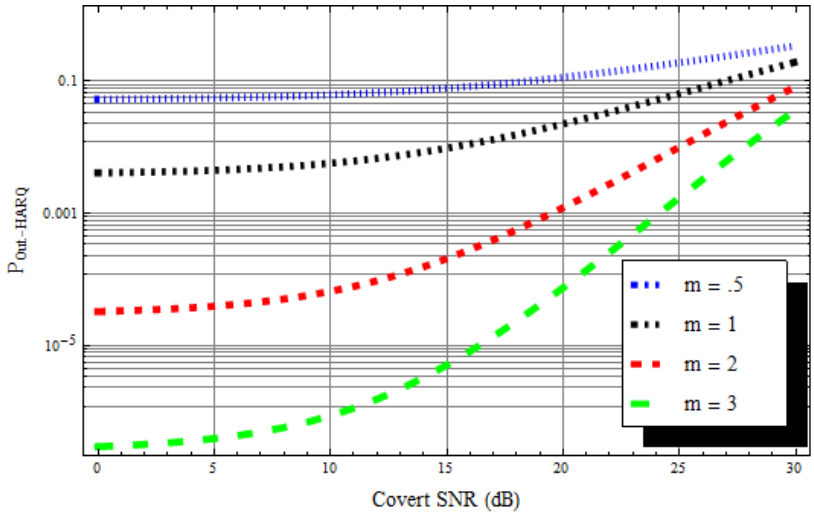


Fig. 5.6. P_{out} of target system with average target SNR = 26.15 dB, Nakagami-*m* fading.

b. TARQ

The numerical results presented here sets $P_{loss} = 0.01$ and $N_r^{max} = 3$. A resource block is comprised of 12 sub-carriers. Each sub-carrier has a symbol rate of 15,000 *symbols/sec*. The covert signal is placed 15 kHz from the first sub-carrier and is characterized by a $sinc^2$ power spectrum operating at 5 dB average transmitted SNR. The parameters of the covert link were selected to match those of the HARQ system.

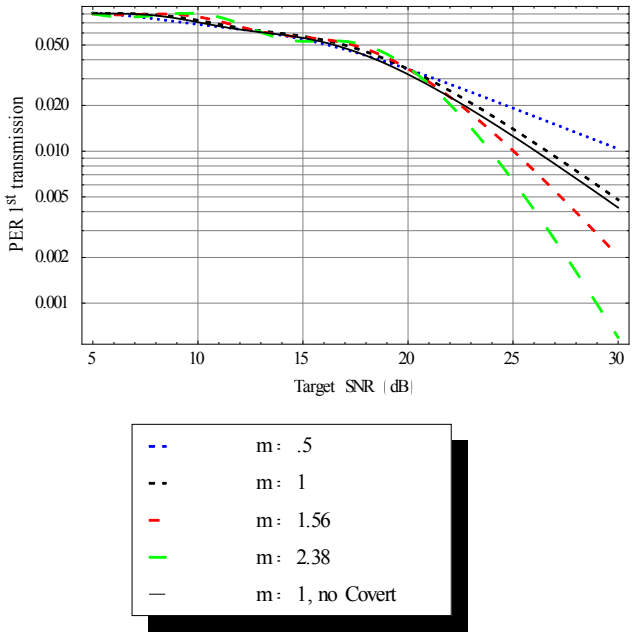


Fig. 5.7. PER of 1st transmission of target system with average covert SNR = 5 dB, Nakagami-*m*=fading parameter.

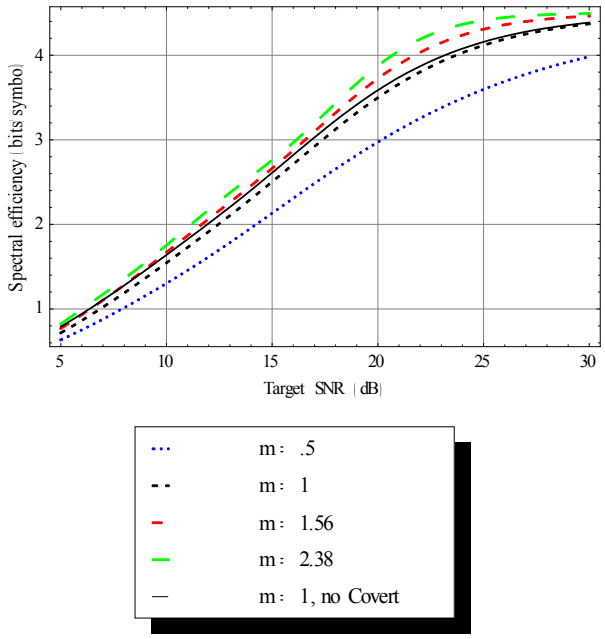


Fig. 5.8. Spectral efficiency of target system with $N_r^{max} = 3$.

Figs. 5.7 and 5.8 include a performance comparison with and without the covert link present for m = 1 (Rayleigh fading). With and without the covert link present, the OFDM performance in terms of PER and spectral efficiency follow the same trend and only show a difference of less than 0.1 bits/symbol. Results are also included for other channel conditions, i.e., for different values of the Nakagami fading parameter m. The performance changes more as the channel conditions change from m = 1 to .5 or when the fading parameter goes from m = 1 to 2.38 compared to the performance degradation introduced by adding the covert link. Fig. 5.7 shows the PER at 25 dB for when m = 1 with and without covert presence having little difference ($> 10^{-2}$) while changing the m to .5 or 1.56 has a much greater impact. The same is also true in relation to spectral efficiency when one takes into account Fig. 5.8

at 25 dB. The spectral efficiency is approximately 4 *bits/symbol* for m =1 and 3.6 and 4.4 *bits/symbol* when m = .5 and 2.38, respectively.

v. Performance Tradeoffs

We present the impact of varying covert power on the performance of the target system for HARQ and TARQ. The performance of the target system is negatively impacted from an increase in power of the covert signal by increasing the target system PER. However, increasing the covert signal power will improve its performance by lowering the covert system BER. However, an increase in covert signal power will also increase its probability of detection.

a. HARQ

Fig. 5.9 shows the impact of the increasing covert signal power on the PER. Fig. 5.10 shows the impact of increasing covert signal power on the spectral efficiency. The target system sub-carrier SNR was held constant at 26.15 dB throughout this study. In Rayleigh fading, when no interference is present a 16-QAM sub-carrier with a SNR of 26.15 dB results in a BER of approximately 0.5×10^{-3}. If we take the line for m=1 as a reference in Figs. 5.9 and 5.10, for average covert SNR=5 dB the PER is approximately 10^{-7} and the spectral efficiency is 4.2 *bits/symbol*; we can compare the impact of fading versus interference from the covert system. For fading parameter m=0.5 and average covert SNR=5 dB, the PER increases to 10^{-4} while this occurs for m=1 at 25 dB average covert SNR, an increase of 20 dB versus a difference of 0.5 in the fading parameter. For fading parameter m=0.5 and average

covert SNR=5 dB, the spectral efficiency decreases to 3.6 *bits/symbol* where this occurs for fading parameter *m*=1 when the covert SNR= 19 dB; a difference of 14 dB versus difference of 0.5 in the fading parameter. It is deduced from the comparison of these observations that a change in *m* has a greater impact on the target system performance than an increase in average covert SNR.

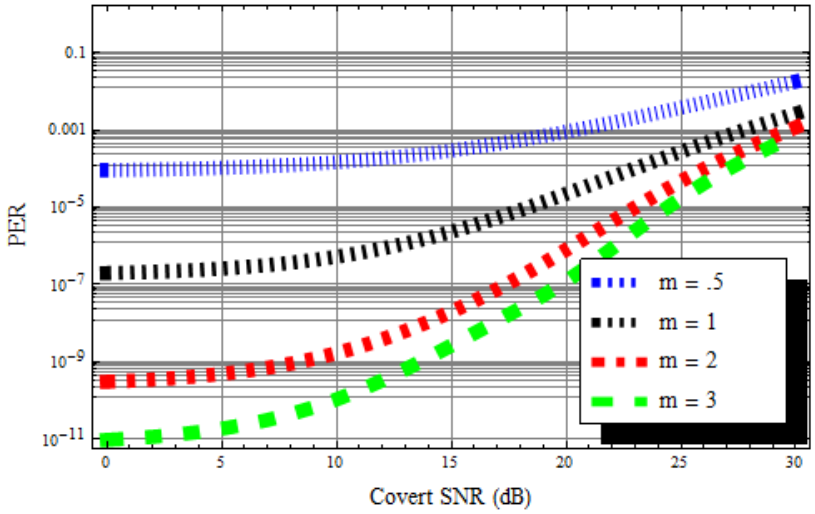


Fig. 5.9. PER of target system with average target SNR = 26.15 dB, Nakagami-*m* fading.

b. TARQ

Fig. 5.11 shows the impact of the increasing covert signal power on the PER. Fig. 5.12 shows the impact of increasing covert signal power on the spectral efficiency. The target system sub-carrier SNR was held constant at 26.15 dB throughout this study. In Rayleigh fading, when no interference is present a 16-QAM sub-carrier with a SNR of 26.15 dB results in a BER of approximately 0.5×10^{-3}. We can see from Fig. 5.11 and Fig. 5.12 that the impact of the covert on the target

network is practically indistinguishable from fading. Approximately equal OFDM performance is obtained (a PER $\cong 10^{-2}$) when m =1 and the covert link has an average SNR of 0 dB, compared to when m = 1.56 with an average covert SNR of 10 dB. For these cases the spectral efficiency is approximately the same, 4.2 *bits/symbol*.

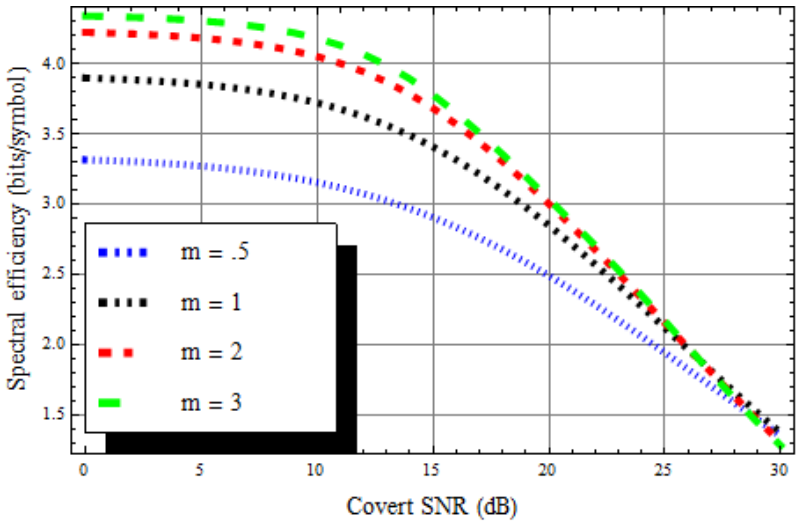


Fig. 5.10. Spectral efficiency of target system with average target SNR = 26.15 dB, Nakagami-*m* fading.

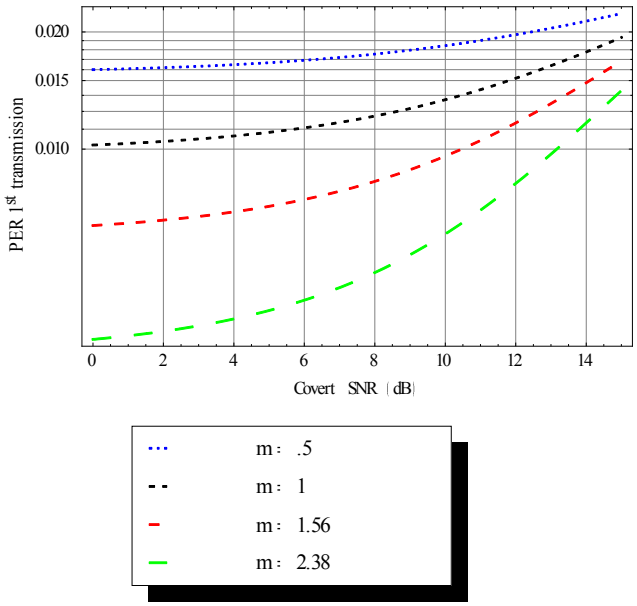


Fig. 5.11. PER of 1st transmission of target system resource block for increasing covert power.

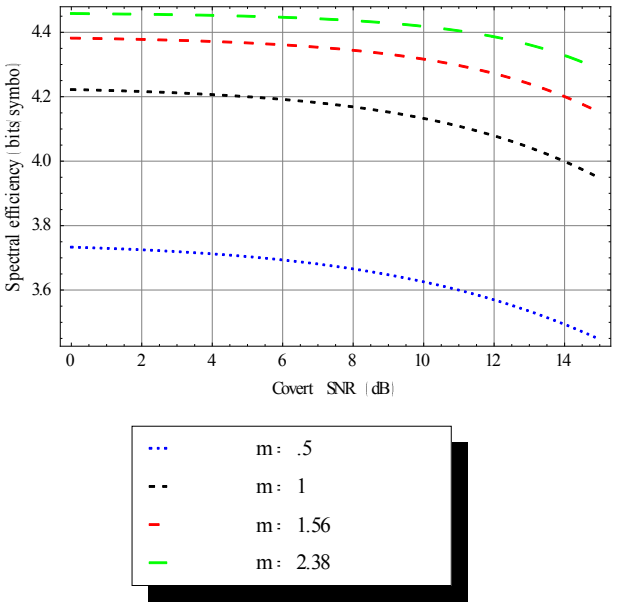


Fig. 5.12. Spectral efficiency of target system resource block for increasing covert power with $N_r^{max} = 3$.

vi. Comparing Hybrid and Truncated ARQ

This comparison will address the question of which ARQ type is less susceptible to interference. Fig. 5.13 and Fig. 5.14 each show the same four scenarios; truncated and hybrid ARQ are both shown with and without a 5 dB average SNR covert. While it is clear from these figures that HARQ has superior performance to TARQ, i.e., lower PER and higher spectral efficiency, they also show that hybrid ARQ is less impacted by the interference than truncated ARQ. It is to be noted that in order to allow for a fair comparison of the two ARQ modes that the SNR mode switching thresholds, γ_n, were held constant for both analysis. It can be easily understood that hybrid ARQ is expected to have superior performance due to the benefit of previous information whereas truncated ARQ discards the information from previous packet transmissions.

The comparisons of Fig. 5.13 show that the PER of the HARQ system is impacted less by the interference than the truncated system. The PER for HARQ increases by an average of approximately $2\text{x}10^{-3}$ while truncated ARQ has an average PER increase of $8\text{x}10^{-3}$ when covert SNR is 5 dB for the ranges in Fig. 5.13 and approximately $2\text{x}10^{-2}$ for HARQ and $4\text{x}10^{-2}$ for TARQ when the covert SNR is 15 dB. While Fig. 5.14 shows that HARQ has higher spectral efficiency, interference did not adversely impact one type of ARQ over the other with any noticeable significance. Figs. 5.13 and 5.14 show the calculated difference between the PER with and without covert interference of 5 and 15 dB, respectively, for both ARQ modes; Figs. 5.13 and 5.14 show that HARQ is less impacted by interference for all

SNRs in the plotted range. The difference in PER is shown in Figs. 5.15 and 5.16 and is defined as

$$\Delta PER(\bar{\gamma}, \bar{\gamma}_c, m) = PER(\bar{\gamma}, No\ interference, m) - PER(\bar{\gamma}, \bar{\gamma}_c, m). \quad (39)$$

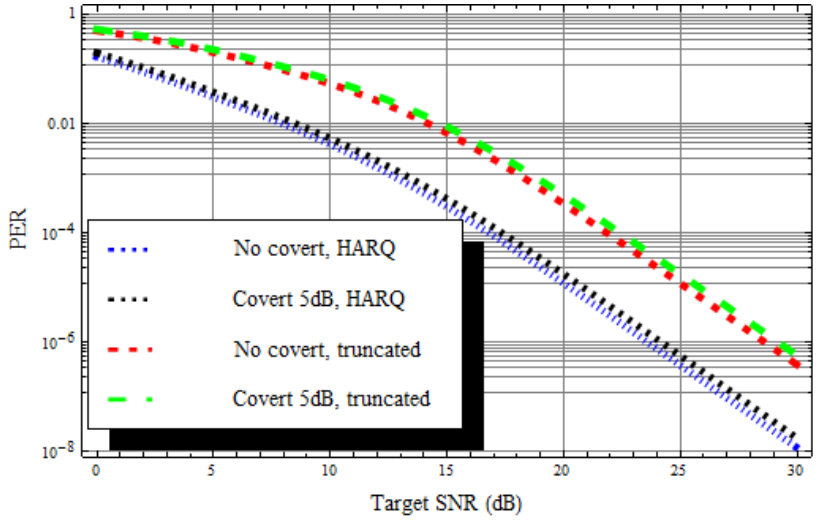


Fig. 5.13. PER of target system with average covert SNR = 5 dB for truncated and hybrid ARQ, Rayleigh fading (m = 1).

