



**ANÁLISE DA MODELAGEM DE CANAIS
SEM FIO SOB DESVANECIMENTO κ - μ SOMBREADO
COM APLICAÇÕES DE SEGURANÇA NA CAMADA FÍSICA E
CONSIDERAÇÕES DE COMBATE AO DESVANECIMENTO**

MÁRCIA MANUELA MEDRADO NUNES

**DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA**

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA

**UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA**

**ANÁLISE DA MODELAGEM DE CANAIS
SEM FIO SOB DESVANECIMENTO κ - μ SOMBREADO
COM APLICAÇÕES DE SEGURANÇA NA CAMADA FÍSICA E
CONSIDERAÇÕES DE COMBATE AO DESVANECIMENTO**

MÁRCIA MANUELA MEDRADO NUNES

Orientador: PROF. UGO SILVA DIAS

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA

**PUBLICAÇÃO PPGEE - 691/2018
BRASÍLIA-DF, 12 DE DEZEMBRO DE 2017.**

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

ANÁLISE DA MODELAGEM DE CANAIS SEM FIO SOB
DESVANECIMENTO K- μ SOMBREADO COM APLICAÇÕES DE
SEGURANÇA NA CAMADA FÍSICA E CONSIDERAÇÕES DE
COMBATE AO DESVANECIMENTO

MÁRCIA MANUELA MEDRADO NUNES

DISSERTAÇÃO DE MESTRADO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA
ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO
PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE.

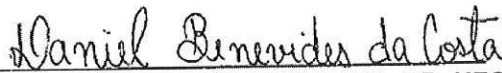
APROVADA POR:



UGO SILVA DIAS, Dr., ENE/UNB
(ORIENTADOR)



GEORGES DANIEL AMVAME NZE, Dr., ENE/UNB
(EXAMINADOR INTERNO)



DANIEL BENEVIDES DA COSTA, DR. UFC
(EXAMINADOR EXTERNO)

Brasília, 29 de março de 2018.

FICHA CATALOGRÁFICA

MÁRCIA MANUELA MEDRADO NUNES

Análise da modelagem de canais sem fio sob desvanecimento κ - μ sombreado com aplicações de segurança na camada física e considerações de combate ao desvanecimento

2017xv, 147p., 201x297 mm

(ENE/FT/UnB, Mestre, Engenharia Elétrica, 2017)

Dissertação de Mestrado - Universidade de Brasília

Faculdade de Tecnologia - Departamento de Engenharia Elétrica

REFERÊNCIA BIBLIOGRÁFICA

MÁRCIA MANUELA MEDRADO NUNES (2017) Análise da modelagem de canais sem fio sob desvanecimento κ - μ sombreado com aplicações de segurança na camada física e considerações de combate ao desvanecimento. Dissertação de Mestrado em Engenharia Elétrica, Publicação 691/2018, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 147p.

CESSÃO DE DIREITOS

AUTOR: MÁRCIA MANUELA MEDRADO NUNES

TÍTULO: Análise da modelagem de canais sem fio sob desvanecimento κ - μ sombreado com aplicações de segurança na camada física e considerações de combate ao desvanecimento.

GRAU: Mestre ANO: 2017

É concedida à Universidade de Brasília permissão para reproduzir cópias desta dissertação de Mestrado e para emprestar ou vender tais cópias somente para propósitos acadêmicos e científicos. O autor se reserva a outros direitos de publicação e nenhuma parte desta dissertação de Mestrado pode ser reproduzida sem a autorização por escrito do autor.

MÁRCIA MANUELA MEDRADO NUNES

Brasília - DF - Brasil

Agradecimentos

A todos que de alguma forma colaboraram para a conclusão desta dissertação.

Márcia Manuela Medrado Nunes

RESUMO

Esta dissertação apresenta uma análise da modelagem de canal sob o desvanecimento κ - μ sombreado com aplicações de segurança na camada física usando o modelo clássico de escuta de Wyner. O modelo κ - μ sombreado foi escolhido por fornecer um modelo geral de desvanecimento e quando comparado a outros modelos de desvanecimento como o Rayleigh, Rice, Nakagami-m e κ - μ , foi encontrado um melhor ajuste utilizando este modelo. Comparações foram feitas utilizando conceitos de Probabilidade de Interrupção de Sigilo (do inglês, *Secrecy Outage Probability*, SOP), de Capacidade de Sigilo Estritamente Positiva (do inglês, *Strictly Positive Secrecy Capacity*, SPSC) e Capacidade Média de Sigilo (do inglês, *Average Secrecy Capacity*, ASC). As formulações fechadas de um caso da SOP e da SPSC foram obtidas e demonstradas. Os resultados e análises são realizados por meio das curvas de SOP, SPSC e ASC, variando as características do canal intruso e do canal principal sob o modelo κ - μ sombreado. Além disso, algumas técnicas de combate ao desvanecimento aplicadas ao canal principal são analisadas como a Combinação Seletiva (do inglês, *Selection Combining*, SC), a Combinação por Razão Máxima (do inglês, *Maximum Ratio Combining*, MRC) e a técnica de Múltiplas Entradas e Múltiplas Saídas (do inglês, *Multiple-In Multiple-Out*, MIMO) com o canal de desvanecimento κ - μ sombreado.

ABSTRACT

This dissertation presents an analysis of shadowed κ - μ fading channel with security applications at the physical layer using the Wyner's classic wiretap model. The κ - μ shadowed model was chosen because it provided a general model of fading and when compared to other fading models such as Rayleigh, Rice, Nakagami-m and κ - μ , a better fit was found using this model. Comparisons were made using concepts of Secrecy Outage Probability (SOP), Strictly Positive Secrecy Capacity (SPSC) and Average Secrecy Capacity (ASC). The closed formulations of a case of SOP and SPSC were obtained and demonstrated. The results and analyzes are performed using the SOP, SPSC and ASC curves, varying the characteristics of the intrusion channel and the main channel under the κ - μ shadowed model. In addition, some techniques to combat fading applied to the main channel are analyzed as the Selective Combining (SC), Maximum Ratio Combining (MRC) e Multiple-Input Multiple-Output (MIMO).

SUMÁRIO

1	INTRODUÇÃO	1
1.1	CONTEXTUALIZAÇÃO	1
1.2	DEFINIÇÃO DO PROBLEMA	3
1.3	OBJETIVOS.....	4
1.4	ESTRUTURA DA DISSERTAÇÃO.....	5
2	MODELAGEM DO CANAL DE COMUNICAÇÕES SEM FIO	6
2.1	MODELO CLÁSSICO DE ESCUTA DE WYNER	6
2.2	MODELOS ESTATÍSTICOS CLÁSSICOS	7
2.2.1	DISTRIBUIÇÃO DE RAYLEIGH	7
2.2.2	DISTRIBUIÇÃO DE NAKAGAMI- m	8
2.2.3	DISTRIBUIÇÃO DE RICE.....	10
2.2.4	DISTRIBUIÇÃO DE κ - μ	12
2.2.5	DISTRIBUIÇÃO DE κ - μ SOMBREADA	14
2.3	CONCLUSÃO	17
3	TÉCNICAS DE COMBATE AO DESVANECIMENTO	18
3.1	MAXIMAL RATIO COMBINING	18
3.2	MULTIPLE-INPUT MULTIPLE-OUTPUT.....	19
3.3	SELECTION COMBINING	21
3.4	CONCLUSÃO	23
4	MÉTRICAS DE SEGURANÇA	24
4.1	CAPACIDADE DE SIGILO	24
4.2	PROBABILIDADE DE INTERRUÇÃO DE SIGILO	26
4.3	PROBABILIDADE DE CAPACIDADE DE SIGILO ESTRITAMENTE POSITIVA	27
4.4	CAPACIDADE MÉDIA DE SIGILO.....	28
4.5	CONCLUSÃO	29
5	CARACTERIZAÇÃO ESTATÍSTICA DA SEGURANÇA DE CANAIS SEM FIO	30
5.1	METODOLOGIA APLICADA	30
5.2	FORMULAÇÕES FECHADAS PARA A SOP E SPSC PARA CANAIS κ - μ SOMBREADOS	30

5.3	ANÁLISE DA SOP	32
5.3.1	SEM TÉCNICAS DE COMBATE AO DESVANECIMENTO	32
5.3.2	COM TÉCNICAS DE COMBATE AO DESVANECIMENTO	34
5.4	ANÁLISE DA SPSC	39
5.4.1	SEM TÉCNICAS DE COMBATE AO DESVANECIMENTO	39
5.4.2	COM TÉCNICAS DE COMBATE AO DESVANECIMENTO	39
5.5	ANÁLISE DA ASC	41
5.5.1	SEM TÉCNICAS DE COMBATE AO DESVANECIMENTO	42
5.5.2	COM TÉCNICAS DE COMBATE AO DESVANECIMENTO	43
5.6	VARIANDO μ	46
5.6.1	ANÁLISE DA SOP	47
5.6.2	ANÁLISE DA SPSC	47
5.6.3	ANÁLISE DA ASC	48
5.7	COMPARAÇÃO COM OUTRAS DISTRIBUIÇÕES	48
6	CONCLUSÃO	51
6.1	TRABALHOS FUTUROS	52
	REFERÊNCIAS BIBLIOGRÁFICAS	53
	APÊNDICES	57
I.1	SOP	58
I.2	SPSC	60

LISTA DE FIGURAS

1.1	Arquitetura em camadas do modelo OSI.	2
1.2	Ataque de escuta.	2
2.1	PDF da distribuição de Rayleigh.....	8
2.2	CDF da distribuição de Rayleigh.	9
2.3	PDF da distribuição de Nakagami- m com m variando.....	10
2.4	CDF da distribuição de Nakagami- m com m variando.	11
2.6	CDF da distribuição de Rice com K variando.....	11
2.5	PDF da distribuição de Rice com K variando.....	12
2.7	PDF da distribuição de Rice com K variando.....	13
2.8	PDF da distribuição κ - μ com K variando.....	13
2.9	CDF da distribuição κ - μ	14
2.10	PDF da distribuição κ - μ sombreada com κ variando.	15
2.11	PDF da distribuição κ - μ sombreada com μ variando.	16
2.12	PDF da distribuição κ - μ sombreada com s variando.	16
2.13	CDF da distribuição de κ - μ sombreada.	17
3.1	<i>Maximal Ratio Combiner</i> com L ramos.....	18
3.2	PDF da distribuição κ - μ sombreada com MRC variando L	19
3.3	Esquema básico de antenas transmissoras e receptoras com a técnica de MIMO.	20
3.4	PDF da distribuição κ - μ sombreada com MIMO variando N_R e N_T	21
3.5	Esquema básico utilizado na técnica SC.	22
3.6	PDF da distribuição κ - μ sombreada com SC variando L	23
4.1	Configuração base.	24
5.1	SOP sob canal κ - μ sombreado por K , variando κ_R e κ_E , com $Cth = 0$ bps. ...	33
5.2	SOP sob canal κ - μ sombreado por K , variando κ_R e κ_E , com $Cth = 1.25$ bps.	33
5.3	SOP sob canal κ - μ sombreado por K , variando κ_R e κ_E , com SC e $Cth = 0$ bps.....	34
5.4	SOP sob canal κ - μ sombreado por K , variando κ_R e κ_E , com SC e $Cth = 1.25$ bps.	35
5.5	SOP sob canal κ - μ sombreado por K , variando κ_R e κ_E , com MRC e $Cth = 0$ bps.	35

5.6	SOP sob canal κ - μ sombreado por K , variando κ_R e κ_E , com MRC e $Cth = 1.25$ bps.	36
5.7	SOP sob canal κ - μ sombreado por K , variando κ_R e κ_E , com MIMO e $Cth = 0$ bps.	37
5.8	SOP sob canal κ - μ sombreado por K , variando κ_R e κ_E , com MIMO e $Cth = 1.25$ bps.	37
5.9	Comparação da SOP sob canal κ - μ sombreado por K com $Cth = 1.25$ bps.	38
5.10	Comparação da SOP sob canal κ - μ sombreado por K com $Cth = 0$ bps.	38
5.11	SPSC sob canal κ - μ sombreado por K , variando κ_R e κ_E	39
5.12	SPSC sob canal κ - μ sombreado por K , variando κ_R e κ_E , com SC no canal principal.	40
5.13	SPSC sob canal κ - μ sombreado por K , variando κ_R e κ_E , com MRC.	41
5.14	SPSC sob canal κ - μ sombreado por K , variando κ_R e κ_E , com MIMO.	42
5.16	ASC sob canal κ - μ sombreado por K , variando κ_R e κ_E	42
5.15	Comparação da SPSC sob canal κ - μ sombreado por K , variando κ_R e κ_E	43
5.17	ASC sob canal κ - μ sombreado por K , variando κ_R e κ_E , com SC e $L = 2$	43
5.18	ASC sob canal κ - μ sombreado por K , variando κ_R e κ_E , com SC e $L = 4$	44
5.19	ASC sob canal κ - μ sombreado por K , variando κ_R e κ_E , com MRC.	44
5.20	ASC sob canal κ - μ sombreado por K , variando κ_R e κ_E , com MIMO.	45
5.21	Comparação da ASC sob canal κ - μ sombreado por K , variando κ_R e κ_E	46
5.22	SOP sob canal κ - μ sombreado por K , variando μ_R , com $Cth = 1.25$ bps.	47
5.23	SPSC sob canal κ - μ sombreado por K , variando μ_R	47
5.24	ASC sob canal κ - μ sombreado por K , variando μ_R	48
5.25	Comparação da curva SOP de várias distribuições por K	49
5.26	Comparação da curva SPSC de várias distribuições por K	49
5.27	Comparação da curva ASC de várias distribuições por K	50

LISTA DE TABELAS

2.1	Distribuições derivadas a partir do modelo κ - μ sombreado.....	17
-----	--	----

LISTA DE TERMOS E SIGLAS

ASC	Average Secrecy Capacity
AWGN	Additive White Gaussian Noise
CDF	Cumulative Distribution Function
DoS	Denial-of-Service
MIMO	Multiple-Input Multiple-Output
MRC	Maximal Ratio Combining
OSI	Open System Interconnection
PDF	Probability Density Function
RMS	Root Mean Square
SC	Selection Combining
SNR	Signal Noise Ratio
SOP	Secrecy Outage Probability
SPSC	Strictly Positive Secrecy Capacity
TDMA	Time Division Multiple Access

LISTA DE SÍMBOLOS

R	Variável Aleatória da magnitude da envoltória
Ω	Potência Média do Sinal Transmitido
$\bar{\gamma}$	SNR média
m	Fator de Desvanecimento
$E[\cdot]$	Esperança
$V[\cdot]$	Variância
K	Fator de Rice
κ	Razão entre a Potência Total das Componentes Dominantes do Sinal e a Potência Total das Componentes Espalhadas
μ	Número de clusters multipercurso presentes no ambiente
$I_x[\cdot]$	Função <i>Bessel</i> modificada de primeiro tipo e ordem x
${}_1F_1$	Função Gamma Hipergeométrica Confluyente
ϕ_2	Função Hipergeométrica Bivariante Confluyente
E_b	Energia por bit
w	Ganho de cada canal MRC
δ^2	Ruído quadrático médio
$\gamma[\cdot]$	Função Gamma Incompleta
$\Gamma[\cdot]$	Função Gamma

Capítulo 1

Introdução

1.1 Contextualização

A segurança nas transmissões já se tornou uma preocupação constante nas arquiteturas de rede, sejam elas cabeadas por fibra ótica, por enlaces de micro-ondas, com ou sem linha de visada. Essa preocupação permitiu um avanço significativo nos campos de estudo especializados na segurança da troca de informações. Devido aos vários tipos de serviços disponíveis atualmente que facilitam a execução das atividades do dia a dia e que necessitam enviar e receber informações privadas de forma segura, como por exemplo, transações bancárias, trocas de informações entre pacientes e médicos, comunicações militares, a segurança na troca de tais informações se tornou algo imprescindível.

Um exemplo de como esse assunto tem sido um item importante da atualidade é a discussão da necessidade de uma Política Nacional de Segurança [1]. No dia 17 de fevereiro de 2017 foi publicado no Diário Oficial da União, no âmbito de seu Departamento de Segurança da Informação e Comunicações, a elaboração de uma proposta desta Política Nacional de Segurança e num próximo passo criar uma Agência Nacional de Segurança. Entre os objetivos está o estabelecimento de mecanismos para o processamento e veiculação de informações seguras. Dentro desta discussão acerca da segurança na troca de informações, várias pesquisas sobre o assunto estão sendo realizadas em todas as camadas de comunicação [2], [3], [4], [5]. A Figura 1.1 mostra como são distribuídas as camadas no modelo OSI, do inglês *Open System Interconnection*. Neste modelo as camadas são separadas em camada de aplicação, camada de apresentação, camada de sessão, camada de transporte, camada de rede, camada de enlace e camada física.

Os ataques mais comuns que são observados nas comunicações de redes sem fio podem ser categorizados em ataques passivos e ativos. Dois exemplos bem comuns de ataques passivos são os de escuta e de análise de tráfego, ou seja, são ataques que não impossibilitam o funcionamento da rede. Em ataques ativos, os quais podem afetar o funcionamento da rede através de alterações na mesma, temos como exemplo os ataques de DoS [6].

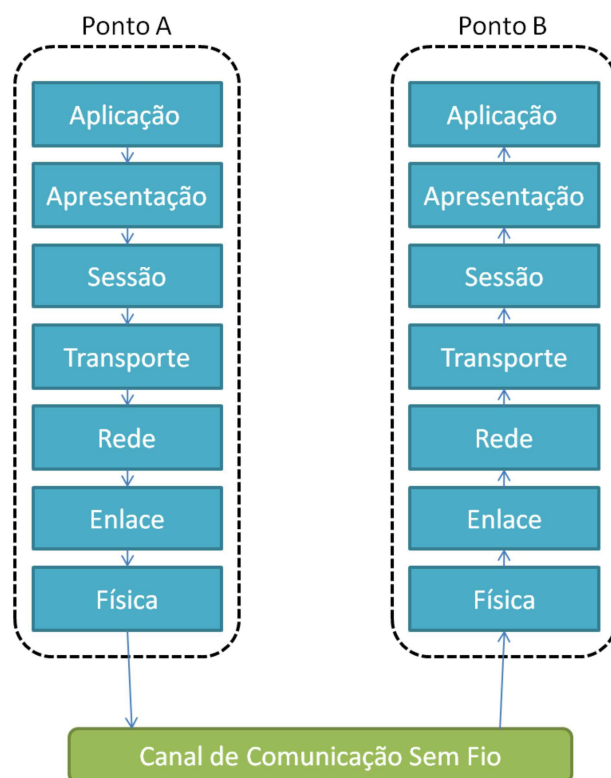


Figura 1.1: Arquitetura em camadas do modelo OSI.

Medidas de segurança na camada física têm ganhado grande importância nos estudos mais recentes da área. Nesta camada estão os ataques de tratamento mais difíceis, eles acabam utilizando de forma indevida o meio sem fio por dispositivos que não participam da rede.

O ataque mais comum observado na camada física é o de escuta, ou *eavesdropping*, que se baseia em um canal de comunicação principal com dois pontos trocando informações privadas, e um terceiro indivíduo tentando interceptar as informações através de uma escuta no canal de comunicação principal, criando assim um segundo canal, o canal intruso. A Figura 1.2 exemplifica como acontece esse tipo de ataque.

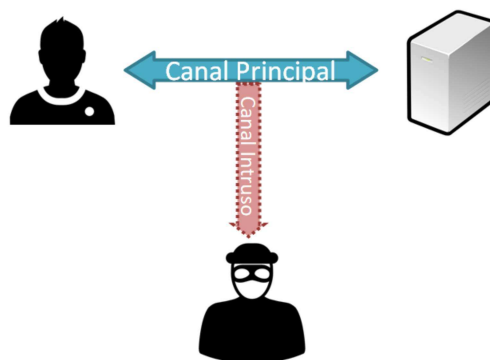


Figura 1.2: Ataque de escuta.

Com a crescente necessidade de mais segurança na troca de informação nos meios de

comunicação, este trabalho se motiva na caracterização estatística do canal sem fio com aplicações de segurança na camada física. E para tal, é grande a importância da modelagem do canal para avaliação do desempenho das redes de comunicação. Devido às características estocásticas dos canais, várias distribuições já foram apresentadas para a modelagem dos meios de propagação, mas este trabalho se propõe a analisar aplicações de segurança na camada física utilizando a distribuição κ - μ sombreada, distribuição esta que apresenta um bom ajuste a dados práticos além de ser um modelo generalista de desvanecimento com boa flexibilidade.

1.2 Definição do problema

A necessidade de explorar o desempenho da segurança na camada física tornou-se incontestável para evitar ataques de escuta. Então, para caracterizar os cenários de propagação quando há canais intrusos no ambiente é necessário aprofundar o estudo das métricas de segurança. Entre as métricas mais utilizadas se encontram a Capacidade de Sigilo Estritamente Positiva (do inglês, *Strictly Positive Secrecy Capacity*, SPSC), a Probabilidade de Interrupção de Sigilo (do inglês, *Secrecy Outage Probability*, SOP), e a Capacidade de Sigilo Média (do inglês, *Average Secrecy Capacity*, ASC).

Trabalhos acerca deste assunto estão sendo amplamente explorados, como em [7] e [8], com o estudo da SPSC para sistemas com canais independentes de desvanecimento Log-Normal com um único intruso e com vários intrusos, respectivamente. Estudos sobre a SPSC sob canais de desvanecimento de Rice e Weibull foram realizados em [9] e [10], respectivamente. A SOP sob canais log-Normal foi investigada em [11]. Em [12], o canal de desvanecimento de Rayleigh foi utilizado para caracterização da SPSC e da SOP para o modelo clássico de escuta de Wyner. Em [13] são apresentadas várias técnicas de diversidade para aumentar a segurança em redes sem fio contra ataques de escuta. Alguns métodos de seleção segura foram propostos com o objetivo de aumentar a segurança na camada física em redes sem fio cooperativas e em redes de rádio cognitivo em [14] e [15], respectivamente. Um estudo da SOP e da SPSC foi realizado em [16], utilizando o canal de desvanecimento α - μ sob o modelo clássico de escuta de Wyner.

Até então, as referências sobre segurança na camada física se concentram em canais como Rayleigh, Rice, Nakagami- m ou log-Normal [7, 8, 9, 17, 18]. Todos estes trabalhos propõem modelos analíticos para tipos específicos de canais de desvanecimento e não cobrem os vários tipos de desvanecimento em cenários práticos. E em contra-partida a distribuição κ - μ sombreada tem sido usada para caracterizar cenários compostos com linha de visada e sombreamento [19]. Esta distribuição fornece um modelo geral de desvanecimento com bom ajuste para dados práticos e podendo ser reduzida para modelos de desvanecimento como a Gaussiana unilateral, Rayleigh, Rice, e Nakagami- m , todas compostas com sombreamento. Também é possível reduzir aos mesmos canais de desvanecimento, porém

sem sombreamento, o que mostra uma excelente flexibilidade da distribuição κ - μ sombreada.

Pelo conhecimento da autora, a literatura ainda carece de estudos específicos para o canal de desvanecimento κ - μ sombreado acerca da SOP, SPSC e ASC na camada física e este trabalho se propõe a realizar uma investigação sobre estas métricas sob o mencionado canal de desvanecimento aplicado ao modelo clássico de escuta de Wyner e também analisar o uso de técnicas de combate ao desvanecimento como a Combinação Seletiva, do inglês *Selection Combining* (SC), a Combinação por Razão Máxima, do inglês *Maximum Ratio Combiner* (MRC) e Múltiplas Entradas e Múltiplas Saídas, do inglês *Multiple-In Multiple-Out* (MIMO) para melhorar a confiabilidade dos sistemas de comunicação sem fio devido às características de um canal com combate ao desvanecimento.

1.3 Objetivos

Este trabalho se propõe a realizar uma análise da segurança na camada física baseando-se nas métricas de segurança SOP, SPSC e ASC sob o canal de desvanecimento κ - μ sombreado. Desta forma, este trabalho tem por objetivo:

- Descrever os modelos de desvanecimentos mais utilizados: Rayleigh, Nakagami- m , Rice, κ - μ e o utilizado como base deste trabalho, κ - μ sombreado;
- Descrever as técnicas de combate ao desvanecimento que podem ser utilizadas para melhorar a segurança nas comunicações sem fio: SC, MRC e MIMO;
- Descrever as métricas de segurança utilizadas na análise dos ambientes propostos: SOP, SPSC e ASC;
- Obter a formulação para um caso da métrica de segurança SOP e SPSC para o modelo de desvanecimento κ - μ sombreado;
- Investigar o comportamento da SOP, SPSC e ASC quando utilizamos o modelo de desvanecimento κ - μ sombreado variando os valores de κ do canal principal e do canal intruso;
- Investigar o comportamento da SOP, SPSC e ASC quando utilizamos o modelo de desvanecimento κ - μ sombreado com técnicas de combate ao desvanecimento variando os valores de κ do canal principal e do canal intruso;
- Investigar o comportamento da SOP, SPSC e ASC quando utilizamos o modelo de desvanecimento κ - μ sombreado variando os valores de μ do canal principal;
- Comparar modelos de desvanecimento variados sob as curvas de SOP, SPSC e ASC.

1.4 Estrutura da Dissertação

Este trabalho está estruturado da seguinte maneira:

- Capítulo 2: Apresenta os modelos de caracterização de canal utilizados neste trabalho como o modelo de escuta de Wyner, os modelos estatísticos de Rayleigh, Nakagami- m , Rice, κ - μ e κ - μ sombreado;
- Capítulo 3: Apresenta as técnicas de combate ao desvanecimento que serão aplicadas aos canais de comunicação propostos, são elas SC, MRC e MIMO;
- Capítulo 4: Apresenta as métricas de segurança aplicadas para a caracterização do sigilo obtido sob os canais de comunicação sem fio estudados, são elas a SOP, a SPSC e a ASC;
- Capítulo 5: Aqui são apresentadas as formulações fechadas para um caso da SOP e para a SPSC, além das análises e caracterização estatística da segurança de canais de comunicação sob a distribuição κ - μ sombreada. Comparações são realizadas com outras distribuições.
- Capítulo 6: Apresenta as conclusões obtidas a partir de todo o trabalho desenvolvido nesta dissertação.
- Apêndice: Demonstração das fórmulas fechadas para a SOP e a SPSC sob o canal de desvanecimento κ - μ sombreado.

