UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA DE TELEINFORMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE TELEINFORMÁTICA

MESTRADO EM ENGENHARIA DE TELEINFORMÁTICA

LUCAS MAGALHÃES VASCONCELOS

SEGURANÇA NA CAMADA FÍSICA EM CANAIS *WIRETAP* COM *GENERALIZED SELECTION COMBINING* E MÚLTIPLAS ANTENAS

FORTALEZA

2017

LUCAS MAGALHÃES VASCONCELOS

SEGURANÇA NA CAMADA FÍSICA EM CANAIS *WIRETAP* COM *GENERALIZED SELECTION COMBINING* E MÚLTIPLAS ANTENAS

Dissertação apresentada ao Curso de Mestrado em Engenharia de Teleinformática do Programa de Pós-Graduação em Engenharia de Teleinformática do Centro de Tecnologia da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Engenharia de Teleinformática. Área de Concentração: Sinais e Sistemas

Orientador: Prof. Dr. Daniel Benevides da Costa

FORTALEZA

2017

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

V45s Vasconcelos, Lucas Magalhães.
Segurança na Camada Física em Canais Wiretap com Generalized Selection Combining e Múltiplas Antenas / Lucas Magalhães Vasconcelos. – 2017.
157 f. : il.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Tecnologia, Programa de Pós-Graduação em Engenharia de Teleinformática, Fortaleza, 2017.
Orientação: Prof. Dr. Daniel Benevides da Costa.

1. Desempenho de sigilo. 2. Combinação por seleção generalizada. 3. Canais espionados. 4. Múltiplas entradas e múltiplas saídas. 5. Sinais interferentes. I. Título.

CDD 621.38

LUCAS MAGALHÃES VASCONCELOS

SEGURANÇA NA CAMADA FÍSICA EM CANAIS *WIRETAP* COM *GENERALIZED SELECTION COMBINING* E MÚLTIPLAS ANTENAS

Dissertação apresentada ao Curso de Mestrado em Engenharia de Teleinformática do Programa de Pós-Graduação em Engenharia de Teleinformática do Centro de Tecnologia da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Engenharia de Teleinformática. Área de Concentração: Sinais e Sistemas

Aprovada em: 26 de Julho de 2017

BANCA EXAMINADORA

Prof. Dr. Daniel Benevides da Costa (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Charles Casimiro Cavalcante
Universidade Federal do Ceará (UFC)

Prof. Dr. Rui Facundo Vigelis
Universidade Federal do Ceará (UFC)

Aos professores e colegas de estudo.

AGRADECIMENTOS

Ao Prof. Dr. Daniel Benevides da Costa pela paciência e compreensão no processo de orientação.

Ao Colega Yosbel Rodriguez Ortega pela ajuda no desenvolvimento do trabalho.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

“O sucesso é ir de fracasso em fracasso sem perder entusiasmo.”

(Winston Churchill)

RESUMO

Esta dissertação investiga o desempenho de sigilo em canais espionados (*wiretap channel*, em inglês) e com múltiplas entradas e múltiplas saídas (MIMO, do inglês, *multiple-input multiple-output*), onde o esquema de combinação por seleção generalizada (GSC, do inglês, *generalized selection combining*) é adotado no receptor legítimo, enquanto o transmissor emprega a técnica de seleção de antena transmissora (TAS, do inglês, *transmit antenna selection*) e o espião (*eavesdropper*, em inglês) adota o esquema de combinação por razão máxima (MRC, do inglês, *maximal-ratio combining*). Se assume que o nó espião esteja sujeito a ruído e interferência (*jamming*, em inglês), e então expressões de forma fechada para a probabilidade de interrupção de sigilo (*secrecy outage probability*, em inglês) e para a taxa de sigilo não nula (*non-zero secrecy rate*, em inglês) são derivadas. Com base na probabilidade de interrupção de sigilo os ganhos de *array* e de diversidade são determinados após a realização de uma análise assintótica. A expressão de probabilidade de interrupção de sigilo obtida admite sinais interferentes de potências arbitrariamente distribuídas, e é simplificada para dois casos especiais, i.e. , sinais interferentes de potências distintas e de potências iguais. Alguns resultados numéricos representativos são apresentados para demonstrar o efeito de parâmetros sistêmicos fundamentais no desempenho de sigilo. Finalmente, a análise proposta é corroborada através de simulações de Monte Carlo.

Palavras-chave: Desempenho de sigilo. Combinação por seleção generalizada. Canais espionados. Múltiplas entradas e múltiplas saídas. Sinais interferentes. seleção de antena transmissora. Probabilidade de interrupção de sigilo. Taxa de sigilo não nula.

ABSTRACT

This thesis investigates the secrecy outage performance of multiple-input multiple-output (MIMO) wiretap channels, where a generalized selection combining (GSC) scheme is assumed at the legitimate receiver, while the transmitter employs a transmit antenna selection (TAS) technique and the eavesdropper adopts a maximal-ratio combining (MRC) scheme. Assuming that the eavesdropper is subject to noise and jamming, closed-form expressions for the secrecy outage probability and for the non-zero secrecy rate are derived. Based on the secrecy outage probability the diversity and array gains are determined after performing an asymptotic analysis. The derived secrecy outage probability expression allows for arbitrary power distributed jamming signals, and are simplified to two special cases, i.e., distinct and equal power distributed jamming signals. Some representative numerical results are depicted to show the effects of the key system parameters on the secrecy performance. Finally, the proposed analysis is corroborated through Monte Carlo simulations.

Keywords: Secrecy performance. Generalized selection combining. MIMO wiretap channels. Jamming signals. Transmit antenna selection. Secrecy outage probability. Non-zero secrecy rate.

LISTA DE FIGURAS

LISTA DE ALGORITMOS

LISTA DE ABREVIATURAS E SIGLAS

AWGN	Additive White Gaussian Noise
AF	Amplify-and-Forward
AM	Adaptive Modulation
BCC	Broadcast Confidential Channels
CDF	Cumulative Distribution Function
CEE	Channel Estimation Errors
CSI	Channel State Information
DOA	Direction of Arrival
EGC	Equal Gain Combining
FEC	Forward Error Correction
FJ	Friendly Jammer
GSC	Generalized Selection Combining
GTEL	Wireless Telecommunications Research Group
IA	Interference Alignment
iid	independent and identically distributed
MIMO	Multiple Input Multiple Output
MISO	Multiple Input Single Output
ML	Maximum Likelihood
MRC	Maximum Ratio Combining
MRT	Maximum Ratio Transmission
PDF	Probability Density Function
PHY	Physical Layer
QoS	Quality of Service
PO	Outage Probability
RF	Rádio Frequência
RMS	Root Mean Square
SC	Selection Combining
SER	Symbol Error Rate
SINR	Signal to Interference-plus-Noise Ratio
SISO	Single Input Single Output

SIMO	Single Input Multiple Output
SIR	Signal to Interference Ratio
SNR	Signal to Noise Ratio
ST	Space-Time Codes
STBC	ST-Block Codes
STTC	ST-Trellis Codes
TAS	Transmit Antenna Selection
TB	Transmit Beamforming
TC	Threshold Combining
UFC	Federal University of Ceará
VA	Variável Aleatória

LISTA DE SÍMBOLOS

$(.)^{\dagger}$	Conjugado trasposto
$\|\|.\|\|$	Norma de Frobenius
$(.)^{T}$	Operador trasposto
$\|.\|$	Valor absoluto
$f_{\gamma_{\mathrm{B,s}}}$	PDF da SNR em Bob
$f_{\gamma_{\mathrm{I}}+1}$	PDF dos sinais interferentes mais o ruído
$f_{\Upsilon_{\mathrm{E,s}}}$	PDF da SINR em Eve
$F_{\gamma_{\mathrm{B,s}}}$	CDF da SNR em Bob
G_{D}	Ganho de diversidade
G_{A}	Ganho de *array*
$\gamma_{\mathrm{B,s}}$	SNR em Bob
$\bar{\gamma}_{\mathrm{B}}$	SNR média em Bob
$\bar{\gamma}_{i}$	Potência do i^{simo} sinal de interferência
γ_{I}	Potência média de interferência
$\bar{\gamma}_{\mathrm{E}}$	Variância do canal Alice-Eve
$\Upsilon_{\mathrm{E,s}}$	SINR em Eve
$\Gamma(.)$	Função Gamma
$\Psi(.,.,.)$	Função de Tricomi
$h^{\delta}_{\mathrm{AB},k}$	Coeficiente de canal entre a k^{sima} antena de Alice e a δ^{sima} antena de Bob
$h_{\mathrm{AB,s}}$	Coeficiente de desvanecimento no enlace Alice-Bob
$\mathbf{h}_{\mathrm{AB},k}$	Vetor de canal com dimensões $N_B \times 1$ entre Bob e a k^{sima} antena em Alice
$\mathbf{h}_{\mathrm{AB,s}}$	Vetor de canal com dimensões $N_B \times 1$ entre a antena selecionada por Alice e Bob
$\mathbf{h}_{\mathrm{AE,s}}$	Vetor de canal com dimensões $N_E \times 1$ entre Eve e a antena selecionada por Alice
$\mathbf{h}_{\mathrm{i}}$	Vetor do canal entre Eve e o i^{simo} sinal de interferência
h_{i}	Coeficiente do canal de interferência

n_{B}	Componente de AWGN
$\mathbf{n}_{\mathrm{B}}$	Vetor de canal do AWGN com dimensões N_Bx1
$\mathbf{n}_{\mathrm{E}}$	Vetor de canal do AWGN com dimensões N_Ex1
P	Potência de transmissão
Pr(.)	Probabilidade
P_{s}	Probabilidade de *outage*
P_{r}	Taxa de sigilo não nula
P_{s}^{∞}	Probabilidade de *outage* assintótica
R	Limiar estabelecido
$R_{\mathrm{B,s}}$	Capacidade do canal Alice-Bob
$R_{\mathrm{E,s}}$	Capacidade do canal Alice-Eve
R_{S}	Capacidade de sigilo
s	Índice da antena de transmissão selecionado por Alice
σ^2	Variância
x	Sinal transmitido
y_{B}	Sinal combinado em Bob
y_{E}	Sinal combinado em Eve

SUMÁRIO

1 INTRODUÇÃO

1.1 Contexto do Problema

As comunicações sem fio se tornaram praticamente onipresentes nos últimos anos. Consequentemente, as informações de indivíduos e corporações em algum momento serão transmitidas em algum enlace sem fio, e isso gera uma grande preocupação de segurança nas comunicações sem fio.

A liberdade de um canal de comunicação sem fio tem uma falha de segurança inerente: a vulnerabilidade à espionagem (SCHNEIER, 1998). Soma-se a isso o fato de que o volume de dados transmitidos em redes sem fio atraem indivíduos maliciosos que objetivam espionar esses dados. Portanto, pode-se concluir que existe um verdadeiro problema de segurança nas comunicações sem fio.

A abordagem de segurança tradicional se baseia na criptografia em camadas mais altas da pilha de protocolos de comunicação (SILVA *et al.*, 2008), no gerenciamento de chaves de segurança (SILVA *et al.*, 2008) ou na codificação de canal (SHANNON, 1949). As técnicas atuais para quebrar essas abordagens tradicionais são muito sofisticadas, tendo isso em vista uma possível medida de segurança complementar foi proposta nos últimos anos em (WYNER, 1975; CSISZAR; KORNER, 1978; LEUNG-YAN-CHEONG; HELLMAN, 1978). Esta nova abordagem de segurança consiste em garantir a transmissão de dados se baseando nas características espaço-temporais do canal sem fio, ou seja, em implementar a segurança na camada física(PHY).

Por causa da relevância atual das comunicações MIMO, a segurança na camada física(PHY) tornou-se uma nova abordagem de segurança relevante para comunicações sem fio e um novo campo de pesquisa.

A segurança na camada física foi introduzida pelos trabalhos desenvolvidos por Wyner (WYNER, 1975), que apresentou o conceito de canais *wiretap*, no qual um Tx legítimo deseja enviar uma mensagem confidencial para um Rx legítimo de modo a evitar que um nó espião tome conhecimento da mensagem. Wyner demostrou que essa estratégia é eficaz para garantir um nível aceitável de sigilo em redes sem fio.

Como este campo de pesquisa ainda é relativamente recente, novas estratégias estão surgindo e trabalhos nesta área são relevantes, pois há bastante espaço para inovação.

1.2 Revisão da Literatura

O canal *wiretap* foi introduzido por Wyner (WYNER, 1975), no qual o canal entre o Transmissor(Tx) e o nó espião é uma versão degradada o canal entre Tx e o receptor legítimo(Rx), ou seja, quando o canal entre Tx e o espião é uma versão degradada do canal entre Tx e Rx o sigilo na transmissão da informação é garantido.

O canal *wiretap* foi generalizado para um canal *wiretap* não degradado por Csiszar and Korner (CSISZAR; KORNER, 1978), e extendido para o canal *wiretap* Gaussiano por Leung-YanCheong e Hellman (LEUNG-YAN-CHEONG; HELLMAN, 1978)

Os resultados desses trabalhos primordiais mostraram que uma capacidade de sigilo positiva pode ser alcançada se o receptor legítimo possuir um canal melhor que o do espião.

Estes estudos seminais (WYNER, 1975; CSISZAR; KORNER, 1978; LEUNG-YAN-CHEONG; HELLMAN, 1978) iniciaram o campo de pesquisa da segurança na camada física(*PHY security*, em inglês) de redes sem fio, que ao longo dos últimos anos tem sido amplamente investigada a partir de diferentes perspectivas.

Em particular, voltando nossa atenção para o desempenho de sigilo, (ALVES *et al.*, 2012; YANG *et al.*, 2013b; YANG *et al.*, 2013a; FERDINAND *et al.*, 2013; COSTA *et al.*, 2016) realizaram uma análise abrangente.

Em (ALVES *et al.*, 2012), os autores propuseram o esquemas TAS, que revelou que níveis mais altos de segurança podem ser atingidos quando o número de antenas no transmissor(Tx) aumenta, mesmo quando o espião possuir múltiplas antenas. TAS é utilizado porque requer *feedback* e processamento de sinais para apenas uma antena.

O trabalho em (ALVES *et al.*, 2012) foi generalizado em (YANG *et al.*, 2013b) se assumindo que todos os nós estão equipados com múltiplas antenas.

Em (YANG *et al.*, 2013a), o impacto da correlação das antenas no desempenho de sigilo foi examinado e chegou-se à conclusões relevantes. Por exemplo, foi demonstrado que quando a relação sinal-ruído(SNR, do inglês, *signal-to-noise ratio*) média do canal legítimo está baixa, maiores níveis de correlação no espião oferecem maiores efeitos benéficos no desempenho de sigilo do que níveis mais altos de correlação no receptor legítimo(Rx).

Em (FERDINAND *et al.*, 2013), se assumindo um canal *wiretap* com MISO com o esquema TAS no Tx, se examinou os efeitos da informação de estado do canal (CSI, do inglês, *channel state information*) desatualizada no desempenho de sigilo. Foi demonstrado que o ganho de diversidade esperado não pode ser alcançado quando a CSI estiver desatualizada durante o

processo de seleção da antena.

Outra maneira de assegurar a segurança na camada física(*PHY security*, em inglês) é através da utilização de sinais interferentes(*jamming signals*, em inglês) para atrapalhar a recepção do espião (COSTA *et al.*, 2016; ZHOU; MCKAY, 2010), e na prática essa técnica tem sido amplamente empregada.

Em (ZHOU; MCKAY, 2010), há o uso simplificado de interferência como ferramenta de garantia de sigilo. O Tx transmite simultaneamente a mensagem para o Rx legítimo e um ruído artificial para o nó espião. Como neste caso Tx é passivo e não há cooperação, não pode-se considerar como uso exato de sinais interferentes.

Mais recentemente, considerando-se um cenário de espionagem com interferência limitada em (COSTA *et al.*, 2016), o desempenho de sigilo de canais *wiretap* com MIMO foi investigado. Os resultados revelaram que o ganho de diversidade foi igual à $min(M, N_A N_B)$, com M indicando o número de sinais interferentes, N_A e N_B sendo, respectivamente, o número de antenas em Tx e no Rx legítimo. Neste caso há o uso de sinais interferentes(*jamming signals*, em inglês), pois existe cooperação entre Rx e FJ(*friendly jammer*, em inglês).

Os trabalhos mencionados anteriormente possuem em comum o fato de que o Rx legítimo emprega o esquema MRC ou SC. Diferentemente desses trabalhos, (YANG *et al.*, 2013c) propôs o esquema TAS com a estratégia GSC no Rx legítimo. Basicamente, o sistema funciona da seguinte maneira, uma única antena das N_A antenas do Tx é selecionada, enquanto L_B antenas das N_B do Rx legítimo são combinadas. Note que GSC pode ser visto como um caso geral do MRC ($L_B = N_B$) e SC ($L_B = 1$). Entretanto, uma das desvantagens de (YANG *et al.*, 2013c) é a fato de que se assumiu que o espião estava sujeito à apenas ruído branco Gaussiano (AWGN, do inglês,*additive white gaussian noise*).

1.3 Motivação e Objetivos

Pela análise dos trabalhos feita anteriormente, podemos concluir que um caso *wiretap*/MIMO com o uso simultâneo de GSC e sinais interferentes ainda não foi investigado .

A maior parte da literatura investiga os casos de canal *wiretap* com MIMO ou MISO e com o uso de MRC ou SC no Rx legítimo. Os casos em que se utiliza GSC, não se faz uso de sinais interferentes no nó espião.

Como GSC é o caso generalizado de MRC e SC, pode-se fazer uma análise mais detalhadas do quão degradado pode estar o canal principal para ainda assim se garantir o sigilo.

Este trabalho visa generalizar os resultado de (COSTA *et al.*, 2016) e (YANG *et al.*, 2013c) ao assumir que o nó espião é afetado simultaneamente por ruído e sinais interferentes.

Motivados pelos benefícios das técnicas discutidas anteriormente, este trabalho vai analisar um cenário único com o uso de TAS, GSC, MIMO e Sinais Interferentes.

Logo, os objetivos desta dissertação serão:

- Descrever o cenário do sistema, no qual Tx, Rx e o nó espião estão equipados com múltiplas antenas. O esquema TAS é utilizado em Tx para selecionar uma de suas antenas. Parte das antenas de Rx são combinadas em Rx através do esquema GSC. O nó espião utiliza o esquema MRC. Múltiplos sinais interferentes são utilizados para atrapalhar o nó espião.
- Derivar expressões de forma fechada para a probabilidade de interrupção de sigilo e para a taxa de sigilo não nula.
- Realizar uma análise assintótica com base na probabilidade de interrupção de sigilo para encontrar os ganhos de *array* e de diversidade.
- Demonstrar o efeito de parâmetros sistêmicos fundamentais no desempenho de sigilo através de alguns resultados numéricos representativos.
- Corroborar a análise proposta neste trabalho através de simulações de Monte Carlo.

1.4 Estrutura da Dissertação

Esta dissertação está organizada da seguinte maneira:

- **Capítulo 2:** Consiste na apresentação dos conceitos teóricos que servirão de base para o entendimento geral desta dissertação e para o desenvolvimento das demonstrações e análises dos capítulos subsequentes.
- **Capítulo 3:** O modelo do sistema *wiretap*/MIMO com TAS, GSC e sinais interferentes será apresentado. Os diferentes canais envolvidos serão modelados matematicamente e expressões de forma fechada que os descrevem estatisticamente serão derivadas, e baseando-se nessas expressões as diferentes métricas de desempenho de sigilo também serão derivadas em expressões de forma fechada, as quais serão: Probabilidade de interrupção de Sigilo, Taxa de Sigilo não Nula, Probabilidade de interrupção de Sigilo Assintótica, Ganho de Diversidade e Ganho de *Array*.
- **Capítulo 4:** Resultados numéricos serão apresentados a fim de validar as expressões de forma fechada que foram derivadas no Capítulo 3 e se analisará os efeitos de parâmetros sistêmicos fundamentais no desempenho de sigilo do sistema. Finalmente, os resultados serão corroborados através de simulações de Monte Carlo.
- **Capítulo 5:** As conclusões e perspectivas futuras desta dissertação serão apresentadas neste capítulo.

1.5 Produção Científica

Artigo publicado:

– **Lucas M. Vasconcelos**, Yosbel R. Ortega, Daniel B. da Costa, Rafael T. de Sousa Jr e William F. Giozza, *"PHY Security of MIMO Wiretap Channels with Generalized Selection Combining"*. XXXIV Simpósio Brasileiro de Telecomunicações e Processamento de Sinais (SBrT), Santarém, Pará, Setembro 2016.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo será apresentada a fundamentação teórica dos conceitos que servirão de base para o entendimento geral desta dissertação e para o desenvolvimento das demonstrações e análises dos capítulos subsequentes. De forma geral, esses conceitos teóricos serão:

- Definições e resultados que serão utilizados ao longo desta dissertação
- AWGN
- Desvanecimento *Rayleigh*
- SISO
- SIMO
- MIMO
- GSC
- MRC
- SC
- TAS
- Métricas de Desempenho
- Segurança na Camada Física
- *Wiretap*
- *Jamming*
- Métricas de Desempenho de Sigilo

Vamos iniciar citando e demonstrando as definições e resultados que serão utilizados ao longo desta dissertação:

Definição 1 *Arranjo simples de n elementos tomados r a r, onde $n \geq 1$ e r é um número natural, é qualquer ordenação de r elementos entre os n elementos, em que cada maneira de tomar os elementos se diferenciam pela ordem e natureza dos elementos.*

A fórmula para cálculo de arranjo simples é dada por:

$$\begin{aligned} A_r^n &= \frac{n!}{(n-r)!} \\ &= r!\binom{n}{r} \end{aligned} \tag{2.1}$$

Onde n é o total de elementos e r o número de elementos escolhidos.

Definição 2 *Se dois eventos, A e B são independentes então a probabilidade conjunta é:*

$$\Pr(A \text{ e } B) = \Pr(A,B) = \Pr(A \cap B) = \Pr(A)\Pr(B) \tag{2.2}$$

Onde $\Pr()$ *é a probabilidade.*

Definição 3 *Se dois eventos, A e B são mutuamente exclusivos então a probabilidade de qualquer um ocorrer é:*

$$\Pr(A \text{ ou } B) = \Pr(A \cup B) = \Pr(A) + \Pr(B) \tag{2.3}$$

Definição 4 *A função de densidade de probabilidade(pdf)* $f_X(x)$ *de uma variável aleatória X é definida por:*

$$\Pr(a \leq X \leq b) = \int_a^b f_X(x)dx \tag{2.4}$$

Definição 5 *A pdf conjunta de n variáveis aleatória contínuas* $\{X_i\}_{i=1}^n$ *é denotada por* $f_{X_1,X_2,...,X_n}(x_1,x_2,...,x_m$ *e definida da seguinte maneira:*

$$\begin{aligned}&\Pr(a_{X_1} \leq X_1 \leq b_{X_1} \cap a_{X_2} \leq X_2 \leq b_{X_2} \cap ... \cap a_{X_n} \leq X_n \leq b_{X_n}) \\ &= \int ... \int_I f_{X_1,X_2,...,X_n}(x_1,x_2,...,x_m)d(x_1,x_2,...,x_n)\end{aligned} \tag{2.5}$$

Onde I representa o conjunto dos intervalos de variação das variáveis

$$= \int ... \int_I f_{X_1,X_2,...,X_n}(x_1,x_2,...,x_m)d(x_1)d(x_2)...d(x_n)$$

A ordem das integrais e os limites de cada integral vão variar de acordo com a definição dos intervalos de variação de cada variável.

Caso os intervalos do conjunto I sejam independentes :

$$\begin{aligned}&\Pr(a_{X_1} \leq X_1 \leq b_{X_1} \cap a_{X_2} \leq X_2 \leq b_{X_2} \cap ... \cap a_{X_n} \leq X_n \leq b_{X_n}) \\ &= \int_{a_{X_n}}^{b_{X_n}} ... \int_{a_{X_2}}^{b_{X_2}} \int_{a_{X_1}}^{b_{X_1}} f_{X_1,X_2,...,X_n}(x_1,x_2,...,x_m)d(x_1)d(x_2)...d(x_n)\end{aligned} \tag{2.6}$$

Definição 6 *Sejam duas variáveis aleatória contínuas: X com pdf* $f_X(x)$ *e Y com pdf* $f_Y(y)$*.*

X e Y são independentes se e somente se a pdf conjunta $f_{X,Y}(x,y)$ *for igual ao produto das pdf's marginais de X e Y:*

$$f_{X,Y}(x,y) = f_X(x) f_Y(y) \tag{2.7}$$

E no caso de n variáveis aleatória contínuas $\{X_i\}_{i=1}^n$ *com as respectivas pdf's* $\{f_{X_i}(x_i)\}_{i=1}^n$*, serão independentes se e somente se a pdf conjunta* $f_{X_1,X_2,...,X_n}(x_1,x_2,...,x_n)$ *for igual ao produto das pdf's marginais de* $\{X_i\}_{i=1}^n$*:*

$$f_{X_1,X_2,...,X_n}(x_1,x_2,...,x_n) = f_{X_1}(x_1) f_{X_2}(x_2) ... f_{X_n}(x_n) \tag{2.8}$$

Lema 2.0.1 *Se n variáveis aleatória contínuas* $\{X_i\}_{i=1}^n$ *com as respectivas pdf's* $\{f_{X_i}(x_i)\}_{i=1}^n$ *forem independentes, então :*

$$\begin{aligned} &\Pr(a_{X_1} \leq X_1 \leq b_{X_1} \cap a_{X_2} \leq X_2 \leq b_{X_2} \cap ... \cap a_{X_n} \leq X_n \leq b_{X_n}) \\ &= \int ... \int_I [f_{X_1}(x_1) d(x_1)] [f_{X_2}(x_2) d(x_2)] ... [f_{X_n}(x_n) d(x_n)] \end{aligned} \tag{2.9}$$

A ordem das integrais e os limites de cada integral vão variar de acordo com a definição dos intervalos de variação de cada variável.

Caso os intervalos do conjunto I também sejam independentes :

$$\begin{aligned} &\Pr(a_{X_1} \leq X_1 \leq b_{X_1} \cap a_{X_2} \leq X_2 \leq b_{X_2} \cap ... \cap a_{X_n} \leq X_n \leq b_{X_n}) \\ &= \int_{a_{X_1}}^{b_{X_1}} f_{X_1}(x_1) d(x_1) \int_{a_{X_2}}^{b_{X_2}} f_{X_2}(x_2) d(x_2) ... \int_{a_{X_n}}^{b_{X_n}} f_{X_n}(x_n) d(x_n) \end{aligned} \tag{2.10}$$

Da ***Definição 6****, como as variáveis são independentes a pdf conjunta será:*

$$f_{X_1,X_2,...,X_n}(x_1,x_2,...,x_n) = f_{X_1}(x_1) f_{X_2}(x_2) ... f_{X_n}(x_n) \tag{2.11}$$

Substituindo na ***Definição 5****:*

$$\Pr(a_{X_1} \leq X_1 \leq b_{X_1} \cap a_{X_2} \leq X_2 \leq b_{X_2} \cap ... \cap a_{X_n} \leq X_n \leq b_{X_n}) \tag{2.12}$$
$$= \int ... \int_I f_{X_1,X_2,...,X_n}(x_1,x_2,...,x_m)d(x_1,x_2,...,x_n)$$

Onde I representa o conjunto dos intervalos de variação das variáveis

$$= \int ... \int_I f_{X_1,X_2,...,X_n}(x_1,x_2,...,x_m)d(x_1)d(x_2)...d(x_n)$$
$$= \int ... \int_I f_{X_1}(x_1)f_{X_2}(x_2)...f_{X_n}(x_n)d(x_1)d(x_2)...d(x_n)$$
$$= \int ... \int_I [f_{X_1}(x_1)d(x_1)]\,[f_{X_2}(x_2)d(x_2)]\,...\,[f_{X_n}(x_n)d(x_n)]$$

A ordem das integrais e os limites de cada integral vão variar de acordo com a definição dos intervalos de variação de cada variável.

Caso os intervalos do conjunto I também sejam independentes :

$$\Pr(a_{X_1} \leq X_1 \leq b_{X_1} \cap a_{X_2} \leq X_2 \leq b_{X_2} \cap ... \cap a_{X_n} \leq X_n \leq b_{X_n}) \tag{2.13}$$
$$= \int_{a_{X_1}}^{b_{X_1}} f_{X_1}(x_1)d(x_1) \int_{a_{X_2}}^{b_{X_2}} f_{X_2}(x_2)d(x_2)... \int_{a_{X_n}}^{b_{X_n}} f_{X_n}(x_n)d(x_n)$$

Definição 7 *A função distribuição acumulada(cdf) de uma variável aleatória X é definida por:*

$$F_X(x) = \Pr(X \leq x) \tag{2.14}$$

Definição 8 *Se a pdf e a cdf de uma variável aleatória X são $f_X(x)$ e $F_X(x)$ respectivamente, então:*

$$F_X(x) = \int_{-\infty}^{x} f_X(u)du \tag{2.15}$$

$$f_X(x) = \frac{d}{dx}F_X(x) \tag{2.16}$$

No caso multivariável:

$$f_X(x) = \frac{\partial}{\partial x}\,[F_X(x)] \tag{2.17}$$

Lema 2.0.2 *A cdf $F_X(x)$ de uma variável aleatória X assume o valor unitário quando $x \in X$ tende ao infinito:*

$$\lim_{x\to+\infty} F_X(x) = 1 \tag{2.18}$$

Podemos considerar verdade a seguinte afirmação:

$$\lim_{x\to+\infty} \Pr(X \leq x) = 1 \tag{2.19}$$

Pois $\forall x \in \mathbb{R}$ *a afirmação acima será sempre verdadeira, implicando que a probabilidade será sempre igual à* 1. *Logo:*

$$\Pr(X \leq x) = F_X(x) \implies \lim_{x\to+\infty} F_X(x) = \lim_{x\to+\infty} \Pr(X \leq x) = 1 \tag{2.20}$$

Corolário 1 ***Corolário do Teorema Fundamental do Cálculo:***

Se f *é uma função de valores reais e contínua no intervalo* $[a,b]$ *e* F *é a anti-derivada ou primitiva de* f *em* $[a,b]$ *então:*

$$\int_a^b f(t)dt = F(b) - F(a) \tag{2.21}$$

Podemos, então, afirmar que:

$$\int_a^b f(t)dt = -\int_b^a f(t)dt \tag{2.22}$$

Do teorema fundamental do cálculo podemos escrever que:

$$\int_a^b f(t)dt = F(b) - F(a) \tag{2.23}$$

$$\int_b^a f(t)dt = F(a) - F(b) \tag{2.24}$$

Logo:

$$\begin{aligned} \int_a^b f(t)dt &= F(b) - F(a) \\ &= -(F(a) - F(b)) \\ &= -\int_b^a f(t)dt \end{aligned} \tag{2.25}$$

Lema 2.0.3 *Seja X uma variável aleatória contínua com pdf $f_X(x)$ e cdf $F_X(x)$. Podemos afirmar que:*

$$\begin{aligned}\Pr(a \leq x \leq b) &= \int_a^b f_X(x)dx \\ &= F_X(b) - F_X(a)\end{aligned} \tag{2.26}$$

*Utilizando a **Definição 4**, a **Definição 8** e o **Corolário 1** :*

$$\begin{aligned}&f_X(x) = \frac{d}{dx}F_X(x) \implies F_X(x) \text{ é a anti-derivada de } f_X(x) \\ &\implies \int_a^b f_X(x)dx = F_X(b) - F_X(a)\end{aligned} \tag{2.27}$$

Logo:

$$\begin{aligned}\Pr(a \leq x \leq b) &= \int_a^b f_X(x)dx \\ &= F_X(b) - F_X(a)\end{aligned} \tag{2.28}$$

Lema 2.0.4 *Seja X uma variável aleatória contínua com pdf $f_X(x)$ e cdf $F_X(x)$. Podemos afirmar que:*

$$\Pr(X \geq x) = 1 - F_X(x) \tag{2.29}$$

*Utilizando o **Lema 2** e o **Lema 3** :*

$$\begin{aligned}\Pr(X \geq x) &\equiv \Pr(x \leq X \leq \infty) \\ &\equiv \int_x^{\infty} f_X(x) \\ &\equiv \lim_{x \to +\infty} F_X(x) - F_X(x) \\ &= 1 - F_X(x)\end{aligned} \tag{2.30}$$

Lema 2.0.5 *Seja X uma variável aleatória contínua com pdf $f_X(x)$ e cdf $F_X(x)$. Podemos afirmar que:*

$$\begin{aligned}\int_a^b f_X(x)dx &= \Pr(a \leq X \leq b) \\ &= \Pr(a < X \leq b) \\ &= \Pr(a \leq X < b) \\ &= \Pr(a < X < b)\end{aligned} \tag{2.31}$$

Utilizando a ***Definição 4*** *e o* ***Lema 3*** *:*

$$\begin{aligned}\Pr(x = a) &= \Pr(a \leq X \leq a) \\ &= \int_a^a f_X(x)dx \\ &= F_X(a) - F_X(a) \\ &= 0\end{aligned} \tag{2.32}$$

Podemos concluir que ao se calcular $\Pr(a \leq X \leq b)$ *em um intervalo* $[a,b]$*, o valor de X em a e em b não vai influenciar no resultado.*

Definição 9 *O valor médio, também chamado de valor esperado ou esperança de uma variável aleatória contínua X com função de densidade de probabilidade* $f(x)$ *é definido por:*

$$\begin{aligned}\mathrm{E}[X] &= \int_{-\infty}^{\infty} x f(x)dx \\ &= \mu \text{ (nomenclatura usual)}\end{aligned} \tag{2.33}$$

Para uma função $g(X,Y)$ *de duas variáveis aleatórias contínuas X e Y, o valor médio será definido por:*

$$\begin{aligned}&\mathrm{E}[g(X,Y)] \\ &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} g(x,y) f_{X,Y}(x,y)dxdy\end{aligned} \tag{2.34}$$

E para uma função $g(X_1, X_2, ..., X_n)$ *de n variáveis aleatórias contínuas* $X_{i=1}^{n}$ *com pdf conjunta* $f_{X_1,X_2,...,X_n}(x_1, x_1, ..., x_n)$*, o valor médio será definido por:*

$$\mathrm{E}[g(X_1,X_2,...,X_n)] \tag{2.35}$$
$$= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty}...\int_{-\infty}^{\infty} g(x_1,x_1,...,x_n) f_{X_1,X_2,...,X_n}(x_1,x_1,...,x_n) d(x_1)d(x_2)...d(x_n)$$

Lema 2.0.6 *O valor médio do produto de duas variáveis aleatórias contínuas e independentes X e Y é dado por:*

$$\mathrm{E}[XY] \tag{2.36}$$
$$= \mathrm{E}[X]\,\mathrm{E}[Y] \tag{2.37}$$

Generalizando, o valor médio para n variáveis aleatórias contínuas e independentes $\{X_i\}_{i=1}^{n}$ *com as respectivas pdf's* $\{f_{X_i}(x_i)\}_{i=1}^{n}$ *é dado por:*

$$\mathrm{E}[X_1X_2...X_n] \tag{2.38}$$
$$= \mathrm{E}[X_1]\,\mathrm{E}[X_2]...\,\mathrm{E}[X_n] \tag{2.39}$$

Da ***Definição 6****, a pdf conjunta de* $f_{X_1,X_2,...,X_n}(x_1,x_2,...,x_n)$ *será:*

$$f_{X_1,X_2,...,X_n}(x_1,x_2,...,x_n) = f_{X_1}(x_1)f_{X_2}(x_2)...f_{X_n}(x_n) \tag{2.40}$$

Substituindo $g(x_1,x_1,...,x_n) = x_1x_2...x_n$ *e* $f_{X_1,X_2,...,X_n}(x_1,x_2,...,x_n)$ *na* ***Definição 9****:*

$$\mathrm{E}[X_1X_2...X_n] \tag{2.41}$$
$$= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty}...\int_{-\infty}^{\infty} x_1x_2...x_n f_{X_1,X_2,...,X_n}(x_1,x_1,...,x_n) d(x_1)d(x_2)...d(x_n)$$
$$= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty}...\int_{-\infty}^{\infty} x_1x_2...x_n f_{X_1}(x_1)f_{X_2}(x_2)...f_{X_n}(x_n) d(x_1)d(x_2)...d(x_n)$$
$$= \int_{-\infty}^{\infty} x_1 f_{X_1}(x_1)d(x_1) \int_{-\infty}^{\infty} x_2 f_{X_2}(x_2)d(x_2)... \int_{-\infty}^{\infty} x_n f_{X_n}(x_n)d(x_n)$$
$$= \mathrm{E}[X_1]\,\mathrm{E}[X_2]...\,\mathrm{E}[X_n]$$

Definição 10 *A variância de uma variável aleatória X com valor médio* $\mathrm{E}[X]$ *é definida por:*

$$\begin{aligned}\mathrm{Var}(X) &= \mathrm{E}[(X-\mathrm{E}[X])^2] \\ &= \mathrm{E}[X^2]-\mathrm{E}[X]^2 \\ &= \sigma^2 \textit{ (nomenclatura usual)}\end{aligned} \tag{2.42}$$

Definição 11 *Regra da cadeia:*

Se $z = f(y)$ e $y = g(x)$ são funções quaisquer , então:

$$\frac{dz}{dx} = \frac{dz}{dy}\frac{dy}{dx} = f'(y)g'(x) = f'(g(x))g'(x) \tag{2.43}$$

Lema 2.0.7 *Seja uma função de valores reais $f(x)$, se $f(x)$ for estritamente crescente(ou decrescente) então a função inversa $f^{-1}(x)$ também será estritamente crescente(ou decrescente)*

Caso estritamente crescente:

$$x < y \iff f(x) < f(y) \tag{2.44}$$

Como $x \equiv f(f^{-1}(x))$ e $y \equiv f(f^{-1}(y))$:

$$x < y \iff f(f^{-1}(x)) < f(f^{-1}(y)) \iff f^{-1}(x) < f^{-1}(y) \tag{2.45}$$

Caso estritamente decrescente:

$$x < y \iff f(x) > f(y) \tag{2.46}$$

Como $x \equiv f(f^{-1}(x))$ e $y \equiv f(f^{-1}(y))$:

$$x < y \iff f(f^{-1}(x)) < f(f^{-1}(y)) \iff f^{-1}(x) > f^{-1}(y) \tag{2.47}$$

Lema 2.0.8 *Seja uma função de valores reais $f(x)$, se $f(x)$ for estritamente crescente sua derivada será sempre maior que zero $f^{'}(x) > 0$ e se $f(x)$ for estritamente decrescente sua derivada será sempre menor que zero $f^{'}(x) < 0$.*

Caso estritamente crescente:

$$x < y \iff f(x) < f(y) \tag{2.48}$$

Como $f^{'}(x)$ é definida por:

$$f^{'}(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h} \tag{2.49}$$

Caso $h > 0$:

$$\begin{aligned} h > 0 &\implies x + h > x \\ &\implies f(x+h) > f(x) \\ &\implies f(x+h) - f(x) > 0 \\ &\implies f^{'}(x) > 0 \text{ , pois } h > 0 \end{aligned} \tag{2.50}$$

Caso $h < 0$:

$$\begin{aligned} h < 0 &\implies x + h < x \\ &\implies f(x+h) < f(x) \\ &\implies f(x+h) - f(x) < 0 \\ &\implies f^{'}(x) > 0 \text{ , pois } h < 0 \end{aligned} \tag{2.51}$$

Logo $f^{'}(x) > 0$ caso $f(x)$ seja estritamente crescente.

Caso estritamente decrescente:

$$x < y \iff f(x) > f(y) \tag{2.52}$$

Como $f^{'}(x)$ é definida por:

$$f^{'}(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h} \tag{2.53}$$

Caso $h > 0$:

$$\begin{aligned} h > 0 &\implies x + h > x \\ &\implies f(x+h) < f(x) \\ &\implies f(x+h) - f(x) < 0 \\ &\implies f^{'}(x) < 0 \text{ , pois } h > 0 \end{aligned} \tag{2.54}$$

Caso $h < 0$:

$$\begin{aligned} h < 0 &\implies x + h < x \\ &\implies f(x+h) > f(x) \\ &\implies f(x+h) - f(x) > 0 \\ &\implies f'(x) < 0 \text{ , pois } h < 0 \end{aligned} \tag{2.55}$$

Logo $f'(x) < 0$ caso $f(x)$ seja estritamente decrescente.

Lema 2.0.9 *Seja $Y = g(X)$, onde X e Y variáveis aleatórias contínuas, a pdf de X é $f_X(x)$, a cdf de X é $F_X(x)$, a pdf de Y é $f_Y(y)$ e a cdf de Y é $F_Y(y)$. A técnica de transformação da função de densidade de probabilidade à partir da função $Y = g(X)$ para obter $f_Y(y)$ em função de $f_X(x)$ será:*

$$f_Y(y) = \left| \frac{d}{dy} \left[g^{-1}(y) \right] \right| f_X\left(g^{-1}(y) \right) \tag{2.56}$$

Caso** $g(X)$ **seja estritamente crescente no intervalo:

*Utilizando a **Definição 7** e o fato de $g(X)$ ser estritamente crescente :*

$$\begin{aligned} F_Y(y) &= \Pr(Y \leq y) \\ &= \Pr(g(X) \leq g(x)) \\ &= \Pr(X \leq x) \\ &= F_X(x) \\ &= F_X(g^{-1}(y)) \end{aligned} \tag{2.57}$$

*Utilizando a **Definição 8**, a **Definição 11**, o **Lema 7** e o **Lema 8**:*

$$\begin{aligned} f_Y(y) &= \frac{d}{dy} \left[F_Y(y) \right] \\ &= \frac{d}{dy} \left[F_X(g^{-1}(y)) \right] \\ &= \frac{d}{dy} \left[g^{-1}(y) \right] f_X(g^{-1}(y)) \\ &= \left| \frac{d}{dy} \left[g^{-1}(y) \right] \right| f_X\left(g^{-1}(y) \right) \text{ , pois } \frac{d}{dy} \left[g^{-1}(y) \right] > 0 \end{aligned} \tag{2.58}$$

Caso** $g(X)$ **seja estritamente decrescente no intervalo:

*Utilizando a **Definição 7**, o fato de $g(X)$ ser estritamente decrescente e o **Lema 4** :*

$$
\begin{aligned}
F_Y(y) &= \Pr(Y \leq y) \\
&= \Pr(g(X) \leq g(x)) \\
&= \Pr(X \geq x) \\
&= 1 - F_X(x) \\
&= 1 - F_X(g^{-1}(y))
\end{aligned}
\tag{2.59}
$$

*Utilizando a **Definição 8**, a **Definição 11**, o **Lema 7** e o **Lema 8**:*

$$
\begin{aligned}
f_Y(y) &= \frac{d}{dy}\left[F_Y(y)\right] \\
&= \frac{d}{dy}\left[1 - F_X(g^{-1}(y))\right] \\
&= 0 - \frac{d}{dy}\left[g^{-1}(y)\right] f_X(g^{-1}(y)) \\
&= -\frac{d}{dy}\left[g^{-1}(y)\right] f_X(g^{-1}(y)) \\
&= \left|\frac{d}{dy}\left[g^{-1}(y)\right]\right| f_X\left(g^{-1}(y)\right) \text{ , pois } \frac{d}{dy}\left[g^{-1}(y)\right] < 0
\end{aligned}
\tag{2.60}
$$

Juntando os dois casos podemos concluir que para qualquer função $g(X) = Y$:

$$
f_Y(y) = \left|\frac{d}{dy}\left[g^{-1}(y)\right]\right| f_X\left(g^{-1}(y)\right) \tag{2.61}
$$

Lema 2.0.10 *Sendo $\alpha \in \mathbb{R}$ e X uma variável aleatória, então* $\mathrm{E}[\alpha X]$ *é:*

$$
\mathrm{E}[\alpha X] = \alpha\,\mathrm{E}[X] \tag{2.62}
$$

*Definindo $Y = \alpha X = g(X)$ onde a pdf de Y é $f_Y(y)$ e a pdf de X é $f_X(x)$. Utilizando o **Lema 9**:*

$$
\begin{aligned}
f_Y(y) &= \left|\frac{d}{dy}\left[g^{-1}(y)\right]\right| f_X\left(g^{-1}(y)\right) \\
&= \left|\frac{d}{dy}\left[y/\alpha\right]\right| f_X\left(y/\alpha\right) \\
&= \left|1/\alpha\right| f_X\left(y/\alpha\right)
\end{aligned}
\tag{2.63}
$$

$$
\tag{2.64}
$$

E utilizando a ***Definição 9****:*

$$\begin{aligned} \mathrm{E}[Y] &= \mathrm{E}[\alpha X] \\ &= \int_{-\infty}^{\infty} y f_Y(y) dy \\ &= \int_{-\infty}^{\infty} y |1/\alpha| \, f_X(y/\alpha) \, dy \end{aligned} \tag{2.65}$$

Considerando que $\alpha \geq 0 \implies |1/\alpha| = 1/\alpha$ *e que* $y = \alpha x \implies dy = \alpha \, dx$*:*

$$\begin{aligned} \mathrm{E}[Y] &= \mathrm{E}[\alpha X] \\ &= \int_{-\infty}^{\infty} y f_Y(y) dy \\ &= \int_{-\infty}^{\infty} y |1/\alpha| \, f_X(y/\alpha) \, dy \\ &= \int_{-\infty}^{\infty} y (1/\alpha) f_X(y/\alpha) \, dy \\ &= \int_{-\infty}^{\infty} \alpha x (1/\alpha) f_X(\alpha x/\alpha) \, \alpha dx \\ &= \int_{-\infty}^{\infty} x f_X(x) \, \alpha dx \\ &= \alpha \int_{-\infty}^{\infty} x f_X(x) \, dx \\ &= \alpha \, \mathrm{E}[X] \end{aligned} \tag{2.66}$$

Considerando agora que $\alpha < 0 \implies |1/\alpha| = -1/\alpha$*, novamente que* $y = \alpha x \implies dy = \alpha \, dx$ *e que ao se fazer a mudança de variável* $dy = \alpha \, dx$ *com* $\alpha < 0$ *a integral tem seus limites invertidos e assim baseando-se no* ***Corolário 1*** *o sinal da integral vai se inverter :*

$$
\begin{aligned}
\mathrm{E}[Y] &= \mathrm{E}[\alpha X] \qquad (2.67)\\
&= \int_{-\infty}^{\infty} y f_Y(y) dy \\
&= \int_{-\infty}^{\infty} y |1/\alpha| f_X(y/\alpha) dy \\
&= \int_{-\infty}^{\infty} y(-1/\alpha) f_X(y/\alpha) dy \\
&= \int_{\infty}^{-\infty} \alpha x(-1/\alpha) f_X(\alpha x/\alpha) \alpha dx \\
&= -\int_{-\infty}^{\infty} \alpha x(-1/\alpha) f_X(\alpha x/\alpha) \alpha dx \\
&= \int_{-\infty}^{\infty} x f_X(x) \alpha dx \\
&= \alpha \int_{-\infty}^{\infty} x f_X(x) dx \\
&= \alpha \mathrm{E}[X]
\end{aligned}
$$

Podemos concluir finalmente que $\forall \alpha \in \mathbb{R}$

$$\mathrm{E}[\alpha X] = \alpha \mathrm{E}[X] \qquad (2.68)$$

Lema 2.0.11 *Sendo* $\alpha \in \mathbb{R}$ *e X uma variável aleatória, então* $\mathrm{Var}(\alpha X)$ *é:*

$$\mathrm{Var}(\alpha X) = \alpha^2 \mathrm{Var}(\alpha X) \qquad (2.69)$$

Utilizando a ***Definição 10*** *e o* ***Lema 10****:*

$$
\begin{aligned}
\mathrm{Var}(\alpha X) &= \mathrm{E}[(\alpha X)^2] - \mathrm{E}[\alpha X]^2 \qquad (2.70)\\
&= \mathrm{E}[\alpha^2 X^2] - (\alpha \mathrm{E}[X])^2 \\
&= \alpha^2 \mathrm{E}[X^2] - \alpha^2 \mathrm{E}[X]^2 \\
&= \alpha^2 \left(\mathrm{E}[X^2] - \mathrm{E}[X]^2\right) \\
&= \alpha^2 \mathrm{Var}(X)
\end{aligned}
$$

Definição 12 *O valor médio de uma variável aleatória complexa Z com função de densidade de probabilidade* $f_Z(z)$ *é:*

$$
\begin{aligned}
\mathrm{E}[Z] &= \mathrm{E}[\mathrm{Re(Z)}] + j\,\mathrm{E}[\mathrm{Im(Z)}] \qquad (2.71)\\
&= \int_{\mathbb{C}} z f_Z(z) dz \qquad (2.72)
\end{aligned}
$$

Definição 13 *O variância de uma variável aleatória complexa Z é dada por:*

$$\begin{aligned}\mathrm{Var}(Z) &= \mathrm{E}[|Z-\mathrm{E}[Z]|^2] \\ &= \mathrm{E}[|Z|^2]-|\mathrm{E}[Z]|^2 \\ &= \mathrm{Var}[\mathrm{Re}(\mathrm{Z})]+\mathrm{Var}[\mathrm{Im}(\mathrm{Z})]\end{aligned} \tag{2.73}$$

Definição 14 *A potência total de um sinal aleatório complexo s é dada por:*

$$\textit{Potência}(s) = \mathrm{E}[|s|^2] \tag{2.74}$$

Lema 2.0.12 *A potência total de um sinal aleatório complexo com valor médio nulo será igual à sua variância.*

$$\mathrm{E}[s] = 0 \implies \textit{Potência}(s) = \mathrm{Var}(s) \tag{2.75}$$

*Utilizando a **Definição 13** e a **Definição 14**, podemos concluir que:*

$$\mathrm{E}[s] = 0 \implies |\mathrm{E}[s]|^2 = 0 \implies \mathrm{Var}(s) = \mathrm{E}[|s|^2] - 0|\mathrm{E}[s]|^2 = \textit{Potência}(s) \tag{2.76}$$

Definição 15 *Uma variável aleatória Gaussiana complexa circularmente simétrica z com valor médio* 0 *e variância* σ^2 *possui a seguinte notação:*

$$z \sim \mathscr{CN}(0,\sigma^2) \tag{2.77}$$

E é definida por:

$$\textit{Considerando que: } z \in \mathbb{C} \implies z \equiv \mathrm{Re}(z) + j\,\mathrm{Im}(z) \tag{2.78}$$

$$\textit{Então definimos que: } \mathrm{Re}(z) \textit{ e } \mathrm{Im}(z) \textit{ são i.i.d. } \mathscr{N}(0,\sigma^2/2) \iff z \sim \mathscr{CN}(0,\sigma^2) \tag{2.79}$$

Definição 16 *A distribuição Normal ou Gaussiana de uma variável aleatória x com valor médio* μ *e variância* σ^2 *possui a seguinte notação:*

$$x \sim \mathcal{N}(\mu, \sigma^2) \tag{2.80}$$

E onde a pdf de x é:

$$f(x|\mu, \sigma^2) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \tag{2.81}$$

Definição 17 *A distribuição Rayleigh de uma variável aleatória x com moda σ, valor médio $\sigma\sqrt{\frac{\pi}{2}}$ e variância $\frac{4-\pi}{2}\sigma^2$ possui a seguinte notação:*

$$x \sim Rayleigh(\sigma) \tag{2.82}$$

E onde a pdf de x é:

$$f(x;\sigma) = \frac{x}{\sigma^2} e^{-\frac{x^2}{2\sigma^2}}, \quad x \geq 0, \tag{2.83}$$

Definição 18 *A distribuição Exponencial de uma variável aleatória x com valor médio λ^{-1} e variância λ^{-2} possui a seguinte notação:*

$$x \sim Exp(\lambda) \tag{2.84}$$

E onde a pdf de x é:

$$f(x;\lambda) = \begin{cases} \lambda e^{-\lambda x} & x \geq 0, \\ 0 & x < 0. \end{cases} \tag{2.85}$$

Definição 19 *A função geradora de momentos de uma variável aleatória X é definida por:*

$$M_X(s) = \mathrm{E}[e^{sX}], \quad s \in \mathbb{R} \tag{2.86}$$

Para uma variável aleatória X contínua com pdf $f(x)$, a função geradora de momentos é definida por:

$$\begin{aligned} M_X(s) &= \mathrm{E}[e^{sX}] \\ &= \int_{-\infty}^{\infty} e^{sx} f(x) dx \end{aligned} \tag{2.87}$$

Definição 20 *Para n inteiro e positivo, a função Gama é definida por:*

$$\Gamma(n) = (n-1)! \tag{2.88}$$

Para $z \in \mathbb{C} : \mathrm{Re}(z) > 0$, a função Gama é definida por:

$$\Gamma(z) = \int_0^\infty x^{z-1} e^{-x} dx \tag{2.89}$$

Definição 21 *A distribuição Gama de uma variável aleatória x com valor médio $\alpha\beta$ e variância $\alpha\beta^2$ possui a seguinte notação:*

$$x \sim \Gamma(\alpha, \beta) \equiv Gama(\alpha, \beta) \tag{2.90}$$

Onde α e β são constantes positivas.