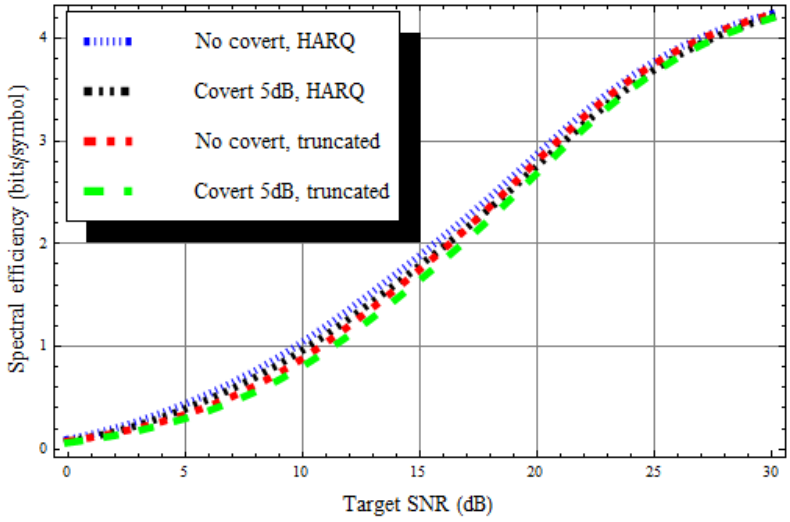


Fig. 5.14. Spectral efficiency of target system with average covert SNR = 5 dB for truncated and hybrid ARQ, m = 1.

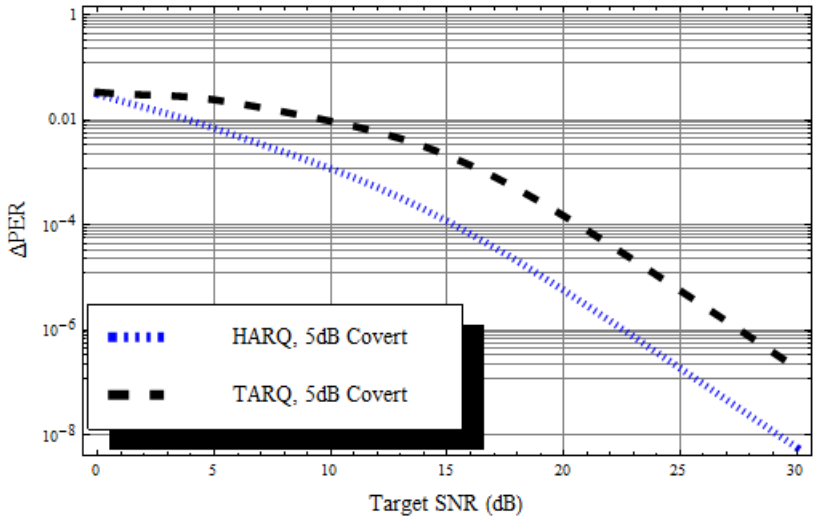


Fig. 5.15. Difference of PER of target system with covert SNR=5 dB for truncated and hybrid ARQ, m = 1.

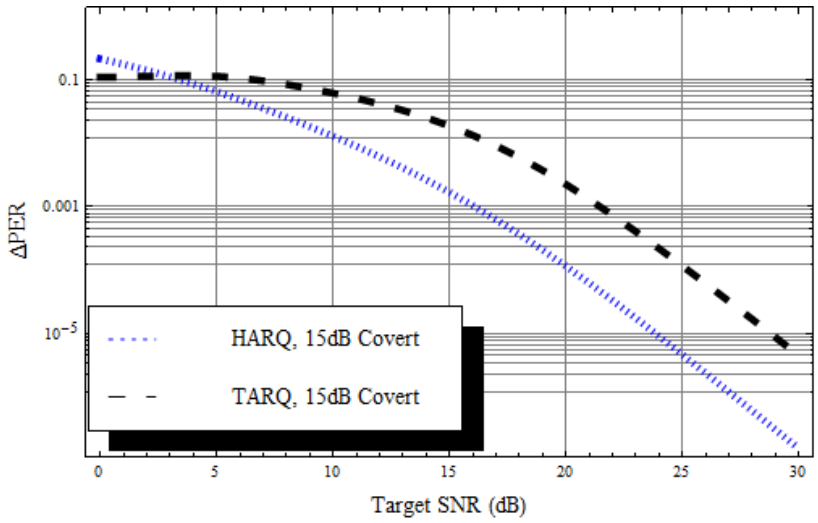


Fig. 5.16. Difference of PER of target system with covert SNR=15 dB for truncated and hybrid ARQ, $m = 1$.

Figs. 5.15 and 5.16 allow us to compare the impact of interference on a target system for that utilizes TARQ versus a system with HARQ in terms of the change in PER. We can see that for 5 or 15 dB interference SNR that the change in the PER of TARQ is consistently worse than HARQ.

vii. Conclusions

The work in this chapter demonstrated the impact of interference from a covert link on a target wireless packet based (infrastructure) system, such as LTE, at the data-link layer. These systems employ OFDM, AMC, and ARQ. The analysis presented here assumed independent Nakagami-*m* fading for both the covert and target link with a shared *m* parameter. The impact of the interference was quantified by the PER and spectral efficiency of the target system. The results show that the change in target system performance is small when a covert link having low power is

present (5 dB) when compared to no interference. The performance tradeoff between target and covert system was shown for different *m* fading parameter, i.e., different fading environments. These results show that for ARQ the channel fading impacts target system performance more than interference from the covert signal. This can render the interference practically indistinguishable from fading when performance at the data-link layer is considered. Results were also presented that compare systems that utilize hybrid ARQ to systems that utilize truncated ARQ in terms of PER and spectral efficiency. It was found that HARQ systems are better candidates than TARQ systems for exploitation by a covert link. This is due to the PER of HARQ systems being impacted less than truncated ARQ systems. Note HARQ is more commonly used and is deployed in LTE [49]. The work presented here in general considers an important aspect of the exploitation of 4^{th} generation wireless networks for covert communication; the impact on the target system. Next, we consider the covert link and its impact on the higher layers of the target system, specifically performance with a finite queue.

Chapter 6

Finite Length Queue

In this chapter we show the impact of interference generated by a covert link on the performance of a packet based (infrastructure) wireless network with a finite length queue. LTE infrastructure networks employ OFDM, AMC, and HARQ to allow them to achieve higher data rates and increase capacity; the adaptive characteristics of these networks make them susceptible to exploitation. Previous chapters have shown the impact of interference from a covert link on infrastructure networks at the physical layer in terms of BER and PER. The work here measures physical layer performance in terms of average spectral efficiency (ASE) and the queue's performance is measured in terms of throughput and packet loss rate versus increased covert signal power while assuming both signals are subject to independent Nakagami-*m* fading. The performance of the queue is shown to be practically

indistinguishable from channel fading when HARQ is utilized. The presented results aid in answering the question of what impact will a covert link that uses the guard band of the target down-link system have on said system.

A. The Impact of a Covert Interferer on an Adaptive Modulation and Coding System with Hybrid ARQ and a Finite Queue

i. Introduction

The work in chapter 4 addressed the interaction between the covert and target signals at the physical layer and quantified the performance of both by measuring the uncoded BER. The work in chapter 5 measured the impact of the covert signal on the target network's performance at the data-link layer; the target network utilized OFDM, AMC, and ARQ. It is to be noted that while the analysis presented here models a covert system as the source of interference, the analysis is general and can be applied to any type of interference, i.e., intentional, unintentional, co-channel, or adjacent channel interference.

ii. System Design and Assumptions

Many of the assumptions here follow from chapter 5. An example of the system considered for exploitation by the covert link is seen in Fig. 6.1. Here a wired network distributes information to base stations serving the users in each cell. Packets from the wired network arrive at the base station queue and are then transmitted through a wireless link to the user equipment (UE). The protocol layers of this communication system are shown below the various system components in Fig. 6.1.

Packets and frames are utilized as the units of transmission at the data-link and physical layers, respectively. The queue at base station, which serves the UE, operates in first-in-first-out (FIFO) mode. We assume a single transmit antenna at the base station and a single receive antenna at the UE.

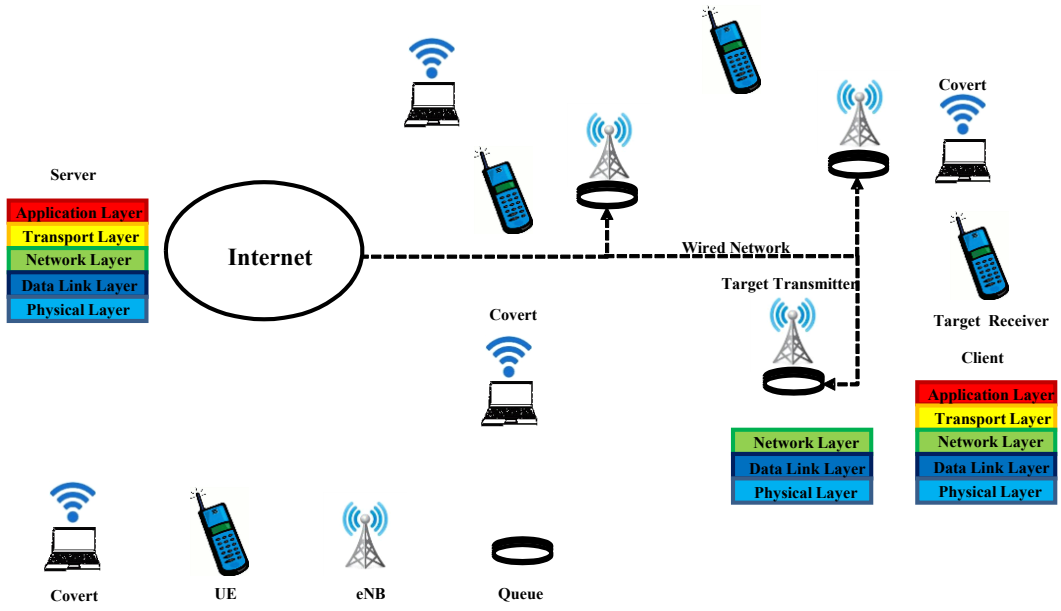


Fig. 6.1. Target and covert networks.

4th generation and beyond wireless networks, such as LTE, implement AMC at the data-link layer [49]. The system proposed here utilizes AMC by selecting one of the available MCS that meets a performance standard while also maximizing throughput over the wireless channel. The selection of a particular MCS is based upon the SNR at the receiver which is sent to the transmitter through a feedback channel. Cross-layer design as in [24-27] is implemented through the utilization of CSI, the received SNR, to select the MCS at the physical layer. Type II hybrid-ARQ with Chase Combining (CC) [52] is used at the data-link layer to recover from packet

errors over the wireless link.

We adopt the physical layer and data-link layer assumptions from Chapter 5. Following [26, 27], a finite state Markov chain (FSMC) channel model is adopted here in order to analyze the performance of the queuing system located at the base station as in Fig. 6.1. A channel is in state n when the received SNR lies between $\gamma \in [\gamma_n, \gamma_{n+1})\}$. By adopting a slowly varying wireless channel, the channel only transitions to an adjacent channel state and the probability the channel will transition two or more states is zero. The queue operates in FIFO mode and is a finite length queue. Arriving packets are dropped if the queue is full.

The system considered here is comprised of both wired and wireless channels. However, performance is dominated by the wireless channel. Therefore, our analysis will focus on the wireless link.

iii. Performance Analysis

We focus our analysis on the performance related to packet overflow loss at the queue and not system delay. As in [26], the queue serves only one traffic flow, the wireless down-link channel between the base station and the UE as in Fig. 6.1. The system here differs from the system in [26] through the use of HARQ as opposed to truncated-ARQ for recovery from packet errors, a 12 sub-carrier link as opposed to HiperLAN, and the presence of interference induced by the covert link. Packets at the queue are grouped together in frames for transmission over the wireless channel. The number of packets per frame relates the queue server state to the selected modulation

and coding rate R_n (bits/symbol) according to

$$c_n = b\, R_n, \tag{40}$$

where c_n is the queue server state and b is the number of packets per frame per designer's choice. One frame is transmitted per server time unit, T_f, and is the time unit throughout this analysis. Therefore, the queue server state is also dependent upon the channel condition.

The average received SNR with interference, $\bar{\gamma}_r$, is calculated by

$$\bar{\gamma}_r = E[\gamma] = \int_0^\infty \gamma f_\gamma(\gamma) d\gamma, \tag{41}$$

where interference from the covert link is included in $f_\gamma(\gamma)$. It is through $\bar{\gamma}_r$ that part of the impact of the interference is included. Thus the following analysis, directly from [26], can be applied here. The analysis from [26] is included here to highlight its assumptions and applicability to this research. By adopting a FSMC channel model, the cross-rate mode n of the channel is estimated as [54, eq. (17)]

$$N_n = \sqrt{2\pi \frac{m\gamma_n}{\bar{\gamma}_r}} \frac{f_d}{\Gamma(m)} \left(\frac{m\gamma_n}{\bar{\gamma}_r}\right)^{m-1} exp\left(-\frac{m\gamma_n}{\bar{\gamma}_r}\right), \tag{42}$$

where m is the fading parameter and f_d is the mobility induced Doppler spread. The cross-rate mode assumes a Nakagami-m fading channel model and does not account for the interference. Development of a cross-rate mode for a channel that includes the interfering link is beyond the scope of the study here. We utilize (42) to simplify the analysis of the queue performance.

Recall that the probability of the channel exceeding two consecutive states is

zero. The adjacent-state transition probability is calculated as [55, eqs. (5) and (6)]

$$P_{n,n+1} = \frac{N_{n+1}T_f}{\Pr(n)}, \quad if\ n = 0, \dots, N-1$$

$$P_{n,n-1} = \frac{N_n T_f}{\Pr(n)}, \qquad if\ n = 1, \dots, N. \tag{43}$$

The probability of remaining in the same state n is determined by [56]

$$P_{n,n} = \begin{cases} 1 - P_{n,n+1} - P_{n,n-1}, & if\ 0 < n < N \\ 1 - P_{0,1}, & if\ n = 0 \\ 1 - P_{N,N-1}, & if\ n = N. \end{cases} \tag{44}$$

Therefore following [26], the channel is modelled as a FSMC with an $(N + 1) \times (N + 1)$ state transition matrix defined to be

$$\boldsymbol{P_c} = \begin{bmatrix} P_{0,0} & P_{0,1} & \cdots & 0 \\ P_{1,0} & P_{1,1} & P_{1,2} & \vdots \\ 0 & \ddots & \ddots & 0 \\ \vdots & P_{N-1,N-2} & P_{N-1,N-1} & P_{N-1,N} \\ 0 & \cdots & P_{N,N-1} & P_{N,N} \end{bmatrix}. \tag{45}$$

Next, the packet arrivals at the queue as in [26], the service process, and the queue state are considered. The maximum number of packets that can be held by the finite length queue is defined by the variable Q. The probability of a packet being dropped due to overflow or blocking, P_d, can be found using the analysis in [26].

Here the packet arrival process is assumed to be Poisson and stationary with $E\{A_t\}=\lambda T_f$, where λT_f represents the number of packets arriving at the queue per server time unit. The packet arrival rate is independent of the queue and server state. The probability of a arrivals in T_f seconds is then as [57, pp. 164]

$$P(A_t = a)\begin{cases}\frac{(\lambda T_f)^a \exp(-\lambda T_f)}{a!}, & if\ a \geq 0\\ 0, & otherwise\end{cases}. \quad (46)$$

As in [26] C_t (packets/time unit) is the number of packets transmitted by the AMC system at the start of T_f which correspond to mode n. This means $C_t \in \mathrm{C}, \mathrm{C} \coloneqq \{c_0, c_1, \dots, c_N\}$.