Capítulo 2

Modelagem do canal de comunicações sem fio

Os sistemas de comunicação sem fio apresentam limitações impostas pelo próprio canal. O caminho do sinal entre o transmissor e receptor pode estar seriamente obstruído por prédios ou montanhas, ou estar com uma linha de visão direta e sem obstáculos. Os canais de comunicação sem fio são aleatórios e não oferecem uma análise simples.

A modelagem do canal de comunicação é uma das partes mais importantes na análise de um sistema seguro e normalmente é realizada estatisticamente, com base em medições realizadas no cenário de interesse.

Este capítulo trará uma breve explicação sobre os conceitos necessários para a análise e modelagem do canal de comunicação proposto neste trabalho.

2.1 Modelo clássico de escuta de Wyner

Para a caracterização de um ambiente com escuta usaremos o modelo clássico de Wyner [20]. Este modelo é baseado em um sistema de comunicação sem fio com três nós diferentes, o transmissor, o receptor e o intruso. Neste cenário, o transmissor S envia mensagens confidenciais para o receptor R , e o intruso E tenta decodificar a mensagem privada pelos outros dois pontos. O canal entre o nó S e R , é considerado como canal principal, e entre S e E , canal intruso.

A partir do conceito defendido por Shannon [21] de que para uma comunicação segura, dada a presença de um intruso, é necessário que os canais principais e intrusos não apresentem ruído e também a presença de uma chave secreta tanto no transmissor quanto no receptor, Wyner expandiu este conceito para canais com ruído.

Wyner diz que uma condição perfeita de sigilo pode ser alcançada desde que a informação obtida pelo intruso seja irrelevante comparada à mensagem original. Ou seja, dado

$I(A; B)$ como a informação mútua entre os pontos A e B , M como o sinal transmitido pelo nó transmissor S , \tilde{M} como o sinal recebido pelo receptor legítimo R , e Z como o sinal recebido pelo intruso, a capacidade máxima do canal é dada como:

$$C = \max_{p_x} I(M; \tilde{M}) - I(M; Z), \quad (2.1)$$

em que p_x é a função distribuição de probabilidade do sinal transmitido.

Para o cenário proposto neste trabalho, considera-se que os canais principal e intruso apresentam desvanecimento independente e também ruídos Gaussianos complexos independentes com média zero e variações unitárias. Ambos os canais possuem blocos de desvanecimento ergódicos em que os coeficientes dos canais permanecem constantes durante o período do bloco, variando independentemente entre eles.

2.2 Modelos estatísticos Clássicos

Em comunicações sem fio, a envoltória e a fase do sinal variam de maneira aleatória devido ao fenômeno do multipercurso. O bom conhecimento dos fenômenos que afetam o canal de propagação e dos parâmetros do sinal propagado têm um impacto direto na qualidade e na confiabilidade de um sistema de comunicações. Conseqüentemente, uma boa caracterização estatística da envoltória torna a análise de qualquer técnica de comunicação bem mais precisa.

O modelo estatístico escolhido para este trabalho é o κ - μ sombreado por ser uma distribuição que fornece um modelo geral de desvanecimento com bom ajuste para dados práticos e podendo ser reduzida para outros modelos de desvanecimento. E para propósitos de comparação, trabalharemos também com as distribuições mais clássicas Rayleigh, Nakagami- m , Rice, Rice sombreado e κ - μ sem sombreado.

2.2.1 Distribuição de Rayleigh

Este modelo é um dos mais utilizados para ambientes com desvanecimento multipercurso sem linha de visada. A função densidade de probabilidade, do inglês *Probability Density Function* (PDF), da envoltória do sinal transmitido com a distribuição de Rayleigh é dada por [22]:

$$f_{R_{Ray}}(r) = \frac{2r}{\Omega_{Ray}} \exp\left[-\frac{r^2}{\Omega_{Ray}}\right], \quad (2.2)$$

em que R_{Ray} é a variável aleatória da magnitude da envoltória do sinal modelado por Rayleigh e Ω é a potência média do sinal transmitido, com $r \geq 0$.

Para a avaliação e caracterização de canais de comunicação sem fio é mais comum o uso da PDF em função da relação sinal ruído, SNR. Desta forma, a PDF da distribuição de

Rayleigh em função da SNR instantânea por símbolo transmitido é dada por:

$$f_{\Gamma_{Ray}}(\gamma) = \frac{1}{\bar{\gamma}} \exp\left[-\frac{\gamma}{\bar{\gamma}}\right], \quad (2.3)$$

em que $\bar{\gamma}$ é a SNR média por símbolo transmitido, com $\gamma \geq 0$.

A curva da PDF de Rayleigh é mostrada na Figura 2.1.

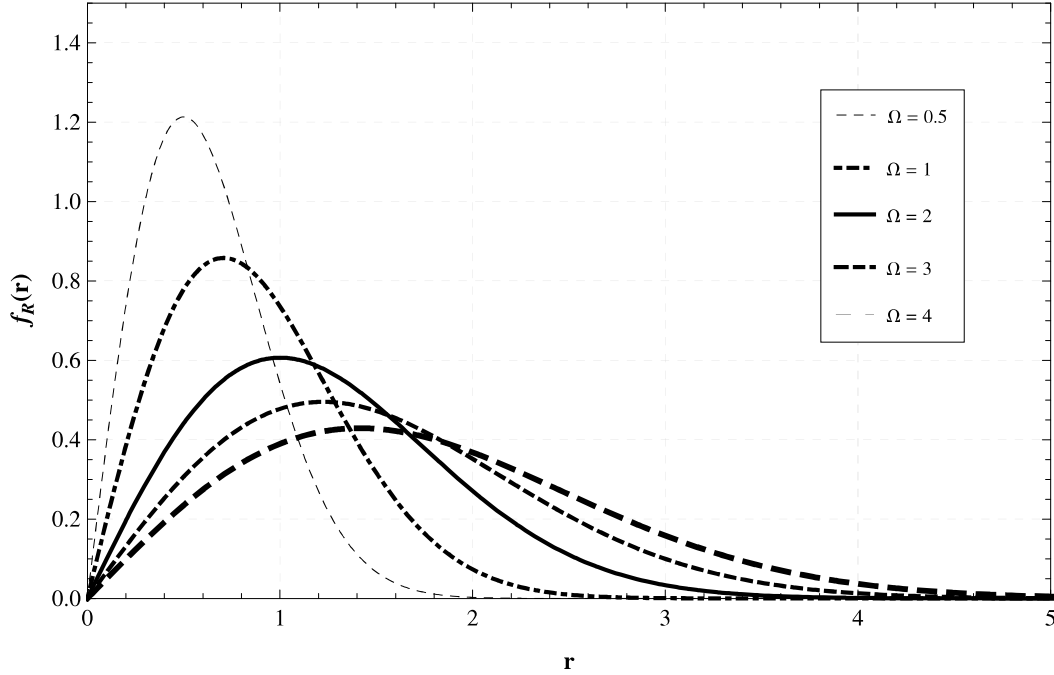


Figura 2.1: PDF da distribuição de Rayleigh.

A função distribuição acumulada, do inglês *Cumulative Distribution Function* (CDF), da distribuição de Rayleigh pode ser obtida a partir da integração da PDF, a Figura 2.2 mostra a CDF da distribuição de Rayleigh.

2.2.2 Distribuição de Nakagami- m

A distribuição Nakagami- m é obtida a partir da distribuição Qui-Quadrado (χ^2) Central em que m é o parâmetro de desvanecimento [22]. Esta é uma distribuição mais flexível, podendo se aproximar à maioria das distribuições. É também empregada para modelar ambientes internos em presença de multipercurso.

A PDF da envoltória R é dada por [22]:

$$f_{R_{Nak}}(r) = \frac{2m^m r^{2m-1}}{\Gamma(m)\Omega_{Nak}^m} \exp\left[-\frac{mr^2}{\Omega_{Nak}}\right], \quad (2.4)$$

em que R_{Nak} é a variável aleatória da magnitude da envoltória do sinal modelado por Nakagami- m e Ω é a potência média do sinal transmitido, com $r \geq 0$.

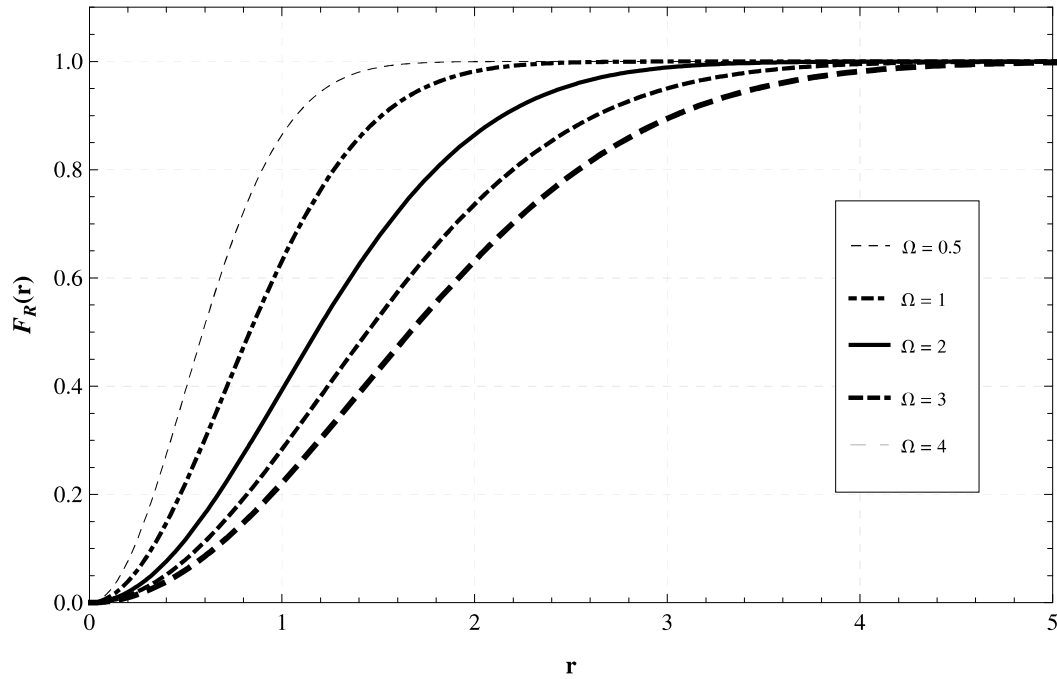


Figura 2.2: CDF da distribuição de Rayleigh.

A PDF da distribuição de Nakagami- m em função da SNR instantânea por símbolo transmitido é dada por:

$$f_{\Gamma_{Nak}}(\gamma) = \frac{m^m \bar{\gamma}^{m-1}}{\Gamma(m) \bar{\gamma}^m} \exp\left[-\frac{m\gamma}{\bar{\gamma}}\right], \quad (2.5)$$

em que $\bar{\gamma}$ é a SNR média por símbolo transmitido, com $\gamma \geq 0$.

O parâmetro m , que é conhecido como fator de desvanecimento, determina a inclinação das curvas traçadas em função dos valores medidos e representa o número de *clusters* multipercurso. O m somente irá garantir uma boa aproximação quando seu valor for definido a partir de $m \geq 1/2$ [22]. O fator de desvanecimento é o fator de maior influência nesta distribuição [23]. O parâmetro Ω é a média da potência do sinal, e $\Gamma[\cdot]$ é a função Gamma. O parâmetro m é definido por [24] como:

$$m = \frac{E^2[r^2]}{V[r^2]}, m \geq \frac{1}{2}, \quad (2.6)$$

em que $E[\cdot]$ é o operador Esperança e $V[\cdot]$ é a variância.

A distribuição Nakagami- m inclui algumas outras distribuições utilizadas para caracterização de canais de comunicação a partir da manipulação de seu parâmetro m . A distribuição Gaussiana Unilateral pode ser obtida com $m = 1/2$ e a distribuição de Rayleigh com $m = 1$.

A curva da PDF da Nakagami- m é mostrada na Figura 2.3.

A CDF da distribuição de Nakagami- m pode ser obtida a partir da integração da PDF é mostrada na Figura 2.4.

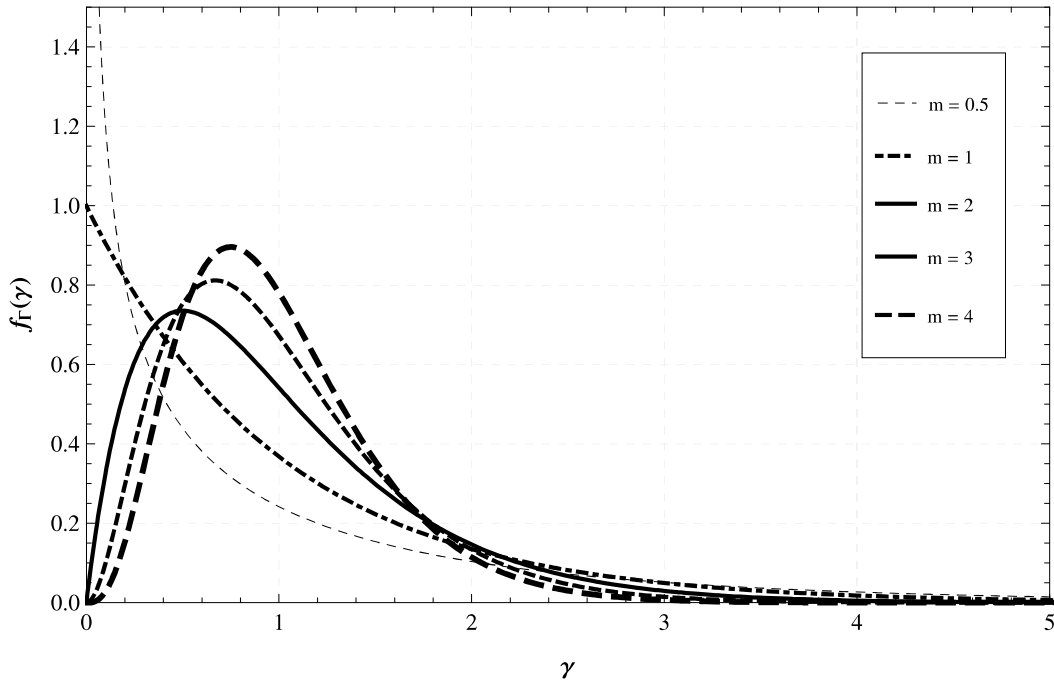


Figura 2.3: PDF da distribuição de Nakagami- m com m variando.

2.2.3 Distribuição de Rice

A distribuição de Rice, também conhecida como distribuição Nakagami- n , tem como característica um bom ajuste para canais de propagação com um componente com linha de visada com maior potência e outros componentes aleatórios com potência menor [22]. O sinal recebido será composto pela soma dos sinais refletidos mais um sinal com potência predominante.

A distribuição de Rice apresenta para sua envoltória R a seguinte PDF [22]:

$$f_{R_{Ric}}(r) = \left(\frac{2(k+1)r}{\Omega_{Ric}} \right) \exp \left[-k - \frac{(k+1)r^2}{\Omega_{Ric}} \right] I_0 \left(2\sqrt{\frac{k(k+1)}{\Omega_{Ric}}} r \right), \quad (2.7)$$

em que R_{Ric} é a variável aleatória da magnitude da envoltória do sinal modelado por Rice e Ω é a potência média do sinal transmitido, com $r \geq 0$. k é conhecido como fator de Rice e representa a razão entre a potência total da componente dominante e a potência total das componentes espalhadas. k provoca o comportamento na distribuição mostrado na Figura 2.5, ou seja, quanto maior k , mais determinística será a distribuição [25].

A PDF da distribuição de Rice em função da SNR instantânea por símbolo transmitido é dada por:

$$f_{\Gamma_{Ric}}(\gamma) = \left(\frac{(K+1)}{\bar{\gamma}} \right) \exp \left[-K - \frac{(K+1)\gamma}{\bar{\gamma}} \right] I_0 \left(2\sqrt{\frac{K(K+1)\gamma}{\bar{\gamma}}} \right), \quad (2.8)$$

em que $\bar{\gamma}$ é a SNR média por símbolo transmitido, e $\gamma \geq 0$.

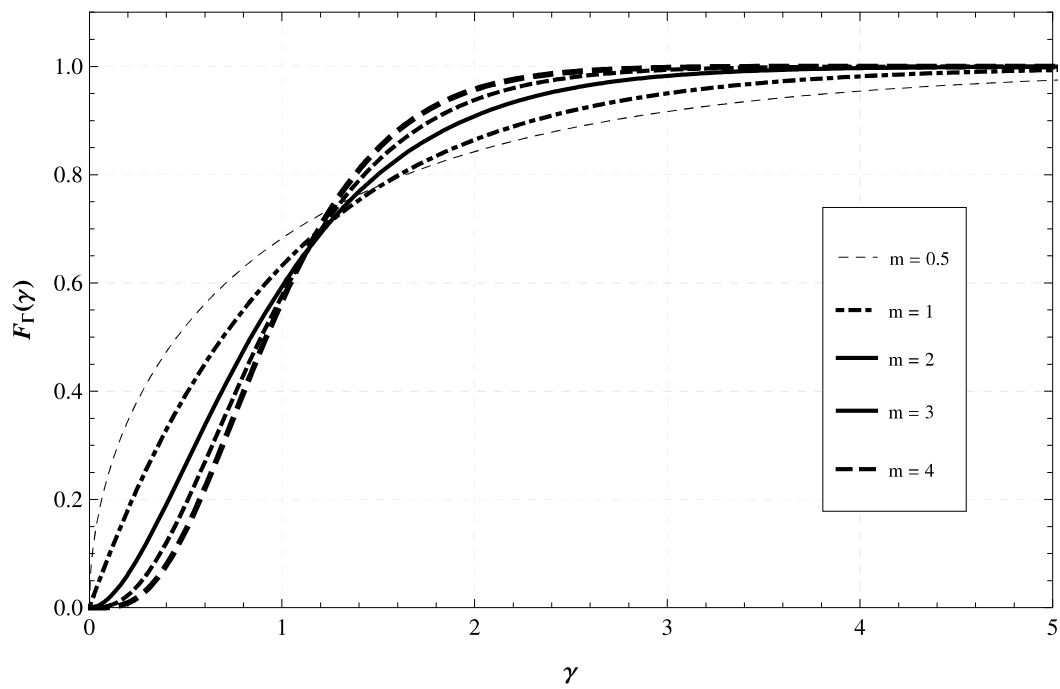


Figura 2.4: CDF da distribuição de Nakagami- m com m variando.

A degeneração da distribuição de Rice, fazendo $K \rightarrow 0$, resulta na distribuição de Rayleigh [26]. A CDF da envoltória para Rice pode ser obtida a partir da integração da PDF e é mostrada na Figura 2.6.

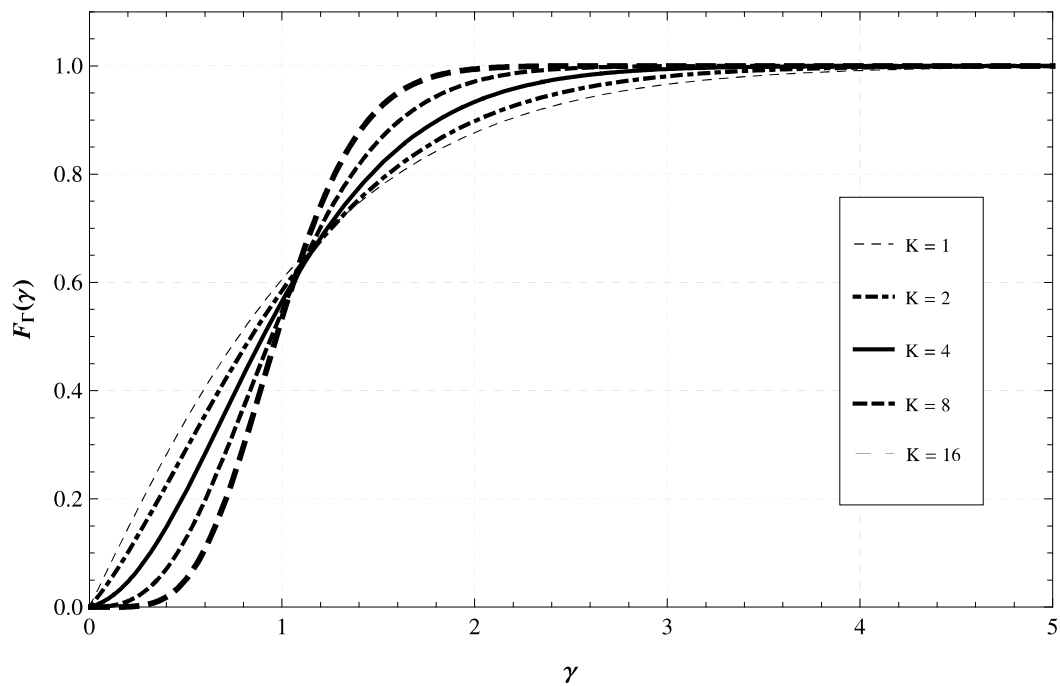


Figura 2.6: CDF da distribuição de Rice com K variando.

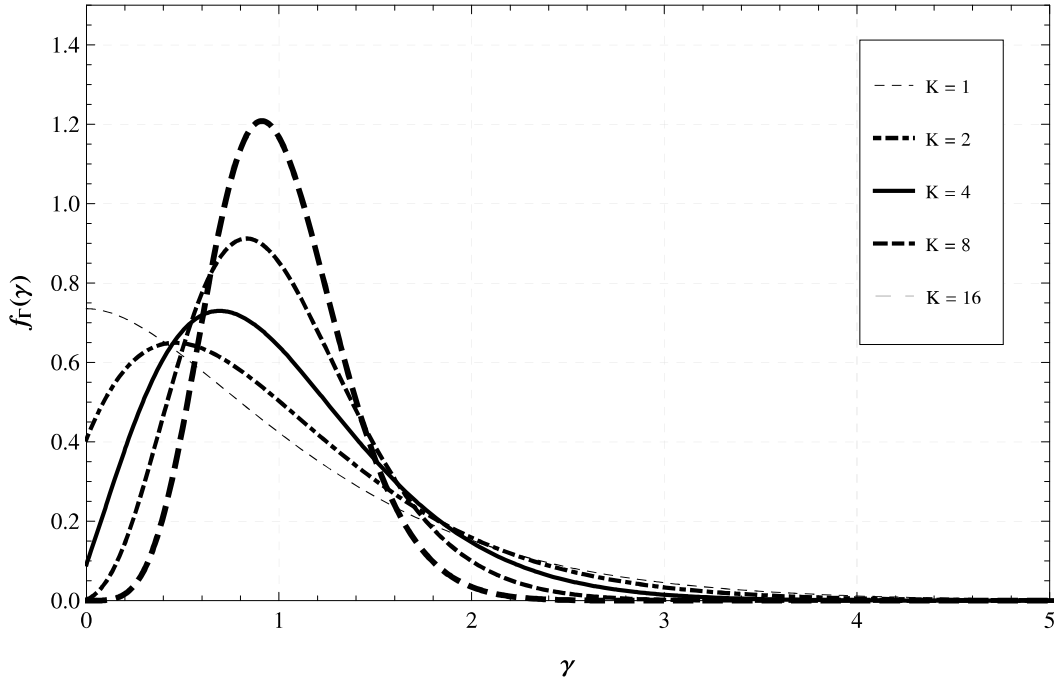


Figura 2.5: PDF da distribuição de Rice com K variando.

2.2.4 Distribuição de κ - μ

Para sinais com variações em pequena escala com linha de visada, a distribuição κ - μ generalizada pode ser usada para a representação desses canais de comunicação sem fio [27]. Os *clusters* de multipercurso possuem ondas dispersas com potências idênticas e dentro de cada *cluster* há uma componente dominante que apresenta uma potência arbitrária. O parâmetro κ representa a razão entre a potência total das componentes dominantes do sinal e a potência total das componentes espalhadas, e o parâmetro μ representa o número de *clusters* multipercursos presentes no ambiente.

A distribuição κ - μ apresenta para sua envoltória a seguinte PDF [27]:

$$f_{R_{\kappa-\mu}}(r) = \frac{2\mu(1+\kappa)^{\frac{\mu+1}{2}}}{\kappa^{\frac{\mu-1}{2}} \exp[\mu\kappa]} \frac{1}{\Omega_{\kappa-\mu}} \left(\frac{r}{\Omega_{\kappa-\mu}}\right)^{\mu} \exp\left[-\mu(1+\kappa)\left(\frac{r}{\Omega_{\kappa-\mu}}\right)^2\right] I_{\mu-1}\left[2\mu\sqrt{\kappa(1+\kappa)}\frac{r}{\Omega_{\kappa-\mu}}\right], \quad (2.9)$$

em que $R_{\kappa-\mu}$ é a variável aleatória da magnitude da envoltória do sinal modelado por κ - μ e Ω é a potência média do sinal transmitido ($E[R^2]$), com $r \geq 0$, $\kappa > 0$, $\mu > 0$ e $I_x[\cdot]$ é a função *Bessel* modificada de primeiro tipo e ordem x .

A PDF da distribuição κ - μ em função da SNR instantânea por símbolo transmitido é dada por:

$$f_{\Gamma_{\kappa-\mu}}(\gamma) = \frac{\mu(1+\kappa)^{\frac{\mu+1}{2}}}{\kappa^{\frac{\mu-1}{2}} \exp[\mu\kappa]} \frac{\gamma^{\frac{\mu-1}{2}}}{\bar{\gamma}^{\frac{\mu+1}{2}}} \exp\left[-\mu(1+\kappa)\frac{\gamma}{\bar{\gamma}}\right] I_{\mu-1}\left[2\mu\sqrt{\kappa(1+\kappa)}\frac{\gamma}{\bar{\gamma}}\right], \quad (2.10)$$

em que $\bar{\gamma}$ é a SNR média por símbolo transmitido, e $\gamma \geq 0$.

Como casos especiais, a distribuição κ - μ pode representar a distribuição Nakagami- m com $\kappa \rightarrow 0$ e $m = \mu$. A distribuição de Rice pode ser obtida com $\mu = 1$ e $\kappa = k$.

A variação dos parâmetros κ e μ é mostrada nas Figuras 2.7 e 2.8. É possível observar pelos gráficos que uma melhor comunicação é obtida quando temos valores altos de κ e μ visto que o desvanecimento é mais suave nestes cenários.