E onde a pdf de x é definida por:

$$f(x; \alpha, \beta) = \frac{\beta^{-\alpha} x^{\alpha-1} e^{-\frac{x}{\beta}}}{\Gamma(\alpha)} \quad para\ x > 0\ e\ \alpha, \beta > 0 \tag{2.91}$$

*Onde $\Gamma(\alpha)$ é a função Gama da **Definição 20**.*

Se α for um inteiro positivo, a cdf de x será:

$$F(x; \alpha, \beta) = 1 - \sum_{i=0}^{\alpha-1} \frac{(\frac{x}{\beta})^i}{i!} e^{-\frac{x}{\beta}} \tag{2.92}$$

Lema 2.0.13 *Se $f_X(x)$ é a pdf de uma variável aleatória contínua X, então:*

$$\int_{-\infty}^{\infty} f_X(x) dx = 1 \tag{2.93}$$

Caso $f_X(x)$ esteja definida em um domínio $[a, b] \in \mathbb{R}^2$, então também teremos que:

$$\int_a^b f_X(x) dx = 1 \tag{2.94}$$

*Da **Definição 4**:*

$$\begin{aligned} \int_{-\infty}^{\infty} f_X(x) dx &= \lim_{a \to \infty} \Pr(-a \leq X \leq a) \\ &= 1 \end{aligned} \tag{2.95}$$

Pois $\lim_{a\to\infty}\Pr(-a \leq X \leq a)$ *sempre será verdade* $\forall X \in \mathbb{R}$.

No caso de $f_X(x)$ *estar definida em um domínio* $[a,b] \in \mathbb{R}^2$*:*

$$\int_a^b f_X(x)dx = \Pr(a \leq X \leq b) \tag{2.96}$$
$$= 1$$

Pois

$Pr(a \leq X \leq b)$ *sempre será verdade* $\forall X \in [a,b]$.

Lema 2.0.14 *A função geradora de momentos de uma variável aleatória X com distribuição Gama(*$X \sim \Gamma(\alpha,\beta)$*), para* $t < 1/\beta$*, será:*

$$M_X(t) = E\left[e^{tx}\right] \tag{2.97}$$
$$= \frac{1}{(1-\beta t)^{\alpha}}$$

*Utilizando a **Definição 19**, a pdf da **Definição 21** e o **Lema 13** :*

$$
\begin{aligned}
M_X(t) &= E\left[e^{tx}\right] \qquad (2.98)\\
&= \int_0^\infty e^{tx}\cdot\frac{1}{\Gamma(\alpha)\beta^\alpha}x^{\alpha-1}\cdot e^{-\frac{x}{\beta}}dx\\
&= \frac{1}{\Gamma(\alpha)\beta^\alpha}\int_0^\infty x^{\alpha-1}\cdot e^{-\frac{x}{\beta}+tx}dx\\
&= \frac{1}{\Gamma(\alpha)\beta^\alpha}\int_0^\infty x^{\alpha-1}\cdot e^{-\frac{x}{\beta}+\frac{\beta tx}{\beta}}dx\\
&= \frac{1}{\Gamma(\alpha)\beta^\alpha}\int_0^\infty x^{\alpha-1}\cdot e^{\frac{x(\beta t-1)}{\beta}}dx\\
&= \frac{1}{\Gamma(\alpha)\beta^\alpha}\int_0^\infty x^{\alpha-1}\cdot e^{\frac{-x(1-\beta t)}{\beta}}dx\\
&= \frac{1}{\Gamma(\alpha)\beta^\alpha}\int_0^\infty x^{\alpha-1}\cdot e^{\frac{-x}{\left[\frac{\beta}{1-\beta t}\right]}}dx\\
&= \frac{1}{\Gamma(\alpha)\beta^\alpha}\Gamma(\alpha)\left(\frac{\beta}{1-\beta t}\right)^\alpha 1 \qquad \underbrace{\int_0^\infty \frac{1}{\Gamma(\alpha)\left(\frac{\beta}{1-\beta t}\right)^\alpha}x^{\alpha-1}\cdot e^{\frac{-x}{\left[\frac{\beta}{1-\beta t}\right]}}dx}_{\text{Integral da pdf de } X\sim Gama\left(\alpha,\frac{\beta}{1-\beta t}\right) \text{ em seu domínio, logo integra para 1}}\\
&= \frac{1}{\Gamma(\alpha)\beta^\alpha}\Gamma(\alpha)\left(\frac{\beta}{1-\beta t}\right)^\alpha\\
&= \frac{1}{\beta^\alpha}\cdot\frac{\beta^\alpha}{(1-\beta t)^\alpha}\\
&= \frac{1}{(1-\beta t)^\alpha}
\end{aligned}
$$

A condição $t < 1/\beta$ é necessária para a integral acima ser finita.

Lema 2.0.15 *A distribuição Qui-quadrado central com n graus de liberdade de uma variável aleatória y com valor médio $n\sigma^2$ e variância $2n\sigma^4$ possui a seguinte notação:*

$$y \sim \chi^2(n,\sigma^2) \qquad (2.99)$$

É definida por:

$$y = \sum_{i=1}^{n} x_i^2 \qquad (2.100)$$

Onde, x_i são variáveis aleátorias gaussianas i.i.d. com valor médio nulo e variância σ^2, ou seja $\{x_i\}_{i=1}^{n} \sim \mathcal{N}(0,\sigma^2)$. E onde $n = 1$ ou um número par.

A pdf de y é:

$$f(y\,|\,n,\sigma^2) = \frac{1}{\sigma^n 2^{n/2}\Gamma(\frac{n}{2})} y^{\frac{n}{2}-1} e^{-\frac{y}{2\sigma^2}}, \qquad y \geq 0 \tag{2.101}$$

E a cdf de y é:

$$F(y\,|\,n,\sigma^2) = 1 - e^{-\frac{y}{2\sigma^2}} \sum_{k=0}^{\frac{n}{2}-1} \frac{1}{k!}\left(\frac{y}{2\sigma^2}\right)^k, \qquad y \geq 0 \tag{2.102}$$

Considerando uma variável aleatória X de distribuição normal com média zero e variância σ^2:

$$X \sim \mathcal{N}(0,\sigma^2) \tag{2.103}$$

Utilizando a definição da distribuição Qui-quadrado central com $n = 1$:

$$X^2 \sim \chi^2(1,\sigma^2) \tag{2.104}$$

*Da **Definição 19** , a função geradora de momentos de X^2 é:*

$$M_{X^2}(t) = \mathrm{E}[e^{tX^2}] \tag{2.105}$$

$$= \int_{-\infty}^{\infty} e^{tx^2} \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{x^2}{2\sigma^2}} dx \tag{2.106}$$

*Fazendo $y = \sqrt{1-2\sigma^2 t}\,x$ e utilizando o **Lema 13**:*

$$\begin{aligned} M_{X^2}(t) &= \mathrm{E}[e^{tX^2}] \qquad (2.107)\\ &= \int_{-\infty}^{\infty} e^{tx^2} \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{x^2}{2\sigma^2}} dx \\ &= \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{y^2}{2\sigma^2}} \frac{dy}{\sqrt{1-2\sigma^2 t}} \\ &= \frac{1}{\sqrt{1-2\sigma^2 t}} 1 \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{y^2}{2\sigma^2}} dy \\ &= \frac{1}{\sqrt{1-2\sigma^2 t}} \\ &= (1-2\sigma^2 t)^{-1/2} \end{aligned}$$

Observe que $M_{X^2}(t)$ possui a mesma expressão da função geradora de momentos para a distribuição $\Gamma(1/2, 2\sigma^2)$ calculada no ***Lema 14*** *.*

Vamos considerar agora n variáveis normais com média zero e variância σ^2 :

$$\{X_i\}_{i=1}^{n} \sim \mathcal{N}(0, \sigma^2) \tag{2.108}$$

Seus quadrados terão distribuição Qui-quadrado central com $n = 1$:

$$\{X_i\}_{i=1}^{n} \sim \mathcal{N}(0, \sigma^2) \tag{2.109}$$

A soma de todos esses quadrados será uma variável Qui-quadrado central para um $n > 1$ qualquer:

$$\begin{aligned} Y &= X_1^2 + X_2^2 + ... + X_n^2 \\ &= \sum_{i=1}^{n} X_i^2 \\ &\implies Y \sim \chi^2(n, \sigma^2)) \end{aligned} \tag{2.110}$$

A função geradora de momentos de Y pode ser calculada ao se utilizar a ***Definição 19****, o* ***Lema 6*** *e o resultado anterior de $M_{X^2}(t) = (1 - 2\sigma^2 t)^{-1/2}$:*

$$\begin{aligned} M_Y(t) &= \mathrm{E}\left[e^{t(X_1^2 + X_2^2 + ... + X_n^2)}\right] \\ &= \mathrm{E}\left[e^{t(X_1^2)} e^{t(X_2^2)} ... e^{t(X_n^2)}\right] \\ &= \mathrm{E}\left[e^{t(X_1^2)}\right] \mathrm{E}\left[e^{t(X_2^2)}\right] ... \mathrm{E}\left[e^{t(X_n^2)}\right] \\ &= \left[(1 - 2\sigma^2 t)^{-1/2}\right]^n \\ &= (1 - 2\sigma^2 t)^{-n/2} \quad t < \frac{1}{2\sigma^2} \end{aligned} \tag{2.111}$$

Comparado a expressão acima com a ***Definição 21****, concluimos que $\beta = 2\sigma^2$ e $\alpha = n/2$. Logo, a pdf e a cdf de Y serão:*

$$\begin{aligned} f(y; \alpha, \beta) &= \frac{\beta^{-\alpha} y^{\alpha - 1} e^{-\frac{y}{\beta}}}{\Gamma(\alpha)} \quad \textit{substituindo } \beta = 2\sigma^2 \textit{ e } \alpha = n/2 \\ &= f(y \,|\, n, \sigma^2) \\ &= \frac{1}{\sigma^n 2^{n/2} \Gamma(\frac{n}{2})} y^{\frac{n}{2} - 1} e^{-\frac{y}{2\sigma^2}}, \qquad y \geq 0 \end{aligned} \tag{2.112}$$

Como $\alpha = n/2$ é um inteiro positivo:

$$F(y;\alpha,\beta) = 1 - \sum_{i=0}^{\alpha-1} \frac{\left(\frac{y}{\beta}\right)^i}{i!} e^{-\frac{y}{\beta}} \quad \textit{substituindo } \beta = 2\sigma^2 \textit{ e } \alpha = n/2 \tag{2.113}$$
$$= F(y\,|\,n,\sigma^2)$$
$$= 1 - e^{-\frac{y}{2\sigma^2}} \sum_{k=0}^{\frac{n}{2}-1} \frac{1}{k!}\left(\frac{y}{2\sigma^2}\right)^k, \qquad y \geq 0$$

Lema 2.0.16 *Se z representa uma variável aleatória Gaussiana complexa circularmente simétrica com valor médio nulo e variância σ^2, então:*

$$z \sim \mathscr{CN}(0,\sigma^2) \implies |z| \sim Rayleigh(\sigma/\sqrt{2}) \implies |z|^2 \sim Exp(1/\sigma^2) \tag{2.114}$$

Como $z \in \mathbb{C}$:

$$z \equiv \mathrm{Re}(z) + j\,\mathrm{Im}(z) \tag{2.115}$$
$$\equiv x + jy$$

$|z|$ é:

$$|z| = \sqrt{x^2+y^2} \tag{2.116}$$
$$= \sqrt{r}$$

*Da **Definição 15** sabemos que x e y são i.i.d. $\mathscr{N}(0,\sigma^2/2)$, logo podemos utilizar o **Lema 15** para definir quer $r \sim \chi^2(2,\sigma^2/2)$:*

$$r = x^2 + y^2 \tag{2.117}$$
$$= x^2 \sim \chi^2(1,\sigma^2/2) + y^2 \sim \chi^2(1,\sigma^2/2)$$
$$\implies r \sim \chi^2(2,\sigma^2/2)$$

*Substituindo os valores na pdf do **Lema 15** teremos a pdf de r:*

$$f_R(r) = f(r\,|\,2,\sigma^2/2) \tag{2.118}$$
$$= \frac{1}{\sigma^2} e^{-\frac{r}{\sigma^2}}, \qquad r \geq 0$$

Utilizando a técnica do ***Lema 9*** *e a expressão de* $f_R(r)$ *acima, a pdf de* $|z| = \sqrt{x^2+y^2} = \sqrt{r}$ *poderá ser calculada definindo-se a função* $g(r)$*, onde* $g(r) = \sqrt{r}$ *e chamando* $v = g(r)$*. Logo:*

$$\begin{aligned} f(|z|) = f_V(v) &= \left|\frac{d}{dv}\left[g^{-1}(v)\right]\right| f_R\left(g^{-1}(v)\right) \\ &= \left|\frac{d}{dv}\left[v^2\right]\right| f\left(v^2\,|\,2,\sigma^2/2\right) \\ &= 2v f(v^2\,|\,2,\sigma^2/2) \\ &= 2v\frac{1}{\sigma^2}e^{-\frac{v^2}{\sigma^2}} \\ &= \frac{2v}{\sigma^2}e^{-\frac{v^2}{\sigma^2}} \end{aligned} \tag{2.119}$$

Fazendo uma simples manipulação de variáveis:

$$\begin{aligned} f_V(v) &= f(|z|) \\ &= \frac{2v}{\sigma^2}e^{-\frac{v^2}{\sigma^2}} \\ &= \frac{v}{(\sigma/\sqrt{2})^2}e^{-\frac{v^2}{2(\sigma/\sqrt{2})^2}} \end{aligned} \tag{2.120}$$

Comparando a expressão acima com a pdf da distribuição Rayleigh na ***Definição 17****, podemos concluir que o parâmetro* σ *da* ***Definição 17*** *será equivalente à* $\sigma/\sqrt{2}$ *da pdf acima, logo:*

$$f(|z|) = f_V(v) = \frac{v}{(\sigma/\sqrt{2})^2}e^{-\frac{v^2}{2(\sigma/\sqrt{2})^2}} \implies |z| \sim Rayleigh(\sigma/\sqrt{2}) \tag{2.121}$$

Como queríamos demonstrar.

Agora vamos demonstrar que $|z|^2 \sim Exp(1/\sigma^2)$*:*

Vamos continuar a chamar $|z| = v$*, então para calcular a pdf de* $|z|^2$ *definimos a função* $g(v) = v^2$*, chamaremos* $s = g(v)$ *e utilizamos novamente a técnica do* ***Lema 9****:*

$$
\begin{aligned}
f(|z|^2) = f_S(s) &= \left| \frac{d}{ds} \left[g^{-1}(s) \right] \right| f_V \left(g^{-1}(s) \right) \\
&= \left| \frac{d}{ds} \left[\sqrt{s} \right] \right| f_V \left(\sqrt{s} \right) \\
&= \frac{1}{2\sqrt{s}} \frac{\sqrt{s}}{(\sigma/\sqrt{2})^2} e^{-\frac{s}{2(\sigma/\sqrt{2})^2}} \\
&= \frac{1}{\sigma^2} e^{-\frac{s}{\sigma^2}}
\end{aligned}
\tag{2.122}
$$

Comparando a expressão acima com a pdf da distribuição exponencial na ***Definição 18****, podemos concluir que* $|z|^2$ *possui distribuição exponencial com o parâmetro* $\frac{1}{\sigma^2}$ *da pdf acima sendo equivalente à* λ *da* ***Definição 18****. Logo:*

$$
|z|^2 \sim Exp(1/\sigma^2) \tag{2.123}
$$

Como queríamos demonstrar.

Definição 22 *A transformada de Laplace de uma função* $f(t)$*, definida* $\forall t \geq 0 : t \in \mathbb{R}$*, é a função* $F(s)$ *definida por:*

$$
F(s) = \int_0^\infty f(t) e^{-st} dt \tag{2.124}
$$

Onde $s \in \mathbb{C}$*. Seguem outras notações equivalentes da transformada de Laplace:*

$$
\mathscr{L}\{f\}(s) = \int_0^\infty f(t) e^{-st} dt \tag{2.125}
$$

$$
\mathscr{L}\{f(t)\} = \int_0^\infty f(t) e^{-st} dt \tag{2.126}
$$

Para uma variável aleatória X com pdf $f_X(x)$*, a transformada de Laplace de* $f_X(x)$ *é definida da seguinte forma:*

$$
\mathscr{L}\{f_X\}(s) = \mathrm{E}[e^{-sX}] \tag{2.127}
$$

A transformada inversa de Laplace é definida da seguinte maneira:

$$f(t) = \mathscr{L}^{-1}\{F\}(t) = \frac{1}{2\pi j}\lim_{T\to\infty}\int_{\gamma-jT}^{\gamma+jT} e^{st}F(s)ds \tag{2.128}$$

Onde a integração é feita ao longo de $\mathrm{Re}(s) = \gamma$*. Onde* γ *é menor do que a parte real de todas as singularidade de* $F(s)$*, isso garante que a integral esteja na ROC(região de convergência).*

Lembrando que se $F(s)$ *é a transformada de Laplace de* $f(t)$*, então* $f(t)$ *é a transformada inversa de Laplace de* $F(s)$ *.*

Lema 2.0.17 *Para uma variável aleatória X com pdf* $f(x)$*, existirá a seguinte relação entre sua transformada de Laplace e a sua função geradora de momentos:*

$$\mathscr{L}\{f\}(s) = M_X(-s) \tag{2.129}$$

Da ***Definição 19*** *e da* ***Definição 22*** *:*

$$\mathscr{L}\{f\}(s) = \mathrm{E}[e^{-sX}] \tag{2.130}$$

$$M_X(s) = \mathrm{E}[e^{sX}] \tag{2.131}$$

Logo:

$$\mathscr{L}\{f\}(s) = M_X(-s) \tag{2.132}$$

Definição 23 *A função de Tricomi(ou função hipergeométrica confluente) é definida como:*

$$\Psi(a,b,z) = \frac{1}{\Gamma(a)}\int_0^\infty e^{-zt}t^{a-1}(1+t)^{b-a-1}dt \tag{2.133}$$

Onde a função $\Gamma()$ *foi definida na* ***Definição 20****.*

Lema 2.0.18 *A técnica da Integração por partes:*

$$\int u\,dv = uv - \int v\,du \tag{2.134}$$

A derivada do produto é:

$$d(uv) = u\,dv + v\,du \tag{2.135}$$

Integrando dos dois lados:

$$\int d(uv) = uv = \int u\,dv + \int v\,du \tag{2.136}$$

Rearranjando os termos:

$$\int u\,dv = uv - \int v\,du \tag{2.137}$$

Lema 2.0.19 *Seja a propriedade da Integração da transformada de Laplace de uma função real qualquer $f(x)$:*

$$\mathscr{L}\left\{\int_{t=0}^{x} f(t)dt\right\} = \frac{\mathscr{L}\{f(x)\}}{s} \tag{2.138}$$

$$\mathscr{L}\left\{\int_{t=0}^{x} f(t)dt\right\} = \int_0^{\infty}\left\{\int_{t=0}^{x} f(t)dt\right\}e^{-sx}dx \tag{2.139}$$

*Utilizando a técnica de integração do **Lema 18** com $u = \int_{t=0}^{x} f(t)dt$, $v = -\frac{1}{s}e^{-sx}$, $du = f(x)dx$ e $dv = e^{-sx}dx$:*

$$\begin{aligned}
&\int_0^{\infty}\left\{\int_{t=0}^{x} f(t)dt\right\}e^{-sx}dx \qquad (2.140)\\
&= \left[-\frac{1}{s}e^{-sx}\int_{t=0}^{x} f(t)dt\right]_0^{\infty} - \int_0^{\infty} -\frac{1}{s}e^{-sx}f(x)dx\\
&= 0 + \frac{1}{s}\int_0^{\infty} e^{-sx}f(x)dx\\
&= \frac{\mathscr{L}\{f(x)\}}{s}
\end{aligned}$$

Lema 2.0.20 *Seja a função $f(x) = x^n$ com $n = 1,2,3,\ldots$. A sua transformada de Laplace será :*

$$f(x) = x^n \iff \mathscr{L}\{f(x)\} = \frac{n!}{s^{n+1}} \tag{2.141}$$

Prova por indução:

Base da Indução: *Para* $n = 0$*:*

$$\begin{aligned}\mathscr{L}\left\{f(x) = x^0 = 1\right\} &= \int_{x=0}^{\infty} (1)e^{-sx}dx \\ &= \left[-\frac{1}{s}e^{-sx}\right]_{x=0}^{\infty} \\ &= \frac{1}{s} \\ &= \frac{0!}{s^{0+1}}\end{aligned} \tag{2.142}$$

Hipótese da Indução: *Para* $n \in \mathbb{N} : n \geq 1$*. Assumimos:*

$$\mathscr{L}\left\{x^n\right\} = \frac{n!}{s^{n+1}} \tag{2.143}$$

Indução:

$$\mathscr{L}\left\{x^{n+1}\right\} = \int_{x=0}^{\infty} x^{n+1}e^{-sx}dx \tag{2.144}$$

Utilizando a técnica de integração do ***Lema 18****, com* $u = x^{n+1}$*,* $du = (n+1)x^n$*,* $dv = e^{-sx}$ *e* $v = -\frac{1}{s}e^{-sx}$*:*

$$\begin{aligned}\int_{x=0}^{\infty} x^{n+1}e^{-sx}dx &= \left[-\frac{x^{n+1}}{s}e^{-sx}\right]_{x=0}^{\infty} + \frac{n+1}{s}\int_{x=0}^{\infty} x^n e^{-sx}dx \\ &= [0-0] + \frac{n+1}{s}\mathscr{L}\left\{x^n\right\} \\ &= \frac{n+1}{s} \times \frac{n!}{s^{n+1}} \\ &= \frac{(n+1)!}{s^{n+1+1}}\end{aligned} \tag{2.145}$$

Lema 2.0.21 *Seja* $f(x)$ *uma função qualquer e* α *uma constante real qualquer:*

$$\mathscr{L}\left\{f(x)\right\} = F(s) \iff \mathscr{L}\left\{\alpha f(x)\right\} = \alpha F(s) \tag{2.146}$$

Da ***Definição 22****:*

$$\begin{aligned}\mathscr{L}\left\{\alpha f(x)\right\} &= \int_{x=0}^{\infty} \alpha f(x)e^{-sx}dx \\ &= \alpha\int_{x=0}^{\infty} f(x)e^{-sx}dx \\ &= \alpha\mathscr{L}\left\{f(x)\right\} \\ &= \alpha F(s)\end{aligned} \tag{2.147}$$

Lema 2.0.22 *Seja $f(x)$ uma função qualquer e a uma constante real qualquer:*

$$\mathscr{L}\{f(x)\} = F(s) \iff \mathscr{L}\left\{e^{-ax}f(x)\right\} = F(s+a) \tag{2.148}$$

$$\begin{aligned}\mathscr{L}\left\{e^{-ax}f(x)\right\} &= \int_{x=0}^{\infty} e^{-ax}f(x)e^{-sx}dx \\ &= \int_{x=0}^{\infty} f(x)e^{-(s+a)x}dx \\ &= F(s+a)\end{aligned} \tag{2.149}$$

Lema 2.0.23

$$\mathscr{L}\left\{\frac{cx^n e^{-ax}}{n!}\right\} = \frac{c}{(s+a)^{n+1}} \tag{2.150}$$

*Do **Lema 20**:*

$$f(x) = x^n \iff \mathscr{L}\{f(x)\} = F(s) = \frac{n!}{s^{n+1}} \tag{2.151}$$

Observamos que:

$$F(s+a) = \frac{n!}{(s+a)^{n+1}} \tag{2.152}$$

*Utilizando o **Lema 22**:*

$$F(s+a) = \mathscr{L}\left\{e^{-ax}x^n f(x) \quad\right\} \implies \mathscr{L}\left\{x^n e^{-ax}\right\} = \frac{n!}{(s+a)^{n+1}} \tag{2.153}$$

*Utilizando o **Lema 21**:*

$$\begin{aligned}\mathscr{L}\left\{\left[\frac{c}{n!}\right] x^n e^{-ax}\right\} &= \left[\frac{c}{n!}\right] \frac{n!}{(s+a)^{n+1}} \\ &= \frac{c}{(s+a)^{n+1}}\end{aligned} \tag{2.154}$$

Lema 2.0.24 *Expansão por frações parciais para cálculo da transformada inversa de Laplace:*

$$\begin{aligned}F(s) = \frac{B(s)}{A(s)} &= \frac{B(s)}{(s+p_1)^{r_1}(s+p_2)^{r_2}...(s+p_n)^{r_n}} \\ &= \sum_{i=1}^{n}\sum_{j=1}^{r_i} \frac{a_{ij}}{(s+p_i)^j}\end{aligned} \tag{2.155}$$

Onde o grau do polinômio $B(s)$ menor que grau do polinômio $A(s)$.

*Do **Lema 23**, a transformada inversa de Laplace será:*

$$\mathscr{L}^{-1}\left\{\frac{a_{ij}}{(s+p_i)^j}\right\} = \frac{a_{ij}t^{j-1}e^{-p_i t}}{(j-1)!} \tag{2.156}$$

Logo:

$$\mathscr{L}^{-1}\left\{F(s) = \sum_{i=1}^{n}\sum_{j=1}^{r_i}\frac{a_{ij}}{(s+p_i)^j}\right\} \tag{2.157}$$
$$= \sum_{i=1}^{n}\sum_{j=1}^{r_i}\frac{a_{ij}t^{j-1}e^{-p_i t}}{(j-1)!}$$

Onde os coeficiente a_{ij} são calculados pelo seguinte sistema de equações lineares:

$$a_{ij} = \frac{d^{r_i-j}}{ds^{r_i-j}}\left[(s+p_i)^{r_i}\frac{B(s)}{A(s)}\right]_{s=-p_i} \tag{2.158}$$

Lema 2.0.25 *Sejam X e Y duas variáveis aleatórias independentes com as respectivas pdf's iguais à $f_X(x)$ e $f_Y(y)$. Então, a cdf $F_Z(z)$ do quociente*

$$Z = \frac{Y}{X} \tag{2.159}$$

será calculada da seguinte maneira:

$$F_Z(z) = \int_{-\infty}^{0}\left[\int_{xz}^{\infty} f_Y(y)dy\right] f_X(x)dx + \int_{0}^{\infty}\left[\int_{-\infty}^{xz} f_Y(y)dy\right] f_X(x)dx \tag{2.160}$$

*Utilizando a **Definição 4**, a **Definição 5**, a **Definição 6**, a **Definição 7** e o **Lema 1**:*

$$\begin{aligned} F_Z(z) &= \Pr(Y/X \leq z) \\ &= \Pr(Y \geq zX, X < 0) + \Pr(Y \leq zX, X > 0) \\ &= \Pr(zX \leq Y \leq \infty, -\infty \leq X < 0) + \Pr(-\infty \leq Y \leq zX, 0 < X \leq \infty) \\ &= \int_{-\infty}^{0}\left[\int_{xz}^{\infty} f_Y(y)dy\right] f_X(x)dx + \int_{0}^{\infty}\left[\int_{-\infty}^{xz} f_Y(y)dy\right] f_X(x)dx \end{aligned} \tag{2.161}$$

Lema 2.0.26 *Seja X uma variável aleatória com média zero e variância σ^2. A variável αX possuirá a mesma distribuição de X mas com variância $\alpha^2\sigma^2$*

*Decorre diretamente da técnica de transformação da pdf e do **Lema 11**.*

Lema 2.0.27 *De acordo com (NABAR et al., 2002), seja* $\boldsymbol{H}$ *uma matriz com número de elementos igual à* $M \in \mathbb{Z}^+$ *e cujos elementos sejam variáveis aleatórias Gaussianas complexas circularmente simétricas. Um elemento H pertencente à* $\boldsymbol{H}$ *será descrito por* $H \sim \mathscr{CN}(0,\sigma^2)$*, e de forma mais detalhada H será descrito como:*

$$H \in \boldsymbol{H} \equiv \begin{cases} H = X + jY \ : \ H \in \boldsymbol{H} \\ \text{em que, } H \text{ representa um elemento qualquer de } \boldsymbol{H} \\ \text{onde, } X \text{ e } Y \text{ são as partes reais e imaginárias de } H. \\ X \text{ e } Y \text{ são variáveis aleatórias Gaussianas i.i.d. com média zero e variância } \sigma^2/2. \\ \text{Logo, } X \text{ e } Y \text{ são } \mathscr{N}(0,\sigma^2/2) \text{ e consequentemente } H \text{ é } \mathscr{CN}(0,\sigma^2) \end{cases} \tag{2.162}$$

Vamos definir $\psi(s)$*, que será a transformada de Laplace da pdf do quadrado da norma de Frobenius de* $\boldsymbol{H}$*, sendo expressa da seguinte maneira:*

$$\psi(s) = \mathbf{E}\left[e^{-s\|\boldsymbol{H}\|^2}\right] = \mathscr{L}\left\{f_{\|\boldsymbol{H}\|^2}\right\}(s) \tag{2.163}$$

Podemos então, baseando-se em (NABAR et al., 2002), escrever que $\psi(s)$ *e a região de convergência associada(ROC) serão dadas por:*

$$\psi(s) = \prod_{i=1}^{M} \frac{1}{1+s\sigma_i}, \qquad \textit{ROC: } \mathbf{Re}(s) > \max_{\sigma_i}\left(-\frac{1}{\sigma_i}\right), \tag{2.164}$$

Onde, $\sigma_i\,(i = 1,2,...,M)$ *são os autovalores da matriz de covariância* $\boldsymbol{R}$*. Em que, a matriz de covariância* $\boldsymbol{R}$ *é definida como a matriz de covariância do correspondente vetor coluna vec*$(\boldsymbol{H})$*. Ou seja:*

$$\boldsymbol{R} = cov(\boldsymbol{H}) = cov(vec(\boldsymbol{H})) = \mathbf{E}\left[vec(\boldsymbol{H})vec(\boldsymbol{H})^{\dagger}\right] \tag{2.165}$$

Os valores σ_i *serão obtido através da decomposição em valores singulares de* $\boldsymbol{R}$

$$\begin{cases} \boldsymbol{R} = \boldsymbol{U}\Sigma\boldsymbol{U}^{\dagger} \\ \text{onde, } \Sigma = \operatorname{diag}\{\sigma_i\}_{i=1}^{M} \\ \text{e, } \boldsymbol{U} \text{ é uma matrix unitária} \end{cases} \tag{2.166}$$

Chamando os autovalores distintos e não nulos de $\boldsymbol{R}$ *como* $\widetilde{\sigma}_i\,(i=1,2,...,t:1\leq t\leq M)$ *e suas respectivas multiplicidades como* $\eta_i\,(i=1,2,...,t)$*, podemos então representar* $\psi(s)$ *de uma forma diferente através da expansão em frações parciais:*

$$\psi(s)=\sum_{i=1}^{t}\sum_{j=1}^{\eta_i}\frac{\Omega_{i,j}}{(1+s\widetilde{\sigma}_i)^j}=\mathscr{L}\{f_{\|\boldsymbol{H}\|^2}\}(s) \tag{2.167}$$

Onde os coeficientes $\Omega_{i,j}\,(i=1,2,...,t\ ;\ j=1,2,...,\eta_i)$ *são determinados ao se resolver um sistema de equações lineares seguindo os passos do capítulo 12 de (NILSSON; RIDEL, 2000):*

$$\Omega_{i,j}=\frac{1}{(\eta_i-j)!\widetilde{\sigma}_i^{\eta_i-j}}\frac{\partial^{\eta_i-j}}{\partial s^{\eta_i-j}}\left[\prod_{k=1,k\neq i}^{t}\left(\frac{1}{1+s\widetilde{\sigma}_i}\right)^{\eta_k}\right]_{s=-\frac{1}{\widetilde{\sigma}_i}}. \tag{2.168}$$

A pdf de $\|\boldsymbol{H}\|^2$ *é simplemente a transformada inversa de Laplace de* $\psi(s)$*, que é:*

$$f_{\|\boldsymbol{H}\|^2}(z)=\sum_{i=1}^{t}\sum_{j=1}^{\eta_i}\frac{\Omega_{i,j}}{(j-1)!\widetilde{\sigma}_i^{j}}z^{j-1}e^{-\frac{z}{\widetilde{\sigma}_i}}, \tag{2.169}$$

Lema 2.0.28 *Se* α *é uma constante real qualquer e Y é uma variável aleatória qualquer, então:*

$$f_{Y+\alpha}(z)=f_Y(z-\alpha) \tag{2.170}$$

Utilizando o ***Lema 9****, podemos definir* $g(Y)=Y+\alpha$*. Logo* $f_{Y+\alpha}(z)$ *será:*

$$\begin{aligned} f_{Y+\alpha}(z)&=\left|\frac{d}{dz}[z-\alpha]\right|f_Y\,(z-\alpha) \\ &=1\left|\frac{d}{dz}[z-\alpha]\right|f_Y\,(z-\alpha) \\ &=f_Y\,(z-\alpha) \end{aligned} \tag{2.171}$$

Definição 24 *Para facilitar as demonstrações, chamarei de* $\text{Parte}(h)_{Re,Im}$ *o operador que representa a parte real ou imaginária de qualquer* $h\in\mathbb{C}$*. Onde* $\mathbb{C}$ *representa o conjunto dos números complexos.*

Definição 25 *Se a variável h representa uma variável aleatória complexa que modela o desvanecimento Rayleigh puro, então h é uma variável aleatória Gaussiana complexa circularmente simétrica com variância normalizada(*$\sigma^2=1$*) e consequentemente com base no* ***Lema 16*** *:*

$$\{\mathrm{Re}(h),\mathrm{Im}(h)\} \sim \mathscr{N}(0,1/2) \iff h \sim \mathscr{CN}(0,1) \implies$$
$$\implies |h| \sim Rayleigh(1/\sqrt{2}) \implies |h|^2 \sim Exp(1) \tag{2.172}$$

Definição 26 *Para inteiros não negativos $b_1, b_2, \ldots, b_k$ onde $\sum_{i=1}^{k} b_i = n$, o coeficiente multinomial é definido por:*

$$\binom{n}{b_1, b_2, \ldots, b_k} = \frac{n!}{b_1! b_2! \cdots b_k!} \tag{2.173}$$

Lema 2.0.29 *A Expansão Binomial para um inteiro qualquer n é definida por:*

$$(x+y)^n = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) x^{n-k} y^k \tag{2.174}$$

Caso especial para $y = 1$:

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k \tag{2.175}$$

Prova por Indução:

Para $n = 1$:

$$(x+y)^1 = x+y = \left(\begin{array}{c} 1 \\ 0 \end{array} \right) x^{1-0} y^0 + \left(\begin{array}{c} 1 \\ 1 \end{array} \right) x^{1-1} y^1 = \sum_{k=0}^{1} \left(\begin{array}{c} 1 \\ k \end{array} \right) x^{1-k} y^k$$

Supondo $(x+y)^{n-1} = \sum_{k=0}^{n-1} \left(\begin{array}{c} n-1 \\ k \end{array} \right) x^{(n-1)-k} y^k$

Considerando $(x+y)^n$*:*

$$
\begin{aligned}
(x+y)^n &= (x+y)(x+y)^{n-1} \\
&= (x+y)\left[\sum_{k=0}^{n-1}\binom{n-1}{k}x^{(n-1)-k}y^k\right] \\
&= \sum_{k=0}^{n-1}\binom{n-1}{k}x^{n-k}y^k + \sum_{j=0}^{n-1}\binom{n-1}{j}x^{(n-1)-j}y^{j+1} \\
&= \sum_{k=0}^{n-1}\binom{n-1}{k}x^{n-k}y^k + \sum_{j=0}^{n-1}\binom{n-1}{(j+1)-1}x^{n-(j+1)}y^{j+1} \\
&= \sum_{k=0}^{n-1}\binom{n-1}{k}x^{n-k}y^k + \sum_{k=1}^{n}\binom{n-1}{k-1}x^{n-k}y^k \\
&= \sum_{k=0}^{n}\left[\binom{n-1}{k}x^{n-k}y^k\right] - \binom{n-1}{n}x^0y^n \\
&\quad + \sum_{k=0}^{n}\left[\binom{n-1}{k-1}x^{n-k}y^k\right] - \binom{n-1}{-1}x^ny^0 \\
&= \sum_{k=0}^{n}\left[\binom{n-1}{k} + \binom{n-1}{k-1}\right]x^{n-k}y^k \\
&= \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k
\end{aligned}
$$

Lema 2.0.30 *A Expansão Multinomial para um inteiro positivo k e um inteiro não negativo n é definida por:*

$$
(x_1+x_2+\cdots+x_k)^n = \sum_{b_1+b_2+\cdots+b_k=n}\binom{n}{b_1,b_2,b_3,\ldots,b_k}\prod_{j=1}^{k}x_j^{b_j} \tag{2.176}
$$

Onde $\binom{n}{b_1,b_2,b_3,\ldots,b_k}$ *foi definido na* ***Definição 26****.*

Prova por Indução:

Quando $k=1$ *o resultado é verdadeiro, quando* $k=2$ *o resultado recai na expansão binomial provada anteriormente no* ***Lema 25****. Considerando* $k\geq 3$ *e que o resultado é verdadeiro para* $k=p$*. Quando* $k=p+1$*:*

$$
(x_1+x_2+\cdots+x_p)^n = \big(x_1+x_2+\cdots+x_{p-1}+(x_p+x_{p+1})\big)^n.
$$

Considerando $x_p + x_{p+1}$ um único termo e usando a hipótese da indução:

$$\sum_{b_1+b_2+\cdots+b_{p-1}+B=n} \binom{n}{b_1, b_2, b_3, \ldots, b_{p-1}, B} \prod_{j=1}^{p-1} x_j^{b_j} \times (x_p + x_{p+1})^B.$$

Pela expansão binomial, teremos:

$$\sum_{b_1+b_2+\cdots+b_{p-1}+B=n} \binom{n}{b_1, b_2, b_3, \ldots, b_{p-1}, B} \prod_{j=1}^{p-1} x_j^{b_j} \times \sum_{b_p+b_{p+1}=B} \binom{B}{b_p} x_p^{b_p} x_{p+1}^{b_{p+1}}.$$

Como $\binom{n}{b_1,b_2,b_3,\ldots,b_{p-1},B}\binom{B}{b_p} = \binom{n}{b_1,b_2,b_3,\ldots,b_{p+1}}$ podemos reescrever como:

$$\sum_{b_1+b_2+\cdots+b_{p+1}=n} \binom{n}{b_1, b_2, b_3, \ldots, b_{p+1}} \prod_{j=1}^{k} x_j^{b_j}.$$

Definição 27 *O conjugado de um número complexo z, onde $z = a + bj$, é definido como:*

$$\bar{z} = z^* = a - bj \tag{2.177}$$

Onde $a = \mathrm{Re}(z)$, $b = \mathrm{Im}(z)$ e $j = \sqrt{-1}$.

Definição 28 *O conjugado transposto ou transposto Hermitiano de uma matriz $\boldsymbol{A}$ de dimensão $m \times n$ com elementos complexos é a matriz $\boldsymbol{A}^H$ ou $\boldsymbol{A}^\dagger$ de dimensão $n \times m$ obtida através através da transposta de $\boldsymbol{A}$ seguida pela substituição de todos os elementos pelos seus respectivos conjugados:*

$$\begin{aligned} \boldsymbol{A}^H &= \boldsymbol{A}^\dagger \\ &= (\overline{\boldsymbol{A}})^T \\ &= \overline{\boldsymbol{A}^T} \end{aligned} \tag{2.178}$$

Definição 29 *O produto interno complexo padrão de dois vetores $\boldsymbol{x} \in \mathbb{C}^n$ e $\boldsymbol{y} \in \mathbb{C}^n$ é definido por:*

$$\begin{aligned} \langle \boldsymbol{x}, \boldsymbol{y} \rangle &= \sum_{i=1}^{n} x_i {y_i}^* \\ &= \boldsymbol{y}^H \boldsymbol{x} \end{aligned} \tag{2.179}$$

De maneira mais detalhada:

$$\left\langle \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \right\rangle = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}^H \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \left({y_1}^*, {y_2}^*, \ldots, {y_n}^* \right) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \sum_{i=1}^{n} x_i {y_i}^* \tag{2.180}$$

Definição 30 *Seja $\boldsymbol{v} = (v_1, v_2, ..., v_n)$ um vetor complexo, onde $\boldsymbol{v} \in \mathbb{C}^n$. A norma de $\boldsymbol{v}$ é definida por:*

$$\begin{aligned} \| \boldsymbol{v} \| &= \| (v_1, v_2, ..., v_n) \| \\ &= \sqrt{|v_1|^2 + |v_2|^2 + ... + |v_n|^2} \\ &= \sqrt{\sum_{k=1}^{n} |v_k|^2} \end{aligned} \tag{2.181}$$

Lema 2.0.31 *Seja um vetor complexo $\boldsymbol{v} = (v_1, v_2, ..., v_n)$, onde $\boldsymbol{v} \in \mathbb{C}^n$:*

$$\begin{aligned} \| \boldsymbol{v} \|^2 &= \langle \boldsymbol{v}, \boldsymbol{v} \rangle \\ &= \boldsymbol{v}^H \boldsymbol{v} \end{aligned} \tag{2.182}$$

Note das definições anteriores que um vetor complexo $\boldsymbol{v} = (v_1, v_2, ..., v_n)$, onde $\boldsymbol{v} \in \mathbb{C}^n$:

$$\begin{aligned} \langle \boldsymbol{v}, \boldsymbol{v} \rangle &= \sum_{i=1}^{n} v_i {v_i}^* \\ &= \sum_{i=1}^{n} |v_i|^2 \\ &= \| \boldsymbol{v} \|^2 \end{aligned} \tag{2.183}$$

Definição 31 *A norma de Frobenius de uma matriz $\boldsymbol{H}$ de dimensão $m \times n$ qualquer é por definição:*

$$\| \boldsymbol{H} \| = \sqrt{\mathrm{tr}(\boldsymbol{H}^\dagger \boldsymbol{H})} = \sqrt{\sum_{i=1}^{m} \sum_{j=1}^{n} |h_{ij}|^2} \tag{2.184}$$

Caso $\boldsymbol{H}$ seja um vetor, $\| \boldsymbol{H} \|$ será a norma do vetor.

Lema 2.0.32 *Sejam dois vetores complexos* $\boldsymbol{x} = \left(x_1, x_2, ..., x_n\right)^T$ *e* $\boldsymbol{y} = \left(y_1, y_2, ..., y_n\right)^T$*, onde* $\boldsymbol{x} \in \mathbb{C}^n$ *e* $\boldsymbol{y} \in \mathbb{C}^n$*. A desigualdade de Cauchy-Schwarz é definida por:*

$$|\langle \boldsymbol{x}, \boldsymbol{y} \rangle| \leq ||\boldsymbol{x}||\, ||\boldsymbol{y}|| \tag{2.185}$$

Ou de forma equivalente:

$$|\langle \boldsymbol{x}, \boldsymbol{y} \rangle|^2 \leq \langle \boldsymbol{x}, \boldsymbol{x} \rangle\, \langle \boldsymbol{y}, \boldsymbol{y} \rangle \tag{2.186}$$

$$|\langle \boldsymbol{x}, \boldsymbol{y} \rangle|^2 \leq ||\boldsymbol{x}||^2\, ||\boldsymbol{y}||^2 \tag{2.187}$$

$$|\boldsymbol{y}^H \boldsymbol{x}|^2 \leq ||\boldsymbol{x}||^2\, ||\boldsymbol{y}||^2 \tag{2.188}$$

Que expandindo fica:

$$\left| \sum_{i=1}^{n} x_i y_i^* \right|^2 \leq \sum_{i=1}^{n} |x_i|^2 \times \sum_{i=1}^{n} |y_i|^2 \tag{2.189}$$

E a igualdade ocorrerá somente se para um $\lambda \in \mathbb{C}$ *qualquer:*

$$\boldsymbol{x} = \lambda \boldsymbol{y} \tag{2.190}$$

Sejam dois vetores complexos $\boldsymbol{x} = \left(x_1, x_2, ..., x_n\right)^T$ *e* $\boldsymbol{y} = \left(y_1, y_2, ..., y_n\right)^T$*, onde* $\boldsymbol{x} \in \mathbb{C}^n$ *e* $\boldsymbol{y} \in \mathbb{C}^n$*. E seja* $\lambda \in \mathbb{C}$ *um número complexo qualquer :*

Para $\langle \boldsymbol{y}, \boldsymbol{y} \rangle \neq 0$*:*

$$0 \leq \|\boldsymbol{x} - \lambda \boldsymbol{y}\|^2 = \langle \boldsymbol{x} - \lambda \boldsymbol{y}, \boldsymbol{x} - \lambda \boldsymbol{y} \rangle = \langle \boldsymbol{x}, \boldsymbol{x} \rangle - \bar{\lambda} \langle \boldsymbol{x}, \boldsymbol{y} \rangle - \lambda \langle \boldsymbol{y}, \boldsymbol{x} \rangle + |\lambda|^2 \langle \boldsymbol{y}, \boldsymbol{y} \rangle \tag{2.191}$$

Observe acima que a igualdade ocorre para $\boldsymbol{x} = \lambda \boldsymbol{y}$*. Agora escolhendo o seguinte valor de* λ*:*

$$\lambda = \langle \boldsymbol{x}, \boldsymbol{y} \rangle \cdot \langle \boldsymbol{y}, \boldsymbol{y} \rangle^{-1} \tag{2.192}$$

Obtemos:

$$0 \leq \langle \boldsymbol{x},\boldsymbol{x} \rangle - |\langle \boldsymbol{x},\boldsymbol{y} \rangle|^2 \cdot \langle \boldsymbol{y},\boldsymbol{y} \rangle^{-1} \tag{2.193}$$

Que é verdade se e somente se:

$$|\langle \boldsymbol{x},\boldsymbol{y} \rangle|^2 \leq \langle \boldsymbol{x},\boldsymbol{x} \rangle \cdot \langle \boldsymbol{y},\boldsymbol{y} \rangle \tag{2.194}$$

Ou de maneira equivalente:

$$\left|\langle \boldsymbol{x},\boldsymbol{y} \rangle\right| \leq \|\boldsymbol{x}\| \, \|\boldsymbol{y}\| \tag{2.195}$$

Definição 32 *Uma matriz* $\text{diag}\,(x_1,x_2,...,x_N)$ *de dimensão* $N \times N$ *é definida por:*

$$\text{diag}\,(x_1,x_2,...,x_N) = \begin{pmatrix} x_1 & & & & & \\ & x_2 & & & & \\ & & \ddots & & & \\ & & & x_{N-1} & & \\ & & & & x_N & \end{pmatrix} \tag{2.196}$$

Ou seja, uma matrix quadrada $N \times N$ *onde a diagonal principal é* $(x_1,x_2,...,x_N)$ *e todos os outros elementos são nulos.*

Lema 2.0.33 *Seja a matriz* $\text{diag}\left(\alpha_1,\alpha_2,...,\alpha_N\right)$ *e o vetor* $\boldsymbol{x} = \left(x_1,x_2,...,x_N\right)^T$*, então a seguinte propriedade é verdadeira:*

$$\begin{aligned} \text{diag}\left(\alpha_1,\alpha_2,...,\alpha_N\right) \boldsymbol{x} &= \text{diag}\left(\alpha_1,\alpha_2,...,\alpha_N\right) \left(x_1,x_2,...,x_N\right)^T \\ &= \left(\alpha_1 x_1,\alpha_2 x_2,...,\alpha_n x_N\right)^T \end{aligned} \tag{2.197}$$

$$\text{diag}\left(\alpha_1,\alpha_2,...,\alpha_N\right)\boldsymbol{x} = \text{diag}\left(\alpha_1,\alpha_2,...,\alpha_N\right)\left(x_1,x_2,...,x_N\right)^T \tag{2.198}$$
$$= \begin{pmatrix} \alpha_1 & & & & \\ & \alpha_2 & & & \\ & & \ddots & & \\ & & & \alpha_{N-1} & \\ & & & & \alpha_N \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_N \end{pmatrix}$$
$$= \begin{pmatrix} \alpha_1 x_1 \\ \alpha_2 x_2 \\ \vdots \\ \alpha_N x_N \end{pmatrix}$$

Lema 2.0.34 *Seja a matriz* $\boldsymbol{M} = \text{diag}\left(\alpha_1,\alpha_2,...,\alpha_N\right)$ *,* $\boldsymbol{M}^{1/2}$ *será:*

$$\boldsymbol{M}^{1/2} = \text{diag}\left(\sqrt{\alpha_1},\sqrt{\alpha_2},...,\sqrt{\alpha_N}\right) \tag{2.199}$$

$$\boldsymbol{M}^{1/2}\boldsymbol{M}^{1/2} = \text{diag}\left(\sqrt{\alpha_1},\sqrt{\alpha_2},...,\sqrt{\alpha_N}\right)\text{diag}\left(\sqrt{\alpha_1},\sqrt{\alpha_2},...,\sqrt{\alpha_N}\right) \tag{2.200}$$
$$= \begin{pmatrix} \sqrt{\alpha_1} & & & & \\ & \sqrt{\alpha_2} & & & \\ & & \ddots & & \\ & & & \sqrt{\alpha_{N-1}} & \\ & & & & \sqrt{\alpha_N} \end{pmatrix} \begin{pmatrix} \sqrt{\alpha_1} & & & & \\ & \sqrt{\alpha_2} & & & \\ & & \ddots & & \\ & & & \sqrt{\alpha_{N-1}} & \\ & & & & \sqrt{\alpha_N} \end{pmatrix}$$
$$= \begin{pmatrix} \alpha_1 & & & & \\ & \alpha_2 & & & \\ & & \ddots & & \\ & & & \alpha_{N-1} & \\ & & & & \alpha_N \end{pmatrix}$$

2.1 Ruído Branco Aditivo e Gaussiano(AWGN)

Uma forma de onda transmitida em um canal sem fio pode ser corrompida pelo ruído, tipicamente referido como Ruído Branco Aditivo e Gaussiano(AWGN, do inglês, *Additive White Gaussian Noise*)

Aditivo : Pois o ruído é "adicionado", e não multiplicado, ao sinal recebido.