The next step in the analysis from [26] is finding the joint stationary distribution of the queue and server states. Let (U_{t-1}, C_t) represent the pair of queue and server states, and $P_{(u,c),(v,d)}$ denote the transition probability from ($U_{t-1} = u$, $C_t = c$) to ($U_t = v$, $C_{t+1} = d$), where (u, c) $\in U \times C$, and (v, d) $\in U \times C$ [26]. The state transition probability matrix has the form

$$\boldsymbol{P} = \begin{bmatrix} \boldsymbol{A_{0,0}} & \boldsymbol{A_{0,1}} & \cdots & \boldsymbol{A_{0,K}} \\ \boldsymbol{A_{1,0}} & \boldsymbol{A_{1,1}} & \cdots & \boldsymbol{A_{1,K}} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{A_{K,0}} & \boldsymbol{A_{K,1}} & \cdots & \boldsymbol{A_{K,K}} \end{bmatrix}, \quad (47)$$

where the submatrix $\boldsymbol{A_{u,v}}$ is defined in [26, eq. (20)] as

$$\boldsymbol{A_{u,v}} = \begin{bmatrix} P_{(u,c_0),(v,c_0)} & \cdots & P_{(u,c_0),(v,c_N)} \\ \vdots & \ddots & \vdots \\ P_{(u,c_N),(v,c_0)} & \cdots & P_{(u,c_N),(v,c_N)} \end{bmatrix}. \quad (48)$$

$P_{(u,c),(v,d)}$ is simplified as [26, eq. (22)]

$$\begin{aligned} & P_{(u,c),(v,d)} \\ & \coloneqq P(U_t = v, C_{t+1} = d | U_{t-1} = u, C_t = c) \\ & = P(C_{t+1} = d | C_t = c) P(U_t = v | U_{t-1} = u, C_t = c) \\ & = P_{c,d} P(U_t = v | U_{t-1} = u, C_t = c). \end{aligned} \quad (49)$$

The last inequality follows from the fact that C_{t+1} only depends on C_t. $P(C_{t+1} = d|C_t =$

c) is found from the entries of $\boldsymbol{P_c}$. Based on the queue state recursion $U_t = \min\{Q, \max\{0, U_{t-1} - C_t\} + A_t\}$, The conditional probability is [26, eq. (19)]

$$P(U_t = v|U_{t-1} = u, C_t = c) = \begin{cases} P(A_t = v - \max\{0, u - c\}), & if\ 0 \le v < Q \\ 1 - \sum_{0 \le v < Q} P(U_t = v|U_{t-1} = u, C_t = c), & if\ v = Q. \end{cases} \quad (50)$$

The stationary joint distribution is defined as [26, eq. (24)]

$$P(U = u, C = c) \coloneqq \lim_{t \to \infty} P(U_{t-1} = u, C_t = c). \quad (51)$$

For notational convenience we let $\pi_{(u,c)} \coloneqq P(U = u, C = c)$ and the row vector is defined by [26, eq. (25)]

$$\boldsymbol{\pi} = [\pi_{(0,c_0)}, \dots, \pi_{(0,c_N)}, \dots, \pi_{(K,c_0)}, \dots, \pi_{(K,c_N)}]. \quad (52)$$

The stationary joint distribution is then computed using the standard method from the equality [57], [58]

$$\boldsymbol{\pi} = \boldsymbol{\pi P}, \quad \sum_{u \in U, c \in C} \pi_{(u,c)} = 1, \quad (53)$$

which means that $\boldsymbol{\pi}$ is the left eigenvector of $\boldsymbol{P}$ corresponding to the eigenvalue 1.

The packet dropping probability, P_d, can now be found as in [26, eq. (31)] according to

$$P_d \coloneqq \frac{E\{D\}}{\lambda T_f}, \quad (54)$$

where $E\{D\}$ is the average number of dropped packets and is calculated by [26, eq. (30)]

$$E\{D\} = \sum_{a \in A, u \in U, c \in C} \begin{bmatrix} \max\{0, a - Q + \max\{o, u - c\}\} \times \\ P(A = a) \times P(U = u, C = c) \end{bmatrix}. \quad (55)$$

The packet loss rate is an important measure of performance for the system queue and as in [26, eq. (13)] is given by

$$\varphi = 1 - (1 - P_d)(1 - P_0), \tag{56}$$

where P_0, calculated from (30), represents the probability a packet is received in error through the wireless channel. Here P_0 from (30) includes the effects of a system that utilizes type II HARQ-CC, with a limit of K transmissions per packet, and interference. It is through P_0 that part of the impact of the interference is included in the analysis. Note that [26] does not include interference or HARQ. Thus the interference impacts both P_d (via $\bar{\gamma}_r$) and P_0 (via the HARQ analysis). The throughput of the queuing system is related to the packet loss rate and as in [26, eq. (14)] defined to be

$$\beta = (\lambda T_f)(1 - \varphi) = (\lambda T_f)(1 - P_d)(1 - P_0). \tag{57}$$

ASE is another measure of system performance of interest. ASE quantifies the utilization of the system's wireless resources. We use the definition of ASE in [26, eq. (32)] to show the impact the covert interferer has on the target system's resources given by

$$\bar{S} = \sum_{u \in U, c \in C, c \neq 0} S(U = u, C = c) P(U = u, C = c). \tag{58}$$

The spectral efficiency given ($U = u$, $C = c$), is expressed as [26, eq. (33)]

$$S(U = u, C = c) = \begin{cases} R_n, & if\ c = c_n, u \geq c \\ \frac{u}{c} R_n, & if\ c = c_n, u < c. \end{cases} \tag{59}$$

iv. Numerical Results

We present results in this section based upon the analysis in the previous

section. We have previously shown that a covert interferer with $1/8^{th}$ the symbol rate of the target down-link system, 5 dB average transmitted SNR, and 4-QAM signaling achieved an uncoded BER of approximately 10^{-2}. The maximum number of HARQ transmissions for a packet, K, at the data-link layer is set to 3 for all figures. The modes and thresholds available to the AMC controller are given in Table II. We set the number of packets per frame $b = 4$ and the queue length $Q = 7$ *packets*. The frame time is $T_f = 0.01 seconds$. The maximum packet arrival rate is set to the maximum queue server state which is 1800 *packets/seconds* (c_5/T_f). The maximum data rate achievable by the resource block in question is 1.944 *Mbit/second* $((c_5 N_p)/T_f)$.

Figs. 6.2, 6.3, and 6.4 show the throughput, packet loss rate, and ASE, respectively for a fixed interference power as a function of target SNR. The dashed lines display the impact of the covert interferer on the target down-link system performance for m = 0.5, 1.0, 2.0, and 3.0. The solid line represents no interference and m = 1.0 (Rayleigh fading) for comparison. It can be seen that the dashed black line (5 dB interference, m = 1) follows the solid black line (no interference, m = 1) closely for all three figures. In fact, it can be deduced that changes in the channel parameter, m, impacts the performance of the target system more than the interferer at 5 dB.

The average transmit power of the target system in Fig. 6.5 was held constant at 26.15 dB based on the system's performance in Chapter 4. This allows us to view the impact of varying levels of interference from the covert link on the target system throughput. For a fading parameter of m = 2, the system throughput is maximum

(1800 *packets/second*) for average covert signal power less than 17 dB and for m = 3.0 less than 20 dB.

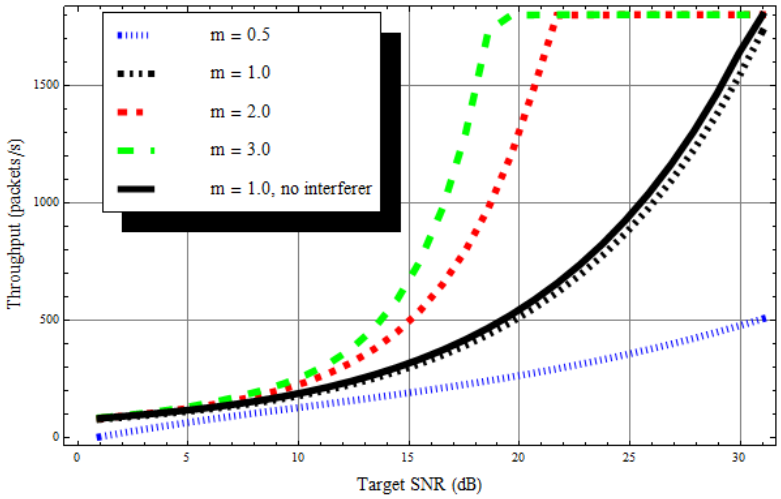


Fig. 6.2. Throughput of target system with average covert SNR = 5 dB, Nakagami-*m* fading.

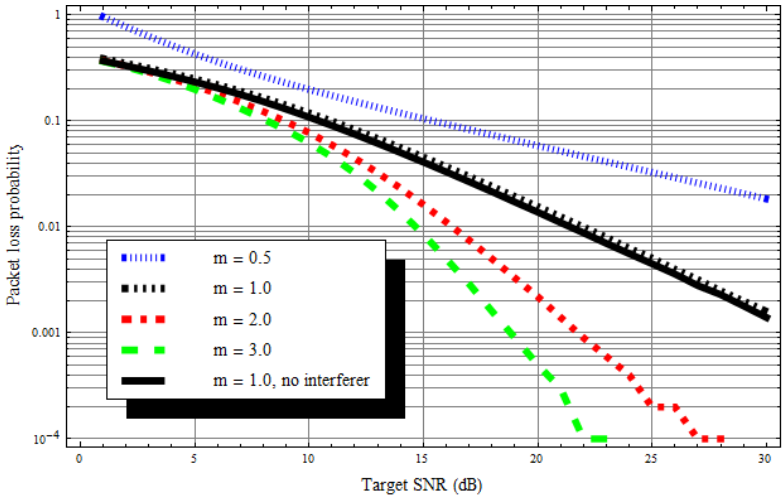


Fig. 6.3. Packet loss probability of target system with average covert SNR = 5 dB, Nakagami-*m* fading.

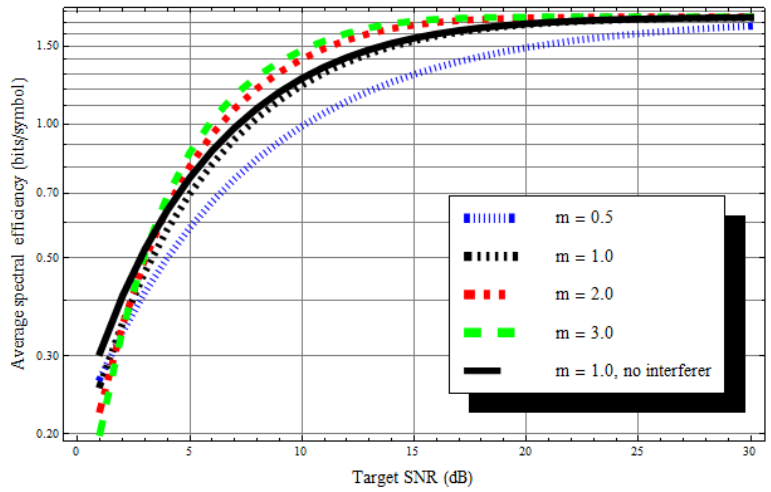


Fig. 6.4. Average spectral efficiency of target system with average covert SNR = 5 dB, Nakagami-*m* fading.

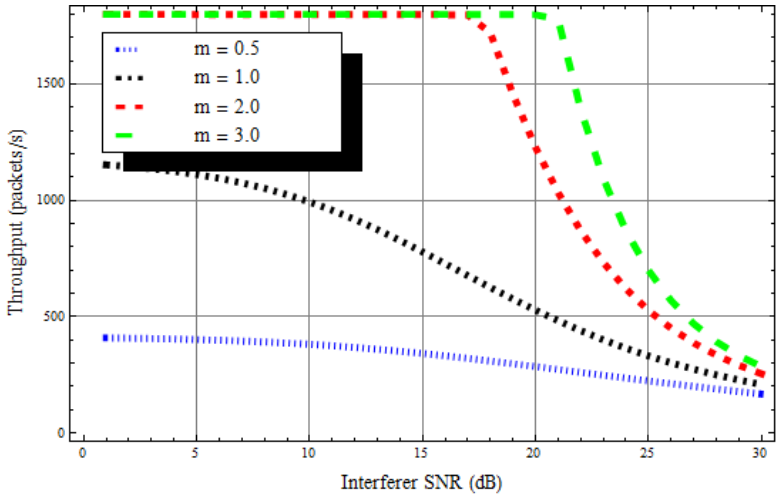


Fig. 6.5. Throughput of target system with average SNR = 26.15 dB vs. covert SNR, Nakagami-*m* fading.

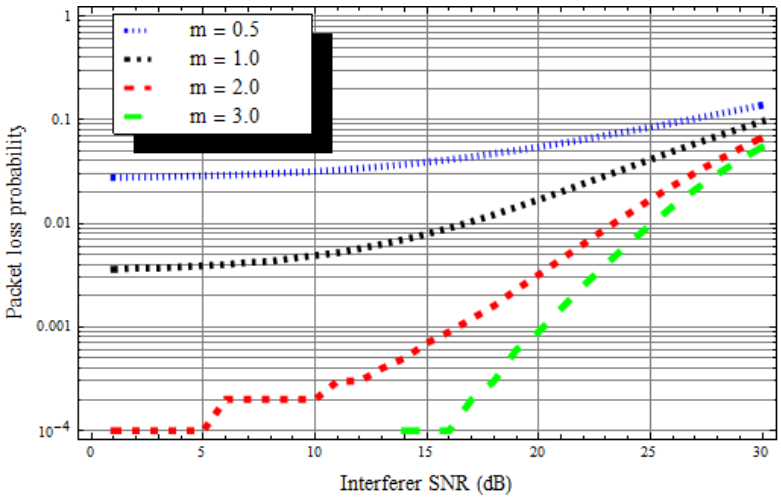


Fig. 6.6. Packet loss probability of target system with average SNR = 26.15 dB vs. covert SNR, Nakagami-*m* fading.

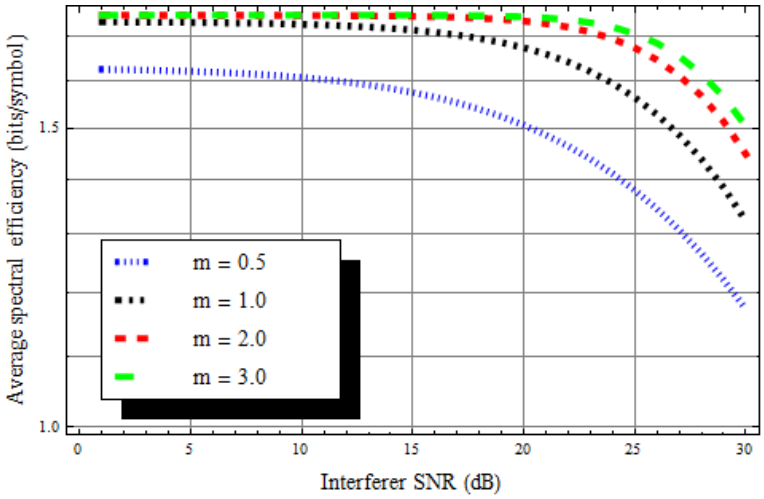


Fig. 6.7. Average spectral efficiency of target system with average SNR = 26.15 dB vs. covert SNR, Nakagami-*m* fading.

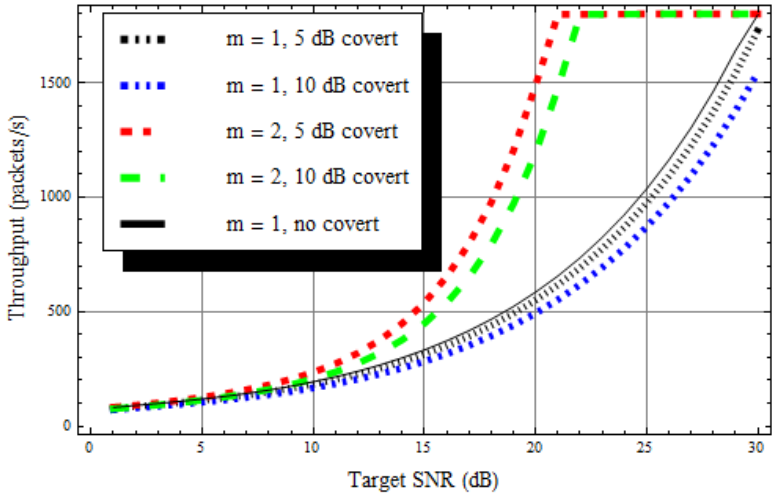


Fig. 6.8. Throughput of target system with varying covert SNR, Nakagami-*m* fading.

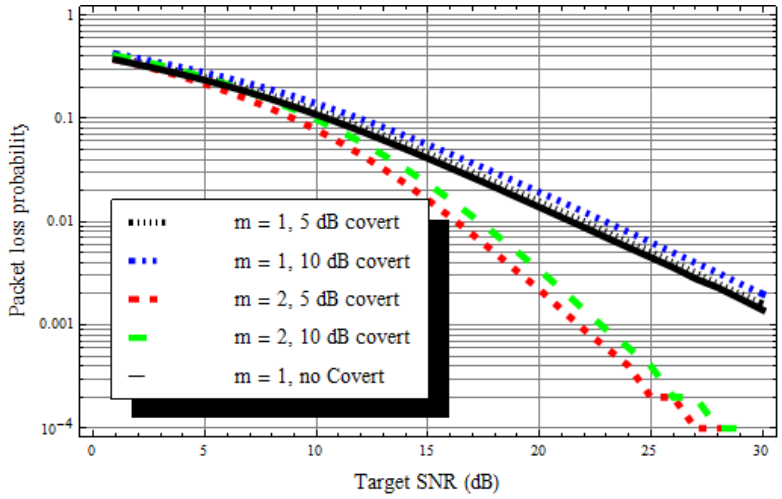


Fig. 6.9. Packet loss probability of target system with varying covert SNR, Nakagami-*m* fading.