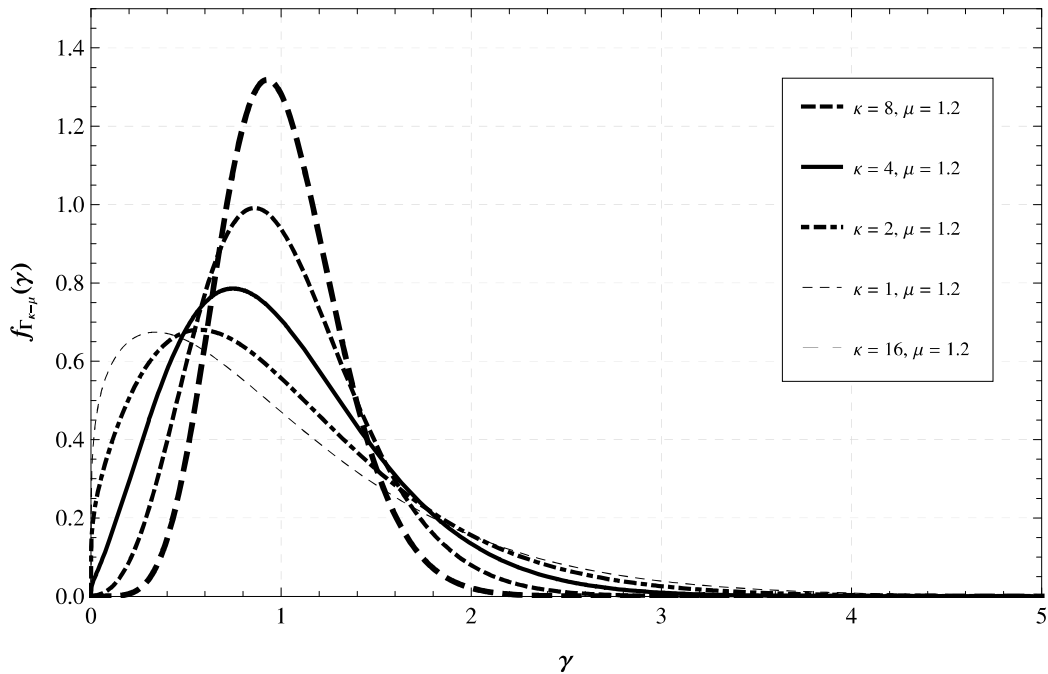


Figura 2.7: PDF da distribuição de Rice com K variando.

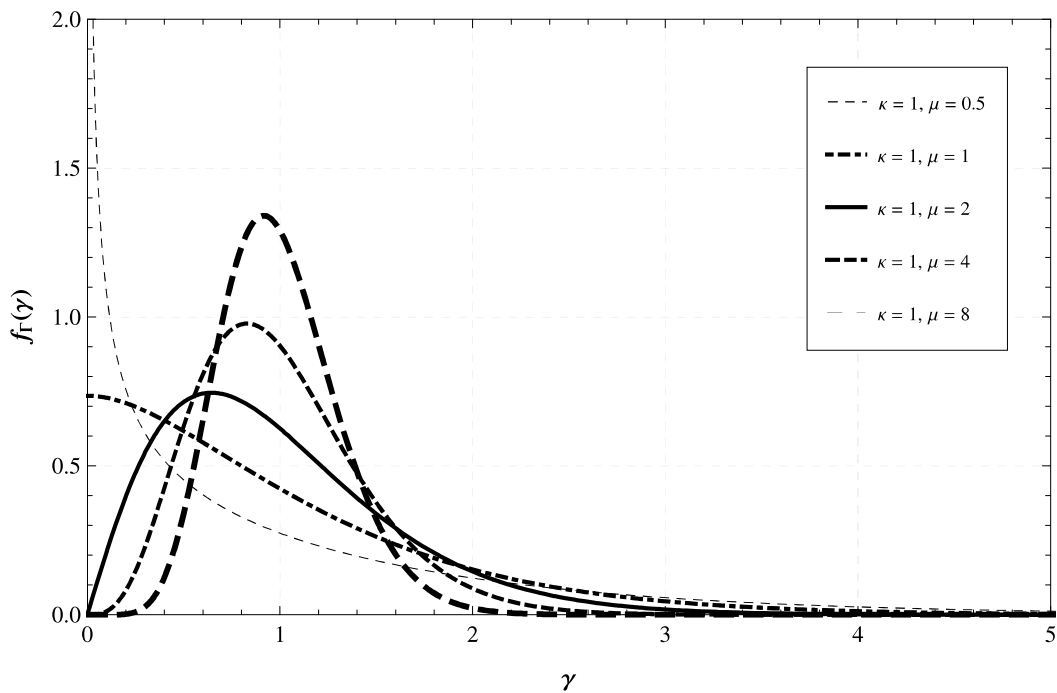


Figura 2.8: PDF da distribuição κ - μ com K variando.

A CDF da envoltória para κ - μ é mostrada na Figura 2.9.

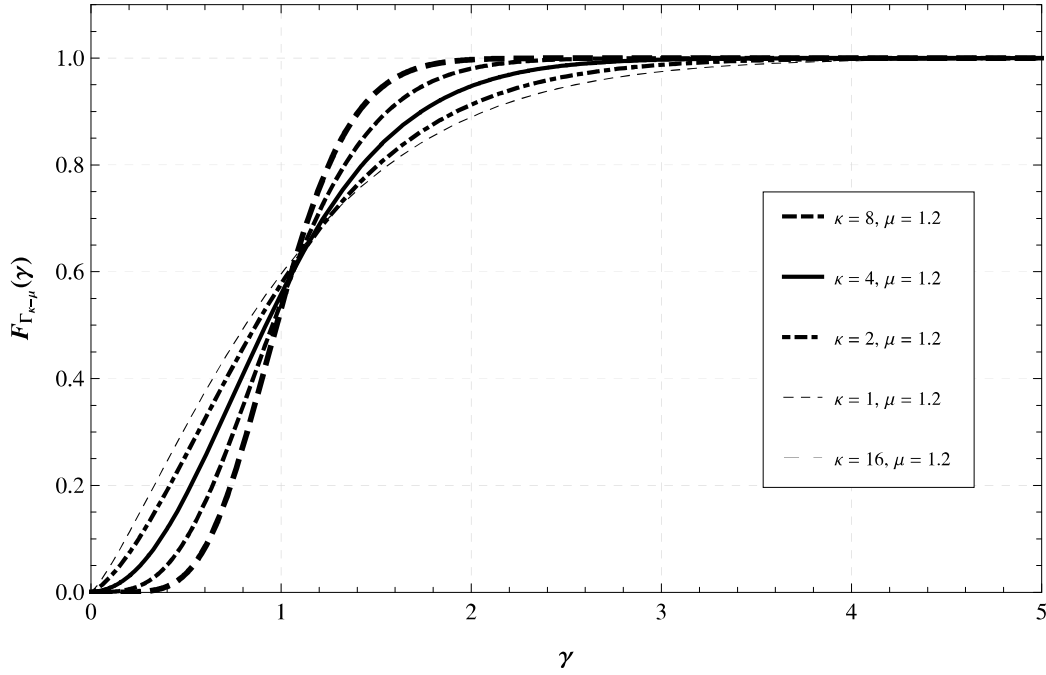


Figura 2.9: CDF da distribuição κ - μ .

2.2.5 Distribuição de κ - μ sombreada

A distribuição κ - μ sombreada é obtida a partir de uma generalização da distribuição κ - μ .

Diferentemente da distribuição κ - μ , no ambiente com sombreamento os componentes dominantes de todos os *clusters* podem flutuar aleatoriamente devido ao sombreamento. Dentro de cada *cluster*, assumimos que as ondas multipercurso espalhadas possuem potência idêntica e uma componente dominante com certa potência arbitrária.

A curva da PDF da SNR transmitida para a distribuição κ - μ sombreada é dada por [19]:

$$f_{\Gamma}(\gamma) = \frac{\mu^{\mu} s^s (1 + \kappa)^{\mu}}{\Gamma(\mu) \bar{\gamma} (\mu\kappa + s)^s} \left(\frac{\gamma}{\bar{\gamma}} \right)^{\mu-1} \exp^{-\frac{\mu(1+\kappa)\gamma}{\bar{\gamma}}} {}_1F_1 \left(s, \mu; \frac{\mu^2 \kappa (1 + \kappa) \gamma}{\mu\kappa + s \bar{\gamma}} \right), \quad (2.11)$$

$\kappa \geq 0$ é a relação entre a potência total das componentes dominantes e a potência total das ondas espalhadas. μ está relacionado ao número de *clusters* dos canais de comunicação. O sombreamento é representado por s . Com um s maior, observa-se um efeito menor de sombreamento. $\bar{\gamma}$ é a SNR média do canal e ${}_1F_1$ é a função Gamma Hipergeométrica Confluyente.

A CDF da SNR do sinal transmitido para a distribuição κ - μ sombreada é dada por [19]:

$$F_{\Gamma}(\gamma) = \frac{\mu^{\mu-1} s^s (1 + \kappa)^{\mu}}{\Gamma(\mu)(\mu\kappa + s)^s} \left(\frac{1}{\bar{\gamma}}\right)^{\mu} \gamma^{\mu} \quad (2.12)$$

$$\times \Phi_2 \left(\mu - s, s; \mu + 1; -\frac{\mu(1 + \kappa)\gamma}{\bar{\gamma}}, -\frac{\mu(1 + \kappa)}{\bar{\gamma}} \frac{s\gamma}{\mu\kappa + s} \right),$$

com Φ_2 como a função Hipergeométrica Bivariante Confluyente [28].

As curvas da PDF da κ - μ sombreada variando seus parâmetros são mostradas nas Figuras 2.10, 2.11 e 2.12.

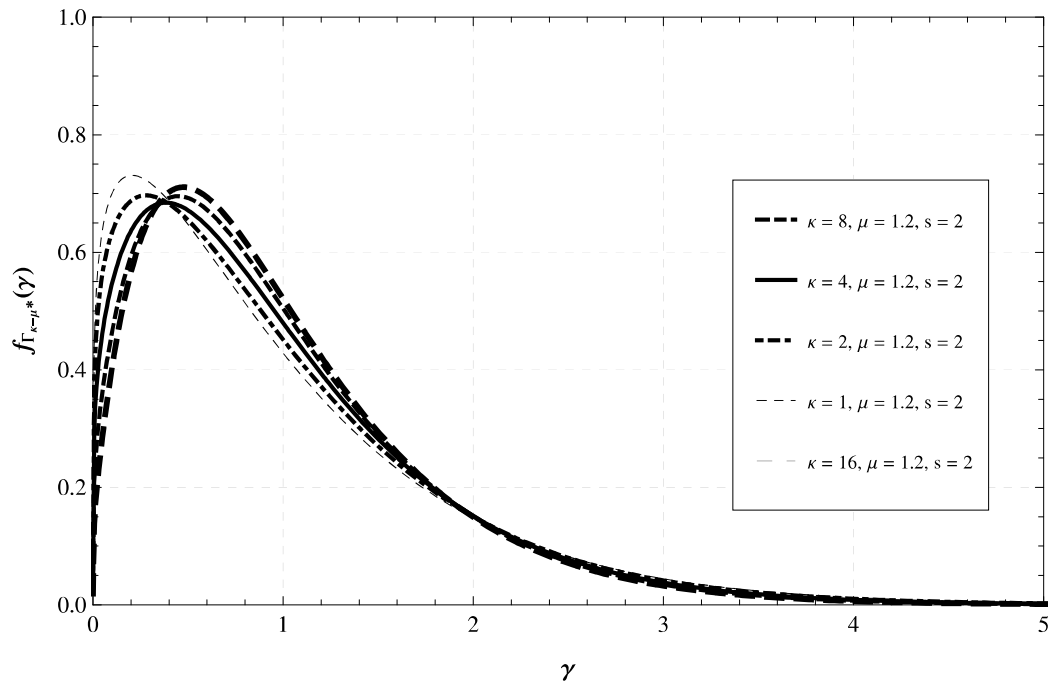


Figura 2.10: PDF da distribuição κ - μ sombreada com κ variando.

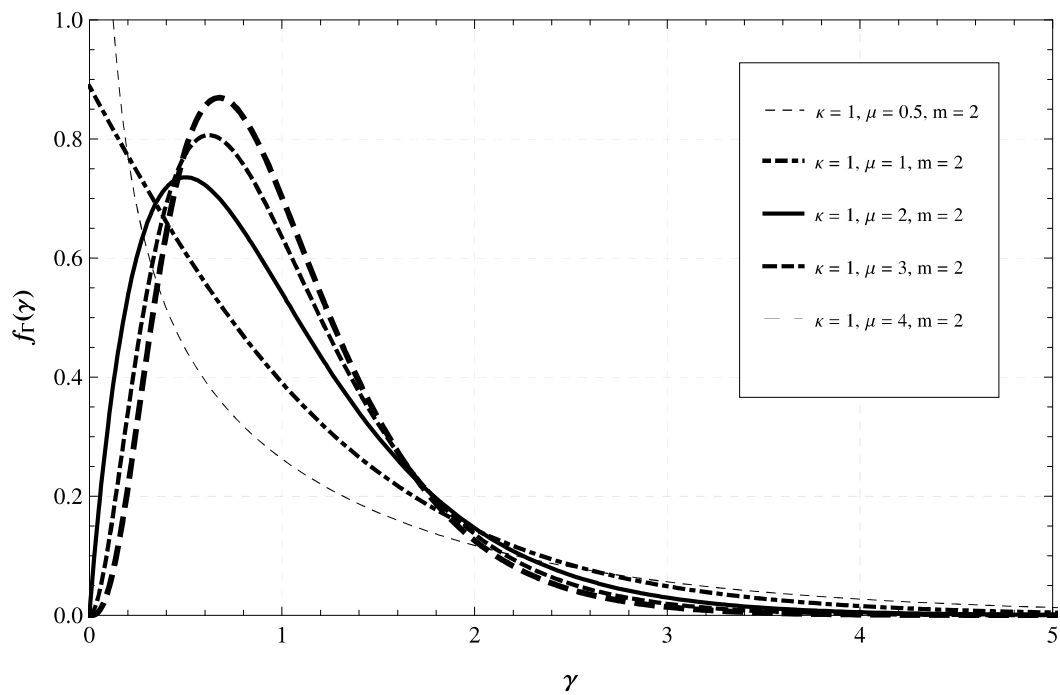


Figura 2.11: PDF da distribuição κ - μ sombreada com μ variando.

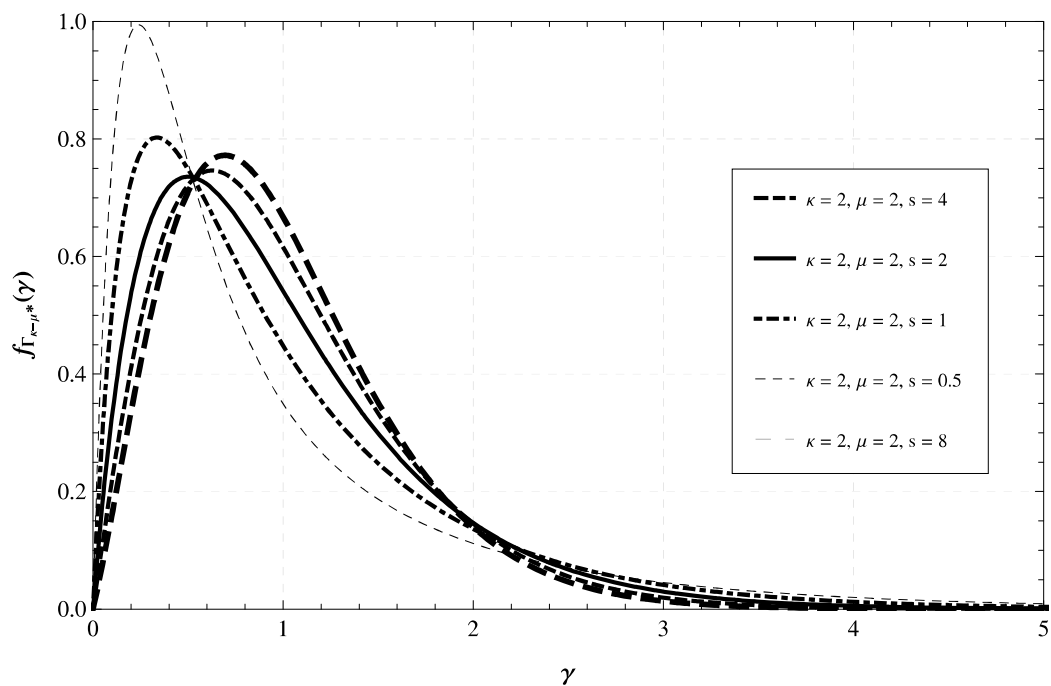


Figura 2.12: PDF da distribuição κ - μ sombreada com s variando.

A curva da CDF da κ - μ sombreada é mostrada na Figura 2.13.

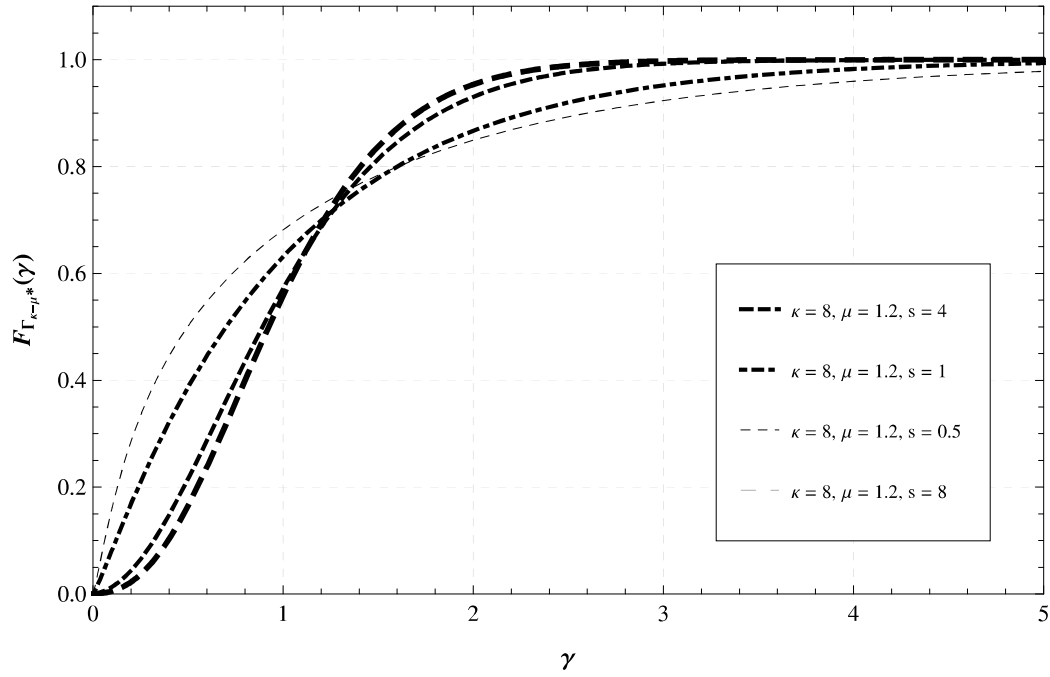


Figura 2.13: CDF da distribuição de κ - μ sombreada.

A variação nos parâmetros mencionados acima permitem a derivação de algumas outras distribuições a partir da própria κ - μ sombreada. Para obter estas distribuições com sombreado é preciso utilizar $s \rightarrow s$ A Tabela 2.1 mostra essa relação.

Tabela 2.1: Distribuições derivadas a partir do modelo κ - μ sombreado.

Modelos de Desvanecimento	Parâmetros do Canal
Gaussiana unilateral	$\mu = 0.5, \kappa \rightarrow 0, s = \infty$
Rayleigh	$\mu = 1, \kappa \rightarrow 0, s = \infty$
Nakagami- m	$\mu = m, \kappa \rightarrow 0, s = \infty$
Rice	$\mu = 1, \kappa = K, s = \infty$
Rice sombreada	$\mu = 1, \kappa = K$
κ - μ	$\mu = \mu, \kappa = \kappa, s = \infty$

2.3 Conclusão

Neste capítulo foram discutidos conceitos estatísticos e de modelagem de canal utilizados nas análises que serão realizadas neste trabalho. No próximo capítulo serão explicadas as técnicas de combate ao desvanecimento.

Capítulo 3

Técnicas de Combate ao Desvanecimento

Uma das formas de se alcançar uma maior confiabilidade e segurança na camada física que tem sido constante nos estudos mais recentes é o uso de técnicas de combate ao desvanecimento para este fim. O uso de múltiplas antenas de transmissão e recepção como MIMO, MRC e SC aumentam a segurança nas transmissões sem fio.

3.1 Maximal Ratio Combining

A técnica de diversidade conhecida como *Maximal Ratio Combiner*, MRC, é uma das arquiteturas de recepção combinada mais estudada. O MRC, normalmente, apresenta formulações analíticas convenientes, permitindo manipulações matemáticas mais fáceis [29] [30] [31].

No MRC os sinais de vários ramos ou canais são combinados juntamente com o ganho de cada um deles de forma proporcional ao nível do sinal RMS e inversamente proporcional ao ruído quadrático médio nesse canal. A Figura 3.1 mostra a arquitetura de uma recepção com MRC.

$$\gamma_{MRC} = \frac{E_b \|w\|^2}{\sigma^2} = \sum_{i=1}^L \frac{w_i^2 E_b}{\sigma^2} = \sum_{i=1}^L \gamma_i \quad (3.1)$$

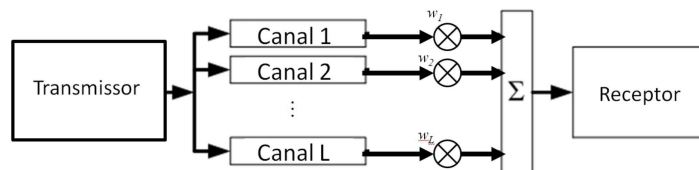


Figura 3.1: *Maximal Ratio Combiner* com L ramos

Com a SNR do MRC dada por $\gamma_{MRC} = \sum_{i=1}^L \gamma_i$, assumimos

$$\tilde{\gamma} = \bar{\gamma}_1 = \bar{\gamma}_2 = \dots = \bar{\gamma}_L, \quad (3.2)$$

com $\bar{\gamma}$ sendo a SNR média.

Então, para a PDF da MRC com a distribuição κ - μ sombreada usamos [31]

$$f_{\Gamma_{MRC}}(\gamma) = \frac{\tilde{\mu}^{\tilde{\mu}} \tilde{m}^{\tilde{m}} (1 + \kappa)^{\tilde{\mu}}}{\Gamma(\tilde{\mu}) (\tilde{\mu} \kappa + \tilde{m})^{\tilde{m}} \eta^{\tilde{\mu}}} \gamma^{\tilde{\mu}-1} \exp\left[-\frac{\tilde{\mu}(1+\kappa)}{\eta} \gamma\right] {}_1F_1\left(\tilde{m}; \tilde{\mu}; \left[\frac{\tilde{\mu}^2 \kappa (1 + \kappa)}{\tilde{\mu} \kappa + \tilde{m} \eta}\right] \gamma\right), \quad (3.3)$$

com $\tilde{\mu} = L\mu$, $\tilde{m} = Lm$, $\eta = L\gamma_0$ e L como número de ramos.

A Figura 3.2 mostra a curva da PDF da κ - μ sombreada com MRC variando a quantidade de ramos utilizados.

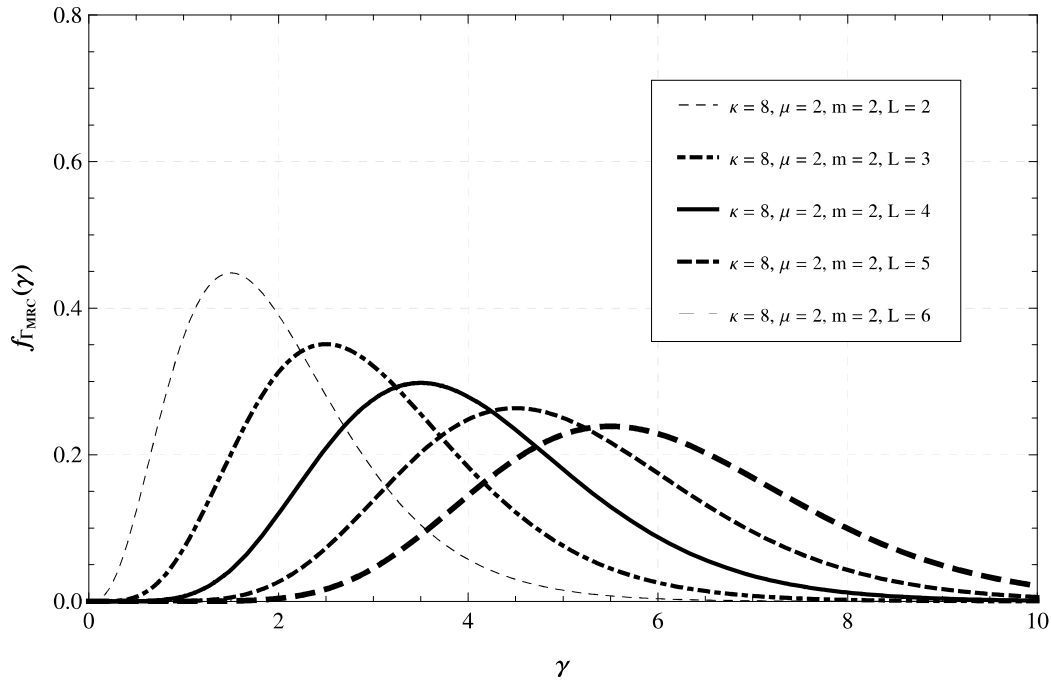


Figura 3.2: PDF da distribuição κ - μ sombreada com MRC variando L .

3.2 Multiple-Input Multiple-Output

Para as comunicações sem fio, a técnica de combate ao desvanecimento chamada de MIMO, do inglês *Multiple-Input Multiple-Output*, é um método para aumentar a capacidade de um link de rádio usando múltiplas antenas de transmissão e recepção explorando a propagação multipercuro. A Figura 3.3 mostra o esquema básico ponto a ponto com N_T antenas transmissoras e N_R antenas receptores utilizado no MIMO.