Branco : O espectro do ruído é constante para todas as frequências

Gaussiano : Seja n uma variável AWGN, que representa o ruído em uma antena, então n é uma variável aleatória Gaussiana complexa circularmente simétrica com o tempo como variável, com variância σ^2 e média nula(**Definição 15**), consequentemente:

$$n \sim \mathscr{CN}(0, \sigma^2) \tag{2.201}$$

Onde:

$$\{\mathrm{Re}(n), \mathrm{Im}(n)\} \sim \mathscr{N}(0, \sigma^2/2) \tag{2.202}$$

Sendo **n** o vetor AWGN que representa o ruído em N antenas receptoras, teremos que:

$$\mathbf{n} = \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_N \end{pmatrix} \tag{2.203}$$

Agora, representando a distribuição de cada n:

$$\mathbf{n} = \begin{pmatrix} n_1 \sim \mathscr{CN}(0, \sigma_1^2) \\ n_2 \sim \mathscr{CN}(0, \sigma_2^2) \\ \vdots \\ n_N \sim \mathscr{CN}(0, \sigma_N^2) \end{pmatrix} \tag{2.204}$$

Normalmente se considera que:

$$\sigma_1^2 = \sigma_2^2 = ... = \sigma_N^2 = \sigma^2 \tag{2.205}$$

Assim:

$$\{n_1, n_2, ..., n_N\} \sim \mathscr{CN}(0, \sigma^2) \tag{2.206}$$

Logo:

$$\{n_1, n_2, ..., n_N\} \text{ são i.i.d.} \tag{2.207}$$

Pela **Definição 13**, a variância de qualquer n_k, $\forall k : 1 \leq k \leq N$ é igual à:

$$\{n_k\}_{k=1}^{N} \sim \mathscr{CN}(0,\sigma^2) \implies \text{Var}[n_k] = \sigma^2 = \text{E}[|n_k|^2] - 0|\,\text{E}[n_k]|^2 = \text{E}[|n_k|^2] \tag{2.208}$$

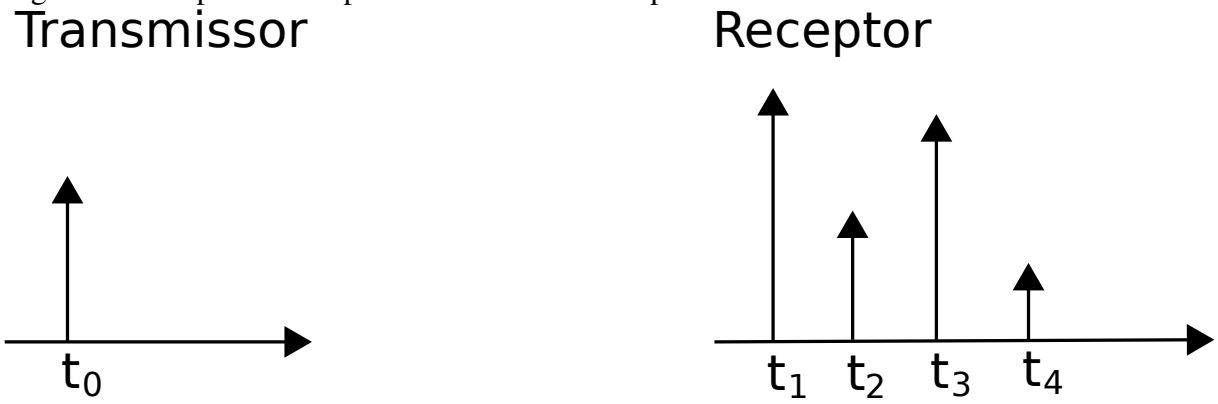
Da **Definição 14**, do **Lema 12** e da variância calculada acima podemos concluir que a potência de qualquer uma dessas variáveis n_k, $\forall k : 1 \leq k \leq N$ é igual à:

$$\text{Potência}(n_k) = \text{E}[|n_k|^2] = \text{Var}[n_k] = \sigma^2 \tag{2.209}$$

2.2 Desvanecimento *Rayleigh* Puro, Plano e Lento

Em um ambiente multipercurso, podemos visualizar de maneira intuitiva que um impulso transmitido de um transmissor chegará no receptor como um trem de impulsos.

Figura 1 – Resposta ao impulso de um canal multipercurso



Fonte: elaborado pelo autor (2017).

Seja $x(t)$ o sinal transmitido em banda passante:

$$x(t) = \text{Re}\left\{\sqrt{P}x_b(t)e^{j2\pi f_c t}\right\} \tag{2.210}$$

Onde f_c é a frequência da portadora, t é o tempo e $x_b(t)$ é o sinal transmitido em banda base com potência normalizada $\text{E}[|x_b(t)|^2] = 1$ e com valor médio nulo $\text{E}[x_b(t)] = 0$(resultados da **Definição 14** e do **Lema 12**). O sinal transmitido $x(t)$ em banda base é $\sqrt{P}x_b(t)$. P é a potência de transmissão, pois pelo **Lema 12** a potência do sinal transmitido em banda base $\sqrt{P}x_b(t)$ é:

$$\begin{aligned}\text{E}\left[\left|\sqrt{P}x_b(t)\right|^2\right] &= \left(\sqrt{P}\right)^2 1\text{E}[|x_b(t)|^2] \\ &= P\end{aligned} \tag{2.211}$$

Como podemos ver na figura acima, o sinal transmitido chega no receptor através de múltiplos percursos onde o n-ésimo percurso possui uma atenuação $\alpha_n(t)$ e um atraso $\tau_n(t)$. O sinal recebido é:

$$r(t) = \sum_n \alpha_n(t)\sqrt{P}x[t-\tau_n(t)] \tag{2.212}$$

Substituindo a expressão de $x(t)$ na expressão de $r(t)$:

$$\mathrm{Re}\left\{\sum_n \alpha_n(t)\sqrt{P}x_b[t-\tau_n(t)]e^{j2\pi f_c[t-\tau_n(t)]}\right\} \tag{2.213}$$

O equivalente em banda base do sinal recebido é:

$$\begin{aligned} r_b(t) &= \sum_n \alpha_n(t)e^{-j2\pi f_c\tau_n(t)}\sqrt{P}x_b[t-\tau_n(t)] \\ &= \sum_n \alpha_n(t)e^{-j\theta_n(t)}\sqrt{P}x_b[t-\tau_n(t)] \end{aligned} \tag{2.214}$$

onde $\theta_n(t) = 2\pi f_c\tau_n(t)$ é a fase do n-ésimo percurso.

A resposta ao impulso é:

$$h_b(t) = \sum_n \alpha_n(t)e^{-j\theta_n(t)} \tag{2.215}$$

Para um sinal $\sqrt{P}x_b(t)$ de banda estreita, a largura de banda de $\sqrt{P}x_b(t)$ será muito menor que a largura de banda do canal (desvanecimento plano). Como o recíproco da largura de banda de $\sqrt{P}x_b(t)$ é o período de símbolo T_S de um símbolo do sinal $\sqrt{P}x_b(t)$ e o espalhamento dos atrasos do canal é inversamente proporcional a largura de banda do canal, então o fato da largura de banda de $\sqrt{P}x_b(t)$ ser muito menor que a largura de banda do canal implica que T_S será muito maior que o espalhamento dos atrasos do canal. Logo, poderemos fazer a seguinte aproximação:

$$\sqrt{P}x_b[t-\tau_n(t)] \approx \sqrt{P}x_b[t] \tag{2.216}$$

Então:

$$\begin{aligned} r_b(t) &= \sum_n \alpha_n(t)e^{-j\theta_n(t)}\sqrt{P}x_b[t-\tau_n(t)] \\ &= \sqrt{P}x_b[t]\sum_n \alpha_n(t)e^{-j\theta_n(t)} \\ &= \sqrt{P}x_b[t]h_b(t) \end{aligned} \tag{2.217}$$

A fase de cada percurso pode mudar em 2π radianos quando o atraso $\tau_n(t)$ mudar em $\frac{1}{f_c}$. Se f_c for grande, movimentos relativamente pequenos no meio podem causar mudanças de 2π radianos. Como a distância entre os dispositivos são bem maiores que o comprimento de onda da portadora, é razoável considerar que a fase está uniformemente distribuída entre 0 e 2π radianos e que as fases de cada percurso são independentes (TSE; VISWANATH, 2004).

Quando há um grande número de percursos, ao se aplicar o Teorema do Limite Central, cada percurso pode ser modelado como uma variável aleatória Gaussiana complexa circularmente simétrica com o tempo como variável. Este modelo é chamado de modelo de canal com desvanecimento *Rayleigh*.

Assim, $h_b(t)$ poderá ser modelado como:

$$h_b(t) = h(t) \tag{2.218}$$

Onde $h(t) \in \mathbb{C}$, logo $h(t) = x + jy$. Como x e y são a soma de uma grande quantidade de componentes aleatórios(fato que surge do multipercurso), então pelo teorema do limite central x e y podem ser modeladas como variáveis Gaussianas. Da **Definição 15**, se $x \sim \mathcal{N}(0, \sigma^2/2)$ e $y \sim \mathcal{N}(0, \sigma^2/2)$, então:

$$h(t) \sim \mathscr{C}\mathcal{N}(0, \sigma^2) \tag{2.219}$$

E no **Lema 16** foi provado que:

$$h(t) \sim \mathscr{C}\mathcal{N}(0, \sigma^2) \implies |h(t)| \sim \text{Rayleigh}(\sigma/\sqrt{2}) \implies |h(t)|^2 \sim \text{Exp}(1/\sigma^2) \tag{2.220}$$

Vamos considerar o desvanecimento *Rayleigh* puro com variância normalizada($\sigma^2 = 1$), que foi definido na **Definição 25**. Assim teremos:

$$h(t) \sim \mathscr{C}\mathcal{N}(0, 1) \implies |h(t)| \sim \text{Rayleigh}(1/\sqrt{2}) \implies |h(t)|^2 \sim \text{Exp}(1) \tag{2.221}$$

Da **Definição 18**, da **Definição 14** e do **Lema 12**:

$$\begin{aligned} \text{E}[|h(t)|^2] &= \text{Var}(h(t)) \\ &= 1 \end{aligned} \tag{2.222}$$

Assim, $|h(t)|$ é uma variável aleatória *Rayleigh*. E pela definição de um número complexo:

$$h(t) = |h(t)|e^{j\phi} \tag{2.223}$$

Onde a distribuição da magnitude $|h(t)|$ de $h(t)$ é:

$$|h(t)| \sim \text{Rayleigh}(1/\sqrt{2}) \tag{2.224}$$

E a distribuição da fase ϕ de $h(t)$ é uniforme em $[0, 2\pi)$. A pdf *Rayleigh* de $|h|$ está definida na **Definição 17**.

Substituindo $h(t)$ na expressão de $r_b(t)$, teremos a representação em banda base de um canal com desvanecimento Rayleigh plano:

$$\begin{aligned} r_b(t) &= \sum_n \alpha_n(t) e^{-j\theta_n(t)} \sqrt{P} x_b[t - \tau_n(t)] \\ &= \sqrt{P} x_b[t] \sum_n \alpha_n(t) e^{-j\theta_n(t)} \\ &= \sqrt{P} x_b[t] h_b(t) \\ &= \sqrt{P} x_b[t] h(t) \\ &= \sqrt{P} |h(t)| e^{j\phi} x_b[t] \end{aligned} \tag{2.225}$$

Caso o canal também seja considerado um canal de desvanecimento lento, então $h(t)$ poderá ser considerado constante durante um período de símbolo $t : t_1 \leq t \leq t_2$ onde $t_2 - t_1 = T_S$, pois as variações de $h(t)$ serão muito mais lentas que as variações do sinal em banda base $\sqrt{P} x_b[t]$. Assim $\sqrt{P} x_b[t]$ em $t : t_1 \leq t \leq t_2$ será apenas um símbolo qualquer do sinal original $\sqrt{P} x_b[t]$. Logo para $t : t_1 \leq t \leq t_2$:

$$\begin{aligned} r_b(t) &= \sqrt{P} h(t) x_b[t] \\ &= \sqrt{P} h x_b[t] \end{aligned} \tag{2.226}$$

Como o tempo t acima representa um período de símbolo genêrico, podemos discretizar a notação dos sinais para um m-ésimo período de símbolo genérico:

$$r_b[m] = \sqrt{P} h x_b[m] \tag{2.227}$$

Mudando a notação do sinal em banda base normalizado x_b para x e do sinal recebido em banda base r_b para y:

$$y[m] = \sqrt{P}hx[m] \tag{2.228}$$

À partir daqui vamos considerar todos os sinais em banda base, pois as análises em banda base são suficientes para caracterizar completamente os sistemas de comunicação considerados neste trabalho.

2.3 Modelo do sistema SISO

Vamos considerar o canal com desvanecimento *Rayleigh* plano e lento e com o ruído AWGN em um sistema SISO(do inglês, *Single-Input Single-Output*). Ou seja, sistema com um único transmissor e um único receptor.

Pelas definições e propriedades do desvanecimento *Rayleigh* puro, plano, lento e do ruído AWGN dadas nas sessões anteriores, podemos escrever que o sinal transmitido em um m-ésimo período de símbolo qualquer é:

$$\sqrt{P}x[m] \tag{2.229}$$

Onde, como demonstrado anteriormente, $\mathrm{E}[|x[m]|^2] = 1$, $\mathrm{E}[x[m]] = 0$ e $\mathrm{E}[|\sqrt{P}x[m]|^2] = P$ é a potência de transmissão.

E o sinal recebido em um m-ésimo período de símbolo qualquer é:

$$y[m] = \sqrt{P}hx[m] + n[m] \tag{2.230}$$

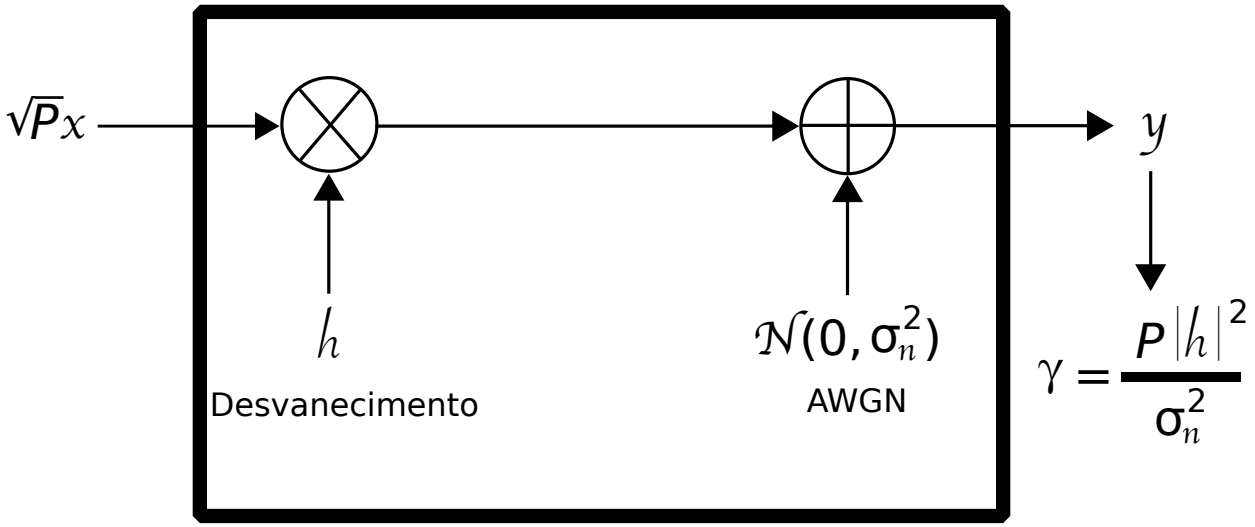
Onde n representa uma variável AWGN já definida na sessão **2.1** como $n \sim \mathscr{CN}(0, \sigma_n^2)$ onde a variável é o tempo. Como um m-ésimo período de símbolo descreve um tempo $t : t_1 \leq t \leq t_2$ onde $t_2 - t_1 = T_S$, também poderemos escrever que $n[m] \sim \mathscr{CN}(0, \sigma_n^2)$ durante um m-ésimo período de símbolo qualquer.

Como os sinais $y[m]$, $x[m]$ e $n[m]$ estão definidos para um m-ésimo período de símbolo genérico, poderemos à partir daqui omitir m na representação dos sinais. Logo a notação ficará:

$$y = \sqrt{P}hx + n \quad \text{, para um m qualquer} \tag{2.231}$$

O canal modelado está representada na figura abaixo:

Figura 2 – Modelo do canal SISO e AWGN com Desvanecimento. *Rayleigh* Puro, Plano e Lento.

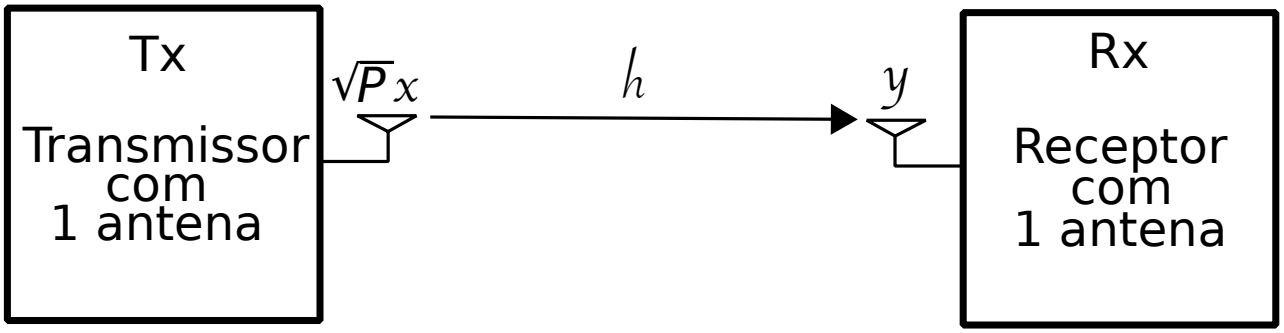


Canal AWGN com Desvanecimento *Rayleigh* Puro, Plano e Lento

Fonte: elaborado pelo autor (2017).

Assim, o sistema SISO é representado por:

Figura 3 – Sistema SISO



Fonte: elaborado pelo autor (2017).

Lembrando que da **Definição 14** e do **Lema 12** que:

$$n \sim \mathscr{CN}(0,\sigma_n^2) \implies \mathrm{E}\left[|n|^2\right] = \sigma_n^2 \tag{2.232}$$

Utilizando a **Definição 14**, o **Lema 10** e o **Lema 12**, podemos definir a relação sinal ruído(SNR, do inglês, *Signal-to-Noise Ratio*) instantânea na antena do receptor como:

$$\begin{aligned}\gamma &= \frac{\textbf{Potência do sinal}}{\textbf{Potência do ruído}} \\ &= \frac{\mathrm{E}\left[\left|\sqrt{P}hx\right|^2\right]}{\mathrm{E}\left[|n|^2\right]} \\ &= \frac{P|h|^2\,\mathrm{E}\left[|x|^2\right]}{\mathrm{E}\left[|n|^2\right]} \\ &= \frac{P|h|^2}{\sigma_n^2}\end{aligned} \tag{2.233}$$

Utilizando o **Lema 10** e o fato de que $\mathrm{E}[|h|^2] = 1$, que foi provado da sessão anterior, teremos a SNR média do receptor $\bar{\gamma}$, que vamos chamar de SNR, definida por :

$$\begin{aligned}\bar{\gamma} &= \mathrm{E}\left[\gamma\right] \\ &= \mathrm{E}\left[\frac{P|h|^2}{\sigma_n^2}\right] \\ &= \frac{P}{\sigma_n^2}1\mathrm{E}\left[|h|^2\right] \\ &= \frac{P}{\sigma_n^2} \\ &= \mathrm{SNR}\end{aligned} \tag{2.234}$$

Teremos, então, a seguinte relação:

$$\gamma = \mathrm{SNR} \times |h|^2 \tag{2.235}$$

Ao longo desta dissertação iremos sempre considerar o canal AWGN com desvanecimento *Rayleigh* puro, plano e lento, e como foi visto o período de símbolo não vai alterar a análise dos resultados. Vamos à partir daqui usar as seguintes notações para o canal AWGN com desvanecimento *Rayleigh* puro, plano e lento:

$$x = \textbf{Sinal Transmitido com Potência normalizada em 1} \tag{2.236}$$

$$\sqrt{P}x = \textbf{Sinal Transmitido com Potência } P \tag{2.237}$$

$y =$ **Sinal Recebido em uma única Antena do Receptor** (2.238)

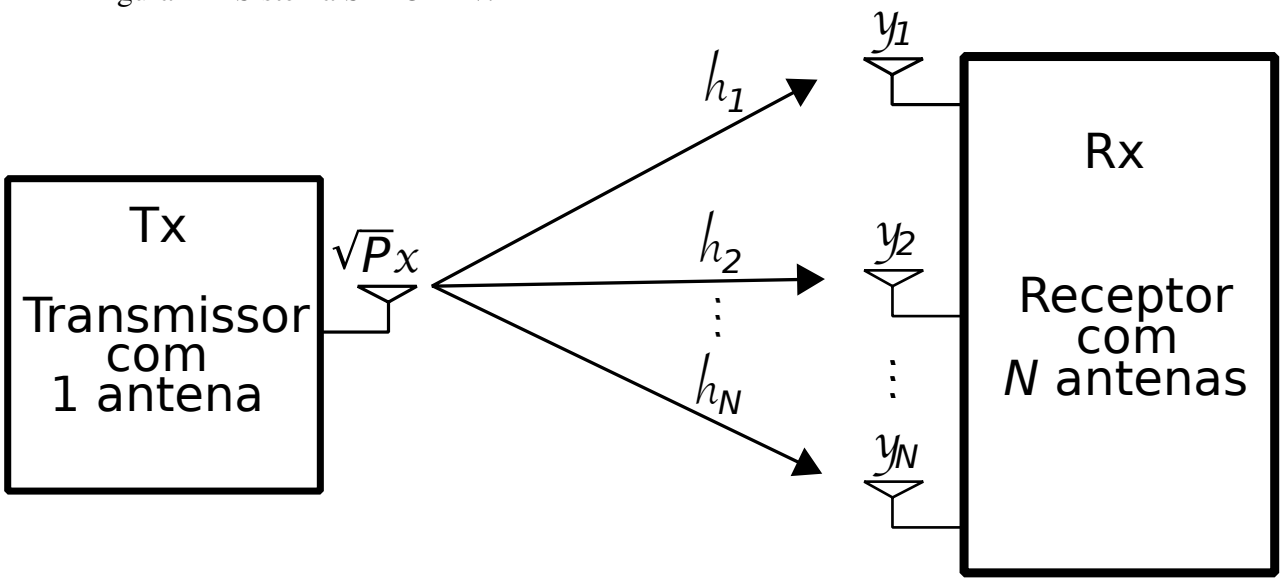
$n =$ **Variável AWGN em uma única Antena do Receptor** (2.239)

$h =$**Variável representante do Desvanecimento *Rayleigh* Puro, Plano e Lento entre uma única Antena do Transmissor e uma única Antena do Receptor** (2.240)

2.4 Modelo do sistema SIMO

Considerando o sistema SIMO(do inglês, *Single-Input Multiple-Output*), ou seja, o sistema onde uma única antena transmissora envia dados para um receptor com N antenas, como mostrado na figurara abaixo:

Figura 4 – Sistema SIMO 1xN.



Fonte: elaborado pelo autor (2017).

Todos os sinais do sistema estão representados na seguinte equação:

$$\mathbf{y} = \sqrt{P}\mathbf{h}x + \mathbf{n} \tag{2.241}$$

Onde:

$\sqrt{P}x$ é o sinal transmitido.

$\mathbf{y}$ é vetor de dimensão $1 \times N$ formado pelos sinais recebidos nas N antenas do receptor, ou seja, $\mathbf{y} = (y_1, y_2, ..., y_N)^T$ onde y_k é o sinal recebido na k-ésima antena receptora e $1 \leq k \leq N$.

$\mathbf{n}$ é vetor de dimensão $1 \times N$ formado pelas variáveis AWGN nas N antenas do receptor, ou seja, $\mathbf{n} = (n_1, n_2, n_N)^T$ onde n_k é o ruído AWGN na k-ésima antena receptora e $1 \leq k \leq N$.

$\mathbf{h}$ é vetor de dimensão $1 \times N$ formado pelas variáveis representantes do desvanecimento nas N antenas do receptor, ou seja, $\mathbf{h} = (h_1, h_2, ..., h_N)^T$ onde h_k é a variável representante do desvanecimento entre a antena transmissora e a k-ésima antena receptora e $1 \leq k \leq N$.

Assim, podemos escrever que:

$$\mathbf{y} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_N \end{pmatrix} \quad \mathbf{h} = \begin{pmatrix} h_1 \\ h_2 \\ \vdots \\ h_N \end{pmatrix} \quad \mathbf{n} = \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_N \end{pmatrix} \tag{2.242}$$

E que:

$$\sqrt{P}\mathbf{h}x = \begin{pmatrix} \sqrt{P}h_1x \\ \sqrt{P}h_2x \\ \vdots \\ \sqrt{P}h_Nx \end{pmatrix} \tag{2.243}$$

Como $\mathbf{y} = \sqrt{P}\mathbf{h}x + \mathbf{n}$:

$$\mathbf{y} = \begin{pmatrix} \sqrt{P}h_1x \\ \sqrt{P}h_2x \\ \vdots \\ \sqrt{P}h_Nx \end{pmatrix} + \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_N \end{pmatrix} \tag{2.244}$$

Logo:

$$\mathbf{y} = \begin{pmatrix} \sqrt{P}h_1 x + n_1 \\ \sqrt{P}h_2 x + n_2 \\ \vdots \\ \sqrt{P}h_N x + n_N \end{pmatrix} \tag{2.245}$$

Relembrando das sessões anteriores que:

x tem potência unitária:

$$\mathrm{E}[|x|^2] = 1 \tag{2.246}$$

O sinal transmitido $\sqrt{P}x$ tem potência P:

O ruído AWGN em cada antena receptora possui a seguinte distribuição:

$$n_k \sim \mathscr{CN}(0, \sigma_k^2) \quad , 1 \leq k \leq N \tag{2.247}$$

Que vamos considerar i.i.d., logo:

$$n_k \sim \mathscr{CN}(0, \sigma_n^2) \quad , \forall k : 1 \leq k \leq N \tag{2.248}$$

Consequentemente:

$$n_k \sim \mathscr{CN}(0, \sigma_n^2) \implies \mathrm{E}\left[|n_k|^2\right] = \sigma_n^2 \quad , \forall k : 1 \leq k \leq N \tag{2.249}$$

E que:

$$\mathrm{E}[|h_k|^2] = 1 \quad , \forall k : 1 \leq k \leq N \tag{2.250}$$

Sabendo que o sinal recebido na k-ésima antena do receptor é:

$$y_k = \sqrt{P}h_k x + n_k \tag{2.251}$$

Podemos utilizar os fatos relembrados acima e o que já foi demonstrado nas sessões anteriores, para definir a SNR instantânea na k-ésima antena do receptor(γ_k) como:

$$\begin{aligned}\gamma_k &= \frac{\textbf{Potência do sinal}}{\textbf{Potência do ruído}} \\ &= \frac{\mathrm{E}\left[\left|\sqrt{P}h_k x\right|^2\right]}{\mathrm{E}\left[|n_k|^2\right]} \\ &= \frac{P|h_k|^2\mathrm{E}\left[|x|^2\right]}{\mathrm{E}\left[|n_k|^2\right]} \\ &= \frac{P|h_k|^2}{\sigma_n^2}\end{aligned} \tag{2.252}$$

E que a SNR média na k-ésima antena do receptor($\bar{\gamma}_k$) é:

$$\begin{aligned}\bar{\gamma}_k &= \mathrm{E}[\gamma_k] \\ &= \mathrm{E}\left[\frac{P|h_k|^2}{\sigma_n^2}\right] \\ &= \frac{P}{\sigma_n^2}1\mathrm{E}\left[|h_k|^2\right] \\ &= \frac{P}{\sigma_n^2} \\ &= \mathrm{SNR} \quad , \forall k : 1 \leq k \leq N\end{aligned} \tag{2.253}$$

Como o valor $\mathrm{SNR} = \frac{P}{\sigma_n^2}$ é o mesmo para todas as antenas receptoras, o valor $\mathrm{SNR} = \frac{P}{\sigma_n^2}$ será chamado de SNR média do receptor.

Teremos, então, a seguinte relação:

$$\gamma_k = \mathrm{SNR} \times |h_k|^2 \tag{2.254}$$

2.4.1 Técnicas para Explorar a Diversidade Espacial

Em sistemas sem fio, falhas de transmissão ocorrem normalmente quando o canal está em desvanecimento profundo, resultando na falha de comunicação. Para combater esse efeito, pode-se explorar diferentes técnicas de diversidade no espaço,tempo, e frequência. Nesta dissertação, iremos focar nas técnicas para explorar a diversidade espacial. Os ganhos de diversidade espacial podem ser alcançados na tanto transmissão como na recepção. Neste trabalho vamos considerar às seguintes técnicas para explorar a diversidade espacial:

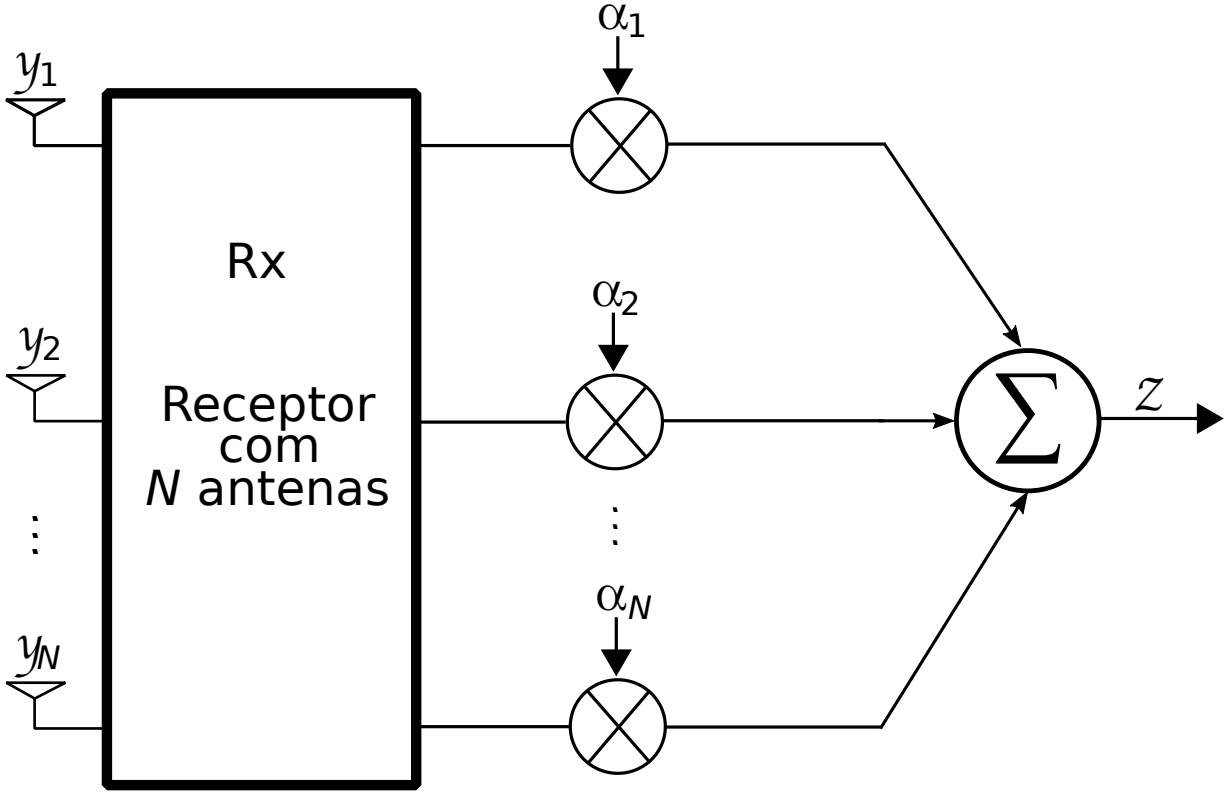
– Diversidade Espacial na Transmissão:

  - Técnica de Seleção de Antena Transmissora (TAS, do inglês, *Transmit Antenna Selection*)
- Diversidade Espacial na Recepção (Técnicas de Combinação):
  - Combinação por Seleção (SC, do inglês, *Selection Combining*)
  - Combinação por Razão Máxima (MRC, do inglês, *Maximal-Ratio Combining*)
  - Combinação por Seleção Generalizada (GSC, do inglês, *Generalized Selection Combining*)

À seguir, vamos apresentar às técnicas de combinação no receptor para o sistema SIMO.

2.4.2 Técnicas de Combinação na Recepção

Figura 5 – Combinador Linear em um Sistema SIMO



Fonte: elaborado pelo autor (2017).

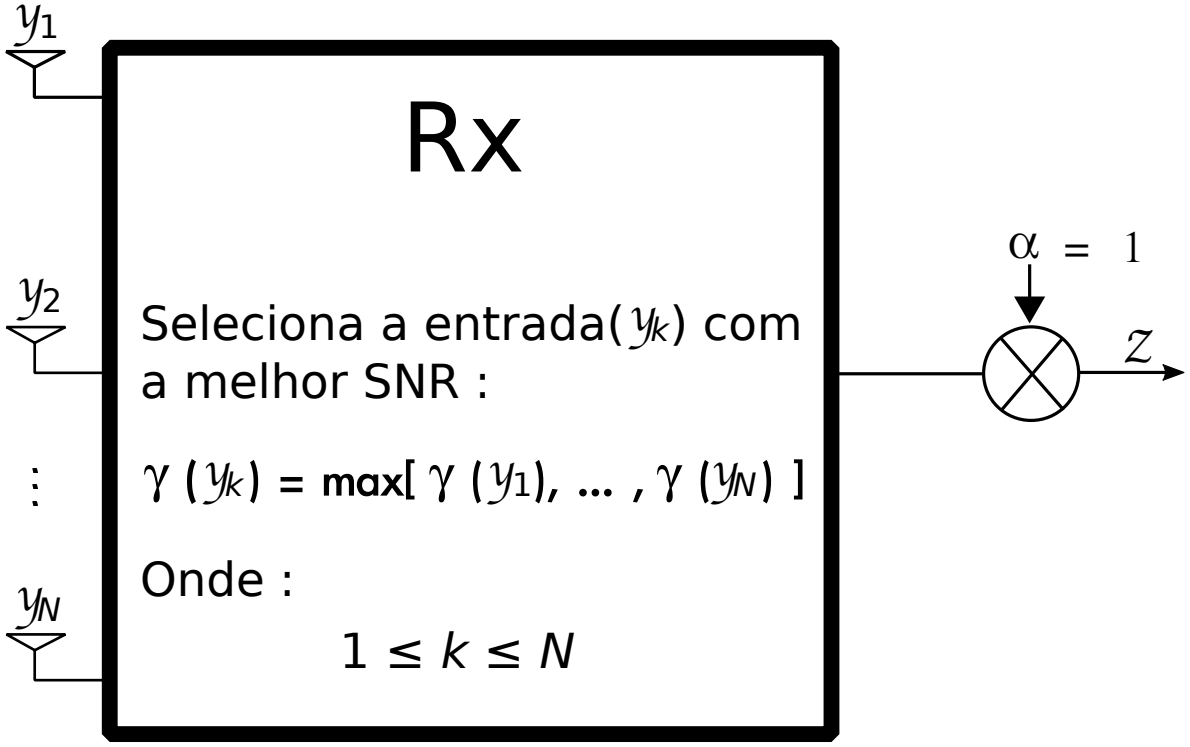
Supondo que a informação de estado do canal (CSI, do inglês, *channel state information*), i.e., o conjunto de coeficiente $(h_1, h_2, ..., h_N)$, seja conhecida no receptor. Então, antes de realizar a detecção do sinal, o receptor vai combinar linearmente os sinais recebidos $y_1, y_2, ..., y_N$ com os respectivos pesos $\alpha_1, \alpha_2, ..., \alpha_N$, como mostrado na figura acima, para obter o sinal:

$$z = \sum_{k=1}^{N} \alpha_k y_k \tag{2.255}$$

Os pesos serão determinados de acordo com a técnica de combinação empregada. Algumas dessas técnicas serão introduzidas à seguir.

2.4.3 Combinação por Seleção (SC) no Sistema SIMO

Figura 6 – Combinação por Seleção (SC)



Fonte: elaborado pelo autor (2017).

No esquema de combinação por seleção (SC, do inglês, *selection combining*) apenas o sinal recebido que tiver a maior SNR será utilizado para detecção. Neste caso, os pesos do combinador serão expressados por:

$$\alpha_k = \begin{cases} 1, & \gamma_k = \max\limits_{1 \le i \le N} \{\gamma_i\}, \\ 0, & \text{caso contrário.} \end{cases} \tag{2.256}$$

Onde $\gamma_k \equiv P|h_k|^2/\sigma_n^2$. O peso da antena onde há a maior SNR será igual à 1 e todos os outros pesos das outras antenas serão nulos. A SNR resultante na saída do combinador SC é:

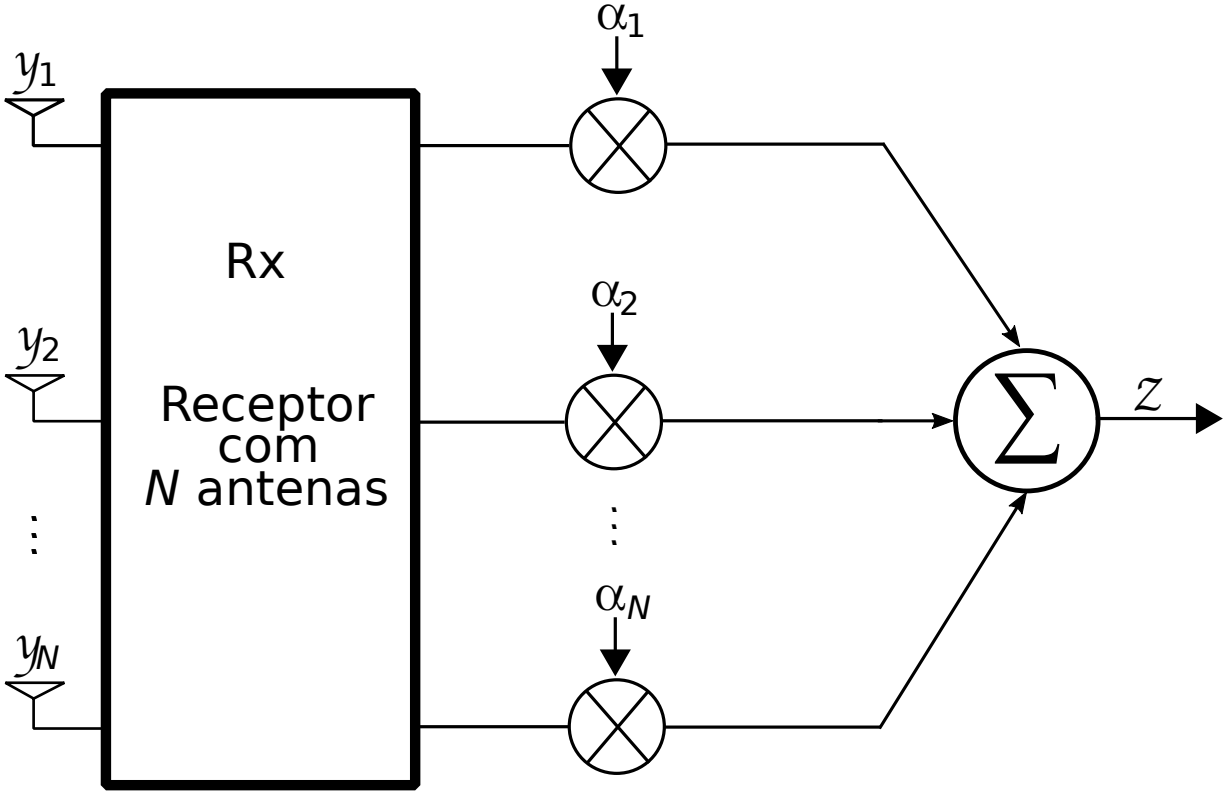
$$\gamma = \max_{1 \le i \le N} \{\gamma_i\} \tag{2.257}$$

E o sinal na saída do combinador SC é:

$$z = y_k = \sqrt{P}h_k x + n_k \tag{2.258}$$

2.4.4 Combinação por Razão Máxima (MRC) no Sistema SIMO

Figura 7 – Combinação por Razão Máxima (MRC)



Fonte: elaborado pelo autor (2017).

No esquema de combinação por razão máxima (MRC, do inglês, *maximal-ratio combining*) a diversidade espacial gerada pelas mútiplas antenas é completamente explorada ao se escolher os pesos que maximizam a SNR na saída do combinador. Mais especificamente, dada a CSI instantânea, os pesos do combinador MRC serão dados por:

$$\alpha_k = \frac{h_k^*}{||\mathbf{h}||}, \ \forall k : 1 \leq k \leq N \tag{2.259}$$

Onde k representa a k-ésima antena do receptor.

Em forma vetorial:

$$\alpha = \frac{\mathbf{h}^H}{||\mathbf{h}||} \tag{2.260}$$

Logo:

$$\alpha = \left(\frac{h_1^*}{||\mathbf{h}||}, \frac{h_2^*}{||\mathbf{h}||}, ..., \frac{h_N^*}{||\mathbf{h}||} \right) \tag{2.261}$$

Onde:

$$||\mathbf{h}|| = \sqrt{|h_1|^2 + |h_2|^2 + ... + |h_N|^2} \tag{2.262}$$

Lembrando que o sinal na entrada do receptor é:

$$\mathbf{y} = \sqrt{P}\mathbf{h}x + \mathbf{n} \tag{2.263}$$

Onde podemos escrever que:

$$\mathbf{y} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_N \end{pmatrix} \quad \mathbf{h} = \begin{pmatrix} h_1 \\ h_2 \\ \vdots \\ h_N \end{pmatrix} \quad \mathbf{n} = \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_N \end{pmatrix} \tag{2.264}$$

E que:

$$\sqrt{P}\mathbf{h}x = \begin{pmatrix} \sqrt{P}h_1x \\ \sqrt{P}h_2x \\ \vdots \\ \sqrt{P}h_Nx \end{pmatrix} \tag{2.265}$$

Como $\mathbf{y} = \sqrt{P}\mathbf{h}x + \mathbf{n}$:

$$\mathbf{y} = \begin{pmatrix} \sqrt{P}h_1x \\ \sqrt{P}h_2x \\ \vdots \\ \sqrt{P}h_Nx \end{pmatrix} + \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_N \end{pmatrix} \tag{2.266}$$

E a SNR na k-ésima antena do receptor é:

$$\gamma_k = \frac{P|h_k|^2}{\sigma_n^2} \ , \ \forall 1 \leq k \leq N \tag{2.267}$$

Assim, a saída do combinador MRC será:

$$
\begin{aligned}
z &= \alpha \mathbf{y} \\
&= \alpha \left(\sqrt{P}\mathbf{h}x + \mathbf{n} \right) \\
&= \sqrt{P}\alpha \mathbf{h}x + \alpha \mathbf{n} \\
&= \sqrt{P}\frac{\mathbf{h}^H}{||\mathbf{h}||}\mathbf{h}x + \frac{\mathbf{h}^H}{||\mathbf{h}||}\mathbf{n} \\
&= \sqrt{P}\frac{||\mathbf{h}||^2}{||\mathbf{h}||}x + \frac{\mathbf{h}_L}{||\mathbf{h}||}\mathbf{n} \\
&= \sqrt{P}||\mathbf{h}||x + \frac{\mathbf{h}^H}{||\mathbf{h}||}\mathbf{n}
\end{aligned}
\tag{2.268}
$$

Onde $\frac{\mathbf{h}^H}{||\mathbf{h}||}\mathbf{n}$ é um escalar:

$$
\begin{aligned}
\frac{\mathbf{h}^H}{||\mathbf{h}||}\mathbf{n} &= \left(\frac{h_1^*}{||\mathbf{h}||}, \frac{h_2^*}{||\mathbf{h}||}, ..., \frac{h_N^*}{||\mathbf{h}||} \right) \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_N \end{pmatrix} \\
&= \frac{h_1^* n_1}{||\mathbf{h}||} + \frac{h_2^* n_2}{||\mathbf{h}||} + ... + \frac{h_N^* n_N}{||\mathbf{h}||} \\
&= \frac{1}{||\mathbf{h}||}\left(h_1^* n_1 + h_2^* n_2 + ... + h_N^* n_N \right)
\end{aligned}
\tag{2.269}
$$

E a distribuição de $\frac{\mathbf{h}^H}{||\mathbf{h}||}\mathbf{n}$ é a mesma de um n_k qualquer(fato obtido através do **Lema 9**, da **Definição 13**, do **Lema 11** e do do **Lema 26**):

$$
\begin{aligned}
& n_k \sim \mathscr{CN}(0, \sigma_n^2) \ , \ \forall 1 \leq k \leq N \\
& \implies h_k^* n_k \sim \mathscr{CN}(0, |h_k|^2 \sigma_n^2) \\
& \implies (h_1^* n_1 + h_2^* n_2 + ... + h_N^* n_N) \sim \mathscr{CN}\left(0, \left(|h_1|^2 + |h_2|^2 + ... + |h_N|^2 \right) \sigma_n^2 \right) \\
& \implies (h_1^* n_1 + h_2^* n_2 + ... + h_N^* n_N) \sim \mathscr{CN}\left(0, ||\mathbf{h}||^2 \sigma_n^2 \right) \\
& \implies \frac{1}{||\mathbf{h}||}(h_1^* n_1 + h_2^* n_2 + ... + h_N^* n_N) \sim \mathscr{CN}\left(0, \frac{1}{||\mathbf{h}||^2}||\mathbf{h}||^2 \sigma_n^2 \right) \\
& \implies \frac{1}{||\mathbf{h}||}(h_1^* n_1 + h_2^* n_2 + ... + h_N^* n_N) \sim \mathscr{CN}\left(0, \sigma_n^2 \right) \\
& \implies \frac{\mathbf{h}^H}{||\mathbf{h}||}\mathbf{n} \sim \mathscr{CN}(0, \sigma_n^2)
\end{aligned}
\tag{2.270}
$$

Logo a potência de $\frac{\mathbf{h}^H}{||\mathbf{h}||}\mathbf{n}$ é:

$$\begin{aligned} \mathrm{E}\left[\left|\frac{\mathbf{h}^H}{||\mathbf{h}||}\mathbf{n}\right|^2\right] &= \mathrm{Var}\left(\frac{\mathbf{h}^H}{||\mathbf{h}||}\mathbf{n}\right) \\ &= \sigma_n^2 \end{aligned} \tag{2.271}$$

Como a saída do combinador é:

$$z = \sqrt{P}||\mathbf{h}||x + \frac{\mathbf{h}^H}{||\mathbf{h}||}\mathbf{n} \tag{2.272}$$

Então, a SNR na saída do combinador MRC é dada por:

$$\begin{aligned} \gamma_z = \mathrm{SNR}_z &= \frac{\textbf{Potência do sinal}}{\textbf{Potência do ruído}} \\ &= \frac{\mathrm{E}\left[\left|\sqrt{P}||\mathbf{h}||x\right|^2\right]}{\mathrm{E}\left[\left|\frac{\mathbf{h}^H}{||\mathbf{h}||}\mathbf{n}\right|^2\right]} \\ &= \frac{P||\mathbf{h}||^2\,\mathrm{E}\left[|x|^2\right]}{\mathrm{E}\left[\left|\frac{\mathbf{h}^H}{||\mathbf{h}||}\mathbf{n}\right|^2\right]} \\ &= \frac{P||\mathbf{h}||^2}{\sigma_n^2} \\ &= \frac{P\left(|h_1|^2 + |h_2|^2 + ... + |h_N|^2\right)}{\sigma_n^2} \\ &= \frac{P|h_1|^2}{\sigma_n^2} + \frac{P|h_2|^2}{\sigma_n^2} + ... + \frac{P|h_N|^2}{\sigma_n^2} \\ &= \gamma_1 + \gamma_2 + ... + \gamma_N \end{aligned} \tag{2.273}$$

Ou seja, a SNR maximizada na saída do combinador MRC é a soma das SNR's de entrada das N antenas do receptor.