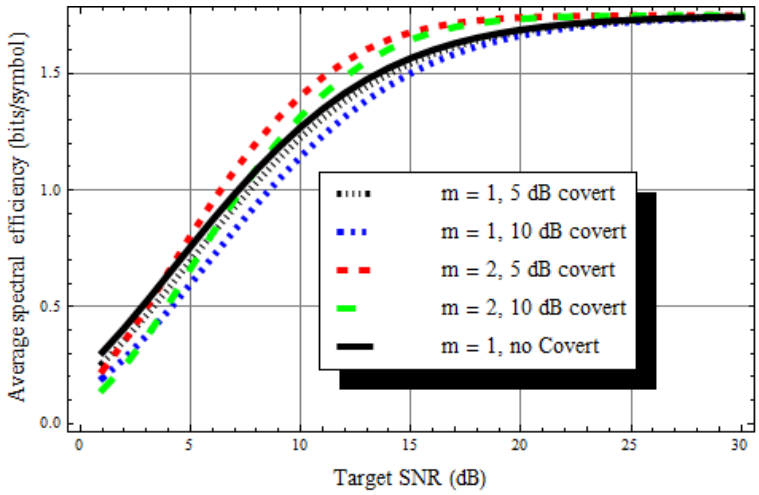


Fig. 6.10. Average spectral efficiency of target system with varying covert SNR, Nakagami-*m* fading.

The purpose of Fig. 6.8 is to compare the impact of fading to covert system power. It is clear from the results presented here that the impact of the interference on the target down-link system is not significant for the cases considered.

v. Conclusions

The work in this chapter demonstrated the impact of interference from a covert link on a target wireless packet based (infrastructure) system, including a system queue. The analysis presented here assumed independent Nakagami-*m* fading for both the covert and target link with a shared *m* parameter. The impact of the interference was quantified by throughput, ASE, and packet loss rate. The results show that the target system's queue performance with no interference is very similar when a covert link having low power is present. The performance tradeoff between target and covert system was shown for different *m* fading parameter, i.e., different

fading environments. These results show that the channel fading impacts target system performance more than interference from the covert signal. This can render the interference practically indistinguishable from fading when performance at the queue is considered. The work presented here in general considers an important aspect of the exploitation of 4^{th} generation wireless networks for covert communication; the impact on the target system. In more general terms, we have presented the impact of interference when the spectral characteristics and location of the interferer is known. The last chapter will determine the impact of the covert link on the transport layer.

Chapter 7

The TCP Layer

Several technologies have been added to wireless communication systems that increase reliability of these systems and afford them higher data rates. These new technologies when combined with the multiple layers of a communications network make the analysis of these systems increasingly complex. The work in this chapter analyzes the impact of placing a modulated interfering transmission in the guard band of a wireless packet based (infrastructure) network on the end user TCP performance. Wireless networks, such as LTE, employ at the physical layer OFDM and AMC while at the data-link layer they use HARQ and a finite length queue; they also utilize cross-layer optimization to improve performance. These protocols allow the wireless network the ability to adapt to an ever changing fading environment. The following work shows the effect of a modulated interfering signal in the guard band of an

OFDM system on the end-to-end TCP performance. In some cases the impact from the interference is indistinguishable from the effects of channel fading.

A. The Impact of Interference on an OFDM System with AMC, Hybrid ARQ, and a Finite Queue on End-to-End Performance

i. Introduction

The performance of the TCP of the internet protocol suite can be utilized to quantify the end user's experience as part of a wireless communications network (see Fig. 7.1). Interference at the physical layer of a wireless packet based (infrastructure) network degrades the user experience. The analysis presented here quantifies the impact of the interference on the end user in terms of TCP throughput, packet loss rate, and end-to-end delay.

There is significant pressure on wireless network resources due to the explosion of data usage by mobile devices. The ability to predict TCP layer performance of multi-carrier systems could lead to better spectrum and interference management. The main goal of the work in this chapter is to provide a blueprint for predicting TCP performance due to modulated interference at the physical layer and show that over a range of interference powers the end-to end performance impact of the interfering signal is indistinguishable from other wireless impairments, specifically fading.

The challenge in performing the analysis stems from the many layers of the internet protocol suite and the technologies utilized by each layer that maximize

throughput and increase reliability. The analysis must take into account all relevant layers impacted by the interference up to the TCP layer. The work here examines the interaction between the interfering signal and the target signal at the physical layer where OFDM and AMC are utilized to maximize spectral efficiency and adapt to an ever changing fading environment, respectively. This analysis considers HARQ at the data-link layer which is utilized to recover from packet errors caused by the wireless channel and a finite queue. We also take into account the cross-layer mechanisms.

Previous work has been done to analyze the impact of an interfering signal at lower network layers. The work in Chapter 4 found the BER of an uncoded multi-carrier system when subject to a fixed channel and interference at the physical layer. The work in chapter 4 also validated a method for estimating the average PER of a coded OFDM system when the signal is subject to interference with a shaped spectral density, i.e., where each sub-carrier in the OFDM system has a different SNR. The analysis in chapter 5 showed that the impact of interference generated by a covert link on the data-link layer of a packet based (infrastructure) wireless network with HARQ was indistinguishable from fading. A method for finding the average PER of a system with AMC and HARQ was presented in [28]. The work in [27] provides a method for analyzing the end-to-end TCP performance for a system with AMC and truncated-ARQ. The principle difference between the previous work in [24-27] and the work in this chapter is the inclusion of interference at the physical layer, HARQ at the data-link layer, and LTE resource block structure as opposed to HiperLAN. Therefore, the work here utilizes aspects of the aforementioned works to analyze the TCP

performance of a wireless network with OFDM, AMC, and HARQ with a finite length queue when subjected to interference from a signal with a shaped spectral density placed in the guard band of the OFDM target signal.

ii. System Design and Assumptions

We adopt the target and interfering covert systems from chapter 6. The TCP Reno mechanism is utilized at the transport layer with the triple-duplicate acknowledgement (ACK) for congestion control [59]. Following [27], we utilize a fixed point procedure to analyze the end-to-end TCP performance which couples the TCP with AMC. The coupling of these two mechanisms maximizes TCP throughput by optimizing the target PER which the TCP throughput is related to [60]. The TCP Reno "congestion control" mechanism is utilized at the TCP layer of both the target server and client as in [59]. We assume only triple duplicate ACK based congestion control for the analysis.

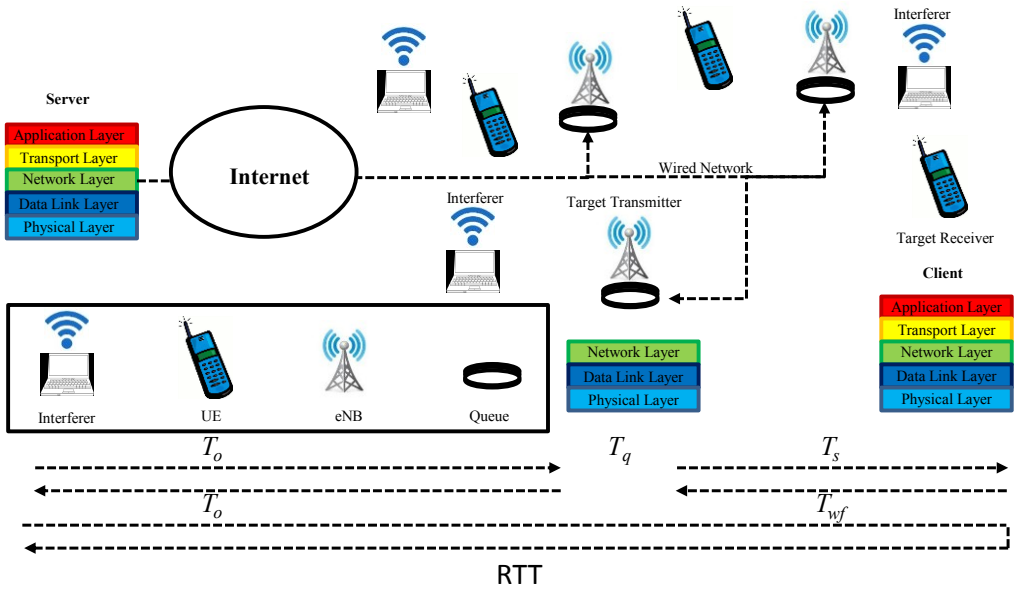


Fig. 7.1. Target and covert networks with TCP parameters.

iii. Performance Analysis

Following the analysis from the previous chapter, we use a recursive algorithm from [27] to find the average TCP performance of the target system with interference. The initial value for the TCP sending rate, β, is set to the maximum server state $c_5 = bR_5$. The TCP segment sending rate is approximated by [59, eq. (30)]

$$\beta = \frac{1}{RTT}\sqrt{\frac{3}{2b\varphi}}, \tag{60}$$

where the RTT is the average end-to-end round-trip-time and b is the number of packets/segments served by a frame per server time unit (T_f) and confirmed by an ACK. The segment loss rate, φ, is from by (56). Unlike the analysis in [26], here φ includes the effects from the interfering signal. In [27, eq. (15)] the TCP throughput

is defined as

$$\eta = \frac{1-\varphi}{RTT}\sqrt{\frac{3}{2b\varphi}}. \tag{62}$$

Following [61, eq. (22)], the RTT is approximated as

$$RTT \approx 2T_0 + T_{wl} + T_{wf}, \tag{63}$$

where $2T_0$ is the average 2-way delay over the wireline connection, T_q is the average waiting time of a segment in the base station queue, T_s is the average transmission time per segment over the wireless channel, and T_{wf} is the feedback delay as in Fig. 7.1. It is assumed that T_0 and T_{wf} are known constants and $T_{wl} \coloneqq T_q + T_s$. This leaves T_{wl} to be determined by the wireless link model as in [27]. As in [27, eq. (22)], the average delay per segment is found by

$$T_{wl} = \frac{N_{wl}}{\beta(1-P_d)}. \tag{64}$$

The average number of segments in the wireless link is found according to [27, eq. (21)]

$$N_{wl} = \sum_{u\in U, c\in C} u \cdot P(U = u, C = c) + \sum_{u\in U, c\in C} \min\{u, c\} \cdot P(U = u, C = c), \tag{65}$$

where the stationary distribution of the queue and server states, $P(U = u, C = c)$, is calculated according to the method outlined in [26]. However, in this work interference is also accounted for in the calculation of N_{wl}. The algorithm from [26] starts by setting the ensemble average packet arrival rate, λ, equal to the TCP segment sending rate, $\lambda = \beta$. The stationary distribution is found from the procedure outlined

in [26] which is then utilized to find P_d and N_{wl}. The average delay per segment is then calculated using (64) and the RTT is found according to (63). Finally, an updated value for the TCP segment sending rate is calculated by (60). This process is repeated until the sending rate converges.

Typically, this algorithm converges after several iterations. However, for a minority of high SNR cases an additional step is needed for convergence; after a predetermined number of iterations, e.g. 100, the new TCP segment sending rate is adjusted according to

$$\beta_{j_{new}} = \begin{cases} (1-x)\beta_j, & \beta_j > \lambda \\ (1+x)\beta, & \beta_j \leq \lambda' \end{cases} \tag{66}$$

where $\beta_{j_{new}}$ represents the updated TCP sending rate on the j^{th} iteration and we set the value of x = 0.01**floor*(j/100). Here the *floor*(·) function rounds the resulting fraction down to the nearest integer.

iv. Numerical Results

The TCP throughput, RTT, and packet loss rate results presented in this section consider the physical layer interaction between target and interfering signals, AMC, HARQ, and the finite queue at the base station. Values for T_f, T_{wf}, T_0, and f_d are taken from [27] and the results in the figures below are based on the parameters in Table III.

TABLE III

SYSTEM PARAMETER VALUES

Parameter	Value
b (packets/frame)	4
K (HARQ parameter)	3
T_f (ms)	10
T_{wf} (ms)	3
T_0 (ms)	50
f_d (Hz)	1
Q (queue length-packets)	7

In the following analysis we compare results of four different m fading parameters. Measurement of channel characteristics at 900 MHz in an urban environment were reported in [46] where the most likely values of m ranged from 0.5 to 3.5 with an average of m= 1.56. While in [47] m= 2.38 was reported at 870.9MHz in an urban environment. However, m= 1.56 and 2.38 are incompatible with the method of calculation used here. Thus values of m = 0.5, 1.0, 2.0, and 3.0 were selected which covers the range of m measured in [46] and [47]. For the cases where the interference power is varied we fix the average target SNR at 26.15 dB; at this SNR an uncoded 16-QAM system in Rayleigh fading (m=1) has a BER = 10^{-3}.

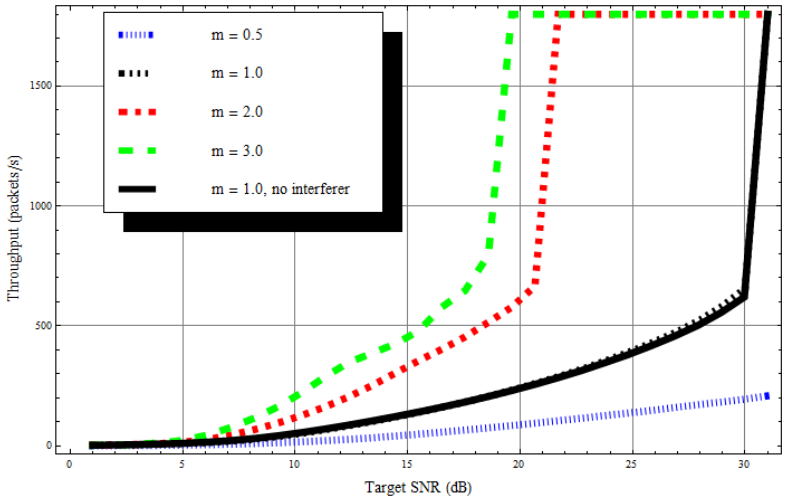


Fig. 7.2. Throughput of target system, Nakagami-*m* fading, interferer SNR = 5dB.

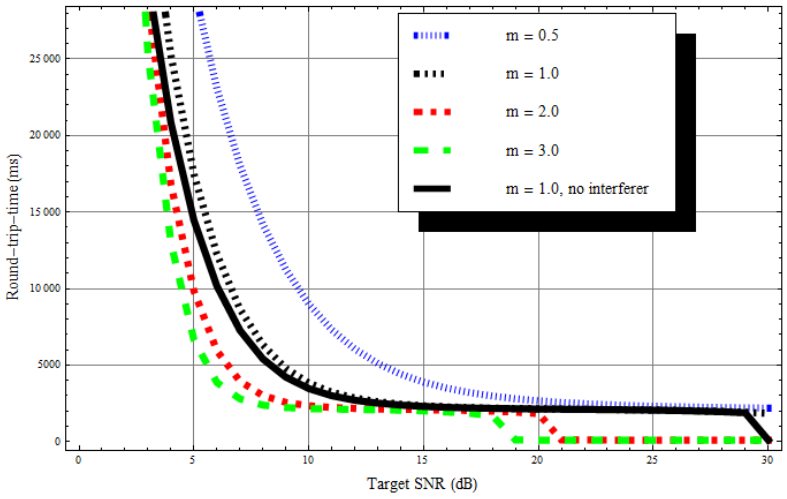


Fig. 7.3. Round-trip-time of target system , Nakagami-*m* fading, interferer SNR = 5dB.

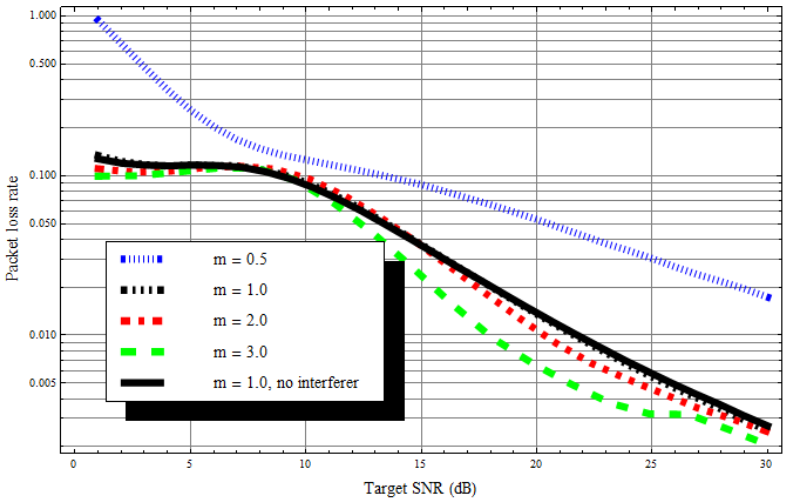


Fig. 7.4. Packet loss rate (φ) of target system , Nakagami-*m* fading, interferer SNR = 5dB.