O sistema pode ser representado pelo modelo discreto no tempo em 3.4, [32].

$$\begin{bmatrix} y_1 \\ \vdots \\ y_{N_R} \end{bmatrix} = \begin{bmatrix} h_{11} & \cdots & h_{N_T} \\ \vdots & \ddots & \vdots \\ h_{N_R1} & \cdots & h_{N_R N_T} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_{N_T} \end{bmatrix} + \begin{bmatrix} n_1 \\ \vdots \\ n_{N_R} \end{bmatrix}, \quad (3.4)$$

x representa o símbolo transmitido, n é o vetor ruído, e H é a matriz de ganho, com h_{ij} representando o ganho da antena transmissora i com a antena receptora j . Consideramos canais de largura de banda B com ruído Gaussiano complexo com média zero e matriz de covariância $\sigma_n^2 \mathbf{I}_{N_R}$, em que $\sigma_n^2 = N_0 B$. Para fins de simplificação, dada uma potência de transmissão constante P iremos assumir um modelo equivalente com potência de ruído e potência de transmissão $P/\sigma_n^2 = \rho$, em que ρ pode ser interpretado como a SNR por antena receptora para cada canal.

O MIMO tem sido bastante investigado em termos de capacidade em vários tipos de canais de desvanecimento [33, 34, 35, 36], inclusive na distribuição κ - μ sombreada utilizada neste trabalho [37].

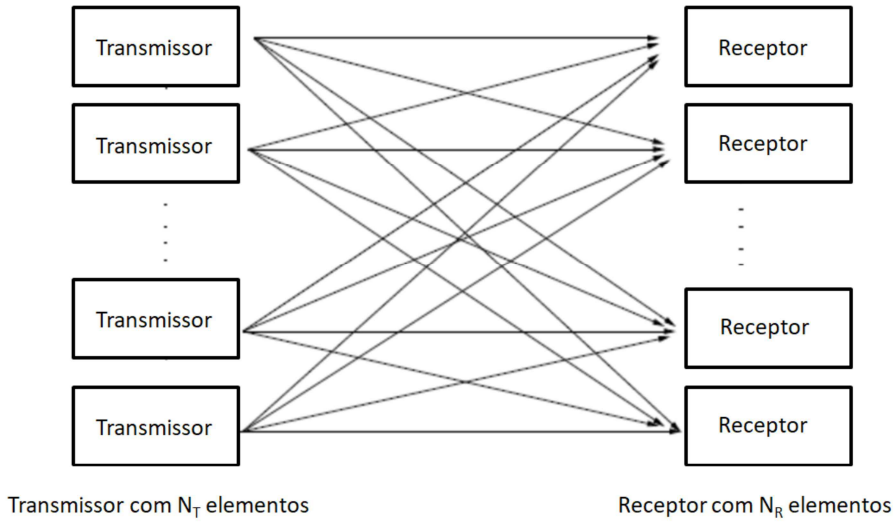


Figura 3.3: Esquema básico de antenas transmissoras e receptoras com a técnica de MIMO.

Em [19] é mostrado que a soma de L variáveis aleatórias κ - μ sombreadas independentes e identicamente distribuídas com parâmetros κ , μ e $\bar{\gamma}$ é também uma variável aleatória com distribuição κ - μ sombreada com parâmetros $L \times \kappa$, $L\mu$ e $L \times SNR$ médio. A partir deste resultado, temos que a pdf da potência recebida com N_t antenas transmissoras e N_r antenas receptoras pode ser expresso por [37]

$$f_{\Gamma_{MIMO}}(\gamma) = \frac{\tilde{\mu}^{\tilde{\mu}} \tilde{m}^{\tilde{m}} (1 + \kappa)^{\tilde{\mu}}}{\Gamma(\tilde{\mu}) (\tilde{\mu} \kappa + \tilde{m})^{\tilde{m}} \tilde{\eta}^{\tilde{\mu}}} \gamma^{\tilde{\mu}-1} \exp^{-[\frac{\tilde{\mu}(1+\kappa)}{\tilde{\eta}}] \gamma} {}_1F_1\left(\tilde{m}; \tilde{\mu}; \left[\frac{\tilde{\mu}^2 \kappa (1 + \kappa)}{\tilde{\mu} \kappa + \tilde{m} \tilde{\eta}}\right] \gamma\right), \quad (3.5)$$

com $\tilde{\mu} = N_t N_r \mu$, $\tilde{m} = N_t N_r m$, $\eta = N_t N_r \bar{\gamma}$ e $\bar{\gamma}$ como a SNR média do sinal transmitido. Esta equação pode ser reduzida para

$$f_{\Gamma}(\gamma) = \psi \gamma^{\tilde{\mu}-1} e^{-\beta\gamma} {}_1F_1(\tilde{m}; \tilde{\mu}; \zeta\gamma), \quad (3.6)$$

em que $\psi = \frac{\tilde{\mu}^{\tilde{\mu}} \tilde{m}^{\tilde{m}} (1+\kappa)^{\tilde{\mu}}}{\Gamma(\tilde{\mu})(\tilde{\mu}\kappa+\tilde{m})^{\tilde{m}} \eta^{\tilde{\mu}}}$, $\beta = \left[\frac{\tilde{\mu}(1+\kappa)}{\eta} \right]$ e $\zeta = \left[\frac{\tilde{\mu}^2 \kappa (1+\kappa)}{(\tilde{\mu}\kappa+\tilde{m})\eta} \right]$.

A Figura 3.4 mostra a curva da PDF da κ - μ sombreada com MIMO variando a quantidade de elementos na transmissão e na recepção.

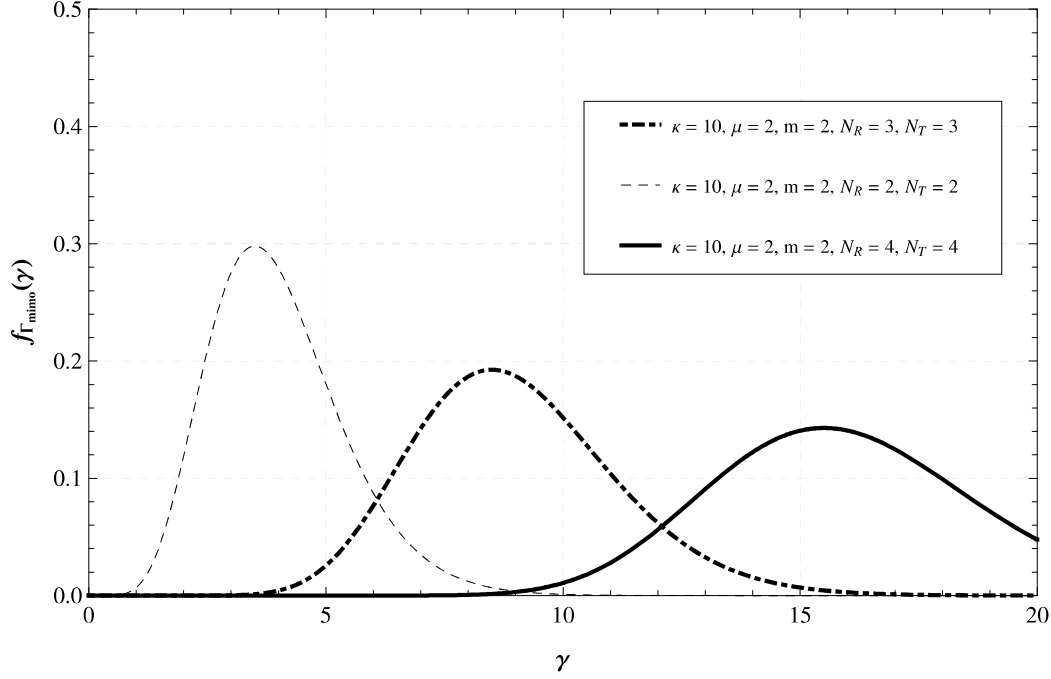


Figura 3.4: PDF da distribuição κ - μ sombreada com MIMO variando N_R e N_T

3.3 Selection Combining

Na técnica *Selection Combining*, o receptor recebe N cópias da mesma mensagem transmitida, como mostrado na Figura 3.5. O receptor seleciona a antena com a potência de sinal recebida mais alta e ignora os sinais das outras antenas. Então no SC

$$w_k = \begin{cases} 1 & \gamma_k = \max_n \{\gamma_n\} \\ 0 & \text{Outros casos} \end{cases} \quad (3.7)$$

em que γ_k é o SNR do sinal de saída.

A CDF da SNR instantânea após utilizada a técnica de SC pode ser escrita da seguinte

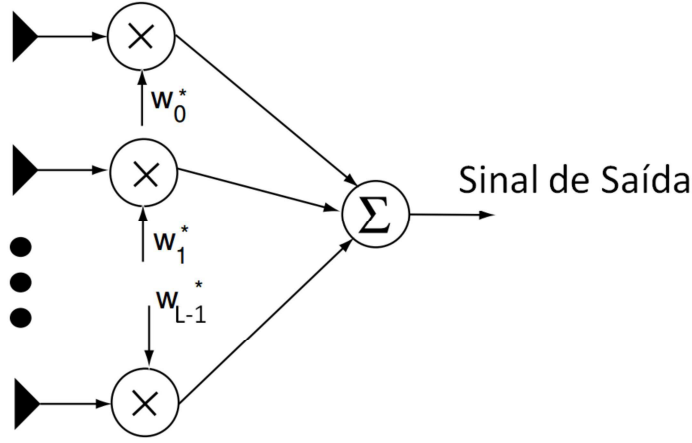


Figura 3.5: Esquema básico utilizado na técnica SC.

forma para ramos independentes e identicamente distribuídos

$$\begin{aligned}
 F_{\Gamma_{SD}}(\gamma_{SD}) &= P(\gamma_i \leq \gamma_{SD}, i = 1, \dots, L) = \prod_{i=1}^L P(\gamma_i \leq \gamma_{SD}) \\
 &= \left(\int_{-\infty}^{\gamma_{SD}} f_{\Gamma_{SD}}(\gamma_i) d\gamma_i \right)^L.
 \end{aligned} \tag{3.8}$$

Então, é possível derivar a PDF da distribuição κ - μ sombreada com SC.

$$\begin{aligned}
 f_{\Gamma_{SD}}(\gamma_{SD}) &= \frac{d}{d\gamma_{SD}} F(\gamma_{SD}) \\
 &= \frac{1}{\gamma_0 \Gamma(\mu)} \exp^{-\frac{\gamma_{SD}(1+\kappa)\mu}{\gamma_0}} L m^m \left(\frac{\gamma_{SD}}{\gamma_0} \right)^{-1+\mu} (1+\kappa)^\mu \mu^\mu (m+\kappa\mu)^{-m} \\
 &\times {}_1F_1 [m; \mu; \gamma_{SD} T] \left(\int_0^{\gamma_{SD}} \frac{1}{\gamma_0 \Gamma(\mu)} \exp^{-\frac{\gamma(1+\kappa)\mu}{\gamma_0}} m^m \left(\frac{\gamma}{\gamma_0} \right)^{-1+\mu} \right. \\
 &\times \left. (1+\kappa)^\mu \mu^\mu (m+\kappa\mu)^{-m} {}_1F_1 [m; \mu; \gamma T] d\gamma \right)^{L-1},
 \end{aligned} \tag{3.9}$$

com $T = \frac{\kappa(1+\kappa)\mu^2}{\gamma_0(m+\kappa\mu)}$, L é o número de ramos e $\gamma_{SD} = \max \{\gamma_1, \gamma_2, \dots, \gamma_L\}$.

A Figura 3.6 mostra a curva da PDF da κ - μ sombreada com Selection Combining comparada com a distribuição κ - μ sombreada sem combate ao desvanecimento.

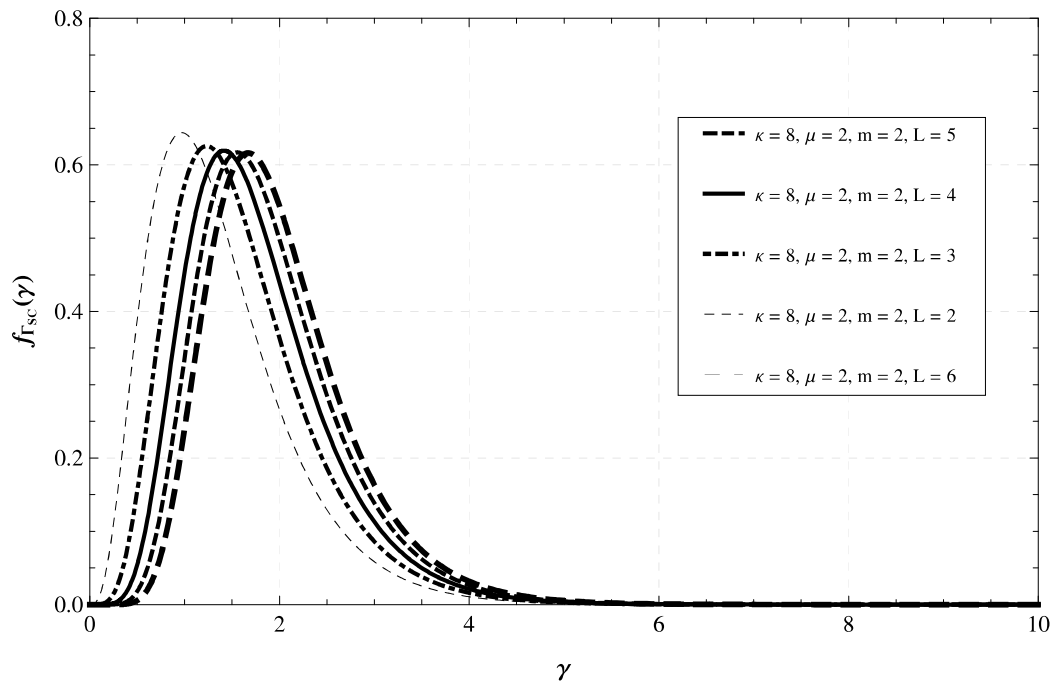


Figura 3.6: PDF da distribuição κ - μ sombreada com SC variando L .

3.4 Conclusão

Neste capítulo foi realizada uma revisão teórica das técnicas de combate ao desvanecimento SC, MRC e MIMO, as quais serão utilizadas nos próximos capítulos deste trabalho na análise de segurança na camada física. No próximo capítulo serão mostradas as métricas de segurança utilizadas na caracterização de um canal seguro.

Capítulo 4

Métricas de Segurança

Como têm sido amplamente discutido neste trabalho, as questões acerca de segurança e privacidade têm ganhado grande importância nas análises das redes de comunicações sem fio. E com o foco nas camadas mais inferiores, mais especificamente na camada física, surge a necessidade da caracterização dos ambientes de propagação quando existem canais intrusos no sistema.

Neste capítulo um estudo mais aprofundado acerca das métricas de segurança é realizado. Entre as métricas analisadas estão a probabilidade de Capacidade Estritamente Positiva (do inglês, *Strictly Positive Secrecy Capacity*, SPSC), a Probabilidade de Interrupção de Sigilo (do inglês, *Secrecy Outage Probability*) e a Capacidade Média de Sigilo (do inglês, *Average Secrecy Capacity*).

4.1 Capacidade de Sigilo

Como já discutido no capítulo 2, este trabalho é baseado no modelo clássico de escuta de Wyner, e a partir desse conceito usaremos a configuração mostrada na Figura 4.1 de [38].

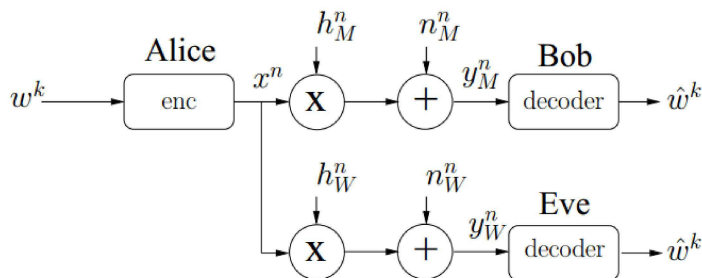


Figura 4.1: Configuração base.

A mensagem w_k é transmitida como a mensagem codificada $x_n = [x(1), \dots, x(i), \dots, x(n)]$. $h_M(i)$ é o ganho do canal complexo do canal principal, entre

Alice e Bob, $h_W(i)$ é o ganho complexo do canal intruso, entre Alice e Eve. $n_m(i)$ é o ruído Gaussiano encontrado no canal principal, e $n_W(i)$ para o canal intruso.

Desta forma, temos como saída o sinal recebido pelo receptor legítimo Bob e o sinal recebido pelo receptor intruso Eve como

$$y_M = h_M(i)x(i) + n_M(i) \quad (4.1)$$

$$y_W = h_W(i)x(i) + n_W(i). \quad (4.2)$$

A SNR instantânea recebida por Bob e por Eve é dada por

$$\gamma_M(i) = \frac{P |h_M(i)|^2}{N_M} = \frac{P |h_M|^2}{N_M} = \gamma_M, \quad (4.3)$$

e

$$\gamma_W(i) = \frac{P |h_W(i)|^2}{N_W} = \frac{P |h_W|^2}{N_W} = \gamma_W, \quad (4.4)$$

em que N_M e N_W representam a potência do ruído no canal principal e intruso, respectivamente, e P é a potência média do sinal transmitido, em que o canal é limitado por $\frac{1}{n} \sum_{i=1}^n E [|X(i)|^2] \leq P$, $X(i)$ é potência do sinal transmitido.

Para um cenário com $N_W > N_M$, ou seja, a potência do ruído no canal intruso é maior que a potência do ruído do canal principal e ambos são canais com ruídos AWGN complexos, a capacidade de sigilo do canal pode ser dada por [39]

$$C_S = C_M - C_W, \quad (4.5)$$

em que a capacidade do canal principal é dada por [40]

$$C_M = \frac{1}{2} \log \left(1 + \frac{P}{N_M} \right), \quad (4.6)$$

e a capacidade do canal intruso é dada por

$$C_W = \frac{1}{2} \log \left(1 + \frac{P}{N_W} \right). \quad (4.7)$$

Dado que ambos canais de ruído são considerados AWGN complexos, cada um deles pode ser considerado como a soma de dois canais AWGN reais [41]. A capacidade de sigilo do canal pode ser dada por

$$C_S = \log \left(1 + \frac{P}{N_M} \right) - \log \left(1 + \frac{P}{N_W} \right). \quad (4.8)$$

Para o cenário proposto anteriormente, temos

$$C_S = \log \left(1 + |h_M|^2 \frac{P}{N_M} \right) - \log \left(1 + |h_W|^2 \frac{P}{N_W} \right). \quad (4.9)$$

Com o SNR do canal principal e intruso como $\gamma_M = P |h_M(i)|^2 / N_M$ e $\gamma_W = P |h_W(i)|^2 / N_W$, respectivamente, e com a não negatividade da capacidade do canal, temos

$$C_S = \begin{cases} \log(1 + \gamma_M) - \log(1 + \gamma_W) & \text{se } \gamma_M > \gamma_W \\ 0 & \text{se } \gamma_M \leq \gamma_W \end{cases} \quad (4.10)$$

4.2 Probabilidade de Interrupção de Sigilo

A primeira métrica de segurança que será tratada é a Probabilidade de Interrupção de Sigilo. A SOP é uma métrica geralmente utilizada como indicador bruto de desempenho, usada para caracterizar a segurança em canais de comunicações sem fio, inclusive em regimes com diversidade. Ela é definida como a probabilidade da capacidade de sigilo ficar abaixo de um determinado limiar, havendo dessa forma a interrupção do sigilo na comunicação entre as partes legítimas quando este limiar não é respeitado. Definimos este limiar como C_{th} , o qual deverá sempre ser maior ou igual a zero. A SOP é definida como [42] com $\Theta = \exp(C_{th}) \geq 1$ como

$$SOP = P \{ C_s(\gamma_R, \gamma_E) \leq C_{th} \} \quad (4.11)$$

Como já definimos anteriormente

$$C_S = \log(1 + \gamma_M) - \log(1 + \gamma_W) \text{ se } \gamma_M > \gamma_W. \quad (4.12)$$

Realizando as devidas substituições

$$\begin{aligned} SOP &= P \{ \ln(1 + \gamma_R) - \ln(1 + \gamma_E) \leq C_{th} \} \\ &= P \left\{ \frac{\exp^{\ln(1 + \gamma_R)}}{\exp^{\ln(1 + \gamma_E)}} \leq \exp^{C_{th}} \right\} \\ &= P \left\{ \frac{1 + \gamma_R}{1 + \gamma_E} \leq \Theta \right\} \\ &= P \{ \gamma_R \leq \Theta \gamma_E + \Theta - 1 \}. \end{aligned} \quad (4.13)$$

Com f_R e f_E como funções de distribuição do canal principal e intruso, a probabilidade

da capacidade de sigilo ficar abaixo de um determinado limiar é dada por

$$SOP = \int_0^\infty \int_0^{\Theta\gamma_E + \Theta - 1} f_R(\gamma_R) d\gamma_R f_E(\gamma_E) d\gamma_E. \quad (4.14)$$

Para o caso específico da distribuição κ - μ sombreada temos

$$\begin{aligned} SOP &= \int_0^\infty \frac{1}{\bar{\gamma}_E \Gamma(\mu_E)} \exp^{-\frac{\gamma_E(1+\kappa_E)\mu_E}{\bar{\gamma}_E}} m^m \left(\frac{\gamma_E}{\bar{\gamma}_E}\right)^{-1+\mu_E} (1+\kappa_E)^{\mu_E} \mu_E^{\mu_E} (m+\kappa_E\mu_E)^{-m} \\ &\times {}_1F_1 \left[m; \mu_E; \frac{\gamma_E \kappa_E (1+\kappa_E) \mu_E^2}{\bar{\gamma}_E (m+\kappa_E\mu_E)} \right] \int_0^{-1+\theta+\gamma_E\theta} \frac{1}{\bar{\gamma}_R \Gamma(\mu_R)} \exp^{-\frac{\gamma_R(1+\kappa_R)\mu_R}{\bar{\gamma}_R}} m^m \\ &\times \left(\frac{\gamma_R}{\bar{\gamma}_R}\right)^{-1+\mu_R} (1+\kappa_R)^{\mu_R} \mu_R^{\mu_R} (m+\kappa_R\mu_R)^{-m} \\ &\times {}_1F_1 \left[m; \mu_R; \frac{\gamma_R \kappa_R \mu_R^2 (1+\kappa_R) \mu_R^2}{\bar{\gamma}_R (m+\kappa_R\mu_R)} \right] d\gamma_R d\gamma_E. \end{aligned} \quad (4.15)$$

4.3 Probabilidade de Capacidade de Sigilo Estritamente Positiva

A Probabilidade de Capacidade de Sigilo Estritamente Positiva é Obtida quando a capacidade de sigilo do canal de comunicação estabelecido é sempre positiva, ou seja, quando caracterizamos um canal seguro.

Supondo que o transmissor tenha informações do estado do canal principal e do canal intruso, como em transmissões que utilizam TDMA, com o intruso sendo mais um usuário interagindo na rede. O transmissor pode aproveitar esta informação acerca do estado da rede em ambos canais para obter uma comunicação segura enviando símbolos úteis ao receptor legítimo somente quando a capacidade de sigilo do canal for estritamente positiva. Dessa forma, mesmo com uma probabilidade de interrupção de sigilo alta, é possível para o transmissor e receptor protegerem a troca de dados.

Esta métrica é definida como [42]

$$SPSC = P \{C_s(\gamma_R, \gamma_E) > 0\} \quad (4.16)$$

Realizando as devidas substituições

$$\begin{aligned}
SPSC &= P \{ \ln(1 + \gamma_R) - \ln(1 + \gamma_E) > 0 \} \\
&= P \left\{ \frac{\exp^{\ln(1+\gamma_R)}}{\exp^{\ln(1+\gamma_E)}} > \exp^0 \right\} \\
&= P \left\{ \frac{1 + \gamma_R}{1 + \gamma_E} > 1 \right\} \\
&= P \{ \gamma_E < \gamma_R \}.
\end{aligned} \tag{4.17}$$

Com f_R e f_E como funções de distribuição do canal principal e intruso, a probabilidade da capacidade de sigilo estritamente positiva é dada por

$$SPSC = \int_0^\infty \int_0^{\gamma_R} f_R(\gamma_R) d\gamma_R f_E(\gamma_E) d\gamma_E. \tag{4.18}$$

Para o caso específico da distribuição κ - μ sombreada temos

$$\begin{aligned}
SPSC &= \int_0^\infty \frac{1}{\bar{\gamma}_R \Gamma(\mu_R)} \exp^{-\frac{\gamma_R(1+\kappa_R)\mu_R}{\bar{\gamma}_R}} m^m \left(\frac{\gamma_R}{\bar{\gamma}_R} \right)^{-1+\mu_R} (1 + \kappa_R)^{\mu_R} \mu_R^{\mu_R} (m + \kappa_R \mu_R)^{-m} \\
&\times {}_1F_1 \left[m; \mu_R; \frac{\gamma_R \kappa_R (1 + \kappa_R) \mu_R^2}{\bar{\gamma}_R (m + \kappa_R \mu_R)} \right] \int_0^{-1+\gamma_R} \frac{1}{\bar{\gamma}_E \Gamma(\mu_E)} \exp^{-\frac{\gamma_E(1+\kappa_E)\mu_E}{\bar{\gamma}_E}} m^m \\
&\times \left(\frac{\gamma_E}{\bar{\gamma}_E} \right)^{-1+\mu_E} (1 + \kappa_E)^{\mu_E} \mu_E^{\mu_E} (m + \kappa_E \mu_E)^{-m} \\
&\times {}_1F_1 \left[m; \mu_E; \frac{\gamma_E \kappa_E (1 + \kappa_E) \mu_E^2}{\bar{\gamma}_E (m + \kappa_E \mu_E)} \right] d\gamma_E d\gamma_R
\end{aligned} \tag{4.19}$$

4.4 Capacidade Média de Sigilo

A Capacidade Média de Sigilo é a média da máxima taxa de transmissão obtida para um canal seguro[12]. Esta métrica é importante para a caracterização do canal de comunicação, por exemplo, quando o transmissor tem informações do estado do canal intruso, o esquema de transmissão pode ser adaptado (como mencionado em 4.3) e teoricamente, qualquer taxa média de comunicação segura abaixo da capacidade média de sigilo do canal é alcançável.