Prova que $\alpha = \frac{\mathbf{h}^H}{||\mathbf{h}||}$:

Relembrando a desigualdade de *Cauchy-Schwarz* definida no **Lema 32**: Sejam dois vetores complexos $\mathbf{x} = \left(x_1, x_2, ..., x_n\right)^T$ e $\mathbf{y} = \left(y_1, y_2, ..., y_n\right)^T$, onde $\mathbf{x} \in \mathbb{C}^n$ e $\mathbf{y} \in \mathbb{C}^n$. A desigualdade de *Cauchy-Schwarz* é definida por:

$$|\langle \mathbf{x}, \mathbf{y} \rangle| \leq ||\mathbf{x}||\,||\mathbf{y}|| \tag{2.274}$$

Ou de forma equivalente:

$$|\langle \mathbf{x}, \mathbf{y} \rangle|^2 \leq \langle \mathbf{x}, \mathbf{x} \rangle \, \langle \mathbf{y}, \mathbf{y} \rangle \tag{2.275}$$

$$|\langle \mathbf{x}, \mathbf{y} \rangle|^2 \leq ||\mathbf{x}||^2 \, ||\mathbf{y}||^2 \tag{2.276}$$

$$|\mathbf{y}^H \mathbf{x}|^2 \leq ||\mathbf{x}||^2 \, ||\mathbf{y}||^2 \tag{2.277}$$

Que expandindo fica:

$$\left| \sum_{i=1}^{n} x_i {y_i}^* \right|^2 \leq \sum_{i=1}^{n} |x_i|^2 \times \sum_{i=1}^{n} |y_i|^2 \tag{2.278}$$

E a igualdade ocorrerá somente se para um $\lambda \in \mathbb{C}$ qualquer:

$$\mathbf{x} = \lambda \mathbf{y} \tag{2.279}$$

Agora, vamos considerar a saída do combinador MRC em função dos pesos genéricos α_k:

$$\begin{aligned} z &= \sum_{k=1}^{N} \alpha_k \left(\sqrt{P} h_k x + n_k \right) \\ &= \sqrt{P} \left(\sum_{k=1}^{N} \alpha_k h_k \right) x + \sum_{k=1}^{N} \alpha_k n_k \end{aligned} \tag{2.280}$$

Logo, a SNR de z será:

$$\begin{aligned} \gamma_z = \text{SNR} &= \frac{\textbf{Potência do sinal}}{\textbf{Potência do ruído}} \\ &= \frac{\mathrm{E}\left[\left| \sqrt{P} \left(\sum_{k=1}^{N} \alpha_k h_k \right) x \right|^2 \right]}{\mathrm{E}\left[\left| \sum_{k=1}^{N} \alpha_k n_k \right|^2 \right]} \\ &= \frac{P \left| \sum_{k=1}^{N} \alpha_k h_k \right|^2 \mathrm{E}\left[|x|^2 \right]}{\sum_{k=1}^{N} \left\{ |\alpha_k|^2 \mathrm{E}\left[|n_k|^2 \right] \right\}} \\ &= \frac{P \left| \sum_{k=1}^{N} \alpha_k h_k \right|^2}{\sum_{k=1}^{N} |\alpha_k|^2 \sigma_n^2} \\ &= \frac{P \left| \sum_{k=1}^{N} \alpha_k h_k \right|^2}{\sigma_n^2 \sum_{k=1}^{N} |\alpha_k|^2} \end{aligned} \tag{2.281}$$

Utilizando a desigualdade de *Cauchy-Schwarz*:

$$\left|\sum_{k=1}^{N} \alpha_k h_k\right|^2 \leq \sum_{k=1}^{N} |\alpha_k|^2 \times \sum_{k=1}^{N} |h_k|^2 \tag{2.282}$$

Assim:

$$\gamma_z = \frac{P\left|\sum_{k=1}^{N} \alpha_k h_k\right|^2}{\sigma_n^2 \sum_{k=1}^{N} |\alpha_k|^2} \leq \frac{P\sum_{k=1}^{N} |\alpha_k|^2 \times \sum_{k=1}^{N} |h_k|^2}{\sigma_n^2 \sum_{k=1}^{N} |\alpha_k|^2}$$

Na igualdade da inequação, teremos:

$$\begin{aligned}
\frac{P\left|\sum_{k=1}^{N} \alpha_k h_k\right|^2}{\sigma_n^2 \sum_{k=1}^{N} |\alpha_k|^2} &= \frac{P\sum_{k=1}^{N} |\alpha_k|^2 \times \sum_{k=1}^{N} |h_k|^2}{\sigma_n^2 \sum_{k=1}^{N} |\alpha_k|^2} \\
&= \frac{P\sum_{k=1}^{N} |h_k|^2}{\sigma_n^2} \\
&= \frac{P\left(|h_1|^2 + |h_2|^2 + ... + |h_N|^2\right)}{\sigma_n^2} \\
&= \frac{P|h_1|^2}{\sigma_n^2} + \frac{P|h_2|^2}{\sigma_n^2} + ... + \frac{P|h_N|^2}{\sigma_n^2} \\
&= \gamma_1 + \gamma_2 + ... + \gamma_N
\end{aligned}$$

Pela desigualdade de *Cauchy-Schwarz*, a igualdade da inequação ocorre para:

$$\alpha_k = ch_k^*, \ \forall k : 1 \leq k \leq N \tag{2.283}$$

Onde c é uma constante qualquer.

Vetorizando, podemos escrever:

$$\alpha = c\mathbf{h}^H \tag{2.284}$$

Vamos normalizar o vetor α para facilitar futuros cálculos:

$$||\alpha|| = 1 \iff \sqrt{\sum_{k=1}^{N} |\alpha_k|^2} = 1 \tag{2.285}$$

$$\iff \sqrt{\sum_{k=1}^{N} |ch_k^*|^2} = 1$$

$$\iff \sqrt{c^2 \sum_{k=1}^{N} |h_k^*|^2} = 1$$

$$\iff \left(\sqrt{c^2 \sum_{k=1}^{N} |h_k^*|^2}\right)^2 = 1^2$$

$$\iff c^2 \sum_{k=1}^{N} |h_k^*|^2 = 1$$

$$\iff c^2 ||\mathbf{h}||^2 = 1$$

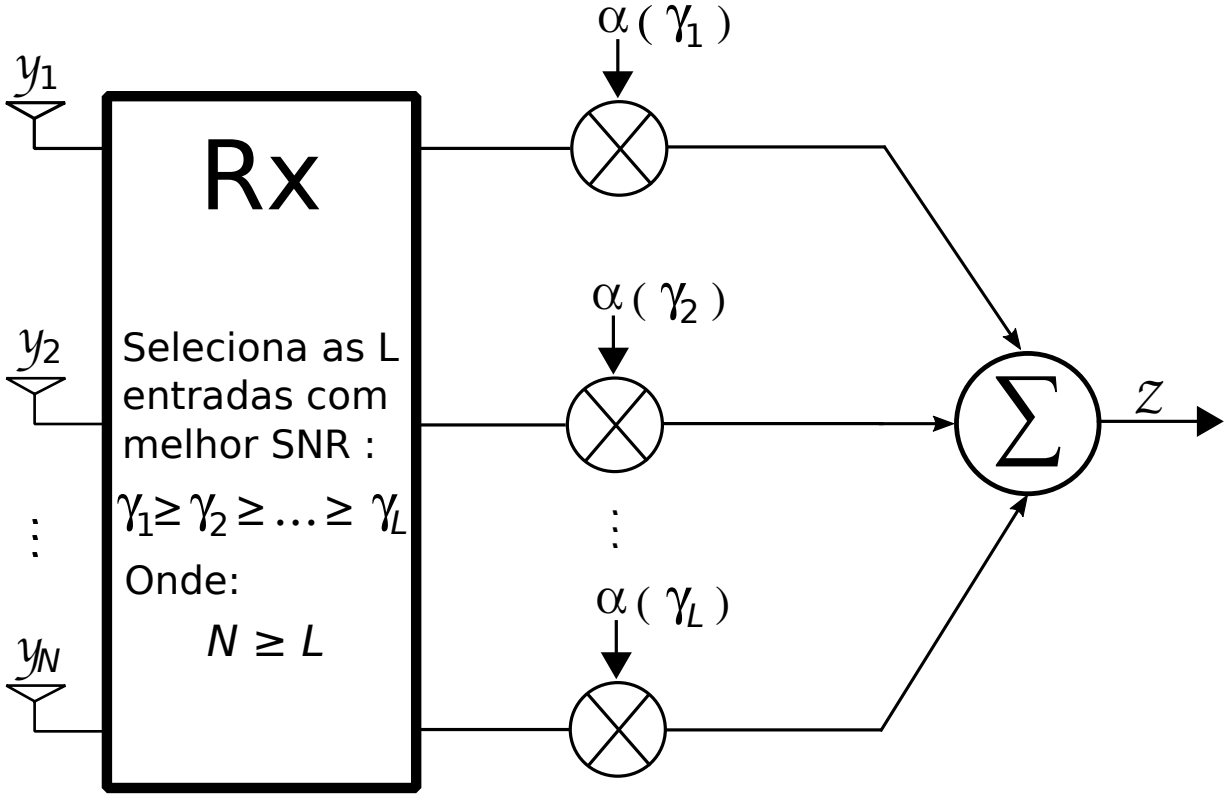
$$\iff c = \frac{1}{||\mathbf{h}||}$$

Logo:

$$\alpha = \frac{\mathbf{h}^H}{||\mathbf{h}||} \tag{2.286}$$

2.4.5 Combinação por Seleção Generalizada (GSC) no Sistema SIMO

Figura 8 – Combinação por Seleção Generalizada (GSC) no Sistema SIMO



Fonte: elaborado pelo autor (2017).

O esquema de combinação por seleção generalizada (GSC, do inglês, *generalized selection combining*) é uma generalização do esquema SC e MRC. No GSC apenas os L sinais com melhor SNR nas k antenas do receptor serão utilizados para detecção. Se $L = 1$ o caso GSC se torna o caso SC e se $L = N$ o caso GSC se torna o caso MRC. No esquema GSC, os pesos do combinador serão expressados da seguinte maneira (onde α_k é o peso na k-ésima antena do receptor):

Se a SNR de uma k-ésima antena $\text{SNR}_k = \gamma_k$ for uma das L maiores SNR's de todas as N SNR's onde $L \leq N$, então $\alpha_k = \frac{h_k^*}{||\mathbf{h}||}$, caso contrário $\alpha_k = 0$. Em linguagem matemática:

$$\alpha_k = \begin{cases} \frac{h_k^*}{||\mathbf{h}_L||}, & ,\exists\{\gamma_{v_1}, \gamma_{v_2}, .., \gamma_{v_{N-L}}\} \subseteq \{\gamma_1, \gamma_2, .., \gamma_N\} : \gamma_k \geq \max\{\gamma_{v_1}, \gamma_{v_2}, .., \gamma_{v_{N-L}}\}, \\ 0, & \text{caso contrário.} \end{cases} \tag{2.287}$$

A aplicação da regra acima seleciona os L maiores γ_k:

$$\{\gamma_{i_1}, \gamma_{i_2}, .., \gamma_{i_L}\} \subseteq \{\gamma_1, \gamma_2, .., \gamma_N\} \tag{2.288}$$

Onde:

$$\gamma_{i_1} \geq \gamma_{i_2} \geq ... \geq \gamma_{i_L} \tag{2.289}$$

Podemos definir:

$$\mathbf{h}_L = (h_{i_1}, h_{i_2}, ..., h_{i_L})^T \tag{2.290}$$

$$\alpha_{i_k} = \frac{h^*_{i_k}}{||\mathbf{h}_L||}\ , 1 \leq k \leq L \tag{2.291}$$

Em forma vetorial:

$$\alpha_L = \frac{\mathbf{h}^H_L}{||\mathbf{h}_L||} \tag{2.292}$$

Logo:

$$\alpha_L = \left(\frac{h^*_{i_1}}{||\mathbf{h}_L||}, \frac{h^*_{i_2}}{||\mathbf{h}_L||}, ..., \frac{h^*_{i_N}}{||\mathbf{h}_L||} \right) \tag{2.293}$$

Onde:

$$||\mathbf{h}_L|| = \sqrt{|h_{i_1}|^2 + |h_{i_2}|^2 + ... + |h_{i_N}|^2} \tag{2.294}$$

O sinal na entrada do receptor é:

$$\mathbf{y} = \sqrt{P}\mathbf{h}x + \mathbf{n} \tag{2.295}$$

Que após a seleção fica:

$$\mathbf{y}_L = \sqrt{P}\mathbf{h}_L x + \mathbf{n}_L \tag{2.296}$$

Assim, podemos escrever que:

$$\mathbf{y}_L = \begin{pmatrix} y_{i_1} \\ y_{i_2} \\ \vdots \\ y_{i_N} \end{pmatrix} \quad \mathbf{h}_L = \begin{pmatrix} h_{i_1} \\ h_{i_2} \\ \vdots \\ h_{i_N} \end{pmatrix} \quad \mathbf{n}_L = \begin{pmatrix} n_{i_1} \\ n_{i_2} \\ \vdots \\ n_{i_N} \end{pmatrix} \tag{2.297}$$

E que:

$$\sqrt{P}\mathbf{h}_L x = \begin{pmatrix} \sqrt{P}h_{i_1}x \\ \sqrt{P}h_{i_2}x \\ \vdots \\ \sqrt{P}h_{i_N}x \end{pmatrix} \tag{2.298}$$

Como $\mathbf{y}_L = \sqrt{P}\mathbf{h}_L x + \mathbf{n}_L$:

$$\mathbf{y}_L = \begin{pmatrix} \sqrt{P}h_{i_1}x \\ \sqrt{P}h_{i_2}x \\ \vdots \\ \sqrt{P}h_{i_N}x \end{pmatrix} + \begin{pmatrix} n_{i_1} \\ n_{i_2} \\ \vdots \\ n_{i_N} \end{pmatrix} \tag{2.299}$$

Onde a distribuição do ruído é:

$$n_{i_k} \sim \mathscr{CN}(0, \sigma_n^2) \ , \ \forall 1 \leq k \leq L \tag{2.300}$$

E cada uma das SNR's é:

$$\gamma_{i_k} = \frac{P|h_{i_k}|^2}{\sigma_n^2} \ , \ \forall 1 \leq k \leq L \tag{2.301}$$

Assim, o sinal na saída do combinador GSC será:

$$\begin{aligned} z &= \alpha_L \mathbf{y}_L \\ &= \alpha_L \left(\sqrt{P}\mathbf{h}_L x + \mathbf{n}_L \right) \\ &= \sqrt{P}\alpha_L \mathbf{h}_L x + \alpha_L \mathbf{n}_L \\ &= \sqrt{P}\frac{\mathbf{h}_L^H}{||\mathbf{h}_L||}\mathbf{h}_L x + \frac{\mathbf{h}_L^H}{||\mathbf{h}_L||}\mathbf{n}_L \\ &= \sqrt{P}\frac{||\mathbf{h}_L||^2}{||\mathbf{h}_L||}x + \frac{\mathbf{h}_L^H}{||\mathbf{h}_L||}\mathbf{n}_L \\ &= \sqrt{P}||\mathbf{h}_L||x + \frac{\mathbf{h}_L^H}{||\mathbf{h}_L||}\mathbf{n}_L \end{aligned} \tag{2.302}$$

Onde $\frac{\mathbf{h}_L^H}{||\mathbf{h}_L||}\mathbf{n}_L$ é um escalar dado por:

$$\begin{aligned}\frac{\mathbf{h}_L^H}{||\mathbf{h}_L||}\mathbf{n}_L &= \left(\frac{h_{i_1}^*}{||\mathbf{h}_L||}, \frac{h_{i_2}^*}{||\mathbf{h}_L||}, ..., \frac{h_{i_N}^*}{||\mathbf{h}_L||}\right) \begin{pmatrix} n_{i_1} \\ n_{i_2} \\ \vdots \\ n_{i_N} \end{pmatrix} \\ &= \frac{h_{i_1}^* n_{i_1}}{||\mathbf{h}_L||} + \frac{h_{i_2}^* n_{i_2}}{||\mathbf{h}_L||} + ... + \frac{h_{i_N}^* n_{i_N}}{||\mathbf{h}_L||} \\ &= \frac{1}{||\mathbf{h}_L||}\left(h_{i_1}^* n_{i_1} + h_{i_2}^* n_{i_2} + ... + h_{i_N}^* n_{i_N}\right)\end{aligned} \tag{2.303}$$

$\frac{\mathbf{h}_L^H}{||\mathbf{h}_L||}\mathbf{n}_L$ possui a mesma distribuição de um ruído n_{i_k} qualquer:

$$\begin{aligned}& n_{i_k} \sim \mathscr{CN}(0, \sigma_n^2)\ ,\ \forall 1 \leq k \leq L \\ &\implies h_{i_k}^* n_{i_k} \sim \mathscr{CN}(0, |h_{i_k}|^2 \sigma_n^2) \\ &\implies \left(h_{i_1}^* n_{i_1} + h_{i_2}^* n_{i_2} + ... + h_{i_N}^* n_{i_N}\right) \sim \mathscr{CN}\left(0, \left(|h_{i_1}|^2 + |h_{i_2}|^2 + ... + |h_{i_N}|^2\right)\sigma_n^2\right) \\ &\implies \left(h_{i_1}^* n_{i_1} + h_{i_2}^* n_{i_2} + ... + h_{i_N}^* n_{i_N}\right) \sim \mathscr{CN}\left(0, ||\mathbf{h}_L||^2 \sigma_n^2\right) \\ &\implies \frac{1}{||\mathbf{h}_L||}\left(h_{i_1}^* n_{i_1} + h_{i_2}^* n_{i_2} + ... + h_{i_N}^* n_{i_N}\right) \sim \mathscr{CN}\left(0, \frac{1}{||\mathbf{h}_L||^2}||\mathbf{h}_L||^2 \sigma_n^2\right) \\ &\implies \frac{1}{||\mathbf{h}_L||}\left(h_{i_1}^* n_{i_1} + h_{i_2}^* n_{i_2} + ... + h_{i_N}^* n_{i_N}\right) \sim \mathscr{CN}\left(0, \sigma_n^2\right) \\ &\implies \frac{\mathbf{h}_L^H}{||\mathbf{h}_L||}\mathbf{n}_L \sim \mathscr{CN}(0, \sigma_n^2)\end{aligned} \tag{2.304}$$

Logo, a potência de $\frac{\mathbf{h}_L^H}{||\mathbf{h}_L||}\mathbf{n}_L$ é:

$$\begin{aligned}\mathrm{E}\left[\left|\frac{\mathbf{h}_L^H}{||\mathbf{h}_L||}\mathbf{n}_L\right|^2\right] &= \mathrm{Var}\left(\frac{\mathbf{h}_L^H}{||\mathbf{h}_L||}\mathbf{n}_L\right) \\ &= \sigma_n^2\end{aligned} \tag{2.305}$$

Como o sinal na saída do combinador GSC é:

$$z = \sqrt{P}||\mathbf{h}_L||x + \frac{\mathbf{h}_L^H}{||\mathbf{h}_L||}\mathbf{n}_L \tag{2.306}$$

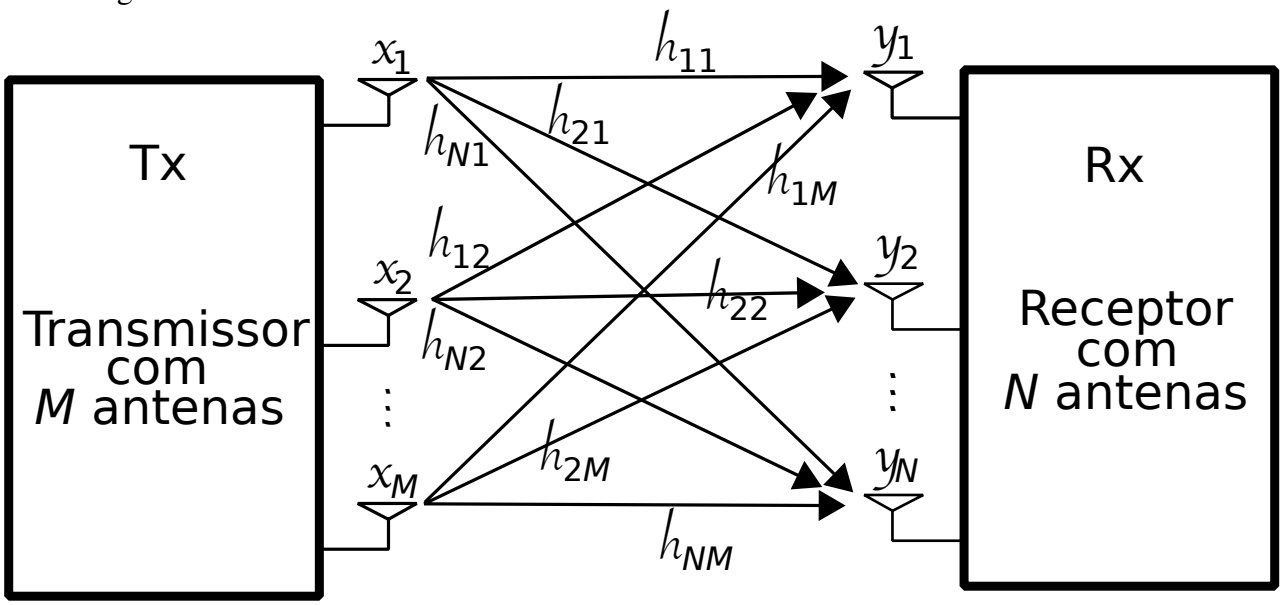
Assim, a SNR na saída do combinador GSC é:

$$\begin{aligned}
\gamma_z = \mathrm{SNR}_z &= \frac{\textbf{Potência do sinal}}{\textbf{Potência do ruído}} \\
&= \frac{\mathrm{E}\left[\left|\sqrt{P}||\mathbf{h}_L||x\right|^2\right]}{\mathrm{E}\left[\left|\frac{\mathbf{h}_L^H}{||\mathbf{h}_L||}\mathbf{n}_L\right|^2\right]} \\
&= \frac{P||\mathbf{h}_L||^2\,\mathrm{E}\left[|x|^2\right]}{\mathrm{E}\left[\left|\frac{\mathbf{h}_L^H}{||\mathbf{h}_L||}\mathbf{n}_L\right|^2\right]} \\
&= \frac{P||\mathbf{h}_L||^2}{\sigma_n^2} \\
&= \frac{P\left(|h_{i_1}|^2 + |h_{i_2}|^2 + \ldots + |h_{i_N}|^2\right)}{\sigma_n^2} \\
&= \frac{P|h_{i_1}|^2}{\sigma_n^2} + \frac{P|h_{i_2}|^2}{\sigma_n^2} + \ldots + \frac{P|h_{i_N}|^2}{\sigma_n^2} \\
&= \gamma_{i_1} + \gamma_{i_2} + \ldots + \gamma_{i_N}
\end{aligned} \tag{2.307}$$

Que é a soma nas L maiores SNR's selecionas.

2.5 Modelo do sistema MIMO

Figura 9 – Sistema MIMO MxN.



Fonte: elaborado pelo autor (2017).

A representação de um canal MIMO (MIMO, do inglês, *Multiple-Input Multiple-Output*) com M antenas no transmissor e N antenas no receptor (sistema MxN), onde se geram MN subcanais entre o transmissor e o receptor, é ilustrada na figura acima.

Na Figura **??**, cada um dos coeficientes h_{ik} representa um canal de desvanecimento *Rayleigh* puro, plano e lento entre a antena transmissora k, com $k \in \{1,\ldots,M\}$, e a antena receptora i, com $i \in \{1,\ldots,N\}$. Os $h_{ik} \sim \mathscr{CN}(0,1)$ são i.i.d., onde a distribuição e caracterização dessa variáveis estão na sessão **2.2**.

O sinal que chega no receptor expresso em forma vetorial é:

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n} \tag{2.308}$$

Onde $\mathbf{y}$ é o vetor dos sinais quem chegam no receptor, $\mathbf{H}$ é a matriz que representa o desvanecimento entre todas as antenas do transmissor e do receptor, $\mathbf{x}$ representa o vetor dos sinais enviados nas antena do transmissor e $\mathbf{n}$ o vetor que representa o ruído AWGN nas antena

do receptor :

$$\mathbf{y} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_N \end{pmatrix} \quad \mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_M \end{pmatrix} \quad \mathbf{H} = \begin{pmatrix} h_{11} & h_{12} & ... & h_{1M} \\ h_{21} & h_{22} & ... & h_{2M} \\ . & . & . & . \\ . & . & . & . \\ h_{N1} & h_{N2} & ... & h_{NM} \end{pmatrix} \quad \mathbf{n} = \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_N \end{pmatrix} \tag{2.309}$$

Logo:

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_N \end{pmatrix} = \begin{pmatrix} h_{11} & h_{12} & ... & h_{1M} \\ h_{21} & h_{22} & ... & h_{2M} \\ . & . & . & . \\ . & . & . & . \\ h_{N1} & h_{N2} & ... & h_{NM} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_M \end{pmatrix} + \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_N \end{pmatrix} \tag{2.310}$$

Consequentemente:

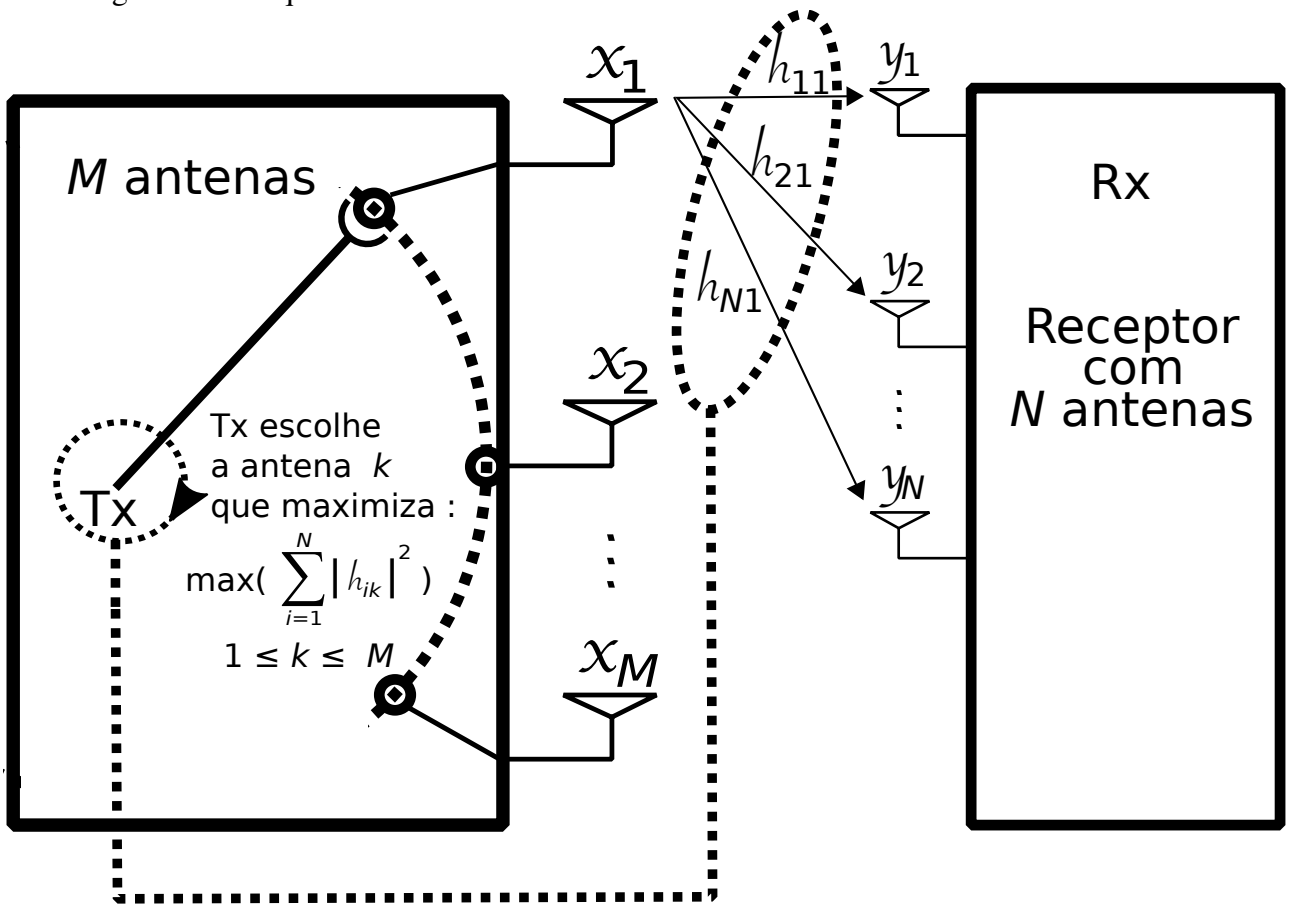
$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_N \end{pmatrix} = \begin{pmatrix} h_{11}x_1 + h_{12}x_2 + ... + h_{1M}x_M \\ h_{21}x_1 + h_{22}x_2 + ... + h_{2M}x_M \\ \vdots \\ h_{N1}x_1 + h_{N2}x_2 + ... + h_{NM}x_M \end{pmatrix} + \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_N \end{pmatrix} \tag{2.311}$$

Assim, cada um dos y_i sinais recebidos em cada uma das N antenas do receptor podem ser descritos matematicamente por:

$$y_i = \sum_{k=1}^{M} h_{ik}x_k + n_i \ \ , \forall i \in \{1, \ldots, N\}. \tag{2.312}$$

2.5.1 Esquema TAS no sistema MIMO

Figura 10 – Esquema TAS



Fonte: elaborado pelo autor (2017).

Outra técnica para explorar a diversidade espacial é Técnica de Seleção de Antena Transmissora (TAS, do inglês, *Transmit Antenna Selection*). Neste caso a diversidade espacial é explorada na transmissão.

O transmissor seleciona uma de suas M antenas, a antena s, para transmitir. A escolha se baseia na seguinte regra que descreve a antena s do transmissor que possui o melhor canal com o receptor:

$$s = \arg \max_{1 \leq k \leq M} \left(\sum_{i=1}^{N} |h_{ik}|^2 \right) \tag{2.313}$$

Note que escolher a antena transmissora que maximiza $\sum_{i=1}^{N} |h_{ik}|^2$ equivale a maximizar a soma das SNR's das antenas do receptor, pois:

$$\max_{1\leq k\leq M}\left(\sum_{i=1}^{N}|h_{ik}|^2\right) \iff \max_{1\leq k\leq M}\left(\sum_{i=1}^{N}P|h_{ik}|^2/\sigma_n^2\right) \tag{2.314}$$

O sistema MIMO/TAS é equivalente ao sistema SIMO, para observar isso basta usar a seguinte notação:

$$\mathbf{y} = \mathbf{h}_s\mathbf{x} + \mathbf{n} \tag{2.315}$$

Onde $\mathbf{h}_s$ é a k-ésima coluna de $\mathbf{H}$:

$$\mathbf{h}_s = \begin{pmatrix} h_{1k} \\ h_{2k} \\ \vdots \\ h_{Nk} \end{pmatrix} \tag{2.316}$$

E assim, toda análise que for feita para o sistema SIMO vale para o sistema MIMO com TAS. Incluindo a análise dos esquema SC, MRC e GSC e qualquer outra análise de performance.

2.6 Capacidade de Canais sem Fio

Nesta sessão, vamos apresentar os limites fundamentais do canal sem fio em termos da Capacidade de Shannon (SHANNON, 1948), i.e., a taxa máxima alcançável entre o transmissor e o receptor. A capacidade de canal é normalmente utilizada para caracterizar as limitações do canal de comunicação. Em geral, para um canal com entrada X e saída Y, a capacidade porde ser expressa por (7.1) de (THOMAS; COVER, 2006):

$$C = \max_{p(x)}\Big(I(X;Y)\Big) \tag{2.317}$$

onde $I(X;Y) \equiv \mathrm{E}\left[\log_2\left(\frac{p(x,y)}{p(x)p(y)}\right)\right]$ é a informação mútua entre X e Y. Através desta expressão pode-se ver a capacidade como a quantidade máxima de informações que a saída do canal pode fornecer sobre a mensagem de entrada, quando otimizada para todas as possíveis distribuições da entrada $p(x)$.

2.7 Capacidade do Canal SISO/AWGN/ *Rayleigh*

Considerando o canal com desvanecimento *Rayleigh* plano e lento e com o ruído AWGN em um sistema SISO já analisado na sessão **2.3**, a relação entre a entrada x e a saída y do canal é:

$$y = \sqrt{P}hx + n \tag{2.318}$$

A capacidade do canal, demonstrada em(TSE; VISWANATH, 2004), será:

$$\begin{aligned} C &= \max_{p(x)} \left(I(x;y) \right) \\ &= \max_{p(x)} \left(\mathrm{E}\left[\log_2 \left(\frac{p(x,y)}{p(x)p(y)} \right) \right] \right) \\ &= \log_2 \left(1 + \mathrm{SNR}_{\text{receptor}} \right) \\ &= \log_2 \left(1 + \frac{P|h|^2}{\sigma_n^2} \right) \end{aligned} \tag{2.319}$$

2.7.1 Probabilidade de Interrupção

Interrupção é um evento que impossibilita a decodificação confiável da mensagem no receptor. Dada uma taxa de trasmissão R, podemos dizer que uma interrupção ocorre se a capacidade do canal for menor que a taxa de transmissão, i.e., $C < R$. Logo, a probabilidade de interrupção será:

$$\begin{aligned} p_{\text{out}}(R) &= \Pr(C < R) \\ &= \Pr\left(\log_2 \left(1 + \mathrm{SNR}_{\text{receptor}} \right) < R \right) \\ &= \Pr\left(\log_2 \left(1 + \frac{P|h|^2}{\sigma_n^2} \right) < R \right) \end{aligned} \tag{2.320}$$

2.8 Capacidade do Canal SIMO/AWGN/*Rayleigh*

Considerando o canal com desvanecimento *Rayleigh* plano e lento e com o ruído AWGN em um sistema SIMO já analisado na sessão **2.4**, a relação entre a entrada x e o vetor de

sinais que chegam nas antenas do receptor **y** é:

$$\mathbf{y} = \sqrt{P}\mathbf{h}x + \mathbf{n} \tag{2.321}$$

Seja $z =$ a saída do combinador do receptor.

A capacidade do canal, demonstrada em (TSE; VISWANATH, 2004), será:

$$\begin{aligned} C &= \max_{p(x)} \left(I(x;z) \right) \\ &= \max_{p(x)} \left(\mathrm{E}\left[\log_2 \left(\frac{p(x,z)}{p(x)p(z)} \right) \right] \right) \\ &= \log_2 (1 + \mathrm{SNR}_z) \end{aligned} \tag{2.322}$$

A expressão para SNR_z vai depender da técnica de combinação utilizada no receptor. Para o caso SC a expressão para SNR_z está em (2.257), pro caso MRC a expressão está em (2.273) e para o caso GSC em (2.307).

Lembrando que toda essa análise para o caso SIMO vale para o caso MIMO/TAS descrito na sessão (2.5.1).

2.8.1 Probabilidade de Interrupção

Dada uma taxa de trasmissão R, podemos dizer que uma interrupção ocorre se a capacidade do canal for menor que a taxa de transmissão, i.e., $C < R$. Logo, a probabilidade de interrupção será:

$$\begin{aligned} p_{\mathrm{out}}(R) &= \Pr(C < R) \\ &= \Pr\left(\log_2 (1 + \mathrm{SNR}_z) < R \right) \end{aligned} \tag{2.323}$$

2.9 Ganho de diversidade e Ganho de *Array*

O ganho de diversidade é a melhoria na confiabilidade de ligação obtida ao se receber múltiplas réplicas do sinal de informação através de diferentes links independentes de desvanecimento. Quanto maior o número de cópias independentes, maior será a probabilidade de que pelo menos um dos dos sinais não esteja em desvanecimento profundo, e consequentemente melhorando a qualidade e a confiabilidade da recepção.

O ganho de *array* denota a melhoria da SNR recebida que resulta do efeito da combinação coerente dos sinais de informação. A combinação coerente pode ser realizada através de processamento espacial no *array* de antenas receptoras e/ou pré-processamento espacial no *array* de antenas transmissoras.

O ganho de diversidade e o ganho de *array* podem ser obtidos do ponto de vista da probabilidade de erro. Por exemplo, em (ZHENG; TSE, 2003) o ganho de diversidade é obtido a partir de

$$d = -\lim_{\mathrm{SNR}\to\infty} \frac{\log p_e(\mathrm{SNR})}{log(\mathrm{SNR})} \tag{2.324}$$

$$\lim_{\mathrm{SNR}\to\infty} p_e(\mathrm{SNR}) \simeq a \times \mathrm{SNR}^{-d} \tag{2.325}$$

Onde SNR é a SNR média do receptor, que neste trabalho é $\mathrm{SNR} = \frac{P}{\sigma_n^2}$. p_e denota a probabilidade de erro, d representa o ganho de diversidade e a representa o ganho de *array*. Perceba que a probabilidade de erro cai com SNR^{-d}, enquanto em um sistema SISO cai com SNR^{-1}. Igualmente, o ganho de diversidade corresponde ao número de percursos independentes que um símbolo pode percorrer, isto é, o número de subcanais que podem detectar o símbolo. Consequentemente, idealmente, a ordem de diversidade de um sistema MIMO MxN é MN, e o ganho de diversidade vai estar limitado pela ordem de diversidade oferecida pelo canal. Logo, $d_{max} = MN$.

2.10 Segurança na camada física.

A natureza *broadcast* do meio sem fio, com um canal de comunicações compartilhado, torna estes sistemas vulneráveis à intervenção de nós maliciosos(espiões) não autorizados na rede. Devido a este fato, um problema inerente das comunicações sem fio é alcançar e conservar o sigilo na informação transmitida. Tradicionalmente, as estratégias para a introdução de segurança nos sistemas de comunicações eram realizadas através da criptografia da informação, utilizando protocolos de criptografia nas camadas superiores da pilha de protocolos (SILVA *et al.*, 2008). Com o desenvolvimento tecnológico, a capacidade de processamento dos nós espiões tem crescido exponencialmente, aumentando a probabilidade de obter a chave de criptografia através da exploração das múltiplas combinações possíveis. Portanto, preservar o sigilo da informação baseado unicamente na estratégia da criptografia tem resultado em sistemas cada vez mais complexos para neutralizar a capacidade dos nós maliciosos(ou espiões) e não se tornarem obsoletos.

Em anos recentes, surgiu como solução ou auxílio, a possibilidade da garantia do sigilo da informação na camada física. Baseadas na premissa introduzida por Wyner em (WYNER, 1975), onde foi apresentado o conceito de canais espionados (*wiretap channel*, em inglês), demostrando que é possível obter um nível aceitável de sigilo na informação transmitida quando o canal de comunicação entre o Tx e o nó malicioso é uma versão degradada do canal entre o Tx e o Rx legítimo. As estratégias de segurança na camada física têm demonstrado a sua eficácia em garantir o sigilo na informação e podem ser implementadas em um sistema em solitário, ou como complemento das técnicas de criptografia acima mencionadas. Aproveitando que a criptografia é realizada em camadas superiores independentes da camada física, ambas as estratégias podem funcionar simultaneamente, surgindo sistemas com uma abordagem multicamadas em termos de segurança.

Basicamente, as estratégias de segurança na camada física podem ser focadas na utilização de códigos, ou em técnicas que aproveitam as características do canal sem fio, explorando as variações espaciais e temporais do canal. As técnicas que baseiam-se na codificação tem a desvantagem de diminuir a eficiência espectral do sistema, uma das questões mais críticas na atualidade. No entanto, as técnicas que aproveitam o canal, além de não provocarem diminuição da eficiência espectral, têm demostrado serem eficazes em cenários dinâmicos. A implementação deste tipo de técnica, em conjunto com a consolidação dos sistemas MIMO e a exploração das características físicas do canal, tornam esta parceria uma solução muito interessante nas novas

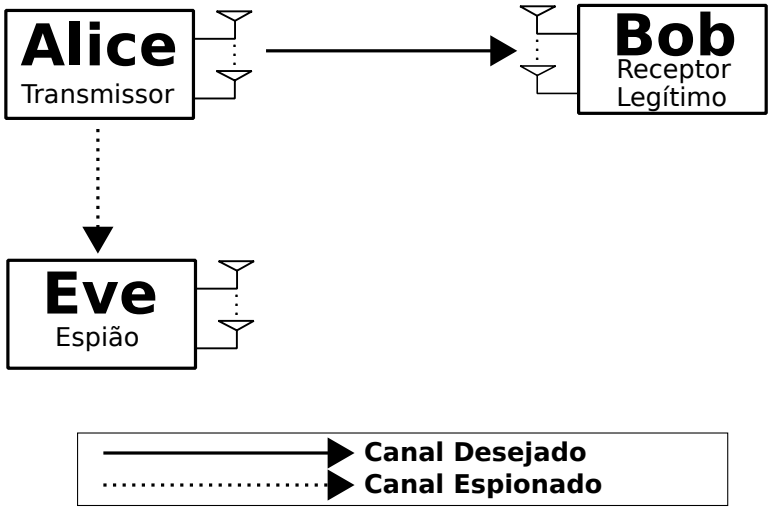
gerações de comunicações sem fio, atingindo altas taxas de transferências, ao mesmo tempo que fornecem níveis apropriados de segurança.

2.10.1 Cenários Wiretap

2.10.1.1 Cenário Wiretap Geral

No cenário de espionagem(ou *wiretap*) geral, Alice é o Tx e Bob é o Rx legítimo que estão se comunicando enquanto o nó espião(ou malicioso) tenta escutar(ou espionar) a mensagem transmitida por Alice. Esse cenário está representado na figura abaixo:

Figura 11 – Cenário *Wiretap* Geral



Fonte: elaborado pelo autor (2017).

2.10.1.2 Cenário Wiretap com Interferência Cooperativa

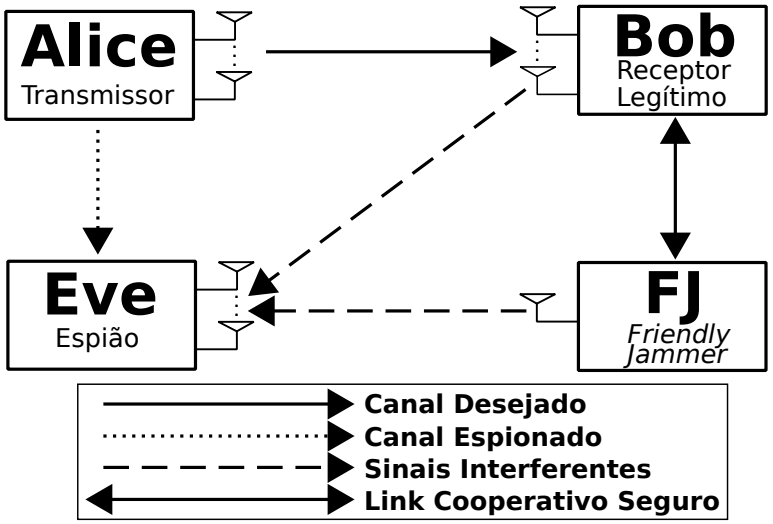
As estratégias para alcançar e preservar o sigilo da informação na camada física são variadas. Um dos métodos mais estudados é a interferência cooperativa, que consiste no envio de sinais de interferência para o nó malicioso(ou espião). Para o envio dos sinais interferentes podem ser utilizados unicamente nós passivos presentes na rede (HUANG; SWINDLEHURST, 2011), conhecidos como nós amigos, ou o caso onde tanto o Rx legítimo quanto um nó interferente amigo enviam sinais de interferência para o nó intruso (TEKIN; YENER, 2008; HAN *et al.*, 2009). Para uma maior eficiência e segurança deste método, é importante garantir uma cooperação completa e segura entre os nós amigos e o Rx legítimo.

A técnica de interferência cooperativa baseia-se na transmissão de ruído artificial

especialmente concebido para que resida perfeitamente no espaço nulo do Rx no canal principal, a fim de afetar o nó intruso e não interferir com o Rx legítimo (DING *et al.*, 2016).

O cenário espionagem(ou *wiretap*) com interferência cooperativa está representado na figura abaixo.

Figura 12 – Cenário *Wiretap* com Sinais Interferentes



Fonte: elaborado pelo autor (2017).

À seguir vamos apresentas alguma métricas de desempenho sigilo.

2.10.2 Capacidade de Sigilo

Utilizando a expressão de capacidade de canal apresentada na sessão(2.8), podemos definir que:

A capacidade do canal principal entre Alice e Bob é $R_{\text{Bob}} = \log_2(1+\gamma_{\text{Bob}})$. Onde γ_{Bob} é a SNR na saída de Bob.

E que, a capacidade do canal *wiretap*, entre Alice e Eve é $R_{\text{Eve}} = \log_2(1+\Upsilon_{\text{Eve}})$ no cenário com interferência cooperativa ou $R_{\text{Eve}} = \log_2(1+\gamma_{\text{Eve}})$ no cenário sem interferência cooperativa. Onde γ_{Eve} é a SNR na saída de Eve e Υ_{Eve} é a SINR na saída de Eve.

SINR é a medida análoga à SNR quando há interferência e é definida por:

$$\text{SINR} = \Upsilon = \frac{\textbf{Potência do sinal}}{\textbf{Potência do ruído} + \textbf{Potência dos sinais interferentes}} \tag{2.326}$$

Logo, a capacidade de sigilo é definida por:

No cenário com interferência cooperativa:

$$R_S = \begin{cases} R_{\text{Bob}} - R_{\text{Eve}}, & \gamma_{\text{Bob}} > \Upsilon_{\text{Eve}}, \\ 0, & \gamma_{\text{Bob}} \leq \Upsilon_{\text{Eve}}. \end{cases} \tag{2.327}$$

No cenário sem interferência cooperativa:

$$R_S = \begin{cases} R_{\text{Bob}} - R_{\text{Eve}}, & \gamma_{\text{Bob}} > \gamma_{\text{Eve}}, \\ 0, & \gamma_{\text{Bob}} \leq \gamma_{\text{Eve}}. \end{cases} \tag{2.328}$$

2.10.3 Probabilidade de Interrupção de Sigilo

De maneira análoga à definição da probabilidade de interrupção apresentada na sessão(2.8.1), a probabilidade de interrupção de sigilo para uma taxa de transmissão R é definida por:

$$P_s(R) = \Pr(R_S < R) \tag{2.329}$$

2.10.4 Probabilidade de Interrupção de Sigilo Assintótica

A probabilidade de interrupção de sigilo assintótica $P_s^{\infty}(R)$ é definida por:

$$P_s^{\infty}(R) = \lim_{\text{SNR}\to\infty} P_s(R) \tag{2.330}$$

Como $P_s(R)$ é uma probabilidade de erro, podemos utilizar as definições de ganho de *array* e de ganho de diversidade apresentadas na sessão(2.9), para concluir que :

$$P_s^{\infty}(R) = G_{\text{A}} \left(\text{SNR}\right)^{-G_{\text{D}}} + o\left(\text{SNR}^{-G_{\text{D}}}\right) \tag{2.331}$$

Onde SNR é a SNR média de Bob, G_{A} é o ganho de array, G_{D} é o ganho de diversidade e $o\left(\text{SNR}^{-G_{\text{D}}}\right)$ são termos que podem sem ignorados. Logo:

$$P_s^{\infty}(R) \simeq G_{\text{A}} \left(\text{SNR}\right)^{-G_{\text{D}}} \tag{2.332}$$

2.10.5 Taxa de Sigilo Não Nula

A taxa de sigilo não nula $P_r(R_S > 0)$ é definida como a probabilidade de $R_S > 0$. Representando a probabilidade da capacidade de sigilo ser diferente de zero, ou seja, do canal entre Alice e Bob ser melhor que o canal entre Alice e Eve garantindo assim o sigilo da comunicação. Logo, da definição de R_S, podemos definir $P_r(R_S > 0)$ como :

No cenário com interferência cooperativa:

$$\begin{aligned} P_r(R_S > 0) &= \Pr(R_{\text{Bob}} > R_{\text{Eve}}) \\ &= \Pr(\gamma_{\text{Bob}} > \Upsilon_{\text{Eve}}) \end{aligned} \tag{2.333}$$

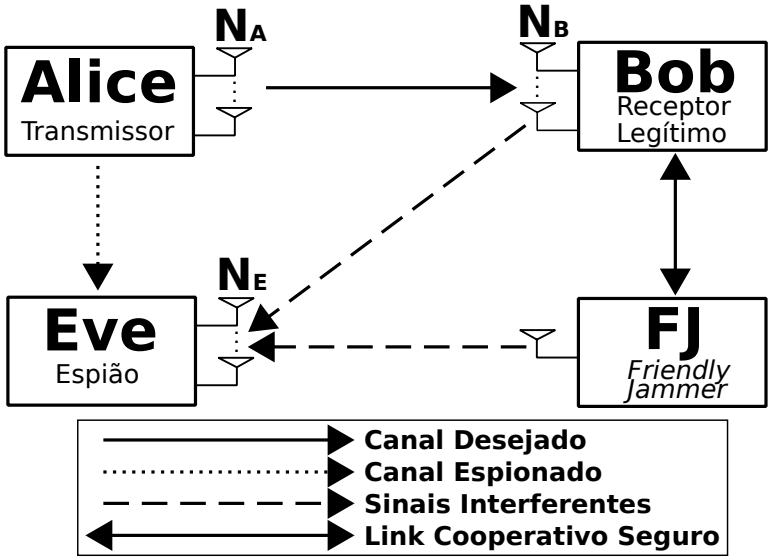
No cenário sem interferência cooperativa:

$$\begin{aligned} P_r(R_S > 0) &= \Pr(R_{\text{Bob}} > R_{\text{Eve}}) \\ &= \Pr(\gamma_{\text{Bob}} > \gamma_{\text{Eve}}) \end{aligned} \tag{2.334}$$

3 SISTEMA *WIRETAP*/MIMO COM TAS, GSC E SINAIS INTERFERENTES

3.1 Modelo do Sistema

Figura 13 – Modelo do Sistema



Fonte: elaborado pelo autor (2017).