Fig. 7.2 gives throughput of the target system with an average interferer SNR of 5 dB; throughput of the target system with no interference and fading parameter *m*= 1.0 is included for comparison. Fig. 7.3 shows the RTT and Fig. 7.4 shows packet loss rate for the same parameters. We can see that the performance of the target system improves while the target SNR increases as expected and as the fading parameter increases. There is only a small difference in performance between the scenarios with *m*= 1.0 with and without interference. It is clear from Figs. 7.2, 7.3, and 7.4 that a change in fading parameter of 1.0 has a greater impact on performance than an interfering signal with average SNR of 5 dB. We can see that the throughput reaches the maximum sending rate at the same point the RTT achieves a minimum. Recall that the maximum TCP sending rate is limited by the maximum server rate (1800 *packets/second*) and the minimum RTT is limited to twice the delay over the wireline ($2T_0$) plus the feedback delay of the ACK over the wireless channel (T_{wf}) for

a total of 103 milliseconds.

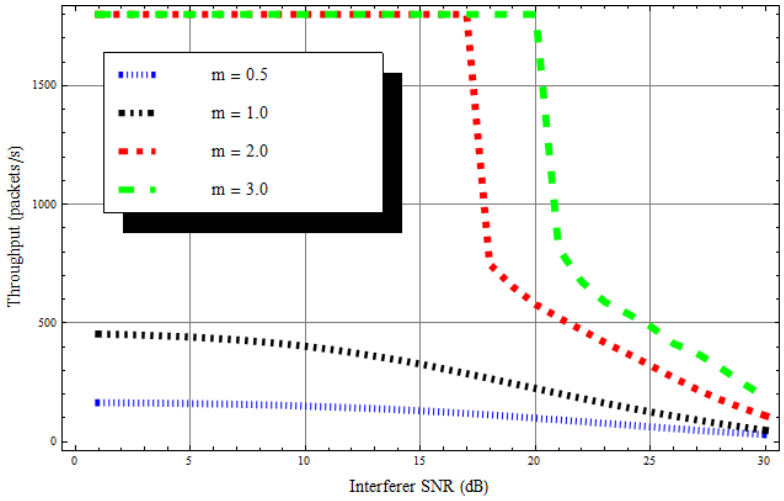


Fig. 7.5. Throughput of target system SNR= 26.15 dB vs. variable interferer SNR, Nakagami-*m* fading.

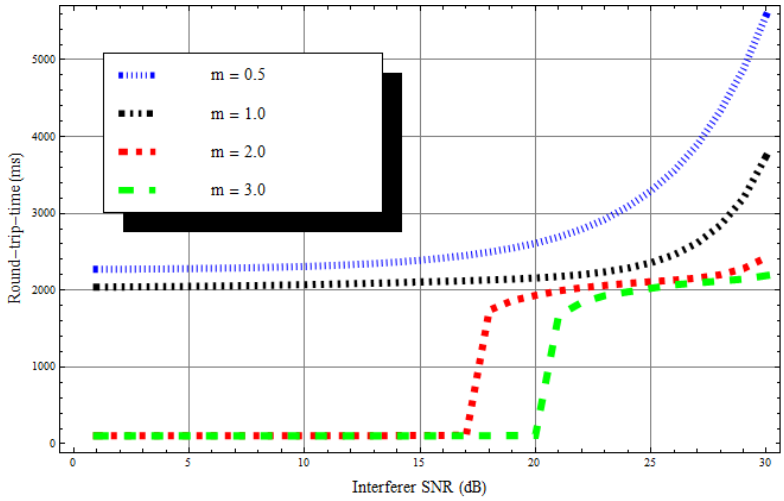


Fig. 7.6. Round-trip-time of target system SNR= 26.15 dB vs. variable interferer SNR, Nakagami-*m* fading.

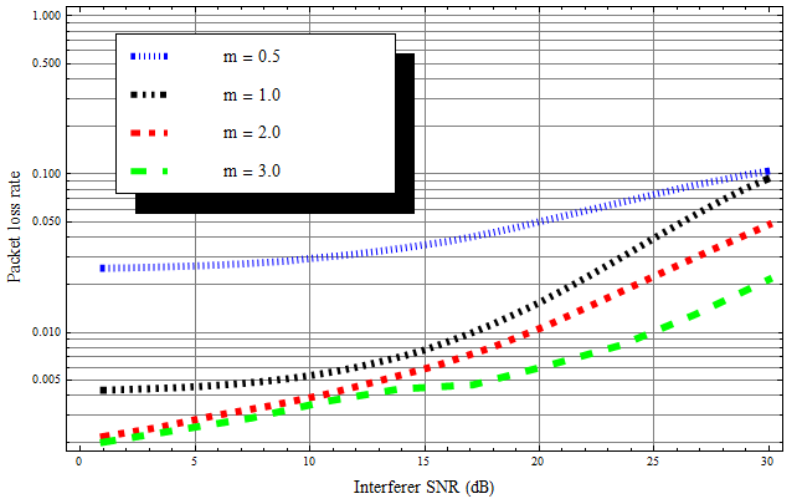


Fig. 7.7. Packet loss rate (φ) of target system SNR= 26.15 dB vs. variable interferer SNR, Nakagami-*m* fading.

The second case considered holds the average target SNR at 26.15 dB while the interfering SNR ranges from 1 to 30 dB. This allows us to see the impact of increasing the interference power on the target system. Figs. 7.5 and 7.6 show that for scenarios with m= 0.5 and 1.0 the maximum TCP sending rate and minimum RTT are never achieved while for cases with m= 2.0 and 3.0 the maximum TCP sending rate and minimum RTT are no longer met after approximately 17 and 20 dB interfering SNR, respectively. Fig. 7.7 provides the packet loss rate. We observe that throughput and RTT are adversely affected by the interference power with little impact on the packet loss rate. We deduce that the tradeoff in introducing the interference lies in lower target system throughput due to the increased likelihood of a lower AMC mode, i.e., a lower transmission rate, to meet the packet error rate requirement of the cross-layer optimization process.

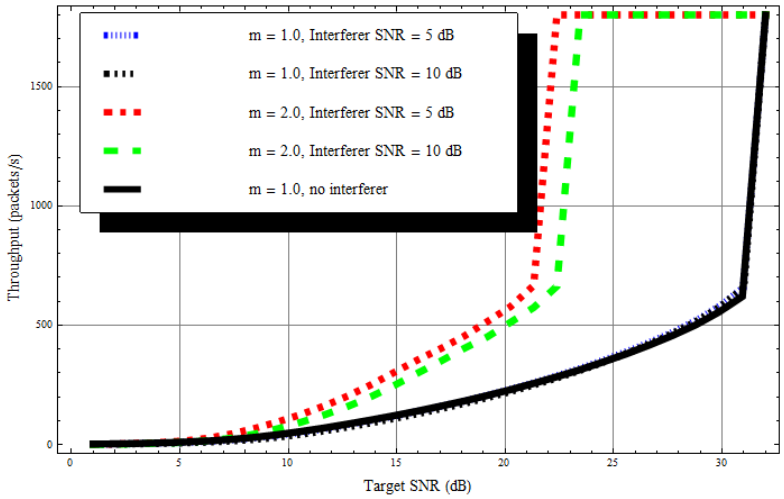


Fig. 7.8. Throughput of target system for interferer SNR 5 and 10 dB, Nakagami-*m* fading.

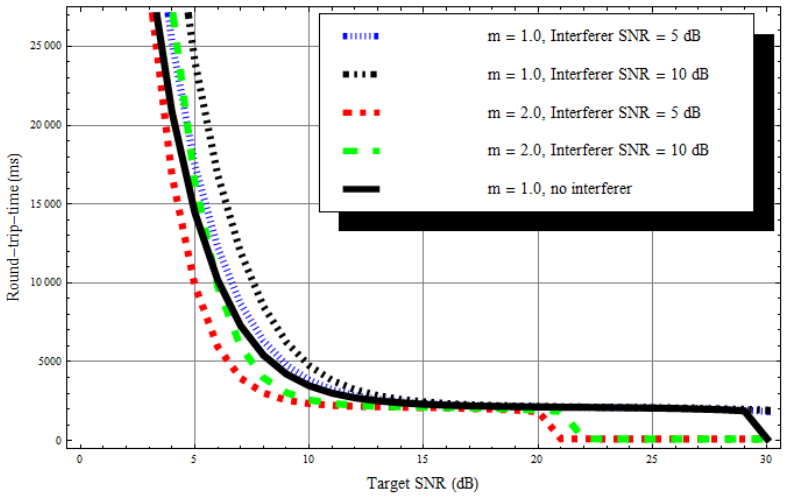


Fig. 7.9. Round-trip-time of target system for interferer SNR 5 and 10 dB, Nakagami-*m* fading.

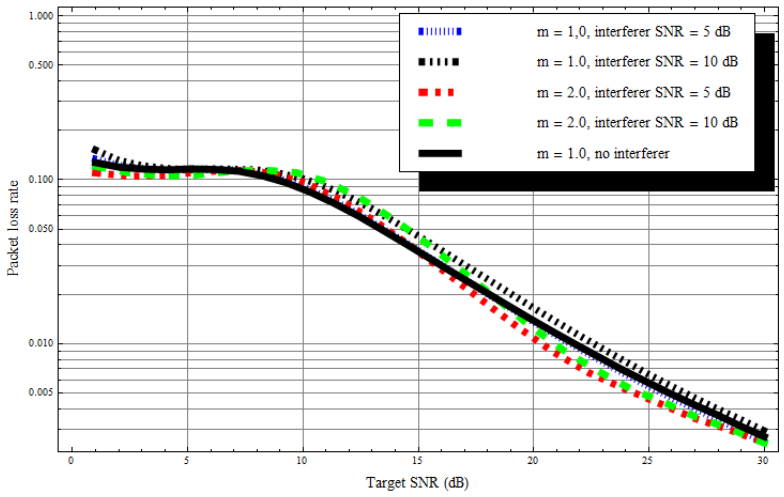


Fig. 7.10. Packet loss rate (φ) of target system for interferer SNR 5 and 10 dB, Nakagami-*m* fading.

Figs. 7.8, 7.9, and 7.10 allow us to more directly compare the impact of increasing the interference power from 5 to 10 dB to an increase of *m* from 1.0 to 2.0 and from 2.0 to 3.0. By comparing the throughput and RTT of the case with *m*= 1.0 and an interfering SNR of 10 dB to the systems with *m*= 2.0 and interfering SNR of 5 dB we can see that decreasing *m* from 2.0 to 1.0 reduce the performance more than an increase of 5 dB in the interference. Specifically, when the target SNR is 15 dB, the TCP throughput with *m*= 1.0 with 5 dB interference and without interference is 135 and 140 *packets/s*, respectively, whereas when *m*= 2.0 and 5 dB interference the throughput is 355 *packets/s*.

Figs. 7.11, 7.12, and 7.13 show the sensitivity of interference versus fading. We define the throughput from (11), η, as a function of the target SNR, interference SNR, and the fading parameter m, $\eta(SNR_{Tar}, SNR_{Int}, m)$, and define the change in throughput, $\Delta\eta$, for two different cases as

$$\Delta\,\eta_{m_1,m_2}(SNR_{Tar}) = \eta(SNR_{Tar}, NI, m_1) - \eta(SNR_{Tar}, NI, m_1 - m_2),$$

$$\Delta\,\eta_{m,Int}(SNR_{Tar}) = \eta(SNR_{Tar}, NI, m) - \eta(SNR_{Tar}, SNR_{Int}, m), \qquad (67)$$

where *NI* is the no interference case. The two definitions of $\Delta\eta$ allow us to directly compare the impact of changing the interference power with the impact of changes in fading environment for a range of target SNR. We observe from Figs. 7.11-13 that the change in throughput caused by a change in *m* is consistently greater than the change in throughput which results from a change in interference power.

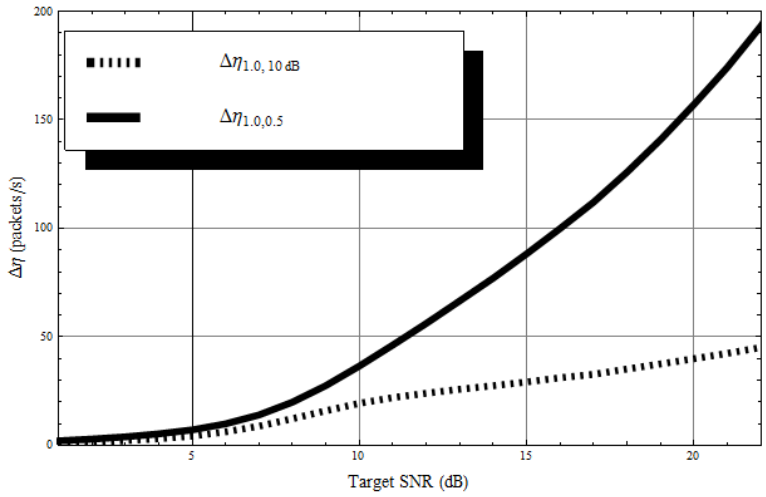


Fig. 7.11. Change in throughput ($\Delta\eta$) of target system, $\Delta\eta_{1.0,0.5}$ compared to $\Delta\eta_{1.0,10\ dB}$.

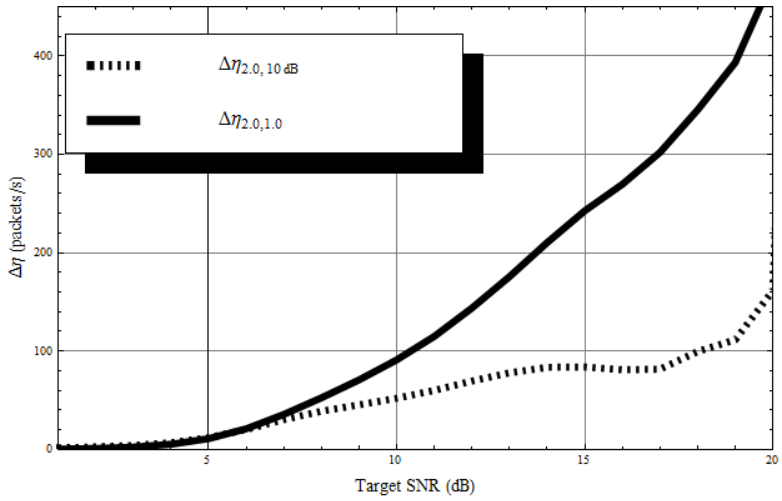


Fig. 7.12. Change in throughput ($\Delta\eta$) of target system, $\Delta\eta_{2.0,1.0}$ compared to $\Delta\eta_{1.0,10\ dB}$.

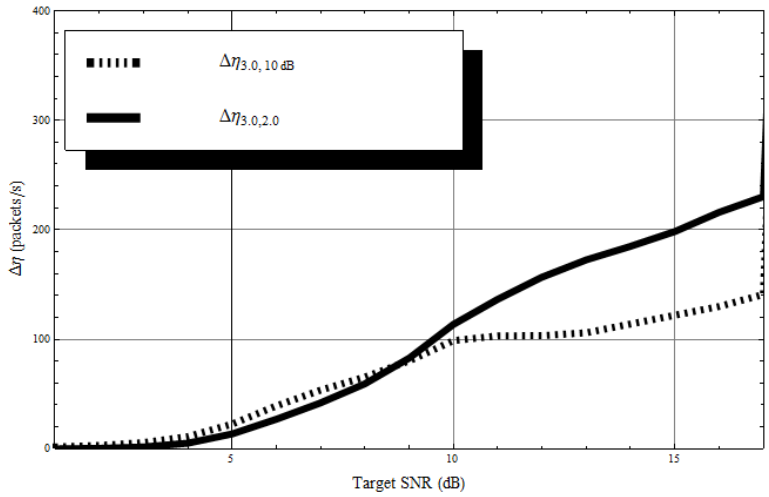


Fig. 7.13. Change in throughput ($\Delta\eta$) of target system, $\Delta\eta_{3.0,2.0}$ compared to $\Delta\eta_{3.0,10\ dB}$.

v. Conclusions

The impact of placing a modulated interfering signal in the guard band of a wireless packet based (infrastructure) network, like LTE, on end-to-end TCP performance has been analyzed. These systems employ OFDM, AMC, and HARQ

with a finite length queue. Target system performance was measured in terms of the TCP throughput. It was assumed that both interfering and target signals were subject to independent Nakagami-*m* fading with a shared *m* fading parameter. Results were presented for different fading environments, i.e., different *m*. The analysis provides a blueprint for predicting the end-to-end TCP performance of 4th generation networks impacted by interference with a shaped spectrum. The results show that the impact of placing a modulated interfering signal with a bandwidth of one sub-carrier of the target OFDM signal in the guard band of the OFDM signal under certain circumstances is indistinguishable from fading at the TCP layer. The work presented considers an important aspect of 4th generation wireless networks; the impact of interference on multi-carrier systems' end-to-end performance where the interferer has a shaped spectrum.