A capacidade média do canal é obtida por [12]

$$\begin{aligned}
ASC &= \int_0^\infty \int_0^\infty C_S(\gamma_R, \gamma_E) f(\gamma_R, \gamma_E) d\gamma_R d\gamma_E \\
&= \int_0^\infty \ln(1 + \gamma_R) f_R \left(\int_0^{\gamma_R} f_E(\gamma_E) d\gamma_E \right) d\gamma_R \\
&\quad - \int_0^\infty \ln(1 + \gamma_E) f_E(\gamma_E) \int_{\gamma_E}^\infty f_R(\gamma_R) d\gamma_R d\gamma_E.
\end{aligned} \tag{4.20}$$

Para o caso específico da distribuição κ - μ sombreada temos

$$\begin{aligned}
ASC &= \int_0^\infty \left(\alpha_R {}_1F_1 [m; \mu_R; \beta_R] \left(\int_0^{\gamma_R} \frac{\alpha_E {}_1F_1 [m; \mu_E; \beta_E]}{\bar{\gamma}_E \Gamma(\mu_E)} d\gamma_E \right) \log(1 + \gamma_R) \right) \\
&\quad / (\bar{\gamma}_R \Gamma(\mu_R)) d\gamma_R - \int_0^\infty \left(\alpha_E {}_1F_1 [m; \mu_E; \beta_E] \left(\int_{\gamma_E}^\infty \frac{\alpha_R {}_1F_1 [m; \mu_R; \beta_R]}{\bar{\gamma}_R \Gamma(\mu_R)} d\gamma_R \right) \log(1 + \gamma_E) \right) \\
&\quad / (\bar{\gamma}_E \Gamma(\mu_E)) d\gamma_E.
\end{aligned} \tag{4.21}$$

Com

$$\alpha_R = \exp^{-\frac{\gamma_R(1+\kappa_R)\mu_R}{\bar{\gamma}_R}} m^m \left(\frac{\gamma_R}{\bar{\gamma}_R} \right)^{-1+\mu_R} (1 + \kappa_R)^{\mu_R} \mu_R^{\mu_R} (m + \kappa_R \mu_R)^{-m}, \tag{4.22}$$

$$\alpha_E = \exp^{-\frac{\gamma_E(1+\kappa_E)\mu_E}{\bar{\gamma}_E}} m^m \left(\frac{\gamma_E}{\bar{\gamma}_E} \right)^{-1+\mu_E} (1 + \kappa_E)^{\mu_E} \mu_E^{\mu_E} (m + \kappa_E \mu_E)^{-m}, \tag{4.23}$$

$$\beta_R = \frac{\gamma_R \kappa_R (1 + \kappa_R) \mu_R^2}{\bar{\gamma}_R (m + \kappa_R \mu_R)}, \tag{4.24}$$

$$\beta_E = \frac{\gamma_E \kappa_E (1 + \kappa_E) \mu_E^2}{\bar{\gamma}_E (m + \kappa_E \mu_E)}. \tag{4.25}$$

4.5 Conclusão

Neste capítulo foram apresentadas as métricas de segurança SOP, SPSC e ASC. Estas métricas serão utilizadas para as análises do próximo capítulo, tornando-as essenciais para a caracterização e análises de canais de comunicação seguros.

Capítulo 5

Caracterização estatística da segurança de canais sem fio

Neste capítulo trataremos dos resultados obtidos. Para as análises realizadas foram utilizados os conceitos explorados nos capítulos anteriores baseados no modelo de desvanecimento κ - μ sombreado. Para este ambiente foram analisadas as métricas de segurança SOP, SPSC e ASC, utilizando técnicas de combate ao desvanecimento de forma a obter ambientes mais seguros. As formulações fechadas da SOP e SPSC também serão abordadas neste capítulo.

5.1 Metodologia Aplicada

A metodologia escolhida para este trabalho é baseada no modelo de escuta clássica de Wyner. O canal principal de comunicação entre os dois pontos legítimos será referenciado pela letra R , o canal intruso estabelecido entre o transmissor e o intruso será referenciado pela letra E .

Os limites analisados neste trabalho (Cth) são de 1.25 bps e 0 bps. Nas curvas de SOP, SPSC e ASC, K representa a relação entre a SNR média do canal principal e a SNR média do canal intruso, $\bar{\gamma}_R = K\bar{\gamma}_E$.

5.2 Formulações fechadas para a SOP e SPSC para canais κ - μ sombreados

Um dos resultados apresentados neste trabalho é a formulação fechada para as métricas de segurança na camada física SOP e a SPSC para o canal de desvanecimento κ - μ sombreado.

A fórmula 5.1, obtida conforme descrito no apêndice I.1, representa a SOP para canais de desvanecimento κ - μ sombreados com um limite para interrupção de sigilo de 0 bps.

$$\begin{aligned}
SOP = C_1 C_2 & \left(\sum_{n=0}^{\infty} \frac{s_R^{(n)} d_1^n}{\mu_R^{(n)} n!} \left(\frac{(1 + \kappa_R) \mu_R}{\bar{\gamma}_R} \right)^{(-\mu_R - n)} \right. \\
& \left(\sum_{s=0}^{\infty} \frac{s_E^{(s)} d_2^s}{\mu_E^{(s)} s!} \left(\frac{\left(\frac{(1 + \kappa_R) \mu_R}{\bar{\gamma}_R} \right)^{\mu_R + n} \Gamma(\mu_E + s + \mu_R + n)}{(\mu_R + n) \left(\frac{(1 + \kappa_R) \mu_R}{\bar{\gamma}_R} + \frac{(1 + \kappa_E) \mu_E}{\bar{\gamma}_E} \right)^{\mu_E + s + \mu_R + n}} \right) \right. \\
& \left. \left. {}_2F_1 \left(1; \mu_E + s + \mu_R + n; \mu_R + n + 1; \frac{\frac{(1 + \kappa_R) \mu_R}{\bar{\gamma}_R}}{\frac{(1 + \kappa_R) \mu_R}{\bar{\gamma}_R} + \frac{(1 + \kappa_E) \mu_E}{\bar{\gamma}_E}} \right) \right) \right), \tag{5.1}
\end{aligned}$$

em que

$$C_1 = \frac{1}{\bar{\gamma}_R \Gamma(\mu_R)} s_R^{s_R} \left(\frac{1}{\bar{\gamma}_R} \right)^{-1 + \mu_R} (1 + \kappa_R)^{\mu_R} \mu_R^{\mu_R} (s_R + \kappa_R \mu_R)^{-s_R} \tag{5.2}$$

$$C_2 = \frac{1}{\bar{\gamma}_E \Gamma(\mu_E)} s_E^{s_E} \left(\frac{1}{\bar{\gamma}_E} \right)^{-1 + \mu_E} (1 + \kappa_E)^{\mu_E} \mu_E^{\mu_E} (s_E + \kappa_E \mu_E)^{-s_E} \tag{5.3}$$

$$d_1 = \frac{\kappa_R (1 + \kappa_R) \mu_R^2}{\bar{\gamma}_R (s_R + \kappa_R \mu_R)}. \tag{5.4}$$

$$d_2 = \frac{\kappa_E (1 + \kappa_E) \mu_E^2}{\bar{\gamma}_E (s_E + \kappa_E \mu_E)}. \tag{5.5}$$

A fórmula 5.6, obtida conforme descrito no apêndice I.2, é a SPSC para canais de desvanecimento κ - μ sombreados.

$$\begin{aligned}
SPSC = C_1 C_2 & \left(\sum_{n=0}^{\infty} \frac{s_E^{(n)} d_1^n}{\mu_E^{(n)} n!} \left(\frac{(1 + \kappa_E) \mu_E}{\bar{\gamma}_E} \right)^{(-\mu_E - n)} \right. \\
& \left(\sum_{s=0}^{\infty} \frac{s_R^{(s)} d_2^s}{\mu_R^{(s)} s!} \left(\frac{\left(\frac{(1 + \kappa_E) \mu_E}{\bar{\gamma}_E} \right)^{\mu_E + n} \Gamma(\mu_R + s + \mu_E + n)}{(\mu_E + n) \left(\frac{(1 + \kappa_E) \mu_E}{\bar{\gamma}_E} + \frac{(1 + \kappa_R) \mu_R}{\bar{\gamma}_R} \right)^{\mu_R + s + \mu_E + n}} \right) \right. \\
& \left. \left. {}_2F_1 \left(1; \mu_R + s + \mu_E + n; \mu_E + n + 1; \frac{\frac{(1 + \kappa_E) \mu_E}{\bar{\gamma}_E}}{\frac{(1 + \kappa_E) \mu_E}{\bar{\gamma}_E} + \frac{(1 + \kappa_R) \mu_R}{\bar{\gamma}_R}} \right) \right) \right), \tag{5.6}
\end{aligned}$$

em que

$$C_1 = \frac{1}{\bar{\gamma}_R \Gamma(\mu_R)} s_R^{s_R} \left(\frac{1}{\bar{\gamma}_R} \right)^{-1+\mu_R} (1 + \kappa_R)^{\mu_R} \mu_R^{\mu_R} (s_R + \kappa_R \mu_R)^{-s_R} \quad (5.7)$$

$$C_2 = \frac{1}{\bar{\gamma}_E \Gamma(\mu_E)} s_E^{s_E} \left(\frac{1}{\bar{\gamma}_E} \right)^{-1+\mu_E} (1 + \kappa_E)^{\mu_E} \mu_E^{\mu_E} (s_E + \kappa_E \mu_E)^{-s_E} \quad (5.8)$$

$$d_1 = \frac{\kappa_E (1 + \kappa_E) \mu_E^2}{\bar{\gamma}_E (s_E + \kappa_E \mu_E)}. \quad (5.9)$$

$$d_2 = \frac{\kappa_R (1 + \kappa_R) \mu_R^2}{\bar{\gamma}_R (s_R + \kappa_R \mu_R)}. \quad (5.10)$$

5.3 Análise da SOP

Com o cenário já apresentado na seção 5.1 os gráficos a seguir foram obtidos para a análise SOP considerando um ambiente sem técnicas aplicadas e com técnicas de combate ao desvanecimento aplicadas.

5.3.1 Sem Técnicas de Combate ao Desvanecimento

Com os parâmetros $s_R = s_E = 3$ e $\mu_R = \mu_E = 2$ fixados, a Figura 5.1 mostra o comportamento da SOP variando os valores de κ_R e κ_E , com C_{th} igual a 0 bps. Em que K é a relação entre a SNR média do canal principal e do canal intruso, $\bar{\gamma}_R = K \bar{\gamma}_E$. A Figura 5.2 mostra o comportamento da SOP quando temos um valor mais alto de C_{th} , no caso $C_{th} = 1.25$ bps.

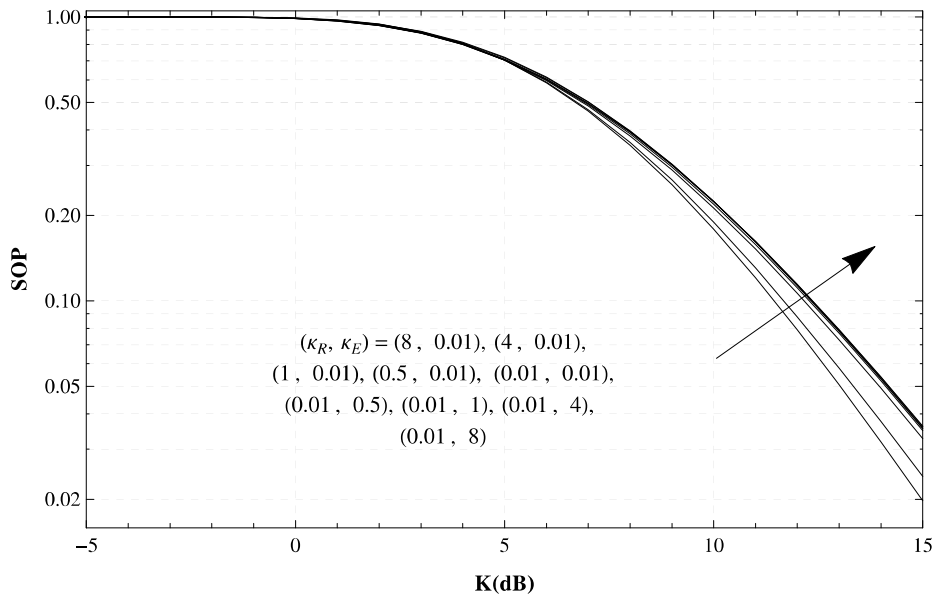


Figura 5.1: SOP sob canal κ - μ sombreado por K , variando κ_R e κ_E , com $Cth = 0$ bps.

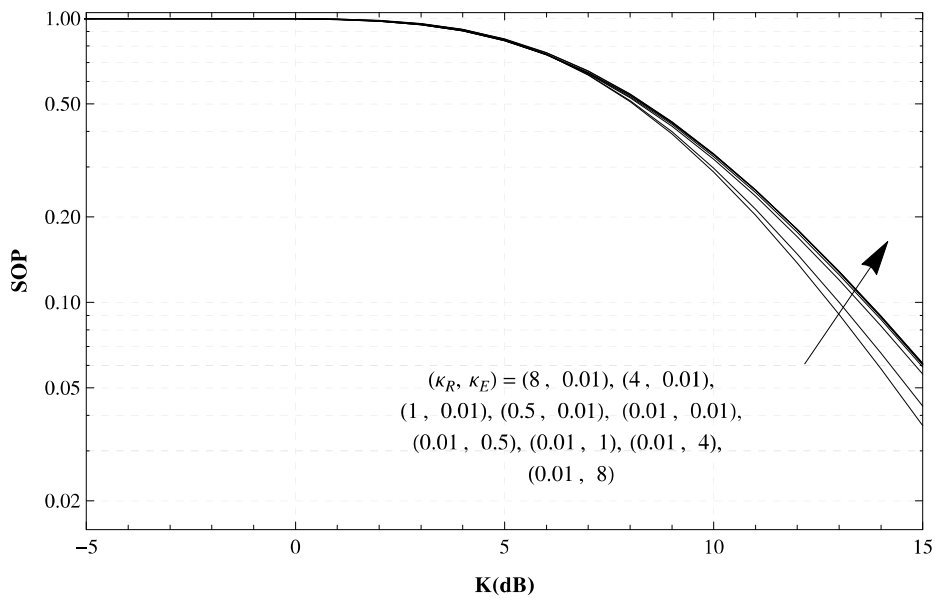


Figura 5.2: SOP sob canal κ - μ sombreado por K , variando κ_R e κ_E , com $Cth = 1.25$ bps.

É possível observar que quando o parâmetro κ do canal principal diminui, e cresce o valor deste parâmetro para o canal intruso temos uma maior SOP na comunicação estabelecida entre os dois pontos legítimos. E também é possível observar uma maior SOP quando temos um Cth maior, justificado pelo fato de que com um limiar maior a probabilidade de interrupção de sigilo aumenta em relação a um limiar mais restrito.

5.3.2 Com Técnicas de Combate ao Desvanecimento

A SOP ao se aplicar as técnicas de combate ao desvanecimento discutidas no capítulo 4 ao cenário apresentado anteriormente é mostrado logo abaixo.

5.3.2.1 Selection Combining

Aplicando a técnica de SC ao canal principal, com os parâmetros $s_R = s_E = 3$ e $\mu_R = \mu_E = 2$ fixados, variou-se κ do canal principal e do canal intruso com 2 ramos e com 4 ramos.

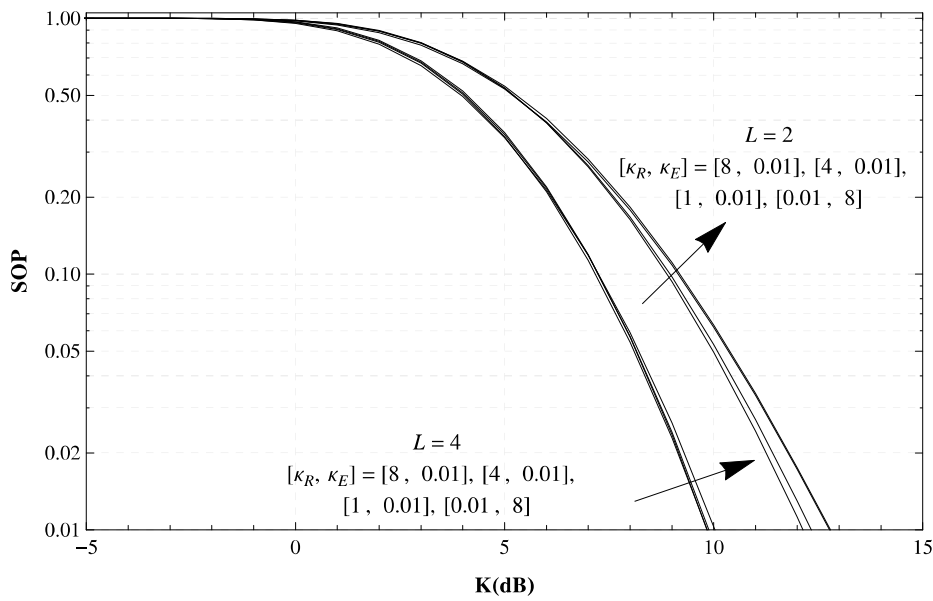


Figura 5.3: SOP sob canal κ - μ sombreado por K , variando κ_R e κ_E , com SC e $C_{th} = 0$ bps.

A Figura 5.3 mostra a SOP quando o canal principal aplica a técnica de diversidade SC com $C_{th}=0$ bps e a Figura 5.4 apresenta a mesma análise com $C_{th} = 1.25$ bps.

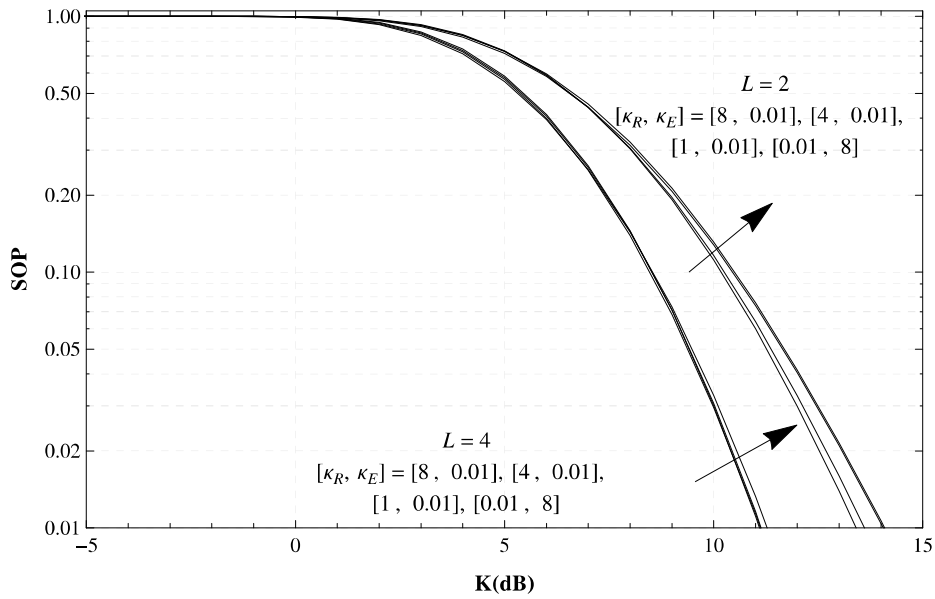


Figura 5.4: SOP sob canal κ - μ sombreado por K , variando κ_R e κ_E , com SC e $Cth = 1.25$ bps.

É possível observar que a SOP é menor quando aplicada a SC, e com uma quantidade maior de ramos a SOP decresce ainda mais.

5.3.2.2 MRC

Aplicando a técnica de MCR ao canal principal, com os parâmetros $s_R = s_E = 2$ e $\mu_R = \mu_E = 1.1$ fixados, variou-se κ do canal principal e do canal intruso com 2 ramos e com 4 ramos.

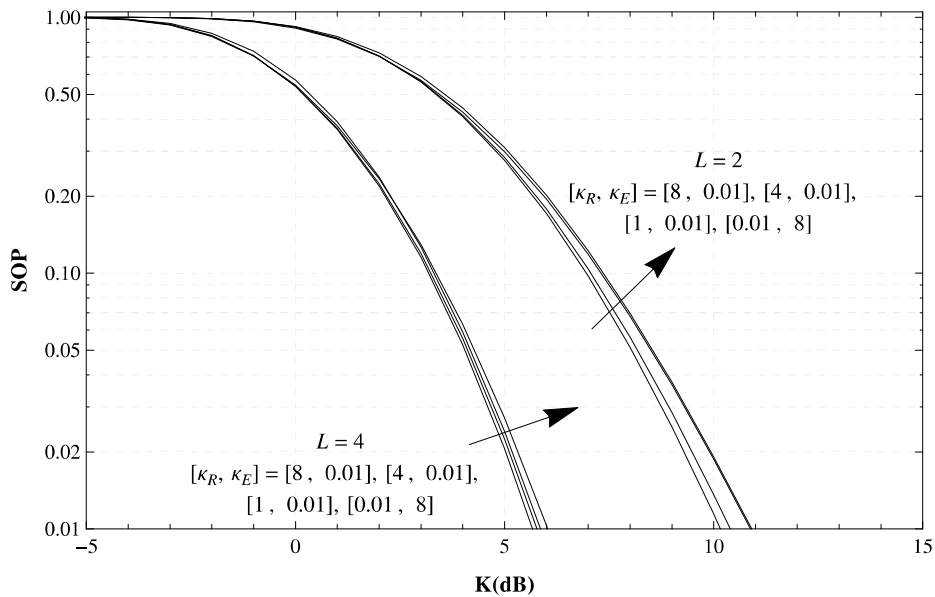


Figura 5.5: SOP sob canal κ - μ sombreado por K , variando κ_R e κ_E , com MRC e $Cth = 0$ bps.

A Figura 5.5 mostra a SOP quando o canal principal aplica a técnica de diversidade MRC com $C_{th}=0$ bps e a Figura 5.6 apresenta a mesma análise com $C_{th} = 1.25$ bps.

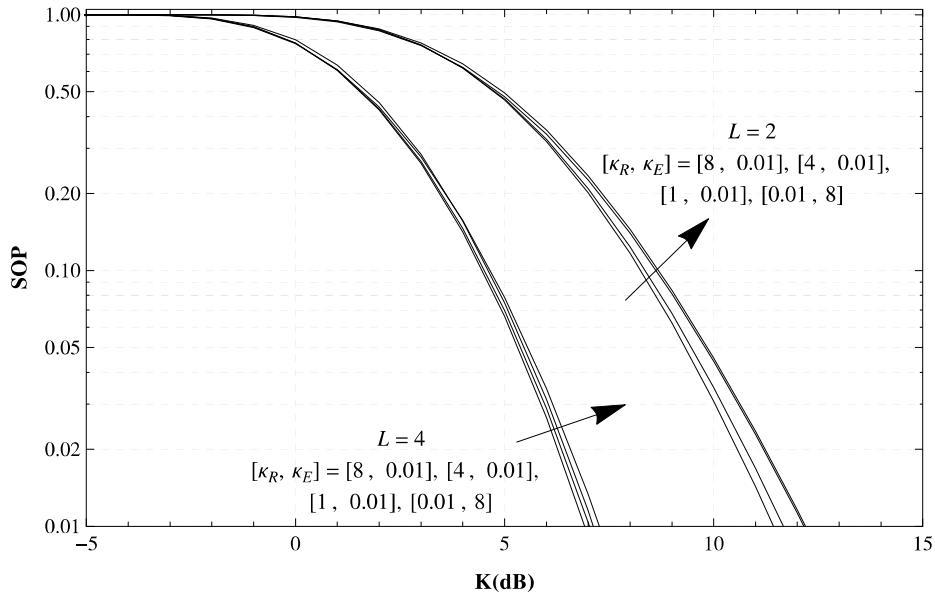


Figura 5.6: SOP sob canal κ - μ sombreado por K , variando κ_R e κ_E , com MRC e $C_{th} = 1.25$ bps.

Como no caso do uso do SC no canal principal, com o MRC é possível observar um menor SOP quando este é aplicado, e quanto maior o número de ramos aplicados, menor é a SOP.

5.3.2.3 MIMO

Aplicando a técnica de MIMO ao canal principal, com os parâmetros $s_R = s_E = 3$ e $\mu_R = \mu_E = 2$ fixados, variou-se κ do canal principal e do canal intruso com 2 e 4 nós na transmissão e com 2 e 4 nós na recepção.

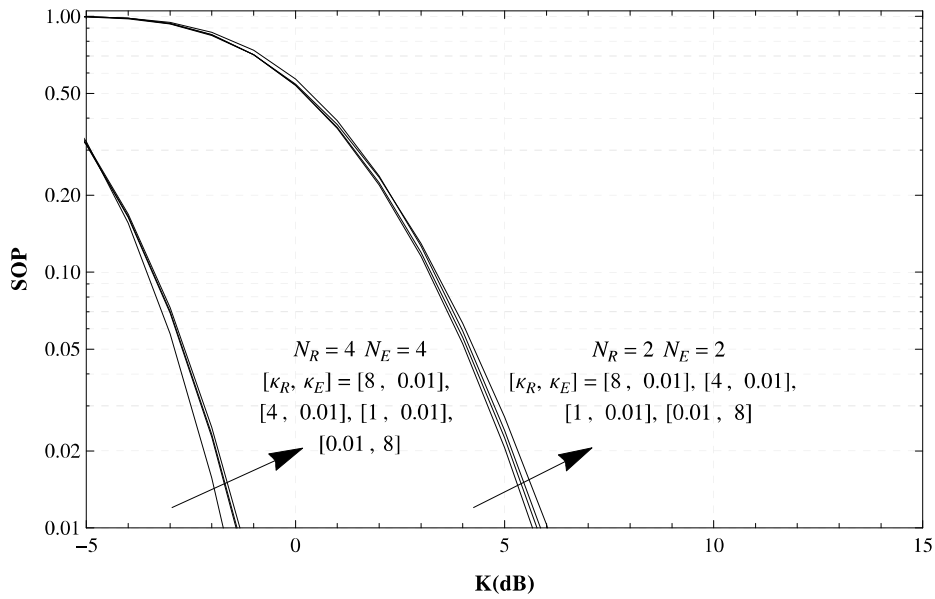


Figura 5.7: SOP sob canal κ - μ sombreado por K , variando κ_R e κ_E , com MIMO e $C_{th} = 0$ bps.

A Figura 5.7 mostra a SOP quando o canal principal aplica a técnica de combate ao desvanecimento MIMO com $C_{th}=0$ bps e a Figura 5.8 apresenta a mesma análise com $C_{th} = 1.25$ bps.