O sistema deste trabalho é um canal MIMO/*wiretap* composto de um Tx, chamado de Alice, um Rx, chamado de Bob, e um nó espião, chamado de Eve, que estão equipados por N_A, N_B e N_E antenas, respectivamente.

O esquema TAS é empregado em Alice, o esquema GSC é adotado em Bob, e Eve utiliza a técnica MRC.

Alice envia dados para Bob enquanto Eve tenta escutar a troca de informações.

Se assume que Eve é acometida simultaneamente por AWGN e sinais interferentes.

Como em (COSTA *et al.*, 2016), assumimos que um Interferente Amigável(ou *Friendly Jammer*) possui cooperação total e segura com Bob e causa interferência em Eve.

O canal legítimo entre Alice e Bob e o canal *wiretap* são considerados independentes e experimentam desvanecimento *Rayleigh* Puro, Plano e Lento.

Empregando o esquema TAS, Alice utiliza a CSI de Bob para maximizar a SNR recebida em Bob. Eve é um nó espião passivo

Além disso, assumimos que Bob possui cooperação total com FJ. Assim, Bob é capaz de cancelar completamente qualquer sinal interferente que venha do FJ ou dele mesmo.

3.1.1 TAS no Transmissor e GSC no Receptor Legítimo

Alice seleciona a antena transmissora com o objetivo de maximizar a SNR recebida em Bob, onde Bob emprega o esquema GSC (YANG *et al.*, 2013c) de forma que as L_{B} antenas mais fortes do total de N_{B} antenas sejam combinadas. Baseando-se nas regras do GSC, considere que $\left|h^{1}{}_{\mathrm{AB},k}\right|^2 \geq \left|h^{2}{}_{\mathrm{AB},k}\right|^2 \geq ... \geq \left|h^{N_{\mathrm{B}}}{}_{\mathrm{AB},k}\right|^2$ sejam as estatísticas ordenadas ao se arranjar $\left\{\left|h^{l_{\mathrm{B}}}{}_{\mathrm{AB},k}\right|\right\}_{l_B=1}^{N_{\mathrm{B}}}$ em ordem decrescente de magnitude. Neste caso, denotamos $\mathbf{h}_{\mathrm{AB},k} = [h^1_{\mathrm{AB},k}, h^2_{\mathrm{AB},k}, ..., h^{N_{\mathrm{B}}}_{\mathrm{AB},k}]^T$ como o vetor de canal, de dimensão $N_{\mathrm{B}} \times 1$, entre Bob e a k-ésima antena de Alice, com $(.)^T$ representando a operação de transposição. Combinando as primeiras L_{B} $(1 \leq L_{\mathrm{B}} \leq N_{\mathrm{B}})$ variáveis em estatísticas ordenadas, Alice obtém $\theta_k = \sum_{l_{\mathrm{B}}=1}^{L_{\mathrm{B}}} \left|h^{l_{\mathrm{B}}}{}_{\mathrm{AB},k}\right|^2$. Logo, a antena de transmissão s selecionada por Alice através da técnica TAS é escolhida de acordo com $s = \arg \max_{k \in \{1,...,N_{\mathrm{A}}\}} (\theta_k)$.

Como Bob cancela totalmente os sinais interferentes, o sinal recebido em Bob quando Alice seleciona a antena s para transmitir o sinal x é:

$$\mathbf{y}_{\mathrm{B}} = \sqrt{P}\mathbf{h}_{\mathrm{AB},s}x + \mathbf{n}_{\mathrm{B}}, \tag{3.1}$$

onde P é a potência de transmissão em Alice, $\mathbf{n}_{\mathrm{B}}$ é o vetor do canal AWGN de dimensão $N_{\mathrm{B}} \times 1$, ${\sigma_{\mathrm{B}}}^2$ é a variância de cada componente de ruído pertencente ao vetor do canal AWGN que chega em Bob e $\mathbf{h}_{\mathrm{AB},s}$ denota o vetor de canal, de dimensão $N_{\mathrm{B}} \times 1$, da antena seleciona em Alice até Bob.

Utilizando os resultados da seção(2.4.5), teremos que o sinal y_{B} na saída do combinador GSC de Bob é:

$$y_{\mathrm{B}} = \frac{\left(\left(\mathbf{h}_{\mathrm{AB},s}\right)_L\right)^H}{||\left(\mathbf{h}_{\mathrm{AB},s}\right)_L||}\mathbf{y}_{\mathrm{B}} \tag{3.2}$$

Onde $\left(\mathbf{h}_{\mathrm{AB},s}\right)_L$ é o vetor formado pelos primeiros L $h^k_{\mathrm{AB},s}$ que satisfazem $\left|h^{1}{}_{\mathrm{AB},s}\right|^2 \geq \left|h^{2}{}_{\mathrm{AB},s}\right|^2 \geq ... \geq \left|h^{L_{\mathrm{B}}}{}_{\mathrm{AB},s}\right|^2 \geq ... \geq \left|h^{N_{\mathrm{B}}}{}_{\mathrm{AB},s}\right|^2$, logo é definido por:

$$\begin{aligned} &\left(\mathbf{h}_{\mathrm{AB},s}\right)_L \\ &= \left(h^1_{\mathrm{AB},s}, h^2_{\mathrm{AB},s}, ..., h^{L_{\mathrm{B}}}_{\mathrm{AB},s}\right)^T \end{aligned} \tag{3.3}$$

E onde $\frac{\left(\left(\mathbf{h}_{\mathrm{AB},s}\right)_L\right)^H}{||\left(\mathbf{h}_{\mathrm{AB},s}\right)_L||}$ é definido por:

$$\frac{\left(\left(\mathbf{h}_{\mathrm{AB},s}\right)_L\right)^H}{||\left(\mathbf{h}_{\mathrm{AB},s}\right)_L||} = \left(\frac{\left(h^1_{\mathrm{AB},s}\right)^*}{||\left(\mathbf{h}_{\mathrm{AB},s}\right)_L||}, \frac{\left(h^2_{\mathrm{AB},s}\right)^*}{||\left(\mathbf{h}_{\mathrm{AB},s}\right)_L||}, ..., \frac{\left(h^{L_\mathrm{B}}_{\mathrm{AB},s}\right)^*}{||\left(\mathbf{h}_{\mathrm{AB},s}\right)_L||}\right) \tag{3.4}$$

Finalmente, baseando-se na análise da seção(2.4.5), a SNR na saída de Bob será:

$$\gamma_{\mathrm{B},s} = \sum_{l_\mathrm{B}=1}^{L_\mathrm{B}} \gamma_{(l_\mathrm{B},s)} \tag{3.5}$$

onde $\gamma_{(1,s)} \geq \gamma_{(2,s)} \geq ... \geq \gamma_{(N_\mathrm{B},s)}$ são as estatísticas ordenadas ao se ordenar $\{\gamma_{(l_\mathrm{B},s)} = |h^{l_\mathrm{B}}_{\mathrm{AB},s}|^2 \frac{P}{{\sigma_\mathrm{B}}^2}\}$ em ordem decrescente de magnitude. Sendo $\frac{P}{{\sigma_\mathrm{B}}^2} = \bar{\gamma}_B$ a SNR média de Bob. De (YANG *et al.*, 2013c), podemos substituir s por um k qualquer($k \in \{1, ..., N_\mathrm{A}\}$):

$$\gamma_{\mathrm{B},k} = \sum_{l_\mathrm{B}=1}^{L_\mathrm{B}} \gamma_{(l_\mathrm{B},k)} \tag{3.6}$$

onde $\gamma_{(1,k)} \geq \gamma_{(2,k)} \geq ... \geq \gamma_{(N_\mathrm{B},k)}$ são as estatísticas ordenadas ao se ordenar $\{\gamma_{(l_\mathrm{B},k)} = |h^{l_\mathrm{B}}_{\mathrm{AB},k}|^2 \bar{\gamma}_B\}$ em ordem decrescente de magnitude. Sendo $\bar{\gamma}_B = \frac{P}{{\sigma_\mathrm{B}}^2}$ e $k \in \{1, ..., N_\mathrm{A}\}$.

Precisamos agora calcular a pdf conjunta $f_{\gamma_{(1,k)},\ldots,\gamma_{(L_\mathrm{B},k)}}(\gamma_{(1,k)}, \ldots, \gamma_{(L_\mathrm{B},k)})$ das estatísticas ordenadas $\{\gamma_{(l_\mathrm{B},k)} = |h^{l_\mathrm{B}}_{\mathrm{AB},k}|^2 \bar{\gamma}_B\}_{l_\mathrm{B}=1}^{L_\mathrm{B}}$, com $\gamma_{(1,k)} \geq \gamma_{(2,k)} \geq ... \geq \gamma_{(L_\mathrm{B},k)}$. Pois essa pdf será necessária para se calcular a pdf de $\gamma_{\mathrm{B},s}$, que é o resultado que queremos chegar nesta seção.

Primeiramente vamos definir o conjunto X para que possamos definir $f_{\gamma_{(1,k)},\ldots,\gamma_{(L_\mathrm{B},k)}}(\gamma_{(1,k)}, \ldots, \gamma_{(L_\mathrm{B},k)})$ em função de X. O conjunto X é formando pelo arranjo simples(**Definição 1**) dos N_B possíveis γ's tomados L_B a L_B .

x_t representa um elemento qualquer de X. Um conjunto $x_t \in X$ é um dos possíveis ordenamentos pelo arranjo simples dos N_B possíveis γ's tomados L_B a L_B . Podemos concluir que X é um conjunto cujos elementos são conjuntos x_t, e também que:

$|X| = \mathrm{A}^{N_\mathrm{B}}_{L_\mathrm{B}}$, ou seja, os elementos de X são $\mathrm{A}^{N_\mathrm{B}}_{L_\mathrm{B}}$ conjuntos x_t. E que $|x_t| = L_\mathrm{B}$, ou seja, os elementos de x_t são L_B variáveis γ's.

Onde $|\,.\,|$ representa o operador de cardinalidade de um conjunto. A^a_b representa o Arranjo simples de a elementos tomados de b a b. O Arranjo simples pode ser visto como todas as possíveis ordenações de um conjunto de elementos não repetidos.

Segue a definição exata de X:

$$X \equiv \begin{cases} X \equiv \left\{ \left\{ \gamma_{r,t} \in \left\{ \gamma_{(l_{\mathrm{B}},k)} = |h^{l_{\mathrm{B}}}_{\mathrm{AB},k}|^2 \, \bar{\gamma}_B \right\}_{l_{\mathrm{B}}=1}^{N_{\mathrm{B}}} \right\}_{r=1}^{L_{\mathrm{B}}} \right\}_{t=1}^{\mathrm{A}_{L_{\mathrm{B}}}^{N_{\mathrm{B}}}} \equiv \left\{ \{\gamma_{r,t}\}_{r=1}^{L_{\mathrm{B}}} \right\}_{t=1}^{\mathrm{A}_{L_{\mathrm{B}}}^{N_{\mathrm{B}}}} \equiv \{x_t\}_{t=1}^{\mathrm{A}_{L_{\mathrm{B}}}^{N_{\mathrm{B}}}} \\ \text{Logo:} \\ \{\gamma_{r,t}\}_{r=1}^{L_{\mathrm{B}}} \equiv x_t \in X \ ; \\ x_t \subseteq \left\{ \gamma_{(l_{\mathrm{B}},k)} = |h^{l_{\mathrm{B}}}_{\mathrm{AB},k}|^2 \, \bar{\gamma}_B \right\}_{l_{\mathrm{B}}=1}^{N_{\mathrm{B}}} \ ; \\ |x_t| = L_{\mathrm{B}} \ ; \\ |X| = \mathrm{A}_{L_{\mathrm{B}}}^{N_{\mathrm{B}}} \ . \end{cases} \tag{3.7}$$

Ou seja, X representa os $\mathrm{A}_{L_{\mathrm{B}}}^{N_{\mathrm{B}}}$ possíveis conjuntos formados por L_{B} de todos os N_{B} γ's em todos os possíveis ordenamentos através de arranjo simples. E, x_t representa um dos $\mathrm{A}_{L_{\mathrm{B}}}^{N_{\mathrm{B}}}$ conjuntos de L_{B} de todos os N_{B} γ's em um dos ordenamento possíveis, enumerado por t, em que $1 \leq t \leq \mathrm{A}_{L_{\mathrm{B}}}^{N_{\mathrm{B}}}$

Lembrando que:

$$\begin{aligned} \mathrm{A}_{L_{\mathrm{B}}}^{N_{\mathrm{B}}} &= \frac{N_{\mathrm{B}}!}{(N_{\mathrm{B}} - L_{\mathrm{B}})!} \\ &= L_{\mathrm{B}}! \binom{N_{\mathrm{B}}}{L_{\mathrm{B}}} \end{aligned} \tag{3.8}$$

Podemos agora escrever à partir da definição da pdf conjunta(**Definição 5**) que a integral de $f_{\gamma_{(1,k)},\ldots,\gamma_{(L_{\mathrm{B}},k)}}(\gamma_{(1,k)}, \ldots, \gamma_{(L_{\mathrm{B}},k)})$ no intervalo:
$-\infty \leq \gamma_{(L_{\mathrm{B}},k)} \leq \gamma_{(L_{\mathrm{B}}-1,k)} \leq \cdots \leq \gamma_{(2,k)} \leq \gamma_{(1,k)} \leq \infty$ será igual à probabilidade do ordenamento dos γ's:

$$\int f_{\gamma_{(1,k)},\ldots,\gamma_{(L_{\mathrm{B}},k)}}(\gamma_{(1,k)}, \ldots, \gamma_{(L_{\mathrm{B}},k)}) d(\gamma_{(1,k)}, \ldots, \gamma_{(L_{\mathrm{B}},k)}) \tag{3.9}$$

integral em $-\infty \leq \gamma_{(L_{\mathrm{B}},k)} \leq \gamma_{(L_{\mathrm{B}}-1,k)} \leq \ldots \leq \gamma_{(2,k)} \leq \gamma_{(1,k)} \leq \infty$

$= \Pr(\gamma_{(L_{\mathrm{B}},k)} \leq \gamma_{(L_{\mathrm{B}}-1,k)} \leq \ldots \leq \gamma_{(2,k)} \leq \gamma_{(1,k)})$

Logo, para um $1 \leq t \leq \mathrm{A}_{L_\mathrm{B}}^{N_\mathrm{B}}$ qualquer, podemos escrever que:

$$\begin{aligned}
&\Pr(\gamma_{(L_\mathrm{B},k)} \leq \gamma_{(L_\mathrm{B}-1,k)} \leq ... \leq \gamma_{(2,k)} \leq \gamma_{(1,k)}) \\
&= \Pr(\gamma_{(1,k)} \geq \gamma_{(2,k)} \geq ... \geq \gamma_{(L_\mathrm{B}-1,k)} \geq \gamma_{(L_\mathrm{B},k)}) \\
&= \Pr\left(\bigcup_{x_t \in X} \{x_t = \{\gamma_{(1,k)}, ..., \gamma_{(L_\mathrm{B},k)}\}\}\right)
\end{aligned} \tag{3.10}$$

Ou seja, a probabilidade do ordenamento dos γ's pode ser representada como o união das probabilidades de que cada um dos conjuntos $x_t \in X$ esteja nessa ordenação específica. Devido à independência dos eventos, a probabilidade da união será a soma das probabilidades de que cada x_t seja o ordenamento em questão(fato que se conclui da **Definição 3**). Assim, teremos que:

$$\begin{aligned}
&\Pr\left(\bigcup_{x_t \in X} \{x_t = \{\gamma_{(1,k)}, ..., \gamma_{(L_\mathrm{B},k)}\}\}\right) \\
&= \sum_{x_t \in X} \Pr(\gamma_{1,t} = \gamma_{(1,k)} \geq ... \geq \gamma_{L_\mathrm{B},t} = \gamma_{(L_\mathrm{B},k)}) \\
&= \sum_{x_t \in X} \Pr(\gamma_{1,t} \geq ... \geq \gamma_{L_\mathrm{B},t} \geq \gamma_{(L_\mathrm{B}+1,k)}, ..., \gamma_{(N_\mathrm{B},k)})
\end{aligned} \tag{3.11}$$

Como são independentes, podemos separar essas probabilidades em todas a probabilidades individuais(**Definição 2** e **Definição 3**):

$$\sum_{x_t \in X} \Pr(\gamma_{1,t} \geq ... \geq \gamma_{L_B,t} \geq \gamma_{(L_B+1,k)}, ..., \gamma_{(N_B,k)}) \tag{3.12}$$

$$= \sum_{x_t \in X} \Pr(\gamma_{1,t} \geq ... \geq \gamma_{L_B,t}) \times \Pr(\gamma_{L_B,t} \geq \gamma_{(L_B+1,k)}, ..., \gamma_{(N_B,k)})$$

$$= \sum_{x_t \in X} \Pr(\gamma_{L_B,t} \geq \gamma_{(L_B+1,k)}, ..., \gamma_{(N_B,k)}) \times \Pr(\gamma_{1,t} \geq ... \geq \gamma_{L_B,t})$$

$$= \sum_{x_t \in X} \Pr(\gamma_{(L_B+1,k)}, ..., \gamma_{(N_B,k)} \leq \gamma_{L_B,t}) \times \Pr(\gamma_{L_B,t} \leq ... \leq \gamma_{1,t})$$

$$= \sum_{x_t \in X} \Pr(\gamma_{(L_B+1,k)} \leq \gamma_{L_B,t}) \times \Pr(\gamma_{(L_B+2,k)} \leq \gamma_{L_B,t}) \times ...$$

$$... \times \Pr(\gamma_{(N_B-1,k)} \leq \gamma_{L_B,t}) \times \Pr(\gamma_{(N_B,k)} \leq \gamma_{L_B,t})$$

$$\times \Pr(-\infty \leq \gamma_{L_B,t} \leq \gamma_{L_B-1,t}) \times \Pr(\gamma_{L_B,t} \leq \gamma_{L_B-1,t} \leq \gamma_{L_B-2,t}) \times ...$$

$$... \times \Pr(\gamma_{3,t} \leq \gamma_{2,t} \leq \gamma_{1,t}) \times \Pr(\gamma_{2,t} \leq \gamma_{1,t} \leq \infty)$$

$$= \sum_{x_t \in X} \prod_{j=L_B+1}^{N_B} \Pr(\gamma_{(j,k)} \leq \gamma_{L_B,t}) \prod_{i=1}^{L_B} \Pr(\inf(\gamma_{i,t}) \leq \gamma_{i,t} \leq \sup(\gamma_{i,t}))$$

$\inf()$ e $\sup()$ para cada $\gamma_{i,t}$ definidos em:

$$-\infty \leq \gamma_{(L_B,k)} \leq \gamma_{(L_B-1,k)} \leq ... \leq \gamma_{(2,k)} \leq \gamma_{(1,k)} \leq \infty$$

Vamos chamar a pdf e a cdf de qualquer um dos N_B $\gamma's$, respectivamente, de $f_\gamma(\gamma)$ e de $F_\gamma(\gamma)$. A pdf e a cdf são as mesmas para qualquer um dos $\gamma's$, isso se deve ao fato de que o sistema está modelado considerando o desvanecimento *Rayleigh* i.i.d., logo todas as variáveis γ's são i.i.d.. Então, podemos escrever através da definição da PDF, da CDF e de algumas de suas propriedades(**Definição 5**, **Definição 6**, **Lema 1**, **Definição 7**) que:

$$\sum_{x_t \in X} \prod_{j=L_B+1}^{N_B} \Pr(\gamma_{(j,k)} \leq \gamma_{L_B,t}) \prod_{i=1}^{L_B} \Pr(\inf(\gamma_{i,t}) \leq \gamma_{i,t} \leq \sup(\gamma_{i,t})) \tag{3.13}$$

$$= \sum_{x_t \in X} [F_\gamma(\gamma_{L_B,t})]^{N_B-L_B} \int_{-\infty}^{\gamma_{L_B-1,t}} \int_{\gamma_{L_B,t}}^{\gamma_{L_B-2,t}} ... \quad \int_{\gamma_{3,t}}^{\gamma_{1,t}} \int_{\gamma_{2,t}}^{\infty} \prod_{i=1}^{L_B} f_\gamma(\gamma_{i,t}) d(\gamma_{i,t})$$

Como $|X| = A_{L_B}^{N_B}$, o somatório acima se repetirá por $A_{L_B}^{N_B} = L_B! \binom{N_B}{L_B}$ vezes, e utilizando o fato que $\gamma_{i,t}$ é igual à $\gamma_{(i,k)}$ para qualquer t e qualquer i (fato da equação (3.11)), poderemos escrever que:

$$\sum_{x_t \in X} [F_\gamma(\gamma_{L_B,t})]^{N_B - L_B} \int_{-\infty}^{\gamma_{L_B-1,t}} \int_{\gamma_{L_B,t}}^{\gamma_{L_B-2,t}} \ldots \int_{\gamma_{3,t}}^{\gamma_{1,t}} \int_{\gamma_{2,t}}^{\infty} \prod_{i=1}^{L_B} f_\gamma(\gamma_{i,t}) d(\gamma_{i,t}) \tag{3.14}$$
$$= L_B! \binom{N_B}{L_B} [F_\gamma(\gamma_{(L_B,k)})]^{N_B - L_B} \int_{-\infty}^{\gamma_{(L_B-1,k)}} \int_{\gamma_{(L_B,k)}}^{\gamma_{(L_B-2,k)}} \ldots \int_{\gamma_{(3,k)}}^{\gamma_{(1,k)}} \int_{\gamma_{(2,k)}}^{\infty} \prod_{i=1}^{L_B} f_\gamma(\gamma_{(i,k)}) d(\gamma_{(i,k)})$$

Agora, rearranjando as variáveis para dentro das integrais:

$$L_B! \binom{N_B}{L_B} [F_\gamma(\gamma_{(L_B,k)})]^{N_B - L_B} \int_{-\infty}^{\gamma_{(L_B-1,k)}} \int_{\gamma_{(L_B,k)}}^{\gamma_{(L_B-2,k)}} \ldots \int_{\gamma_{(3,k)}}^{\gamma_{(1,k)}} \int_{\gamma_{(2,k)}}^{\infty} \prod_{i=1}^{L_B} f_\gamma(\gamma_{(i,k)}) d(\gamma_{(i,k)})$$
$$= \int_{-\infty}^{\gamma_{(L_B-1,k)}} \int_{\gamma_{(L_B,k)}}^{\gamma_{(L_B-2,k)}} \ldots \int_{\gamma_{(3,k)}}^{\gamma_{(1,k)}} \int_{\gamma_{(2,k)}}^{\infty} L_B! \binom{N_B}{L_B} [F_\gamma(\gamma_{(L_B,k)})]^{N_B - L_B} \prod_{i=1}^{L_B} f_\gamma(\gamma_{(i,k)}) d(\gamma_{(i,k)}) \tag{3.15}$$

Utilizando a notação curta para às integrais, uma propriedade básica dos produtórios, e o fato que as variáveis γ's são i.i.d.:

$$\int_{-\infty}^{\gamma_{(L_B-1,k)}} \int_{\gamma_{(L_B,k)}}^{\gamma_{(L_B-2,k)}} \ldots \int_{\gamma_{(3,k)}}^{\gamma_{(1,k)}} \int_{\gamma_{(2,k)}}^{\infty} L_B! \binom{N_B}{L_B} [F_\gamma(\gamma_{(L_B,k)})]^{N_B - L_B} \prod_{i=1}^{L_B} f_\gamma(\gamma_{(i,k)}) d(\gamma_{(i,k)}) \tag{3.16}$$
$$= \int L_B! \binom{N_B}{L_B} [F_\gamma(\gamma_{(L_B,k)})]^{N_B - L_B} \prod_{i=1}^{L_B} f_\gamma(\gamma_{(i,k)}) \prod_{i=1}^{L_B} d(\gamma_{(i,k)})$$
$$= \int L_B! \binom{N_B}{L_B} [F_\gamma(\gamma_{(L_B,k)})]^{N_B - L_B} \prod_{i=1}^{L_B} f_\gamma(\gamma_{(i,k)}) d(\gamma_{(1,k)}, ..., \gamma_{(L_B,k)})$$

integral em $-\infty \leq \gamma_{(L_B,k)} \leq \gamma_{(L_B-1,k)} \leq \ldots \leq \gamma_{(2,k)} \leq \gamma_{(1,k)} \leq \infty$

Comparando a última expressão com a expressão da equação (3.9) do início desta demonstração:

$$\int f_{\gamma_{(1,k)},\ldots,\gamma_{(L_B,k)}}(\gamma_{(1,k)}, \ldots, \gamma_{(L_B,k)}) d(\gamma_{(1,k)}, \ldots, \gamma_{(L_B,k)}) \tag{3.17}$$
$$= \int L_B! \binom{N_B}{L_B} [F_\gamma(\gamma_{(L_B,k)})]^{N_B - L_B} \prod_{i=1}^{L_B} f_\gamma(\gamma_{(i,k)}) d(\gamma_{(1,k)}, ..., \gamma_{(L_B,k)})$$

Logo:

$$f_{\gamma_{(1,k)},\ldots,\gamma_{(L_B,k)}}(\gamma_{(1,k)}, \ldots, \gamma_{(L_B,k)}) = L_B! \binom{N_B}{L_B} [F_\gamma(\gamma_{(L_B,k)})]^{N_B - L_B} \prod_{i=1}^{L_B} f_\gamma(\gamma_{(i,k)}) \tag{3.18}$$

Encontramos $f_{\gamma_{(1,k)},\ldots,\gamma_{(L_B,k)}}(\gamma_{(1,k)}, \ldots, \gamma_{(L_B,k)})$ em função de $f_\gamma(\gamma)$. Precisamos, então, achar a expressão para $f_\gamma(\gamma)$ em função dos parâmetros do sistema.

Vamos calcular as expressões da pdf $f_\gamma(\gamma)$ e da cdf $F_\gamma(\gamma)$ originais não ordenadas.

Lembrando que $\gamma_{(l_\mathrm{B},k)}$ é dado por:

$$\left\{ \gamma_{(l_\mathrm{B},k)} = |h_{\mathrm{AB},k}^{l_\mathrm{B}}|^2 \frac{P}{{\sigma_\mathrm{B}}^2} \right\}_{l_\mathrm{B}=1}^{N_\mathrm{B}} \tag{3.19}$$

Para um l_B qualquer, $\gamma_{(l_\mathrm{B},k)}$ será:

$$\gamma_{(l_\mathrm{B},k)} = |h_{\mathrm{AB},k}^{l_\mathrm{B}}|^2 \frac{P}{{\sigma_\mathrm{B}}^2} = |h_{\mathrm{AB},k}^{l_\mathrm{B}}|^2 \bar{\gamma}_\mathrm{B} \tag{3.20}$$

Como cada $h_{\mathrm{AB},k}^{l_\mathrm{B}}$ é um número complexo, seu módulo ao quadrado será a soma dos quadrados de sua parte imaginária com sua parte real, ou seja:

$$|h_{\mathrm{AB},k}^{l_\mathrm{B}}|^2 = |\,\mathrm{Re}(h_{\mathrm{AB},k}^{l_\mathrm{B}})|^2 + |\,\mathrm{Im}(h_{\mathrm{AB},k}^{l_\mathrm{B}})|^2 \tag{3.21}$$

Utilizado a **Definição 24**, teremos:

$$|h_{\mathrm{AB},k}^{l_\mathrm{B}}|^2 = |\,\mathrm{Re}(h_{\mathrm{AB},k}^{l_\mathrm{B}})|^2 + |\,\mathrm{Im}(h_{\mathrm{AB},k}^{l_\mathrm{B}})|^2 = \sum_{i=1}^{2} |\,\mathrm{Parte}_i(h_{\mathrm{AB},k}^{l_\mathrm{B}})_{\mathrm{Re,Im}}|^2 \tag{3.22}$$

Assim:

$$\gamma_{(l_\mathrm{B},k)} = |h_{\mathrm{AB},k}^{l_\mathrm{B}}|^2 \bar{\gamma}_\mathrm{B} = \bar{\gamma}_\mathrm{B} \sum_{i=1}^{2} |\,\mathrm{Parte}_i(h_{\mathrm{AB},k}^{l_\mathrm{B}})_{\mathrm{Re,Im}}|^2 \tag{3.23}$$

Fazendo uma pequena manipulação algébrica:

$$\gamma_{(l_\mathrm{B},k)} = \sum_{i=1}^{2} |\sqrt{\bar{\gamma}_\mathrm{B}}\,\mathrm{Parte}_i(h_{\mathrm{AB},k}^{l_\mathrm{B}})_{\mathrm{Re,Im}}|^2 = \sum_{i=1}^{2} (\sqrt{\bar{\gamma}_\mathrm{B}}\,\mathrm{Parte}_i(h_{\mathrm{AB},k}^{l_\mathrm{B}})_{\mathrm{Re,Im}})^2 \tag{3.24}$$

Podemos escrever que:

$$\gamma_{(l_\mathrm{B},k)} = \sum_{i=1}^{2} (\sqrt{\bar{\gamma}_\mathrm{B}}\,\mathrm{Parte}_i(h_{\mathrm{AB},k}^{l_\mathrm{B}})_{\mathrm{Re,Im}})^2 = \sum_{i=1}^{2} x_i^2 \tag{3.25}$$

Onde x_i é uma variável aleatória representada pela seguinte equivalência:

$$x_i \equiv \sqrt{\bar{\gamma}_\mathrm{B}}\,\mathrm{Parte}_i(\mathrm{h}_{\mathrm{AB},k}^{l_\mathrm{B}})_{\mathrm{Re,Im}} \tag{3.26}$$

Sendo p uma $\text{Parte}_i(\text{h}^{l_\text{B}}_{\text{AB},k})_{\text{Re,Im}}$ qualquer e utilizando a **Definição 16** da distribuição Gaussiana e a definição de desvanecimento *Rayleigh* dado na seção (2.2) , teremos que:

$$\text{Parte}_i(\text{h}^{l_\text{B}}_{\text{AB},k})_{\text{Re,Im}} \sim \mathcal{N}(0,1/2) \implies \text{pdf}\left(\text{Parte}_i(\text{h}^{l_\text{B}}_{\text{AB},k})_{\text{Re,Im}}\right) = \frac{1}{\sqrt{\pi}} e^{-p^2} \tag{3.27}$$

Utilizando o **Lema 9** da técnica de transformação da pdf e que $x_i = \sqrt{\bar{\gamma}_\text{B}}\, p$, podemos definir $g(p) = \sqrt{\bar{\gamma}_\text{B}}\, p$ e denotando $v = g(p)$ teremos que:

$$\begin{aligned} \text{pdf}(x_i) = \text{pdf}(g(p)) = f_V(v) &= \left| \frac{d}{dv}\left[g^{-1}(v)\right] \right| \frac{1}{\sqrt{\pi}} e^{-\left(g^{-1}(v)\right)^2} \\ f_V(v) &= \left| \frac{d}{dv}\left[v/\sqrt{\bar{\gamma}_\text{B}}\right] \right| \frac{1}{\sqrt{\pi}} e^{-\frac{v^2}{\bar{\gamma}_\text{B}}} \\ f_V(v) &= \frac{1}{\sqrt{\bar{\gamma}_\text{B}}} \frac{1}{\sqrt{\pi}} e^{-\frac{v^2}{\bar{\gamma}_\text{B}}} \end{aligned} \tag{3.28}$$

Fazendo uma pequena manipulação algébrica para comparar com a expressão (2.81) da pdf geral da distribuição Normal:

$$\begin{aligned} \text{pdf}(x_i) = f_V(v) &= \frac{1}{\sqrt{\bar{\gamma}_\text{B}}} \frac{1}{\sqrt{\pi}} e^{-\frac{v^2}{\bar{\gamma}_\text{B}}} \\ f_V(v) &= \frac{1}{\sqrt{2\pi\left(\frac{\bar{\gamma}_\text{B}}{2}\right)}} e^{-\frac{v^2}{2\left(\frac{\bar{\gamma}_\text{B}}{2}\right)}} \end{aligned} \tag{3.29}$$

Então, podemos concluir que:

$$\text{var}(x_i) = \frac{\bar{\gamma}_\text{B}}{2} \tag{3.30}$$

$$\text{E}[x_i] = 0 \tag{3.31}$$

Como:

$$\gamma_{(l_\text{B},k)} = \sum_{i=1}^{2} x_i^2 \tag{3.32}$$

Então pelo **Lema 15**, $\gamma_{(l_\text{B},k)} \sim \chi^2(2, \frac{\bar{\gamma}_\text{B}}{2})$. Basta agora substituir $n = 2$, $\sigma^2 = \frac{\bar{\gamma}_\text{B}}{2}$ nas expressões da cdf e da pdf da distribuição Qui-quadrado(**Lema 15**) para encontrar a cdf e a pdf de $\{\gamma = |h^{l_\text{B}}_{\text{AB},k}|^2 \frac{P}{{\sigma_\text{B}}^2}\}_{l_\text{B}=1}^{N_\text{B}}$ originais e não ordenadas, que serão:

$$F_{\gamma}(\gamma) = 1 - e^{-\left(\frac{\gamma}{\bar{\gamma}_{\mathrm{B}}}\right)} \tag{3.33}$$

$$f_{\gamma}(\gamma) = \frac{1}{\bar{\gamma}_{\mathrm{B}}} e^{-\left(\frac{\gamma}{\bar{\gamma}_{\mathrm{B}}}\right)} \tag{3.34}$$

Com os resultados anteriores, podemos aplicar a **Definição 19**:

$$\begin{aligned} \mathscr{M}_{\gamma_{\mathrm{B},k}}(s) &= \mathrm{E}_{\gamma_{\mathrm{B},k}}\left[e^{s\gamma_{\mathrm{B},k}}\right] \\ &= \mathrm{E}_{\gamma_{(1,k)},\cdots,\gamma_{(L_{\mathrm{B}},k)}}\left[e^{s\sum_{l_{\mathrm{B}}=1}^{L_{\mathrm{B}}}\gamma_{(l_{\mathrm{B}},k)}}\right] \end{aligned} \tag{3.35}$$

Aplicando a **Definição 19** e substituindo os valores:

$$\begin{aligned} \mathscr{M}_{\gamma_{\mathrm{B},k}}(s) &= \\ &= \int_0^{\infty}\int_{\gamma_{(L_{\mathrm{B}},k)}}^{\infty}\cdots\int_{\gamma_{(2,k)}}^{\infty} f_{\gamma_{(1,k)},\cdots,\gamma_{(L_{\mathrm{B}},k)}}(\gamma_{(1,k)},\cdots,\gamma_{(L_{\mathrm{B}},k)})e^{s\sum_{l_{\mathrm{B}}=1}^{L_{\mathrm{B}}}\gamma_{(l_{\mathrm{B}},k)}}d\gamma_{(1,k)}\ldots d\gamma_{(L_{\mathrm{B}},k)} \end{aligned} \tag{3.36}$$

A integral é resolvida em (ALOUINI; SIMON, 2000), resultando em:

$$\begin{aligned} \mathscr{M}_{\gamma_{\mathrm{B},k}}(s) &= (1-s\bar{\gamma}_{\mathrm{B}})^{-L_{\mathrm{B}}+1}\prod_{l_{\mathrm{B}}=L_{\mathrm{B}}}^{N_{\mathrm{B}}}\left(1-\frac{s\bar{\gamma}_{\mathrm{B}}L_{\mathrm{B}}}{l_{\mathrm{B}}}\right)^{-1} \\ &= (1-s\bar{\gamma}_{\mathrm{B}})^{-L_{\mathrm{B}}}\prod_{l_{\mathrm{B}}=L_{\mathrm{B}}+1}^{N_{\mathrm{B}}}\left(1-\frac{s\bar{\gamma}_{\mathrm{B}}L_{\mathrm{B}}}{l_{\mathrm{B}}}\right)^{-1} \end{aligned} \tag{3.37}$$

Pelo **Lema 17**:

$$\mathscr{L}_{\gamma_{\mathrm{B},k}}\{f_{\gamma_{\mathrm{B},k}}(x)\}(s) = \mathscr{M}_{\gamma_{\mathrm{B},k}}(-s) \tag{3.38}$$

3.1.1.1 Derivação da CDF e da PDF de $\gamma_{B,s}$

Agora vamos derivar as expressões da cdf e da pdf de $\gamma_{\mathrm{B},s}$ para usá-las nas próximas seções.

Primeiramente, temos que obter a pdf e a cdf da variável aleatória $\gamma_{\mathrm{B},k}$ ($k \in \{1,\ldots,N_{\mathrm{A}}\}$). De (3.38), concluimos que a transformada inversa de Laplace de $\mathscr{L}_{\gamma_{\mathrm{B},k}}(s)$ é $f_{\gamma_{\mathrm{B},k}}(x)$, então substituindo (3.37) em (3.38) teremos :

$$\mathscr{L}\{f_{\gamma_{\mathrm{B},k}}(x)\} = (1+s\bar{\gamma}_{\mathrm{B}})^{-L_{\mathrm{B}}} \prod_{l_{\mathrm{B}}=L_{\mathrm{B}}+1}^{N_{\mathrm{B}}} \left(1+\frac{s\bar{\gamma}_{\mathrm{B}} L_{\mathrm{B}}}{l_{\mathrm{B}}}\right)^{-1} \tag{3.39}$$

Seja a propriedade da Integração da transformada de Laplace de uma função qualquer f (**Lema 19**):

$$\mathscr{L}\left\{\int_{t=0}^{x} f(t)dt\right\} = \frac{\mathscr{L}\{f(x)\}}{s} \tag{3.40}$$

Como $f_{\gamma_{\mathrm{B},k}}(x)$ se define apenas para $x \geq 0$, então pelo **Lema 3** e pela **Definição 7** :

$$\int_{t=-\infty}^{x} f_{\gamma_{\mathrm{B},k}}(t)dt = \int_{t=0}^{x} f_{\gamma_{\mathrm{B},k}}(t)dt = F_{\gamma_{\mathrm{B},k}}(x) - 0F_{\gamma_{\mathrm{B},k}}(0) = F_{\gamma_{\mathrm{B},k}}(x) \tag{3.41}$$

Logo:

$$\begin{aligned}\mathscr{L}\{F_{\gamma_{\mathrm{B},k}}(x)\} &= \frac{\mathscr{L}\{f_{\gamma_{\mathrm{B},k}}(x)\}}{s} \\ &= \frac{1}{s} \times \left((1+s\bar{\gamma}_{\mathrm{B}})^{-L_{\mathrm{B}}} \prod_{l_{\mathrm{B}}=L_{\mathrm{B}}+1}^{N_{\mathrm{B}}} \left(1+\frac{s\bar{\gamma}_{\mathrm{B}} L_{\mathrm{B}}}{l_{\mathrm{B}}}\right)^{-1}\right) \\ &= \frac{1}{s} \times \frac{\bar{\gamma}_{\mathrm{B}}^{-L_{\mathrm{B}}}}{(s+\frac{1}{\bar{\gamma}_{\mathrm{B}}})^{L_{\mathrm{B}}}} \times \prod_{l_{\mathrm{B}}=L_{\mathrm{B}}+1}^{N_{\mathrm{B}}} \frac{\frac{l_{\mathrm{B}}}{L_{\mathrm{B}}}\bar{\gamma}_{\mathrm{B}}^{-L_{\mathrm{B}}}}{s+\frac{l_{\mathrm{B}}}{L_{\mathrm{B}}\bar{\gamma}_{\mathrm{B}}}}\end{aligned} \tag{3.42}$$

Utilizando a expansão por frações parciais para calcular a transformada inversa de Laplace(**Lema 24**):

$$\mathscr{L}\{F_{\gamma_{\mathrm{B},k}}(x)\} = \frac{1}{s} + \sum_{l_{\mathrm{B}}=1}^{L_{\mathrm{B}}} \frac{\varepsilon_{l_{\mathrm{B}}}}{(s+\frac{1}{\bar{\gamma}_{\mathrm{B}}})^{l_{\mathrm{B}}}} + \sum_{l_{\mathrm{B}}=L_{\mathrm{B}}+1}^{N_{\mathrm{B}}} \frac{\varepsilon_{l_{\mathrm{B}}}}{s+\frac{l_{\mathrm{B}}}{L_{\mathrm{B}}\bar{\gamma}_{\mathrm{B}}}} \tag{3.43}$$

Onde os coeficientes $\varepsilon_{l_{\mathrm{B}}}$ são calculados através do sistema de equações lineares da expressão (2.158) do **Lema 24**, obtendo-se:

$$\varepsilon_{l_{\mathrm{B}}} = \begin{cases} 1, & l_{\mathrm{B}} = 0, \\ \bar{\gamma}_{\mathrm{B}}^{1-l_{\mathrm{B}}}\left[-1+\sum_{k=L_{\mathrm{B}}+1}^{N_{\mathrm{B}}}(-1)^{k-l_{\mathrm{B}}}\frac{\binom{N_{\mathrm{B}}}{N_{\mathrm{B}}-k}\binom{k-1}{k-L_{\mathrm{B}}-1}}{\binom{k}{L_{\mathrm{B}}}-1)^{L_{\mathrm{B}}-l_{\mathrm{B}}+1}}\right], & 1 \leq l_{\mathrm{B}} < L_{\mathrm{B}}, \\ -\bar{\gamma}_{\mathrm{B}}{}^{1-l_{\mathrm{B}}}\binom{N_{\mathrm{B}}}{N_{\mathrm{B}}-L_{\mathrm{B}}}, & l_{\mathrm{B}} = L_{\mathrm{B}}, \\ \frac{(-1)^{l_{\mathrm{B}}}\binom{N_{\mathrm{B}}}{N_{\mathrm{B}}-l_{\mathrm{B}}}\binom{l_{\mathrm{B}}-1}{l_{\mathrm{B}}-L_{\mathrm{B}}-1}}{\left(\frac{l_{\mathrm{B}}}{L_{\mathrm{B}}}-1\right)^{L_{\mathrm{B}}}}, & L_{\mathrm{B}} < l_{\mathrm{B}} \leq N_{\mathrm{B}}. \end{cases} \tag{3.44}$$

Assim, a transformada inversa da cdf pode ser calculada utilizando a expressão (2.157) do **Lema 24**, obtendo-se:

$$F_{\gamma_{\mathrm{B},k}}(x) = 1 + \sum_{l_{\mathrm{B}}=1}^{L_{\mathrm{B}}} \varepsilon_{l_{\mathrm{B}}} x^{l_{\mathrm{B}}-1} \frac{e^{\frac{-x}{\bar{\gamma}_{\mathrm{B}}}}}{(l_{\mathrm{B}}-1)!} + \sum_{l_{\mathrm{B}}=L_{\mathrm{B}}+1}^{N_{\mathrm{B}}} \varepsilon_{l_{\mathrm{B}}} e^{\frac{-l_{\mathrm{B}}x}{L_{\mathrm{B}}\bar{\gamma}_{\mathrm{B}}}} \tag{3.45}$$

Derivando a cdf acima obtemos a pdf:

$$f_{\gamma_{\mathrm{B},k}}(x) = \sum_{l_{\mathrm{B}}=1}^{L_{\mathrm{B}}} \left[\frac{\varepsilon_{l_{\mathrm{B}}}(l_{\mathrm{B}}-1)}{(l_{\mathrm{B}}-1)!} x^{l_{\mathrm{B}}-2} e^{\frac{-x}{\bar{\gamma}_{\mathrm{B}}}} - \frac{\varepsilon_{l_{\mathrm{B}}}}{(l_{\mathrm{B}}-1)!\bar{\gamma}_{\mathrm{B}}} x^{l_{\mathrm{B}}-1} e^{\frac{-x}{\bar{\gamma}_{\mathrm{B}}}} \right] - \sum_{l_{\mathrm{B}}=L_{\mathrm{B}}+1}^{N_{\mathrm{B}}} \varepsilon_{l_{\mathrm{B}}} e^{\frac{-l_{\mathrm{B}}x}{L_{\mathrm{B}}\bar{\gamma}_{\mathrm{B}}}} \frac{l_{\mathrm{B}}}{L_{\mathrm{B}}\bar{\gamma}_{\mathrm{B}}} \tag{3.46}$$

Vamos agora calcular a cdf de $\gamma_{\mathrm{B},s}$, para tanto, vamos utilizar a definição da cdf(**Definição 7**), da qual podemos concluir que:

$$F_{\gamma_{\mathrm{B},s}}(x) = \Pr(\gamma_{\mathrm{B},s} \leq x) \tag{3.47}$$

E também que para um $1 \leq k \leq N_{\mathrm{A}}$ qualquer:

$$F_{\gamma_{\mathrm{B},k}}(x) = \Pr(\gamma_{\mathrm{B},k} \leq x) \tag{3.48}$$

Mas pela definição do esquema TAS analisado anteriormente, teremos que:

$$\exists!\, i:\ \gamma_{\mathrm{B},s} = \max\{\gamma_{\mathrm{B},i}\}_{i=1}^{N_{\mathrm{A}}} \implies i = s \tag{3.49}$$

Observe que mudamos a notação de k para i, pois no caso acima estamos especificando valores dessas variáveis aleatórias, já k denota uma antena qualquer de Alice.

Substituindo em (3.49) em (3.48):

$$F_{\gamma_{\mathrm{B},s}}(x) = \Pr(\gamma_{\mathrm{B},s} \leq x) = \Pr(\max\{\gamma_{\mathrm{B},i}\}_{i=1}^{N_{\mathrm{A}}} \leq x) \tag{3.50}$$

Como $\gamma_{\mathrm{B},i}$ são variáveis i.i.d., $\Pr(\max\{\gamma_{\mathrm{B},i}\}_{i=1}^{N_{\mathrm{A}}} \leq x)$ será a probabilidade de que $\forall i$, $\gamma_{\mathrm{B},i} \leq x$, ou seja:

$$\begin{aligned}\Pr(\max\{\gamma_{\mathrm{B},i}\}_{i=1}^{N_\mathrm{A}} \leq x) &= \Pr(\gamma_{\mathrm{B},1},...,\gamma_{\mathrm{B},N_\mathrm{A}} \leq x) \\ &= \Pr(\gamma_{\mathrm{B},1} \leq x) \times ... \times \Pr(\gamma_{\mathrm{B},N_\mathrm{A}} \leq x) \\ &= \prod_{i=1}^{N_\mathrm{A}} \Pr(\gamma_{\mathrm{B},i} \leq x) \\ &= \prod_{i=1}^{N_\mathrm{A}} F_{\gamma_{\mathrm{B},i}}(x)\end{aligned} \tag{3.51}$$

Como $F_{\gamma_{\mathrm{B},k}}(x)$ foi calculada para um $1 \leq k \leq N_\mathrm{A}$ qualquer:

$$\begin{aligned}&\prod_{i=1}^{N_\mathrm{A}} F_{\gamma_{\mathrm{B},i}}(x) \\ &= \left[F_{\gamma_{\mathrm{B},k}}(x)\right]^{N_\mathrm{A}}\end{aligned} \tag{3.52}$$

Juntando (3.50), (3.51) e (3.52), teremos que:

$$F_{\gamma_{\mathrm{B},s}}(x) = \left[F_{\gamma_{\mathrm{B},k}}(x)\right]^{N_\mathrm{A}} \tag{3.53}$$

Então, substitui-se (3.45) em (3.53), e se utilizando da expansão multinomial(**Lema 30**), $F_{\gamma_{\mathrm{B},s}}$ é calculado como:

$$F_{\gamma_{\mathrm{B},s}}(x) = \sum_{S_k \in S} \alpha_k x^{\beta_k} e^{\frac{-\delta_k x}{\bar{\gamma}_\mathrm{B}}} \tag{3.54}$$

onde S é definido por:

$$S = \left\{ S_k \middle| \sum_{n=0}^{N_\mathrm{B}} n_{k,n} = N_\mathrm{A} \right\}, \{n_{k,n}\} \in \mathbb{Z}^+ \tag{3.55}$$

Onde:

$$\alpha_k = N_\mathrm{A}! \prod_{l_\mathrm{B}=1}^{L_\mathrm{B}} \left(\frac{\varepsilon_{l_\mathrm{B}}}{(l_\mathrm{B}-1)!} \right)^{n_{k,l_\mathrm{B}}} \frac{\prod_{l_\mathrm{B}=L_\mathrm{B}+1}^{N_\mathrm{B}} {\varepsilon_{l}}_\mathrm{B}^{n_{k,l_\mathrm{B}}}}{\prod_{n=0}^{N_\mathrm{B}} n_{k,n}!} \tag{3.56}$$

$$\beta_k = \sum_{l_\mathrm{B}=1}^{L_\mathrm{B}} (l_\mathrm{B}-1)\, n_{k,l_\mathrm{B}} \tag{3.57}$$

$$\delta_k = \sum_{l_\mathrm{B}=1}^{L_\mathrm{B}} n_{k,l_\mathrm{B}} + \sum_{l_\mathrm{B}=L_\mathrm{B}+1}^{N_\mathrm{B}} \frac{l_\mathrm{B} n_{k,l_\mathrm{B}}}{L_\mathrm{B}} \tag{3.58}$$

E onde os coeficientes $\varepsilon_{l_\mathrm{B}}$ foram definidos na expressão (3.44).