Conclusions

The impact and performance of a modulated (covert) interfering signal in the guard band of a wireless packet based (infrastructure) network, like LTE, on end-to-end TCP performance has been presented. The interaction between the two systems occurs at the physical layer where OFDM and AMC are employed. It was assumed that both interfering and target signals were subject to independent Nakagami-*m* fading with a shared *m* fading parameter. However, future work may consider different channels with different *m* using (11) and (12). The impact on the target system was then analyzed at the data-link layer where ARQ and a finite length queue were assumed. Finally, the impact of the interference was presented at the TCP layer. Results were presented for different fading environments, i.e., different *m*. The analysis provides a blueprint for predicting the performance of 4^{th} generation

networks impacted by interference with a shaped spectrum (covert) at all relevant layers. The results show that the impact of placing a modulated interfering signal with a bandwidth of one sub-carrier of the target OFDM signal in the guard band of the OFDM signal under certain conditions is indistinguishable from fading throughout the target system. The work presented considers two important aspect of 4^{th} generation wireless networks; the impact of interference on multi-carrier systems' end-to-end performance where the interferer has a shaped spectrum and the performance of the interfering covert system. Designing a covert signal waveform that has a lower impact on the target system performance and exploits cognitive aspects of the target system are important questions for future work. Additional research is needed to design covert signals that reduce the probability of detection.

Appendix

A. Mathematica

The following code provides analytic performance of target and covert systems based upon SNR of interference and target system parameters.

Define Assumptions
$Assumptions=k1>0&&Real
$Assumptions=k2>0&&Real
$Assumptions=m>0&&Real
$Assumptions=y>0&&Real
k1>0&&Real
k2>0&&Real
m>0&&Real
y>0&&Real
$Assumptions=$\gamma$1>0&&Real
$Assumptions=$\gamma$2>0&&Real
$Assumptions=$\gamma$3>0&&Real
$Assumptions=$\gamma$>0&&Real
γ1>0&&Real

γ2>0&&Real
γ3>0&&Real
γ>0&&Real
$Assumptions=a>0&&Real
$Assumptions=g>0&&Real
a>0&&Real
g>0&&Real
Define bit error rates
Q[z_]:=Erfc[z/$\sqrt{2}$]/2

BER[γ_, M_]:=4/Log2[M]*(($\sqrt{M}$ -1)/$\sqrt{M}$)* $\sum_{i=0}^{\frac{\sqrt{M}}{2}-1}$ Q[(2 i+1) $\sqrt{\frac{3}{M-1}}$]

BERBPSK[γ_]:=Q[$\sqrt{2\,}$]
Define constants
T:=1
k:=3
NrMax:=2
PLoss:=10^{-2}
R0:=.5 1
R1:=.5 2
R2:=.75 2
R3:=.5625 4
R4:=.75 4
R5:=.75 6
γM0:=10^(1/10)
γM1:=10^(03.82877/10)
γM2:=10^(06.86698/10)
γM3:=10^(10.81470/10)
γM4:=10^(13.62620/10)
γM5:=10^(19.71630/10)
F0:=γM0+1/7.993
F1:=γM1+1/1.9992800
F2:=γM2+1/0.6920240
F3:=γM3+1/0.3116290
F4:=γM4+1/0.1679410
F5:=γM5+1/0.0488942
γS1:=((R0 F1-R1 F0)/(R1-R0))
γS2:=((R1 F2-R2 F1)/(R2-R1))
γS3:=((R2 F3-R3 F2)/(R3-R2))
γS4:=(R3 F4-R4 F3)/(R4-R3)
γS5:=(R4 F5-R5 F4)/(R5-R4)
γT1:=2/(k+1) (γM1+Log[1/PLoss]/(k 1.9992800))
γT2:=2/(k+1) (γM2+Log[1/PLoss]/(k 0.6920240))

γT3:=2/(k+1) (γM3+Log[1/PLoss]/(k 0.3116290))
γT4:=2/(k+1) (γM4+Log[1/PLoss]/(k 0.1679410))
γT5:=2/(k+1) (γM5+Log[1/PLoss]/(k 0.0488942))
g1:=Max[γS1,γT1]
g2:=Max[γS2,γT2]
g3:=Max[γS3,γT3]
g4:=Max[γS4,γT4]
g5:=Max[γS5,γT5]
g1t:=Max[γS1,γT1]
g2t:=Max[γS2,γT2]
g3t:=Max[γS3,γT3]
g4t:=Max[γS4,γT4]
g5t:=Max[γS5,γT5]
Define packet error rates for a given mode
PER1[γ_]:=UnitStep[γ]-UnitStep[γ-γM1]+UnitStep[γ-γM1] 124.9390 e-1.9992800 γ
PER2[γ_]:=UnitStep[γ]-UnitStep[γ-γM2]+UnitStep[γ-γM2] 028.8989 e-0.6920240 γ
PER3[γ_]:=UnitStep[γ]-UnitStep[γ-γM3]+UnitStep[γ-γM3] 042.9191 e-0.3116290 γ
PER4[γ_]:=UnitStep[γ]-UnitStep[γ-γM4]+UnitStep[γ-γM4] 047.9713 e-0.1679410 γ
PER5[γ_]:=UnitStep[γ]-UnitStep[γ-γM5]+UnitStep[γ-γM5] 097.5387 e-0.0488942 γ
Define Nakgami pdf of SNR and SINR
PDFNakM[y_, k1_, m_]:= (m^m*$y^{(m-1)}$*Exp[(-m*y)/k1])/($k1^m$*Gamma[m])
PDFNakMInt[y_,k1_,k2_,m_]:=($\frac{m^{\frac{k1}{2}} k2^{\frac{y}{2}}}{k1\,k2}$ $(1/k2)^m$ $m^{2\,m}$ $(y/k1)^{\frac{m}{2}}$ BesselK[m, $\frac{1}{k2}$, $\frac{y}{k1}$] (BesselK[-(1/2)-m,(m (k1+k2 y))/(2 k1 k2)]+BesselK[1/2-m,(m (k1+k2 y))/(2 k1 k2)]))/(2 $\sqrt{\ }$ y Gamma[m])
Calculate the amount of interference
r[Idx_]:=NIntegrate[T Sinc[T π x]^2,{x,Idx-1,Idx+1}]
rAv:=Sum[r[Idx],{Idx,1,12}]/12
Define equations that calculate probability that SNR and SINR lies in a given region
Pr1NakM[k1_,m_]:=NIntegrate[PDFNakM[γ,k1,m],{γ,g1,g2}]
Pr2NakM[k1_,m_]:=NIntegrate[PDFNakM[γ,k1,m],{γ,g2,g3}]
Pr3NakM[k1_,m_]:=NIntegrate[PDFNakM[γ,k1,m],{γ,g3,g4}]
Pr4NakM[k1_,m_]:=NIntegrate[PDFNakM[γ,k1,m],{γ,g4,g5}]
Pr5NakM[k1_,m_]:=NIntegrate[PDFNakM[γ,k1,m],{γ,g5,∞}]
Pr1NakMInt[k1_,k2_,m_]:=NIntegrate[PDFNakMInt[γ,k1,rAv k2,m],{γ,g1,g2}]
Pr2NakMInt[k1_,k2_,m_]:=NIntegrate[PDFNakMInt[γ,k1,rAv k2,m],{γ,g2,g3}]
Pr3NakMInt[k1_,k2_,m_]:=NIntegrate[PDFNakMInt[γ,k1,rAv k2,m],{γ,g3,g4}]
Pr4NakMInt[k1_,k2_,m_]:=NIntegrate[PDFNakMInt[γ,k1,rAv k2,m],{γ,g4,g5}]

```
Pr5NakMInt[k1_,k2_,m_]:=NIntegrate[PDFNakMInt[γ,k1,rAv k2,m],{γ,g5,∞}]
Pr1NakMT[k1_,m_]:=NIntegrate[PDFNakM[γ,k1,m],{γ,g1t,g2t}]
Pr2NakMT[k1_,m_]:=NIntegrate[PDFNakM[γ,k1,m],{γ,g2t,g3t}]
Pr3NakMT[k1_,m_]:=NIntegrate[PDFNakM[γ,k1,m],{γ,g3t,g4t}]
Pr4NakMT[k1_,m_]:=NIntegrate[PDFNakM[γ,k1,m],{γ,g4t,g5t}]
Pr5NakMT[k1_,m_]:=NIntegrate[PDFNakM[γ,k1,m],{γ,g5t,∞}]
Pr1NakMIntT[k1_,k2_,m_]:=NIntegrate[PDFNakMInt[γ,k1,rAv k2,m],{γ,g1t,g2t}]
Pr2NakMIntT[k1_,k2_,m_]:=NIntegrate[PDFNakMInt[γ,k1,rAv k2,m],{γ,g2t,g3t}]
Pr3NakMIntT[k1_,k2_,m_]:=NIntegrate[PDFNakMInt[γ,k1,rAv k2,m],{γ,g3t,g4t}]
Pr4NakMIntT[k1_,k2_,m_]:=NIntegrate[PDFNakMInt[γ,k1,rAv k2,m],{γ,g4t,g5t}]
Pr5NakMIntT[k1_,k2_,m_]:=NIntegrate[PDFNakMInt[γ,k1,rAv k2,m],{γ,g5t,∞}]
The average PER for a given mode when k=1
AvPER1NakM1[k1_,m_]:=NIntegrate[PER1[γ1] PDFNakM[γ1,k1,m],{γ1,g1,g2}]
AvPER2NakM1[k1_,m_]:=NIntegrate[PER2[γ1] PDFNakM[γ1,k1,m],{γ1,g2,g3}]
AvPER3NakM1[k1_,m_]:=NIntegrate[PER3[γ1] PDFNakM[γ1,k1,m],{γ1,g3,g4}]
AvPER4NakM1[k1_,m_]:=NIntegrate[PER4[γ1] PDFNakM[γ1,k1,m],{γ1,g4,g5}]
AvPER5NakM1[k1_,m_]:=NIntegrate[PER5[γ1] PDFNakM[γ1,k1,m],{γ1,g5,∞}]
AvPER1NakMInt1[k1_,k2_,m_]:=NIntegrate[PER1[γ1] PDFNakMInt[γ1,k1,rAv
k2,m],{γ1,g1,g2}]
AvPER2NakMInt1[k1_,k2_,m_]:=NIntegrate[PER2[γ1] PDFNakMInt[γ1,k1,rAv
k2,m],{γ1,g2,g3}]
AvPER3NakMInt1[k1_,k2_,m_]:=NIntegrate[PER3[γ1] PDFNakMInt[γ1,k1,rAv
k2,m],{γ1,g3,g4}]
AvPER4NakMInt1[k1_,k2_,m_]:=NIntegrate[PER4[γ1] PDFNakMInt[γ1,k1,rAv
k2,m],{γ1,g4,g5}]
AvPER5NakMInt1[k1_,k2_,m_]:=NIntegrate[PER5[γ1] PDFNakMInt[γ1,k1,rAv
k2,m],{γ1,g5,∞}]
The average PER over all modes when k=1
AvPERNakM1[k1_,m_]:=(R1 AvPER1NakM1[k1,m]+R2
AvPER2NakM1[k1,m]+R3 AvPER3NakM1[k1,m]+R4 AvPER4NakM1[k1,m]+R5
AvPER5NakM1[k1,m])/(R1 Pr1NakM[k1,m]+R2 Pr2NakM[k1,m]+R3
Pr3NakM[k1,m]+R4 Pr4NakM[k1,m]+R5 Pr5NakM[k1,m])
AvPERNakMInt1[k1_,k2_,m_]:=(R1 AvPER1NakMInt1[k1,k2,m]+R2
AvPER2NakMInt1[k1,k2,m]+R3 AvPER3NakMInt1[k1,k2,m]+R4
AvPER4NakMInt1[k1,k2,m]+R5 AvPER5NakMInt1[k1,k2,m])/(R1
Pr1NakMInt[k1,k2,m]+R2 Pr2NakMInt[k1,k2,m]+R3 Pr3NakMInt[k1,k2,m]+R4
Pr4NakMInt[k1,k2,m]+R5 Pr5NakMInt[k1,k2,m])
The average PER for a given mode when k=2
AvPER1NakM2[k1_,m_]:=NIntegrate[PER1[γ1] PER1[γ1+γ2]
PDFNakM[γ1,k1,m] PDFNakM[γ2,k1,m],{γ1,g1,g2},{γ2,0,∞}]
AvPER2NakM2[k1_,m_]:=NIntegrate[PER2[γ1] PER2[γ1+γ2]
PDFNakM[γ1,k1,m] PDFNakM[γ2,k1,m],{γ1,g2,g3},{γ2,0,∞}]
```

```
AvPER3NakM2[k1_,m_]:=NIntegrate[PER3[γ1] PER3[γ1+γ2]
PDFNakM[γ1,k1,m] PDFNakM[γ2,k1,m],{γ1,g3,g4},{γ2,0,∞}]
AvPER4NakM2[k1_,m_]:=NIntegrate[PER4[γ1] PER4[γ1+γ2]
PDFNakM[γ1,k1,m] PDFNakM[γ2,k1,m],{γ1,g4,g5},{γ2,0,∞}]
AvPER5NakM2[k1_,m_]:=NIntegrate[PER5[γ1] PER5[γ1+γ2]
PDFNakM[γ1,k1,m] PDFNakM[γ2,k1,m],{γ1,g5,∞},{γ2,0,∞}]
AvPER1NakMInt2[k1_,k2_,m_]:=NIntegrate[PER1[γ1] PER1[γ1+γ2]
PDFNakMInt[γ1,k1,rAv k2,m] PDFNakMInt[γ2,k1,rAv
k2,m],{γ1,g1,g2},{γ2,0,∞}]
AvPER2NakMInt2[k1_,k2_,m_]:=NIntegrate[PER2[γ1] PER2[γ1+γ2]
PDFNakMInt[γ1,k1,rAv k2,m] PDFNakMInt[γ2,k1,rAv
k2,m],{γ1,g2,g3},{γ2,0,∞}]
AvPER3NakMInt2[k1_,k2_,m_]:=NIntegrate[PER3[γ1] PER3[γ1+γ2]
PDFNakMInt[γ1,k1,rAv k2,m] PDFNakMInt[γ2,k1,rAv
k2,m],{γ1,g3,g4},{γ2,0,∞}]
AvPER4NakMInt2[k1_,k2_,m_]:=NIntegrate[PER4[γ1] PER4[γ1+γ2]
PDFNakMInt[γ1,k1,rAv k2,m] PDFNakMInt[γ2,k1,rAv
k2,m],{γ1,g4,g5},{γ2,0,∞}]
AvPER5NakMInt2[k1_,k2_,m_]:=NIntegrate[PER5[γ1] PER5[γ1+γ2]
PDFNakMInt[γ1,k1,rAv k2,m] PDFNakMInt[γ2,k1,rAv k2,m],{γ1,g5,∞},{γ2,0,∞}]
The average PER over all modes when k=2
AvPERNakM2[k1_,m_]:=(R1 AvPER1NakM2[k1,m]+R2
AvPER2NakM2[k1,m]+R3 AvPER3NakM2[k1,m]+R4 AvPER4NakM2[k1,m]+R5
AvPER5NakM2[k1,m])/(R1 Pr1NakM[k1,m]+R2 Pr2NakM[k1,m]+R3
Pr3NakM[k1,m]+R4 Pr4NakM[k1,m]+R5 Pr5NakM[k1,m])
AvPERNakMInt2[k1_,k2_,m_]:=(R1 AvPER1NakMInt2[k1,k2,m]+R2
AvPER2NakMInt2[k1,k2,m]+R3 AvPER3NakMInt2[k1,k2,m]+R4
AvPER4NakMInt2[k1,k2,m]+R5 AvPER5NakMInt2[k1,k2,m])/(R1
Pr1NakMInt[k1,k2,m]+R2 Pr2NakMInt[k1,k2,m]+R3 Pr3NakMInt[k1,k2,m]+R4
Pr4NakMInt[k1,k2,m]+R5 Pr5NakMInt[k1,k2,m])
The average PER for a given mode when k=3
AvPER1NakM3[k1_,m_]:=NIntegrate[PER1[γ1] PER1[γ1+γ2] PER1[γ1+γ2+γ3]
PDFNakM[γ1,k1,m] PDFNakM[γ2,k1,m]
PDFNakM[γ3,k1,m],{γ1,g1,g2},{γ2,0,∞},{γ3,0,∞}]
AvPER2NakM3[k1_,m_]:=NIntegrate[PER2[γ1] PER2[γ1+γ2] PER2[γ1+γ2+γ3]
PDFNakM[γ1,k1,m] PDFNakM[γ2,k1,m]
PDFNakM[γ3,k1,m],{γ1,g2,g3},{γ2,0,∞},{γ3,0,∞}]
AvPER3NakM3[k1_,m_]:=NIntegrate[PER3[γ1] PER3[γ1+γ2] PER3[γ1+γ2+γ3]
PDFNakM[γ1,k1,m] PDFNakM[γ2,k1,m]
PDFNakM[γ3,k1,m],{γ1,g3,g4},{γ2,0,∞},{γ3,0,∞}]
AvPER4NakM3[k1_,m_]:=NIntegrate[PER4[γ1] PER4[γ1+γ2] PER4[γ1+γ2+γ3]
PDFNakM[γ1,k1,m] PDFNakM[γ2,k1,m]
PDFNakM[γ3,k1,m],{γ1,g4,g5},{γ2,0,∞},{γ3,0,∞}]
```

```
AvPER5NakM3[k1_,m_]:=NIntegrate[PER5[γ1] PER5[γ1+γ2] PER5[γ1+γ2+γ3]
PDFNakM[γ1,k1,m] PDFNakM[γ2,k1,m]
PDFNakM[γ3,k1,m],{γ1,g5,∞},{γ2,0,∞},{γ3,0,∞}]
AvPER1NakMInt3[k1_,k2_,m_]:=NIntegrate[PER1[γ1] PER1[γ1+γ2]
PER1[γ1+γ2+γ3] PDFNakMInt[γ1,k1,rAv k2,m] PDFNakMInt[γ2,k1,rAv k2,m]
PDFNakMInt[γ3,k1,rAv k2,m],{γ1,g1,g2},{γ2,0,∞},{γ3,0,∞}]
AvPER2NakMInt3[k1_,k2_,m_]:=NIntegrate[PER2[γ1] PER2[γ1+γ2]
PER2[γ1+γ2+γ3] PDFNakMInt[γ1,k1,rAv k2,m] PDFNakMInt[γ2,k1,rAv k2,m]
PDFNakMInt[γ3,k1,rAv k2,m],{γ1,g2,g3},{γ2,0,∞},{γ3,0,∞}]
AvPER3NakMInt3[k1_,k2_,m_]:=NIntegrate[PER3[γ1] PER3[γ1+γ2]
PER3[γ1+γ2+γ3] PDFNakMInt[γ1,k1,rAv k2,m] PDFNakMInt[γ2,k1,rAv k2,m]
PDFNakMInt[γ3,k1,rAv k2,m],{γ1,g3,g4},{γ2,0,∞},{γ3,0,∞}]
AvPER4NakMInt3[k1_,k2_,m_]:=NIntegrate[PER4[γ1] PER4[γ1+γ2]
PER4[γ1+γ2+γ3] PDFNakMInt[γ1,k1,rAv k2,m] PDFNakMInt[γ2,k1,rAv k2,m]
PDFNakMInt[γ3,k1,rAv k2,m],{γ1,g4,g5},{γ2,0,∞},{γ3,0,∞}]
AvPER5NakMInt3[k1_,k2_,m_]:=NIntegrate[PER5[γ1] PER5[γ1+γ2]
PER5[γ1+γ2+γ3] PDFNakMInt[γ1,k1,rAv k2,m] PDFNakMInt[γ2,k1,rAv k2,m]
PDFNakMInt[γ3,k1,rAv k2,m],{γ1,g5,∞},{γ2,0,∞},{γ3,0,∞}]
The average PER over all modes when k=3
AvPERNakM3[k1_,m_]:=(R1 AvPER1NakM3[k1,m]+R2
AvPER2NakM3[k1,m]+R3 AvPER3NakM3[k1,m]+R4 AvPER4NakM3[k1,m]+R5
AvPER5NakM3[k1,m])/(R1 Pr1NakM[k1,m]+R2 Pr2NakM[k1,m]+R3
Pr3NakM[k1,m]+R4 Pr4NakM[k1,m]+R5 Pr5NakM[k1,m])
AvPERNakMInt3[k1_,k2_,m_]:=(R1 AvPER1NakMInt3[k1,k2,m]+R2
AvPER2NakMInt3[k1,k2,m]+R3 AvPER3NakMInt3[k1,k2,m]+R4
AvPER4NakMInt3[k1,k2,m]+R5 AvPER5NakMInt3[k1,k2,m])/(R1
Pr1NakMInt[k1,k2,m]+R2 Pr2NakMInt[k1,k2,m]+R3 Pr3NakMInt[k1,k2,m]+R4
Pr4NakMInt[k1,k2,m]+R5 Pr5NakMInt[k1,k2,m])
Find average PER for each mode in truncated
AvPER1NakMT[k1_,m_]:=NIntegrate[PER1[γ] PDFNakM[γ,k1,m],{γ,g1t,g2t}]
AvPER2NakMT[k1_,m_]:=NIntegrate[PER2[γ] PDFNakM[γ,k1,m],{γ,g2t,g3t}]
AvPER3NakMT[k1_,m_]:=NIntegrate[PER3[γ] PDFNakM[γ,k1,m],{γ,g3t,g4t}]
AvPER4NakMT[k1_,m_]:=NIntegrate[PER4[γ] PDFNakM[γ,k1,m],{γ,g4t,g5t}]
AvPER5NakMT[k1_,m_]:=NIntegrate[PER5[γ] PDFNakM[γ,k1,m],{γ,g5t,∞}]
AvPER1NakMIntT[k1_,k2_,m_]:=NIntegrate[PER1[γ] PDFNakMInt[γ,k1,rAv
k2,m],{γ,g1t,g2t}]
AvPER2NakMIntT[k1_,k2_,m_]:=NIntegrate[PER2[γ] PDFNakMInt[γ,k1,rAv
k2,m],{γ,g2t,g3t}]
AvPER3NakMIntT[k1_,k2_,m_]:=NIntegrate[PER3[γ] PDFNakMInt[γ,k1,rAv
k2,m],{γ,g3t,g4t}]
AvPER4NakMIntT[k1_,k2_,m_]:=NIntegrate[PER4[γ] PDFNakMInt[γ,k1,rAv
k2,m],{γ,g4t,g5t}]
```