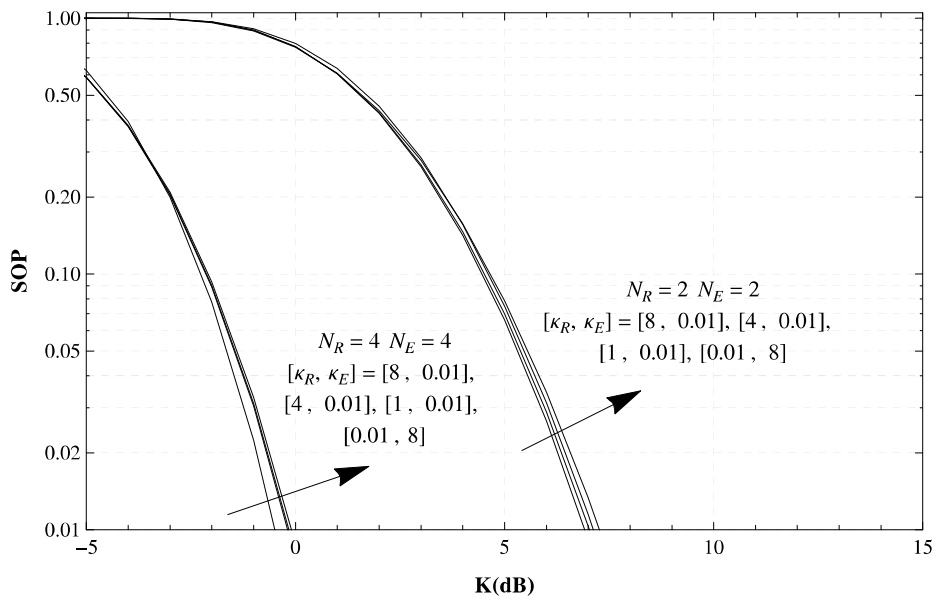


Figura 5.8: SOP sob canal κ - μ sombreado por K , variando κ_R e κ_E , com MIMO e $C_{th} = 1.25$ bps.

Com o MIMO temos o menor valor para a SOP dentre as técnicas aplicadas. Quanto maior o número de nós aplicados menores são os SOPs encontrados.

5.3.2.4 Comparação

Para analisar todos os casos juntos, os parâmetros do canal principal κ_R , μ_R e s_R foram fixados em 8, 2 e 3, respectivamente. Para o canal intruso os parâmetros κ_E , μ_E e s_E foram fixados em 0.01, 2 e 3.

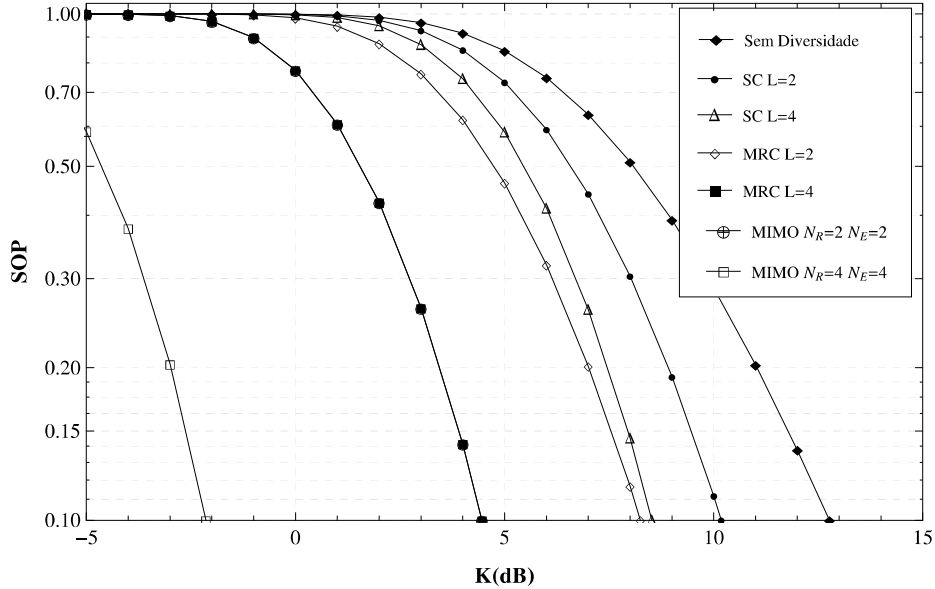


Figura 5.9: Comparação da SOP sob canal κ - μ sombreado por K com $Cth = 1.25$ bps.

A Figura 5.9 mostra a comparação entre as curvas de SOP quando aplicamos nenhuma técnica e com SC, MRC e MIMO nos cenários já apresentados. O caso com a menor SOP é quando aplicamos a técnica de MIMO com o maior número de nós na transmissão e na recepção. A Figura 5.10 mostra a mesma análise com $Cth=0$ bps.

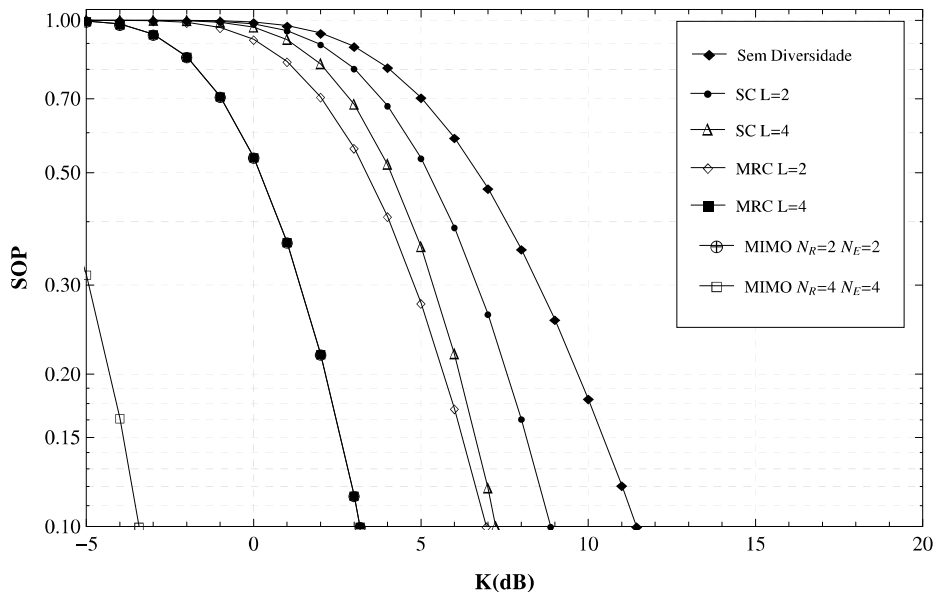


Figura 5.10: Comparação da SOP sob canal κ - μ sombreado por K com $Cth = 0$ bps.

5.4 Análise da SPSC

Mantendo o cenário apresentado na seção 5.1, os gráficos a seguir representam a Probabilidade de Capacidade de Sigilo Estritamente Positiva. Da mesma forma realizada com a SOP, será feito para a SPSC, cenários com técnicas de combate ao desvanecimento irão ser aplicados ao canal principal para análise.

5.4.1 Sem Técnicas de Combate ao Desvanecimento

Com os parâmetros $s_R = s_E = 3$ e $\mu_R = \mu_E = 2$ fixados, a Figura 5.11 mostra o comportamento da SPSC variando os valores de κ_R e κ_E . Continuamos relacionando a SNR média do canal principal com o canal intruso através de K , $\bar{\gamma}_R = K\bar{\gamma}_E$.

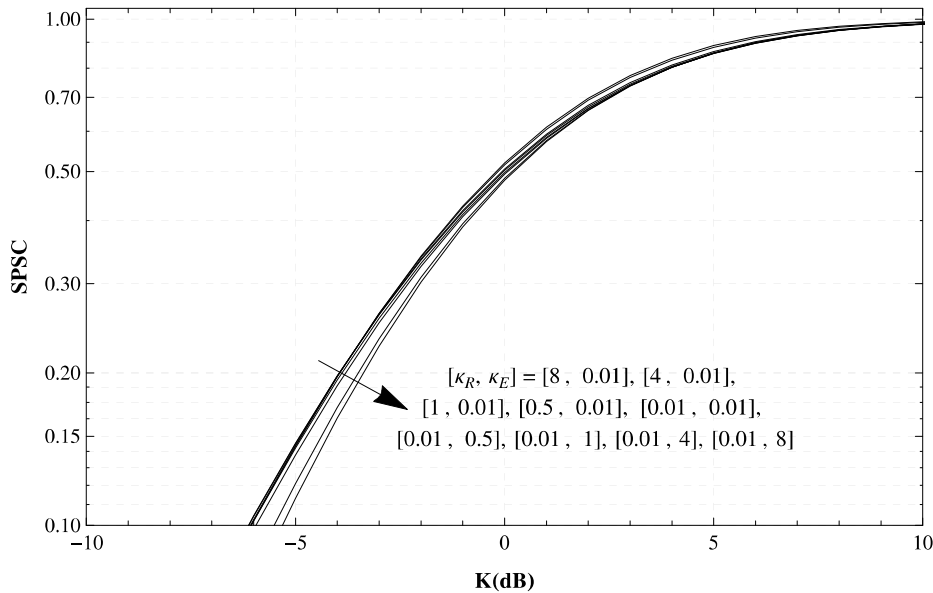


Figura 5.11: SPSC sob canal κ - μ sombreado por K , variando κ_R e κ_E .

É possível observar que quando o parâmetro κ do canal principal diminui, e cresce o valor deste parâmetro para o canal intruso temos uma menor SPSC na comunicação estabelecida entre os dois pontos legítimos.

5.4.2 Com Técnicas de Combate ao Desvanecimento

As técnicas de combate ao desvanecimento discutidas no capítulo 4 e na seção anterior serão também tratadas na análise da SPSC.

5.4.2.1 Selection Combining

Aplicando a técnica de SC ao canal principal, com os parâmetros $s_R = s_E = 3$ e $\mu_R = \mu_E = 2$ fixados, variou-se κ do canal principal e do canal intruso com 2 ramos e com 4 ramos.

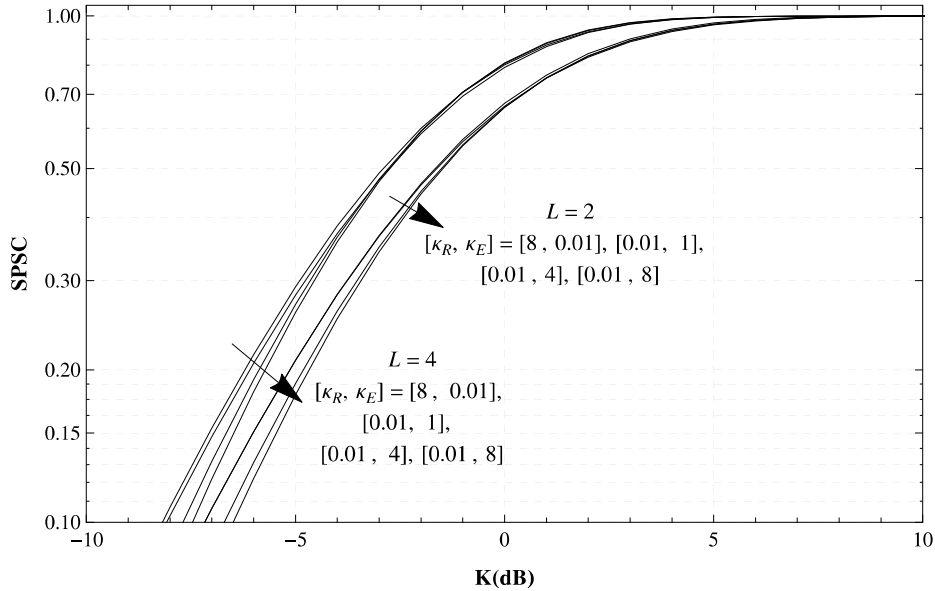


Figura 5.12: SPSC sob canal κ - μ sombreado por K , variando κ_R e κ_E , com SC no canal principal.

A Figura 5.12 mostra a SPSC quando o canal principal aplica a técnica de diversidade SC. É possível observar que a SPSC é maior quando aplicada a SC, e com uma quantidade maior de ramos a SPSC aumenta.

5.4.2.2 MRC

Aplicando a técnica de MRC ao canal principal, com os parâmetros $s_R = s_E = 3$ e $\mu_R = \mu_E = 2$ fixados, variou-se κ do canal principal e do canal intruso com 2 ramos e com 4 ramos.

A Figura 5.13 mostra a SPSC quando o canal principal aplica a técnica de diversidade MRC. Como no caso do uso do SC no canal principal, com o MRC é possível observar um maior SPSC quando este é aplicado, e quanto maior o número de ramos utilizados, maior é a SPSC.

5.4.2.3 MIMO

Aplicando a técnica de MIMO ao canal principal, com os parâmetros $s_R = s_E = 3$ e $\mu_R = \mu_E = 2$ fixados, variou-se κ do canal principal e do canal intruso com 2 e 4 nós na transmissão e com 2 e 4 nós na recepção.

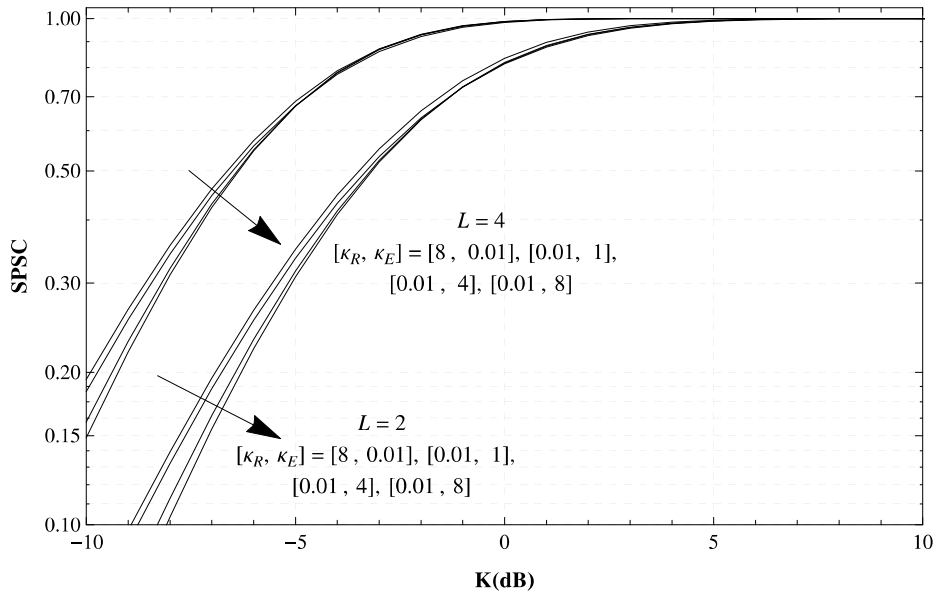


Figura 5.13: SPSC sob canal κ - μ sombreado por K , variando κ_R e κ_E , com MRC.

A Figura 5.14 mostra a SPSC quando o canal principal aplica a técnica de combate ao desvanecimento MIMO. Com esta técnica temos o maior valor para a SPSC dentre as técnicas aplicadas, de forma análoga ao menor SOP obtido anteriormente. Quanto maior o número de nós aplicados maiores são os SPSCs encontrados, com $N_R = 4$ e $N_T = 4$ as SPSCs, as variações de κ_R e κ_E são muito próximas.

5.4.2.4 Comparação

Para analisar todos os casos juntos, os parâmetros do canal principal κ_R , μ_R e s_R foram fixados em 8, 2 e 3, respectivamente. Para o canal intruso os parâmetros κ_E , μ_E e s_E foram fixados em 0.01, 2 e 3.

A Figura 5.15 mostra a comparação entre as curvas de SPSC quando aplicamos nenhuma técnica e com SC, MRC e MIMO nos cenários já apresentados. O caso com a maior SPSC é quando aplicamos a técnica de MIMO com o maior número de nós na transmissão e na recepção.

5.5 Análise da ASC

A terceira métrica de segurança abordada neste trabalho é a ASC que apresenta a Capacidade Média de Sigilo obtida na comunicação sem fio, no nosso caso com o uso específico da distribuição κ - μ sombreada. Da mesma forma como nas análises da SOP e da SPSC, iremos fixar alguns parâmetros e variar os valores de κ_R e κ_E , com K relacionando a SNR média dos canais principal e intruso, $\bar{\gamma}_R = K\bar{\gamma}_E$.

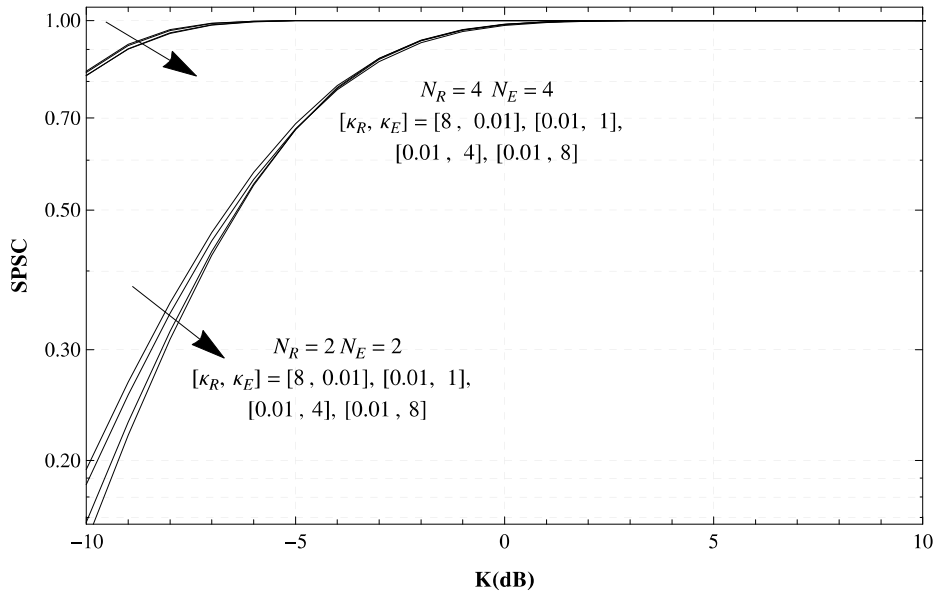


Figura 5.14: SPSC sob canal κ - μ sombreado por K , variando κ_R e κ_E , com MIMO.

5.5.1 Sem Técnicas de Combate ao Desvanecimento

Com os parâmetros $s_R = s_E = 3$ e $\mu_R = \mu_E = 2$ fixados, a Figura 5.16 mostra o comportamento da ASC variando os valores de κ_R e κ_E .

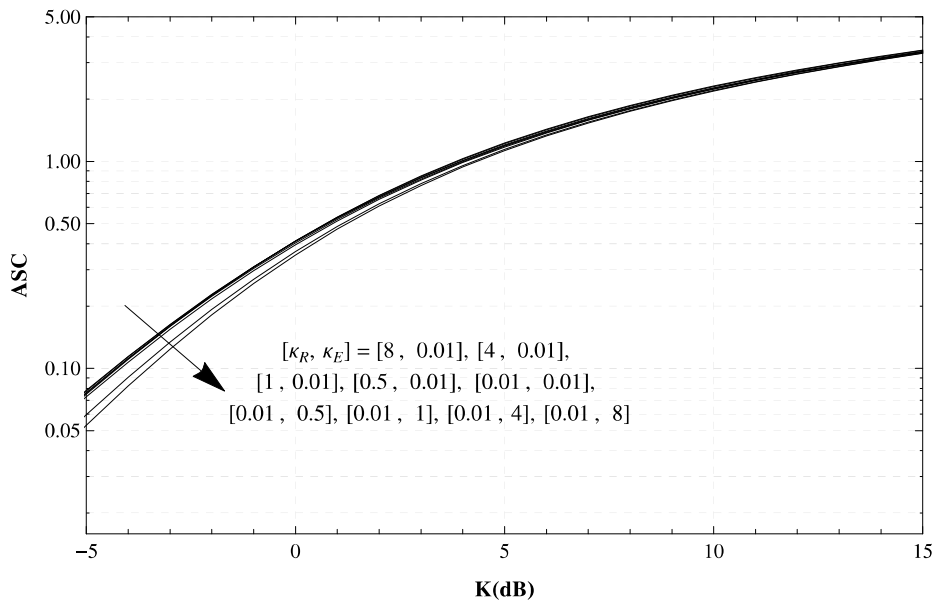


Figura 5.16: ASC sob canal κ - μ sombreado por K , variando κ_R e κ_E .

É possível observar que quando o parâmetro κ do canal principal diminui, e cresce o valor deste parâmetro para o canal intruso temos uma menor ASC na comunicação estabelecida entre os dois pontos legítimos.

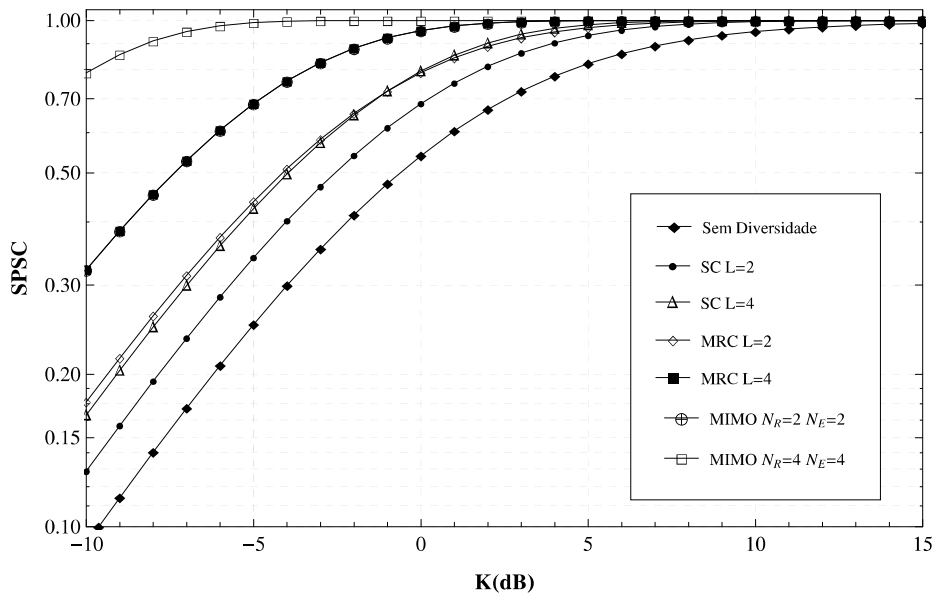


Figura 5.15: Comparação da SPSC sob canal κ - μ sombreado por K , variando κ_R e κ_E

5.5.2 Com Técnicas de Combate ao Desvanecimento

A ASC ao se aplicar as técnicas de combate ao desvanecimento discutidas no capítulo 4 ao cenário apresentado anteriormente é mostrada logo abaixo.

5.5.2.1 Selection Combining

Aplicando a técnica de SC ao canal principal, com os parâmetros $s_R = s_E = 3$ e $\mu_R = \mu_E = 2$ fixados, variou-se κ do canal principal e do canal intruso com 2 ramos e com 4 ramos.

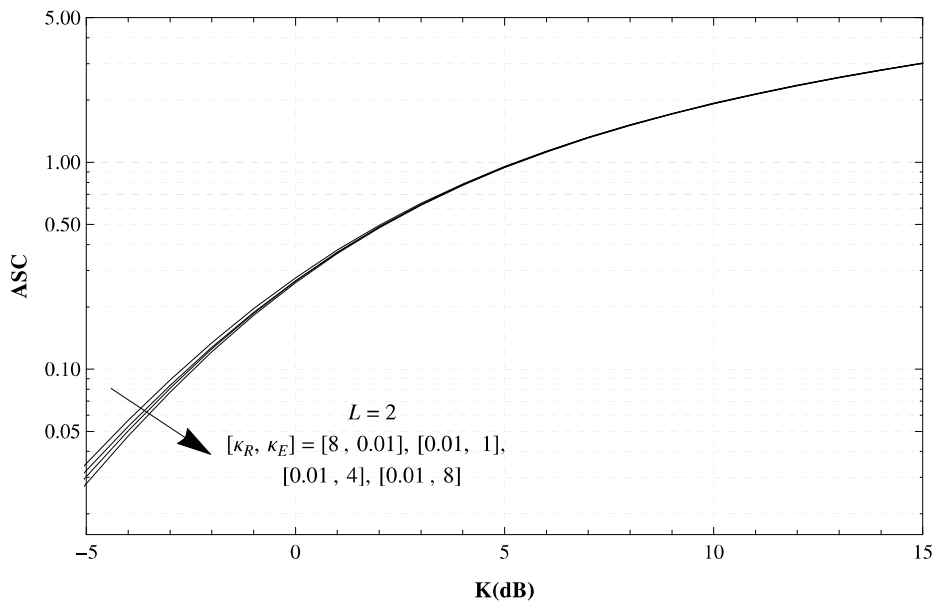


Figura 5.17: ASC sob canal κ - μ sombreado por K , variando κ_R e κ_E , com SC e $L = 2$.

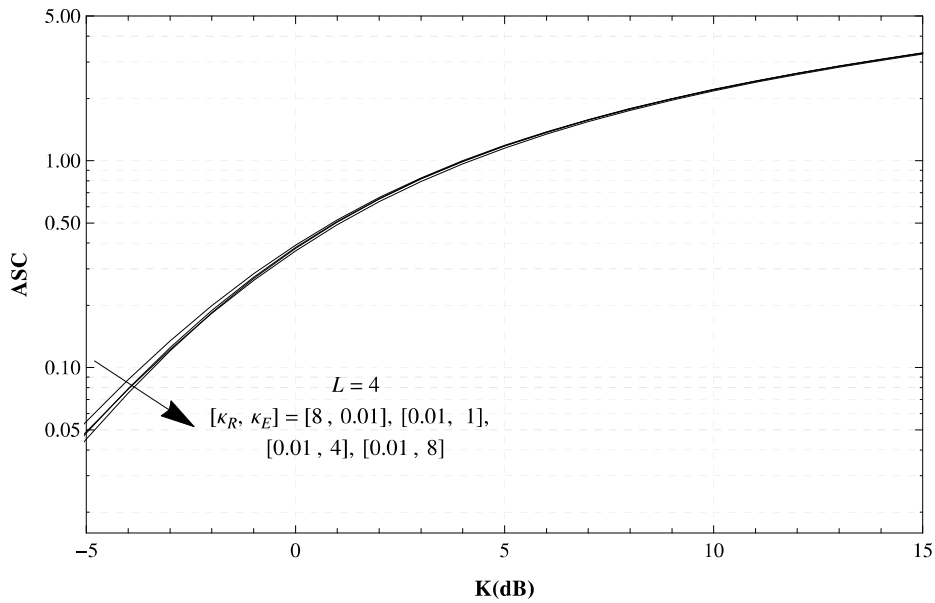


Figura 5.18: ASC sob canal κ - μ sombreado por K , variando κ_R e κ_E , com SC e $L = 4$.