Da relação entre a pdf e cdf(**Definição 8**), a pdf de $\gamma_{\mathrm{B},s}$ pode ser expressa da seguinte maneira:

$$f_{\gamma_{\mathrm{B},s}}(x) = \frac{d}{dx}\left[F_{\gamma_{\mathrm{B},s}}(x)\right] = \frac{d}{dx}\left[\left(F_{\gamma_{\mathrm{B},k}}(x)\right)^{N_\mathrm{A}}\right] \tag{3.59}$$

Após aplicação da regra da cadeia(**Definição 11**):

$$\frac{d}{dx}\left[\left(F_{\gamma_{\mathrm{B},k}}(x)\right)^{N_\mathrm{A}}\right] = N_\mathrm{A}\left(F_{\gamma_{\mathrm{B},k}}(x)\right)^{N_\mathrm{A}-1} f_{\gamma_{\mathrm{B},k}}(x) \tag{3.60}$$

Fazendo a expressão da cdf de $F_{\gamma_{\mathrm{B},s}}(x)$(expressões (3.54) e (3.55)) para $N_\mathrm{A}-1$ em vez de N_A, teremos que $\left(F_{\gamma_{\mathrm{B},k}}(x)\right)^{N_\mathrm{A}-1} = \sum_{S_k \in S'} \alpha_k x^{\beta_k} e^{\frac{-\delta_k x}{\bar{\gamma}_\mathrm{B}}}$, sendo S' definido por:

$$S' = \left\{ S_k \middle| \sum_{n=0}^{N_\mathrm{B}} n_{k,n} = N_\mathrm{A} - 1 \right\}, \{n_{k,n}\} \in \mathbb{Z}^+ \tag{3.61}$$

Portanto:

$$f_{\gamma_{\mathrm{B},s}}(x) = N_\mathrm{A} f_{\gamma_{\mathrm{B},k}}(x) \sum_{S_k \in S'} \alpha_k x^{\beta_k} e^{\frac{-\delta_k x}{\bar{\gamma}_\mathrm{B}}} \tag{3.62}$$

Substituindo todos os valores chegamos à expressão de forma fechada da pdf de $\gamma_{\mathrm{B},s}$:

$$\begin{aligned} f_{\gamma_{\mathrm{B},s}}(x) =& N_\mathrm{A} \sum_{S_k \in S} \alpha_k x^{\beta_k} e^{\frac{-\delta_k x}{\bar{\gamma}_\mathrm{B}}} \left[\sum_{l_\mathrm{B}=1}^{L_\mathrm{B}} \left[\frac{\varepsilon_{l_\mathrm{B}}(l_\mathrm{B}-1)}{(l_\mathrm{B}-1)!} x^{l_\mathrm{B}-2} e^{\frac{-x}{\bar{\gamma}_\mathrm{B}}} - \frac{\varepsilon_{l_\mathrm{B}}}{(l_\mathrm{B}-1)!\bar{\gamma}_\mathrm{B}} x^{l_\mathrm{B}-1} e^{\frac{-x}{\bar{\gamma}_\mathrm{B}}} \right] \right. \\ & \left. - \sum_{l_\mathrm{B}=L_\mathrm{B}+1}^{N_\mathrm{B}} \varepsilon_{l_\mathrm{B}} e^{\frac{-l_\mathrm{B} x}{L_\mathrm{B}\bar{\gamma}_\mathrm{B}}} \frac{l_\mathrm{B}}{L_\mathrm{B}\bar{\gamma}_\mathrm{B}} \right] \end{aligned} \tag{3.63}$$

3.1.2 MRC em Eve

Como Eve é afetada tanto por ruído quanto por sinais interferentes, o sinal recebido será escrito da seguinte maneira:

$$\mathbf{y}_\mathrm{E} = \sqrt{P}\mathbf{h}_{\mathrm{AE},s} x + \sum_{i=1}^{M} \sqrt{\bar{\gamma}_i}\mathbf{h}_\mathrm{i} i + \mathbf{n}_\mathrm{E}, \tag{3.64}$$

P denota a potência de transmissão de Alice. $\mathbf{h}_{\mathrm{AE},s}$ é o vetor, de dimensão $N_\mathrm{E} \times 1$, dos coeficiente do canal entre Eve e a antena selecionada em Alice(equivalendo a um sistema

SIMO). x é o sinal transmitido de potência unitária. $\mathbf{h}_{\mathrm{i}}$ é o vetor de canal, de dimensão $N_{\mathrm{E}} \times 1$, entre Eve e o i-ésimo sinal interferente. $\bar{\gamma}_i$ é a potência do i-ésimo sinal interferente. i é o sinal interferente de potência unitária. $\mathbf{n}_{\mathrm{E}}$ é o vetor AWGN em Eve, de dimensão $N_{\mathrm{E}} \times 1$, com componentes de variância unitária. O sinal y_{E} na saída do combinador MRC de Eve é dado por(definido na seção (2.4.4)):

$$y_{\mathrm{E}} = \frac{\mathbf{h}_{\mathrm{AE},s}{}^{H}}{||\mathbf{h}_{\mathrm{AE},s}||}\mathbf{y}_{\mathrm{E}} \tag{3.65}$$

Onde $\frac{\mathbf{h}_{\mathrm{AE},s}{}^{H}}{||\mathbf{h}_{\mathrm{AE},s}||}$ é definido por:

$$\begin{aligned} &\frac{\mathbf{h}_{\mathrm{AE},s}{}^{H}}{||\mathbf{h}_{\mathrm{AE},s}||} \\ &= \left(\frac{\left(h^1_{\mathrm{AE},s}\right)^*}{||\mathbf{h}_{\mathrm{AE},s}||}, \frac{\left(h^2_{\mathrm{AE},s}\right)^*}{||\mathbf{h}_{\mathrm{AE},s}||}, ..., \frac{\left(h^{N_{\mathrm{E}}}_{\mathrm{AE},s}\right)^*}{||\mathbf{h}_{\mathrm{AE},s}||} \right) \end{aligned} \tag{3.66}$$

Então:

$$\begin{aligned} y_{\mathrm{E}} &= \sqrt{P}\frac{\mathbf{h}^H_{\mathrm{AE},s}}{||\mathbf{h}_{\mathrm{AE},s}||}\mathbf{h}_{\mathrm{AE},s}x + \sum_{i=1}^{M}\sqrt{\bar{\gamma}_i}\frac{\mathbf{h}^H_{\mathrm{AE},s}}{||\mathbf{h}_{\mathrm{AE},s}||}\mathbf{h}_i\, i + \frac{\mathbf{h}_{\mathrm{AE},s}{}^{H}}{||\mathbf{h}_{\mathrm{AE},s}||}\mathbf{n}_{\mathrm{E}} \\ &= \sqrt{P}||\mathbf{h}_{\mathrm{AE},s}||x + \sum_{i=1}^{M}\sqrt{\bar{\gamma}_i}\bar{h}_i\, i + \frac{\mathbf{h}_{\mathrm{AE},s}{}^{H}}{||\mathbf{h}_{\mathrm{AE},s}||}\mathbf{n}_{\mathrm{E}} \end{aligned} \tag{3.67}$$

O último termo $\frac{\mathbf{h}_{\mathrm{AE},s}{}^{H}}{||\mathbf{h}_{\mathrm{AE},s}||}\mathbf{n}_{\mathrm{E}}$ é um escalar:

$$\begin{aligned} \frac{\mathbf{h}_{\mathrm{AE},s}{}^{H}}{||\mathbf{h}_{\mathrm{AE},s}||}\mathbf{n}_{\mathrm{E}} &= \left(\frac{\left(h^1_{\mathrm{AE},s}\right)^*}{||\mathbf{h}_{\mathrm{AE},s}||}, \frac{\left(h^2_{\mathrm{AE},s}\right)^*}{||\mathbf{h}_{\mathrm{AE},s}||}, ..., \frac{\left(h^{N_{\mathrm{E}}}_{\mathrm{AE},s}\right)^*}{||\mathbf{h}_{\mathrm{AE},s}||} \right) \begin{pmatrix} n^1_{\mathrm{E}} \\ n^2_{\mathrm{E}} \\ \vdots \\ n^{N_{\mathrm{E}}}_{\mathrm{E}} \end{pmatrix} \\ &= \frac{\left(h^1_{\mathrm{AE},s}\right)^* n^1_{\mathrm{E}}}{||\mathbf{h}_{\mathrm{AE},s}||} + \frac{\left(h^2_{\mathrm{AE},s}\right)^* n^2_{\mathrm{E}}}{||\mathbf{h}_{\mathrm{AE},s}||} + ... + \frac{\left(h^{N_{\mathrm{E}}}_{\mathrm{AE},s}\right)^* n^{N_{\mathrm{E}}}_{\mathrm{E}}}{||\mathbf{h}_{\mathrm{AE},s}||} \\ &= \frac{1}{||\mathbf{h}_{\mathrm{AE},s}||}\left(\left(h^1_{\mathrm{AE},s}\right)^* n^1_{\mathrm{E}} + \left(h^2_{\mathrm{AE},s}\right)^* n^2_{\mathrm{E}} + ... + \left(h^{N_{\mathrm{E}}}_{\mathrm{AE},s}\right)^* n^{N_{\mathrm{E}}}_{\mathrm{E}} \right) \end{aligned} \tag{3.68}$$

E a distribuição de $\frac{\mathbf{h}_{\mathrm{AE},s}{}^{H}}{||\mathbf{h}_{\mathrm{AE},s}||}\mathbf{n}_{\mathrm{E}}$ é a mesma de um n^k_{E} qualquer (fato obtido através do

Lema 9, da **Definição 13**, do **Lema 11** e do do **Lema 26**):

$$
\begin{aligned}
& n_{\mathrm{E}}^{k} \sim \mathscr{CN}(0,1)\ ,\ \forall k : 1 \leq k \leq N_{\mathrm{E}} \qquad (3.69)\\
& \implies \left(h_{\mathrm{AE},s}^{k}\right)^{*} n_{\mathrm{E}}^{k} \sim \mathscr{CN}(0, |h_{\mathrm{AE},s}^{k}|^{2})\\
& \implies \left(\left(h_{\mathrm{AE},s}^{1}\right)^{*} n_{\mathrm{E}}^{1} + \left(h_{\mathrm{AE},s}^{2}\right)^{*} n_{\mathrm{E}}^{2} + \ldots + \left(h_{\mathrm{AE},s}^{N_{\mathrm{E}}}\right)^{*} n_{\mathrm{E}}^{N_{\mathrm{E}}}\right) \sim \mathscr{CN}\left(0, \left(|h_1|^2 + |h_2|^2 + \ldots + |h_N|^2\right)\right)\\
& \implies \left(\left(h_{\mathrm{AE},s}^{1}\right)^{*} n_{\mathrm{E}}^{1} + \left(h_{\mathrm{AE},s}^{2}\right)^{*} n_{\mathrm{E}}^{2} + \ldots + \left(h_{\mathrm{AE},s}^{N_{\mathrm{E}}}\right)^{*} n_{\mathrm{E}}^{N_{\mathrm{E}}}\right) \sim \mathscr{CN}\left(0, ||\mathbf{h}_{\mathrm{AE},s}||^{2}\right)\\
& \implies \frac{1}{||\mathbf{h}_{\mathrm{AE},s}||}\left(\left(h_{\mathrm{AE},s}^{1}\right)^{*} n_{\mathrm{E}}^{1} + \left(h_{\mathrm{AE},s}^{2}\right)^{*} n_{\mathrm{E}}^{2} + \ldots + \left(h_{\mathrm{AE},s}^{N_{\mathrm{E}}}\right)^{*} n_{\mathrm{E}}^{N_{\mathrm{E}}}\right) \sim \mathscr{CN}\left(0, \frac{1}{||\mathbf{h}_{\mathrm{AE},s}||^{2}} ||\mathbf{h}_{\mathrm{AE},s}||^{2}\right)\\
& \implies \frac{1}{||\mathbf{h}_{\mathrm{AE},s}||}\left(\left(h_{\mathrm{AE},s}^{1}\right)^{*} n_{\mathrm{E}}^{1} + \left(h_{\mathrm{AE},s}^{2}\right)^{*} n_{\mathrm{E}}^{2} + \ldots + \left(h_{\mathrm{AE},s}^{N_{\mathrm{E}}}\right)^{*} n_{\mathrm{E}}^{N_{\mathrm{E}}}\right) \sim \mathscr{CN}\left(0, 1\right)\\
& \implies \frac{\mathbf{h}_{\mathrm{AE},s}{}^{H}}{||\mathbf{h}_{\mathrm{AE},s}||}\mathbf{n}_{\mathrm{E}} \sim \mathscr{CN}(0,1)
\end{aligned}
$$

Logo a potência de $\frac{\mathbf{h}_{\mathrm{AE},s}{}^{H}}{||\mathbf{h}_{\mathrm{AE},s}||}\mathbf{n}_{\mathrm{E}}$ é:

$$
\begin{aligned}
\mathrm{E}\left[\left|\frac{\mathbf{h}_{\mathrm{AE},s}{}^{H}}{||\mathbf{h}_{\mathrm{AE},s}||}\mathbf{n}_{\mathrm{E}}\right|^{2}\right] &= \mathrm{Var}\left(\frac{\mathbf{h}_{\mathrm{AE},s}{}^{H}}{||\mathbf{h}_{\mathrm{AE},s}||}\mathbf{n}_{\mathrm{E}}\right) \qquad (3.70)\\
&= 1
\end{aligned}
$$

O termo dentro do somatório dos sinais interferentes $\frac{\mathbf{h}_{\mathrm{AE},s}{}^{H}}{||\mathbf{h}_{\mathrm{AE},s}||}\mathbf{h}_i$ é um escalar($\forall i : 1 \leq i \leq M$):

$$
\begin{aligned}
\frac{\mathbf{h}_{\mathrm{AE},s}{}^{H}}{||\mathbf{h}_{\mathrm{AE},s}||}\mathbf{h}_i &= \left(\frac{\left(h_{\mathrm{AE},s}^{1}\right)^{*}}{||\mathbf{h}_{\mathrm{AE},s}||}, \frac{\left(h_{\mathrm{AE},s}^{2}\right)^{*}}{||\mathbf{h}_{\mathrm{AE},s}||}, \ldots, \frac{\left(h_{\mathrm{AE},s}^{N_{\mathrm{E}}}\right)^{*}}{||\mathbf{h}_{\mathrm{AE},s}||}\right)\begin{pmatrix} h_i^1 \\ h_i^2 \\ \vdots \\ h_i^{N_{\mathrm{E}}} \end{pmatrix} \qquad (3.71)\\
&= \frac{\left(h_{\mathrm{AE},s}^{1}\right)^{*} h_i^1}{||\mathbf{h}_{\mathrm{AE},s}||} + \frac{\left(h_{\mathrm{AE},s}^{2}\right)^{*} h_i^2}{||\mathbf{h}_{\mathrm{AE},s}||} + \ldots + \frac{\left(h_{\mathrm{AE},s}^{N_{\mathrm{E}}}\right)^{*} h_i^{N_{\mathrm{E}}}}{||\mathbf{h}_{\mathrm{AE},s}||}\\
&= \frac{1}{||\mathbf{h}_{\mathrm{AE},s}||}\left(\left(h_{\mathrm{AE},s}^{1}\right)^{*} h_i^1 + \left(h_{\mathrm{AE},s}^{2}\right)^{*} h_i^2 + \ldots + \left(h_{\mathrm{AE},s}^{N_{\mathrm{E}}}\right)^{*} h_i^{N_{\mathrm{E}}}\right)\\
&= \bar{h}_i
\end{aligned}
$$

Pela simetria da expressão acima e pelo fato de todas as variáveis serem i.i.d., teremos que a distribuição de $\frac{\mathbf{h}_{\mathrm{AE},s}{}^{H}}{||\mathbf{h}_{\mathrm{AE},s}||}\mathbf{h}_i = \bar{h}_i$ é a mesma de um h_i^k qualquer:

$$h_i^k \sim \mathscr{CN}(0,1)\ ,\ \forall i : 1 \leq i \leq M \text{ e } \forall k : 1 \leq k \leq N_{\mathrm{E}} \tag{3.72}$$
$$\implies \left(\frac{\mathbf{h}_{\mathrm{AE},s}{}^H}{||\mathbf{h}_{\mathrm{AE},s}||} \mathbf{h}_i = \bar{h}_i \right) \sim \mathscr{CN}(0,1)$$

A potência de $\sum_{i=1}^{M} \sqrt{\bar{\gamma}_i}\bar{h}_i\, i$ é:

$$\begin{aligned} \mathrm{E}\left[\left| \sum_{i=1}^{M} \sqrt{\bar{\gamma}_i}\bar{h}_i\, i \right|^2 \right] &= \sum_{i=1}^{M} \bar{\gamma}_i \left|\bar{h}_i\right|^2 1\mathrm{E}\left[|i|^2 \right] \\ &= \sum_{i=1}^{M} \bar{\gamma}_i \left|\bar{h}_i\right|^2 \\ &= \gamma_{\mathrm{I}} \end{aligned}$$

A potência de $\sqrt{P}||\mathbf{h}_{\mathrm{AE},s}||x$ é:

$$\begin{aligned} \mathrm{E}\left[\left| \sqrt{P}||\mathbf{h}_{\mathrm{AE},s}||x \right|^2 \right] &= P||\mathbf{h}_{\mathrm{AE},s}||^2 1\mathrm{E}\left[|x|^2 \right] \\ &= P||\mathbf{h}_{\mathrm{AE},s}||^2 \\ &= \gamma_{\mathrm{E},s} \end{aligned}$$

Onde $\|\,.\,\|$ é a norma de Frobenius e $(\,.\,)^H$ é o conjugado transposto. $\bar{h}_i = \frac{\mathbf{h}_{\mathrm{AE},s}^H}{||\mathbf{h}_{\mathrm{AE},s}||}\mathbf{h}_i$. Então, a SINR na saída de Eve será:

$$\Upsilon_{\mathrm{E},s} = \frac{\gamma_{\mathrm{E},s}}{\gamma_{\mathrm{I}} + 1}, \tag{3.73}$$

onde $\gamma_{\mathrm{E},s} = \bar{\gamma}_{\mathrm{E}}||\mathbf{h}_{\mathrm{AE},s}||^2$, $\gamma_{\mathrm{I}} = \sum_{i=1}^{M} \bar{\gamma}_i|\bar{h}_i|^2$, e $\bar{\gamma}_{\mathrm{E}} = P$.

O objetivo desta seção é obter uma solução de forma fechada da pdf de $\Upsilon_{\mathrm{E},s} = f_{\frac{\gamma_{\mathrm{E},s}}{\gamma_{\mathrm{I}}+1}}(x)$, que de acordo com a **Definição 8** , será:

$$f_{\frac{\gamma_{\mathrm{E},s}}{\gamma_{\mathrm{I}}+1}}(x) = \frac{\partial}{\partial x}\left[F_{\frac{\gamma_{\mathrm{E},s}}{\gamma_{\mathrm{I}}+1}}(x) \right]. \tag{3.74}$$

Para encontrar $F_{\frac{\gamma_{\mathrm{E},s}}{\gamma_{\mathrm{I}}+1}}(x)$ vamos utilizar o **Lema 25**:

$$F_{\frac{\gamma_{\mathrm{E},s}}{\gamma_I+1}}(x) = P(\gamma_{E,s} \geq x(\gamma_I+1), (\gamma_I+1) < 0) \tag{3.75}$$
$$+ P(\gamma_{E,s} \leq x(\gamma_I+1), (\gamma_I+1) > 0)$$
$$= P(\gamma_{E,s} \leq x(\gamma_I+1), (\gamma_I+1) > 0)$$

$P(\gamma_{E,s} \geq x(\gamma_I+1), (\gamma_I+1) < 0) = 0$ pois $\gamma_I > 0 \implies (\gamma_I+1) < 0$ é impossível, ou seja, a probabilidade é zero.

Logo, baseado no **Lema 25**, $P(\gamma_{E,s} \leq x(\gamma_I+1), (\gamma_I+1) > 0)$ será:

$$F_{\frac{\gamma_{\mathrm{E},s}}{\gamma_I+1}}(x) = P(\gamma_{E,s} \leq x(\gamma_I+1), (\gamma_I+1) > 0) \tag{3.76}$$
$$= \int_0^\infty \left[\int_{-\infty}^{xz} f_{\gamma_{E,s}}(y)dy \right] f_{\gamma_I+1}(z)dz$$
$$= \int_0^\infty F_{\gamma_{E,s}}(xz) f_{\gamma_I+1}(z)dz$$

Assim, $F_{\frac{\gamma_{\mathrm{E},s}}{\gamma_I+1}}(x)$ será:

$$F_{\frac{\gamma_{\mathrm{E},s}}{\gamma_I+1}}(x) = \int_0^\infty F_{\gamma_{\mathrm{E},s}}(xz) f_{\gamma_I+1}(z)dz \tag{3.77}$$

Substituindo (3.77) em (3.74), teremos então a expressão para $f_{\frac{\gamma_{\mathrm{E},s}}{\gamma_I+1}}(x)$:

$$f_{\frac{\gamma_{\mathrm{E},s}}{\gamma_I+1}}(x) = \frac{\partial}{\partial x} \left[\int_0^\infty F_{\gamma_{\mathrm{E},s}}(xz) f_{\gamma_I+1}(z)dz \right]. \tag{3.78}$$

onde $F_{\gamma_{\mathrm{E},s}}(z)$ é a cdf da SNR da saída de Eve. $f_{\gamma_I+1}(z)$ é a pdf de γ_I mais o ruído. Vamos agora calcular essas duas funções.

3.1.2.1 Derivação da CDF de Eve

A SNR da saída de Eve $\gamma_{\mathrm{E},s}$, calculada na sessão anterior, é:

$$\gamma_{\mathrm{E},s} = \bar{\gamma}_{\mathrm{E}} ||\mathbf{h}_{\mathrm{AE},s}||^2 = \bar{\gamma}_{\mathrm{E}} \sum_{i=1}^{N_{\mathrm{E}}} |\mathrm{h}^i_{\mathrm{AE},s}|^2 \tag{3.79}$$

Como cada $\mathrm{h}^i_{\mathrm{AE},s}$ é um número complexo, seus quadrados serão a soma dos quadrados de sua parte imaginária com sua parte real, ou seja:

$$|\mathrm{h}^i_{\mathrm{AE},s}|^2 = |\,\mathrm{Re}(\mathrm{h}^i_{\mathrm{AE},s})|^2 + |\,\mathrm{Im}(\mathrm{h}^i_{\mathrm{AE},s})|^2 \tag{3.80}$$

Logo (3.79) pode ser escrita da seguinte maneira:

$$\begin{aligned}\gamma_{\mathrm{E},s} &= \bar{\gamma}_{\mathrm{E}} \sum_{i=1}^{N_{\mathrm{E}}} |\mathrm{h}^i_{\mathrm{AE},s}|^2 \\ &= \bar{\gamma}_{\mathrm{E}} \sum_{i=1}^{N_{\mathrm{E}}} |\,\mathrm{Re}(\mathrm{h}^i_{\mathrm{AE},s})|^2 + |\,\mathrm{Im}(\mathrm{h}^i_{\mathrm{AE},s})|^2\end{aligned} \tag{3.81}$$

Utilizando a notação da **Definição 24**, podemos escrever:

$$\begin{aligned}\gamma_{\mathrm{E},s} &= \bar{\gamma}_{\mathrm{E}} \sum_{i=1}^{N_{\mathrm{E}}} |\,\mathrm{Re}(\mathrm{h}^i_{\mathrm{AE},s})|^2 + |\,\mathrm{Im}(\mathrm{h}^i_{\mathrm{AE},s})|^2 \\ &= \bar{\gamma}_{\mathrm{E}} \sum_{i=1}^{2N_{\mathrm{E}}} |\,\mathrm{Parte}(\mathrm{h}^i_{\mathrm{AE},s})_{\mathrm{Re,Im}}|^2\end{aligned} \tag{3.82}$$

Para chegar na expressão equivalente ao da distribuição Qui-quadrado(**Lema 15**), basta fazermos as seguintes manipulações algébrica:

$$\begin{aligned}\gamma_{\mathrm{E},s} &= \bar{\gamma}_{\mathrm{E}} \sum_{i=1}^{2N_{\mathrm{E}}} |\,\mathrm{Parte}(\mathrm{h}^i_{\mathrm{AE},s})|^2 \\ &= \sum_{i=1}^{2N_{\mathrm{E}}} |\sqrt{\bar{\gamma}_{\mathrm{E}}}\,\mathrm{Parte}(\mathrm{h}^i_{\mathrm{AE},s})_{\mathrm{Re,Im}}|^2 \\ &= \sum_{i=1}^{2N_{\mathrm{E}}} |\sqrt{\bar{\gamma}_{\mathrm{E}}}\,\mathrm{Parte}(\mathrm{h}^i_{\mathrm{AE},s})_{\mathrm{Re,Im}}|^2 \\ &= \sum_{i=1}^{2N_{\mathrm{E}}} \left(\sqrt{\bar{\gamma}_{\mathrm{E}}}\,\mathrm{Parte}(\mathrm{h}^i_{\mathrm{AE},s})_{\mathrm{Re,Im}}\right)^2 \\ &= \sum_{i=1}^{2N_{\mathrm{E}}} x_i^2\end{aligned} \tag{3.83}$$

Onde:

$$x_i \equiv \sqrt{\bar{\gamma}_{\mathrm{E}}}\,\mathrm{Parte}(\mathrm{h}^i_{\mathrm{AE},s})_{\mathrm{Re,Im}} \tag{3.84}$$

Dado o fato que $\mathbf{h}_{\mathrm{AE},s}$ representa um canal *Rayleigh* puro e levando em consideração a **Definição 16** da pdf Normal , e as características do canal *Rayleigh* apresentadas na seção (2.2), teremos que para qualquer i:

$$\text{Parte}(\text{h}^i_{\text{AE},s})_{\text{Re,Im}} \sim \mathcal{N}(0,1/2) \implies \text{pdf}\left(\text{Parte}(\text{h}^i_{\text{AE},s})_{\text{Re,Im}}\right) = \frac{1}{\sqrt{\pi}} e^{-p^2} \tag{3.85}$$

Onde p representa uma variável $\text{Parte}(\text{h}^i_{\text{AE},s})_{\text{Re,Im}}$ qualquer.

Utilizando o **Lema 9** da técnica de transformação da pdf e que $x_i = \sqrt{\bar{\gamma}_\text{E}}\, p$, poderemos definir $g(p) = \sqrt{\bar{\gamma}_\text{E}}\, p$ e denotando $v = g(p)$ teremos que:

$$\begin{aligned} \text{pdf}(x_i) = \text{pdf}(g(p)) = f_V(v) &= \left| \frac{d}{dv}\left[g^{-1}(v)\right] \right| \frac{1}{\sqrt{\pi}} e^{-\left(g^{-1}(v)\right)^2} \\ f_V(v) &= \left| \frac{d}{dv}\left[v/\sqrt{\bar{\gamma}_\text{E}}\right] \right| \frac{1}{\sqrt{\pi}} e^{-\frac{v^2}{\bar{\gamma}_\text{E}}} \\ f_V(v) &= \frac{1}{\sqrt{\bar{\gamma}_\text{E}}} \frac{1}{\sqrt{\pi}} e^{-\frac{v^2}{\bar{\gamma}_\text{E}}} \end{aligned} \tag{3.86}$$

Fazendo uma pequena manipulação algébrica para comparar com a expressão (2.81) da pdf geral da distribuição Normal:

$$\begin{aligned} \text{pdf}(x_i) = f_V(v) &= \frac{1}{\sqrt{\bar{\gamma}_\text{E}}} \frac{1}{\sqrt{\pi}} e^{-\frac{v^2}{\bar{\gamma}_\text{E}}} \\ f_V(v) &= \frac{1}{\sqrt{2\pi\left(\frac{\bar{\gamma}_\text{E}}{2}\right)}} e^{-\frac{v^2}{2\left(\frac{\bar{\gamma}_\text{E}}{2}\right)}} \end{aligned} \tag{3.87}$$

Então, podemos concluir que:

$$\text{var}(x_i) = \frac{\bar{\gamma}_\text{E}}{2} \tag{3.88}$$

$$\text{E}[x_i] = 0 \tag{3.89}$$

Assim, baseando-se na definição da distribuição Qui-quadrado no **Lema 15** podemos escrever a cdf de $\gamma_{\text{E},s}$ através da substituição dos devidos valores em (2.102) do **Lema 15**. Mudando a notação da variável y pela variável z, mudando a notação da variável k pela variável u, substituindo a variância σ^2 pelo seu valor calculado anteriormente $\sigma^2 = \frac{\bar{\gamma}_\text{E}}{2}$ e fazendo a substituição do valor de n calculado como $n = 2N_\text{E}$:

$$F_{\gamma_{\text{E},s}}(z) = 1 - e^{-\frac{z}{\bar{\gamma}_\text{E}}} \sum_{u=0}^{N_\text{E}-1} \frac{1}{u!} \left(\frac{z}{\bar{\gamma}_\text{E}}\right)^u. \tag{3.90}$$

3.1.2.2 *Derivação da PDF de γ_I mais o ruído*

Agora vamos utilizar o método do **Lema 27** para calcular a pdf de γ_{I}, cuja expressão inicial é:

$$\gamma_{\mathrm{I}} = \sum_{i=1}^{M} \bar{\gamma}_i |\bar{h}_i|^2 \tag{3.91}$$

Para tanto, iremos definir uma matriz $\mathbf{H}$, que possua o número de elementos igual à M, tal que $M = r \times t$, onde $\{r,t\} \subset \mathbb{Z}^+$. A definição da matriz $\mathbf{H}$ será dada por

$$\mathbf{H} \equiv \begin{cases} \{\mathrm{H}_i = \sqrt{\bar{\gamma}_i}\,\bar{h}_i\}_{i=1}^{M} \in \mathbf{H}_{r\times t} \ : \ r \times t = M \ , \ \forall \{r,t\} \subset \mathbb{Z}^+ \\ \text{onde, } \{\mathrm{H}_i\} \text{representa um elemento qualquer de } \mathbf{H} \\ \text{e, } r \times t \text{ representa as dimensões de } \mathbf{H} \ . \end{cases} \tag{3.92}$$

Sem perda de generalidade, vamos definir $\mathbf{H}$ com $r = M$ e $t = 1$

$$\mathbf{H} = \mathbf{H}_{M\times 1} = \begin{pmatrix} \sqrt{\bar{\gamma}_1}\,\bar{h}_1 \\ \sqrt{\bar{\gamma}_2}\,\bar{h}_2 \\ \vdots \\ \sqrt{\bar{\gamma}_{M-1}}\,\bar{h}_{M-1} \\ \sqrt{\bar{\gamma}_M}\,\bar{h}_M \end{pmatrix} \tag{3.93}$$

Logo, vec$\{\mathbf{H}\}$, que chamaremos de $\mathbf{h}$, será dado por

$$\mathrm{vec}\{\mathbf{H}\} = \mathbf{H} = \mathbf{h} = \begin{pmatrix} \sqrt{\bar{\gamma}_1}\,\bar{h}_1 \\ \sqrt{\bar{\gamma}_2}\,\bar{h}_2 \\ \vdots \\ \sqrt{\bar{\gamma}_{M-1}}\,\bar{h}_{M-1} \\ \sqrt{\bar{\gamma}_M}\,\bar{h}_M \end{pmatrix} \tag{3.94}$$

A norma de Frobenius de $\mathbf{H}$ é por definição

$$\| \mathbf{H} \| = \sqrt{\mathrm{tr}(\mathbf{H}^{\dagger}\mathbf{H})} \tag{3.95}$$

Logo, $\|\mathbf{H}\|$ será igual à

$$\|\mathbf{H}\| = \sqrt{\text{tr}(\mathbf{H}^\dagger\mathbf{H})} = \sqrt{\text{tr}(\mathbf{h}^\dagger\mathbf{h})} \tag{3.96}$$

Como $\mathbf{h}^\dagger\mathbf{h}$ tem dimensão 1×1, o traço será igual à $\mathbf{h}^\dagger\mathbf{h}$. Assim, teremos

$$\|\mathbf{H}\| = \sqrt{\mathbf{h}^\dagger\mathbf{h}} \tag{3.97}$$

Agora podemos definir $\gamma_\mathbf{I}$ em função de $\mathbf{H}$:

$$\gamma_\mathbf{I} = \|\mathbf{H}\|^2 = \mathbf{h}^\dagger\mathbf{h} \tag{3.98}$$

Basta agora encontrar os autovalores σ_i da matriz de covariância $\mathbf{R}$, que será

$$\mathbf{R} = \text{cov}(\mathbf{H}) = \text{cov}(\text{vec}(\mathbf{H})) = \mathbf{E}\left[\text{vec}(\mathbf{H})\text{vec}(\mathbf{H})^\dagger\right] = \mathbf{E}\left[\mathbf{h}\mathbf{h}^\dagger\right] \tag{3.99}$$

Assim, temos que $\mathbf{R}$ será

$$\mathbf{R} = \mathbf{E}\left[\mathbf{h}\mathbf{h}^\dagger\right] \tag{3.100}$$

Sabendo que um elemento qualquer $h \in \mathbf{h}$, será da forma $\{h_i = \sqrt{\bar{\gamma}_i}\,\bar{h}_i\}_{i=1}^{M}$. Então, para encontrar todos os elementos de $\mathbf{R}$ temos que analisar apenas dois casos:

$$R \in \mathbf{R} \equiv \begin{cases} R_{i,j} = \mathbf{E}\left\{\sqrt{\bar{\gamma}_i}\sqrt{\bar{\gamma}_j}\,\bar{h}_i\bar{h}_j^*\right\}_{i=j} & \text{ou seja, na diagonal principal de } \mathbf{R} \\ R_{i,j} = \mathbf{E}\left\{\sqrt{\bar{\gamma}_i}\sqrt{\bar{\gamma}_j}\,\bar{h}_i\bar{h}_j^*\right\}_{i\neq j} & \text{ou seja, fora da diagonal principal de } \mathbf{R} \end{cases} \tag{3.101}$$

Precisamos primeiramente calcular o valor esperado de $\bar{h}_i\bar{h}_j^*$ para os dois casos. No caso $i = j$, utilizando algumas equivalências entre diferentes distribuições de probabilidade encontradas no **Lema 16**, utilizando a **Definição 18** da distribuição exponencial e o fato que $\bar{h}_i \sim \mathscr{CN}(0,1)$ que foi provado na expressão (3.72), teremos que:

$$\begin{aligned} &\{\text{Re}(\bar{h}_i), \text{Im}(\bar{h}_i)\} \sim \mathscr{N}(0, 1/2) \implies \bar{h}_i \sim \mathscr{CN}(0,1) \implies \\ &\implies |\bar{h}_i| \sim \text{Rayleigh}(1/\sqrt{2}) \implies |\bar{h}_i|^2 \sim \text{Exp}(1) \implies 1\mathbf{E}\left\{|\bar{h}_i|^2\right\}_{i=1}^{M} \end{aligned} \tag{3.102}$$

Logo,

$$\mathbf{E}\left\{\sqrt{\bar{\gamma}_i}\sqrt{\bar{\gamma}_j}\,\bar{h}_i\bar{h}_j^*\right\}_{i=j} = \mathbf{E}\left\{\bar{\gamma}_i|\bar{h}_i|^2\right\}_{i=1}^{M} = \bar{\gamma}_i\,1\mathbf{E}\left\{|\bar{h}_i|^2\right\}_{i=1}^{M} = \{\bar{\gamma}_i\}_{i=1}^{M} \tag{3.103}$$

Para o caso $i \neq j$ basta utilizar o fato que que as variáveis $\bar{h}_i$ são i.i.d. Assim teremos:

$$\mathbf{E}\left\{\sqrt{\bar{\gamma}_i}\sqrt{\bar{\gamma}_j}\,\bar{h}_i\bar{h}_j^*\right\}_{i\neq j} = \sqrt{\bar{\gamma}_i}\sqrt{\bar{\gamma}_j}\,0\mathbf{E}\left\{\bar{h}_i\bar{h}_j^*\right\}_{i\neq j} \quad = \{0\}_{i\neq j} \tag{3.104}$$

Logo, $\mathbf{R}$ será:

$$\mathbf{R} = \operatorname{diag}\{\bar{\gamma}_1,\ldots,\bar{\gamma}_M\} = \begin{pmatrix} \bar{\gamma}_1 & & & & \\ & \bar{\gamma}_2 & & & \\ & & \ddots & & \\ & & & \bar{\gamma}_{M-1} & \\ & & & & \bar{\gamma}_M \end{pmatrix} \tag{3.105}$$

Para garantir que fizemos tudo certo, vamos confirmar o resultado de $\mathbf{R}$ com a seguinte equivalência demonstrada em (SHIU *et al.*, 2000):

$$\mathbf{h} = \mathbf{R}^{1/2}\mathbf{h}_W \tag{3.106}$$

Onde $\mathbf{h}_W$ é um vetor coluna de dimensão $M \times 1$ formado por variáveis aleatórias Gaussianas complexas circularmente simétricas que possuam matriz de covariância igual à identidade, logo i.i.d., ou seja, variáveis representantes de um canal com desvanecimento Rayleigh puro como realmente é no caso deste trabalho. $\mathbf{R}^{1/2}$ e $\mathbf{h}_W$ serão respectivamente:

$$\mathbf{R}^{1/2} = \operatorname{diag}\left\{\sqrt{\bar{\gamma}_1},\ldots,\sqrt{\bar{\gamma}_M}\right\} = \begin{pmatrix} \sqrt{\bar{\gamma}_1} & & & & \\ & \sqrt{\bar{\gamma}_2} & & & \\ & & \ddots & & \\ & & & \sqrt{\bar{\gamma}_{M-1}} & \\ & & & & \sqrt{\bar{\gamma}_M} \end{pmatrix} \tag{3.107}$$

$$\mathbf{h}_W = \begin{pmatrix} \bar{h}_1 \\ \bar{h}_2 \\ \vdots \\ \bar{h}_{M-1} \\ \bar{h}_M \end{pmatrix} \tag{3.108}$$

Portanto, concluímos que (3.105) está correto, pois comparando com (3.94) a expressão abaixo é verdadeira:

$$\mathbf{h} = \begin{pmatrix} \sqrt{\bar{\gamma}_1} & & & & \\ & \sqrt{\bar{\gamma}_2} & & & \\ & & \ddots & & \\ & & & \sqrt{\bar{\gamma}_{M-1}} & \\ & & & & \sqrt{\bar{\gamma}_M} \end{pmatrix} \begin{pmatrix} \bar{h}_1 \\ \bar{h}_2 \\ \vdots \\ \bar{h}_{M-1} \\ \bar{h}_M \end{pmatrix} \tag{3.109}$$

Como $\mathbf{R} = \text{diag}\{\bar{\gamma}_1, \ldots, \bar{\gamma}_M\}$, mas pela definição $\mathbf{R} = \mathbf{U}\Sigma\mathbf{U}^{\dagger}$((2.166) do **Lema 27**). Fazendo $\mathbf{U}$ como a matriz identidade de mesma dimensão, teremos de (2.166) do **Lema 27** que:

$$\mathbf{R} = \Sigma = \text{diag}\{\sigma_i\}_{i=1}^{M} = \text{diag}\{\bar{\gamma}_1, \ldots, \bar{\gamma}_M\} = \text{diag}\{\bar{\gamma}_i\}_{i=1}^{M} \tag{3.110}$$

Logo os autovalores de $\mathbf{R}$ serão:

$$\{\sigma_i\}_{i=1}^{M} \equiv \{\bar{\gamma}_i\}_{i=1}^{M} \tag{3.111}$$

Basta agora substituir os resultados nas expressões anteriormente calculadas no **Lema 27**. Assim, a transformada de Laplace da PDF de $\gamma_{\mathfrak{l}}$ será:

$$\psi(s) = \text{E}\{e^{-s\|\mathbf{H}\|^2}\} = \mathscr{L}\{f_{\gamma_{\mathfrak{l}}}\}(s) \tag{3.112}$$

A expressão geral de $\psi(s)$ calculada no **Lema 27** ficará:

$$\psi(s) = \prod_{i=1}^{M} \frac{1}{1+s\bar{\gamma}_i}, \qquad \text{ROC: } \mathbf{Re}(s) > \max_{\bar{\gamma}_i}\left(-\frac{1}{\bar{\gamma}_i}\right), \tag{3.113}$$

Para calcular a forma final da expressão precisamos lembrar que $\bar{\gamma}_i$ são os autovalores de $\mathbf{R}$, e $\widetilde{\bar{\gamma}}_i$ serão os autovalores distintos e não nulos de $\mathbf{R}$, onde $1 \leq t \leq M$ é a quantidade de autovalores distintos e não nulos de $\mathbf{R}$, e η_i é a multiplicidade de cada autovalor, tal que: $\sum_{i=1}^{t} \eta_i = M$. Assim, podemos rescrever (3.113) como:

$$\psi(s) = \prod_{i=1}^{t} \frac{1}{\left(1+s\widetilde{\bar{\gamma}}_i\right)^{\eta_i}} \tag{3.114}$$

E através da expansão por frações parciais(**Lema 24**):

$$\psi(s) = \sum_{i=1}^{t} \sum_{j=1}^{\eta_i} \frac{\Omega_{i,j}}{\left(1 + s\widetilde{\overline{\gamma}}_i\right)^j} = \mathscr{L}\{f_{\gamma}\}(s) \tag{3.115}$$

A pdf de γ, $f_{\gamma}(z)$, será portanto:

$$f_{\gamma}(z) = \sum_{i=1}^{t} \sum_{j=1}^{\eta_i} \frac{\Omega_{i,j}}{(j-1)!\widetilde{\overline{\gamma}}_i^j} z^{j-1} e^{-\frac{z}{\widetilde{\overline{\gamma}}_i}}, \tag{3.116}$$

Onde $\Omega_{i,j}$, calculado em (2.168) do **Lema 27**, será:

$$\Omega_{i,j} = \frac{1}{(\eta_i - j)!\widetilde{\overline{\gamma}}_i^{\eta_i - j}} \frac{\partial^{\eta_i - j}}{\partial s^{\eta_i - j}} \left[\prod_{k=1, k\neq i}^{t} \left(\frac{1}{1 + s\widetilde{\overline{\gamma}}_i} \right)^{\eta_k} \right]_{s=-\frac{1}{\widetilde{\overline{\gamma}}_i}}. \tag{3.117}$$

Podemos calcular $f_{\gamma_{+1}}(z)$ através das seguintes propriedades:

$$\text{Solução de } f_{\gamma_{+1}}(z) \iff \begin{cases} f_{\gamma_{+1}}(z) = f_{\gamma}(z-1) & \text{, consequência do } \textbf{Lema 28} \\ (1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k & \text{, expansão binomial(}\textbf{Lema 29}\text{)} \\ \text{simples substituições de variáveis} \end{cases} \tag{3.118}$$

Poderemos então obter $f_{\gamma+1}(z)$ como:

$$f_{\gamma_{+1}}(z) = \sum_{i=1}^{t} \sum_{j=1}^{\eta_i} \frac{\Omega_{i,j}}{(j-1)!\widetilde{\overline{\gamma}}_i^j} \sum_{k=1}^{j} \sum_{p=1}^{k} \binom{j-1}{k-1} \binom{k-1}{p-1} z^{p-1} e^{-\frac{z}{\widetilde{\overline{\gamma}}_i}}, \tag{3.119}$$

Para calcular a pdf de $\Upsilon_{\mathrm{E},s} = \frac{\gamma_{\mathrm{E},s}}{\gamma+1}$ basta substituir (3.90) e (3.119) em (3.78), e resolver a integral resultante através da utilização das seguintes propriedades:

$$\text{Solução de } f_{\frac{\gamma_{\mathrm{E},s}}{\gamma+1}} \iff \begin{cases} \Gamma(x) = \int_0^{\infty} s^{x-1} e^{-s} ds & \text{, função Gama(}\textbf{Definição 20}\text{)} \\ (1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k & \text{, expansão binomial(}\textbf{Lema 29}\text{)} \\ \text{manipulações algébricas simples} \end{cases} \tag{3.120}$$

Finalmente, a expressão em forma fechada da pdf de $\Upsilon_{\mathrm{E},s}$ é obtida como:

$$f_{\frac{\gamma_{\mathrm{E},s}}{\gamma_{\mathrm{I}}+1}}(x) = \sum_{i=1}^{t}\sum_{j=1}^{\eta_i}\Omega_{i,j}\sum_{k=1}^{j}\sum_{p=1}^{k}(-1)^{j-k}\sum_{u=0}^{N_{\mathrm{E}}-1} \times \sum_{q=0}^{u}\frac{\Gamma(p+q)\widetilde{\bar{\gamma}}_i^{p+q-j}}{(j-k)!(k-p)!(p-1)!(u-q)!q!} \times \left(\frac{x}{\bar{\gamma}_{\mathrm{E}}}\right)^{u} e^{-\frac{x}{\bar{\gamma}_{\mathrm{E}}}}\left[(p+q)\frac{\widetilde{\bar{\gamma}}_i}{\bar{\gamma}_{\mathrm{E}}}\left(1+\frac{x\widetilde{\bar{\gamma}}_i}{\bar{\gamma}_{\mathrm{E}}}\right)^{-p-q-1} + \frac{1}{\bar{\gamma}_{\mathrm{E}}}\left(1+\frac{x\widetilde{\bar{\gamma}}_i}{\bar{\gamma}_{\mathrm{E}}}\right)^{-p-q} - ux^{-1}\left(1+\frac{x\widetilde{\bar{\gamma}}_i}{\bar{\gamma}_{\mathrm{E}}}\right)^{-p-q}\right] \tag{3.121}$$

3.2 Desempenho de Sigilo

Nesta seção, iremos derivar as expressões das principais métricas de desempenho de sigilo, que serão:

- Capacidade de sigilo
- Probabilidade de interrupção de sigilo
- Probabilidade de interrupção de sigilo assintótica
  - Ganho de diversidade
  - Ganho de *array*
- Taxa de sigilo não nula

3.2.1 Capacidade de Sigilo

Como mostrado na seção (2.10.2), a capacidade do canal principal, entre Alice e Bob será $R_{\mathrm{B},s} = \log_2(1+\gamma_{\mathrm{B},s})$. E a capacidade do canal *wiretap*, entre Alice e Eve será $R_{\mathrm{E},s} = \log_2(1+\Upsilon_{\mathrm{E},s})$. Logo, a capacidade de sigilo pode ser definida como:

$$R_S = \begin{cases} R_{\mathrm{B},s} - R_{\mathrm{E},s}, & \gamma_{\mathrm{B},s} > \Upsilon_{\mathrm{E},s}, \\ 0, & \gamma_{\mathrm{B},s} \leq \Upsilon_{\mathrm{E},s}. \end{cases} \tag{3.122}$$

3.2.2 Probabilidade de Interrupção de Sigilo

No contexto deste trabalho, um evento de interrupção de sigilo ocorre quando o canal principal for interrompido ou quando Eve puder interceptar a troca de informações entre Alice e Bob. A probabilidade de interrupção de sigilo é uma ferramenta prática e viável para estimar

a segurança. Particularmente, a probabilidade de interrupção de sigilo pode ser definida como a probabilidade de R_S cair para um valor abaixo de um limiar definido por uma taxa R, sendo matematicamente expressa por:

$$P_s(R) = \Pr(R_S < R) \tag{3.123}$$

onde $\Pr(\,.\,)$ representa probabilidade.