AvPER5NakMIntT[k1_,k2_,m_]:=NIntegrate[PER5[γ] PDFNakMInt[γ,k1,rAv k2,m],{γ,g5t,∞}]
The average number of transmissions for k=3
AvTranNakM[k1_,m_]:=1+AvPERNakM1[k1,m]+AvPERNakM2[k1,m]
AvTranNakMInt[k1_,k2_,m_]:=1+AvPERNakMInt1[k1,k2,m]+AvPERNakMInt2[k1,k2,m]
Average PER for truncated ARQ over all modes
AvPERNakMTFirst[k1_,m_]:=(R1 AvPER1NakMT[k1,m]+R2 AvPER2NakMT[k1,m]+R3 AvPER3NakMT[k1,m]+R4 AvPER4NakMT[k1,m]+R5 AvPER5NakMT[k1,m])/(R1 Pr1NakMT[k1,m]+R2 Pr2NakMT[k1,m]+R3 Pr3NakMT[k1,m]+R4 Pr4NakMT[k1,m]+R5 Pr5NakMT[k1,m])
AvPERNakMIntTFirst[k1_,k2_,m_]:=(R1 AvPER1NakMIntT[k1,k2,m]+R2 AvPER2NakMIntT[k1,k2,m]+R3 AvPER3NakMIntT[k1,k2,m]+R4 AvPER4NakMIntT[k1,k2,m]+R5 AvPER5NakMIntT[k1,k2,m])/(R1 Pr1NakMIntT[k1,k2,m]+R2 Pr2NakMIntT[k1,k2,m]+R3 Pr3NakMIntT[k1,k2,m]+R4 Pr4NakMIntT[k1,k2,m]+R5 Pr5NakMIntT[k1,k2,m])
AvPERNakMT[k1_,m_]:=AvPERNakMTFirst[k1,m]$^{NrMax+1}$
AvPERNakMIntT[k1_,k2_,m_]:=AvPERNakMIntTFirst[k1,k2,m]$^{NrMax+1}$
Find spectral efficiency HARQ
SpecEffNakM[k1_,m_]:=R1 Pr1NakM[k1,m] (1-AvPER1NakM3[k1,m])+R2 Pr2NakM[k1,m] (1-AvPER2NakM3[k1,m])+R3 Pr3NakM[k1,m] (1-AvPER3NakM3[k1,m])+R4 Pr4NakM[k1,m] (1-AvPER4NakM3[k1,m])+R5 Pr5NakM[k1,m] (1-AvPER5NakM3[k1,m])
SpecEffNakMInt[k1_,k2_,m_]:=R1 Pr1NakMInt[k1,k2,m] (1-AvPER1NakMInt3[k1,k2,m])+R2 Pr2NakMInt[k1,k2,m] (1-AvPER2NakMInt3[k1,k2,m])+R3 Pr3NakMInt[k1,k2,m] (1-AvPER3NakMInt3[k1,k2,m])+R4 Pr4NakMInt[k1,k2,m] (1-AvPER4NakMInt3[k1,k2,m])+R5 Pr5NakMInt[k1,k2,m] (1-AvPER5NakMInt3[k1,k2,m])
Throughput when k=3
ThroughputNakM[k1_,m_]:=SpecEffNakM[k1,m]/AvTranNakM[k1,m]
ThroughputNakMInt[k1_,k2_,m_]:=SpecEffNakMInt[k1,k2,m]/AvTranNakMInt[k1,k2,m]
Find spectral efficiency truncated
NrAvNakMT[k1_,m_]:=(1-AvPERNakMTFirst[k1,m]$^{NrMax+1}$)/(1-AvPERNakMTFirst[k1,m])
NrAvNakMIntT[k1_,k2_,m_]:=(1-AvPERNakMIntTFirst[k1,k2,m]$^{NrMax+1}$)/(1-AvPERNakMIntTFirst[k1,k2,m])
SpecEffNakMT[k1_,m_]:=R1 Pr1NakMT[k1,m] (1-AvPER1NakMT[k1,m])+R2 Pr2NakMT[k1,m] (1-AvPER2NakMT[k1,m])+R3 Pr3NakMT[k1,m] (1-AvPER3NakMT[k1,m])+R4 Pr4NakMT[k1,m] (1-AvPER4NakMT[k1,m])+R5 Pr5NakMT[k1,m] (1-AvPER5NakMT[k1,m])
SpecEffNakMIntT[k1_,k2_,m_]:=R1 Pr1NakMIntT[k1,k2,m] (1-AvPER1NakMIntT[k1,k2,m])+R2 Pr2NakMIntT[k1,k2,m] (1-

AvPER2NakMIntT[k1,k2,m])+R3 Pr3NakMIntT[k1,k2,m] (1-
AvPER3NakMIntT[k1,k2,m])+R4 Pr4NakMIntT[k1,k2,m] (1-
AvPER4NakMIntT[k1,k2,m])+R5 Pr5NakMIntT[k1,k2,m] (1-
AvPER5NakMIntT[k1,k2,m])
ThroughputNakMT[k1_,m_]:=SpecEffNakMT[k1,m]/NrAvNakMT[k1,m]
ThroughputNakMIntT[k1_,k2_,m_]:=SpecEffNakMIntT[k1,k2,m]/NrAvNakMIntT[k
1,k2,m]
AvBERIntFad[k1_,k2_,m_]:=NIntegrate[BER[y,16] PDFNakMInt[y,k1,rAv

k2,m],{y,0,∞}]

B. Mat Lab

The following code simulates the PER of a target system subject to interference from a covert link.

```
% This function returns PER and BER for a given covert and target
SNR and
% AMC mode, multi-carrier, fading, interference

function [PER,BER] = PER6MCFad(TarSNRdB,CovSNRdB)

% Seed the random number generators with the current time
rand('state',sum(100*clock));
randn('state',sum(100*clock));

% Parameters and initializations
BiCv    = 2;      % No. of bits per symbol covert
NumCar  = 12;     % No. of sub-carriers
NumPack = 1e4;    % No. of packets
No      = .002;   % Noise power
N       = 512;    % No. of available sub-carriers
NumSam  = 28;     % Oversampling rate
IdxCov  = 13;     % Sub-carrier location of interferer
Offset  = 7;      % Synchronous offset
FreqOf  = 1.00;   % Frequency offset
NakM    = 1;      % Nakagami faidng parameter

BitsErrors = 0;
PackErrors = 0;

% Set mode parameters
Bi     = 6;  % Bits per carrier
NumSym = 20; % Symbols per packet
m      = 3;  % Code rate numerator
n      = 4;  % Code rate denominator
```

```
% Set transmission parameters
NumBitsPerPacket = Bi*NumCar*NumSym; % Number of coded bits per
packet
NumBitsSym       = Bi*NumCar;

% Puncture pattern rate 3/4 code
PuncPattern = [1 1 1 0 0 1];

% Coding trellis
t = poly2trellis(7,[133 171]);

% Order of 1st permutation
NBI       = NumBitsPerPacket/Bi;
BitsIdx   = [1:1:NumBitsPerPacket]-1;
FirstPerm = Bi*mod(BitsIdx,NBI)+floor(BitsIdx/NBI);

% Order of 2nd permutation
s          = max(Bi/2,1);
SecondPerm = (s*floor(FirstPerm/s))+mod((FirstPerm+NumBitsPerPacket-
floor(NBI*FirstPerm/NumBitsPerPacket)),s);
SecondPerm = SecondPerm+1;

% Compute sub-carrier power
Es = db2pow(TarSNRdB)*No;
Ej = db2pow(CovSNRdB)*No;

% Set up a cell array of QAM constellations with an average energy
of
% unity and grey coded
Const{1} = UnitQamConstellation(1);
for ii=2:2:max(Bi)

    Const{ii} = Constellation(ii);
end;

% Select the constellation from which points will be selected
ThisConst = Const{Bi};
CovConst  = Const{BiCv};

% Create Rayleigh fading variables
%X1I    = sqrt(1/2)*randn(1,NumPack);
%X1Q    = sqrt(1/2)*randn(1,NumPack);

%R1 = sqrt(X1I.^2+X1Q.^2);

%X2I = sqrt(1/2)*randn(1,NumPack);
%X2Q = sqrt(1/2)*randn(1,NumPack);

%R2 = sqrt(X2I.^2+X2Q.^2);
```

```
% Create the modulated carriers
%I = zeros(NumCar,NumSam);
%Q = zeros(NumCar,NumSam);

for ll = 1:NumCar

    I(ll,:) = sqrt(2)*cos(2*pi*ll*[0:1:NumSam-1]./NumSam);
    Q(ll,:) = sqrt(2)*sin(2*pi*ll*[0:1:NumSam-1]./NumSam);
end;

ICv = sqrt(2)*cos(2*pi*IdxCov*FreqOf*[0:1:NumSam-1]./NumSam);
QCv = sqrt(2)*sin(2*pi*IdxCov*FreqOf*[0:1:NumSam-1]./NumSam);


% Packet loop
for ii = 1:NumPack

    fprintf(1,'Packet %i of %i SNR= %i dB\n',ii,NumPack,TarSNRdB);

    % Generate random information bits at the transmitter
    InBits              = (rand(1,(Bi*NumSym*NumCar*m)/n) > .5);

    % Set last six bits to zero, terminate encoder to zero state
    InBits([end-5:end]) = [0 0 0 0 0 0];

    % Encode bits and puncture
    CodedBits  = convenc(InBits,t,PuncPattern);
    InputBits  = CodedBits;

    % Interleave-1st permutation
    B     = reshape(InputBits,Bi,[]);
    C     = B';
    IBits = reshape(C,1,[]);

    % Interleave-2nd permutation
    IntBits = zeros(1,NumBitsPerPacket);

    for pp = 1:1:NumBitsPerPacket

        IntBits(pp) = IBits(SecondPerm(pp));
    end;

    % Track errors in each packet
    PackBitErr = 0;

    % Generate covert bits
    CovertBits = (rand(1,2*BiCv) > .5);

    % Allocate an array for received bits
    RxBits     = zeros(1,NumCar*NumSym*Bi);
```

```
    R1 = sqrt(gamrnd(NakM,1/NakM));
    R2 = sqrt(gamrnd(NakM,1/NakM));

    % Symbols per packet loop
    for kk = 1:NumSym

        % Allocate an array of the QAM symbols
        X = zeros(1,N);

        % Convert each group of bits into a QAM symbol
        for jj = 1:NumCar
            Idx1  = NumBitsSym*(kk-1)+(jj-1)*Bi+1;
            Idx2  = NumBitsSym*(kk-1)+jj*Bi;
            Xtemp = (IntBits([Idx1:Idx2])* 2.^[0:1:Bi-1]') + 1;
            X(jj) = sqrt(Es)*ThisConst(Xtemp);
        end;

        XCv1  = (CovertBits([1:BiCv])* 2.^[0:1:BiCv-1]') + 1;
        XCv1i = sqrt(Ej)*CovConst(XCv1);

        XCv2  = (CovertBits([BiCv+1:2*BiCv])* 2.^[0:1:BiCv-1]') + 1;
        XCv2i = sqrt(Ej)*CovConst(XCv2);

        % Modulate signals
        ITx = zeros(NumCar,NumSam);
        QTx = zeros(NumCar,NumSam);

        for mm = 1:NumCar

            ITx(mm,:) = real(X(mm)).*I(mm,:);
            QTx(mm,:) = imag(X(mm)).*Q(mm,:);
        end;

        % Shift & modulate Covert
        if Offset > 0

            ITxCv = [real(XCv1i).*ICv([Offset+1:end])
real(XCv2i).*ICv([1:Offset])];
            QTxCv = [imag(XCv1i).*QCv([Offset+1:end])
imag(XCv2i).*QCv([1:Offset])];
        else

            ITxCv = real(XCv1i).*ICv;
            QTxCv = imag(XCv1i).*QCv;
        end;

        % Combine in-phase & quadriture components, Rayleigh effects
        s1 = R1*(ITx - QTx);

        % Combine the sub-carriers
```

```
        s1 = sum(s1);

        % Combine in-phase & quadriture components of covert,
Rayleigh effects
        s2 = R2*(ITxCv - QTxCv);

        % Combine covert and subcarriers
        s = [s1; s2];
        s = sum(s);

        % Add noise
        r = s + sqrt(NumSam*No/2)*randn(1,length(s));

       % Equalizer
        Rx = r./R1;

        % Demodulate signals
        for nn = 1:NumCar

            RlDem = sum(Rx.*I(nn,:))/NumSam;
            ImDem = sum(Rx.*-Q(nn,:))/NumSam;
            XRx   = (RlDem + i*ImDem)/sqrt(Es);

            % Convert to bits
            Idx3                = NumBitsSym*(kk-1)+(nn-1)*Bi+1;
            Idx4                = NumBitsSym*(kk-1)+nn*Bi;
            [Dist, Index]       = min(abs(ThisConst - XRx));
            RxBits([Idx3:Idx4]) = dec2binvec(Index-1,Bi);
        end;

    end;

    % Deinterleave-undo 2nd permutation
    DeIntBits = zeros(1,NumBitsPerPacket);

    for qq = 1:1:NumBitsPerPacket

        DeIntBits(SecondPerm(qq)) = RxBits(qq);
    end;

    % Deinterleave-undo 1st permutation
    D      = reshape(DeIntBits,NumBitsPerPacket/Bi,[]);
    E      = D';
    DeBits = reshape(E,1,[]);

    % Decode bits
    OutBits = vitdec(DeBits,t,24,'term','hard',PuncPattern);

    % Find bit errors
    BitsErrors = BitsErrors + sum(OutBits ~= InBits);
    PackBitErr = PackBitErr + sum(OutBits ~= InBits);
```

```
    if PackBitErr > 0
        PackErrors = PackErrors + 1;
    else
    end;

end;

fprintf(1,'Packet errors = %i\n',PackErrors);

% Calculate error rates
BER = BitsErrors/(NumCar*Bi*NumSym*NumPack*m/n);
PER = PackErrors/NumPack;
```