A Figura 5.17 mostra a ASC quando o canal principal utiliza a técnica de diversidade SC com 2 ramos. A Figura 5.18 mostra o caso quando 4 ramos são utilizados no canal principal com SC. É possível observar que a ASC aumenta quando é aplicada a SC, e com uma quantidade maior de ramos a ASC apresenta valores maiores.

5.5.2.2 MRC

Aplicando a técnica de MRC ao canal principal, com os parâmetros $s_R = s_E = 3$ e $\mu_R = \mu_E = 2$ fixados, variou-se κ do canal principal e do canal intruso com 2 ramos e com 4 ramos.

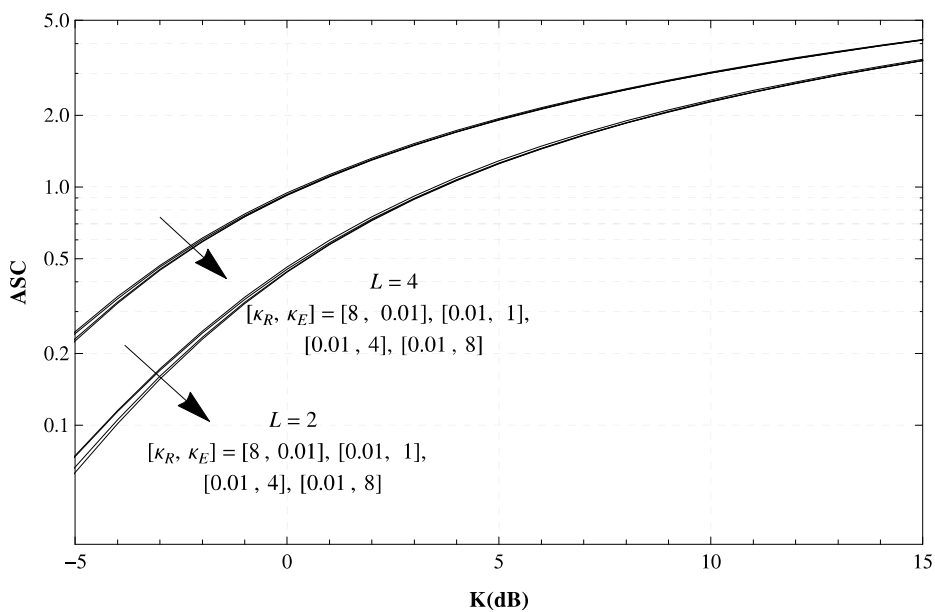


Figura 5.19: ASC sob canal κ - μ sombreado por K , variando κ_R e κ_E , com MRC.

A Figura 5.19 mostra a ASC quando o canal principal aplica a técnica de diversidade MRC. Como no caso do uso do SC no canal principal, com o MRC é possível observar uma maior ASC quando este é aplicado, e quanto maior o número de ramos aplicados, maior é a ASC obtida.

5.5.2.3 MIMO

Aplicando a técnica de MIMO ao canal principal, com os parâmetros $s_R = s_E = 3$ e $\mu_R = \mu_E = 2$ fixados, variou-se κ do canal principal e do canal intruso com 2 e 4 nós na transmissão e com 2 e 4 nós na recepção.

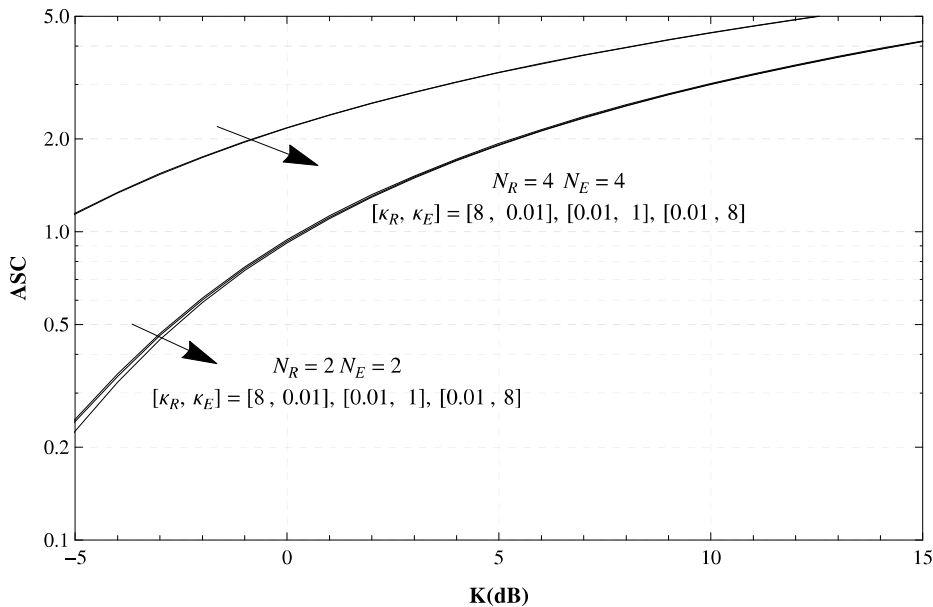


Figura 5.20: ASC sob canal κ - μ sombreado por K , variando κ_R e κ_E , com MIMO.

A Figura 5.20 mostra a ASC quando o canal principal aplica a técnica de combate ao desvanecimento MIMO. Com o MIMO temos novamente o maior valor para a ASC dentre as técnicas aplicadas. Quanto maior o número de nós aplicados, maiores são as ASCs encontradas.

5.5.2.4 Comparação

Para a análise entre todas as técnicas apresentadas, os parâmetros do canal principal κ_R , μ_R e s_R foram fixados em 8, 2 e 3, respectivamente. Para o canal intruso os parâmetros κ_E , μ_E e s_E foram fixados em 0.01, 2 e 3, respectivamente.

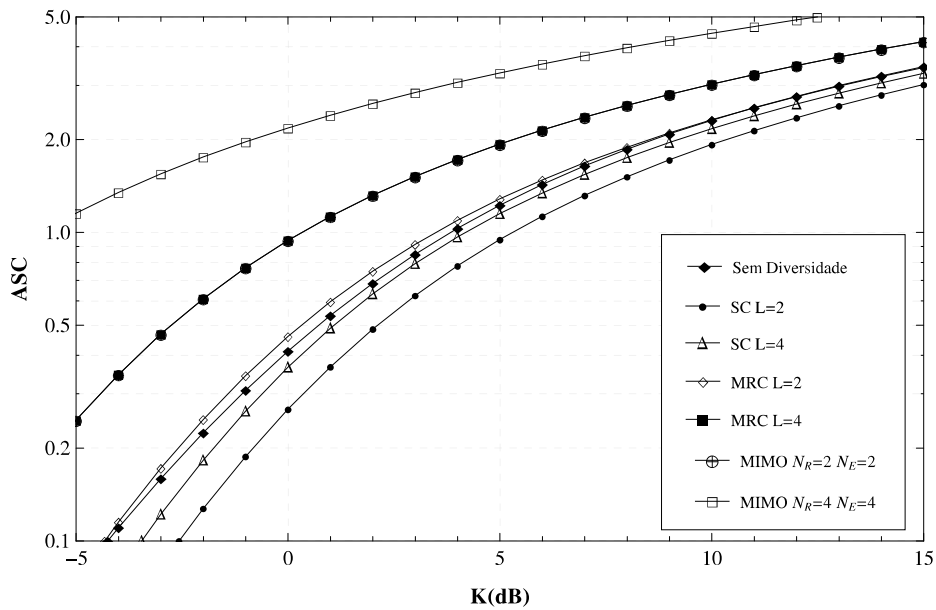


Figura 5.21: Comparação da ASC sob canal κ - μ sombreado por K , variando κ_R e κ_E .

A Figura 5.21 mostra a comparação entre as curvas de ASC quando aplicamos nenhuma técnica e com SC, MRC e MIMO nos cenários já apresentados. O caso com a maior ASC é quando aplicamos a técnica de MIMO com o maior número de nós na transmissão e na recepção.

5.6 Variando μ

As análises anteriores foram baseadas na variação do parâmetro κ_R e κ_E , nesta seção a variação de μ_R e μ_E será analisada no âmbito das métricas de segurança.

5.6.1 Análise da SOP

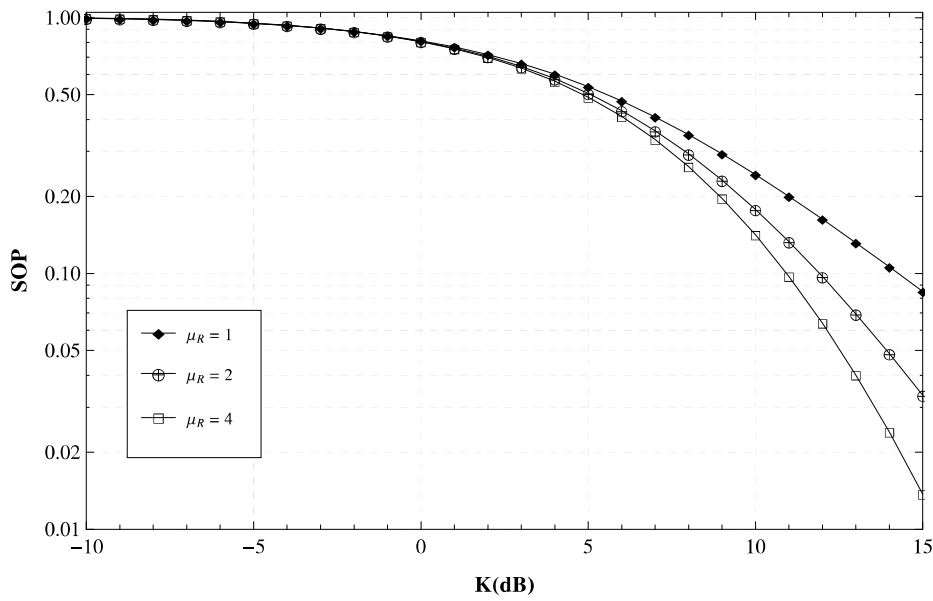


Figura 5.22: SOP sob canal κ-μ sombreado por K, variando μ_R, com Cth = 1.25 bps.

No canal principal foram fixados os parâmetros κ_R e s_R em 2 e 2, respectivamente. No canal intruso foram fixados os parâmetros κ_E, μ_E e s_E em 1, 1.1 e 2, respectivamente. O valor de μ_R do canal principal que varia na Figura 5.22. Com o aumento do valor de μ_R no canal principal observa-se uma diminuição da SOP.

5.6.2 Análise da SPSC

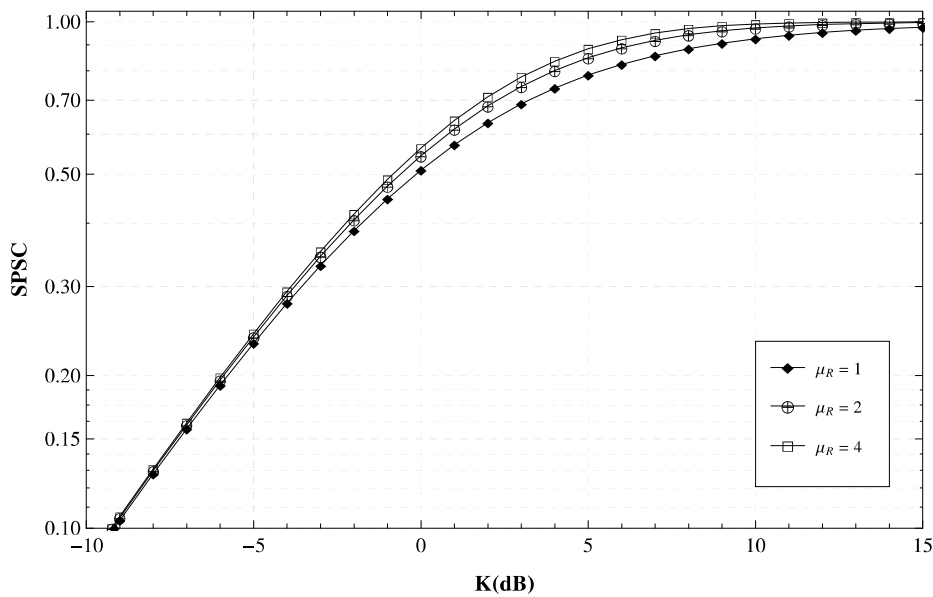


Figura 5.23: SPSC sob canal κ-μ sombreado por K, variando μ_R.

No canal principal foram fixados os parâmetros κ_R e s_R em 2 e 2, respectivamente. No canal intruso foram fixados os parâmetros κ_E , μ_E e s_E em 1, 1.1 e 2, respectivamente. O valor de μ_R do canal principal que varia na Figura 5.23. Com o aumento do valor de μ_R observa-se um aumento da SPSC na comunicação.

5.6.3 Análise da ASC

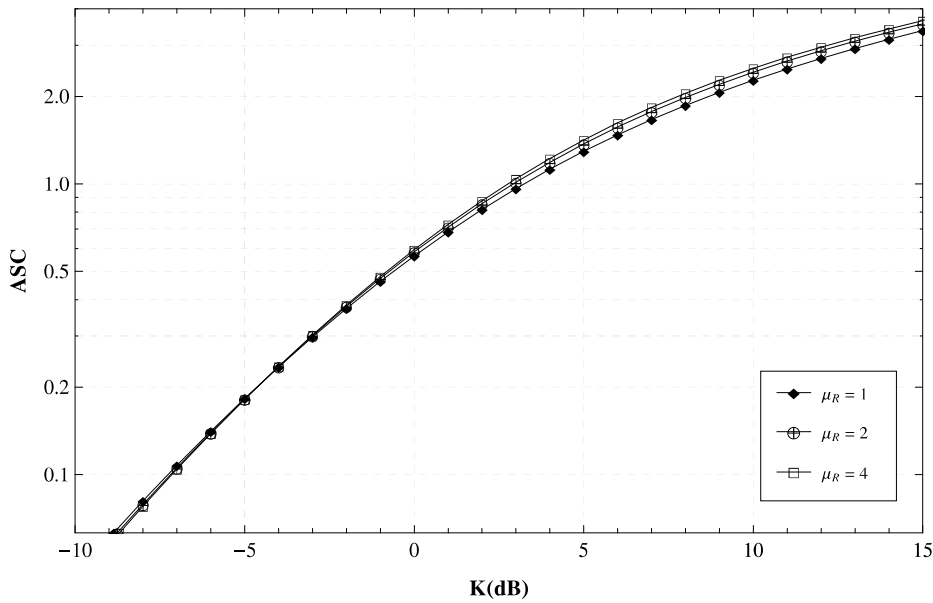


Figura 5.24: ASC sob canal κ - μ sombreado por K , variando μ_R .

No canal principal foram fixados os parâmetros κ_R e s_R em 2 e 2, respectivamente. No canal intruso foram fixados os parâmetros κ_E , μ_E e s_E em 1, 1.1 e 2, respectivamente. O valor de μ_R do canal principal que varia na Figura 5.24. Com o aumento do valor de μ_R observa-se um aumento da ASC na comunicação.

5.7 Comparação com outras distribuições

A distribuição κ - μ sombreada, como dito no capítulo 2, inclui algumas outras distribuições clássicas como a Gaussiana Unilateral, a Nakagami- m , a Rayleigh, a Rice, a Rice sombreada e a própria κ - μ , da qual é obtida a κ - μ sombreada. Esta seção irá mostrar uma comparação entre estas distribuições mostradas na Tabela 2.1.

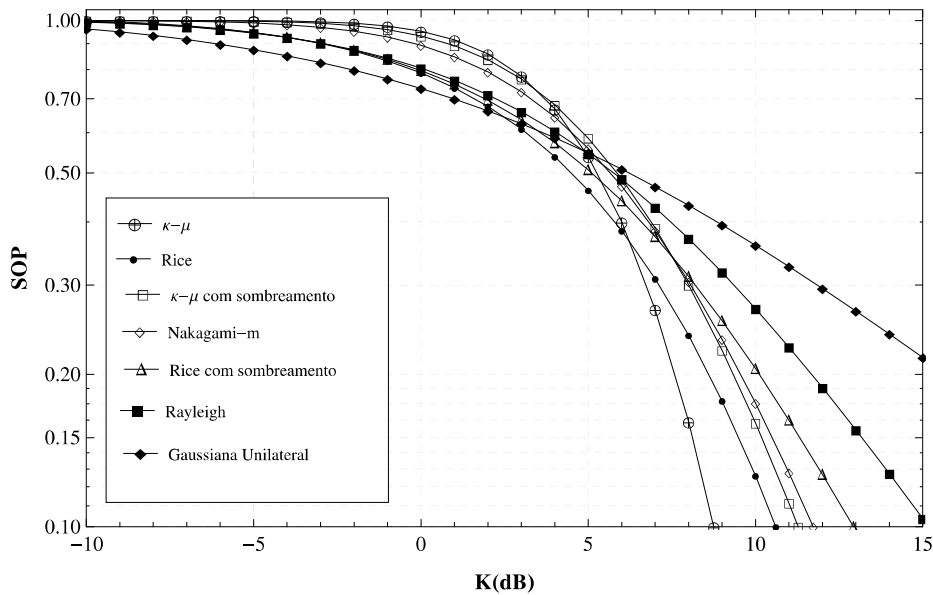


Figura 5.25: Comparação da curva SOP de várias distribuições por K .

Na Figura 5.25 é mostrada a comparação entre as distribuições Gaussiana Unilateral, Rayleigh, Nakagami- m , Rice, Rice sombreada e κ - μ . Neste gráfico é possível verificar que a κ - μ sombreada tem um bom ajuste devido aos parâmetros para caracterização do canal de comunicação sem fio, varrendo as outras distribuições mencionadas. As Figuras 5.26 e 5.27 mostram como as curvas de SPSC e ASC, respectivamente, se comportam com a distribuição κ - μ sombreada comparada às outras distribuições já mencionadas.

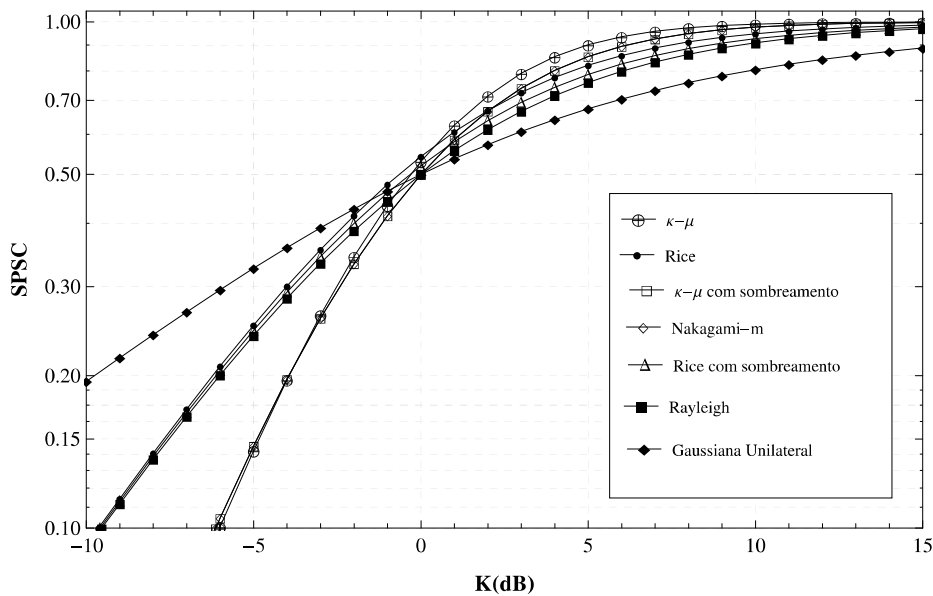


Figura 5.26: Comparação da curva SPSC de várias distribuições por K .

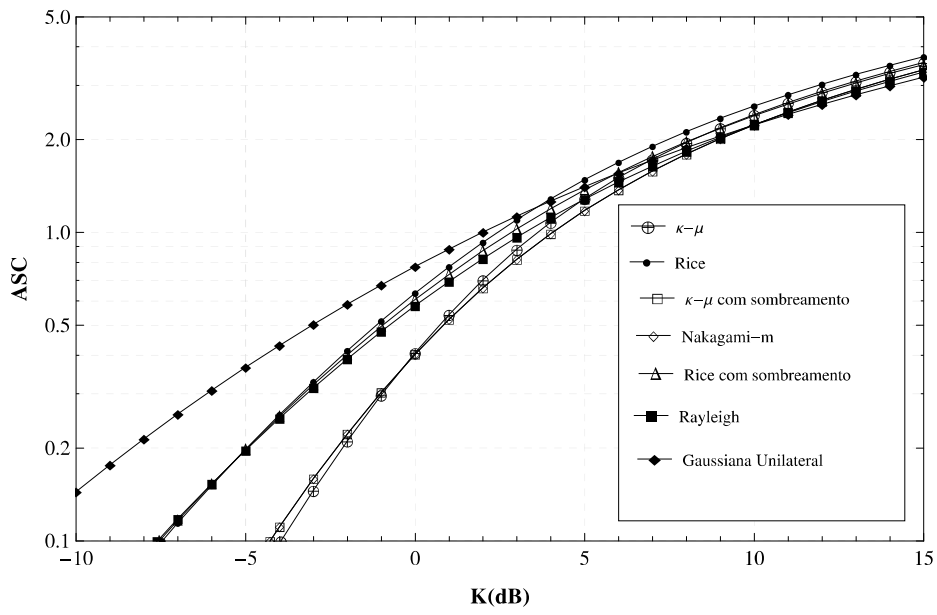


Figura 5.27: Comparação da curva ASC de várias distribuições por K .

Capítulo 6

Conclusão

Este trabalho se propôs a realizar uma análise da modelagem de canais sem fio com aplicações de segurança na camada física. Para isso foi utilizado o modelo de desvanecimento κ - μ sombreado. Este modelo de desvanecimento, apesar de apresentar características boas de ajuste para canais de comunicação sem fio, não possui estudos acerca das métricas de segurança SOP, SPSC e ASC. Este trabalho se propôs a realizar tal estudo e para poder aumentar o grau de sigilo de comunicações sem fio na camada física, também foram realizados estudos aplicando técnicas de combate ao desvanecimento.

Utilizando o modelo de escuta de Wyner, foram realizadas simulações e analisadas as métricas de segurança SOP, SPSC e ASC, com e sem técnicas de combate ao desvanecimento aplicadas. As análises foram realizadas alterando os parâmetros do canal principal e intruso.

Neste trabalho também foram obtidas as formulações fechadas para a SPSC e para a SOP quando temos um limiar C_{th} de 0 bps.

Dentre as análises realizadas vale ressaltar a melhoria da SPSC e ASC quando apresentada uma melhor SNR do canal principal em relação ao canal intruso, o que também foi possível observar quando temos um aumento dos valores dos parâmetros κ e μ para o canal principal. Assim como observamos uma melhoria da SPSC e ASC, foi possível verificar uma diminuição da SOP quando as mesmas análises são realizadas: aumento do SNR do canal principal e aumento dos valores dos parâmetros κ e μ do canal principal. Comparações com outros modelos de desvanecimentos foram realizadas a fim de mostrar como o κ - μ sombreado se ajusta melhor a canais de comunicação sem fio.

Quando aplicadas as técnicas de combate ao desvanecimento, melhores valores para SPSC, SOP e ASC foram obtidos quando utilizado MIMO com 4 nós da transmissão e 4 nós da recepção para o canal principal, o pior caso foi verificado quando não aplicamos nenhum tipo de técnica de combate ao desvanecimento.

6.1 Trabalhos Futuros

Finalmente, podem ser sugeridos alguns tópicos para trabalhos futuros para dar continuidade ao estudo desenvolvido neste trabalho. São eles:

- Obter a formulação da métrica de segurança ASC para a o modelo de desvanecimento κ - μ sombreado;
- Obter a formulação da métrica de segurança SOP para a o modelo de desvanecimento κ - μ sombreado com técnicas de combate ao desvanecimento aplicadas;
- Obter a formulação da métrica de segurança SPSC para a o modelo de desvanecimento κ - μ sombreado com técnicas de combate ao desvanecimento aplicadas;
- Obter a formulação da métrica de segurança ASC para a o modelo de desvanecimento κ - μ sombreado com técnicas de combate ao desvanecimento aplicadas;
- Investigar o comportamento da SOP quando utilizamos o modelo de desvanecimento κ - μ sombreado com outras técnicas de combate ao desvanecimento;

REFERÊNCIAS BIBLIOGRÁFICAS

- [1] GSI. *Política Nacional de Segurança da Informação*. [Http://www.gsi.gov.br/noticias/2017/politica-nacional-de-seguranca-da-informacao](http://www.gsi.gov.br/noticias/2017/politica-nacional-de-seguranca-da-informacao). Acessado 07 de outubro de 2017.
- [2] KORDE, S.; SARODE, M. Review on network layer attacks detection and prevention techniques in mobile ad hoc networks. In: IEEE. *Inventive Systems and Control (ICISC), 2017 International Conference on*. [S.l.], 2017. p. 1–5.
- [3] XIE, Y.; YU, S.-Z. Monitoring the application-layer ddos attacks for popular websites. *IEEE/ACM Transactions on Networking (TON)*, IEEE Press, v. 17, n. 1, p. 15–25, 2009.
- [4] OZHIGANOVA, M.; KOSTYUKOV, A.; MASLOVA, M. Functional model of firewall application layer protection for web-based information systems. In: IEEE. *Industrial Engineering, Applications and Manufacturing (ICIEAM), 2017 International Conference on*. [S.l.], 2017. p. 1–5.
- [5] RHEE, M. Y. Transport layer security: Sslv3 and tlv1. *Wireless Mobile Internet Security, Second Edition*, Wiley Online Library, p. 325–352.
- [6] SHIU, Y.-S. et al. Physical layer security in wireless networks: A tutorial. *IEEE wireless Communications*, IEEE, v. 18, n. 2, 2011.
- [7] LIU, X. Strictly positive secrecy capacity of log-normal fading channel with multiple eavesdroppers. In: IEEE. *Communications (ICC), 2014 IEEE International Conference on*. [S.l.], 2014. p. 775–779.
- [8] LIU, X. Secrecy capacity of wireless links subject to log-normal fading. In: IEEE. *Communications and Networking in China (CHINACOM), 2012 7th International ICST Conference on*. [S.l.], 2012. p. 167–172.
- [9] LIU, X. Probability of strictly positive secrecy capacity of the rician-rician fading channel. *IEEE Wireless Communications Letters*, IEEE, v. 2, n. 1, p. 50–53, 2013.
- [10] LIU, X. Probability of strictly positive secrecy capacity of the weibull fading channel. In: IEEE. *Global Communications Conference (GLOBECOM), 2013 IEEE*. [S.l.], 2013. p. 659–664.