De (3.123), podemos inferir que $\Pr(R_S < R)$ será a probabilidade de $(R_S = 0) < R$, quando $\gamma_{\mathrm{B},s} \leq \Upsilon_{\mathrm{E},s}$ ou a probabilidade de $(R_{\mathrm{B},s} - R_{\mathrm{E},s}) < R$, quando $\gamma_{\mathrm{B},s} > \Upsilon_{\mathrm{E},s}$. Logo, $P_s(R)$ poderá ser expressa da seguinte maneira:

$$\begin{aligned}
P_s(R) &= \Pr(R_S < R) \qquad (3.124)\\
&= \Pr\Big((R_{\mathrm{B},s} - R_{\mathrm{E},s} < R), (\gamma_{\mathrm{B},s} > \Upsilon_{\mathrm{E},s})\Big) + \Pr\Big((0 < R), (\gamma_{\mathrm{B},s} \leq \Upsilon_{\mathrm{E},s})\Big)\\
&= \Pr\left(R_{\mathrm{B},s} - R_{\mathrm{E},s} < R\right)\Pr\left(\gamma_{\mathrm{B},s} > \Upsilon_{\mathrm{E},s}\right) + \Pr\left(0 < R\right)\Pr\left(\gamma_{\mathrm{B},s} \leq \Upsilon_{\mathrm{E},s}\right)\\
&= \Pr\Big(\log_2\left(1+\gamma_{\mathrm{B},s}\right) - \log_2\left(1+\Upsilon_{\mathrm{E},s}\right) < R\Big)\Pr\left(\gamma_{\mathrm{B},s} > \Upsilon_{\mathrm{E},s}\right) + \Pr\left(0 < R\right)\Pr\left(\gamma_{\mathrm{B},s} \leq \Upsilon_{\mathrm{E},s}\right)\\
&= \Pr\left(\log_2\left(\frac{1+\gamma_{\mathrm{B},s}}{1+\Upsilon_{\mathrm{E},s}}\right) < R\right)\Pr\left(\gamma_{\mathrm{B},s} > \Upsilon_{\mathrm{E},s}\right) + 1\Pr\left(0 < R\right)\Pr\left(\gamma_{\mathrm{B},s} \leq \Upsilon_{\mathrm{E},s}\right)\\
&= \Pr\left(\frac{1+\gamma_{\mathrm{B},s}}{1+\Upsilon_{\mathrm{E},s}} < 2^R\right)\Pr\left(\gamma_{\mathrm{B},s} > \Upsilon_{\mathrm{E},s}\right) + \Pr\left(\gamma_{\mathrm{B},s} \leq \Upsilon_{\mathrm{E},s}\right)\\
&= \Pr\left(\frac{1+\gamma_{\mathrm{B},s}}{1+\frac{\gamma_{\mathrm{E},s}}{\gamma_{\mathrm{I}}+1}} < 2^R\right)\Pr\left(\gamma_{\mathrm{B},s} > \frac{\gamma_{\mathrm{E},s}}{\gamma_{\mathrm{I}}+1}\right) + \Pr\left(\gamma_{\mathrm{B},s} \leq \frac{\gamma_{\mathrm{E},s}}{\gamma_{\mathrm{I}}+1}\right)
\end{aligned}$$

Agora vamos resolver (3.124):

$$\begin{aligned}
P_s(R) &= \Pr(R_S < R) \qquad (3.125)\\
&= \Pr\left(\frac{1+\gamma_{\mathrm{B},s}}{1+\frac{\gamma_{\mathrm{E},s}}{\gamma_{\mathrm{I}}+1}} < 2^R\right)\Pr\left(\gamma_{\mathrm{B},s} > \frac{\gamma_{\mathrm{E},s}}{\gamma_{\mathrm{I}}+1}\right) + \Pr\left(\gamma_{\mathrm{B},s} \leq \frac{\gamma_{\mathrm{E},s}}{\gamma_{\mathrm{I}}+1}\right)\\
&= \Pr\left(\gamma_{\mathrm{B},s} < 2^R\left(1+\frac{\gamma_{\mathrm{E},s}}{\gamma_{\mathrm{I}}+1}\right) - 1\right)\Pr\left(\gamma_{\mathrm{B},s} > \frac{\gamma_{\mathrm{E},s}}{\gamma_{\mathrm{I}}+1}\right) + \Pr\left(\gamma_{\mathrm{B},s} \leq \frac{\gamma_{\mathrm{E},s}}{\gamma_{\mathrm{I}}+1}\right)\\
&= \underbrace{\Pr\left(\frac{\gamma_{\mathrm{E},s}}{\gamma_{\mathrm{I}}+1} < \gamma_{\mathrm{B},s} < 2^R\left(1+\frac{\gamma_{\mathrm{E},s}}{\gamma_{\mathrm{I}}+1}\right) - 1\right)}_{I_1} + \underbrace{\Pr\left(\gamma_{\mathrm{B},s} \leq \frac{\gamma_{\mathrm{E},s}}{\gamma_{\mathrm{I}}+1}\right)}_{I_2}.
\end{aligned}$$

Onde:

$$I_1 = \int_0^{\infty} \left[\int_{\frac{\gamma_{\mathrm{E},s}}{\gamma_1+1}}^{2^R\left(1+\frac{\gamma_{\mathrm{E},s}}{\gamma_1+1}\right)-1} f_{\gamma_{\mathrm{B},s}}(\gamma_{\mathrm{B},s}) d\gamma_{\mathrm{B},s} \right] f_{\frac{\gamma_{\mathrm{E},s}}{\gamma_1+1}} \left(\frac{\gamma_{\mathrm{E},s}}{\gamma_1+1} \right) d \left(\frac{\gamma_{\mathrm{E},s}}{\gamma_1+1} \right) \tag{3.126}$$
$$= \int_0^{\infty} \left[\int_y^{2^R(1+y)-1} f_{\gamma_{\mathrm{B},s}}(x) dx \right] f_{\frac{\gamma_{\mathrm{E},s}}{\gamma_1+1}}(y)\, d(y)$$

$$I_2 = \int_0^{\infty} \left[\int_0^{\frac{\gamma_{\mathrm{E},s}}{\gamma_1+1}} f_{\gamma_{\mathrm{B},s}}(\gamma_{\mathrm{B},s}) d\gamma_{\mathrm{B},s} \right] f_{\frac{\gamma_{\mathrm{E},s}}{\gamma_1+1}} \left(\frac{\gamma_{\mathrm{E},s}}{\gamma_1+1} \right) d \left(\frac{\gamma_{\mathrm{E},s}}{\gamma_1+1} \right) \tag{3.127}$$
$$= \int_0^{\infty} \left[\int_0^{y} f_{\gamma_{\mathrm{B},s}}(x) dx \right] f_{\frac{\gamma_{\mathrm{E},s}}{\gamma_1+1}}(y)\, d(y)$$

Então:

$$P_s(R) = I_1 + I_2 \tag{3.128}$$
$$= \int_0^{\infty} \left[\int_0^{y} f_{\gamma_{\mathrm{B},s}}(x) dx + \int_y^{2^R(1+y)-1} f_{\gamma_{\mathrm{B},s}}(x) dx \right] f_{\frac{\gamma_{\mathrm{E},s}}{\gamma_1+1}}(y)\, d(y)$$
$$= \int_0^{\infty} \left[\int_0^{2^R(1+y)-1} f_{\gamma_{\mathrm{B},s}}(x) dx \right] f_{\frac{\gamma_{\mathrm{E},s}}{\gamma_1+1}}(y)\, d(y)$$
$$= \int_0^{\infty} F_{\gamma_{\mathrm{B},s}}\left(2^R(1+y)-1\right) f_{\frac{\gamma_{\mathrm{E},s}}{\gamma_1+1}}(y)\, d(y)$$
$$= \int_0^{\infty} F_{\gamma_{\mathrm{B},s}}\left(2^R y + 2^R - 1\right) f_{\frac{\gamma_{\mathrm{E},s}}{\gamma_1+1}}(y)\, d(y) \tag{3.129}$$

Fazendo a mudança de variável de volta para x, chegamos à integral geradora da expressão de forma fechada de $P_s(R)$:

$$P_s(R) = \int_0^{\infty} F_{\gamma_{\mathrm{B},s}}(2^R x + 2^R - 1) f_{\frac{\gamma_{\mathrm{E},s}}{\gamma_1+1}}(x) dx. \tag{3.130}$$

Para resolver (3.130) basta substituir $f_{\frac{\gamma_{\mathrm{E},s}}{\gamma_1+1}}(x)$ e $F_{\gamma_{\mathrm{B},s}}$ por (3.121) e (3.54), e utilizar a definição de $\Psi(.,.,.)$. Onde $\Psi(.,.,.)$ denota a função de Tricomi(ou função hipergeométrica confluente), definida na **Definição 23** como:

$$\Psi(a,b,z) = \frac{1}{\Gamma(a)} \int_0^{\infty} e^{-zt} t^{a-1} (1+t)^{b-a-1} dt \tag{3.131}$$

Logo, a expressão de forma fechada da probabilidade de interrupção de sigilo para o esquema GSC será:

$$P_s(R) = \tag{3.132}$$
$$\sum_{S_k \in S} \alpha_k e^{\frac{-\delta_k(2^R-1)}{\bar{\gamma}_B}} \sum_{f=0}^{\beta_k} \binom{\beta_k}{f} (2^R-1)^{\beta_k - f} 2^{Rf} \sum_{i=1}^{t} \sum_{j=1}^{\eta_i} \Omega_{i,j}$$
$$\times \sum_{k=1}^{j} \sum_{p=1}^{k} (-1)^{j-k} \sum_{u=0}^{N_E-1} \sum_{q=0}^{u} \frac{\Gamma(p+q)\widetilde{\bar{\gamma}}_i^{p+q-j}}{(j-k)!(k-p)!(u-q)!(p-1)!q!}$$
$$\times \left(\frac{1}{\bar{\gamma}_E}\right)^u \left[\Psi\left(u+f+1, u+f+1-p-q, \frac{1}{\widetilde{\bar{\gamma}}_i} + \frac{\delta_k \bar{\gamma}_E 2^R}{\bar{\gamma}_B \widetilde{\bar{\gamma}}_i}\right)\right.$$
$$\times \Gamma(u+f+1)\left(\frac{\bar{\gamma}_E}{\widetilde{\bar{\gamma}}_i}\right)^{u+f} (p+q)$$
$$+ \Psi\left(u+f+1, u+f+2-p-q, \frac{1}{\widetilde{\bar{\gamma}}_i} + \frac{\delta_k \bar{\gamma}_E 2^R}{\bar{\gamma}_B \widetilde{\bar{\gamma}}_i}\right) \Gamma(u+f+1)$$
$$\left. \times \left(\frac{\bar{\gamma}_E}{\widetilde{\bar{\gamma}}_i}\right)^{u+f} \left(\frac{1}{\widetilde{\bar{\gamma}}_i}\right) - \Theta_1 \right]$$

Onde Θ_1 é:

$$\Theta_1 = \begin{cases} \Psi\left(u+f, u+f+1-p-q, \frac{1}{\widetilde{\bar{\gamma}}_i} + \frac{\delta_k \bar{\gamma}_E 2^R}{\bar{\gamma}_B \widetilde{\bar{\gamma}}_i}\right) \times \Gamma(u+f) \left(\frac{\bar{\gamma}_E}{\widetilde{\bar{\gamma}}_i}\right)^{u+f} u, & u \neq 0 \\ 0, & u = 0 \end{cases} \tag{3.133}$$

3.2.2.1 Simplificação da Probabilidade de interrupção de Sigilo para o Caso de Sinais Interferentes Iguais

Sinais interferentes iguais $\implies \bar{\gamma}_1 = \bar{\gamma}_2 = ... = \bar{\gamma}_M \implies j = M$.

$\Omega_{i,j}$, definido em (3.117), é dado por:

$$\Omega_{i,j} = \frac{1}{(\eta_i - j)! \widetilde{\bar{\gamma}}_i^{\eta_i - j}} \frac{\partial^{\eta_i - j}}{\partial s^{\eta_i - j}} \left[\prod_{k=1, k\neq i}^{t} \left(\frac{1}{1+s\widetilde{\bar{\gamma}}_k}\right)^{\eta_k}\right]_{s=-\frac{1}{\widetilde{\bar{\gamma}}_i}}. \tag{3.134}$$

Mas, como $\widetilde{\bar{\gamma}}_1, \widetilde{\bar{\gamma}}_2, \ldots \widetilde{\bar{\gamma}}_t$ são valores diferentes entre si(não repetidos) com multiplicidades $\eta_1, \eta_2, \ldots \eta_t$ e como todos os $\bar{\gamma}_i$'s são iguais isso implica que existe apenas um valor único de $\widetilde{\bar{\gamma}}_i = \bar{\gamma}_1$, e consequentemente $t = 1$. Se $t = 1 \implies i = 1$. Assim temos que $t = i = 1$. Além disso, $\sum_{i=1}^{t} \eta_i = M \implies \sum_{i=1}^{1} \eta_i = M \implies \eta_i = \eta_1 = M$. Como o j de $\Omega_{i,j}$ varia entre 1 e η_i para cada i, e como neste caso $i = 1$ e $\eta_i = \eta_1 = M \implies 1 \leq j \leq M$. Como o produtório em

(3.134) não se define para $t = 1$, o valor de $\Omega_{i,j}$ só se definirá para $j = M$, pois a derivada parcial desaparece e fica apenas o termo $\frac{1}{(\eta_i - j)!\widetilde{\bar{\gamma}}_i^{\eta_i - j}}$. Substituindo em (3.134) os valores de $\eta_i = M$ e $j = M$:

$$\Omega_{i,j} = \frac{1}{(\eta_i - j)!\bar{\gamma}_1^{\eta_i - j}} = \frac{1}{(M-M)!\bar{\gamma}_1^{M-M}} = \frac{1}{0!\bar{\gamma}_1^{0}} = 1 \tag{3.135}$$

Substituindo $\Omega_{i,j} = 1$, $t = 1$, $\eta_i = M$ e $j = M$ em (3.132), a expressão simplificada para a probabilidade de interrupção de sigilo no caso de sinais interferentes iguais será:

$$\begin{aligned} P_s(R) = & \qquad (3.136)\\ & \sum_{S_k \in S} \alpha_k e^{\frac{-\delta_k(2^R-1)}{\bar{\gamma}_B}} \sum_{f=0}^{\beta_k} \binom{\beta_k}{f} (2^R-1)^{\beta_k - f} 2^{Rf} \\ & \times \sum_{k=1}^{M} \sum_{p=1}^{k} (-1)^{M-k} \sum_{u=0}^{N_E-1} \sum_{q=0}^{u} \frac{\Gamma(p+q)\bar{\gamma}_1^{p+q-M}}{(M-k)!(k-p)!(u-q)!(p-1)!q!} \\ & \times \left(\frac{1}{\bar{\gamma}_E}\right)^u \left[\Psi\left(u+f+1, u+f+1-p-q, \frac{1}{\bar{\gamma}_1} + \frac{\delta_k \bar{\gamma}_E 2^R}{\bar{\gamma}_B \bar{\gamma}_1}\right) \right. \\ & \times \Gamma(u+f+1)\left(\frac{\bar{\gamma}_E}{\bar{\gamma}_1}\right)^{u+f}(p+q) \\ & + \Psi\left(u+f+1, u+f+2-p-q, \frac{1}{\bar{\gamma}_1} + \frac{\delta_k \bar{\gamma}_E 2^R}{\bar{\gamma}_B \bar{\gamma}_1}\right)\Gamma(u+f+1) \\ & \left. \times \left(\frac{\bar{\gamma}_E}{\bar{\gamma}_1}\right)^{u+f}\left(\frac{1}{\bar{\gamma}_1}\right) - \Theta_{1(\widetilde{\bar{\gamma}}_i = \bar{\gamma}_1)} \right] \end{aligned}$$

3.2.2.2 Simplificação da Probabilidade de interrupção de Sigilo para o Caso de Sinais Interferentes Distintos

Sinais interferentes distintos $\implies \{\widetilde{\bar{\gamma}}_1, \widetilde{\bar{\gamma}}_2, \ldots \widetilde{\bar{\gamma}}_t\} \equiv \{\bar{\gamma}_1, \bar{\gamma}_2, \ldots \bar{\gamma}_M\}$, onde os $\widetilde{\bar{\gamma}}$'s possuem valores diferentes com multiplicidades $\eta_1, \eta_2, \ldots \eta_t$ de forma que $\sum_{i=1}^{t} \eta_i = M \implies t = M$ e $\eta_i = 1(\forall i)$. Como $\eta_i = 1(\forall i)$, então $j = k = p = 1$. $\Omega_{i,j}$ será definido com $\eta_i - j = 1 - 1 = 0$, e então :

$$\Omega_{i,j} = \frac{1}{(\eta_i - j)!\widetilde{\bar{\gamma}}_i^{\eta_i - j}} \frac{\partial^{\eta_i - j}}{\partial s^{\eta_i - j}} \left[\prod_{k=1,k\neq i}^{t} \left(\frac{1}{1 + s\widetilde{\bar{\gamma}}_k} \right)^{\eta_k} \right]_{s=-\frac{1}{\widetilde{\bar{\gamma}}_i}} \tag{3.137}$$

$$= \frac{1}{(\eta_i - j)!\bar{\gamma}_i^{\eta_i - j}} \frac{\partial^{\eta_i - j}}{\partial s^{\eta_i - j}} \left[\prod_{k=1,k\neq i}^{t} \left(\frac{1}{1 + s\bar{\gamma}_k} \right)^{\eta_k} \right]_{s=-\frac{1}{\bar{\gamma}_i}}$$

$$= \frac{1}{(0)!\bar{\gamma}_i^{0}} \frac{\partial^{0}}{\partial s^{0}} \left[\prod_{k=1,k\neq i}^{t=M} \left(\frac{1}{1 + s\bar{\gamma}_k} \right)^{\eta_k = 1} \right]_{s=-\frac{1}{\bar{\gamma}_i}}$$

$$= \prod_{k=1,k\neq i}^{M} \left(\frac{1}{1 + s\bar{\gamma}_k} \right)^{1}_{s=-\frac{1}{\bar{\gamma}_i}} = \prod_{k=1,k\neq i}^{M} \left(\frac{1}{1 - \frac{1}{\bar{\gamma}_i}\bar{\gamma}_k} \right)$$

$$= \prod_{k=1,k\neq i}^{M} \left(\frac{\bar{\gamma}_i}{\bar{\gamma}_i - \bar{\gamma}_k} \right) = \prod_{k=1,k\neq i}^{M} \left(\frac{\bar{\gamma}_i}{\bar{\gamma}_i - \bar{\gamma}_k} \right)$$

$$= \bar{\gamma}_i^{M-1} \prod_{k=1,k\neq i}^{M} \left(\frac{1}{\bar{\gamma}_i - \bar{\gamma}_k} \right) = \bar{\gamma}_i^{M-1} \prod_{k=1,k\neq i}^{M} (\bar{\gamma}_i - \bar{\gamma}_k)^{-1}$$

Substituindo $\Omega_{i,j}$ de (3.137) e $j = k = p = 1$ em (3.132), a expressão simplificada para a probabilidade de interrupção de sigilo no caso de sinais interferentes distintos será:

$$P_s(R) = \tag{3.138}$$

$$\sum_{S_k \in S} \alpha_k e^{\frac{-\delta_k(2^R-1)}{\bar{\gamma}_B}} \sum_{f=0}^{\beta_k} \binom{\beta_k}{f} (2^R - 1)^{\beta_k - f} 2^{Rf}$$

$$\times \sum_{i=1}^{M} \bar{\gamma}_i^{M-1} \prod_{k=1,k\neq i}^{M} (\bar{\gamma}_i - \bar{\gamma}_k)^{-1} \sum_{u=0}^{N_E-1} \sum_{q=0}^{u} \frac{\Gamma(1+q)\bar{\gamma}_i^{q}}{(u-q)!q!}$$

$$\times \left(\frac{1}{\bar{\gamma}_E} \right)^{u} \left[\Psi\left(u+f+1, u+f-q, \frac{1}{\bar{\gamma}_i} + \frac{\delta_k \bar{\gamma}_E 2^R}{\bar{\gamma}_B \bar{\gamma}_i} \right) \right.$$

$$\times \Gamma(u+f+1) \left(\frac{\bar{\gamma}_E}{\bar{\gamma}_i} \right)^{u+f} (1+q)$$

$$+ \Psi\left(u+f+1, u+f+1-q, \frac{1}{\bar{\gamma}_i} + \frac{\delta_k \bar{\gamma}_E 2^R}{\bar{\gamma}_B \bar{\gamma}_i} \right)$$

$$\left. \times \Gamma(u+f+1) \left(\frac{\bar{\gamma}_E}{\bar{\gamma}_i} \right)^{u+f} \left(\frac{1}{\bar{\gamma}_i} \right) - \Theta_{1(p=1)} \right]$$

3.2.3 Probabilidade de Interrupção de Sigilo Assintótica

Embora a expressão de forma fechada da probabilidade de interrupção de sigilo seja importante na avaliação do desempenho de sigilo, ela não fornece diretamente muitas

informações relevantes sobre o sistema. Logo, a fim de obter mais informações relevantes sobre o desempenho de sigilo, uma análise assintótica é realizada, e baseada nesta análise a ordem de diversidade e o ganho de *array* do sistema são determinados.

Para a análise assintótica, temos que assumir que $\bar{\gamma}_{\mathrm{B}} \to \infty$ e que $\bar{\gamma}_{\mathrm{B}} \gg \frac{\bar{\gamma}_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{I}}+1}$, ou seja, a SNR média de Bob tende a infinito e que a SNR média de Bob é muito maior que a SINR média de Eve.

Como $\bar{\gamma}_{\mathrm{B}} \to \infty$, antes de calcular a probabilidade de interrupção de sigilo assintótica, teremos que encontrar a cdf assintótica de Bob $F^{\infty}_{\gamma_{\mathrm{B},s}}(x)$.

Precisaremos dos resultados (3.39) e (3.42), que são:

$$\mathscr{L}\{f_{\gamma_{\mathrm{B},k}}(x)\} = (1+s\bar{\gamma}_{\mathrm{B}})^{-L_{\mathrm{B}}} \prod_{l_{\mathrm{B}}=L_{\mathrm{B}}+1}^{N_{\mathrm{B}}} \left(1+\frac{s\bar{\gamma}_{\mathrm{B}} L_{\mathrm{B}}}{l_{\mathrm{B}}}\right)^{-1} \tag{3.39}$$

$$\mathscr{L}\{F_{\gamma_{\mathrm{B},k}}(x)\} = \frac{\mathscr{L}\{f_{\gamma_{\mathrm{B},k}}(x)\}}{s} \tag{3.42}$$

Fazendo $\bar{\gamma}_{\mathrm{B}} \to \infty$ em (3.39) o número 1 somado pode ser descartado pois $\bar{\gamma}_{\mathrm{B}} \gg 1$:

$$\mathscr{L}\{f^{\infty}_{\gamma_{\mathrm{B},k}}(x)\} = (1+s\bar{\gamma}_{\mathrm{B}})^{-L_{\mathrm{B}}} \prod_{l_{\mathrm{B}}=L_{\mathrm{B}}+1}^{N_{\mathrm{B}}} \left(1+\frac{s\bar{\gamma}_{\mathrm{B}} L_{\mathrm{B}}}{l_{\mathrm{B}}}\right)^{-1} \tag{3.139}$$

$$\simeq (s\bar{\gamma}_{\mathrm{B}})^{-L_{\mathrm{B}}} \prod_{l_{\mathrm{B}}=L_{\mathrm{B}}+1}^{N_{\mathrm{B}}} \left(\frac{s\bar{\gamma}_{\mathrm{B}} L_{\mathrm{B}}}{l_{\mathrm{B}}}\right)^{-1}$$

$$\simeq \frac{1}{s^{L_{\mathrm{B}}}\bar{\gamma}_{\mathrm{B}}^{L_{\mathrm{B}}}} \frac{N_{\mathrm{B}}!}{L_{\mathrm{B}}! s^{N_{\mathrm{B}}-L_{\mathrm{B}}} \bar{\gamma}_{\mathrm{B}}^{N_{\mathrm{B}}-L_{\mathrm{B}}} L_{\mathrm{B}}^{N_{\mathrm{B}}-L_{\mathrm{B}}}}$$

$$\simeq \frac{N_{\mathrm{B}}!}{s^{N_{\mathrm{B}}} L_{\mathrm{B}}! \bar{\gamma}_{\mathrm{B}}^{N_{\mathrm{B}}} L_{\mathrm{B}}^{N_{\mathrm{B}}-L_{\mathrm{B}}}}$$

$$\simeq \frac{N_{\mathrm{B}}!}{s^{N_{\mathrm{B}}}} \frac{1}{L_{\mathrm{B}}! \bar{\gamma}_{\mathrm{B}}^{N_{\mathrm{B}}} L_{\mathrm{B}}^{N_{\mathrm{B}}-L_{\mathrm{B}}}}$$

Aplicando o resultado acima em (3.42):

$$\mathscr{L}\{F^{\infty}_{\gamma_{\mathrm{B},k}}(x)\} = \frac{\mathscr{L}\{f^{\infty}_{\gamma_{\mathrm{B},k}}(x)\}}{s} \tag{3.140}$$

$$\simeq \frac{N_{\mathrm{B}}!}{s^{N_{\mathrm{B}}+1}} \frac{1}{L_{\mathrm{B}}!\bar{\gamma}_{\mathrm{B}}^{N_{\mathrm{B}}} L_{\mathrm{B}}^{N_{\mathrm{B}}-L_{\mathrm{B}}}}$$

Aplicando o **Lema 20** e o **Lema 21** em (3.140):

$$\mathscr{L}\{F^{\infty}_{\gamma_{\mathrm{B},k}}(x)\} = \frac{\mathscr{L}\{f^{\infty}_{\gamma_{\mathrm{B},k}}(x)\}}{s} \tag{3.141}$$

$$\simeq \frac{N_{\mathrm{B}}!}{s^{N_{\mathrm{B}}+1}} \frac{1}{L_{\mathrm{B}}!\bar{\gamma}_{\mathrm{B}}^{N_{\mathrm{B}}} L_{\mathrm{B}}^{N_{\mathrm{B}}-L_{\mathrm{B}}}}$$

$$\simeq \mathscr{L}\{x^{N_{\mathrm{B}}}\} \frac{1}{L_{\mathrm{B}}!\bar{\gamma}_{\mathrm{B}}^{N_{\mathrm{B}}} L_{\mathrm{B}}^{N_{\mathrm{B}}-L_{\mathrm{B}}}}$$

$$\simeq \mathscr{L}\left\{ \frac{x^{N_{\mathrm{B}}}}{L_{\mathrm{B}}!\bar{\gamma}_{\mathrm{B}}^{N_{\mathrm{B}}} L_{\mathrm{B}}^{N_{\mathrm{B}}-L_{\mathrm{B}}}} \right\}$$

$$\simeq \mathscr{L}\left\{ \frac{1}{L_{\mathrm{B}}^{N_{\mathrm{B}}-L_{\mathrm{B}}} L_{\mathrm{B}}!} \left(\frac{x}{\bar{\gamma}_{\mathrm{B}}} \right)^{N_{\mathrm{B}}} \right\}$$

Podemos concluir que:

$$\mathscr{L}\{F^{\infty}_{\gamma_{\mathrm{B},k}}(x)\} \simeq \mathscr{L}\left\{ \frac{1}{L_{\mathrm{B}}^{N_{\mathrm{B}}-L_{\mathrm{B}}} L_{\mathrm{B}}!} \left(\frac{x}{\bar{\gamma}_{\mathrm{B}}} \right)^{N_{\mathrm{B}}} \right\} \implies F^{\infty}_{\gamma_{\mathrm{B},k}}(x) \simeq \frac{1}{L_{\mathrm{B}}^{N_{\mathrm{B}}-L_{\mathrm{B}}} L_{\mathrm{B}}!} \left(\frac{x}{\bar{\gamma}_{\mathrm{B}}} \right)^{N_{\mathrm{B}}} \tag{3.142}$$

De (3.53) sabemos que $F_{\gamma_{\mathrm{B},s}}(x) = \left[F_{\gamma_{\mathrm{B},k}}(x)\right]^{N_{\mathrm{A}}}$, logo:

$$F^{\infty}_{\gamma_{\mathrm{B},s}}(x) \simeq \left[F^{\infty}_{\gamma_{\mathrm{B},k}}(x)\right]^{N_{\mathrm{A}}} \simeq \frac{1}{L_{\mathrm{B}}^{N_{\mathrm{A}}(N_{\mathrm{B}}-L_{\mathrm{B}})} (L_{\mathrm{B}}!)^{N_{\mathrm{A}}}} \left(\frac{x}{\bar{\gamma}_{\mathrm{B}}} \right)^{N_{\mathrm{A}}N_{\mathrm{B}}} \tag{3.143}$$

A cdf $F_{\gamma_{\mathrm{B},s}}$ da expressão de forma fechada de $P_s(R)$ em (3.132) deve ser substituida por $F^{\infty}_{\gamma_{\mathrm{B},s}}(x)$ para se chegar à expressão de forma fechada da probabilidade de interrupção de sigilo assintótica $P^{\infty}_s(R)$:

$$P_s^{\infty}(R) \simeq \tag{3.144}$$
$$\sum_{i=1}^{t}\sum_{j=1}^{\eta_i}\Omega_{i,j}\sum_{k=1}^{j}\sum_{p=1}^{k}\sum_{n=0}^{N_{\mathrm{A}}N_{\mathrm{B}}}\sum_{m=0}^{n}\binom{N_{\mathrm{A}}N_{\mathrm{B}}}{n}\binom{n}{m}(-1)^{N_{\mathrm{A}}N_{\mathrm{B}}+j-k-n}$$
$$\times\sum_{u=0}^{N_{\mathrm{E}}-1}\sum_{q=0}^{u}\frac{\Gamma(p+q)\tilde{\bar{\gamma}}_i^{p+q-j-m-u}\bar{\gamma}_E^m}{(j-k)!(k-p)!(u-q)!(p-1)!q!}\times\frac{1}{L_B^{N_A(N_B-L_B)}(L_B!)^{N_A}}$$
$$\times\left[(p+q)\Gamma(m+u+1)\Psi\left(m+u+1,m+u-p-q+1,\frac{1}{\tilde{\bar{\gamma}}_i}\right)\right.$$
$$\left.+\Gamma(m+u+1)\frac{1}{\tilde{\bar{\gamma}}_i}\Psi\left(m+u+1,m+u-p-q+2,\frac{1}{\tilde{\bar{\gamma}}_i}\right)-\Theta_2\right]\frac{1}{\bar{\gamma}_B^{N_{\mathrm{A}}N_{\mathrm{B}}}}$$

Onde Θ_2 é:

$$\Theta_2=\begin{cases}\Psi\left(m+u,m+u-p-q+1,\dfrac{1}{\tilde{\bar{\gamma}}_i}\right)u\Gamma(m+u), & u\neq 0\\ 0, & u=0\end{cases} \tag{3.145}$$

Como vimos na seção (2.10.4), a expressão para a probabilidade de interrupção de sigilo assintótica pode ser lida da seguinte maneira generalizada:

$$P_s^{\infty}(R)=G_{\mathrm{A}}\left(\bar{\gamma}_{\mathrm{B}}\right)^{-G_{\mathrm{D}}}+o\left(\bar{\gamma}_{\mathrm{B}}^{-G_{\mathrm{D}}}\right) \tag{3.146}$$

$$P_s^{\infty}(R)\simeq G_{\mathrm{A}}\left(\bar{\gamma}_{\mathrm{B}}\right)^{-G_{\mathrm{D}}} \tag{3.147}$$

Onde G_{A} e G_{D} simbolizam, respectivamente, o ganho de *array* e o ganho de diversidade para o sistema.

3.2.3.1 Ganho de Diversidade

Comparando (3.147) com (3.144) podemos concluir que o ganho de diversidade será:

$$G_{\mathrm{D}}=N_{\mathrm{A}}N_{\mathrm{B}} \tag{3.148}$$

Este resultado contrasta com a conclusão de (COSTA *et al.*, 2016), no qual um nó espião também sofre interferência de M sinais mas não é acometido por ruído e o ganho de diversidade foi $G_{\mathrm{D}} = min(M, N_{\mathrm{A}} N_{\mathrm{B}})$. Logo, quando se considera ruído e interferência ao mesmo tempo em Eve, o ganho de diversidade fica limitado pelo número de antenas em Alice e Bob, independentemente do número de sinais interferentes em Eve.

Curiosamente, o ganho de diversidade é o mesmo em (YANG *et al.*, 2013c), no qual o esquema GSC é empregado em Bob, mas Eve fica sujeita à apenas ruído. Isso nos permite concluir que a interferência em Eve não altera o ganho de diversidade do sistema, tendo efeito apenas no ganho de *array* do sistema.

3.2.3.2 Ganho de Array

Novamente, comparando (3.147) com (3.144) podemos concluir que o ganho de *array* será:

$$
\begin{aligned}
G_{\mathrm{A}} = & \qquad (3.149)\\
&\sum_{i=1}^{t}\sum_{j=1}^{\eta_i}\Omega_{i,j}\sum_{k=1}^{j}\sum_{p=1}^{k}\sum_{n=0}^{N_{\mathrm{A}}N_{\mathrm{B}}}\sum_{m=0}^{n}\binom{N_{\mathrm{A}}N_{\mathrm{B}}}{n}\binom{n}{m}(-1)^{N_{\mathrm{A}}N_{\mathrm{B}}+j-k-n}\\
&\times\sum_{u=0}^{N_{\mathrm{E}}-1}\sum_{q=0}^{u}\frac{\Gamma(p+q)\tilde{\bar{\gamma}}_i^{p+q-j-m-u}\bar{\gamma}_E^{m}}{(j-k)!(k-p)!(u-q)!(p-1)!q!}\times\frac{1}{L_B^{N_A(N_B-L_B)}(L_B!)^{N_A}}\\
&\times\left[(p+q)\Gamma(m+u+1)\Psi\left(m+u+1,m+u-p-q+1,\frac{1}{\tilde{\bar{\gamma}}_i}\right)\right.\\
&\left.+\Gamma(m+u+1)\frac{1}{\tilde{\bar{\gamma}}_i}\Psi\left(m+u+1,m+u-p-q+2,\frac{1}{\tilde{\bar{\gamma}}_i}\right)-\Theta_2\right]
\end{aligned}
$$

3.2.4 Taxa de Sigilo Não Nula

A taxa de sigilo não nula é definida como a probabilidade de $R_S > 0$. Representando a probabilidade da capacidade de sigilo ser diferente de zero, ou seja, do canal entre Alice e Bob ser melhor que o canal entre Alice e Eve garantindo assim o sigilo da comunicação. Logo, temos que:

$$P_r(R_S > 0) = \Pr(R_{\mathrm{B},s} > R_{\mathrm{E},s}) = \Pr(\gamma_{\mathrm{B},s} > \Upsilon_{\mathrm{E},s}) \tag{3.150}$$
$$= \int_0^{\infty} \int_0^{x} f_{\gamma_{\mathrm{B},s}}(x) f_{\Upsilon_{\mathrm{E},s}}(y) dy dx$$
$$= \int_0^{\infty} \int_0^{x} f_{\gamma_{\mathrm{B},s}}(x) f_{\frac{\gamma_{\mathrm{E},s}}{\eta+1}}(y) dy dx$$

A expressão exata de $P_r(R_S > 0)$ é derivada ao se substituir $f_{\gamma_{\mathrm{B},s}}(x)$ e $f_{\Upsilon_{\mathrm{E},s}}(y)$ por suas expressões de forma fechada já demonstradas anteriormente e utilizando a **Definição 23** da função de Tricomi. Resultando em:

$$P_r(R_S>0)= \tag{3.151}$$

$$N_A\sum_{S_k\in S'}\alpha_k\sum_{l_B=1}^{L_B}\frac{\varepsilon_{l_B}(l_B-1)}{(l_B-1)!}\sum_{i=1}^{t}\sum_{j=1}^{\eta_i}\Omega_{i,j}\sum_{k=1}^{j}\sum_{p=1}^{k}(-1)^{j-k}\sum_{u=0}^{N_E-1}\sum_{q=0}^{u}\Bigg\{$$

$$\left(\frac{1}{\bar{\gamma}_E}\right)^u\frac{\Gamma(p+q)\widetilde{\bar{\gamma}}_i^{p+q-j}}{(j-k)!(k-p)!(u-q)!(p-1)!q!}\Bigg[\left(\frac{1+\delta_k}{\bar{\gamma}_B}\right)^{1-\beta_k-l_B}\Gamma(-1+\beta_k+l_B)\Delta(u)$$

$$-\left(\frac{\bar{\gamma}_E}{\widetilde{\bar{\gamma}}_i}\right)^{\beta_k+l_B+u-1}\Gamma(\beta_k+l_B+u-1)$$

$$\times\Psi\left(\beta_k+l_B+u-1,\beta_k+l_B+u-p-q,\frac{\delta_k\bar{\gamma}_E}{\bar{\gamma}_B\widetilde{\bar{\gamma}}_i}+\frac{\bar{\gamma}_E}{\bar{\gamma}_B\widetilde{\bar{\gamma}}_i}+\frac{1}{\widetilde{\bar{\gamma}}_i}\right)\Bigg]\Bigg\}$$

$$+N_A\sum_{S_k\in S'}\alpha_k\sum_{l_B=1}^{L_B}\frac{-\varepsilon_{l_B}}{(l_B-1)!\bar{\gamma}_B}\sum_{i=1}^{t}\sum_{j=1}^{\eta_i}\Omega_{i,j}\sum_{k=1}^{j}\sum_{p=1}^{k}(-1)^{j-k}\sum_{u=0}^{N_E-1}\sum_{q=0}^{u}\Bigg\{$$

$$\left(\frac{1}{\bar{\gamma}_E}\right)^u\frac{\Gamma(p+q)\widetilde{\bar{\gamma}}_i^{p+q-j}}{(j-k)!(k-p)!(u-q)!(p-1)!q!}\Bigg[\left(\frac{1+\delta_k}{\bar{\gamma}_B}\right)^{-\beta_k-l_B}\Gamma(\beta_k+l_B)\Delta(u)$$

$$-\left(\frac{\bar{\gamma}_E}{\widetilde{\bar{\gamma}}_i}\right)^{\beta_k+l_B+u}\Gamma(\beta_k+l_B+u)$$

$$\times\Psi\left(\beta_k+l_B+u,1+\beta_k+l_B+u-p-q,\frac{\delta_k\bar{\gamma}_E}{\bar{\gamma}_B\widetilde{\bar{\gamma}}_i}+\frac{\bar{\gamma}_E}{\bar{\gamma}_B\widetilde{\bar{\gamma}}_i}+\frac{1}{\widetilde{\bar{\gamma}}_i}\right)\Bigg]\Bigg\}$$

$$+N_A\sum_{S_k\in S'}\alpha_k\sum_{l_B=L_B+1}^{N_B}\frac{-l_B\varepsilon_{l_B}}{L_B\bar{\gamma}_B}\sum_{i=1}^{t}\sum_{j=1}^{\eta_i}\Omega_{i,j}\sum_{k=1}^{j}\sum_{p=1}^{k}(-1)^{j-k}\sum_{u=0}^{N_E-1}\sum_{q=0}^{u}\Bigg\{$$

$$\left(\frac{1}{\bar{\gamma}_E}\right)^u\frac{\Gamma(p+q)\widetilde{\bar{\gamma}}_i^{p+q-j}}{(j-k)!(k-p)!(u-q)!(p-1)!q!}\Bigg[\left(\frac{l_B+L_B\delta_k}{L_B\bar{\gamma}_B}\right)^{-1-\beta_k}\Gamma(1+\beta_k)\Delta(u)$$

$$-\left(\frac{\bar{\gamma}_E}{\widetilde{\bar{\gamma}}_i}\right)^{\beta_k+u+1}\Gamma(\beta_k+u+1)$$

$$\times\Psi\left(\beta_k+u+1,\beta_k+u+2-p-q,\frac{\delta_k\bar{\gamma}_E}{\bar{\gamma}_B\widetilde{\bar{\gamma}}_i}+\frac{l_B\bar{\gamma}_E}{L_B\bar{\gamma}_B\widetilde{\bar{\gamma}}_i}+\frac{1}{\widetilde{\bar{\gamma}}_i}\right)\Bigg]\Bigg\}$$

$$\text{Onde }\Delta(u)=\begin{cases}0, & u\neq 0\\ 1, & u=0\end{cases}$$

4 RESULTADOS NUMÉRICOS E DISCUSSÕES

4.1 Introdução

O objetivo deste capítulo é apresentar resultados numéricos relevantes na avaliação do desempenho de sigilo do sistema em estudo. Essa avaliação de desempenho será realizada através de simulações dos valores das diferentes métricas de sigilo que foram apresentadas nos capítulos anteriores para se observar e entender como essas métricas se comportam com a variação de parâmetros sistêmicos fundamentais como M, N_{A}, N_{B}, N_{E}, L_{B}, $\bar{\gamma}_i$, e $\bar{\gamma}_{\mathrm{B}}$

O sistema deste trabalho e as métricas de sigilo também foram simuladas numericamente através do método de Monte Carlo. O objetivo disso é comparar e validar os valores simulados pelo método de Monte Carlo com os valores gerados pelas expressões analíticas das métricas encontradas no capítulo anterior.

Todas as métricas de desempenho de sigilo apresentadas no capítulo anterior serão observadas de alguma maneira nas figuras das simulações. As métricas são:

- Probabilidade de interrupção de sigilo($P_s(R)$)
- Probabilidade de interrupção de sigilo assintótica($P_s^{\infty}(R)$)
  - Ganho de diversidade(G_{D})
  - Ganho de *array*(G_{A})
- Taxa de sigilo não nula($P_r(R_S > 0)$)

Mas apenas algumas dessas métricas serão vistas e analisadas diretamente, enquanto outras serão vistas e analisadas de maneira indireta a partir dos resultados.

O ganho de diversidade é a única métrica que não é simulada diretamente, pois é vista e analisada a partir do coeficiente angular(ou inclinação) das retas representantes da probabilidade de interrupção de sigilo assintótica quando plotadas em função da SNR média de Bob($\bar{\gamma}_{\mathrm{B}}$).

A probabilidade de interrupção de sigilo e a taxa de sigilo não nula são as únicas métricas de desempenho de sigilo que são simuladas simultaneamente pelo método de Monte Carlo e pela expressão analítica. O objetivo disso é validar os resultados.

Os valores simulados pelo método de Monte Carlo serão representados por pontos e os valores simulados à partir das expressões analíticas serão representados por curvas. Com excessão do plot do ganho de *array*, onde os pontos representam também os valores gerados pela expressão analítica.

Múltiplos parâmetros sistémicos serão variados, mas haverá um parâmetro de variação principal que representará o eixo das abscissas dos gráficos. Esse parâmetro principal é o que terá variação mais contínua e servirá de base para observação do comportamento das métricas de desempenho de sigilo cujos valores estarão no eixo das ordenadas.

Outros parâmetros sistêmicos serão variados ao se plotar múltiplas curvas em cada figura, assim pode-se analisar ao mesmo tempo os efeitos da variação do parâmetro sistêmico principal(variação representada no eixo x) e dos outros parâmetros sistêmicos(variação representa uma curva diferente).

Para a probabilidade de interrupção de sigilo e para a taxa de sigilo não nula o parâmetro sistêmico de variação principal será $\bar{\gamma}_{\mathrm{B}}$(que é a SNR média de Bob). Já para o ganho de *array* o parâmetro sistêmico de variação principal será N_{A}

O parâmetro sistêmico $\bar{\gamma}_{\mathrm{B}}$, que é a SNR média de Bob, sempre será representado em dB no eixo das abscissas dos gráficos. Já N_{A} ficará original, ou seja, em escala linear.

Em todos os plots o eixo das ordenadas está em escala logarítmica na base 10.

Sem perda de generalidade, se assumiu $R = 1$ em todas as simulações.

4.2 Algoritmos

Definições para os algoritmos:

A variável q representa as iterações da simulação de Monte Carlo. E o valor N representa o número total de iterações para cada valor de $\bar{\gamma}_{\mathrm{B}}$.

$\bar{\gamma}_B$ representa o vetor com todos os valores de $\bar{\gamma}_{\mathrm{B}}$ que serão simulados.

A função RANDN gera variáveis pseudoaleatórias de distribuição Gaussiana com média nula e variância unitária, $N(0,1)$, através do método de Monte Carlo.

A função TIMES faz a multiplicação elemento por elemento entre dois vetores.

A função LENGTH mede o número de elementos de um vetor.

A função SORT(. , "decrescente") ordena os elementos de um vetor de maneira decrescente.

A função MAX seleciona o maior de dois valores.

A função return representa o *output* do algoritmo.

As variáveis com primeiro símbolo em negrito representam vetores, e a variáveis que não estiverem em negrito representam escalares.

Os algoritmos que geram os resultados simulados estão descritos à seguir:

Algoritmo 1 Simulação da Probabilidade de Interrupção de Sigilo, $P_s(R)$, pelo método de Monte Carlo

for $p = 1, \ldots, \text{LENGTH}(\bar{\gamma}_B)$ **do**
  contador $\leftarrow 0$
  $\bar{\gamma}_B \leftarrow \bar{\gamma}_B[p]$
  for $q = 1, \ldots, N$ **do**

    $\mathbf{h}_{\text{AE},s} \leftarrow \{\text{RANDN}(1, N_E) + j\text{RANDN}(1, N_E)\}\sqrt{\frac{1}{2}}$
    $\gamma_{\text{E},s} \leftarrow \bar{\gamma}_{\text{E}}||\mathbf{h}_{\text{AE},s}||^2$
    $T \leftarrow \text{LENGTH}(\bar{\gamma}_i)$
    $\mathbf{h}_i \leftarrow \{\text{RANDN}(1, T) + j\text{RANDN}(1, T)\}\sqrt{\frac{1}{2}}$
    $\mathbf{h}_i^{'} \leftarrow \text{TIMES}(\mathbf{h}_i, \sqrt{\bar{\gamma}_i})$
    $\gamma_1 \leftarrow \left|\left|\mathbf{h}_i^{'}\right|\right|^2$
    $\Upsilon_{\text{E},s} \leftarrow \frac{\gamma_{\text{E},s}}{\gamma_1 + 1}$

    for $v = 1, \ldots, N_A$ **do**
      $\mathbf{h}_{\text{AB},k} \leftarrow \{\text{RANDN}(1, N_B) + j\text{RANDN}(1, N_B)\}\sqrt{\frac{1}{2}}$
      $\mathbf{h} \leftarrow \text{SORT}(\mathbf{h}_{\text{AB},k}, \text{"decrescente"})$
      for $z = 1, \ldots, L_B$ **do**
        $\mathbf{h}^{'}[z] \leftarrow \mathbf{h}[z]$
      end for
      $\gamma_{\text{B},k}[v] \leftarrow \bar{\gamma}_{\text{B}}\left|\left|\mathbf{h}^{'}\right|\right|^2$
    end for
    $\gamma_{\text{B},s} \leftarrow \text{MAX}(\gamma_{\text{B},k})$

    $R_{\text{B},s} \leftarrow \log_2(1 + \gamma_{\text{B},s})$
    $R_{\text{E},s} \leftarrow \log_2(1 + \Upsilon_{\text{E},s})$
    $R_S \leftarrow \text{MAX}(R_{\text{B},s} - R_{\text{E},s}\ ,\ 0)$

    if $R_S < R$ **then**
      contador $\leftarrow$ contador $+ 1$
    end if

  end for
  $\mathbf{P}_s(R)[p] \leftarrow$ contador$/N$
end for
return $\mathbf{P}_s(R)$

Algoritmo 2 Simulação da Taxa de Sigilo Não Nula, $P_r(R_S > 0)$, pelo método de Monte Carlo

for $p = 1, \ldots, \text{LENGTH}(\bar{\gamma}_B)$ **do**
  $\bar{\gamma}_B \leftarrow \bar{\gamma}_B[p]$
  for $q = 1, \ldots, N$ **do**

    $\mathbf{h}_{\text{AE},s} \leftarrow \{\text{RANDN}(1, N_E) + j\text{RANDN}(1, N_E)\}\sqrt{\frac{1}{2}}$
    $\gamma_{\text{E},s} \leftarrow \bar{\gamma}_{\text{E}}||\mathbf{h}_{\text{AE},s}||^2$
    $T \leftarrow \text{LENGTH}(\bar{\gamma}_i)$
    $\mathbf{h}_i \leftarrow \{\text{RANDN}(1, T) + j\text{RANDN}(1, T)\}\sqrt{\frac{1}{2}}$
    $\mathbf{h}_i^{'} \leftarrow \text{TIMES}(\mathbf{h}_i\,, \sqrt{\bar{\gamma}_i})$
    $\gamma_{\text{I}} \leftarrow \left|\left|\mathbf{h}_i^{'}\right|\right|^2$
    $\Upsilon_{\text{E},s} \leftarrow \frac{\gamma_{\text{E},s}}{\gamma_{\text{I}}+1}$

    for $v = 1, \ldots, N_A$ **do**
      $\mathbf{h}_{\text{AB},k} \leftarrow \{\text{RANDN}(1, N_B) + j\text{RANDN}(1, N_B)\}\sqrt{\frac{1}{2}}$
      $\mathbf{h} \leftarrow \text{SORT}(\mathbf{h}_{\text{AB},k}\,, \text{"decrescente"})$
      for $z = 1, \ldots, L_B$ **do**
        $\mathbf{h}^{'}[z] \leftarrow \mathbf{h}[z]$
      end for
      $\gamma_{\text{B},k}[v] \leftarrow \bar{\gamma}_{\text{B}}\left|\left|\mathbf{h}^{'}\right|\right|^2$
    end for
    $\gamma_{\text{B},s} \leftarrow \text{MAX}(\gamma_{\text{B},k})$

    $R_{\text{B},s} \leftarrow \log_2(1 + \gamma_{\text{B},s})$
    $R_{\text{E},s} \leftarrow \log_2(1 + \Upsilon_{\text{E},s})$
    $R_S \leftarrow \text{MAX}(R_{\text{B},s} - R_{\text{E},s}\ ,\ 0)$

    if $R_S > 0$ **then**
      contador $\leftarrow$ contador $+ 1$
    end if

  end for
  $\mathbf{P}_r(R_S > 0)[p] \leftarrow \text{contador}/N$
end for
return $\mathbf{P}_r(R_S > 0)$

Algoritmo 3 Simulação da Expressão Analítica da Probabilidade de Interrupção de Sigilo Assintótica $P_s^{\infty}(R)$

1: **for** $p = 1, \ldots, \text{LENGTH}(\bar{\gamma}_B)$ **do**
2: $\quad \mathbf{P}_s^{\infty}(R)[p] \leftarrow P_s^{\infty}(R)\Big|_{\bar{\gamma}_B \leftarrow \bar{\gamma}_B[p]}$
3: **end for**
4: **return** $\mathbf{P}_s^{\infty}(R)$

Algoritmo 4 Simulação da Expressão Analítica da Probabilidade de Interrupção de Sigilo $P_s(R)$

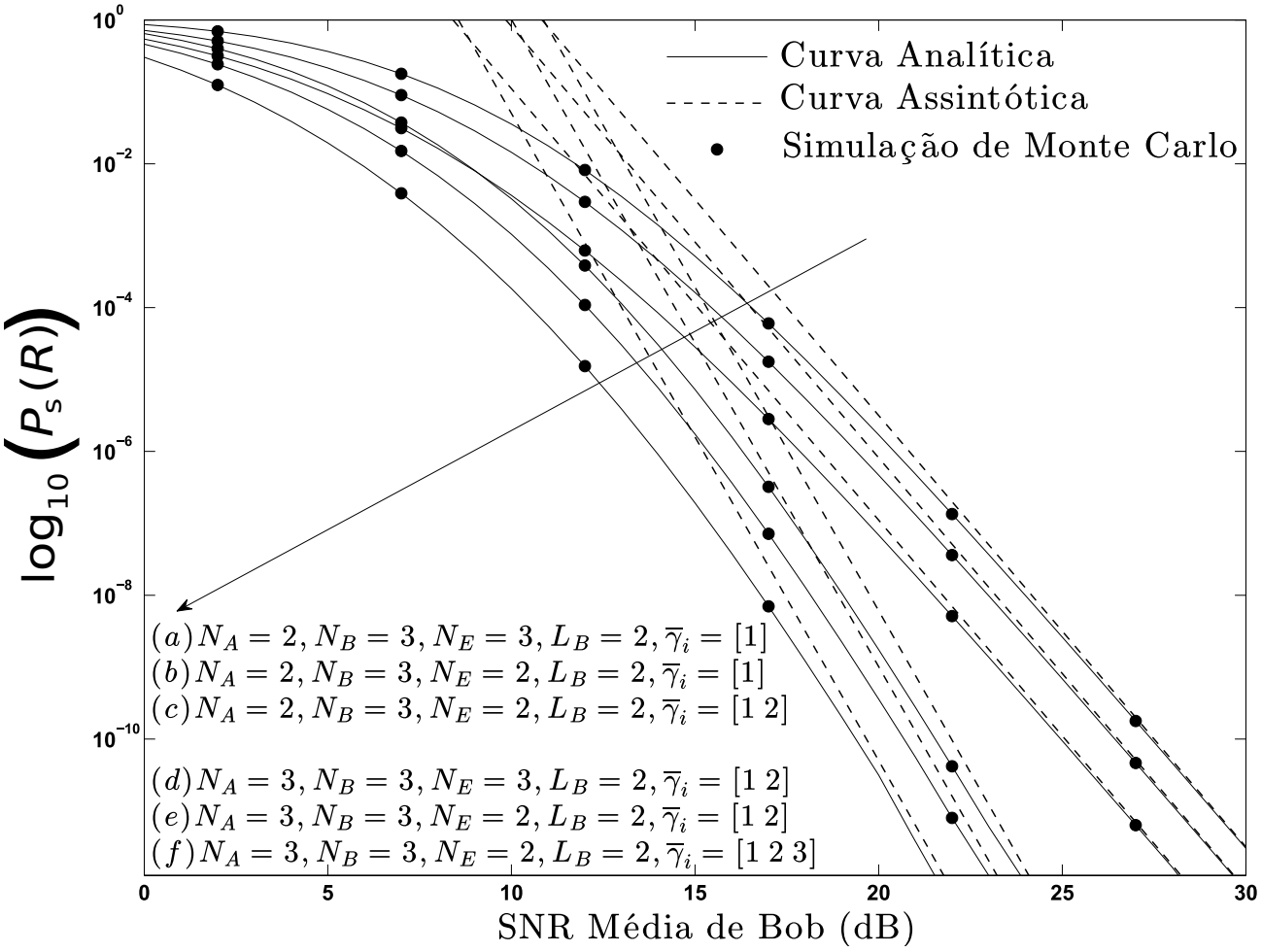
for $p = 1, \ldots,$ LENGTH$(\bar{\gamma}_B)$ **do**
$\quad \mathbf{P}_s(R)[p] \leftarrow P_s(R)\Big|_{\bar{\gamma}_B \leftarrow \bar{\gamma}_B[p]}$
end for
return $\mathbf{P}_s(R)$

Algoritmo 5 Simulação da Expressão Analítica da Taxa de Sigilo Não Nula $P_r(R_S > 0)$

for $p = 1, \ldots,$ LENGTH$(\bar{\gamma}_B)$ **do**
$\quad \mathbf{P}_r(R_S > 0)[p] \leftarrow P_r(R_S > 0)\Big|_{\bar{\gamma}_B \leftarrow \bar{\gamma}_B[p]}$
end for
return $\mathbf{P}_r(R_S > 0)$

4.3 Apresentação dos resultados numéricos

Figura 14 – Probabilidade de interrupção de sigilo versus a SNR média de Bob considerando o esquema GSC em Bob. Considerações gerais: $N_{\mathrm{B}} = 3$; $L_{\mathrm{B}} = 2$; $\bar{\gamma}_{\mathrm{E}} = 4$ dB; $R = 1$; sinais interferentes distintos.