C. Packet Error Rate Simulation Results

The following tables are the numerical results of PER simulations for the modes given in Table II.

Mode 1

E_b/N_o (dB)	E_s/N_o (dB)	Packet errors	Bit errors
-1.77	3	9988	4.405×10^5
-0.77	4	8222	81171
0.23	5	2330	9366
1.23	6	250	767

Mode 2

E_b/N_o (dB)	E_s/N_o (dB)	Packet errors	Bit errors
2.23	7	8925	1.04×10^5
3.23	8	4007	18067
4.23	9	809	2325
5.23	10	82	213

Mode 3

E_b/N_o (dB)	E_s/N_o (dB)	Packet errors	Bit errors
6.23	11	8451	81977
7.23	12	3252	12972
8.23	13	611	1656
9.23	14	57	135

Mode 4

E_b/N_o (dB)	E_s/N_o (dB)	Packet errors	Bit errors
9.23	14	7091	4.97×10^4
10.23	15	2432	8665
11.23	16	444	1126
12.23	17	51	112

Mode 5

E_b/N_o (dB)	E_s/N_o (dB)	Packet errors	Bit errors
15.23	20	7057	5.37×10^4
16.23	21	2829	10762
17.23	22	545	1448
18.23	23	70	167

References

[1] S. Choney. (2009). *Is 2010 the year of wireless congestion?* Available: http://www.msnbc.msn.com/id/34634571/ns/technology_and_science_tech_and_gadgets/

[2] C. E. Shannon, "Communication in the Presence of Noise," *Proceedings of the IRE,* vol. 37, pp. 10-21, 1949.

[3] J. Proakis and M. Salehi, *Digital Communications*. New York: McGraw-Hill, 2008.

[4] I. Poole, "Elements tutorial - what exactly is... LTE?," *Communications Engineer,* vol. 5, pp. 46-47, 2007.

[5] M. Rumney, "IMT-Advanced: 4G wirelss takes shape in an olympic year," *Agilent Measurement Journal,* September 2008.

[6] G. Blackwell. (2009). *The future of 4G: LTE vs. WiMAX*. Available: http://www.wi-fiplanet.com/news/article.php/3845111/The-Future-of-4G-LTE-vs-WiMAX.htm

[7] J. Lubacz, W. Mazurczyk, and K. Szczypiorski. (2010, March) Voice over IP. *IEEE Spectrum*. pp. 42-47.

[8] S. Zander, G. Armitage, and P. Branch, "A Survey of Covert Channels and Countermeasures in Computer Network Protocols," *IEEE Communications Surveys & Tutorials,* vol. 9, pp. 44-57, 2007.

[9] NCSC, "Trusted Computer System Evaluation Criteria," National Computer Security Center Tech. Rep. DOD 5200.28-STD, Dec. 1985 1985.

[10] D. L. Nicholson, *Spread Spectrum Signal Design: LPE and AJ*: Computer Scince Press, 1988.
[11] R. A. Dillard, "Detectability of Spread-Spectrum Signals," *IEEE Transactions on Aerospace and Electronic Systems,* vol. AES-15, pp. 526-537, 1979.
[12] D. J. Torrieri, *Principles of spread-spectrum communication systems*: Artech House, 1985.
[13] J. Glanz and J. Markoff, "U.S. Underwrites Internet Detour Around Censors," in *The New York Times*, ed. New York, New York, June 11, 2011.
[14] A. Zyoud, M. H. Habaebi, J. Chebil, and M. R. Islam, "Femtocell interference mitigation," in *Control and System Graduate Research Colloquium (ICSGRC), 2012 IEEE*, 2012, pp. 94-99.
[15] N. Saquib, E. Hossain, L. Long Bao, and K. Dong In, "Interference management in OFDMA femtocell networks: issues and approaches," *Wireless Communications, IEEE,* vol. 19, pp. 86-95, 2012.
[16] V. A. Aalo and Z. Jingjun, "Performance analysis of maximal ratio combining in the presence of multiple equal-power cochannel interferers in a Nakagami fading channel," *Vehicular Technology, IEEE Transactions on,* vol. 50, pp. 497-503, 2001.
[17] F. Rezaei, M. Hempel, P. Dongming, Q. Yi, and H. Sharif, "Analysis and evaluation of covert channels over LTE advanced," in *Wireless Communications and Networking Conference (WCNC), 2013 IEEE*, 2013, pp. 1903-1908.
[18] Z. Hijaz and V. S. Frost, "Exploiting OFDM systems for covert communication," in *MILITARY COMMUNICATIONS CONFERENCE 2010 - MILCOM 2010*, 2010, pp. 2149-2155.
[19] Z. Hijaz and V. Frost, "The impact of interference on an OFDM system with AMC, hybrid ARQ, and a finite queue on end-to-end performance," in *IEEE International Symposium on Communication Systems, Networks and Digital Signal Processing-CSNDSP14*, Manchester, UK, 2014 (submitted).
[20] Z. Hijaz and V. S. Frost, "The impact of interference from a covert link on a data link using OFDM, AMC, and Hybrid ARQ," in *IEEE International Performance Computing and Communication Conference*, San Diego, CA, 2013.
[21] Z. Hijaz and V. S. Frost, "A method for estimating the average packet error rates of multi carrier systems with interference," in *IEEE Communications Quality and Reliability Conference-CQR 2014*, Tucson, AZ, 2014.
[22] J. Park, D. Kim, C. Kang, and D. Hong, "Effect of partial band jamming on OFDM-based WLAN in 802.11g," in *IEEE International Conference on Acoustics, Speech, and Signal Processing, 2003 - (ICASSP '03)* 2003, pp. IV-560-3 vol.4.
[23] C. S. Patel, G. L. Stuber, and T. G. Pratt, "Analysis of OFDM/MC-CDMA under channel estimation and jamming," in *IEEE Wireless Communications and Networking Conference, 2004 - WCNC*, 2004, pp. 954-958 Vol.2.
[24] Q. Liu, S. Zhou, and G. B. Giannakis, "Cross-layer combining of queuing

with adaptive modulation and coding over wireless links," in *Military Communications Conference, 2003. MILCOM '03. 2003 IEEE*, 2003, pp. 717-722 Vol.1.

[25] Q. Liu, S. Zhou, and G. B. Giannakis, "Cross-Layer combining of adaptive Modulation and coding with truncated ARQ over wireless links," *IEEE Transactions on Wireless Communications,* vol. 3, pp. 1746-1755, 2004.

[26] Q. Liu, S. Zhou, and G. B. Giannakis, "Queuing with adaptive modulation and coding over wireless links: cross-Layer analysis and design," *IEEE Transactions on Wireless Communications,* vol. 4, pp. 1142-1153, 2005.

[27] Q. Liu, S. Zhou, and G. B. Giannakis, "TCP performance in wireless access with adaptive modulation and coding," in *IEEE International Conference on Communications, 2004*, 2004, pp. 3989-3993 Vol.7.

[28] X. Lagrange, "Performance analysis of HARQ protocols with link adaptation on fading channels," *Anals of Telecommunications,* vol. 66, pp. 695-705, December 2011.

[29] S. A. Ahmadzadeh and G. Agnew, "Turbo covert channel: An iterative framework for covert communication over data networks," in *INFOCOM, 2013 Proceedings IEEE*, 2013, pp. 2031-2039.

[30] H. Okhravi, S. Bak, and S. T. King, "Design, implementation and evaluation of covert channel attacks," in *Technologies for Homeland Security (HST), 2010 IEEE International Conference on*, 2010, pp. 481-487.

[31] W. Mazurczyk, K. Szczypiorski, and J. Lubacz, "Four ways to smuggle messages through internet services," *Spectrum, IEEE,* vol. 50, pp. 42-45, 2013.

[32] S. Zander, G. Armitage, and P. Branch, "Covert Channels and Countermeasures in Computer Network Protocols[Reprinted from IEEE Communications Surveys and Tutorials]," *IEEE Communications Magazine,* vol. 45, pp. 136-142, 2007.

[33] L. Jun, J. H. Andrian, and Z. Chi, "Bit Error Rate Analysis of jamming for OFDM systems," in *Wireless Telecommunications Symposium, 2007. WTS 2007*, 2007, pp. 1-8.

[34] M. K. Simon and M. S. Alouini, *Digital communication over fading channels* vol. 86: Wiley-IEEE Press, 2004.

[35] K. A. Hamdi, "A Useful Technique for Interference Analysis in Nakagami Fading," *Communications, IEEE Transactions on,* vol. 55, pp. 1120-1124, 2007.

[36] E. K. Al Hussaini, "Effects of Nakagami fading on antijam performance requirements," *Electronics Letters,* vol. 24, pp. 208-209, 1988.

[37] A. Mraz and L. Pap, "General performance analysis of M-PSK and M-QAM wireless communications applied to OFDMA interference," in *Wireless Telecommunications Symposium (WTS), 2010*, 2010, pp. 1-7.

[38] C. Tellambura, "Cochannel interference computation for arbitrary Nakagami fading," *Vehicular Technology, IEEE Transactions on,* vol. 48, pp. 487-489, 1999.

[39] A. A. Abu-Dayya and N. C. Beaulieu, "Outage probabilities of cellular mobile radio systems with multiple Nakagami interferers," *Vehicular Technology, IEEE Transactions on,* vol. 40, pp. 757-768, 1991.

[40] Y. Yu-Dong and A. U. H. Sheikh, "Investigations into cochannel interference in microcellular mobile radio systems," *Vehicular Technology, IEEE Transactions on,* vol. 41, pp. 114-123, 1992.

[41] M. Smadi, V. Prabhu, and S. Al-jazzar, "Analytical study on the effect of cochannel interference on partially coherent diversity systems," *Communications, IEEE Transactions on,* vol. 57, pp. 117-124, 2009.

[42] A. Mraz and L. Pap, "General interference analysis of M-QAM transmission applied to LTE performance evaluation," in *EUROCON - International Conference on Computer as a Tool (EUROCON), 2011 IEEE*, 2011, pp. 1-4.

[43] K. S. Shanmugan and A. Breipohl, *Random Signals; Detection, Estimation and Data Analysis*: Wiley, 1998.

[44] E. W. Weisstein. *Confluent Hypergeometric Function of the First Kind*. Available: http://mathworld.wolfram.com/ConfluentHypergeometricFunctionoftheFirstKind.html

[45] C. R. Wylie, *Advanced Enginering Mathematics*. New York, New York: McGraw Hill, 1966.

[46] L. Rubio, J. Reig, and N. Cardona, "Evaluation of Nakagami fading behaviour based on measurements in urban scenarios," *AEU - International Journal of Electronics and Communications,* vol. 61, pp. 135-138, 2007.

[47] M. D. Yacoub, M. V. Barbin, M. S. de Castro, and J. E. Vargas B, "Level crossing rate of Nakagami-m fading signal: field trials and validation," *Electronics Letters,* vol. 36, pp. 355-357, 2000.

[48] M.-S. Alouini and A. J. Goldsmith, "Adaptive Modulation over Nakagami Fading Channels," *Wireless Personal Communications,* vol. 13, pp. 119-143, 2000.

[49] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation," vol. TS 36.211, ed, September 2012.

[50] W. Zhengdao, X. Ma, and G. B. Giannakis, "OFDM or single-carrier block transmissions?," *Communications, IEEE Transactions on,* vol. 52, pp. 380-394, 2004.

[51] O. Awoniyi and F. A. Tobagi, "Packet Error Rate in OFDM-Based Wireless LANs Operating in Frequency Selective Channels," in *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*, 2006, pp. 1-13.

[52] D. Chase, "Code Combining--A Maximum-Likelihood Decoding Approach for Combining an Arbitrary Number of Noisy Packets," *Communications, IEEE Transactions on,* vol. 33, pp. 385-393, 1985.

[53] Z. Xuemei and Y. Dongfeng, "Analysis of the AMC-ARQ System over MIMO Correlated Fading Channels," in *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on*, 2008,

pp. 1-4.
[54] M. D. Yacoub, J. E. V. Bautista, and L. Guerra de Rezende Guedes, "On higher order statistics of the Nakagami-m distribution," *Vehicular Technology, IEEE Transactions on,* vol. 48, pp. 790-794, 1999.
[55] J. Razavilar, K. J. R. Liu, and S. I. Marcus, "Jointly optimized bit-rate/delay control policy for wireless packet networks with fading channels," *Communications, IEEE Transactions on,* vol. 50, pp. 484-494, 2002.
[56] W. Hong-Shen and N. Moayeri, "Finite-state Markov channel-a useful model for radio communication channels," *Vehicular Technology, IEEE Transactions on,* vol. 44, pp. 163-171, 1995.
[57] D. Bertsekas and R. Gallager, *Data Networks*, 2nd ed. Upper Saddle River, NJ: Prentice-Hall, 1992.
[58] P. Bremaud, *Markov Chains: Gibbs Fields, Monte Carlo Simulation, and Queues*. New York: Springer-Verlag, 1999.
[59] J. Padhye, V. Firoiu, D. F. Towsley, and J. F. Kurose, "Modeling TCP Reno performance: a simple model and its empirical validation," *Networking, IEEE/ACM Transactions on,* vol. 8, pp. 133-145, 2000.
[60] L. Benyuan, D. L. Goeckel, and D. Towsley, "TCP-cognizant adaptive forward error correction in wireless networks," in *Global Telecommunications Conference, 2002. GLOBECOM '02. IEEE*, 2002, pp. 2128-2132 vol.3.
[61] C. Chiasserini and M. Meo, "A reconfigurable protocol setting to improve TCP over wireless," *Vehicular Technology, IEEE Transactions on,* vol. 51, pp. 1608-1620, 2002.