- [11] LIU, X. Outage probability of secrecy capacity over correlated log-normal fading channels. *IEEE Communications Letters*, IEEE, v. 17, n. 2, p. 289–292, 2013.
- [12] SUN, X. et al. Performance of secure communications over correlated fading channels. *IEEE Signal Processing Letters*, IEEE, v. 19, n. 8, p. 479–482, 2012.
- [13] ZOU, Y. et al. Improving physical-layer security in wireless communications using diversity techniques. *IEEE Network*, IEEE, v. 29, n. 1, p. 42–48, 2015.
- [14] ZOU, Y.; WANG, X.; SHEN, W. Optimal relay selection for physical-layer security in cooperative wireless networks. *IEEE Journal on Selected Areas in Communications*, IEEE, v. 31, n. 10, p. 2099–2111, 2013.
- [15] ZOU, Y. et al. Relay-selection improves the security-reliability trade-off in cognitive radio systems. *IEEE Transactions on Communications*, IEEE, v. 63, n. 1, p. 215–228, 2015.
- [16] KONG, L.; TRAN, H.; KADDOUM, G. Performance analysis of physical layer security over α - μ fading channel. *Electronics Letters*, IET, v. 52, n. 1, p. 45–47, 2015.
- [17] LIU, X. Probability of strictly positive secrecy capacity of the weibull fading channel. In: IEEE. *Global Communications Conference (GLOBECOM), 2013 IEEE*. [S.l.], 2013. p. 659–664.
- [18] PAN, G. et al. Physical-layer security over non-small-scale fading channels. *IEEE Transactions on Vehicular Technology*, IEEE, v. 65, n. 3, p. 1326–1339, 2016.
- [19] PARIS, J. F. Statistical characterization of κ - μ shadowed fading. *IEEE Transactions on Vehicular Technology*, IEEE, v. 63, n. 2, p. 518–526, 2014.
- [20] WYNER, A. D. The wire-tap channel. *Bell Labs Technical Journal*, Wiley Online Library, v. 54, n. 8, p. 1355–1387, 1975.
- [21] SHANNON, C. E. Communication theory of secrecy systems. *Bell Labs Technical Journal*, Wiley Online Library, v. 28, n. 4, p. 656–715, 1949.
- [22] SIMON, M. K.; ALOUINI, M.-S. *Digital communication over fading channels*. [S.l.]: John Wiley & Sons, 2005.
- [23] ANTÔNIO, J. R. Área de cobertura em ambiente de propagação modelado com a distribuição κ - μ . *Instituto Nacional de Telecomunicações*, 2003.
- [24] ABDI, A. et al. On the estimation of the k parameter for the rice fading distribution. *IEEE Communications letters*, IEEE, v. 5, n. 3, p. 92–94, 2001.
- [25] RAPPAPORT, T. S. *Comunicações sem fio: princípios e práticas*. [S.l.]: Pearson Prentice Hall, 2009.

- [26] ARAGON-ZAVALA, A. *Antennas and propagation for wireless communication systems*. [S.l.]: John Wiley & Sons, 2008.
- [27] YACOUB, M. D. The κ - μ distribution and the η - μ distribution. *IEEE Antennas and Propagation Magazine*, IEEE, v. 49, n. 1, p. 68–81, 2007.
- [28] GRADSHTEYN, I. S.; RYZHIK, I. M. *Table of integrals, series, and products*. [S.l.]: Academic press, 2014.
- [29] SALAHAT, E. Unified performance analysis of maximal ratio combining in η - μ , λ - μ and κ - μ generalized fading channels. In: IEEE. *Vehicular Technology Conference (VTC Fall), 2014 IEEE 80th*. [S.l.], 2014. p. 1–5.
- [30] SALAHAT, E.; ABUALHAOL, I. Y. Generalized average ber expression for sc and mrc receiver over nakagami-m fading channels. In: *PIMRC*. [S.l.: s.n.], 2013. p. 3360–3365.
- [31] SALAHAT, E.; HAKAM, A. Maximal ratio combining diversity analysis of underwater acoustic communications subject to $\{\kappa\}$ - $\{\mu\}$ shadowed fading channels. *arXiv preprint arXiv:1605.02152*, 2016.
- [32] GOLDSMITH, A. *Wireless communications*. [S.l.]: Cambridge university press, 2005.
- [33] TELATAR, E. Capacity of multi-antenna gaussian channels. *Transactions on Emerging Telecommunications Technologies*, Wiley Online Library, v. 10, n. 6, p. 585–595, 1999.
- [34] FOSCHINI, G. J.; GANS, M. J. On limits of wireless communications in a fading environment when using multiple antennas. *Wireless personal communications*, Springer, v. 6, n. 3, p. 311–335, 1998.
- [35] KANG, M.; ALOUINI, M.-S. Capacity of mimo rician channels. *IEEE Transactions on Wireless Communications*, IEEE, v. 5, n. 1, p. 112–122, 2006.
- [36] MAAREF, A.; AISSA, S. Performance analysis of orthogonal space-time block codes in spatially correlated mimo nakagami fading channels. *IEEE Transactions on Wireless Communications*, IEEE, v. 5, n. 4, p. 807–817, 2006.
- [37] SALAHAT, E.; HAKAM, A. Unified error rates analysis of mimo space-time block codes over generalized shadowed $\{\kappa\}$ - $\{\mu\}$ and $\{\eta\}$ - $\{\mu\}$ fading and awggn. *arXiv preprint arXiv:1605.02147*, 2016.
- [38] BHARGAV, N.; COTTON, S. L.; SIMMONS, D. E. Secrecy capacity analysis over κ - μ fading channels: Theory and applications. *IEEE Transactions on Communications*, IEEE, v. 64, n. 7, p. 3011–3024, 2016.
- [39] BARROS, J.; RODRIGUES, M. R. Secrecy capacity of wireless channels. In: IEEE. *Information Theory, 2006 IEEE International Symposium on*. [S.l.], 2006. p. 356–360.

- [40] LEUNG-YAN-CHEONG, S.; HELLMAN, M. The gaussian wire-tap channel. *IEEE transactions on information theory*, IEEE, v. 24, n. 4, p. 451–456, 1978.
- [41] TSE, D.; VISWANATH, P. *Fundamentals of wireless communication*. [S.l.]: Cambridge university press, 2005.
- [42] BLOCH, M. et al. Wireless information-theoretic security. *IEEE Transactions on Information Theory*, IEEE, v. 54, n. 6, p. 2515–2534, 2008.

APÊNDICES

I.1 SOP

Temos que a métrica *SOP* é dada pela seguinte probabilidade:

$$\begin{aligned}
 SOP &= P \{C_s(\gamma_R, \gamma_E) \leq Cth\} \\
 &= P \{\ln(1 + \gamma_R) - \ln(1 + \gamma_E) \leq Cth\} \\
 &= P \{\gamma_R \leq \theta\gamma_E + \theta - 1\} \\
 &= \int_0^\infty \int_0^{\theta\gamma_E + \theta - 1} f_R(\gamma_R) d\gamma_R f_E(\gamma_E) d\gamma_E.
 \end{aligned} \tag{1}$$

Considerando o desvanecimento $\kappa - \mu$ com sombreamento, temos o seguinte:

$$\begin{aligned}
 SOP &= C_1 C_2 \int_0^\infty \exp^{-\frac{\gamma_E(1+\kappa_E)\mu_E}{\bar{\gamma}_E}} \gamma_E^{-1+\mu_E} {}_1F_1\left(m_E; \mu_E; \frac{\gamma_E \kappa_E (1 + \kappa_E) \mu_E^2}{\bar{\gamma}_E (m_E + \kappa_E \mu_E)}\right) \\
 &\quad \int_0^{\gamma_E \theta + \theta - 1} \exp^{-\frac{\gamma_R(1+\kappa_R)\mu_R}{\bar{\gamma}_R}} \gamma_R^{-1+\mu_R} {}_1F_1\left(m_R; \mu_R; \frac{\gamma_R \kappa_R (1 + \kappa_R) \mu_R^2}{\bar{\gamma}_R (m_R + \kappa_R \mu_R)}\right) d\gamma_R d\gamma_E,
 \end{aligned} \tag{2}$$

com os valores das constantes C_1 e C_2 dados pelas equações 17 e 18, respectivamente:

$$C_1 = \frac{1}{\bar{\gamma}_R \Gamma(\mu_R)} m_R^{m_R} \left(\frac{1}{\bar{\gamma}_R}\right)^{-1+\mu_R} (1 + \kappa_R)^{\mu_R} \mu_R^{\mu_R} (m_R + \kappa_R \mu_R)^{-m_R}, \tag{3}$$

$$C_2 = \frac{1}{\bar{\gamma}_E \Gamma(\mu_E)} m_E^{m_E} \left(\frac{1}{\bar{\gamma}_E}\right)^{-1+\mu_E} (1 + \kappa_E)^{\mu_E} \mu_E^{\mu_E} (m_E + \kappa_E \mu_E)^{-m_E}. \tag{4}$$

A fim de encontrar a fórmula fechada para a métrica *SOP*, verifica-se a integral interna inicialmente com a substituição em série da função hipergeométrica ${}_1F_1$ [28]:

$$INT_1 = \int_0^{\gamma_E \theta + \theta - 1} \exp^{-\frac{\gamma_R(1+\kappa_R)\mu_R}{\bar{\gamma}_R}} \gamma_R^{-1+\mu_R} \left(\sum_{n=0}^{\infty} \frac{m_R^{(n)} (d_1 \gamma_R)^n}{\mu_R^{(n)} n!} \right) d\gamma_R, \tag{5}$$

considerando d_1 dado pela equação 20:

$$d_1 = \frac{\kappa_E (1 + \kappa_E) \mu_E^2}{\bar{\gamma}_E (m_E + \kappa_E \mu_E)}. \tag{6}$$

Assim sendo, temos:

$$INT_1 = \sum_{n=0}^{\infty} \frac{m_R^{(n)} d_1^n}{\mu_R^{(n)} n!} \int_0^{\gamma_E \theta + \theta - 1} \exp^{-\frac{\gamma_R(1+\kappa_R)\mu_R}{\bar{\gamma}_R}} \gamma_R^{-1+\mu_R+n} d\gamma_R. \tag{7}$$

De acordo com [28], temos o seguinte resultado para a integral interna:

$$INT_1 = \sum_{n=0}^{\infty} \frac{m_R^{(n)} d_1^n}{\mu_R^{(n)} n!} \left(\left(\frac{(1 + \kappa_R) \mu_R}{\bar{\gamma}_R} \right)^{(-\mu_R - n)} \gamma \left(\mu_R + n, \frac{(1 + \kappa_R) \mu_R}{\bar{\gamma}_R} (\gamma_E \theta + \theta - 1) \right) \right). \quad (8)$$

A partir do resultado acima, temos que a métrica é dada por:

$$\begin{aligned} SOP &= C_1 C_2 \int_0^{\infty} \exp^{-\frac{\gamma_E (1 + \kappa_E) \mu_E}{\bar{\gamma}_E}} \gamma_E^{-1 + \mu_E} {}_1F_1 \left(m_E; \mu_E; \frac{\gamma_E \kappa_E (1 + \kappa_E) \mu_E^2}{\bar{\gamma}_E (m_E + \kappa_E \mu_E)} \right) \\ &\quad \left(\sum_{n=0}^{\infty} \frac{m_R^{(n)} d_1^n}{\mu_R^{(n)} n!} \left(\left(\frac{(1 + \kappa_R) \mu_R}{\bar{\gamma}_R} \right)^{(-\mu_R - n)} \gamma \left(\mu_R + n, \frac{(1 + \kappa_R) \mu_R}{\bar{\gamma}_R} (\gamma_E \theta + \theta - 1) \right) \right) \right) d\gamma_R \\ &= C_1 C_2 \left(\sum_{n=0}^{\infty} \frac{m_R^{(n)} d_1^n}{\mu_R^{(n)} n!} \left(\frac{(1 + \kappa_R) \mu_R}{\bar{\gamma}_R} \right)^{(-\mu_R - n)} \right. \\ &\quad \left. \int_0^{\infty} \exp^{-\frac{\gamma_E (1 + \kappa_E) \mu_E}{\bar{\gamma}_E}} \gamma_E^{-1 + \mu_E} {}_1F_1 \left(m_E; \mu_E; \frac{\gamma_E \kappa_E (1 + \kappa_E) \mu_E^2}{\bar{\gamma}_E (m_E + \kappa_E \mu_E)} \right) \right. \\ &\quad \left. \gamma \left(\mu_R + n, \frac{(1 + \kappa_R) \mu_R}{\bar{\gamma}_R} (\gamma_E \theta + \theta - 1) \right) d\gamma_E \right) \end{aligned} \quad (9)$$

Verificando a integral da equação acima, temos:

$$\begin{aligned} INT_2 &= \int_0^{\infty} \exp^{-\frac{\gamma_E (1 + \kappa_E) \mu_E}{\bar{\gamma}_E}} \gamma_E^{-1 + \mu_E} \left(\sum_{s=0}^{\infty} \frac{m_E^{(s)} (d_2 \gamma_E)^s}{\mu_E^{(s)} s!} \right) \\ &\quad \gamma \left(\mu_R + n, \frac{(1 + \kappa_R) \mu_R}{\bar{\gamma}_R} (\gamma_E \theta + \theta - 1) \right) d\gamma_E, \end{aligned} \quad (10)$$

considerando d_2 dado pela equação 25

$$d_2 = \frac{\kappa_E (1 + \kappa_E) \mu_E^2}{\bar{\gamma}_E (m_E + \kappa_E \mu_E)}. \quad (11)$$

Assim sendo, temos:

$$\begin{aligned} INT_2 &= \sum_{s=0}^{\infty} \frac{m_E^{(s)} d_2^s}{\mu_E^{(s)} s!} \int_0^{\infty} \exp^{-\frac{\gamma_E (1 + \kappa_E) \mu_E}{\bar{\gamma}_E}} \gamma_E^{-1 + \mu_E + s} \\ &\quad \gamma \left(\mu_R + n, \frac{(1 + \kappa_R) \mu_R}{\bar{\gamma}_R} (\gamma_E \theta + \theta - 1) \right) d\gamma_E. \end{aligned} \quad (12)$$

Para o caso em que $\theta = 1$, ou seja, o limiar C_{th} é igual a 0 bps, de acordo com [28],

temos o seguinte resultado para essa integral:

$$INT_2 = \sum_{s=0}^{\infty} \frac{m_E^{(s)} d_2^s}{\mu_E^{(s)} s!} \left(\left(\frac{\left(\frac{(1+\kappa_R)\mu_R}{\bar{\gamma}_R} \right)^{\mu_R+n} \Gamma(\mu_E + s + \mu_R + n)}{(\mu_R + n) \left(\frac{(1+\kappa_R)\mu_R}{\bar{\gamma}_R} + \frac{(1+\kappa_E)\mu_E}{\bar{\gamma}_E} \right)^{\mu_E+s+\mu_R+n}} \right) \right. \\ \left. {}_2F_1 \left(1; \mu_E + s + \mu_R + n; \mu_R + n + 1; \frac{\frac{(1+\kappa_R)\mu_R}{\bar{\gamma}_R}}{\frac{(1+\kappa_E)\mu_E}{\bar{\gamma}_E} + \frac{(1+\kappa_R)\mu_R}{\bar{\gamma}_R}} \right) \right). \quad (13)$$

Assim sendo, a métrica *SOP* é dada pela seguinte fórmula fechada:

$$SOP = C_1 C_2 \left(\sum_{n=0}^{\infty} \frac{m_R^{(n)} d_1^n}{\mu_R^{(n)} n!} \left(\frac{(1 + \kappa_R)\mu_R}{\bar{\gamma}_R} \right)^{(-\mu_R-n)} \right. \\ \left(\sum_{s=0}^{\infty} \frac{m_E^{(s)} d_2^s}{\mu_E^{(s)} s!} \left(\frac{\left(\frac{(1+\kappa_R)\mu_R}{\bar{\gamma}_R} \right)^{\mu_R+n} \Gamma(\mu_E + s + \mu_R + n)}{(\mu_R + n) \left(\frac{(1+\kappa_E)\mu_E}{\bar{\gamma}_E} + \frac{(1+\kappa_R)\mu_R}{\bar{\gamma}_R} \right)^{\mu_R+s+\mu_E+n}} \right) \right. \\ \left. \left. {}_2F_1 \left(1; \mu_E + s + \mu_R + n; \mu_R + n + 1; \frac{\frac{(1+\kappa_R)\mu_R}{\bar{\gamma}_R}}{\frac{(1+\kappa_E)\mu_E}{\bar{\gamma}_E} + \frac{(1+\kappa_R)\mu_R}{\bar{\gamma}_R}} \right) \right) \right). \quad (14)$$

I.2 SPSC

Temos que a métrica *SPSC* é dada pela seguinte probabilidade:

$$SPSC = P \{C_s(\gamma_R, \gamma_E) > 0\} \\ = P \{ \ln(1 + \gamma_R) - \ln(1 + \gamma_E) > 0 \} \\ = P \{ \gamma_E < \gamma_R \} \\ = \int_0^{\infty} \int_0^{\gamma_R} f_E(\gamma_E) d\gamma_E f_R(\gamma_R) d\gamma_R. \quad (15)$$

Considerando o desvanecimento $\kappa - \mu$ com sombreado, temos o seguinte:

$$SPSC = C_1 C_2 \int_0^{\infty} \exp^{-\frac{\gamma_R(1+\kappa_R)\mu_R}{\bar{\gamma}_R}} \gamma_R^{-1+\mu_R} {}_1F_1 \left(m_R; \mu_R; \frac{\gamma_R \kappa_R (1 + \kappa_R) \mu_R^2}{\bar{\gamma}_R (m_R + \kappa_R \mu_R)} \right) \\ \int_0^{\gamma_R} \exp^{-\frac{\gamma_E(1+\kappa_E)\mu_E}{\bar{\gamma}_E}} \gamma_E^{-1+\mu_E} {}_1F_1 \left(m_E; \mu_E; \frac{\gamma_E \kappa_E (1 + \kappa_E) \mu_E^2}{\bar{\gamma}_E (m_E + \kappa_E \mu_E)} \right) d\gamma_E d\gamma_R, \quad (16)$$

com os valores das constantes C_1 e C_2 dados pelas equações 17 e 18, respectivamente:

$$C_1 = \frac{1}{\bar{\gamma}_R \Gamma(\mu_R)} m_R^{m_R} \left(\frac{1}{\bar{\gamma}_R} \right)^{-1+\mu_R} (1 + \kappa_R)^{\mu_R} \mu_R^{\mu_R} (m_R + \kappa_R \mu_R)^{-m_R}, \quad (17)$$

$$C_2 = \frac{1}{\bar{\gamma}_E \Gamma(\mu_E)} m_E^{m_E} \left(\frac{1}{\bar{\gamma}_E} \right)^{-1+\mu_E} (1 + \kappa_E)^{\mu_E} \mu_E^{\mu_E} (m_E + \kappa_E \mu_E)^{-m_E}. \quad (18)$$

A fim de encontrar a fórmula fechada para a métrica *SPSC*, verifica-se a integral interna inicialmente:

$$INT_1 = \int_0^{\gamma_R} \exp^{-\frac{\gamma_E(1+\kappa_E)\mu_E}{\bar{\gamma}_E}} \gamma_E^{-1+\mu_E} \left(\sum_{n=0}^{\infty} \frac{m_E^{(n)} (d_1 \gamma_E)^n}{\mu_E^{(n)} n!} \right) d\gamma_E, \quad (19)$$

considerando d_1 dado pela equação 20:

$$d_1 = \frac{\kappa_E(1 + \kappa_E)\mu_E^2}{\bar{\gamma}_E(m_E + \kappa_E \mu_E)}. \quad (20)$$

Assim sendo, temos:

$$INT_1 = \sum_{n=0}^{\infty} \frac{m_E^{(n)} d_1^n}{\mu_E^{(n)} n!} \int_0^{\gamma_R} \exp^{-\frac{\gamma_E(1+\kappa_E)\mu_E}{\bar{\gamma}_E}} \gamma_E^{-1+\mu_E+n} d\gamma_E. \quad (21)$$

De acordo com [28], temos o seguinte resultado para a integral interna:

$$INT_1 = \sum_{n=0}^{\infty} \frac{m_E^{(n)} d_1^n}{\mu_E^{(n)} n!} \left(\left(\frac{(1 + \kappa_E)\mu_E}{\bar{\gamma}_E} \right)^{(-\mu_E-n)} \gamma \left(\mu_E + n, \frac{(1 + \kappa_E)\mu_E}{\bar{\gamma}_E} \gamma_R \right) \right). \quad (22)$$

A partir do resultado acima, temos que a métrica é dada por:

$$\begin{aligned} SPSC &= C_1 C_2 \int_0^{\infty} \exp^{-\frac{\gamma_R(1+\kappa_R)\mu_R}{\bar{\gamma}_R}} \gamma_R^{-1+\mu_R} {}_1F_1 \left(m_R; \mu_R; \frac{\gamma_R \kappa_R (1 + \kappa_R) \mu_R^2}{\bar{\gamma}_R (m_R + \kappa_R \mu_R)} \right) \\ &\quad \left(\sum_{n=0}^{\infty} \frac{m_E^{(n)} d_1^n}{\mu_E^{(n)} n!} \left(\left(\frac{(1 + \kappa_E)\mu_E}{\bar{\gamma}_E} \right)^{(-\mu_E-n)} \gamma \left(\mu_E + n, \frac{(1 + \kappa_E)\mu_E}{\bar{\gamma}_E} \gamma_R \right) \right) \right) d\gamma_R \\ &= C_1 C_2 \left(\sum_{n=0}^{\infty} \frac{m_E^{(n)} d_1^n}{\mu_E^{(n)} n!} \left(\frac{(1 + \kappa_E)\mu_E}{\bar{\gamma}_E} \right)^{(-\mu_E-n)} \right. \\ &\quad \left. \int_0^{\infty} \exp^{-\frac{\gamma_R(1+\kappa_R)\mu_R}{\bar{\gamma}_R}} \gamma_R^{-1+\mu_R} {}_1F_1 \left(m_R; \mu_R; \frac{\gamma_R \kappa_R (1 + \kappa_R) \mu_R^2}{\bar{\gamma}_R (m_R + \kappa_R \mu_R)} \right) \right. \\ &\quad \left. \gamma \left(\mu_E + n, \frac{(1 + \kappa_E)\mu_E}{\bar{\gamma}_E} \gamma_R \right) d\gamma_R \right) \end{aligned} \quad (23)$$

Verificando a integral da equação acima, temos:

$$INT_2 = \int_0^\infty \exp^{-\frac{\gamma_R(1+\kappa_R)\mu_R}{\bar{\gamma}_R}} \gamma_R^{-1+\mu_R} \left(\sum_{s=0}^\infty \frac{m_R^{(s)} (d_2 \gamma_R)^s}{\mu_R^{(s)} s!} \right) \gamma \left(\mu_E + n, \frac{(1+\kappa_E)\mu_E}{\bar{\gamma}_E} \gamma_R \right) d\gamma_R, \quad (24)$$

considerando d_2 dado pela equação 25

$$d_2 = \frac{\kappa_R(1+\kappa_R)\mu_R^2}{\bar{\gamma}_R(m_R + \kappa_R\mu_R)}. \quad (25)$$

Assim sendo, temos:

$$INT_2 = \sum_{s=0}^\infty \frac{m_R^{(s)} d_2^s}{\mu_R^{(s)} s!} \int_0^\infty \exp^{-\frac{\gamma_R(1+\kappa_R)\mu_R}{\bar{\gamma}_R}} \gamma_R^{-1+\mu_R+s} \gamma \left(\mu_E + n, \frac{(1+\kappa_E)\mu_E}{\bar{\gamma}_E} \gamma_R \right) d\gamma_R. \quad (26)$$

De acordo com [28], temos o seguinte resultado para essa integral:

$$INT_2 = \sum_{s=0}^\infty \frac{m_R^{(s)} d_2^s}{\mu_R^{(s)} s!} \left(\left(\frac{\left(\frac{(1+\kappa_E)\mu_E}{\bar{\gamma}_E} \right)^{\mu_E+n} \Gamma(\mu_R + s + \mu_E + n)}{(\mu_E + n) \left(\frac{(1+\kappa_E)\mu_E}{\bar{\gamma}_E} + \frac{(1+\kappa_R)\mu_R}{\bar{\gamma}_R} \right)^{\mu_R+s+\mu_E+n}} \right) {}_2F_1 \left(1; \mu_R + s + \mu_E + n; \mu_E + n + 1; \frac{\frac{(1+\kappa_E)\mu_E}{\bar{\gamma}_E}}{\frac{(1+\kappa_E)\mu_E}{\bar{\gamma}_E} + \frac{(1+\kappa_R)\mu_R}{\bar{\gamma}_R}} \right) \right). \quad (27)$$

Assim sendo, a métrica *SPSC* é dada pela seguinte fórmula fechada:

$$SPSC = C_1 C_2 \left(\sum_{n=0}^\infty \frac{m_E^{(n)} d_1^n}{\mu_E^{(n)} n!} \left(\frac{(1+\kappa_E)\mu_E}{\bar{\gamma}_E} \right)^{(-\mu_E-n)} \left(\sum_{s=0}^\infty \frac{m_R^{(s)} d_2^s}{\mu_R^{(s)} s!} \left(\frac{\left(\frac{(1+\kappa_E)\mu_E}{\bar{\gamma}_E} \right)^{\mu_E+n} \Gamma(\mu_R + s + \mu_E + n)}{(\mu_E + n) \left(\frac{(1+\kappa_E)\mu_E}{\bar{\gamma}_E} + \frac{(1+\kappa_R)\mu_R}{\bar{\gamma}_R} \right)^{\mu_R+s+\mu_E+n}} \right) {}_2F_1 \left(1; \mu_R + s + \mu_E + n; \mu_E + n + 1; \frac{\frac{(1+\kappa_E)\mu_E}{\bar{\gamma}_E}}{\frac{(1+\kappa_E)\mu_E}{\bar{\gamma}_E} + \frac{(1+\kappa_R)\mu_R}{\bar{\gamma}_R}} \right) \right) \right). \quad (28)$$