Fonte: elaborado pelo autor (2017).

A Figura 4.1 retrata:

- Curva analítica da probabilidade de interrupção de sigilo($P_s(R)$ no eixo das ordenadas) versus a SNR média de Bob($\bar{\gamma}_{\mathrm{B}}$ no eixo das abscissas)
- Curva analítica da probabilidade de interrupção de sigilo assintótica($P_s^{\infty}(R)$ no eixo das ordenadas) versus a SNR média de Bob($\bar{\gamma}_{\mathrm{B}}$ no eixo das abscissas)
- Simulação de Monte Carlo da probabilidade de interrupção de sigilo(eixo das ordenadas) versus a SNR média de Bob($\bar{\gamma}_{\mathrm{B}}$ no eixo das abscissas)

O objetivo da figura 4.1 é observar os efeitos da variação dos seguintes parâmetros sistêmicos N_{A}, N_{E} e $\bar{\gamma}_i$ no caso GSC puro. GSC puro significa que não recai no caso SC($L_{\mathrm{B}} = 1$) ou MRC($L_{\mathrm{B}} = N_{\mathrm{B}}$), assim teremos que fixar um $N_{\mathrm{B}} \geq 3$ e um $2 \leq L_{\mathrm{B}} \leq N_{\mathrm{B}} - 1$ que neste caso

escolhemos $N_{\mathrm{B}} = 3$ e $L_{\mathrm{B}} = 2$.

Observamos na figura três fatos previstos na teoria:

- A curva analítica da probabilidade de interrupção de sigilo e os pontos simulados pelo método de Monte Carlo da probabilidade de interrupção de sigilo coincidem. O que é esperado, já que ambos valores representam exatamente a mesma métrica e apenas são calculados por métodos diferentes.
- A curva analítica da probabilidade de interrupção de sigilo assintótica e a curva analítica da probabilidade de interrupção de sigilo coincidem para SNR média de Bob alta. Isso é previsto teoricamente, pois $P_s^{\infty}(R)$ é definida fazendo $\bar{\gamma}_{\mathrm{B}} \to \infty$ em $P_s(R)$.
- Podemos observar o ganho de diversidade(G_{D}) através da inclinação da curva analítica da probabilidade de interrupção de sigilo assintótica($P_s^{\infty}(R)$). Observamos então que há dois *clusters* de curvas na figura, o *cluster* formado pelo conjunto {(a), (b), (c)} e o *cluster* formado pelo conjunto {(d), (e), (f)}. Como a inclinação de todas a curvas no conjunto {(a), (b), (c)} são iguais, concluímos que possuem o mesmo ganho de diversidade e isso é previsto teoricamente, pois para esse conjunto $G_{\mathrm{D}} = N_{\mathrm{A}}N_{\mathrm{B}} = 2 \times 3 = 6$ e no caso do conjunto {(d), (e), (f)} teremos $G_{\mathrm{D}} = N_{\mathrm{A}}N_{\mathrm{B}} = 3 \times 3 = 9$. Este item será provado à seguir.

De (3.148), provamos que o valor do ganho de diversidade é $G_{\mathrm{D}} = N_{\mathrm{A}}N_{\mathrm{B}}$. E de (3.147), concluimos que $P_s^{\infty}(R) \simeq G_{\mathrm{A}} \left(\bar{\gamma}_{\mathrm{B}}\right)^{-G_{\mathrm{D}}}$. Como a figura representa $\bar{\gamma}_{\mathrm{B}}$ em dB e $P_s(R)$ em escala logarítmica na base 10, teremos que:

$$P_s^{\infty}(R) = G_{\mathrm{A}} \left(\bar{\gamma}_{\mathrm{B}}\right)^{-G_{\mathrm{D}}} \tag{4.1}$$

Onde G_{A} e G_{D} simbolizam, respectivamente, o ganho de *array* e o ganho de diversidade para o sistema. Logo, $P_s^{\infty}(R)$ em escala logarítmica no eixo y será $y' = \log_{10}\{P_s^{\infty}(R)\}$ e $\bar{\gamma}_{\mathrm{B}}$ em escala dB no eixo x será $x' = 10\log_{10}\{\bar{\gamma}_{\mathrm{B}}\}$. Como a função $y'(x')$ é a representação de $P_s^{\infty}(R)$ na figura, teremos que :

$$
\begin{aligned}
y' &= \log_{10}\{P_s^{\infty}(R)\} \qquad (4.2)\\
&= \log_{10}\{G_{\mathrm{A}}\,(\bar{\gamma}_{\mathrm{B}})^{-G_{\mathrm{D}}}\}\\
&= -G_{\mathrm{D}}\log_{10}\{G_{\mathrm{A}}\bar{\gamma}_{\mathrm{B}}\}\\
&= -G_{\mathrm{D}}\left[\log_{10}\{G_{\mathrm{A}}\}+\log_{10}\{\bar{\gamma}_{\mathrm{B}}\}\right]\\
&= -G_{\mathrm{D}}\left[\log_{10}\{G_{\mathrm{A}}\}+\frac{x'}{10}\right]\\
&= -\frac{G_{\mathrm{D}}}{10}x' - G_{\mathrm{D}}\log_{10}\{G_{\mathrm{A}}\}\\
&= \left(-\frac{G_{\mathrm{D}}}{10}\right)x' - G_{\mathrm{D}}\log_{10}\{G_{\mathrm{A}}\}
\end{aligned}
$$

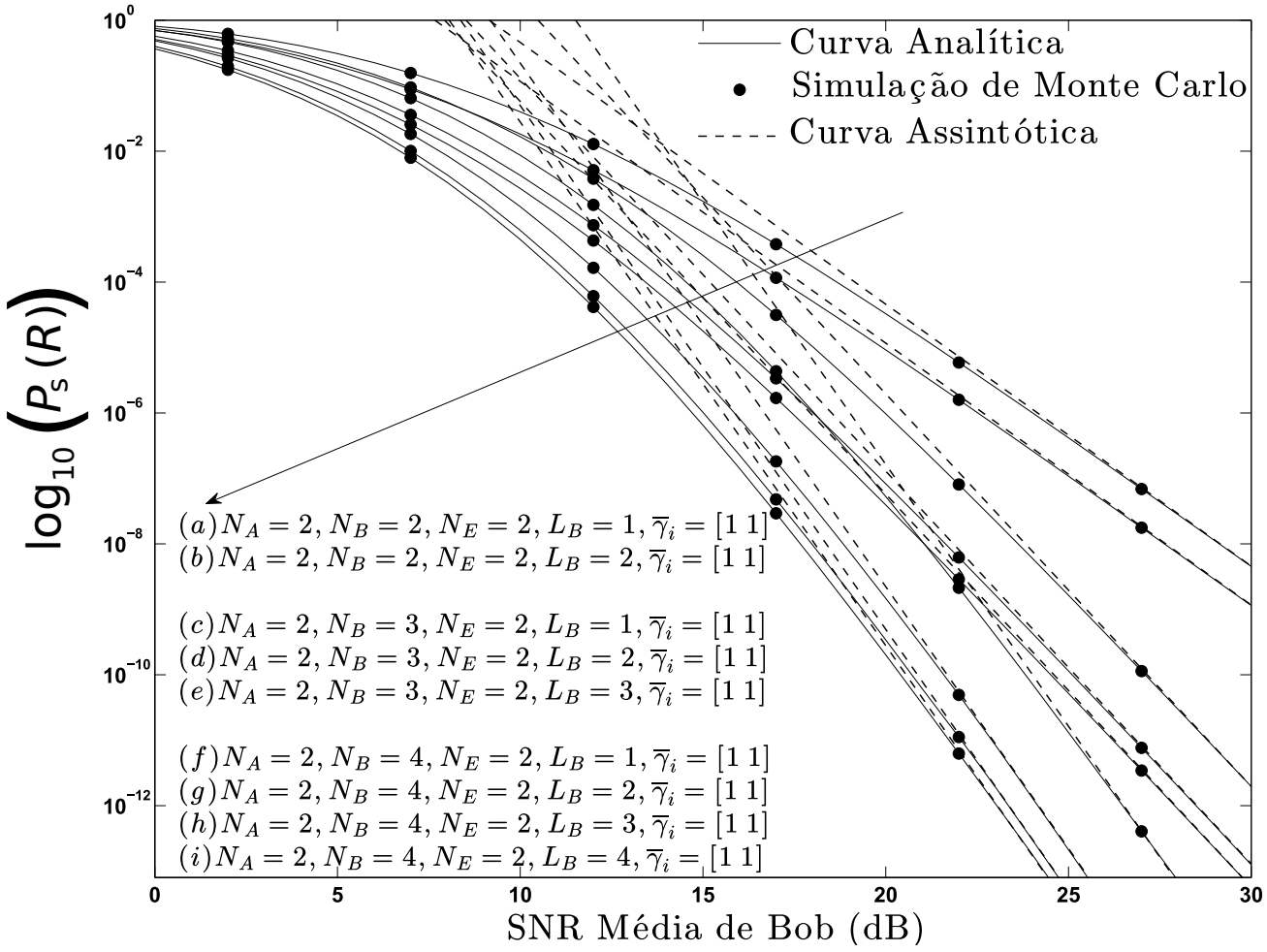
Logo, $y'(x')$ é uma reta de coeficiente angular igual à $-\frac{G_{\mathrm{D}}}{10}$. Concluimos que na figura, $-\frac{G_{\mathrm{D}}}{10}$ é o coeficiente angular que indica a inclinação da retas representantes da probabilidade de interrupção de sigilo assintótica. Assim, as retas que tiverem a mesma inclinação representarão o mesmo ganhos de diversidade, pois $-\frac{G_{\mathrm{D}}}{10}$ é uma função direta de G_{D} somente.

Voltando à análise dos resultado. Os parâmetros sistêmicos variados são N_{A}, N_{E} e $\bar{\gamma}_i$. N_{A} varia entre 2 e 3. N_{E} também varia entre 2 e 3. $\bar{\gamma}_i$ varia de $[1]$(onde $M=1$) para $[1 \quad 2]$(onde $M=2$) e para $[1 \quad 2 \quad 3]$(onde $M=3$).

Podemos concluir, ao analisar a figura 4.1, que os parâmetros sistêmicos variados terão diferentes pesos na melhoria do desempenho de sigilo do sistema. Definindo "Peso$(\,.\,)$"como o operador que representa o quanto um parâmetro vai afetar o desempenho de sigilo do sistema, poderemos então escrever que:

$$\text{Peso(aumento de } N_{\mathrm{A}}) > \text{Peso(aumento de } M \text{ de } \bar{\gamma}_i) > \text{Peso(diminuição de } N_{\mathrm{E}})$$

Figura 15 – Probabilidade de interrupção de sigilo versus a SNR média de Bob considerando o esquema GSC em Bob. Considerações gerais: $N_{\mathrm{A}} = 2$; $N_{\mathrm{E}} = 2$; $\bar{\gamma}_{\mathrm{E}} = 4$ dB; $R = 1$; sinais interferentes iguais.



Fonte: elaborado pelo autor (2017).

A Figura 4.2 retrata:

- Curva analítica da probabilidade de interrupção de sigilo($P_s(R)$ no eixo das ordenadas) versus a SNR média de Bob($\bar{\gamma}_{\mathrm{B}}$ no eixo das abscissas)
- Curva analítica da probabilidade de interrupção de sigilo assintótica($P_s^{\infty}(R)$ no eixo das ordenadas) versus a SNR média de Bob($\bar{\gamma}_{\mathrm{B}}$ no eixo das abscissas)
- Simulação de Monte Carlo da probabilidade de interrupção de sigilo(eixo das ordenadas) versus a SNR média de Bob($\bar{\gamma}_{\mathrm{B}}$ no eixo das abscissas)

O objetivo da figura 4.2 é observar os efeitos da variação do parâmetro sistêmico L_{B} ao variar seu valor do caso SC($L_{\mathrm{B}} = 1$) até o(s) caso(s) GSC puro($2 \leq L_{\mathrm{B}} \leq N_{\mathrm{B}} - 1$) e daí até o caso MRC($L_{\mathrm{B}} = N_{\mathrm{B}}$), para tanto, se mantém todos os outros parâmetros contantes e varia-se apenas $1 \leq L_{\mathrm{B}} \leq N_{\mathrm{B}}$ para cada valor de N_{B}. Neste caso escolhemos $N_{\mathrm{B}} = 2$, $N_{\mathrm{B}} = 3$ e $N_{\mathrm{B}} = 4$.

Observamos na figura três fatos previstos na teoria:

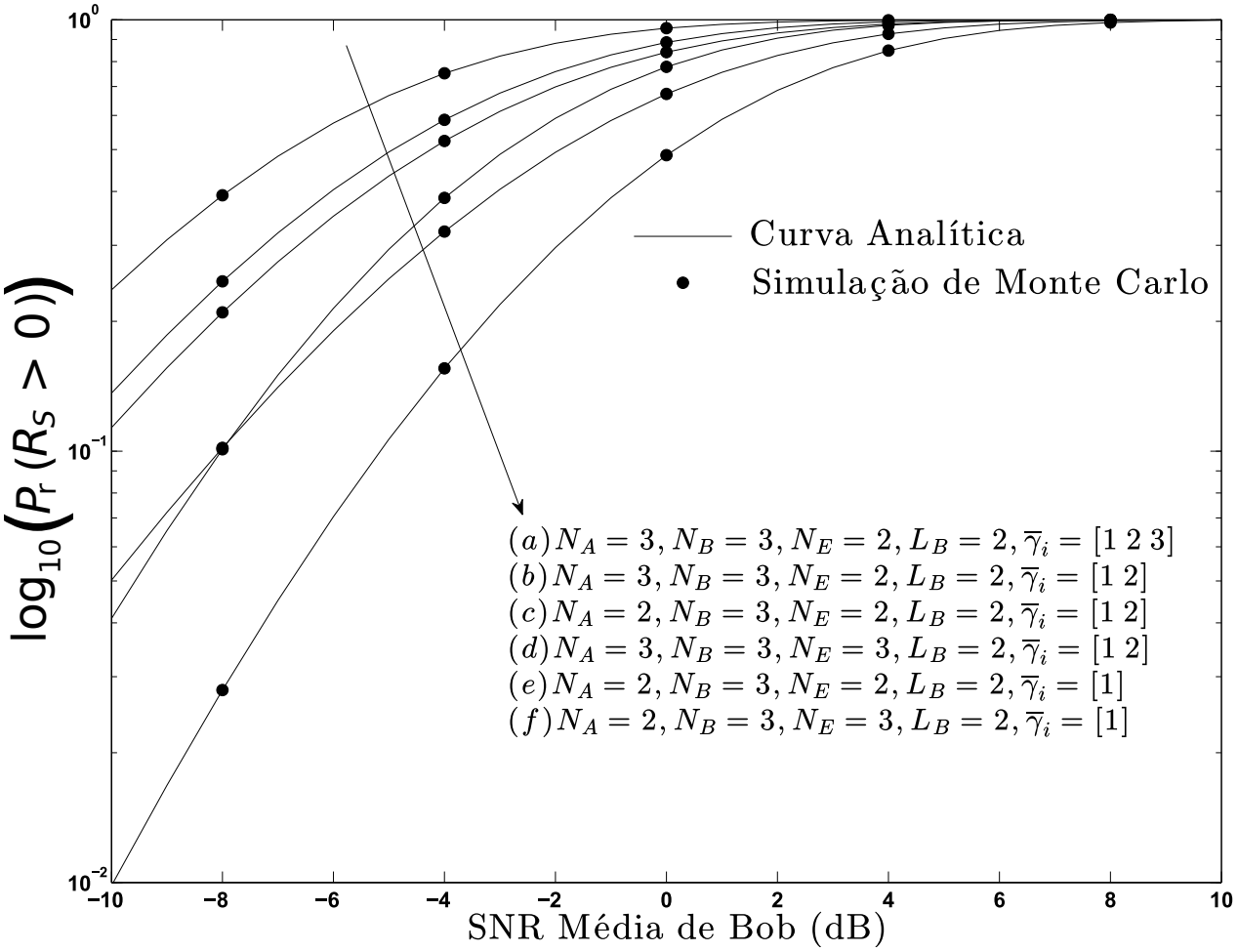
– A curva analítica da probabilidade de interrupção de sigilo e os pontos simulados pelo método de Monte Carlo da probabilidade de interrupção de sigilo coincidem. O que é esperado, já que ambos valores representam exatamente a mesma métrica e apenas são calculados por métodos diferentes.
– A curva analítica da probabilidade de interrupção de sigilo assintótica e a curva analítica da probabilidade de interrupção de sigilo coincidem para SNR média de Bob alta. Isso é previsto teoricamente, pois $P_s^{\infty}(R)$ é definida fazendo $\bar{\gamma}_{\mathrm{B}} \to \infty$ em $P_s(R)$.
– Podemos observar o ganho de diversidade(G_{D}) através da inclinação da curva analítica da probabilidade de interrupção de sigilo assintótica($P_s^{\infty}(R)$). Observamos então que há três *clusters* de curvas na figura, o *cluster* formado pelo conjunto {(a), (b)} , o *cluster* formado pelo conjunto {(c), (d), (e)} e o *cluster* formado pelo conjunto {(f), (g), (h), (i)}. Como a inclinação de todas a curvas em cada conjunto são iguais, concluímos que possuem o mesmo ganho de diversidade e isso é previsto teoricamente, pois para esses conjuntos teremos respectivamente: $G_{\mathrm{D}} = N_{\mathrm{A}}N_{\mathrm{B}} = 2 \times 2 = 4$, $G_{\mathrm{D}} = N_{\mathrm{A}}N_{\mathrm{B}} = 2 \times 3 = 6$ e $G_{\mathrm{D}} = N_{\mathrm{A}}N_{\mathrm{B}} = 2 \times 4 = 8$.

Os parâmetros sistêmicos variados são L_{B} e N_{B}. N_{B} varia entre 2, 3 e 4, enquanto $1 \leq L_{\mathrm{B}} \leq N_{\mathrm{B}}$.

Podemos concluir, ao analisar a figura 4.2, que os parâmetros sistêmicos variados terão diferentes pesos na melhoria do desempenho de sigilo do sistema. Utilizando "Peso(.)"definido anteriormente, poderemos escrever que:

$$\text{Peso(aumento de } N_{\mathrm{B}}) > \text{Peso(aumento de } L_{\mathrm{B}})$$

Figura 16 – Taxa de sigilo não nula versus a SNR média de Bob considerando o esquema GSC em Bob. Considerações gerais: $N_{\mathrm{B}} = 3$; $L_{\mathrm{B}} = 2$; $\bar{\gamma}_{\mathrm{E}} = 4$ dB; $R = 1$; sinais interferentes distintos.



Fonte: elaborado pelo autor (2017).

A Figura 4.3 retrata:

- Curva analítica da taxa de sigilo não nula($P_r(R_S > 0)$ no eixo das ordenadas) versus a SNR média de Bob($\bar{\gamma}_{\mathrm{B}}$ no eixo das abscissas)
- Simulação de Monte Carlo da taxa de sigilo não nula(eixo das ordenadas) versus a SNR média de Bob($\bar{\gamma}_{\mathrm{B}}$ no eixo das abscissas)

O objetivo da figura 4.3 é o mesmo objetivo da figura 4.1. A variação e os valores dos parâmetros sistêmicos são os mesmos da figura 4.1, o que muda é que neste caso o desempenho de sigilo será medido através da taxa de sigilo não nula em vez da probabilidade de interrupção de sigilo.

Relembrando, o objetivo da figura é observar os efeitos da variação dos seguintes parâmetros sistêmicos N_{A}, N_{E} e $\bar{\gamma}_i$ no caso GSC puro. GSC puro significa que não recai no caso SC($L_{\mathrm{B}} = 1$) ou MRC($L_{\mathrm{B}} = N_{\mathrm{B}}$), assim teremos que fixar um $N_{\mathrm{B}} \geq 3$ e um $2 \leq L_{\mathrm{B}} \leq N_{\mathrm{B}} - 1$

que neste caso escolhemos $N_{\mathrm{B}} = 3$ e $L_{\mathrm{B}} = 2$.

Observamos na figura dois fatos previstos na teoria:

- A curva analítica da taxa de sigilo não nula e os pontos simulados pelo método de Monte Carlo da probabilidade de interrupção de sigilo coincidem. O que é esperado, já que ambos valores representam exatamente a mesma métrica e apenas são calculados por métodos diferentes.
- Podemos observar que a taxa de sigilo não nula sempre tende à 1 para valores altos da SNR média de Bob. Isso é previsto teoricamente, pois de (3.150) sabemos que $P_r(R_S > 0) = \Pr(\gamma_{\mathrm{B},s} > \Upsilon_{\mathrm{E},s})$ e que $\bar{\gamma}_{\mathrm{B}} \to \infty \implies \gamma_{\mathrm{B},s} \to \infty$, logo teremos que $\gamma_{\mathrm{B},s} \to \infty \implies P_r(R_S > 0) \to \Pr(\infty > \Upsilon_{\mathrm{E},s}) = 1$ pois $\Upsilon_{\mathrm{E},s}$ fica constante.

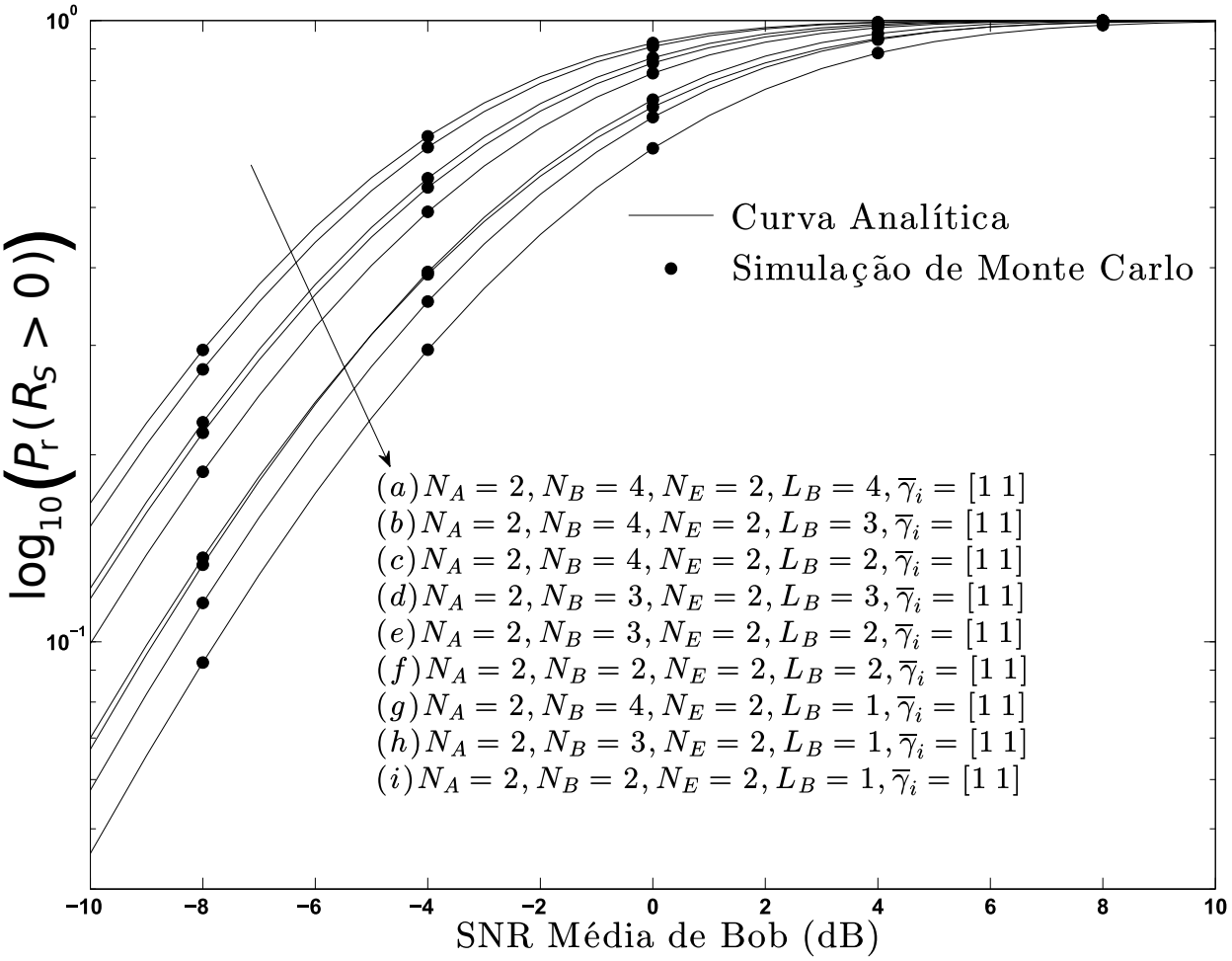
Os parâmetros sistêmicos variados são N_{A}, N_{E} e $\bar{\gamma}_i$. N_{A} varia entre 2 e 3. N_{E} também varia entre 2 e 3. $\bar{\gamma}_i$ varia de $[1]$(onde $M = 1$) para $[1 \quad 2]$(onde $M = 2$) e para $[1 \quad 2 \quad 3]$(onde $M = 3$).

Podemos concluir, ao analisar a figura 4.2, que os parâmetros sistêmicos variados terão diferentes pesos na melhoria do desempenho de sigilo do sistema. Utilizando "Peso(.)"definido anteriormente, poderemos escrever que:

$$\text{Peso}(\text{diminuição de } N_{\mathrm{E}}) > \text{Peso}(\text{aumento de } M \text{ de } \bar{\gamma}_i) > \text{Peso}(\text{aumento de } N_{\mathrm{A}})$$

Observamos que diminuição de N_{E} trocou de lugar com aumento de N_{A} na comparação com o mesmo resultado na figura 4.1. Podemos interpretar que o efeito da diminuição de N_{E} em diminuir $\Upsilon_{\mathrm{E},s}$ é maior do que o efeito do aumento de N_{A} em aumentar $\gamma_{\mathrm{B},s}$. Assim, $P_r(R_S > 0) = \Pr(\gamma_{\mathrm{B},s} > \Upsilon_{\mathrm{E},s})$ vai aumentar mais com a diminuição de N_{E} do que com o aumento de N_{A}. Isso acontece porque N_{A} tem um efeito menor no valor de $\gamma_{\mathrm{B},s}$ devido à técnica TAS empregada em Alice. Como TAS não existe para Eve, o efeito de N_{E} em $\Upsilon_{\mathrm{E},s}$ é direto e consequentemente maior.

Figura 17 – Taxa de sigilo não nula versus a SNR média de Bob considerando o esquema GSC em Bob. Considerações gerais: $N_{\mathrm{A}} = 2$; $N_{\mathrm{E}} = 2$; $\bar{\gamma}_{\mathrm{E}} = 4$ dB; $R = 1$; sinais interferentes iguais.



Fonte: elaborado pelo autor (2017).

A Figura 4.4 retrata:

– Curva analítica da taxa de sigilo não nula($P_r(R_S > 0)$ no eixo das ordenadas) versus a SNR média de Bob($\bar{\gamma}_{\mathrm{B}}$ no eixo das abscissas)
– Simulação de Monte Carlo da taxa de sigilo não nula(eixo das ordenadas) versus a SNR média de Bob($\bar{\gamma}_{\mathrm{B}}$ no eixo das abscissas)

O objetivo da figura 4.4 é o mesmo objetivo da figura 4.2. A variação e os valores dos parâmetros sistêmicos são os mesmos da figura 4.2, o que muda é que neste caso o desempenho de sigilo será medido através da taxa de sigilo não nula em vez da probabilidade de interrupção de sigilo.

Relembrando, o objetivo da figura é observar os efeitos da variação do parâmetro sistêmico L_{B} ao variar seu valor do caso SC($L_{\mathrm{B}} = 1$) até o(s) caso(s) GSC puro($2 \leq L_{\mathrm{B}} \leq N_{\mathrm{B}} - 1$) e daí até o caso MRC($L_{\mathrm{B}} = N_{\mathrm{B}}$), para tanto, se mantém todos os outros parâmetros contantes

e varia-se apenas $1 \leq L_B \leq N_B$ para cada valor de N_B. Neste caso escolhemos $N_B = 2$, $N_B = 3$ e $N_B = 4$.

Observamos na figura dois fatos previstos na teoria:

– A curva analítica da taxa de sigilo não nula e os pontos simulados pelo método de Monte Carlo da probabilidade de interrupção de sigilo coincidem. O que é esperado, já que ambos valores representam exatamente a mesma métrica e apenas são calculados por métodos diferentes.
– Podemos observar que a taxa de sigilo não nula sempre tende à 1 para valores altos da SNR média de Bob. Isso é previsto teoricamente, pois de (3.142) sabemos que $P_r(R_S > 0) = \Pr(\gamma_{B,s} > \Upsilon_{E,s})$ e que $\bar{\gamma}_B \to \infty \implies \gamma_{B,s} \to \infty$, logo teremos que $\gamma_{B,s} \to \infty \implies P_r(R_S > 0) \to \Pr(\infty > \Upsilon_{E,s}) = 1$ pois $\Upsilon_{E,s}$ fica constante.

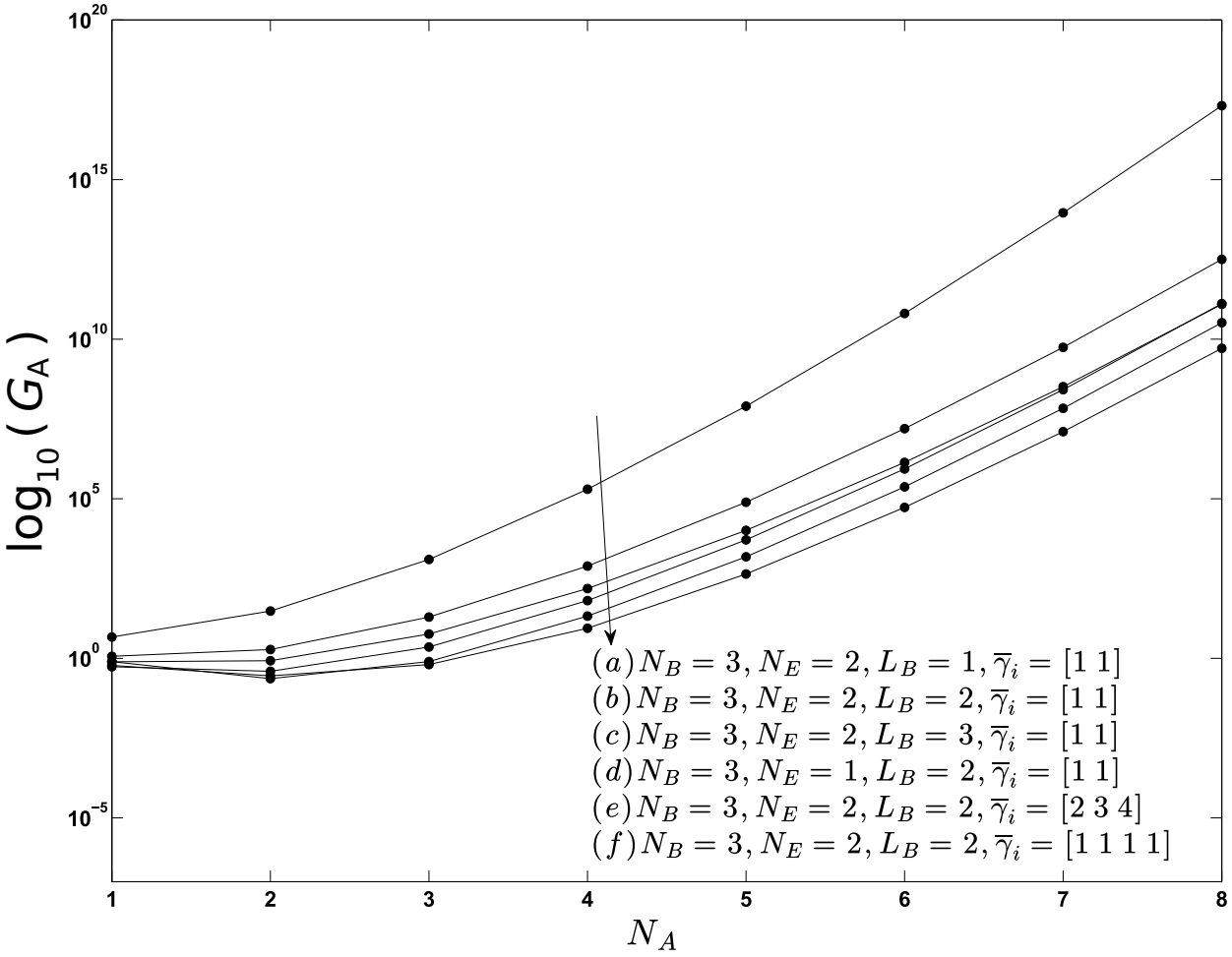
Os parâmetros sistêmicos variados são L_B e N_B. N_B varia entre 2, 3 e 4, enquanto $1 \leq L_B \leq N_B$.

Podemos concluir, ao analisar a figura 4.4, que os parâmetros sistêmicos variados terão diferentes pesos na melhoria do desempenho de sigilo do sistema. Utilizando "Peso(.)"definido anteriormente, poderemos escrever que:

$$\text{Peso}(\text{aumento de } N_B) \simeq \text{Peso}(\text{aumento de } L_B)$$

Concluímos isso pois pela figura 4.4, na qual a performance do sistema pela métrica analisada vai depender diretamente do produto $N_B \times L_B$. As curvas que possuem esse produto maior sempre são superiores, e no caso de igualdade como do par de curvas {(f), (g)} onde para (f) $N_B \times L_B = 2 \times 2 = 4$ e para (g) $N_B \times L_B = 4 \times 1 = 4$ implica nas curvas bem mais próximas, tanto que chegam a coincidir em alguns ponto.

Figura 18 – Ganho de *array* versus o número de antenas em Alice(N_A).
Considerações gerais: $N_{\mathrm{B}} = 3$; $\bar{\gamma}_E = -5$ dB.



Fonte: elaborado pelo autor (2017).

A Figura 4.5 retrata:

– Curva analítica do ganho de *array*(G_{A} no eixo das ordenadas) versus o número de antenas em Alice(N_{A} no eixo das abscissas)

O objetivo da figura 4.5 é observar os efeitos da variação dos seguintes parâmetros sistêmicos N_{A}(eixo x), L_{B}, N_{E} e $\bar{\gamma}_i$, enquanto N_{B} se mantém constante. Variando $1 \leq L_{\mathrm{B}} \leq N_{\mathrm{B}}$, N_{E} entre 1 e 2, $\bar{\gamma}_i$ igual à [1 1]($M = 2$ com sinais interferentes iguais), [2 3 4]($M = 3$ com sinais interferentes distintos) ou [1 1 1 1]($M = 4$ com sinais interferentes iguais). Onde $N_{\mathrm{B}} = 3$ é constante, para que através da variação de $1 \leq L_{\mathrm{B}} \leq N_{\mathrm{B}}$ se possa definir os casos SC, GSC puro e MRC.

Observamos pela figura que o ganho de *array* aumenta com o aumento de N_{A}. Isso é previsto pela expressão já calculada de G_{A}.

Podemos concluir, ao analisar a figura 4.5, que os parâmetros sistêmicos vari-

ados terão diferentes pesos na melhoria do desempenho de sigilo do sistema. Utilizando "Peso(.)"definido anteriormente, poderemos escrever que:

$$\text{Peso}(\text{aumento de } N_{\text{A}}) \gg \text{Peso}(\text{diminuição de } M \text{ de } \bar{\gamma}_l)$$
$$> \text{Peso}(\text{aumento de } N_{\text{E}}) > \text{Peso}(\text{diminuição de } L_{\text{B}})$$

Logo, concluímos que quanto melhor a situação for para Eve(M e L_{B} mais baixos, e N_{E} mais alto) maior será o efeito do aumento de N_{A} no aumento de G_{A}. E quanto pior for a situação for para Eve(M e L_{B} mais altos, e N_{E} mais baixo) o efeito de N_{A} no aumento de G_{A} será mais brando. A conclusão geral que tiramos desses fatos é que caso Eve esteja em posição muito favorável, uma boa estratégia de sigilo é aumentar o número de antenas em Alice(N_{A}) em vez de alterar os outros parâmetros sistêmicos(M, L_{B} e N_{E}).

5 CONCLUSÕES E PERSPECTIVAS

Nesta dissertação, propusemos um cenário com TAS no transmissor, GSC no receptor legítimo e sinais interferentes no espião com o objetivo de investigar a melhoria do desempenho de sigilo através de melhorias da segurança na camada física em canais *wiretap* com MIMO. Derivamos expressões de forma fechada para a probabilidade de interrupção de sigilo e para a taxa de sigilo não nula. Com base na probabilidade de interrupção de sigilo os ganhos de *array* e de diversidade foram determinados após a realização de uma análise assintótica. Resultados numéricos foram apresentados para demonstrar o efeito de parâmetros sistêmicos fundamentais(M, N_{A}, N_{B}, N_{E}, L_{B}, $\bar{\gamma}_i$ e $\bar{\gamma}_{\mathrm{B}}$) no desempenho de sigilo. *Trade-offs* entre esses parâmetros e as diferentes métricas de desempenho de sigilo foram analisados. Todos esse resultados foram validados através de simulações pelo método de Monte Carlo.

Resumindo, os objetivos gerais alcançados nesta dissertação foram:

- Descrever o cenário do sistema.
- Derivar expressões de forma fechada para a probabilidade de interrupção de sigilo e para a taxa de sigilo não nula.
- Realizar uma análise assintótica com base na probabilidade de interrupção de sigilo para encontrar a probabilidade de interrupção de sigilo assintótica e os ganhos de *array* e de diversidade.
- Demonstrar o efeito de parâmetros sistêmicos fundamentais no desempenho de sigilo através de alguns resultados numéricos representativos.
- Corroborar a análise proposta neste trabalho através de simulações de Monte Carlo.

Vamos recapitular como esses objetivos foram alcançados ao longo dos capítulos deste trabalho.

No Capítulo 1, os objetivos e métodos gerais desta dissertação foram expostos e explicados.

No Capítulo 2, apresentamos os conceitos teóricos que serviram de base para o entendimento geral desta dissertação e para o desenvolvimento das demonstrações e análises dos capítulos subsequentes.

No Capítulo 3, o modelo do sistema *wiretap*/MIMO com TAS, GSC e sinais interferentes foi apresentado. Os diferentes canais envolvidos foram modelados matematicamente e expressões de forma fechada que os descrevem estatisticamente foram derivadas, e baseando-se nessas expressões as diferentes métricas de desempenho de sigilo foram derivadas em expressões

de forma fechada, as quais foram: Probabilidade de Interrupção de Sigilo, Probabilidade de Interrupção de Sigilo Assintótica, Taxa de Sigilo não Nula, Ganho de Diversidade e Ganho de *Array*.

No Capítulo 4, resultados numéricos foram apresentados a fim de validar as expressões de forma fechada que foram derivadas no Capítulo 3 e se analisou os efeitos de parâmetros sistêmicos fundamentais(M, N_{A}, N_{B}, N_{E}, L_{B}, $\bar{\gamma}_i$ e $\bar{\gamma}_{\mathrm{B}}$) no desempenho de sigilo do sistema. Esse resultados foram corroborados através de simulações de Monte Carlo.

Os resultados numéricos obtidos no Capítulo 4 confirmam as análises do Capítulo 3 através de algumas observações no comportamento das curvas que condizem com o comportamento previsto na teoria. Importantes *trade-offs* entre os parâmetros sistêmicos e seus efeitos no desempenho de sigilo foram concluídos através das inequações com o operador "Peso(.)"na análise de cada uma das figuras. Cada uma das inequações com "Peso(.)"nos permitiu aprender qual a melhor maneira de se definir os parâmetros sistêmicos em diferentes situações para obter a melhor performance do sistema. Relembrando de forma mais detalhada:

No cenário da figura 4.1:

$$\text{Peso}(\text{aumento de } N_{\mathrm{A}}) > \text{Peso}(\text{aumento de } M \text{ de } \bar{\gamma}_i) > \text{Peso}(\text{diminuição de } N_{\mathrm{E}})$$

No cenário da figura 4.2:

$$\text{Peso}(\text{aumento de } N_{\mathrm{B}}) > \text{Peso}(\text{aumento de } L_{\mathrm{B}})$$

No cenário da figura 4.3:

$$\text{Peso}(\text{diminuição de } N_{\mathrm{E}}) > \text{Peso}(\text{aumento de } M \text{ de } \bar{\gamma}_i) > \text{Peso}(\text{aumento de } N_{\mathrm{A}})$$

No cenário da figura 4.4:

$$\text{Peso}(\text{aumento de } N_{\mathrm{B}}) \simeq \text{Peso}(\text{aumento de } L_{\mathrm{B}})$$

No cenário da figura 4.5:

$$\text{Peso}(\text{aumento de } N_{\mathrm{A}}) \gg \text{Peso}(\text{diminuição de } M \text{ de } \bar{\gamma}_i)$$
$$> \text{Peso}(\text{aumento de } N_{\mathrm{E}}) > \text{Peso}(\text{diminuição de } L_{\mathrm{B}})$$

Essas cinco expressões levam à seguinte conclusão:

Em um sistema real com cenário semelhante ao da figura específica, o ideal é sempre considerar alterar primeiramente os parâmetros mais à esquerda(com maior peso) para melhorar

o desempenho de sigilo do sistema. Caso não seja possível alterar o parâmetro de maior peso, deve-se considera os outros na sequência do de maior peso até o de menor peso.

Em conclusão, as análises teóricas e de simulação do esquema proposto permitiram a obtenção de *insights* importantes em como melhor planejar o sistema de comunicação para garantir a segurança na camada física e consequentemente o sigilo no processo de comunicação.

Segurança na camada física é um campo de pesquisa emergente onde há espaço para inovações. A seguir, listamos possíveis mudanças e generalizações do cenário desta dissertação para desenvolvimento em possíveis futuros trabalhos nesta mesma linha de pesquisa:

- Generalizar o modelo de desvanecimento do canal. Do modelo *Rayleigh* para o modelo *Nakagami-m*.
- Considerar CSI imperfeita no transmissor para gerar resultados e análises mais realistas.
- Adotar o esquema GSC no nó espião como forma de generalização do esquema MRC já empregado no cenário deste trabalho.
- Considerar um cenário com o uso de *relays* e técnicas de comunicações cooperativas.
- Adotar outros esquemas de transmissão, como códigos espaço-temporais ortogonais(ST, do inglês, *Space-Time codes*) ou *beamforming*.
- Considerar múltiplos nós espiões.

REFERÊNCIAS

ALOUINI, M. S.; SIMON, M. K. An mgf-based performance analysis of generalized selection combining over rayleigh fading channels. **IEEE Trans. Commun.**, IEEE, v. 48, p. 401–415, 2000.

ALVES, H.; SOUZA, R. D.; DEBBAH, M.; BENNIS, M. Performance of transmit antenna selection physical layer security schemes. **IEEE Signal Process. Lett.**, IEEE, v. 19, n. 6, p. 372–375, 2012.

COSTA, D. B. d.; FERDINAND, N. S.; DIAS, U. S.; SOUSA, R. T. d.; LATVA-AHO, M. Secrecy outage performance of mimo wiretap channels with multiple jamming signals. **Journal Commun. Inf. Syst.**, v. 31, n. 1, p. 30–40, 2016.

CSISZAR, I.; KORNER, J. Broadcast channels with confidential messages. **IEEE Trans. Inf. Theory**, IEEE, v. 3, n. 24, p. 339—-348, 1978.

DING, X.; SONG, T.; ZOU, Y.; CHEN, X. Security-reliability tradeoff for friendly jammer assisted user-pair selection in the face of multiple eavesdroppers,. **IEEE Access**, IEEE, PP, n. 99, p. 1–1, 2016.

FERDINAND, N. S.; COSTA, D. B. d.; LATVA-AHO, M. Effects of outdated csi on the secrecy performance of miso wiretap channels with transmit antenna selection. **IEEE Commun. Lett.**, IEEE, v. 17, n. 5, p. 864–867, 2013.

HAN, Z.; MARINA, N.; DEBBAH, M.; HJøRUNGNES, A. Physical layer security game: interaction between source, eavesdropper, and friendly jammer. **Journal Wireless Commun. and Net.**, v. 2009, p. 1–10, 2009.

HUANG, J.; SWINDLEHURST, A. L. Cooperative jamming for secure communications in mimo relay networks. **IEEE Trans. Signal Proces.**, IEEE, v. 59, p. 4871–4884, 2011.

LEUNG-YAN-CHEONG, S. K.; HELLMAN, M. E. Gaussian wiretap channel. **IEEE Trans. Inf. Theory**, IEEE, v. 4, n. 24, p. 451–456, 1978.

NABAR, R. U.; BöLCSKEI, H.; PAULRAJ, A. J. Outage performance of space-time block codes for generalized mimo channels. **European Wireless 2002 Conference**, 2002.

NILSSON, J. W.; RIDEL, S. A. **Electric Circuits**. [*S. l.*]: Prentice-Hall, 2000.

SCHNEIER, B. Cryptographic design vulnerabilities. **Computer**, Computer, v. 31, n. 9, p. 29–33, 1998.

SHANNON, C. A mathematical theory of communication. **Bell System Technical Journal**, Bell System, v. 3, p. 379–423, 623–656, 1948.

SHANNON, C. Communication theory of secrecy systems. **Bell System Technical Journal**, Bell System, v. 28, p. 656–715, 1949.

SHIU, D.; FOSCHINI, G. J.; GANS, M. J.; KAHN, J. M. Fading correlation and its effect on the capacity of multi-element antenna systems. **IEEE Trans. Commun.**, v. 48, p. 502–512, 2000.

SILVA, E.; SANTOS, A. D.; ALBINI, L. C. P.; LIMA, M. N. e. Identity-based key management in mobile ad hoc networks: Techniques and applications. **IEEE Trans. Wireless Commun.**, IEEE, v. 15, n. 5, p. 46–52, 2008.

TEKIN, E.; YENER, A. The general gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming. **IEEE Trans. Inform. Theory**, IEEE, v. 54, p. 2735–2751, 2008.

THOMAS, J. A.; COVER, T. M. **Digital Communication**. 2. ed. [*S. l.*]: Wiley-Interscience, 2006.

TSE, D.; VISWANATH, P. **Fundamentals of Wireless Communications**. 4. ed. [*S. l.*: *s. n.*], 2004.

WYNER, A. The wire-tap channel. **Bell Syst. Technol. J**, Bell System, v. 54, n. 8, p. 1355–1387, 1975.

YANG, N.; SURAWEERA, H. A.; COLLINGS, I. B.; YUEN, C. Physical layer security of tas/mrc with antenna correlation. **IEEE Trans. Inf. Forensics Security**, IEEE, v. 8, n. 1, p. 254–259, 2013.

YANG, N.; YEOH, P.; ELKASHLAN, M.; SCHOBER, R.; COLLINGS, I. Transmit antenna selection for security enhancement in mimo wiretap channels. **IEEE Trans. Commun.**, IEEE, v. 61, n. 1, p. 144–154, 2013.

YANG, N.; YEOH, P. L.; ELKASHLAN, M.; SCHOBER, R.; YUAN, J. Mimo wiretap channels: Secure transmission using transmit antenna selection and receive generalized selection combining. **IEEE Commun. Lett.**, IEEE, v. 17, n. 9, p. 1754–1757, 2013.

ZHENG, L.; TSE, D. N. C. Diversity and multiplexing: A fundamental tradeoff in multiple-antenna channels. **IEEE Transactions on Information Theory**, IEEE, v. 49, p. 1073–1096, 2003.

ZHOU, X.; MCKAY, M. Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation. **Vehicular Technology, IEEE Transactions on**, IEEE, v. 59, n. 8, p. 3831–3842, 2010.